發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96149789

※ 申請日期：2007 年 12 月 24 日

※IPC 分類：

~~G06F 21/00 (2006.01)~~

G06F 9/50 (2006.01)

G06F 21/51 (2006.01)

G06F 21/53 (2006.01)

一、發明名稱：（中文/英文）

保護作業系統資源

PROTECTING OPERATING-SYSTEM RESOURCES

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商．微軟公司

Microsoft Corporation

代表人：（中文/英文）

艾芊那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：（中文/英文）

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國　籍：（中文/英文）

美國/USA

三、發明人：（共 7 人）

姓　名：（中文/英文）

1.費爾德史考特 A/FIELD, SCOTT A.

2.巴克布蘭登/BAKER, BRANDON

3.特洛特艾瑞克/TRAUT, ERIC

4.辛哈蘇亞栩/SINHA, SUYASH

5.剛古理喬伊/GANGULY, JOY

6.福滋福瑞思/FOLTZ, FORREST

7.卡特勒大衛/CUTLER, DAVID

國　籍：(中文/英文)

1.英國/UK

2.美國/USA

3.美國/USA

4.印度/INDIA

5.印度/INDIA

6.美國/USA

7.美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

美國；2007 年 1 月 25 日；11/627,314

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

103年6月30日修正本

全本

五、中文發明摘要：

本發明揭示一種工具，其能致使一保護代理器(protection agent)可從一作業系統特權模式無法存取之記憶體中決定一作業系統之一或多數資源是否已被修改。在一些實例中，此等工具可致使該保護代理器常駐在一虛擬機器監視器內。在其他實例中，該等工具可致使該保護代理器常駐在由虛擬機器監視器提供之不同虛擬分區內。藉由在該作業系統特權模式之外操作，該保護代理器更不易遭受在作業系統特權模式內操作的實體攻擊。

六、英文發明摘要：

This document describes tools capable of enabling a protection agent to determine, from memory inaccessible from an operating-system privilege mode, Whether one or more resources of an operating system have been modified. In some instances, these tools may enable the protection agent to reside withina virtual machine monitor. In other instances, the tools may enable the protection agent to reside within a distinct virtual partition provided by the virtual machine monitor. By operating outsidc of the operating-system privilege mode, the protection agent may be less vulnerable to attacks by entities operating within the operating-system privilege mode.

七、指定代表圖：

(一)、本案指定代表圖為：第(1)圖。

(二)、本代表圖之元件代表符號簡單說明：

100	範例性環境	102	計算裝置
104	處理器	106	電腦可讀媒體
108	虛擬機器監控器	110	第一虛擬分區
112	第二虛擬分區	114	作業系統
116	使用者應用	118	作業系統服務
120	作業系統資源	122	有毒軟體
124	虛擬機器監視器	126	作業系統特權模式
128	使用者特權模式	130	第二虛擬分區特權模式
132	保護代理商特權模式	134	保護代理器
136	資源識別符	138	工具性質規定檔
140	保護代理器服務	142	保護代理器
144	保護代理器	146	管理器

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

九、發明說明：

【發明所屬之技術領域】

本發明係有關於保護作業系統資源。

【先前技術】

計算裝置內之處理器通常包括特權及非特權模式。在特權模式中執行之軟體大體上係能執行由處理器支援的每一指令。典型地，作業系統核心在特權模式內執行，其有時稱為「第0級(Ring 0)」、「監督器模式」或「核心模式」。

相反地，一些在計算裝置上執行之軟體可能受限制僅在非特權模式中執行。此模式大體上允許該軟體執行處理器之指令的一子集。一作業系統因而可使用非特權模式來限制在此模式中執行之軟體的活動。例如，軟體可受限於計算裝置之記憶體的一特殊子集。此非特權模式有時係稱為「第3級(Ring 3)」或「使用者模式」。一般而言，計算裝置使用者應用在此非特權模式中操作。

若一軟體應用在此非特權模式中操作時，該應用可能請求存取非特權模式無法直接存取之記憶體的一部分。該應用可能(例如)欲在記憶體之此部分中施行一操作，例如「產生一新檔案」。此請求通常係透過一呼叫閘控或其他系統呼叫指令選路，其將此非特權碼轉換成特權模式碼。此轉換確保該非特權模式無法直接存取被指定僅特權模式可存取的記憶體。

依據此等模式，一惡意碼之作者可能存取特權模式及

安裝有毒軟體，其改變計算裝置的行為。此有毒軟體(例如)可變更檔案位置、隱藏檔案、修改檔案、改變鍵次或類似者。一些此有毒軟體可包含一「根套件(rootkit)」，其不僅改變計算裝置之行為且亦將其本身隱藏在特權模式之記憶體內。在計算裝置上執行之防毒應用可能因此無法發現此隱藏根套件，因而允許有毒軟體持續其惡意行為。此外，此有毒軟體可修補(patch)作業系統之內建保護系統，如以下討論。

有毒軟體作者可存取特權模式且依各種方式將有毒軟體載於計算裝置上，包括藉由欺騙計算裝置使用者以無知地將有毒軟體安裝至使用者本身之計算裝置上。結果，目前作業系統通常使用一或更多保護系統來偵測此有毒軟體。此等保護系統大體上會監控某些重要作業系統資源以偵測對於此等資源之任何變化。若此一保護系統偵測此一改變，則保護系統可決定該特定資源已被有毒軟體傳染。此等保護系統亦可將目前常駐於非特權模式之記憶體中的一列表提供予使用者之防毒應用。當然，若有毒軟體成功隱藏，則其將不會出現在所提供之列表上。再者，若有毒軟體成功修補保護系統，則該保護系統可能無法執行或無法偵測對於重要作業系統資源之任何改變。

雖然此等保護系統可能有效，其亦可能存在少數缺點。首先，此等系統通常依靠隱匿性，且此等系統若由有毒軟體所辨識出則此等系統將因此而易受利用。即，若有毒軟體破解保護系統之身分及找到保護系統位置，則有毒

軟體將可能使保護系統本身停用。有毒軟體作者亦可指導他人關於如何做同樣行為。再者，而仍與前述內容相關，此等保護系統大體上在如同作業系統的保護領域之相同保護領域中(如在特權模式本身內)操作。因此，若有毒軟體獲准存取特權模式且能揭露隱匿之保護系統，則保護系統本身將易於遭受到攻擊。最後，此等保護系統與作業系統或特權模式同時初始化。因此，若有毒軟體或有毒軟體作者在此初始化前獲得計算裝置之控制，則其可防止保護系統初始化。

【發明內容】

此文件描述能致使一保護代理器可從一作業系統特權模式無法存取之記憶體中決定一作業系統之一或多數資源是否已被修改的工具。在一些具體實施例中，此等工具可致使該保護代理器常駐在一虛擬機器監視器中。在其他具體實施例中，該等工具可致使該保護代理器常駐在由虛擬機器監視器提供的不同虛擬分區內。藉由在作業系統特權模式外操作，保護代理器可較少受到在作業系統特權模式內操作之實體的攻擊。

此發明內容係提供以簡化形式來介紹的多種概念，本發明將在實施方式中進一步加以描述。此發明內容無意於識別申請專利範圍標的之關鍵或基本特徵，亦無意於用作限制申請專利範圍標的之範疇。術語「工具」例如可稱為系統、方法、電腦可讀指令、及/或技術，其可由以上脈絡

及遍及文件所許可。

【實施方式】

概述

以下文件描述能以使該保護代理器不能變更或不可自一作業系統特權模式存取之方式操作一保護代理器的工具。此等工具因此致能保護該保護代理器本身，因而確保保護代理器偵測對於重要作業系統資源之變更。此外，此等工具可關閉一作業系統或一作業系統特權模式，以回應偵測資源變更或回應至試圖修改該保護代理器本身。此外，此等工具可致使保護代理器加強作業系統資源之不可變性，之後無須偵測資源修改。

一其中該等工具可致動此等及其他活動之環境以下係在標題為「範例性操作環境(*Exemplary Operating Environment*)」區段中提出。一標題為「自主性保護代理器(*Autonomous Protection Agents*)」接著並包括兩子區段。第一子區段標題為「虛擬機器監視器保護代理器(*Virtual-Machine-Monitor Protection Agents*)」描述一其中保護代理器可在一虛擬機器監視器內常駐及執行的範例性方法。之後係另一子區段，標題為「虛擬分區保護代理器(*Virtual-Partition Protection Agents*)」，其描述一其中一保護代理器可在一與作業系統之分區分離的虛擬分區中存在及執行的範例性方法。

另一區段標題為「自主性保護代理器特權模式(*Autonomous Protection-Agents Privilege Modes*)」接續並包括兩子區段。第一子區

段描述一虛擬機器監視器計時器可增加一保護代理器特權模式至一下方處理器之範例性方法，且標題為「虛擬機器監視器之保護請求(*Protection Request to a Virtua lMachine Monitor.*)」。一子區段標題為「保護代理器虛擬處理器(*Protection-Agent Virtual Processor*)」接續並描述其中可產生保護代理器特權模式的另一方式(在使用多虛擬處理器之此事例中)，包括一經組態以在保護代理器特權模式中執行保護代理器者。一標題為「工具之範例性用法(*Exemplary Use of the Tools*)」之區段接續且描述操作中之先前描述工具的實例。最後，一標題為「工具之其他具體實施例(*Other Embodiments of the Tools*)」之區段描述其中工具可動作之各種其他具體實施例及方式。此綜述(包括此等區段標題及概要)係提供為了讀者之便利且無意限制申請專利範圍或標題區段之範疇。

範例性操作環境

在詳述該等工具前，係提供一範例性作業系統之以下討論，以協助讀者瞭解其中可執行之該等工具的各種發明態樣之一些方式。以下描述之環境僅構成一實例且無意於將該等工具之應用限制至任一特定操作環境。其他環境亦可使用而不脫離申請專利範圍標的之精神及範疇。例如，雖然以下區段描述具有一單一保護代理器之具體實施例，亦可利用多保護代理器。在一些實例中，此等保護代理器可獨立及併行地執行。在此等實例中，保護代理器典型係僅能在其各自分區內存取記憶體。再者，以下描述之技術

可並行地使用。即在一相同操作環境內，不同保護代理器可利用不同技術。

參考目前實例，第1圖說明一大體上指示為100之此範例性環境。此環境包括一計算裝置102，其本身包括一或多數處理器104以及電腦可讀媒體106。電腦可讀媒體106包括一虛擬機器監控器108(如超管理器)，其可致使一或多數處理器虛擬化成為多虛擬處理器。虛擬機器監視器108亦可致能多虛擬分區。一或多數虛擬處理器可關聯各分區，且此等虛擬處理器被排程至可用實體處理器上。如所示，虛擬機器監視器在一些具體實施例中可允許實現第一虛擬分區110及第二虛擬分區112。如以下詳盡討論，此等分區可作用以使作業系統功能與保護代理器服務分離。

另如所示，電腦可讀媒體106更包括一作業系統(operating system, OS)114以及一或多數使用者應用116。作業系統114將作業系統服務118提供予使用者應用116，因而允許該等應用在計算裝置上執行。此外，一或多數作業系統資源120常駐在作業系統上。範例性資源包括一系統服務調度表(system service dispatch table, SSDT)、一中斷調度表(interrupt dispatch table, IDT)、一全域描述符表(global descriptor table, GDT)及類似者。另如所示，作業系統可包括有毒軟體122(即具有惡意企圖之碼)，其可能已依以上討論或其他方法載於計算裝置上。一或多數保護代理器(以下討論)可偵測由有毒軟體對於作業系統資源進行之改變，及回應於該偵測而採取防禦動作。若該代理器作

成此一決定，則保護代理器可關閉該作業系統及/或計算裝置或可採取其他反對動作。

已討論計算裝置之結構，現注意力轉向變化出現在下方一或多數實體處理器104上之特權模式。虛擬機器監視器124代表第1圖中所示之最具特權模式。此特權模式可存取所有或實質上所有裝置之資源及記憶體。從虛擬機器監視器特權模式124，虛擬機器監視器可排程處理器及允許存取用於各虛擬分區之記憶體的區域。雖然可相信一在一分區內執行的作業系統控制一實體處理器中之所有資源，實際上其僅控制由虛擬機器監視器決定之一部分。

比虛擬機器監視器特權模式較少特權之作業系統特權模式126，可存取所有作業系統資源120及大多數或所有作業系統記憶體。然而，此特權模式無法存取關聯另一分區(例如第二虛擬分區112)的任何資源或記憶體。然而，由於此特權模式大體上可存取所有作業系統記憶體，因此有時其亦稱為「特權模式」。「第0級」、「監督器模式」或「核心模式」亦可描述此特權模式。如以上討論，一在作業系統特權模式126中操作之使用者應用大體上係能執行由處理器提供的大多數指令，除了保留用於虛擬機器監視器模式之該等指令。

此作業系統特權模式係與使用者特權模式128對比，有時稱為「非特權模式」、「第3級」、或直接稱「使用者模式」。另如以上討論，當從使用者特權模式128操作時，使用者應用可能不存取或變更關聯作業系統的某記憶體。一般而

言，當施行基本操作時，計算裝置使用者應用在此使用者特權模式中操作。

除予以上討論之模式外，第1圖亦說明一第二虛擬分區特權模式130及一保護代理商特權模式132。如以下詳盡討論，儘管保護代理器特權模式132大體上無法存取如虛擬機器監視器特權模式那樣多的記憶體，但保護代理器特權模式132可存取作業系統特權模式無法存取之記憶體的一部分。因此，此特權模式可比作業系統特權模式更多特權，但比虛擬機器監視器特權模式較少特權。

另如以下詳盡討論，第二虛擬分區特權模式大體上可存取關聯第二虛擬分區112之記憶體。此外，此模式可存取第一虛擬分區。此額外存取可(例如)允許一常駐在第二虛擬分區中之保護代理器掃描關聯第一虛擬分區之記憶體及其對應作業系統。此模式大體上無法存取虛擬機器監視器，而因此比虛擬機器監視器特權模式較少特權。然而，第二虛擬分區特權模式仍可存取作業系統特權模式無法存取之記憶體的一部分。

同時，第2圖說明計算裝置記憶體權利200。此圖式因此表示可由第1圖之模組存取之記憶體量。如所示，虛擬機器監視器108(其在虛擬機器監視器特權模式124中操作)具有所有已說明模組之大多數記憶體權利。事實上，虛擬機器監視器常駐且可單獨存取記憶體202之一部分。其次，保護代理器204(如第1圖中所示的任何保護代理器)在保護代理器特權模式132中操作，且可存取除了對應於虛擬機器監

視器之部分202的所有記憶體。然而，保護代理器確實可存取記憶體206的一部分，此部分係保護代理器本身常駐在其中之記憶體的部分。

同時，作業系統114在作業系統特權模式126中操作，且其可存取除了部分202及部分206之所有記憶體。儘管該作業系統可能無法存取關聯保護代理器之記憶體206的部分，作業系統及其關聯特權模式確實可存取記憶體208的一部分。記憶體208之此部分有時稱為核心記憶體或一作業系統之最下層組件，且大體上含有第1圖所示的資源。然而，即使有毒軟體在記憶體208之部分中載入及操作，有毒軟體同樣無法存取關聯保護代理器之記憶體206的部分。

最後，第2圖說明使用者應用116僅可存取記憶體210的一部分。此等使用者應用及對應使用者特權模式無法存取關聯作業系統之最下層組件的記憶體208之部分。記取此操作環境，以下四區段詳述範例性方法，其使一保護代理器無法從作業系統特權模式變更或存取。

自主性保護代理器

以下區段描述能從一作業系統特權模式內操作之實體無法存取的記憶體中決定一或多數作業系統資源是否已被修改之工具。因此，該等工具可允許一保護代理器常駐在一除了作業系統記憶體本身之位置以外的位置。更特別言之，以下子區段描述保護代理器如何可常駐在一虛擬機器監視器內或在自主性虛擬分區內。

虛擬機器監視器保護代理器

此子區段描述一保護代理器134如何可常駐在虛擬機器監視器本身內，如第1圖所示。因為作業系統特權模式無法存取虛擬機器監視器，此位置保護該保護代理器避免受到位於作業系統記憶體中之任何有毒軟體影響。為了從此位置操作，保護代理器接收一保護代理器134可監控之一或多數作業系統資源120的識別。此識別可經由資源識別符136接收。如所示，該作業系統可將此資訊透過應用程式化介面(application programming interface, API)呼叫提供予虛擬機器監視器，或該作業系統可依一工具性質規定檔138形式提供該資訊。如以上討論，此等資源可包括SSDT、IDT及GDT。

一旦其已接收資源之識別，保護代理器134擴展保護代理器服務140至作業系統114。此等保護代理器服務大體上包含決定是否已變更任何經識別資源。若作成此一決定，保護代理器或虛擬機器監視器可(例如)關閉作業系統。保護代理器服務亦可加強相對於標示為不可變更(如「唯讀」)之任何資源的不可變性。

使用此一架構以載入及初始化虛擬機器監視器開始，其係能主控一或多數作業系統。在此實例中，虛擬機器監視器主控單一作業系統114，其本身在虛擬機器監視器載入後開始初始化。在作業系統之初始化期間，關聯作業系統的最下層組件(如核心)之記憶體208的部分首先載入。一些

或所有作業系統資源120(如SSDT、GDT、IDT)大體上存在於記憶體208之此部分。

在作業系統初始化之前或同時，保護代理器134可從虛擬機器監視器內開始執行。如以上討論，保護代理器大體上接收一組一或多數作業系統資源之識別及決定經識別資源之一或多數是否已變更。應注意的是，各經識別資源通常包含在多位置處之多組件，該保護代理器可監控其各者以徹底保護整體資源。例如，若工具性質規定檔識別一SSDT為欲監控及保護的資源，則保護代理器不僅保護SSDT之實際表且其他組件。例如，保護代理器亦可監控及掃描指向該表之位置的暫存器。此外，保護代理器亦可監控該記憶體翻譯資料結構(如頁面表)，其翻譯SSDT之虛擬位址成為實體位址。若該保護代理器無法如此進行，則惡意碼可用不同頁表映射產生另一表(即跳過SSDT本身)。

除了識別以外，保護代理器亦可接收一保護屬性，其指令保護代理器如何保護一對應資源。例如，保護代理器可接收SSDT資源之一識別，以及「唯讀」的一對應保護屬性。因此保護代理器得知SSDT應保持唯讀，且因此不應被變更，「初始唯讀」係另一可能保護屬性，其指令保護代理器該對應資源可在初始化期間寫一次，但在此時間後資源應保持唯讀。

保護代理器可依一些方法(主動及被動兩者)接收資源及資源保護屬性的此識別。例如，作業系統可提供一數位簽名工具性質規定檔，其識別保護代理器可監控的資源。

此數位簽名工具性質規定檔可依許多方法識別該等資源，例如藉由名稱(如SSDT、IDT、GDT等等)或藉由位址，其映射資源至記憶體208之部分中的對應位置。在此後一事例中，工具性質規定檔可識別一資源之客方實體位址，客方虛擬位址或系統實體位址。應注意在一些實例中，一客方實體位址可映射至一實際系統實體位置，以發現對應資源組件之實際實體位置。

在虛擬機器監視器或保護代理器接收該工具性質規定檔後，此等組件可決定該工具性質規定檔是否已被篡改或修改。若虛擬機器監視器或保護代理器作成此一決定，則虛擬機器監視器或保護代理器可選擇無法開始作業系統。此外，關聯資源之列表的密碼可能無效，因而保護其安全。

除了工具性質規定檔，保護代理器可經由一或多數應用設計介面(API)呼叫進入虛擬機器監視器(如「超呼叫(hypercall)」)內，來接收資源及保護屬性識別。隨著作業系統初始化，作業系統(及可能作業系統208之最下層組件)可使超呼叫進入虛擬機器監視器內以通知保護代理器可監視及保護某些資源。此等超呼叫可依以上討論的相同方法識別該等有關資源。另外，如以上討論，此等超呼叫亦可識別資源的保護屬性。

在利用數位簽名工具性質規定檔以及一或多數超呼叫之具體實施例中，保護代理器可在作業系統啟動之前或同時首先掃描在工具性質規定檔中識別的資源。在此初始掃描後，作業系統可接著使超呼叫進入虛擬機器監視器內，

以指令保護代理器決定經超呼叫識別之頁是否已被變更。工具性質規定檔因此識別資源以在每次作業系統啟動時掃描，而超呼叫識別資源以在其各自初始化時動態地掃描。

已識別欲監控的資源後，保護代理器接著決定資源(如以上討論SSDT之所有部分)是否已被變更。保護代理器亦可加強相對於經識別資源之不可變性。例如，保護代理器可確保經指定為「唯讀」之任何資源不改變成「可寫」。

為了依此方法監控及保護資源，在虛擬機器監視器內執行之碼可使用一虛擬機器監視器截取管理器(如第1圖之管理器146)。若經如此指令，此截取管理器可登記用於在經識別資源之各種組件上截取。由於此登記，若試圖存取或修改此等經識別資源，則虛擬機器監視器內之保護代理器現可接收截取。因此，保護代理器可檢查及掃描經識別資源的各種組件。其亦可主動地阻擋對於修改此等資源之企圖。

在一些具體實施例中，保護代理器掃描資源及決定資源之初始狀態用於比較未來掃描的結果。在其他具體實施例中，保護代理器已知該資源的初始狀態，用於比較未來掃描之結果。在任何事件中，保護代理器可計算此初始狀態之一雜湊或核對和值。在此比較後，保護代理器在作業系統啟動前、後或同時掃描資源。在掃描後，保護代理器計算該等結果之雜湊或核對和值且將此與初始狀態雜湊或核對和值比較。若相等，保護代理器決定對應資源未被變更。當然，保護代理器可略過雜湊或核對和值且另外直接

比較初始狀態與掃描。

然而，若該等值不同，保護代理器及/或虛擬機器監視器可採取一或多數回應動作。首先，保護代理器本身可關閉作業系統或作業系統特權模式，或其可指令虛擬機器監視器來如此進行。再次，因為保護代理器常駐在虛擬機器監視器中，且因為虛擬機器監視器主控作業系統，此兩組件可將作業系統關閉。此外，因為保護代理器常駐在虛擬機器監視器內，作業系統的關閉不可能從甚至作業系統特權模式篡改。

除了關閉作業系統外，保護代理器及/或虛擬機器監視器可首先警告作業系統即將發生關閉。一在虛擬機器監視器及作業系統間之通訊通道可允許此一通訊。在替代例中，保護代理器及/或虛擬機器監視器可將一警告寫入一記憶體位置或將作業系統監控的一事件發訊。

不論是否已提供一警告，作業系統關閉可為突然或緩慢的。在前一情況中，虛擬機器監視器可單純在得知不同雜湊或核對和值後立即切斷作業系統之電源。在後一情況中，虛擬機器監視器可允許作業系統某一時間量以將其本身徹底地關機。在此時，作業系統可(例如)關閉任何開啟檔案及消除任何對應資料。作業系統亦可釋放經指定資源。此外，關機可利用兩方法。例如，若虛擬機器監視器主控多分區，則其可立即將具有不同雜湊或核對和值之分區關閉而允許其他分區時間來徹底地關機。不管如何，關機之方式可藉由策略來組態及可調整。

除了關機及對應之警告以外，保護代理器及/或虛擬機器監視器可採取後啟動動作，以回應一經識別資源之非允許變更。例如，虛擬機器監視器及/或保護代理器可在作業系統再啟動時，通知作業系統資源變更。為了回應，作業系統可施行一防毒掃描以偵測是否有任何有毒軟體確實常駐在作業系統記憶體內，例如部分208(如核心)。此外，虛擬機器監視器可將作業系統啟動成為一安全模式，或作業系統本身可選擇啟動成為安全模式。另回應於該通知，作業系統可識別本身為已受攻擊，及因此可能不允許本身存取任何其耦合之網路。

虛擬分區保護代理器

與常駐在虛擬機器監視器本身內不同，一保護代理器(如第1圖之保護代理器142)可常駐在一分離的虛擬分區(如第1圖之第二虛擬分區112)中。在此等具體實施例中，此分離的分區作為虛擬機器監視器之可信賴委派。保護代理器142因此係不可自作業系統特權模式存取。如以上討論，虛擬機器監視器108提供計算裝置102的此虛擬化。儘管虛擬機器監視器可將計算裝置虛擬化成任何數目之分區，第1圖說明一主控作業系統之第一分區，及一主控保護代理器之第二分區。其中保護代理器常駐之第二虛擬分區在一些實例中可為一專用安全分區，其主要或唯一功能係執行保護代理器。在其他具體實施例中，此第二虛擬分區可施行額外功能，例如主控另一作業系統。

常駐在第二虛擬分區內之保護代理器142係能施行以上有關常駐在虛擬機器監視器內之保護代理器134描述的許多或所有相同功能。即，保護代理器142可主動或被動地接收一或多數作業系統資源120之一識別。回應於該識別，保護代理器可再次擴展保護代理器服務140，其大體上包含決定經識別資源之一或多數是否已被變更，且若如此則採取回應動作。此等服務亦可包括加強特定資源的不可變性。保護代理器142可經由類似以上所述的技術施行此等功能。

如所示，保護代理器142係可自第二虛擬分區特權模式130存取，但不可自作業系統特權模式126存取。因此，產生之架構允許保護該保護代理器本身，防止任何位於作業系統內之有毒軟體，即使該有毒軟體常駐在關聯該作業系統之最下層組件的記憶體208之部分內。

自主性保護代理器特權模式

此區段描述能使關聯一保護代理器之作業系統記憶體的一部分，作業系統特權模式無法變更或存取此一部分，而仍允許記憶體之此部分實體上常駐在作業系統實體記憶體空間中。此等工具因此產生一自主性保護代理器特權模式，其可存取關聯保護代理器之記憶體的部分，以及在作業系統特權模式內可存取之其餘記憶體。此特權模式係因此比作業系統特權模式更具特權。

該第一子區段描述可藉由請求虛擬機器監視器保護關

聯保護代理器之記憶體的一部分，而產生保護代理器特權模式之工具。同時，第二子區段描述允許藉由虛擬化一實體處理器成為多虛擬處理器(包括一執行保護代理器之專用虛擬處理器)，來產生保護代理器特權模式的工具。

對於虛擬機器監視器之保護請求

此子區段描述一保護代理器如何可請求一虛擬機器監視器，以保護關聯保護代理器之記憶體，且因此保護代理器本身。此保護導致一保護代理器144在保護代理器特權模式132中操作，如第1圖中所示。如所示，保護代理器144可在轉移至保護代理器特權模式前，初始地常駐在作業系統特權模式中。當在此後一特權模式中操作時，保護代理器大體上不受來自以作業系統特權模式126操作之實體的攻擊之影響。

當在保護代理器特權模式132中操作時，一實體具有比在作業系統特權模式126中操作稍微多之特權，但仍比虛擬機器監視器特權模式124較少特權。如第2圖中所示，一在此特權模式中操作之保護代理器可存取關聯該作業系統之所有記憶體，除了關聯該保護代理器本身之記憶體206的部分以外。虛擬機器監視器108強制該經增加保護代理器可存取性。

第3及4圖說明產生此保護代理器特權模式的範例性模式。第3圖描述所有或實質上所有計算裝置記憶體300。計算裝置記憶體300包括一關聯作業系統特權模式之記憶體

302的部分(如核心)，及一關聯使用者特權模式之記憶體304的部分。記憶體302之部分亦包括(如所示)關聯保護代理器144之記憶體306的一部分，及驅動器載入之記憶體308的一部分。

如第4圖所示，一產生保護代理器特權模式132之程序400藉由初始化記憶體302之部分(如核心)而在動作1處開始。在動作2處，記憶體306之部分或保護代理器144本身呼叫虛擬機器監視器108，以請求虛擬機器監視器保護關聯保護代理器之記憶體的部分。當如此請求時，保護代理器或對應記憶體要求在作業系統特權模式內執行的碼不允許變更或觸碰記憶體306之此部分。保護代理器亦可對虛擬機器監視器108證實其本身(如藉由數位簽名)。記憶體之此部分(或保護代理器本身)亦可請求虛擬機器監視器設定一計時器，及當計時器過期時執行該保護代理器。動作3表示虛擬機器監視器保護記憶體，防止在作業系統特權模式內操作的實體及設定一計時器以回應該請求。應注意，因為關聯保護代理器之記憶體306的此部分現無法自作業系統特權模式變更及/或存取，故保護代理器現常駐在保護代理器特權模式中。

在動作4處，驅動器載入記憶體308的部分內。應注意動作2之請求及動作3的對應保護大體上在驅動器載入記憶體內之前發生，因為有毒軟體可依驅動器的形式存在。如以下在「工具之範例性使用」區段中討論，有毒軟體作者經常欺騙使用者將惡意驅動器安裝在一計算裝置上。若一

或多數惡意驅動器確實在記憶體306之部分受保護前載入記憶體內，則惡意驅動器可潛在地修補用於保護本身之請求。此修補將因而阻止保護代理器經由虛擬機器監視器的週期性執行，且因而產生保護代理器特權模式。然而，藉由請求虛擬機器監視器提早設定一計時器，此程序確保在作業系統特權模式中之碼不能如此停用保護代理器的週期性執行。

同時，動作5很可能在驅動器已載入後的某時間發生。如所示，動作5表示虛擬機器監視器計時器之過期，及因此保護代理器的執行。當執行時，保護代理器144施行在先前區段中所討論之類似或相同功能。另如以上討論，保護代理器可採取動作以回應一或多數經識別資源已變更之決定。保護代理器亦可採取此動作，以回應一從在作業系統特權模式內操作之實體試圖存取或變更保護代理器(或其對應記憶體)。

動作6表示當保護代理器結束執行時，該保護代理器通知虛擬機器監視器。最後，動作7表示動作3、5及6的重覆。因此，虛擬機器監視器可重設其計時器及在週期性間隔處執行保護代理器，例如每100毫秒(ms)。

藉由在虛擬機器監視器處設定一失效安全計時器，程序400因而消除作業系統碼篡改關聯保護代理器之記憶體的部分之能力。因此，此程序確保該保護代理器將持續執行且不受到在作業系統特權模式中動作之有毒軟體的修補。取而代之的是該保護代理器將在一自主性特權模式內

執行，而仍常駐在配置予作業系統之實體記憶體內。

保護代理器虛擬處理器

此子區段描述一虛擬機器監視器如何可藉由排程一虛擬處理器以執行保護代理器144，來產生一保護代理器特權模式。第5圖說明一結構500，其包括虛擬化計算裝置102成為兩分區(各包括一作業系統)之虛擬機器監視器108。如所示，此實例中之計算裝置包括兩真實處理器104(a)及104(b)，在其各者上虛擬處理器可將多虛擬處理器排程。另如所示，虛擬機器監視器產生一第一虛擬分區502及一第二虛擬分區504。第一虛擬分區包括一第一虛擬處理器506以執行一第一作業系統。同樣地，第二虛擬分區包括一第二虛擬處理器508以執行一第二作業系統。然而，在此實例中，虛擬機器監視器亦包括一保護代理器虛擬處理器510以執行一保護代理器，例如第1圖之保護代理器144。

為產生架構500，虛擬機器監視器首先載入及初始化。如第6圖中說明，虛擬機器監視器接著虛擬化各種虛擬處理器，且如此進行時，會配置真實處理器頻寬600。為了開始此虛擬化及配置，虛擬機器監視器虛擬化該第一虛擬處理器至第一真實處理器上。在目前實例中，此虛擬化係在一對一之基礎上進行，如由第6圖說明。即，僅此單一虛擬處理器506對應於真實處理器104(a)，及因而虛擬機器監視器配置所有真實處理器之頻寬至此虛擬處理器。虛擬機器監視器接著虛擬化第二虛擬處理器508至第二真實處理器

104(b)上。然而，與一對一基礎不同的係，虛擬機器監視器保持第二真實處理器之頻寬的一些部分。虛擬機器監視器接著虛擬化保護代理器虛擬處理器510至第二真實處理器104(b)之此剩餘頻寬，亦如第6圖所示。

在第二真實處理器上操作之各虛擬處理器大體上依一時間切片基礎來動作。即，第二虛擬處理器可在第二虛擬處理器懸置前在第二真實處理器上操作達到一些時間量。在此時，第二真實處理器切換至操作保護代理器虛擬處理器達到一些其他時間量。例如，第二虛擬處理器可在第二真實處理器上操作達到90ms，在該點此第二虛擬處理器之操作懸置且保護代理器虛擬處理器之操作開始達到10ms。保護代理器虛擬處理器大體上對於兩作業系統分區及第一及第二虛擬處理器兩者係透通(transparent)。因此，兩作業系統相信其對應虛擬處理器對應於一各自之真實處理器。

除了配置真實處理器頻寬以外，虛擬機器監視器亦管理各虛擬處理器可存取之記憶體的部分。在目前實例中，第一虛擬處理器可存取所有關聯第一作業系統之記憶體。同時，第二虛擬處理器可存取所有關聯第二作業系統之記憶體，除了關聯保護代理器之記憶體的部分以外。保護代理器虛擬處理器已單獨存取關聯保護代理器之記憶體的部分，除了配置予第二作業系統之記憶體以外。

再者，第一及第二虛擬處理器僅具有變更其關聯記憶體之能力。因此，操作其各自作業系統之虛擬處理器皆不

可變更關聯保護代理器之記憶體的部分。然而，保護代理器虛擬處理器可變更關聯保護代理器之記憶體，及(在一些具體實施例中)關聯第二虛擬處理器的記憶體。

藉由其程式化本身，保護代理器虛擬處理器將週期性地執行保護代理器。儘管在一些實例中該保護代理器虛擬處理器可執行其他應用，目前實例說明一專用保護代理器虛擬處理器。因此，此虛擬處理器大體上僅作用於週期性地執行保護代理器。再次，保護代理器可用類似或相同方式施行類似或相同功能，如以上描述之保護代理器。

藉由排程一專用保護代理器虛擬處理器，虛擬機器監視器確保保護代理器將會在此處理器之控制下及在自主性保護代理器特權模式中週期性地執行。再者，因為僅此保護代理器虛擬處理器可存取關聯保護代理器之記憶體的部分，故虛擬機器監視器保護此記憶體，防止在一作業系統內之碼。因此，在一作業系統特權模式內之操作的有毒軟體不能修補保護代理器及防止保護代理器執行。因此，此技術基本上消除作業系統篡改保護代理器之能力。

工具之範例性用法

先前已描述可確保一保護代理器之保護的工具，以下區段僅描述在操作中之此等工具的一實例。首先，想像一電腦使用者瀏覽網際網路及當瀏覽某一網站時，一具有惡意企圖之對話方塊跳出在使用者的顯示器上。該對話方塊向使用者請求允許在使用者電腦上安裝某種類之有毒軟

體。雖然此請求可能係直接，但想像該偽裝該請求為通常之情況。對話方塊可(例如)偽稱使用者其已贏得獎品。在此通知時，對話方塊惡意地指示使用者按下對話方塊上的「OK」鍵以接受該獎品。想像該使用者確實選擇OK鍵且使用者選擇持續該請求操作而不理會來自在計算裝置上執行之軟體(如防毒應用)的一或多數警告。

此時，計算裝置開始安裝含有有毒軟體的驅動器。如大體上驅動器之真實操作，此惡意驅動器獲准存取一作業系統特權模式且載入關聯此特權模式之記憶體(如核心)。一旦載入該核心，惡意驅動器及其伴隨有毒軟體基本上已全權委任地存取電腦之記憶體及作業系統。對於使用者而言，不幸的係可想像此有毒軟體包括一記錄使用者之鍵次的鍵記錄器。現想像使用者導航至其銀行網站且簽入其銀行帳戶。由於其記錄鍵次的能力，該鍵記錄器得知使用者之銀行帳戶密碼，且透過網際網路將此密碼發送至惡意驅動器之作者。

最壞打算，想像該有毒軟體係一「根套件」-或試圖對保護代理器及使用者防毒軟體主動隱藏之有毒軟體。在習知系統中，一保護代理器常駐在核心內(即在惡意驅動器可存取的記憶體中)。因此，在此等習知系統中，有毒軟體可存取保護代理器及可能試圖向保護代理器隱藏其本身。若成功，有毒軟體對於保護代理器似乎不存在於核心內。因此，當使用者之防毒軟體呼叫保護代理器及請求一出現在電腦中記憶體內之所有應用的列表時，有毒軟體將不出

現。此不出現使防毒軟體無力知悉及移除有毒軟體。此外，有毒軟體可修補保護代理器，因而完全防止保護代理器執行。因此，若有毒軟體變更任何作業系統資源，保護代理器可能無法注意到。

然而，與習知系統中常駐在在核心內不同，想像在使用者計算裝置上之保護代理器常駐記憶體中，或在一作業系統特權模式無法存取之模式中。因此，當惡意驅動器載入核心內時，其無法存取其中保護代理器常駐之記憶體或其中保護代理器執行的模式。因此，該驅動器及其伴隨有毒軟體無法存取保護代理器本身。該有毒軟體係因此無法對於保護代理器及因此防毒軟體隱藏其本身。因此，當防毒軟體向保護代理器要求一在電腦記憶體中出現之所有應用的列表時，所回覆列表會包括該有毒軟體。防毒軟體接著認知此碼係有毒軟體及因此將其從使用者電腦移除。此外，保護代理器本身可注意到該有毒軟體是否變更作業系統資源，且可回應而關閉使用者之計算裝置。

因此，藉由常駐在記憶體中或在一作業系統特權模式無法存取之模式中執行，在此描述之具體實施例防止有毒軟體隱藏其本身或修補保護代理器。在以上實例中，使用者之計算裝置係因此能將有毒軟體從機器移除，或在一些實例中，當有毒軟體變更重要資源時關閉該系統。在任一情況中，此等具體實施例係作用以減少有毒軟體希望造成損害之效用。

工具之其他具體實施例

以上區段描述一其中使一保護代理器無法自作業系統特權模式中變更或存取之少數特例。在此區段中，係描述工具之其他具體實施例，如增加一特權模式至一未出現在一下方處理器上之處理器。

此等範例性具體實施例係描述為第7至11圖之程序700至1100的部分。此等程序以及參考第1至6圖描述或說明之範例性程序，可在任何適合硬體、軟體、韌體或其結合中實施；在軟體及韌體之情況下，此等程序表示實施為儲存在電腦可讀媒體及可由一或多數處理器執行之電腦可執行指令的成組操作。在此區段中描述之工具的此等具體實施例無意於限制工具或申請專利範圍之範疇。

參考第7圖，步驟702接收一識別一或多數作業系統資源之強制策略。此強制策略(其可包含加密資料)可經由一數位簽名工具性質規定檔(manifest)或藉由將一應用程式介面(API)曝露至作業系統(如超呼叫)來接收。步驟704從一不可由在作業系統特權模式內操作之實體存取的記憶體，來識別一或多數作業系統資源。範例性資源包括一系統服務調度表(SSDT)、一中斷調度表(IDT)及/或一全域描述符表(GDT)。如以上描述，此識別可出現在一虛擬機器監視器(如藉由第1圖之保護代理器134)內或在一分離虛擬分區(如藉由第1圖之保護代理器142)內。

同時，步驟706表示決定任何經識別資源是否已被變更。再次，此可發生在虛擬機器監視器內或分離分區內。

若步驟706決定一或多數經識別資源的確已被變更，則步驟708回應此決定而終止作業系統。最後，步驟710在作業系統再啟動時通知作業系統一不合法操作。

第8圖說明一用於允許保護代理器在一虛擬機器監視器內執行之程序800。步驟802變更一虛擬機器監視器截取管理器，其係用以允許接收一關聯一作業系統資源之記憶體頁面或暫存器已被變更之指示。此資源可包含參考第7圖描述之該等資源其一，或可為另一作業系統資源。不論如何，步驟804接收一識別該作業系統資源及可能一或多數其他作業系統資源之強制策略。再次，此識別可經由以上討論之技術完成。如以上描述，資源之一保護屬性(即「唯讀」或「初始唯讀」)可伴隨資源之識別。同時，步驟806表示接收一關聯作業系統資源之記憶體頁面或暫存器的確已被變更的指示。回應時，步驟808關閉一用以將關聯作業系統資源之作業系統關閉的作業系統特權模式。在一些實例中，第1圖中虛擬機器監視器108可達成作業系統特權模式的此一關閉。

其次，第9圖描述一用於產生保護代理器特權模式(如第1圖中說明之保護代理器特權模式132)之範例性程序900。步驟902接收一請求，其使一特定範圍之記憶體不可從一作業系統特權模式變更或存取。再次，一虛擬機器監視器可接收此請求，其可起源於記憶體本身之該範圍或自一以該記憶體的範圍常駐之保護代理器。步驟904保護記憶體的該範圍及設定一計時器以週期性地執行以記憶體之該

範圍常駐之保護代理器。再次，一虛擬機器監視器可設定此一計時器，其可指令虛擬機器監視器以規則性間隔執行保護代理器。

同時，步驟906接收一描述作業系統資源的強制策略。再次，強制策略及所述資源可與以上所討論者類似或相同。步驟908執行保護代理器，其可藉由虛擬機器監視器達到。決策步驟910詢問作業系統資源是否已被變更。保護代理器可藉由依以上詳述之方法起作用來作成此決定。若步驟910的確決定一變更已發生，則步驟912將作業系統關機。然而，若未作成此決定，則步驟914接收一保護代理器已結束執行之通知。在一些實例中及如以上描述，保護代理器本身可因此通知虛擬機器監視器。同時，步驟916表示在執行保護代理器及不執行保護代理器間之循環。最後，應注意儘管保護代理器未執行，虛擬機器監視器可將作業系統關機，以回應一自作業系統特權模式內操作的實體試圖存取關聯保護代理器之記憶體的該範圍。

第10圖說明用於產生一保護代理器特權模式(如第1圖中說明之保護代理器特權模式132)之另一範例性程序1000。步驟1002將一真實電腦處理器虛擬化成為多虛擬電腦處理器。此等虛擬處理器可包含一或多數作業系統虛擬處理器，其各具有一特權以變更其自己之作業系統記憶體，及使用真實處理器之處理頻寬的一部分，如第6圖中說明。該等虛擬處理器亦可包括至少一保護代理器虛擬處理器，其具有一特權以變更自己的保護代理器記憶體及使用

真實處理器之處理頻寬的一不同部分。雖然所有虛擬處理器可藉由虛擬機器監視器排程，保護代理器虛擬處理對於作業系統虛擬處理器可為透通。在一些實例中，作業系統的虛擬處理器可能無法變更指定予保護代理器虛擬處理器之記憶體。此外，保護代理器虛擬處理器可為一專用處理器，其主要或唯一目的係使保護代理器執行，如以上討論。

其次，步驟1004造成保護代理器虛擬處理器執行一保護代理器，其可為用以決定該作業系統記憶體之一部分是否已被變更。同時，步驟1006接收一該作業系統記憶體之一部分已被變更的指示。回應時，步驟1008關閉一對應作業系統。

最後，第11圖描述一用於將一特權模式增加至一真實計算處理器的程序1100。步驟1102表示出現在一下方實體處理器之一或多數特權模式的決定、識別或分類。此等特權模式大體上係藉由下方實體處理器本身來定義。在任何情況下，步驟1104增加一不出現在下方實體處理器上的特權模式。在一些實例中，所增加特權模式係能變更計算裝置的記憶體之一部分，其與可藉由一或多數目前特權模式變更之記憶體的一部分不同。所增加之特權模式亦可能增加且執行先前在下方處理器中不存在或不可執行的指令。

此外，在下方實體處理器上出現之一或多數特權模式可包括一使用者特權模式及一作業系統特權模式。在此等具體實施例中，所增加特權模式可比使用者特權模式及作業系統特權模式兩者更具特權，比使用者特權模式更具特

權但比作業系統特權模式較少特權，或比使用者及作業系統特權模式兩者較少特權。最後，應注意到增加特權模式之一實例可包含依以上討論之許多方法增加一保護代理器特權模式(如第1圖中說明之保護代理器132)。例如，一保護代理器或其關聯範圍之記憶體，可請求該範圍之記憶體無法由作業系統特權模式內操作之實體存取。一虛擬機器監視器亦可藉由排程一保護代理器虛擬處理器執行保護代理器來產生此特權模式。

結論

以上所述工具係能藉由致使一保護代理器常駐在一作業系統特權模式無法存取之位置，或藉由產生一保護代理器特權模式，而使該保護代理器無法從一作業系統特權模式變更或存取。儘管已在特定於結構特徵及/或方法動作之語言中描述該等工具，但應理解在隨附申請專利範圍中定義之工具，無須受限於所描述之該等特定特徵或動作。而是該等特定特徵及動作係揭示為實施該等工具之範例性形式。

【圖式簡單說明】

第1圖說明其中工具之各種具體實施例可操作之一範例性操作環境。

第2圖示範第1圖中所示之模組的變化計算裝置記憶體權利。

第3圖表示其中第1圖中所示的一些模組常駐之計算裝置記憶體的變化部分。

第4圖係一說明其中一虛擬機器監視器可保護關聯一保護代理器之記憶體部分且設定一計時器以執行該代理器的範例性方式之流程圖。

第5圖說明一具有一虛擬機器監視器之範例性架構，其能將實體處理器虛擬化成為多作業系統虛擬處理器及一保護代理器虛擬處理器。

第6圖說明第5圖之實體處理器的頻寬如何配置在各種虛擬處理器中。

第7圖係一說明其中該等工具可致動及執行一常駐在一作業系統特權模式無法存取之位置的保護代理器之一些方式的範例性程序。

第8圖係一說明其中該等工具可變更虛擬機器監視器以致動和執行一常駐在一作業系統特權模式無法存取之位置的保護代理器之一些方式的範例性程序。

第9圖係一說明其中該等工具可藉由進行一對於一虛擬機器監視器之請求來產生一保護代理器特權模式之一些方式的範例性程序。

第10圖係一說明其中該等工具可藉由將真實電腦處理器虛擬化成為虛擬電腦監視器來產生一保護代理器特權模式之一些方式的範例性程序。

第11圖係一說明其中該等工具可致能增加未出現在一下方實體處理器之特權模式的一些方式之範例性程序。

遍及揭露書及圖式中係用相同數字來指示類似組件及特徵。

【主要元件符號說明】

100 範例性環境	102 計算裝置
104 處理器	104(a)真實處理器
104(b) 真實處理器	106 電腦可讀媒體
108 虛擬機器監控器	110 第一虛擬分區
112 第二虛擬分區	114 作業系統
116 使用者應用	118 作業系統服務
120 作業系統資源	122 有毒軟體
124 虛擬機器監視器	126 作業系統特權模式
128 使用者特權模式	130 第二虛擬分區特權模式
132 保護代理商特權模式	134 保護代理器
136 資源識別符	138 工具性質規定檔
140 保護代理器服務	142 保護代理器
144 保護代理器	146 管理器
200 計算裝置記憶體權	202 記憶體
204 保護代理器	206 記憶體
208 記憶體/作業系統	210 記憶體
300 計算裝置記憶體	302 記憶體
304 記憶體	306 記憶體
308 記憶體	400 程序
500 結構	502 第一虛擬分區

504 第二虛擬分區

506 第一虛擬處理器

508 第二虛擬處理器

510 保護代理器虛擬處理器

600 真實處理器頻寬

十、申請專利範圍：

1. 一種電腦可讀取媒體，其上具有電腦可讀取指令，當藉由一計算裝置執行該些指令時，可使該計算裝置執行包含以下步驟之動作：

藉由一虛擬機器監視器來提供至少一第一分區(partition)與一第二分區；

於記憶體處接收一強制策略(enforcement policy)，該記憶體係無法由在一作業系統特權模式內操作的一實體所存取，該強制策略用於識別在由該虛擬機器監視器所提供的該第一分區中操作的一作業系統的一組一或更多個資源；

利用該強制策略及從在該作業系統特權模式內操作的該實體所無法存取的該記憶體，來識別在由該虛擬機器監視器所提供的該第一分區中操作的該作業系統的該組一或更多個資源；

從該記憶體來決定是否該組一或更多個資源中之一或更多者已被變更；及

響應於決定出該組一或更多個資源中之一或更多者已被變更，來(i)終止該作業系統或(ii)就一不合法操作的再啟動(reboot)的情況而通知該作業系統；

其中接收該強制策略的步驟、識別該組一或更多個資源的步驟、及決定是否該組一或更多個資源中之一或更多者已被變更的步驟係發生於(i)該虛擬機器監視器內或(ii)由該虛擬機器監視器所提供的該第二分區內。

2. 如申請專利範圍第 1 項所述之媒體，更包含將一應用程式介面(application program interface, API)曝露予該作業系統，及透過該 API 接收該組一或更多個資源中之一或更多者的一識別之步驟。

3. 如申請專利範圍第 1 項所述之媒體，其中該組一或更多個資源包括一系統服務調度表(system service dispatch table, SSDT)、一中斷調度表(interrupt dispatch table, IDT)、或一全域描述符表(global descriptor table, GDT)。

4. 一種用於保護作業系統資源之方法，該方法包含以下步驟：

為有效的啟動關聯於一作業系統資源之一記憶體頁面或暫存器已被變更的一指示之接收而變更一虛擬機器監視器的一截取管理器，該作業系統資源係位於由該虛擬機器監視器所提供的一分區內；

於該虛擬機器監視器處接收識別該作業系統資源及一或更多個額外的作業系統資源的一強制策略；

藉由該虛擬機器監視器的該截取管理器來接收關聯於該作業系統資源之該記憶體頁面或暫存器已被變更的一指示；及

響應於接收到該指示，來為有效的關閉(shut down)

關聯於該作業系統資源之一作業系統而關閉一作業系統特權模式。

5. 如申請專利範圍第4項所述之方法，其中該作業系統資源係位在該記憶體頁面處之一中斷調度表(IDT)，且關聯於作業系統資源之該暫存器係一IDT暫存器。

6. 如申請專利範圍第4項所述之方法，其中該作業系統資源係一系統服務調度表(SSDT)或一全域描述符表(GDT)。

7. 如申請專利範圍第4項所述之方法，其中關閉該作業系統特權模式之步驟係藉由一虛擬機器監視器所執行。

8. 如申請專利範圍第4項所述之方法，其中該強制策略亦描述關聯於該等識別的作業系統資源中之每一者的一保護屬性，保護屬性中之至少一者描述一對應的資源為唯讀的(read-only)。

9. 如申請專利範圍第8項所述之方法，更包含強制執行(enforce)相對於關聯於該唯讀的保護屬性之該資源的不可變性(invariance)之步驟。

10. 一種電腦可讀取媒體，其上具有電腦可讀取指令，當藉

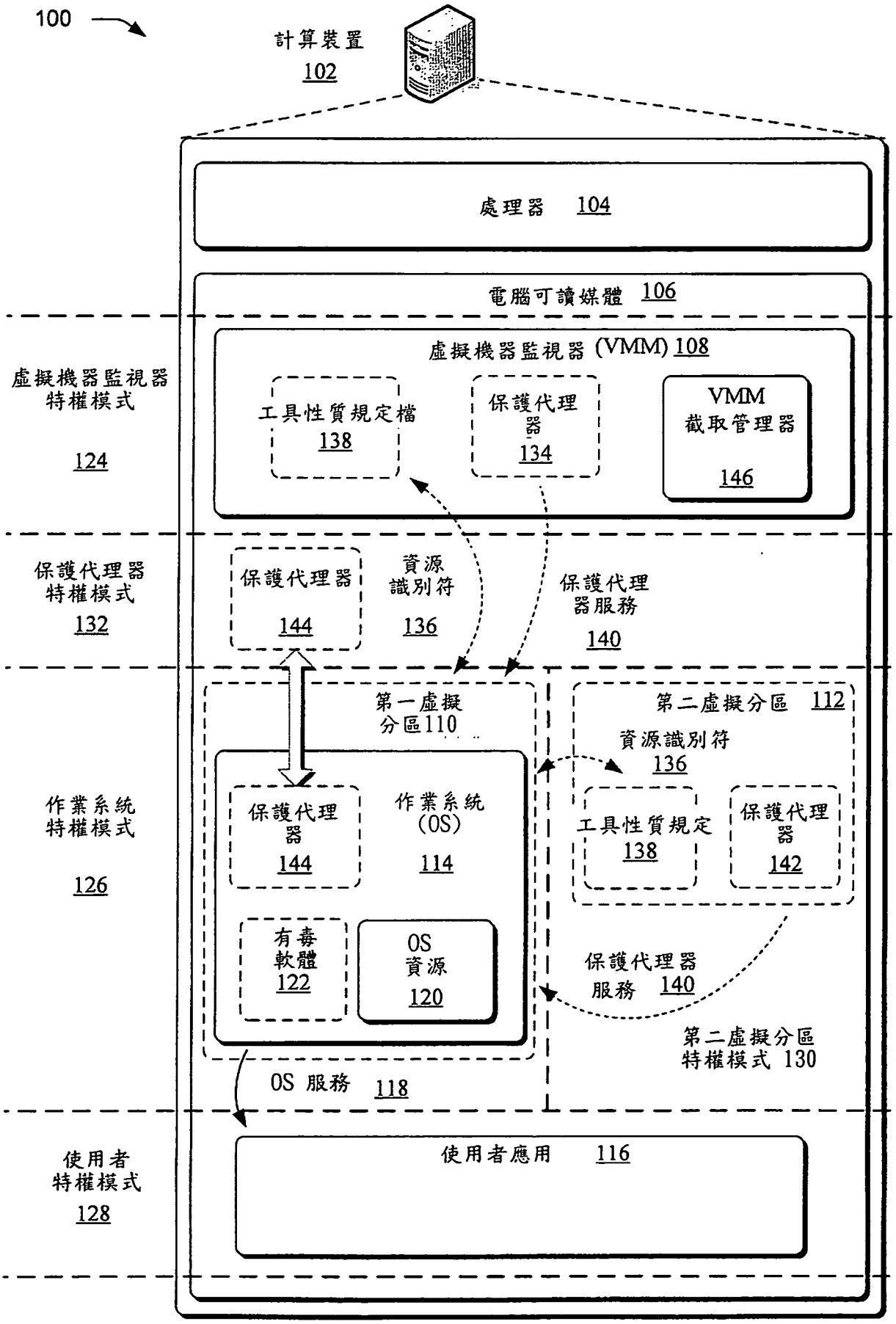
由一計算裝置執行該些指令時，可使該計算裝置執行包含以下步驟之動作：

經由一虛擬機器監視器來虛擬化該計算裝置為至少第一和第二虛擬機器分區，其中關聯於一作業系統特權模式的一作業系統常駐於該第一虛擬機器分區內，且一保護代理器(protection agent)常駐於該第二虛擬機器分區或該虛擬機器監視器內；

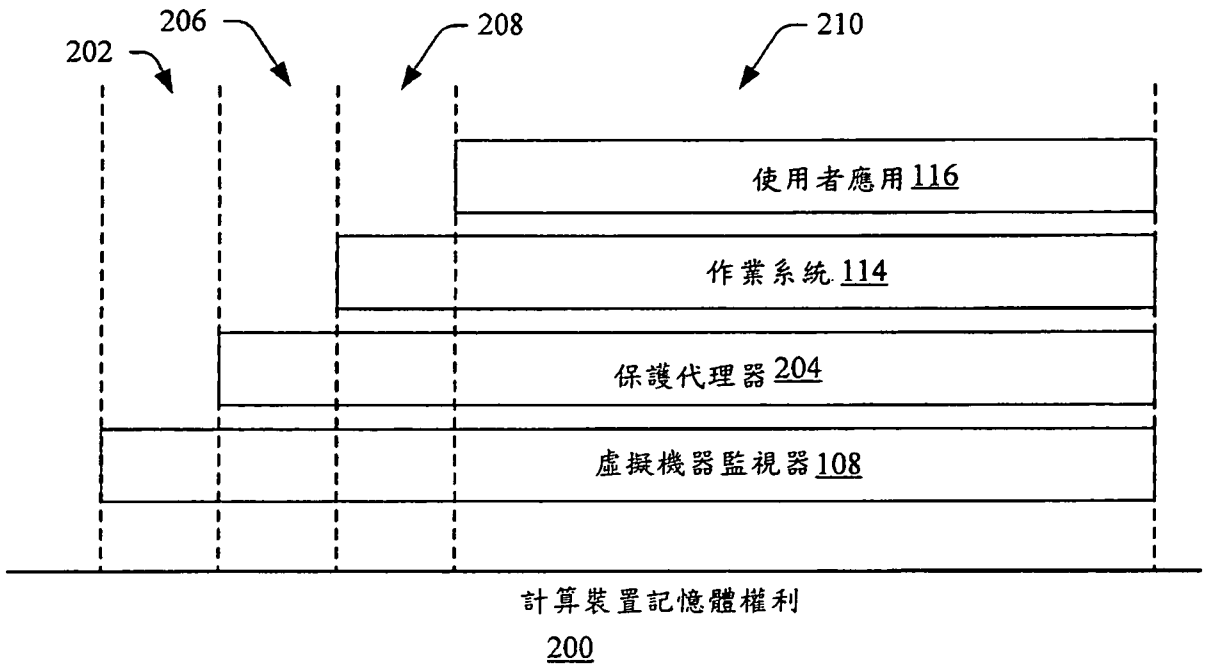
藉由該保護代理器來識別(i)常駐於該第一虛擬機器分區中的及(ii)經設計以在該作業系統特權模式內操作的一或更多個作業系統資源；

藉由該保護代理器來決定是否常駐於該第一虛擬機器分區中的該一或更多個作業系統資源中之一或更多者已被變更，其中常駐於該第二虛擬機器分區或該虛擬機器監視器內的該保護代理器不易遭受到來自該作業系統特權模式內的攻擊；

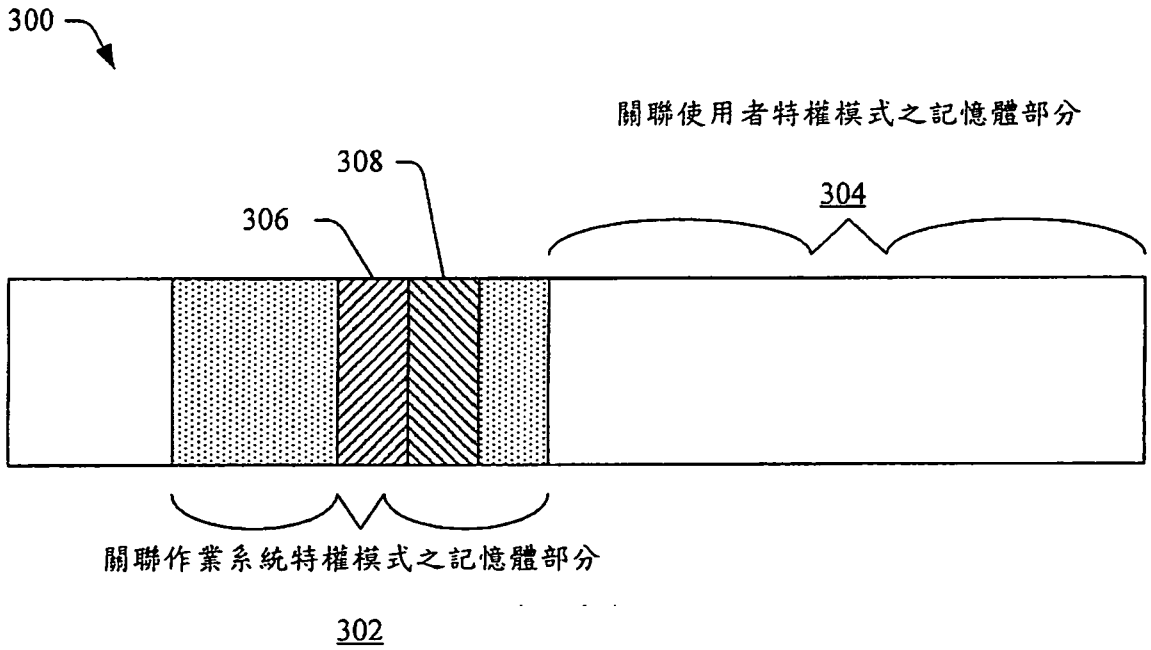
響應於決定出該一或更多個作業系統資源中之一或更多者已被變更，來關閉在該第一虛擬機器分區的關聯於該作業系統特權模式的該作業系統。


100
計算裝置
102
處理器 104
電腦可讀媒體 106
虛擬機器監視器 (VMM) 108
工具性質規定檔
138
保護代理器
134
VMM
截取管理器
146
虛擬機器監視器
特權模式
124
保護代理器
144
資源
識別符
136
保護代理
器服務
140
保護代理器
特權模式
132
第一虛擬
分區110
第二虛擬分區 112
資源識別符
136
保護代理
器
144
作業系統
(OS)
114
工具性質規定
138
保護代理
器
142
作業系統
特權模式
126
有毒
軟體
122
OS
資源
120
保護代理器
服務 140
第二虛擬分區
特權模式 130
OS 服務 118
使用者應用 116
使用者
特權模式
128

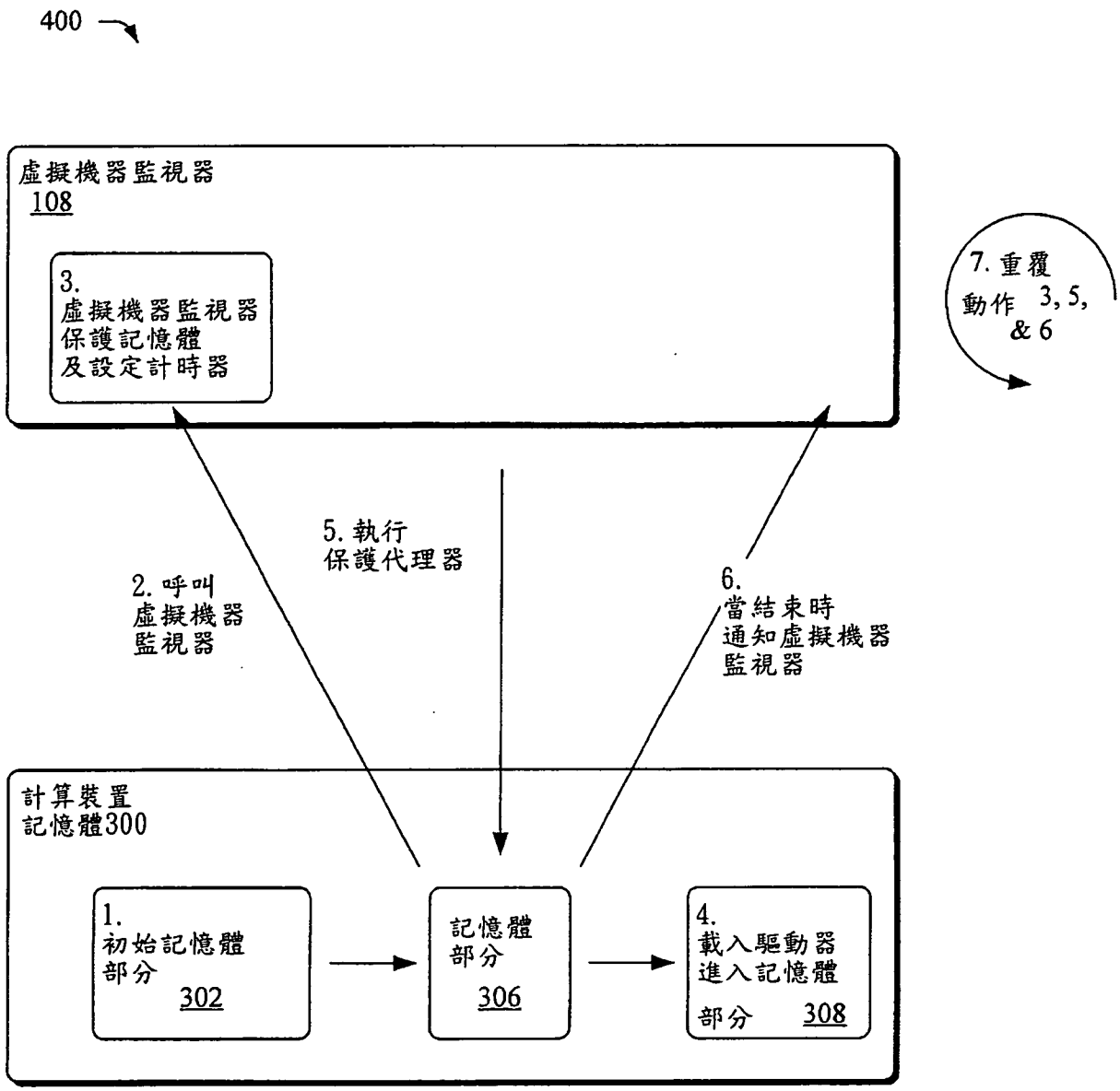
第1圖


206
208
210
202
使用者應用116
作業系統114
保護代理器204
虛擬機器監視器108
計算裝置記憶體權利
200

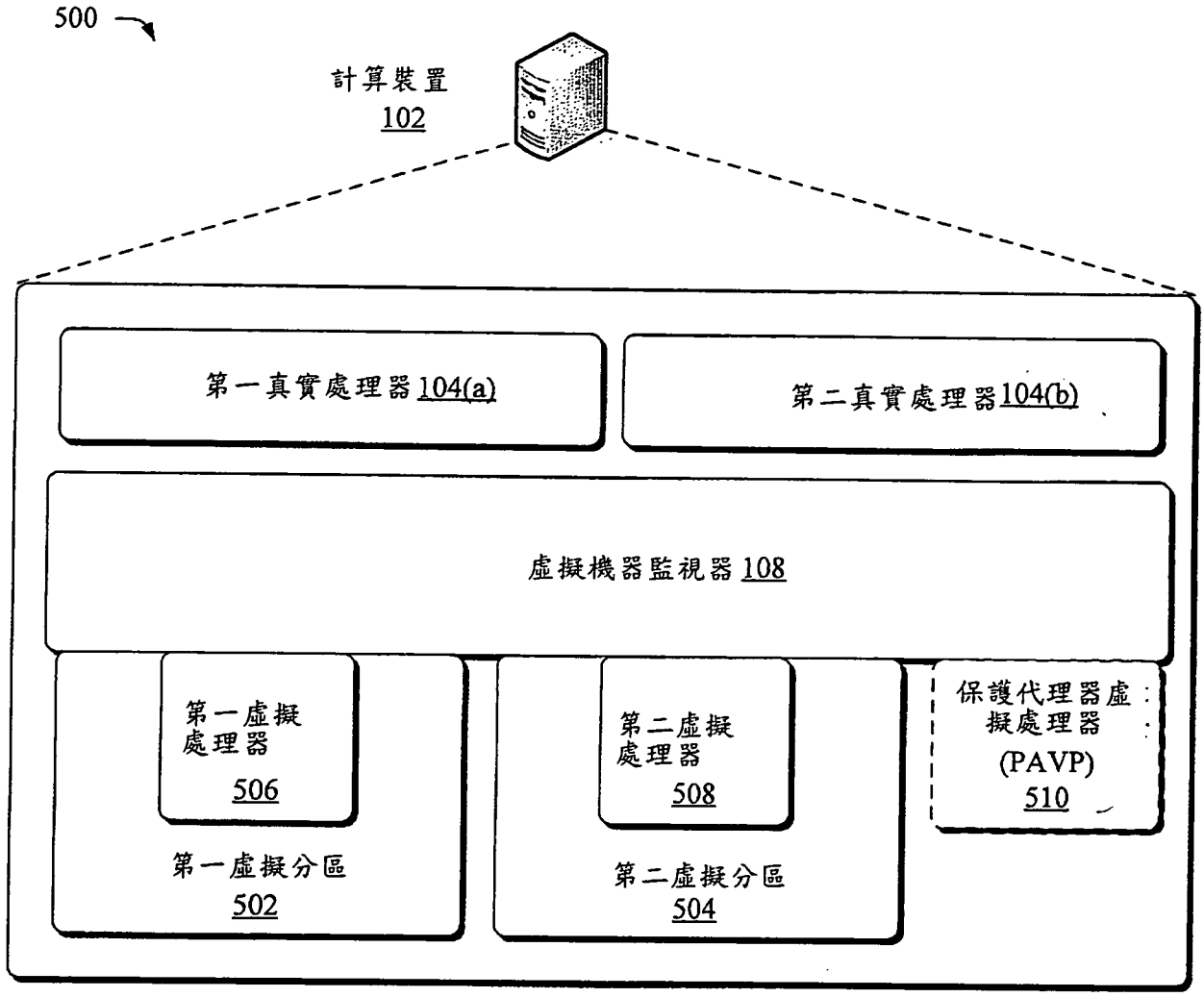
第2圖


300
關聯使用者特權模式之記憶體部分
308
306
304
關聯作業系統特權模式之記憶體部分
302

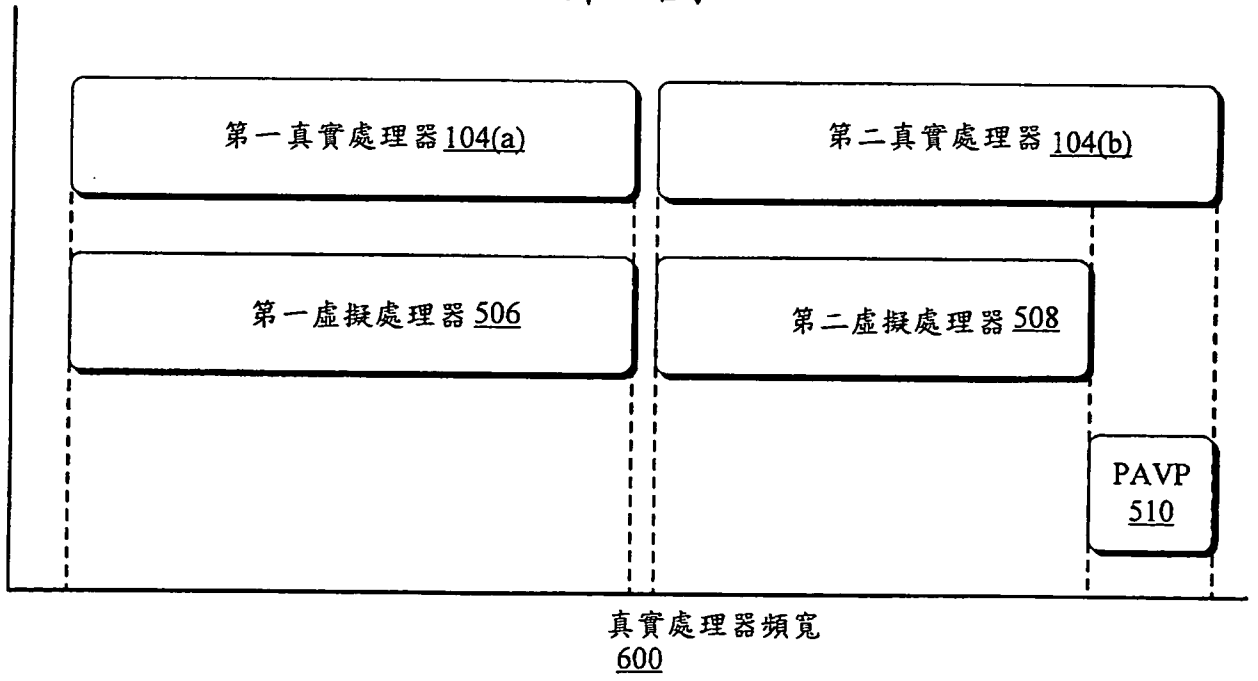
第3圖


400
虛擬機器監視器
108
3.
虛擬機器監視器
保護記憶體
及設定計時器
7. 重覆
動作 3, 5,
& 6
5. 執行
保護代理器
2. 呼叫
虛擬機器
監視器
6.
當結束時
通知虛擬機器
監視器
計算裝置
記憶體300
1.
初始記憶體
部分
302
記憶體
部分
306
4.
載入驅動器
進入記憶體
部分
308

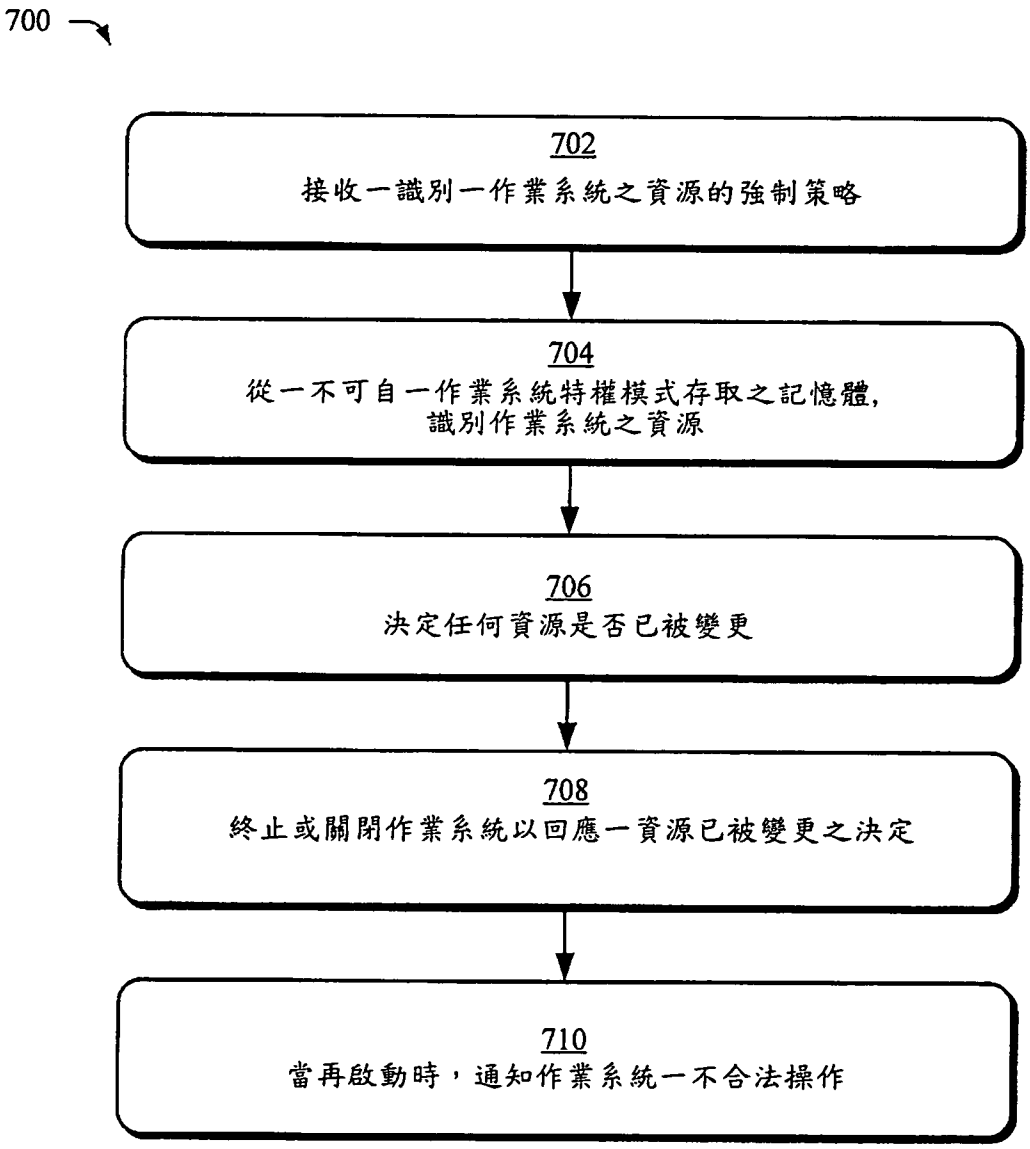
第4圖


500
計算裝置
102
第一真實處理器104(a)
第二真實處理器104(b)
虛擬機器監視器 108
第一虛擬處理器
506
第一虛擬分區
502
第二虛擬處理器
508
第二虛擬分區
504
保護代理器虛擬處理器
(PAVP)
510

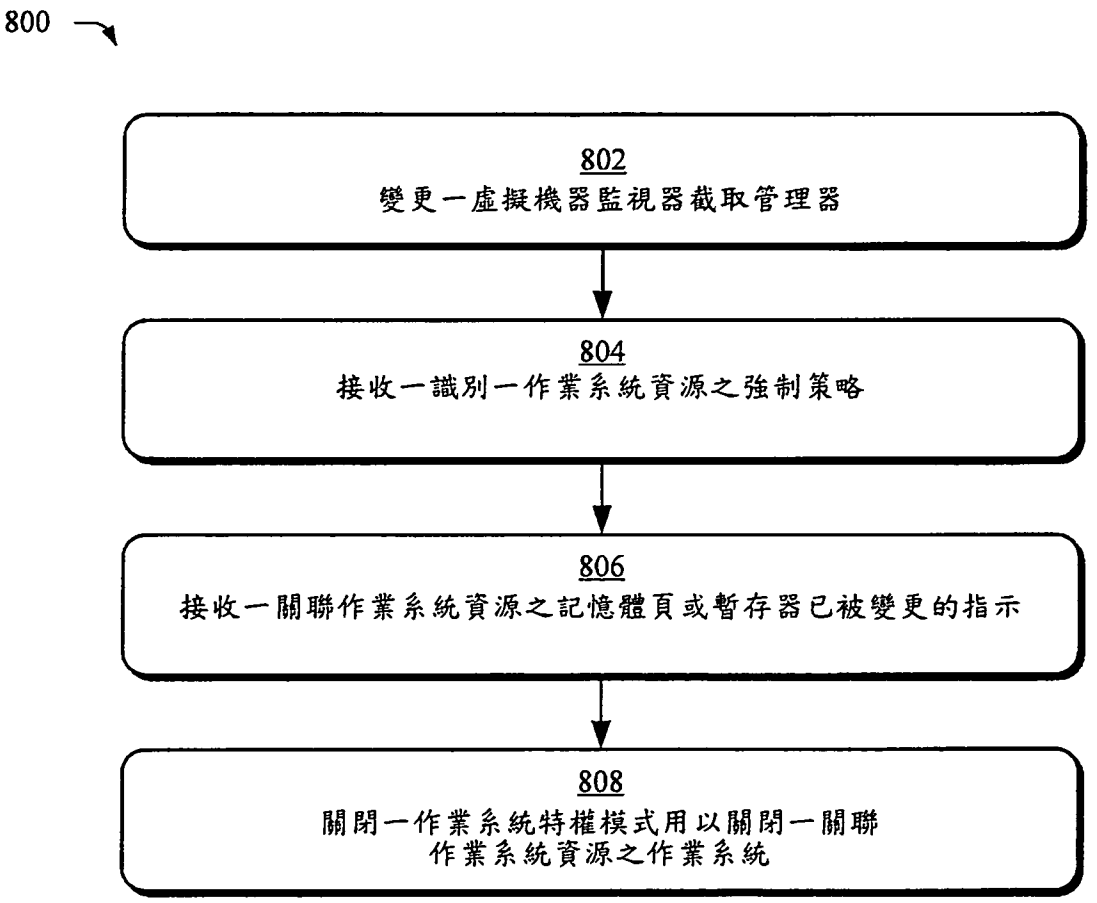
第5圖


第一真實處理器104(a)
第二真實處理器 104(b)
第一虛擬處理器 506
第二虛擬處理器 508
PAVP
510
真實處理器頻寬
600

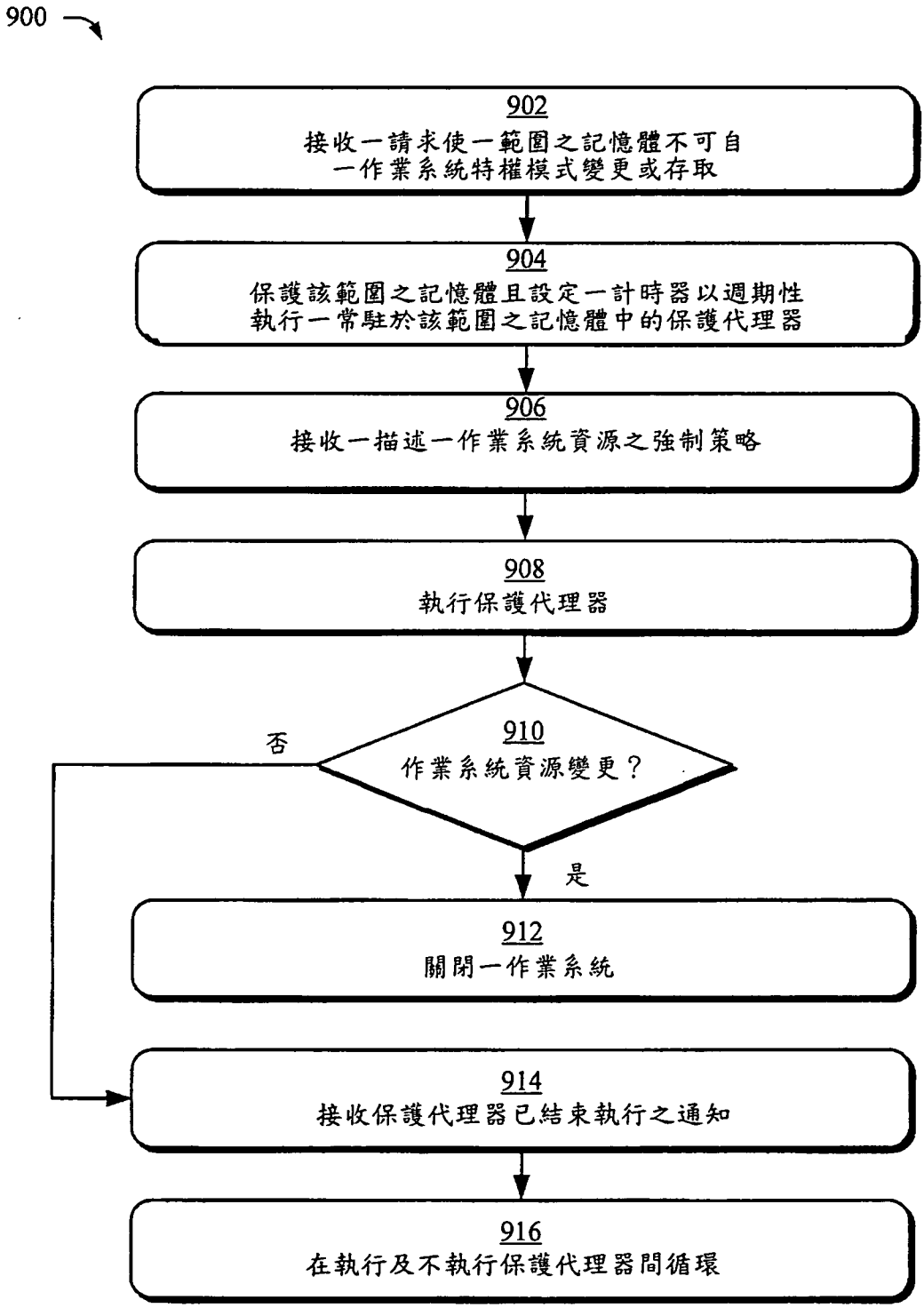
第6圖


700
702
接收一識別一作業系統之資源的強制策略
704
從一不可自一作業系統特權模式存取之記憶體，識別作業系統之資源
706
決定任何資源是否已被變更
708
終止或關閉作業系統以回應一資源已被變更之決定
710
當再啟動時，通知作業系統一不合法操作

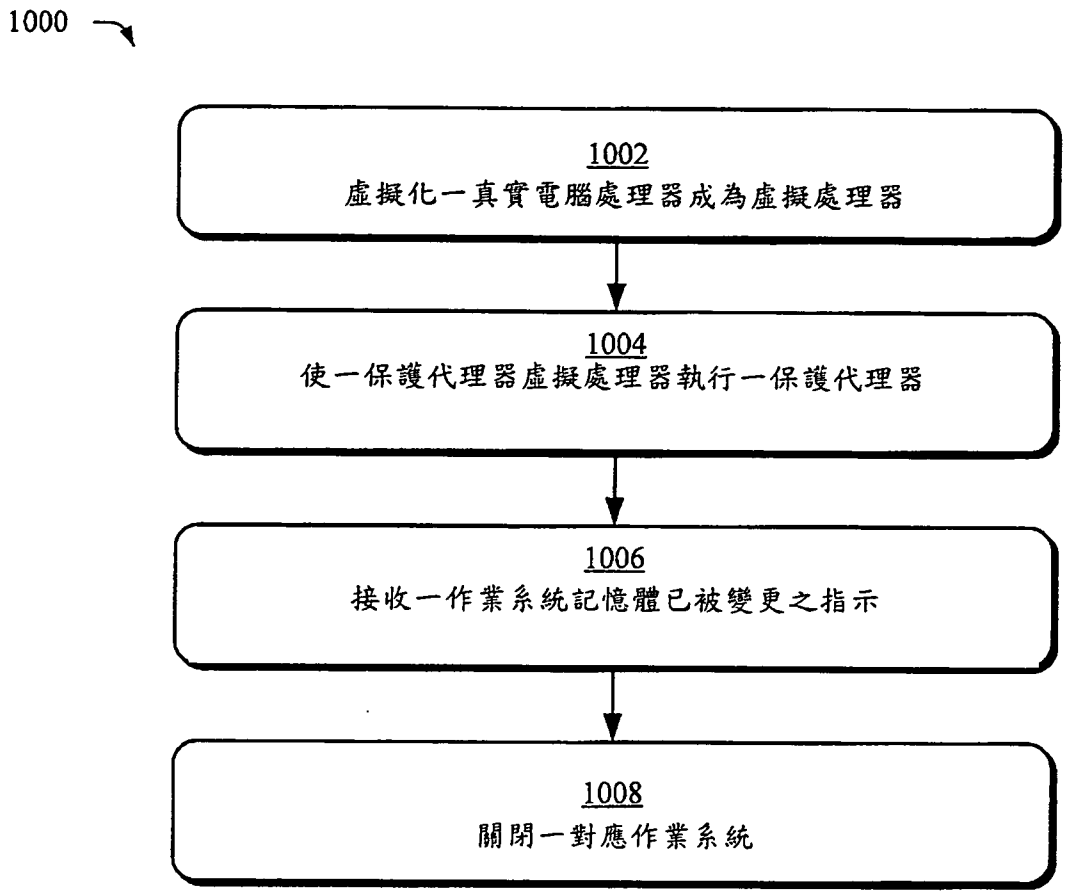
第7圖


800
802
變更一虛擬機器監視器截取管理器
804
接收一識別一作業系統資源之強制策略
806
接收一關聯作業系統資源之記憶體頁或暫存器已被變更的指示
808
關閉一作業系統特權模式用以關閉一關聯
作業系統資源之作業系統

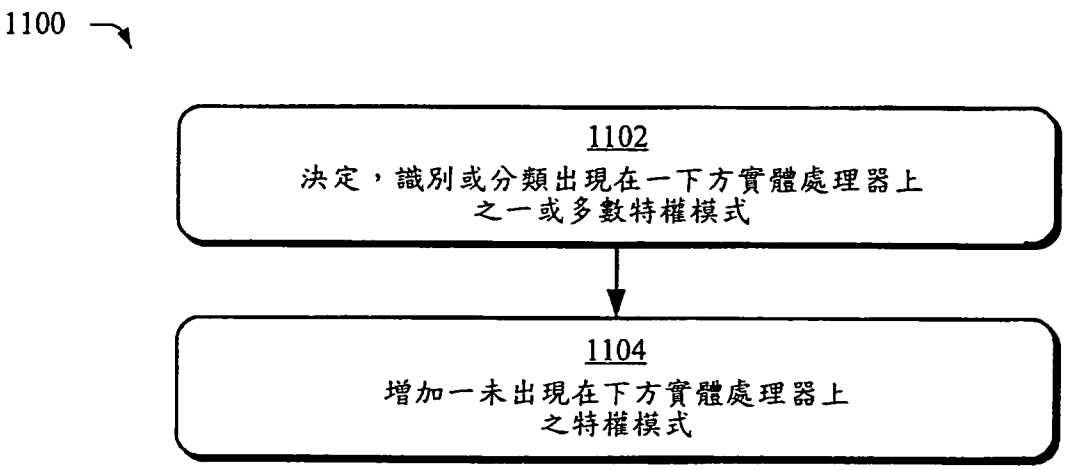
第8圖


900
902
接收一請求使一範圍之記憶體不可自一作業系統特權模式變更或存取
904
保護該範圍之記憶體且設定一計時器以週期性執行一常駐於該範圍之記憶體中的保護代理器
906
接收一描述一作業系統資源之強制策略
908
執行保護代理器
910
作業系統資源變更？
否
是
912
關閉一作業系統
914
接收保護代理器已結束執行之通知
916
在執行及不執行保護代理器間循環

第9圖


1000
1002
虛擬化一真實電腦處理器成為虛擬處理器
1004
使一保護代理器虛擬處理器執行一保護代理器
1006
接收一作業系統記憶體已被變更之指示
1008
關閉一對應作業系統

第10圖


1100
1102
決定，識別或分類出現在一下方實體處理器上之一或多數特權模式
1104
增加一未出現在下方實體處理器上之特權模式

第11圖