I387923

公告本

# 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：94137180

※ 申請日期：2005 年 10 月 24 日

※IPC 分類：
G06F 9/44, 9/54

## 一、發明名稱：（中文/英文）

用於在一例如虛擬機器或固化作業系統內管理電腦安全的方法及系統

COMPUTER SECURITY MANAGEMENT, SUCH AS IN A VIRTUAL MACHINE OR HARDENED OPERATING SYSTEM

## 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）

艾苹那諾爾 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 6 人）

**姓　名：**（中文/英文）

1.阿姆斯壯班哲明/ARMSTRONG, BENJAMIN

2.卡門斯強森/GARMS, JASON

3.雷肯尼士 D/RAY, KENNETH D.

4.奎瑞莫麥克/KRAMER, MICHAEL

5.英格蘭保羅/ENGLAND, PAUL

6.費爾德史考特 A/FIELD, SCOTT A.

國　籍：(中文/英文)

1.美國/USA

2.美國/USA

3.美國/USA

4.美國/USA

5.美國/USA

6.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；2004 年 12 月 21 日；11/019,094

☐ 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。

97.10.23 修正
年 月 日
P3~26 補充

## 五、中文發明摘要：

本發明揭示一種安全性方案，其對在一電腦上執行之一或多自我包含的作業環境實例提供安全性。該安全性方案包括實施一組安全性應用程式，其可由一監督處理或類似者控制。該組安全性應用程式及該監督處理兩者皆可在該電腦之一主控系統上作業，其亦可提供一平台以執行該等一或多自我包含的作業環境。該安全性方案保護在該等一或多自我包含的作業環境中執行的處理，及保護在該等自我包含的作業環境之外的電腦上執行的處理。

## 六、英文發明摘要：

A security scheme provides security to one or more self-contained operating environment instances executing on a computer. The security scheme may include implementing a set of security applications that may be controlled by a supervisory process, or the like. Both the set of security applications and the supervisory process may operate on a host system of the computer, which may also provide a platform for execution of the one or more self-contained operating environments. The security scheme protects processes running in the one or more self-contained operating environment and processes running on the computer outside of the self-contained operating environments.

## 七、指定代表圖：

(一)、本案指定代表圖為：第 2 圖。

(二)、本代表圖之元件代表符號簡單說明：

100 電腦系統

102 主控系統

118 虛擬機器

128 監督處理

200 離線掃描組態

202 安全性應用程式

## 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】

本發明概言之關於維護電腦作業系統之安全性及整合性。

【先前技術】

當特別設計來毀壞或混亂一系統之軟體(例如惡意軟體"malware")侵入一電腦系統時，該電腦之作業系統之整合性以及整個電腦系統即面臨極大的危險。電腦使用者在面對病毒、破壞程式及特洛伊木馬(Trojan)的威脅時，會有相當多的安全性考量及需求，大多數的電腦使用者係考慮到他們電腦的關鍵架構組件之整合性，例如作業系統處理、記憶體處理等。

某些型態的惡意軟體使用該作業系統授權的作業來攻擊電腦。這種授權的作業基本上包含指令或指令組，其僅可由一授權的使用者或處理來存取。例如，當惡意軟體不知何故能夠存取一或多這些授權的作業時，便會造成作業系統檔案之刪除或毀損、攻擊記憶體中之作業系統組件、刪除使用者檔案、以及許多其它有害的可能性。在某些案例中，甚至非惡意的處理也會透過存取授權的作業之未注意的行為而損害到一電腦系統。一般來說，只要藉由假冒一授權使用者之身份，幾乎任何的處理皆能夠存取授權的作業。

通常作業系統提供一種架構，以進行主控處理及提供

系統服務給那些處理。作業系統通常提供基本的安全性保護，例如加強系統資源的存取控制及擁有者權限。舉例而言，在正常作業系統環境中，保護性安全性服務(像是主控台防火牆、弱點評估、修補偵測、行為阻隔、主控台或網路侵入偵測及防毒科技等)皆在該作業系統中以本身的應用程式方式執行。雖然有這些方法，該作業系統有時候無法正確地決定是否已經被攻擊。特別是一旦有一段惡意碼或其它惡意軟體攻擊一電腦系統，並取得充份的控制時(例如管理者層級的存取)，因為嘗試判定其是否正遭受攻擊的機制亦會被破壞，所有作業系統判定其是否正遭受攻擊之嘗試即不再可靠。此係因為該惡意碼可以有效地修改該作業系統或應用程式用來保護它在記憶體中或磁碟上的結構。

一種保護一電腦系統及其作業系統的方式包含安裝一組安全性應用程式，例如防毒軟體、個人防火牆、及指令偵測系統。在具有多個電腦系統之系統中，例如一電腦網路或是在一陣列中部署的一電腦系統的叢集，每個個別電腦執行其本身的安全性應用程式組合。此係因為在該網路或陣列上的每個電腦系統實質上為與其本身網路附屬物、其本身的中央處理單元、及其本身一作業系統之實例等為一獨立的個體。這些安全性應用程式可以安裝在每個電腦系統上，以防止該電腦系統及其作業系統遭到危害，因為就像任何在該電腦系統上執行的其它應用程式，這種安全性應用程式亦會遭受攻擊，因此也無法保護該電腦系統。

在另一種保護一電腦系統及其作業系統之方法中，係由隔離該電腦系統之態樣來保護該電腦系統之一些態樣，例如計憶體。

【發明內容】

此處所述之電腦安全性技術提供了多種安全性特徵，其包括使用一單一安全性處理(或安全性處理組合)以監視、保護及修護在一主控系統上執行之多個邏輯性相隔離的虛擬機器。在一些具體實施例中，該等安全性技術提供了安全性給在一電腦上執行之一或多自我包含的作業環境實例(instance)。該等安全性技術可以包括實施一可由一監督處理控制的安全性應用程式。該安全性應用程式可以監視一或多個虛擬機器。該監視可使用多種技術完成，包括對於該安全性應用程式之虛擬機器的離線掃描、在每個虛擬機器上執行的一代理安全性處理等。

在一些具體實施例中，該組安全性應用程式及該監督處理皆可在該電腦之一主控系統上作業，其亦可提供一平台以執行該一或多自我包含的作業環境。該等安全性技術可以保護在該一或多自我包含的作業環境當中執行的處理，及在該自我包含的作業環境之外的電腦上所執行的處理。

【實施方式】

現在本發明將對於多個具體實施例來加以說明。以下

的說明提供了特定的細節以完整瞭解並進行說明本發明之這些具體實施例。但是，熟知該項技藝者將可瞭解本發明可以不利用這些細節來實施。在其它狀況中，並不會詳細顯示或說明熟知的結構與功能，以避免不必要地混淆本發明之具體實施例的描述。

本發明之目的在於使得在本說明中使用的該技術可以用其最廣泛的合理方式來解譯，即使其係配合本發明之某些特定具體實施例的詳細說明。某些用語甚至會在以下強調；但是，想要以任何有限的方式解譯的任何詞彙將會明顯及特定地定義為如同於此詳細說明章節中所述。

I. 概述

此處所述之電腦安全性技術提供了多種安全性特徵，其包括使用一單一安全性處理(或安全性處理組合)以監視、保護及修護在一主控系統上執行之多個邏輯性隔離的虛擬機器。

在一些具體實施例中，於一實體機器上執行的一主控系統提供一虛擬機器，在其上可以執行一作業系統及應用程式。雖然許多處理可在該虛擬機器上執行，概言之，在該虛擬機器上執行的作業系統及應用程式不能夠存取資源(例如記憶體及裝置)，除非由提供該虛擬機器的該主控系統所允許，或是由分派給一虛擬機器的一請求所指定。

如果一虛擬機器執行惡意軟體，任何的損害會侷限於該虛擬機器的作業系統、應用程式、及可存取的資源。依此方式，該電腦實質上可避免受到在該虛擬機器上所執行

的惡意軟體之影響。

在一些具體實施例中，該主控系統可防止在該等虛擬機器上執行的該作業系統及應用程式執行授權的作業，其會造成對於該實體機器之資源或作業系統的不想要的改變。例如，在該虛擬機器內而非在該實體機器內，對該虛擬機器上執行的作業系統給予管理授權。

在一些具體實施例中，該主控系統可實施主動安全性處理。這種安全性處理之範例包括主控端防火牆監視器，弱點評估監視器、修補偵測監視器、行為阻隔監視器、主控端或網路侵入偵測監視器、及防毒技術。概言之，該等安全性處理係設置以增進該等虛擬機器、該主控系統以及接下來之實體機器的安全性。

在一些具體實施例中，該等安全性處理係由該主控系統上執行的一監督處理所實施或控制。該監督處理可對該等虛擬機器之組件協助或提供該等安全性處理某種層級之存取及能見度，其中包括虛擬記憶體、虛擬磁碟、虛擬網路配接器、虛擬驅動程式等(例如型式上為記憶體中的資料結構或物件模型)。例如，該監督處理可允許該安全性處理在對應於一虛擬機器之虛擬硬碟上有惡意軟體或安全性侵害之跡象時，即掃描在記憶體中或儲存在磁碟上的一資料結構。此外(或另外)，當所提供的一物件模型由該主控系統支援時，該監督處理可造成回傳關於該虛擬機器之狀態的資訊(例如記憶體狀態或通信狀態)到該主控系統。概言之，因為該主控系統及監督處理提供某種層級的隔離，該

等安全性處理可監督及監視該等虛擬機器之安全性，而仍舊可以使得在這些虛擬機器中正執行的有害程式無法進行存取。依此方式，該等安全性處理即可利用使得這些程式在工作中受到監視的方式而可避免被損害或擊敗。

在一些具體實施例中，該等安全性處理可用於監視及修護一虛擬機器，其係在一儲存的狀態，其中該虛擬機器監視器已經停止執行，且其中所有關於該虛擬機器的記憶體、裝置及CPU狀態之資訊已經被寫出到一實體檔案。該等安全性處理亦可用於監視及修護處於暫停狀態中的一虛擬機器，其基本上由一虛擬機器管理者所喚起。在該暫停的狀態期間，該等虛擬機器停止執行，但隨時準備好來恢復進行下一個指令及處理。在該暫停或儲存狀態方案中，在該虛擬機器內的虛擬作業系統並不知道該狀態改變。類似地，該等安全性處理有能力在一虛擬機器被載入到該主控系統之前，即可進行掃描及修護或清除。

在一些具體實施例中，該主控系統可安裝一虛擬機器的硬碟，如同其為一實體硬碟，然後以一區塊層級來掃描該虛擬硬碟(類似任何其它安裝的硬碟)。舉例而言，該主控系統可利用能夠被載入到該實體機器的作業系統之一碟碟驅動程式。然後此碟碟驅動程式可轉譯該虛擬硬碟，並將其提交給該主控系統做為一當地附屬的磁碟。

另一種監視該等虛擬機器之方法為在每個虛擬機器中執行一「代理“agent”」安全性處理。依此方式，該代理安全性處理係關連於在該主控系統上的一主要安全性處

理。該代理安全性處理開啟一通信通道到該主要安全性處理，並協助發現及恢復來自該虛擬機器的攻擊。當此方案牽涉到於一攻擊期間該代理安全性處理遭到危害的風險時，該代理仍可透過該主要安全性處理而使其可使用一外部恢復選項。在一些方案中(例如牽涉到使用一超遮罩之方案)，該代理可在與其實際上監視的虛擬機器不同的一虛擬機器上執行。

在一些具體實施例中，該主控系統可對每個虛擬機器之整個狀態取出定期的快照“snapshot”。理論上，此取出的快照可即時地執行，而僅具有少許的效能負擔。但是，此技術可能有許多種變化。如果一安全性處理偵測到該虛擬機器內的一異常(例如惡意軟體覆寫了該作業系統或是惡意軟體將其本身顯示成記憶體中的程式)，然後該主控系統可恢復該虛擬機器的狀態回到最近的快照之狀態，採取行動以防止該異常的復發，並重新開始該虛擬機器。

II. 代表性系統

第 1-5 圖及以下的討論提供了對於可以實施本發明的一適當環境之簡短概要性描述。雖然並非必要，本發明的許多態樣仍以電腦可執行指令的一般內文來描述，例如可由一泛用型電腦執行的例式“routine”(例如一伺服器電腦、無線裝置或個人/膝上型電腦)。熟知該項技藝者將可瞭解到本發明可利用其它通信、資料處理、或電腦系統組態來實現，其中包括網際網路家電、掌上型裝置(包括個人數位助理 PDA)、穿戴式電腦、所有細胞式或行動電話類

型、嵌入式電腦(包括耦合到汽車者)、多處理器系統、微處理器為主或可程式化消費電子產品、機上盒、網路PC、迷你級電腦、主架構電腦及類似者。

本發明的各態樣可以實施在一具有特定目的之電腦或資料處理器中，其可被特定地程式化、設定或建構以執行在此處詳細描述之一或多電腦可執行指令。本發明的各態樣亦可實施於分散式運算環境中，其中工作或模組係由遠端處理裝置所執行，其係透過一通信網路所鏈結。在一分散式運算環境中，程式模組可同時位在本地或遠端記憶體儲存裝置中。

本發明之各態樣可被儲存或分配到電腦可讀取媒體上，其包括磁性或光學可讀取電腦磁碟，做為半導體記憶體上之微程式碼、奈米科技記憶體、有機或光學記憶體、或其它可攜式資料儲存媒體。實際上，在本發明各態樣中的電腦實施的指令、資料結構、螢幕顯示器及其它資料可被分佈在網際網路或其它網路上(包括無線網路)，可為一段時間內一傳遞媒體上的一傳遞信號(例如一電磁波、聲波等)、或可在任何類比或數位網路上提供(封包交換、電路交換或其它方式)。熟知該項技藝者將可瞭解到本發明的部份係置於一伺服器電腦上，而相對應的部份置於一客戶端電腦上，例如一行動裝置。

請參考第1圖，可以實施電腦安全性技術的一電腦系統(實體機器)100可提供多個組件。這些組件包括一主控系統102，其設置成在該電腦系統100上執行，其附加、

結合或取代一標準或泛用型電腦作業系統 104。在一些具體實施例中，該主控系統 102 可被設置成其可存取任何事物，除了是其本身固有及/或授權的監督及安全性功能之外。該主控系統 102 可以連繫一或多電腦資源，例如具有一記憶體管理單元(MMU)108、一磁碟 110、一記憶體 112、一通信子系統 114 及一或多系統驅動程式 116 之一處理器 106。

在一些具體實施例中，該等一或多虛擬機器 118 可在該主控系統 102 的控制之下執行，並可隸屬於該主控系統 102。每個該等虛擬機器 118 可以包含組件的集合，其可協助一處理器及其它機器資源之虛擬化或仿真“emulation”。例如在所例示的具體實施例中所示，每個該等虛擬機器 118 可存取一組仿真的資源，其包括虛擬網路配接器 119、虛擬記憶體 120(其可包含該實體機器的記憶體 112 之一配置的部份)、虛擬磁碟 122、及一或多虛擬驅動程式 124，其每一個代表了非虛擬系統驅動程式 116 之一虛擬實例。一虛擬作業系統實例 126 可在每一個這些虛擬機器 118 上執行。在一些具體實施例中，該虛擬作業系統實例 126 可為該實體機器的作業系統 104 之完整或部份的複製。

概言之，該等虛擬機器 118 可根據該 MMU 108 以提供多種頁面層級的保護。概言之，在每個該等虛擬機器上執行的應用程式或處理 129 僅使用它們個別的虛擬機器之該等仿真的資源(例如虛擬記憶體 120、虛擬磁碟 122、虛

擬驅動程式 124、作業系統 126 等)。這些應用程式或處理 129 有時候稱之為「訪客」(guest)碼。該等仿真的資源通常係假設有某種程度的信任度，使它們可具有在該主控系統 102 上的標準保護機制，且除非有明確的指示，否則不能暴露任何主控系統使用者資料給該訪客碼。

在一些具體實施例中，該等仿真的資源可在該主控系統 102 與在該虛擬機器 118 上執行之訪客碼之間使用數種整合技術來交換資料，例如 I/O 埠存取、記憶體映射暫存器、直接記憶體存取(DMA)、中斷等。其它資料交換技術包括剪貼簿共享、檔案拖放、時間同步化等。為了支援這些資料交換技術，該等虛擬機器 118 可提供數種設施，其包括非同步訪客事件、同步主控端呼叫、該訪客碼與主控系統 102 之間的資料傳遞，整合服務註冊等。

該等虛擬機器 118 可在該主控系統 102 上使用任何數種可能的技術來產生或啟始。舉例而言，在一具體實施例中，該主控系統 102 可產生並啟用一虛擬機器的實例，並在產生當時設置該虛擬機器之參數。在一些具體實施例中，該主控系統 102 可定位在磁碟 110 上一既存的虛擬機器影像(可能是共享形式)，並載入該影像做為一新的虛擬機器實例。在一些狀況中，此載入係稱之為「匯入」一虛擬機器實例，且某種程度類似於一「匯入」功能，由一個應用程式帶入資料到另一個應用程式。

在一些具體實施例中，一組一或多監督處理 128 在該主控系統 102 上執行。在一些具體實施例中，該一或多監

督處理 128 可以完整或部份地存取該虛擬作業系統實例 126，並可提供一安全性服務到每個該等虛擬機器 118。在一些具體實施例中，該等監督處理 128 亦可管理活動，例如數位權限管理(DRM)及版權控制。因為此組態提供了在該等虛擬機器 118 上執行的任何惡意軟體無法存取每個虛擬機器之外的資源，該監督處理 128 概言之即為安全，可不受到惡意軟體之破壞。

在一些具體實施例中，該一或多監督處理 128 控制一組安全性應用程式(如防毒軟體、個人防火牆、入侵偵測系統等)，其可保護及/或監督所有在該主控系統 102 上的虛擬機器 118。舉例而言，該一或多監督處理可以由該組安全性應用程式協助離線掃描多個虛擬機器。離線掃描可包括設置該組安全性應用程式為知道每個該等虛擬機器之虛擬資源，因為它們皆為存在於該電腦系統(實體機器)上的虛擬物件。依此方式，該組安全性應用程式可以由該虛擬機器外部來檢查(掃描)那些虛擬資源(例如使用對於該虛擬機器資料結構的內部格式的知識)。

雖然此處使用用語「安全性應用程式」及「監督處理」，這些觀念並不限於應用程式或處理。而是，用以提供服務給一虛擬機器及/或其資源的任何公用程式或設施均可在該主控系統上實施，並達到所要的結果，其皆不背離本發明之範圍。這種公用程式或設施之一些範例包括一防廣告軟體公用程式、一防間碟軟體公用程式、及一磁碟重整器等。

離線掃描虛擬機器資源可以在當該等虛擬機器正在運行或休眠時(例如在暫停或儲存的狀態)來進行。舉例而言，如果一虛擬機器係藉由定位並載入一既有的虛擬機器影像進入到該主控系統 102 上所產生，該離線掃描(及任何所需要的清除或修護)皆在該虛擬機器實例被「匯入」之前發生。可在一暫停或儲存的狀態中掃描的虛擬機器資源包括虛擬硬碟、虛擬機器記憶體內容、虛擬通信埠緩衝器結構等。在一些實施例中，其不可能存取一暫停之虛擬機器的記憶體。但是，該虛擬機器記憶體仍可在當該虛擬機器在一儲存的狀態時或透過一虛擬機器的快照來進行存取。

請參考第 2 圖，所示為一離線掃描組態 200 之範例，其例示出第 1 圖之多種組件。在此組態中，一安全性應用程式 202 及一選擇性監督處理 128 存在於該主控系統 102 上。該安全性應用程式 202 可至少部份地由該監督處理 128 所控制，其可檢視該虛擬機器 118 之資源做為一資料結構或資料結構組合，並可在有安全性破壞跡象時進行掃描。為了允許它可用原始型式來存取該虛擬機器 118 之資源，並正確地偵測安全性破壞，該安全性應用程式 202 可依賴有關關連於該等資源之資料結構的語法及組態之資訊。在一些具體實施例中，此資訊可被更新來反應出該等資料結構之語法及組態中任何刻意的改變。

例如，第 2 圖之安全性應用程式 202 可為一防毒掃描引擎，其可掃描該虛擬機器 118 以決定是否其被一種或多種已知的病毒或破壞程式所感染。當該掃描處理開始時，

該防毒引擎202載入一目前簽章定義檔案到其程式記憶體中。例如，該簽章定義檔案可定義該虛擬機器的虛擬硬碟結構之語法及組態，藉此當其掃描在該虛擬機器之硬碟本身的目前狀態，即可提供該防毒引擎之參考點。

接著，該防毒引擎指引其掃描以讀取該實體機器之硬碟中關連於該虛擬機器之虛擬硬碟的一部份。依此方式，該防毒引擎可有效地讀取該虛擬硬碟之內容，並比較其內容(例如一內容物件)與其已知惡意內容之表列，其為偵測惡意軟體技術之專業人士所使用的方法及技術。為達到此範例之目的，在該虛擬硬碟內的一內容物件可為一檔案、或由該作業系統所操縱的另一個物件，例如來自 Microsoft Windows System Registry 的一金鑰；或在磁碟上任何其它物件，其可辨識為惡意或不想要之軟體的一實例之一部份。在發現到惡意軟體時，該防毒引擎可嘗試移除任何攻擊物件，或移除位在一物件內之感染。

第 3A 圖提供了一離線掃描組態 300 之第二範例。在此組態中，由該監督處理 128 所支援的一虛擬機器物件介面 302 透過一安全性應用程式 304 可存取該等虛擬機器之資源來提供一致性介面。該虛擬機器物件介面 302 可映射不同虛擬機器之間會有所變化之虛擬機器資料結構到一共用格式，其可由用以掃描及其它活動之安全性應用程式 304 所存取。因此，該安全性應用程式 304 僅需要被開發以存取此共用格式，而不需要是一虛擬機器所會具有的每一種格式變化。舉例而言，該主控系統 102 可以發現關於

該等虛擬機器 118 之狀態的資訊(例如磁碟狀態、記憶體狀態或通信狀態等)，所以一安全性應用程式 304 可監視它們，尋找安全性危害或其它問題。此外，該虛擬機器物件介面 302 可提供會由多種安全性應用程式使用的功能。舉例而言，該虛擬機器物件介面 302 可提供一種功能，以允許另一個安全性處理對於具有惡意內容(像是破壞程式有效負載)之進入的網路封包來掃描該虛擬機器之虛擬網路配接器。

此組態提供了該虛擬機器之設計者與該安全性應用程式之設計者有一些彈性。舉例而言，該虛擬機器之設計者可以改變該虛擬機器之資料結構，而對於該安全性應用程式之設計者沒有影響。因此，該安全性應用程式 304 僅需要被開發以存取此共用格式，而不需要是一虛擬機器所會具有的每一種格式變化。

在一些具體實施例中，該離線掃描技術協助該虛擬機器之目前狀態與該安全性應用程式所察覺的該虛擬機器之目前狀態兩者的同步化，藉此提供更為準確及一致性的掃描能力。此同步化可使用於當該虛擬機器的狀態快速變化時。

請參考第 3B 圖，一種可達到此同步化之方法為藉由執行一代理處理 322，其可提供對於該虛擬機器之近乎即時性的自我一致性觀點。該可在該虛擬機器 118 上執行代理處理 322 即可匯出該虛擬機器的此觀點到該虛擬機器物件介面 302，其即可提供適當的資訊到該監督處理及/或安

全性應用程式。在一些具體實施例中，該代理處理 322 可提供一應用程式化介面(API)給該虛擬機器物件介面 302 使用。(另外，該安全性應用程式可提供一類似的 API 給該虛擬機器物件介面 302 使用)

另一種達到此同步化之方式為其可使得該虛擬機器 118 產生其狀態之恆定的快照，並儲存這些快照在記憶體中或磁碟上。當這些快照可為數秒的「失效性」，它們仍然將是自我一致性。

請參考第 3C 圖，其為用以提供該等虛擬機器之安全性掃描之另一種技術，其中設置一系統 330，所以一安全性應用程式 336 與監督處理 334 係在一指定的虛擬機器 332 上執行(而非直接在該主控系統 102 上執行)。然後該安全性應用程式 336 與監督處理 334 可以監視及/或掃描其它的虛擬機器 118 來偵測問題。依此方式，該指定的虛擬機器 332(其可專屬於提供安全性監視)可以維持保護而不受到攻擊。

III. 系統流程

第 4 圖到第 8 圖為代表性的流程圖，其顯示了在第 1 圖之系統內發生的處理。這些流程圖並未顯示出所有功能或資料的交換，而是提供了對於命令及在該系統之下交換的資料的瞭解。熟知該項技藝者將可瞭解到一些功能或命令與資料的交換可以重複、改變、省略、或增補、並可以立即地實施其它未顯示的態樣。

請參考第 4 圖，例如由第 1 圖之監督處理所執行的一

監督例式“routine”400，其可在該主控系統上執行(或在其之外執行)，以監視、修正及/或設置在該虛擬機器上執行之處理或虛擬作業系統。另外，該監督例式400可以監視、修正及/或設置在一固化“hardened”(但非虛擬)作業系統上執行的處理。

在方塊401中，該例式400暫停該虛擬機器作業系統。在決策方塊402中，該例式400檢查由於在該虛擬機器內發生之破壞活動(如惡意處理“rogue processes”)所造成的改變。舉例而言，該例式400可以掃描該虛擬機器作業系統核心之一部份來檢查問題。另一種(或在其之外)監視該虛擬作業系統核心的方法為該例式400可以監視連接到該虛擬(或固化)作業系統之其它態樣。舉例而言，該例式400可監視虛擬位址空間、監視仿真的裝置、監視一仿真的硬碟機、執行整合性驗證(例如執行總和檢查)、檢查存在於該虛擬磁碟或在記憶體中之檔案的整合性等等。

在決策方塊402中，如果該例式400並未偵測到由於危害活動所造成的改變，該例式400進行到方塊404來在結束之前重新啟動該虛擬作業系統核心。但是，在一些具體實施例中(未例示)，該例式400可以迴路到方塊401(在一段時間過去之後)，以執行該暫停，並再次檢查步驟(除非該虛擬作業系統實例已經終止)。但是在決策方塊402中，如果該例式400偵測到由於危害活動所造成的改變，該程序進行到方塊403，其中該程序啟始了封鎖動作。範例性封鎖動作可包括的活動像是暫停該訪客作業系統來進

行額外的掃描、暫停選擇處理、清除該惡意軟體、重新格式化該虛擬作業系統來修護任何的損害、在取出一「快照」之後關閉該虛擬機器，所以該虛擬機器環境可在一旦重新開始該虛擬機器之後或多或少地恢復。

第5圖提供了由一監督處理所協助的一離線掃描例式500之範例，其可控制一組安全性應用程式(例如防毒軟體)用以執行離線掃描，並修復在該主控系統上執行的一虛擬機器。在方塊501中，該例式500取得該執行中虛擬機器的目前狀態之定期快照。在方塊502中，該程序掃描所取得的定期快照。在決策方塊503中，如果偵測到一問題，該程序進行到方塊504，其中該程序通知該執行中虛擬機器的問題，或是另可指示該虛擬機器來退回到問題發生之前的最後儲存之狀態。在決策方塊503中，如果該例式500並未偵測到一問題，該程序即回到方塊501以取得下一個定期快照。

第6圖提供了由一監督處理所協助的一離線掃描例式600之範例，其可控制一組安全性應用程式(例如防毒軟體)用以執行離線掃描，並修復在該主控系統上執行的多個虛擬機器。舉例而言，該例式600可用以偵測及恢復由於一惡意軟體感染所除能的一虛擬機器。在方塊601中，該例式600安裝該虛擬機器的下一個結構或組件到該主控系統上，其方式可類似於安裝一實體磁碟。依此方式，該結構或組件係加入成為電腦之作業系統之一部份，而非視為一外部掃描的物件。該結構或組件由該主控系統之觀點來看

可為一仿真的組件。在一些具體實施例中，該虛擬機器之結構或組件可被物件化，使得該主控系統可提供一介面給該組安全性應用程式來掃描它們。例如，該虛擬機器的記憶體可被物件化以掃描記憶體中的惡意軟體。

在方塊602中，該組安全性應用程式掃描該虛擬硬碟結構(或記憶體中結構等)。在決策方塊603中，如果該掃描的結構有危險，則該例式600繼續到方塊604，其中該等安全性應用程式修護該虛擬硬碟機結構(或記憶體中結構)。但是在決策方塊603中，如果該掃描組件並無危險，該程序進行到程序方塊605。

在決策方塊605中，如果該虛擬機器之所有結構或組件皆已被掃描，該程序即結束。否則，該程序回到方塊601，以安裝下一個虛擬機器結構或組件。

在一些具體實施例中，該例式600可用於結合最佳化技術，其可追蹤每個虛擬機器硬碟機中掃描之間所發生的變化。依此方式，該例式600可以僅自從上一次掃描之後的變化，藉此可改善掃描的效率。舉例而言，一最佳化程序可在一區塊層級上來追跡該虛擬機器之硬碟機中的變化。然後為了掃描的目的，該區塊層級上的變化可以映射到在一檔案層級上的變化(因為典型的防毒軟體係在檔案層級掃描)。另外，變化可由檢視修正來追跡，以主控檔案表結構。其中可包含在該主控系統中先前主要檔案表之檢查點儲存。

第7圖提供了由一監督處理所協助的一離線掃描例式

700之範例，其可控制一組安全性應用程式(例如防毒軟體)用以執行離線掃描，並修復在該主控系統上執行的多個虛擬機器。舉例而言，該例式700可用以偵測及恢復由於一惡意軟體感染所除能的一虛擬機器。相對於第6圖之離線掃描程序，其在掃描之前安裝該虛擬機器之結構或組件，第7圖之程序可在外部掃描該結構或組件。在方塊701中，該例式700掃描該虛擬機器之下一個結構或組件。該結構或組件由該主控系統之觀點來看可為一仿真的組件。在一些具體實施例中，該虛擬機器之結構或組件可被物件化，使得該主控系統可提供一介面給該組安全性應用程式來掃描它們。例如，該虛擬機器的記憶體可被物件化以掃描記憶體中的惡意軟體。

在決策方塊702中，如果該掃描的結構有危險，則該例式700繼續到方塊703，其中該等安全性應用程式修護該虛擬硬碟機結構(或記憶體中結構)。但是在決策方塊702中，如果該被掃描的組件並無危險，該程序進行到決策方塊704。在決策方塊704中，如果該虛擬機器的所有結構或組件皆已被掃描，該程序即終止。否則，該程序回到方塊701，以安裝下一個虛擬機器結構或組件。

第8圖提供了由一監督處理所協助的一離線掃描例式800之第二範例的流程圖，其可控制一組安全性應用程式(例如防毒軟體)用以執行離線掃描，並修復在該主控系統上執行的多個虛擬機器。在該例式800中，一代理處理(像是第3B圖之代理處理322)使得該虛擬機器在其正被掃描

時之達到其實際狀態的同步化，且該虛擬機器之狀態係由該等安全性應用程式所察覺。

在方塊 801 中，例式 800 透過一些機器間通信介面以建立了該安全性應用程式(像是第 3B 圖之安全性應用程式 304，其係在該主控系統或一虛擬機器物件介面上執行)及該代理處理之間的通信。在方塊 802 中，該例式 800 可建立對於該虛擬機器之記憶體的存取。舉例而言，在該主控系統上執行之代理處理可提供對於對應於該虛擬機器之應用程式記憶體的一虛擬緩衝器之存取。該程序繼續到方塊 803，其中當出現一安全性問題時，該安全性應用程式掃描該記憶體。舉例而言，當該安全性應用程式為一防毒掃描引擎，該防毒掃描引擎可以掃描該記憶體，以尋找可符合已知惡意軟體之簽章的編碼樣式。在決策方塊 804 中，如果該虛擬機器之任何結構或組件已受到危害，該程序繼續到方塊 805，其中該安全性應用程式及/或該代理處理可清除該電腦記憶體。另外，該安全性應用程式可發信給該代理處理來採取導引到該虛擬機器之修正動作。但是在決策方塊 804 中，如果沒有結構或組件受到危害，則該程序即結束。

IV. 結論

除非該內文清楚地需要，否則在整個說明及申請專利範圍中，該用語「包含」及類似者可被視為一種包含式的意義，相對於一排除式或窮盡式的意含；也就是說，其意義為「包括，但不限於」。此外，當用於此申請案中，該用

語「此處」、「以上」、「以下」及類似匯入的用語等，必須將此申請案視為一個整體，並非對於此申請案的任何特定部份。當該等申請專利範圍使用用語「或」來參照到兩個或更多項目之表列時，該用語涵蓋該用語之以下所有的轉譯：在該表列中任何的項目、在該表列中所有項目、及在該表列中項目的任何組合。

以上本發明之具體實施例的詳細描述並非是要窮盡，或是要限制本發明到上述之精確的形式。本發明之特定具體實施例及範例在上述是以例示性的目地來描述，在本發明內有多種同等之修正的可能性，其皆為熟知該項技藝者可瞭解。例如，處理或方塊係以一特定順序呈現，其它的具體實施例則可用不同的步驟順序來執行程序或利用具有區塊的系統，且一些處理或區塊可被刪除、移動、加入、分離、組合及/或修正。每個這些處理或區塊可用多種不同的方式來實施。同時，當處理或區塊有時候係以序列的方式顯示時，這些處理或區塊可另以平行的方式執行，或可在不同的時間執行。當該內文允許時，在上述詳細說明中使用單數或複數的用語亦可分別包括該內文所允許之複數或單數。

在此提供之本發明的教示可以應用到其它系統，而非必要為此處所述的系統。上述多個具體實施例之元素及動作可被結合來提供另外的具體實施例。

此申請案係關連於相同受讓人的美國專利申請案，其名稱為「自我治療裝置之方法及系統」"Method and System

for a Self-healing Device"，其於 2004 年 12 月 21 日申請。所有上述之專利及申請案及其它參考文件，包括任何在附屬申請文件中所列出者，皆在此引用參照。如果需要的話，本發明之各態樣可被修正以使用上述之多種參照的系統、功能及觀念，以提供本發明進一步的具體實施例。

在上述的說明之下，可對本發明進行這些及其它改變。當以上的說明詳述了本發明之某些具體實施例，並描述了所認知的最佳模式，不論以上在文字中出現如何詳細的說明，本發明可用許多方式來實施。如上所述，當說明本發明之某些特徵或層面所使用的特定技術必須不能視為代表該詞彙在此處重新定義，並限制到該詞彙所關連之本發明的任何特定特性、特徵或層面。概言之，在以下申請專利範圍中所使用的用語必須不能視為限制在本說明書中所揭示的該等特定具體實施例，除非以上詳述之說明段落明確地定義這些用語。因此，本發明之實際範圍不僅包含所揭示的具體實施例，但是實施或實現本發明之所有同等的方式皆在申請專利範圍之下。

當本發明之某些層面在以下採用某種申請專利範圍型式來呈現時，本發明人係以任何數目之申請專利範圍型式來考慮本發明之不同層面。舉例而言，單僅列舉了本發明的一個層面如同在一電腦可讀取媒體中所包含者，其它的層面亦可類似地包含在一電腦可讀取媒體上。因此，本發明人在提出該申請案之後保留權限來加入額外的申請專利範圍，以對於本發明之其它層面繼續進行這種額外的申請

專利範圍型式。

【圖式簡單說明】

第 1 圖所示為在一具體實施例用以實施安全性技術之系統的範例方塊圖。

第 2 圖所示為在第 1 圖之系統中虛擬機器之離線掃描範例的方塊圖。

第 3A 圖所示為在第 1 圖之系統中虛擬機器之離線掃描另一個範例的方塊圖。

第 3B 圖所示為在第 1 圖之系統中虛擬機器之掃描的另一範例之方塊圖。

第 3C 圖所示為在第 1 圖之系統中虛擬機器之掃描的又另一範例之方塊圖。

第 4 圖所示為在第 1 圖之系統中監視一作業系統的一監督處理所執行之程序的流程圖。

第 5 圖所示為在第 1 圖之系統中使用定期掃描之監視該等虛擬機器之一安全性監視程序的範例之流程圖。

第 6 圖所示為在第 1 圖之系統中使用虛擬機器結構安裝以監視該等虛擬機器之一安全性監視程序的第二範例之流程圖。

第 7 圖所示為在第 1 圖之系統中使用虛擬機器結構安裝以監視該等虛擬機器之一安全性監視程序的第三範例之流程圖。

第 8 圖所示為在第 1 圖之系統中使用在該虛擬機器上

執行之一代理處理以監視該等虛擬機器之一安全性監視程序的第二範例之流程圖。

在圖面中，相同的參考編號可識別相同或實質上類似的元素或行為。為了進行任何特定元素或行為之討論，在一參考編號中最有意義的單一數字或多個數字係只該圖面編號，其中該元素為第一次引入(例如元素 204 為第一次引入，並對照第 2 圖來討論)。

【主要元件符號說明】

100 電腦系統(實體機器)
102 主控系統
104 作業系統
106 處理器
110 磁碟
112 記憶體
114 通信子系統
116 系統驅動程式
118 虛擬機器
119 虛擬網路配接器
120 虛擬記憶體
122 虛擬磁碟
124 虛擬驅動程式
126 訪客作業系統
128 監督處理
129 應用程式
200 離線掃描組態
202 安全性應用程式
300 離線掃描組態
302 虛擬機器物件介面
304 安全性應用程式
322 代理處理
330 系統
332 指定的虛擬機器
334 監督處理
336 安全性應用程式

第 94137180 號專利案 101.8.14 修正 年 月 日修正本

# 十、申請專利範圍：

1. 一種在一電腦上用以監視及保護一內含的處理執行環境之多重實例（instance）的方法，其中該等多重實例之每一者皆可存取該電腦之仿真（emulated）的資源，該方法包含下列步驟：

在該電腦上執行至少一安全性應用程式，該至少一安全性應用程式監視一內含的處理執行環境之該等多重實例之每一者，以偵測有害的處理，其中該至少一安全性應用程式係在一內含的處理執行環境之該等多重實例之外部執行；

藉由單一組安全性應用程式，協助掃描一內含的處理執行環境之該等多重實例之該每一者的虛擬資源，其中該等虛擬資源包括該電腦之該等仿真的資源，且其中該協助包括：在該電腦之一主要作業系統知道該等資源的情況下，設置該組安全性應用程式為知道該等資源；及

其中藉由該單一組安全性應用程式，協助掃描一內含的處理執行環境之該等多重實例之每一者的虛擬資源之該步驟，包括以下步驟：提供對關連於一內含的處理執行環境之該等多重實例之一者之一虛擬網路配接器結構的存取。

2. 如申請專利範圍第 1 項所述之方法，其中該至少一安全性應用程式透過以一對一對應的方式與相對應的代理安全性處理通信，以存取一內含的處理執行環境之

該等多重實例之每一者，該等安全性處理在一內含的處理執行環境之該等多重實例之每一者中運行。

3. 如申請專利範圍第 1 項所述之方法，其中該至少一安全性應用程式透過一虛擬機器物件介面以存取一內含的處理執行環境之該等多重實例之每一者，其中虛擬機器物件介面係提供一致性的介面，使得該至少一安全性應用程式 304 能夠存取該等仿真的資源。

4. 如申請專利範圍第 1 項所述之方法，其中該至少一安全性應用程式係在由該電腦所提供的一主控系統中執行，且其中一內含的處理執行環境之該等多重實例之每一者亦在該主控系統中執行。

5. 如申請專利範圍第 1 項所述之方法，其中該至少一安全性應用程式在由該電腦提供的一主控系統中執行，其中一內含的處理執行環境之該等多重實例之每一者亦在該主控系統中執行，且其中該至少一安全性應用程式至少部份地由在該主控系統中執行的一監督處理所控制。

6. 如申請專利範圍第 1 項所述之方法，其中藉由該單一組安全性應用程式，協助掃描一內含的處理執行環境之該等多重實例之每一者之虛擬資源之該步驟，包括以下步驟：提供對關連於一內含的處理執行環境之該等多重實例之一者之一虛擬記憶體結構的存取。

7. 如申請專利範圍第 1 項所述之方法，其中藉由該單一組安全性應用程式，協助掃描一內含的處理執行環境

之該等多重實例之該每一者之虛擬資源之該步驟，包括以下步驟：提供對關連於一內含的處理執行環境之該等多重實例之一者之一虛擬硬碟結構的存取。

8. 一種在一電腦上用以監視及保護一內含的處理執行環境之多重實例的方法，其中該等多重實例之每一者皆可存取該電腦之仿真的資源，該方法包含下列步驟：

在該電腦上執行至少一安全性應用程式，該至少一安全性應用程式監視一內含的處理執行環境之該等多重實例之每一者，以偵測有害的處理，其中該至少一安全性應用程式係在一內含的處理執行環境之該等多重實例之外部執行；

藉由單一組安全性應用程式，協助掃描一內含的處理執行環境之該等多重實例之該每一者的虛擬資源，其中該等虛擬資源包括該電腦之該等仿真的資源，且其中該協助包括：在該電腦之一主要作業系統知道該等資源的情況下，設置該組安全性應用程式為知道該等資源；及

其中藉由單一組安全性應用程式，協助掃描一內含的處理執行環境之該等多重實例之該每一者的虛擬資源之該步驟，包括以下步驟：提供對關連於一內含的處理執行環境之該等多重實例之一者之一虛擬驅動程式結構的存取。

9. 一種在一電腦上用以監視及保護一內含的處理執行環境之多重實例的方法，其中該等多重實例之每一者皆

可存取該電腦之仿真的資源，該方法包含下列步驟：

在該電腦上執行至少一安全性應用程式，該至少一安全性應用程式監視一內含的處理執行環境之該等多重實例之該每一者，以偵測有害的處理，其中該至少一安全性應用程式係在一內含的處理執行環境之該等多重實例之外部執行；

藉由單一組安全性應用程式，協助掃描一內含的處理執行環境之該等多重實例之每一者的虛擬資源，其中該等虛擬資源包括該電腦之該等仿真的資源，且其中該協助包括：在該電腦之一主要作業系統知道該等資源的情況下，設置該組安全性應用程式為知道該等資源；及

其中在一內含的處理執行環境之該等多重實例之一者中偵測到一有害的處理，如果該實例尚未停用時即停用該實例；修護該實例；及載入該修護過的實例到該電腦的一主控環境中，以使該修護過的實例作用。

10. 一種在一電腦系統中用以保護一作業系統之方法，以防止由不想要之處理動作所引起的傷害，該方法包含下列步驟：

暫停在該作業系統上運行的一核心，其中該作業系統係至少部份地與該電腦系統之架構的核心態樣隔離；

檢查該核心，以決定是否出現一不想要之處理動作，其中至少部份由一與該至少部份隔離的作業系統

隔開的一監督處理以執行該檢查；及

當在該至少部份隔離的作業系統中出現一不想要之處理動作時，即採取步驟以控制該不想要的處理動作。

11. 如申請專利範圍第 10 項所述之方法，其中控制該不想要處理動作之該等步驟包括以下步驟：暫停該至少部份隔離的作業系統，並執行另外的監視。

12. 如申請專利範圍第 10 項所述之方法，其中控制該不想要處理動作之該等步驟包括暫停在該至少部份隔離的作業系統上執行的選擇處理之步驟。

13. 如申請專利範圍第 10 項所述之方法，其中控制該不想要處理動作之該等步驟包括終止關連於該不想要的處理動作之一處理之步驟。

14. 一種用以保護對關連於該電腦系統之核心組件的授權作業的存取之電腦系統，該系統包含：

一處理器；

一主要記憶體儲存，該主要記憶體儲存與該處理器通信；

一輔助儲存裝置；

一作業系統；及

一主控系統，其中該主控系統包括：

一或多虛擬機器，其中該等一或多虛擬機器之每一者係與該電腦系統之核心組件隔離，使得當在關連於該虛擬機器之環境中運行時，有害的處理並不能夠

直接存取該等核心組件，且其中該等一或多虛擬機器之每一者包括下列之一實例：一虛擬作業系統、對一虛擬記憶體之存取、及至少一虛擬驅動程式；及

至少一監督處理，該至少一監督處理用於監視結合一安全性應用程式之該等一或多虛擬機器，其中該監視包括一有害處理之可能偵測，且其中該至少一監督處理及該安全性應用程式係與該虛擬機器隔離。

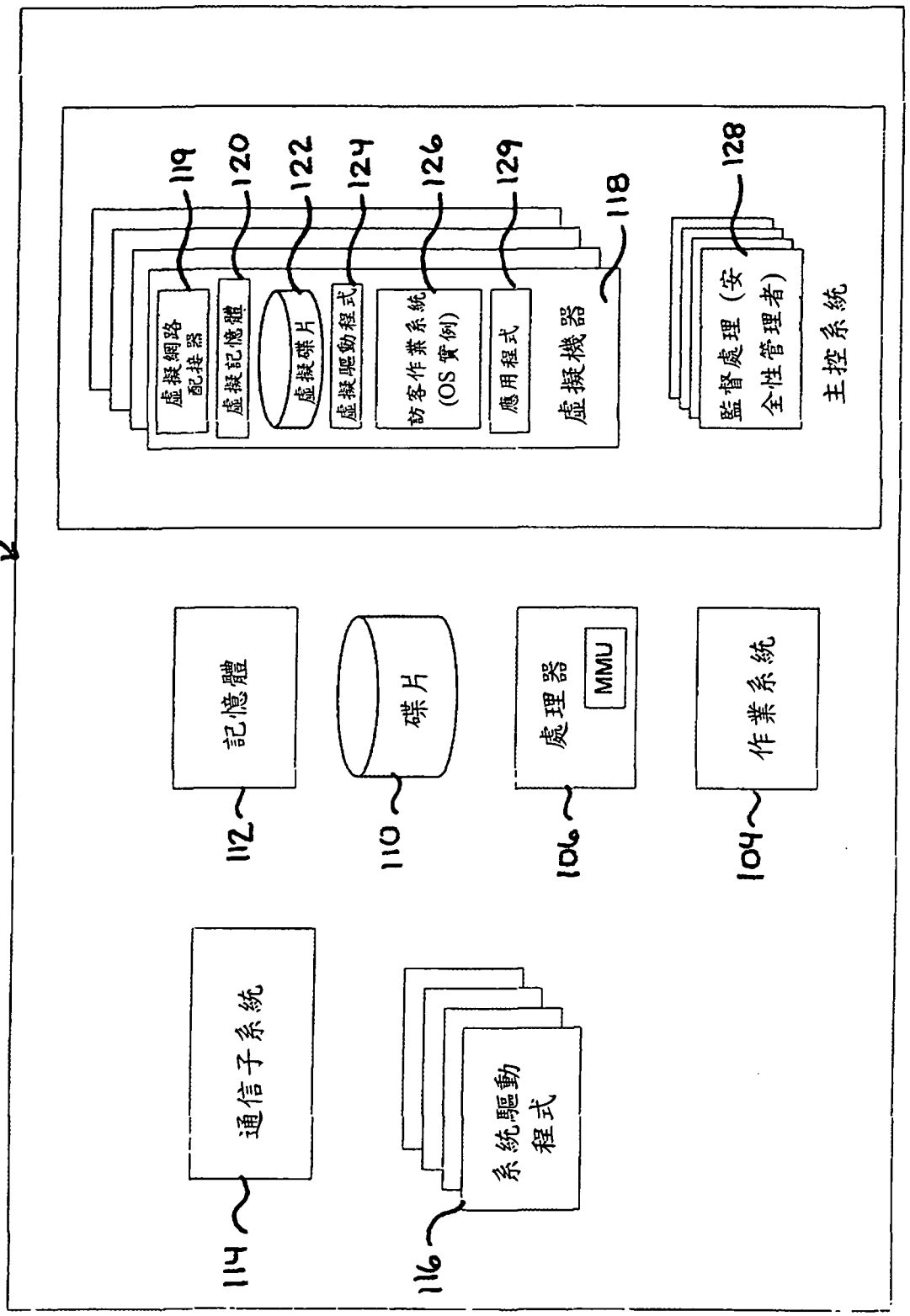
15. 如申請專利範圍第14項所述之系統，其中該監視另包括監視該虛擬記憶體之位址空間。

16. 如申請專利範圍第14項所述之系統，其中該虛擬機器另包括存取一或多仿真的裝置，且其中該監視另包括監視該等仿真的裝置。

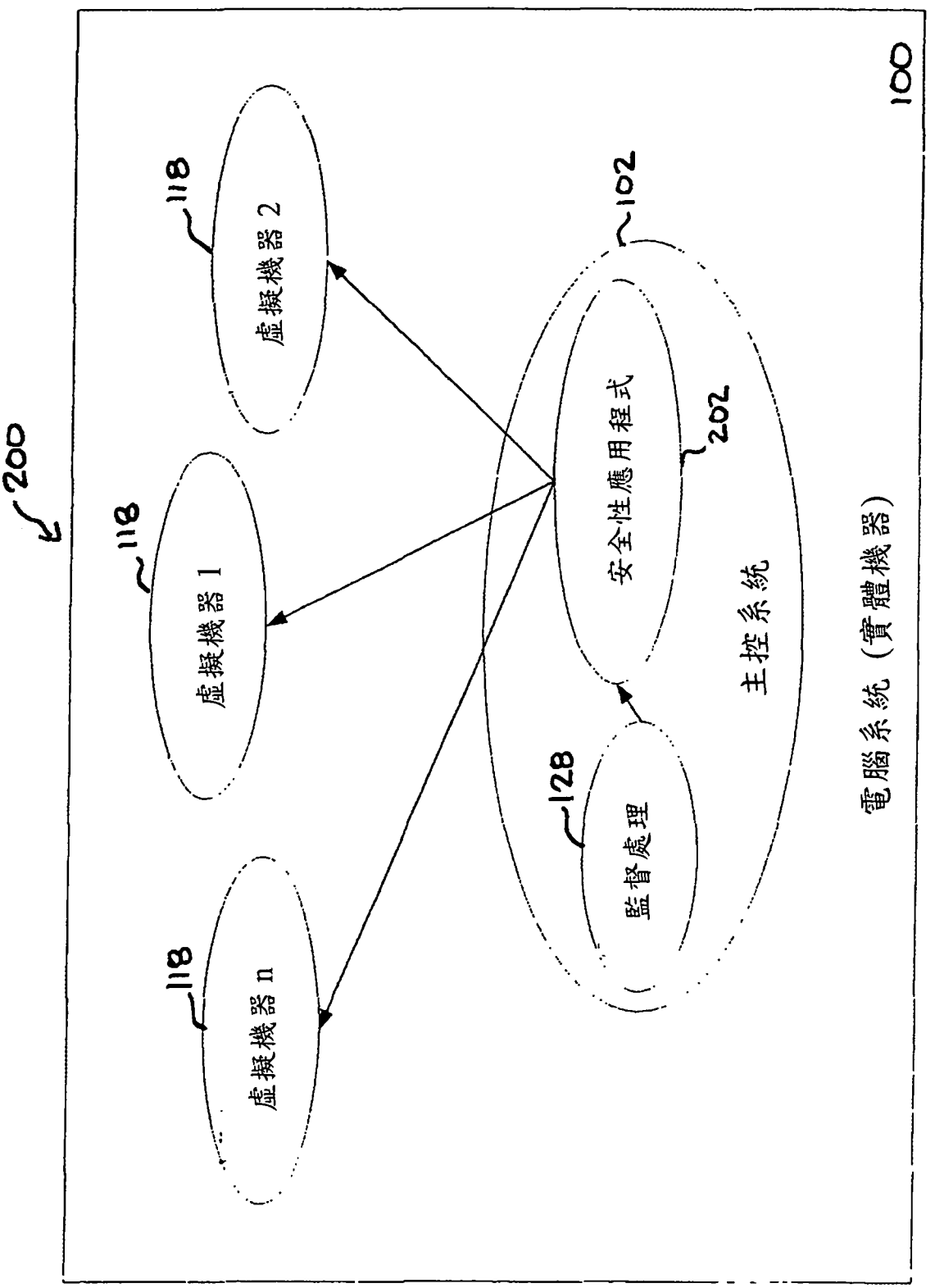
17. 如申請專利範圍第14項所述之系統，其中該虛擬機器另包括存取一仿真的硬碟機，且其中該監視另包括監視該仿真的硬碟機。

18. 如申請專利範圍第14項所述之系統，其中該監視另包括對於在該虛擬機器上之輸入、輸出或執行之處理進行整合性驗證。

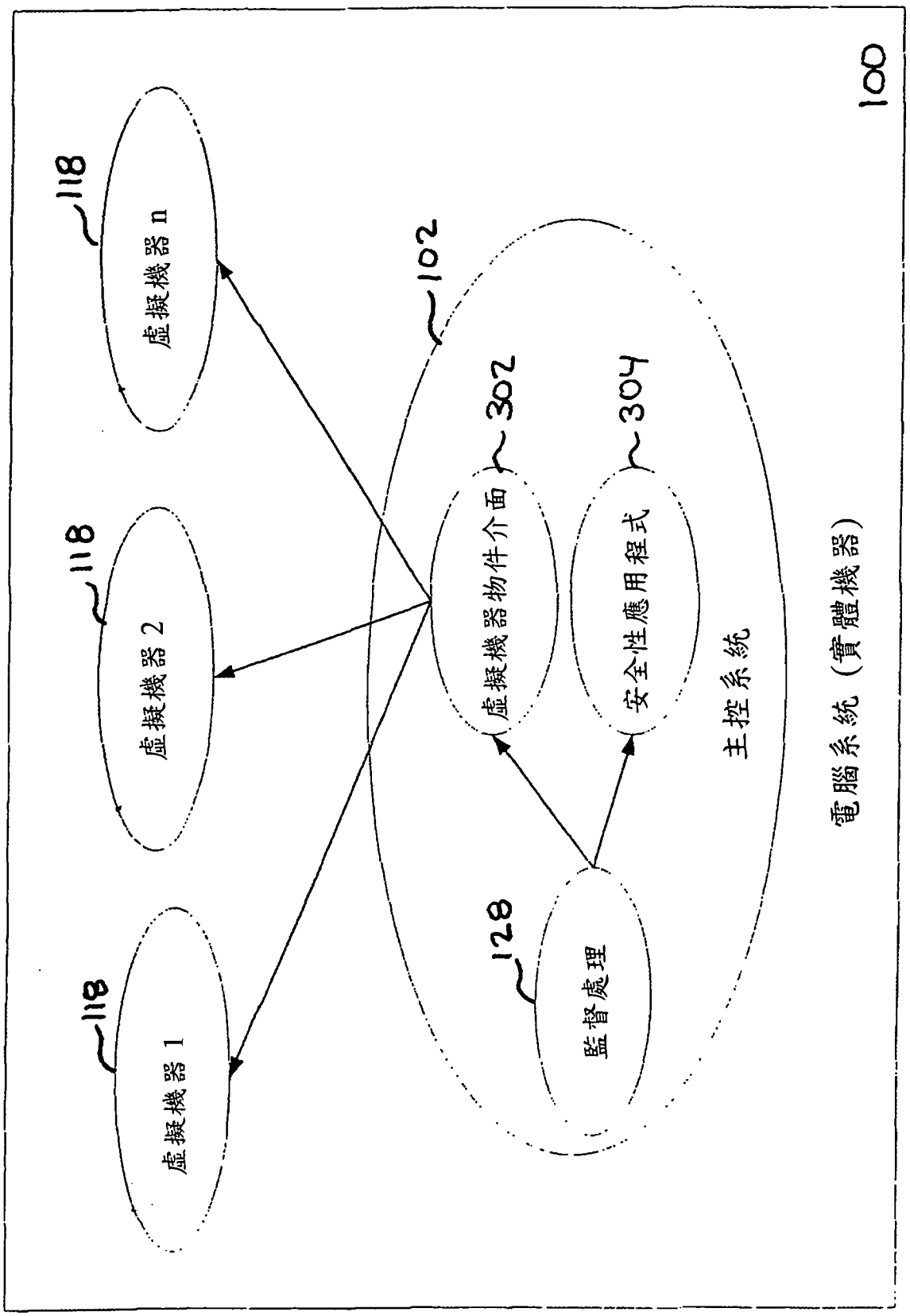
19. 如申請專利範圍第14項所述之系統，其中該虛擬機器另包括對一仿真的硬碟機之存取，且其中該監視另包括檢查存在於該虛擬記憶體或該仿真的硬碟機之上的檔案之整合性。


100
主控系統
虛擬機器
118
虛擬網路配接器
119
虛擬記憶體
120
虛擬碟片
122
虛擬驅動程式
124
訪客作業系統 (OS 實例)
126
應用程式
129
監督處理 (安全性管理者)
128
記憶體
112
碟片
110
處理器
MMU
106
作業系統
104
通信子系統
114
系統驅動程式
116

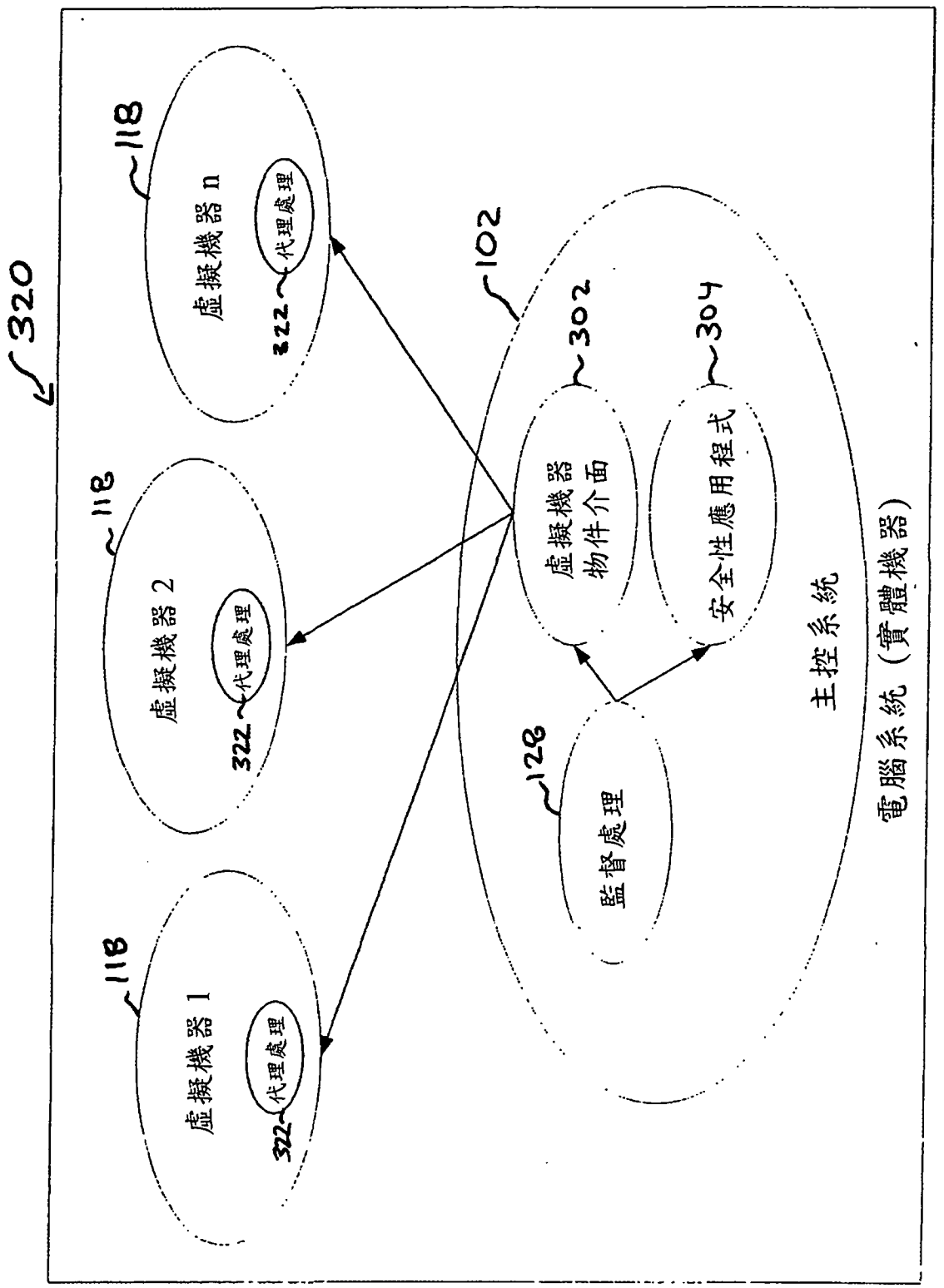
第 1 圖


200
100
電腦系統（實體機器）
118
虛擬機器 2
118
虛擬機器 1
118
虛擬機器 n
102
安全性應用程式
202
主控系統
128
監督處理

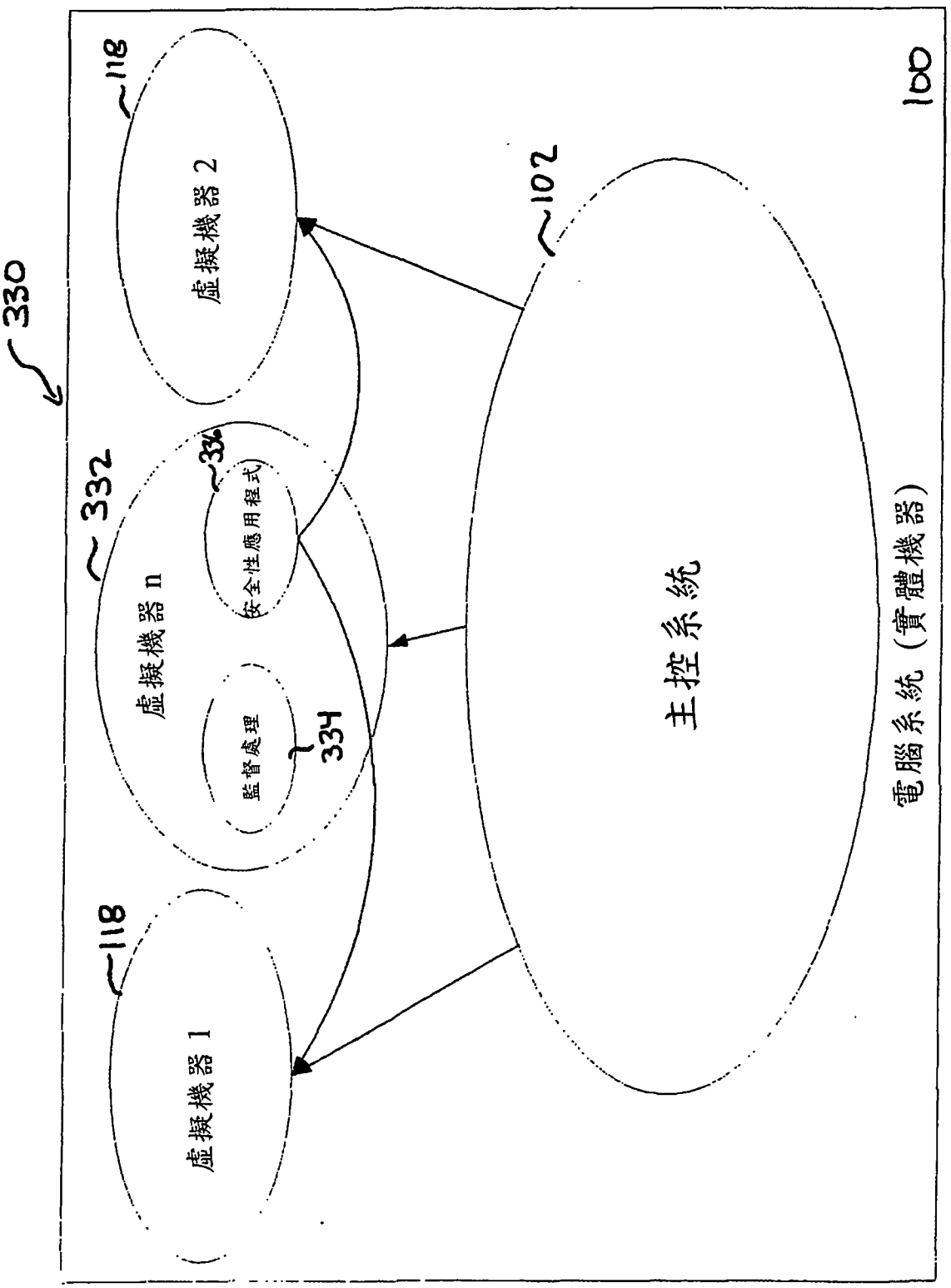
第 2 圖


100
電腦系統（實體機器）
主控系統
102
虛擬機器物件介面
302
安全性應用程式
304
監督處理
128
虛擬機器 1
118
虛擬機器 2
118
虛擬機器 n
118

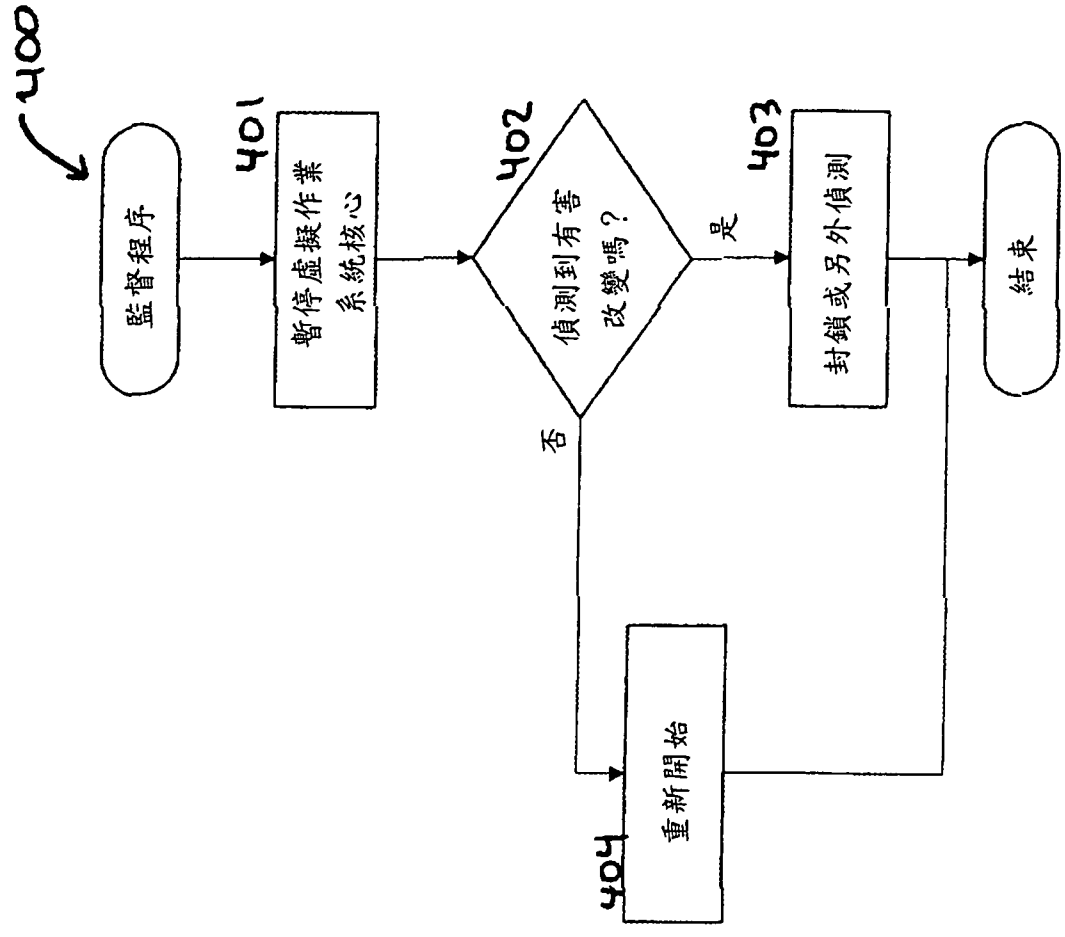
第 3A 圖


320
118
虛擬機器 n
322
代理處理
118
虛擬機器 2
322
代理處理
118
虛擬機器 1
322
代理處理
102
302
虛擬機器
物件介面
304
安全性應用程式
128
監督處理
主控系統
電腦系統（實體機器）

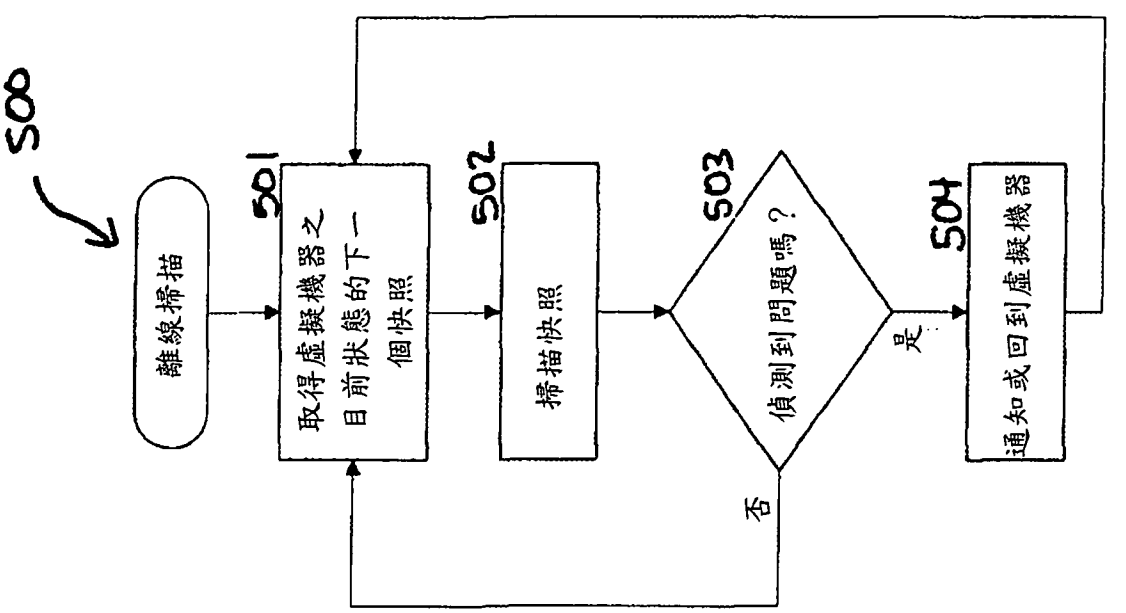
第 3B 圖


330
118
虛擬機器 2
332
336
虛擬機器 n
安全性應用程式
監督處理
334
102
主控系統
118
虛擬機器 1
電腦系統（實體機器）
100

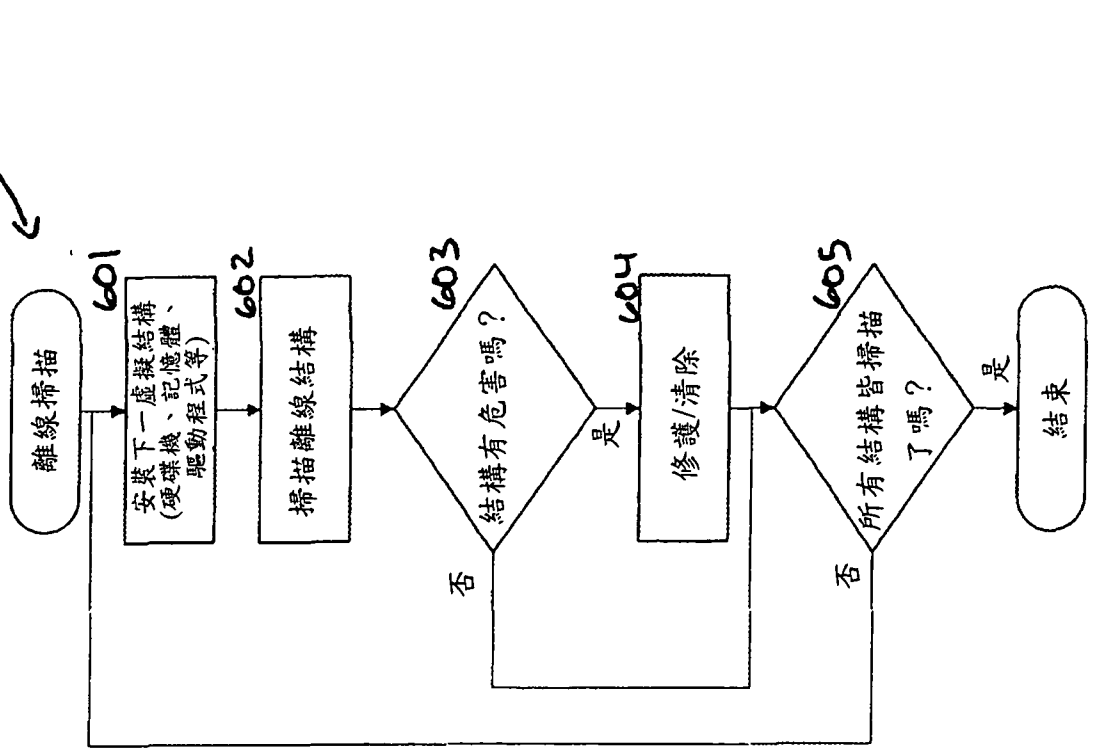
第 3C 圖


400
監督程序
401
暫停虛擬作業系統核心
402
偵測到有害改變嗎？
是
403
封鎖或另外偵測
結束
否
404
重新開始

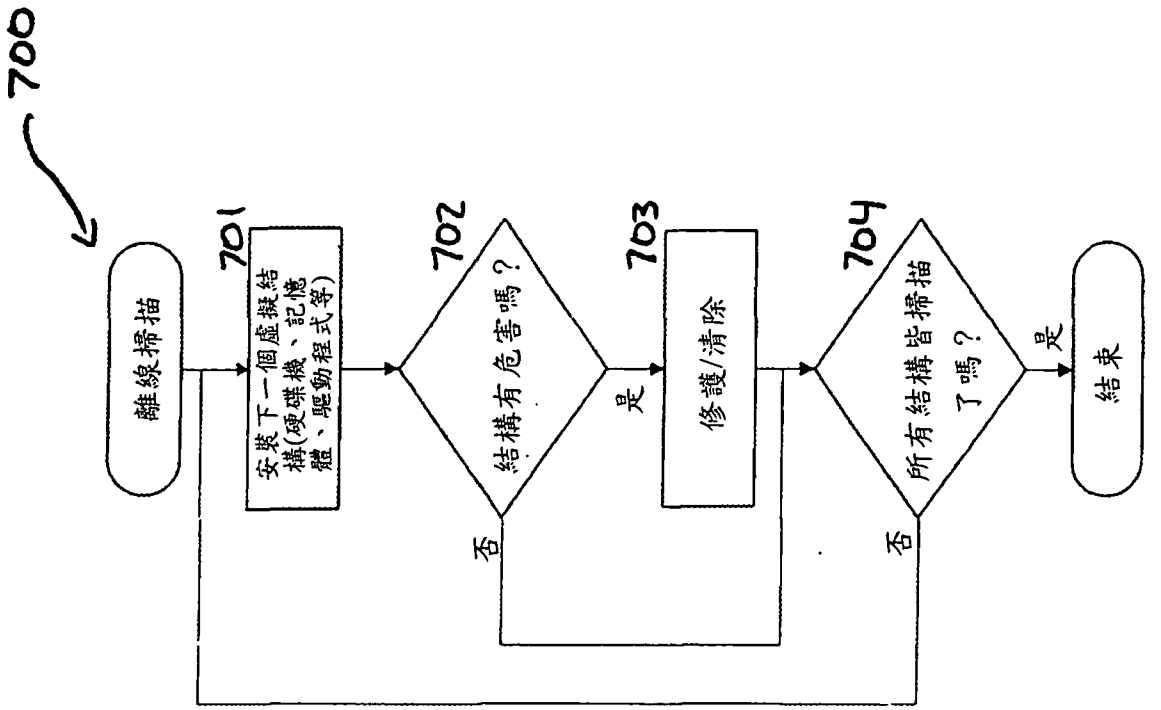
第 4 圖


500
離線掃描
501
取得虛擬機器之目前狀態的下一個快照
502
掃描快照
503
偵測到問題嗎？
否
是
504
通知或回到虛擬機器

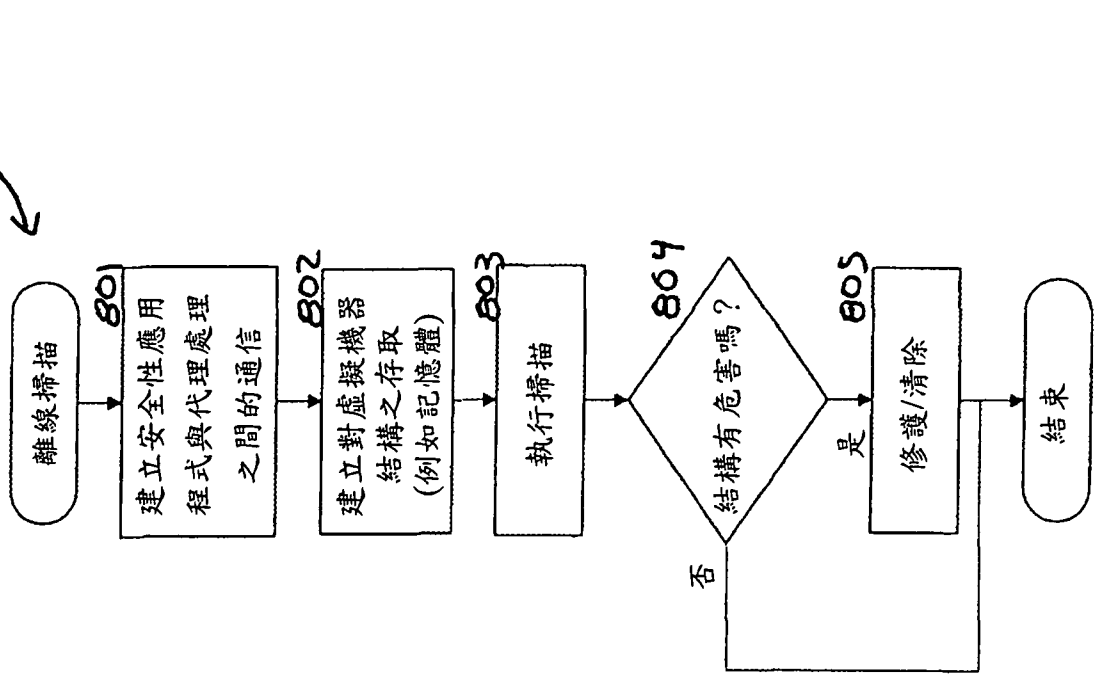
第 5 圖


600
離線掃描
601
安裝下一虛擬結構
(硬碟機、記憶體、
驅動程式等)
602
掃描離線結構
603
結構有危害嗎？
否
是
604
修護/清除
605
所有結構皆掃描
了嗎？
否
是
結束

第 6 圖


700
離線掃描
701
安裝下一個虛擬結構(硬碟機、記憶體、驅動程式等)
702
結構有危害嗎？
否
是
703
修護/清除
704
所有結構皆掃描了嗎？
否
是
結束

第 7 圖


800
離線掃描
801
建立安全性應用程式與代理處理之間的通信
802
建立對虛擬機器結構之存取(例如記憶體)
803
執行掃描
804
結構有危害嗎？
否
是
805
修護/清除
結束

第 8 圖