

發明專利說明書 200525346

(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：93137805

※申請日期：93年12月7日

※IPC分類：

G06F11/36

一、發明名稱：(中文/英文)

沒有病毒程式感染之檔案偵測

DETECTION OF CODE-FREE FILES

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)

艾華那諾爾 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4人)

姓名：(中文/英文)

1. 塞納費爾德馬克 E/SEINFELD, MARC E.

2. 薛爾頓麥可 G/SHELDON, MICHAEL G.

3. 柯斯堤亞米海/COSTEA, MIHAI

4. 歐迪恩斯陸喀斯什克 B/ODINS-LUCAS, ZEKE B.

國 籍：(中文/英文)

- 1.美國/USA
- 2.美國/USA
- 3.羅馬尼亞/Romania
- 4.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 1 月 30 日；10/769,106

☐ 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。

玖、發明說明：

【發明所屬之技術領域】

本發明係有關於可執行的沒有病毒感染程式電腦檔案 (code-free computer files) 的檢測。

【先前技術】

複雜電腦檔案格式，因其可容許擴充且功能性較高，因而變得越來越受歡迎。不幸地，他們也提供一惡意的病毒軟體之作者可隱藏惡意病毒之可執行程式碼的傳播媒介。為了對抗這種情勢，因此出現抗病毒 (anti-viral, AV) 軟體製造者與病毒製造者間的抗爭競賽，其中抗病毒 (anti-viral, AV) 軟體製造者需隔離每種新出現的病毒的複製本並且為該種新病毒添增一識別標誌 (signature)，以便在後續能認出該種新病毒。

因此，設置抗病毒的 (AV) 軟體來掃描輸入檔案以尋找每種已知病毒的識別標誌。如果沒有發現已知的識別標誌，即假設一輸入檔案無病毒感染。

但不幸地，經常出現的情況是，因 AV 軟體尚未更新將一新病毒納入其中致使新病毒將可通過 AV 軟體的檢測。雖然 AV 軟體製造者傾向於能更迅速地回應，在許多情況下是在他們能以一升級做出回應之前及消費者在安裝該升級版之前，該新病毒已造成許多案件損害。因此，仍然需要一種更好、能防止一新軟體病毒感染電腦系統的技術。

【發明內容】

所揭示者為一種沒有病毒感染程式檔案的檢測方法。根據一實施態樣，分析一輸入檔案來識別一檔案格式。根據所檢測出的檔案格式，如果有的話，檢查該輸入檔案的內容，試圖確定是否在該輸入檔案內存在可執行的病毒感染程式。然後傳送一狀態以回應該檢查。

【實施方式】

使用相同的參照數字貫穿參照所有圖示中相同部件和特徵。

概述

下列討論係關於沒有病毒感染程式之檔案的偵測技術。偵測沒有病毒感染程式的檔案的優點在於這樣的檔案可大大降低對使用者之電子郵件、即時傳訊、網際網路瀏覽和其他應用程式之安全性所造成的風險。知道一檔案是沒有病毒感染程式的，使用者也更有機會享受沒有一更高惡意“病毒”軟體的可能。

一般性方法

第1圖示出該沒有病毒感染程式的檔案偵測之一般的方法。在方塊102，藉由將一輸入檔案組態來分析該輸入檔案使能識別一檔案格式。檔案格式是按可供使用和貯存組

織該資料的協定；許多這樣的檔案格式是著名的，並且與檔案名字擴展有關，其中一有限和非全涵蓋的項目包括：jpeg，pdf，doc(Word®)，vsd(Visio®)，等等。在第104方塊中，根據該識別的檔案格式，如果有的話，來檢查輸入檔案的內容，以便在該輸入檔案內找到可執行的程式碼。在第106塊中，根據所檢查到的可執行的程式碼的結果傳送一狀態。須知在此「程式碼」或者「可執行的程式碼」採其廣義解釋，包括但不限於：處理器可執行的指令、語言(script)和其他高階語言，擴充機制和任何其他邏輯，裝置或者可設計、損毀(corrupted)或在任何其他模式實施來制定一病毒，蠕蟲(worm)的機制或者惡意的、未經授權、不需要或非故意的惡性產物(malware)的任何其他形式。在一些實施例中，可傳送該(例如反映出一檔案有病毒感染程式狀態，或者一檔案沒有病毒感染程式或不知道是否有病毒感染程式狀態)狀態至電子郵件、即時傳訊、網際網路瀏覽和其他的應用程式，其中由防禦病毒感染之軟體而來的該安全性是有助益的。

示範的環境

第2至4圖說明在其示範環境內可操作一系統偵測沒有病毒感染程式檔案的示範環境200-400。尤其，第2-4圖說明在環境200-400內分別設置一電子郵件客戶端應用程式202、一即時傳訊應用程式302或者網際網路瀏覽程式402

接收可包含一或更多夾帶檔案204的訊息。須知應用程式202、302、402代表多種硬體或者軟體設備，可加以設定以從一病毒檢測模組206來接收訊息。另外的代表性裝置包含一防火牆(硬體和/或軟體)，一個主機入侵檢測器(供一伺服器，客戶端，工作站，等等使用)，一主機受入侵鑑定器(供一伺服器，客戶端，工作站，等等使用)，一軟體備份的管理程式，CD和/或DVD燒錄程式，一個點對點(對等)檔案分享的程式或者多種其他應用程式。設置一病毒檢測模組206模來分析夾帶檔案204確定是否存在可執行的程式碼。藉著該分析，病毒檢測模組206的輸出提供該應用程式202、302、402以下三種可能的輸入之一：一檔案有病毒感染程式狀態208、一檔案沒有病毒感染程式狀態210或者一未知(如果該檔案有病毒感染程式)狀態212。在第一個情況中，檔案有病毒感染程式狀態208反映出根據檔案格式充分識別出一輸入檔案且發現在該輸入檔案內含可執行程式碼。由於一檔案內存在有可執行程式碼的危險，應用程式202，302，402等等可使用該狀態的消息來在一與這些危險一致的模式上執行。在第二種情況裡，檔案沒有病毒感染程式狀態210反映出根據檔案格式充分識別出一輸入檔案和發現在輸入檔案內沒有可執行程式碼。應用程式202，302，402確信該檔案204是沒有病毒感染程式的，該使用者不必被該使用者的對話框或一用戶界面的其他方面麻煩地請求其決定是否信賴該檔案。在第三種情況裡，未知(如果檔案

有可執行程式碼)狀態212反映出無法識別該輸入檔案的檔案格式以及不確定輸入檔案內是否存在有可執行程式碼這樣的結果。

示範系統

第5圖示出在第2-4圖裡描述的該程式檢測模組206的示範細節，可將該示範病毒檢測模組206設置在軟體、韌體或硬體中，例如透過ASIC(特定功能積體電路)來進行設置。可將一可擴展的分析模組502設置成包含複數組成元件分析模件506(1)-506(N)的一目錄。例如以在第6圖所示的示範方法600，可擴展該可擴展的分析模組。隨著新檔案格式變為已知及希望知道該等已知檔案格式的興趣愈來愈高的同時，可擴充性是合乎需要。因此，可擴展的分析模組502可被擴大來包含設置來識別一附加檔案格式以及設置來在新檔案格式內檢查可執行程式碼之附加的組成分析模組506(N+1)。第6圖示出擴展該病毒檢測模組206的可擴展分析模組502的一示範處理600。在第602方塊，識別出一檔案格式並將其增加至該可擴展分析模組502中。例如，可能想要擴展可擴展分析模組502供jpeg檔案使用。在第604方塊，根據新檔案格式(例如jpeg)設置一新組成元件分析，其中設置該新組成元件來識別該新格式的檔案並且在該檔案內識別可執行的程式碼。在第606方塊，在可擴展分析模組502內透過該增加新組成元件分析506(N+1)至一可擴展

的目錄，擴展可擴展分析模組502的功能性。

再次參照第5圖，設置可擴展分析模組502來包含複數組成元件分析模組506(1)-506(N)，其中為簡明起見，只示出兩個組成元件分析模組。設置每組組成元件分析模組第506(1)-506(N)來識別一特定檔案格式的檔案，並且當識別出該特定檔案格式時，額外設置其來識別該檔案內所包含的可執行程式碼。例如，可設置該分析模組506(1)來識別一(例如，用於儲存組織該資料的格式)Word®文件之檔案格式。也可設置分析模組506(1)，經檔案格式的識別，在一含Word®檔案格式之輸入檔案內識別可執行的程式碼。這樣的話，識別檔案格式有助於識別可執行程式碼。

該組成元件分析模組506每組包含格式調查模組508，設置該模組來分析該輸入檔案204，並且確定是否該輸入檔案與分析器鑑定的檔案格式相配。該組成元件分析模組也包括病毒感染程式部分檢測器510，在發現該檔案具有與組成元件分析模組相關的檔案格式的地方，在輸入檔案內設置該檢測器來檢測可執行程式碼。

也設置每組組成元件分析模組506來包含表明該輸入檔案204有病毒感染程式512、輸入檔案沒有病毒感染程式514和未知是否該輸入檔案有病毒感染程式516的三組輸出。在第5圖的實施例中，當格式調查模組508不能檢測與輸入檔案204相關的格式時，該組成元件分析器返回一未知狀態516。當識別出該檔案格式時，該病毒檢測器510的輸

出可用來確定是否該輸入檔案有病毒感染程式512(即病毒檢測器510發現病毒程式)或該輸入檔案沒有病毒感染程式514這樣的輸出是適當的(即病毒檢測器510沒發現病毒程式)。

該可擴展的分析模組502也包含一控制器或者分派處理504，典型上設置該模組來：對所有可得到的組成元件分析模組506(1)-506(N)服務該輸入檔案；處理組成元件分析器所有的輸出；並且傳送一整體的回應(即病毒感染程式/沒有病毒感染程式/未知)至一適當的應用程式。設置控制單元504包含複合病毒程式部分檢測器518，設置該來接收從每組組成元件分析器506(1)-506(N)的輸入和確定是否組成元件分析器中任何一組發現病毒程式。藉由該組成元件分析器506(1)-506(N)之一來檢測這裡的病毒程式，該病毒檢測模組206的輸出將是檔案有病毒感染程式狀態208。設置一複合格式調查模組520來確定是否該組成元件分析506(1)-506(N)的任一組來識別輸入檔案204的格式。這樣的調查通常適合在沒有該組成元件分析器506(1)-506(N)檢測可執行程式的地方。藉由組成元件分析器506(1)-506(N)之一來檢測這裡的檔案格式，該病毒程式檢測模組206的輸出將是檔案沒有病毒感染程式狀態210。當未識別出一檔案格式時，該病毒程式檢測模組206的「未知的」輸出(如果那些檔案有病毒程式)將是該未知狀態212。

示範方法

將在主要參照之第7圖的流程圖下描述一種用以實行沒有病毒感染程式檔案檢測之態樣的示範方法700。該方法一般係關於如上關於第2-4圖之討論，和特別是第5圖之示範元件的操作。可藉適當的構件來執行該描述方法的要素例如，包含，在一ASIC上的硬體邏輯區塊或者經由在處理器可讀媒介上定義的處理器可讀指令的執行。

在此，一種「處理器可讀的媒介」包含，儲存，交流，傳播，或者經由一處理器傳送用以使用指令或經由一處理器實行的任何構件。一種處理器可讀媒介包含但不限於一電子，磁，光學，電磁，紅外線，或者半導體系統，儀器，裝置或者傳播媒介。一種處理器可讀媒介的更多的具體的例子包含，其中有，具一或更多電線的電力接駁位置，一便攜式電腦軟碟，一個隨機存取記憶體(RAM)，一唯讀記憶體(ROM)，一可抹拭的可編程式唯讀的記憶體(EPROM或者快閃記憶體)，一光纖，一可複寫的光碟(CD-RW)和便攜式光碟唯讀的記憶體(CDROM)。

第7圖示一示範方法700用以在檔案內檢測可執行病毒感染程式。在方塊702，分析一輸入檔案啟動該檔案格式的識別藉此以設定該輸入檔案。該分析器可能以混合的模式設置，例如第5圖的該複合或可擴展性的分析器502，其中該複合分析器包含複數組成元件分析器506(1)-506(N)，每一個設置來識別特定的檔案格式。

在方塊 704，如果一檔案格式已被識別出，然做出一決定。如一檔案格式已被識出(隨著方塊 704 這個 Yes 支流跳至方塊 706)，然後在方塊 706 根據該識別出的檔案格式來檢查輸入檔案的內容以尋找在輸入檔案內可執行的病毒感染程式。注意到分析器 502 是具可擴展和/或複合的，藉由設置該組成元件分析器 506(1)-506(N)來作識別，一檔案格式可與該檔案格式相符合。因此，當確定是否識別一檔案格式，該控制器 504(第 5 圖)將從每組組成元件分析器 506(1)-506(N)鑑定訊息。

在方塊 708，如果發現可執行的病毒感染程式，做出一決定。如果發現可執的病毒感染程式(隨著方塊 708 的 Yes 支流跳至方塊 712)，然後在方塊 712，傳送檔案有病毒感染程式狀態，即當該識別出輸入檔案的檔案格式和發現可執行的病毒感染程式時傳送檔案有病毒感染程式狀態。經由任何組成元件分析器 506(1)-506(N)可分析出該識別。以第 5 圖所示該示範病毒感染程式檢測模組 206 的架構的回顧來看，在識別該檔案格式的地方，如果提出，一組成元件分析器能檢測可執行的病毒感染程式。這樣的病毒感染程式不符合於該檔案格式，或者根據檔案格式的集合被指派於該位置，並且因此容易被認出。因此，組成元件分析器之一識別出可執行的病毒感染程式的地方，該控制器適當的回應用以提供一檔案有病毒感染信號或消息。

在方塊 708，如果做出該表明沒有發現可執行的病毒感

染程式的一決定(隨著方塊708支流No跳至方塊710)，當該識別出輸入檔案的檔案格式和發現沒有可執行的病毒感染程式時，然後在方塊710傳送一檔案沒有病毒感染程式狀態。尤其參照第5圖，顯然在輸入檔案內如果沒有組成元件分析器識別出可執行的病毒感染程式，並且該檔案格式已經被至少組成元件分析器之一組所識別出，則記錄該檔案沒有病毒感染程式狀態。注意到已發現該輸入檔案沒有可執行的病毒感染程式的察覺通常是有利的，因為無可執行的病毒感染程式保證無蓄意的可執行的病毒感染程式，例如一種病毒。

返回參照方塊704，如果無法識別出一檔案格式(隨著方塊714的No支流跳至方塊704)，然後在方塊714(如果該輸入檔案有可執行的病毒感染程式)當該檔案格式是未知的時，傳送一未知狀態212。如參照所示看第5圖中的方塊212，每組該組成元件分析器不能確定該檔案的格式，設置控制器504來發出一未知狀態至適當的接收者，例如電子郵件應用程式202(第2圖)，一即時訊息應用程式302(第3圖)，一網際網路瀏覽程式的402(第4圖)等等。

在方塊716，在一些應用過程中，即使在該組成元件分析器之一組識別出該輸入檔案的格式之後，該組成元件分析器506(1)-506(N)可繼續分析該輸入檔案204。此提供多一層的安全，即在極少數的情形下，多於一組成元件分析器可以有效的識別出該檔案格式(即，一檔案能在稀有的實

例內與兩不同的檔案格式一致)。因此在極少數的情形內，其中第二組成元件分析器識別出該輸入檔案的格式，如果任何一個該組成元件分析器識別出可執行的病毒感染程式，可設定該控制器504報告該輸入檔案有病毒感染程式。或者，當該組成元件分析器之一識別出該輸入檔案的格式時，可設置該複合分析器中斷分析。這傾向於降低在分析操作上花費的時間。

如上面所示，可傳送該檔案沒有病毒感染程式、檔案有病毒感染程式或者未知的狀態至電子郵件程式、即時訊息程式、網際網路瀏覽程式和其他的應用程式，其中該防禦病毒影響的軟體之安全性是有利的。第2-4圖說明病毒感染程式檢測模組206的示範用途。但是，對病毒感染程式檢測模組之其他用途是可能的，例如在檔案儲存器應用，其中期望該儲存器只儲存可執行的沒有病毒感染程式的檔案，等等。

當經由流程圖方法已透露出一種或更多方法並且文字與流程圖的方塊相關時，應該瞭解到該方塊不一定必須被在他們被提出的命令裡依序執行，並且一另外的順序可以導致相似的利益。而且，該方法並不是唯一的，並且能單獨執行或在與另一的結合。

示範電腦

第8圖是一示範電腦系統，其中可實行第1-7圖的該示

範病毒程式感染檢測模組和操作方法。雖然顯示一特定的構造，但是在其他計算的構造過程中可實現該病毒程式感染檢測模組。該計算環境800在一電腦802的形式上包含一通用的計算系統。該電腦802的部件能包含，一或更多處理器或處理單元804，一系統記憶體806，和聯接各種包括該處理器804至該系統記憶體806的不同系統部件之一系統匯流排808，但不以此為限制。

該系統匯流排808代表一或多個任何不同種類的匯流排架構，包含一記憶體匯流排或記憶體控制器，一外部匯流排，一加速圖形埠和一處理器或一使用任何各種匯流排結構的本區匯流排。一系統匯流排808的例子將是一周邊零件連接界面(PCI)匯流排，也是被稱為一夾層匯流排。

電腦802通常包含多種電腦可讀的媒介。這樣的媒介可能是經電腦802存取和包括揮發和非揮發性，可抹除和非可抹除媒介的任何可得到的媒介。該系統記憶體806包括以揮發性記憶體形式的電腦可讀媒介，例如隨機存取存儲器810(RAM)，和/或非揮發性記憶體，例如唯讀記憶體812(ROM)。一基本輸入/輸出系統(BIOS)814，包含幫助轉移在電腦802內元件之間訊息的那些例如在開機期間儲存在ROM 812的基本常規。RAM 810通常包含由處理單元804立即存取和/或當即操作的資料和/或程式模組。

電腦802也能包含其他可抹除/非可抹除，揮發/非揮發性電腦儲存媒介。在例子方面，第8圖說明一用於讀取和寫

入至非可抹除、非揮發性之磁性媒介(未示出)的硬碟驅動器 816，用於讀取和寫入至可抹除的磁性磁碟驅動器 818，非揮發性磁性磁碟片 820(例如，軟磁片)，和一用於讀取和/或寫入至可抹除、非揮發性光碟 824(例如 CD-ROM，DVD-ROM)磁片，或者其他光學媒介的光碟機 822。該硬碟機 816、磁性磁碟機 818和光碟機 822是經由一或更多資料媒介界面 825每個連接至系統匯流排 808。或者，藉由一 SCSI 界面(未示出)可連接該硬碟機 816、磁性磁碟機 818，和光碟機 822至系統匯流排 808。

該磁碟機和他們的相關電腦可讀媒介提供電腦可讀指令、資料節構、程式模組和電腦 802之其他資料的非揮發性儲存。雖然該例子說明一硬碟 816，一可抹除磁碟片 820，以及可抹除光碟片 824，它將被領會到例如磁帶盒(magnetic cassettes)或其他磁性的儲存裝置、快閃記憶卡、CD-ROM、數位多用途磁碟片(DVD)或其他光學儲存器、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、電力可抹除的可編程唯讀記憶體(EEPROM)和其他類似裝置之經由一電腦可存取儲存資料的電腦其他類型的可讀媒介，也能被利用實施至該示範計算系統和環境。

可能被儲存許多例如包含，一作業系統 826、一或更多應用程式 828、其他程式模組 830和程式資料 832的程式模組在硬碟 816，磁碟片 820，光碟片 824，ROM 812，和/或 RAM 810。應該瞭解到該病毒感染程式檢測模組 206可能設置作

為一應用程式 828，或者一程式模組 830 或作為一位於其他合宜位置的模組。另外，在資料 832 之中包含該輸入檔案 204 或者包含在其他合宜的位置。這樣的作業系統 826 中的每個、一或更多應用程式 828、其他程式模組 830，和程式資料 832（或者一些其結合）可以包含一使用者網路存取資訊之快取方案的具體例。

電腦 802 能包含多種定義為通訊介質之電腦/處理器的可讀的媒介。通訊介質通常具體實現於電腦可讀指令、資料結構、程式模組或在例如一載波或者其他傳送機制和包含任何訊息交付媒介之一調整的資料上的不同信號。該項”調整的資料信號”表示有一或多個它的特徵集合或者在如此的方法上把在信號裡的訊息進行編碼的改變的一信號。藉由該例子，並非限制於通訊介質包含例如一有線網路或者直接線 (direct-wired) 之連接的有線媒介，以及例如聲波、射頻 (RF)、紅外線和其他無線媒介的無線媒介。在電腦可讀媒介範圍內也包含任何在上面的結合。

一使用者能透過例如一鍵盤 834 和一指向裝置 836 (例如，一”滑鼠”) 的輸入裝置把命令和訊息輸入電腦系統 802。其他輸入裝置 838 (不特定顯示) 可包含一麥克風、遊戲控制桿 (joystick)、遊戲搖桿 (game pad)、衛星天線接收器 (satellite dish)、序列埠、掃描器和/或其他類似裝置。透過連接到系統匯流排 808 的輸入/輸出界面 840 來連接這些和其他輸入裝置至處理單元 804，但是經由其他界面和匯流

排架構可連結，例如平行埠，遊戲連接埠或者一通用序列匯流排(USB)。

一監控器842或例如視訊配接器844的其他類型的顯示裝置也能透過一界面連接至系統匯流排808。除監控器842之外，其他可能透過輸入/輸出界面840連接電腦802的輸出外部裝置能包含如一擴音器(未示出)和一印表機846。

電腦802能對一或更多遠端電腦使用邏輯連接在一網路環境裡操作，例如一遠端電腦裝置848。在例子方面，遠端電腦裝置848可是一個人電腦，便攜式電腦，一伺服器，一路由器，一網路電腦，一位於同網路層位的裝置(peer device)或者其他常見的網路節點，和其他類似裝置。描述該遠端計算裝置848作為一便攜式電腦，該能包含此中描述相關於電腦系統802的很多或所有元件和特徵。

描述在電腦802之間的邏輯連接和遠端電腦848為一區域網路(LAN)850和一般的廣域網路(WAN)852。這樣的網路環境通常佈於辦公室，企業廣域電腦網路，企業內部網路和網際網路。當被在一區域網路環境裡實現時，連接該電腦802透過一網路界面或配接器854至一區域網路850。當被在一廣域網路環境裡實現時，該電腦802為通常包含一數據機856或其他裝置用以透過廣域網路852上建立通訊。該數據機856，該可能是在電腦802內部或者外部，該也可透過輸入/輸出界面840或其他合適的機制連接該系統匯流排808。它應該被瞭解到該描述的網路連接是示範並且可利

用在電腦802和848之間建立通訊鏈結的不同裝置。

在一網路的環境裡，可能儲存如該用計算環境800說明的，相對於電腦802描述的程式模組，或者關於那部分，在一套遠端記憶體儲存裝置裡。在例子方面，遠端應用程式858保存在一遠程電腦848的記憶體裝置裡。為此說明意圖，此中描述例如作業系統的應用程式和其他可執行的程式部件為分離的區塊(discrete blocks)，雖然理解到這樣的程式和部件在電腦系統802不同的儲存部件裡在不同時間存在，並且經由電腦的資料處理器執行。

結 論

雖然僅特定用於構造特徵和方法邏輯技藝的語言描述該發明，應該理解到定義在如附的申請專利範圍的本發明不一定局限於描述的特定特徵或者行為。反之，揭露該特定特徵和行為作為實現如實施該申請專利範圍發明的示範形式。

【圖式簡單說明】

第1圖是描述一藉該來檢測病毒感染程式檔案的流程圖，包含利用使用在識別檔案格式和檢測可執行病毒感染程式的方法。

第2圖說明一示範環境，其中設置一病毒感染程式檢測模組來提供在一檔案內包含可執行病毒感染程式的資訊至一電子郵件程式。

第 3 圖說明一第二示範環境，其中設置一病毒感染程式檢測模組來提供在一檔案內包含可執行病毒感染程式的資訊至即時通訊程式。

第 4 圖說明一第三示範環境，其中設置一病毒感染程式檢測模組來提供在一檔案內包含可執行病毒感染程式的資訊至網際網路瀏覽程式。

第 5 圖說明在該地 2-4 圖病毒感染程式檢測模組內包含的結構示範細節，包含一可擴充分析模組。

第 6 圖是藉該第 5 圖上所示可擴充分析模組描述一示範方法的流程圖。

第 7 圖描述一示範方法來檢測沒有病毒感染程式的一流程圖。

第 8 圖是一示範電腦系統，其中可實施一病毒感染程式檢測模組。

【主要元件符號說明】

801	計算環境	818	磁性磁碟機
820	磁碟片	822	光碟機
824	光碟	842	監視器
848	遠端計算裝置	850	系統匯流排
852	網際網路	858	遠端應用程式
802	電腦	806	系統記憶體
826	作業系統	828	應用程式
830	其他程式模組	832	程式資料

810	隨機存取記憶體	812	唯讀記憶體
815	基本輸出/輸入系統	808	系統匯流排
804	處理單元	840	輸出/入介面
844	視訊配接器	854	網路配接器
825	資料媒介介面	816	硬碟
826	作業系統	828	應用程式
830	程式模組	832	程式資料
846	印表機	836	滑鼠
834	鍵盤	838	其他裝置

伍、中文發明摘要：

所揭示者為一種沒有病毒感染程式檔案的檢測方法。根據一實施態樣，分析一輸入檔案來識別一檔案格式。根據檢測出的檔案格式，如果有的話，檢查該輸入檔案的內容，試圖確定是否在該輸入檔案內存在可執行的病毒感染程式。然後傳送一狀態以回應該檢查。

陸、英文發明摘要：

Detection of code-free files is described. According to one implementation, an input file is parsed to recognize a file format. Contents of the input file are checked according to the recognized file format, if available, in an effort to determine whether executable code might exist within the input file. A status is then sent in response to the checking.

拾、申請專利範圍：

1. 一種處理器可讀媒介，至少包含處理器可執行指令用以：

分析一輸入檔案來識別該輸入檔案的檔案格式；

根據該識別出的檔案格式，如果有的話，檢查該輸入檔案的內容，以確定是否在該輸入檔案內存在有可執行病毒感染程式；並且

傳送一狀態以回應該檢查結果。

2. 如申請專利範圍第1項所述之處理器可讀媒介，其中傳送一狀態的動作更至少包含用以執行下列動作的指令：

當識別出該輸入檔案的檔案格式和沒發現可執行病毒感染程式時，傳送一「檔案沒有病毒感染程式(file-has-no-code)」狀態；並且

當發現可執行的病毒感染程式時，傳送一「檔案有病毒感染程式(file-has-code)」的狀態。

3. 如申請專利範圍第1項所述之處理器可讀媒介，另外至少更包含當未識別出該輸入檔案的檔案格式時用以傳送一「未知(don't-know)」狀態的指令。

4. 如申請專利範圍第1項所述之處理器可讀媒介，其

中分析該輸入檔案更至少包含在可擴展的語法分析程式內用具有複數個部件分析器以反覆分析該輸入檔案的指令。

5. 如申請專利範圍第4項所述之處理器可讀媒介，另外更至少包含當在該可擴展的分析器內所包含的複數部件分析器的每組均不能識別出該輸入檔案的部分時，用以傳送一「未知(don't-know)」狀態的指令。

6. 如申請專利範圍第1項所述之處理器可讀媒介，其中傳送該狀態更至少包含用以傳送該狀態至一電子郵件程式的指令。

7. 如申請專利範圍第1項所述之處理器可讀媒介，其中傳送該狀態更至少包含用以傳送該狀態至一即時訊息的指令。

8. 如申請專利範圍第1項所述之處理器可讀媒介，其中傳送該狀態更至少包含用以傳送該狀態至一網際網路瀏覽程式的指令。

9. 如申請專利範圍第1項所述之處理器可讀媒介，其中檢查該輸入檔案的內容至少更包含操作一可擴展的部件分析器的部件分析器部分來識別一特定的資料檔案格式的

指令。

10. 如申請專利範圍第1項所述之處理器可讀媒介，其中分析該輸入檔案至少包含用以操作一設置來識別一複數檔案格式之分析器的指令。

11. 如申請專利範圍第1項所述之處理器可讀媒介，其中檢查該輸入檔案的內容至少更包含用於具一複數部件分析器的複合分析器之操作的指令，其中設置該複數部件分析器的每組用於對一特定檔案格式的識別。

12. 如申請專利範圍第11項所述之處理器可讀媒介，另外更包含在至少一組部件分析器識別出該輸入檔案的檔案格式之後，用以提交給全部剩下的部件分析器繼續分析該輸入檔案的指令。

13. 如申請專利範圍第11項所述之處理器可讀媒介，另外更至少包含用以分析該輸入檔案直到一部件分析器識別出該輸入檔案的檔案格式。

14. 一種沒有病毒感染程式之檔案的檢測方法，至少包含：

使用設置來包含複數個部件分析器的一複合部件分析

器來分析一輸入檔案，其中設置每組部件分析器來識別一特定的資料檔案格式；

根據該識別出的特定檔案格式如果有的話，來分析該輸入檔案的內容，以確定是否該輸入檔案包含可執行的病毒感染程式；並且

傳送一狀態以回應該分析結果。

15. 如申請專利範圍第14項所述之方法，另外至少包括：

當識別出該輸入檔案的檔案格式和沒發現可執行病毒感染程式時，傳送一「檔案沒有病毒感染程式(file-has-no-code)」狀態；並且

當發現可執行的病毒感染程式時，傳送一「檔案有病毒感染程式(file-has-code)」的狀態。

16. 如申請專利範圍第14項所述之方法，另外至少包含當未識別出該輸入檔案的檔案格式時傳送一「未知的(don't-know)」狀態。

17. 如申請專利範圍第14項所述之方法，另外至少包含傳送該狀態至一電子郵件程式。

18. 如申請專利範圍第14項所述之方法，另外至少包

含傳送該狀態至一即時訊息程式。

19. 如申請專利範圍第14項所述之方法，另外至少包含傳送該狀態至一網際網路瀏覽程式。

20. 如申請專利範圍第14項所述之方法，其中在該複合分析器內使用該複數個部件分析器的每組來分析該輸入檔案。

21. 一種用以檢測沒有病毒感染程式之檔案的裝置，至少包含：

一複合分析器，其係設置用以反覆分析一輸入檔案，其中在該複合分析器之內的每組部件分析器係被設置成可從一組資料檔案格式之中選擇出來的一特定檔案格式內來識別出可執行的病毒感染程式；及

一控制器，用以檢查每組部件分析器成功識別出之該特定的檔案格式，該控制器係被設置成來識別和發現在該輸入檔案內可執行的病毒感染程式，其中該控制器係被設置成可傳送一狀態以回應該檢查結果。

22. 如申請專利範圍第21項所述之裝置，另外設置成如果任何一該部件分析器都不能識別出該輸入檔案的檔案格式時，即傳送一「未知的(don't-know)」狀態。

23. 如申請專利範圍第21項所述之裝置，其中該用以檢測沒有病毒感染程式檔案的裝置被額外設置成可把狀態傳送至一電子郵件程式。

24. 如申請專利範圍第21項所述之裝置，其中該用以檢測沒有病毒感染程式檔案的裝置被額外設置成可把狀態傳送至一即時訊息程式。

25. 如申請專利範圍第21項所述之裝置，其中該用以檢測沒有病毒感染程式檔案的裝置被額外設置成可把狀態傳送至一網際網路的瀏覽程式。

26. 如申請專利範圍第21項所述之裝置，另外設置來傳送該狀態至：

- 一防火牆；
- 一主機入侵檢測器；或者
- 一主機易入侵鑑定器(host vulnerability assessor)。

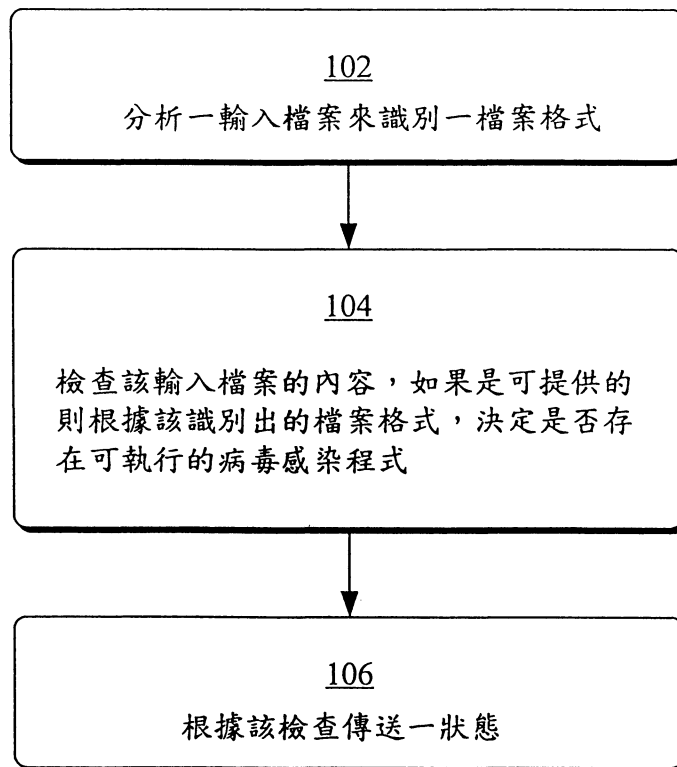
27. 如申請專利範圍第21項所述之裝置，另外設置來傳送一狀態至從一組程式中選出來的一程式，其至少包含：

- 一備份的程式；

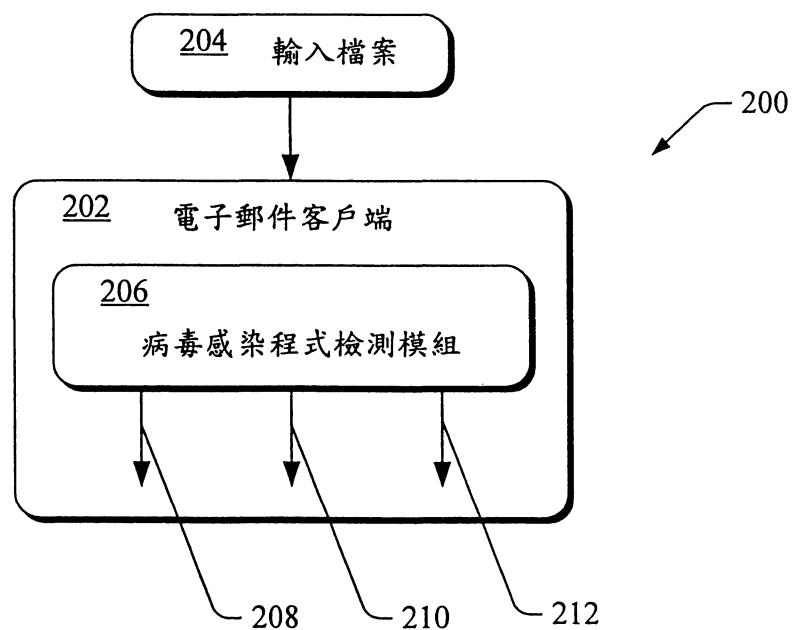
- CD/DVD燒錄程式；及
- 一點對點檔案分享的程式。

28. 如申請專利範圍第21項所述之裝置，其中每組部件分析器係被設置成可識別該複數個資料檔案格式中之一。

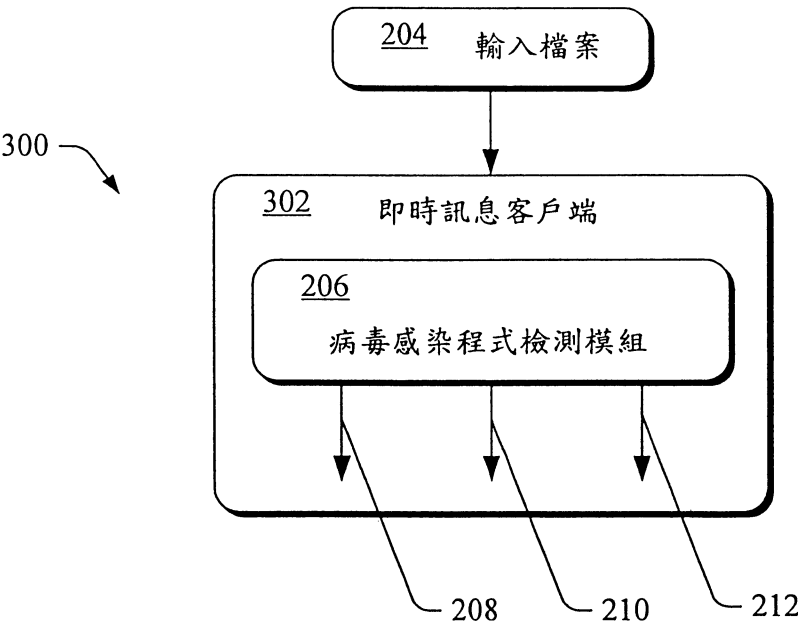
29. 如申請專利範圍第21項所述之裝置，其中該複合分析器係設置成可透過增加一新的部件分析器至該複合部件分析器的方式來擴展該複合分析器，其中該新部件分析器可識別一更進一步的檔案格式並且在該更進一步的檔案格式內識別出可執行的病毒感染程式。



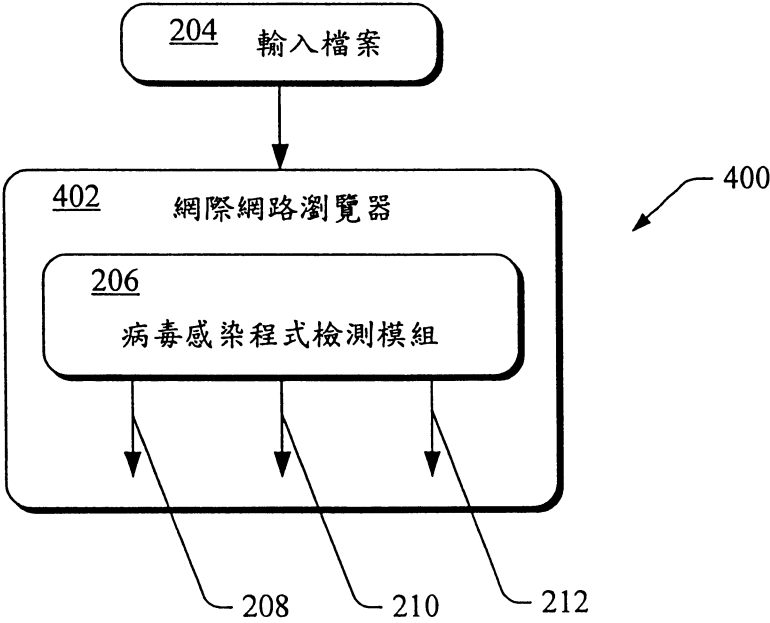
第 1 圖



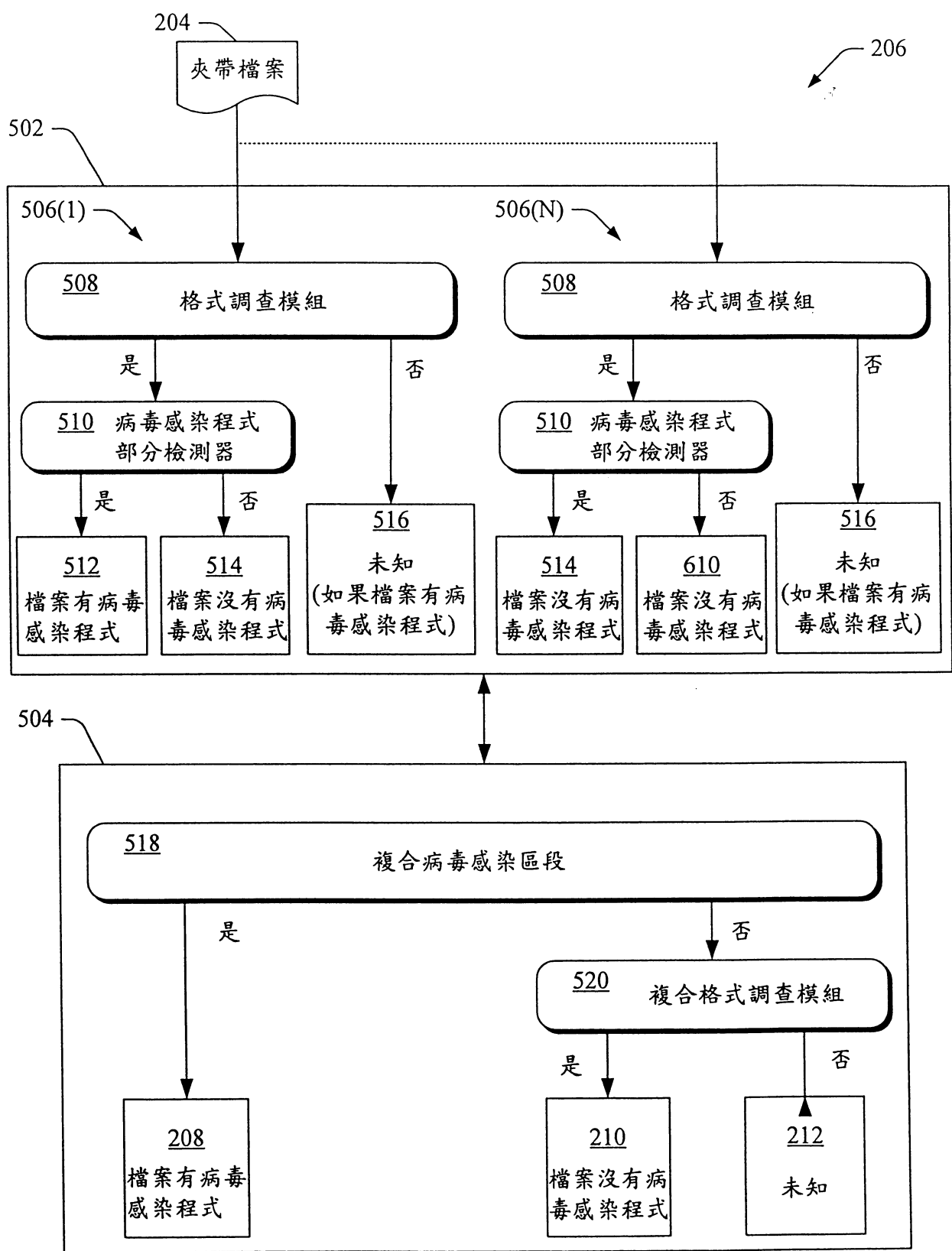
第 2 圖



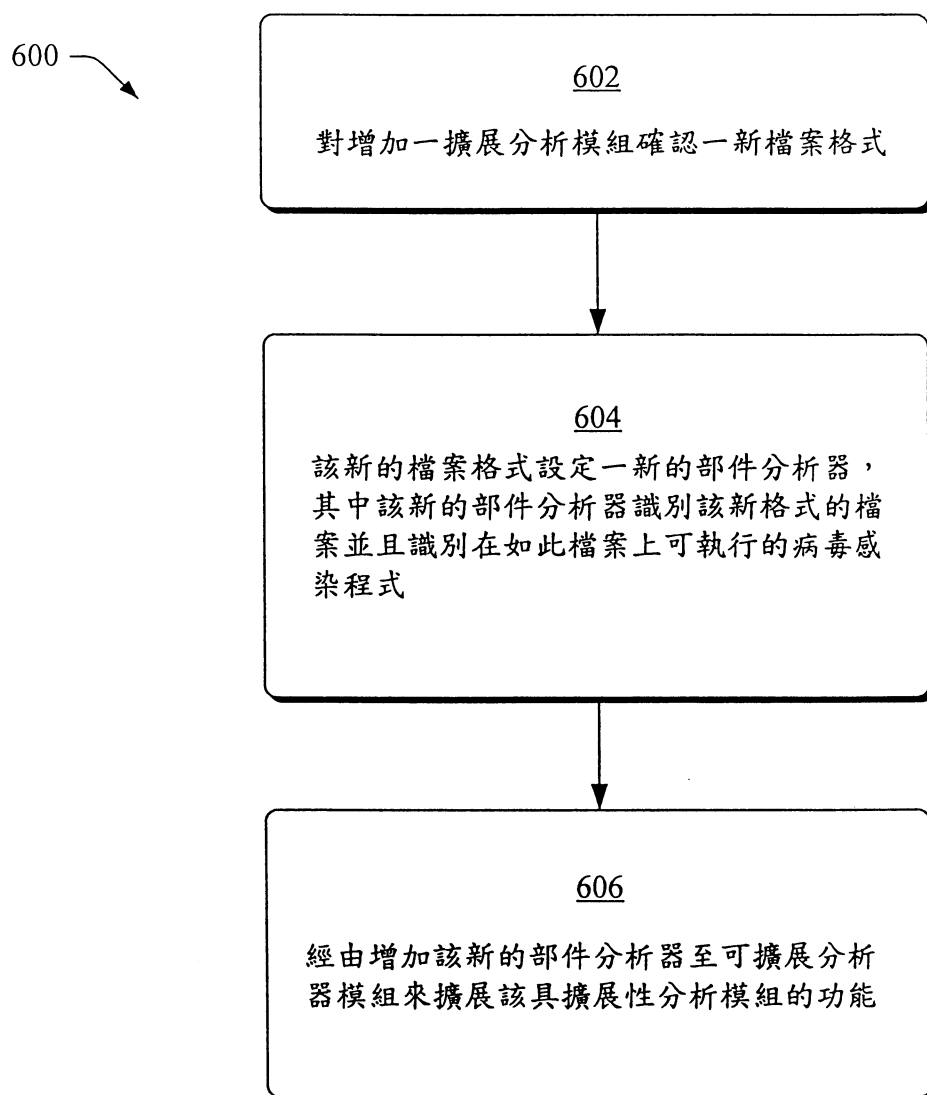
第 3 圖



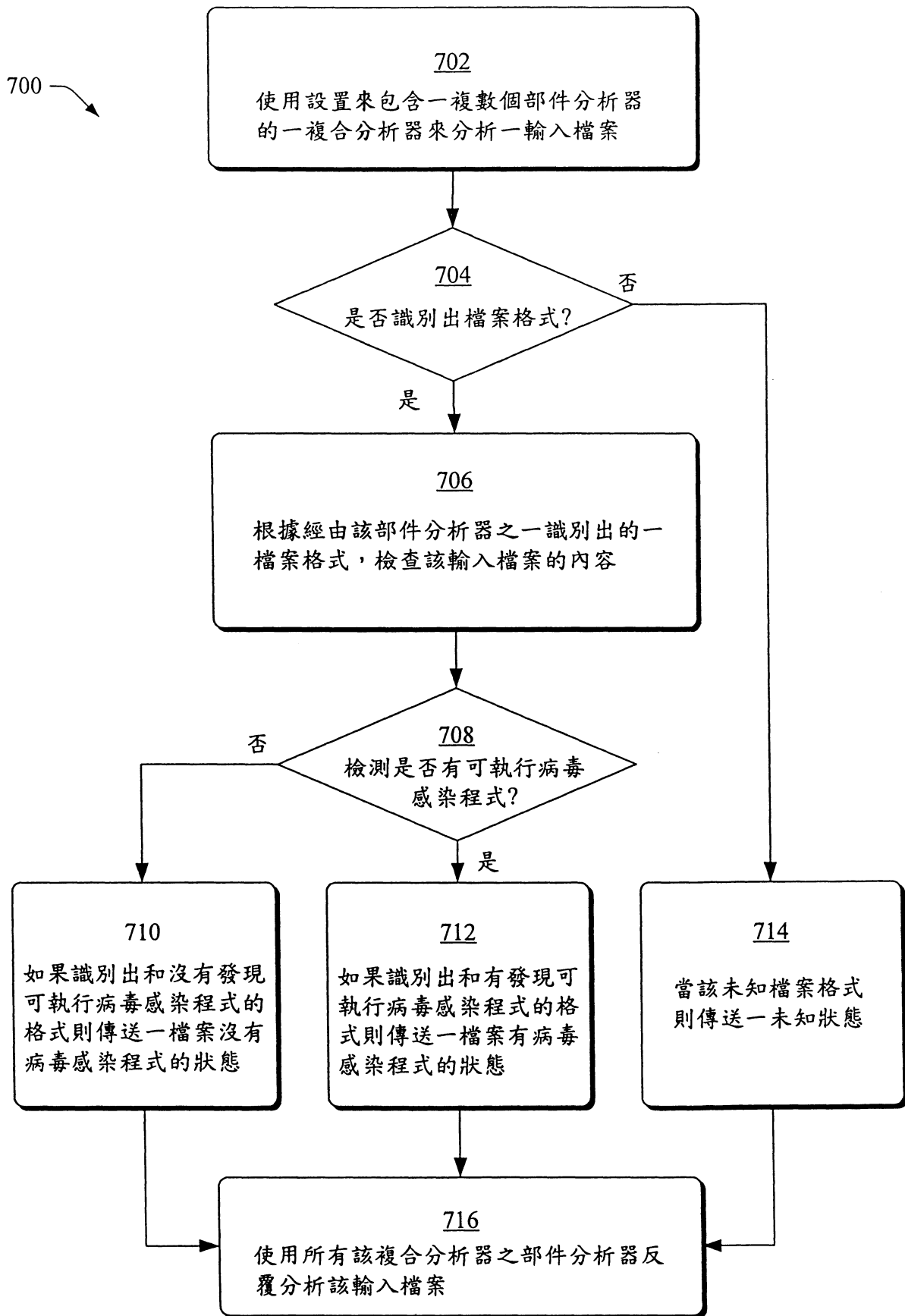
第 4 圖



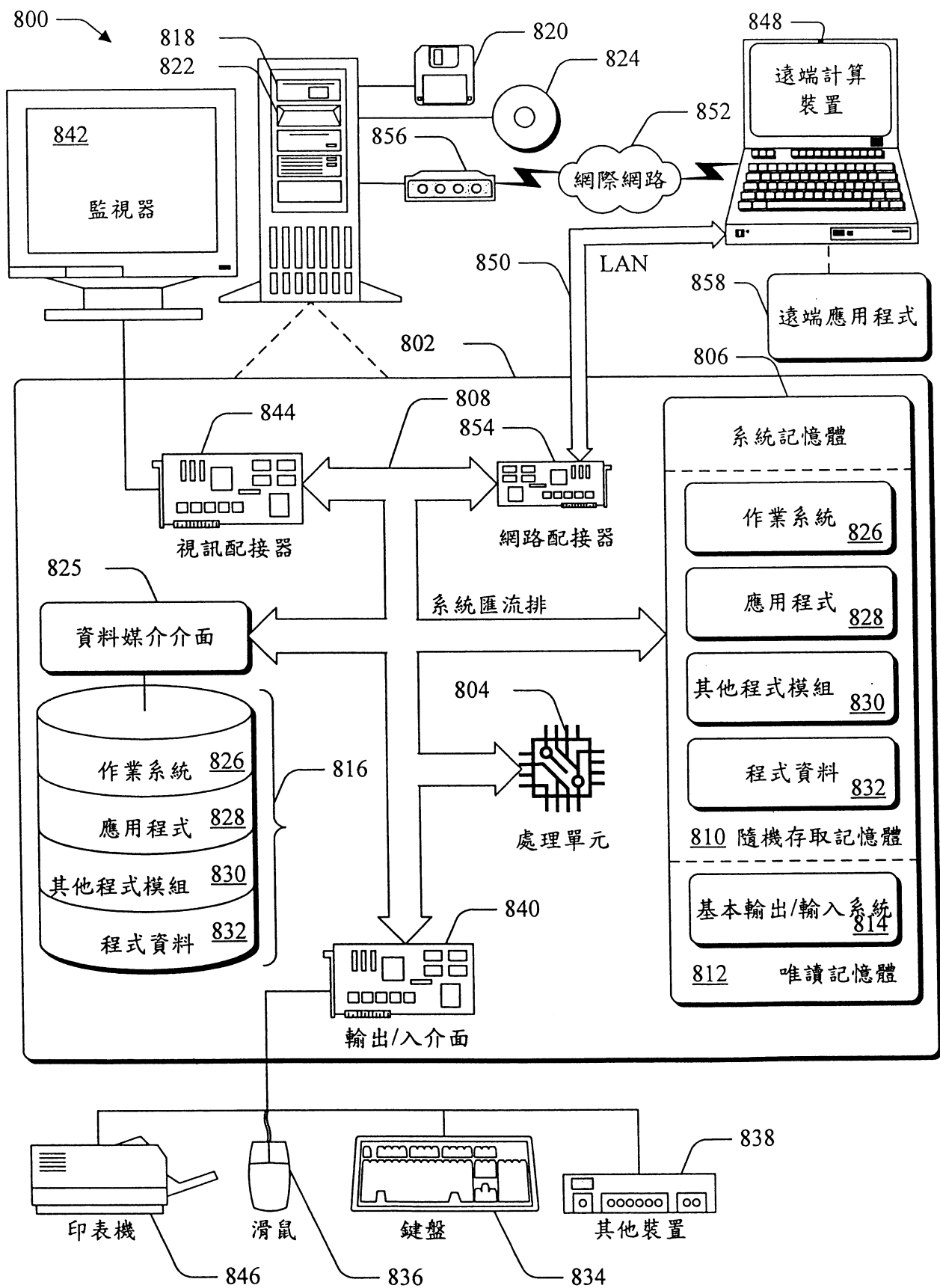
第 5 圖



第 6 圖



第 7 圖



第 8 圖

柒、指定代表圖：

(一)、本案指定代表圖為：第 8 圖。

(二)、本代表圖之元件代表符號簡單說明：

800	計算環境	802	電腦
818	磁性磁碟機	806	系統記憶體
820	磁碟片	826	作業系統
822	光碟機	828	應用程式
824	光碟	830	其他程式模組
842	監視器	832	程式資料
848	遠端計算裝置	810	隨機存取記憶體
850	系統匯流排	812	唯讀記憶體
852	網際網路	814	基本輸出/輸入系統
858	遠端應用程式	808	系統匯流排
804	處理單元	840	輸出/入介面
844	視訊配接器	828	應用程式
854	網路配接器	830	程式模組
825	資料媒介介面	832	程式資料
816	硬碟	846	印表機
826	作業系統	836	滑鼠
834	鍵盤	838	其他裝置

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無