

# 公告本

|      |            |
|------|------------|
| 申請日期 | 89.7.26    |
| 案號   | 89114949   |
| 類別   | G06F 9/445 |

A4  
C4

(以上各欄由本局填註)

| 發明專利說明書 480443 |               |                                                                         |
|----------------|---------------|-------------------------------------------------------------------------|
| 一、發明名稱         | 中文            | 可防病毒及與硬體不相關地閃沖改寫系統基本輸出入系統之方法                                            |
|                | 英文            | VIRUS RESISTANT AND HARDWARE INDEPENDENT METHOD OF FLASHING SYSTEM BIOS |
| 二、發明人          | 姓名            | 克瑞格L. 賈肯                                                                |
|                | 國籍            | 美國                                                                      |
|                | 住、居所          | 美國德州湯寶市卡爾頓谷巷16411號                                                      |
| 三、申請人          | 姓名<br>(名稱)    | 美商·康培克電腦公司                                                              |
|                | 國籍            | 美國                                                                      |
|                | 住、居所<br>(事務所) | 美國德州休士頓市·S.H. 249 20555號                                                |
|                | 代表人<br>姓名     | 艾琳·柯斯圖拉吉斯                                                               |

裝

訂

線

(由本局填寫)

|           |
|-----------|
| 承辦人代碼：    |
| 大類：       |
| I P C 分類： |

A6  
B6

本案已向：

美 國 ( 地 區 ) 申請專利，申請日期： 案號：，☒有 ☐無主張優先權  
1999.07.27 09/362.077

有關微生物已寄存於：，寄存日期：，寄存號碼：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝 訂 線

經濟部智慧財產局員工消費合作社印製

五、發明說明 ( 1 )

本發明之領域

本發明一般係關於一般用途電腦之 BIOS 並且尤其是關於可防止 BIOS 被不小心或未被授權的重新規劃之允許 BIOS 被重新規劃的技術。

相關技術說明

BIOS (基本的輸入/輸出系統) 是一般儲存於電腦特定記憶體區域中的軟體片段或指令碼。當被通電時電腦使用 BIOS 使其本身適當地啟動。BIOS 可以不時地被使用，隨後協助管理在硬體和程式之間的資料交換。

許多不像標準個人電腦一般操作之電子裝置已經開始將 BIOS 併入他們的電路。例如，一組數據機可以包含採用 BIOS 之 80C186 微處理機。進一步地，包含微控制器或微處理機為主之計算電路的 CD 和磁帶寫入器，雷射和噴墨印表機已經開始併入某類 BIOS 以便在開始時使用當被導通時讓裝置操作並且執行。

某些 PC (個人電腦) 操作系統 (例如，Linux，NT) 當系統被執行時分配 BIOS 服務，但是當 PC 開始或被導通時它們全部需要依賴 BIOS。PC 晶片組 (在 PC 主機板上一些晶片之內可看到之 PC 之互連和控制電路主要部份) 具有許多可組態選擇，例如記憶體和匯流排時序，埠組態等等，它們在開始時被 BIOS 組態。但是，如果該等選擇未在開始時被 BIOS 正確地組態則電腦將不操作。

BIOS 被一次地規劃進入 PC 主機板上之 ROM 晶片。BIOS ROM 晶片無法被重新規劃，而需要以新規劃

(請先閱讀背面之注意事項再填寫本頁)

裝  
訂  
線

經濟部智慧財產局員工消費合作社印製

五、發明說明 ( 2 )

的 BIOS ROM 晶片取代。

由於 ROM 晶片成為可被規劃，EEPROM，以及快閃 ROM 開始被使用於 BIOS 晶片。尤其是，快閃 ROM 可被規劃而不需要從電路板被移動。這在個人電腦工業中是有用的，因為快閃 ROM BIOS 晶片 ("快閃 BIOS") 可被重新規劃 ("閃沖改寫") 並且以新的資料升級而不需要打開個人電腦機架。

目前，有各種電腦系統允許 BIOS 指令碼被閃沖改寫。在目前既有之電腦系統閃沖改寫系統 BIOS 之前，閃沖改寫 (重新規劃) 應用一般需確認將被規劃 / 閃沖改寫進入快閃 BIOS 之 BIOS 影像是正確大小或具有正確電腦檔案名稱，但在目前系統中不可能主動地檢查 BIOS 影像以確保它將可與它所欲被載入之電腦匹配。進一步地，在目前不可能規劃例如操作於視窗 '95 或 '98 中之電腦操作系統之 "保護程式" 模式中之一組快閃 ROM BIOS。因此，ROM BIOS 閃沖改寫必須於例如 MS-DOS 之 "實際" 模式操作系統中執行。這閃沖改寫 BIOS 技術之缺點是用以閃沖改寫 ROM BIOS 所需的確認指令碼是以駭客可以發現並且解組合之可執行檔案存在。駭客可容易地從被解組合指令碼識別足夠資訊以產生將被接受為 BIOS 影像並且使電腦無法被使用之快閃 ROM BIOS 影像。

關於電腦使用者閃沖改寫其獨有電腦的 BIOS 能力具有其他的嚴重問題。例如，假定使用者希望升級其快閃 BIOS 中資訊。他將需要從電腦製造商，國際網路，或另

(請先閱讀背面之注意事項再填寫本頁)

裝  
訂  
線

經濟部智慧財產局員工消費合作社印製

## 五、發明說明(3)

一資源得到新的BIOS程式。接著為進行快閃BIOS升級，使用者將啟動其PC上面之"燒寫"程式。亦即，燒寫程式將使用建立於PC之主機板的電路(假設其支援快閃升級)並且清除快閃BIOS晶片中現有資料/資訊並且接著規劃或裝載新的BIOS資料/資訊進入晶片。這是良好的，如果得到適當的BIOS程式並且接著裝載進入快閃BIOS。如果不適當的BIOS程式被裝載進入BIOS晶片，則使用者之電腦將無法操作。

如上面討論，另一問題是駭客將寫入會啟動燒寫軟體並且閃沖改寫無懷疑使用者之電腦的電腦病毒因而使電腦無法操作。

因此，需要一種電腦系統，其抗拒使其BIOS被閃沖改寫而使不匹配之BIOS程式，其他的資料，或無資料留在BIOS程式之記憶體區域中。進一步地，需要一種電腦系統，其具有病毒抗拒性以及硬體獨立方法而閃沖改寫BIOS使得僅匹配於BIOS指令碼之系統可被閃沖改寫進入快閃BIOS晶片。

本發明之一組實施例中，一組電腦系統包含BIOS影像可被儲存於磁性媒體上之一組硬碟驅動器。如果使用者希望以BIOS影像重新規劃一組ROM BIOS部份，一組利用程式將被執行。該利用程式產生一組軟體系統管理中斷以觸發一組處理器程式。處理器程式被儲存於使用者不可存取之RAM的系統管理記憶體部份。處理器程式在BIOS影像找尋一組特定指令碼以決定BIOS影像是

(請先閱讀背面之注意事項再填寫本頁)

訂  
線

五、發明說明（4）

否為被操作電腦系統所認可的認可BIOS影像。如果處理器程式決定BIOS影像是被認可的，它將接著以被認可的BIOS影像重新規劃ROM BIOS部份。

圖形之摘要說明

本發明之各種目的和優點將從下面較佳的實施範例，配合附圖的說明成為明顯並且更容易了解：

第1圖示出可採用本發明之實施例的一組範例電腦系統。

第2圖示出依據本發明用以閃沖改寫ROM BIOS的範例方法之流程圖；以及

第3圖示出依據本發明的硬體和軟體之間的關係範例圖。

較佳實施範例的詳細說明

本發明的實施例將接著被說明。本發明可以用許多不同的形式實施並且不應該被見認為受限制於此處所提出之實施例；反之，這些實施例被提供以使這揭示清楚並且完全，並且將完全地傳達本發明之重要論點至熟習本技術者。

首先參看第1圖，採用本發明之實施例的一般電腦或個人電腦(PC)100之選擇部份被展示。在啟動PC 100時，儲存於快閃ROM BIOS記憶體102中的BIOS程式，被中央處理機("CPU")104所中斷。BIOS是當電腦開啓時被PC 100使用以自行開始的一段指令碼。在某些情況中，BIOS被進一步地採用以管理在硬體和程式

(請先閱讀背面之注意事項再填寫本頁)

裝  
訂  
線

經濟部智慧財產局員工消費合作社印製

五、發明說明 ( 5 )

之間資料交換。被BIOS所"設定"的硬體可以包含RAM記憶體106、硬碟機或磁碟機108、輸入/輸出電路110、以及數據機電路112。

有時使用者可能希望升級或重新規劃快閃BIOS 102。更進一步地，有惡意的駭客可能嘗試著寫入一組'病毒'程式，其導致以新的無效或損壞的BIOS程式或BIOS影像閃沖改寫快閃BIOS 102。在任何情況中，本發明之實施例將協助防止使用者或病毒程式以免有'不被認可的'或不相容的BIOS影像閃沖改寫系統BIOS。利用防止BIOS被以無效，不被認可的或不相容BIOS程式閃沖改寫，電腦修護成本可被避免並且使用者操作之電腦100將成為更可靠的系統。

在本發明之一組實施例中，所有被採用以閃沖改寫ROM BIOS的硬體相依指令碼被儲存在不可存取的SMM(系統管理記憶體)片段。另外，在將硬體相依指令碼複製至記憶體之SMM片段之前，指令碼僅以一種抗解組合壓縮格式存在。更進一步地，一組範例電腦系統將僅在SMI(系統管理中斷)模式時閃沖改寫BIOS，因此，在電腦系統以一種實際模式(例如，MS-DOS模式)、一種虛擬Intel 8086模式或一種保護模式(例如、在視窗'95、'98、NT中操作時，使用虛擬記憶體管理器例如EMM386.exe的MS-DOS)操作時，可以重新規劃或閃沖改寫ROM BIOS。

最好是，本發明使駭客或使用者非常不易決定如何

(請先閱讀背面之注意事項再填寫本頁)

裝  
訂  
線

經濟部智慧財產局員工消費合作社印製

五、發明說明( 6 )

更動或閃沖改寫目前快閃ROM BIOS，因為閃沖改寫BIOS所需的必須指令碼僅在系統管理中斷('SMI')模式時被執行。極度有限機構供駭客或使用者步經在SMI模式時操作之指令碼而得知指令碼如何閃沖改寫ROM BIOS。指令碼是在隱藏於其他程式外的電腦記憶體之部份中被操作；閃沖改寫BIOS之指令碼僅在電腦處理SMI時可被BIOS'見到'。

更進一步地，在電腦電路之內被使用以閃沖改寫BIOS的軟體需要BIOS影像(使用者希望閃沖改寫既有的快閃ROM BIOS部份之新的BIOS資料)具有證實BIOS影像與將被置入之電腦相容的方法。確認的方法可以是被添加至BIOS影像的末端，中間或其他位置之檢查和。確認的方法可以是具有由將被安裝入之電腦之特定模式所了解的編碼格式之BIOS影像。確認方法的目的是在於電腦將不允許其BIOS被閃沖改寫，除非BIOS影像可被確認或被認可為特定電腦模式的有效、被認可的或真正的BIOS影像。

再次參看至第1圖，可以在稍後被閃沖改寫進入ROM BIOS 102之一組BIOS影像可以多種不同方式提供並且儲存於電腦100內。該影像可經由磁碟機、硬碟機、zip驅動器108或其他的資料儲存媒體而被提供。更進一步地，BIOS影像可由廣域網路(例如網際網路)下載、由LAN或WAN取得、或經由電話線數據機或經由一組I/O埠110的其他外部資料連接所提供。

(請先閱讀背面之注意事項再填寫本頁)

裝  
訂  
線

經濟部智慧財產局員工消費合作社印製

五、發明說明 ( 7 )

第2圖示出描述產生被認可的ROM BIOS影像的範例程序以及更新或閃沖改寫ROM BIOS部份之範例步驟的流程圖。產生被認可的BIOS影像之範例程序由步驟200開始，其中一組ROM BIOS影像被處理以產生一組被認可的ROM BIOS影像。有多種方式可以處理BIOS影像以使其被認可。三種使ROM BIOS影像被認可的範例技術被示出，但熟悉本技術者可知有其他的認可技術。產生被認可的BIOS影像之一種技術是使用僅被SMI處理器軟體所得知的一組私用鑰匙將整個BIOS影像加密碼。ROM影像，可被以私用鑰匙解密碼並且接著在閃沖改寫進入ROM BIOS之前確定被解密碼影像是被認可的影像。如果ROM影像無法使用私用鑰匙而被解密碼，它將接著不被認可。各模式的電腦將包含不同的私用鑰匙，因此被加密碼BIOS影像僅可被使用於SMI處理器中具有正確的私用鑰匙以將BIOS影像解密碼之電腦模式中。

產生被認可的BIOS影像之第二種技術是利用在僅被SMI處理器所得知的偏移量或預定指令碼位置將一組隱藏檢查和或循環冗餘檢查('CRC')坎入BIOS影像。該偏移量可在製造程序時被儲存於SMI處理器。只要SMI處理器指令碼知道在BIOS影像中如何找尋認可資訊，偏移量或位置的值並不重要。

產生使用者希望閃沖改寫他的電腦之快閃ROM BIOS部份102的被認可ROM BIOS影像之第三種

(請先閱讀背面之注意事項再填寫本頁)

訂  
線

經濟部智慧財產局員工消費合作社印製

五、發明說明( 8 )

技術是使用一組私用鑰匙將加密碼檢查和或循環冗餘檢查('CRC')附帶或附加至BIOS影像的末端。該私用鑰匙僅可被相似電腦模式之SMI處理器軟體所得知。SMI處理器將協助將檢查和或CRC解密碼以決定BIOS影像是否為一組被認可的影像並且適合被載入電腦之ROM BIOS部份。一旦確認是特定電腦模式的被認可BIOS影像，被認可的BIOS影像將接著可被電腦製造商提供給使用者以使用於他們的電腦。使用者的電腦，在收到BIOS影像後，將具有決定一組所接收之BIOS影像對於特定的電腦是否為被認可的或適當的有效BIOS之方法。由步驟202開始，決定BIOS影像是否為一組適當的被認可BIOS影像之一組範例技術以及閃沖改寫被認可的BIOS影像進入ROM BIOS部份的步驟將被揭露。

在某些情況中製造商將提供一組軟體檔案或具有多數個BIOS影像之檔案。各BIOS影像可被用於不同的電腦模式。在步驟202和204中，電腦的軟體或預載電腦軟體必須決定在多數個BIOS影像中，哪一組是適合被載入特定電腦的RAM BIOS部份的BIOS影像。

在步驟202中，一組硬體無關BIOS閃沖改寫應用程式由一組ACPI支援BIOS中之ACPI表蒐集資訊，但由內存BIOS指令碼在啓始時所產生。在較佳的實施例中，檔案名稱、檔案大小以及軟體SMI埠位置是由ACPI表所蒐集的。檔案名稱最好是特定電腦的BIOS影像可被發現之檔案名稱。檔案大小資訊是BIOS影像檔案的大小。

(請先閱讀背面之注意事項再填寫本頁)

裝  
訂  
線

五、發明說明( 9 )

軟體 SMI 埠是在被寫入時產生一組軟體 SMI 之 I/O 埠位置。

尤其是，一組範例硬體無關快閃應用程式在 RAM 記憶體位址 0E0000H 至 0FFFFFFH 搜尋 ACPI 表簽字 "RSDPTR,"。如果該簽字不被發現，應用程式顯示一組錯誤訊息並且終止。如果該簽字被發現，程式由 ACPI 表讀取下列項目：開機系統說明表 (RSD) 中的 OEM 表 ID，那是包含導出快閃 BIOS 檔案名稱之檔案資訊的欄；2) 以及固定 ACPI 說明表中的 SMI 埠位址。SMI 埠位址是提供 SMI 中斷之 SMI 埠位址。

在步驟 204，硬體無關 BIOS 快閃應用程式將檔案名稱中所發現的 BIOS 影像，如步驟 202 所指定，讀入 RAM 記憶體的鄰近方塊或最好是連續方塊。CPU 暫存器被設定以指示被儲存的 BIOS 影像之位置和大小。

在步驟 206，硬體無關 BIOS 快閃應用程式將一組快閃簽字或其他的資料資訊傳送進入一組或更多組 CPU 暫存器以指示閃沖改寫更動是實際被要求，所需並且有意的。

在步驟 208，BIOS 快閃應用程式利用將一組指令碼寫入至軟體 SMI I/O 埠而產生一組軟體 SMI。該指令碼可以是在步驟 206 時傳送進入一組或更多組 CPU 暫存器的快閃簽字之全部或一部份。這導致 SMI 的發生。ROM

BIOS 的閃沖改寫僅可在一組軟體 SMI 事件時發生於一組範例實施例中。

(請先閱讀背面之注意事項再填寫本頁)

訂  
線

經濟部智慧財產局員工消費合作社印製

五、發明說明 (10 )

步驟 210 中，軟體 SMI 處理器開始操作並且確認快閃簽字。再一次地，快閃簽字指示一組閃沖改寫更動是實際被要求，所需並且有意的。如果軟體 SMI 處理器決定快閃簽字無效，閃沖改寫 BIOS 程序將接著停止並且一組錯誤將在步驟 212 和 214 被顯示給使用者。

在步驟 212，如果快閃簽字是有效的，SMI 處理器將接著前進至步驟 216，其中 SMI 處理器採用僅被 SMI 處理器（如步驟 200 所討論）所得知的一組私用鑰匙或其他資訊以決定 BIOS 影像是否為一組被認可的 BIOS 影像。一組被認可的 BIOS 影像是目前電腦系統之正確的 BIOS 影像。利用要求 SMI 處理器具有一組私用鑰匙或其他的資訊以將一部份解密碼或由其他方式決定 BIOS 影像是一組被認可的 BIOS 影像，將可阻撓駭客以及無經驗的電腦使用者以不適當的 BIOS 影像閃沖改寫一組 ROM BIOS 部份。

如果在 RAM 中的 BIOS 影像不被軟體 SMI 處理器所認可，閃沖改寫程序將接著停止並且一組錯誤訊息將在步驟 218 和 214 被顯示。

如果儲存於 RAM 中的 BIOS 影像在步驟 216 至 218 被軟體 SMI 處理器所認可，一組寫入引動信號將接著在步驟 200 被提供至 ROM 部份。寫入引動信號可以是需要被開啓或關閉的一般用途 I/O。一般用途 I/O 位置也將僅被 SMI 處理器指令碼所得知並且不應該在電腦中任何其他地方被得知或存取，以使駭客難以得知如何引動傳

(請先閱讀背面之注意事項再填寫本頁)

裝  
訂  
線

五、發明說明（11）

送至ROM BIOS部份並且將它們閃沖改寫之信號。

在步驟221中，BIOS SMI處理器將BIOS影像寫入至ROM BIOS部份（亦即，快閃ROM BIOS部份）。寫入引動信號在步驟222被設定為不引動或不作用。在此，BIOS影像已被載入ROM BIOS部份以代替原先存在的ROM BIOS指令碼。在步驟223中，閃沖改寫BIOS程序結束而無錯誤。

接著參看至第3圖，在各種子系統以及開和關電腦主機板的軟體/韌體之間的資料或資訊一般流程被展示用以製作範例抗病毒ROM BIOS閃沖改寫方法和發明。

該注意的是，快閃應用程式300、快閃影像302、操作系統304、軟體處理器306、RAM快閃影像308、以及ACPI表310皆為軟體，韌體或資料指令碼。

在一組實施範例中，使用者或病毒程式將要求快閃應用程式300的執行以將新的BIOS影像302閃沖改寫進入目前的ROM BIOS部份314。BIOS影像302可以被儲存於例如一組硬碟機或磁碟機316的儲存媒體。快閃應用程式300由儲存於RAM記憶體312之ACPI表310取得所需要BIOS檔案名稱和檔案大小資訊。正確的BIOS影像302可接著由儲存媒體316被取得並且被置於RAM308之連續的區塊中。快閃應用程式將接著指示一組ACPI晶片組318以啟動一組軟體SMI中斷，但僅在CPU提供一組快閃簽字以指示閃沖改寫BIOS之要求是有意的之後。軟體SMI處理器接著決定儲存於RAM

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

## 五、發明說明(12)

308之快閃影像是否為一組被認可的BIOS影像。認可程序是經由僅被使用以檢查BIOS影像被授權和認可之SMI軟體處理器所得知的一組秘密加密碼鑰匙或其他秘密資料而建立的。

因為SMI處理器僅在軟體SMI中斷被應用時操作；並且因為SMI處理器被儲存於使用者不可存取的RAM部份，因此駭客非常不易決定認可一組BIOS影像所需或被使用的秘密指令碼或資訊。因此，如果軟體SMI處理器不認可BIOS影像，ROM BIOS部份將接著無法被閃沖改寫。

此實施範例因此建立一種抗病毒供閃沖改寫ROM BIOS之方法。本實施例需要非常不易被駭客所產生的一組被認可BIOS影像，因為該資訊被隱藏在軟體SMI處理器內。軟體SMI處理器指令碼顯著地不可被使用者或駭客所存取，因為它被置放在系統管理記憶體片段(SMM片段)之記憶體部份並且，此外，在不被使用時僅以一種抗解組合壓縮格式存在。

雖然本發明和方法的各種較佳實施例已被展示並且說明，熟習此技術者將了解這些實施例可有各種非主要和主要改變而不脫離本發明之原理和精神，本發明之範疇由所附加之申請專利範圍定義。

(請先閱讀背面之注意事項再填寫本頁)

裝  
訂  
線

五、發明說明 ( 13 )

元 件 標 號 對 照 表

- 1 0 0 … … 個 人 電 腦
- 1 0 2 … … 快 閃 R O M B I O S 記 憶 體
- 1 0 4 … … 中 央 處 理 機
- 1 0 6 … … R A M 記 憶 體
- 1 0 8 … … 硬 碟 機 或 磁 碟 機
- 1 1 0 … … 輸 入 / 輸 出 電 路
- 1 1 2 … … 數 據 機 電 路
- 3 0 0 … … 快 閃 應 用 程 式
- 3 0 2 … … 快 閃 影 像
- 3 0 4 … … 操 作 系 統
- 3 0 6 … … 軟 體 處 理 器
- 3 0 8 … … R A M 快 閃 影 像
- 3 1 0 … … A C P I 表
- 3 1 2 … … R A M 記 憶 體
- 3 1 4 … … R O M B I O S 部 份
- 3 1 6 … … 儲 存 媒 體
- 3 1 8 … … A C P I 晶 片 組
- 3 2 0 … … 中 央 處 理 機

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

經濟部智慧財產局員工消費合作社印製

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

四、中文發明摘要 (發明之名稱：可防病毒及與硬體不相關地閃沖改寫系統基本輸出入系統之方法)

一種在個人電腦之ROM BIOS被重新規劃之前，確定BIOS影像是與BIOS將被重新規劃之電腦匹配的系統和方法。這是利用要求進行ROM BIOS之重新規劃的應用程式具有儲存於使用者無法存取之電腦記憶體部份中的安全部份指令碼而達成。該安全部份指令碼被使用以確保將被規劃進入電腦的BIOS影像是與該電腦匹配。

英文發明摘要 (發明之名稱：VIRUS RESISTANT AND HARDWARE INDEPENDENT METHOD OF FLASHING SYSTEM BIOS)

A system and method for making sure that before the ROM BIOS of a personal computer is reprogrammed, the BIOS image is compatible with the computer whose BIOS are being reprogrammed. This is done by requiring the utility that performs the reprogramming of the ROM BIOS to have a secure portion of code that is stored in a portion of the computer's memory that is inaccessible to a user. The secure portion of code is used to make sure that the BIOS image to be programmed into the computer is compatible with the computer.

## 六、申請專利範圍

1. 一種電腦系統，其包含：

一組硬碟驅動器，用以接收以及儲存BIOS影像；

一組快閃ROM BIOS部份，用於以該BIOS影像被閃沖改寫；

一組RAM記憶體，用以當該BIOS影像是將被閃沖改寫進入該快閃ROM BIOS部份時從該硬碟接收以及儲存該BIOS影像；以及

一組軟體SMI處理器程式，用以在允許該BIOS影像被閃沖改寫進入該快閃ROM BIOS部份之前決定該BIOS影像是否為特定電腦系統的被認可BIOS影像。

2. 如申請專利範圍第1項之電腦系統，其中該軟體SMI處理器程式進一步地包含電腦使用者大致無法存取之一組指令碼。

3. 如申請專利範圍第1項之電腦系統，其中該軟體SMI處理器僅可經由一組軟體SMI中斷被存取。

4. 如申請專利範圍第1項之電腦系統，其中該BIOS影像至少包含一組加密碼部份，該加密碼部份是利用該軟體SMI處理器程式解密碼。

5. 如申請專利範圍第4項之電腦系統，其中該軟體SMI處理器程式使用該加密碼部份決定是否該BIOS影像為該被認可的BIOS影像。

6. 如申請專利範圍第1項之電腦系統，其中該BIOS影像包含CRC以及檢查和之至少一組，該至少一組CRC以及檢查和被該軟體SMI處理器程式使用以決定該

(請先閱讀背面之注意事項再填寫本頁)

訂

線

## 六、申請專利範圍

BIOS 影像是否為該被認可的 BIOS 影像。

7. 如申請專利範圍第 1 項之電腦系統，其中該軟體 SMI 處理器程式是一種硬體無關程式。

8. 如申請專利範圍第 1 項之電腦系統，其中該軟體 SMI 處理器程式被儲存於記憶體之系統管理記憶體片段中。

9. 如申請專利範圍第 1 項之電腦系統，其中該軟體 SMI 處理器程式以抗解組合壓縮格式存在。

10. 一種用以提供被認可影像的方法，該方法包含的步驟有：

產生一組 BIOS 影像；以及

將該 BIOS 影像後處理以產生被認可的 BIOS 影像，該被認可的 BIOS 影像至少包含可被一組預定電腦模式上面所發現的程式解釋之一組預定指令碼。

11. 如申請專利範圍第 10 項之提供被認可 BIOS 影像的方法，其中該預定指令碼至少包含公用鑰匙、檢查和、CRC、以及加密碼部份之一種。

12. 一種用以閃沖改寫電腦系統中 ROM BIOS 部份之方法，該方法包含的步驟有：

決定一組快閃 BIOS 檔案名稱以及一組快閃 BIOS 檔案大小；

決定一組軟體 SMI 埠中斷；

置放具有該被決定快閃 BIOS 檔案名稱以及該快閃 BIOS 檔案大小之一組 BIOS 影像進入 RAM；

## 六、申請專利範圍

使用一組快閃 BIOS 簽字以指示閃沖改寫該 BIOS 是有意的；

產生一組軟體 SMI 中斷；

在該軟體 SMI 中斷時執行一組特定指令碼以決定該 BIOS 影像是否為該電腦系統之被認可的 BIOS 影像；並且

如果該 BIOS 影像被決定為該被認可的 BIOS 影像則閃沖改寫該 ROM BIOS 部份。

13. 如申請專利範圍第 12 項之用以閃沖改寫該電腦系統中該 ROM BIOS 部份之方法，其中該 BIOS 影像具有該被決定之快閃 BIOS 檔案名稱並且該快閃 BIOS 檔案大小是被置於連續的 RAM 區塊中。

14. 如申請專利範圍第 12 項之用以閃沖改寫該電腦系統中該 ROM BIOS 部份之方法，其中該執行特定指令碼的步驟包含將該 BIOS 影像之預定部份解密碼之步驟。

15. 如申請專利範圍第 12 項之用以閃沖改寫該電腦系統中該 ROM BIOS 部份之方法，其中該執行特定指令碼的步驟包含檢查發現於該 BIOS 影像之預定部份中之檢查和以及 CRC 之至少一組的步驟。

16. 一種用以重新規劃電腦系統中 ROM BIOS 部份之方法，該方法包含的步驟有：

決定是否使用者有意地啟動 ROM BIOS 部份之重新規劃；

建立可與該電腦系統匹配之被認可的 ROM BIOS 影

六、申請專利範圍

像之一組ROM BIOS影像；並且

如果該ROM BIOS影像是被認可的ROM BIOS影像則重新規劃該ROM BIOS部份。

17.如申請專利範圍第16項之用以重新規劃電腦系統中ROM BIOS部份之方法，其中該決定步驟採用軟體SMI啟動之一組程式。

18.如申請專利範圍第16項之用以重新規劃電腦系統中ROM BIOS部份之方法，其中該建立步驟包含反應於軟體SMI而執行儲存於RAM之系統管理記憶體片段中軟體的步驟。

19.如申請專利範圍第16項之用以重新規劃電腦系統中ROM BIOS部份之方法，其中該建立步驟包含至少將該BIOS影像之預定部份以一組私用鑰匙解密碼的步驟。

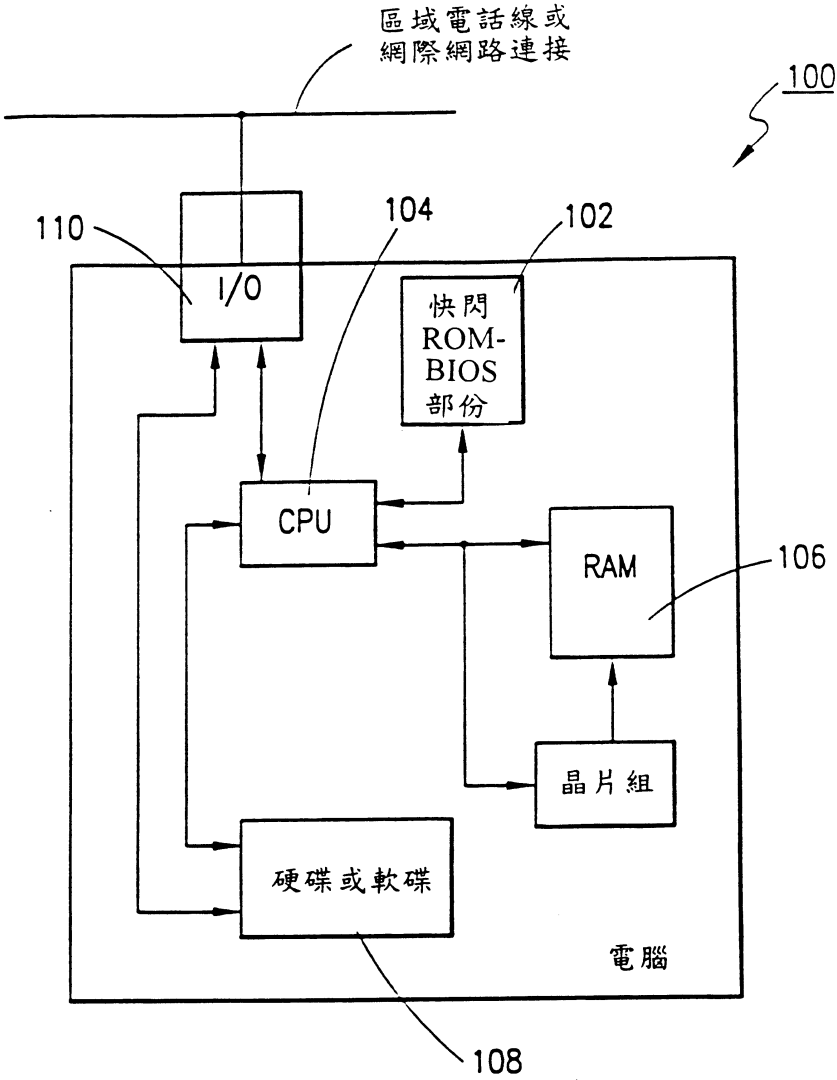
20.如申請專利範圍第16項之用以重新規劃電腦系統中ROM BIOS部份之方法，其中該重新規劃該ROM BIOS部份之步驟包含以該ROM BIOS影像閃沖改寫該ROM BIOS部份的步驟。

(請先閱讀背面之注意事項再填寫本頁)

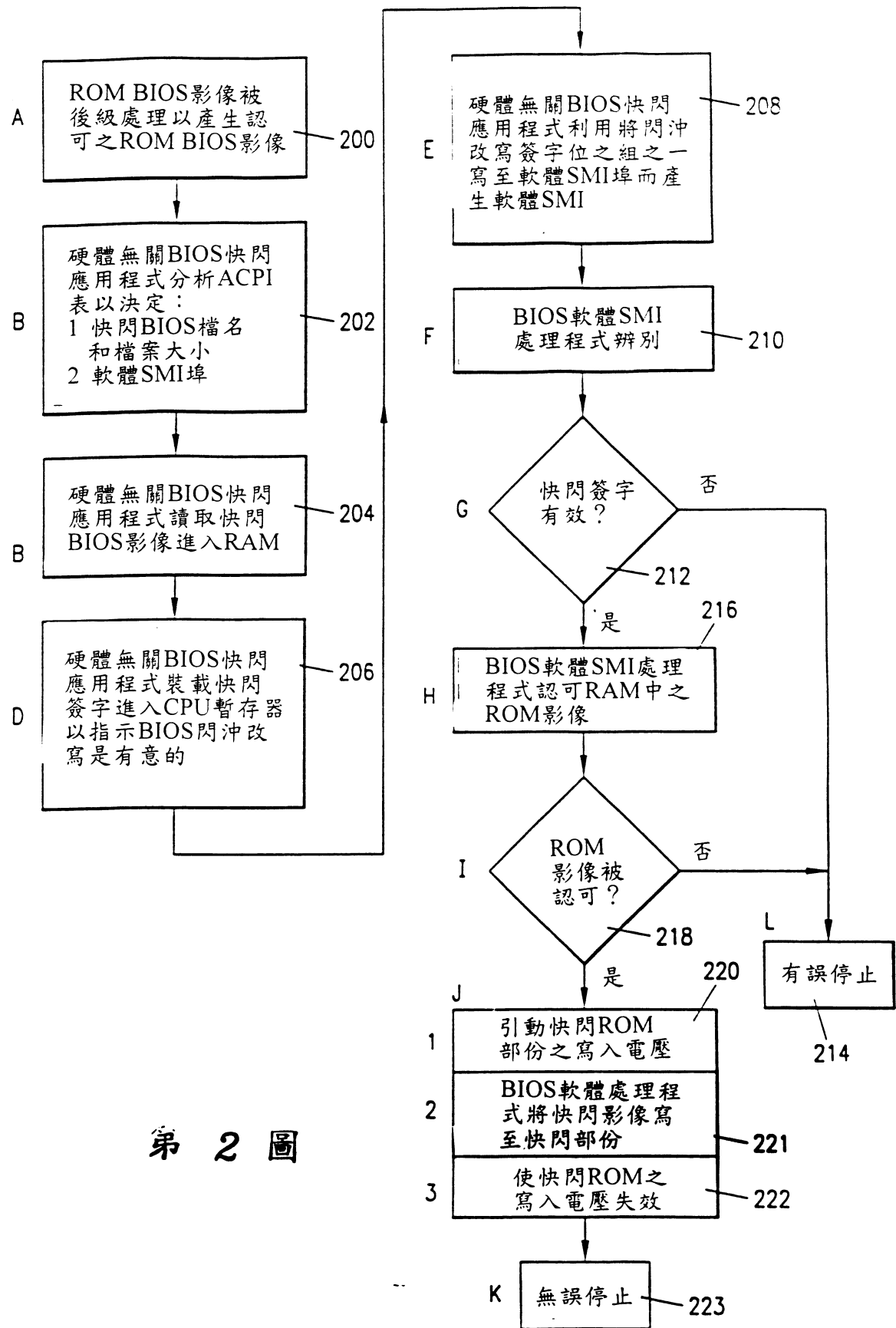
裝

訂

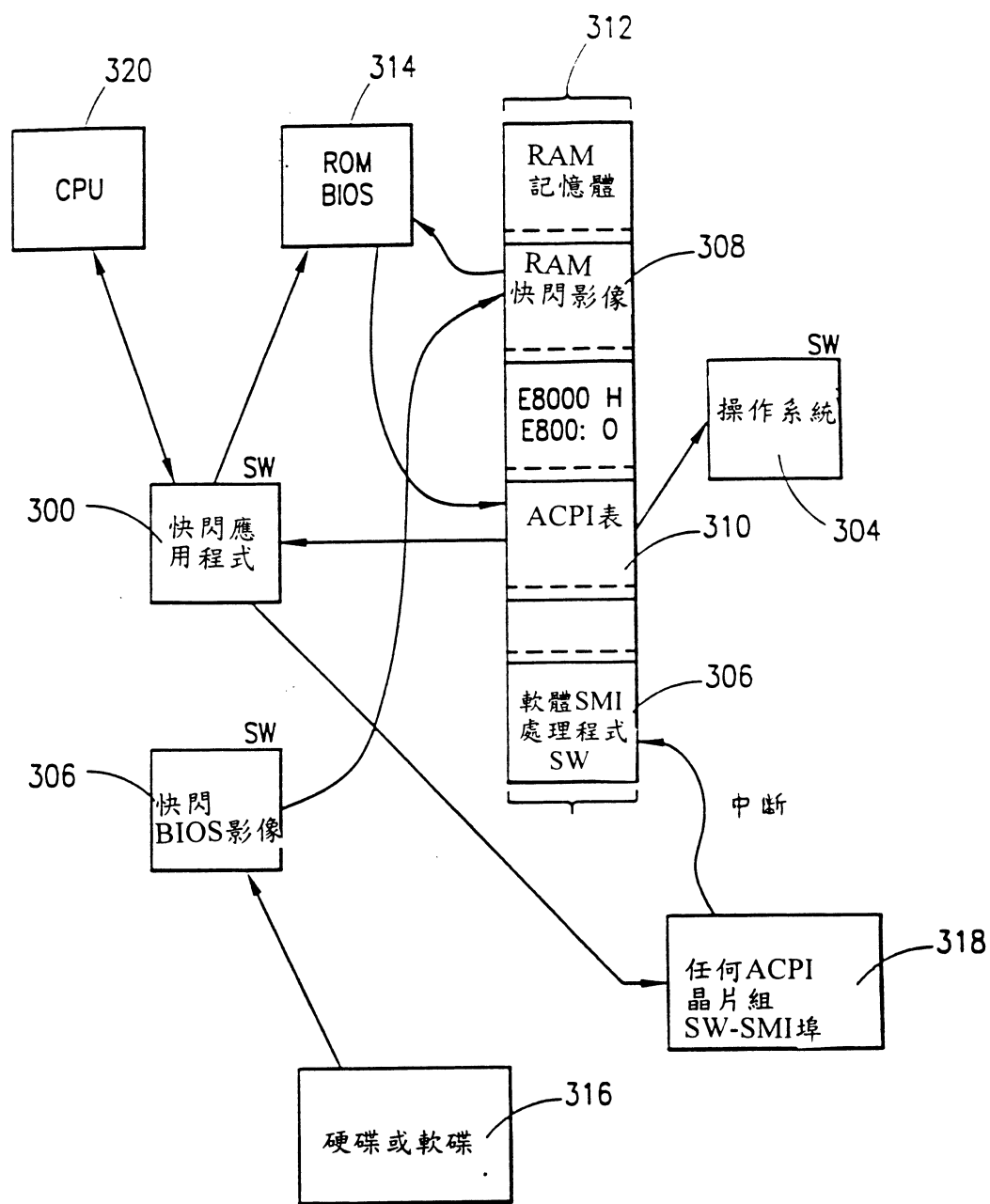
線



第 1 圖



第 2 圖



第 3 圖