

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：**96128093**

※ 申請日期：**96.1.31**

※IPC 分類：

G06F 3/06
G06F 2/00

一、發明名稱：(中文/英文)

硬碟資料防護方法 / HARDDISK SECURITY METHOD

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

緯創資通股份有限公司 / WISTRON CORP.

代表人：(中文/英文)

林憲銘 / LIN, HSIENMING

住居所或營業所地址：(中文/英文)

台北縣汐止市新台五路一段 88 號 21 樓

21F, NO.88, SEC.1, HSIN TAI WU RD., HSICHIH, TAIPEI HSIEN 221,
TAIWAN, R.O.C.

國 籍：(中文/英文)

中華民國 / R.O.C.

三、發明人：(共 1 人)

姓 名：(中文/英文)

卓叔靜 / CHO, SHUCHING

國 籍：(中文/英文)

中華民國 / R.O.C.

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：

1.

2.

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。

九、發明說明：

【發明所屬之技術領域】

本發明是有關於一種硬碟資料防護方法，且特別是有關於一種存取硬碟分割表(Partition Table)的方式，達到保護硬碟資料的方法。

【先前技術】

以個人電腦而言，多使用硬碟作為資料儲存裝置，因此對於個人電腦資料儲存裝置的安全保護機制日益重要。電腦硬碟遭竊常常造成隱私資料外流，若遭人不當利用時損失將會嚴重。常見的防護方法是對檔案、資料夾設定密碼，讓未通過認證的使用者無法窺視這些資料。但是這樣仍有缺點，其一是使用上不方便，每次要開啟或加密檔案時，都必須個別輸入一組密碼，除了造成使用者密碼記憶上的困擾，另一方面是保護範圍不夠全面。

因此更發展出一些透過對整顆硬碟以韌體(firmware)加密的方式，例如在硬碟與電腦系統間加上一硬體晶片，使用者必須透過實體金鑰或指紋來啟動硬碟。韌體加密的共同概念，使用者只需在啟用韌體加密硬碟時完成認證設定，以後使用此加密硬碟時，便會在存取所有資料時作即時的加密，因此使用者在使用上不需改變任何使用習慣而可將之視為一般硬碟使用，亦不須針對個別檔案再作任何加密的設定。但透過韌體加密的硬碟，即相當於將整顆硬碟鎖死，即使將加密硬碟接到另一部電腦來使用，也只會看到一個未格式化或錯誤格式的硬碟，或甚至連硬碟名稱

都抓不到。因此韌體加密方式雖然能全面保護硬碟上所有資料，但是在實際使用上，將造成加密硬碟在被重複利用上的不便，因為透過韌體加密的硬碟，若未再經由韌體解密，即使欲格式化該加密硬碟以重新使用都不行。因此，假設公司員工離職，並未將加密硬碟解密，或遺失了實體金鑰，則加密硬碟即形同一個報廢的硬碟而無法再被重複使用。

【發明內容】

有鑑於此，本發明係提出一種硬碟資料防護方法，主要係利用基本輸入輸出系統(Basic Input-Output System, BIOS)來儲存/覆寫硬碟分割表(Partition Table)的方式，並結合系統的開機密碼(Power-On Password)，而實現的一種硬碟資料防護機制。在啟用本發明之硬碟資料防護機制時，電腦於休眠或關機前，會先將欲保護之硬碟的主啟動磁區(Master Boot Record, MBR)中的硬碟分割表資料儲存並保留在 BIOS 記憶體，再透過覆寫一空值以覆蓋硬碟主啟動磁區(MBR)中之硬碟分割表，即寫入 00h 至主啟動磁區(MBR)中的硬碟分割表的特定儲存位置，以覆蓋該硬碟原有之硬碟分割表。待下次電腦開機，使用者輸入了正確的開機密碼，並經比對該硬碟之硬碟序號(HDD Serial Number)無誤後，才會將先前儲存於 BIOS 記憶體中的硬碟分割表資料，覆寫回該硬碟之主啟動磁區(MBR)以回復該硬碟之硬碟分割表，使得該硬碟回復原本的硬碟分割表可供存取參考，而使該硬碟恢復可被存取及使用的狀態。

因此，若啟用本發明之硬碟資料防護機制，於每次電腦休眠或關機前，系統 BIOS 均會記錄該欲受保護的硬碟之硬碟序號，並儲存該硬碟之硬碟分割表的內容於 BIOS 記憶體中，然後在硬碟主啟動磁區(MBR)裡硬碟分割表的儲存磁區寫入空值 00h，以覆蓋原有的硬碟分割表的內容，最後才切斷系統電源。使得該欲受保護的硬碟失去原本硬碟分割表的內容供存取參考而無法被讀取。即使該硬碟被移至別台電腦使用，也會因為無硬碟分割表供存取時的參考，而使該硬碟就像是一個未經格式化的磁碟，無從取得任何儲存於該硬碟內之檔案資料，以達到保護硬碟內資料的目的。

待下次電腦開機或結束休眠，BIOS 執行系統初始化時，會要求使用者輸入開機密碼，除了判斷該開機密碼是否正確外，同時判斷該開機密碼是否符合相對之該硬碟的硬碟序號。若上述條件之一不符合，系統 BIOS 便會停止開機或停止離開休眠模式的後續動作，使得系統無法進入作業系統的環境中。但若使用者輸入之開機密碼正確，亦符合相對應的硬碟序號，系統 BIOS 才會將先前存於 BIOS 記憶體中的該硬碟之硬碟分割資料，覆寫回復至該硬碟主啟動磁區(MBR)裡的硬碟分割表，使得該硬碟回復原本的硬碟分割表可供存取參考，而使該硬碟恢復可被存取及使用的狀態。

【實施方式】

本發明係為一種硬碟資料防護方法，主要係利用基本

輸入輸出系統記憶體(BIOS ROM)，來儲存/覆寫硬碟分割表(Partition Table)的方式，同時亦可結合開機密碼(Power-On Password)機制，而實現的一種硬碟資料防護方法。以下配合圖示詳細先說明本發明之內容及技術，再應用本發明方法技術之較佳實施例詳細說明本發明方法之步驟流程。

首先，請先配合參照第 1 圖，係為本發明之硬碟資料防護方法實施例步驟流程圖。本發明所提之硬碟資料防護方法，至少包含步驟：當一電腦系統關機或進行一休眠模式(Suspend To Disk, STD)時，讀取一硬碟之一硬碟序號與一硬碟分割表(Partition Table)，並儲存該硬碟序號與該硬碟分割表於一基本輸入輸出系統記憶體(步驟 100)；以及，於儲存該硬碟序號與該硬碟分割表後，抹除儲存於該硬碟之該硬碟分割表(步驟 110)。其中，上述之硬碟分割表為儲存於該硬碟之主啟動磁區(Master Boot Record, MBR)中固定位置之該硬碟的分割資訊。而休眠(STD)係指在系統關機時，將所有的動作與狀態暫時全部儲存在系統磁碟中再關閉電源之模式。另外，上述步驟 100 更包含提供使用者選擇對至少一個該硬碟使用硬碟資料防護(步驟 101)。而步驟 110 抹除儲存於該硬碟之該硬碟分割表，係透過覆寫入一空值至該主啟動磁區(MBR)中之該硬碟分割表的儲存位置。

接著，請配合參照第 2 圖，係為本發明之硬碟資料防護方法解除硬碟資料防護的步驟流程圖。然而，在對電腦系統啟用本發明之硬碟資料防護方法時，更包含解除硬碟資料防護的步驟：當該電腦系統開機或自休眠模式(STD)回復時，將儲存於該基本輸入輸出系統記憶體之該硬碟分

割表覆寫回符合該硬碟序號之硬碟(步驟 120)。其更包含一細部流程 A: 要求使用者輸入一開機密碼(步驟 121), 其中, 開機密碼為電腦透過基本輸入輸出系統(BIOS)啟動時要求使用者輸入的使用者密碼; 接著, 判斷該開機密碼否正確(步驟 122); 然後, 比對該基本輸入輸出系統記憶體中儲存之該硬碟序號與該電腦系統上之該硬碟是否相符(步驟 123); 若步驟 123 的比對結果不相符, 則停止該電腦系統開機或停止該電腦系統自該休眠模式回復, 並提示一錯誤訊息(步驟 124); 但若步驟 123 中該硬碟序號符合該電腦系統上安裝之該硬碟, 表示於該基本輸入輸出系統記憶體中儲存之該硬碟分割表為該硬碟所原有, 因此, 才將儲存於該基本輸入輸出系統記憶體之該硬碟分割表覆寫回符合該硬碟序號之該硬碟(步驟 125); 如此, 即解除該硬碟受資料防護的狀態。

因此, 本發明之方法係於電腦休眠或關機前, 先將欲保護之硬碟的主啟動磁區(MBR)中的硬碟分割表資料儲存於 BIOS 記憶體, 並透過覆寫(overwrite)一空值以覆蓋該硬碟主啟動磁區(MBR)中之硬碟分割表, 即寫入 00h 至該硬碟上之該硬碟分割表的儲存位置, 以覆蓋該硬碟原有之硬碟分割表。待下次電腦開機時, 使用者輸入了正確的開機密碼後, 再將先前儲存保留於 BIOS 記憶體中的硬碟分割表, 覆寫回符合該硬碟之該硬碟主啟動磁區(MBR)中, 以回復使用該硬碟時必須存取參照之硬碟分割表。

接下來, 請配合參照第 3A、3B、3C 圖, 係為應用本發明硬碟資料防護方法的系統之操步驟流程圖。首先, 請

先參照第 3A 圖，本發明所提供的硬碟資料防護機制時，若結合開機密碼的功能，則每當電腦系統開機或自休眠模式 (STD) 回復時，先由 BIOS 程式進行一開機程序並要求使用者輸入開機密碼 (步驟 200)；接著，判斷該開機密碼是否正確 (步驟 210)；若該步驟 210 之開機密碼輸入錯誤，則系統將顯示錯誤並停止開機程序 (步驟 221)；但若於步驟 210 中輸入之開機密碼正確，則接著比對該 BIOS 記憶體中儲存之該硬碟序號與該電腦系統上之該硬碟是否相符 (步驟 220)；若該步驟 220 比對結果不相符時，則系統亦會顯示錯誤並停止開機程序 (步驟 221)；但若於步驟 220 中之比對結果相符，則將先前儲存於 BIOS 記憶體中的該硬碟之硬碟分割表覆寫回符合該硬碟序號之硬碟 (步驟 230)；接著，完成 BIOS 開機程序，並完成作業系統 (Operation System, OS) 的載入，以供使用者操作該電腦；於步驟 230 之後，電腦系統的控制權遂由 BIOS 交給作業系統接管，以處理使用者的命令和輸入輸出的資料。而後，請接著參照第 3B 圖，當使用者欲結束使用電腦系統時，選擇使該電腦是否進行關機或休眠模式 (步驟 240)；此時，系統可提出詢問使用者是否啟用硬碟資料防護 (步驟 250)，以供使用者選擇；若於步驟 250 中，使用者選擇不啟用，則結束本流程並直接進行休眠或關機；但若步驟 250 中選擇啟用硬碟資料防護，則會讀取該硬碟之序號，並記錄下該硬碟序號於 BIOS 記憶體中 (步驟 270)；然後，再透過程式讀取該硬碟之硬碟分割表並儲存於 BIOS 記憶體中 (步驟 280)；而後，抹除該硬碟主

啟動磁區(MBR)中之該硬碟分割表(步驟 290)；最後，結束本流程並進行系統休眠或關機程序。

於上述步驟 250 詢問使用者是否啟用該硬碟防護機制之後，可再包含一細部流程 B，請配合參照第 3C 圖，當使用者選擇是否對該硬碟啟用硬碟資料防護時，可再包含該電腦系統提示出該電腦上所有硬碟的硬碟序號(步驟 260)；以及，由使用者選擇對特定之硬碟啟用硬碟資料防護(步驟 261)。

藉此，凡是啟用本發明硬碟資料防護之硬碟，只要電腦一經關機或休眠，該硬碟之硬碟分割表的內容即被儲存並保留在 BIOS 記憶體中，並且抹除該硬碟之硬碟分割表，使該硬碟無法被存取而進入被保護的狀態。同時，藉由比對該 BIOS 記憶體中儲存之該硬碟序號與該電腦系統上之硬碟的硬碟序號，以確保受保護狀態下的硬碟於原電腦系統再次開機時，可順利寫回其原有之硬碟分割表。另外，亦確保若將其他硬碟安裝於此電腦上，而當電腦再次開機時，其另外安裝的硬碟之硬碟分割表不致被覆寫，而造成其他硬碟的資料遺失。因此，受保護狀態下的硬碟，必須安裝於與關機前同一台之電腦上才能回復該硬碟之硬碟分割表，也才能繼續正常使用該硬碟，以確保受保護狀態下的硬碟中的資料於電腦關機中被有心人士盜用，達到保護硬碟內資料的目的。

再者，本發明所提出的為一種利用硬碟分割表結合開機密碼的硬碟資料防護機制，使得受保護狀態下之硬碟，因其僅為失去硬碟分割表供存取參考而無法被讀取，但仍

然可經由重新格式化而成為一空的硬碟而可供重複使用，達到簡單保護硬碟資料檔案之目的，同時受保護之硬碟仍然具有高度可重複再使用之特性。

雖然本發明已以一較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作各種之更動與潤飾，因此本發明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】

為讓本發明之上述和其他目的、特徵、優點與實施例能更明顯易懂，所附圖式之詳細說明如下：

第 1 圖，係為本發明之硬碟資料防護方法實施例步驟流程圖。

第 2 圖，係為本發明之硬碟資料防護方法之解除硬碟資料防護的步驟流程圖。

第 3A，3B，3C 圖，係為應用本發明硬碟資料防護方法的系統之操作步驟流程圖。

【主要元件符號說明】

步驟 100 ~ 125	方法步驟
步驟 200 ~ 290	方法步驟

五、中文發明摘要

硬碟資料防護方法

本發明係為一種硬碟資料防護方法，該方法提供一硬碟資料防護機制，結合開機密碼(Power-On Password)的機制，藉由將硬碟的主啟動磁區(Master Boot Record, MBR)中的硬碟分割表(Partition Table)的內容儲存於 BIOS 記憶體中，並抹除該硬碟之硬碟分割表的方式，達到保護硬碟資料的目的。

六、英文發明摘要

HARDDISK SECURITY METHOD

A harddisk security method, provides a security mechanism combining with the power-on password function for the storage data in a harddisk. By restoring the partition table into the BIOS ROM in advance, and erasing the partition table of the harddisk, thus the harddisk is secured.

十、申請專利範圍：

1.一種硬碟資料防護方法，至少包含下列步驟：

當一電腦系統關機或進行一休眠模式(Suspend To Disk, STD)時，讀取一硬碟之一硬碟序號與一硬碟分割表(Partition Table)，並儲存該硬碟序號與該硬碟分割表於一基本輸入輸出系統記憶體(BIOS ROM)；以及

儲存該硬碟序號與該硬碟分割表後，抹除儲存於該硬碟之該硬碟分割表。

2.如申請專利範圍第1項所述之硬碟資料防護方法，其中該硬碟分割表係儲存於該硬碟之一主啟動磁區(Master Boot Record, MBR)中固定位置之該硬碟的分割資訊。

3.如申請專利範圍第1項所述之硬碟資料防護方法，其中該休眠模式(STD)係指系統關機時，將所有的動作與使用狀態暫時全部儲存在系統磁碟中，再關閉電源之模式。

4.如申請專利範圍第1項所述之硬碟資料防護方法，其中該抹除儲存於該硬碟之該硬碟分割表的步驟，係透過覆寫入一空值至該主啟動磁區(MBR)中之該硬碟分割表的儲存位置。

5.如申請專利範圍第 1 項所述之硬碟資料防護方法，其中更包含提供使用者選擇對至少一個該硬碟使用硬碟資料防護。

6.如申請專利範圍第 1 項所述之硬碟資料防護方法，其中更包含解除硬碟資料防護之步驟如下：

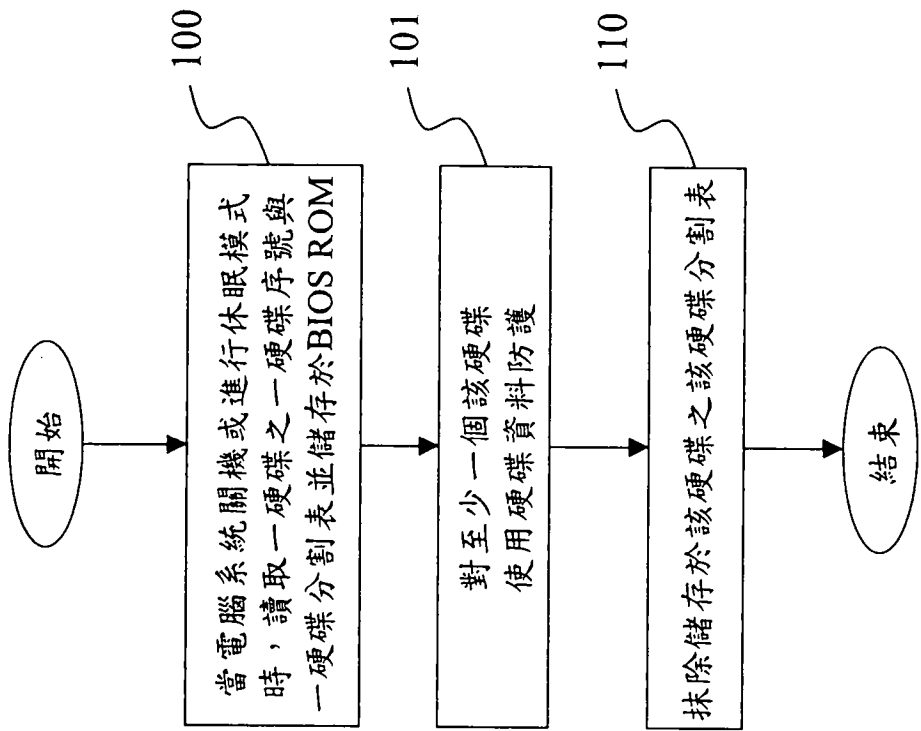
當該電腦系統開機或自該休眠模式回復時，將儲存於該基本輸入輸出系統記憶體之該硬碟分割表覆寫回符合該硬碟序號之該硬碟。

7.如申請專利範圍第 6 項所述之硬碟資料防護方法，更包含比對該基本輸入輸出系統記憶體中儲存之該硬碟序號與該電腦系統上之該硬碟是否相符之步驟。

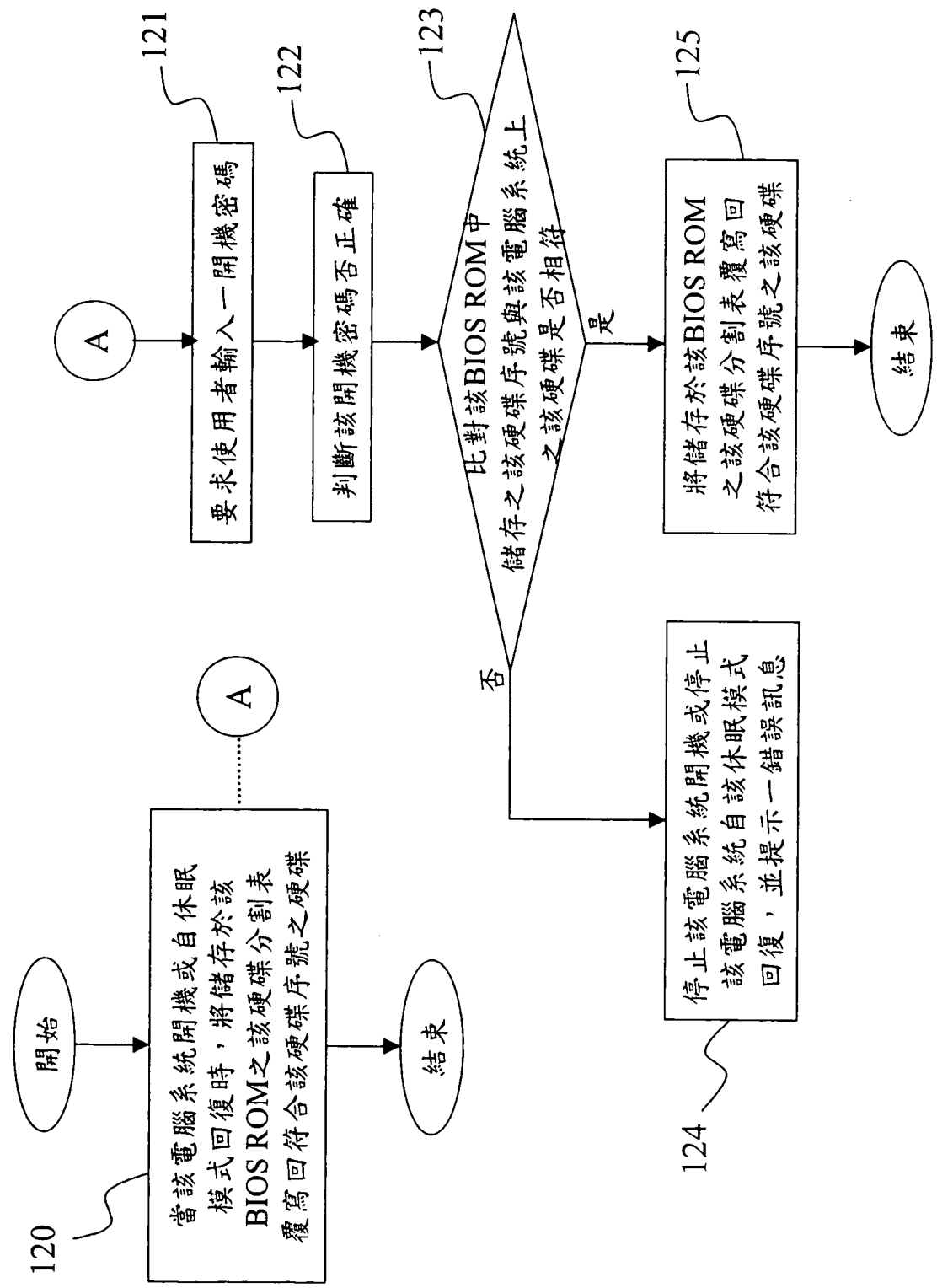
8.如申請專利範圍第 7 項所述之硬碟資料防護方法，其中比對該基本輸入輸出系統記憶體中儲存之該硬碟序號與該電腦系統上之該硬碟是否相符之步驟，包含當比對結果不符時，停止該電腦系統開機或停止該電腦系統自該休眠模式回復，並提示一錯誤訊息。

9.如申請專利範圍第 6 項所述之硬碟資料防護方法，可再包含一要求使用者輸入一開機密碼(Power-On Password)之步驟。

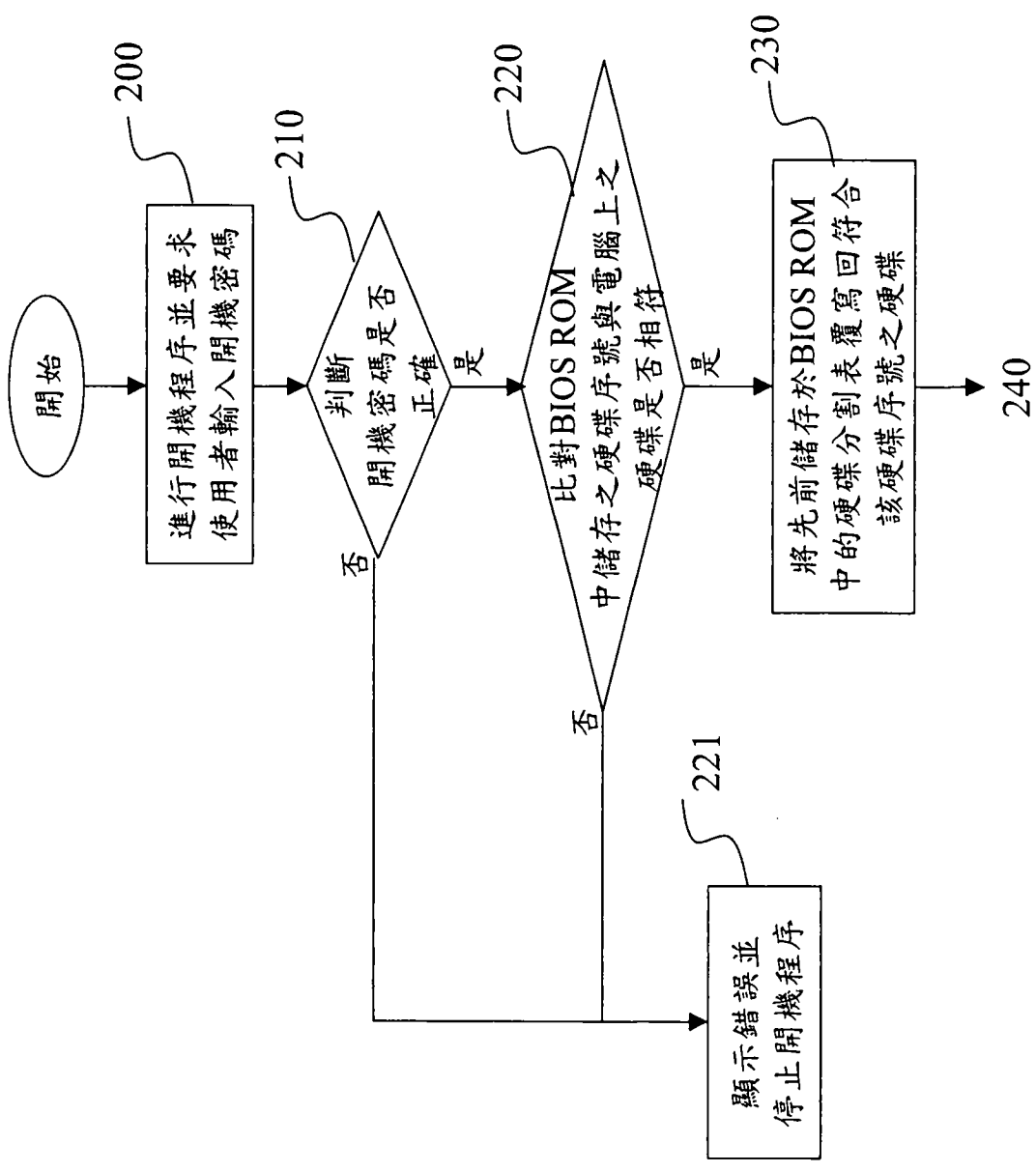
10.如申請專利範圍第9項所述之硬碟資料防護方法，再包含判斷該開機密碼正確之後，才將儲存於該基本輸入輸出系統記憶體之該硬碟分割表覆寫回符合該硬碟序號之該硬碟。



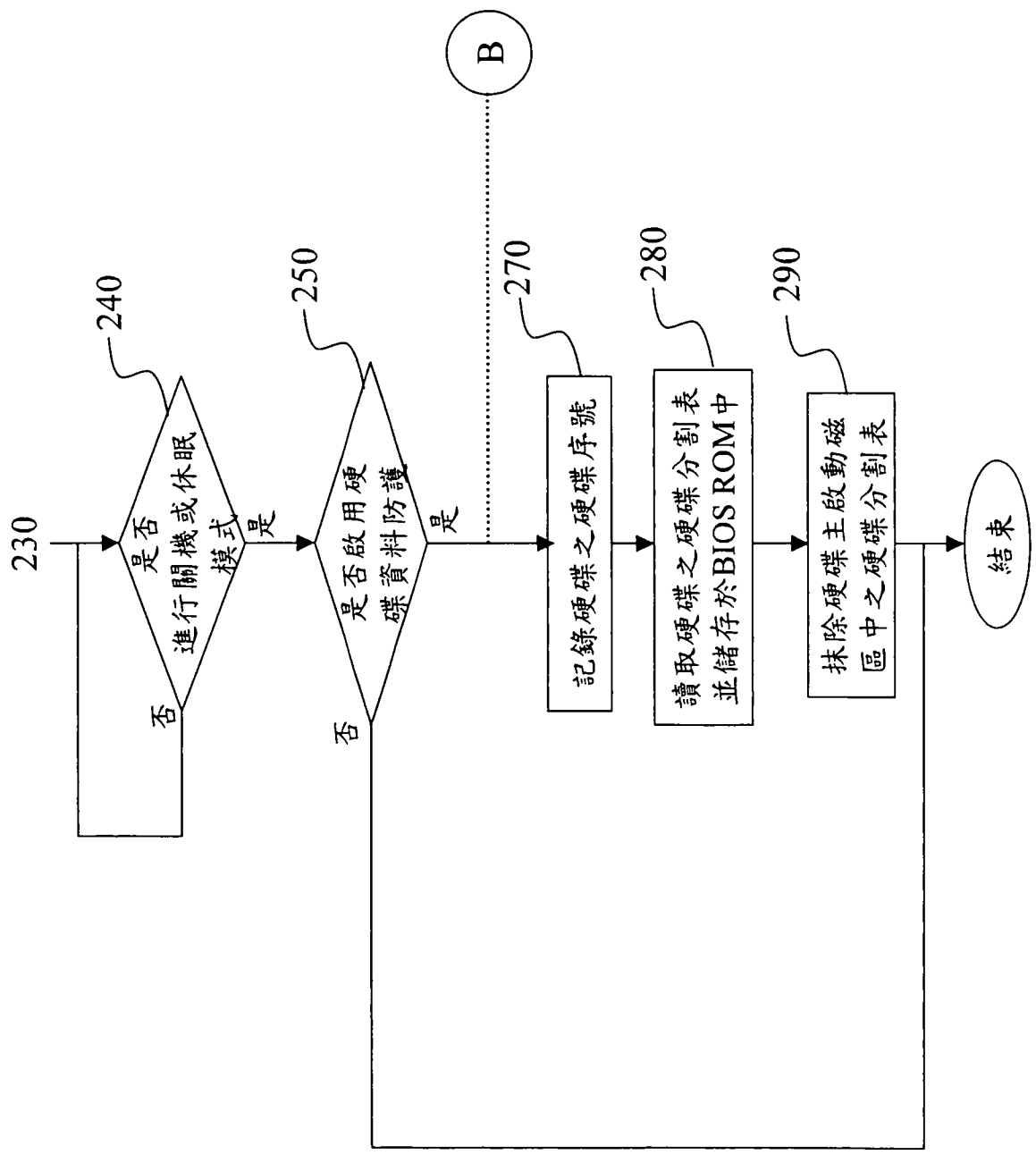
第 1 圖



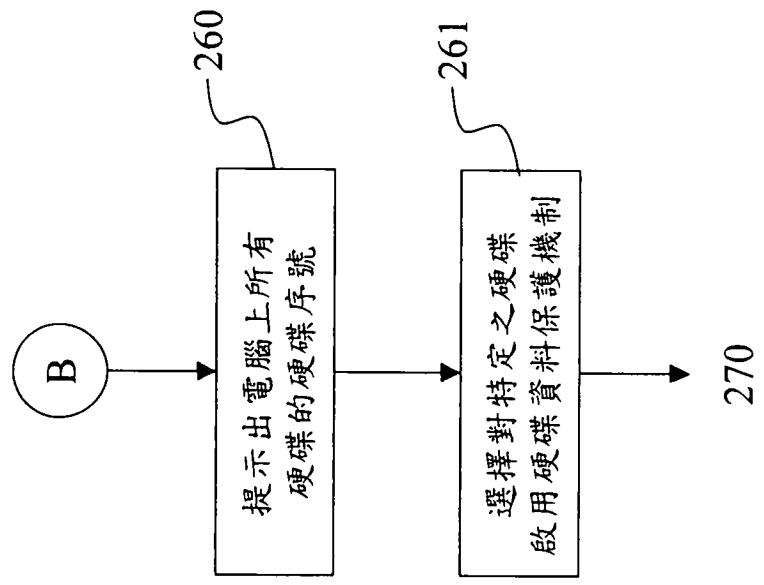
第 2 圖



第 3A 圖



第 3B 圖



第 3C 圖

七、指定代表圖：

(一)、本案指定代表圖為：第(1)圖

(二)、本案代表圖之元件符號簡單說明：

步驟 100 ~ 125 方法步驟

步驟 200 ~ 290 方法步驟

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：