(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201025001 A1
(43)公開日： 中華民國 99 (2010) 年 07 月 01 日

(21)申請案號：098139137 (22)申請日： 中華民國 98 (2009) 年 11 月 18 日
(51)Int. Cl.： *G06F12/02 (2006.01)*
(30)優先權：2008/12/18 美國 12/338,738
(71)申請人：桑迪士克股份有限公司 (美國) SANDISK CORPORATION (US)
美國
(72)發明人：席拉 羅坦 SELA, ROTEM (IL)；侯茲曼 邁可 HOLTZMAN, MICHAEL (IL)；巴利列 羅 BARZILAI, RON (IL)；布萊恩特 理奇 唐納 雷 BRYANT-RICH, DONALD RAY (US)
(74)代理人：黃章典；樓穎智
申請實體審查：無 申請專利範圍項數：35 項 圖式數：9 共 67 頁

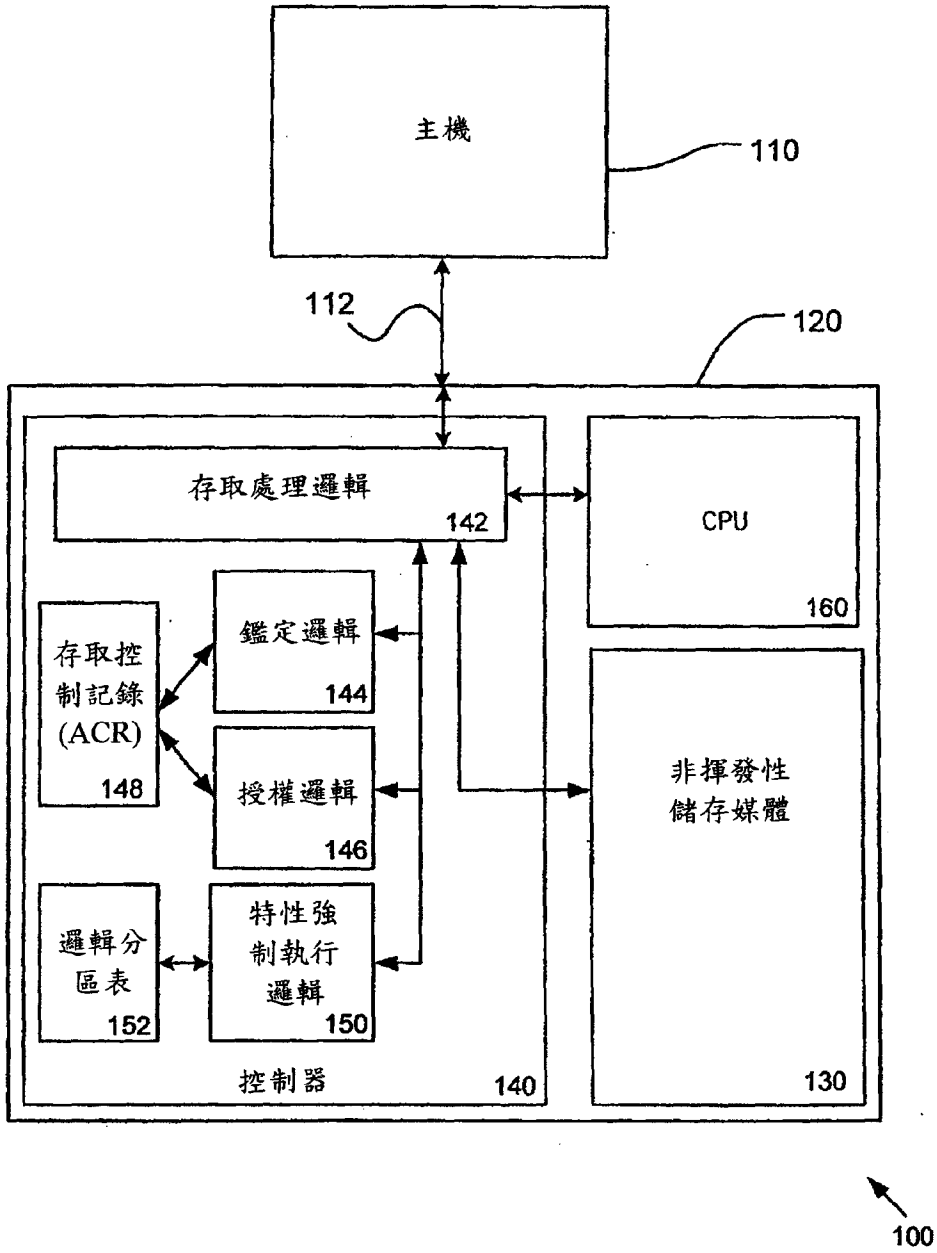
(54)名稱

管理一儲存裝置內之位址範圍之存取

MANAGING ACCESS TO AN ADDRESS RANGE IN A STORAGE DEVICE

(57)摘要

本發明揭示用於一儲存裝置中之資料之安全及存取控制之增強型組態。接收存取該儲存裝置內一儲存媒體中之一可定址記憶體位置之一請求。將具有藉由一位址範圍識別之相鄰接位址之一組可定址記憶體位置與第一及第二特性相關聯。若該可定址記憶體位置在該組可定址記憶體位置內且一實體當前經鑑定並被授權以存取該組可定址記憶體位置，則應用該第一特性。若該可定址記憶體位置在該組可定址記憶體位置內且沒有實體當前經鑑定並被授權以存取該組可定址記憶體位置，則應用該第二特性。該組可定址記憶體位置亦可係一邏輯分區，其中該第一及第二特性儲存於一邏輯分區表中。



100：系統
110：主機
112：通信介面
120：非揮發性儲存裝置
130：非揮發性儲存媒體
140：控制器
142：存取處理邏輯塊
144：鑑定邏輯塊
146：授權邏輯塊
148：存取控制記錄
150：特性強制執行邏輯塊
152：邏輯分區表
160：處理器

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201025001 A1
(43)公開日： 中華民國 99 (2010) 年 07 月 01 日

(21)申請案號：098139137 (22)申請日： 中華民國 98 (2009) 年 11 月 18 日
(51)Int. Cl.： *G06F12/02 (2006.01)*
(30)優先權：2008/12/18 美國 12/338,738
(71)申請人：桑迪士克股份有限公司 (美國) SANDISK CORPORATION (US)
美國
(72)發明人：席拉 羅坦 SELA, ROTEM (IL)；侯茲曼 邁可 HOLTZMAN, MICHAEL (IL)；巴利列 羅 BARZILAI, RON (IL)；布萊恩特 理奇 唐納 雷 BRYANT-RICH, DONALD RAY (US)
(74)代理人：黃章典；樓穎智
申請實體審查：無 申請專利範圍項數：35 項 圖式數：9 共 67 頁

(54)名稱

管理一儲存裝置內之位址範圍之存取

MANAGING ACCESS TO AN ADDRESS RANGE IN A STORAGE DEVICE

(57)摘要

本發明揭示用於一儲存裝置中之資料之安全及存取控制之增強型組態。接收存取該儲存裝置內一儲存媒體中之一可定址記憶體位置之一請求。將具有藉由一位址範圍識別之相鄰接位址之一組可定址記憶體位置與第一及第二特性相關聯。若該可定址記憶體位置在該組可定址記憶體位置內且一實體當前經鑑定並被授權以存取該組可定址記憶體位置，則應用該第一特性。若該可定址記憶體位置在該組可定址記憶體位置內且沒有實體當前經鑑定並被授權以存取該組可定址記憶體位置，則應用該第二特性。該組可定址記憶體位置亦可係一邏輯分區，其中該第一及第二特性儲存於一邏輯分區表中。

六、發明說明：

【發明所屬之技術領域】

此申請案一般而言係關於非揮發性快閃記憶體系統之運作，且更具體而言係關於管理一儲存裝置中之位址範圍之存取。

【先前技術】

現今正使用許多商業上成功的非揮發性記憶體產品，尤其以小形狀因數卡的形式，其採用形成於一個或多個積體電路裝置上之快閃EEPROM(電可擦除且可程式化唯讀記憶體)單元。某些市售卡形式包含小型快閃(CF)卡、多媒體卡(MMC)、安全數位(SD)卡及個人標籤(P-Tag)。可併入或存取非揮發性小形狀因數卡之主機包含個人電腦、筆記型電腦、個人數位助理(PDA)、各種資料通信裝置、數位相機、蜂巢式電話、可攜式音訊播放器、汽車音響系統及類似類型之設備。在某些系統中，一可抽換卡不包含一控制器且主機控制該卡中記憶體之運作。此種類型之記憶體系統之實例包含智慧媒體卡及xD卡。因此，可藉由卡中之一控制器上之軟體或藉由主機中之控制軟體來達成對記憶體之控制。除一記憶體卡實施方案外，另一選擇為，此種類型之記憶體可嵌入至各種類型之主機系統中。在可抽換及嵌入式應用程式兩者中，可根據由記憶體控制器軟體及/或硬體實施之一儲存方案來將主機資料儲存於記憶體中。經由藉由一程式(且在某些情形下，安全硬體或軟體)控制之一介面存取一卡內所儲存之資料。

非揮發性記憶體卡之儲存密度之增加允許日益增長數目個主機應用程式利用額外儲存空間。舉例而言，額外儲存器可用於MP3音訊檔案、高解析度影像檔案、視訊檔案及文件以及多種高級蜂巢式電話服務，例如儲存多媒體發訊服務(MMS)物件附加檔，並提供完整個人資訊管理(PIM)功能性，例如電子郵件聯絡人列表及日曆。因此，多種應用程式可共享非揮發性儲存裝置之存取並存取資料或儲存且管理其自己的資料。雖然每一應用程式可共享一非揮發性記憶體卡中之總體儲存空間量，但每一應用程式之頻寬、功率消耗及檔案安全要求可不同。

舉例而言，手持式計算裝置(例如蜂巢式電話)可提供內容儲存(或許在一可抽換非揮發性儲存裝置中)以藉由在一行動網路上產生更多資料交換來增加平均收益。此內容包含有價值的資料，該有價值的資料可係由除製造或出售該非揮發性儲存裝置之一方之外的一方所擁有之資料。因此，可需要保護一非揮發性儲存裝置中之內容免於由未授權之使用者或應用程式存取。另一方面，藉助一蜂巢式電話相機拍攝圖像之一應用程式可需要允許其他應用程式存取該非揮發性儲存卡中所儲存之圖像檔案。在另一實例中，應用程式(例如視訊播放器)可需要非揮發性儲存器之高頻寬、低延時存取。同時，共享非揮發性儲存器之存取之其他應用程式(例如電話通訊錄)可具有較少苛刻頻寬及延時要求。如由該等實例所示，當存取一非揮發性儲存裝置之主機應用程式之數目增加時，一非揮發性儲存裝置內

可儲存之資料的量及類型亦增加。此外，對日益複雜的應用程式之要求擴大超過所需小儲存空間量。舉例而言，若一非揮發性儲存卡不辨識或容許該等不同應用程式要求，則可危害卡上所儲存之資料之安全，或可在共享非揮發性儲存卡之存取之應用程式中誤分配頻寬。

【發明內容】

為解決該等問題，需要界定與一非揮發性儲存裝置內之非揮發性儲存器之位址範圍相關聯之特性。可應用該等特性以在處理自一所界定位址範圍讀取資料或向一所界定位址範圍寫入資料之一請求時控制功能性，例如加密、功率消耗、頻寬消耗及存取許可。可由一個或多個應用程式利用與一位址範圍相關聯之儲存空間。在這樣做時，可針對存取彼位址範圍之應用程式之要求自訂儲存裝置特性，例如安全、效能及功率消耗。所應用之該等特性可相依於一實體是否當前經鑑定並被授權以存取該位址範圍。若一個應用程式當前經鑑定並被授權以存取一位址範圍，則存取彼位址範圍之所有實體可具有在彼位址範圍之一存取期間所應用之一第一特性集。若沒有使用程式當前經鑑定並被授權以存取一位址範圍，則存取彼位址範圍之任一實體可具有在彼位址範圍之一存取期間所應用之一第二特性集。一第一或第二特性集端視一實體當前是否經鑑定並被授權以存取一位址範圍之應用提供對非揮發性儲存裝置之行為之進一步控制以及行為靈活性。本文中所提出之概念可實施於各種實施例中，且此發明內容包含多個例示性實施

例。

在一個實施例中，一儲存裝置接收存取該儲存裝置之一儲存媒體中之一可定址記憶體位置之一請求，其中該儲存媒體含有可定址記憶體位置，且其中將具有藉由一位址範圍識別之相鄰接位址之一組可定址記憶體位置與一第一特性及一第二特性相關聯。若該經定址記憶體位置在該組可定址記憶體位置內且任一實體當前經鑑定並被授權以存取該組可定址記憶體位置，則應用該第一特性。若該經定址記憶體位置在該組可定址記憶體位置內且沒有實體當前經鑑定並被授權以存取該組可定址記憶體位置，則應用該第二特性。在一個實施例中，若該經定址記憶體位置不在該組可定址記憶體位置內，則應用一預設特性。在另一實施例中，該儲存裝置向該組可定址記憶體位置鑑定該實體。使用來自一樹之一存取控制記錄來向該組可定址記憶體位置鑑定該實體。該樹含有以層級方式組織之節點，其中每一節點包含至少一個存取控制記錄，其中一存取控制記錄包含用於鑑定該實體並授權實體存取該組可定址記憶體位置中所儲存之資料之憑證及許可。一儲存裝置亦可接收由一實體改變該第一特性及該第二特性中之至少一者之一請求，且若該實體當前經鑑定並被授權這樣做，則准予該請求。

在另一實施例中，接收存取該儲存裝置內一儲存媒體中之一可定址記憶體位置之一請求，其中該儲存媒體包括可定址記憶體位置，且其中一邏輯分區包含一組可定址記憶

體位置，該組可定址記憶體位置具有藉由一位址範圍識別之相鄰接位址且與一第一特性及一第二特性相關聯。若一實體當前經鑑定並被授權以存取該邏輯分區，則自一邏輯分區表檢索該第一特性。該邏輯分區表包含複數個條目，其中每一條目包含與該邏輯分區相關聯之一邏輯分區識別符、該位址範圍、該第一特性及該第二特性。回應於該請求應用該第一特性。若該實體當前不經鑑定並被授權以存取該邏輯分區，則自對應於欲存取之該邏輯分區之該邏輯分區表條目檢索該第二特性，且回應於該請求應用該第二特性。在再一實施例中，若該經定址記憶體位置不在該邏輯分區內，則應用一預設特性。在一個實施例中，該儲存裝置向該邏輯分區鑑定該實體。在此實施例中，該儲存裝置使用來自一樹之一存取控制記錄來向該邏輯分區鑑定該實體，其中該樹含有以層級方式組織於其中之節點，每一節點包含至少一個存取控制記錄，其中該存取控制記錄包含用於鑑定該實體並授權實體存取該邏輯分區中所儲存之資料之憑證及許可。

在另一實施例中，帶有具有可定址記憶體位置之一儲存媒體之一儲存裝置自一實體接收創建一組一個或多個可定址記憶體位置與一第一特性及一第二特性之間的一關聯之一請求。藉由相鄰接位址之一位址範圍識別該組一個或多個可定址記憶體位置。若該實體當前經鑑定並被授權以創建該關聯，則該儲存裝置准予該請求。若准予創建該關聯之該請求，則可在任一實體經鑑定並被授權以存取該位址

範圍時回應於存取該位址範圍內之一可定址記憶體位置之一請求應用該第一特性。另外，可在沒有實體經鑑定並被授權以存取該位址範圍時回應於存取該位址範圍內之該可定址記憶體位置之一請求應用該第二特性。

在一個實施例中，自一實體接收改變該第一特性及該第二特性中之至少一者之一請求。若該實體當前經鑑定並被授權這樣做，則准予該請求。在另一實施例中，自一實體接收創建該邏輯分區之一請求。在該實體當前經鑑定並被授權以創建該邏輯分區，則准予該請求。該儲存裝置可使用來自一樹之一存取控制記錄鑑定該實體，其中該樹含有以層級方式組織之節點，每一節點包含至少一個存取控制記錄，其中該存取控制記錄包含用於鑑定該實體並授權該實體之憑證及許可。該儲存裝置可授權該實體，並使用一存取控制記錄創建、存取或改變該邏輯分區。

在另一實施例中，一儲存裝置包含一儲存媒體及一控制器。該儲存媒體具有可定址記憶體位置，其中藉由與一第一特性及一第二特性相關聯之相鄰接位址之一位址範圍識別該等可定址記憶體位置中之一組一個或多個可定址記憶體位址。該控制器可運作以接收存取該儲存媒體中之一可定址記憶體位置之一請求，若該可定址記憶體位置在該組可定址記憶體位置內且此時任一實體經鑑定並被授權以存取該組可定址記憶體位置，則應用該第一特性，及若該可定址記憶體位置在該組可定址記憶體位置內且此時沒有實體經鑑定並被授權以存取該組可定址記憶體位置，則應用

該第二特性。

其他實施例及其特徵及優點亦可行，且熟悉此項技術者在檢查下圖及實施方式時，該等其他實施例及其特徵及優點將或將變得明瞭。因此，如以下申請專利範圍中所陳述之所主張發明之範疇將不意欲限於本文中所示及所述之實施例。

【實施方式】

非揮發性儲存裝置可用於多種主機系統中，包含個人電腦、筆記型電腦、個人數位助理(PDA)、各種資料通信裝置、數位相機、蜂巢式電話、可攜式音訊播放器、汽車音響系統及類似類型之設備。不斷開發新的主機應用程式來利用非揮發性儲存裝置之增加之儲存容量。舉例而言，個別主機應用程式可讀取或寫入MP3音訊檔案、高解析度影像檔案、視訊檔案、文件、多媒體發訊服務(MMS)物件附加檔、電子郵件訊息、通訊錄及日曆。

一次可在一主機上執行多於一個應用程式，且因此，兩個或更多個主機應用程式可需要共享一非揮發性儲存裝置之存取。甚至在其中一次僅執行一個應用程式之系統中，需要限制一非揮發性儲存裝置上所儲存之資料之存取。在一個實例中，一應用程式可僅自非揮發性儲存裝置讀取其自己的資料。在再一實例中，兩個使用者可執行相同應用程式，但一個使用者之資料應對執行相同應用程式之另一使用者不可存取。在另一實例中，一使用者可選擇與另一使用者共享資料。類似地，一個應用程式可創建另一應用

程式可使用之資料。然而，在該等情形下，期望允許一應用程式或使用者讀取由另一應用程式或使用者所創建之資料，但禁止修改、寫入、覆寫或擦除由另一應用程式或使用者所創建之資料。

前述實例係可在多個應用程式及使用者共享一個非揮發性儲存裝置內之儲存空間時發生之多種互動之一小樣本。因此，期望提供一種具有可更好地管理一非揮發性儲存裝置內之儲存器之存取之控制特徵之記憶體系統。

在一個實施例中，使用者或應用程式可讀取、寫入、修改或擦除一非揮發性儲存裝置內之所界定位址範圍內之資料。每一位址範圍或邏輯分區可與特性集相關聯。可在接收讀取、寫入、擦除或修改具有相關聯之位址範圍之資料之一請求時應用一特性集。一特性集中之某些特性可包含功能性，例如所儲存資料之加密及解密、在執行存取時之功率消耗、在執行存取時之頻寬消耗及存取許可(例如讀取、寫入、修改及擦除許可)。可界定一個或多個位址範圍，每一位址範圍具有其自己的特性集。以此方式，一個或多個實體可在一非揮發性儲存裝置內創建自訂儲存區域。當在該等所界定位址範圍中之任一者外部接收一存取請求時，可在處理該請求中應用一預設特性集。

在一個實施例中，一位址範圍可與兩個特性集相關聯。在一實體(例如一使用者、主機或應用程式)當前經鑑定並被授權以存取該位址範圍時將一第一特性集應用於一請求，且若沒有實體經鑑定並被授權以存取該位址範圍，則

應用一第二不同特性集。在其中應用該第一特性集之情形中，請求存取該位址範圍之實體可係當前經鑑定並被授權以存取該位址範圍之實體中之一者。另一選擇為，請求存取之實體非係當前經鑑定並被授權以存取該位址範圍之實體中之一者。在此情形下，可向一位址範圍鑑定一第一實體自身並授權該第一實體存取該位址範圍。一旦完成了此過程，即可在一第二實體嘗試存取該位址範圍時應用該第一特性集，即使該第二實體可尚未完成該鑑定及授權過程。關於此方面,該第二實體依賴於由該第一實體先前所完成之鑑定，且在執行彼位址範圍之一存取時享有由該第一特性集所規定之屬性。在一個實施例中，在處理該請求時，請求存取之實體之身份對非揮發性儲存裝置不可用或不由非揮發性儲存裝置使用。在此實施方案中，確定應用哪一特性集係相依於授權存取該位址範圍之當前正鑑定之實體且獨立於請求存取該位址範圍之實體之身份。

特性集之此用途呈現數個重要的安全及效能優點。舉例而言，與一位址範圍相關聯之該第一特性集可允許彼位址範圍之讀取及寫入存取，而該第二特性集可禁止讀取及寫入存取兩者。可委託一個應用程式以憑證及所需程序來向該位址範圍鑑定其自身，並變得授權存取該位址範圍。一旦完成了該鑑定及授權過程，即將該第一特性集應用於嘗試存取彼位址範圍之其他應用程式。然而，該等其他應用程式無需委託以該等憑證及該等鑑定程序。系統之安全可得以改良，乃因需要具有該憑證及鑑定程序之知識之實體

的數目已減少。此外，其他應用程式可避免重複該鑑定程序以得以存取，此可減少存取該位址範圍中之延時。因此，在此實例中，一個應用程式可充當一閘管理者以使得其他應用程式能夠具有一位址範圍之讀取及寫入存取。只要該應用程式當前經鑑定並被授權以存取該位址範圍，其他應用程式即可存取彼位址範圍而無須執行一安全、耗時或麻煩的鑑定及授權過程。

圖1係圖解說明用於存取一非揮發性儲存裝置內之非揮發性儲存器之一例示性系統100之一圖示。系統100包含一主機110及一非揮發性儲存裝置120。主機110及非揮發性儲存裝置120可實施於硬體、軟體或硬體與軟體之一組合中。在一個實施例中，非揮發性儲存裝置120係一TrustedFlash™卡，來自加利福尼亞、米爾皮塔斯之SanDisk公司之一儲存裝置。主機110與非揮發性儲存裝置120可經由一通信介面112通信。該通信介面可係一通用串列匯流排(USB)介面、一安全數位(SD)介面或任一通信介面或協定或能夠在主機110與一非揮發性儲存裝置120之間交換命令及資料之協定之組合。舉例而言，主機110可經由通信介面112傳輸資料及一命令以將該資料儲存於非揮發性儲存裝置120中。在另一實例中，主機110可經由通信介面112傳輸一命令以自非揮發性儲存裝置120讀取資料，且非揮發性儲存裝置120可經由通信介面112將資料返回至主機110。可經由通信介面112傳輸之其他檔案操作包含打開、關閉、創建、擴大及擦除一檔案。

主機110可包括可儲存或存取非揮發性儲存裝置120中之資料之一個或多個應用程式。在另一實施例中，一個或多個使用者可使用一個或多個應用程式來儲存或存取非揮發性儲存裝置120中之資料。此外，在非揮發性儲存裝置120內之一處理器160上運行之應用程式可儲存或存取其中之資料。自非揮發性儲存裝置120之角度來看，某些或所有該等存取嘗試可表現為來自兩個或更多個單獨實體。

非揮發性儲存裝置120可包括非揮發性儲存媒體130、一控制器140及一CPU或處理器160。非揮發性儲存媒體130可儲存資料，例如經由一通信介面112自一主機110接收之資料、自處理器160接收之資料或在製造過程期間程式化或寫入至非揮發性儲存裝置120之資料。非揮發性儲存媒體130可係一快閃記憶體、電可擦除可程式唯讀記憶體(EEPROM)、唯讀記憶體(ROM)、硬碟、光碟或能夠儲存資訊並在不施加一電源時保持彼資訊之任一其他類型之記憶體。

控制器140包含一存取處理邏輯塊142、一鑑定邏輯塊144、一授權邏輯塊146、一個或多個存取控制記錄(ACR)148、一特性強制執行邏輯塊150及一邏輯分區表152。控制器140及其所有組件可實施於硬體中(例如適於實施如下所述功能性之電路)、軟體或硬體與軟體之一組合。在一個實施例中，將控制器140實施為於非揮發性儲存裝置120內之一CPU或處理器(例如處理器160)上執行之軟體或韌體。

控制器140經由通信介面112自主機110接收請求。該等所接收之請求可包含讀取、寫入、擦除或修改非揮發性儲存媒體130中之資料之請求。所接收之請求可包含一位址，或可基於一先前所接收之請求來推斷或計算該位址。在一個實施例中，該位址係一邏輯塊位址(LBA)，其可由控制器140重新映射至非揮發性儲存媒體130中之一實體儲存位置。存取處理邏輯塊142確定該請求之該位址是否在非揮發性儲存媒體130之一個或多個位址範圍或邏輯分區內。可在特性強制執行邏輯塊150的幫助下執行該確定，該特性強制執行邏輯塊可審查邏輯分區表152中之條目以確定該請求之該位址是否在該表中之邏輯分區中之任一者之位址範圍內。若不在，則自特性強制執行邏輯塊150檢索一預設特性，並將其返回至存取處理邏輯塊142。存取處理邏輯塊142接著在處理非揮發性儲存媒體130之存取請求時應用該預設特性或特性集。

若該請求之該位址在邏輯分區表152中之邏輯分區中之任一者之位址範圍內，則確定是否已鑑定任一實體，且若已鑑定，則確定是否授權該經鑑定之實體存取所請求之位址範圍或邏輯分區。在一個實施例中，存取處理邏輯塊142可自鑑定邏輯塊144檢索經鑑定之實體之一列表。該列表可指示已透過鑑定邏輯塊144成功地完成一鑑定過程(例如提供一密碼、完成一詢問-回應演算法或適於驗證設法存取非揮發性儲存器130之一實體之身份之任一其他程序)之實體。一經鑑定之實體可藉由完成一鑑定過程來「登

入」至該系統。類似地，一經鑑定之實體可藉由向鑑定邏輯144指示不再期望彼存取來「登出」該系統。因此，在另一實施例中，經鑑定之實體之該列表可包含當前正鑑定之實體，換言之，已「登入」且尚未「登出」之實體。在一個實施例中，在處理一存取請求時，可咨詢該列表以確定是否授權一「已登入」經鑑定之實體在正處理該存取請求時存取該邏輯分區。

由授權邏輯塊146審查對應於每一經鑑定之實體或當前正鑑定實體之存取控制記錄148以確定是否授權該經鑑定之實體存取對應於非揮發性儲存器130之存取請求之位址範圍或邏輯分區。若對應，則由特性強制執行邏輯塊150檢索一第一特性或特性集，並將其返回至存取處理邏輯塊142。若不對應，則由特性強制執行邏輯塊150檢索一第二特性或特性集，並將其返回至存取處理邏輯塊142。存取處理邏輯塊142接收該特性或特性集並在處理非揮發性儲存媒體130之存取請求時應用其。在一個實施例中，將該第一特性及該第二特性儲存於邏輯分區表152中。

控制器140亦可自一實體接收創建、更新及刪除邏輯分區以及其相關聯之特性或特性集之請求。存取處理邏輯塊142可在鑑定邏輯塊144及存取控制記錄148的幫助下確定是否鑑定一實體。若鑑定一實體，則由授權邏輯塊146審查對應於該經鑑定之實體之存取控制記錄148以確定是否授權該經鑑定之實體創建一新的邏輯分區或更新/刪除一現有邏輯分區。接著由存取處理邏輯塊142根據自存取控

制記錄148檢索之授權來處理該請求(包含允許或否認該請求)。

控制器140亦可自一實體接收添加、刪除或更新一個或多個存取控制記錄(ACR)148之請求。存取處理邏輯142可在鑑定邏輯塊144及存取控制記錄148的幫助下確定是否鑑定一實體。接著由存取處理邏輯塊142根據由授權邏輯146自存取控制記錄148檢索之授權來處理該請求。

透過以下描述及附圖，系統100之實施例之運作之進一步細節將變得顯而易見。

在一個實施例中，非揮發性儲存裝置120中之一安全儲存應用程式(SSA)為非揮發性儲存裝置120中所儲存之資料提供資料安全、完整性及存取控制。該資料可包含原本將明白地(不加密或存取控制)儲存於某一種大容量儲存裝置上之檔案。SSA系統位於儲存系統的頂上並向安全層添加非揮發性儲存器130中所儲存之檔案及資料。SSA可在控制器140及/或理器160內實施於硬體、軟體或硬體與軟體之一組合中。

在可利用一邏輯分區之一例示性架構之背景中可更好地理解一邏輯分區之操作。在一個實施例中，非揮發性儲存媒體130係被劃分成獨立實體分區之一NAND快閃晶片，雖然在替代實施例中亦可利用其他類型之非揮發性儲存器。該等實體分區係邏輯位址之連續緒，其中一開始及一結束位址界定其邊界。在一個實施例中，每一實體分區皆可具有一分區名稱。在此實施例中，該實體分區名稱及一邏輯

塊位址係由存取非揮發性儲存媒體130中之實體儲存位置之命令所使用之定址機制。非揮發性儲存裝置120可管理一分區名稱及一邏輯塊位址至非揮發性儲存媒體130內之一實體儲存位置之映射。使用某些SSA命令，主機110可改變一特定實體分區之存取屬性及大小。然而,所有實體分區之大小的總和保持不變。

一實體分區可係一公用實體分區或一專用實體分區。可由可存取非揮發性儲存裝置120之非揮發性儲存媒體130之任一實體偵測一公用實體分區。換言之，可在無先前鑑定之情形下存取一公用實體分區。另一方面，僅經鑑定之實體可存取且知曉專用或隱藏實體分區。即使可偵測一專用或隱藏實體分區，亦可視期望藉助硬體及/或軟體(例如控制器140)對專用或隱藏實體分區之存取施加限制，該硬體及/或軟體將此等限制與此等邊界內之位址相關聯。

實體分區可藉助其名稱及/或由其所管理之邏輯位址邊界來對SSA完全辨識。SSA系統使用專用實體分區來在實體上保護資料免受未經授權之主機應用程式。對於主機110，該等實體分區係界定其中儲存資料檔案之專屬空間之一機制。如上文所指示，該等實體分區可係：公用實體分區，其中存取儲存裝置之任何人皆可看見且知曉該分區在裝置上之存在；或專用或隱藏實體分區，其中僅選定主機應用程式可存取且知曉該等專用或隱藏實體分區在儲存裝置中之存在。可在一公用實體分區或一專用實體分區內界定一個或多個邏輯分區或位址範圍。一邏輯分區可允許

主機110在界定與非揮發性儲存裝置120之非揮發性儲存媒體130中之儲存位址之一相鄰接範圍相關聯之安全、存取及效能特性中進一步細化。

圖2係圖解說明將非揮發性儲存媒體(例如圖1中之非揮發性儲存媒體130)分區成實體及邏輯分區之例示性分區之一圖示。可將非揮發性儲存媒體130劃分成複數個實體分區202、204、206、208。在圖2中所示之實施例中，顯示N個實體分區，但任一數目個實體分區亦可行。該等實體分區可係公用實體分區或專用實體分區。

一專用實體分區(例如P1分區204、P2分區206或P(N-1)分區208)隱藏其內檔案之存取。藉由防止主機110存取該專用實體分區，非揮發性儲存裝置120保護該實體分區內部之資料檔案。然而，此類保護藉由對在實體分區內之邏輯位址處所儲存之資料之存取施加限制來涵蓋駐存於該公用實體分區中之所有檔案。換言之，該等限制係與整個專用實體分區相關聯。可存取彼專用實體分區之所有應用程式、使用者或主機將具有該專用實體分區內之所有檔案之無限制存取。經鑑定之實體可在授權存取一專用實體分區時這樣做。

與此相反，通常可由任一實體在無鑑定或授權之情形下存取一公用分區(例如P0分區202)。因此，可由標準主機讀取/寫入命令或透過專門讀取/寫入命令(該等專門讀取/寫入命令透過SSA系統對經鑑定之實體可用)存取一公用分區。使用SSA命令存取檔案允許透過加密之基於檔案之存

取控制之額外選項，如上所述。具體而言，可利用SSA命令來加密並並向公用分區寫入檔案，且讀取及解密公用分區中所儲存之檔案。

為使一實體分區內之不同檔案或檔案群組彼此隔離，使用加密密鑰及密鑰參考或密鑰ID提供檔案級安全。用於加密不同記憶體位址處之資料之一特定密鑰值之一密鑰參考或密鑰ID可類推至含有經加密之資料或檔案之專用實體分區內之一容器或域。即使一應用程式、一使用者或一主機可存取含有以一密鑰加密之一檔案之一專用實體分區，亦可不解密該檔案，除非該應用程式、使用者或主機可存取彼密鑰。在不存取該密鑰之情形下，該應用程式、使用者或主機可覆寫或破壞經加密之檔案，但可不解密該等經加密之檔案。因此，可利用複數個密鑰來加密一專用實體分區內之複數個對應檔案，因此保護檔案資料免於可存取該專用實體分區但不可存取所需解密密鑰之一應用程式、一使用者或一主機。

在一公用實體分區或專用實體分區內界定之邏輯分區亦可使一實體分區內之不同檔案或檔案群組彼此隔離或區分開。在一個實施例中，可創建一邏輯分區212以進一步為非揮發性儲存器130之一公用分區202內之邏輯分區內所儲存之資料提供資料安全、完整性及存取控制。具體而言，當在於公用分區202內界定一邏輯分區212之位址之一範圍內請求一存取時，控制器130可在處理該存取時應用一第一特性集或一第二特性集，其中該第一及第二特性集可不

同於預設特性集。可在非揮發性儲存媒體130內界定複數個邏輯分區212、214、216。可在一單個實體分區206內界定兩個或更多個邏輯分區214、216。此外，可在一專用實體分區206(例如專用實體分區216)內界定一邏輯分區216。可將關於在非揮發性儲存裝置120中所界定之邏輯分區之資訊儲存於邏輯分區表152中。

當一實體請求存取不在所界定邏輯分區212、214、216中之一者內之公用分區202或專用分區204、206及208之區域時，控制器140可回應於該存取請求應用一組預設特性。可應用該等預設特性來控制功能性，例如加密、功率消耗、頻寬消耗及存取許可。

因此，一例示性非揮發性儲存裝置120可使用本文中所揭示之保護方案中之任一組合來控制非揮發性儲存媒體130中所儲存之資料之存取。主機110可藉由將檔案儲存於僅可對經鑑定之實體存取之一專用實體分區中來選擇利用實體保護。主機110可將一檔案儲存於在一實體分區內所界定之一邏輯分區內，其中在存取該邏輯分區內所儲存之檔案時應用加密、功率消耗、頻寬消耗及存取許可。可藉由以僅可對一個或多個經鑑定之實體存取之一密鑰加密非揮發性儲存媒體130內任一處所儲存之一個別檔案來有效地禁止該檔案之存取。可使用該等保護方案之任一組合來管理非揮發性儲存裝置120中所儲存之資料之存取。下文將進一步詳細討論每一內容保護方案之細節。

如上所述，可將關於在非揮發性儲存裝置120中所界定

之邏輯分區之資訊儲存於邏輯分區表152中。圖3係圖解說明一例示性邏輯分區表152、其中之條目及在非揮發性儲存裝置120之存取期間所應用之各種特性之編碼之一圖示。在一個實施例中，邏輯分區表152包括M個條目，其中M等於邏輯分區之數目。在另一實施例中，該邏輯分區表亦含有一額外條目來儲存應用於該等所界定邏輯分區中之任一者外部之位址之存取請求之一預設特性集。

邏輯分區表152中之每一條目對應於非揮發性儲存媒體130內之一邏輯分區，如圖2中所圖解說明。舉例而言，圖2中之邏輯分區216在邏輯分區表152中具有一對應邏輯分區表條目302。邏輯分區表152中之一條目(例如邏輯分區表條目302)含有資訊，例如邏輯分區名稱或識別符、其中界定邏輯分區之源實體分區之一識別符、及邏輯分區之開始及結束邏輯塊位址(LBA)。另外，邏輯分區表條目302含有兩組特性312及314。在圖3中所示之實例中，兩組特性312及314中之每一者可規定存取屬性特性、密碼編譯屬性特性、效能屬性特性及功率存取屬性特性。可自該表檢索第一特性集312並在一實體當前經鑑定並被授權以存取邏輯分區216時將該第一特徵集用於處理邏輯分區216內之一存取請求。可自該表檢索第二特性集312並在沒有實體當前經鑑定並被授權以任一實體存取邏輯分區216時將該第二特徵集用於處理邏輯分區216內之一存取請求。

在存取屬性特性、密碼編譯屬性特性、效能屬性特性及功率消耗特性之寬廣類別內，許多特性設定可行。舉例而

言，如表320中所示，存取屬性特性可包含抑制寫入存取、抑制讀取存取或抑制擦除邏輯分區內之資料。在另一實施例中，存取屬性特性可抑制或允許使用標準主機讀取/寫入/擦除命令來存取一邏輯分區，例如公用實體分區202中之邏輯分區212。如例示性表330中所示，密碼編譯屬性特性值可需要在向一邏輯分區寫入資料或自一邏輯分區讀取資料時利用選定加密演算法。

表340展示例示性效能屬性值。在一個實施例中，選擇高效能、正常效能或低效能可允許應用該特性之控制器140優先考量較高效能請求、中斷其他非揮發性儲存器存取或採取其他動作來改良一存取請求之延時或資料頻寬。類似地，當控制器140應用一低效能特性時，控制器140可允許其他過程或存取優先於該所請求之存取。其他效能編碼方案亦可行。在一個實施例中，該效能屬性特性值可指示控制器140在處理一特定邏輯分區之請求時所應用之一資料頻寬量或延時量特性。

如表350中所示，例示性功率消耗特性可規定一高功率消耗值、正常功率消耗值或低功率消耗值。在一個實施例中，控制器140可藉由停用或減慢非揮發性儲存裝置120內之至少某些時鐘樹來應用一低功率特性以便在處理一特定邏輯分區之請求時減少功率消耗。其他功率消耗特性可編碼於邏輯分區表條目302中並由控制器140應用。

本文中所述之特性類別及編碼係例示性且並不意欲具有限制性。可控制、限制或對許可、加密、效能、功率消耗

或與存取一非揮發性儲存器有關之任一其他屬性施加要求或限制之任一特性可編碼於一特性中並由控制器140回應於一存取請求應用。

藉由具有與一邏輯分區相關聯之一第一特性集312及一第二特性集314，可針對該邏輯分區創建數個有用資料安全、完整性及存取控制組態。舉例而言，該第一特性集內之一存取屬性特性可允許讀取及寫入存取，而該第二特性集內之另一存取屬性特性可允許讀取存取而不允許寫入存取。因此，在一實體當前經鑑定並被授權以存取一邏輯分區時，可允許該邏輯分區之讀取及寫入存取。在沒有實體當前經鑑定並被授權以存取一邏輯分區時，可讀取但不寫入該邏輯分區。在另一實例中，在一實體當前經鑑定並被授權以存取該邏輯分區時，可應用一高效能存取特性來請求存取一分區。在一實體當前經鑑定並被授權以存取該邏輯分區時，可應用一低效能存取特性。資料安全、完整性及存取控制組態之許多其他有用組合亦可行。

如上所述，為確定是否回應於一邏輯分區之一存取請求應用來自第一特性集312或第二特性集314之一特性，控制器140確定是否授權一當前正鑑定之實體存取該邏輯分區。創建、更新或刪除一邏輯分區必須透過一存取控制記錄(ACR)登入至SSA系統從而允許在存取該邏輯分區時應用一第一特性集。需要創建密鑰及實體分區以及自其寫入及讀取資料或使用該等密鑰之能力之一實體亦需要透過一ACR登入至SSA系統。

SSA系統中一ACR之特權稱為動作。每一ACR可具有執行以下類別之動作之授權：創建邏輯分區、實體分區及密鑰/密鑰ID、存取實體分區及密鑰、在存取一邏輯分區時啟用一第一特性集之應用、並創建/更新其他ACR。按群組組織ACR稱為ACR群組或AGP。一旦已成功鑑定了一ACR，SSA系統即打開一會話，一ACR之動作中之任一者可透過該會話執行。

圖4係圖解說明一存取控制群組(AGP)內之例示性存取控制記錄(ACR)(包含鑑定及授權資訊)之一圖示。ACR係至SSA系統之一個別「登入」點。ACR保持「登入」或鑑定憑證及鑑定方法。許可控制記錄(PCR)(SSA系統內之許可或授權)亦駐存於ACR中，在其中讀取及寫入特權。此圖解說明於圖4中，該圖圖解說明相同AGP中之N個ACR。由於該等ACR在相同AGP內，因此該N個ACR中之至少某些可共享相同密鑰之存取。因此，ACR #1及ACR # N共享具有密鑰ID「密鑰3」之一密鑰之存取，其中ACR #1及ACR #N係ACR ID，且「密鑰3」係用於加密與「密鑰3」相關聯之資料之密鑰之一密鑰ID。亦可使用相同密鑰來加密及/或解密多個檔案或多組資料。

為登入至一ACR或變得向一ACR鑑定，一實體需要規定ACR ID，以便SSA將建立正確的「登入」或鑑定演算法，並在已滿足所有「登入」或鑑定要求時選擇正確的PCR。當創建ACR時，將ACR ID提供給SSA系統。SSA系統支援登入到系統上之數種「登入」類型，其中一旦實體成功登

入或經鑑定，演算法及實體憑證即可隨著該實體在系統中之特權或授權而變化。圖4再次圖解說明不同「登入」演算法及憑證。ACR #1需要一密碼「登入」演算法及作為憑證之密碼，而ACR #2需要一PKI (公用密鑰基礎架構)「登入」演算法及作為憑證之公用密鑰。因此，為登入或被鑑定，一實體將需要提出一有效ACR ID及憑證，以及完成正確的鑑定或登入演算法。鑑定演算法規定該實體將使用哪類「登入」程序，及提供使用者之身份的證明需要哪種憑證。SSA系統支援數個標準「登入」演算法，其範圍自無程序(及無憑證)及基於密碼之程序至基於對稱或非對稱加密術之一雙向鑑定協定。

實體之憑證對應於「登入」演算法，且由SSA用於驗證及鑑定該實體。憑證之一實例可係用於密碼鑑定之一密碼/PIN-數、用於AES鑑定之AES-密鑰等。憑證之類型/格式(亦即，PIN、對稱密鑰等)係由鑑定模式預界定且自該鑑定模式導出；其在創建ACR時提供至SSA系統。在此實施例中，SSA系統不參與界定、分配及管理此等憑證，其中儲存裝置120可用於產生可匯出用於憑證產生之RSA密鑰對及公用密鑰之基於PKI之鑑定除外。

一ACR可具有一封鎖計數器，該封鎖計數器在實體關於系統之ACR鑑定過程不成功時遞增。當達到某一最大數目個不成功鑑定時，可由SSA系統封鎖該ACR，且無對彼ACR將成功之進一步鑑定嘗試。

一旦一實體登入至SSA系統之一ACR中，即在與該ACR

相關聯之許可控制記錄(PCR)中界定其許可(其使用SSA命令之權利)。換言之，PCR指示授權一經成功鑑定實體使用之SSA命令及密鑰、及授權一實體存取及創建之實體及邏輯分區，以及允許一實體採取之ACR及AGP管理動作。

PCR之此分區列表部分含有在成功地完成ACR階段後授權實體存取之分區之列表(使用其提供給SSA系統之ID)。因此，圖4中之ACR #1可存取實體分區#2且不可存取實體分區#1。如圖4中所示，授權向ACR #2鑑定之一實體存取邏輯分區#0，且授權向ACR #N鑑定之一實體存取邏輯分區#X。雖然一ACR之PCR可證實(例如)授權向ACR #N鑑定之一實體存取邏輯分區#X，可利用與邏輯分區集相關聯之特性集來確定所許可之特定存取類型。參考回圖3，對應於邏輯分區#X之一邏輯分區表條目可含有存取屬性作為第一特性集312及第二特性集314之一部分。

舉例而言，假定該第一特性集中針對邏輯分區#X之存取屬性為0x4，且因此許可該邏輯分區中之讀取/寫入/擦除存取。另外，假定該第二特性集中針對邏輯分區#X之存取屬性為0x1，此意味著允許該邏輯分區中之唯讀存取。當接收寫入至邏輯分區#X內之一可定址記憶體位置之一請求時，控制器140可確定是否向ACR #N(及具有授權存取邏輯分區#X之一PCR之任一其他ACR)鑑定一實體。在一個實施例中，當確定在處理該存取請求時應用哪一邏輯分區特性集時，該存取請求者之身份係已知但不由控制器140使用。在另一實施例中，該請求者之身份不對控制器140

已知。在任一情形下，確定在處理該請求時應用哪一邏輯分區特性集不需要該請求者之身份。簡要參考圖3，ACR #N之PCR授權存取邏輯分區#X。因此，若在處理該請求時向ACR #N鑑定任一實體，則將在處理該請求時應用來自與與邏輯分區#X相關聯之第一特性集之特性，且將准予該寫入請求。若在由控制器140處理該請求時不向ACR #N(或具有授權存取邏輯分區#X之一PCR之任一其他ACR)鑑定任一實體，則將應用與邏輯分區#X集相關聯之第二特性集，且將否認該寫入請求。

PCR之密鑰ID部分含有與當實體之「登入」過程已滿足ACR策略時實體可存取之密鑰ID之列表(由主機110提供給SSA系統)相關聯之資料。所規定之密鑰ID係與駐存於出現於PCR中之分區中之一個或多個檔案相關聯。由於該等密鑰ID不與該儲存裝置中之邏輯位址相關聯，因此當多於一個分區與一特定ACR相關聯時，檔案可在該等分區中之任一者中。PCR中所規定之密鑰ID可各自具有一組不同存取權利。可將對密鑰ID所指向資料之存取限制為唯寫或唯讀，或可將其規定為全寫入/讀取存取權利。

ACR之ACR屬性管理部分(ACAM)描述授權向彼ACR鑑定之一實體執行之管理動作。SSA系統中可許可之動作包含創建、刪除或更新AGP及ACR，創建或刪除邏輯分區、實體分區或密鑰，及將存取權利委派給密鑰及分區。將較佳地向一ACR鑑定一實體以改變由彼ACR所界定之該等ACAM許可。較佳地，刪除ACR及藉助已改變之ACAM許

可重新創建ACR簡單地改變一現有ACR之ACAM許可。較佳地，可不取消對由ACR所創建之一密鑰ID之存取許可。一ACR可具有創建其他ACR及AGP之能力。創建ACR亦可意味著將由其創建者所擁有之某些或所有ACAM許可委派給該等ACR。在此實施例中，具有創建ACR之許意味著具有執行如下動作之許可：

1. 界定及編輯所創建ACR之(子代之)憑證 - 較佳地，該鑑定方法一旦藉由創建ACR設定即不可編輯。可在已為子代界定之鑑定演算法之邊界內該等更改憑證。

2. 刪除一ACR。

3. 將創建許可委派給子代ACR(因此具有孫代)。

父代ACR較佳係具有刪除其子代ACR之許可之唯一ACR。當一ACR刪除其所創建之一較低級ACR時，則亦自動刪除由此較低級ACR所繁衍之所有ACR。當刪除一ACR時，刪除其所創建之所有密鑰ID及分區。存在一ACR可藉以更新其自己的記錄之兩個例外。首先，當創建者ACR為一ACR建立一密碼或PIN時，僅該ACR自身可更新其自己的密碼或PIN。其次，一根ACR可刪除其自身及其駐存於其中之AGP。

如上所述，一ACR可具有一封鎖計數器，該封鎖計數器在實體關於系統之ACR鑑定過程不成功時遞增。當達到某一最大數目個不成功鑑定時，將由SSA系統封鎖該ACR。亦可界定一解封許可以允許解封已封閉之一ACR。具有創建其他ACR之許可之一ACR具有將解封許可委派給其所創

建之ACR之許可(雖然其較佳不具有解封ACR之許可)。父代ACR將對該父代ACR之解封者之參考置於子代ACR中。被封鎖ACR可由由該被封鎖ACR所參考之另一ACR解封。對解封ACR之參考係由其創建者設定。較佳地，解封ACR位於與被封鎖ACR之創建者相同的AGP中，且具有「解封」許可。系統中之任一其他ACR皆不可解封該被封鎖ACR。一ACR可組態有一封鎖計數器但無一解封者ACR。在此情形下，若此ACR得以封鎖，則不可將其解封。

較佳地，創建密鑰之許可包含委派使用該等密鑰之存取許可之許可。密鑰之許可被劃分成三個類別：

1.存取 - 此界定密鑰之存取許可，例如許可分別使用密鑰來解密或加密資料之讀取或寫入操作。

2.所有權 - 依據定義，創建一密鑰之一ACR是其所有者。此所有權可自一個ACR委派給另一ACR(假定其在在相同AGP中或在一子代AGP中)。一密鑰之所有權提供將其刪除以及將許可委派給其之許可。

3.存取權利/委派 - 此許可使得ACR能夠委派由該ACR所持有之權利。

一ACR可將存取許可委派給由彼ACR所創建之邏輯或實體分區，以及該ACR具有存取許可之邏輯或實體分區。該許可委派係藉由向所指定ACR之PCR添加邏輯分區之名稱、邏輯分區及密鑰ID來進行。委派密鑰存取許可可藉由密鑰ID或藉由聲明存取許可係用於委派ACR之所有所創建密鑰實施。

因此，審查圖4中ACR之PCR部分，ACR #1向與「密鑰3」相關聯之實體分區#2中之資料准予唯讀許可，其中可利用「密鑰3」來解密自非揮發性儲存器130讀取之資料，且ACR #2准予讀取及寫入與「密鑰5」相關聯之實體分區#1中之資料之許可，且可利用「密鑰5」來根據所示PCR加密或解密資料。如上所述，在將一檔案寫入至某一隱藏分區(例如圖2之P1、P2或P(N-1)分區204、206及208)時，使其不被一般公用且僅可透過SSA命令由一經鑑定並被授權之實體存取。但，一旦一實體(敵方或非敵方)瞭解並存取此分區，該檔案即變得可用並清晰可見。為進一步確保檔案安全，SSA可在隱藏分區中加密其，其中用於存取用於解密檔案之密鑰之憑證較佳地不同於用於存取分區之彼等憑證。因檔案並非SSA所知曉之某物(因為檔案由主機完全控制及管理)之事實，將一內容加密密鑰(CEK)與一檔案相關聯係一問題。將檔案鏈接至SSA認可之某物- 密鑰ID，糾正此問題。

因此，當SSA創建一密鑰時，主機將此密鑰之密鑰ID與使用由SSA所創建之密鑰加密之資料相關聯。密鑰值及密鑰ID提供邏輯安全。與一既定密鑰ID相關聯(不管其位置)之所有資料皆係藉助相同CEK(其參考名稱或密鑰ID係在創建時由主機應用程式唯一提供)加密。一旦一實體獲得一隱藏分區之存取(藉由透過一ACR鑑定)並希望讀取或寫入此分區內之一經加密檔案，其即需要存取與該檔案相關聯之密鑰ID。當准予存取此密鑰ID之密鑰時，SSA載入與

此密鑰ID相關聯之CEK中之密鑰值且在將資料發送至主機110之前解密資料或在將資料寫入至非揮發性儲存器130之前加密資料。與一密鑰ID相關聯之CEK中之一密鑰值一旦由SSA系統隨機創建即由其來維持。在SSA系統外部沒有任一實體知曉或可存取CEK中之此密鑰值。外部世界僅提供及使用一參考或密鑰ID，而非CEK中之密鑰值。該密鑰值係由SSA完全管理，且僅可由SSA存取。

在另一實例中，在圖4中，授權向ACR #2鑑定之一實體存取邏輯分區#0，且授權向ACR #N鑑定之一實體存取邏輯分區#X。因此，若當前正向ACR #2鑑定一實體，則在接收邏輯分區#0之一存取請求時，在處理一存取請求時應用一第一特性集312。在另一實例中，若當前正向ACR #N鑑定一實體，則在接收邏輯分區#X之一存取請求時，在處理一存取請求時應用一第一特性集312。

不同ACR可在系統中共享共同興趣及特權，例如藉助其進行讀取及寫入之密鑰，及授權存取之邏輯分區。為達成此，將具有某些共同處之ACR按AGP或ACR群組分組。因此，ACR #1及ACR #N共享具有密鑰ID「密鑰3」之一密鑰之存取。雖然未顯示於圖4中，但一AGP內之ACR亦可共享一邏輯分區之存取。

可進一步按以層級方式樹集合ACR及其AGP。圖5係圖解說明配置成一樹狀階層結構之存取控制記錄及存取控制群組之一例示性配置之一圖示。根AGP及其內之ACR係在樹的頂部(例如，圖5中之根AGP 530)。在SSA系統中可存

在數個AGP樹，雖然該等樹完全彼此分離。一AGP內之一ACR可將其密鑰之存取許可委派給其所在之相同AGP內之所有ACR，且委派給由彼ACR所創建之所有ACR。

因此，除含有向密鑰、邏輯分區、實體分區及管理命令界定授權之資訊外，一ACR亦可較佳地創建其他(子代)ACR條目。該等ACR子代將具有與其父代/創建者相同或較少的許可，且可給予對父代ACR所創建之密鑰及分區之許可。該等子代ACR得到其所創建之任一密鑰之存取許可。此圖解說明於圖5中。因此，AGP 520之所有ACR係由ACR 522創建，且此等ACR中之兩者自ACR 522繼承存取與「密鑰3」相關聯之資料之許可。

藉由規定一AGP及該AGP內之一ACR來進行至SSA系統上之登入。每一AGP具有一唯一ID(參考名稱)，該唯一ID用作對每一AGP在SSA資料庫中之條目之一索引。當創建AGP時，將AGP名稱提供給SSA系統。若在系統中已存在所提供之AGP名稱，則SSA將拒絕創建操作。

AGP用於對委派存取及管理許可施予限制。雖然在圖5中僅顯示一個樹，但在SSA系統中可存在多於一個樹。由圖5中之樹所提供之一個功能係施予由一實體(此一主機應用程式或使用者)之存取。可為每一實體界定一單獨樹。出於此等目的，重要的是每一樹中ACR之存取過程大致彼此獨立(亦即，大致無串擾)，即使兩者同時出現。此意謂著每一樹中與另一樹中之額外ACR及AGP之鑑定、許可以及創建沒有聯繫且彼此不相依。因此，當在非揮發性儲存

裝置120中使用SSA系統時，兩個應用程式同時存取兩組單獨資料，且彼此獨立。

AGP系統之樹結構係用於識別及隔離應用程式特有資料之主要工具。根AGP在一應用程式SSA資料庫樹的頂端，且遵守稍微有些不同的行為規則。可在SSA系統中組態數個根AGP。主機110中之一新的主機應用程式或實體可在非揮發性儲存裝置120內透過向該裝置添加一新的AGP/ACR樹之過程界定其自己的安全資料空間或安全組態。

在此實施例中，SSA系統支援三種不同模式之根AGP創建(以及根AGP之所有ACR及其許可)：

1.開放 - 不需要任一類鑑定之任一實體(例如一使用者或應用程式)或透過系統ACR鑑定之實體(將在下文予以解釋)可創建一新的根AGP。該開放模式在無任何安全措施同時所有資料傳送係在一開放通道上進行(亦即，在一發佈機構之安全環境中)之情形下，或透過一透過系統ACR鑑定建立之安全通道(亦即，在空中(OTA)及後發佈程序)達成根AGP之創建。若未組態可選系統ACR並將根AGP創建模式設定為開放，則僅開放通道選項可用。

2.受控 - 僅透過系統ACR鑑定之實體可創建一新的根AGP。若未組態系統ACR，則不可將SSA系統設定為此模式。

3.鎖定 - 停用根AGP之創建，且不可向該系統添加額外根AGP。

兩個SSA命令控制此特徵(該等命令對未經鑑定之任一使用者/實體可用)：

1.方法組態命令 - 用於組態SSA系統以使用三種根AGP創建模式中之任一者。僅允許以下模式改變： a)開放至受控之一改變， b)受控至鎖定之一改變(亦即，若SSA系統當前正組態為受控，則其可僅改變為鎖定)。

2.方法組態鎖定命令 - 用於停用方法組態命令並永久地鎖定當前選定方法。

當創建一根AGP時，其處於達成其ACR之創建及組態(使用與應用於根AGP之創建相同的存取限制)之一特殊初始化模式。在該根AGP組態過程結束時，當實體明確地將其切換至運作模式時，可不再更新現有ACR且不再創建額外ACR。

一旦將一根AGP置於標準模式中，即可藉由透過其ACR中指派有刪除該根AGP之許可之一者登入至系統中來將其刪除。此係除特殊初始化模式之外之根AGP之另一例外；較佳地，與下一樹層級中之AGP相反，其係可含有具有刪除其自己的AGP之許可之一ACR之唯一AGP。在其他情形下，創建AGP之ACR具有僅在AGP無ACR條目時才可刪除其之許可。一根ACR與一標準ACR之間的另一差別係在於其係該系統中可具有創建及刪除實體分區之許可之唯一ACR。

控制器140亦可利用一專門ACR(稱為系統ACR)來執行以下兩個SSA操作：

1.在一安全通道之保護下於敵方環境內創建一ACR/AGP樹。

2.識別及鑑定託管SSA系統之裝置。

在SSA中較佳僅存在一個系統ACR，且較佳一旦被界定即不可改變。在創建該系統ACR時無需系統鑑定；僅需要一SSA命令。可停用「創建系統ACR」特徵(類似於創建根AGP特徵)。在創建系統ACR之後，「創建系統ACR」命令失效，乃因較佳地僅允許一個系統ACR。

當在創建過程中時，系統ACR不運作。在完成之後，較佳地，需要發佈指示系統ACR已創建且且已準備被使用之一特殊命令。在發佈此命令之後，較佳地不可更新或替換該系統ACR。

系統ACR在SSA中創建根ACR/AGP。其具有添加/改變根層級ACR/AGP之許可，直至主機對其滿意並將其封鎖之時間。透過一SSA命令封鎖根AGP實質上切斷其至系統ACR之連接並使其防竄改。不可改變或編輯根AGP及其內之ACR。停用根AGP之創建具有一永久效應且不可逆。使用系統ACR來創建不同根AGP，例如圖5中之根AGP 530。在創建了該等根AGP之後之某一時間，可自主機發送另一SSA命令來封鎖自系統ACR創建根AGP，藉此停用「創建根AGP」特徵。在這樣做時，使已創建之根AGP防竄改。在封鎖該等根AGP之前或之後，可使用該等根AGP來創建子代AGP。

上述特徵向內容所有者提供在組態具有內容之安全產品

方面之更大靈活性。需要「發佈」安全產品。發佈係放置非揮發性儲存裝置120可藉以識別主機110且反之亦然之識別密鑰之過程。識別非揮發性儲存裝置120使得主機110能夠決定其是否可將其秘密託付給非揮發性儲存裝置120。另一方面，識別主機110使得裝置120能夠僅在允許主機110強制執行安全策略(准予及執行一特定主機命令)時才執行安全策略。

設計用於服務多個應用程式之產品將具有數個識別密鑰。若係在裝運之前於製造期間所儲存之密鑰，則可「預發佈」產品，或若係在裝運之後所添加之新密鑰，則可「後發佈」產品。對於後發佈，記憶體裝置(例如，記憶體卡)需要含有某種主密鑰或裝置級密鑰，該等密鑰用於識別允許向該裝置添加應用程式之實體。

上述特徵使得能夠組態一產品從而啟用/停用後發佈。另外，可在裝運之後安全地進行該後發佈組態。該裝置可作為一零售產品購買，該零售產品不具有除上述主裝置或裝置級密鑰之外的密鑰，且接著可由新的所有者組態以進一步啟用或停用後發佈應用程式。

因此，系統ACR特徵提供達成以上目標之能力。不具有系統ACR之記憶體裝置將允許應用程式之不受限且不受控添加。不具有一系統ACR之記憶體裝置可經組態以停用系統ACR創建，此意味著無法控制新的應用程式之添加(除非亦停用創建新的根AGP之特徵)具有一系統ACR之記憶體裝置將僅允許應用程式經由透過使用系統ACR憑證之一鑑

定程序建立一安全通道之受控添加。具有一系統ACR之記憶體裝置可經組態以在添加應用程式之前或之後停用應用程式添加特徵。

可利用該SSA系統來處理存取、創建、修改及刪除經組態位址範圍或邏輯分區之請求。圖6顯示用於處理一非揮發性儲存裝置內之非揮發性儲存器之一存取嘗試之例示性步驟600。簡要參考圖1，接收存取非揮發性儲存裝置120之非揮發性儲存媒體130之一請求。可經由通信介面112自主機110接收該請求。返回至圖6，在步驟602，控制器140之存取處理邏輯塊142確定所接收之請求是否係存取(例如讀取、寫入或擦除)在非揮發性儲存媒體130內所界定之一邏輯分區中之資料。存取處理邏輯塊142咨詢特性強制執行邏輯塊150，且若邏輯分區表152係適當，則確定與該存取請求相關聯之位址是否處於邏輯分區表152中所界定之一邏輯分區或位址範圍內。若不在，則控制轉到步驟610，且存取處理邏輯塊142藉助控制器140檢索邏輯分區表152中或別處所儲存之一預設特性集，並在處理該存取請求時應用該預設特性或特性集。

若與該存取請求相關聯之位址在於邏輯分區表152中所界定之一邏輯分區或位址範圍內，則所接收之請求係藉助一邏輯分區或位址範圍之一存取。控制接著自步驟602轉到步驟604。在步驟604，控制器140確定是否授權一當前正鑑定之實體存取經組態之LBA範圍。存取處理邏輯塊142可咨詢鑑定邏輯塊144內之條目之一表或列表以確定當

前正鑑定或「登入」該系統之實體。存取處理邏輯塊142可接著利用授權邏輯塊142來檢查與每一經鑑定之實體相關聯之ACR以確定是否任一經鑑定之實體具有存取所請求之邏輯分區或位址範圍之一授權。

若至少一個實體當前經鑑定並被授權以存取該分區，則控制轉到步驟610，且存取處理邏輯塊142使用特性強制執行邏輯塊150來自邏輯分區表152檢索與該邏輯分區相關聯之一第一特性集。若適當，則存取處理邏輯塊142結合特性強制執行邏輯塊150在處理該存取請求時應用該第一特性或特性集。若沒有實體當前經鑑定，或若不授權當前正鑑定之實體中之任一者存取在存取嘗試中所請求之邏輯分區，則控制轉到步驟608，其中一檢索第二特性集並在處理該存取請求時應用該第二特性集。

在一個實施例中，在步驟604中，經鑑定並被授權之實體必須係請求存取該邏輯分區或位址範圍之相同實體。在另一實施例中，經鑑定並被授權之實體可係(但不必須係)請求存取該邏輯分區或位址範圍之實體。在此實施例中，若授權一當前正鑑定之實體存取該位址範圍，則包含該當前正鑑定之實體之任何實體可接著存取該邏輯分區。在一個實施方案中，非揮發性儲存裝置120之安全儲存應用程式(SSA)可確定請求存取該邏輯分區或位址範圍之實體之身份，且當選擇在處理該存取請求時所應用之特性時不利用此身份資訊。在另一實施方案中，SSA不可確定請求存取該邏輯分區或位址範圍之實體之身份。舉例而言，請求

存取之實體可不提供識別資訊作為該存取請求之一部分。在此情形下，若授權一當前正鑑定之實體存取該位址範圍，則任一實體(不管該實體之未知身份)可接著處理該邏輯分區。

除處置讀取資料或向一邏輯分區或位址範圍寫入資料之請求外，控制器140亦可處理管理邏輯分區或經組態之位址範圍之請求。管理邏輯分區可包含創建一邏輯分區、刪除一邏輯分區及修改與一邏輯分區或位址範圍相關聯之特性或特性集之中之一者或多者。

圖7顯示用於在非揮發性儲存裝置120內之非揮發性儲存媒體130中創建一邏輯分區之例示性步驟700。簡要參考圖1，接收在非揮發性儲存裝置120之非揮發性儲存媒體130內創建一邏輯分區之一請求。可經由通信介面112自主機110接收該請求。返回至圖7，在步驟702，控制器140自一實體接收一命令。控制轉到步驟704，其中該控制器確定該請求是否係創建一邏輯分區。若不是，則該控制器在步驟714中處理該命令，且步驟700完成。若該請求係創建一邏輯分區，則控制轉到步驟706，其中控制器140確定是否自一經鑑定之實體接收該請求。在一個實施例中，在向一ACR鑑定一實體時，SSA系統向該實體發佈一會話ID。在另一實施例中，在成功鑑定時，在新近經鑑定之實體與控制器140之間建立一安全通道。在一個實施例中，藉由在經由通信介面112傳輸資料之前以一通道密鑰加密資料並藉由在目的地處接收到資料之後以一通道密鑰解密資料來

恢復資料，在通信介面112上建立主機110與非揮發性儲存裝置120之間一安全通道。在創建邏輯分區時，一安全通道可保護由實體規定或由非揮發性儲存裝置120返回之敏感資訊。該經鑑定之實體可能經由一安全通道將會話ID(且可能ACR ID)傳輸至控制器140以將其自身識別為一經鑑定之實體。若創建一邏輯分區之請求不係來自一經鑑定之實體，則步驟700終止，且不創建一邏輯分區。

若當前正鑑定該實體，則控制自步驟706轉到步驟708。在步驟708中，控制器140確定該經鑑定之實體是否具有創建一邏輯分區之許可。存取處理邏輯塊142利用授權邏輯塊146來檢測與該經鑑定之實體相關聯之ACR。舉例而言，參考圖4，ACR #2之PCR指示授權使用ACR #2鑑定之一實體創建一邏輯分區。比較起來，ACR #1及ACR #N之PCR不授權一經鑑定之實體創建一邏輯分區。若不授權該實體創建一邏輯分區，則步驟700終止，且不創建一邏輯分區。

若授權該經鑑定之實體，則控制轉到步驟710，其中控制器140檢測欲創建之邏輯分區之位址範圍，並確定該位址範圍是否重疊或在已存在之一邏輯分區之位址範圍內。若重疊，則拒絕該命令，步驟700終止、且不創建一邏輯分區。若不重疊，則控制轉到步驟712，且使用在於步驟702中所傳輸之命令中所接收之資訊創建一邏輯分區。自該實體接收之命令可包含第一及第二特性集中之特性、該邏輯分區之位址範圍及創建該分區所需之其他參數。創建

一邏輯分區亦可包含向邏輯分區表152添加一條目。在創建該邏輯分區之後，步驟700終止。

圖8顯示用於刪除非揮發性儲存裝置120內之非揮發性儲存媒體130中之一邏輯分區之例示性步驟800。簡要參考圖1，接收刪除非揮發性儲存裝置120之非揮發性儲存媒體130內之一邏輯分區之一請求。可經由通信介面112自主機110接收該請求。返回至圖8，在步驟802，控制器140自一實體接收一命令。控制轉到步驟804，其中控制器140檢查該命令以確定請求是否係刪除一邏輯分區。若不是，則該控制器在步驟814中處理該命令，且步驟800完成。若該請求係刪除一邏輯分區，則控制轉到步驟806，其中控制器140確定是否自一經鑑定之實體接收該請求。在一個實施例中，經由在成功鑑定時在該實體與控制器140之間建立的一安全通道接收來自一經鑑定之實體之一請求。若刪除一邏輯分區之請求不係來自一經鑑定之實體，則步驟800終止，且不刪除一邏輯分區。

若當前正鑑定該實體，則控制自步驟806轉到步驟808。在步驟808中，控制器140確定該經鑑定之實體是否具有刪除一邏輯分區之許可。存取處理邏輯塊142利用授權邏輯塊142來檢查與該經鑑定之實體相關聯之ACR。在一個實施例中，一ACR可含有允許刪除任一邏輯分區之一授權。在另一實施例中，一ACR可含有允許刪除一特定邏輯分區或若干分區(例如由向彼ACR或彼ACR之父代鑑定之一實體先前所創建之一邏輯分區)之一授權。在一個實施方案

中，具有組態一邏輯分區之許可之一實體亦具有刪除該邏輯分區之許可。若不授權該實體刪除該分區，則步驟800終止，且不刪除一邏輯分區。

若授權該經鑑定之實體，則該控制器認可來自該實體之請求，且控制轉到步驟810，其中控制器140驗證欲刪除之所規定經組態之位址範圍或邏輯分區實際上存在。若其不存在，則控制器140已接收刪除一不存在的邏輯分區之一命令，且因此拒絕該命令，且步驟800終止。若該經組態之位址範圍或邏輯分區存在，則控制轉到步驟812，並刪除一邏輯分區。刪除一邏輯分區亦可包含自邏輯分區表152移除一條目。在一個實施例中，刪除一邏輯分區亦包擦除該邏輯分區內之資料。在另一實施例中，保持不碰觸該位址範圍或邏輯分區內之資料。在刪除該邏輯分區之後，步驟800終止。

圖9顯示用於修改一非揮發性儲存裝置內之非揮發性儲存器中之一邏輯分區之例示性步驟900。修改一邏輯分區或經組態之位址範圍可包含改變一特性、刪除一特性、改變與一經組態之位址範圍或分區相關聯之最大及最小位址範圍、或任一其他組態、維持或管理操作。簡要參考圖1，接收修改非揮發性儲存裝置120之非揮發性儲存媒體130內之一邏輯分區之一請求。可經由通信介面112自主機110接收該請求。返回至圖9，在步驟902，控制器140自一實體接收一命令。控制轉到步驟904，其中該控制器確定該請求是否係修改一邏輯分區。若不係，則該控制器在步

驟914中處理該命令，且步驟900完成。若該請求係修改一邏輯分區，則控制轉到步驟906，其中控制器140確定是否自一經鑑定之實體接收該請求。在一個實施例中，經由在成功鑑定時在該實體與控制器140之間建立的一安全通道接收來自一經鑑定之實體之一請求。若修改一邏輯分區之請求不係來自一經鑑定之實體，則步驟900終止，且不改變一邏輯分區。

若當前正鑑定該實體，則控制自步驟906轉到步驟908。在步驟908中，控制器140確定該經鑑定之實體是否具有修改一邏輯分區之許可。存取處理邏輯塊142利用授權邏輯塊142來檢查與該經鑑定之實體相關聯之ACR。在一個實施例中，一ACR可含有允許修改任一邏輯分區之一授權。在另一實施例中，一ACR可含有允許修改一特定邏輯分區或若干分區(例如由向彼ACR或彼ACR之父代鑑定之一實體先前所創建之一邏輯分區)之一授權。若不授權該實體刪除該分區，則步驟900終止，且保持不改變一邏輯分區。

若授權該經鑑定之實體，則控制器140認可來自該實體之請求，且控制轉到步驟910，其中控制器140驗證所規定經組態之位址範圍或邏輯分區實際上存在。若其不存在，則該控制器已接收修改一不存在的邏輯分區之一命令，且因此拒絕該命令，且步驟900終止。在步驟910，若該請求係擴展該分區之位址範圍，則控制器140亦檢查該經擴展之邏輯分區是否將重疊另一現有位址範圍或邏輯分區。若

重疊，則拒絕該命令，且步驟900終止。否則，控制轉到步驟912，且根據在步驟902中自該實體接收之命令修改一邏輯分區。該請求可識別該位址範圍或該邏輯分區，及修改該分區所需之其他參數，例如自第一及/或第二特性集改變或刪除特性。修改一邏輯分區亦可包含更新邏輯分區表152中之一條目。在修改該邏輯分區或經組態之位址範圍之後，步驟900終止。

因此，邏輯分區或經組態之位址範圍允許對非揮發性儲存裝置120之非揮發性儲存媒體130內之資料安全、完整性及存取控制之增強型控制。本文中所揭示之該等實施例中之一者或多者可併入一非揮發性可抽換媒體卡內。一非揮發性可抽換媒體卡之一個實例係TrustedFlash™卡，來自加利福尼亞、米爾皮塔斯之SanDisk公司之一儲存裝置。一TrustedFlash™卡內之非揮發性儲存器可被劃分成公用實體分區及專用實體分區。在不利用與特性相關聯之邏輯分區或位址範圍之情形下，可透過具有很少限制之標準主機命令或藉由在向TrustedFlash™裝置之SSA系統中之一ACR鑑定時利用專門存取命令來達成公用實體分區中之資料之存取。專用實體分區之存取在實體上限制於向在TrustedFlash™裝置之SSA系統中所界定之一ACR鑑定之實體。可藉由向選定經鑑定之實體授權存取某些加密或解密密鑰並藉由利用彼等密鑰來在將資料儲存於一專用實體分區或一公用實體分區中之前加密資料來在邏輯上限制一專用實體分區或一公用實體分區中之資料之存取。

藉由界定應用於邏輯分區或經組態之位址範圍之特性集，可達成對資料安全、完整性及存取控制之增強型控制。一TrustedFlash™裝置可含有公用實體分區或專用實體分區中之邏輯分區。該等邏輯分區係與界定及/或調整該裝置之一特定位址範圍之存取請求之特性集相關聯。除控制存取許可之外，可界定一特性集以亦控制功能性，例如加密、功率消耗及頻寬消耗。可界定兩個特性集。在授權至少一個當前正鑑定實體存取一邏輯分區時，在處理該邏輯分區之一存取請求時應用一第一特性集。在不授權任一當前正鑑定實體存取一邏輯分區時，應用一第二特性集來存取該邏輯分區。在向任一邏輯分區外部之一位址進行一存取嘗試時，使用一預設特性集來處理該存取請求。按組合，可組合該等特性集以提供針對在TrustedFlash™裝置之公用或專用實體分區內所界定之個別邏輯分區自訂之有用功率、效能、加密及存取組態。

該等邏輯分區係與通常不指派給一實體分區或與一實體分區相關聯之特性相關聯，且可比邏輯分區貯存於其中之實體分區更靈活地創建、改變及刪除該等邏輯分區。因此，邏輯分區補充並增強一TrustedFlash™裝置之實體分區，及藉由在儲存之前使用檔案資料之加密並限制密鑰之存取所達成之逐檔案保護。同時，邏輯分區存取、創建、刪除及管理之授權可容易地併入至存取控制群組及存取控制記錄之靈活TrustedFlash™階層樹結構中。透過使用存取控制群組及存取控制記錄，允許存取、創建、刪除或維

持一邏輯分區之實體(應用程式、使用者或主機)之進一步自訂可行。

雖然已參考各種系統及方法實施例描述了本發明，但將理解，本發明有權在隨附申請專利範圍之完整範疇內受到保護。

【圖式簡單說明】

該等圖中之組件未必按比例繪製，而是強調圖解說明其各種態樣。此外，在該等圖中，相同參考編號標示不同視圖中之對應部件。

圖1係圖解說明用於存取一非揮發性儲存裝置內之非揮發性儲存器之一例示性系統之一圖示；

圖2係圖解說明將非揮發性儲存媒體分區成實體及邏輯分區之例示性分區之一圖示；

圖3係圖解說明一例示性邏輯分區表、其中之條目及在一非揮發性儲存裝置之存取期間所應用之各種特性之編碼之一圖示；

圖4係圖解說明一存取控制群組(AGP)內之例示性存取控制記錄(ACR)(包含鑑定及授權資訊)之一圖示；

圖5係圖解說明配置成一樹狀階層結構之存取控制記錄及存取控制群組之一例示性配置之一圖示；

圖6顯示用於處理一非揮發性儲存裝置內之非揮發性儲存器之一存取嘗試之例示性步驟；

圖7顯示用於在一非揮發性儲存裝置內之非揮發性儲存器中創建一邏輯分區之例示性步驟；

圖8顯示用於刪除一非揮發性儲存裝置內之非揮發性儲存器中之一邏輯分區之例示性步驟；及

圖9顯示用於修改一非揮發性儲存裝置內之非揮發性儲存器中之一邏輯分區之例示性步驟。

【主要元件符號說明】

100	系統
110	主機
112	通信介面
120	非揮發性儲存裝置
130	非揮發性儲存媒體
140	控制器
142	存取處理邏輯塊
144	鑑定邏輯塊
146	授權邏輯塊
148	存取控制記錄
150	特性強制執行邏輯塊
152	邏輯分區表
160	處理器
202	實體分區
204	實體分區
206	實體分區
208	實體分區
212	邏輯分區
214	邏輯分區

216	邏輯分區
520	AGP
522	ACR
530	根 AGP

201025001

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：98139137

※ 申請日：98.11.18　　※IPC 分類：~~G06K~~ G06F 12/02 (2006.01)

一、發明名稱：（中文/英文）

管理一儲存裝置內之位址範圍之存取

MANAGING ACCESS TO AN ADDRESS RANGE IN A STORAGE DEVICE

二、中文發明摘要：

本發明揭示用於一儲存裝置中之資料之安全及存取控制之增強型組態。接收存取該儲存裝置內一儲存媒體中之一可定址記憶體位置之一請求。將具有藉由一位址範圍識別之相鄰接位址之一組可定址記憶體位置與第一及第二特性相關聯。若該可定址記憶體位置在該組可定址記憶體位置內且一實體當前經鑑定並被授權以存取該組可定址記憶體位置，則應用該第一特性。若該可定址記憶體位置在該組可定址記憶體位置內且沒有實體當前經鑑定並被授權以存取該組可定址記憶體位置，則應用該第二特性。該組可定址記憶體位置亦可係一邏輯分區，其中該第一及第二特性儲存於一邏輯分區表中。

三、英文發明摘要：

Enhanced configuration of security and access control for data in a storage device is disclosed. A request is received to access an addressable memory location in a storage media within the storage device. A set of addressable memory locations with contiguous addresses identified by an address range is associated with first and second characteristics. The first characteristic is applied if the addressable memory location is within the set of addressable memory locations, and an entity is currently authenticated to and authorized to access the set of addressable memory locations. The second characteristic is applied if the addressable memory location is within the set of addressable memory locations, and no entity is currently authenticated to and authorized to access the set of addressable memory locations. The set of addressable memory locations can also be a logical partition, where the first and second characteristics are stored in a logical partition table.

七、申請專利範圍：

1. 一種用於管理一儲存裝置中之一可定址記憶體位置之存取之方法，該方法包括：

在帶有具有可定址記憶體位置之一儲存媒體之一儲存裝置中，將該等可定址記憶體位置中藉由相鄰接位址之一位址範圍識別之一組一個或多個可定址記憶體位址與一第一特性及一第二特性相關聯，藉由如下步驟管理此等可定址記憶體位置之存取：

接收存取該儲存媒體中之一可定址記憶體位置之一請求；

若該可定址記憶體位置在該組可定址記憶體位置內且此時任一實體經鑑定並被授權以存取該組可定址記憶體位置，則應用該第一特性；及

若該可定址記憶體位置在該組可定址記憶體位置內且此時沒有實體經鑑定並被授權以存取該組可定址記憶體位置，則應用該第二特性。

2. 如請求項1之方法，其中管理該存取進一步包括若該可定址記憶體位置不在該組可定址記憶體位置內，則應用一預設特性。

3. 如請求項1之方法，其中，若該可定址記憶體位置在該組可定址記憶體位置內，則管理該存取進一步包括若此時進行該請求之一特定實體經鑑定並被授權以存取該組可定址記憶體位置則應用該第一特性，且若此時進行該請求之該特定實體未經鑑定且未被授權以存取該組可定

址記憶體位置則應用該第二特性。

4. 如請求項1之方法，其中當該儲存裝置利用來自一樹之一存取控制記錄時向該組可定址記憶體位置鑑定該實體，其中該樹包括以階層方式組織於其中之節點，每一節點包括至少一個存取控制記錄，其中該存取控制記錄包括用於向該組可定址位置鑑定該實體並授權由該實體存取該組可定址記憶體位置中所儲存之資料之憑證及許可。

5. 如請求項1之方法，其進一步包括授權該實體存取該組可定址記憶體位置，其中由該儲存裝置執行該授權。

6. 如請求項5之方法，其中授權該實體存取該組可定址記憶體位置包括利用來自一樹之一存取控制記錄來授權該實體存取該組可定址記憶體位置，其中該樹包括以階層方式組織於其中之節點，每一節點包括至少一個存取控制記錄，其中該存取控制記錄包括用於鑑定該實體並授權實體存取該組可定址記憶體位置中所儲存之資料之憑證及許可。

7. 如請求項5之方法，其進一步包括將一授權自該實體委派給一額外實體。

8. 如請求項7之方法，其中將一授權自該實體委派給該額外實體包括將該存取控制記錄中之至少一個許可委派給一額外存取控制記錄。

9. 如請求項1之方法，其進一步包括創建該組可定址記憶體位置與該第一特性及該第二特性之間的一關聯。

10. 如請求項9之方法，其中創建該邏輯分區與該第一特性及該第二特性之間的該關聯包括在一邏輯分區表中創建一新的條目。

11. 如請求項1之方法，其進一步包括移除該組可定址記憶體位置與該第一特性及該第二特性之間的一關聯。

12. 如請求項11之方法，其中移除該邏輯分區與該第一特性及該第二特性之間的該關聯包括自一邏輯分區表移除一條目。

13. 如請求項1之方法，其進一步包括創建一組新的可定址記憶體位置與該第一特性及該第二特性之間一關聯。

14. 如請求項1之方法，其進一步包括改變與該組可定址記憶體位置相關聯的該第一特性及該第二特性中之至少一者。

15. 如請求項1之方法，其進一步包括在應用該第一特性及該第二特性中之該至少一者之前檢索與該組可定址記憶體位置相關聯的該第一特性及該第二特性中之該至少一者。

16. 如請求項15之方法，其中將該第一特性及該第二特性儲存於一邏輯分區表中，其中該邏輯分區表包括複數個條目，其中一條目包括與相鄰接位址之該位址範圍相關聯之一邏輯分區識別符、該第一特性及該第二特性。

17. 如請求項1之方法，其中該組可定址記憶體位置在一分區表之一可定址範圍內。

18. 如請求項1之方法，其中該第一特性及該第二特性包括

存取特性。

19. 如請求項18之方法，其中該存取特性包括與一讀取命令相關聯之一讀取存取許可。

20. 如請求項18之方法，其中該存取特性包括與一寫入命令相關聯之一寫入存取許可。

21. 如請求項18之方法，其中該存取特性包括與一讀取命令相關聯之一讀取存取許可及與一寫入命令相關聯之一寫入存取許可。

22. 如請求項1之方法，其中該第一特性及該第二特性包括保護特性。

23. 如請求項22之方法，其中該保護特性包括一加密指令。

24. 如請求項1之方法，其中該第一特性及該第二特性包括效能特性。

25. 如請求項24之方法，其中該效能特性係一第一效能位準及一第二效能位準中之一者。

26. 如請求項1之方法，其中該第一特性及該第二特性包括功率消耗特性。

27. 如請求項26之方法，其中該功率消耗特性係一第一功率消耗位準及一第二功率消耗位準中之一者。

28. 如請求項1之方法，其中該儲存裝置係一非揮發性可抽換記憶體卡。

29. 如請求項1之方法，其進一步包括：

接收由一實體改變該第一特性及該第二特性中之至少一者之一請求；及

若該實體當前經鑑定並被授權以改變與該組可定址記憶體位置相關聯之該第一特性及該第二特性中之至少一者，則准予該請求。

30. 如請求項29之方法，其中改變該第一特性及該第二特性中之至少一者之該請求係刪除該第一特性及該第二特性之一請求，其中不再應用一已刪除之特性。

31. 一種儲存裝置，其包括：

一儲存媒體，其具有可定址記憶體位置，該等可定址記憶體位置中藉由相鄰接位址之一位址範圍識別之一組一個或多個可定址記憶體位址係與一第一特性及一第二特性相關聯；及

一控制器，其可運作以：

接收存取該儲存媒體中之一可定址記憶體位置之一請求；

若該可定址記憶體位置在該組可定址記憶體位置內且此時任一實體經鑑定並被授權存取該組可定址記憶體位置，則應用該第一特性；及

若該可定址記憶體位置在該組可定址記憶體位置內且此時沒有實體經鑑定並被授權存取該組可定址記憶體位置，則應用該第二特性。

32. 如請求項31之儲存裝置，其中該控制器進一步可運作以若該可定址記憶體位置不在該組可定址記憶體位置內則應用一預設特性。

33. 如請求項31之儲存裝置，其中當該儲存裝置利用來自一

樹之一存取控制記錄時向該組可定址記憶體位置鑑定一實體，其中該樹包括以階層方式組織於其中之節點，每一節點包括至少一個存取控制記錄，其中該存取控制記錄包括用於向該組可定址位置鑑定該實體並授權由該實體存取該組可定址記憶體位置中所儲存之資料之憑證及許可。

34. 如請求項31之儲存裝置，其中當該儲存裝置利用來自一樹之一存取控制記錄時授權一實體存取該組可定址記憶體位置，其中該樹包括以階層方式組織於其中之節點，每一節點包括至少一個存取控制記錄，其中該存取控制記錄包括用於鑑定該實體並授權實體存取該組可定址記憶體位置中所儲存之資料之憑證及許可。

35. 如請求項31之儲存裝置，其中該儲存媒體進一步包括一邏輯分區表，其中該邏輯分區表包括複數個條目，其中該邏輯分區表包括複數個條目，其中一條目包括與相鄰接位址之該位址範圍相關聯之一邏輯分區識別符、該第一特性及該第二特性。

八、圖式：

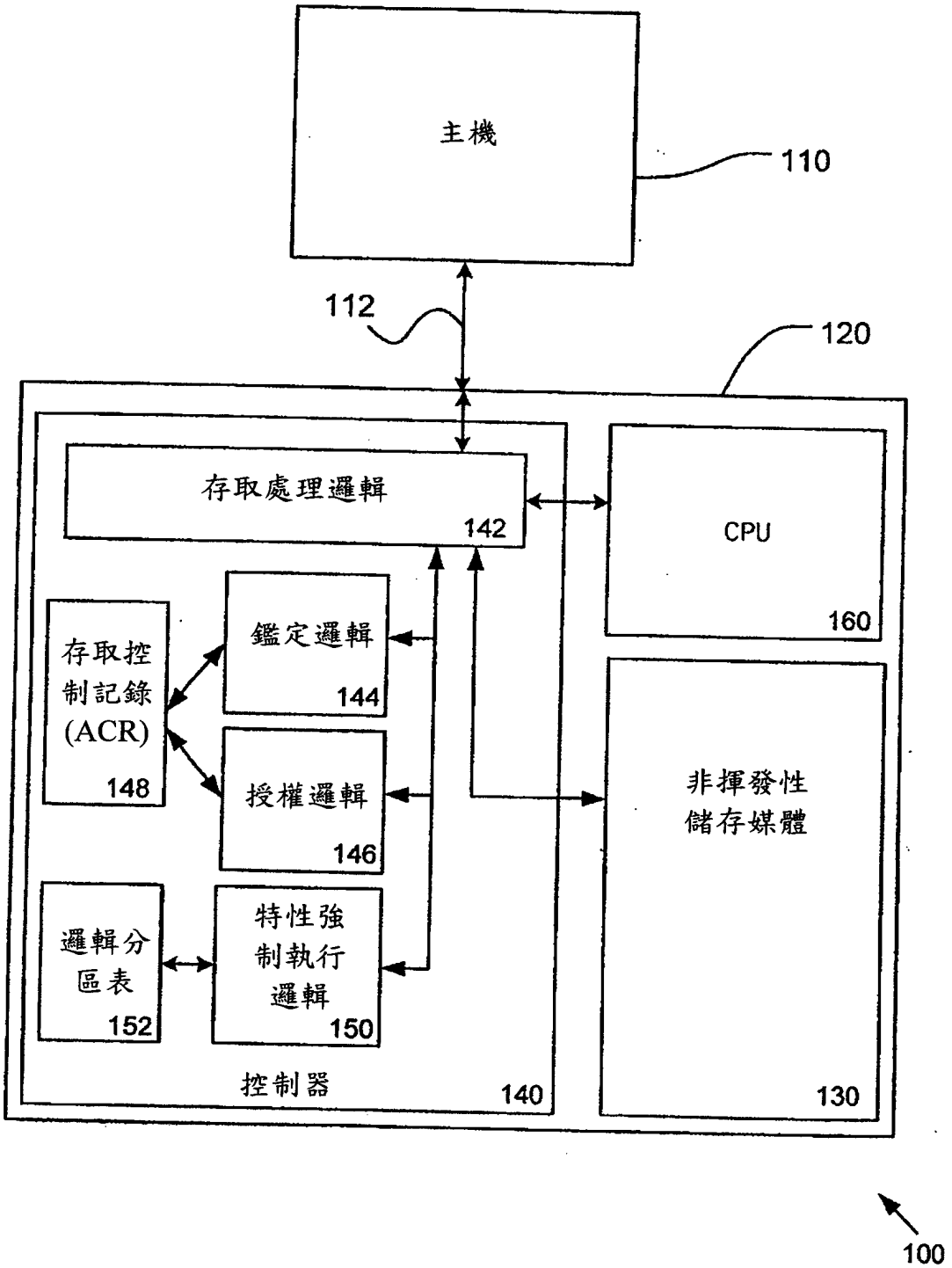

主機
110
112
120
存取處理邏輯
142
CPU
160
存取控制記錄(ACR)
148
鑑定邏輯
144
授權邏輯
146
非揮發性儲存媒體
130
邏輯分區表
152
特性強制執行邏輯
150
控制器
140
100

圖 1

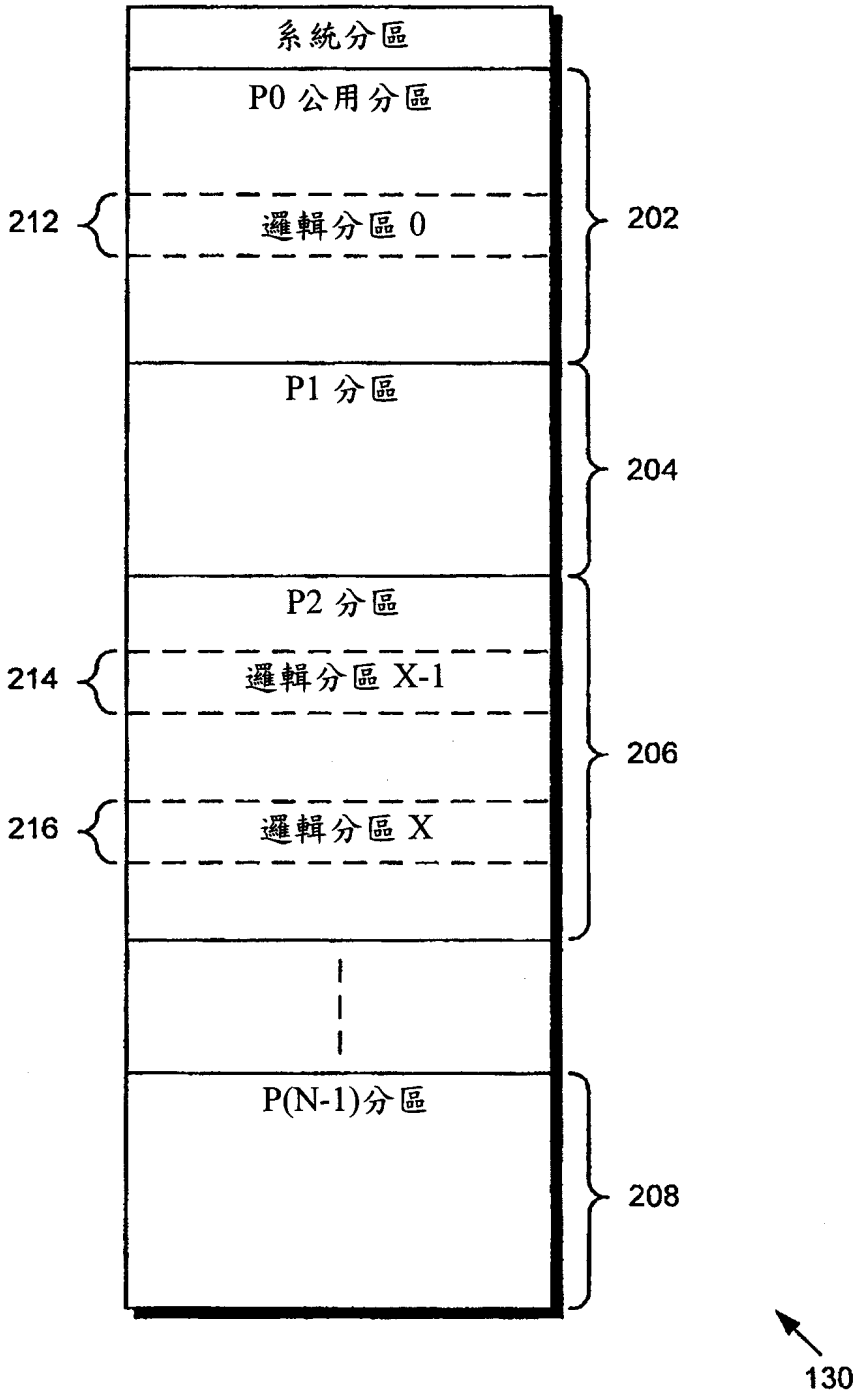
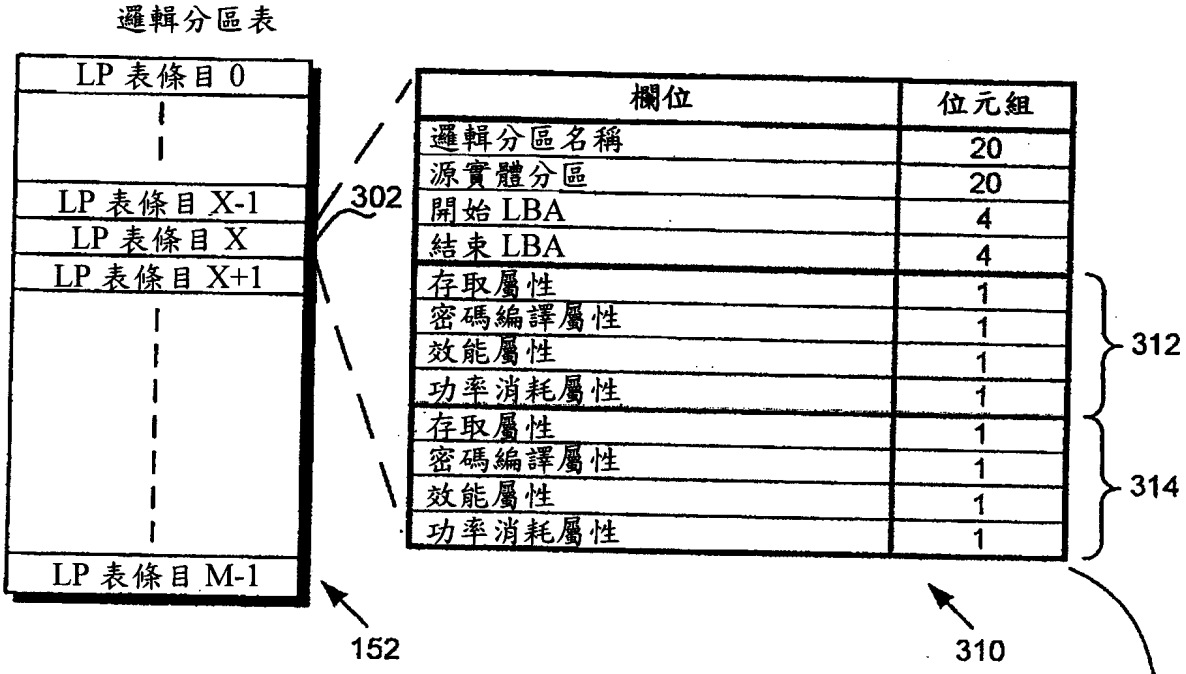

系統分區
P0 公用分區
212
邏輯分區 0
202
P1 分區
204
P2 分區
214
邏輯分區 X-1
206
216
邏輯分區 X
P(N-1)分區
208
130

圖 2



欄位	位元組
邏輯分區名稱	20
源實體分區	20
開始 LBA	4
結束 LBA	4
存取屬性	1
密碼編譯屬性	1
效能屬性	1
功率消耗屬性	1
存取屬性	1
密碼編譯屬性	1
效能屬性	1
功率消耗屬性	1

320

存取屬性值	描述
0x1	所允許之唯讀存取
0x2	所允許之唯寫存取
0x3	所允許之讀取/寫入存取
0x4	所允許之讀取/寫入/擦除存取

330

密碼編譯屬性值	描述
0x1	不完整之明文
0x2	不完整之經加密 AES

340

效能屬性值	描述
0x1	低效能
0x2	正常效能
0x3	高效能

350

功率消耗屬性	描述
0x1	高功率消耗
0x2	正常功率消耗
0x3	低功率消耗

圖 3

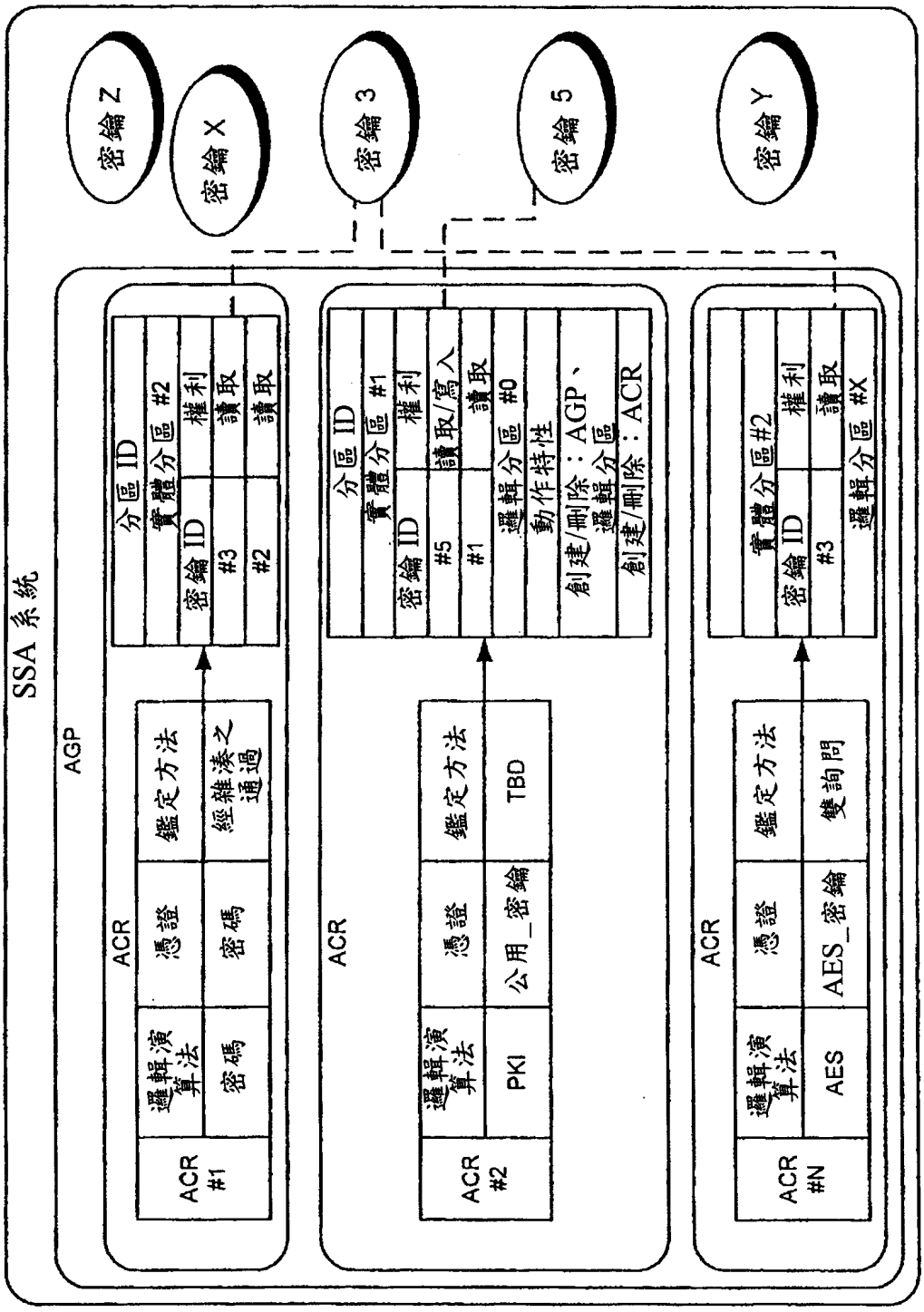

SSA 系統
AGP
密鑰 Z
密鑰 X
密鑰 3
密鑰 5
密鑰 Y
ACR
ACR #1
邏輯演算法
密碼
憑證
鑑定方法
密碼
經雜湊之通過
分區 ID
實體分區 #2
密鑰 ID
權利
#3
讀取
#2
讀取
ACR
ACR #2
邏輯演算法
PKI
憑證
公用_密鑰
鑑定方法
TBD
分區 ID
實體分區 #1
密鑰 ID
權利
#5
讀取/寫入
#1
讀取
邏輯分區 #0
動作特性
創建/刪除：AGP、邏輯分區
創建/刪除：ACR
ACR
ACR #N
邏輯演算法
AES
憑證
AES_密鑰
鑑定方法
雙詢問
實體分區#2
密鑰 ID
權利
#3
讀取
邏輯分區 #X

圖 4

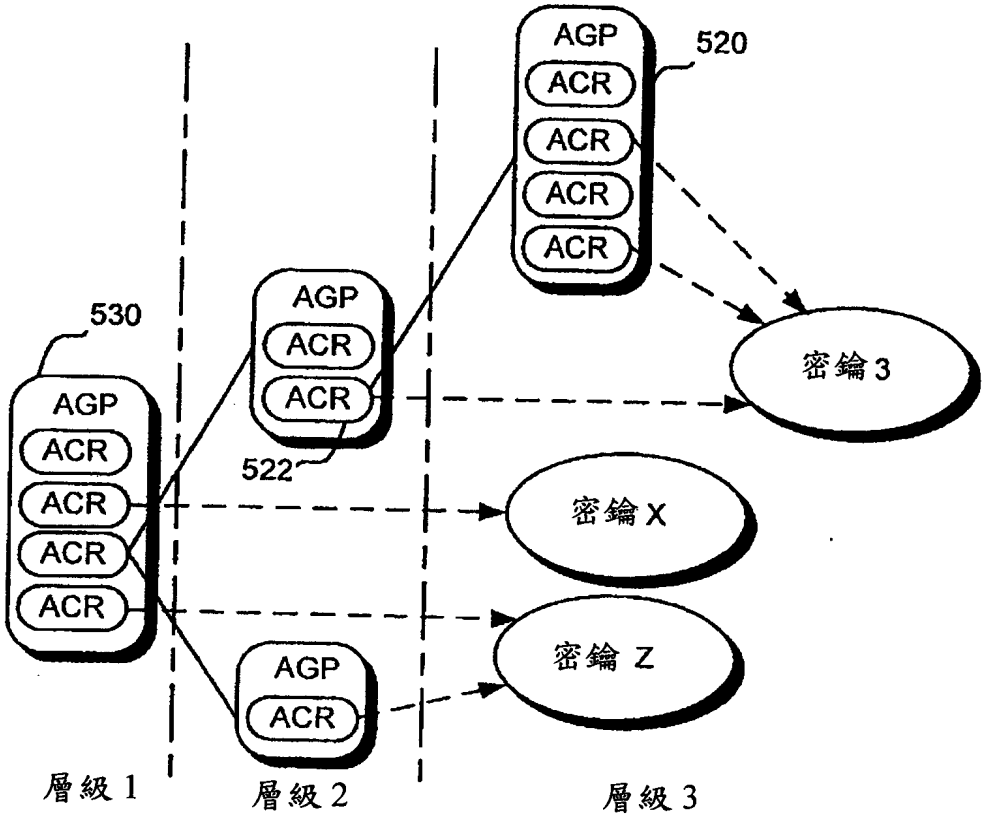

AGP
ACR
ACR
ACR
ACR
520
AGP
ACR
ACR
522
530
AGP
ACR
ACR
ACR
ACR
AGP
ACR
密鑰3
密鑰X
密鑰 Z
層級 1
層級 2
層級 3

圖 5

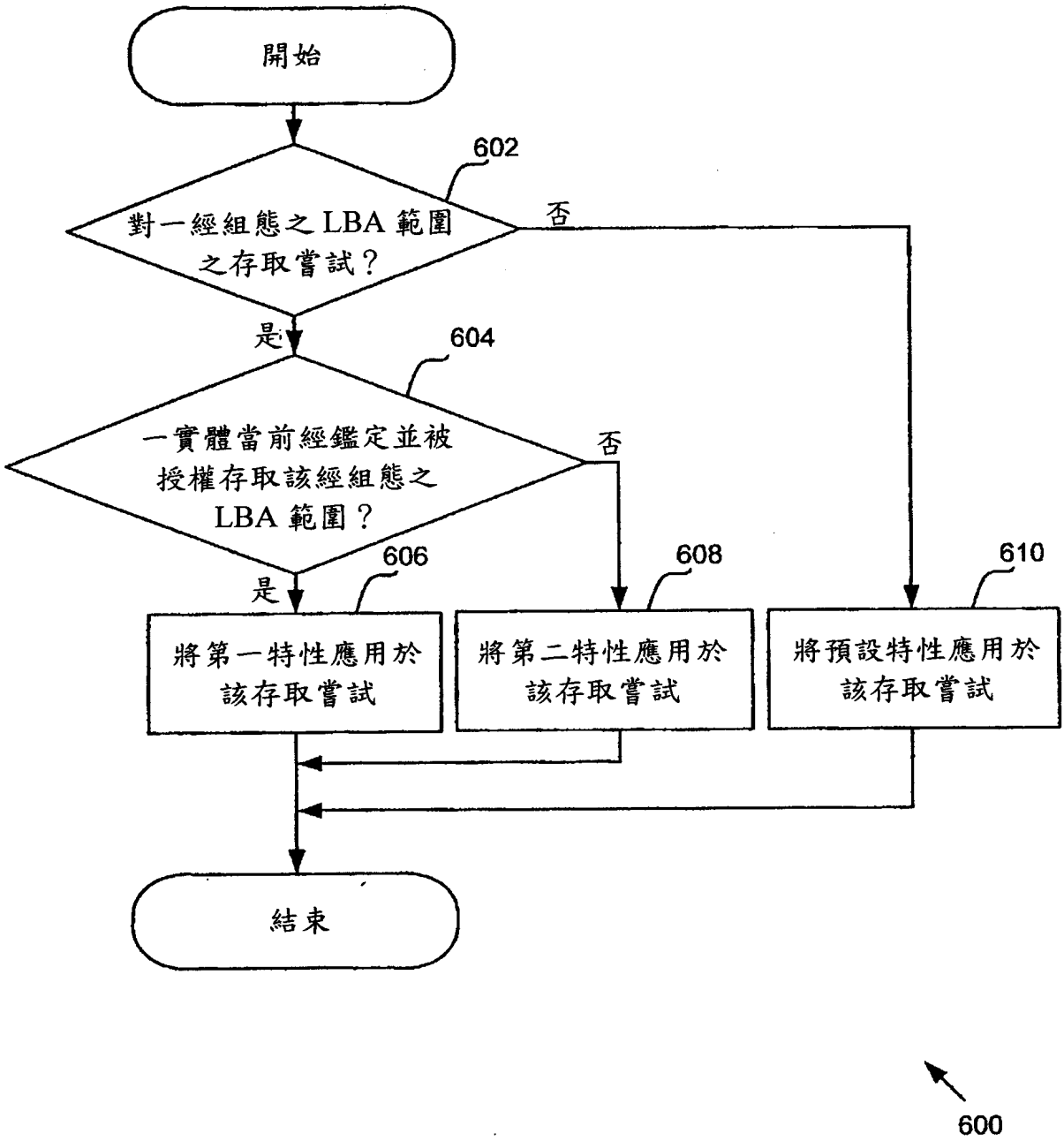

開始
602
對一經組態之 LBA 範圍之存取嘗試？
否
是
604
一實體當前經鑑定並被授權存取該經組態之 LBA 範圍？
否
是
606
608
610
將第一特性應用於該存取嘗試
將第二特性應用於該存取嘗試
將預設特性應用於該存取嘗試
結束
600

圖 6

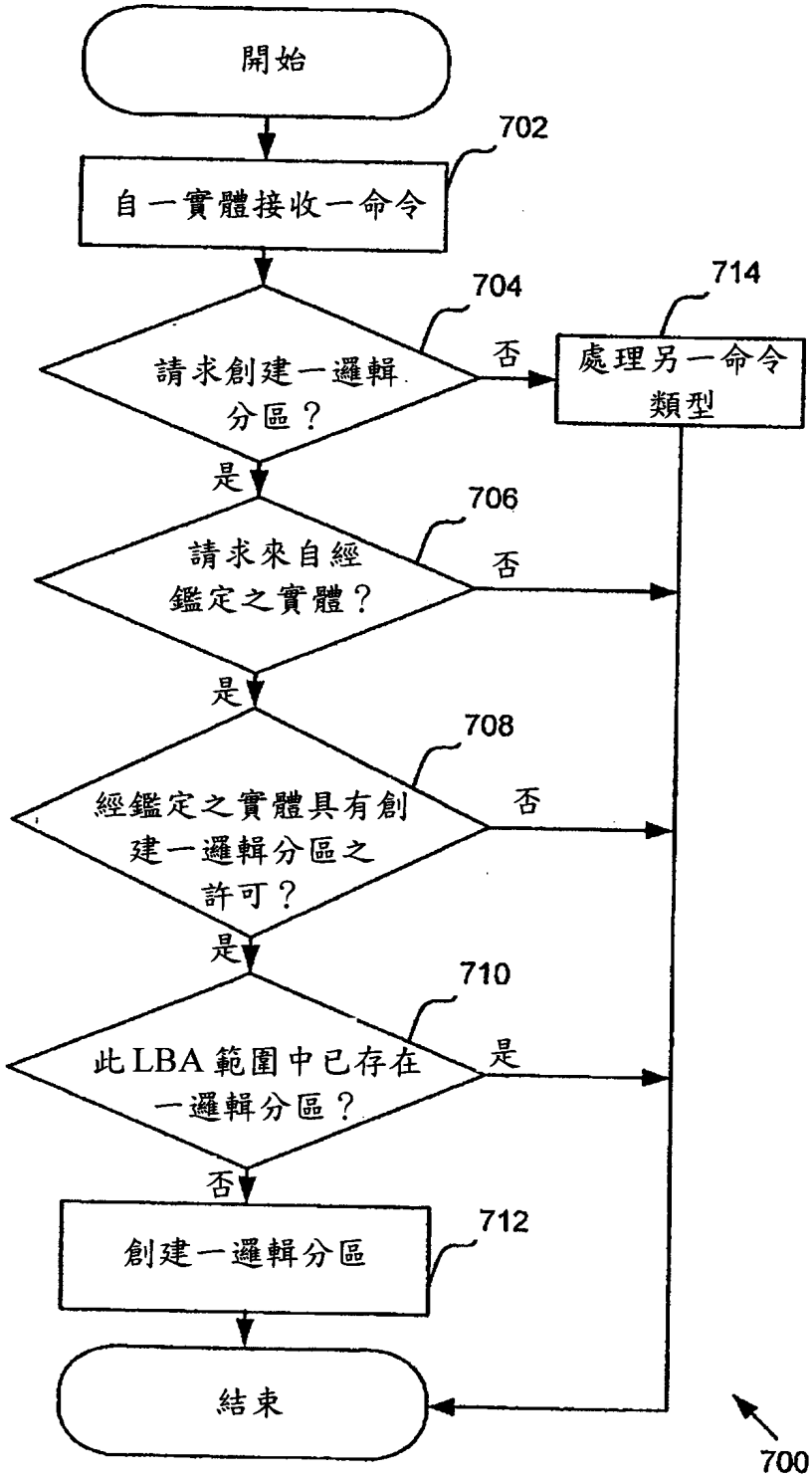

開始
702
自一實體接收一命令
704
請求創建一邏輯分區？
否
714
處理另一命令類型
是
706
請求來自經鑑定之實體？
否
是
708
經鑑定之實體具有創建一邏輯分區之許可？
否
是
710
此LBA範圍中已存在一邏輯分區？
是
否
712
創建一邏輯分區
結束
700

圖 7

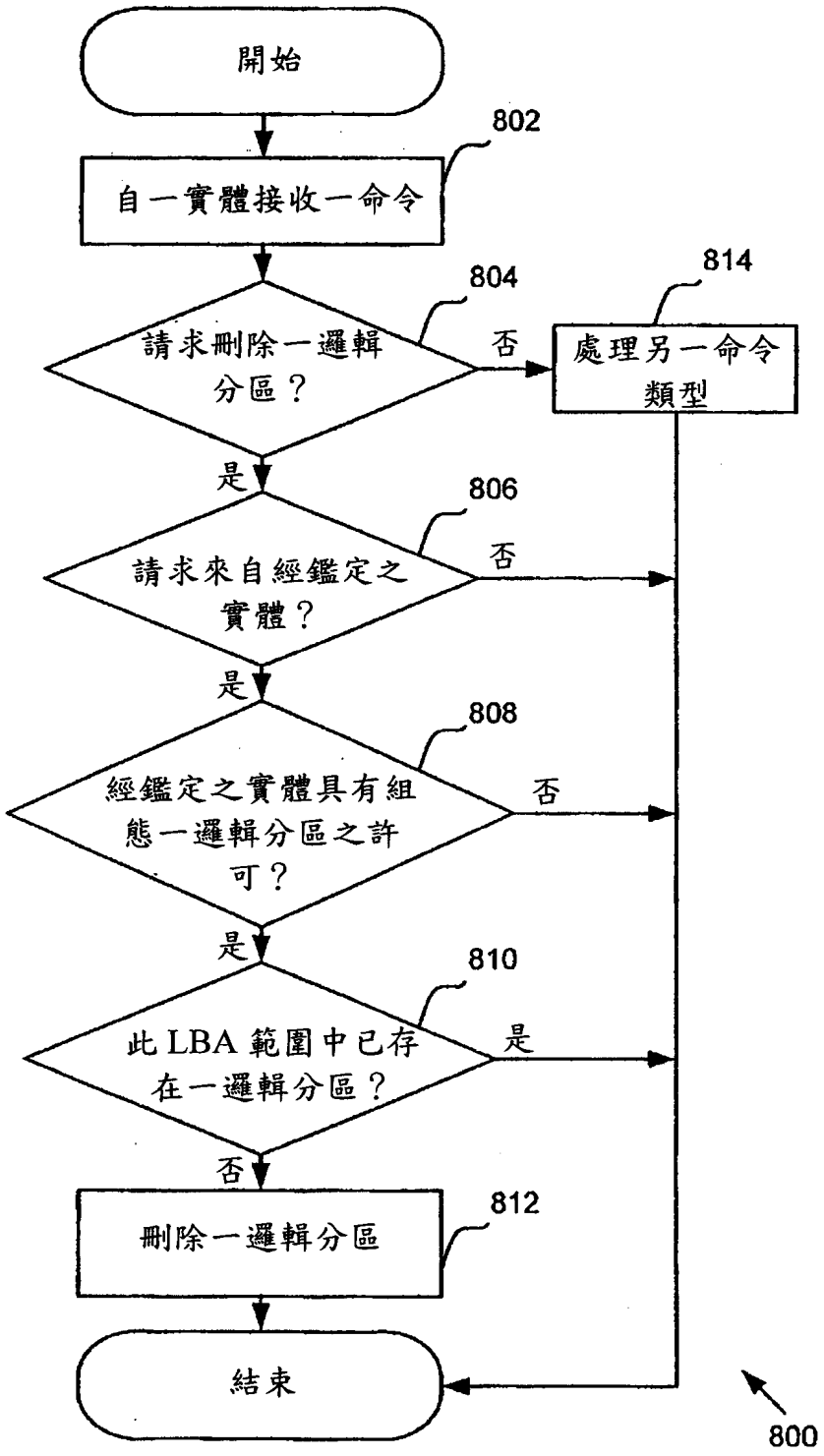

開始
802
自一實體接收一命令
804
請求刪除一邏輯分區？
否
814
處理另一命令類型
是
806
請求來自經鑑定之實體？
否
是
808
經鑑定之實體具有組態一邏輯分區之許可？
否
是
810
此 LBA 範圍中已存在一邏輯分區？
是
否
812
刪除一邏輯分區
結束
800

圖 8

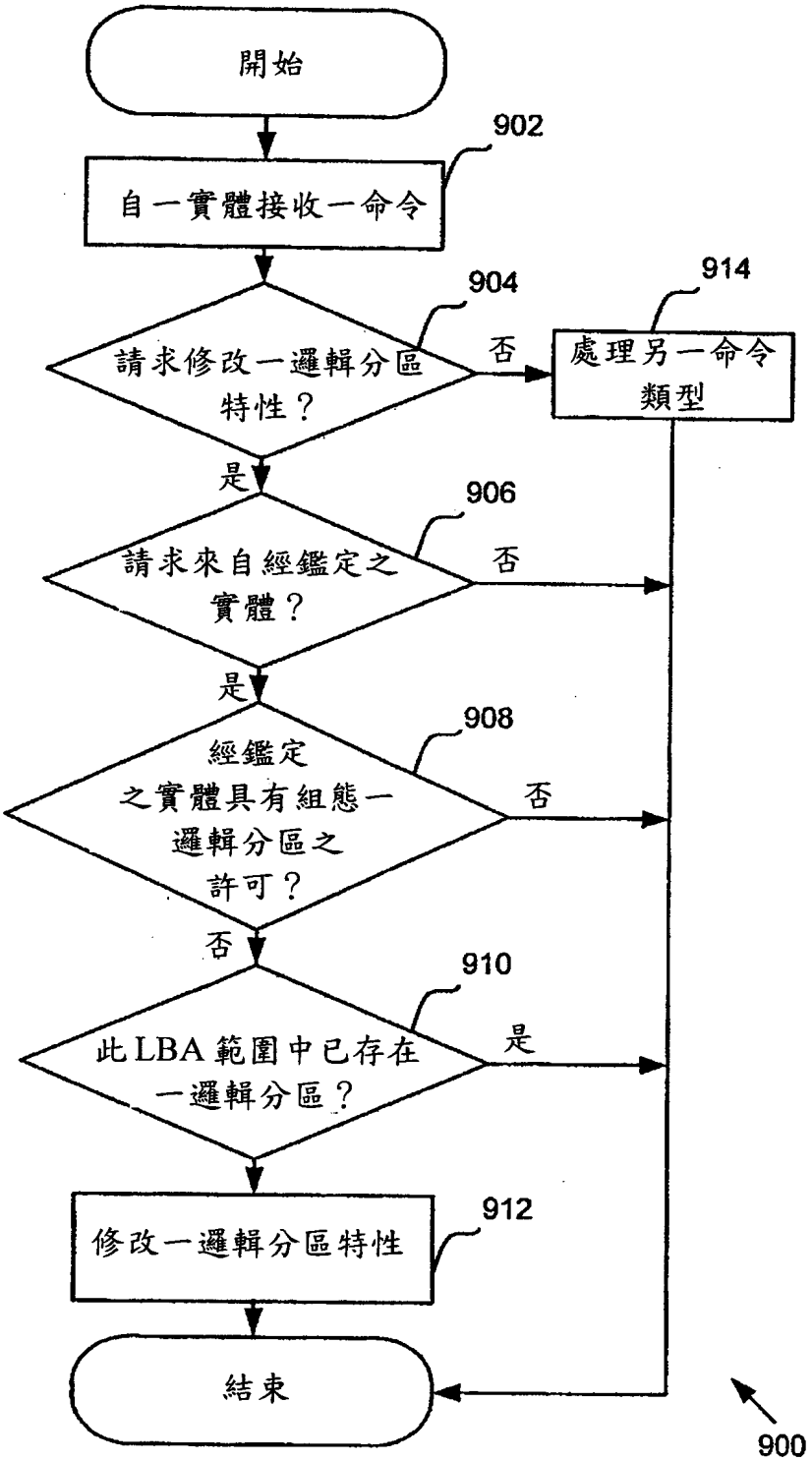

開始
902
自一實體接收一命令
904
914
請求修改一邏輯分區特性？
否
處理另一命令類型
是
906
請求來自經鑑定之實體？
否
是
908
經鑑定之實體具有組態一邏輯分區之許可？
否
否
910
此LBA範圍中已存在一邏輯分區？
是
912
修改一邏輯分區特性
結束
900

圖 9

四、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100	系統
110	主機
112	通信介面
120	非揮發性儲存裝置
130	非揮發性儲存媒體
140	控制器
142	存取處理邏輯塊
144	鑑定邏輯塊
146	授權邏輯塊
148	存取控制記錄
150	特性強制執行邏輯塊
152	邏輯分區表
160	處理器

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)