(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 201203092 A1
(43)公開日： 中華民國 101 (2012) 年 01 月 16 日

(21)申請案號：100109460 (22)申請日： 中華民國 100 (2011) 年 03 月 18 日
(51)Int. Cl.： *G06F3/06 (2006.01)* *G06F21/02 (2006.01)*
(30)優先權：2010/06/30 日本 2010-150042
(71)申請人：東芝股份有限公司 (日本) KABUSHIKI KAISHA TOSHIBA (JP)
日本
(72)發明人：松川伸一 MATSUKAWA, SHINICHI (JP) ；笠原章裕 KASAHARA, AKIHIRO (JP) ；坂本廣幸 SAKAMOTO, HIROYUKI (JP)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：21 項 圖式數：19 共 79 頁

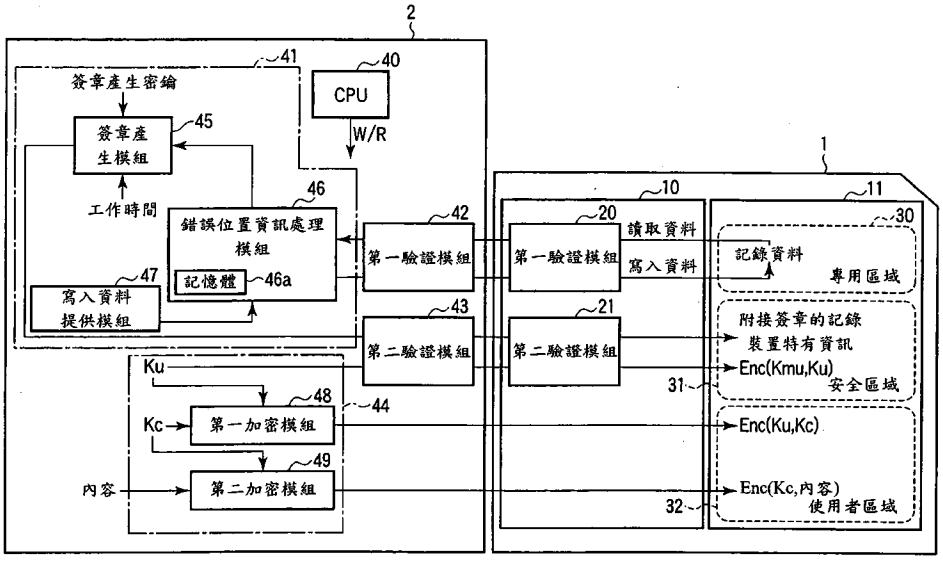
(54)名稱

記錄裝置、寫入裝置、讀出裝置及控制記錄裝置之方法

RECORDING APPARATUS, WRITING APPARATUS, READING APPARATUS, AND METHOD OF CONTROLLING RECORDING APPARATUS

(57)摘要

根據一實施例，一種記錄裝置包含一記憶體及一控制器。該記憶體能夠記錄資料。該控制器將該記憶體劃分成一第一區域及一第二區域且控制資料之記錄。該控制器在不對外部供應的資料執行錯誤校正編碼及一邏輯位址至一實體位址之位址轉換情況下將該外部供應的資料寫入至該第一區域中，且該控制器對該資料執行錯誤校正編碼及位址轉換，且接著將所得資料寫入至該第二區域中。



1：記憶卡
2：寫入裝置
10：記憶體控制器
11：NAND 快閃記憶體
20：第一驗證模組
21：第二驗證模組
30：專用區域
31：安全區域
32：使用者區域
40：CPU
41：產生模組
42：第一驗證模組
43：第二驗證模組
44：內容加密模組
45：簽章產生模組

46：錯誤位置資訊處理模組/處理模組

46a：暫時記憶體

47：寫入資料提供模組/提供模組

48：第一加密模組

49：第二加密模組

Kc：內容密鑰

Ku：使用者密鑰

(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 201203092 A1
(43)公開日： 中華民國 101 (2012) 年 01 月 16 日

(21)申請案號：100109460 (22)申請日： 中華民國 100 (2011) 年 03 月 18 日
(51)Int. Cl.： *G06F3/06 (2006.01)* *G06F21/02 (2006.01)*
(30)優先權：2010/06/30 日本 2010-150042
(71)申請人：東芝股份有限公司 (日本) KABUSHIKI KAISHA TOSHIBA (JP)
日本
(72)發明人：松川伸一 MATSUKAWA, SHINICHI (JP) ；笠原章裕 KASAHARA, AKIHIRO (JP) ；坂本廣幸 SAKAMOTO, HIROYUKI (JP)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：21 項 圖式數：19 共 79 頁

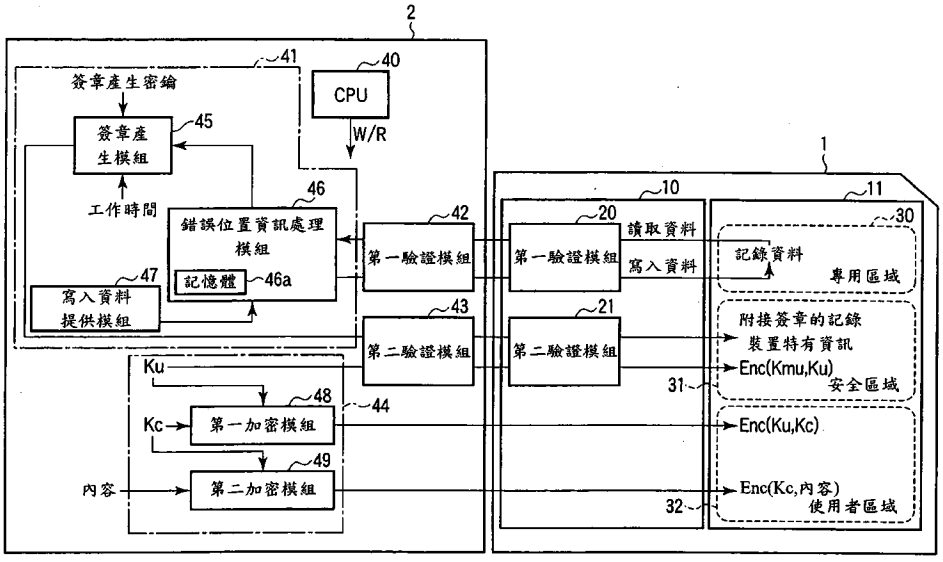
(54)名稱

記錄裝置、寫入裝置、讀出裝置及控制記錄裝置之方法

RECORDING APPARATUS, WRITING APPARATUS, READING APPARATUS, AND METHOD OF CONTROLLING RECORDING APPARATUS

(57)摘要

根據一實施例，一種記錄裝置包含一記憶體及一控制器。該記憶體能夠記錄資料。該控制器將該記憶體劃分成一第一區域及一第二區域且控制資料之記錄。該控制器在不對外部供應的資料執行錯誤校正編碼及一邏輯位址至一實體位址之位址轉換情況下將該外部供應的資料寫入至該第一區域中，且該控制器對該資料執行錯誤校正編碼及位址轉換，且接著將所得資料寫入至該第二區域中。



1：記憶卡
2：寫入裝置
10：記憶體控制器
11：NAND 快閃記憶體
20：第一驗證模組
21：第二驗證模組
30：專用區域
31：安全區域
32：使用者區域
40：CPU
41：產生模組
42：第一驗證模組
43：第二驗證模組
44：內容加密模組
45：簽章產生模組

六、發明說明：

【發明所屬之技術領域】

本文描述的實施例一般係關於一種記錄裝置、一種寫入裝置、一種讀出裝置及一種控制該記錄裝置之方法。

本申請案係基於且主張2010年6月30日申請的日本專利申請案第2010-150042號之優先權之權利，該案之全文內容以引用方式併入本文中。

【先前技術】

已知利用記錄媒體(諸如SD™記憶卡)之內容散佈。在此一內容散佈系統中，用於阻止非法內容拷貝之內容保護技術係重要的。

【實施方式】

一般而言，根據一實施例，一種記錄裝置包含一記憶體及一控制器。該記憶體能夠記錄資料。該控制器將該記憶體劃分成一第一區域及一第二區域且控制資料之記錄。該控制器在不對外部供應的資料執行錯誤校正編碼及一邏輯位址至一實體位址之位址轉換情況下，將該外部供應的資料寫入至該第一區域中，且該控制器對該資料執行錯誤校正編碼及位址轉換，且接著將所得資料寫入至該第二區域中。

[第一實施例]

將闡述根據一第一實施例之一種記錄裝置、一種寫入裝置、一種讀出裝置及一種控制該記錄裝置之方法。下文中，將以一SD記憶卡(下文中，簡稱為一記憶卡)為例闡述

該記錄裝置。

1.記憶卡之組態

將參考圖1簡要描述根據該第一實施例之一記憶卡之組態。稍後將在一第二實施例中詳細闡述該記憶卡之組態。圖1係一記憶卡及一寫入裝置之一方塊圖。

如圖1中顯示，一記憶卡1包含一記憶體控制器10及一NAND快閃記憶體11。可在分開基板上或在一單一基板上形成該記憶體控制器10及NAND快閃記憶體11。

該記憶體控制器10執行必要的程序以將資料寫入至該NAND快閃記憶體11中、自該NAND快閃記憶體11讀取資料、或根據來自一主機裝置之一存取擦除該NAND快閃記憶體11中之資料，該記憶卡1連接至該主機裝置(該實施例中之一寫入裝置或一讀出裝置)。

該記憶體控制器10包含一第一驗證模組20及一第二驗證模組21。該第一驗證模組20及該第二驗證模組21與該主機裝置協作執行該記憶卡1之驗證程序。藉由此驗證程序准許該主機裝置存取該記憶卡1。

此外，該記憶體控制器10將該NAND快閃記憶體11之記憶體區域劃分成至少三個區域且管理之。該三個區域係一專用區域30、一安全區域31及一使用者區域32。當在該第一驗證模組20處驗證該主機裝置時，該記憶體控制器10准許該主機裝置存取該專用區域30。當在該第二驗證模組21處驗證該主機裝置時，該記憶體控制器10准許該主機裝置存取該安全區域31。該主機裝置不需要經驗證即可存取該

使用者區域32。

在該安全區域31中，記錄記錄裝置特有資訊(下文中，簡稱為特有資訊)。特有資訊係每一記憶卡1之該NAND快閃記憶體11特有的資訊，更明確言之，係當將資料寫入至該NAND快閃記憶體11中時，可能發生一錯誤之位置上之資訊。該特有資訊由記憶卡1之該寫入裝置2產生且記錄在該安全區域31中。該專用區域30係由該寫入裝置2用於產生特有資訊的一區域。該使用者區域32係儲存有網路使用者(net user)資料之一區域。各種內容資料(包含音樂資料及電影資料)記錄在該使用者區域32中。用於加密該內容資料之加密密鑰之一者可記錄於該使用者區域32中。此外，另一加密密鑰可記錄在該安全區域31中。

2.寫入裝置2之組態

繼而，將參考圖1闡述根據該第一實施例之該寫入裝置2之組態。該寫入裝置2產生特有資訊且將該資訊寫入至該記憶卡1中且進一步將各種內容寫入至該記憶卡1中。

舉例而言，該寫入裝置2可係提供各種內容之一資訊站終端或一內容提供者。該寫入裝置2可係用於經由網際網路或類似物散佈的內容(諸如電影)之一記錄及再現設備。如圖1中顯示，該寫入裝置2粗略包含一CPU 40、一產生模組41、一第一驗證模組42、一第二驗證模組43及一內容加密模組44。

該CPU 40控制整個寫入裝置2之操作。當該寫入裝置寫入資料時，該CPU 40發出一寫入命令，且當該寫入裝置讀

取資料時，該CPU 40發出讀取命令。

當該寫入裝置存取該記憶卡1之該NAND快閃記憶體11之該專用區域30時，該第一驗證模組42與該控制器10之該第一驗證模組20協作執行一驗證程序。

當該寫入裝置存取該記憶卡1之該NAND快閃記憶體11之該安全區域31時，該第二驗證模組43與該控制器10之該第二驗證模組21協作執行一驗證程序。

該產生模組41根據來自該CPU 40之一指令產生特有資訊且將該資訊寫入至該記憶卡1中。該產生模組41包含一簽章產生模組45、一錯誤位置資訊處理模組46(下文中，簡稱為一處理模組46)及一寫入資料提供模組47(下文中，簡稱為一提供模組47)。當產生特有資訊時，該提供模組47產生待寫入至該NAND快閃記憶體11之該專用區域30中之資料。該處理模組46將由該提供模組47產生的資料寫入至該專用區域30中且讀取寫入的資料。接著，該處理模組46基於該寫入的資料與讀取的資料間之差異而產生特有資訊且將該特有資訊傳送至該簽章產生模組45。該簽章產生模組45基於一外部供應的(或內部產生的)簽章產生密鑰而將一數位簽章附接至該特有資訊。接著，該簽章產生模組45將附接數位簽章的特有資訊寫入至該NAND快閃記憶體11之該安全區域31中。

該內容加密模組44加密待記錄在該記憶卡1之該使用者區域32中之內容及一內容密鑰。以引用方式包含在本說明書中的日本專利申請KOKAI公開案第2005-341156號中揭

示的方法可應用於該內容加密模組44處之程序。稍後將闡述此之一實例作為一第三實施例。

3.讀出裝置之組態

繼而，將參考圖2闡述根據該第一實施例之該讀出裝置之組態。圖2係該記憶卡及讀出裝置之一方塊圖。

該讀出裝置係再現由(舉例而言)一資訊站終端或一內容提供者提供的內容之一裝置。在經由網際網路或類似物散佈內容(包含電影)之一系統中，可組合該讀出裝置與寫入裝置以形成一單一裝置(或整合至一單一裝置中)。如圖2中顯示，該讀出裝置3粗略包含一CPU 50、一判定模組51、一第一驗證模組52、一第二驗證模組53及一內容解密模組54。

該CPU 50控制整個讀出裝置3。當該讀出裝置寫入資料時，該CPU 50發出一寫入命令，且當該讀出裝置讀取資料時，該CPU 50發出一讀取命令。

當該讀出裝置存取該記憶卡1之該NAND快閃記憶體11之該專用區域30時，該第一驗證模組52與該控制器10之該第一驗證模組20協作執行一驗證程序。

當該讀出裝置存取該記憶卡1之該NAND快閃記憶體11之該安全區域31時，該第二驗證模組53與該控制器10之該第二驗證模組21協作執行一驗證程序。

該判定模組51根據來自該CPU 50之一指令而產生記錄裝置特有資訊(下文中，簡稱為特有資訊)。基於產生的特有資訊及由該寫入裝置2寫入該記憶卡1中之特有資訊，該判

定模組51判定該記憶卡1是否是一合法記錄媒體，換言之，該記憶卡1是否是一盜版媒體。下文中，為區分由該寫入裝置產生的特有資訊與由該讀出裝置產生的特有資訊，由該寫入裝置產生的特有資訊稱為第一特有資訊且由該讀出裝置3產生的特有資訊稱為第二特有資訊。如圖2中顯示，該判定模組51包括一簽章檢驗模組55、一錯誤位置資訊處理模組56(下文中，簡稱為一處理模組56)、一寫入資料提供模組57(下文中，簡稱為提供模組57)及一比較模組58。

當產生第二特有資訊時，該提供模組57產生待寫入至該NAND快閃記憶體11之該專用區域30中之資料。該處理模組56將由該提供模組57產生的資料寫入至該專用區域30中且讀取寫入的資料。接著，該處理模組56基於該寫入的資料與讀取的資料間之差異而產生第二特有資訊且將該第二特有資訊傳送至該比較模組58。該簽章檢驗模組55讀取來自該NAND快閃記憶體11之該專用區域30之該第一特有資訊。接著，基於一外部供應的(或內部產生的)簽章檢驗密鑰，該簽章檢驗模組55檢驗附接至該第一特有資訊之該數位簽章是否正確且將檢驗結果輸出至該CPU 50。該比較模組58讀取來自該NAND快閃記憶體11之該安全區域31之該第一特有資訊。接著，該比較模組58比較該第一特有資訊與由該處理模組56供應的該第二特有資訊且基於比較結果判定該記憶卡1是否是一合法記錄媒體。接著，該比較模組58將判定結果輸出至該CPU 50。

該內容解密模組54讀取來自該記憶卡1之該使用者區域32之內容及內容密鑰且接著解密此等資訊。以引用方式包含在本說明書中的日本專利申請KOKAI公開案第2005-341156號中揭示的方法可用於該內容解密模組54處之程序。稍後將闡述該方法之一實例作為一第三實施例。

4.寫入裝置2之操作

繼而，將參考圖3闡述當產生該第一特有資訊且將該第一特有資訊寫入至該記憶卡1中時該寫入裝置2之操作。圖3係闡述該寫入裝置2之操作之一流程圖。

如圖3中顯示，首先，回應於來自該CPU 40之一指令，該第一驗證模組42與該記憶卡1之該第一驗證模組20協作執行一驗證程序(步驟S10)。一器件(該第一實施例之該寫入裝置2)與(舉例而言)在參考文檔(CPRM Specification for SD Memory Card 4C Entity, LLC, <URL:http://www.4centity.com>)中揭示的一SD記憶卡間執行的一驗證程序可用作為該驗證程序。

將簡要闡述該驗證程序。該寫入裝置2與記憶卡1兩者具有相同的稱為一媒體特有密鑰之保密資訊。該寫入裝置2與記憶卡1之每一者將每次產生的一隨機數字傳給對方、藉由基於一媒體特有密鑰之一特定方法處理接收的值且將所得值回傳給對方。接著，檢驗回傳值。若檢驗顯示已準確執行該程序，則判定對方具有相同的保密資訊。即，判定對方係一經驗證的接收者。在參考文檔中，該器件讀取該記憶卡1中記錄的一媒體密鑰塊及一媒體ID且利用該器

件具有之一器件密鑰組實行一特定程序，藉此形成一媒體特有密鑰。與該媒體特有密鑰之值相同的值亦保存在該記憶卡中。

可藉由一公開密鑰基礎結構(PKI)方法來實行驗證程序。在該PKI方法中，當該器件驗證接收者之合法性時，該器件執行如下程序。當該器件與該接收者協作執行通信時，該器件具有一對具有一不對稱密碼演算法之一隱秘密鑰及一公開密鑰。該器件將每次產生的一隨機數字傳輸至該接收者。接著，該接收者利用一隱秘密鑰加密接收的隨機數字且送回經加密的隨機數字及一公開密鑰。當該器件接收此等時，該器件利用該公開密鑰解密該經加密的隨機數字。當經解密的隨機數字符合由該器件產生的一隨機數字時，判定該接收者係該隱秘密鑰之所有者之一方。即，判定該方係一經驗證的接收者。在器件側及接收者側之每一者處執行該程序。作為一實例，可應用參考文檔(Advanced Access Content System(AACS)Introduction and Common Cryptographic Elements Book <**URL:http://www.aacsla.com/specifications/AACS_Spec_Common_FINAL_0951.pdf**>)中寫的在一主機裝置與一驅動單元間實施的驗證方法。

由上文方法實行驗證程序之後，該提供模組47根據來自該CPU 40之一指令而產生且準備寫入資料(步驟S11)。該資料可係預定的特定資料或每次使用一隨機數字產生的資料。該提供模組47將產生的資料傳送至該處理模組46。

繼而，根據來自該CPU 40之一指令，該處理模組46經由該等第一驗證模組42、20將接收的資料寫入至該NAND快閃記憶體11之該專用區域30中(步驟S12)。此時，該CPU 40對該專用區域30發出一寫入命令及一位址。

接著，根據來自該CPU 40之一指令，該處理模組46讀取來自該專用區域30之資料(步驟S13)。此時，該CPU 40對該專用區域30發出一讀取命令及一位址。當然，步驟S13中讀取的資料係緊接先前步驟S12中寫入的資料。可在步驟S12與步驟S13間實行一驗證程序。

接著，該處理模組46比較步驟S13中讀取的資料與步驟S12中寫入的資料(步驟S14)。在該比較中，該處理模組46偵測到前者資料不符合後者之一資料位置，即，資料未正確寫入該記憶卡(及/或自該記憶卡正確讀出)之位置(或一錯誤之位置)。接著，該處理模組46將位置資訊記錄在一暫時記憶體46a中(步驟S15)。該暫時記憶體46a可定位在該處理模組46之內部或外部。此外，該暫時記憶體46a可係一揮發性半導體記憶體(諸如一DRAM或一SRAM)或一非揮發性半導體記憶體(諸如一NOR快閃記憶體)。

該寫入裝置2將步驟S11至S15中之程序重複一特定次數(n次，其中n係不小於2之一自然數)(步驟S16)。每次重複該等程序時，將一錯誤之位置額外寫入至該暫時記憶體46a中。因此，對於n次寫入之每一者將一錯誤之位置記錄在該暫時記憶體46a中。在重複寫入該專用區域30之前，該CPU 40發出一擦除命令及一位址至該專用區域30以預先

擦除資料。

此後，根據來自該CPU 40之一指令，該處理模組46參照該暫時記憶體46a且判定在n次寫入中寫入失敗不小於m次(m係不小於2之一自然數)之一錯誤之位置係第一特有資訊(步驟S17)。

此外，根據來自該CPU 40之一指令，該簽章產生模組45使用給至該寫入裝置2之一數位簽章產生密鑰產生一數位簽章以防止該第一特有資訊被變更且將該數位簽章附接至該第一特有資訊(步驟S18)。一數位簽章係附接至僅具有特定保密資訊之人可產生的數位資訊之一簽章。其係基於一通用資訊理論方法，該方法允許其他人檢驗該簽章係正確的，但阻止其等偽造該簽章。舉例而言，參考(Digital Signature Standard, FIPS186, **<URL:http://www.itl.nist.gov/fipspubs/index.htm>**)中描述的方法可應用於數位簽章。在一數位簽章中，基於一不對稱演算法加密待簽章的資料之一匯編(digest)值，其中一加密密鑰與一解密密鑰彼此不相同且經加密的資料被視為簽章資料。該數位簽章係基於檢驗時利用一解密密鑰解密簽章資料之一方法，且若經解密的資料符合待簽章的資料之該匯編值，則判定該數位簽章係真實的。一般使用上文參考文檔中描述的方法。

此後，根據來自該CPU 40之一指令，該簽章產生模組45將步驟S18中產生的附接簽章的第一特有資訊寫入至該NAND快閃記憶體11之該安全區域31中(步驟S19)。此時，該CPU 40對該安全區域31發出一寫入命令及一位址。

因為在步驟S19中存取該安全區域31，所以可在步驟S18與步驟S19間執行一驗證程序。由該等第二驗證模組21、43實行此程序。

在由步驟S10至S19中之程序將該附接簽章的第一特有資訊寫入至該記憶卡1中之後，該寫入裝置2接著將內容寫入至該記憶卡1中。可由一熟知方法執行該寫入。

5.讀出裝置3之操作

繼而，將參考圖4闡述在基於該第一特有資訊及該第二特有資訊判定該記憶卡1是否是一合法記錄媒體時該讀出裝置3之操作。圖4係闡述該讀出裝置3之操作之一流程圖。

如圖4中顯示，回應於來自該CPU 50之一指令，該第一驗證模組52與該記憶卡1之該第一驗證模組20協作執行一驗證程序(步驟S20)。類似於圖3中闡述的步驟S10中之驗證方法之一驗證方法可應用於該驗證程序。

繼而，根據來自該CPU 50之一指令，該提供模組57產生且準備寫入資料(步驟S21)。該資料可係預定的特定資料或每次使用一隨機數字產生的資料。此外，該資料可等於或不同於由該寫入裝置2之該提供模組47產生的資料。該提供模組57接著將產生的資料傳送至該處理模組56。

繼而，根據來自該CPU 50之一指令，該處理模組56經由該等第一驗證模組52、20將接收的資料寫入至該NAND快閃記憶體11之該專用區域30中(步驟S22)。此時，該CPU 50對該專用區域30發出一寫入命令及一位址。

接著，根據來自該CPU 50之一指令，該處理模組56讀取來自該專用區域30之資料(步驟S23)。此時，該CPU 50對該專用區域30發出一讀取命令及一位址。當然，步驟S23中讀取的資料係緊接先前步驟S22中寫入的資料。可在步驟S22與步驟S23間實行一驗證程序。

接著，根據來自該CPU 50之一指令，該處理模組56比較步驟S23中讀取的資料與步驟S22中寫入的資料(步驟S24)。在該比較中，該處理模組56偵測到前者資料不符合後者之一資料位置，即，資料未正確寫入該記憶卡1(及/或自該記憶卡1正確讀出)之位置(或一錯誤之位置)。接著，該處理模組56將位置資訊記錄在一暫時記憶體56a中(步驟S25)。該暫時記憶體56a可定位在該處理模組56之內部或外部。此外，該暫時記憶體56a可係一揮發性半導體記憶體(諸如一DRAM或一SRAM)或一非揮發性半導體記憶體(諸如一NOR快閃記憶體)。

該讀出裝置3將步驟S21至S25中之程序重複一特定次數(n次，其中n係不小於2之一自然數)(步驟S26)。每次重複該等程序時，將一錯誤之位置額外寫入至該暫時記憶體56a中。因此，對於n次寫入之每一者將一錯誤之位置記錄在該暫時記憶體56a中。此處，n及m可等於或不同於該寫入裝置2中使用的n及m。在重複寫入至該專用區域30之前，該CPU 50可發出一擦除命令及一位址至該專用區域30以預先擦除資料。

此後，根據來自該CPU 50之一指令，該處理模組56參照

該暫時記憶體56a且判定在n次寫入中寫入失敗不小於m次(m係不小於2之一自然數)之一錯誤之位置係第二特有資訊(步驟S27)。步驟S20至步驟S27中之具體程序與由該寫入裝置2實行的步驟S10至S17中之程序相同。

繼而，該簽章檢驗模組55與比較模組58讀取來自該NAND快閃記憶體11之該安全區域31之該第一特有資訊(步驟S28)。此時，該CPU 50對該安全區域31發出一寫入命令及一位址。因為在步驟S28中存取該安全區域31，所以可在步驟S27與步驟S28間執行一驗證程序。由該等第二驗證模組21、53執行此程序。

接著，根據來自該CPU 50之一指令，該簽章檢驗模組55驗證附接至讀取的第一特有資訊之該數位簽章之合法性。若檢驗結果顯示該數位簽章不真實，則該CPU 50中斷該程序且判定該記憶卡1係一非法記錄媒體或一盜版卡(步驟S29)。因此，阻止該讀出裝置3存取該記憶卡1。

此外，根據來自該CPU 50之一指令，該比較模組58比較該讀取的第一特有資訊與由該處理模組56供應的該第二特有資訊。若比較結果顯示前者不符合後者，則該CPU 50中斷該程序且判定該記憶卡1係一非法記錄媒體或一盜版卡(步驟S30)。因此，阻止該讀出裝置3存取該記憶卡1。

接著，若在步驟S29及S30中判定該記憶卡係一合法記錄媒體，則該讀出裝置3開始再現該NAND快閃記憶體11之該使用者區域32中記錄的內容。可由一熟知方法執行該再現。

6.驗證記憶卡1之一方法之具體實例

繼而，將闡述圖3及圖4中描述的操作之一具體實例。如上文描述，為檢驗該記憶卡1是否是一合法記錄媒體，使用該第一特有資訊及該第二特有資訊。使用由該等提供模組47、57產生的寫入資料來產生此等資訊。該寫入資料並不限於此。舉例而言，寫入資料之量係大約1百萬位元組(megabyte)。此後，為簡化闡述且促進理解，將闡述寫入資料含有16位元且該寫入裝置2及該讀出裝置3之每一者係基於假設n=5及m=3之一情況作為一實例。

首先，該寫入裝置2記錄該第一特有資訊。將參考圖5闡述此記錄程序。圖5係闡述每次重複步驟S11至S15中的寫入資料、讀取資料、該暫時記憶體56a中的資料及該第一特有資訊之一表。在圖5中，讀取資料項目中之下劃線顯示與寫入資料項目中的此等位元位置不同的位元位置。

如圖5中顯示，假定在一第一寫入中由該提供模組47產生的寫入資料係(0000_0000_0000_0000)且在將該寫入資料寫入至該區域30中之後自該專用區域30讀取的係(0000_0100_0000_0001)。即，自該讀取資料之開始數來之一第六位元及一第十六位元經倒置(有錯誤)。因此，錯誤位置(第六位元及第十六位元)記錄在該暫時記憶體46a中。

繼而，假定在一第二寫入中產生(1111_1111_1111_1111)作為寫入資料且讀取的係(1111_1011_1011_1100)。因此，錯誤位置(第六位元、第十位元、第十五位元及第十六位元)額外記錄在該暫時記憶體46a中。

繼而，假定在一第三寫入中產生(1111_0000_0000_0000)作為寫入資料且讀取的係(1101_0100_0000_0001)。因此，錯誤位置(第三位元、第六位元及第十六位元)額外記錄在該暫時記憶體46a中。

下文中，假定一第四寫入、一第五寫入及讀取的係如圖5中顯示的。接著，看出位元已倒置不少於m=3次之錯誤位置係第六位元及第十六位元。因此，該處理模組46將該等錯誤位置作為第一特有資訊寫入至該安全區域31中。

繼而，該讀出裝置3產生第二特有資訊且比較該第一特有資訊與該第二特有資訊。將參考圖6闡述比較程序。圖6係每次重複步驟S21至S25中的寫入資料、讀取資料、該暫時記憶體56a中的資料及該第二特有資訊之一表。在圖6中，下劃線與圖5中的下劃線意思相同。

如圖6中顯示，假定寫入資料之型樣與圖5之寫入資料之型樣相同。假定在一第一讀取中倒置一第六位元及一第十六位元，在一第二讀取中倒置一第三位元、一第六位元、一第十位元及一第十六位元，且剩餘的如圖6中顯示。

接著，看出位元已倒置不少於m=3次之錯誤位置係該暫時記憶體54中之第六位元及第十六位元。因此，該處理模組56將該等錯誤位置作為第二特有資訊傳送至該比較模組58。

該比較模組58比較圖5之該第一特有資訊與圖6之該第二特有資訊。接著，該第一特有資訊及該第二特有資訊在第六位元及第十六位元處之錯誤位置中彼此符合。因此，該

比較模組58判定該記憶卡係一合法記錄媒體。

7.第一實施例之作用

如上文描述，利用根據該第一實施例之該記錄裝置及其之控制方法，可抑制內容資料之未授權使用。下文將闡述此作用。

隨著資訊社會之最近發展，散佈內容(諸如電腦化書、報紙、音樂或移動影像)至使用者終端且使使用者能夠瀏覽該內容之一內容散佈系統已受到廣泛使用。

電腦化內容可被輕易複製(下文中，簡稱為內容)，且因此藉由侵犯版權而可能做出一非法行為。為保護內容免受此一非法行為之侵犯，一般利用一加密密鑰加密內容且接著記錄該內容。經加密的內容在再現時被解密。此類型內容保護技術包含可記錄媒體內容保護(CPRM)。此外，已考慮一種由兩種密鑰雙重加密一內容密鑰之加密雙重密鑰方法(例如，參考日本專利申請KOKAI公開案第2005-341156號)。舉例而言，此類型加密雙重密鑰方法用在MQbic(一註冊商標)。對於該等加密密鑰，一記錄媒體特有之一密鑰(諸如一媒體特有密鑰)安全儲存在一儲存媒體之一隱秘區域中且完全不能經外部存取。因此，舉例而言，即使已非法拷貝僅加密內容密鑰資料，但非法拷貝的人在沒有該媒體特有密鑰情況下不能使用內容資料。

然而，若此一媒體特有密鑰已藉由一些方法經非法讀取且傳遞至一非法卡製造者，則藉由拷貝一合法卡製成的盜版卡開始出現，結果係可非法使用內容資料。

在這方面，利用根據該第一實施例之一記憶卡，基於記錄裝置特有資訊判定該記憶卡是否是一合法記錄器件。相應地，即使已非法讀取該媒體特有密鑰，可阻止存取內容。因此，可抑制盜版卡之流通且可有效保護內容資料。

該記錄裝置特有資訊係指示由於將資料寫入至該NAND快閃記憶體中且接著讀取該資料而使寫入資料與讀取資料間不一致之頻率變高之位元位置。即，該資訊顯示已形成該NAND快閃記憶體11之一記憶體晶片中特別低效能記憶體單元之位置。當然，該記憶體晶片中之效能差記憶體單元之位置在各個記憶體晶片中係不同的。相應地，該記錄裝置特有資訊亦係每一NAND快閃記憶體11特有的資訊。

舉例而言，當寫入內容時，產生第一特有資訊且將其寫入至一記憶卡中。此後，當再現內容時，產生第二特有資訊且將之與該第一特有資訊進行比較。若該第二特有資訊符合該第一特有資訊，則該記憶卡被視為一合法記錄裝置。

舉例而言，考慮如圖7中顯示的情況。圖7顯示一合法記憶卡1-1及一非法拷貝的記憶卡1-2。

在該記憶卡1-1中，內容90記錄在一使用者區域32-1中且一控制器10-1保存一媒體特有密鑰92。一安全區域31-1保存第一特有資訊91。該資訊91符合該記憶卡1-1之一專用區域30-1中之錯誤位置。

假定該內容90、媒體特有密鑰92及第一特有資訊91已經非法拷貝於記憶卡1-2中。當再現該記憶卡1-2中之該內容

90時，使用該記憶卡1-2之一專用區域30-2產生第二特有資訊93。接著，該專用區域30-1中之記憶體單元之特性散佈不同於該專用區域30-2中之記憶體單元之特性散佈。因此，當然，該第二特有資訊93不同於該第一特有資訊91。因此，判定該記憶卡1-2係一非法卡，從而阻止再現該內容90。

在該第一實施例中，當產生該第一特有資訊及該第二特有資訊時，該專用區域30經複數次寫入及讀取。此使該第一實施例之方法更有效率。明確言之，若在僅一次寫入及讀取操作中產生該第一特有資訊及該第二特有資訊，則前者與後者彼此符合的機會係非常低的。因此，雖然其係一合法記錄媒體，但可能判定該記憶卡係一非法拷貝的卡。然而，實行複數次之寫入及讀取操作且僅使用錯誤數目超過一特定值之位置，藉此自該第一特有資訊及該第二特有資訊排除較不易於發生一錯誤之位元位置。

此外，基於發生錯誤之資料位置(或位元位置)產生該第一特有資訊及該第二特有資訊，藉此使上文方法更容易使用。在寫入/讀取失敗之一區域中，有許多有缺陷的記憶體單元。因此，考慮使用禁止使用的記憶體塊(所謂壞塊)。當然，期望該NAND快閃記憶體應具有盡可能少的壞塊。有一種具有非常少壞塊或沒有壞塊之產品。在此一情況下，若使用壞塊產生該第一特有資訊及該第二特有資訊，則其等全部將係無意義的資訊且因此一數位簽章亦將係無意義的。反而，從小資料單位(諸如位元單位)觀點來

看，無疑有兩個或兩個以上錯誤。因此，期望應使用根據該第一實施例之一方法。

此外，將一數位簽章附接至該第一特有資訊91有助於內容保護。以此方式，阻止盜版卡之擴展，藉此有效保護內容。

8.修改

雖然在該第一實施例中，已使用彼此完全符合的第一特有資訊及第二特有資訊之一情況給出闡述，但該第一特有資訊及該第二特有資訊彼此可能不完全符合。即，當該第一特有資訊與該第二特有資訊以一特定比率彼此符合時，可判定該記憶卡係一合法產品。明確言之，當該第一特有資訊中之錯誤位置數目與該第二特有資訊中之錯誤位置數目比較時，若其等彼此符合的百分比等於該第一特有資訊或該第二特有資訊中之錯誤位置之總數目之一特定百分比，則可判定該記憶卡係一合法產品。

舉例而言，在參考圖5及圖6闡述的實例中，若50%之一符合比率係可接受，則即使包含第六位元或第十六位元僅任一者作為該第二特有資訊，仍判定該記憶卡係一合法產品。然而，從一高階內容保護觀點來看，提高一要求的符合比率係較佳的。

該記憶卡1中寫入的資料可隨時間改變。相應地，將符合比率設定為小於100%，藉此使該第一實施例之系統更容易使用。

此外，不僅符合比率而且該第一特有資訊及該第二特有

資訊中包含的錯誤位置間之關係亦可考慮在內。舉例而言，預先判定錯誤位置間之關係。即使當在錯誤位置中該第一特有資訊未符合該第二特有資訊時，若獲得錯誤位置間之經判定的關係具有一特定量，則可判定該記憶卡係一合法產品。

舉例而言，可理解該第二特有資訊中之錯誤位置數目一般增加多於該第一特有資訊中之錯誤位置數目。原因係每當寫入/擦除該專用區域30時，該等記憶體單元之特性便劣化。此時，當增加的錯誤位置數目不多於一特定數目時或當增加比率不多於該第一特有資訊中之錯誤位置數目之一特定百分比時，可判定該記憶卡係一合法產品。

此外，在該第一實施例中，已使用特有資訊指示倒置資料中位元之位元位置之一情況給出闡述。然而，特有資訊並不限於位元位置，只要資訊代表該等位元位置。例如，可由一位址代表特有資訊。該位址係發生一錯誤之一區域之一實體位址。該位址係指定可由該寫入裝置2及該讀出裝置3存取的最小記憶體區域(例如，叢集)之一位址。

[第二實施例]

將闡述根據一第二實施例之一記錄裝置、一寫入裝置、一讀出裝置及控制該記錄裝置之一方法。該第二實施例係關於該第一實施例之一SD記憶卡1之細節。因此，將省略對一寫入裝置2及一讀出裝置3之一詳細闡述。

1.記憶卡之組態

首先，將參考圖8闡述一記憶卡1之一整體組態。圖8係

根據該第二實施例之該記憶卡1之一方塊圖。

該記憶卡1可經由一匯流排介面5連接至一主機裝置4。當該記憶卡1連接至該主機裝置4時，電能供應至該記憶卡1，接著該記憶卡1根據自該主機裝置4之存取操作並執行處理。該主機裝置4對應於該第一實施例中闡述的該寫入裝置2及讀出裝置3。

該記憶卡1粗略包含上文提到的記憶體控制器10、NAND快閃記憶體11及一資料匯流排12。該記憶體控制器10及NAND快閃記憶體11由該資料匯流排12而連接至彼此。

1.1 記憶體控制器10之組態

繼而，將參考圖8闡述該記憶體控制器10之細節。如圖8中顯示，該記憶體控制器10包含一SD卡介面70、一MPU 71、一預記錄媒體拷貝保護(CPRM)電路72、一ROM 73、一RAM 74及一NAND介面75。此等在一單一半導體基板上形成且經由一內部匯流排76彼此連接，以便彼此進行通信。

可經由一匯流排介面5(SD卡匯流排)連接至該主機裝置4之該SD卡介面70監管與該主機裝置4之通信。可經由資料匯流排12連接至該NAND快閃記憶體11之該NAND介面75監管與該NAND快閃記憶體11之通信。

該MPU 71控制整個記憶卡1之操作。舉例而言，當電能供應至該記憶卡1時，該MPU 71讀出該ROM 73中儲存的韌體(控制程式)至該RAM 74上且執行特定處理，藉此在該RAM 74上創建各種表。此外，該MPU 71接收來自該主機

裝置4之一寫入命令、一讀取命令或一擦除命令而在該NAND快閃記憶體11上執行一特定處理或控制一資料傳送程序。稍後將詳細闡述該MPU 71具有的具體功能之一些。

該ROM 73儲存由該MPU 71及其他元件控制的一控制程式。用作為該MPU 71之一工作區域之該RAM 74儲存該控制程式及各種表。

該CPRM電路72監管該記憶卡1之一版權保護功能。即，當該主機裝置4存取該NAND快閃記憶體11中應為隱秘之資訊時，該CPRM電路72判定是否准許該存取。

1.2 NAND快閃記憶體11之組態

繼而，將參考圖8闡述該NAND快閃記憶體11之組態。如圖8中顯示，該NAND快閃記憶體11包含一記憶體單元陣列80、一列解碼器81、一頁面緩衝器82及一NAND介面83。

該記憶體單元陣列80包含複數個記憶體塊BLK。該等記憶體塊之每一者係能夠保存資料之一組記憶體單元。以一矩陣配置該等記憶體單元。相同列中之複數個記憶體單元連接至相同的字線。資料被整塊寫入至連接至相同字線之該等記憶體單元中或自該等記憶體單元中讀出。該等記憶體單元之每一者可保存1位元資料(2層級模式)或2位元資料(4層級模式)。擦除記憶體塊BLK中的資料。

該NAND介面83監管該記憶體控制器10與NAND介面75間經由該資料匯流排12之通信。接著，該NAND介面83將由該記憶體控制器10給出的一列位址傳送至該列解碼器81

且將資料寫入至該頁面緩衝器82。此外，該NAND介面83將自該頁面緩衝器82傳送的資料傳輸至一記憶體控制器10。

該列解碼器81解碼由該NAND介面83給出的一列位址。根據解碼結果，該列解碼器81選擇該記憶體單元陣列80中之該等記憶體塊BLK之任一者之一列方向。即，該列解碼器81選擇該等頁面之任一者。

將資料輸入至該記憶體單元陣列80或輸出來自該記憶體單元陣列80之資料之該頁面緩衝器82暫時保存資料。該頁面緩衝器82以頁面將資料輸入至該記憶體單元陣列80或輸出來自該記憶體單元陣列80之資料。當寫入資料時，該頁面緩衝器82暫時保存由該NAND介面83給出的寫入資料且將該資料寫入至記憶體單元中。當讀取資料時，該頁面緩衝器82暫時保存所讀取的資料且將該資料傳送至該NAND介面83。

1.3 記憶體控制器10之功能

如該第一實施例中描述，該記憶體控制器10將該NAND快閃記憶體11之記憶體區域劃分成複數個區域(明確言之，係一專用區域30、一安全區域31及一使用者區域32)且管理此等區域。下文中，將參考圖9具體闡述用以存取經劃分的區域之該記憶體控制器10之該MPU 71之功能。圖9係該記憶卡1之一功能方塊圖，其顯示該MPU 71具有的功能及經劃分的區域。

如圖9中顯示，該記憶體控制器10之該MPU 71不僅包含

該第一實施例中闡述的該第一驗證模組20及第二驗證模組21而且包含一寫入控制模組22、一邏輯位址至實體位址轉換模組(下文中，稱為一L2P處理模組)23、一錯誤校正編碼模組(下文中，稱為一ECC模組)24、一耗損平均控制模組25及一隨機化控制模組26。該MPU 71可藉由實施軟體或利用獨立於該MPU 71之硬體或軟體而實現此等功能。該第一驗證模組20及該第二驗證模組21係如該第一實施例中描述的且因此將省略其等之闡述。

該L2P處理模組23將由該主機裝置4給出的一邏輯位址轉換成一實體位址(此程序稱為一L2P程序)。

該ECC模組24使資料經受錯誤校正編碼。明確言之，當寫入資料時，該ECC模組24使由該主機裝置4供應的資料經受錯誤校正編碼，以產生一同位檢查位元且將其加至該資料。當讀取資料時，該ECC模組24基於自該NAND快閃記憶體11讀取的資料產生一校驗子。基於該校驗子，該ECC模組24偵測該資料中之一錯誤位置且校正錯誤資料。

該耗損平均控制模組25使該NAND快閃記憶體11經受耗損平均。耗損平均係管理該等記憶體塊BLK之每一者之重寫數目以便阻止資料存取集中在一特定記憶體塊BLK處之一程序。舉例而言，當將資料寫入至記憶體塊BLK1時，若記憶體塊BLK1中之寫入頻率高，則將資料寫入至寫入頻率較低之另一記憶體塊BLK2中，且將已經寫入記憶體塊BLK1中之資料拷貝至記憶體塊BLK2中。

該隨機化控制模組26在寫入資料中隨機化由該主機裝置

4供應的資料，藉此阻止「1」或「0」繼續。基於(舉例而言)由一偽隨機數字產生器產生的偽隨機數字與該資料之邏輯互斥或操作而執行隨機化資料。當讀取資料時，該隨機化控制模組26解碼由該NAND快閃記憶體11供應的所讀取的資料。

該寫入控制模組22控制該L2P處理模組23、ECC模組24、耗損平均控制模組25及隨機化控制模組26。當寫入資料時，該寫入控制模組22產生該NAND介面中定義的一寫入命令且將該寫入命令與待寫入至之一區域之實體位址及寫入資料一起輸出至該NAND快閃記憶體11。當讀取資料時，該寫入控制模組22產生該NAND介面中定義的一讀取命令且將該讀取命令與待讀取該命令之一區域之實體位址一起輸出至該NAND快閃記憶體11。

利用此組態，該記憶體控制器10使該第一驗證模組20驗證自該主機裝置4至該專用區域30之存取之合法性。該L2P處理模組23、ECC模組24、耗損平均控制模組25及隨機化控制模組26不執行處理。即，該專用區域30不經受一L2P程序、一ECC程序及耗損平均。此外，用於該專用區域30之資料不經隨機化。換言之，該主機裝置4使用一實體位址存取該專用區域30。又換言之，該記憶卡1將自該主機裝置4接收的一位址視為一實體位址而不是一邏輯位址。接著，當寫入資料時，該寫入控制模組22將該實體位址、由該主機裝置4供應的資料及由該NAND介面定義的一寫入命令輸出至該NAND快閃記憶體11。此時，該寫入控制模

組22以4層級模式寫入資料。當讀取資料時，該寫入控制模組22將一實體位址及一讀取命令輸出至該NAND快閃記憶體11。

此外，該記憶體控制器10使該第二驗證模組21驗證自該主機裝置4至該安全區域31之存取之合法性。接著，在該寫入控制模組22之控制下，該L2P處理模組23、ECC模組24、耗損平均控制模組25及隨機化控制模組26執行處理。即，執行一L2P程序、一ECC程序及耗損平均。此外，隨機化該資料。取決於情況，可省略該ECC程序、耗損平均及資料隨機化之至少一者。接著，當寫入資料時，該寫入控制模組22將在該L2P處理模組23處獲得的一實體位址、增加一同位檢查位元(如需要)之隨機化資料及一寫入命令輸出至該NAND快閃記憶體11。此時，該寫入控制模組22以2層級模式寫入資料。當讀取資料時，該寫入控制模組22將一實體位址及一讀取命令輸出至該NAND快閃記憶體11。

對該使用者區域32之存取與對該安全區域31之存取為相同的，除了不需要該第二驗證模組21處之一驗證程序之外。

上文所描述的已如圖10中顯示予以總結。圖10係顯示由該記憶體控制器10控制的該專用區域30與其他區域(該安全區域31及使用者區域32)間之差異之一表。

如圖10中顯示，該專用區域30經受一驗證程序，但不經受一ECC程序、耗損平均及隨機化。以4層級模式控制該

專用區域30。相反，其他區域31、32經受一驗證程序(如需要)。其他區域亦經受一L2P程序、一ECC程序、耗損平均及隨機化。以2層級模式控制用於該等區域31、32之資料。

在寫入模式中，保存在該專用區域30之該等記憶體單元中之資料量應大於保存在該等其他區域31、32中之資料量。舉例而言，不小於3層級資料可儲存在該專用區域30中之該等記憶體單元中且2層級資料可儲存在該等其他區域31、32中。即，可以一M位元模式(M係不小於2之一自然數)控制該專用區域30且可以一N位元模式(N係不小於1且滿足運算式N<M之一自然數)控制該等其他區域31、32。

用於該主機裝置4存取該專用區域30之一命令(該SD介面上定義的一命令)可不同於用以存取該等其他區域31、32之一命令。此能使該記憶體控制器10容易認知該存取係對該專用區域30之一存取。即使使用相同的命令，仍可基於一位址區分待存取之一區域。

1.4 NAND快閃記憶體11之記憶體空間

圖11係該NAND快閃記憶體11之一記憶體空間之一概念圖，其顯示該NAND快閃記憶體11中保存的資訊。

如圖11中顯示，該NAND快閃記憶體11儲存一啟動區段、FAT1、FAT2、一根目錄項、第一特有資訊及使用者資料。此外，在該NAND快閃記憶體11中，一特定區域係固定作為一專用區域30。如上文描述，在此區域中，寫入

用於產生第一特有資訊及第二特有資訊之資料。

該啟動區段、FAT1、FAT2及根目錄項係用於管理該NAND快閃記憶體11中記錄的檔案(資料)之管理資訊。圖11顯示作為一實例之一檔案分配表(FAT)檔案系統。該使用者資料包含內容(包含音樂及電影)及用於加密/解密該等內容之加密密鑰。

如上文描述，將該第一特有資訊寫入至該安全區域31中。將該FAT1、FAT2、根目錄項及使用者資料寫入至該使用者區域32中。

當存取該專用區域30時，既不執行一L2P程序也不執行耗損平均。即，分配至該專用區域30之記憶體塊係固定的(例如，BLK11至BLK14)。因此，當將資料寫入至該專用區域30時，將資料寫入至記憶體塊BLK11至BLK14之任一者。由該主機裝置4直接選擇待寫入資料之一地方。換言之，每次在相同記憶體單元上執行經實行用以產生第一特有資訊及第二特有資訊的複數個寫入及讀取操作。

相反，分配至其他區域的記憶體塊BLK不是固定的。當更新資料或完成耗損平均時，寫入資料之記憶體塊BLK始終改變。即，雖然邏輯位址本身保持不變，但其等之實體位址隨時間改變。

2.記憶卡1之操作

繼而，將參考圖12闡述產生並記錄第一特有資訊時記憶卡1之操作。圖12係闡述記憶體控制器10之該MPU 71之操作之一流程圖。

如圖12中顯示，首先，藉由該寫入裝置2之請求，該第一驗證模組20實行一驗證程序(圖3之步驟S10及圖12之步驟S40)。若驗證失敗，則該記憶體控制器10禁止該寫入裝置2存取該記憶卡1。

若驗證成功，則該記憶卡1接收來自該寫入裝置2之寫入命令、資料及位址(實體位址)(步驟S41)。接著，該記憶體控制器10將接收的資料寫入至對應於接收的位址之一區域(即，該專用區域30)中(步驟S42)。如上文描述，不執行一L2P程序、一ECC程序、耗損平均及(隨機化寫入資料之)一隨機化程序。

該記憶卡1進一步接收來自該寫入裝置2之一讀取命令及位址(實體位址)(步驟S43)。接著，該記憶體控制器10讀取來自對應於接收的位址之一區域(即，該專用區域30)之資料(步驟S44)。如上文描述，不實行該L2P程序、ECC程序及隨機化程序(或將所讀取的隨機化資料轉換回原始資料之一程序：一解碼程序)。

重複一特定次數(n次)上文的讀取及寫入操作(步驟S45)。在重複寫入該專用區域30之前，該記憶體控制器10發出一擦除命令及一位址至該專用區域30且擦除資料一次。該寫入裝置2之該CPU 40可發出一擦除命令及一位址至該專用區域30且擦除資料一次。由於上文程序，該寫入裝置2產生第一特有資訊。

此後，將該第一特有資訊寫入至該記憶卡1中。明確言之，藉由該寫入裝置2之請求，該第二驗證模組21與該寫

入裝置2協作執行一驗證程序(步驟S46)。若驗證失敗，則從此時開始禁止該寫入裝置2存取該記憶卡1。

若驗證成功，則該記憶卡1接收來自該主機裝置2之一寫入命令、資料(第一特有資訊)及一位址(邏輯位址)(步驟S47)。接著，該記憶體控制器10將接收的資料寫入至對應於接收的位址之一區域(即，該安全區域31)中(步驟S48)。此時，執行該L2P程序、ECC程序、耗損平均及隨機化。

上文程序之後，各種內容記錄在該記憶卡1中。

由該讀出裝置3存取該記憶卡1之程序幾乎係相同的。即，步驟S40至S46之程序之後，該記憶卡1接收一讀取命令及一位址(邏輯位址)。接著，該記憶卡1讀取來自該安全區域31之該第一特有資訊且輸出資訊至該讀出裝置3。

3.第二實施例之作用

根據該第二實施例之一記憶卡不僅能有效率產生特有資訊而且可抑制非法拷貝特有資訊。

首先，當存取該專用區域30時，該第二實施例之該記憶卡在該專用區域30上既不實行一L2P程序也不執行耗損平均。即，分配至該專用區域30之記憶體塊BLK係固定的。因此，在自產生第一特有資訊至產生第二特有資訊之時間期間，待寫入/讀出的記憶體單元始終係相同的。因此，可改良驗證該第二實施例之該記憶卡之方法之可靠性(即，藉由相互比較該第一特有資訊與該第二特有資訊而驗證該記憶卡之方法)。

當注意力僅集中於產生該第一特有資訊時，期望應在許

多位元中發生一錯誤。原因係若在該等位元之任一者中均不發生一錯誤，則沒有待附接一數位簽章之目標。在此態樣中，利用該第二實施例之該記憶卡1，該專用區域30不經受一ECC程序及/或一隨機化程序。此外，將具有比該使用者區域32及該安全區域31之該等記憶體單元中之位元數目較大的位元數目之資料寫入至該專用區域30之該等記憶體單元中。相應地，可增加該專用區域30中之錯誤發生率，其能使記錄裝置特有資訊有效率地產生。

可由另一方式實現增加該專用區域30中之錯誤發生率之方法。例如，一種方法係相比於其他區域31、32，改變施加至連接至該專用區域30中之該等記憶體單元之該等字線WL之電壓。明確言之，施加至待讀出之一字線之讀取電壓可變換至高於通常之一值。或者，在不改變該讀取電壓情況下寫入中的檢驗電壓可變換至低於通常之一值。

此外，增加該專用區域30中之錯誤發生率之方法可係將認為具有一較高錯誤發生率之一資料型樣寫入至該專用區域30中之該等記憶體單元中。利用該第二實施例之該記憶卡，因為在該專用區域30上不執行隨機化，所以可將任意資料型樣直接寫入至記憶體單元中。或者，若有在該專用區域30之區塊中錯誤發生率高之字線，則僅可使用此等字線。

此外，在該第二實施例中，在圖12之步驟S41至S45中已重複寫入並讀取資料。然而，不必要每次寫入資料。即，在第一次將資料寫入至該專用區域30中之後，資料可被讀

取一特定次數。因此，基於所讀取資料中發生的錯誤，可判定該記憶卡是否是一盜版卡。在此情況下，獲得防止記錄元件劣化之作用。此也適用於該記錄裝置之操作(圖4之步驟S21至S25)。

此外，當執行寫入以產生特有資訊(圖3中之步驟S12及圖4中之步驟S22)時，可使用該專用區域30之一部分(而不是全部)。接著，根據此後之情況，可改變待寫入用於產生特有資訊之資料之一地方。舉例而言，改變該地方之一準則係ECC之一錯誤校正率。明確言之，當在寫入某一地方之資料中ECC之錯誤校正數目超過一特定次數時，認為該區域係太頻繁發生錯誤之一地點。此後，使用另一地方作為用於產生特有資訊之一區域。

在該第二實施例中，已將特有資訊寫入該安全區域31中。然而，可將特有資訊寫入普通使用者區域32中。或者，可預先判定特有資訊係在記錄裝置間之特定資料且不記錄在一記憶卡中。即，可預先判定用作為特有資訊之資料且該寫入裝置與該讀出裝置可共用該資訊。當該讀出裝置讀取特有資訊時，准許該記憶卡保存作為特有資訊寫入的資料。或者，在該特有資訊不記錄在該記憶卡中之情況下，該讀出裝置可事先知道特有資訊。

[第三實施例]

繼而，將闡述根據一第三實施例之一記錄裝置、一寫入裝置、一讀出裝置及控制該記錄裝置之一方法。該第三實施例顯示該第一實施例及該第二實施例之內容之加密及解

密之一實例。

1.加密方法

首先，將參考圖13闡述一加密方法。圖13係一記憶卡1及一寫入裝置2之一方塊圖，其特別顯示加密所必要的資訊及處理之流程。

如圖13中顯示，該寫入裝置2具有一預設器件密鑰Kd且該記憶卡1具有密鑰管理資訊MKB(媒體密鑰塊)。該寫入裝置2讀取來自該記憶卡1之一MKB且使用其自己的器件密鑰Kd執行一MKB程序，藉此獲得一媒體密鑰Km(步驟S50)。

繼而，該寫入裝置2讀取來自該記憶卡1之一媒體識別符IDm且使用該媒體識別符IDm及該媒體密鑰Km執行一散列程序(步驟S51)。由於該散列程序，該寫入裝置2獲得一媒體特有密鑰Kmu。舉例而言，由該CPU 40實行上文程序。

此後，基於獲得的媒體特有密鑰Kmu，該寫入裝置2與該記憶卡1協作執行一驗證程序及密鑰交換。舉例而言，此由該等第二驗證模組43、21實行。由於驗證及密鑰交換，該寫入裝置2與該記憶卡1共用一會期密鑰Ks。當該寫入裝置2之該媒體特有密鑰Kmu符合該記憶體1中保存的該媒體特有密鑰Kmu時，此程序成功，結果係共用該會期密鑰Ks。

繼而，該寫入裝置2使用該媒體特有密鑰Kmu加密一使用者密鑰Ku(步驟S52)且藉由使用該會期密鑰Ks之密碼通信將經加密的密鑰寫入至該記憶卡1之該安全區域31中。

在圖13中，用該媒體特有密鑰Kmu加密的該使用者密鑰Ku表示為Enc(Kmu, Ku)。由圖1之該內容加密模組44之加密模組(未顯示)之任一者執行此加密。

此外，該寫入裝置2使用該使用者密鑰Ku加密一內容密鑰Kc(步驟S53)且將經加密的密鑰寫入至該記憶卡1之該使用者區域32中。在圖13中，用該使用者密鑰Ku加密的該內容密鑰Kc表示為Enc(Ku, Kc)。舉例而言，由一第一加密模組48執行該加密。

此外，該寫入裝置2使用該內容密鑰Kc加密內容(步驟S54)且將經加密的內容寫入至該記憶卡1之該使用者區域32中。在圖13中，用該內容密鑰Kc加密的內容表示為Enc(Ku, 內容)。舉例而言，由一第二加密模組49執行該加密。

2.解密方法

繼而，將參考圖14闡述一解密方法。圖14係一記憶卡1及一讀出裝置3之一方塊圖，其特別顯示解密所必要的資訊及處理之流程。

如圖14中顯示，該讀出裝置3如同在加密過程中與該記憶卡協作執行一驗證程序及密鑰交換。由該CPU 50及該第二驗證模組53實行至現在的程序。

繼而，該讀出裝置3讀取來自該記憶卡1之該安全區域31之一經加密的使用者密鑰Enc(Kmu, Ku)且使用其自身中保存的一媒體特有密鑰Kmu解密該經加密的密鑰(步驟S55)，藉此獲得一使用者密鑰Ku。由圖2之該內容解密模組54中

之解密模組(圖中未顯示)之任一者執行該解密。

此外，該讀出裝置3讀取來自該記憶卡1之該使用者區域32之一經加密的內容密鑰Enc(Ku, Kc)且使用該使用者密鑰Ku解密該經加密的內容密鑰(步驟S56)，藉此獲得一內容密鑰Kc。舉例而言，由一第一解密模組59執行該解密。

接著，該讀出裝置3讀取來自該記憶卡1之該使用者區域32之一經加密的內容Enc(Kc, 內容)(步驟S57)，藉此獲得內容。舉例而言，由一第二解密模組60執行該解密。

此外，可對已記錄的資料讀取一特定次數而不過度寫入，而不是每次在將資料寫入至該專用區域30時讀取該資料。因此，可使用一種使用所讀取資料中發生的錯誤之方法。在此情況下，因為不執行寫入，所以可防止記錄元件之劣化。此與該第二實施例中描述的相同。

3.第三實施例之作用

上文提到的方法可用於加密及解密內容。然而，該第三實施例僅係說明性且可使用各種適宜方法。

此外，可基於該第一特有資訊產生該記憶卡1之媒體識別符IDm。明確言之，在該第一實施例中闡述的圖3之程序之後，基於產生的第一特有資訊處理該記憶卡1中保存的該媒體識別符IDm。或者，可基於該第一特有資訊新產生一媒體識別符IDm。又或者，該第一特有資訊可用作為一媒體識別符IDm。此能進一步增加內容之保護。

此外，該寫入裝置可將分配至每一寫入裝置之一序號、時間及藉由序連序號而獲得之一值記錄在一數位簽章中，

且可使用該值作為一媒體識別符。此能使該寫入裝置防止其之媒體識別符偶然地與另一媒體之值符合。

[第四實施例]

繼而，將闡述根據一第四實施例之一記錄裝置。該第四實施例係使得該記錄裝置應用於該第一實施例至該第三實施例之一固態驅動器(SSD)。

圖15係顯示一SSD 100之組態之一方塊圖。如圖15中顯示，該SSD 100包含用於資料儲存之複數個NAND快閃記憶體(NAND記憶體)10、用於資料傳送或工作區域之一DRAM 101、用於控制此等之一驅動控制電路102、及一電源供應電路103。該驅動控制電路102輸出一控制信號用於控制該SSD 100外部提供的一狀態顯示LED。可使用一鐵電隨機存取記憶體(FeRAM)取代該DRAM 101。

該SSD 100經由一ATA介面(ATA I/F)將資料傳輸至一主機裝置(諸如一個人電腦)且自該主機裝置接收資料。該SSD 100經由一RS232C介面(RS232C I/F)將資料傳輸至一除錯單元且自該除錯單元接收資料。

該電源供應電路103接收一外部電源且使用該外部電源產生複數個內部電源。此等內部電源被供應至該SSD 100之各個部分。此外，該電源供應電路103偵測該外部電源之上升且產生一電源接通重設信號。該電源接通重設信號被發送至該驅動控制電路102。

圖16係顯示該驅動控制電路102之組態之一方塊圖。該驅動控制電路102包含一資料存取匯流排104、一第一電路

控制匯流排105及一第二電路控制匯流排106。

控制整個驅動控制電路102之一處理器107連接至該第一電路控制匯流排105。其中儲存用於各種管理程式(FW：韌體)之一啟動程式之一啟動ROM 108亦經由一ROM控制器109連接至該第一電路控制匯流排105。另外連接至該第一電路控制匯流排105的係一時脈控制器110，該時脈控制器110接收來自該電源供應電路103之一電源接通重設信號且供應一重設信號及一時脈信號至各個部分。

該第二電路控制匯流排106連接至該第一電路控制匯流排105。連接至該第二電路控制匯流排106的係供應一狀態顯示信號至一狀態顯示LED之一並聯IO(PIO)電路111及控制一RS232C介面之一串列IO(SIO)電路112。

一ATA介面控制器(ATA控制器)113、一第一錯誤檢查及校正(ECC)電路114、一NAND控制器115及一DRAM控制器119連接至該資料存取匯流排104與該第一電路控制匯流排105兩者。該ATA控制器113經由該ATA介面將資料傳輸至該主機裝置且自該主機裝置接收資料。用作為一資料工作區域之一SRAM 120經由該SRAM控制器121連接至該資料存取匯流排104。

該NAND控制器115包含與四個NAND記憶體10介接之一NAND介面電路(NAND I/F)118、一第二ECC電路117、及用於DMA傳送控制之一DMA控制器116，該DMA控制器116執行NAND記憶體與DRAM間之存取控制。

圖17係顯示該處理器107之組態之一方塊圖。該處理器

107包含一資料管理模組122、一ATA命令處理模組123、一安全管理模組124、一啟動載入器125、一初始化管理模組126及一除錯支援模組127。

該資料管理模組122經由該第一ECC電路控制NAND記憶體與DRAM間之資料傳送及關於一NAND晶片之各種功能。

該ATA命令處理模組123經由該ATA控制器113及該DRAM控制器119與該資料管理模組122協作實行一資料傳送程序。該安全管理模組124與該資料管理模組122及該ATA命令處理模組123協作管理各種安全資訊。該安全管理模組124執行由(舉例而言)該第二實施例中闡述的該第一驗證模組20及第二驗證模組實行的程序。

當打開電源時，該啟動載入器125將來自該NAND記憶體10之各種管理程式(FW)載入至該SRAM 120中。該初始化管理模組126初始化該驅動控制電路102中之各種控制器/電路。該除錯支援模組127處理經由該RS232C介面外部供應的除錯資料。

圖18係嵌有該SSD 100之一可攜式電腦200之一透視圖。該可攜式電腦200包含一本體201及一顯示單元202。該顯示單元202包含一顯示外殼203及設置在該顯示外殼203中之一顯示器件204。

該本體201包含一底板205、一鍵盤206及充當一指標器件之一觸控板207。該底板205容納一主電路板、一光碟器件(ODD)單元、一插卡槽及該SSD 100等等。

靠近該底板205之周邊壁提供該插卡槽。在該周邊壁中，製作一開口208以便面對該插卡槽。使用者可從該底板205外部穿過該開口208將一額外器件插入該插卡槽中。

該SSD 100可藉由嵌入該可攜式電腦200中用作為一習知HDD之一替代或藉由插入該可攜式電腦200之該插卡槽中用作為一額外器件。或者，該SSD 100可用作為一USB外部器件。此外，該第一實施例中闡述的該寫入裝置2及該讀出裝置3可嵌入該可攜式電腦200中。該可攜式電腦200可用作為內容記錄及再現器件，諸如透過網際網路及類似物散佈的電影。

圖19顯示嵌有該SSD 100之該可攜式電腦200之一系統組態。該可攜式電腦200包含一CPU 301、一北橋302、一主記憶體303、一視訊控制器304、一音訊控制器305、一南橋306、一BIOS-ROM 307、一SSD 100、一ODD單元308、一嵌入式控制器/鍵盤控制器IC(EC/KBC)309及一網路控制器310。

該CPU 301(其係用以控制該可攜式電腦200之操作而提供之一處理器)執行從該SSD 100載入至該主記憶體303中之一作業系統(OS)。此外，當該ODD單元308致能在安裝的光碟上執行一讀取程序及一寫入程序之至少一者時，該CPU 301實行該程序。

此外，該CPU 301亦執行該BIOS-ROM 307中儲存的一系統基礎輸入輸出系統(BIOS)。該系統BIOS係用於控制該可攜式電腦200之硬體之一程式。

該北橋302係連接該CPU 301之局部匯流排及該南橋306之一橋接器件。該北橋302容納一記憶體控制器，該記憶體控制器執行該主記憶體303之存取操作。

該北橋302亦具有經由一加速圖形埠(AGP)匯流排與該視訊控制器304通信且進一步與該音訊控制器305通信之功能。

該主記憶體303暫時儲存一程式或資料且作用為該CPU 301之一工作區域。舉例而言，該主記憶體303係一DRAM。

該視訊控制器304係控制用作為該可攜式電腦200之一顯示監視器之一顯示單元(LCD)202之一視訊再現控制器。

該音訊控制器305係控制該可攜式電腦200之一揚聲器311之一音訊再現控制器。

該南橋306控制一少接腳數(LPC)匯流排上之每一器件及一周邊組件互連(PCI)匯流排上之每一器件。該南橋306亦經由該ATA介面控制該SSD 100、用於儲存各種類型的軟體及資料之一儲存單元。

該可攜式電腦200以區段存取該SSD 100。一寫入命令、一讀取命令、一快閃命令及類似物經由該ATA介面被輸入至該SSD 100。

該南橋306亦具有執行該BIOS-ROM 307及ODD單元308之存取控制之功能。

該EC/KBC 309係一單晶片微電腦，用於電源管理之一嵌入式控制器及用於控制該鍵盤(KB)206及觸控板207之一

鍵盤控制器已經整合至該單晶片微電腦中。

該EC/KBC 309具有根據一電源按鈕312之使用者操作而接通或關斷該可攜式電腦200之電源之功能。該網路控制器310係與一外部網路(諸如網際網路)通信之一通信器件。

在上文組態中，圖15中顯示的該等NAND快閃記憶體10之至少一者具有一專用區域30(及一安全區域31)。接著，該寫入裝置2及該讀出裝置3存取該SSD之該專用區域(及安全區域31)且判定該SSD是否是一合法記錄媒體。

該第一實施例至該第三實施例不僅可應用於該SSD而且可應用於其他記錄媒體，包含一硬碟或一DVD。

[修改及其他]

如上文描述，根據該第一實施例至第四實施例之一記錄裝置包含：一記憶體11，其能夠記錄資料；及一控制器10，其將該記憶體11劃分成一第一區域30及一第二區域31且控制資料之記錄。該控制器10在不對外部供應的資料執行錯誤校正編碼及一邏輯位址至一實體位址之位址轉換情況下，將該外部供應的資料寫入至該第一區域30中。該資料經受錯誤校正編碼及位址轉換且所得資料被寫入至該第二區域31中。

此外，根據該第一實施例至第四實施例之一寫入裝置2包含提供資料之一提供模組47及一處理模組46。該處理模組46將由該提供模組47提供的資料寫入至該記錄裝置1之該第一區域30中、讀取寫入資料、比較該寫入資料與所讀取資料且將基於前者不同於後者之資料位置之資訊(第一

特有資訊)寫入至該記錄裝置1之該第二區域31中。

此外，根據該第一實施例至第四實施例之一讀出裝置3包括提供資料之一提供模組57、一處理模組56及一比較模組58。該處理模組56將由該提供模組57提供的資料寫入至該記錄裝置1之該第一區域30中、讀取寫入資料、比較該寫入資料與所讀取資料、且基於前者不同於後者之資料位置產生第一資訊(第二特有資訊)。該比較模組讀取來自該記錄裝置1之該第二區域31之第二資訊(第一特有資訊)、比較該第二資訊與由該處理模組56產生的該第一資訊(第二特有資訊)、且基於比較結果判定該記錄裝置1是否是一合法記錄裝置。

利用上文組態，可抑制內容資料之未授權使用。實施例並不限於上文的實施例且可經各種修改。

如上文描述，該記錄裝置1並不限於一SD記憶卡且可係能夠儲存資料之其他記錄媒體。該半導體記憶體並不限制於一NAND快閃記憶體且可係一NOR快閃記憶體或其他適宜之半導體記憶體。該記錄裝置1並不限於一卡器件且可應用於多種記錄媒體，包含一磁性記錄媒體及一光學記錄媒體。

此外，期望當產生該第一特有資訊及該第二特有資訊時應發生一特定數目個錯誤。因此，較佳使用一種使得在該專用區域30中比在該安全區域31及該使用者區域32中更易於發生一錯誤之方法作為將資料寫入至該專用區域30或自該專用區域30讀取資料之一方法。雖然在該等實施例中，

不執行耗損平均、ECC處理或隨機化之一方法已經闡述為上文方法之一實例，但可應用另一方法。例如，在一快閃記憶體中，可使施加至一記憶體單元之閘極(字線)之電壓在該專用區域30中高於該安全區域31及該使用者區域32中。此能使該專用區域30中之該等記憶體單元上之應力更大。此外，寫入具有一系列「1」或「0」之資料亦能使錯誤發生率增加。相應地，可使用所有位元皆為「1」之資料或所有位元皆為「0」之資料。或者，可使用不少於一特定數目個連續「1」或「0」之資料。

雖然在上文實施例中，已使用一資訊站終端、一內容提供者或一內容再現器件作為該寫入裝置2之一實例，但可使用另一適宜器件。例如，可使用記憶卡1之製造者方面之一適宜器件作為該寫入裝置2之一實例。在此情況下，製造者將第一特有資訊寫入至該記憶卡1中且銷售該卡。或者，可使用一內容提供者之組織方面之一適宜器件作為該寫入裝置2之一實例。在此情況下，經由網際網路或類似物可將第一特有資訊寫入至由一使用者購買的該記憶卡1中。當該寫入裝置2僅提供第一特有資訊而不提供內容時，不需要該內容加密模組44。

此外，已使用一內容再現器件作為該讀出裝置3之一實例。然而，可使用另一適宜器件作為該讀出裝置3之一實例。若不使用一內容再現器件，則不需要解密模組。

此外，時間、日期及環境溫度之至少一者可包含在附接至該第一特有資訊之一數位簽章中。例如，當包含時間或

日期且自時間或日期包含在該數位簽章中起已經過一段特定時間時，假設不考慮該第一特有資訊與該第二特有資訊之比較結果，且應更確實阻止一非法拷貝之時期已經過去，則該簽章檢驗模組55可准許再現內容。或者，此時，可更新該數位簽章。即，可新產生一簽章且將新產生的數位簽章寫入至該記錄裝置中。

此外，當溫度資訊包含在該數位簽章中時，可在複數個溫度下產生第一特有資訊。例如，在一高溫下產生的第一特有資訊及在一低溫下產生的第一特有資訊可記錄在該專用區域30中。當在該讀出裝置3處執行檢驗時，可使用更接近當前溫度之任一第一特有資訊。取決於情況，首先，當在該讀出裝置3處執行檢驗時，可檢查該數位簽章中之溫度且在經設定用於檢查溫度之環境溫度下實行圖4之程序。當溫度資訊包含在該數位簽章中時，該寫入裝置2及該讀出裝置3之每一者中需要一溫度感測器。雖然該寫入裝置2與該讀出裝置3均不具有一溫度感測器，但可自另一器件獲得溫度資訊。例如，該第四實施例中闡述的該SDD中具有一溫度感測器。因此，在圖3及圖4之程序中，可將該SDD處測量的溫度輸出至該寫入裝置2及該讀出裝置3。

此外，關於將資料寫入至該專用區域30中使用的電壓之資訊(例如，字線電壓)可包含在該數位簽章中。在此情況下，在該讀出裝置3中，首先，可檢查來自該數位簽章之該字線電壓且可使用該字線電壓將資料寫入至該專用區域30中。

此外，在該第三實施例中，該第一特有資訊亦用作為一媒體識別符IDm。然而，該第一特有資訊在各種應用中可用作為每一記憶卡1特有的資訊。此外，包含在該第一特有資訊及該第二特有資訊中的內容並不限於錯誤位置且可係基於錯誤位置的一記憶卡1特有的任何適宜資訊。

雖然已描述某些實施例，但此等實施例僅呈現作為實例且並不意欲限制本發明之範圍。的確，可以各種其他形式體現本文描述的新穎實施例；此外，在不背離本發明之精神情況下可作出本文描述的實施例之形式之各種省略、取代及改變。隨附申請專利範圍及其等之等效物意欲涵蓋落在本發明之範圍及精神內之此等形式或修改。

【圖式簡單說明】

圖1係根據一第一實施例之一記錄裝置及一寫入裝置之一方塊圖；

圖2係根據該第一實施例之一記錄裝置及一讀出裝置之一方塊圖；

圖3及圖4分別係用以闡述根據該第一實施例之該寫入裝置及該讀出裝置之操作之流程圖；

圖5及圖6分別係用以闡述根據該第一實施例之一寫入方法及一讀取方法之具體實例之概念圖；

圖7係根據該第一實施例之該記錄裝置之一方塊圖；

圖8及圖9係根據一第二實施例之一記錄裝置之方塊圖；

圖10係顯示控制根據該第二實施例之該記錄裝置之一方法之一表；

圖11係根據該第二實施例之該記錄裝置之一記憶體空間之一概念圖；

圖12係用以闡述根據該第二實施例之該記錄裝置之操作之一流程圖；

圖13係根據一第三實施例之一記錄裝置及一寫入裝置之一方塊圖；

圖14係根據該第三實施例之一記錄裝置及一讀出裝置之一方塊圖；

圖15係根據一第四實施例之一記錄裝置之一方塊圖；

圖16係根據該第四實施例之一驅動控制電路之一方塊圖；

圖17係根據該第四實施例之一處理器之一方塊圖；

圖18係根據該第四實施例之一個人電腦之一透視圖，其顯示個人電腦之外觀；及

圖19係顯示根據該第四實施例之該個人電腦之一內部組態之一方塊圖。

【主要元件符號說明】

1	記憶卡
1-1	記憶卡
1-2	非法拷貝的記憶卡/記憶卡
2	寫入裝置
3	讀出裝置
4	主機裝置
5	匯流排介面

10	記憶體控制器
10-1	控制器
11	NAND快閃記憶體
12	資料匯流排
20	第一驗證模組
21	第二驗證模組
22	寫入控制模組
23	邏輯位址至實體位址轉換模組(L2P處理模組)
24	錯誤校正編碼模組/ECC模組
25	耗損平均控制模組
26	隨機化控制模組
30	專用區域
30-1	專用區域
30-2	專用區域
31	安全區域
31-1	安全區域
32	使用者區域
32-1	使用者區域
40	CPU
41	產生模組
42	第一驗證模組
43	第二驗證模組
44	內容加密模組

45	簽章產生模組
46	錯誤位置資訊處理模組/處理模組
46a	暫時記憶體
47	寫入資料提供模組/提供模組
48	第一加密模組
49	第二加密模組
50	CPU
51	判定模組
52	第一驗證模組
53	第二驗證模組
54	內容解密模組
55	簽章檢驗模組
56	錯誤位置資訊處理模組/處理模組
56a	暫時記憶體
57	寫入資料提供模組/提供模組
58	比較模組
59	第一解密模組
60	第二解密模組
70	SD卡介面
71	MPU
72	預記錄媒體拷貝保護(CPRM)電路
73	ROM
74	RAM
75	NAND介面

76	內部匯流排
80	記憶體單元陣列
81	列解碼器
82	頁面緩衝器
83	NAND介面
90	內容
91	第一特有資訊
92	媒體特有密鑰
93	第二特有資訊
100	SSD
101	DRAM
102	驅動控制電路
103	電源供應電路
104	資料存取匯流排
105	第一電路控制匯流排
106	第二電路控制匯流排
107	處理器
108	啟動ROM
109	ROM控制器
110	時脈控制器
111	並聯IO(PIO)電路
112	串列IO(SIO)電路
113	ATA介面控制器(ATA控制器)
114	第一錯誤檢查及校正(ECC)電路

115	NAND控制器
116	DMA控制器
117	第二ECC電路
118	NAND介面電路(NAND I/F)
119	DRAM控制器
120	SRAM
121	SRAM控制器
122	資料管理模組
123	ATA命令處理模組
124	安全管理模組
125	啟動載入器
126	初始化管理模組
127	除錯支援模組
200	可攜式電腦
201	本體
202	顯示單元
203	顯示外殼
204	顯示器件
205	底盤
206	鍵盤
207	觸控板
208	開口
301	CPU
302	北橋

303	主記憶體
304	視訊控制器
305	音訊控制器
306	南橋
307	BIOS-ROM
308	光碟器件(ODD)單元
309	嵌入式控制器/鍵盤控制器IC(EC/KBC)
310	網路控制器
311	揚聲器
312	電源按鈕
IDm	媒體識別符
Kc	內容密鑰
Km	媒體密鑰
Kmu	媒體特有密鑰
Ks	會期密鑰
Ku	使用者密鑰
MKB	媒體密鑰塊

201203092

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：100109460

※ 申請日： 100. 3. 18　　※IPC 分類：G06F 3/06 (2006.01)
G06F 21/02 (2006.01)

一、發明名稱：（中文/英文）

記錄裝置、寫入裝置、讀出裝置及控制記錄裝置之方法

RECORDING APPARATUS, WRITING APPARATUS, READING APPARATUS, AND METHOD OF CONTROLLING RECORDING APPARATUS

二、中文發明摘要：

根據一實施例，一種記錄裝置包含一記憶體及一控制器。該記憶體能夠記錄資料。該控制器將該記憶體劃分成一第一區域及一第二區域且控制資料之記錄。該控制器在不對外部供應的資料執行錯誤校正編碼及一邏輯位址至一實體位址之位址轉換情況下將該外部供應的資料寫入至該第一區域中，且該控制器對該資料執行錯誤校正編碼及位址轉換，且接著將所得資料寫入至該第二區域中。

三、英文發明摘要：

According to one embodiment, a recording apparatus includes a memory and a controller. The memory is capable of recording data. The controller divides the memory into a first region and a second region and controls the recording of the data. The controller writes externally supplied data into the first region without performing error correction coding and address conversion of a logical address into a physical address for the externally supplied data, and performs the error correction coding and the address conversion for the data, and then writes resulting data into the second region.

七、申請專利範圍：

1. 一種記錄裝置，其包括：

一記憶體，其能夠記錄資料；及

一控制器，其將該記憶體劃分成一第一區域及一第二區域且控制該資料之記錄，

其中該控制器在不對外部供應的資料執行錯誤校正編碼及一邏輯位址至一實體位址之位址轉換情況下將該外部供應的資料寫入至該第一區域中，且

該控制器對該資料執行錯誤校正編碼及位址轉換，且接著將所得資料寫入至該第二區域中。

2. 一種記錄裝置，其包括：

一記憶體，其能夠記錄資料；及

一控制器，其將該記憶體劃分成一第一區域及一第二區域且控制該資料之記錄，

其中該控制器將內容資料及關於該第一區域之寫入或讀取錯誤資訊寫入至該第二區域中，且

該寫入或讀取錯誤資訊用於判定是否准許或禁止存取該記憶體。

3. 如請求項1或2之裝置，其中該控制器不在該第一區域上執行耗損平均而在該第二區域上執行耗損平均。

4. 如請求項1或2之裝置，其中該記憶體包含各自能夠保存資料之複數個記憶體單元，且

該控制器將M位元資料(M係不小於2之一自然數)寫入至該第一區域中之該等記憶體單元之每一者中且將N位

元資料(N係不小於1且滿足運算式N<M之一自然數)寫入至該第二區域中之該等記憶體單元中。

5. 如請求項1或2之裝置，其中該記憶體包含各自能夠保存資料之複數個記憶體單元，且

該控制器造成該第一區域中之該等記憶體單元保存不小於3層級資料且造成該第二區域中之該等記憶體單元之每一者保存2層級資料。

6. 如請求項1或2之裝置，其中該控制器不隨機化該第一區域中之資料而隨機化該第二區域中之資料。

7. 如請求項1之裝置，其中該控制器具有一第一操作模式及一第二操作模式，

在該第一操作模式中，自外部接受該記憶體之一實體位址之一輸入且存取由該實體位址直接指定的一區域，且

在該第二操作模式中，自外部接受該記憶體之一邏輯位址之輸入且存取藉由將該邏輯位址轉換成一實體位址而指定的一區域。

8. 一種寫入裝置，其包括：

一提供模組，其提供資料；及

一處理模組，其將由該提供模組提供的該資料寫入至一記錄裝置之一第一區域中、讀取該寫入的資料、比較該寫入的資料與該所讀取資料、且將基於該寫入的資料與該所讀取資料彼此不同之一資料位置之資訊寫入至該記錄裝置之一第二區域中。

9. 如請求項8之裝置，其中該處理模組執行複數次寫入、

讀取及比較且不少於一特定次數地產生基於該寫入的資料與該所讀取資料彼此不同之一位置之該資訊。

10. 如請求項8之裝置，其中該處理模組藉由使用一實體位址存取該第一區域且藉由使用一邏輯位址存取該第二區域。

11. 如請求項8之裝置，其進一步包括：

一簽章產生模組，其產生用於由該處理模組產生的該資訊之一數位簽章且將該簽章附接至該資訊，

其中該處理模組將附接數位簽章的資訊寫入至該記錄裝置中。

12. 如請求項11之裝置，其中該數位簽章包含一日期、一時間及附接該簽章時之一環境溫度之至少一者。

13. 一種讀出裝置，其包括：

一提供模組，其提供資料；

一處理模組，其將由該提供模組提供的該資料寫入至一記錄裝置之一第一區域中、讀取該寫入的資料、比較該寫入的資料與該所讀取資料、且產生基於該寫入的資料與該所讀取資料彼此不同之一資料位置之第一資訊；及

一比較模組，其讀取來自該記錄裝置之一第二區域之第二資訊、比較該第二資訊與由該處理模組產生的該第一資訊、且根據比較結果判定該記錄裝置是否是一合法記錄裝置。

14. 如請求項13之裝置，其中該處理模組執行複數次寫入、讀取及比較且不少於一特定次數地產生基於該寫入的資

料與該所讀取資料彼此不同之一位置之該第一資訊。

15. 如請求項13之裝置，其中該處理模組藉由使用一實體位址存取該第一區域且藉由使用一邏輯位址存取該第二區域。

16. 如請求項13之裝置，其進一步包括：一簽章檢驗模組，其檢驗附接至該第二資訊之一數位簽章是否是正確的且根據檢驗結果判定該記錄裝置是否是一合法記錄裝置。

17. 如請求項13之裝置，其中該第二資訊係基於將資料寫入至該第一區域或自該第一區域讀取資料失敗之一資料位置之資訊且早於該第一資訊而產生。

18. 一種控制一記錄裝置之方法，其包括：

將資料寫入至一記錄裝置之一第一區域中；

讀取該寫入的資料；

比較該寫入的資料與該所讀取資料且偵測該寫入的資料與該所讀取資料彼此不同之一資料位置；

基於偵測的該資料位置產生第一資訊；且

將該第一資訊寫入至該記錄裝置之一第二區域中。

19. 一種控制一記錄裝置之方法，其包括：

將資料寫入至一記錄裝置之一第一區域中；

讀取該寫入的資料；

比較該寫入的資料與該所讀取資料且偵測該寫入的資料與該所讀取資料彼此不同之一資料位置；

基於偵測的該資料位置產生第一資訊；

讀取來自該記錄裝置之一第二區域之第二資訊；及

比較該第一資訊與該第二資訊且基於比較結果判定該記錄裝置是否是一合法記錄裝置。

20. 如請求項18或19之方法，其進一步包括：複數次地寫入並讀取資料且偵測資料位置，

其中基於複數次偵測資料位置之結果產生該第一資訊。

21. 如請求項20之方法，其中每次將具有相同位址之資料寫入至相同記憶體單元中。

八、圖式：

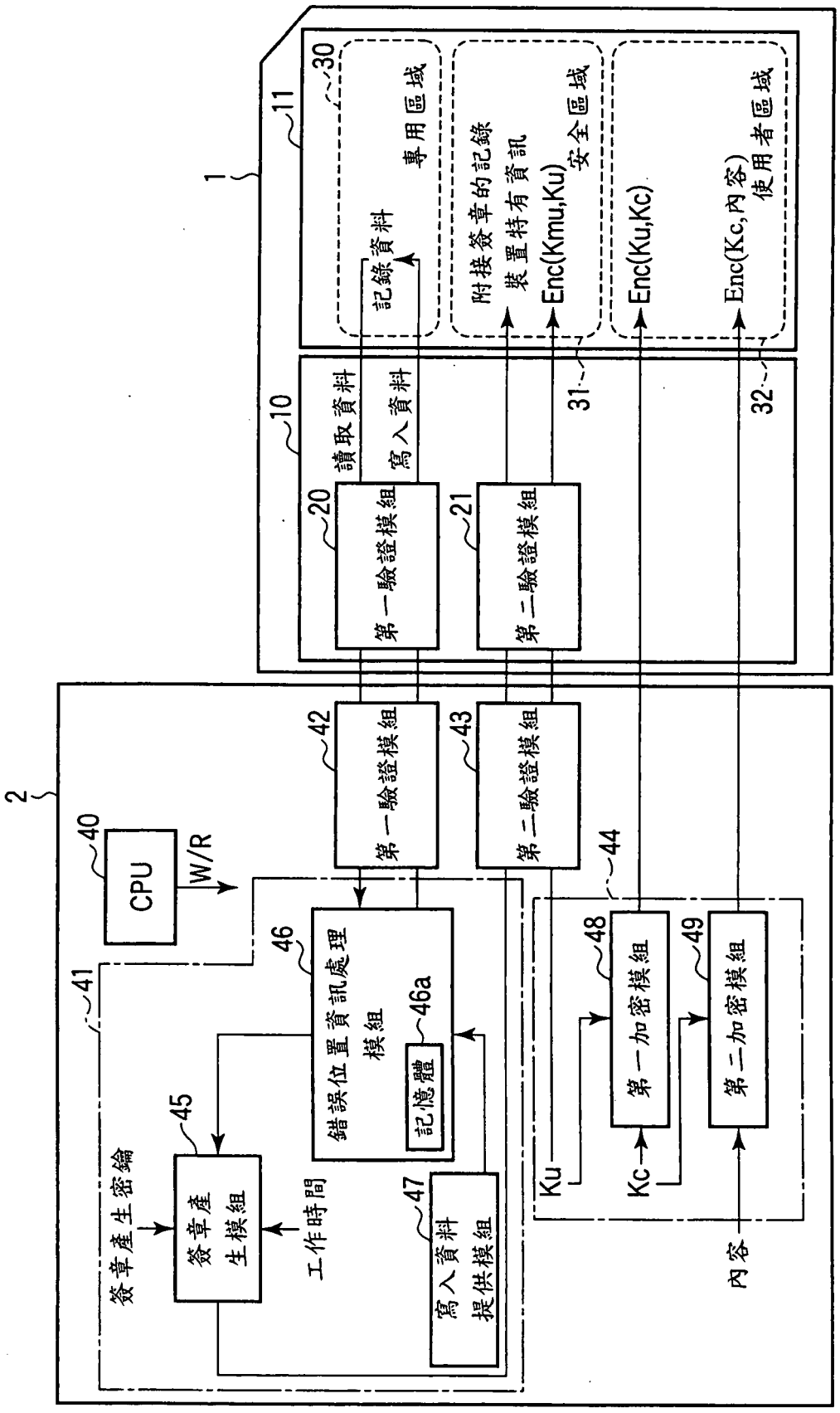

1
11
30
專用區域
記錄資料
附接簽章的記錄
裝置特有資訊
安全區域
Enc(Kmu,Ku)
Enc(Ku,Kc)
Enc(Kc,內容)
使用者區域
10
讀取資料
寫入資料
31
32
20
第一驗證模組
21
第二驗證模組
2
42
第一驗證模組
43
第二驗證模組
40
CPU
W/R
44
41
簽章產生密鑰
45
簽章產生模組
工作時間
46
錯誤位置資訊處理模組
46a
記憶體
47
寫入資料提供模組
48
第一加密模組
49
第二加密模組
Ku
Kc
內容

圖 1

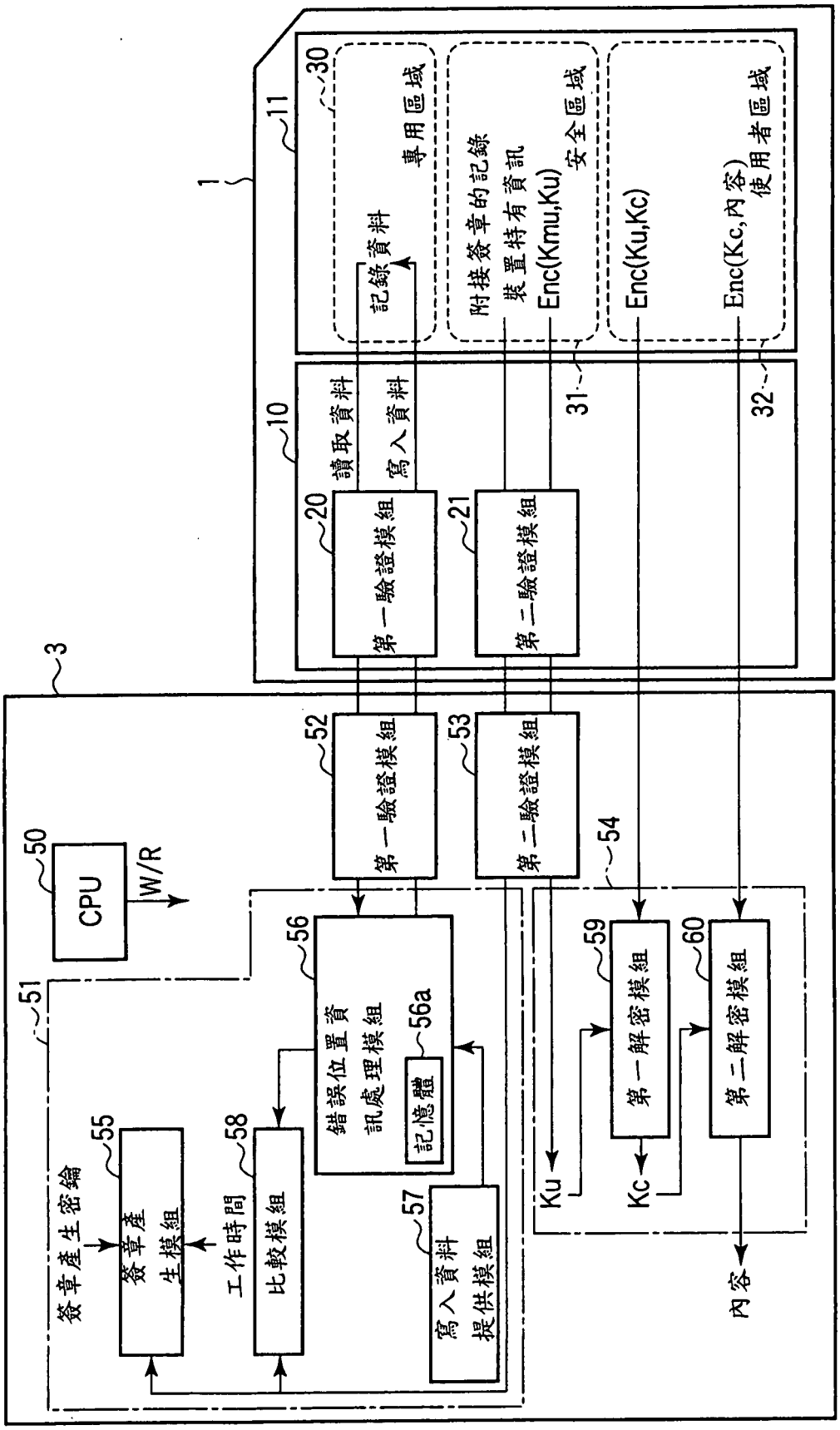

1
11
30
專用區域
記錄資料
附接簽章的記錄
裝置特有資訊
Enc(Kmu,Ku)
安全區域
Enc(Ku,Kc)
Enc(Kc,內容)
使用者區域
10
讀取資料
寫入資料
20
第一驗證模組
21
第二驗證模組
31
32
3
52
第一驗證模組
53
第二驗證模組
54
50
CPU
W/R
51
簽章產生密鑰
55
簽章產生模組
工作時間
58
比較模組
56
錯誤位置資訊處理模組
56a
記憶體
57
寫入資料提供模組
59
第一解密模組
60
第二解密模組
Ku
Kc
內容

圖 2

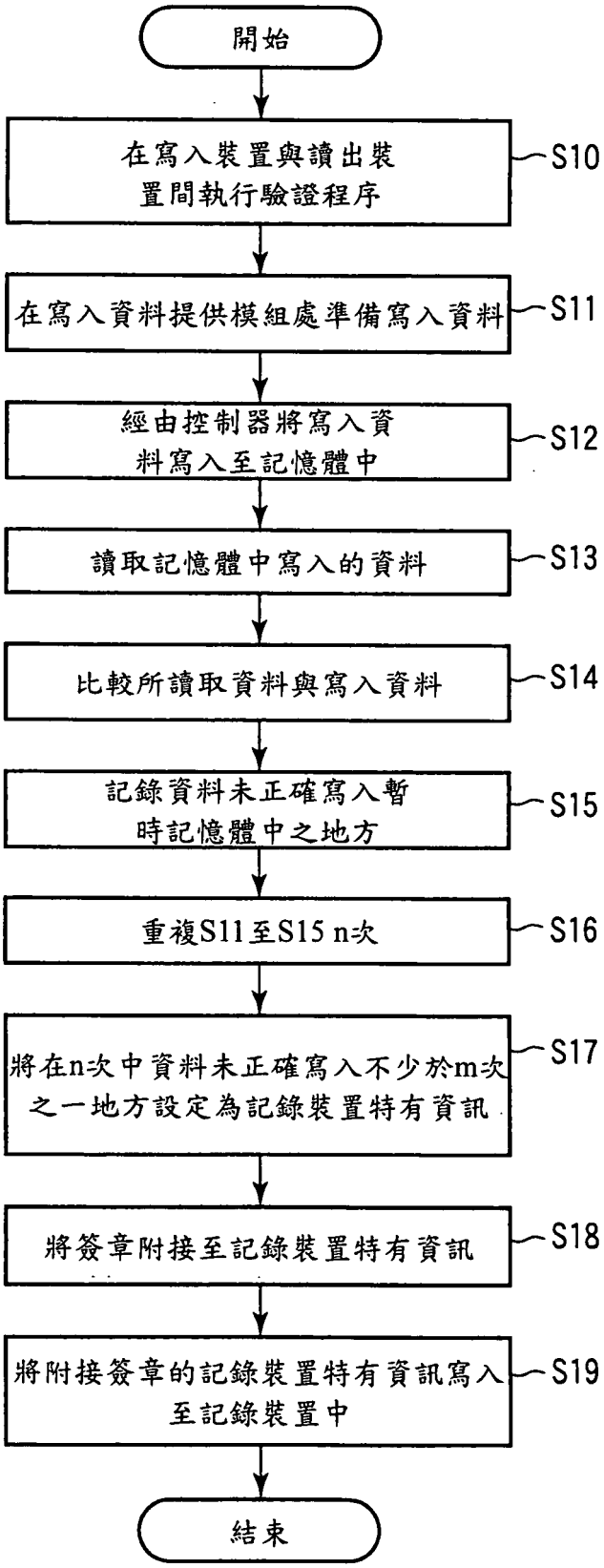

開始
在寫入裝置與讀出裝置間執行驗證程序
S10
在寫入資料提供模組處準備寫入資料
S11
經由控制器將寫入資料寫入至記憶體中
S12
讀取記憶體中寫入的資料
S13
比較所讀取資料與寫入資料
S14
記錄資料未正確寫入暫時記憶體中之地方
S15
重複S11至S15 n次
S16
將在n次中資料未正確寫入不少於m次之一地方設定為記錄裝置特有資訊
S17
將簽章附接至記錄裝置特有資訊
S18
將附接簽章的記錄裝置特有資訊寫入至記錄裝置中
S19
結束

圖 3

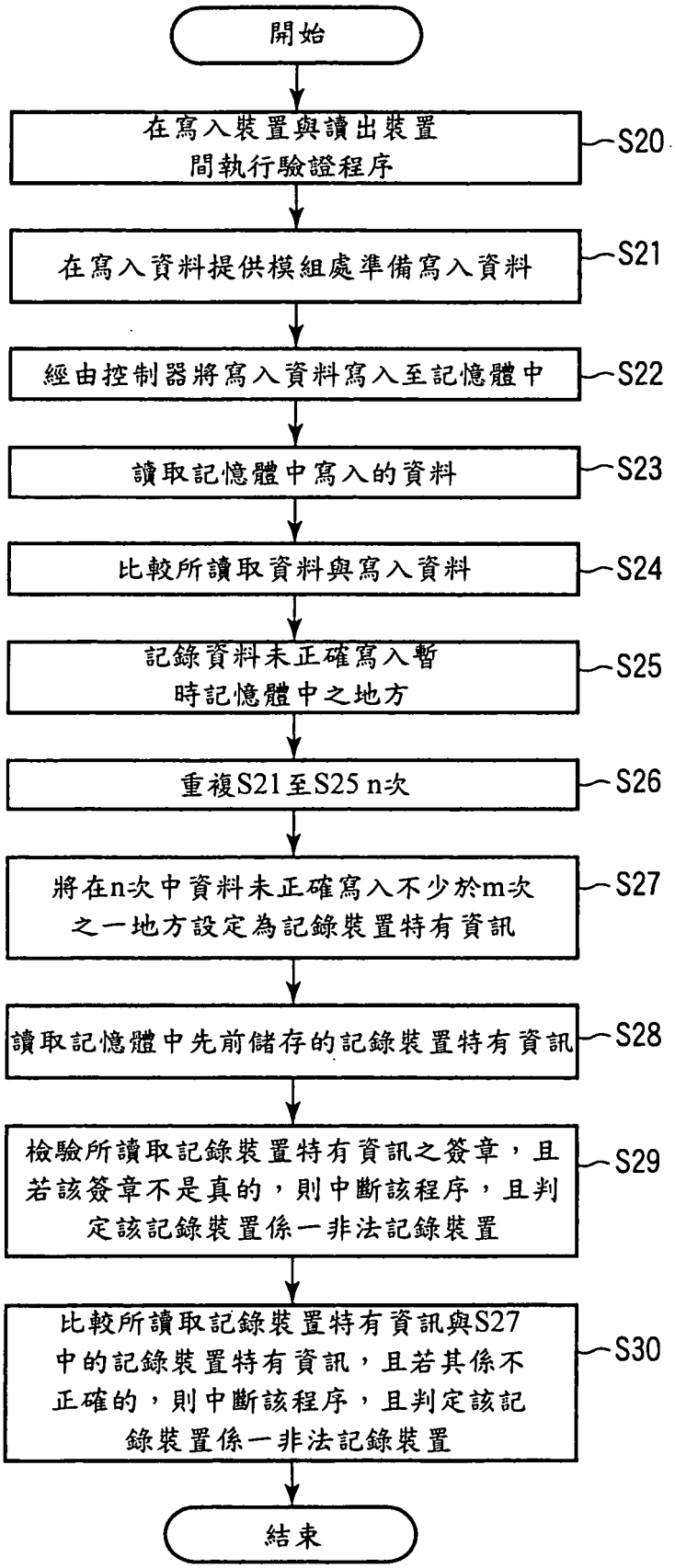

開始
在寫入裝置與讀出裝置間執行驗證程序
S20
在寫入資料提供模組處準備寫入資料
S21
經由控制器將寫入資料寫入至記憶體中
S22
讀取記憶體中寫入的資料
S23
比較所讀取資料與寫入資料
S24
記錄資料未正確寫入暫時記憶體中之地方
S25
重複S21至S25 n次
S26
將在n次中資料未正確寫入不少於m次之一地方設定為記錄裝置特有資訊
S27
讀取記憶體中先前儲存的記錄裝置特有資訊
S28
檢驗所讀取記錄裝置特有資訊之簽章，且若該簽章不是真的，則中斷該程序，且判定該記錄裝置係一非法記錄裝置
S29
比較所讀取記錄裝置特有資訊與S27中的記錄裝置特有資訊，且若其係不正確的，則中斷該程序，且判定該記錄裝置係一非法記錄裝置
S30
結束

圖 4

次數	寫入資料 → 讀取資料	暫時記憶體46a中的資訊 (發生錯誤的位元位置)
第一次	0000 0000 0000 0000 → 0000 0100 0000 0001	6, 16
第二次	1111 1111 1111 1111 → 1111 1011 1011 1100	6, 16/ 6, 10, 15, 16
第三次	1111 0000 0000 0000 → 1101 0100 0000 0001	6, 16/ 6, 10, 15, 16/ 3, 6, 16
第四次	0000 1111 0000 0000 → 0000 1011 0000 1001	6, 16/ 6, 10, 15, 16/ 3, 6, 16/ 6, 13, 16
第五次	0000 0000 1111 0000 → 0000 0100 1010 0001	**6,16/6**,10,15,**16/3,6,16/6**,13,**16/6**,10,12,**16**

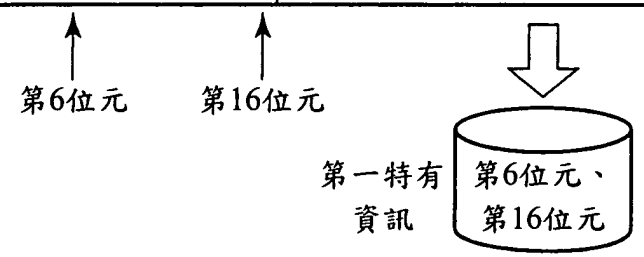


圖 5

次數	寫入資料 → 讀取資料	暫時記憶體56a中的資訊 (發生錯誤的位元位置)
第一次	0000 0000 0000 0000 → 0000 0100 0000 0001	6, 16
第二次	1111 1111 1111 1111 → 1101 1011 1011 1110	6, 16/ 3, 6, 10, 16
第三次	1111 0000 0000 0000 → 1111 0100 0010 0001	6, 16/ 3, 6, 10, 16/ 3, 6, 11, 16
第四次	0000 1111 0000 0000 → 1000 1111 0000 1001	6, 16/ 3, 6, 10, 16/ 3, 6, 11, 16/ 1, 13, 16
第五次	0000 0000 1111 0000 → 0001 0100 1011 1001	**6,16**/3,**6**,10,**16**/3,**6**,11,**16**/1,13,**16**/4,**6**,10,13,**16**

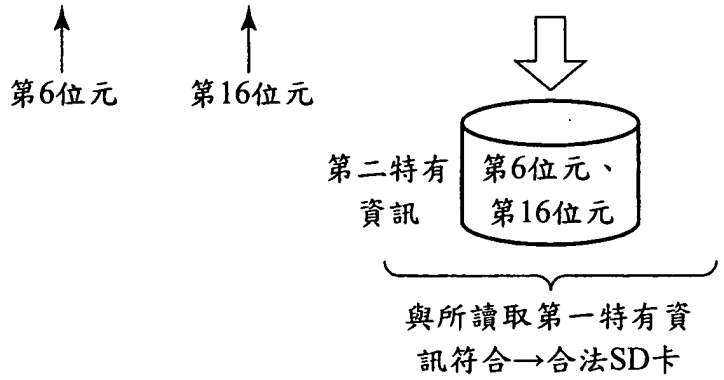


圖 6

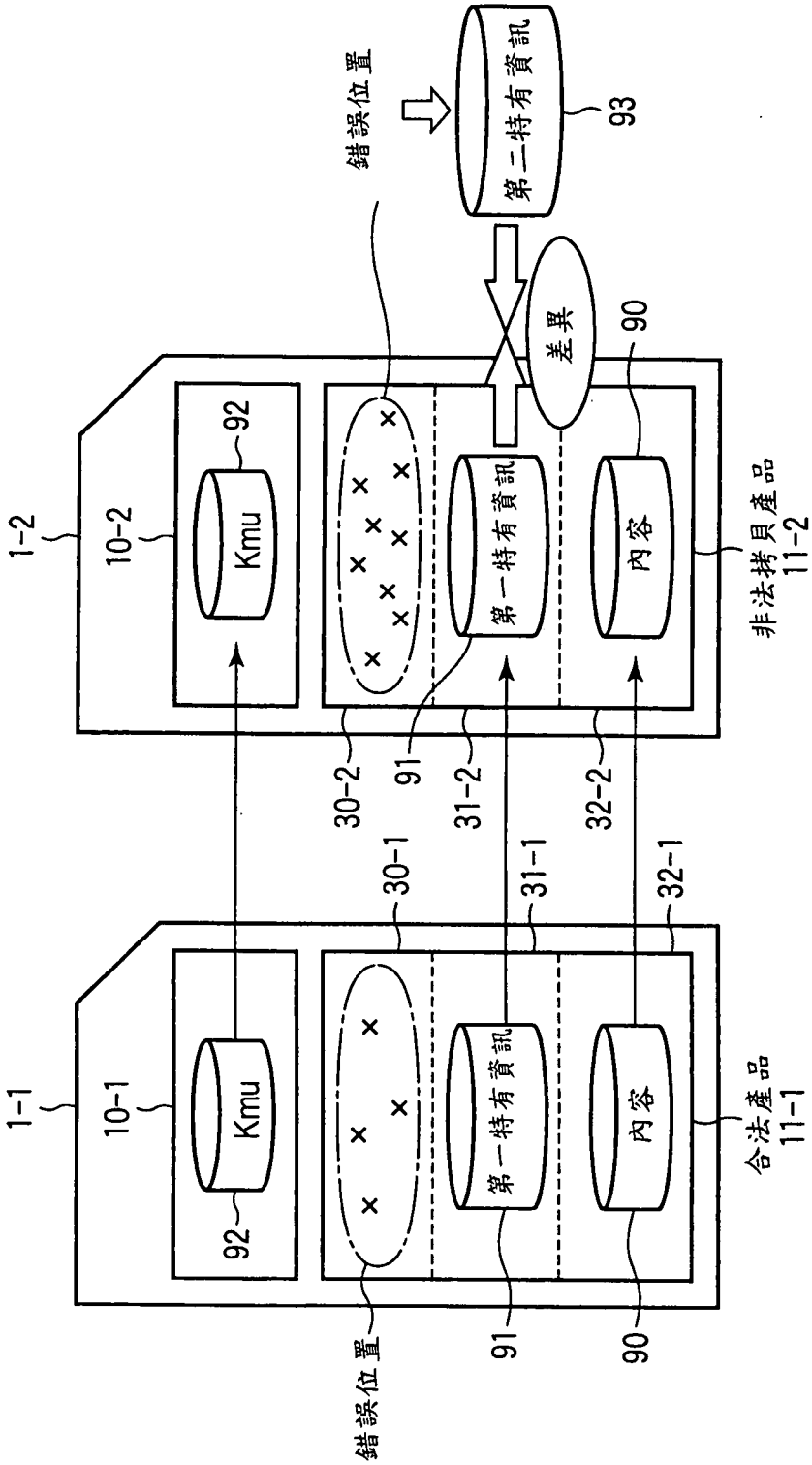

1-1
10-1
Kmu
92
第一特有資訊
內容
合法產品
11-1
30-1
31-1
32-1
錯誤位置
91
90
1-2
10-2
Kmu
92
第一特有資訊
內容
非法拷貝產品
11-2
30-2
31-2
32-2
91
差異
90
錯誤位置
第二特有資訊
93

圖 7

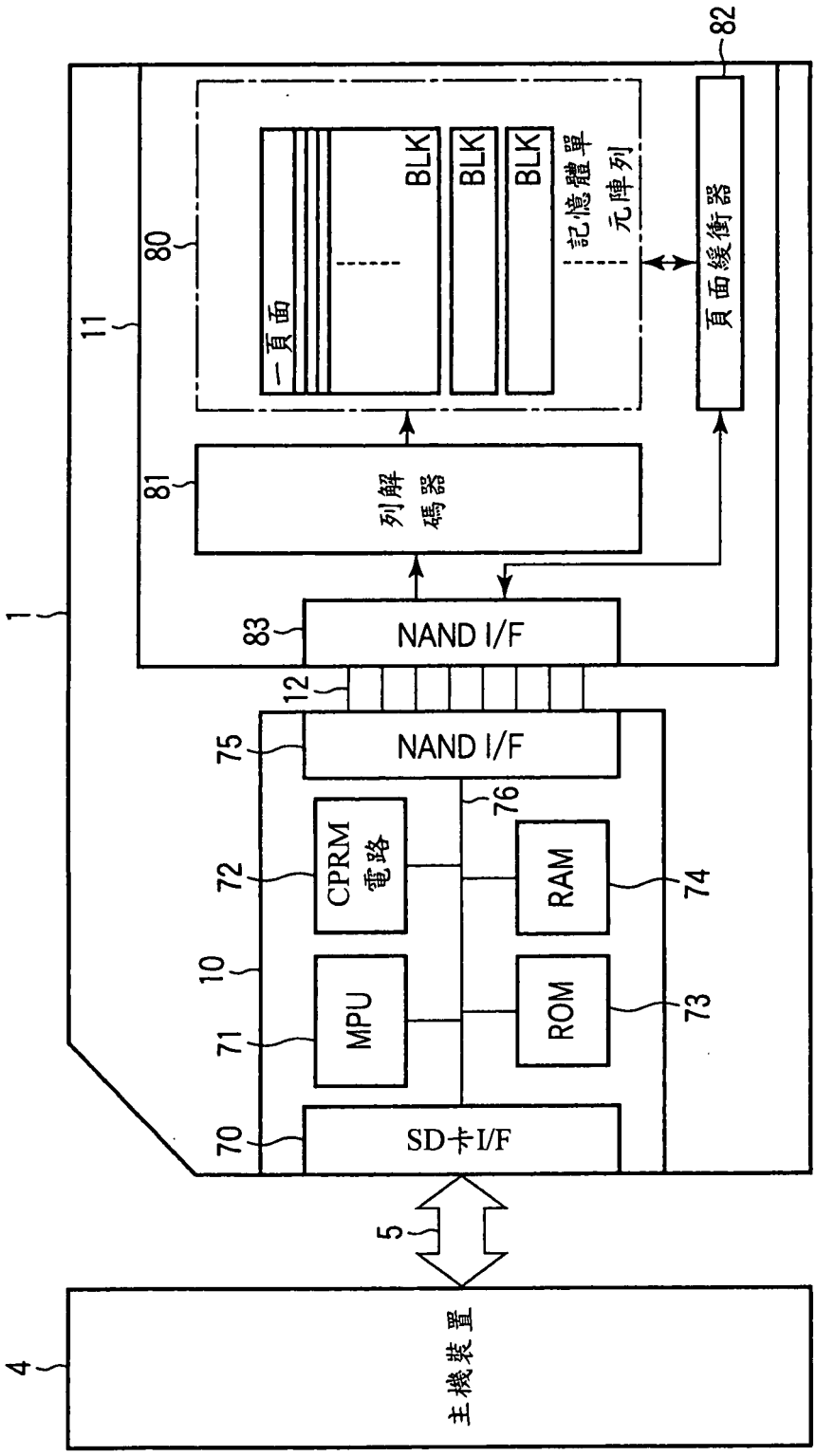

82
80
11
一頁面
BLK
BLK
BLK
記憶體單元陣列
頁面緩衝器
81
列解碼器
1
83
NAND I/F
12
75
NAND I/F
76
72
CPRM電路
RAM
74
10
MPU
ROM
73
71
70
SD卡I/F
5
4
主機裝置

圖 8

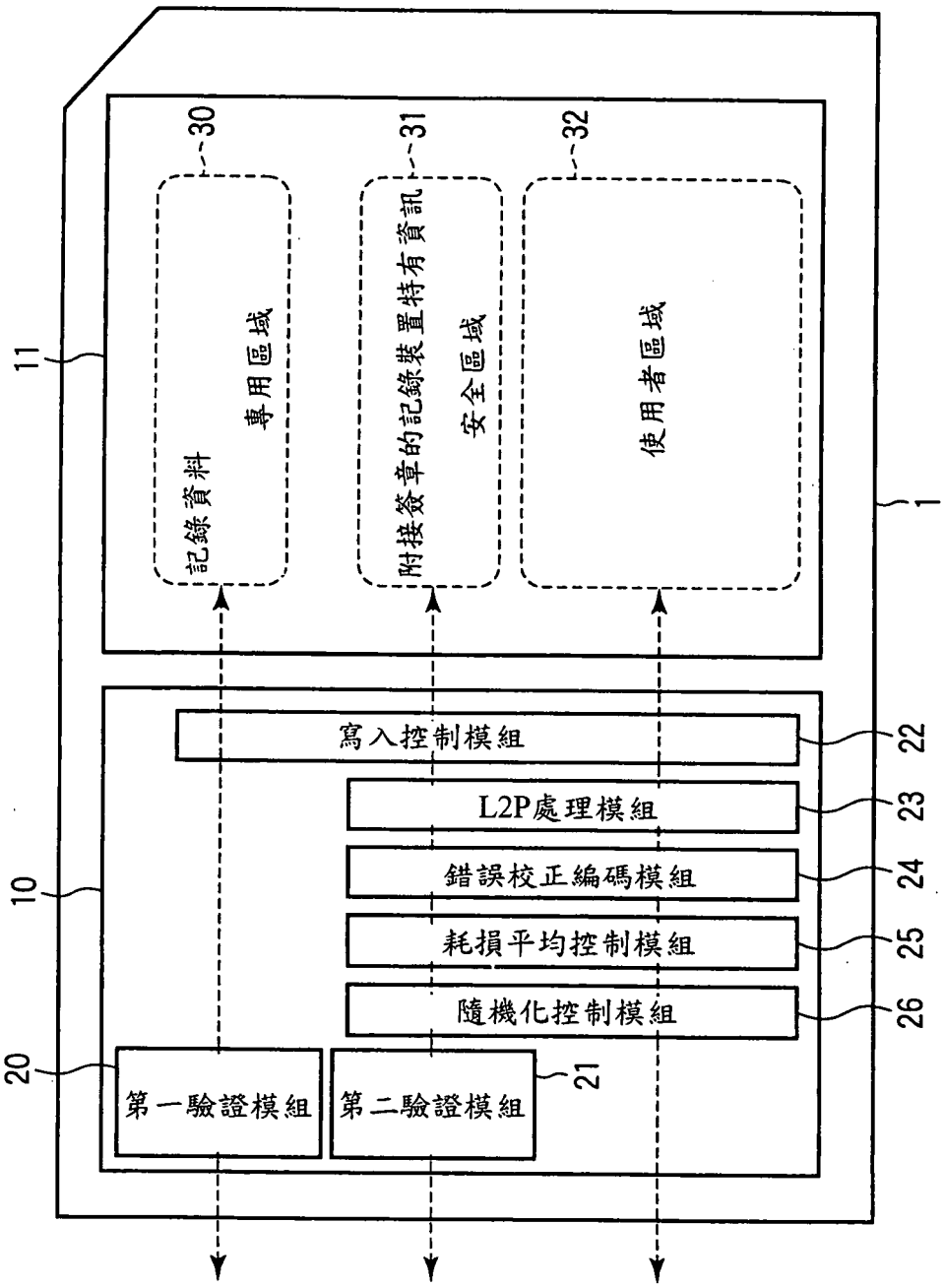

1
11
30
專用區域
記錄資料
31
安全區域
附接簽章的記錄裝置特有資訊
32
使用者區域
10
寫入控制模組
22
L2P處理模組
23
錯誤校正編碼模組
24
耗損平均控制模組
25
隨機化控制模組
26
20
第一驗證模組
第二驗證模組
21

圖 9

	專用區域	其他區域
驗證	必要	必要/不必要
接收位址	實體位址	邏輯位址
L2P處理	不執行	執行
ECC程序	不執行	執行
耗損平均	不執行	執行
隨機化	不執行	執行
寫入模式	4層級模式(M位元模式)	2層級模式(N位元模式，N<M)

圖 10

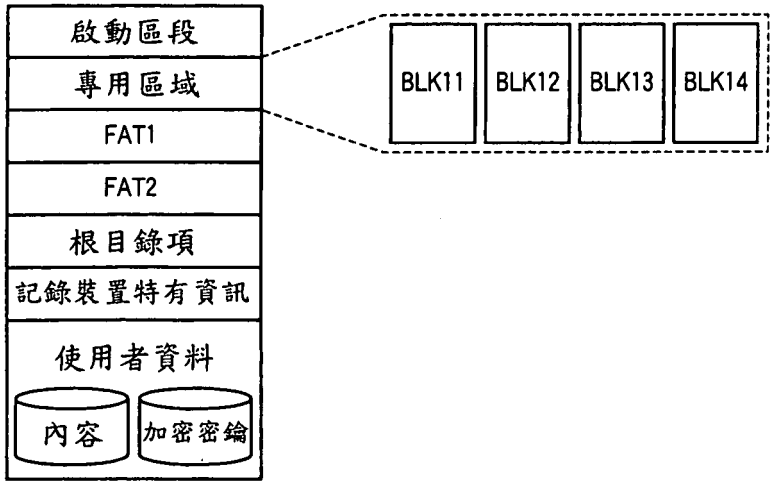


圖 11

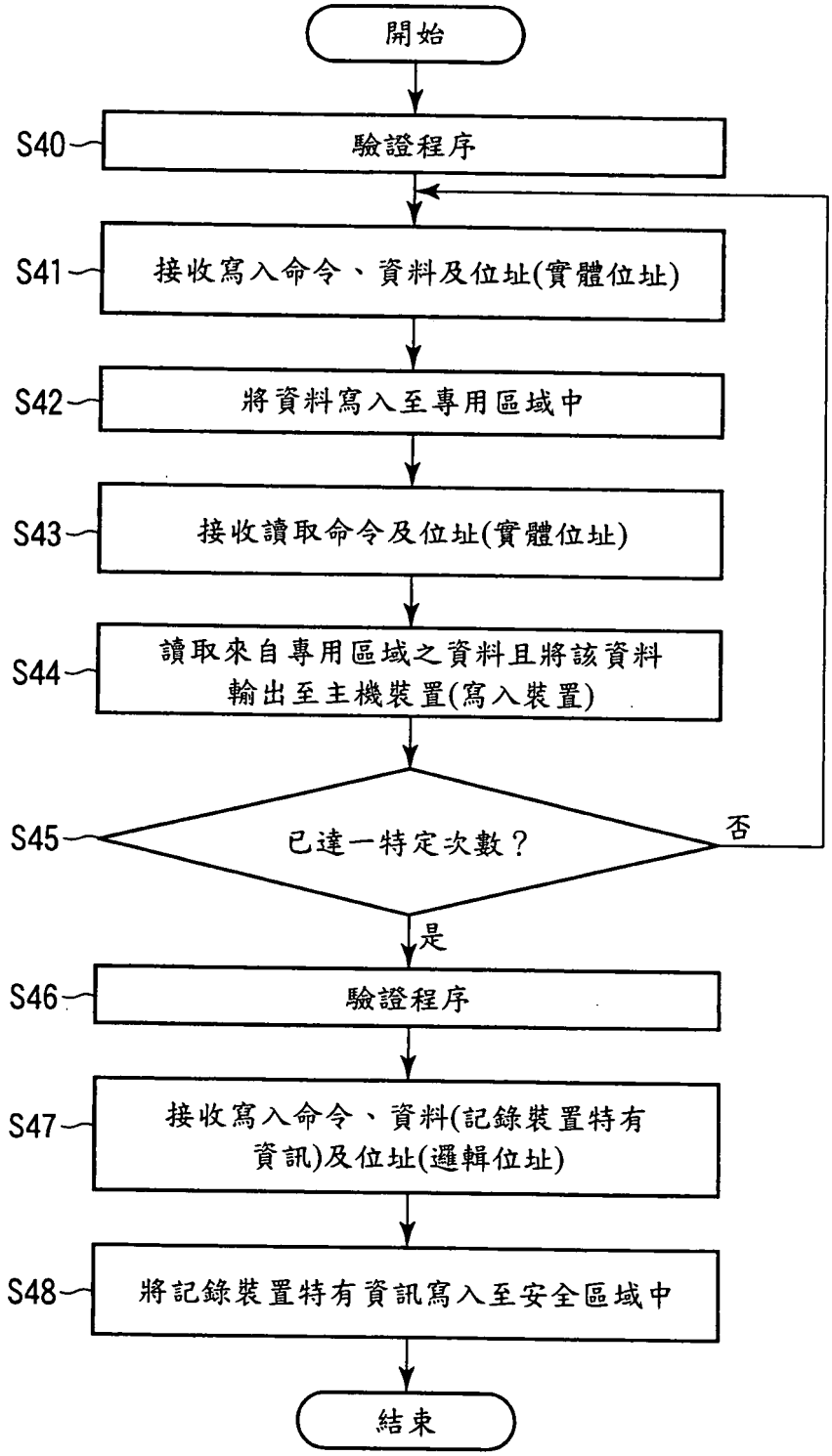

開始
S40
驗證程序
S41
接收寫入命令、資料及位址(實體位址)
S42
將資料寫入至專用區域中
S43
接收讀取命令及位址(實體位址)
S44
讀取來自專用區域之資料且將該資料輸出至主機裝置(寫入裝置)
S45
已達一特定次數？
否
是
S46
驗證程序
S47
接收寫入命令、資料(記錄裝置特有資訊)及位址(邏輯位址)
S48
將記錄裝置特有資訊寫入至安全區域中
結束

圖 12

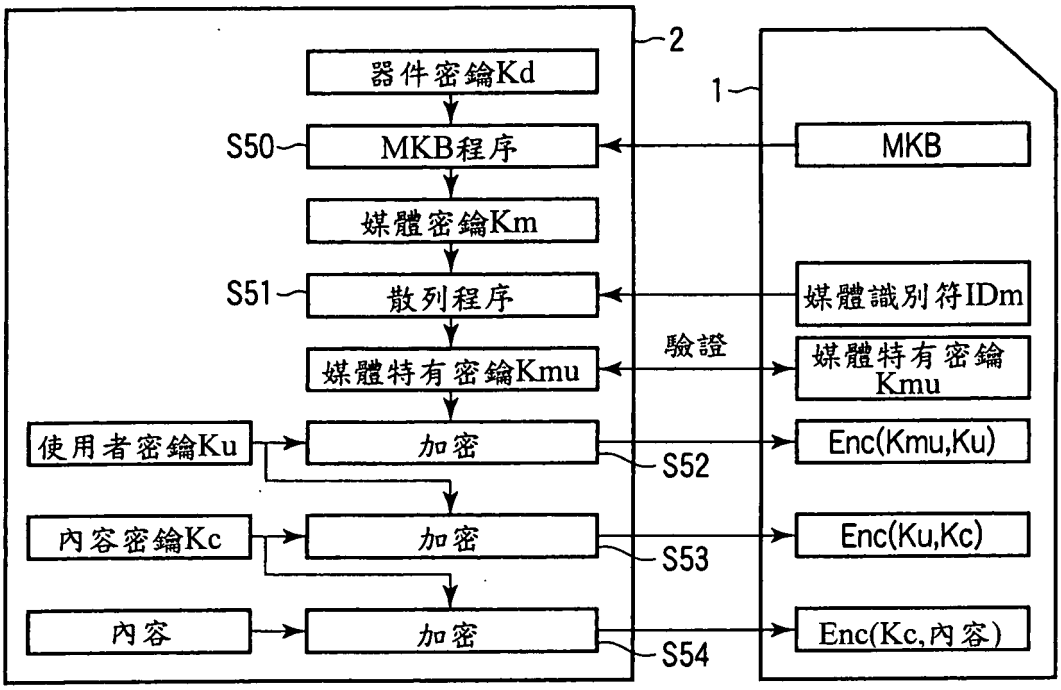

2
器件密鑰Kd
1
S50
MKB程序
MKB
媒體密鑰Km
S51
散列程序
媒體識別符IDm
驗證
媒體特有密鑰Kmu
媒體特有密鑰Kmu
使用者密鑰Ku
加密
Enc(Kmu,Ku)
S52
內容密鑰Kc
加密
Enc(Ku,Kc)
S53
內容
加密
Enc(Kc,內容)
S54

圖 13

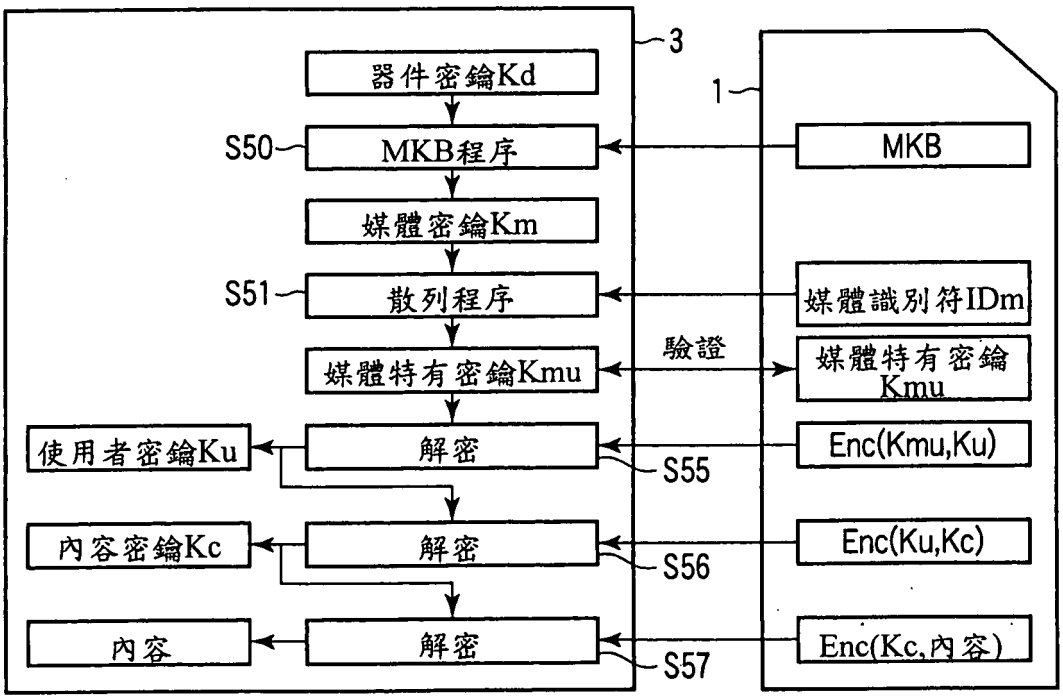

3
器件密鑰Kd
1
S50
MKB程序
MKB
媒體密鑰Km
S51
散列程序
媒體識別符IDm
驗證
媒體特有密鑰Kmu
媒體特有密鑰Kmu
使用者密鑰Ku
解密
Enc(Kmu,Ku)
S55
內容密鑰Kc
解密
Enc(Ku,Kc)
S56
內容
解密
Enc(Kc,內容)
S57

圖 14

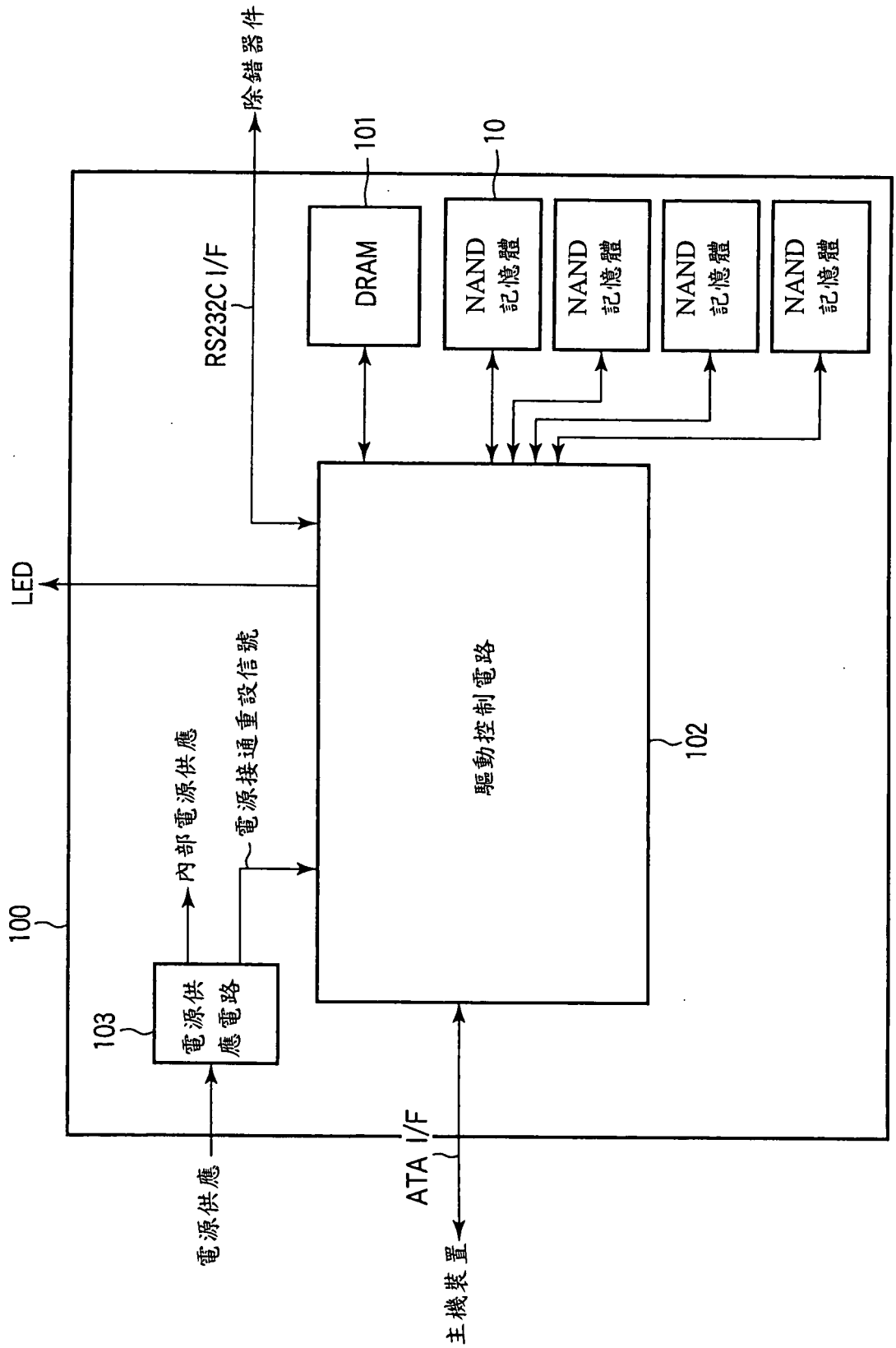

除錯器件
101
10
DRAM
NAND 記憶體
NAND 記憶體
NAND 記憶體
NAND 記憶體
RS232C I/F
LED
驅動控制電路
102
內部電源供應
電源接通重設信號
100
103
電源供應電路
電源供應
ATA I/F
主機裝置

圖 15

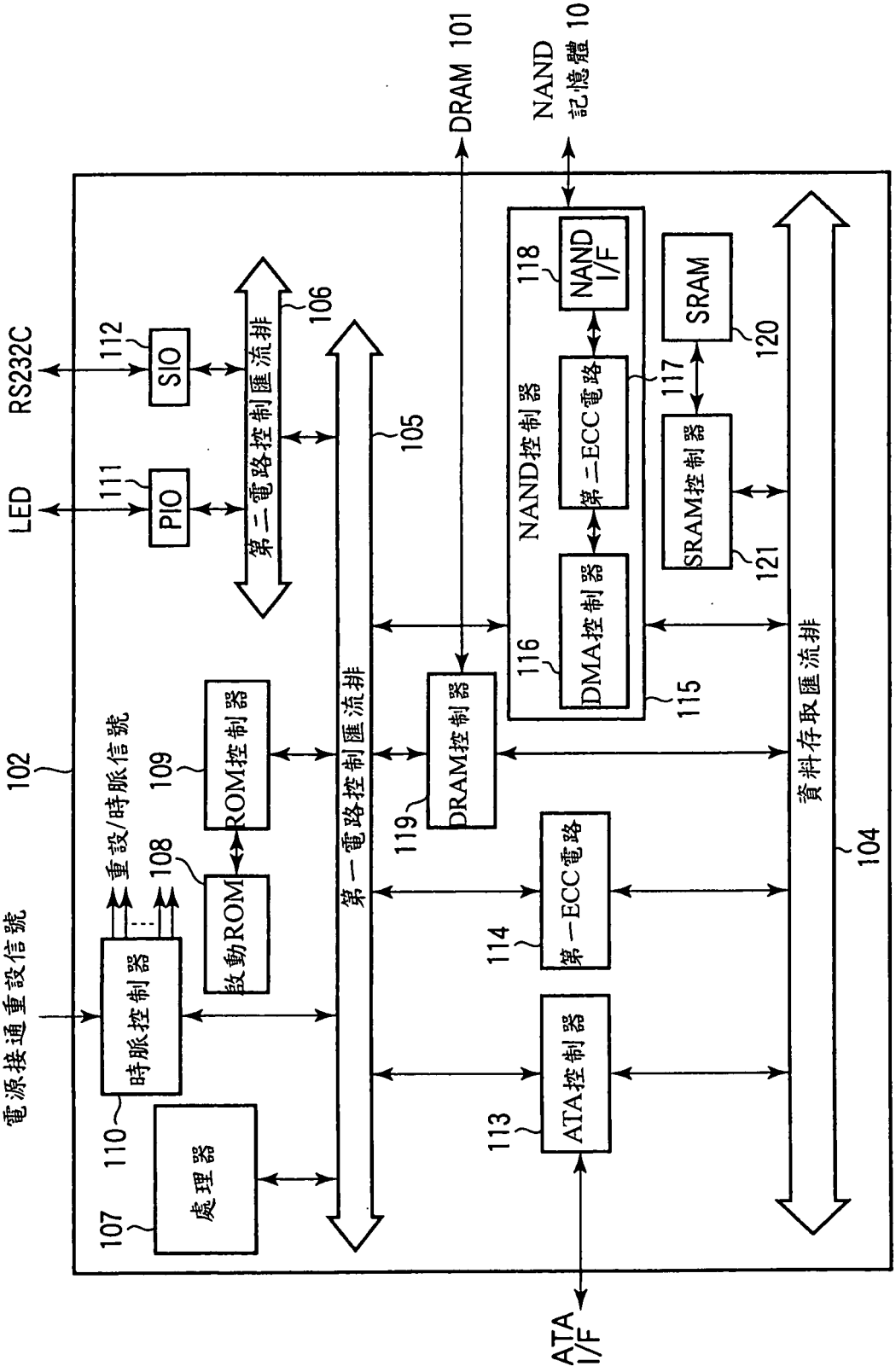

DRAM 101
NAND
記憶體 10
RS232C
LED
電源接通重設信號
重設/時脈信號
102
112
SIO
111
PIO
106
第二電路控制匯流排
105
第一電路控制匯流排
109
ROM控制器
108
啟動ROM
110
時脈控制器
107
處理器
119
DRAM控制器
114
第一ECC電路
113
ATA控制器
ATA
I/F
NAND控制器
118
NAND
I/F
116
DMA控制器
115
第二ECC電路
117
SRAM控制器
121
SRAM
120
資料存取匯流排
104

圖 16

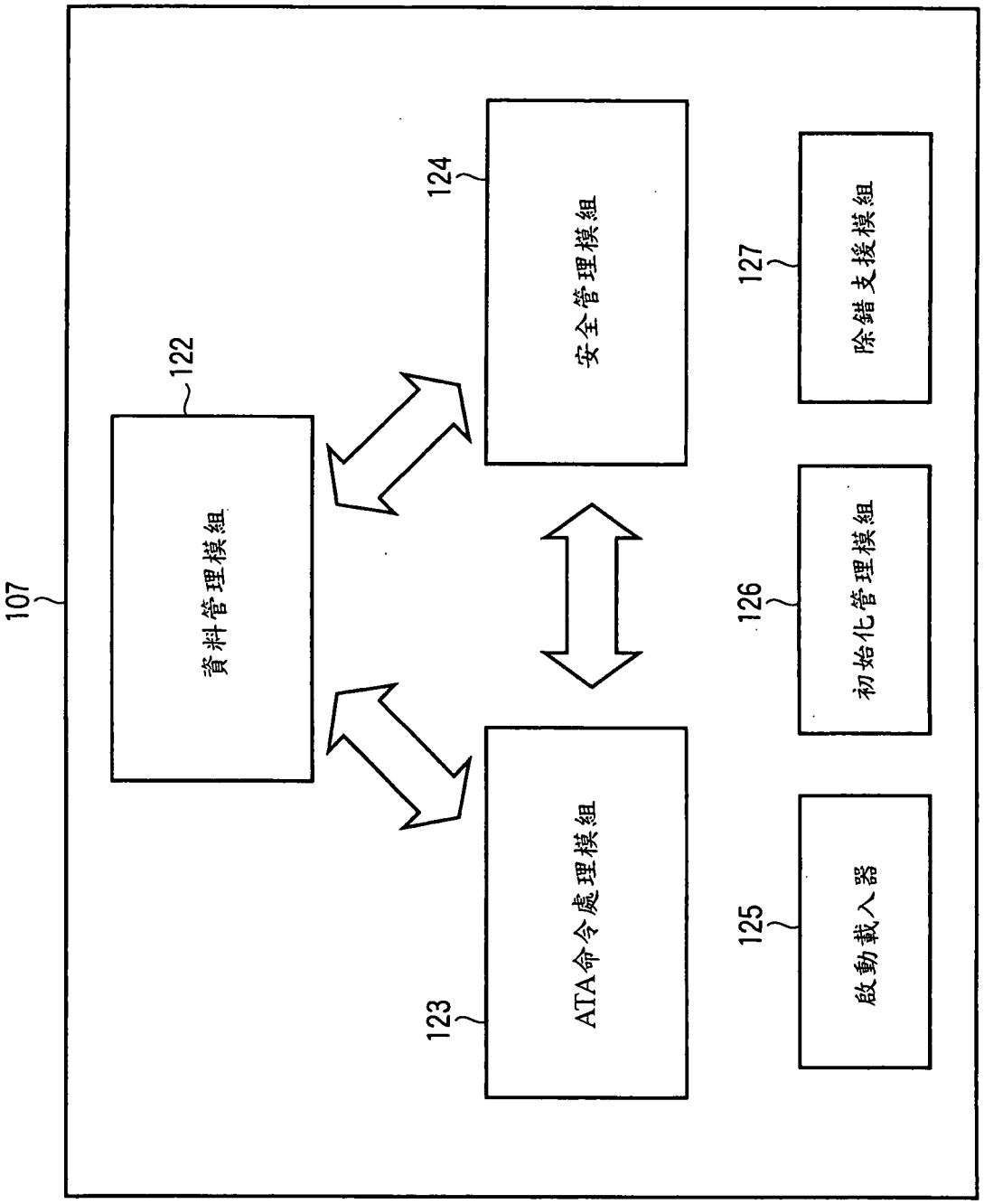

107
資料管理模組
122
安全管理模組
124
ATA命令處理模組
123
初始化管理模組
126
啟動載入器
125
除錯支援模組
127

圖 17

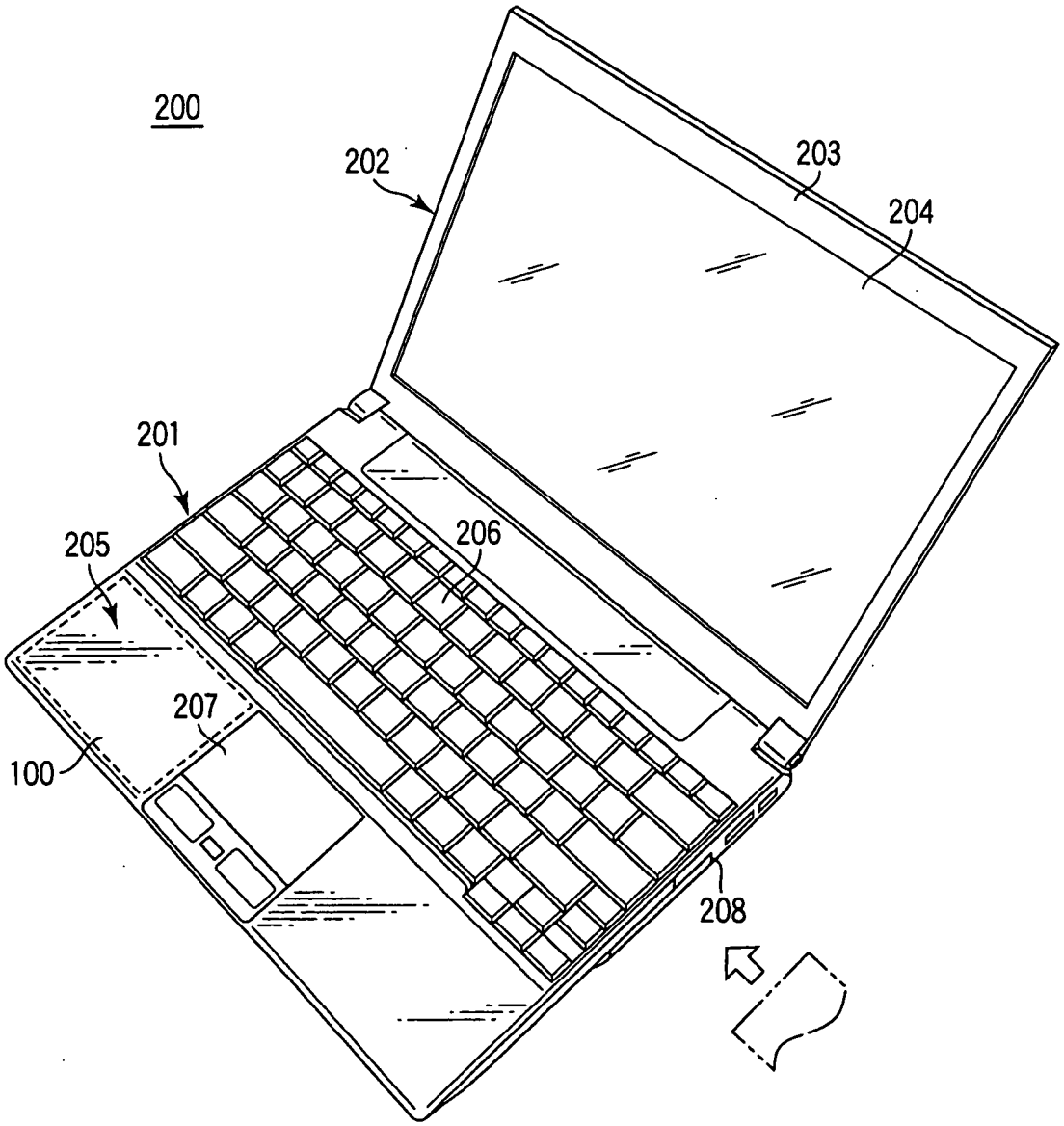


圖 18

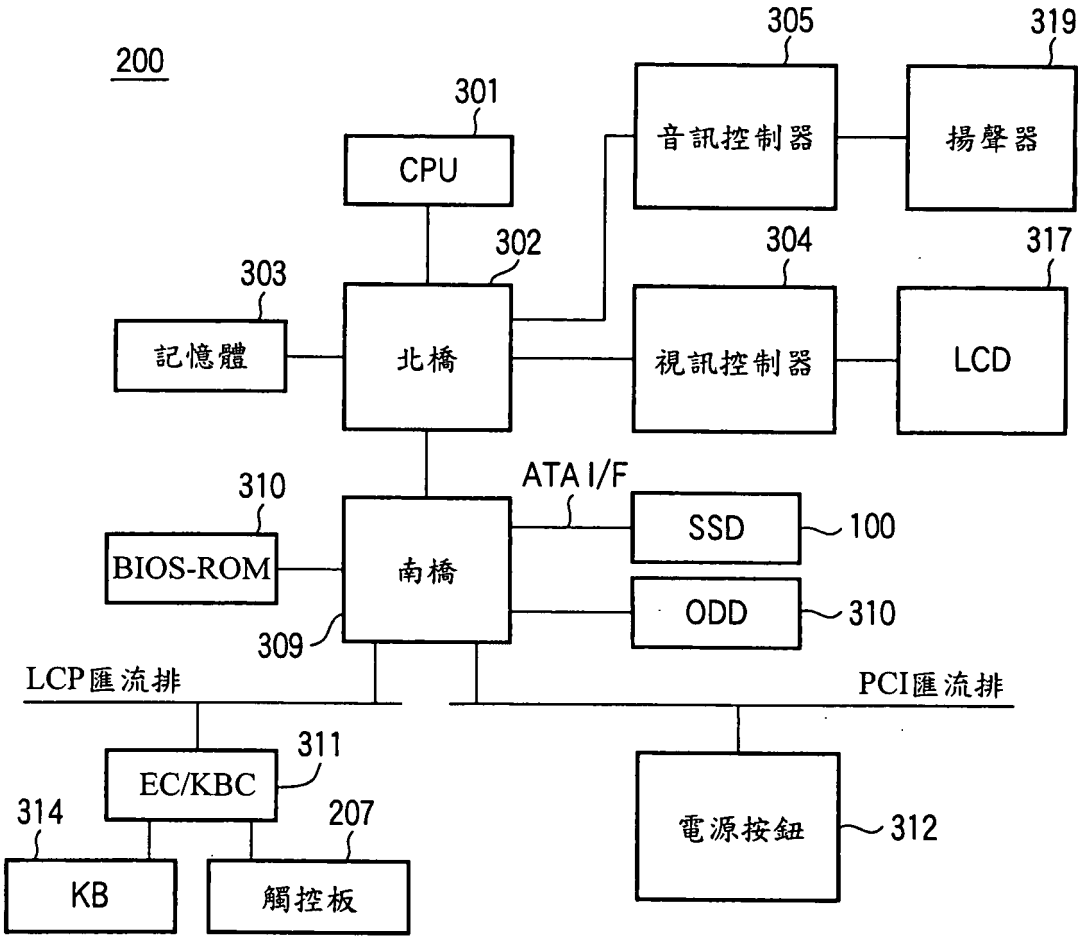

200
301
CPU
305
音訊控制器
319
揚聲器
303
記憶體
302
北橋
304
視訊控制器
317
LCD
310
BIOS-ROM
ATA I/F
南橋
SSD
100
ODD
310
309
LCP匯流排
PCI匯流排
311
EC/KBC
314
KB
207
觸控板
電源按鈕
312

圖 19

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：

1	記憶卡
2	寫入裝置
10	記憶體控制器
11	NAND快閃記憶體
20	第一驗證模組
21	第二驗證模組
30	專用區域
31	安全區域
32	使用者區域
40	CPU
41	產生模組
42	第一驗證模組
43	第二驗證模組
44	內容加密模組
45	簽章產生模組
46	錯誤位置資訊處理模組/處理模組
46a	暫時記憶體
47	寫入資料提供模組/提供模組
48	第一加密模組
49	第二加密模組
Kc	內容密鑰
Ku	使用者密鑰

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）