參、發明人：（共 4 人）

姓　名：（中文/英文）

1.岡上 拓己
TAKUMI OKAUE

2.中西 健一
KENICHI NAKANISHI

3.田代 淳
JUN TASHIRO

4.大久保 英明
HIDEAKI OKUBO

住居所地址：（中文/英文）

1.日本東京都品川區北品川六丁目七番35號
7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, TOKYO, JAPAN

2.日本東京都品川區北品川六丁目七番35號
7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, TOKYO, JAPAN

3.日本東京都品川區北品川六丁目七番35號
7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, TOKYO, JAPAN

4.日本東京都品川區北品川六丁目七番35號
7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, TOKYO, JAPAN

國　籍：（中文/英文）

1.日本　JAPAN
2.日本　JAPAN
3.日本　JAPAN
4.日本　JAPAN

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

☑ 本案申請前已向下列國家（地區）申請專利：

1.日本；2002 年 06 月 25 日；特願 2002-183881

2.

3.

4.

5.

☑ 主張國際優先權(專利法第二十四條)：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記]

1.日本；2002 年 06 月 25 日；特願 2002-183881

2.

3.

4.

5.

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數 順序註記]

1.

2.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記]

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記]

☐ 熟習該項技術者易於獲得，不須寄存。

471

玖、發明說明：

【發明所屬之技術領域】

本發明係關於資訊記憶裝置、記憶體存取控制系統及方法以及電腦程式。更詳言之，係關於可實現對記憶卡等資訊記憶裝置之儲存資料，以各種形態限制其存取之構成，並依據資訊記憶裝置具有之識別符等所構成之鍵組之驗證，執行資訊記憶裝置內之記憶體之鎖定處理或非鎖定處理，藉以實現安全之記憶體存取控制管理之資訊記憶裝置、記憶體存取控制系統及方法以及電腦程式。

【先前技術】

在PC(Personal Computer；個人電腦)、PDA(Personal Digital Assistants；個人數位助理)、數位攝影機、資料記錄播放裝置或遊戲機器等各種資訊處理裝置中，均可利用硬碟、DVD、CD、記憶卡等各種記憶媒體，執行資料之記錄、播放處理。

最近，具有由快閃記憶體等構成之記憶體部、與CPU等構成之控制部之小型卡片式記憶裝置被利用作為音樂資料、圖像資料、程式等各種軟體資料(內容(Content))之記憶手段之情形逐漸增多。

儲存於記憶卡等之資料之讀出或資料之寫入，可利用將卡片裝入具有記憶卡介面之機器中，透過介面執行資料轉送之方式達成。固然也可採用使任何人均可自由執行利用記憶裝置之資料記錄播放之構成，但例如可利用密碼設定或密碼處理等，以實現僅允許特定用戶或特定機器執行記憶體存取，而排除未被授權之第三者之存取之所謂限制存

取之構成。

例如，有下列之構成：設定僅具有存取權限之用戶才能得知之密碼，由作為資訊播放裝置之內容利用機器，將密碼轉送至記憶卡等之內容儲存機器，在記憶卡側之控制部(CPU等)執行密碼驗證，以驗證成立為條件，由記憶卡等之內容儲存機器，對作為資訊播放裝置之內容利用機器輸出內容之構成、或在作為資訊播放裝置之內容利用機器、與記憶卡等之內容儲存機器之間執行相互認證處理以相互認證成立為條件，由記憶卡等之內容儲存機器，對作為資訊播放裝置之內容利用機器輸出內容之構成等。

【發明內容】

如此，在確認資料(內容)利用權限後，可利用資料之形態有各式各樣之形態。

但，記憶卡等資料記憶裝置可裝入於PC、PDA、數位攝影機等各種機器，且在此等機器中，相互利用1個記憶卡之情形也相當多。在此種資料利用形態中，每當將記憶卡裝入於機器，並被要求執行上述密碼驗證處理、認證處理時，至資料讀取或資料寫入等之處理完成為止，需要相當時間，因而可能降低處理效率。

本發明係鑒於上述問題，經多方研發而成，其目的在於提供依據資訊記憶裝置具有之識別符等所構成之鍵組之驗證，執行資訊記憶裝置內之記憶體之鎖定處理或非鎖定處理，實現安全之記憶體存取控制管理之資訊記憶裝置、記憶體存取控制系統及方法以及電腦程式。

475

本發明之第一側面所提供之資訊記憶裝置之特徵在於包含：

資料記憶用之記憶體及執行對記憶體之存取控制之控制部；

前述控制部係構成

由資訊處理裝置輸入前述記憶體之鎖定處理要求指令、或要求解除鎖定之非鎖定處理要求指令，執行對應於輸入指令之處理；

並依據對應於輸出前述指令之資訊處理裝置所設定之識別符(ID)，執行前述資訊處理裝置是否具有含該識別符(ID)之正當之鍵組之驗證處理，並以該驗證成立為條件，依據前述指令執行其處理者。

另外，在本發明之資訊記憶裝置之一實施形態中，以採用下列構成為其特徵：前述資訊處理裝置具有之鍵組係包含資訊處理裝置之固有ID (ID)與對應於該固有ID之鎖定鍵(LK)之鍵組[ID, LK]，前述資訊記憶裝置具有可算出鎖定鍵(LK)，以作為適用LK=H (LMK, ID)之關係，即對ID之鎖定主鍵(LMK)之雜湊值之鎖定主鍵(LMK)；前述控制部係依據由適用前述鎖定主鍵(LMK)之雜湊值之算出所取得之鎖定鍵(LK)，執行由資訊處理裝置輸入之資訊處理裝置固有之鍵組之驗證。

另外，在本發明之資訊記憶裝置之一實施形態中，以採用下列構成為其特徵：前述控制部係執行隨機數產生處理，由資訊處理裝置接收依據該資訊處理裝置所具有之鎖定

476

鍵(LK)之前述隨機數(Rms)之加密資料[E (Lk, Rms)]，以執行包含核對該接收之加密資料、與依據前述雜湊值之算出所取得之鎖定鍵(LK)所算出之加密資料[E (Lk, Rms)]之驗證處理。

另外，在本發明之資訊記憶裝置之一實施形態中，以採用下列構成為其特徵：前述控制部在來自前述資訊處理裝置之輸入指令為鎖定指令時，係由前述資訊處理裝置輸入識別符(ID)，依據該輸入之識別符(ID)執行驗證處理。

另外，在本發明之資訊記憶裝置之一實施形態中，以採用下列構成為其特徵：前述控制部在來自前述資訊處理裝置之輸入指令為解除鎖定指令時，係由記憶體讀出在執行鎖定處理之際由資訊處理裝置輸入並儲存於該記憶體之識別符(ID)，依據該讀出之識別符(ID)執行驗證處理。

另外，本發明之第二側面所提供之記憶體存取控制系統之特徵在於包含：資訊記憶裝置，其係包含資料記憶用之記憶體與執行對該記憶體之存取控制之控制部者；及資訊處理裝置，其係包含對前述資訊記憶裝置之介面，經由該介面執行資訊記憶裝置內之記憶體存取者；

前述資訊處理裝置係

將含識別符(ID)及鎖定鍵(LK)之鍵組儲存於記憶手段，

前述資訊記憶裝置之控制部係構成

由資訊處理裝置輸入前述記憶體之鎖定處理要求指令或要求解除鎖定之非鎖定處理要求指令，執行對應於輸入指令之處理；

477

並依據對應於輸入前述指令之資訊處理裝置所設定之識別符(ID)，執行前述資訊處理裝置是否具有含該識別符(ID)之正當之鍵組之驗證處理，並以該驗證成立為條件，依據前述指令執行其處理者。

另外，在本發明之記憶體存取控制系統之一實施形態中，以採用下列構成為其特徵：前述資訊處理裝置具有之鍵組係包含資訊處理裝置之固有ID (ID)與對應於該固有ID之鎖定鍵(LK)之鍵組[ID, LK]，前述資訊記憶裝置具有可算出鎖定鍵(LK)，以作為適用LK=H (LMK, ID)之關係，即對ID之鎖定主鍵(LMK)之雜湊值之鎖定主鍵(LMK)；前述資訊記憶裝置之控制部係依據由適用前述鎖定主鍵(LMK)之雜湊值之算出所取得之鎖定鍵(LK)，執行由資訊處理裝置輸入之資訊處理裝置固有之鍵組之驗證。

另外，在本發明之記憶體存取控制系統之一實施形態中，以採用下列構成為其特徵：前述資訊記憶裝置之控制部係執行隨機數產生處理，由資訊處理裝置接收依據該資訊處理裝置所具有之鎖定鍵(LK)之前述隨機數(Rms)之加密資料[E (Lk, Rms)]，以執行包含核對該接收之加密資料與依據前述雜湊值之算出所取得之鎖定鍵(LK)所算出之加密資料[E (Lk, Rms)]之驗證處理。

另外，在本發明之記憶體存取控制系統之一實施形態中，以採用下列構成為其特徵：前述資訊記憶裝置之控制部在來自前述資訊處理裝置之輸入指令為鎖定指令時，係由前述資訊處理裝置輸入識別符(ID)，依據該輸入之識別符

(ID)執行驗證處理。

另外，在本發明之記憶體存取控制系統之一實施形態中，以採用下列構成為其特徵：前述資訊記憶裝置之控制部在來自前述資訊處理裝置之輸入指令為解除鎖定指令時，係由記憶體讀出在執行鎖定處理之際由資訊處理裝置輸入並儲存於該記憶體之識別符(ID)，依據該讀出之識別符(ID)執行驗證處理。

本發明之第三側面所提供之記憶體存取控制方法之特徵在於執行資訊記憶裝置中之記憶體存取控制，而該資訊記憶裝置係包含資料記憶用之記憶體與執行對該記憶體之存取控制之控制部者；且包含：

由資訊處理裝置輸入前述記憶體之鎖定處理要求指令或要求解除鎖定之非鎖定處理要求指令之步驟；

依據對應於輸出前述指令之資訊處理裝置所設定之識別符(ID)，執行前述資訊處理裝置是否具有含該識別符(ID)之正當之鍵組之驗證處理之驗證步驟；及

以前述驗證成立為條件，依據前述指令執行其處理之步驟者。

另外，在本發明之記憶體存取控制方法之一實施形態中，其特徵在於：前述資訊處理裝置具有之鍵組係包含資訊處理裝置之固有ID (ID)與對應於該固有ID之鎖定鍵(LK)之鍵組[ID, LK]，前述資訊記憶裝置具有可算出鎖定鍵(LK)，以作為適用LK=H(LMK, ID)之關係，即對ID之鎖定主鍵(LMK)之雜湊值之鎖定主鍵(LMK)；前述驗證步驟係包含依據由

適用前述鎖定主鍵(LMK)之雜湊值之算出所取得之鎖定鍵(LK)，執行由資訊處理裝置輸入之資訊處理裝置固有之鍵組之驗證處理之步驟。

另外，在本發明之記憶體存取控制方法之一實施形態中，其特徵在於：前述驗證步驟係包含執行隨機數產生處理，由資訊處理裝置接收依據該資訊處理裝置所具有之鎖定鍵(LK)之前述隨機數(Rms)之加密資料[E (Lk, Rms)]，以執行包含核對該接收之加密資料與依據前述雜湊值之算出所取得之鎖定鍵(LK)所算出之加密資料[E (Lk, Rms)]之驗證處理之步驟。

另外，在本發明之記憶體存取控制方法之一實施形態中，其特徵在於：前述驗證步驟係包含在來自前述資訊處理裝置之輸入指令為鎖定指令時，由前述資訊處理裝置輸入識別符(ID)，依據該輸入之識別符(ID)執行驗證處理之步驟。

另外，在本發明之記憶體存取控制方法之一實施形態中，其特徵在於：前述驗證步驟係包含在來自前述資訊處理裝置之輸入指令為解除鎖定指令時，由記憶體讀出在執行鎖定處理之際由資訊處理裝置輸入並儲存於該記憶體之識別符(ID)，依據該讀出之識別符(ID)執行驗證處理之步驟。

另外，本發明之第四側面所提供之電腦程式之特徵在於

執行資訊記憶裝置中之記憶體存取控制處理，而該資訊記憶裝置係包含資料記憶用之記憶體與執行對該記憶體之存取控制之控制部者；且包含：

由資訊處理裝置輸入前述記憶體之鎖定處理要求指令或

480

要求解除鎖定之非鎖定處理要求指令之步驟；

依據對應於輸出前述指令之資訊處理裝置所設定之識別符(ID)，執行前述資訊處理裝置是否具有含該識別符(ID)之正當之鍵組之驗證處理之驗證步驟；及

以前述驗證成立為條件，依據前述指令執行其處理之步驟者。

依據本發明之構成，由於在記憶卡等資訊記憶裝置中，在由PC等資訊處理裝置輸入記憶體之鎖定處理要求指令或要求解除鎖定之非鎖定處理要求指令，以執行對應於輸入指令之處理之際，依據對應於輸出指令之資訊處理裝置所設定之識別符(ID)，由資訊處理裝置執行是否具有含該識別符(ID)之正當之鍵組之驗證處理，並以該驗證成立為條件，依據前述指令執行其處理，因此，可實現在安全管理下之記憶體存取控制。

依據本發明之構成，由於構成可儲存包含資訊處理裝置之固有ID (ID)與對應於該固有ID之鎖定鍵(LK)之鍵組[ID, LK]，另一方面，前述資訊記憶裝置儲存可算出鎖定鍵(LK)，以作為適用LK=H (LMK, ID)之關係，即對ID之鎖定主鍵(LMK)之雜湊值之鎖定主鍵(LMK)，依據由適用前述鎖定主鍵(LMK)之雜湊值之算出所取得之鎖定鍵(LK)，執行由資訊處理裝置輸入之資訊處理裝置固有之鍵組之驗證處理，因此，可依據1個鎖定主鍵(LMK)執行對多數不同之鎖定鍵(LK)之驗證。

另外，依據本發明之構成，由於在資訊處理裝置之驗證

481

中，係構成以資訊記憶裝置執行隨機數產生處理，由資訊處理裝置接收依據該資訊處理裝置所具有之鎖定鍵(LK)之前述隨機數(Rms)之加密資料[E (Lk, Rms)]，以執行包含該接收之加密資料、與依據前述雜湊值之算出所取得之鎖定鍵(LK)所算出之加密資料[E (Lk, Rms)]之核對，因此，可執行適用每次核對時不同之隨機數之驗證，排除利用過去之核對史資料之不正確之存取。

又，本發明之電腦程式例如係可利用電腦可讀取之型式提供之記憶媒體、通訊媒體(例如CD或FD、MO等記憶媒體或網路等通訊媒體)，對可執行各種程式碼之通用電腦系統所提供之電腦程式。利用電腦可讀取之型式提供此種程式時，可在電腦系統上實現對應於程式之處理。

本發明之其他目的、特徵及優點可由後述本發明之實施例及依據附圖之更詳細之說明獲得更明確之瞭解。又，在本專利說明書中，所謂系統，係指多數裝置之邏輯的集合構成，各構成之裝置不限於設置在同一框體內。

【實施方式】

以下，參照圖式詳細說明本發明之資訊記憶裝置、記憶體存取控制處理之實施例之詳情。

首先，參照圖1說明適用本發明之資訊記憶裝置之資料利用構成之概要。資訊處理裝置20例如係可裝定PC (Personal Computer；個人電腦)21、PDA (Personal Digital Assistants；個人數位助理)23、攜帶式終端24、數位攝影機25等資訊記憶裝置30，並輸出來自資訊記憶裝置30之資訊之機器。

482

此等資訊處理裝置20係裝定例如搭載快閃記憶體等非揮發性記憶體(NVM: Non-Volatile Memory)之記憶卡30，對記憶卡30儲存資料或執行儲存於記憶卡之資料之讀出。

各PC (Personal Computer) 21、22、PDA (Personal Digital Assistants) 23、攜帶式終端24、數位攝影機25有時也相互利用1個記憶卡30。例如，將數位攝影機25攝影之圖像資料儲存於記憶卡30，然後，將記憶卡30裝定於PC 21而執行儲存之圖像資料之顯示、圖像處理，或在PC 21中，將經由網際網路等網路或經由CD、DVD等所獲得之音樂資料等內容儲存於記憶卡30，然後，將儲存內容之記憶卡30裝定於PDA 23，以便在外出之場所隨時可利用PDA 23執行內容之播放等。

圖2係表示可裝定記憶卡等之資訊記憶裝置之資訊處理裝置之構成例。CPU (Central Processing Unit；中央處理器)101係執行各種應用程式、操作系統(OS: Operation System)之處理器。可執行後段所詳述之包含作為對資訊記憶裝置之存取限制處理之鎖定處理、非鎖定處理中之雜湊值算出、隨機數產生等之各種密碼處理及指令收發等之控制。

ROM (Read Only Memory；唯讀記憶體)102係儲存CPU 101執行之程式及運算用之參數中之固定資料等。可儲存後段所詳述之作為對資訊記憶裝置之存取限制處理之鎖定處理、非鎖定處理程式等。RAM (Random Access Memory；隨機存取記憶體)103係儲存適用於CPU 101之執行程式之資訊及其執行中適當變化之參數等。

DSP (Digital Signal Processor；數位訊號處理器)104係執行例

如由記憶卡等之資訊記憶裝置200，經記憶裝置I/F(介面)113輸入之內容之播放處理之際之密碼處理、均衡器調整(對應於聲音訊號之頻帶之增益調整)、壓縮擴張(編碼/解碼)處理等。

被解碼、擴張之內容在數位類比變換電路105被變換成類比聲音訊號，並在放大電路106被放大後，經由聲音輸出部107被輸出。又，圖像資料之輸出係經由顯示控制器108，在LCD等之顯示部109中被執行。由輸入I/F 112輸入來自外部來源之數位訊號或類比訊號，輸入類比訊號時，施行A/D變換。A/D變換係將輸入之輸入訊號變換成數位訊號。又，來自外部來源之輸入數位訊號係被SRC(抽樣比率控制器)變換成具有特定抽樣頻率、量子化位元數之數位訊號後被輸入。

輸出入I/F 115係連接外部機器之介面，施行利用例如USB、IEEE 1394等之連接形態之連接，以執行與其所連接之機器之資料轉送。

其次，參照圖3說明搭載快閃記憶體等非揮發性記憶體(NVM: Non-Volatile Memory)之記憶卡等之資訊記憶裝置200之構成例。快閃記憶體係所謂EEPROM (Electrically Erasable Programmable ROM；電可消除可程式化唯讀記憶體)之電可改寫之非揮發性記憶體之一種形態。以往之EEPROM由於係以2個電晶體構成1位元，因此，1位元所佔面積較大，在積體度之提高上有其界限，但快閃記憶體則由於採用全部位元整批消除方式，故可實現以1個電晶體構成1位元。

具有此種快閃記憶體之資訊記憶裝置200可裝入於PC、PDA、數位攝影機等資訊處理裝置，將由資訊處理裝置輸入之資料儲存於記憶體部220，且對資訊處理裝置輸出儲存於記憶體部220之資料。

資訊記憶裝置200另外具有控制部210，控制部210具有作為執行各種程式之處理器之CPU (Central Processing Unit) 211、儲存CPU 211執行之程式及運算用之參數中之固定資料等之ROM (Read Only Memory) 212、儲存適用於CPU 211之執行程式之資訊及其執行中適當變化之參數等之RAM (Random Access Memory) 213。

RAM (Random Access Memory) 213也被使用作為因後段所詳述之作為對資訊記憶裝置之存取限制處理之鎖定處理、非鎖定處理而變化之鎖定狀態之狀態值資料之儲存區域。

控制部210另外具有作為與資訊處理裝置間之資料輸出入用之介面之機器介面214與記憶體部220間之資料輸出入用之介面之記憶體介面216。

CPU 211係執行後段所詳述之包含作為與資訊處理裝置間執行之存取限制處理之鎖定處理、非鎖定處理中之雜湊值算出、隨機數產生等之各種密碼處理及指令收發等之控制。

[依據鎖定主鍵(LMK)之處理]

其次，說明適用鎖定主鍵(LMK)之鎖定處理及非鎖定處理，以作為對資訊記憶裝置之存取限制機構之一處理例。參照圖4說明本處理例，即說明適用鎖定主鍵(LMK)之處理之概要。

可使對記憶卡等資訊記憶裝置320之內容等之資料儲存區域之快閃記憶體等構成之記憶體部(圖3之記憶體部220)之存取限制成為有效之處理稱為鎖定處理，解除存取限制之處理稱為非鎖定處理。此鎖定處理及非鎖定處理係由主裝置310負責執行。

主裝置310如前面參照圖1、圖2所述，係包含具有執行與記憶卡等資訊記憶裝置320之資料轉送之介面，且執行對資訊記憶裝置320之資料寫入或來自資訊記憶裝置320之資料讀出，以執行資料之利用之PC、PDA、數位攝影機、DSC(Digital Still Camera；數位靜物攝影機)等之資訊處理裝置。另外，主裝置310中也包含作為對記憶卡等資訊記憶裝置320之鎖定處理/非鎖定處理執行專用機器之鎖定・非鎖定用機器312。

鎖定・非鎖定用機器312具有作為執行鎖定・非鎖定處理運算法之控制手段之CPU及作為資料儲存記憶體之ROM、RAM，另外具有執行記憶卡等資訊記憶裝置320之裝定、資料轉送之介面，構成作為對資訊記憶裝置320之鎖定處理及非鎖定處理專用之機器。

在以下之說明中，所稱之主裝置係包含對資訊記憶裝置320執行鎖定處理、非鎖定處理之機器，即PC、PDA及其他資訊處理裝置、鎖定・非鎖定用機器312。

主裝置內之ROM等之記憶體315中，儲存著作為各主裝置固有之識別符之ID(例如16位元組資料)與適用於鎖定處理、非鎖定處理之關鍵資料之鎖定鍵(LK)(例如8位元組資料)

。主裝置所具有之各主裝置固有之識別符(ID)與鎖定鍵(LK)之組[ID, LK]稱為鍵組。

另一方面，在記憶卡等資訊記憶裝置320內之控制部內之ROM等記憶體325中儲存著鎖定主鍵(LMK)。此等資訊例如在各機器之製造時，即已被寫入各機器中，成為用戶不能改寫之資料。

儲存於資訊記憶裝置320之鎖定主鍵(LMK)與儲存於主裝置之ID、鎖定鍵(LK)具有以下之關係：

LK=H (LMK, ID)

又，H (X, Y)係表示對適用鍵值X之信息Y之雜湊值之算出處理。即，對ID，可利用適用鎖定主鍵(LMK)之雜湊值之算出處理求出對應於ID之鎖定鍵(LK)。

雜湊函數係一方向性函數，屬於一種非常難以由其輸出反過來求輸入之函數。在上述式中，係對各主裝置固有之ID，以鎖定主鍵(LMK)作為鍵值而適用一方向性函數，將其輸出設定作為對應於各主裝置固有之ID之鎖定鍵(LK)。作為雜湊值算法，可適用MD5、SHA等。

(鎖定處理)

其次，說明有關適用上述鎖定主鍵(LMK)之鎖定處理，即說明有關使對資訊記憶裝置之存取限制成為有效之處理。

圖5係表示鎖定處理中之主裝置與資訊記憶裝置間所執行之處理順序圖。主裝置與資訊記憶裝置係被連接成可分別相互轉送資料之狀態。首先，主裝置對資訊記憶裝置輸出隨機數產生指令。接收到隨機數產生指令後，資訊記憶裝

置即執行特定長度，例如16位元組隨機數(Rms)之產生處理，並對主裝置發送所產生之隨機數(Rms)。於是，資訊記憶裝置將所產生之隨機數(Rms)儲存於控制部內之RAM等之記憶體。

由資訊記憶裝置接收到隨機數(Rms)之主裝置執行以早已事先儲存於主裝置內之鎖定鍵(LK)作為密碼處理鍵之接收隨機數(Rms)之密碼處理：E (LK, Rms)。又，E (X, Y)係表示適用鍵值[X]之信息[Y]之密碼處理。密碼處理算法可適用各種算法，例如可適用DES密碼處理算法。

主裝置執行以鎖定鍵(LK)作為密碼處理鍵之接收隨機數(Rms)之密碼處理：E (LK, Rms)，其結果，將資料[E (LK, Rms)]與主裝置事先儲存於主裝置內之記憶體之主裝置固有之識別符(ID)和鎖定指令共同地發送至資訊記憶裝置。

接到資料：ID, E (LK, Rms)之資訊記憶裝置首先對所接到之ID，利用適用儲存於自己之記憶體之鎖定主鍵(LMK)之雜湊值算出處理，算出對應於接到之ID之鎖定鍵(LK)。即利用：

LK=H (LMK, ID)

算出對應於接到之ID之鎖定鍵(LK)。又，接到之ID係儲存保持於自己之記憶體中。接到之ID係供後述非鎖定處理之際使用。

另外，資訊記憶裝置係對儲存於自己之記憶體之隨機數Rms，執行適用上述雜湊值算出所求出之鎖定鍵(LK)之密碼處理：E (LK, Rms)，並執行與由主裝置所接收之密碼處理資

料：E(LK, Rms)是否一致之核對處理。又，密碼處理算法採用與主裝置同一算法時，可適用各種算法。

來自主裝置之接收資料：E(LK, Rms)、與本身算出之密碼處理資料：E(LK, Rms)一致時，判定屬於來自具有正當ID與LK之組資料之主裝置之鎖定處理要求，並執行鎖定處理，然後對主裝置發送鎖定完畢通知。資訊記憶裝置將執行鎖定處理之主裝置之鍵組[ID, LK]儲存保持於快閃記憶體等非揮發性記憶體(NVM: Non-Volatile Memory)構成之記憶體部220。

來自主裝置之接收資料：E(LK, Rms)與本身算出之密碼處理資料：E (LK, Rms)不一致時，判定非屬於具有正當ID與LK之組資料之主裝置，且判定屬於來自不正當機器之鎖定處理要求，故不執行鎖定處理，而對主裝置發送有錯誤之通知。

又，資訊記憶裝置執行之鎖定處理係在以執行下列說明之非鎖定處理為條件，將對內容等之資料儲存區域之快閃記憶體等所構成之記憶體部(圖3之記憶體部220)之存取設定為許可之處理。

其次，參照圖6所示之流程圖，說明有關鎖定處理之步驟。在步驟S101，作為資訊記憶裝置之記憶卡依據接收來自主裝置之隨機數產生要求指令之接收而產生隨機數(Rms)。產生之隨機數在步驟S102，被主裝置讀出，在步驟S103，與鎖定指令共同地，將主裝置之ID及隨機數(Rms)以主裝置之鎖定鍵(LK)加密後之資料：E(LK, Rms)發送至作為資訊記憶裝置之記憶卡。

在步驟S104，記憶卡將接收之ID及加密資料：E (LK, Rms)寫入資訊記憶裝置內之記憶體。在步驟S105，記憶卡利用適用儲存於本身之記憶體之鎖定主鍵(LMK)算出接收之ID之雜湊值，即執行：

H (LMK, ID)=LK

以算出對應於接到之ID之鎖定鍵(LK)。

另外，記憶卡依據算出之鎖定鍵(LK)，執行前述在步驟S101所產生之隨機數(Rms)之加密處理，算出加密資料：E (LK, Rms)，以作為核對用資料。

其次，記憶卡在步驟S106，執行在步驟S105算出之加密資料：E (LK, Rms)和在步驟S103與鎖定指令共同地由主裝置所接收，且與在步驟S104儲存於記憶體之加密資料：E (LK, Rms)之比較核對處理[E (LK, Rms)=E (LK, Rms)？]。

在此比較核對處理中，兩值相等時，判定主裝置屬於擁有正當之正確ID與鎖定鍵(LK)之組資料之正當機器，在步驟S107，執行對應於鎖定指令之鎖定處理，即，以後述之非鎖定處理之成功為條件，執行可對記憶體存取之設定。此時，資訊記憶裝置將執行鎖定處理之主裝置之鍵組[ID, LK]儲存保持於快閃記憶體等非揮發性記憶體(NVM: Non-Volatile Memory)所構成之記憶體部220。

另一方面，在步驟S106之比較核對處理中，判定兩值不相等時，判定在步驟S108中送來鎖定指令之主裝置屬於未擁有正確之ID與鎖定鍵(LK)之組資料之不正當機器，故不執行鎖定處理，而對主裝置發送有錯誤之通知。

(非鎖定處理)

其次，說明有關解除適用上述鎖定主鍵(LMK)之鎖定處理之鎖定之非鎖定處理，即說明有關解除對資訊記憶裝置之存取限制之處理。

圖7係表示非鎖定處理中之主裝置與資訊記憶裝置間所執行之處理順序圖。主裝置與資訊記憶裝置係被連接成可分別相互轉送資料之狀態。首先，主裝置對資訊記憶裝置輸出隨機數產生指令。接收到隨機數產生指令後，資訊記憶裝置即執行特定長度，例如16位元組隨機數(Rms)之產生處理，並對主裝置發送所產生之隨機數(Rms)與先前鎖定處理之際早已儲存於記憶體之主裝置之ID(即執行鎖定處理之主裝置之ID)。又，資訊記憶裝置將所產生之隨機數(Rms)儲存於控制部內之RAM等之記憶體。

由資訊記憶裝置接收到ID與隨機數(Rms)之主裝置，首先判定接收之ID與自己之ID是否一致。未一致時，表示係由其他主裝置執行鎖定，而不能解除其鎖定。

接收之ID與自己之ID一致時，表示該鎖定係該主裝置本身所執行之鎖定，故可執行作為解除處理之解除鎖定。此時，主裝置執行以已事先儲存於主裝置之記憶體內之鎖定鍵(LK)作為密碼處理鍵之接收隨機數(Rms)之密碼處理：E(LK, Rms)，並將其結果資料與解除鎖定指令發送至資訊記憶裝置。

接到加密資料：E(LK, Rms)之資訊記憶裝置首先讀出儲存於自己之記憶體之主裝置之ID(即執行鎖定處理之主裝置之

491

ID)，對讀出之ID，利用適用鎖定主鍵(LMK)之雜湊值算出處理，算出對應於執行鎖定處理之主裝置之ID之鎖定鍵(LK)。即利用：

LK=H(LMK, ID)

算出對應於執行鎖定處理之主裝置之ID之鎖定鍵(LK)。

另外，資訊記憶裝置係對儲存於自己之記憶體之隨機數Rms，執行適用上述雜湊值算出所求出之鎖定鍵(LK)之密碼處理：E(LK, Rms)，並執行與由主裝置所接收之密碼處理資料：E(LK, Rms)是否一致之核對處理。

來自主裝置之接收資料：E(LK, Rms)與本身算出之密碼處理資料：E (LK, Rms)一致時，判定屬於來自具有正當ID與LK之組資料之主裝置之非鎖定處理要求，並執行非鎖定處理，然後對主裝置發送解除鎖定完畢通知。不一致時，判定非為具有正當ID與LK之組資料之主裝置，而屬於來自不正當機器之鎖定處理要求，故不執行非鎖定處理，而對主裝置發送有錯誤之通知。

又，資訊記憶裝置執行之非鎖定處理具有鎖定處理之解除之意，係對內容等之資料儲存區域之快閃記憶體等所構成之記憶體部(圖3之記憶體部220)之存取設定為許可之處理。

其次，參照圖8所示之流程圖，說明有關非鎖定處理之步驟。在步驟S201，作為資訊記憶裝置之記憶卡依據接收來自主裝置之隨機數產生要求指令之接收而產生隨機數(Rms)。產生之隨機數在步驟S202，與先前執行鎖定處理之主裝置之ID共同地被主裝置讀出。

492

主裝置在由記憶卡讀出之ID與自己之主ID一致時，判斷可解除鎖定，在步驟S203，與解除鎖定指令共同地，將接收之隨機數(Rms)以主裝置之鎖定鍵(LK)加密後之資料：E(LK, Rms)發送至作為資訊記憶裝置之記憶卡。

在步驟S204，記憶卡將接收之加密資料：E(LK, Rms)寫入資訊記憶裝置內之記憶體。在步驟S205，記憶卡讀出先前鎖定處理時儲存於記憶體之執行鎖定處理之主裝置ID，而對讀出之ID，適用儲存於本身之記憶體之鎖定主鍵(LMK)算出雜湊值，即執行：

H(LMK, ID)=LK

以算出對應於ID之鎖定鍵(LK)。

另外，記憶卡依據算出之鎖定鍵(LK)，執行先前在步驟S201所產生之隨機數(Rms)之加密處理，算出加密資料：E(LK, Rms)，以作為核對用資料。

其次，記憶卡在步驟S206，執行在步驟S205算出之加密資料：E(LK, Rms)和在步驟S203與解除鎖定指令共同地由主裝置所接收，且與在步驟S204儲存於記憶體之加密資料：E(LK, Rms)之比較核對處理[E(LK, Rms)=E(LK, Rms)？]。

在此比較核對處理中，兩值相等時，判定主裝置屬於擁有正當之正確ID與鎖定鍵(LK)之組資料之正當機器，在步驟S207，執行對應於解除鎖定指令之非鎖定處理，即，執行可對記憶體存取之設定。另一方面，在步驟S206之比較核對處理中，判定兩值不相等時，判定在步驟S208中送來解除鎖定指令之主裝置屬於未擁有執行鎖定處理之正確之

ID與鎖定鍵(LK)之組資料之主裝置，故不執行非鎖定處理，而對主裝置發送有錯誤之通知。

如上所述，依據本處理例，僅具有與主裝置ID相對應之鎖定鍵(LK)之正當組合資料之主裝置才可執行對資訊記憶裝置之鎖定處理，且只有利用執行過鎖定處理之主裝置才可執行作為鎖定解除之非鎖定處理。又，在上述鎖定處理及非鎖定處理中，由於採用僅資訊記憶裝置才可執行主裝置之認證處理之所謂單方面認證處理，故可減輕主裝置方面之處理負擔，達成有效率之處理。

又，上述鎖定處理、非鎖定處理由於在資訊記憶裝置方面採用適用每次處理時所產生之隨機數之構成，不能適用過去處理中之記錄資料，故可有效防指依據過去處理軌跡之不正確之處理。

[在機器群之鎖定處理之構成]

上述鎖定處理、非鎖定處理係以資訊記憶裝置對應於每1主裝置之處理方式被執行，而屬於僅執行過鎖定處理之主裝置才可執行非鎖定處理之構成例。但，在多數主裝置利用1個資訊記憶裝置(記憶卡)之構成中，可能發生在某一主裝置(機器A)儲存並鎖定資料之資訊記憶裝置(記憶卡)，希望在另一主裝置(機器B)中予以利用之狀況。

在此種情形下，只要不利用主裝置(機器A)執行非鎖定處理，即無法利用主裝置(機器B)執行解除鎖定。以下，說明可應付在此種情形下之需要之構成，即說明在多數主裝置所構成之主裝置群中，各主裝置均可分別執行鎖定處理、

非鎖定處理之處理例。首先，參照圖9說明本處理例之概要。

可使對記憶卡等資訊記憶裝置520之內容等之資料儲存區域之快閃記憶體等構成之記憶體部(圖3之記憶體部220)之存取限制成為有效之處理稱為鎖定處理，解除存取限制之處理稱為非鎖定處理。此點與前述處理例相同。鎖定處理及非鎖定處理係由主裝置510負責執行。

主裝置510如前面參照圖1、圖2所述，係包含具有執行與記憶卡等資訊記憶裝置520之資料轉送之介面，且執行對資訊記憶裝置520之資料寫入或來自資訊記憶裝置520之資料讀出，以執行資料之利用之PC、PDA、數位攝影機、DSC(Digital Still Camera：數位靜物攝影機)等之資訊處理裝置。另外，也包含作為對記憶卡等資訊記憶裝置520之鎖定處理、非鎖定處理執行專用機器之鎖定・解除鎖定用機器512。

主裝置內之ROM等之記憶體515中，儲存著作為各主裝置固有之識別符之IDs(例如16位元組資料)與適用於鎖定處理、非鎖定處理之關鍵資料之鎖定鍵(LKs)(例如8位元組資料)。此IDs、LKs係對應於上述處理例之ID、LK之資料組，可適用於與上述之處理同樣之鎖定處理、非鎖定處理。

此IDs、LKs係主ID、主鎖定鍵，在各主裝置製造時即已被寫入主裝置內之ROM等記憶體，成為用戶不能改寫之資料。此等主ID (IDs)、主鎖定鍵(LKs)與上述適用LMK之處理完全同樣地，可適用於主裝置對資訊記憶裝置之1比1對應之鎖定處理、非鎖定處理。此各主裝置固有之主ID、主鎖定鍵組成之鍵組：[IDs, LKs]稱為主鍵組。

適用此主鍵組：[IDs, LKs]之鎖定處理稱為標準鎖定處理，由作為主裝置之資訊處理裝置對資訊記憶裝置輸出標準鎖定指令時，可執行標準鎖定，利用解除鎖定指令之輸出，可執行非鎖定處理。

在主裝置內之ROM等之記憶體515中，另外可儲存可對其他主裝置提供拷貝之作為鍵組之副ID與副鎖定鍵之組資料之副鍵組：[IDen, Lken](n=1、2、・・)1個以上。

此副鍵組：[IDen, Lken]係可在多數主裝置中共通儲存之鍵值，利用後述之處理步驟，將已儲存於其他主裝置之副鍵組：[IDen, Lken]，經由資訊記憶裝置拷貝儲存於另一主裝置。

可適用副鍵組：[IDen, Lken]對資訊記憶裝置(記憶卡)執行鎖定處理，將適用於鎖定處理之副鍵組經由資訊記憶裝置(記憶卡)拷貝輸出至其他主裝置之形態之鎖定處理稱為匯出鎖定處理。

適用此副鍵組：[IDen, Lken]之鎖定處理稱為匯出鎖定處理，利用由作為主裝置之資訊處理裝置對資訊記憶裝置輸出匯出鎖定指令時，可執行匯出鎖定處理，利用解除鎖定指令之輸出，執行非鎖定處理。

主裝置由已完成匯出鎖定之資訊記憶裝置(記憶卡)取得之副鍵組：[IDen, Lken]可寫入該主裝置內之記憶體。此副鍵組之拷貝寫入處理稱為匯入處理。利用匯入處理，可形成由具有同一副鍵組：[IDen, Lken]之多數主裝置所組成之主裝置群。

496

如此，副鍵組：[IDen, Lken]係可適用於可設定輸出至外部之鎖定處理，即匯出(export)鎖定處理之鍵組，分別在ID、LK之後附加[e]予以表示。[en]之n係表示副鍵組號碼，相當於所設定之群數。

各主裝置可儲存多數不同之副鍵組。例如，將副鍵組1：[IDe1, LKe1]設定作為主裝置之PC(Personal Computer)-a、PC-b、PDA(Personal Digital Assistants)-a之3個主裝置組成之群共享之副鍵組(副1)，將副鍵組2：[IDe2, LKe2]設定作為PC-a、PDA-a、PDA-b之群共享之副鍵組(副2)時，各主裝置可將各主ID(IDs)、主鎖定鍵(LKs)組成之主鍵組[IDs, LKs]儲存於記憶體，且使：

PC-a儲存[IDe1, LKe1]、[IDe2, LKe2]

PC-b儲存[IDe1, LKe1]

PDA-a儲存[IDe1, LKe1]、[IDe2, LKe2]

PDA-b儲存[IDe2, LKe2]

之各副ID與副區段鍵組成之副鍵組。

將此等副ID與副區段鍵組成之副鍵組：[IDen, LKen]寫入自己之記憶體515內時，即可成為1個以上之主裝置組成之主裝置群-n之構成成員，群n之號碼可適用共通擁有之副ID(IDn)、共通之副鎖定鍵(LKn)，而對1個資訊記憶裝置(記憶卡)執行鎖定處理、非鎖定處理。

另一方面，在記憶卡等資訊記憶裝置520內之控制部內之ROM等記憶體525中儲存著鎖定主鍵(LMK)。儲存於資訊記憶裝置520之鎖定主鍵(LMK)與儲存於主裝置之ID(含IDs及

IDen)、鎖定鍵(LK)(含LKs與LKen)具有以下之關係：

LK=H(LMK, ID)

此鎖定主鍵(LMK)與ID、LK之對應關係和前述LMK之適用處理之情形完全相同，利用對主ID (IDs)之鎖定主鍵LMK之雜湊值算出處理，算出主鎖定鍵(LKs)，利用對副ID (IDen)之鎖定主鍵LMK之雜湊值算出處理，算出副鎖定鍵(LKen)。

其次，參照圖10說明有關利用主鍵組：[IDs, LKs]、副鍵組：[IDen, LKen]之鎖定處理形態。鎖定處理形態中有圖10(a)～圖10(c)所示之3種形態。

(a)係適用各主裝置510固有之主ID (IDs)、與主鎖定鍵(LKs)組成之主鍵組：[IDs, LKs] 531之標準鎖定處理。

適用主鍵組：[IDs, LKs] 531之標準鎖定處理係利用由主裝置510對資訊記憶裝置520輸出標準鎖定指令所執行，利用解除鎖定指令之輸出而執行非鎖定處理。

執行標準鎖定處理時，將主鍵組：[IDs, LKs]儲存於鎖定資訊記憶裝置(記憶卡)520之記憶部(快閃記憶體)之標準鎖定鍵組儲存區域541。執行此鎖定處理時，適用於標準鎖定之主鍵組：[IDs, LKs]不必由鎖定資訊記憶裝置(記憶卡)520輸出至外部，而可執行鎖定解除(非鎖定)處理之主裝置係具有同一主鍵組：[IDs, LKs]之主裝置，即執行標準鎖定處理之唯一之主裝置。

主ID (IDs)、與主鎖定鍵(LKs)組成之主鍵組：[IDs, LKs]與適用上述LMK處理情形完全相同，可適用於主裝置對資訊記憶裝置之1比1對應之鎖定處理、非鎖定處理，可執行與

參照圖5至圖8所述之處理相同之鎖定處理、非鎖定處理。

(b)係適用多數主裝置可共享之副ID (IDen)、與副鎖定鍵(LKen)組成之副鍵組：[IDen, LKen] 532之匯出鎖定處理。

適用副鍵組：[IDen, LKen] 532之匯出鎖定處理係利用由主裝置510對資訊記憶裝置520輸出匯出鎖定指令所執行，利用解除鎖定指令之輸出而執行非鎖定處理。

執行匯出鎖定處理時，將副鍵組：[IDen, LKen]儲存於鎖定資訊記憶裝置(記憶卡)520之記憶部(快閃記憶體)之匯出鎖定鍵組儲存區域542。執行此鎖定處理時，可利用執行後段所詳述之印刷處理，使其他主裝置可由鎖定資訊記憶裝置(記憶卡)520取得適用於匯出鎖定之副鍵組：[IDen, LKen]。

執行此匯出鎖定處理時，可執行鎖定解除(非鎖定)處理之主裝置係可執行鎖定處理之主裝置、與利用印刷處理而可取得適用於匯出鎖定之副鍵組：[IDen, LKen]之主裝置。

(c)係適用各主裝置510可共享之副ID (IDen)、與副鎖定鍵(LKen)組成之副鍵組：[IDen, LKen] 532之標準鎖定處理。此處理稱為群鎖定處理。

適用副鍵組：[IDen, LKen] 532之標準鎖定處理，即群鎖定處理係利用由主裝置510對資訊記憶裝置520輸出標準鎖定指令所執行，利用解除鎖定指令之輸出而執行非鎖定處理。但，此處理之際所適用之鍵組為副鍵組：[IDen, LKen] 532。

此處理基本上係與標準鎖定同樣之處理，以所適用之鍵組作為副鍵組：[IDen, LKen] 532之處理。執行群鎖定處理時，將副鍵組：[IDen, LKen]儲存於鎖定資訊記憶裝置(記憶

卡)520之記憶部(快閃記憶體)之標準鎖定鍵組儲存區域541。執行此鎖定處理時，適用於群鎖定之副鍵組：[IDen, LKen]會儲存於標準鎖定鍵組儲存區域541，故不會由鎖定資訊記憶裝置(記憶卡)520輸出至外部。

可執行此群鎖定之解除(非鎖定)處理之主裝置係具有同一副鍵組：[IDen, LKen]之主裝置。但，此時，並不限定於執行群鎖定之主裝置，也包含事前已取得同一副鍵組：[IDen, LKen]之主裝置。

例如，事前執行適用同一副鍵組：[IDen, LKen]之匯出鎖定處理，在其匯出鎖定處理之執行時，取得同一副鍵組：[IDen, LKen]，並將其儲存於記憶體之主裝置即可執行解除鎖定。

適用副鍵組：[IDen, LKen]之標準鎖定處理，即群鎖定中之鎖定處理、非鎖定處理之順序採用與上述適用LMK之處理同樣之順序(參照圖5至圖8)。但相異之點在於可利用印刷處理使可執行鎖定處理/非鎖定處理之主裝置變成多數個。

以下，說明有關適用可在多數主裝置中共享之副ID(IDen)、副鎖定鍵(LKen)，即，副鍵組：[IDen, LKen]之鎖定處理及經由資訊記憶裝置(記憶卡)而對主裝置之副鍵組：[IDen, LKen]之拷貝儲存處理(印刷處理)以及作為匯出鎖定之解除之非鎖定處理之概況。

(依據副鍵組之鎖定處理)

首先，說明對適用副ID (IDen)、副鎖定鍵(LKen)組成之副鍵組：[IDen, LKen]之資訊記憶裝置(記憶卡)之鎖定處理之詳

500

細情形。

如前所述，利用對適用副鍵組：[IDen, LKen]之資訊記憶裝置(記憶卡)之鎖定處理，可執行經由資訊記憶裝置(記憶卡)將適用於鎖定處理之副鍵組拷貝輸出至其他主裝置之匯出鎖定處理。

圖11係表示依據副鍵組之鎖定處理中之主裝置與資訊記憶裝置間所執行之處理順序圖。主裝置與資訊記憶裝置係被連接成可分別相互轉送資料之狀態。

又，資訊記憶裝置具有圖11所示之鎖定狀態旗標551，保持著表示資訊記憶裝置之鎖定狀態之值。上段之NVM係儲存於圖3中所述之快閃記憶體等構成之記憶體部220之NVM(Non-Volatile Memory：非揮發性記憶體)區域之旗標，下段係儲存於控制部210內之RAM 213之旗標。資訊記憶裝置之電源斷電時，RAM內之旗標會消除，但NVM之旗標資料則可維持。因此，可對應RAM之旗標之改寫，執行對NVM之旗標資料之拷貝，在電源斷電後，電源重新通電時，NVM之旗標資訊會被拷貝至RAM。又，SL表示標準鎖定，EL表示匯出鎖定，1表示鎖定狀態，0表示非鎖定狀態。

標準鎖定係不准適用於鎖定之鍵組[ID, LK]輸出外部之鎖定形態，匯出鎖定係准許適用於鎖定之鍵組[ID, LK]輸出外部之鎖定形態，SL=1係表示處於標準鎖定狀態，EL=1係表示處於匯出鎖定狀態。

資訊記憶裝置(記憶卡)在記憶部(快閃記憶體(NVM))內具有分別儲存適用於標準鎖定之鍵組與儲存適用於匯出鎖定

501

之鍵組之資料儲存區域。

作為初始狀態，如圖所示，SL=0、EL=0，表示均未執行標準鎖定(SL)、匯出鎖定(EL)，即處於所有主裝置均可對資訊記憶裝置之記憶部存取之狀態。

在此初始狀態中，首先，主裝置對資訊記憶裝置輸出隨機數產生指令。接收到隨機數產生指令後，資訊記憶裝置即執行特定長度，例如16位元組隨機數(Rms)之產生處理，並對主裝置發送所產生之隨機數(Rms)。於是，資訊記憶裝置將所產生之隨機數(Rms)儲存於控制部內之RAM等之記憶體。

由資訊記憶裝置接收到隨機數(Rms)之主裝置執行以早已事先儲存於主裝置內之副鎖定鍵(LKen)作為密碼處理鍵之接收隨機數(Rms)之密碼處理：E (LKen, Rms)。密碼處理算法可適用各種算法，例如可適用DES密碼處理算法。

主裝置執行以副鎖定鍵(LKen)作為密碼處理鍵之接收隨機數(Rms)之密碼處理：E (LKen, Rms)，其結果，將資料[E (LKen, Rms)]、與主裝置事先儲存於主裝置內之記憶體之作為對應於副鎖定鍵(LKen)之組資料之副ID (IDen)和鎖定指令共同地發送至資訊記憶裝置。

接到資料：IDen、E (LKen, Rms)之資訊記憶裝置首先對所接到之副ID (IDen)，利用適用儲存於自己之記憶體之鎖定主鍵(LMK)之雜湊值算出處理，算出對應於接到之副ID (IDen)之副鎖定鍵(LKen)。即利用：

LKen=H (LMK, IDen)

502

算出對應於接到之副ID (IDen)之副鎖定鍵(LKen)。又，接到之副ID (IDen)係儲存保持於自己之記憶體中。接到之副ID (IDen)係供後述非鎖定處理之際使用。

另外，資訊記憶裝置係對儲存於自己之記憶體之隨機數Rms，執行適用上述雜湊值算出所求出之副鎖定鍵(LKen)之密碼處理：E (LKen, Rms)，並執行與由主裝置所接收之密碼處理資料：E (LKen, Rms)是否一致之核對處理。又，密碼處理算法採用與主裝置同一算法時，可適用各種算法。

來自主裝置之接收資料：E (LKen, Rms)、與本身算出之密碼處理資料：E (LKen, Rms)一致時，判定屬於來自具有正當副ID (IDen)與副鎖定鍵(LKen)之組資料之主裝置之鎖定處理要求，並執行匯出鎖定處理，對主裝置發送鎖定完畢通知。不一致時，判定非屬於具有正當副ID (IDen)與副鎖定鍵(LKen)之組資料之主裝置，並判定屬於來自不正當機器之鎖定處理要求，故不執行鎖定處理，而對主裝置發送有錯誤之通知。

又，資訊記憶裝置執行之匯出鎖定處理係在以執行適用下列說明之副ID、副鎖定鍵之非鎖定處理為條件，將對內容等之資料儲存區域之快閃記憶體等所構成之記憶體部(圖3之記憶體部220)之存取設定為許可之處理，將適用於匯出鎖定之匯出鍵組：[IDen, LKen]儲存於資訊記憶裝置(記憶卡)之記憶部(快閃記憶體(NVM))之匯出鎖定鍵組儲存區域，再執行鎖定狀態旗標之改寫。

執行匯出鎖定時，如圖所示，鎖定狀態旗標中，表示匯

503

出鎖定為有效狀態之旗標：EL=1被分別儲存於NVM、RAM。此等旗標首先在資訊記憶裝置之控制部內之RAM 213(參照圖3)設定EL=1後，將EL=1拷貝至NVM(快閃記憶體所構成之記憶體部220)。在此狀態下，資訊記憶裝置之電源斷電時，RAM之旗標資訊會被消除，但NVM之旗標資訊則可被維持。其後，資訊記憶裝置之電源重新通電時，NVM之旗標資訊(EL=1)會被拷貝至RAM，控制部210(參照圖3)執行依據RAM之旗標資訊(EL=1)之處理。

旗標資訊為EL=1時，表示處於匯出鎖定狀態，儲存於資訊記憶裝置(記憶卡)之NVM(快閃記憶體構成之記憶體部220)之匯出鎖定鍵組儲存區域之副鍵可藉後述之印刷處理而被輸出至其他主裝置。

其次，參照圖12所示之流程，說明有關匯出鎖定處理之步驟。在步驟S301，作為資訊記憶裝置之記憶卡依據接收來自主裝置之隨機數產生要求指令之接收而產生隨機數(Rms)。產生之隨機數在步驟S302，被主裝置讀出，在步驟S303，與鎖定指令共同地取得已儲存於主裝置之記憶部之副ID (IDen)，再將隨機數(Rms)以已儲存於主裝置之記憶部之副鎖定鍵(LKen)加密，產生資料：E (LKen, Rms)，將此等連結資料：IDen、E (LKen, Rms)發送至作為資訊記憶裝置之記憶卡。

在步驟S304，記憶卡將接收之副ID (IDen)及加密資料：E (LKen, Rms)寫入資訊記憶裝置內之記憶體。在步驟S305，記憶卡利用適用儲存於本身之記憶體之鎖定主鍵(LMK)算出

504

接收之副ID(IDen)之雜湊值，即執行：

H(LMK, IDen)=LKen

以算出對應於接到之副ID(IDen)之副鎖定鍵(LKen)。

另外，記憶卡依據算出之副鎖定鍵(LKen)，執行前述在步驟S301所產生之隨機數(Rms)之加密處理，算出加密資料：E(LKen, Rms)，以作為核對用資料。

其次，記憶卡在步驟S306，執行在步驟S305算出之加密資料：E (LKen, Rms)和在步驟S303與鎖定指令共同地由主裝置所接收，且與在步驟S304儲存於記憶體之加密資料：E (LKen, Rms)之比較核對處理[E(LKen, Rms)=E(LKen, Rms)？]。

在此比較核對處理中，兩值相等時，判定主裝置屬於擁有作為正當之副ID (IDen)與副鎖定鍵(LKen)之組資料之副鍵組：[IDen, LKen]之正當機器，在步驟S307，執行對應於鎖定指令之鎖定處理，即，以作為適用後述之副鍵組：[IDen, LKen]之鎖定之解除處理之非鎖定處理之成功為條件，執行可對記憶體存取之設定。此時，將前述鎖定狀態旗標設定為EL=1。

另一方面，在步驟S306之比較核對處理中，判定E (LKen, Rms)=E(LKen, Rms)不成立時，判定在步驟S308中送來鎖定指令之主裝置屬於未擁有正確之副ID (IDen)與副鎖定鍵(LKen)之組資料之不正當機器，故不執行鎖定處理，而對主裝置發送有錯誤之通知。

依照上述之處理，被執行匯出鎖定之資訊記憶裝置若屬於擁有同一副鍵組：[IDen, LKen]作為執行鎖定處理之副ID

505

(IDen)與副鎖定鍵(LKen)之組資料之主裝置時，即可利用與在前述[依據鎖定主鍵(LMK)之處理]中所述之非鎖定處理相同之處理程序，執行非鎖定處理。即，可利用將適用之ID與鎖定鍵置換成副ID (IDen)與副鎖定鍵(LKen)之方式執行非鎖定處理。

但，未擁有與執行鎖定處理之副鍵組：[IDen, LKen]同一鍵組之其他主裝置只要不取得適用於鎖定處理之副鍵組：[IDen, LKen]，便無法執行資訊記憶裝置之鎖定解除，即無法存取。

具有作為正當之主ID (IDs)與主鎖定鍵(LKs)之組資料之主鍵組：[IDs, LKs]主裝置可由資訊記憶裝置取得儲存於被執行匯出鎖定之資訊記憶裝置之副鍵組：[IDen, LKen]，並適用所取得之副鍵組：[IDen, LKen]解除鎖定。經由資訊記憶裝置取得副鍵組：[IDen, LKen]之動作稱為印刷處理。

如此，依據某一副鍵組：[IDen, LKen]變成鎖定狀態，而可將該副鍵組：[IDen, LKen]輸出至其他主裝置之鎖定狀態稱為匯出鎖定狀態。

主裝置利用由處於匯出鎖定狀態之資訊記憶裝置，取得(印刷)適用於匯出鎖定處理之副鍵組：[IDen, LKen]時，即成為擁有同一副鍵組：[IDen, LKen]之多數主裝置構成之群之構成成員，其後，即可適用取得之副鍵組：[IDen, LKen]解除鎖定。以下，說明此印刷及鎖定解除處理(非鎖定處理)之詳細情形。

(印刷及非鎖定處理)

506

首先，說明主裝置由依據上述匯出鎖定處理被鎖定之資訊記憶裝置，取得副ID (IDen)與副鎖定鍵(LKen)組成之副鍵組：[IDen, LKen]之印刷處理及解除依據匯出鎖定處理被鎖定之資訊記憶裝置之鎖定之非鎖定處理。

圖13係表示在主裝置與資訊記憶裝置間所執行之印刷處理及非鎖定處理之處理順序圖。主裝置與資訊記憶裝置係被連接成可分別相互轉送資料之狀態。又，資訊記憶裝置之鎖定狀態旗標如圖所示，表示匯出鎖定為有效狀態之旗標：EL=1被分別設定於NVM、RAM。

主裝置並未具有適用於對資訊記憶裝置之匯出鎖定之副ID (IDen)與副鎖定鍵(LKen)組成之副鍵組：[IDen, LKen]，資訊記憶裝置將副鍵組：[IDen, LKen]儲存於匯出鎖定儲存區域。資訊記憶裝置處於所謂匯出鎖定狀態。

首先，主裝置對資訊記憶裝置輸出隨機數產生指令。接收到隨機數產生指令後，資訊記憶裝置即執行特定長度，例如16位元組隨機數(Rms)之產生處理，並對主裝置發送所產生之隨機數(Rms)、與先前匯出鎖定處理之際早已儲存於記憶體之副ID (IDen)(即適用於匯出鎖定處理之副鍵組：[IDen, LKen]中之副ID (IDen))。又，資訊記憶裝置將所產生之隨機數(Rms)儲存於控制部內之RAM等之記憶體。

由資訊記憶裝置接到副ID (IDen)與隨機數(Rms)之主裝置首先判定所接到之副ID (IDen)與自己之主ID (IDs)是否一致。一致時，可執行適用與前述適用LMK之處理(參照圖7)同樣之主鎖定鍵(LKs)之非鎖定。

507

接到之副ID (IDen)與自己之主ID (IDs)不一致時，表示係由其他主裝置執行鎖定，但可利用取得此接到之副ID (IDen)及副鎖定鍵(LKen)之印刷處理，而使自己屬於與執行適用副鍵組：[IDen, LKen]之匯出鎖定之其他主裝置同一群。

即，可執行印刷處理，分別取得副ID (IDen)及副鎖定鍵(LKen)，將作為此等之組資料之副鍵組：[IDen, LKen]儲存於自己之記憶體，而使自己屬於該群之主裝置，因此，可適用取得之副鍵組：[IDen, LKen]執行匯出鎖定之解除。執行印刷處理時，主裝置將由資訊記憶裝置接收之副ID (IDen)儲存於記憶體。

執行印刷處理之主裝置其次執行以已事先儲存於主裝置之記憶體內之主鎖定鍵(LKs)作為密碼處理鍵之接收隨機數(Rms)之密碼處理：E (LKs, Rms)，並將其結果資料和主ID (IDs)與標準鎖定指令發送至資訊記憶裝置。又，此鎖定處理由於係對已利用副鎖定鍵(LKen)執行匯出鎖定之資訊記憶裝置，再利用主鎖定鍵(LKs)施以標準鎖定之處理，故稱為重疊鎖定處理。

由主裝置接到主ID (IDs)與加密資料：E (LKs, Rms)之資訊記憶裝置首先對接到之主ID (IDs)，利用適用鎖定主鍵(LMK)之雜湊值算出處理，算出對應於主ID (IDs)之主鎖定鍵(LKs)。即利用：

LKs=H (LMK, IDs)

算出對應於主ID (IDs)主鎖定鍵(LKs)。

另外，資訊記憶裝置係對儲存於自己之記憶體之隨機數

Rms，執行適用上述雜湊值算出所求出之主鎖定鍵(LKs)之密碼處理：E (LKs, Rms)，並執行與由主裝置所接收之密碼處理資料：E(LKs, Rms)是否一致之核對處理。

來自主裝置之接收資料：E (LKs, Rms)、與本身算出之密碼處理資料：E (LKs, Rms)一致時，判定屬於來自具有作為正當之主ID (IDs)與主鎖定鍵(LKs)之組資料之主鍵組：[IDs, LKs]之主裝置之重疊鎖定處理要求，並執行重疊鎖定處理，然後對主裝置發送重疊鎖定完畢通知。

來自主裝置之接收資料：E (LKs, Rms)、與本身算出之密碼處理資料：E (LKs, Rms)不一致時，判定非屬於具有作為正當之主ID (IDs)與主鎖定鍵(LKs)之組資料之主鍵組：[IDs, LKs]之主裝置，並判定屬於來自不正當機器之重疊鎖定處理要求，故不執行重疊鎖定處理，而對主裝置發送有錯誤之通知。

又，資訊記憶裝置執行之重疊鎖定處理係在匯出鎖定狀態中再重疊執行標準鎖定之狀態，故資訊記憶裝置之鎖定狀態旗標如圖所示，係將表示匯出鎖定為有效狀態之旗標：EL=1分別設定於NVM、RAM，另外，將因重疊鎖定處理而表示標準鎖定為有效狀態之旗標：SL=1設定於RAM。又，設定於RAM之旗標資訊在電源斷電前會被拷貝至NVM。

另外，接到重疊鎖定完畢通知之主裝置會繼續執行印刷處理及鎖定解除。主裝置會再度將隨機數產生指令發送至資訊記憶裝置。

接到隨機數產生指令之資訊記憶裝置重新執行第2隨機數

509

(Rms2)之產生處理，

將產生之隨機數(Rms2)、

執行標準鎖定之主裝置之主ID (IDs)、適用於匯出鎖定處理之副ID (IDen)以及利用對應於主ID (IDs)之主鎖定鍵(LKs)將對應於副ID (IDen)之副鎖定鍵(LKen)加密之加密資料：E (LKs, LKen)之連結資料，

即：

IDs、Rms2、IDen、E (LKs, LKen)

發送至主裝置。又，資訊記憶裝置事先將產生之隨機數(Rms2)儲存於控制部內之RAM等之記憶體。

由資訊記憶裝置接收到資料：IDs、Rms2、IDen、E (LKs, LKen)之主裝置首先適用儲存於自己之記憶體之主鎖定鍵(LKs)，將加密資料：E (LKs, LKen)解碼，以取得副鎖定鍵(LKen)。此係對應於先取得之副ID (IDen)之副鎖定鍵(LKen)，將取得之副鍵組：[IDen, LKen]儲存於記憶體。利用此印刷程序，即可使此主裝置隸屬於群No.n(第n群)之群。

其次，主裝置持續執行資訊記憶裝置之鎖定解除處理。主裝置依據適用主鎖定鍵(LKs)將接收自資訊記憶裝置之加密資料：E (LKs, LKen)解碼所取得副鎖定鍵(LKen)，執行接收自資訊記憶裝置之隨機數(Rms2)之加密處理，產生加密資料：E (LKen, Rms2)，將其與解除鎖定指令共同地發送至資訊記憶裝置。

由主裝置，與解除鎖定指令共同地接收到加密資料：E (LKen, Rms2)之資訊記憶裝置首先對已儲存於自己之記憶體

510

之副ID (IDen)，利用適用鎖定主鍵(LMK)之雜湊值算出處理，算出對應於副ID(IDen)之副鎖定鍵(LKen)。即，利用

LKen=H(LMK, IDen)

算出對應於副ID(IDen)之副鎖定鍵(LKen)。

另外，資訊記憶裝置對已儲存於自己之記憶體之隨機數(Rms2)，執行利用適用上述雜湊值算出所求得之副鎖定鍵(LKen)之加密處理：E(LKen, Rms2)，並執行與接收自主裝置之加密處理資料：E(LKen, Rms2)是否一致之核對處理。

接收自主裝置之資料：E(LKen, Rms2)與自己算出之加密處理資料：E(LKen, Rms2)一致時，判定屬於來自具有正當之副ID (IDen)、與副鎖定鍵(LKen)之組資料之主裝置之鎖定解除，即非鎖定處理要求，並執行非鎖定處理，然後對主裝置發送解除鎖定完畢通知。

接收自主裝置之資料：E(LKen, Rms2)與自己算出之加密處理資料：E(LKen, Rms2)不一致時，判定非屬於具有正當之副ID (IDen)、與副鎖定鍵(LKen)之組資料之副鍵組：[IDen, LKen]之主裝置，並判定屬於來自不正當機器之解除鎖定要求，故不執行非鎖定處理，而對主裝置發送有錯誤之通知。

因非鎖定處理，鎖定狀態旗標由EL=1被變更成EL=0，且設定作為對匯出鎖定之重疊鎖定之標準鎖定也被解除，而使旗標由SL=1被變更為SL=0。即，標準鎖定與匯出鎖定之解除被一併解除。

又，鎖定狀態旗標之變更順序係採用首先改寫控制部內之RAM之儲存旗標，然後，適宜地，例如在執行電源斷電

511

前，將RAM內之旗標資訊拷貝至NVM，在電源再通電時，再將NVM內之旗標資訊拷貝至RAM之順序，控制部依據RAM內之旗標資訊執行存取限制處理。

其次，參照圖14及圖15所示之流程，說明由被執行依據匯出鎖定處理之鎖定之資訊記憶裝置取得副ID (IDen)、與副鎖定鍵(LKen)組成之副鍵組：[IDen, LKen]之印刷處理、及解除被執行依據匯出鎖定處理之鎖定之資訊記憶裝置之鎖定之非鎖定處理之步驟。

在步驟S401，作為資訊記憶裝置之記憶卡依據接收來自主裝置之隨機數產生要求指令之接收而產生隨機數(Rms)。產生之隨機數在步驟S402，與由先前執行匯出鎖定處理之主裝置發送至資訊記憶裝置，且被儲存於資訊記憶裝置之記憶體部之匯出鎖定鍵組儲存區域之副ID (IDen)共同地被主裝置讀出。主裝置在此時點取得副鍵組：[IDen, LKen]中之副ID (IDen)。

主裝置因確認在由記憶卡讀出之副ID (IDen)與自己之主ID (IDs)不一致，判斷資訊記憶裝置處於匯出鎖定狀態而非處於標準鎖定狀態。其次，主裝置在步驟S403，與作為重疊鎖定之標準鎖定指令共同地，將接收之隨機數(Rms)以主裝置之主鎖定鍵(LKs)加密後之資料：E (LKs, Rms)、與自己之主ID (IDs)發送至作為資訊記憶裝置之記憶卡。

在步驟S404，資訊記憶裝置(記憶卡)將接收自主裝置之主ID (IDs)、與加密資料：E (LKs, Rms)寫入資訊記憶裝置內之記憶體。在步驟S405，記憶卡對接收之主ID (IDs)，適用儲

512

存於本身之記憶體之鎖定主鍵(LMK)算出雜湊值，即執行：

H(LMK, IDs)=LKs

以算出對應於主ID(IDs)之主鎖定鍵(LKs)。

另外，記憶卡依據算出之主鎖定鍵(LKs)，執行先前在步驟S401所產生之隨機數(Rms)之加密處理，算出加密資料：E(LKs, Rms)，以作為核對用資料。

其次，記憶卡在步驟S406，執行在步驟S405算出之加密資料：E(LKs, Rms)和在步驟S403中與標準鎖定指令共同地由主裝置所接收，且在步驟S404儲存於記憶體之加密資料：E(LKs, Rms)之比較核對處理[E(LKs, Rms)=E(LKs, Rms)？]。

在此比較核對處理中，兩值相等時，判定主裝置屬於擁有作為正當之正確主ID (IDs)與主鎖定鍵(LKs)之組資料之主鍵組：[IDs, LKs]之正當機器，在步驟S407，執行對應於標準鎖定指令之標準鎖定處理。此處理係在匯出鎖定狀態中再重疊執行標準鎖定之處理。資訊記憶裝置之鎖定狀態旗標係將表示匯出鎖定、標準鎖定均為有效狀態之EL=1、SL=1設定於RAM。

另一方面，在步驟S406之比較核對處理中，判定兩值不相等時，判定在步驟S408中送來標準鎖定指令之主裝置屬於未擁有作為正當之主ID (IDs)與主鎖定鍵(LKs)之組資料之主鍵組：[IDs, LKs]之主裝置，故不執行重疊鎖定處理，而對主裝置發送有錯誤之通知。

欲執行作為步驟S407之重疊鎖定處理之標準鎖定，再執

513

行印刷處理、鎖定解除時，進入圖15之步驟S501。

接到重疊鎖定完畢通知之主裝置再度對資訊記憶裝置發送隨機數產生要求指令，接到隨機數產生指令之資訊記憶裝置在步驟S501重新執行第2隨機數(Rms2)之產生處理。

在步驟S502，主裝置由資訊記憶裝置讀出

隨機數(Rms2)、

執行標準鎖定之主裝置之主ID(IDs)、副ID(IDen)、以及

利用作為對應於主ID (IDs)之組資料之主鎖定鍵(LKs)將作為對應於副ID (IDen)之組資料之副鎖定鍵(LKen)加密之加密資料：E(LKs, LKen)、

此等之連結資料，即：[IDs、Rms2、IDen、E(LKs, LKen)]。

在步驟S503，主裝置發送作為對資訊記憶裝置之鎖定解除要求之非鎖定指令。主裝置將加密資料E (LKen, Rms2)併在此非鎖定指令中發送。

加密資料E (LKen, Rms2)之產生方法依據以下之步驟：在步驟S502，由資訊記憶裝置讀出資料：IDs、Rms2、IDen、E(LKs, LKen)之主裝置首先適用儲存於自己之記憶體之主鎖定鍵(LKs)，將加密資料：E(LKs, LKen)解碼，以取得副鎖定鍵(LKen)。此係對應於先取得之副ID (IDen)之副鎖定鍵(LKen)。其次，主裝置依據副鎖定鍵(LKen)執行接收自資訊記憶裝置之隨機數(Rms2)之加密處理，產生加密資料：E (LKen, Rms2)。

又，主裝置將取得之副鍵組：[IDen, LKen]儲存於記憶體，印刷處理即告完成。即，利用印刷處理，即可使此主裝

514

置隸屬於群No.n(第n群)之群。

在步驟S504，由主裝置取得加密資料：E(LKen, Rms2)之資訊記憶裝置將接收之資料：E(LKen, Rms2)寫入記憶體。另外，在步驟S505，執行核對用資料之算出。

核對用資料之算出處理依據以下步驟執行。首先，對儲存於自己之記憶體之副ID(IDen)，利用適用鎖定主鍵(LMK)之雜湊值算出處理，算出對應於副ID(IDen)之副鎖定鍵(LKen)。即，利用

LKen=H(LMK, IDen)

算出對應於副ID(IDen)之副鎖定鍵(LKen)。另外，對在步驟S501產生而儲存於自己之記憶體之隨機數Rms2，執行適用上述雜湊值算出所求出之副鎖定鍵(LKen)之密碼處理：E(LKen, Rms2)，以產生核對用資料。

在步驟S506，執行由主裝置所接收之資料：E(LKen, Rms2)與本身算出之密碼處理資料：E(LKen, Rms2)是否一致之核對處理。

來自主裝置之接收資料：E(LKen, Rms2)與本身算出之密碼處理資料：E(LKen, Rms2)一致時，判定屬於來自具有作為正當副ID(IDen)與副鎖定鍵(LKen)之組資料之副鍵組：[IDen, LKen]之主裝置之鎖定之解除，即非鎖定處理要求，進入步驟S507，執行非鎖定處理，然後對主裝置發送非鎖定完畢通知。不一致時，判定非屬於具有正當之副鍵組：[IDen, LKen]之主裝置，且判定屬於不正當機器之鎖定處理要求，故不執行非鎖定處理，而在步驟S508，對主裝置發

送有錯誤之通知。

依據本處理例，多數主裝置可擁有共通之副鍵組：[IDen, LKen]，執行利用1個資訊記憶裝置(記憶卡)之鎖定、非鎖定。又，副鍵組：[IDen, LKen]可藉執行匯出鎖定，經由資訊記憶裝置拷貝儲存至其他主裝置而可形成彈性之共用群。又，在副鍵組：[IDen, LKen]對主裝置之拷貝，即印刷中，由於係以擁有正當之主ID (IDs)與主鎖定鍵(LKs)，且可執行重疊鎖定處理為條件，故可防止副鍵組：[IDen, LKen]對不正當機器之拷貝(印刷)。

又，如參照圖10(c)所述，也可執行適用副鍵組：[IDen, LKen]之標準鎖定處理(=群鎖定處理)，執行此群鎖定處理時，副鍵組：[IDen, LKen]儲存於資訊記憶裝置之標準鎖定鍵儲存區域(參照圖10)，不會被拷貝輸出至其他主裝置。即，只有已取得同一副鍵組：[IDen, LKen]之主裝置才能以不附帶印刷處理之通常非鎖定處理之方式加以存取。

[鎖定狀態旗標之維持構成]

在以上之[在機器群之鎖定處理之構成]中，對處於匯出鎖定狀態之資訊記憶裝置執行非鎖定時，所有鎖定狀態(status)旗標被復位，即將表示匯出鎖定解除之EL=0、標準鎖定解除之SL=0設定於NVM、RAM。如此，保持EL=0、SL=0之設定不變，使電源斷電，然後，再使電源通電時，由於EL=0、SL=0設定於NVM，故控制部之RAM也處於SL=0、EL=0之設定狀態，表示所有鎖定狀態被解放，各主裝置可自由地執行對記憶體之存取。

516

如此，鎖定被解除之資訊記憶裝置因遺失或遭竊等而被第三者所取得時，第三者即可自由地加以存取。此種狀況，對儲存有秘密資訊之情形而言，並非好現象。

以下說明之例係專為解決上述問題而設計，此例採用下列構成：主裝置藉非鎖定處理而執行匯出鎖定之解除後，即使在電源斷電時，仍然維持匯出鎖定狀態，當電源再度通電時，只容許資訊記憶裝置以匯出鎖定之解除處理為條件執行存取。

本構成例與先前[在機器群之鎖定處理之構成]中參照圖9所說明之情形同樣地，在主裝置內之ROM等之記憶體中儲存主ID (IDs)、主鎖定鍵(LKs)組成之主鍵組：[IDs, LKs]，另外儲存可適用於匯出鎖定處理之作為副ID與副鎖定鍵之組資料之副鍵組：[IDen, LKen](n=1、2、・・)1個以上，在記憶卡等資訊記憶裝置內之控制部內之ROM等之記憶體中，儲存有鎖定主鍵(LMK)。儲存於資訊記憶裝置之鎖定主鍵(LMK)與儲存於主裝置之ID(含IDs及IDen)、鎖定鍵(LK(含LKs與LKen))具有以下之關係：

LK=H(LMK, ID)

依據主裝置之主ID (IDs)、主鎖定鍵(LKs)之鎖定處理、非鎖定處理係利用與前述[依據鎖定主鍵(LMK)之處理]中所說明同樣之順序執行，又，依據副ID (IDen)、副鎖定鍵(LKen)之鎖定處理係利用與前述[在機器群之鎖定處理之構成]中所說明同樣之順序執行。以下，說明有關本處理例之印刷及非鎖定處理中之鎖定狀態旗標之維持處理。

517

(印刷及非鎖定處理中之鎖定狀態旗標之維持處理)

茲參照圖16以下，說明主裝置由依據匯出鎖定處理被鎖定之資訊記憶裝置取得副鎖定鍵(LKen)與副ID (IDen)組成之副鍵組：[IDen, LKen]之印刷處理、解除依據匯出鎖定處理被鎖定之資訊記憶裝置之鎖定之非鎖定處理以及資訊記憶裝置所執行之鎖定狀態旗標之維持處理。

圖16所示之順序圖基本上與先前[在機器群之鎖定處理之構成]中參照圖13所說明之主裝置與資訊記憶裝置間執行之印刷處理與匯出鎖定之非鎖定處理之處理順序圖相同，其處理步驟亦同。

但，其不同之點在於：在作為順序圖之最終處理所執行之非解除完畢通知之後，資訊記憶裝置需要執行NVM旗標設定處理。在前述[在機器群之鎖定處理之構成]中所說明之處理中，執行匯出鎖定之非鎖定處理時，將表示匯出鎖定解除之EL=0、標準鎖定解除之SL=0設定於NVM、RAM。但在本構成中，將表示已執行匯出鎖定、標準鎖定之EL=1、SL=1設定於NVM。

參照圖17說明對NVM之鎖定狀態旗標設定處理之詳細情形。圖17之處理流程係說明在圖16(與圖13相同)之順序圖中，接收到鎖定解除要求(非鎖定指令)以後之資訊記憶裝置之處理步驟之流程。

首先，在步驟S601，資訊記憶裝置(記憶卡)接收到鎖定解除要求(非鎖定指令)時，作為用來判定可否執行非鎖定指令之驗證處理，在步驟S602，資訊記憶裝置執行與非鎖定

指令共同由主裝置所接收之加密資料：E (LKen, Rms2)和自己產生之加密資料：E (LKen, Rms2)之核對處理。此處理係與[在機器群之鎖定處理之構成]中所說明之處理相同。

來自主裝置之接收資料：E (LKen, Rms2)和自己算出之加密資料：E (LKen, Rms2)不一致時，在步驟S607，將有錯誤之通知送回主裝置後結束處理動作。

另一方面，來自主裝置之接收資料：E (LKen, Rms2)和自己算出之加密資料：E (LKen, Rms2)一致時，判定屬於來自具有正當副鍵組：[IDen, LKen]之主裝置之非鎖定處理要求，在步驟S603，執行非鎖定處理，然後對主裝置發送非鎖定完畢通知。

另外，資訊記憶裝置(記憶卡)在步驟S604，將儲存於控制部之RAM之鎖定狀態旗標(SL=1、EL=1)拷貝至NVM，將NVM之鎖定狀態旗標設定為SL=1、EL=1。SL=1表示已執行標準鎖定，EL=1表示已執行匯出鎖定。

步驟S604之旗標拷貝處理完畢時，再於步驟S605，執行控制部之RAM之鎖定狀態旗標(SL=1、EL=1)之復位，即將RAM之鎖定狀態旗標設定為SL=0、EL=0。SL=0表示未執行標準鎖定，EL=0表示未執行匯出鎖定。

此設定狀態，即，設定RAM之鎖定狀態旗標為SL=0、EL=0時，可自由執行記憶體存取，已執行非鎖定處理之主裝置可執行對資訊記憶裝置之記憶體部(圖3之記憶體部220)之存取。

但，其後，由主裝置抽出資訊記憶裝置(記憶卡)等時，

519

資訊記憶裝置(記憶卡)停止對主裝置之電源供應，在電源再度通電之時點，將設定於NVM之鎖定狀態旗標(SL=1、EL=1)資訊下載至控制部之RAM，於是，控制部即可執行依據設定於RAM之鎖定狀態旗標(SL=1、EL=1)之處理。其次，參照圖18之處理流程，說明有關資訊記憶裝置之電源再通電後之處理情形。

圖18之處理流程係表示資訊記憶裝置之電源斷電後，再度轉移至通電狀態時之處理情形。

在步驟S701，因資訊記憶裝置(記憶卡)裝定於主裝置等，而由電源斷電狀態轉移至電源通電狀態時，在步驟S702，資訊記憶裝置將儲存於NVM之鎖定狀態旗標(SL、EL)拷貝至控制部之RAM。控制部依據RAM之狀態旗標執行控制。

在步驟S703，由所連接之主裝置輸入記憶體存取要求或非鎖定指令時，資訊記憶裝置之控制部參照RAM之鎖定狀態旗標。

在步驟S704，判定RAM之狀態旗標為EL=1時，在步驟S705，執行鎖定解除處理(圖13~圖15)。此時，主裝置未擁有適用於該資訊記憶裝置之匯出鎖定之副鍵組：[IDen, LKen]時，有必要執行印刷處理。在此處理中，利用先前參照圖13~圖15所述之驗證，確認屬於來自正當之主裝置之非鎖定要求時，執行非鎖定處理(步驟S708：Yes)，在步驟S709，允許其執行記憶體存取。驗證結果判定屬於來自不正當之主裝置之非鎖定要求時，不執行非鎖定處理(步驟S708：No)，而執行錯誤通知(步驟S710)。

520

又，在步驟S704，判定RAM之狀態旗標為EL=0時，在步驟S706，判定RAM之狀態旗標是否為SL=1。判定RAM之狀態旗標為SL=1時，在步驟S707，執行標準鎖定解除處理(圖7~圖8)。利用先前參照圖7~圖8所述之驗證，確認屬於來自正當之主裝置之非鎖定要求時，執行非鎖定處理(步驟S708：Yes)，在步驟S709，允許其執行記憶體存取。驗證結果判定屬於來自不正當之主裝置之非鎖定要求時，不執行非鎖定處理(步驟S708：No)，而執行錯誤通知(步驟S710)。

在步驟S704，判定RAM之狀態旗標為EL=0，且在步驟S706，判定RAM之狀態旗標為SL=0時，表示非處於鎖定狀態，進入步驟S709，允許其執行記憶體存取。

如前面參照圖16、圖17所述，利用某一主裝置解除匯出鎖定，其後，電源斷電時，將NVM之鎖定狀態旗標設定為SL=1、EL=1，其後，在電源通電之時點，將RAM之鎖定狀態旗標設定為SL=1、EL=1，圖18之處理流程中在步驟S704之判定(EL=1？)之結果為Yes，故可執行以步驟S705之處理，即匯出鎖定解除處理(圖13~圖15)為條件之記憶體存取。

如以上所述，在本處理例中，對於是否為容許可適用於鎖定處理或非鎖定處理之鍵組輸出至外部之鎖定狀態之匯出鎖定(EL)狀態及是否為不容許可適用於鎖定處理或非鎖定處理之鍵組輸出至外部之鎖定狀態之標準鎖定(SL)狀態之問題，由於採用將可供判別之狀態資訊組成之鎖定狀態旗標之非鎖定處理前之資訊儲存於NVM之構成方式，故在資訊記憶裝置之電源斷電後電源再度通電時，可依據儲存

521

於NVM之旗標忠實地重現非鎖定處理前之鎖定狀態。

依據本處理例，例如，即使在某一主裝置執行匯出鎖定之解除時，仍可維持匯出鎖定狀態，在資訊記憶裝置之電源斷電後電源再度通電時，可容許執行已鎖定之解除處理為條件之記憶體存取。因此，擁有正當之主鍵組：[IDs, LKs]主裝置再執行包含前述重疊鎖定處理之特定程序時，才能解除鎖定，可藉此排除不正當裝置之存取動作。

[依據讀出檢測特定資料區域之自動鎖定處理]

其次，說明有關在資訊記憶裝置(記憶卡)之控制部監視資料由資訊記憶裝置對主裝置之讀出，並以執行某一預定資料區域(例如特定叢集)之讀出作為觸發器而執行鎖定處理之處理例。

儲存於資訊記憶裝置(記憶卡)之記憶體部(圖2之記憶體部220)之資料之讀出係被例如依據儲存資料而產生之播放管理檔案(PBLIST)所管理，在控制部中，依據播放管理檔案，由記憶體部(圖2之記憶體部220)讀出資料後，輸出至主裝置。

資料被讀出時，資訊記憶裝置之控制部可執行讀出資料之監視。例如，ATRAC3所壓縮之音頻資料可利用特定資料單位之叢集作為讀出資料單位加以監視。

如圖19所示，ATRAC3所壓縮之音頻資料係由多數個最小資料單位之SU(聲音單元)集合成1個叢集，再由多數個叢集構成1個聲部。SU(聲音單元)係將44.1 kHz之抽樣頻率所獲得之1024樣本份(1024×16位元×2通道)之音頻資料壓縮成約

522

1/10之數百位元組之資料，叢集係由多數SU(例如42個SU)構成之資料。1個叢集由42個SU構成時，1個叢集可表示約1秒之聲音。

各叢集附有各叢集固有之邏輯號碼，可利用邏輯號碼加以管理。資訊記憶裝置之控制部210(參照圖3)可依據邏輯號碼檢查有無讀出特定叢集。例如，輸出資料為某一音樂之內容時，抽出相當於該音樂內容之前奏或幽雅聲音部分之1個以上之叢集之邏輯號碼，作為對應於該內容之鎖定對應叢集，並將所抽出之叢集邏輯號碼設定作為對應於內容之編目資訊而一併儲存於儲存內容之記憶體部(快閃記憶體)。

讀出內容時，將編目資訊一次儲存於資訊記憶裝置之控制部內之記憶體(RAM)，在控制部中，執行讀出內容之叢集與鎖定對應叢集之核對處理，讀出內容之叢集與鎖定對應叢集之邏輯號碼一致時，執行鎖定處理。又，鎖定處理之時間可設定於鎖定對應叢集之讀出開始時點、鎖定對應叢集之讀出結束時點或具有鎖定對應叢集之整個內容之讀出結束時點等各種時點，執行對應於設定之檢測處理，並依據設定條件之檢測執行鎖定處理。執行鎖定時，欲再度讀出時，必須執行非鎖定處理。

以下，參照圖20，說明在資訊記憶裝置之控制部210中，以由記憶體部220(參照圖3)讀出特定資料區域(例如特定叢集)為條件而執行鎖定處理之處理情形。

又，在圖20之處理流程中，為了簡化說明，僅記載標準鎖定(SL)之部分，但匯出鎖定(EL)部分，也可執行同樣之

523

處理。

首先，在步驟S801，資訊記憶裝置之電源通電時，在步驟S802，儲存於NVM之鎖定狀態旗標被儲存於控制部210(參照圖3)內之RAM 213。控制部執行對應於RAM 213之狀態旗標之控制。

在步驟S803，判定標準鎖定是否為SL=1，即是否為鎖定狀態。為SL=1時，在步驟S804，執行非鎖定處理。非鎖定處理例如係與參照圖7、圖8所示之處理相同之處理。

利用資訊記憶裝置之驗證處理，驗證主裝置擁有正當之主ID與主鎖定鍵時，非鎖定成功(步驟S805：Yes)，而進入步驟S806。非鎖定失敗時，在步驟S810，執行對主裝置之錯誤通知而結束處理。

在步驟S806，依據非鎖定之成功，執行RAM、NVM之鎖定狀態旗標之更新，即執行表示鎖定解除狀態之SL=0之設定。

其次，由主裝置開始讀出資料時，資訊記憶裝置之控制部在步驟S807，執行事先設定之對應於鎖定叢集有無讀出處理之監視。當檢測出有讀出鎖定對應叢集之資料時，在步驟S808，將控制部210(參照圖3)內之RAM 213之鎖定狀態旗標設定為鎖定狀態(SL=1)。再於步驟S809，將NVM之鎖定狀態旗標設定為鎖定狀態(SL=1)。

如此，利用執行特定叢集之讀出處理，即可執行鎖定，其後，欲再度執行讀出處理時，必須執行非鎖定處理。非鎖定處理僅具有與執行鎖定相同之主ID (IDs)與主鎖定鍵

524

(LKs)之主裝置才能執行，故可防止已被鎖定之資訊記憶裝置(記憶卡)遭到濫用。

另外，也可採用在資訊記憶裝置電源斷電時解除鎖定資訊之設定，或如前所述，採用在電源斷電時將鎖定狀態旗標置於NVM，在電源再通電時，將NVM之鎖定狀態旗標拷貝至RAM，以維持電源斷電前之鎖定狀態而予以重現之構成。

如此，在本處理例中，可實現在非鎖定處理後，欲執行資料讀出處理時僅能讀出1次之所謂1次唯讀之存取限制處理之構成。

又，在圖20之處理例中，雖僅顯示標準鎖定之情形，但在匯出鎖定之情形也可採用同樣之構成，即，採用以特定資料區域之讀出作為觸發器而執行匯出鎖定之構成。

[主裝置之鎖定狀態之提示構成]

其次，說明有關在對可取得各種鎖定狀態之資訊記憶裝置執行存取之主裝置中，用於檢測資訊記憶裝置之鎖定狀態之提示構成及提示處理之情形。

圖21係表示鎖定/非鎖定專用機器之鎖定狀態提示指示器與具有各種開關之構成例。具有作為資訊記憶裝置之記憶卡710與可轉送資料之介面之鎖定/非鎖定專用機器720作為鎖定狀態指示器，具有：

表示鎖定解除狀態之[Unlocked(非鎖定)]指示器721

表示鎖定狀態之[Locked(鎖定)]指示器722

表示匯出鎖定狀態之[E-Locked(匯出鎖定)]指示器723

525

表示有錯誤之通知之[ERR(錯誤)]指示器724。

又，作為各種處理要求開關，具有：

作為鎖定解除處理要求開關之[Unlock(非鎖定)]開關731

作為利用主鍵組之標準鎖定處理要求開關之[P-Lock]開關732

作為利用副鍵組之標準鎖定(群鎖定)處理要求開關之[G-Lock]開關733

作為利用副鍵組之匯出鎖定處理要求開關之[E-Lock]開關734。

另外，圖21(b)所示之鎖定/非鎖定專用機器之例除了上述開關外，尚有[Imprint(印刷)]開關735，此開關係作為僅執行將儲存於匯出鎖定狀態之資訊記憶裝置之副ID(IDen)與副鎖定鍵(LKen)，即副鍵組：[IDen, LKen]儲存至主裝置之印刷處理之執行要求開關之用。

又，在圖21中，雖顯示鎖定/非鎖定專用機器之指示器構成與處理要求開關之構成例，但如前所示，主裝置中包含PC、PDA等資訊處理裝置、DSC等數位攝影機、攜帶式通訊終端等各種裝置，在此等裝置中，可採用經由各輸入手段對資訊記憶裝置(記憶卡)送出指令之構成。又，鎖定狀態顯示處理也可在各機器中，採用顯示於LCD等顯示器或利用聲音、警告聲等發出通知之構成方式。

茲參照圖22以下，說明有關在主裝置之鎖定狀態提示處理及由主裝置對資訊記憶裝置(記憶卡)之指令發送處理之情形。

526

圖22係說明例如將資訊記憶裝置(記憶卡)連接於主裝置時所執行之鎖定狀態讀出處理之流程。鎖定狀態讀出處理固然可構成利用用戶輸入指令而執行之方式，但也可構成將資訊記憶裝置(記憶卡)連接於主裝置時即可自動執行之方式。

在步驟S901，鎖定狀態由資訊記憶裝置被讀出。此狀態資訊係依據儲存於先前所述之資訊記憶裝置之控制部210(參照圖3)內之RAM 213之鎖定狀態旗標。在步驟S902，對應於鎖定狀態之指示器721~724依據此鎖定狀態讀出資訊而點亮。即，執行標準鎖定、群鎖定時，顯示(點亮)表示鎖定狀態之[Locked(鎖定)]指示器722，執行匯出鎖定時，顯示(點亮)表示匯出鎖定狀態之[E-Locked(匯出鎖定)]指示器723，不處於鎖定狀態時，顯示(點亮)表示鎖定解除狀態之[Unlocked(非鎖定)]指示器721。

其次，參照圖23說明鎖定處理要求、依據執行之指示器顯示處理之情形。鎖定處理係依據圖21之處理要求開關732~734之開關輸入動作而被執行。

適用主ID (IDs)與主鎖定鍵(LKs)之主鍵組：[IDs, LKs]之標準鎖定處理要求之情形，利用[P-Lock]開關732執行輸入，適用副ID (IDen)與副鎖定鍵(LKen)之副鍵組：[IDen, LKen]之匯出鎖定處理要求之情形，利用[E-Lock]開關734執行輸入，適用副鍵組：[IDen, LKen]之標準鎖定，即群鎖定處理要求之情形，利用[G-Lock]開關733執行輸入。

接收到此等開關中之一種輸入時，在步驟S911，檢測資

訊記憶裝置(記憶卡)之鎖定狀態，不處於非鎖定狀態時，在步驟S914，執行ERR(錯誤)指示器之顯示。處於非鎖定狀態時，在步驟S912，執行標準鎖定處理或匯出鎖定處理或群鎖定處理中之一種，鎖定處理完畢後，執行主裝置之對應鎖定指示器，即，表示鎖定狀態之[Locked(鎖定)]指示器722、或表示匯出鎖定狀態之[E-Locked(匯出鎖定)]指示器723之顯示。

其次，參照圖24說明非鎖定處理時之主裝置之操作、指示器之顯示情形。

非鎖定處理係利用按下圖21之非鎖定要求開關731之方式執行。按下非鎖定要求開關時，首先執行資訊記憶裝置之鎖定狀態之檢測。狀態之檢測係依據先前說明之控制部內之RAM之鎖定狀態旗標執行。不處於鎖定狀態時(步驟S921：No)，在步驟S923，執行ERR(錯誤)指示器724之顯示。

又，在步驟S922之鎖定狀態讀出中，判定資訊記憶裝置處於匯出鎖定狀態或標準鎖定狀態。依據前述之鎖定狀態旗標識別處於匯出鎖定狀態或標準鎖定狀態。然後，依據識別結果，使對應於圖21所示之鎖定狀態之指示器721~724點亮。

首先，屬於匯出鎖定時(步驟S924：Yes)，執行前述參照圖16至圖18所述之印刷及非鎖定處理。即，執行步驟S925所示依據主ID (IDs)與主鎖定鍵(LKs)之重疊鎖定處理、步驟S926之副ID (IDen)與副鎖定鍵(LKen)之印刷(輸入儲存)處理以及步驟S927之適用副ID (IDen)與副鎖定鍵(LKen)之鎖定解

528

除處理。此處理之詳細情形如前述參照圖16至圖18所說明。利用此等處理解除鎖定時，在步驟S928，鎖定解除指示器721執行其顯示。

在步驟S924，判定處於匯出鎖定以外之鎖定狀態，即處於標準鎖定狀態時，在步驟S929，判定是否被執行標準鎖定，有被執行標準鎖定時，在步驟S930，執行非鎖定處理。適用於此非鎖定處理之鍵組為主鍵組：[IDs, LKs]，或在群鎖定之情形時，為副鍵組：[IDen, LKen]。在步驟S928，鎖定解除指示器721執行其顯示。

在步驟S924，判定處於匯出鎖定以外之鎖定狀態，在步驟S929，判定非為標準鎖定時，進入步驟S931，使ERR(錯誤)指示器724執行顯示。

以上，一面參照特定之實施例，一面詳細說明本發明，但顯然地，本業業者在不脫離本發明之要旨之範圍內，可對該實施例進行修正及代用。即，以上之說明係以例示之形態揭示本發明，本發明之內容不應受到限定性之解釋。為判斷本發明之要旨，應參酌後述申請專利範圍之項所記載。

又，專利說明書中所說明之一連串之處理可利用硬體或軟體或兩者之複合構成予以執行。執行利用軟體之處理時，可將記錄處理順序之程式安裝於裝入專用之硬體之電腦內之記憶體而使其執行，或將程式安裝於可執行各種處理之通用電腦而使其執行。

例如，程式可預先記錄於作為記錄媒體之硬碟及ROM

(Read Only Memory：唯讀記憶體)。或者，程式可暫時地或永續地儲存(記錄)於軟碟、CD-ROM (Compact Disc Read Only Memory：音碟唯讀記憶體)、MO (Magneto optical：磁光)碟、DVD (Digital Versatile Disc；數位多用途光碟)、磁碟、半導體記憶體等可裝卸記錄媒體。此種可裝卸記錄媒體可以所謂套裝軟體之形態提供。

又，程式除了由上述可裝卸記錄媒體安裝至電腦以外，也可由下載網站無線轉送至電腦，或經由LAN (Local Area Network；區域網路)、網際網路等網路有線轉送至電腦，電腦可接收如此轉送來之程式，將其安裝於內建之硬碟等記錄媒體。

又，記載於專利說明書之各種處理不僅依照記載以時間系列執行以外，也可依照執行處理之裝置之處理能力或依照需要，並行地或個別地執行。又，在本專利說明書中，所謂系統，係指多數裝置之邏輯的集合構成，各構成之裝置不限於設置在同一框體內。

產業上之可利用性

如以上所說明，依據本發明之構成，由於係在記憶卡等資訊記憶裝置中，在由PC等資訊處理裝置輸入記憶體之鎖定處理要求指令或要求解除鎖定之非鎖定處理要求指令，以執行對應於輸入指令之處理之際，採用依據對應於輸出指令之資訊處理裝置所設定之識別符(ID)，執行資訊處理裝置是否具有含該識別符(ID)之正當之鍵組之驗證處理，並以該驗證成立為條件，依據前述指令執行處理之構成，

因此，可實現在安全管理下之記憶體存取控制。

另外，依據本發明之構成，由於構成可儲存包含資訊處理裝置之固有ID (ID)與對應於該固有ID之鎖定鍵(LK)之鍵組[ID, LK]，另一方面，資訊記憶裝置儲存可算出鎖定鍵(LK)，以作為適用LK=H (LMK, ID)之關係，即對ID之鎖定主鍵(LMK)之雜湊值之鎖定主鍵(LMK)，依據由適用前述鎖定主鍵(LMK)之雜湊值之算出所取得之鎖定鍵(LK)，執行由資訊處理裝置輸入之資訊處理裝置固有之鍵組之驗證處理，因此，可依據1個鎖定主鍵(LMK)執行對多數不同之鎖定鍵(LK)之驗證。

另外，依據本發明之構成，由於在資訊記憶裝置之驗證中，係構成可在資訊記憶裝置側執行隨機數產生處理，由該資訊處理裝置接收依據資訊處理裝置所具有之鎖定鍵(LK)之隨機數(Rms)之加密資料[E (Lk, Rms)]，以執行該接收之加密資料、與依據前述雜湊值之算出所取得之鎖定鍵(LK)所算出之加密資料[E (Lk, Rms)]之核對，因此，可執行適用每次核對時不同之隨機數之驗證，排除利用過去之核對史資料之不正確之存取。

【圖式簡單說明】

圖1係本發明之資訊記憶裝置之利用形態之概要之說明圖。

圖2係表示利用資訊記憶裝置之主裝置之硬體構成例之圖。

圖3係表示資訊記憶裝置之硬體構成例之圖。

圖4係本發明之資訊記憶裝置及主裝置之儲存資料之說明圖。

531

圖5係對資訊記憶裝置之鎖定處理中之資訊記憶裝置與主裝置間之通訊處理順序之說明圖。

圖6係表示說明對資訊記憶裝置之鎖定處理之處理流程之圖。

圖7係對資訊記憶裝置之非鎖定處理中之資訊記憶裝置與主裝置間之通訊處理順序之說明圖。

圖8係表示說明對資訊記憶裝置之非鎖定處理之處理流程之圖。

圖9係本發明之資訊記憶裝置及主裝置之儲存資料之說明圖。

圖10係對本發明之資訊記憶裝置之鎖定處理形態之說明圖。

圖11係適用對資訊記憶裝置之副鍵組之鎖定處理中之資訊記憶裝置與主裝置間之通訊處理順序之說明圖。

圖12係表示說明適用對資訊記憶裝置之副鍵組之鎖定處理之處理流程圖。

圖13係適用對資訊記憶裝置之印刷及副鍵組之非鎖定處理中之資訊記憶裝置與主裝置間之通訊處理順序之說明圖。

圖14係表示說明適用對資訊記憶裝置之印刷及副鍵組之非鎖定處理之流程圖。

圖15係表示說明適用對資訊記憶裝置之印刷及副鍵組之非鎖定處理之流程圖。

圖16係表示說明適用對資訊記憶裝置之印刷及副鍵組之非鎖定處理之資訊記憶裝置與主裝置間之通訊處理順序之

532

說明圖。

圖17係表示說明適用對資訊記憶裝置之印刷及副鍵組之非鎖定處理之鎖定狀態旗標之更新處理之流程圖。

圖18係說明對資訊記憶裝置之非鎖定處理之鎖定狀態旗標之參照處理之流程圖。

圖19係對資訊記憶裝置之資料儲存形態之叢集構成之說明圖。

圖20係依據特定資料區域(叢集)之讀出而執行鎖定處理之流程說明圖。

圖21(a)、(b)係對資訊記憶裝置之鎖定/非鎖定執行機器之構成之說明圖。

圖22係主裝置之鎖定狀態讀出處理之流程圖。

圖23係說明主裝置之鎖定處理時之處理及指示器顯示處理之流程圖。

圖24係說明主裝置之非鎖定處理時之處理及指示器顯示處理之流程圖。

【圖式代表符號說明】

20	資訊處理裝置
21	PC
23	PDA
24	攜帶式終端
25	數位攝影機
104	DSP
105	數位類比變換電路

533

106	放大電路
107	聲音輸出部
108	顯示控制器
109	顯示部
113	記憶裝置I/F
210	控制部
214	機器介面
216	記憶體介面
220	記憶體部
512	鎖定・解除鎖定用機器
532	副鍵組
541	標準鎖定鍵組儲存區域
542	匯出鎖定鍵組儲存區域
551	鎖定狀態旗標
30, 710	記憶卡
101, 211	CPU
102, 212	ROM
103, 213	RAM
310, 510	主裝置
312, 720	鎖定・非鎖定用機器
30, 520, 200, 320	資訊記憶裝置
315, 325, 515, 525	記憶體
721~724	指示器

534

731~735	開關
111	操作輸入部
112	輸入I/F
110	操作輸入部控制器
113	記憶裝置I/F(記憶卡I/F)
115	輸出入I/F (USB、IEEE 1394等)

535

伍、中文發明摘要：

本發明係用於提供依據存取要求單位所輸出之鍵組之驗證，執行作為記憶體之存取控制處理之鎖定、解除鎖定之裝置及方法。在記憶卡等資訊記憶裝置中，在由PC等資訊處理裝置輸入記憶體之鎖定處理要求指令、或要求解除鎖定之非鎖定處理要求指令，以執行對應於輸入指令之處理之際，針對資訊處理裝置是否具有由ID及鎖定鍵(LK)組成之正當之鍵組之問題，適用由LK=H (LMK, ID)之關係組成之鎖定主鍵(LMK)執行其驗證處理，並以驗證成立為條件，依據前述指令執行其處理動作。

陸、日文發明摘要：

メモリのアクセス制御処理としてのロック、アンロックをアクセス要求元の出力するキーセットの検証に基づいて実行する装置および方法を提供する。メモリカード等の情報記憶装置において、ＰＣ等の情報処理装置からメモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力し、入力コマンドに応じた処理を実行する際に、情報処理装置がＩＤおよびロックキー（ＬＫ）からなる正当なキーセットを有しているか否かの検証処理を、ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係からなるロックマスターキー（ＬＭＫ）を適用して実行する。検証の成立を条件として、前記コマンドに基づく処理を実行する。

柒、指定代表圖：

(一)本案指定代表圖為：第(4)圖。

(二)本代表圖之元件代表符號簡單說明：

310	主裝置
312	鎖定・非鎖定用機器
320	資訊記憶裝置
315, 325	記憶體

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

拾壹、圖式：

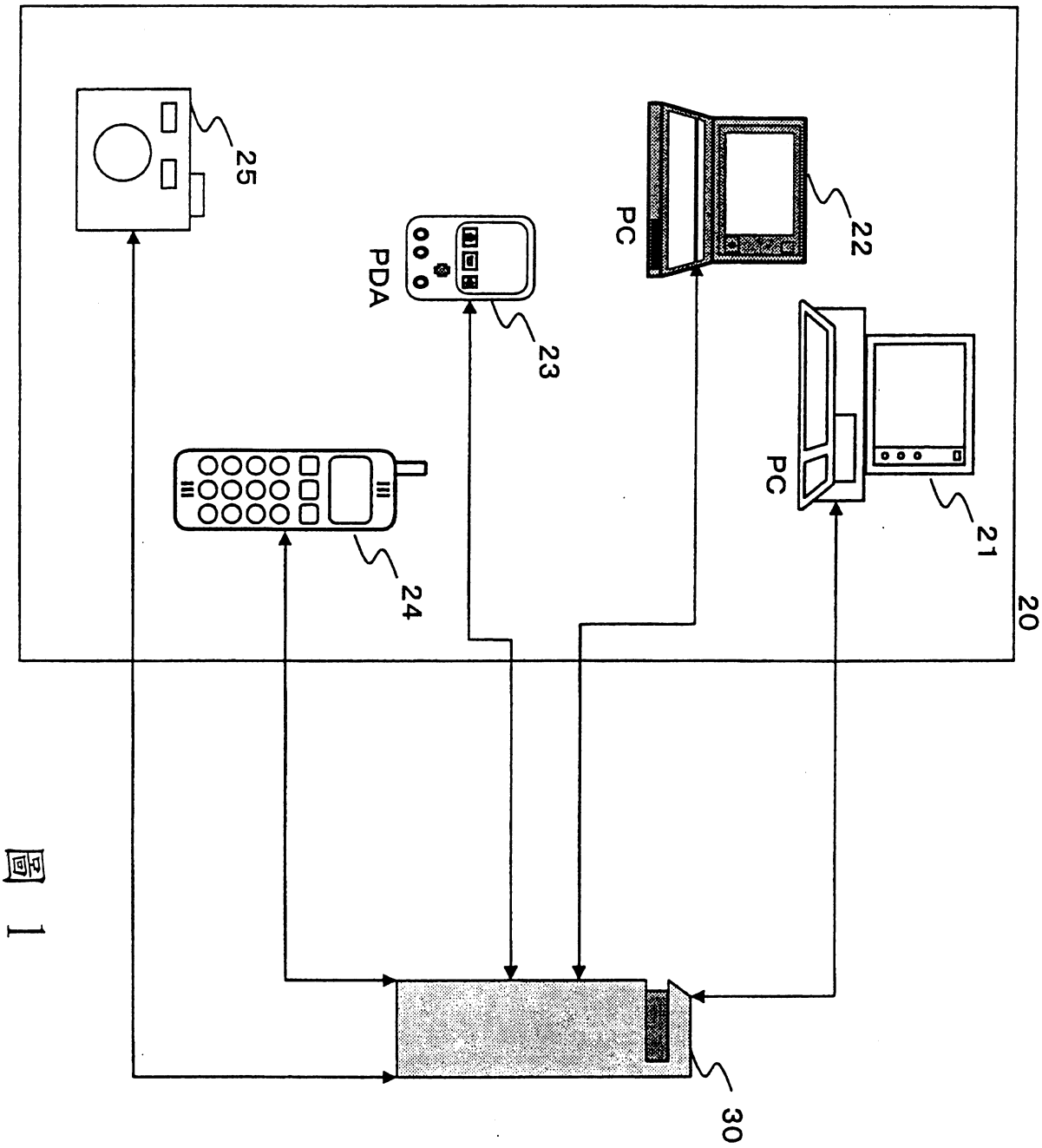


圖 1

542

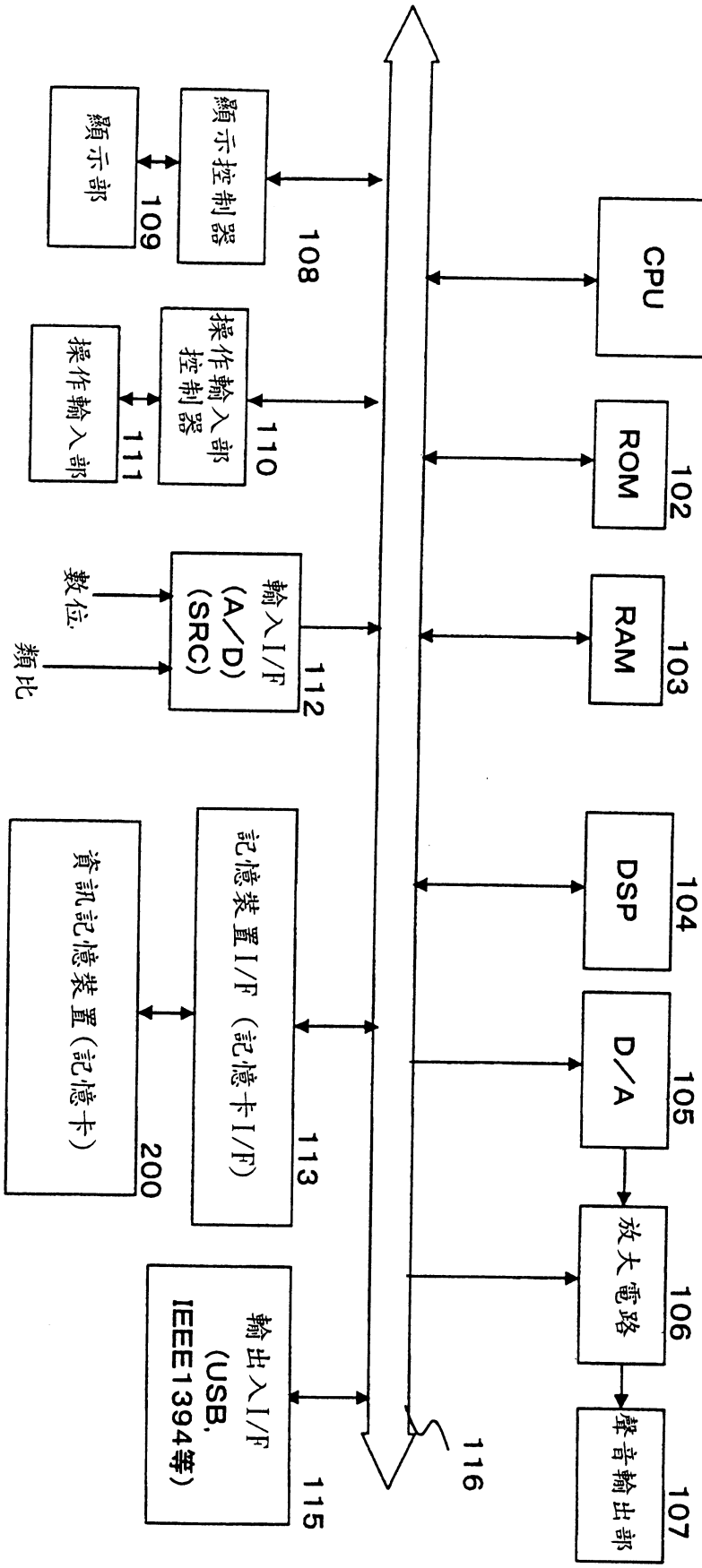

101
CPU
ROM
102
RAM
103
DSP
104
D／A
105
放大電路
106
聲音輸出部
107
116
115
輸出入I/F
(USB,
IEEE1394等)
113
記憶裝置I/F（記憶卡I/F）
200
資訊記憶裝置（記憶卡）
112
輸入I/F
(A／D)
(SRC)
數位.
類比
108
顯示控制器
109
顯示部
110
操作輸入部
控制器
111
操作輸入部

圖 2

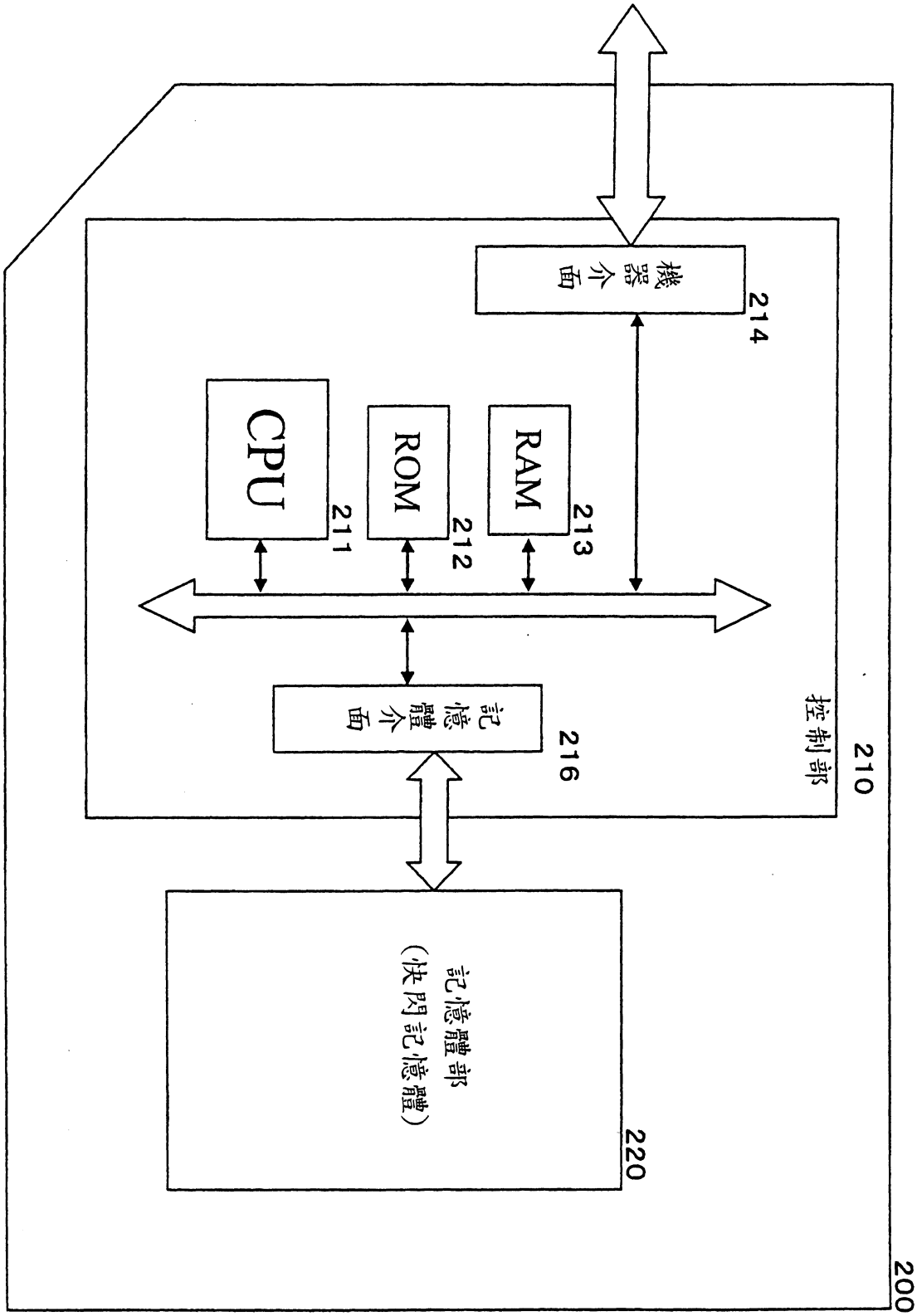

機器介面
214
CPU
211
ROM
212
RAM
213
記憶體介面
216
控制部
210
記憶體部
(快閃記憶體)
220
200

圖 3

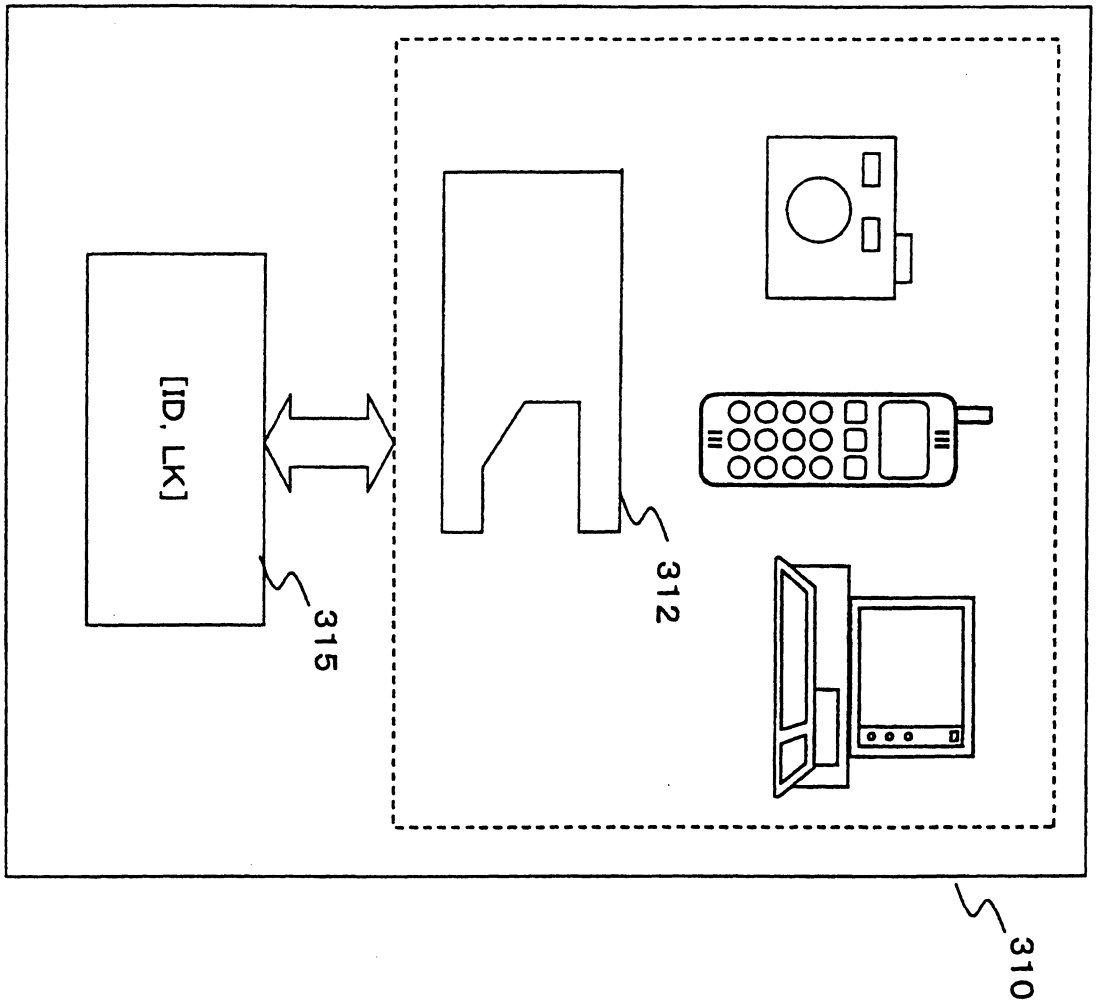
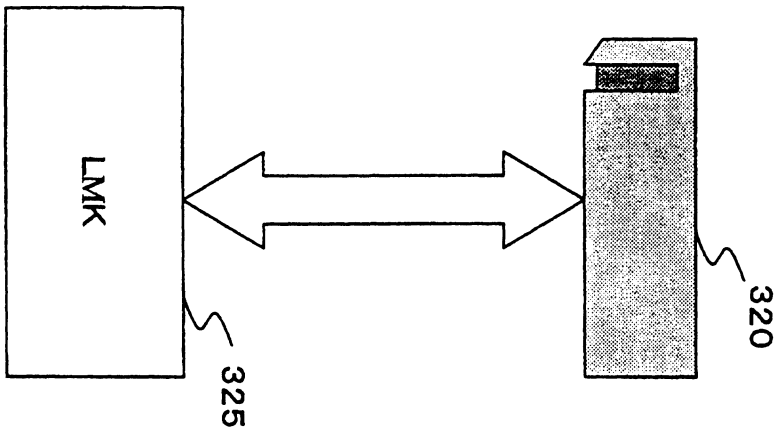


圖 4



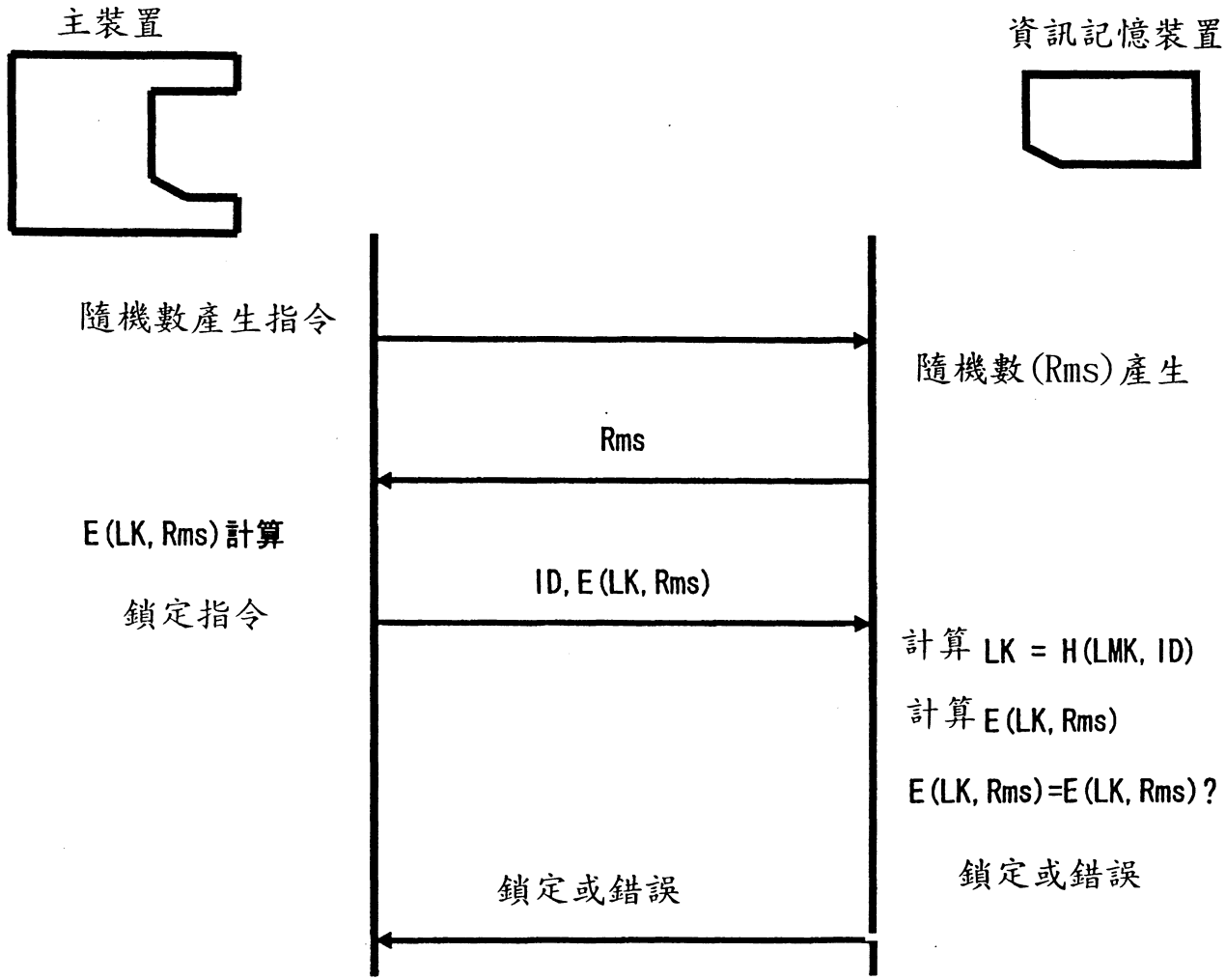

主裝置
資訊記憶裝置
隨機數產生指令
隨機數(Rms)產生
Rms
E(LK, Rms)計算
ID, E(LK, Rms)
鎖定指令
計算 LK = H(LMK, ID)
計算 E(LK, Rms)
E(LK, Rms)=E(LK, Rms)?
鎖定或錯誤
鎖定或錯誤

圖 5

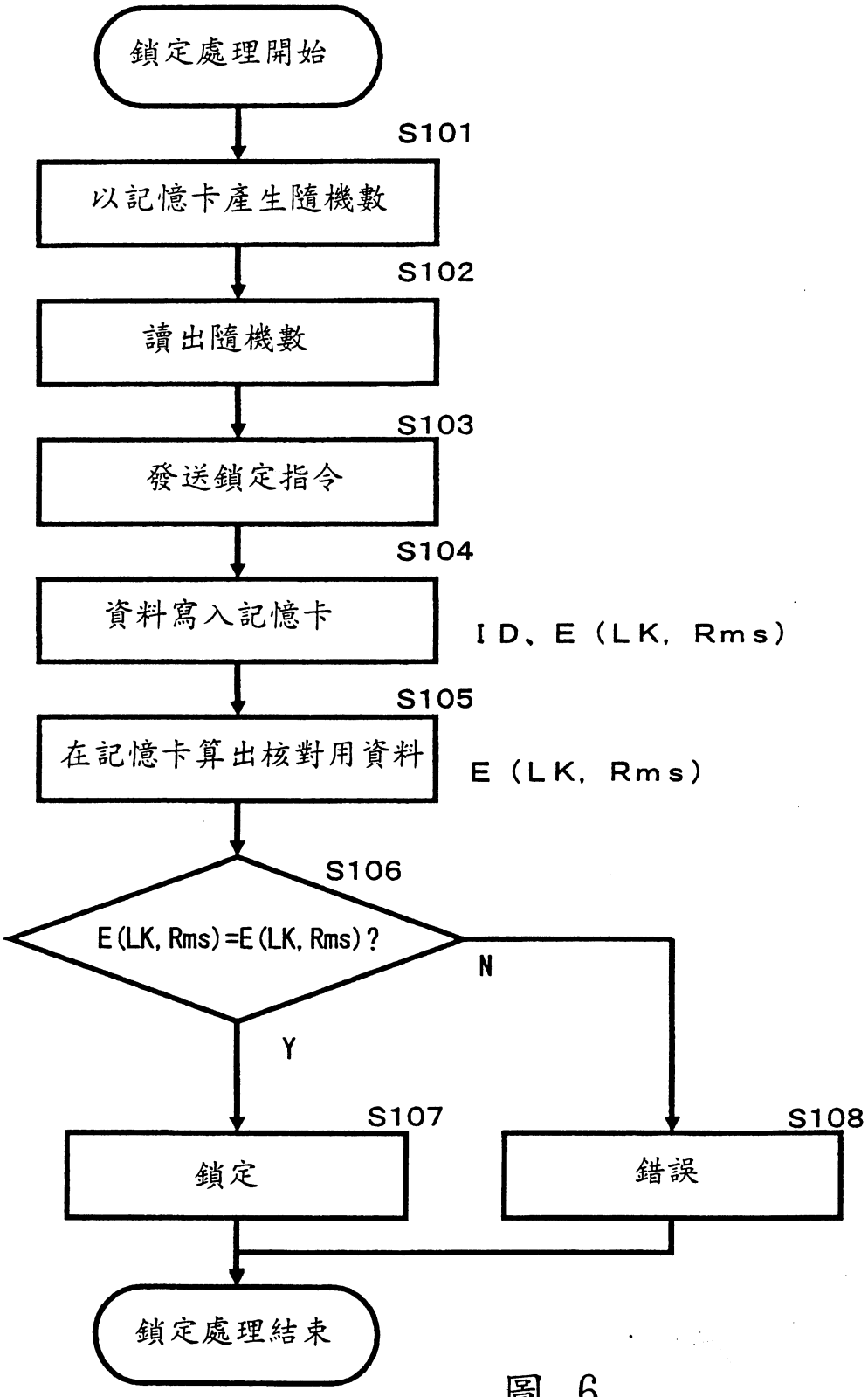

鎖定處理開始
S101
以記憶卡產生隨機數
S102
讀出隨機數
S103
發送鎖定指令
S104
資料寫入記憶卡
ID、E（LK, Rms）
S105
在記憶卡算出核對用資料
E（LK, Rms）
S106
E(LK, Rms)=E(LK, Rms)?
N
Y
S107
鎖定
S108
錯誤
鎖定處理結束

圖 6

547

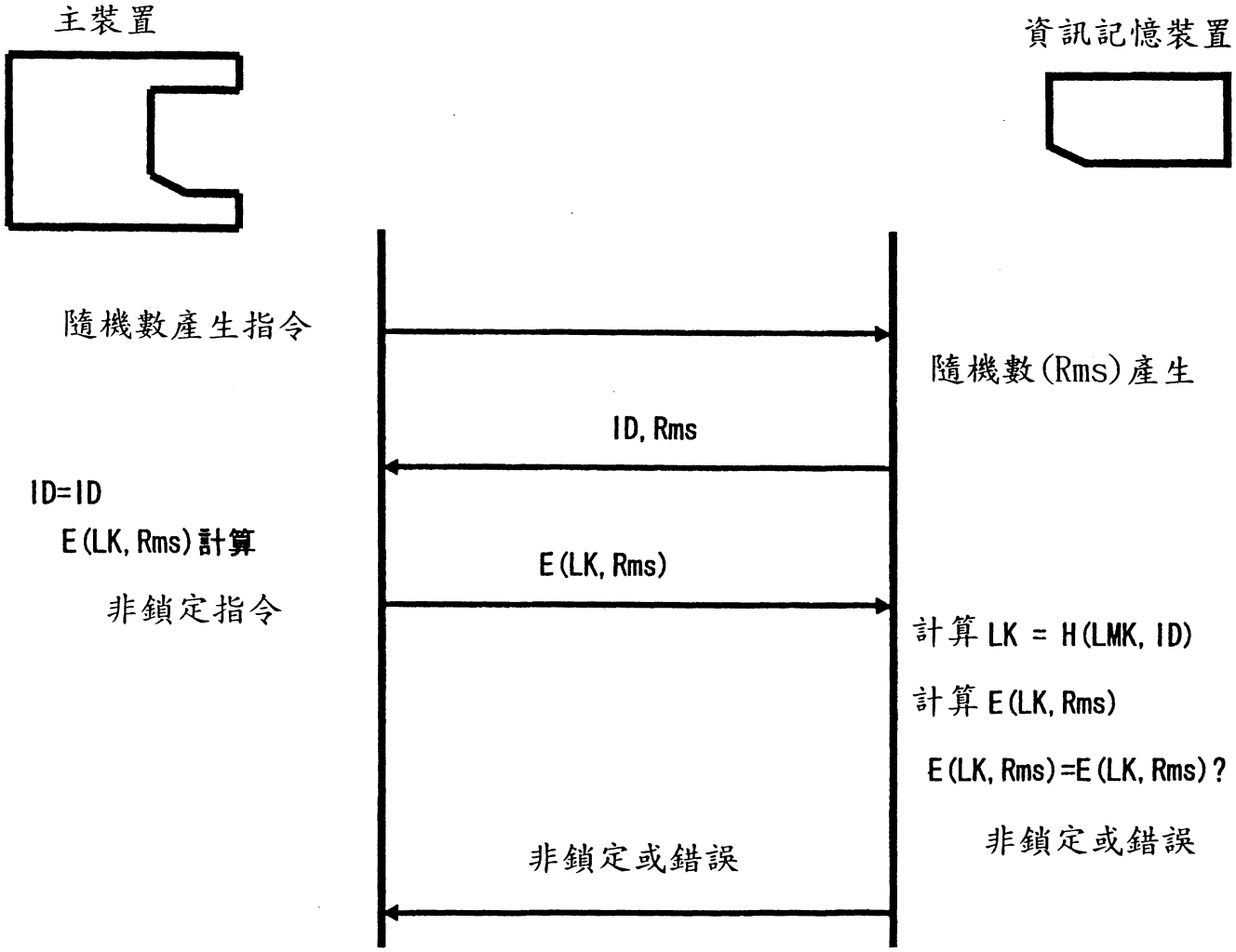

主裝置
資訊記憶裝置
隨機數產生指令
隨機數(Rms)產生
ID, Rms
ID=ID
E(LK, Rms)計算
E(LK, Rms)
非鎖定指令
計算 LK = H(LMK, ID)
計算 E(LK, Rms)
E(LK, Rms)=E(LK, Rms)?
非鎖定或錯誤
非鎖定或錯誤

圖 7

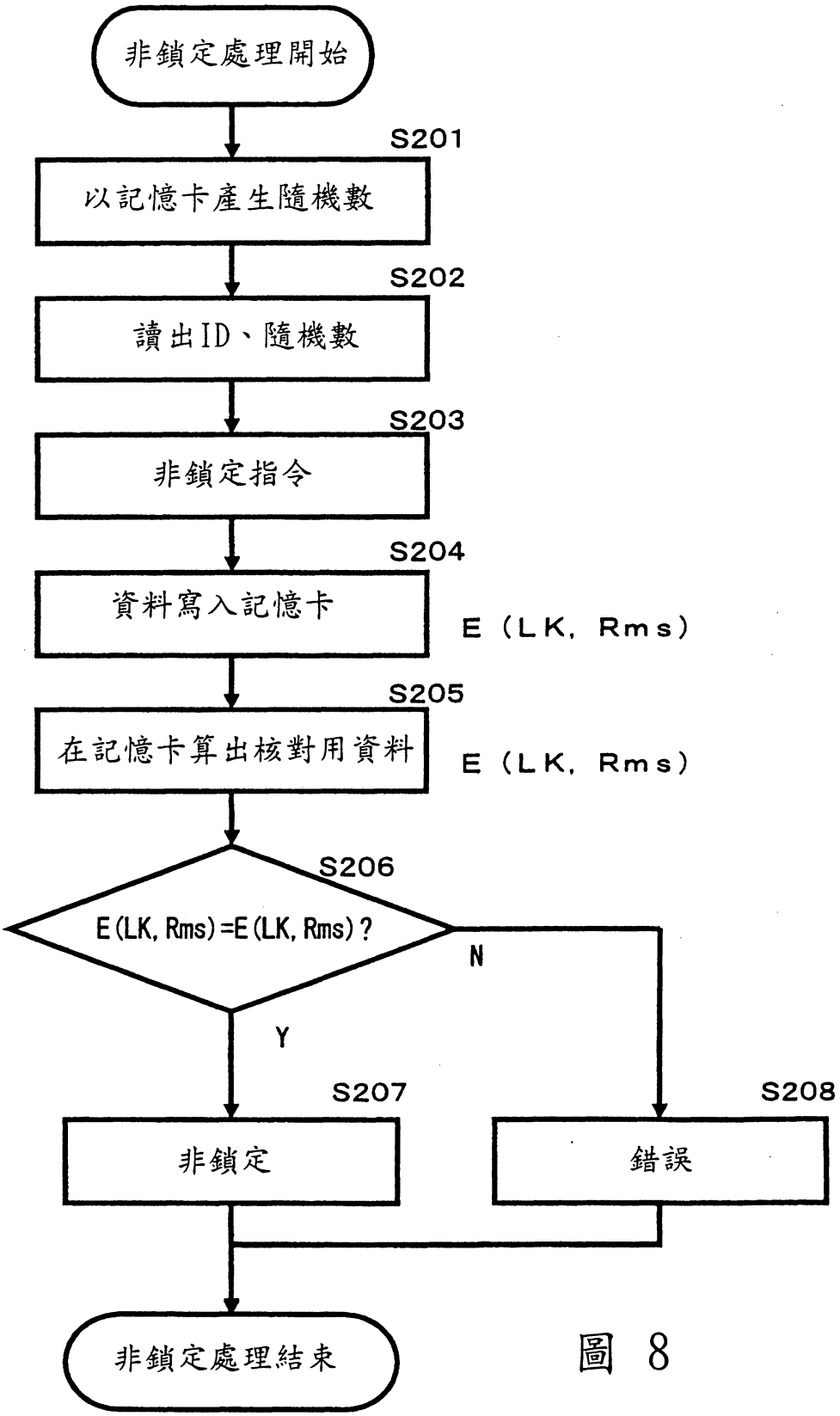

非鎖定處理開始
S201
以記憶卡產生隨機數
S202
讀出ID、隨機數
S203
非鎖定指令
S204
資料寫入記憶卡
E（LK, Rms）
S205
在記憶卡算出核對用資料
E（LK, Rms）
S206
E(LK, Rms)=E(LK, Rms)?
N
Y
S207
非鎖定
S208
錯誤
非鎖定處理結束

圖 8

549

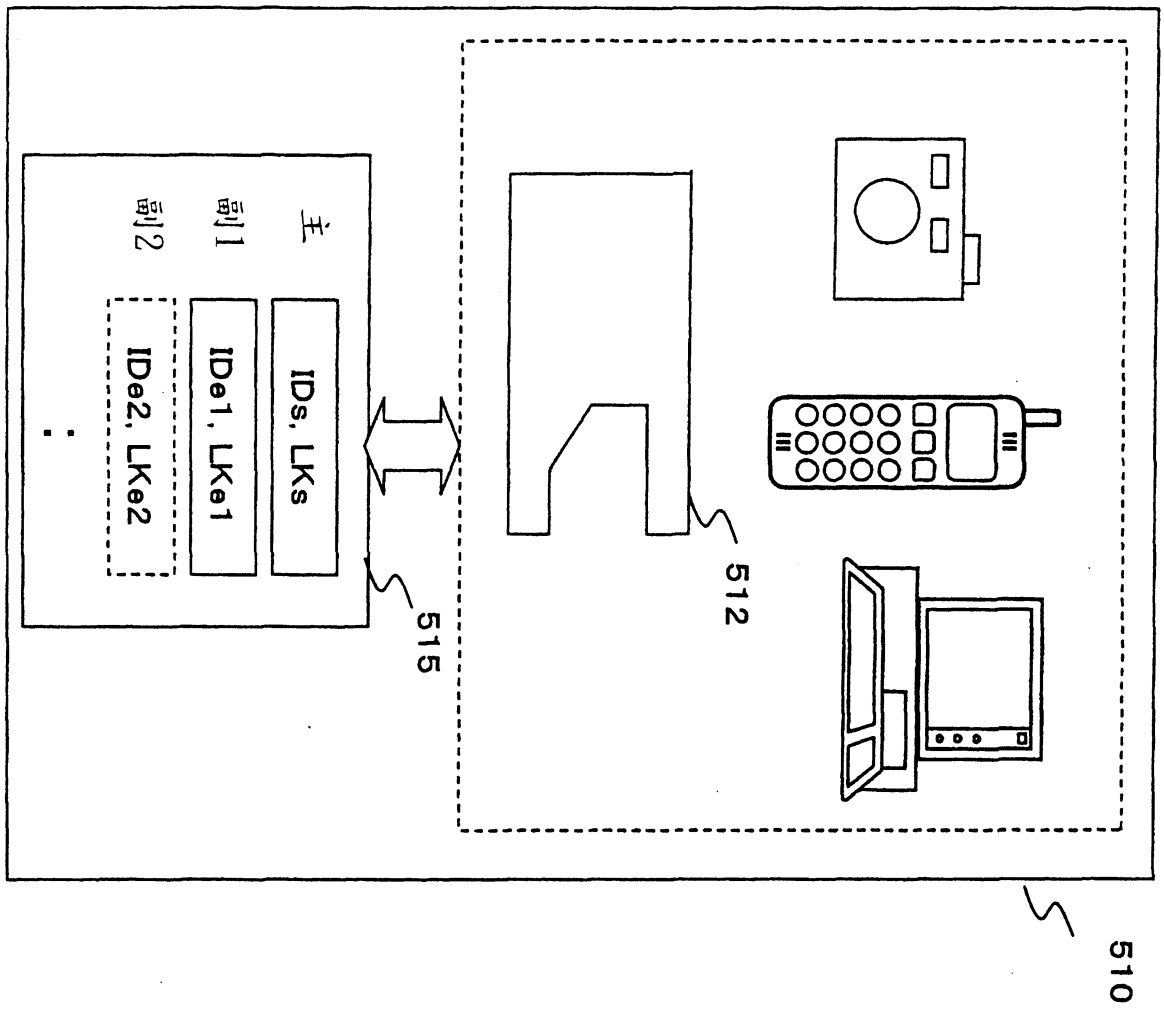
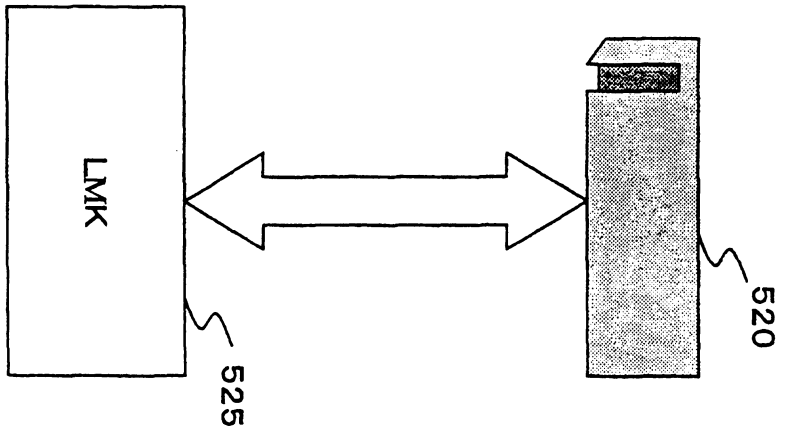


圖 9



550

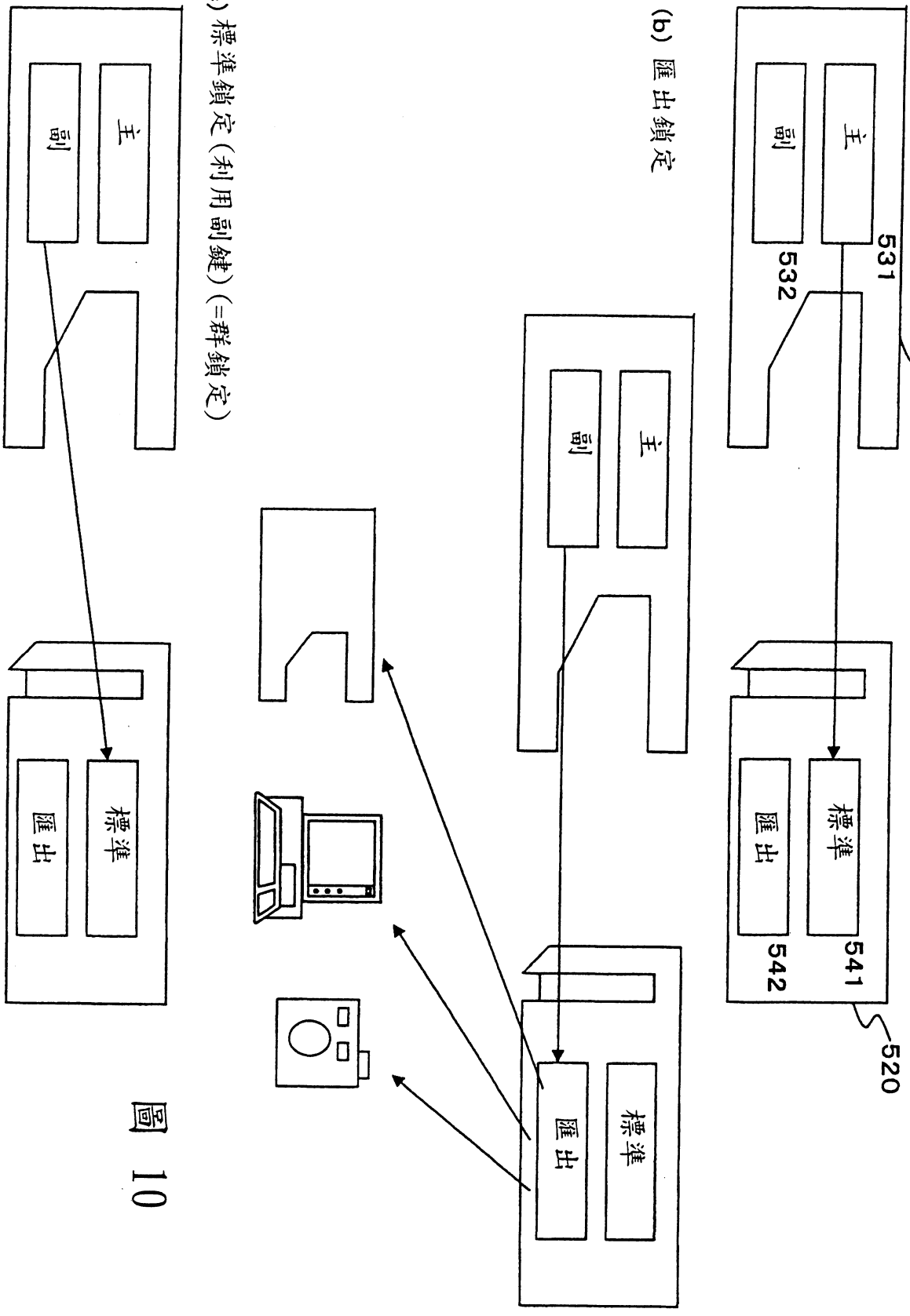

(a) 標準鎖定
主
副
531
532
510
標準
匯出
541
542
520
(b) 匯出鎖定
主
副
標準
匯出
(c) 標準鎖定(利用副鍵)(=群鎖定)
主
副
標準
匯出

圖 10

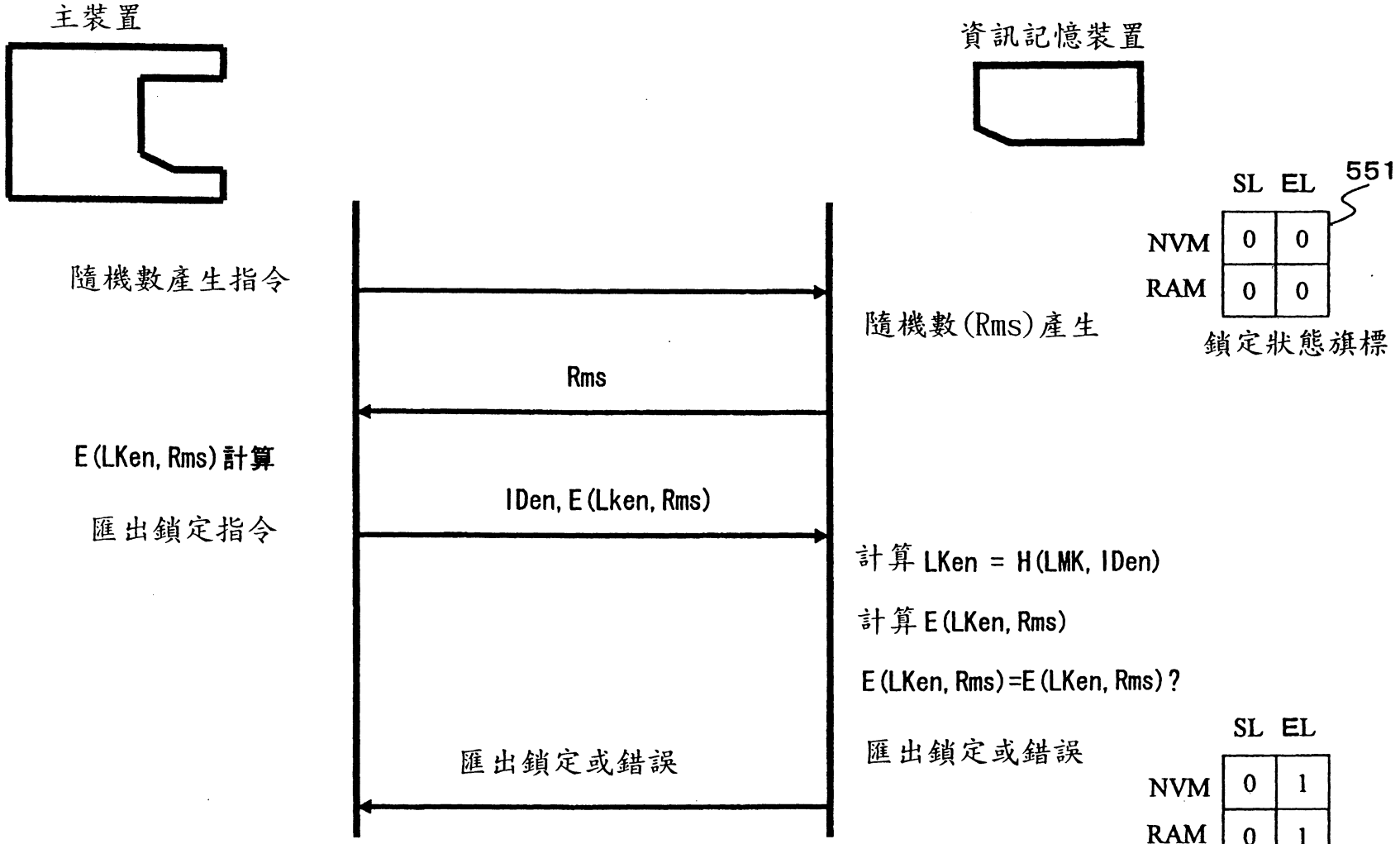

主裝置
資訊記憶裝置
隨機數產生指令
隨機數(Rms)產生
SL EL
551
NVM 0 0
RAM 0 0
鎖定狀態旗標
Rms
E(LKen, Rms)計算
IDen, E(Lken, Rms)
匯出鎖定指令
計算 LKen = H(LMK, IDen)
計算 E(LKen, Rms)
E(LKen, Rms)=E(LKen, Rms)?
匯出鎖定或錯誤
匯出鎖定或錯誤
SL EL
NVM 0 1
RAM 0 1

圖 11

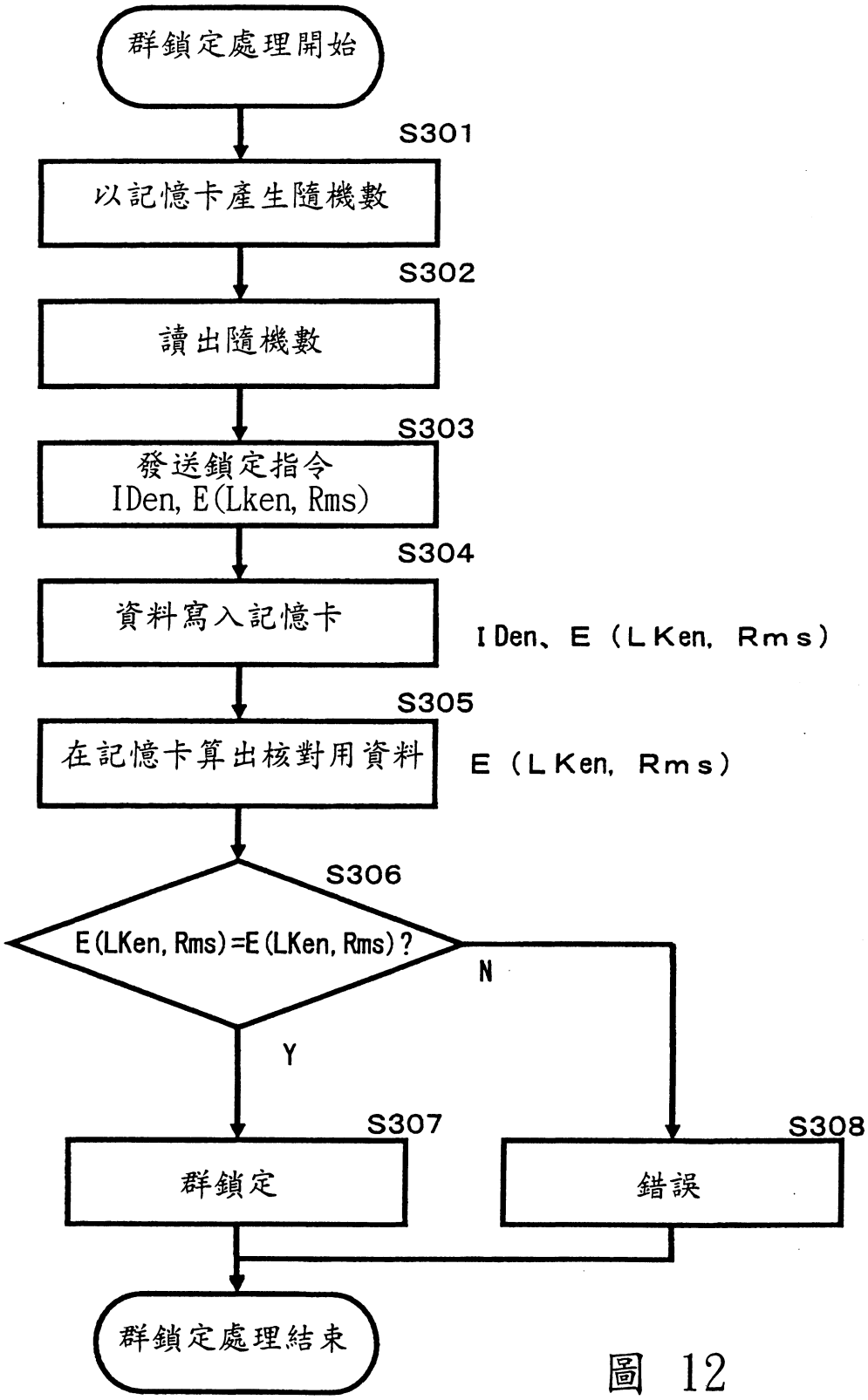

群鎖定處理開始
S301
以記憶卡產生隨機數
S302
讀出隨機數
S303
發送鎖定指令
IDen, E(Lken, Rms)
S304
資料寫入記憶卡
IDen、E（LKen, Rms）
S305
在記憶卡算出核對用資料
E（LKen, Rms）
S306
E(LKen, Rms)=E(LKen, Rms)?
N
Y
S307
群鎖定
S308
錯誤
群鎖定處理結束

圖 12

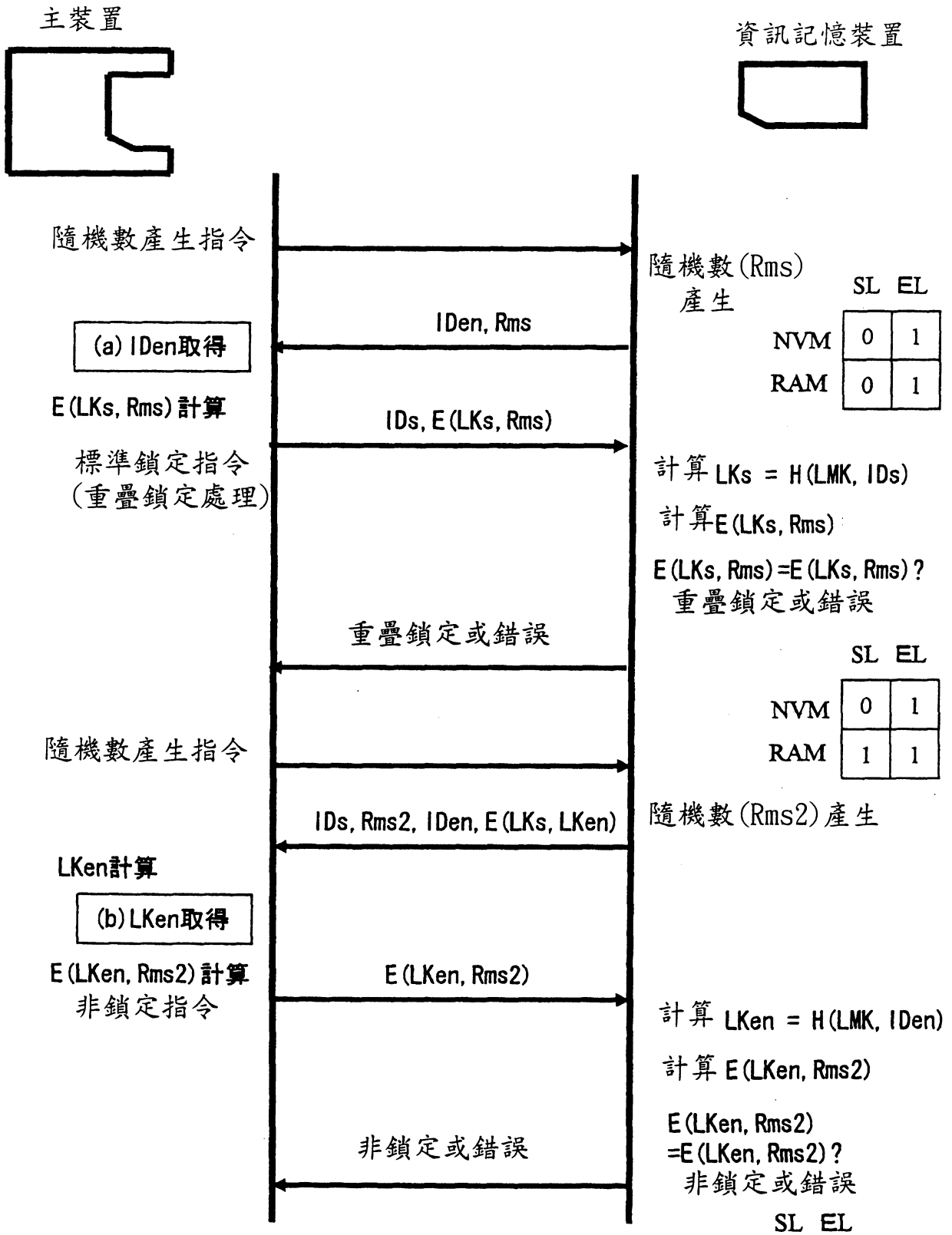

主裝置
資訊記憶裝置
隨機數產生指令
隨機數(Rms)
產生
SL EL
NVM 0 1
RAM 0 1
IDen, Rms
(a) IDen取得
E(LKs, Rms)計算
IDs, E(LKs, Rms)
標準鎖定指令
(重疊鎖定處理)
計算 LKs = H(LMK, IDs)
計算E(LKs, Rms)
E(LKs, Rms)=E(LKs, Rms)?
重疊鎖定或錯誤
重疊鎖定或錯誤
SL EL
NVM 0 1
RAM 1 1
隨機數產生指令
IDs, Rms2, IDen, E(LKs, LKen)
隨機數(Rms2)產生
LKen計算
(b) LKen取得
E(LKen, Rms2)計算
非鎖定指令
E(LKen, Rms2)
計算 LKen = H(LMK, IDen)
計算 E(LKen, Rms2)
E(LKen, Rms2)
=E(LKen, Rms2)?
非鎖定或錯誤
非鎖定或錯誤
SL EL
NVM 0 0
RAM 0 0

圖 13

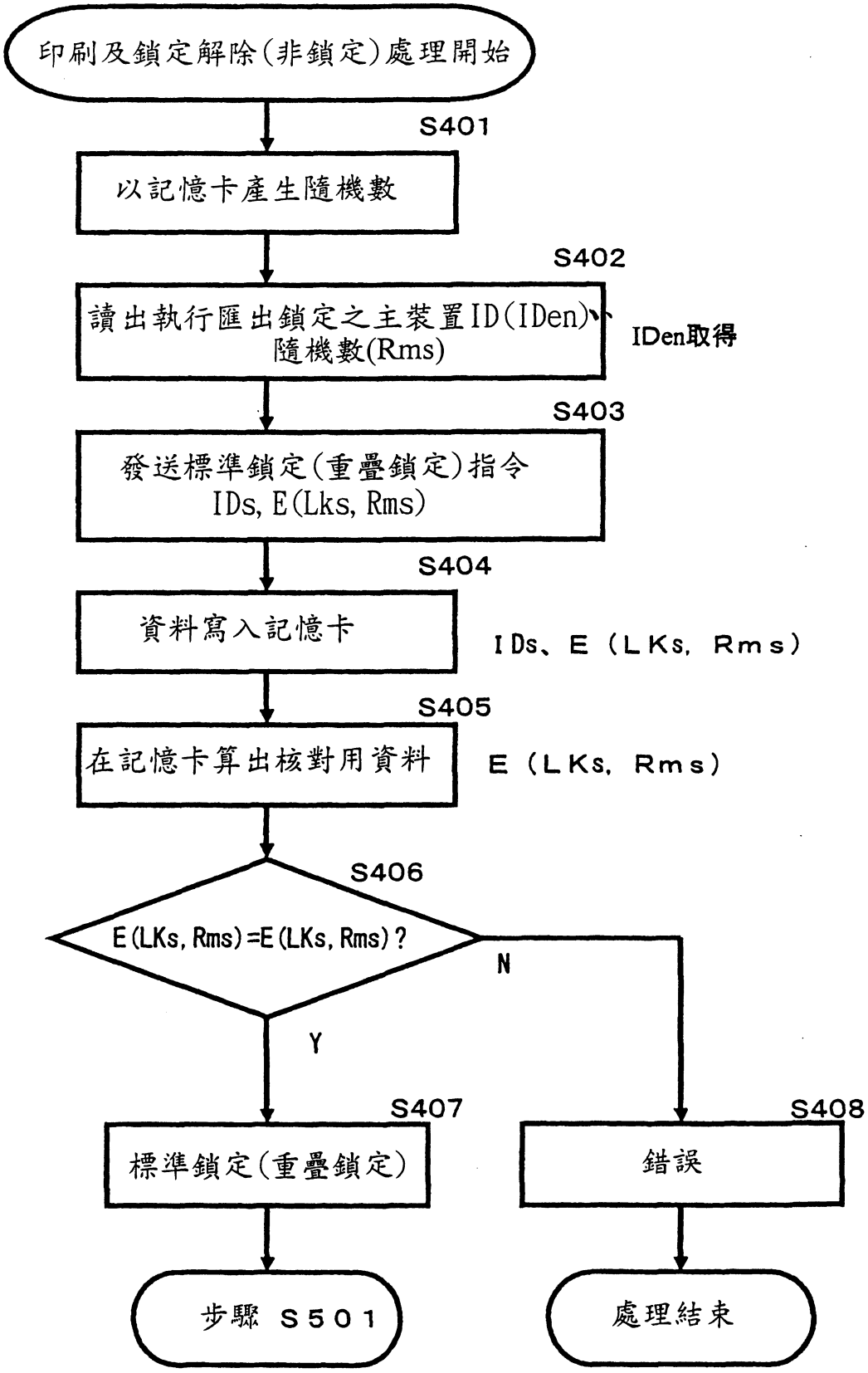

印刷及鎖定解除(非鎖定)處理開始
S401
以記憶卡產生隨機數
S402
讀出執行匯出鎖定之主裝置ID(IDen)、隨機數(Rms)
IDen取得
S403
發送標準鎖定(重疊鎖定)指令
IDs, E(Lks, Rms)
S404
資料寫入記憶卡
IDs、E（LKs, Rms）
S405
在記憶卡算出核對用資料
E（LKs, Rms）
S406
E(LKs, Rms)=E(LKs, Rms)?
N
Y
S407
標準鎖定(重疊鎖定)
S408
錯誤
步驟 S501
處理結束

圖 14

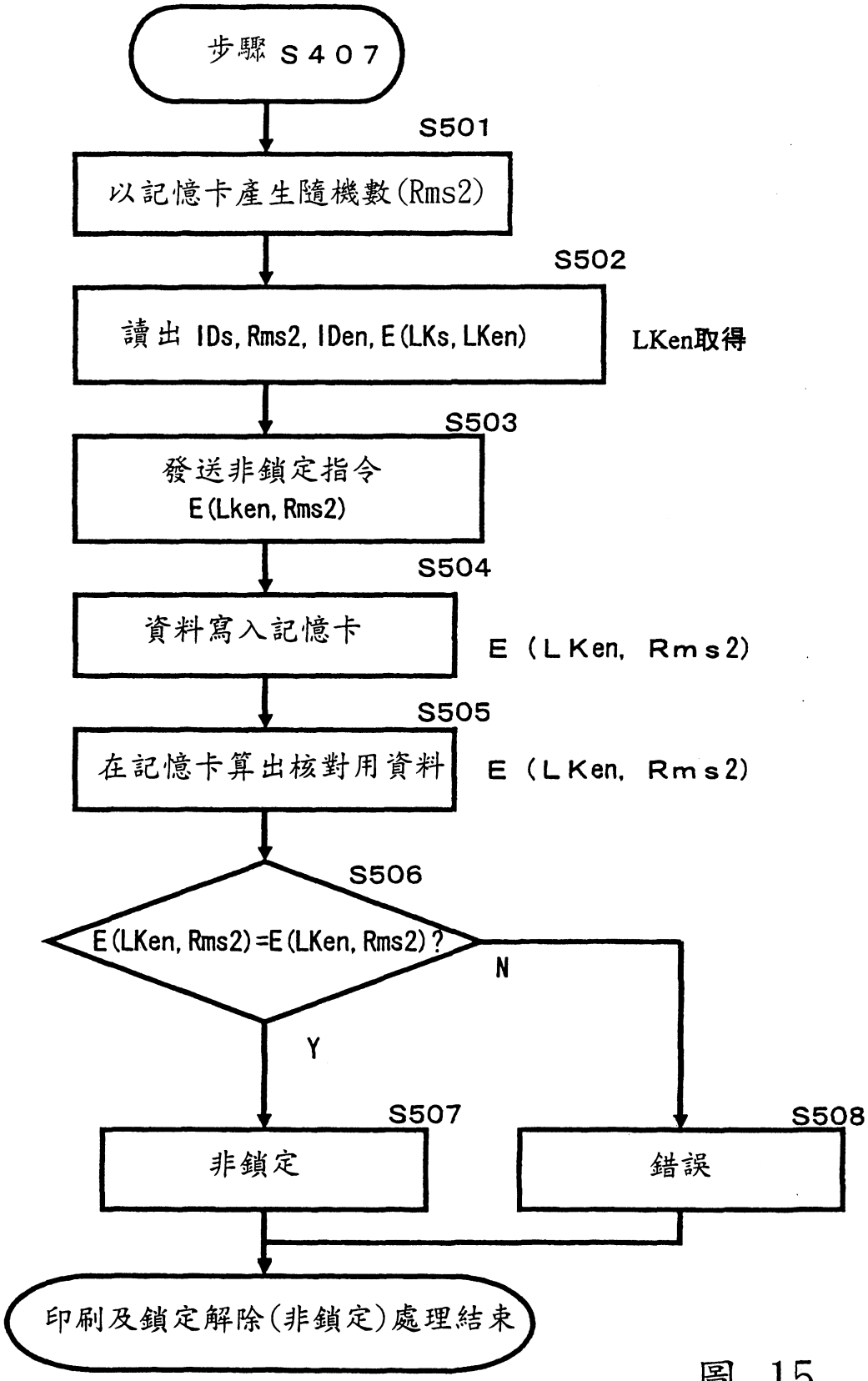

步驟 S407
S501
以記憶卡產生隨機數(Rms2)
S502
讀出 IDs, Rms2, IDen, E(LKs, LKen)
LKen取得
S503
發送非鎖定指令
E(Lken, Rms2)
S504
資料寫入記憶卡
E (LKen, Rms2)
S505
在記憶卡算出核對用資料
E (LKen, Rms2)
S506
E(LKen, Rms2)=E(LKen, Rms2)?
N
Y
S507
非鎖定
S508
錯誤
印刷及鎖定解除(非鎖定)處理結束

圖 15

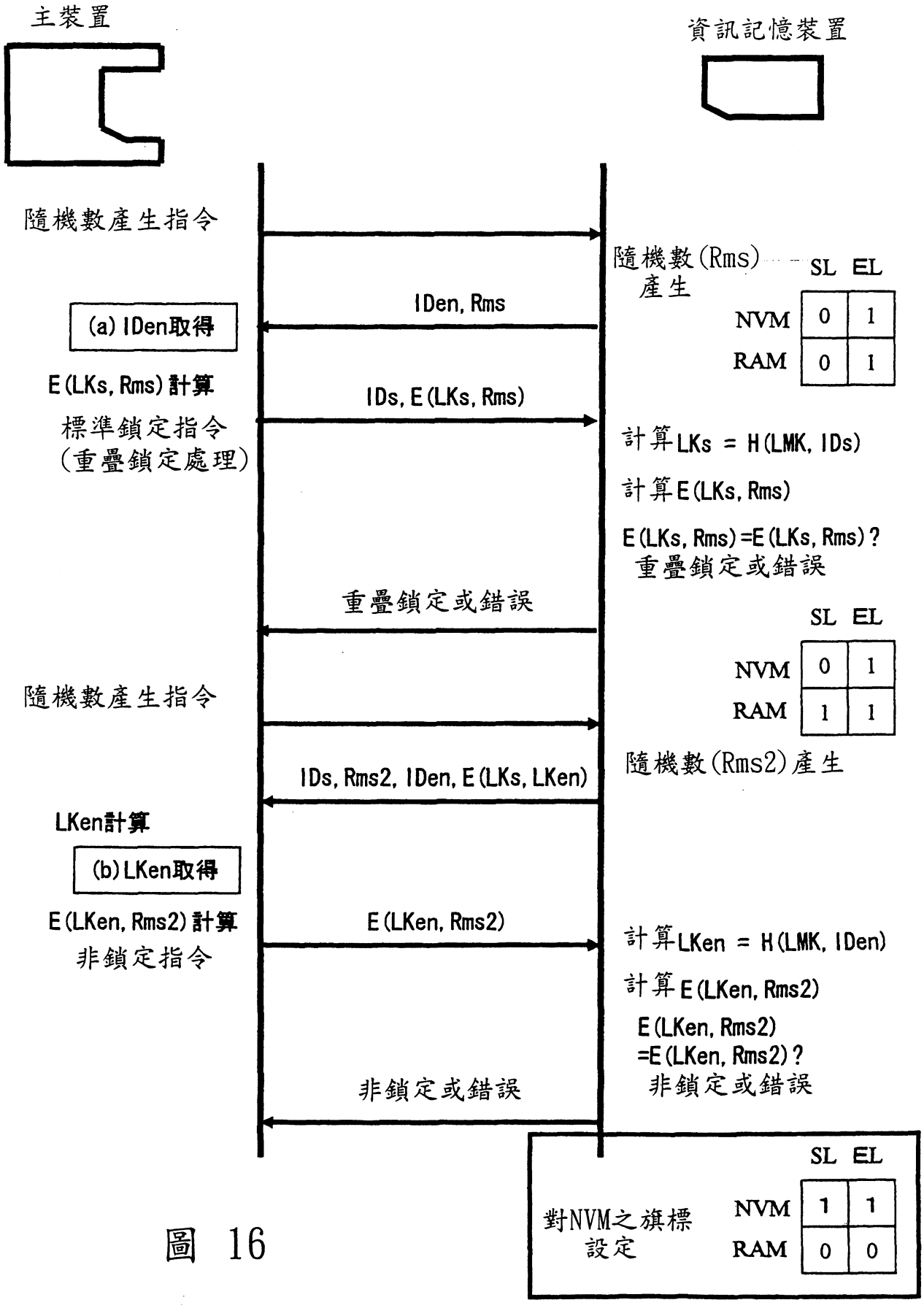

主裝置
資訊記憶裝置
隨機數產生指令
隨機數(Rms)產生
SL EL
NVM 0 1
RAM 0 1
IDen, Rms
(a) IDen取得
E(LKs, Rms)計算
IDs, E(LKs, Rms)
標準鎖定指令
(重疊鎖定處理)
計算LKs = H(LMK, IDs)
計算E(LKs, Rms)
E(LKs, Rms)=E(LKs, Rms)?
重疊鎖定或錯誤
重疊鎖定或錯誤
SL EL
NVM 0 1
RAM 1 1
隨機數產生指令
隨機數(Rms2)產生
IDs, Rms2, IDen, E(LKs, LKen)
LKen計算
(b) LKen取得
E(LKen, Rms2)計算
E(LKen, Rms2)
非鎖定指令
計算LKen = H(LMK, IDen)
計算E(LKen, Rms2)
E(LKen, Rms2)
=E(LKen, Rms2)?
非鎖定或錯誤
非鎖定或錯誤
SL EL
對NVM之旗標設定
NVM 1 1
RAM 0 0

圖 16

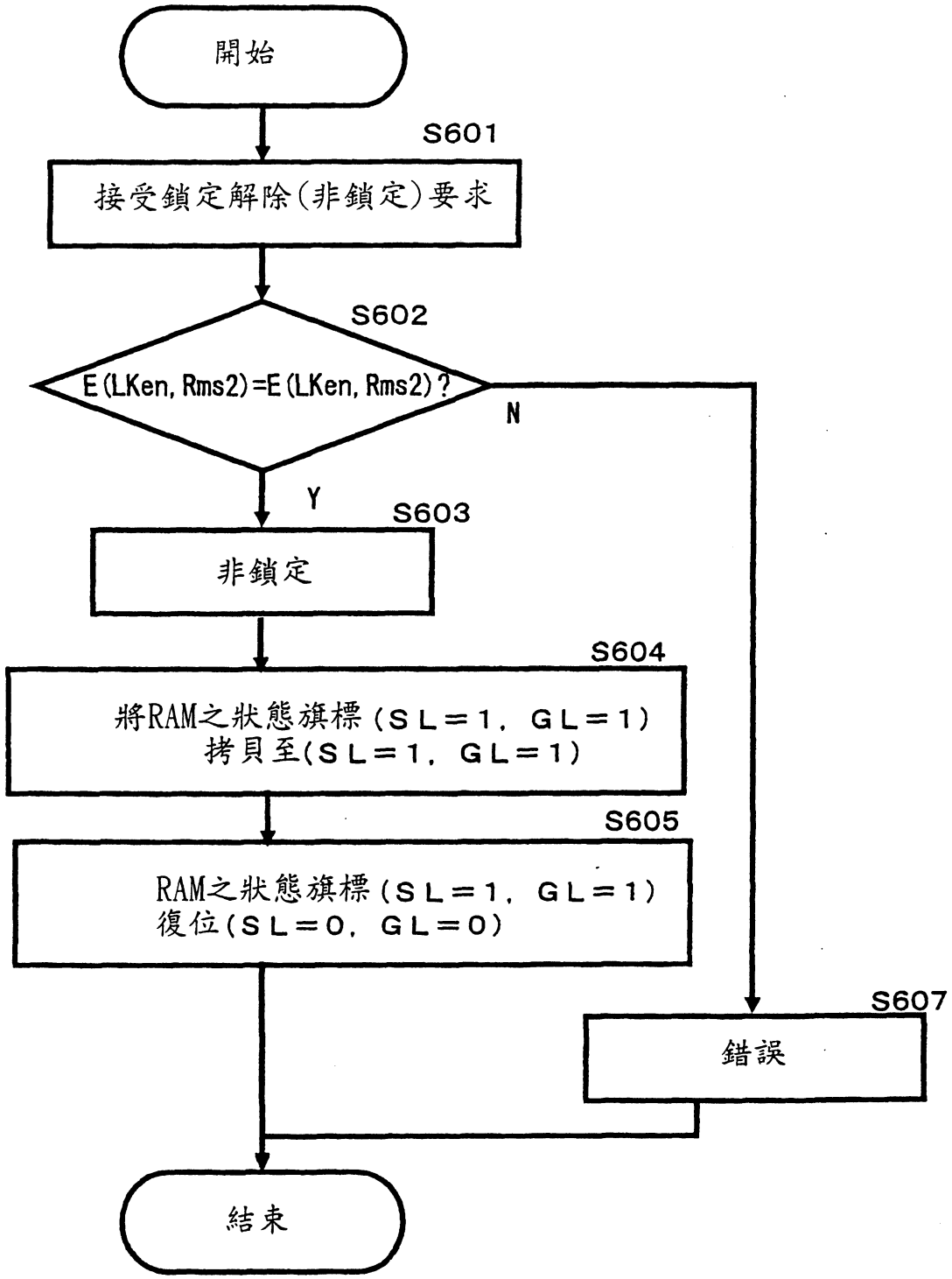

開始
S601
接受鎖定解除(非鎖定)要求
S602
E(LKen, Rms2)=E(LKen, Rms2)?
N
Y
S603
非鎖定
S604
將RAM之狀態旗標(SL=1, GL=1)
拷貝至(SL=1, GL=1)
S605
RAM之狀態旗標(SL=1, GL=1)
復位(SL=0, GL=0)
S607
錯誤
結束

圖 17

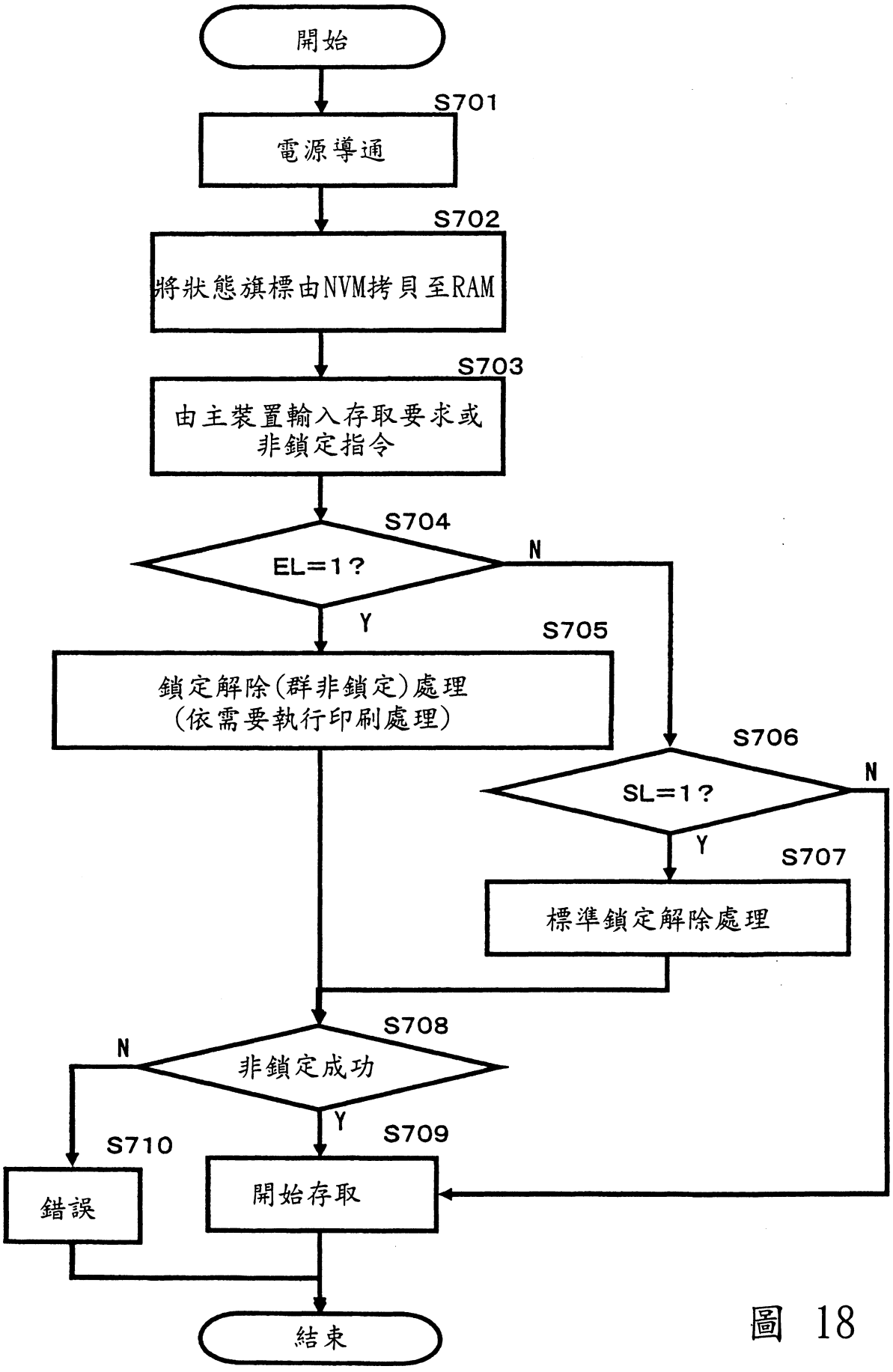

開始
S701
電源導通
S702
將狀態旗標由NVM拷貝至RAM
S703
由主裝置輸入存取要求或
非鎖定指令
S704
EL=1?
N
Y
S705
鎖定解除(群非鎖定)處理
(依需要執行印刷處理)
S706
SL=1?
N
Y
S707
標準鎖定解除處理
S708
非鎖定成功
N
Y
S710
錯誤
S709
開始存取
結束

圖 18

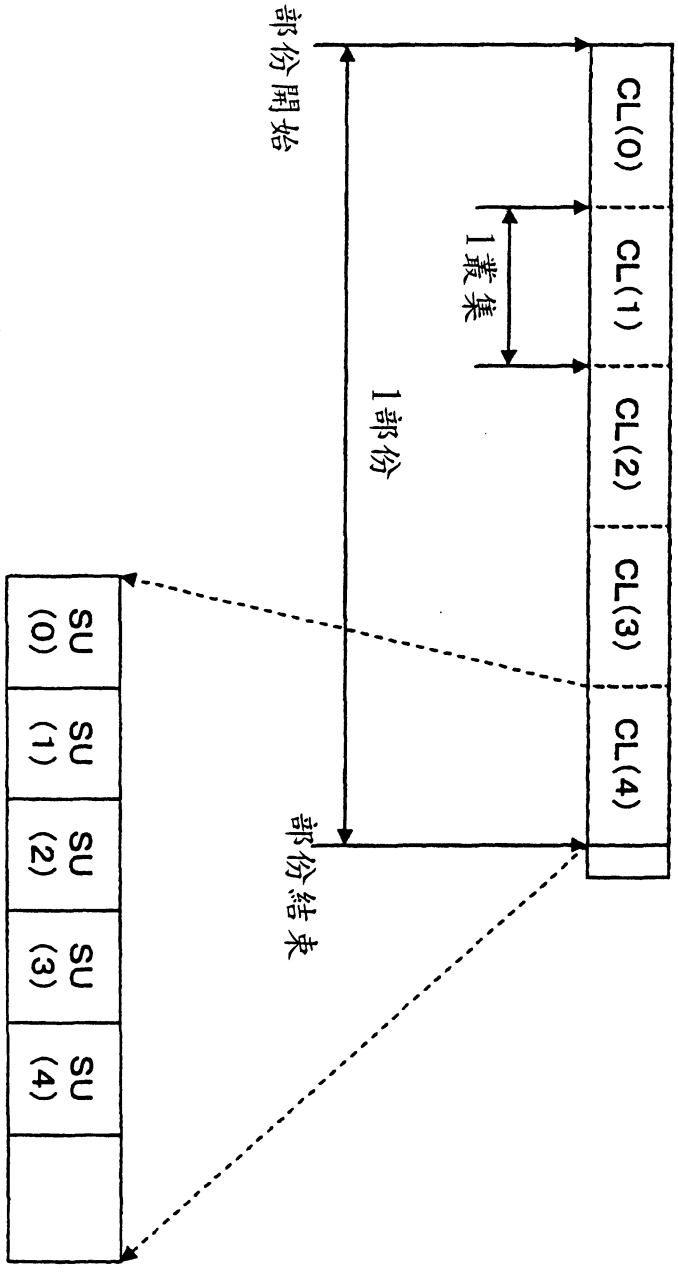


圖 19

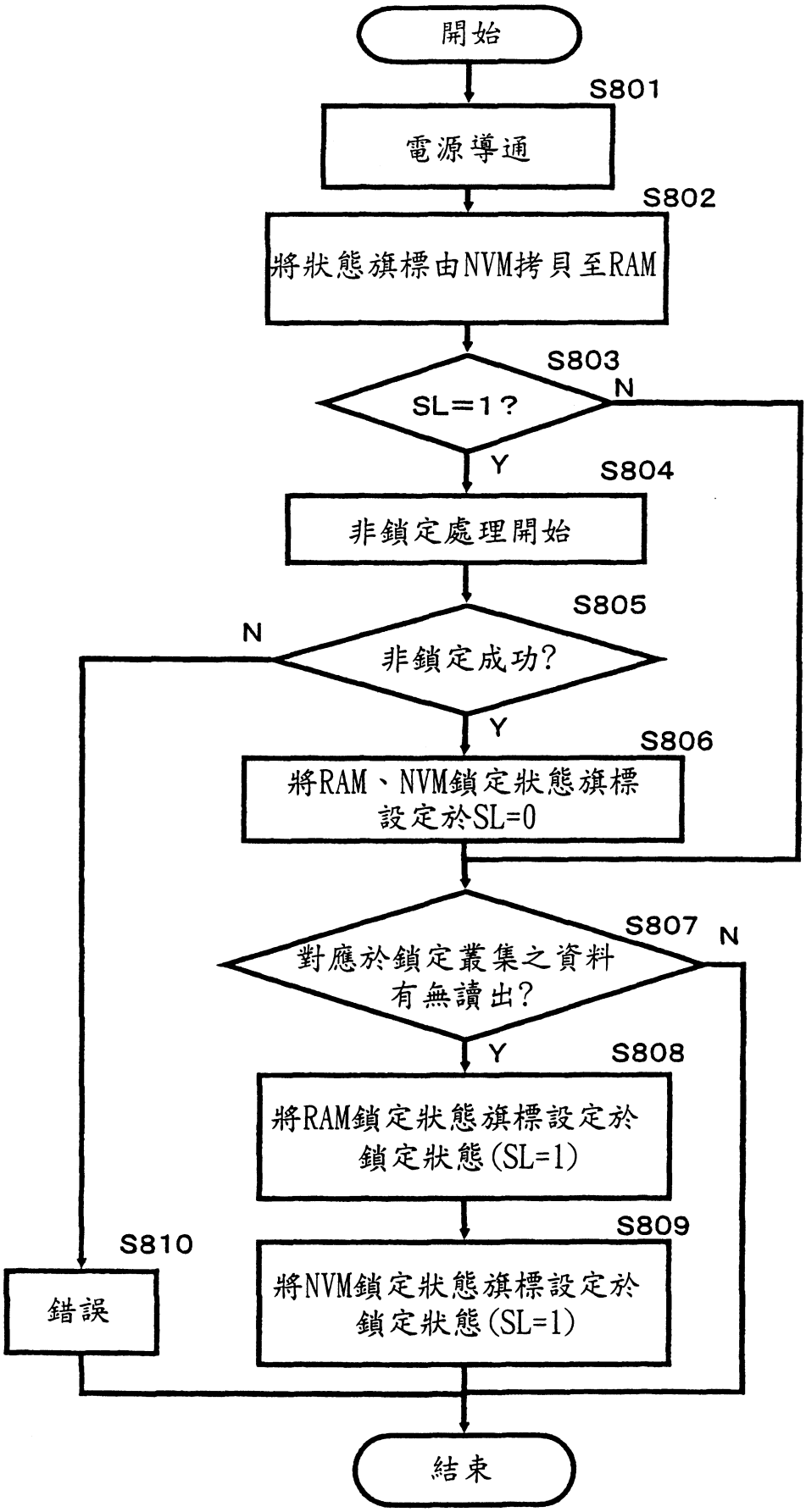

開始
S801
電源導通
S802
將狀態旗標由NVM拷貝至RAM
S803
SL=1?
N
Y
S804
非鎖定處理開始
S805
N
非鎖定成功?
Y
S806
將RAM、NVM鎖定狀態旗標
設定於SL=0
S807
N
對應於鎖定叢集之資料
有無讀出?
Y
S808
將RAM鎖定狀態旗標設定於
鎖定狀態(SL=1)
S809
將NVM鎖定狀態旗標設定於
鎖定狀態(SL=1)
S810
錯誤
結束

圖 20

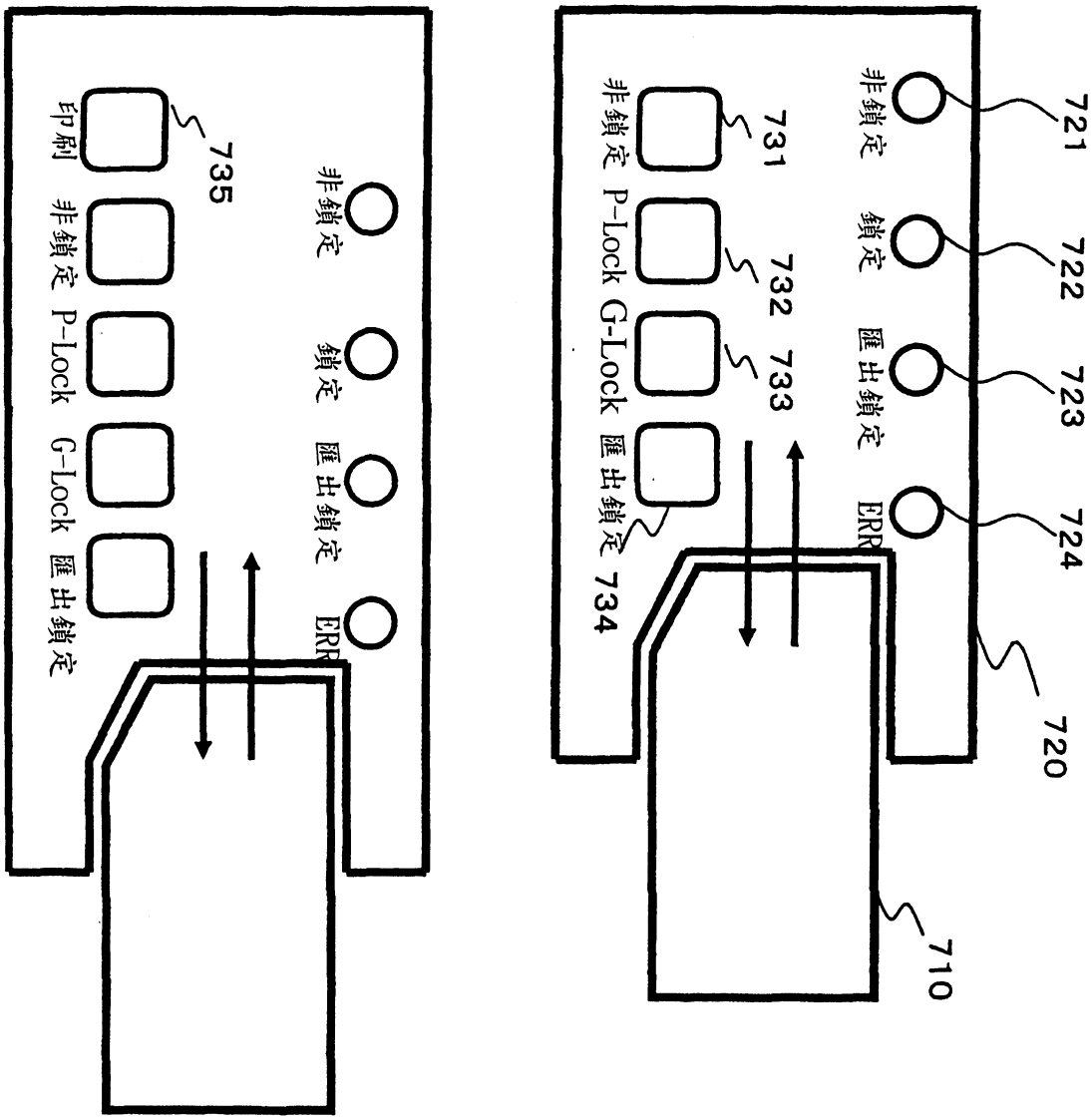

(a)
721
722
723
724
720
非鎖定
鎖定
匯出鎖定
ERR
731
732
733
734
710
非鎖定
P-Lock
G-Lock
匯出鎖定
(b)
非鎖定
鎖定
匯出鎖定
ERR
735
印刷
非鎖定
P-Lock
G-Lock
匯出鎖定

圖 21

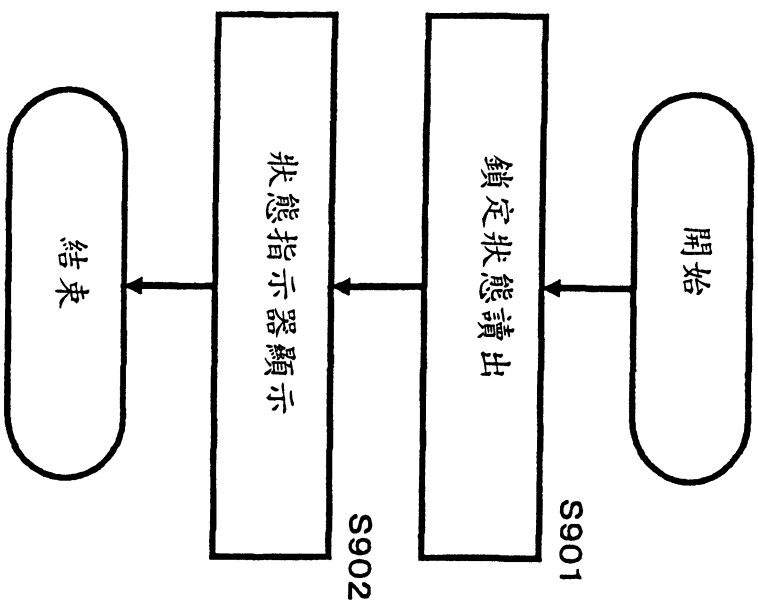


圖 22

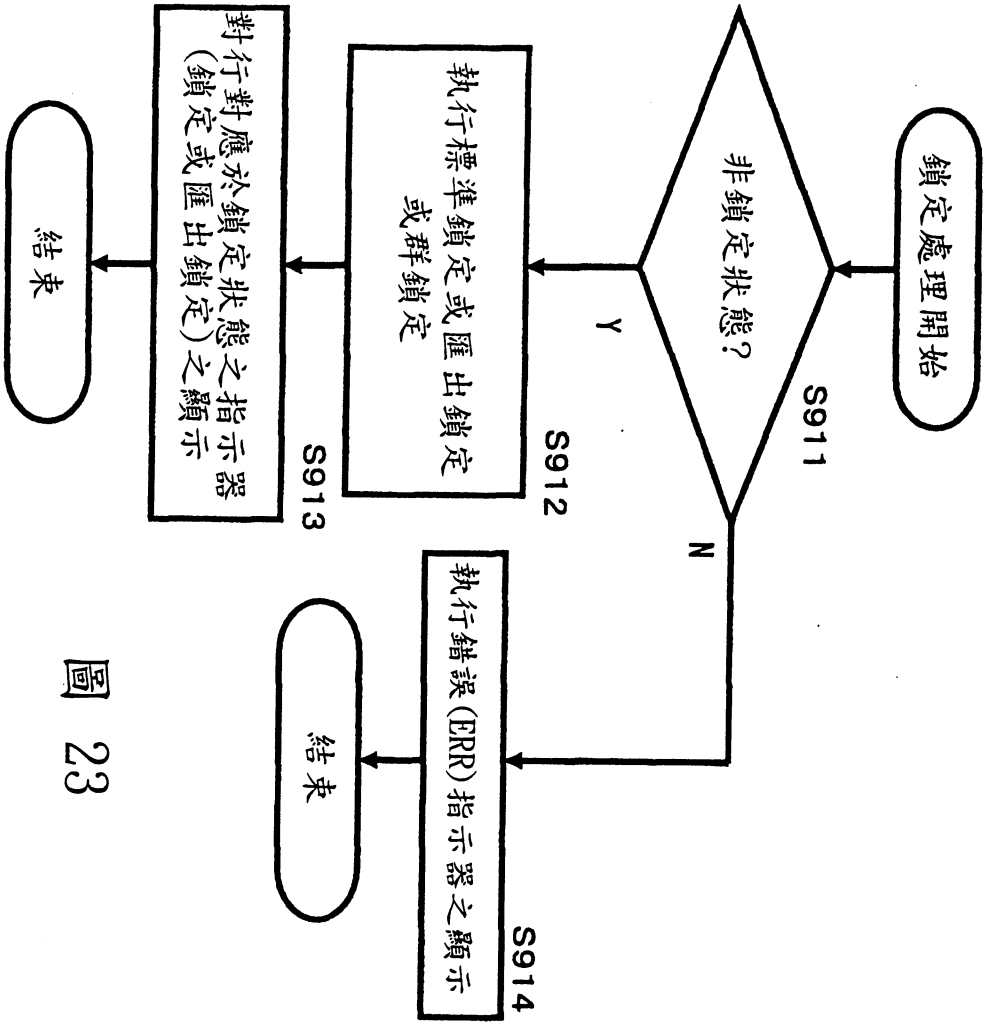
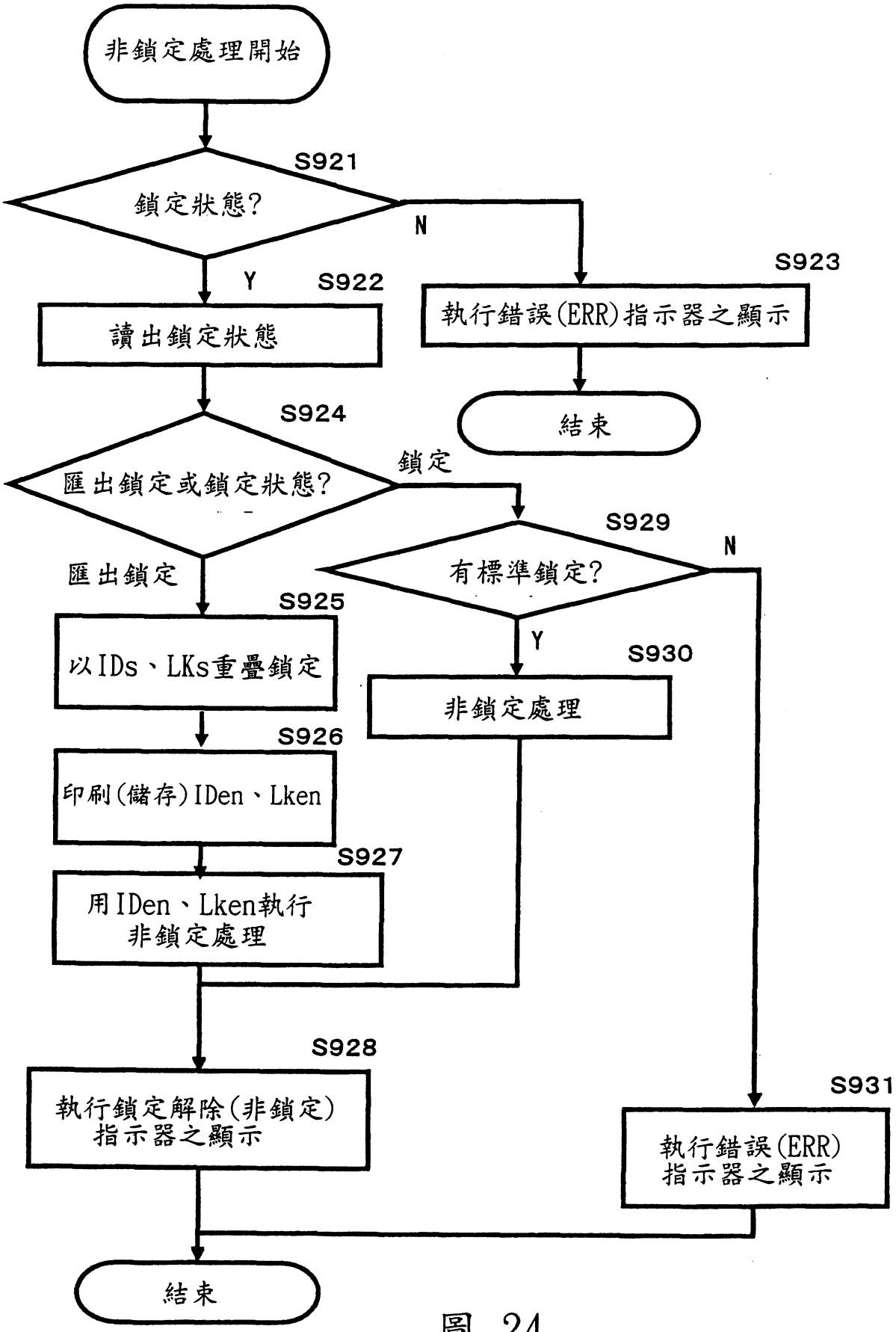

鎖定處理開始
非鎖定狀態?
S911
Y
N
執行標準鎖定或匯出鎖定或群鎖定
S912
執行錯誤(ERR)指示器之顯示
S914
對行對應於鎖定狀態之指示器(鎖定或匯出鎖定)之顯示
S913
結束
結束

圖 23


非鎖定處理開始
S921
鎖定狀態?
N
Y
S922
讀出鎖定狀態
S923
執行錯誤(ERR)指示器之顯示
結束
S924
匯出鎖定或鎖定狀態?
鎖定
匯出鎖定
S929
有標準鎖定?
N
Y
S925
以IDs、LKs重疊鎖定
S930
非鎖定處理
S926
印刷(儲存)IDen、Lken
S927
用IDen、Lken執行
非鎖定處理
S928
執行鎖定解除(非鎖定)
指示器之顯示
S931
執行錯誤(ERR)
指示器之顯示
結束

565

圖 24

94年1月25日 修正補充

I240165

發明專利說明書

中文說明書替換頁(94年1月)

（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：92116160

※ 申請日期：92.6.13　　※IPC 分類：G06F 12/00

壹、發明名稱：（中文/日文）

資訊記憶裝置、記憶體存取控制系統及方法、以及電腦可讀取之記錄媒體

情報記憶装置、およびメモリアクセス制御システム、および方法、並びにコンピュータが読取可能な記録媒体

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

日商新力股份有限公司

SONY CORPORATION

代表人：（中文/英文）

安藤 國威

KUNITAKE ANDO

住居所或營業所地址：（中文/英文）

日本東京都品川區北品川六丁目七番35號

7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, TOKYO, JAPAN

國　籍：（中文/英文）

日本　　JAPAN

94年1月15日
修正本

拾、申請專利範圍：

1. 一種資訊記憶裝置，其特徵在於包含：資料記憶用之記憶體、及執行對該記憶體之存取控制之控制部；

前述控制部在構成上係

由資訊處理裝置，輸入前述記憶體之鎖定處理要求指令或要求解除鎖定之解除鎖定處理要求指令，執行對應於輸入指令之處理；

並依據對應於輸出前述指令之資訊處理裝置所設定之識別符(ID)，執行前述資訊處理裝置是否具有含該識別符(ID)之正當之鍵組之驗證處理，並以該驗證成立為條件，依據前述指令執行其處理者。

2. 如申請專利範圍第1項之資訊記憶裝置，其中前述資訊處理裝置具有之鍵組係包含

資訊處理裝置之固有ID(ID)與對應於該固有ID之鎖定鍵(LK)之鍵組[ID, LK]；

前述資訊記憶裝置係

包含可算出鎖定鍵(LK)，以作為適用LK=H (LMK, ID)之關係，即對ID之鎖定主鍵(LMK)之雜湊值之鎖定主鍵(LMK)；

前述控制部在構成上，係依據由適用前述鎖定主鍵(LMK)之雜湊值之算出所取得之鎖定鍵(LK)，執行由資訊處理裝置輸入之資訊處理裝置固有之鍵組之驗證者。

3. 如申請專利範圍第2項之資訊記憶裝置，其中前述控制部在構成上係執行隨機數產生處理，由資訊處理裝置接收

依據該資訊處理裝置所包含之鎖定鍵(LK)之前述隨機數(Rms)之加密資料[E (Lk, Rms)]，以執行包含該接收之加密資料與依據前述雜湊值之算出所取得之鎖定鍵(LK)所算出之加密資料[E (Lk, Rms)]之核對之驗證處理者。

4. 如申請專利範圍第1項之資訊記憶裝置，其中前述控制部在構成上，係在來自前述資訊處理裝置之輸入指令為鎖定指令時，由前述資訊處理裝置輸入識別符(ID)，並依據該輸入之識別符(ID)執行驗證處理者。

5. 如申請專利範圍第1項之資訊記憶裝置，其中前述控制部在構成上，係在來自前述資訊處理裝置之輸入指令為解除鎖定指令時，由記憶體讀出在執行鎖定處理之際由資訊處理裝置輸入並儲存於該記憶體之識別符(ID)，並依據該讀出之識別符(ID)執行驗證處理者。

6. 一種記憶體存取控制系統，其特徵在於包含：資訊記憶裝置，其係包含資料記憶用之記憶體與執行對該記憶體之存取控制之控制部者；及資訊處理裝置，其係包含對前述資訊記憶裝置之介面，經由該介面執行資訊記憶裝置內之記憶體存取者；

前述資訊處理裝置係將含識別符(ID)及鎖定鍵(LK)之鍵組儲存於記憶手段；

前述資訊記憶裝置之控制部在構成上係由資訊處理裝置，輸入前述記憶體之鎖定處理要求指令或要求解除鎖定之解除鎖定處理要求指令，執行對應於輸入指令之處理；

並依據對應於輸入前述指令之資訊處理裝置所設定之識別符(ID)，執行前述資訊處理裝置是否包含含有該識別符(ID)之正當之鍵組之驗證處理，以該驗證成立為條件，依據前述指令執行其處理者。

7. 如申請專利範圍第6項之記憶體存取控制系統，其中前述資訊處理裝置包含之鍵組係包含資訊處理裝置之固有ID(ID)與對應於該固有ID之鎖定鍵(LK)之鍵組[ID, LK]；

前述資訊記憶裝置係包含可算出鎖定鍵(LK)，以作為適用LK=H (LMK, ID)之關係，即對ID之鎖定主鍵(LMK)之雜湊值之鎖定主鍵(LMK)；

前述資訊記憶裝置之控制部在構成上係依據由適用前述鎖定主鍵(LMK)之雜湊值之算出所取得之鎖定鍵(LK)，執行由資訊處理裝置輸入之資訊處理裝置固有之鍵組之驗證者。

8. 如申請專利範圍第7項之記憶體存取控制系統，其中前述資訊記憶裝置之控制部在構成上係執行隨機數產生處理，由資訊處理裝置接收依據該資訊處理裝置所有之鎖定鍵(LK)之前述隨機數(Rms)之加密資料[E (Lk, Rms)]，以執行包含該接收之加密資料與依據前述雜湊值之算出所取得之鎖定鍵(LK)所算出之加密資料[E (Lk, Rms)]之核對之驗證處理者。

9. 如申請專利範圍第6項之記憶體存取控制系統，其中前述資訊記憶裝置之控制部在構成上係在來自前述資訊處理裝置之輸入指令為鎖定指令時，由前述資訊處理裝置輸

入識別符(ID)，並依據該輸入之識別符(ID)執行驗證處理者。

10. 如申請專利範圍第6項之記憶體存取控制系統，其中前述資訊記憶裝置之控制部在構成上係在來自前述資訊處理裝置之輸入指令為解除鎖定指令時，由記憶體讀出在執行鎖定處理之際由資訊處理裝置輸入並儲存於該記憶體之識別符(ID)，依據該讀出之識別符(ID)執行驗證處理者。

11. 一種記憶體存取控制方法，其特徵在於執行資訊記憶裝置中之記憶體存取控制，而該資訊記憶裝置係包含資料記憶用之記憶體、與執行對該記憶體之存取控制之控制部者；此方法包含：

由資訊處理裝置，輸入前述記憶體之鎖定處理要求指令或要求解除鎖定之解除鎖定處理要求指令之步驟；

依據對應於輸出前述指令之資訊處理裝置所設定之識別符(ID)，執行前述資訊處理裝置是否包含含有該識別符(ID)之正當之鍵組之驗證處理之驗證步驟；及

以前述驗證成立為條件，依據前述指令執行其處理之步驟者。

12. 如申請專利範圍第11項之記憶體存取控制方法，其中前述資訊處理裝置包含之鍵組係包含

資訊處理裝置之固有ID(ID)與對應於該固有ID之鎖定鍵(LK)之鍵組[ID, LK]；

前述資訊記憶裝置係包含

可算出鎖定鍵(LK)，以作為適用LK=H (LMK, ID)之關係，即對ID之鎖定主鍵(LMK)之雜湊值之鎖定主鍵(LMK)；

前述驗證步驟係包含下列之步驟者：

依據由適用前述鎖定主鍵(LMK)之雜湊值之算出所取得之鎖定鍵(LK)，執行由資訊處理裝置輸入之資訊處理裝置固有之鍵組之驗證處理。

13. 如申請專利範圍第12項之記憶體存取控制方法，其中前述驗證步驟係包含下列步驟者：

執行隨機數產生處理，由資訊處理裝置接收依據該資訊處理裝置所包含之鎖定鍵(LK)之前述隨機數(Rms)之加密資料[E(Lk, Rms)]，以執行包含該接收之加密資料與

依據前述雜湊值之算出所取得之鎖定鍵(LK)所算出之加密資料[E(Lk, Rms)]之核對之驗證處理。

14. 如申請專利範圍第11項之記憶體存取控制方法，其中前述驗證步驟係包含下列步驟者：

在來自前述資訊處理裝置之輸入指令為鎖定指令時，由前述資訊處理裝置輸入識別符(ID)，依據該輸入之識別符(ID)執行驗證處理。

15. 如申請專利範圍第11項之記憶體存取控制方法，其中前述驗證步驟係包含下列步驟者：

在來自前述資訊處理裝置之輸入指令為解除鎖定指令時，由記憶體讀出在執行鎖定處理之際由資訊處理裝置輸入並儲存於該記憶體之識別符(ID)，依據該讀出之識別符(ID)執行驗證處理。

16. 一種電腦可讀取之記錄媒體，其記錄有電腦程式，該電腦程式執行資訊記憶裝置中之記憶體存取控制處理，而該資訊記憶裝置係包含資料記憶用之記憶體、與執行對該記憶體之存取控制之控制部者；該電腦程式且包含：

由資訊處理裝置，輸入前述記憶體之鎖定處理要求指令或要求解除鎖定之解除鎖定處理要求指令之步驟；

依據對應於輸出前述指令之資訊處理裝置所設定之識別符(ID)，執行前述資訊處理裝置是否包含含有該識別符(ID)之正當之鍵組之驗證處理之驗證步驟；及

以前述驗證成立為條件，依據前述指令執行其處理之步驟者。