I489280

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I489280 B**

(45)公告日： 中華民國 104 (2015) 年 06 月 21 日

(21)申請案號：099111023 (22)申請日： 中華民國 99 (2010) 年 04 月 09 日

(51)Int. Cl.： *G06F12/14 (2006.01)*

(30)優先權：2009/04/14 日本 2009-097829

(71)申請人：邁格技富股份有限公司 (日本) MEGA CHIPS CORPORATION (JP)
日本

(72)發明人：管原崇彥 SUGAHARA, TAKAHIKO (JP) ；古都哲生 FURUICHI, TETSUO (JP) ；
山口育男 YAMAGUCHI, IKUO (JP) ；押切崇 OSHIKIRI, TAKASHI (JP)

(74)代理人：賴經臣；宿希成

(56)參考文獻：

TW	200629068A	TW	200845689A
US	6307940B1	US	2006/0282898A1
US	2007/0136407A1	US	2008/0260159A1

審查人員：簡大翔

申請專利範圍項數：8 項 圖式數：8 共 42 頁

(54)名稱

記憶體控制器，記憶體控制裝置，記憶體裝置，記憶體資訊保護系統及記憶體控制裝置之控制方法
MEMORY CONTROLLER, MEMORY CONTROL DEVICE, MEMORY DEVICE, MEMORY INFORMATION PROTECTING SYSTEM, AND METHOD OF CONTROLLING A MEMORY CONTROL DEVICE

(57)摘要

本發明係提供一種可提高記憶於記憶體裝置中的資訊之機密性之技術。記憶體控制器包括：密鑰生成部 112，於每既定時序生成新的用於資訊之加密/解碼之密鑰資訊；及資料轉換電路 113，根據資訊對輸出至記憶體裝置 20 之資訊進行加密，同時根據密鑰資訊對自記憶體裝置 20 所輸入之經加密的資訊進行解碼；而於資料轉換電路 113 中，每當密鑰生成部 112 生成新的密鑰資訊時，則進行將該新的密鑰資訊作為密鑰資訊的密鑰資訊更新。

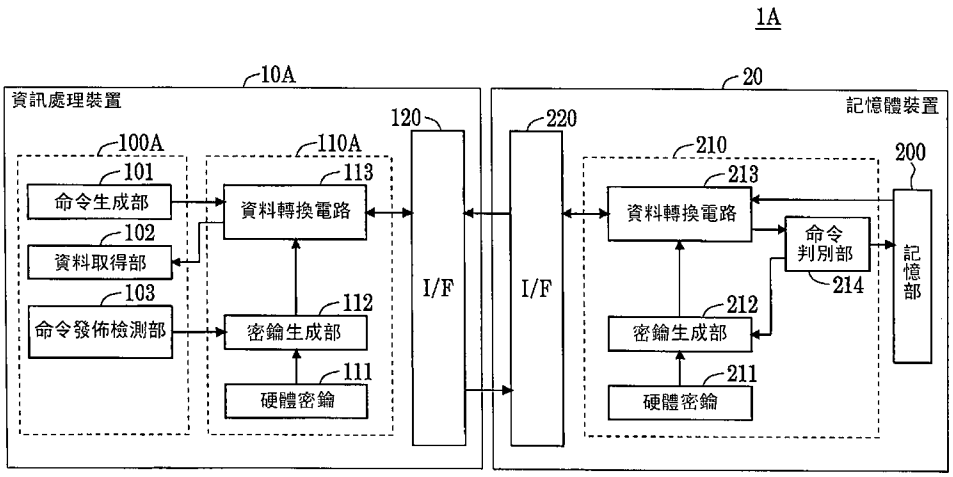

圖2

1A・・・記憶體資訊保護系統

10A・・・資訊處理裝置

20・・・記憶體裝置

100A・・・全體控制部

101・・・命令生成部

102・・・資料取得部

103・・・命令發佈檢測部

110A・・・記憶體控制部

111、211・・・硬體密鑰

112、212・・・密鑰生成部

113、213・・・資料轉換電路

120、220・・・介面部

200・・・記憶部

210・・・記憶體內控制部

214・・・命令判別部

發明專利說明書

公告本

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：099111023

※申請日：99/04/09　　※IPC 分類：G06F 12/14　(2006.01)

一、發明名稱：（中文/英文）

記憶體控制器，記憶體控制裝置，記憶體裝置，記憶體資訊保護系統及記憶體控制裝置之控制方法

MEMORY CONTROLLER, MEMORY CONTROL DEVICE, MEMORY DEVICE, MEMORY INFORMATION PROTECTING SYSTEM, AND METHOD OF CONTROLLING A MEMORY CONTROL DEVICE

二、中文發明摘要：

本發明係提供一種可提高記憶於記憶體裝置中的資訊之機密性之技術。記憶體控制器包括：密鑰生成部 112，於每既定時序生成新的用於資訊之加密/解碼之密鑰資訊；及資料轉換電路 113，根據資訊對輸出至記憶體裝置 20 之資訊進行加密，同時根據密鑰資訊對自記憶體裝置 20 所輸入之經加密的資訊進行解碼；而於資料轉換電路 113 中，每當密鑰生成部 112 生成新的密鑰資訊時，則進行將該新的密鑰資訊作為密鑰資訊的密鑰資訊更新。

三、英文發明摘要：

四、指定代表圖：

(一)本案指定代表圖為：第（ 2 ）圖。

(二)本代表圖之元件符號簡單說明：

1A	記憶體資訊保護系統
10A	資訊處理裝置
20	記憶體裝置
100A	全體控制部
101	命令生成部
102	資料取得部
103	命令發佈檢測部
110A	記憶體控制部
111、211	硬體密鑰
112、212	密鑰生成部
113、213	資料轉換電路
120、220	介面部
200	記憶部
210	記憶體內控制部
214	命令判別部

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

六、發明說明：

【發明所屬之技術領域】

本發明係關於一種確保資訊之機密性之技術。

【先前技術】

眾所周知有如下一種技術：將半導體記憶體等裝卸自由之記憶體裝置安裝於資訊處理裝置，利用記憶於該記憶體裝置中之軟體程式或者資料等之資訊，於資訊處理裝置中實現既定之功能。

於此種記憶體裝置中，有搭載用於確保記憶於記憶體裝置中的資訊之機密性之安全功能者。例如，專利文獻 1 中表示有利用關鍵資料對自記憶部輸出之資料進行加密之方法。

[先前技術文獻]

[專利文獻]

專利文獻 1：日本專利特開平 7-219852 號公報

【發明內容】

(發明所欲解決之問題)

然而，於上述專利文獻 1 中，當藉由對經加密之輸出信號進行解析而取得密鑰(key)資訊時，會有記憶於記憶體裝置中的資訊之機密性喪失之虞。

對此，本發明之目的在於提供一種可提高記憶於記憶體裝置中之資訊之機密性之技術。

(解決問題之手段)

本發明之第 1 側面係一種記憶體控制器，其包括：密鑰生成手段，於每既定時序，生成新的用於資訊之加密/解碼之密鑰資訊；及資料轉換手段，根據上述密鑰資訊對輸出至記憶有既定資訊之記憶體裝置之資訊進行加密，同時根據上述密鑰資訊對自上述記憶體裝置所輸入之經加密的上述既定資訊進行解碼；而於上述資料轉換手段中，每當上述密鑰生成手段生成新的密鑰資訊時，則進行將該新的密鑰資訊作為上述密鑰資訊的密鑰資訊更新。

又，本發明之第 2 側面係一種記憶體裝置，其包括：指示手段，於每既定時序，指示生成用於資訊之加密/解碼之密鑰資訊；密鑰生成手段，根據上述生成指示生成新的上述密鑰資訊；記憶手段，記憶有既定資訊；及資料轉換手段，根據上述密鑰資訊對上述既定資訊中作為讀出對象之資訊進行加密，同時根據上述密鑰資訊對自外部裝置所輸入之經加密的資訊進行解碼；而於上述資料轉換手段中，每當上述密鑰生成手段生成新的密鑰資訊時，則進行將該新的密鑰資訊作為上述密鑰資訊的密鑰資訊更新。

又，本發明之第 3 側面係一種記憶體資訊保護系統，其包括：記憶體裝置，記憶有既定資訊；及記憶體控制裝置，與上述記憶體裝置相對應；而上述記憶體控制裝置包括：第 1 密鑰生成手段，於每既定時序，生成新的用於資訊之加密/解碼之第 1 密鑰資訊；及第 1 資料轉換手段，根據上述第 1

密鑰資訊對輸出至上述記憶體裝置之資訊進行加密，同時根據上述第 1 密鑰資訊對自上述記憶體裝置所輸入之經加密的資訊進行解碼；於上述第 1 資料轉換手段中，每當上述第 1 密鑰生成手段生成新的第 1 密鑰資訊時，則進行將該新的第 1 密鑰資訊作為上述第 1 密鑰資訊的密鑰資訊更新，上述記憶體裝置包括：第 2 密鑰生成手段，與上述既定時序同步，生成與上述第 1 密鑰資訊相同之新的第 2 密鑰資訊；記憶手段，記憶有既定資訊；及第 2 資料轉換手段，根據上述第 2 密鑰資訊對上述既定資訊中作為讀出對象之資訊進行加密，同時根據上述第 2 密鑰資訊對自上述記憶體控制裝置所輸入之經加密的資訊進行解碼；於上述第 2 資料轉換手段中，每當上述第 2 密鑰生成手段生成新的第 2 密鑰資訊時，則進行將該新的第 2 密鑰資訊作為上述密鑰資訊的密鑰資訊更新。

(發明效果)

根據本發明，可提高記憶於記憶體裝置中的資訊之機密性。

【實施方式】

以下，參照圖式對本發明之實施形態進行說明。

<1.第 1 實施形態>

[1-1.構成概要]

圖 1 係表示記憶體資訊保護系統 1A 之外觀構成之圖。

如圖 1 所示，記憶體資訊保護系統 1A 係包括資訊處理裝置 10A 與記憶體裝置 20。

記憶體裝置 20 於通用罩幕式唯讀記憶體等記憶體核心內，記憶程式及/或資料等之資訊(亦稱為「記憶資訊」或「儲存資訊」)。該記憶資訊例如為由一種作為電腦裝置之資訊處理裝置 10A 所執行作為應用軟體之資料、及/或該應用軟體中所使用之資料等。該記憶體裝置 20 具有例如卡片或者卡匣之態樣，且可自由裝卸在資訊處理裝置 10A。記憶體裝置 20 係於安裝於資訊處理裝置 10A 之狀態下使用。

作為利用儲存於記憶體裝置 20 之記憶資訊的資訊處理裝置 10A，例如可包含有個人電腦(Personal Computer)、PDA(Personal Digital Assistant，個人數位助理)之類的攜帶式資訊終端裝置、或者影像處理裝置。

於此種記憶體資訊保護系統 1A 中，當將經加密之命令(加密命令)自資訊處理裝置 10A 供給至記憶體裝置 20 時，於記憶體裝置 20 中，對加密命令進行解碼，並執行由命令所指定之處理。

[1-2.功能區塊]

進而，對記憶體資訊保護系統 1A 之功能進行詳細敘述。圖 2 係表示第 1 實施形態記憶體資訊保護系統 1A 之功能構成之方塊圖。

如圖 2 所示，構成記憶體資訊保護系統 1A 之資訊處理裝

置 10A 係包括全體控制部 100A、記憶體控制部(記憶體控制器)110A 及介面部 120。

全體控制部 100A 為微電腦構成，主要包括 CPU(Central Processing Unit，中央處理單元)、RAM(Random Access Memory，隨機存取記憶體)及 ROM(Read Only Memory，唯讀記憶體)等。全體控制部 100A 讀出儲存於 ROM 內之程式，並由 CPU 執行該程式，藉此實現各種功能。

具體而言，全體控制部 100A 藉由上述程式之執行，功能性地實現命令生成部 101、資料取得部 102 及命令發佈檢測部 103。

命令生成部 101 具有生成對記憶體裝置 20 之命令所相關之命令碼、或者含有該命令碼及位址之命令之功能。例如，當讀出儲存於記憶體裝置 20 中之資料時，包含讀出命令碼與成為讀出對象之資料之位址的命令(亦稱為「讀出命令」)藉由命令生成部 101 而生成。

資料取得部 102 使自記憶體裝置 20 讀出之資料依序記憶於全體控制部 100A 內之記憶部(RAM)中，並判斷作為讀出對象之資料的取得是否已結束(完成)。

命令發佈檢測部 103 具有檢測來自命令生成部 101 之命令之輸出之功能，當檢測到命令之輸出時，對下述密鑰生成部 112 進行用於加密或解碼之密鑰資訊(密鑰資料)之生成指示。即，命令發佈檢測部 103 亦具有根據命令之輸出而對密

鑰生成部 112 指示生成密鑰資訊之指示手段作用。

記憶體控制部 110A 包括硬體密鑰 111、密鑰生成部(密鑰生成手段)112 及資料轉換電路(資料轉換手段)113。

硬體密鑰 111 為硬體晶片上所執行之固定資料。硬體密鑰 111 係例如使用與硬體密鑰 111 之位元長度相應之複數個反相器(NOT 電路)，將該反相器之輸入鉗位成電源電壓(Vcc)或者 GND(接地電位)而得以實現。再者，因硬體密鑰 111 係以硬體所實現之固定資料，故而亦可表現為未被 CPU 干涉之密鑰資料。

密鑰生成部 112 具有於每既定時序執行運算處理，新生成用於資訊之加密/解碼之密鑰資訊之功能。

具體而言，若接通資訊處理裝置 10A 之電源，則密鑰生成部 112 根據硬體密鑰 111 而生成初始密鑰資訊(密鑰生成部 112 之初始化)。又，密鑰生成部 112 係包括使構成密鑰資訊之位元串移位之移位手段而構成，根據命令發佈檢測部 103 之密鑰生成指示，使構成初始密鑰資訊之位元串依序移位，藉此生成新的密鑰資訊。

作為移位手段，例如可採用移位暫存器。當採用移位暫存器作為移位手段時，亦可按照以下方式構成密鑰生成部 112、即，每當接受密鑰生成指示時，即將時脈輸入至移位暫存器中，同時根據該時脈之輸入而將硬體密鑰 111 之位元串依序輸入至移位暫存器。

再者，於初始密鑰資訊之生成時，例如可使用虛擬亂數生成電路。於密鑰生成部 112 設為包括虛擬亂數生成電路之構成時，係根據硬體密鑰 111 由虛擬亂數生成電路生成虛擬亂數，且所生成之虛擬亂數被用作初始密鑰資訊。

如此，資訊處理裝置 10A 中之密鑰資訊之生成係根據與命令發佈同步之來自命令發佈檢測部 103 的密鑰生成指示而執行，且於每當發佈新的命令時即生成新的密鑰資訊。

資料轉換電路 113 具有下述之功能：對於自命令生成部 101 所輸出之命令，實施使用由密鑰生成部 112 所生成之密鑰資訊之既定的運算處理，藉此生成加密命令。藉由資料轉換電路 113 加密之加密命令經由介面部 120 而被供給至記憶體裝置 20。再者，關於加密方式，可採用例如串流加密方式或者區塊加密方式。

又，資料轉換電路 113 亦具有下述功能：使用由密鑰生成部 112 所生成之密鑰資訊對自記憶體裝置 20 提供之加密資料進行解碼。經解碼之資料被供給至資料取得部 102。

於進行資訊之加密/解碼之資料轉換電路 113 中，每當密鑰生成部 112 生成新的密鑰資訊時，即進行將該新的密鑰資訊作為用於加密/解碼之密鑰資訊的密鑰資訊更新。

包括此種記憶體控制部 110A 之裝置，係作為控制記憶體裝置 20 之動作之記憶體控制裝置而動作。於本實施形態中，例示記憶體控制部 110A 包含於資訊處理裝置 10A 中、

且資訊處理裝置 10A 作為記憶體控制裝置而動作之情形。

另一方面，構成記憶體資訊保護系統 1A 之記憶體裝置 20 包括記憶部(記憶手段)200、記憶體內控制部 210 及介面部 220。

記憶部 200 係罩幕式唯讀記憶體之類之非揮發性記憶體，其記憶有成為機密保護或防止不正當讀出之保護對象之程式及/或資料等。再者，該記憶部 200 並不受限為罩幕式唯讀記憶體，亦可為快閃記憶體、可抹除可程式唯讀記憶體(EP-ROM)或者硬碟(HD，Hard Disk)等。

記憶體內控制部 210 包括硬體密鑰 211、密鑰生成部 212、資料轉換電路 213 及命令判別部 214。

硬體密鑰 211 係硬體晶片上所執行之固定資料，該硬體密鑰 211 具有與資訊處理裝置 10A 之硬體密鑰 111 相同之資料構成。

密鑰生成部 212 具有下述功能：與資訊處理裝置 10A 之密鑰生成部 112 同樣地，於每既定時序執行運算處理，並生成用於加密/解碼之新密鑰資訊。具體而言，於資訊處理裝置 10A 之電源接通後，當對自資訊處理裝置 10A 發佈之初始化命令進行檢測時，密鑰生成部 212 根據硬體密鑰 211 而生成初始密鑰資訊(密鑰生成部 212 之初始化)。又，密鑰生成部 212 構成為包括使構成密鑰資訊之位元串移位之移位手段(例如移位暫存器)，根據命令判別部 214 之密鑰生成

指示，使初始密鑰資訊依序移位，藉此生成新的密鑰資訊。

資料轉換電路 213 係具有下述功能：對經由介面部 220 接收之加密命令，實施使用由密鑰生成部 212 所生成之密鑰資訊之既定之運算處理，藉此對加密命令進行解碼。藉由資料轉換電路 213 解碼之命令被供給至命令判別部 214。

又，資料轉換電路 213 亦具有下述功能：利用由密鑰生成部 212 生成之密鑰資訊，對自記憶部 200 讀出之資料進行加密，而生成加密資料。由資料轉換電路 213 加密之加密資料將經由介面部 220 而被供給至資訊處理裝置 10A。

於進行資訊之加密/解碼之資料轉換電路 213 中，每當由密鑰生成部 212 生成新的密鑰資訊時，進行將該新的密鑰資訊作為用於加密/解碼之密鑰資訊的密鑰資訊之更新。

命令判別部 214 判別經解碼之命令，並指示執行與該命令相應之既定動作。例如，於經資料轉換電路 213 解碼之來自資訊處理裝置 10A 的命令為來自記憶部 200 之資料的讀出命令之情形時，則自該讀出命令中抽取讀出命令碼與讀出位址資料，並將讀出信號與讀出位址資料提供給記憶部 200。

又，命令判別部 214 亦具有根據命令之輸入而對密鑰生成部 212 指示生成密鑰資訊之指示手段作用。

如此，記憶體裝置 20 中密鑰資訊之生成係根據與命令之接收同步之來自命令判別部 214 的密鑰生成指示而執行，每當記憶體裝置 20 接受新的命令時，密鑰資訊將會被更新。

如上述般，於包括資訊處理裝置 10A 與記憶體裝置 20 之記憶體資訊保護系統 1A 中，資訊處理裝置 10A 與記憶體裝置 20 之間所進行之命令或資料等之資訊(亦稱為「通訊資訊」)之通訊係經加密進行。而且，用於加密及/或解碼之密鑰資訊係於資訊處理裝置 10A 與記憶體裝置 20 之間，在以既定時序且同步之狀態下隨時更新。

具體而言，以下舉例說明讀出儲存於記憶體裝置 20 中之資料之情形。圖 3 係表示資料讀出時之記憶體資訊保護系統 1A 之狀態變遷之圖。

如圖 3 所示，當自資訊處理裝置 10A 發佈根據密鑰資訊 K1 加密之讀出命令(狀態 st1)後，資訊處理裝置 10A 及記憶體裝置 20 各自生成新的密鑰資訊 K2(狀態 st2)。

當傳輸與讀出命令相對應之讀出資料 D1 時，於記憶體裝置 20 中，根據新的密鑰資訊 K2 對該讀出資料 D1 進行加密，經加密之讀出資料將被傳輸至資訊處理裝置 10A(狀態 st3)。於資訊處理裝置 10A 中，使用密鑰資訊 K2 對經加密之讀出資料進行解碼，並接收讀出資料。進行資料之讀出直至指定之資料長度之讀出資料結束為止，當已讀出指定長度之讀出資料 D1 時，則結束讀出(狀態 st4)。

於自記憶體裝置 20 中進一步進行資料之讀出之情形時，於資訊處理裝置 10A 中使用密鑰資訊 K2 對讀出命令進行加密，並再次發佈經加密之讀出命令(狀態 st5)。當發佈讀出

命令時，資訊處理裝置 10A 及記憶體裝置 20 分別生成新的密鑰資訊 K3(狀態 st6)。

而且，當傳輸與讀出命令相對應之讀出資料 D2 時，於記憶體裝置 20 中根據新的密鑰資訊 K3 對該讀出資料 D2 進行加密，經加密之讀出資料被傳輸至資訊處理裝置 10A(狀態 st7)。於資訊處理裝置 10A 中，使用密鑰資訊 K3 對經加密之讀出資料進行解碼，並接收讀出資料。

如此，資訊處理裝置 10A 與記憶體裝置 20 係分別包括共通之密鑰生成部 112、212 及共通之硬體密鑰 111、211，於每既定時序在同步之狀態下分別生成彼此共通之新密鑰資訊。而且，資訊處理裝置 10A 與記憶體裝置 20 係於彼此共通之資料轉換電路 113、213 中，使用新生成之密鑰資訊，進行將用於對通訊資訊進行加密/解碼之密鑰資訊予以更新之更新動作。

藉此，於資訊處理裝置 10A 與記憶體裝置 20 之間，可於每既定時序使用更新之共通密鑰資訊，進行加密/解碼，因此可提高記憶於記憶體裝置 20 中的記憶資訊之機密性。例如，即便可解讀某一週期之密鑰資訊，而取得記憶資訊所包含內容之一部分，亦可降低取得資訊之全部內容之可能性。

又，於記憶體資訊保護系統 1A 中，密鑰資訊係於資訊處理裝置 10A 及記憶體裝置 20 各個中獨自生成，而在資訊處理裝置 10A 與記憶體裝置 20 之間並未進行密鑰資訊之交

換，因而可更進一步確保密鑰資訊之機密性。

又，於記憶體資訊保護系統 1A 中，使用由硬體構成之密鑰生成部 112、212 與硬體密鑰 111、211 而生成密鑰資訊，CPU 不參與密鑰資訊之生成。藉此，無法藉由解析 CPU 所執行之程式而特定密鑰資訊，因而可進一步確保密鑰資訊之機密性。

再者，上述雖已例示密鑰生成部 112、212 包括移位手段、且使用該移位手段使密鑰資訊移位而生成新的密鑰資訊之情形，但並不受限於此。具體而言，密鑰生成部 112、212 亦可構成為包括加密電路，且以串流加密方式或者區塊加密方式進行加密，並根據硬體密鑰 111、211 生成新的密鑰資訊。

於採用上述構成之情形時，於由密鑰生成部 112、212 及資料轉換電路 113、213 執行一系列處理中，亦可表現為：密鑰生成部 112、212 對硬體密鑰 111、211 進行第 1 階段加密處理而生成密鑰資訊，資料轉換電路 113、213 使用密鑰資訊進行將命令加密之第 2 階段加密處理。

[1-3.記憶體資訊保護系統 1A 之動作]

以下，對記憶體資訊保護系統 1A 之動作進行說明。圖 4 及圖 5 係表示記憶體資訊保護系統 1A 之動作之流程圖。於圖 4 及圖 5 中，左側係表示資訊處理裝置 10A 之動作之流程圖，右側係表示記憶體裝置 20 之動作之流程圖。再者，

記憶體裝置 20 非為包含如 CPU 之處理手段者，而係以硬體電路進行動作，此處，方便起見以與資訊處理裝置 10A 之動作流程相對應之流程來表示。

於記憶體資訊保護系統 1A 之動作開始前，記憶體裝置 20 係安裝於資訊處理裝置 10A，各個介面部 120、220 保持電性連接。而且，隨資訊處理裝置 10A 之電源接通，啟動資訊處理裝置 10A，同時對記憶體裝置 20 供電，開始系統之動作。

如圖 4 所示，於資訊處理裝置 10A 中，當電源接通時，於步驟 SP101 中進行密鑰生成部 112 之初始化。在密鑰生成部 112 之初始化中，根據硬體密鑰 111 生成初始密鑰資訊。

於步驟 SP102 中，使用初始密鑰資訊進行資料轉換電路 113 之初始化。

於步驟 SP103 中，藉由命令生成部 101 生成初始化命令，對記憶體裝置 20 發佈初始化命令。而且，當初始化命令發佈後，於資料轉換電路 113 中，加密/解碼功能有效接通(ON)。藉此，於資料轉換電路 113 中，可進行使用初始密鑰資訊之資料加密/解碼。

另一方面，於記憶體裝置 20 中，當電源供給開始後，則於步驟 SP201 中，藉由命令判別部 214 判定有無初始化命令之輸入。命令判別部 214 在檢測到初始化命令之輸入後，則對密鑰生成部 212 指示進行初始化。

於步驟 SP202 中，根據命令判別部 214 之初始化指示而對密鑰生成部 212 進行初始化，且根據硬體密鑰 211 生成初始密鑰資訊。

於步驟 SP203 中，使用初始密鑰資訊對資料轉換電路 213 進行初始化。藉此，於資料轉換電路 213 中，可使用初始密鑰資訊進行資料之加密/解碼。

其次，於資訊處理裝置 10A 中，於步驟 SP104 中，判定資訊處理裝置 10A 之電源是否關閉，於資訊處理裝置 10A 之電源關閉之情形時，則結束資訊處理裝置 10A 之動作。於資訊處理裝置 10A 之電源接通之情形時，動作步驟過渡至步驟 SP105。

於步驟 SP105(參照圖 5)中，藉由命令生成部 101 生成對記憶體裝置 20 之命令。

於步驟 SP106 中，由命令生成部 101 生成之命令被輸入至資料轉換電路 113，於資料轉換電路 113 中，使用初始密鑰資訊進行命令之加密。再者，當經重複處理而再次執行步驟 SP106 時，則使用新的密鑰資訊對命令進行加密。

於步驟 SP107 中，將經資料轉換電路 113 加密之加密命令經由介面部 120 而向記憶體裝置 20 發佈。

又，若命令發佈檢測部 103 檢測到命令生成部 101 之命令輸出後，則命令發佈檢測部 103 對密鑰生成部 112 指示生成密鑰資訊。藉此，於步驟 SP108 中，藉由密鑰生成部 112

生成新的密鑰資訊，於資料轉換電路 113 中進行密鑰資訊之更新。

另一方面，於記憶體裝置 20 中，若於步驟 SP204 中輸入加密命令，則動作步驟過渡至步驟 SP205。

於步驟 SP205 中，使用初始密鑰資訊對加密命令進行解碼。

若經解碼之命令輸入至命令判別部 214，則命令判別部 214 對密鑰生成部 212 指示生成密鑰資訊。藉此，於步驟 SP206 中，藉由密鑰生成部 212 生成新的密鑰資訊，並於資料轉換電路 213 中進行密鑰資訊之更新。

又，於步驟 SP207 中，藉由命令判別部 214 判定資訊處理裝置 10A 之命令是否為讀出命令。於自資訊處理裝置 10A 輸入之命令不為讀出命令之情形時，動作步驟過渡至步驟 SP208，執行基於所輸入命令之讀出處理以外的其他處理。

於自資訊處理裝置 10A 輸入之命令為讀出命令之情形時，則過渡至步驟 SP209，並執行資料之讀出處理(步驟 SP209～步驟 SP211)。

具體而言，於步驟 SP209 中，將讀出信號與讀出位址資料提供給記憶部 200，且自記憶部 200 讀出記憶於所指定讀出位址之資料。而且，於步驟 SP210 中，資料轉換電路 213 使用新的密鑰資訊對讀出之資料進行加密。於步驟 SP211 中，將經加密之讀出資料經由介面部 220 而輸出至資訊處理

裝置 10A。

於資訊處理裝置 10A 中，當在步驟 SP108 中進行密鑰資訊之更新後，動作步驟過渡至步驟 SP109。

於步驟 SP109 中，判定是否已在步驟 SP105 中生成讀出命令，於未生成讀出命令之情形時，動作步驟過渡至步驟 SP104，並再次執行命令生成處理等。另一方面，於已生成讀出命令之情形時，動作步驟過渡至步驟 SP110，並進行自記憶體裝置 20 接收讀出資料之處理。

具體而言，於步驟 SP110 中，若自記憶體裝置 20 輸入讀出資料後，則資料轉換電路 113 使用已於步驟 SP108 中生成之新密鑰資訊而對讀出資料進行解碼。

於步驟 SP111 中，藉由資料取得部 102 而將讀出資料記憶於 RAM 中。

於步驟 SP112 中，藉由資料取得部 102，判定所指定資料長度之資料取得是否已結束。於讀出資料之取得尚未結束之情形時，重複執行步驟 SP110～步驟 SP112 之處理，直至指定資料長度之資料取得結束為止。於指定資料長度之資料取得已結束之情形時，則過渡至步驟 SP104，視需要生成新的命令，並執行與該新的命令相對應之動作。

如以上般，記憶體資訊保護系統 1A 包括記憶有既定資訊之記憶體裝置 20、及與記憶體裝置 20 相對應之記憶體控制裝置 10A。而且，記憶體控制裝置 10A 包括：密鑰生成部

112，於每既定時序生成用於資訊之加密/解碼之新第 1 密鑰資訊；及資料轉換電路 113，根據第 1 密鑰資訊對輸出至記憶體裝置 20 之資訊進行加密，同時根據第 1 密鑰資訊對自記憶體裝置 20 輸入之加密資訊進行解碼；而於資料轉換電路 113 中，每當密鑰生成部 112 生成新的第 1 密鑰資訊時，則進行將該新的第 1 資訊作為密鑰資訊的密鑰資訊之更新。另一方面，記憶體裝置 20 包括：密鑰生成部 212，與上述既定時序同步地，生成與第 1 資訊相同之新第 2 密鑰資訊；記憶部 200，記憶有既定資訊；及資料轉換電路 213，根據第 2 密鑰資訊對既定資訊中作為讀出對象之資訊進行加密，同時根據第 2 資訊對自記憶體控制裝置 10A 所輸入之經加密的資訊進行解碼；而於資料轉換電路 213 中，每當藉由密鑰生成部 212 生成新的第 2 密鑰資訊時，則進行將該新的第 2 密鑰資訊作為密鑰資訊的密鑰資訊之更新。

藉由上述記憶體資訊保護系統 1A，於記憶體控制裝置 10A 及記憶體裝置 20 中，可使用於每既定時序更新之共通之密鑰資訊進行加密/解碼，因此可提高記憶於記憶體裝置 20 中之既定資訊之機密性。

<2.第 2 實施形態>

其次，對本發明第 2 實施形態進行說明。關於上述第 2 實施形態之記憶體資訊保護系統 1B，除包括亂數生成部之部分外，其餘具有與記憶體資訊保護系統 1A 幾乎相同之構

造及功能，對於共通之部分附加相同之元件符號並省略說明。圖 6 係表示第 2 實施形態記憶體資訊保護系統 1B 之功能構成之方塊圖。

如圖 6 所示，記憶體資訊保護系統 1B 之資訊處理裝置 10B 包括全體控制部 100B、與第 1 實施形態相同之記憶體控制部 110B 及與第 1 實施形態相同之介面部 120。

全體控制部 100B 主要包括 CPU、RAM 及 ROM 等，除命令生成部 101、資料取得部 102 及命令發佈檢測部 103 以外，其進一步功能性地實現亂數生成部 104 與控制暫存器部 105。

亂數生成部 104，具有當資訊處理裝置 10B 之啟動時根據虛擬亂數生成演算法而生成亂數值之功能。

亂數生成部 104 中所生成之亂數值被發送至命令生成部 101。取得亂數值之命令生成部 101 亦生成包含亂數值之命令(亦稱為「亂數儲存命令」)。又，亂數生成部 104 中所生成之亂數值經由控制暫存器部 105 發送至密鑰生成部 112。

記憶體控制部 110B 之密鑰生成部 112 具有自較記憶體控制部 110B 更靠近外部之全體控制部 100B 取得亂數值之功能，且於初始化時根據硬體密鑰 111 與亂數值生成初始密鑰資訊。

此處，對記憶體資訊保護系統 1B 之動作進行說明。圖 7 係表示記憶體資訊保護系統 1B 啟動後之初始動作之流程

圖。圖 7 中，左側係表示資訊處理裝置 10B 之動作之流程圖，右側係表示記憶體裝置 20 之動作之流程圖。

記憶體裝置 20 安裝於資訊處理裝置 10B，當對資訊處理裝置 10B 接通電源後，開始系統之動作。

具體而言，如圖 7 所示，於資訊處理裝置 10B 中，於步驟 SP51 中，藉由亂數生成部 104 生成亂數值。

於下一步驟 SP52 中，藉由命令生成部 101，生成包含亂數值之亂數儲存命令，並對記憶體裝置 20 發佈亂數儲存命令。

而且，於步驟 SP101 中，進行密鑰生成部 112 之初始化，並根據硬體密鑰 111 與亂數值生成初始密鑰資訊。

於步驟 SP102 中，使用初始密鑰資訊進行資料轉換電路 113 之初始化。

於步驟 SP103 中，藉由命令生成部 101 生成初始化命令，對記憶體裝置 20 發佈初始化命令。而且，於初始化命令發佈後，於資料轉換電路 113 中使加密/解碼功能有效接通(ON)。藉此，於資料轉換電路 113 中，可使用初始密鑰資訊而進行資料之加密/解碼。

另一方面，於記憶體裝置 20 中，當電源供給開始後，於步驟 SP61 中，藉由命令判別部 214 判定亂數儲存命令之輸入有無。當命令判別部 214 判定已輸入有亂數儲存命令時，動作步驟過渡至步驟 SP62。

於步驟 SP62 中，命令判別部 214 自亂數儲存命令中抽取亂數值，並將該亂數值發送至密鑰生成部 212。

於下一步驟 SP201 中，藉由命令判別部 214 判定初始化命令之輸入有無。若命令判別部 214 判定為已輸入有初始化命令，則動作步驟過渡至步驟 SP202。

於步驟 SP202 中，進行密鑰生成部 212 之初始化，並根據硬體密鑰 211 及亂數值生成初始密鑰資訊。

於步驟 SP203 中，使用初始密鑰資訊進行資料轉換電路 213 之初始化。藉此，於資料轉換電路 213 中，可使用初始密鑰資訊進行資料之加密或解碼。

於資訊處理裝置 10B 及記憶體裝置 20 中，當上述初始動作結束後，執行與第 1 實施形態之資訊處理裝置 10A 及記憶體裝置 20 各自之動作(參照圖 5)相同之動作。

如以上，於記憶體資訊保護系統 1B 中，分別於資訊處理裝置 10B 及記憶體裝置 20 中，根據相同之亂數值生成最初之初始密鑰資訊。藉此，可避免每當啟動時生成相同之初始密鑰資訊，因此可使第三者對硬體密鑰 111、211 之特定變得更困難。

再者，密鑰生成部 112、212 具有加密電路，使用串流加密方式或者區塊加密方式進行加密，於生成密鑰資訊之構成之情形時，密鑰生成部 112、212 透過該加密而根據硬體密鑰 111 及亂數值生成新的密鑰資訊。

<3.變形例>

以上，已對本發明之實施形態進行說明，但本發明並不受限於上述說明之內容。

例如，於上述各實施形態中，已例示資訊處理裝置 10A、10B 與記憶體裝置 20 中用於密鑰生成之硬體構成為共通之情形，但並不受限於此。具體而言，只要可生成共通之密鑰資訊，則資訊處理裝置 10A、10B 與記憶體裝置 20 中用於密鑰生成之硬體構成亦可不同。

又，於上述各實施形態中，已例示資訊處理裝置 10A、10B 及記憶體裝置 20 分別各包括一個硬體密鑰 111、211 之情形，但並不受限於此。具體而言，亦可包括複數個硬體密鑰。圖 8 係表示變形例記憶體資訊保護系統 1H 之功能構成之方塊圖。

例如，如圖 8 所示，記憶體資訊保護系統 1H 之記憶體控制部 110H 包括第 1 硬體密鑰 151、第 2 硬體密鑰 152、密鑰生成部 112H 及資料轉換電路 113H。

於密鑰生成部 112H 中，初始化時根據第 2 硬體密鑰 152 生成初始密鑰資訊。又，於初始密鑰資訊生成後，根據密鑰生成指示而使初始密鑰資訊依序移位，藉此生成新的密鑰資訊。

於資料轉換電路 113H 中，根據第 1 硬體密鑰 151 及由密鑰生成部 112 所生成之密鑰資訊進行資料轉換電路 113H 之

初始化，並進行用於加密/解碼的密鑰資訊之更新。

又，記憶體資訊保護系統 1H 之記憶體內控制部 210H 亦包括第 1 硬體密鑰 153、第 2 硬體密鑰 154、密鑰生成部 212H 及資料轉換電路 213H。

於密鑰生成部 212H 中，初始化時根據第 2 硬體密鑰 154 生成初始密鑰資訊。又，於初始密鑰資訊生成後，根據密鑰生成指示使初始密鑰資訊依序移位，藉此生成新的密鑰資訊。

於資料轉換電路 213H 中，根據第 1 硬體密鑰 153 及由密鑰生成部 212H 生成之密鑰資訊進行資料轉換電路 213H 之初始化，並進行用於加密/解碼的密鑰資訊之更新。

如此，記憶體資訊保護系統 1H 中之資訊處理裝置 10H 及記憶體裝置 20H 係分別使用兩個硬體密鑰而生成用於加密/解碼之密鑰資訊。藉此，可使第三者對於硬體密鑰之特定變得更困難。

又，於上述第 2 實施形態之亂數生成部 104 中，係以計算機演算法所產生之虛擬亂數作為亂數值而使用，但不受限於此，亦可將根據物理現象等產生之真亂數作為亂數值使用。

【圖式簡單說明】

圖 1 係表示記憶體資訊保護系統之外觀構成之圖。

圖 2 係表示第 1 實施形態記憶體資訊保護系統之功能構成之方塊圖。

圖 3 係表示資料讀出時記憶體資訊保護系統之狀態轉變之圖。

圖 4 係表示第 1 實施形態記憶體資訊保護系統之動作之流程圖。

圖 5 係表示第 1 實施形態記憶體資訊保護系統之動作之流程圖。

圖 6 係表示第 2 實施形態記憶體資訊保護系統之功能構成之方塊圖。

圖 7 係表示第 2 實施形態記憶體資訊保護系統啟動後之初始動作之流程圖。

圖 8 係表示變形例記憶體資訊保護系統之功能構成之方塊圖。

【主要元件符號說明】

1A、1B、1H	記憶體資訊保護系統
10A、10B、10H	資訊處理裝置
20、20H	記憶體裝置
100A、100B	全體控制部
101	命令生成部
102	資料取得部
103	命令發佈檢測部
104	亂數生成部
105	控制暫存器部

110A、110B、110H	記憶體控制部
111、211	硬體密鑰
112、212、112H、212H	密鑰生成部
113、213、113H、213H	資料轉換電路
151、153	第一硬體密鑰
152、154	第二硬體密鑰
120、220	介面部
200	記憶部
210、210H	記憶體內控制部
214	命令判別部
D1、D2	讀出資料
K1、K2、K3	密鑰資訊
st1～st8	狀態
Y	是
N	否

七、申請專利範圍：

P.27-31

1.一種記憶體控制器，其包括：

密鑰(key)生成手段，於每既定時序，生成新的用於資訊之加密/解碼之密鑰資訊；

資料轉換手段，根據上述密鑰資訊對輸出至記憶有既定資訊之記憶體裝置之資訊進行加密，同時根據上述密鑰資訊對自上述記憶體裝置所輸入之經加密的上述既定資訊進行解碼；

由硬體所實現之固定硬體密鑰；及

取得外部所生成亂數值之亂數取得手段，

其中，於上述資料轉換手段中，每當上述密鑰生成手段生成新的密鑰資訊時，則進行將該新的密鑰資訊作為上述密鑰資訊的密鑰資訊更新，

上述密鑰生成手段係包括於每上述既定時序使構成上述密鑰資訊之位元串移位而生成上述新的密鑰資訊之移位手段，

上述密鑰生成手段係於上述記憶體控制裝置之啟動時，使用上述硬體密鑰與上述亂數值而生成初始密鑰資訊，及

上述新的密鑰資訊係經由於每上述既定時序使構成上述初始密鑰資訊之位元串依序移位而取得。

2.如申請專利範圍第1項之記憶體控制器，其中，

上述移位手段係包含移位暫存器。

3.一種記憶體控制裝置，其係包括申請專利範圍第 1 或 2 項之記憶體控制器。

4.一種記憶體裝置，其包括：

指示手段，於每既定時序，指示生成用於資訊之加密/解碼之密鑰資訊；

密鑰生成手段，根據上述生成指示生成新的上述密鑰資訊；

記憶手段，記憶有既定資訊；及

資料轉換手段，根據上述密鑰資訊對上述既定資訊中作為讀出對象之資訊進行加密，同時根據上述密鑰資訊對自外部裝置所輸入之經加密的資訊進行解碼，

其中，於上述資料轉換手段中，每當上述密鑰生成手段生成新的密鑰資訊時，則進行將該新的密鑰資訊作為上述密鑰資訊的密鑰資訊更新，

上述指示手段係根據自上述外部裝置之初始化命令輸入，進行上述密鑰生成手段之初始化指示，

上述密鑰生成手段係包括於每上述既定時序使構成上述密鑰資訊之位元串移位而生成上述新的密鑰資訊之移位手段，

上述記憶體裝置取得由上述外部裝置所生成之亂數值，

上述密鑰生成手段係根據上述初始化指示，使用上述硬體密鑰與上述亂數值而生成初始密鑰資訊，及

上述新的密鑰資訊係經由根據上述生成指示使構成上述初始密鑰資訊之位元串依序移位而取得。

5.如申請專利範圍第4項之記憶體裝置，其中，

上述移位手段係包含移位暫存器。

6.如申請專利範圍第4或5項之記憶體裝置，其中，

上述指示手段係根據自上述外部裝置之命令輸入，進行上述生成指示。

7.一種記憶體資訊保護系統，其包括

記憶體裝置，記憶有既定資訊；及

記憶體控制裝置，與上述記憶體裝置相對應；

而上述記憶體控制裝置包括：

第1密鑰生成手段，於每既定時序，生成新的用於資訊之加密/解碼之第1密鑰資訊；及

第1資料轉換手段，根據上述第1密鑰資訊對輸出至上述記憶體裝置之資訊進行加密，同時根據上述第1密鑰資訊對自上述記憶體裝置所輸入之經加密的資訊進行解碼；

於上述第1資料轉換手段中，每當上述第1密鑰生成手段生成新的第1密鑰資訊時，則進行將該新的第1密鑰資訊作為上述第1密鑰資訊的密鑰資訊更新，

上述記憶體裝置包括：

第2密鑰生成手段，與上述既定時序同步，生成與上述第1密鑰資訊相同之新的第2密鑰資訊；

記憶手段，記憶有既定資訊；及

第 2 資料轉換手段，根據上述第 2 密鑰資訊對上述既定資訊中作為讀出對象之資訊進行加密，同時根據上述第 2 密鑰資訊對自上述記憶體控制裝置所輸入之經加密的資訊進行解碼；

於上述第 2 資料轉換手段中，每當上述第 2 密鑰生成手段生成新的第 2 密鑰資訊時，則進行將該新的第 2 密鑰資訊作為上述密鑰資訊的密鑰資訊更新。

8.一種記憶體控制裝置之控制方法，其包括：

a)於每既定時序，生成新的用於資訊之加密/解碼之密鑰資訊之步驟；

b)根據上述密鑰資訊對輸出至記憶有既定資訊之記憶體裝置之資訊進行加密，同時根據上述密鑰資訊對自上述記憶體裝置所輸入之經加密的資訊進行解碼之步驟；

c)取得由硬體所實現之固定硬體密鑰之步驟；及

d)取得外部所生成亂數值之步驟；

其中，於上述 b)步驟中，每當在上述 a)步驟生成新的密鑰資訊時，則進行將該新的密鑰資訊作為上述密鑰資訊的密鑰資訊更新，

上述 a)步驟係包括於每上述既定時序使構成上述密鑰資訊之位元串移位而生成上述新的密鑰資訊，

上述 a)步驟之生成密鑰資訊係包括於上述記憶體控制裝

置之啟動時，使用上述硬體密鑰與上述亂數值而生成初始密鑰資訊，及

上述新的密鑰資訊係經由於每上述既定時序使構成上述初始密鑰資訊之位元串依序移位而取得。

八、圖式：

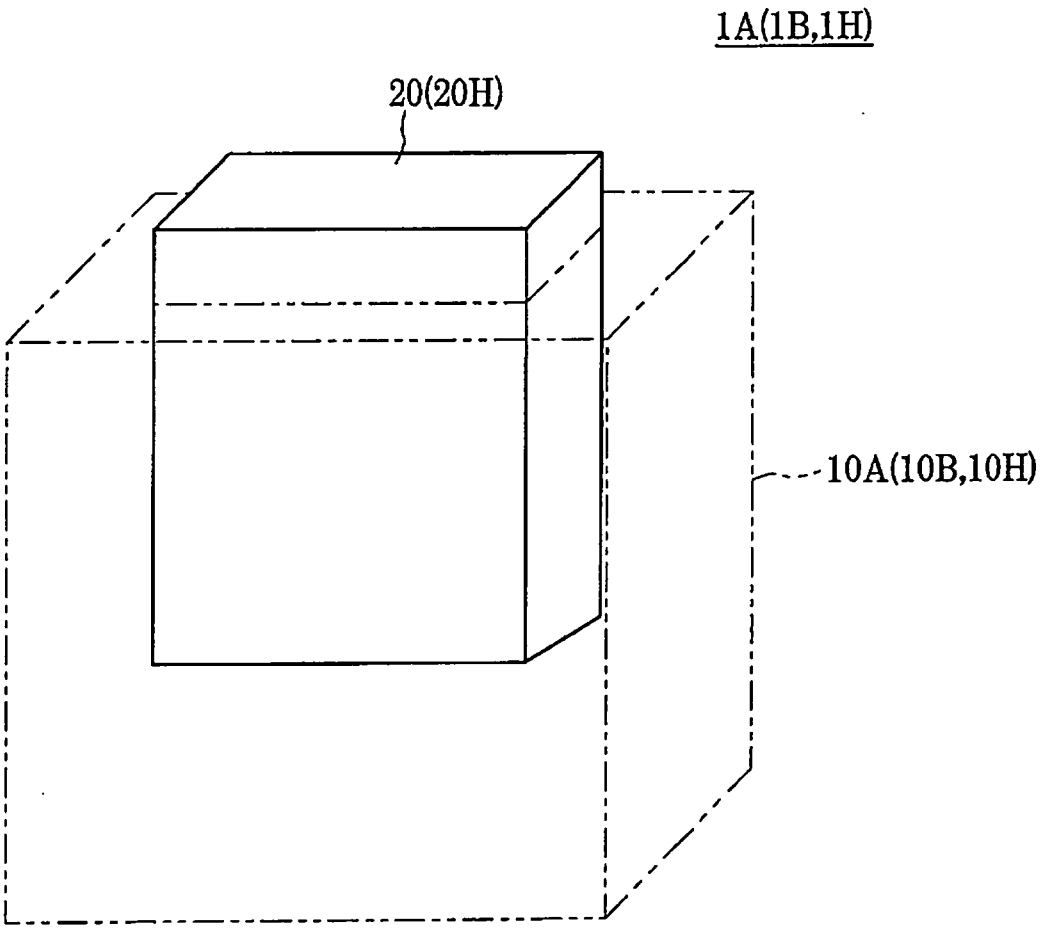

圖1

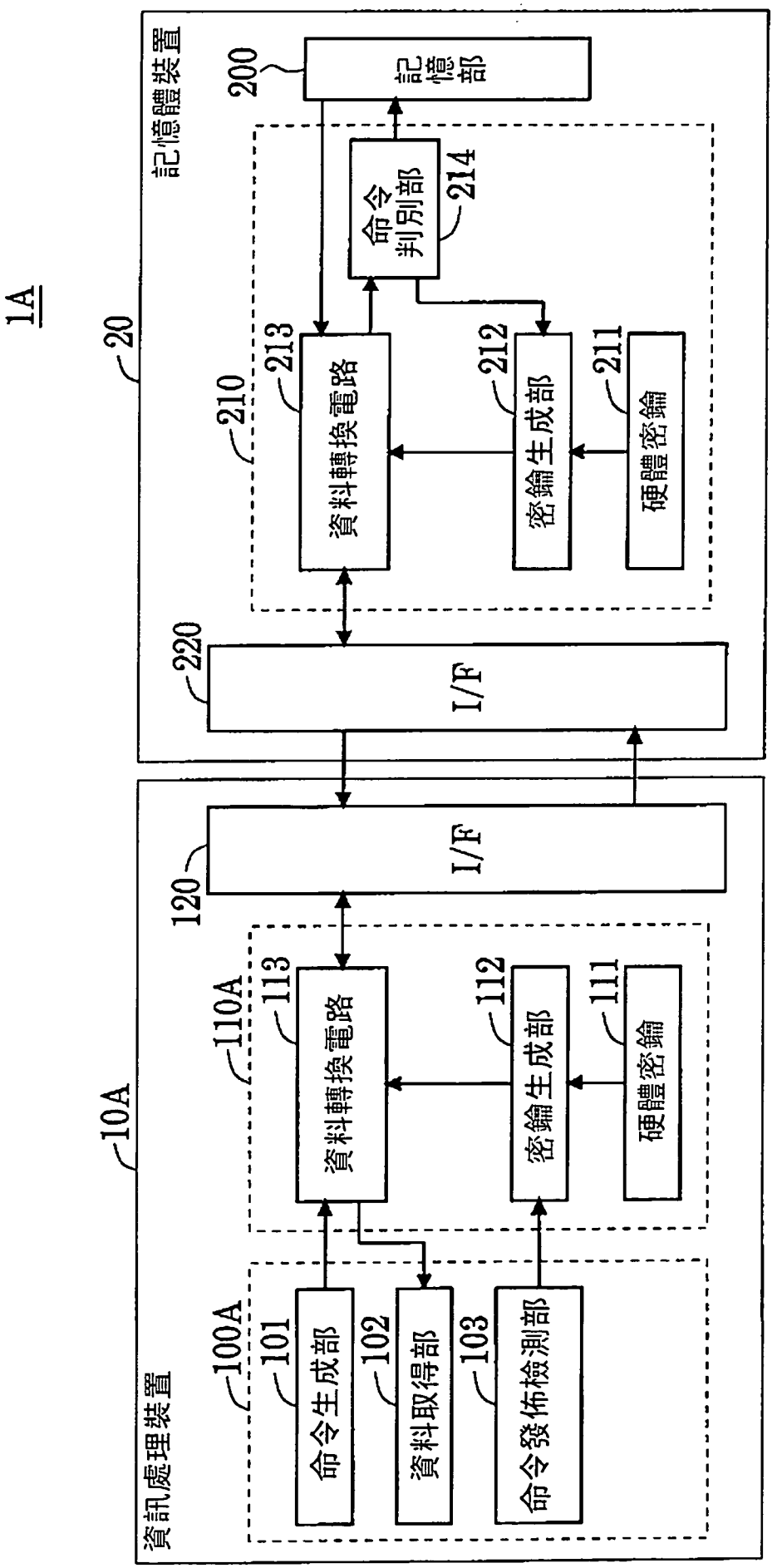
1A
資訊處理裝置
10A
100A
101
命令生成部
102
資料取得部
103
命令發佈檢測部
110A
113
資料轉換電路
112
密鑰生成部
111
硬體密鑰
120
I/F
記憶體裝置
20
200
記憶部
214
命令判別部
210
213
資料轉換電路
212
密鑰生成部
211
硬體密鑰
220
I/F

圖2

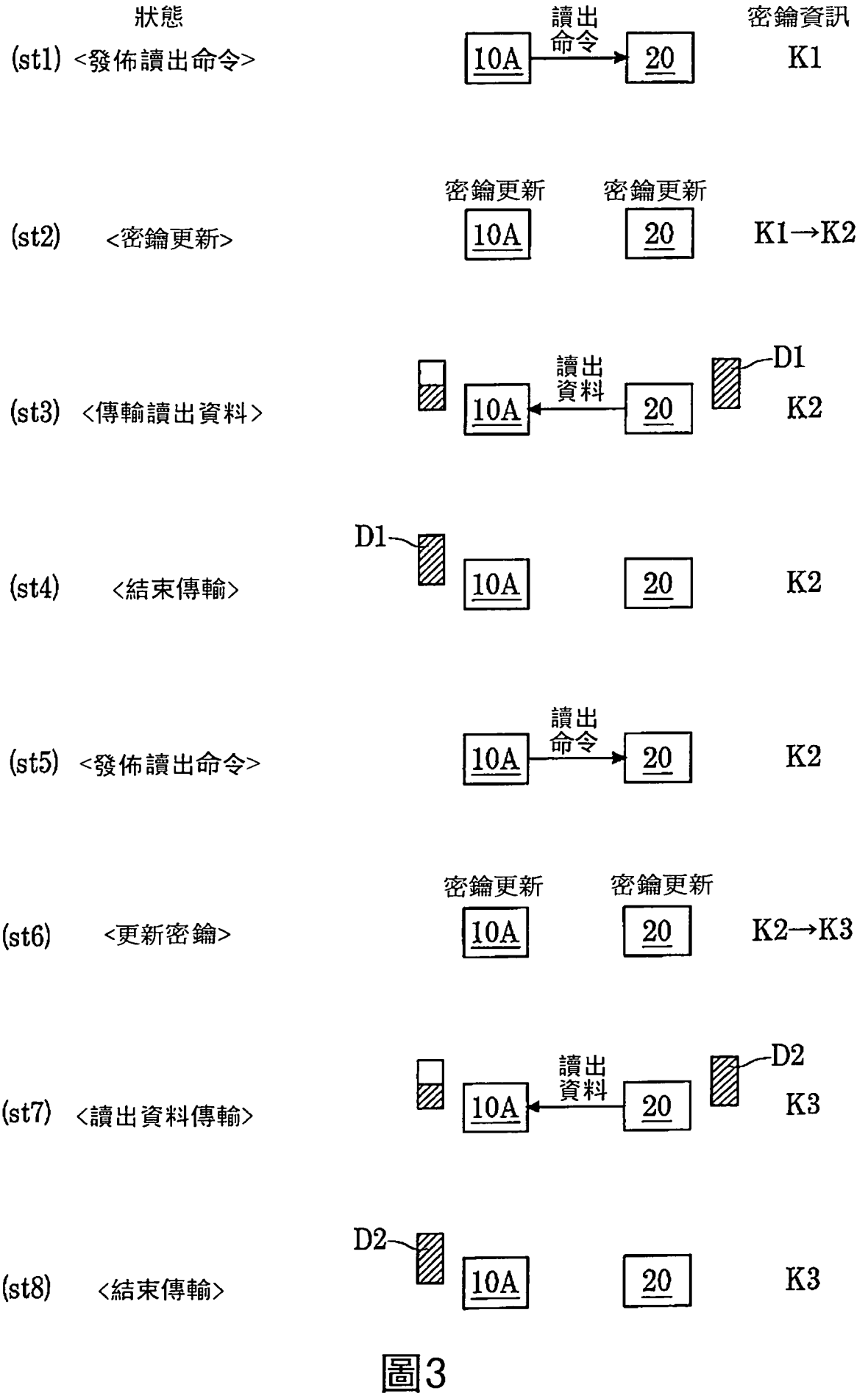
狀態
密鑰資訊
(st1) <發佈讀出命令>
讀出命令
10A
20
K1
密鑰更新
密鑰更新
(st2) <密鑰更新>
10A
20
K1→K2
讀出資料
D1
(st3) <傳輸讀出資料>
10A
20
K2
D1
(st4) <結束傳輸>
10A
20
K2
讀出命令
(st5) <發佈讀出命令>
10A
20
K2
密鑰更新
密鑰更新
(st6) <更新密鑰>
10A
20
K2→K3
讀出資料
D2
(st7) <讀出資料傳輸>
10A
20
K3
D2
(st8) <結束傳輸>
10A
20
K3

圖3

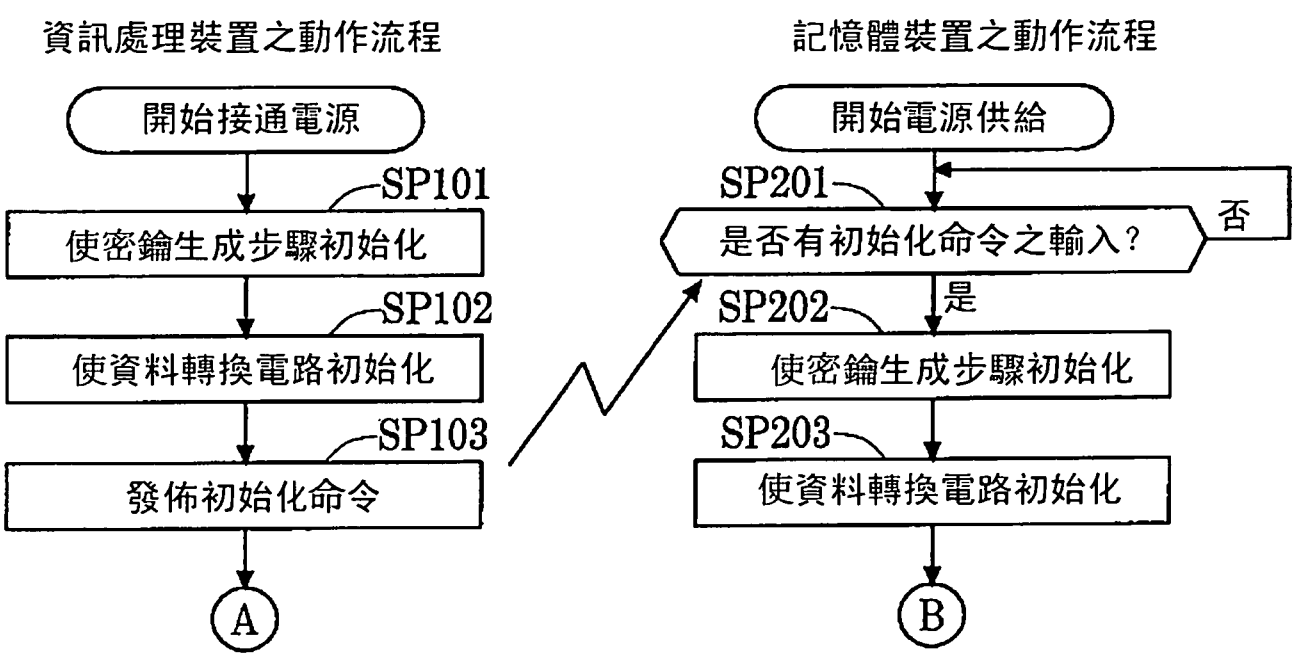
資訊處理裝置之動作流程
開始接通電源
SP101
使密鑰生成步驟初始化
SP102
使資料轉換電路初始化
SP103
發佈初始化命令
A
記憶體裝置之動作流程
開始電源供給
SP201
是否有初始化命令之輸入？
否
是
SP202
使密鑰生成步驟初始化
SP203
使資料轉換電路初始化
B

圖4

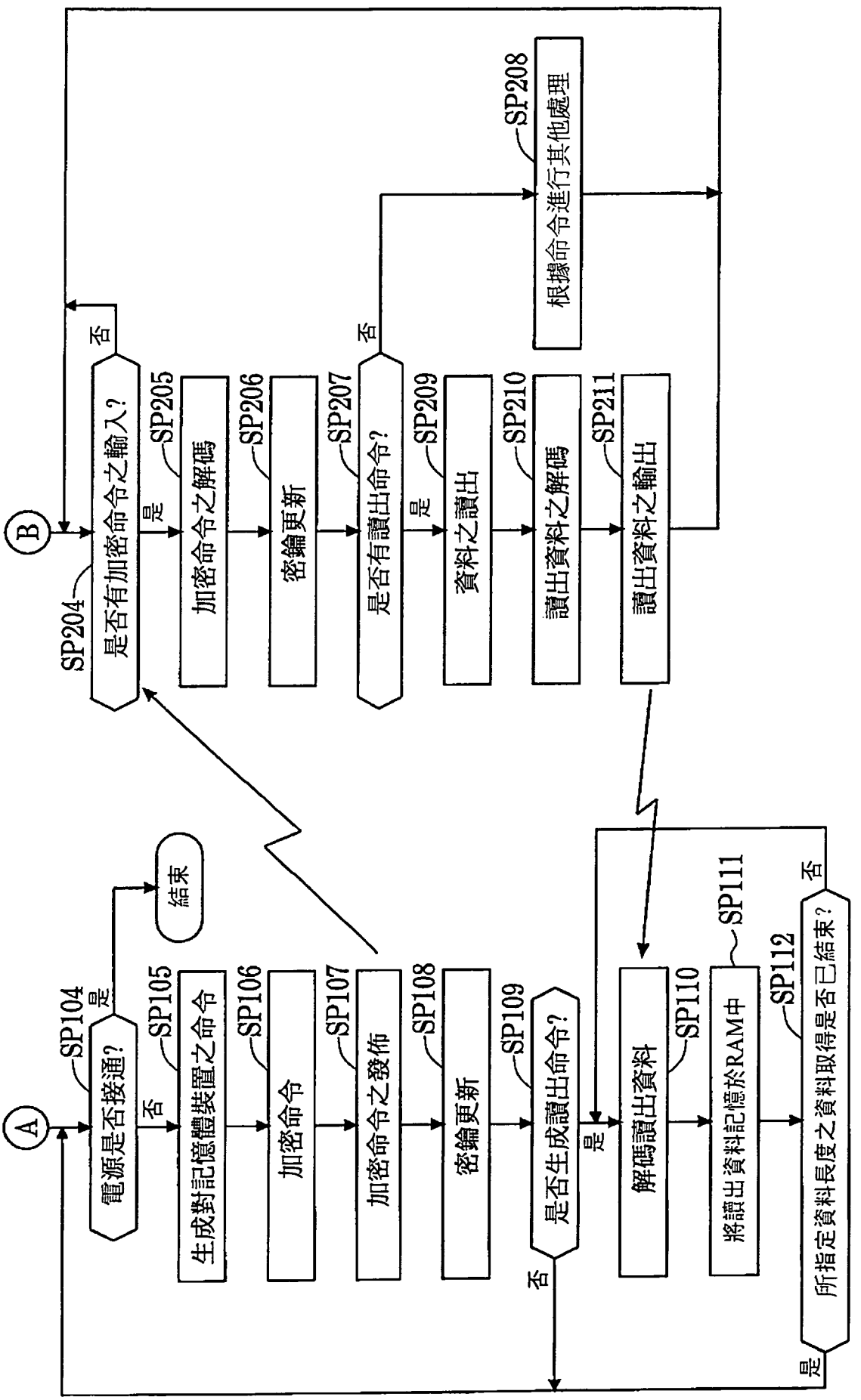
A
SP104
電源是否接通?
是
結束
否
SP105
生成對記憶體裝置之命令
SP106
加密命令
SP107
加密命令之發佈
SP108
密鑰更新
SP109
是否生成讀出命令?
否
是
SP110
解碼讀出資料
SP111
將讀出資料記憶於RAM中
SP112
所指定資料長度之資料取得是否已結束?
否
是
B
SP204
是否有加密命令之輸入?
是
否
SP205
加密命令之解碼
SP206
密鑰更新
SP207
是否有讀出命令?
是
否
SP208
根據命令進行其他處理
SP209
資料之讀出
SP210
讀出資料之解碼
SP211
讀出資料之輸出

圖5

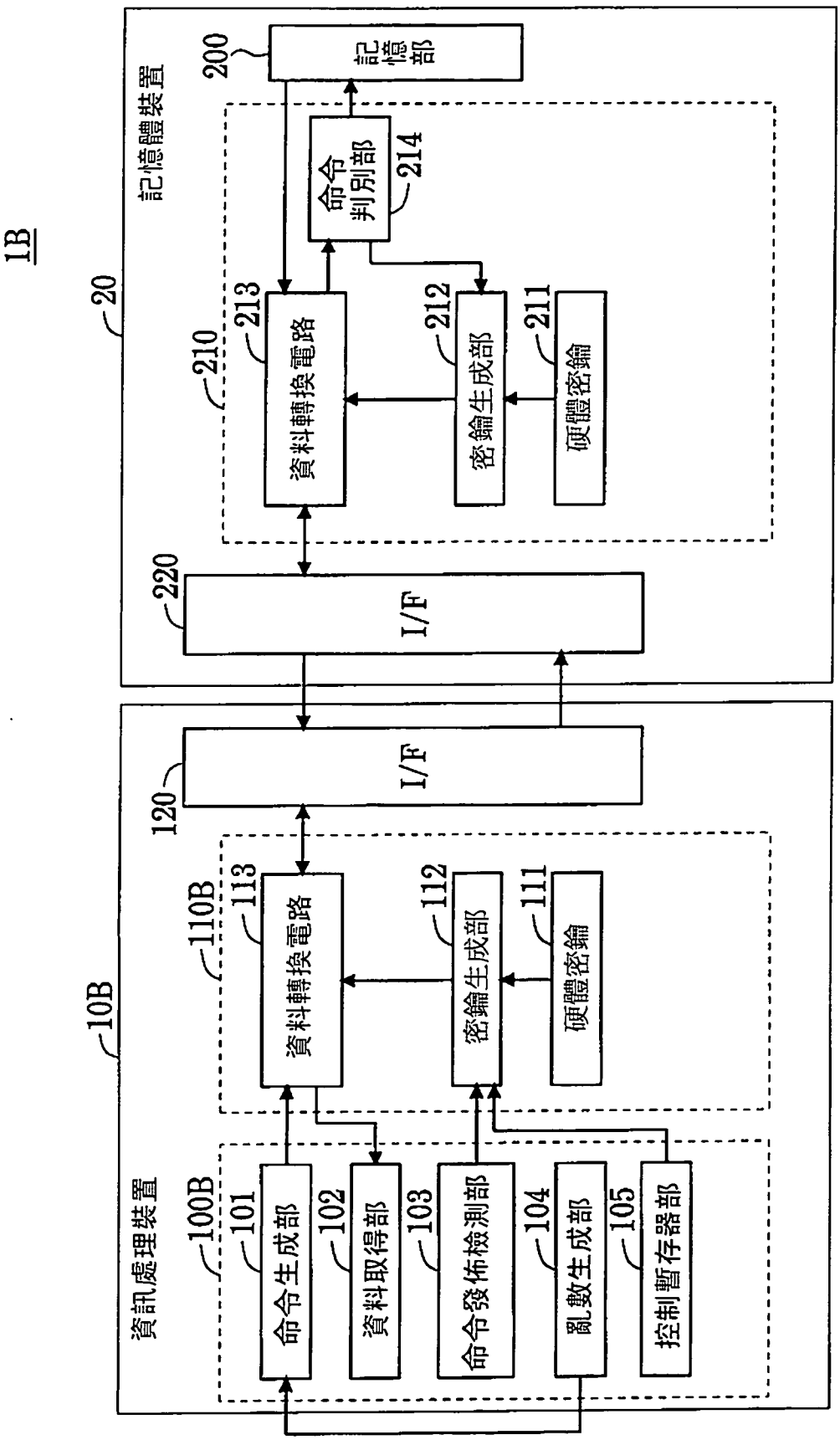
1B
20
記憶體裝置
200
記憶部
命令判別部
214
210
213
資料轉換電路
212
密鑰生成部
211
硬體密鑰
220
I/F
120
I/F
10B
資訊處理裝置
110B
113
資料轉換電路
112
密鑰生成部
111
硬體密鑰
100B
101
命令生成部
102
資料取得部
103
命令發佈檢測部
104
亂數生成部
105
控制暫存器部

圖6

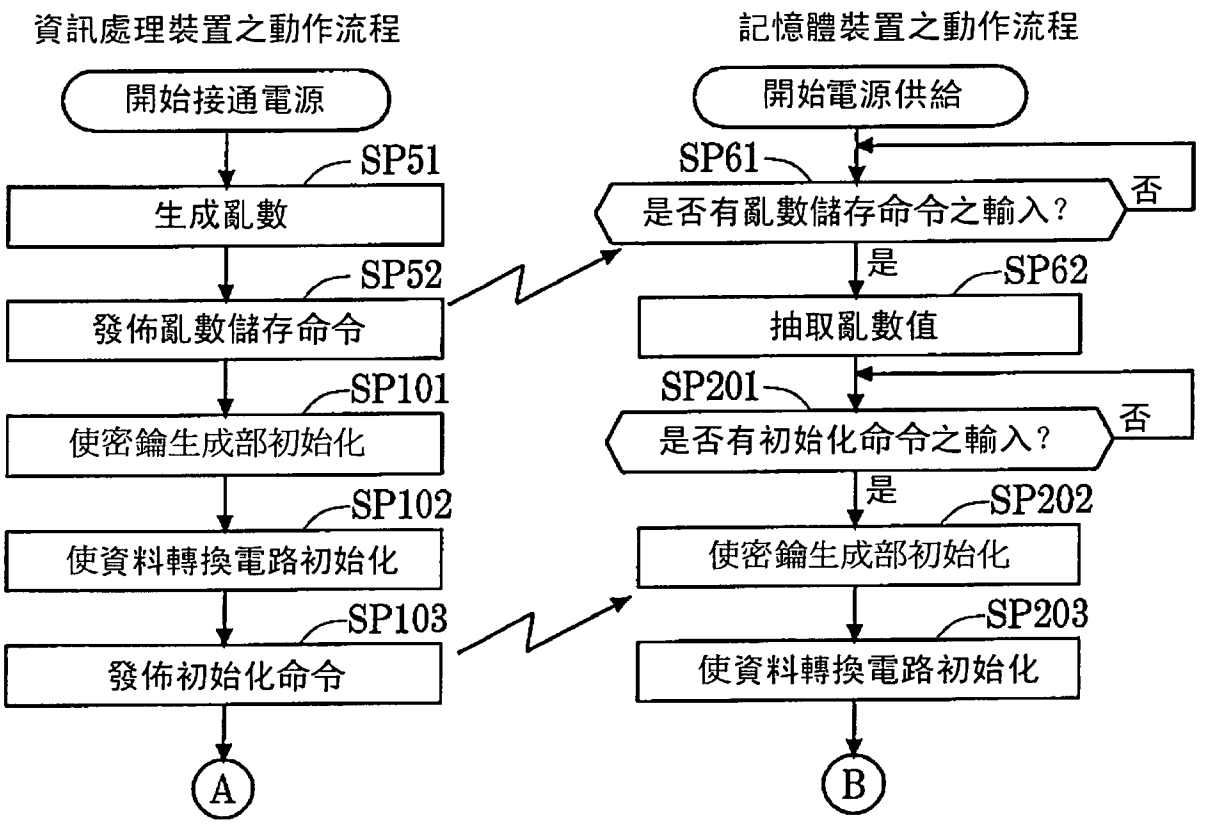
資訊處理裝置之動作流程
開始接通電源
SP51
生成亂數
SP52
發佈亂數儲存命令
SP101
使密鑰生成部初始化
SP102
使資料轉換電路初始化
SP103
發佈初始化命令
A
記憶體裝置之動作流程
開始電源供給
SP61
是否有亂數儲存命令之輸入？
否
是
SP62
抽取亂數值
SP201
是否有初始化命令之輸入？
否
是
SP202
使密鑰生成部初始化
SP203
使資料轉換電路初始化
B

圖7

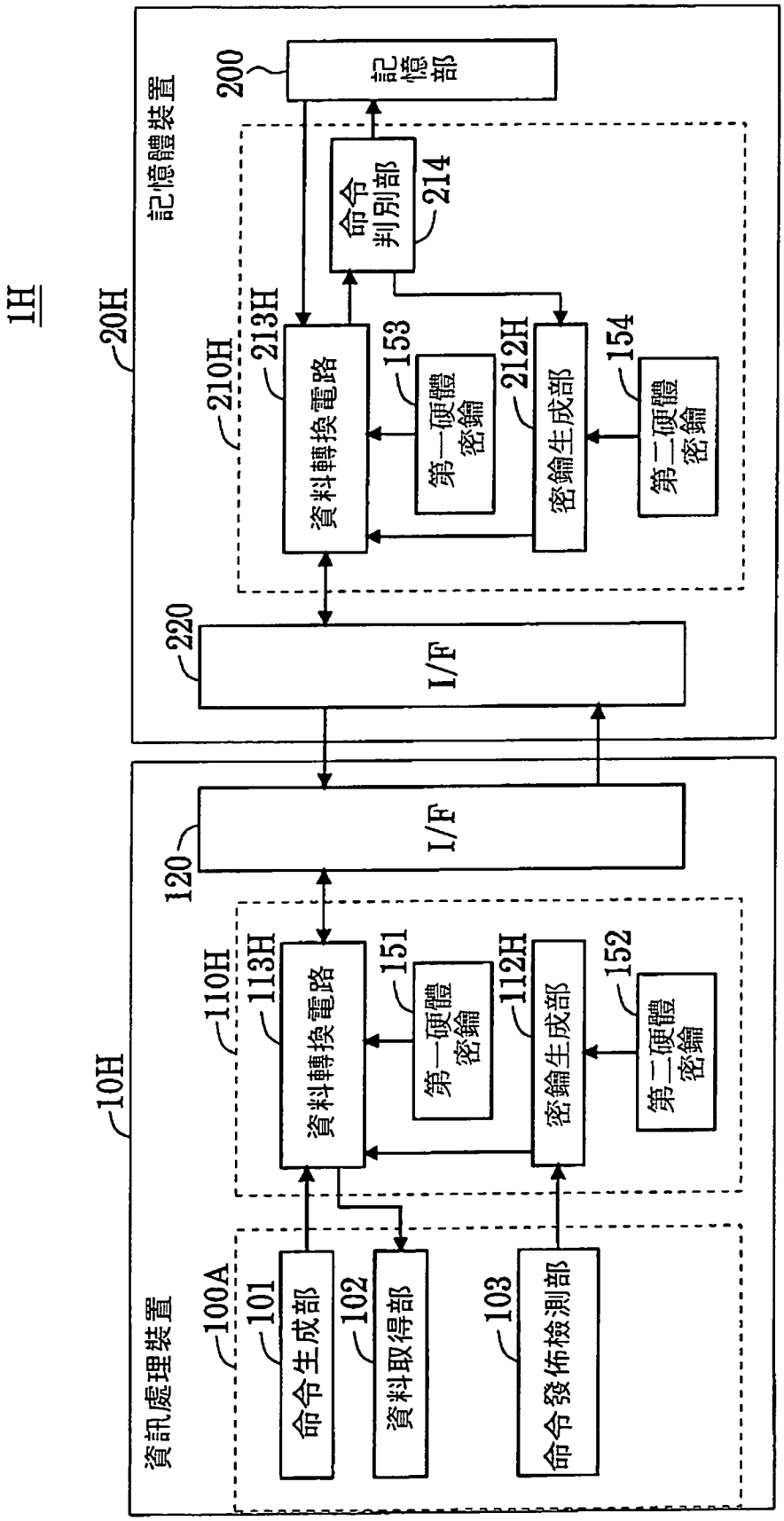
1H
10H
資訊處理裝置
100A
101
命令生成部
102
資料取得部
103
命令發佈檢測部
110H
113H
資料轉換電路
151
第一硬體密鑰
112H
密鑰生成部
152
第二硬體密鑰
120
I/F
20H
記憶體裝置
210H
213H
資料轉換電路
153
第一硬體密鑰
212H
密鑰生成部
154
第二硬體密鑰
220
I/F
200
記憶部
命令判別部
214

圖8