公告本

申請日期	89 10 27
案號	89122735
類別	G11B 20/00, G06F 1/00, 9/14

（以上各欄由本局填註）

A4
C4

556160

發明 專利說明書

一、發明名稱	中文	失效資訊更新方法與裝置、及儲存媒體
	英文	REVOCATION INFORMATION UPDATING METHOD, REVOCATION INFORMATION UPDATING APPARATUS AND STORAGE MEDIUM
二、發明人	姓名	(1)原田俊治 (4)廣田照人 (2)館林誠 (5)上林達 (3)小塚雅之 (6)田村正文
	國籍	日本
	住、居所	(1)日本國大阪市西成區玉出西2-20-52 (2)日本國寶塚市賣布1之16之21 (3)美國加州阿卡地亞市柯伊爾街501號 (4)日本國守口市梶町1-20-1-306 (5)日本國神奈川縣茅崎市本宿町3-18-108 (6)日本國東京都調布市調布丘1-18-76
三、申請人	姓名（名稱）	(1)日商・松下電器產業股份有限公司 (2)日商・東芝股份有限公司
	國籍	日本
	住、居所（事務所）	(1)日本國大阪府門真市大字門真1006番地 (2)日本國神奈川縣川崎市幸區堀川町72番地
	代表人姓名	(1)中村邦夫 (2)岡村正

裝 訂 線

（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

美　　國（地區）　申請專利，申請日期：1999,11,08　案號：09/436,035　，☑有　□無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（　）[1]

<發明之技術背景Background of the Invention>

1.發明之技術領域Field of the Invention

本發明係有關一種用以儲存數位內容如程式、數位化文字、音頻及影像的儲存媒體，以及有關一種能防止未經授權的電子裝置錄製或再製數位內容的更新失效資料方法。

2. 相關技藝之說明Description of the Related Art

近年來，數位及微處理器的進步已使得電子裝置朝著多樣性的方向發展。其中一個例子便是備有多媒體設備的個人電腦、轉頻器、再製裝置與遊戲控制台。除了自錄製媒體再製影像資料、音頻資料與其他的數位內容之外，電子裝置也能從網際網路上下載數位內容。

數位內容大都是以一種用MPEG2 (動畫壓縮標準2)或MPEG3 (動畫壓縮標準-音頻層3)技術數位編碼的著作權資料。這些資料能在不損及其品質的情況下在網路上被複製並傳送。這表示對發展防止侵害數位內容的著作權等不恰當動作的技術有著迫切的需求。

目前的電子裝置，如個人電腦、轉頻器、再製裝置等大多使用"可逆寫"的錄製媒體，該可逆寫的錄製媒體在此表示非相依參與者的錄製媒體。此種媒體根據公開規格運作。這使得使用者能任意地傳輸或複製數位內容到其他的媒體上，根本沒有有效的方法能保護已錄製在錄製媒體上的數位內容。

整合錄製媒體與控制器的記憶卡近來已出現在市場

五、發明說明（　）[2]

上。這種卡備置一種透過特殊程序利用控制器的存取控制功能才可進入的被保護區域(此後稱隱式區域)，否則使用者便無法進出。人們相信利用隱式區域儲存重要資料(如複製控制資料與傳輸控制資料)能更安全地保護數位內容。

以下將敘述一種能夠保護數位內容著作權的方法。當數位內容在上述任一電子裝置與一錄製媒體之間傳輸時，二種裝置都將首先進行互相鑑別的工作。這意味著每一裝置互相檢查對方是否為配備有相同著作權保護機制(即事先決定的內容保護功能)的裝置。當二方裝置的真實性確定後，它們根據雙方都備置的鑰匙碼產生演算法來交換鑰匙碼。二方裝置因而都取得鑑別鑰匙碼，並利用此鑑別鑰匙碼來個別加密並解密任一內容鑰匙碼(不同於用於加密數位內容的鑰匙碼)，或加密並解密數位內容本身。

上述技術有以下的問題。電子裝置中的內容保護機制(如用來互相鑑別的資料或程式)必須在電子裝置從工廠出貨前就先設定好。在消費者購買之後，電子裝置(或者更確定來說是運作電子裝置的程式)可能會受到干預，使得內容保護機制無法有效地運作。光靠互相鑑別的方法並無法檢測或停止該改良電子裝置，因此數位內容仍有可能不恰當地被使用。

藉著在錄製媒體上一特殊區域中事先錄製失效資料可能可以對數位內容提供較佳的保護。失效資料會顯示無效電子裝置應該被禁止存取儲存在錄製媒體上的內容。該失

五、發明說明（　）[3]

效資料能為無效電子裝置以識別資料表單的方式形成。當錄製媒體載入登錄在失效資料的一電子裝置中時，此電子裝置便被禁止進入錄製媒體。換言之，利用使電子裝置進入錄製媒體的權利無效的方法，錄製媒體上的內容得以被保護。

這方法有一個缺點，就是它仍必須在電子裝置從工廠出貨前，在一不可逆寫的區域中設定失效資料。這表示了一旦玩弄電子裝置(或電子裝置的程式)將導致在錄製媒體被製造後新型無效電子裝置的出現，該電子裝置便無法加諸至錄製媒體上的失效資料中。此種電子裝置的違法存取便無法被防止。

<發明之概要說明Summary of the Invention>

有鑑於上述問題，本發明的目的是對失效資料提供一儲存媒體，即使是未經授權電子裝置出現於儲存媒體已經被製造之後，也能防止一未經授權電子裝置進入數位內容。本發明的目標同時也提供了一種適合於儲存媒體的失效資料更新裝置與方法。

上述目的藉由一已安裝入電子裝置的儲存媒體而達成，此儲存媒體包含了，一用以儲存數位內容的內容儲存區；一用以儲存對應於電子裝置的識別資料的資料的失效資料儲存區，該識別資料防止存取儲存於內容儲存區中的數位內容；一用以儲存對應於一電子裝置的識別資料的資料的主失效資料儲存區，該識別資料防止更新儲存於失效

五、發明說明（　）[4]

資料儲存區中的失效資料。

根據以上的構造，應該不可更新失效資料的對應於未經授權電子裝置的識別資料的資料，必須事先在儲存媒體的主失效資料儲存區中登錄。藉由提及此資料，儲存媒體能知道嘗試著進入失效資料的電子裝置是一授權的電子裝置或是一未經授權的電子裝置。

該失效資料儲存於一安全而可逆寫的儲存區，即便當一未經授權的電子裝置在儲存媒體已被製造後才出現，對應於該未經授權電子裝置的識別資料的資料也能另登錄於失效資料儲存區。如此一來，可以防止未經授權的電子裝置存取儲存在儲存媒體中的數位產品。

在這，儲存媒體可另包含：一用以執行第一判斷的內容保護部件，它判斷已安裝儲存媒體的一電子裝置是否擁有對應儲存於失效資料儲存區的失效資料的鑑別資料，當第一判斷的結果呈否定時，該內容保護部件允許電子裝置進入儲存在內容儲存資料區的數位內容；一用以執行第二判斷的失效資料更新部件，它判斷已安裝儲存媒體的一電子裝置是否擁有對應儲存於主失效資料儲存區的主失效資料的鑑別資料，當第二判斷結果呈否定時，該更新部件允許電子裝置更新儲存在失效資料儲存資料區的失效資料。

根據以上的構造，只有擁有不對應於主失效資料儲存區的鑑別資料的電子裝置，才能更新儲存在儲存媒體上的失效資料。這表示能防止未經授權的電子裝置玩弄失效資料。

五、發明說明（　）5

在這，主失效資料儲存區可備置在ROM(唯讀記憶體)中，其中主失效資料已事先被儲存。

它能在製造儲存媒體後，保護儲存媒體免於被主失效資料的攻擊玩弄。

在這，儲存媒體可另包含：一用以在失效資料更新部件執行第二判斷前，利用已安裝儲存媒體的一電子裝置執行互相鑑別的互相鑑別部件，並且當互相鑑別成功時，該互相鑑別部件也製造一能與電子裝置共享的私密鑰匙碼，其中，失效資料更新部件利用以互相鑑別部件製造的私密鑰匙碼更新失效資料。

根據以上的構造，關於何種裝置有更新失效資料的權限的決定性鑑別資料被安全地轉移到儲存媒體與一電子裝置之間。這增加了保護失效資料的安全性。

在這，唯有當第二判斷結果呈否定時，失效資料更新部件可傳送電子裝置必須更新失效資料的一私密鑰匙碼到電子裝置。

因此，判斷一電子裝置是否有權限更新失效資料的結果是保密的。這可以阻撓第三者試著攔截儲存媒體與一電子裝置之間的通訊。

在這，失效資料可分類成數個群組，而失效資料儲存區可包含多個儲存區，而每個群組被儲存在不同的儲存區中，而失效資料更新部件可判斷以下情況做為第二判斷：(1)安裝了儲存媒體的電子裝置是否擁有不對應於儲存於主失效資料儲存區域的主失效資料的識別資料；及(2)該

五、發明說明（　）[6]

電子裝置是否擁有不對應於電子裝置希望更新的失效資料的特定組群中的識別資料。只有在當(1)與(2)都是肯定的答案時，第二判斷才是否定的，而失效資料更新部件只允許電子裝置更新特定群組中的失效資料。

因此，即使當一未經授權第三者想玩弄失效資料，損害也可控制在失效資料的一個群組中。失效資料的其他群組則不會受到影響。

前述的發明目的也能藉由在儲存媒體上更新失效資料的方法達成。此方法包含：一用以檢測儲存媒體是否已安裝到電子裝置的的檢測步驟；一用以執行第一判斷對電子裝置的第一鑑別是否不對應於儲存於儲存媒體的主失效資料儲存區的主失效資料的判斷步驟；以及，只有在第一判斷的結果是肯定時，用以更新儲存於失效資料儲存區的失效資料的更新步驟。

前述的發明目的也能藉由用以更新儲存媒體上失效資料的一失效資料更新裝置達成。該裝置包含：一用以儲存第一鑑別資料的第一鑑別資料儲存部件，該第一鑑別資料不對應於儲存於儲存媒體的主失效資料儲存區域的主限制區；一用以取得與使用對應於儲存在第一鑑別資料儲存方法之第一鑑別資料的許可取得部件，從儲存媒體取得更新儲存於儲存媒體上的失效資料的許可；以及根據自許可取得部件取得許可，用以更新儲存於儲存媒體上的失效資料的更新部件。

五、發明說明（　）[7]

<圖示的簡要說明Brief Description of the Drawings>

本發明的以上及其他目的、優點及特徵將在以下的敘述、所附的圖示及具體施實例更明顯地顯現出來。

第1圖顯示本發明中一個實施例中著作權保護系統的完整構造；

第2圖為一個內容分散系統(CDS)的構造的方塊圖；

第3圖為一個錄製媒體(PM)的構造的方塊圖；

第4圖顯示一PM中開放ROM區域的錄製內容與構成；

第5圖顯示CDS的邏輯儲存區域；

第6圖為一錄製/回放裝置(可攜式裝置PD)的構造的方塊圖；

第7圖顯示PD的邏輯儲存區域；

第8圖為一內容使用管理系統(特許依從模組LCM)的構造的方塊圖；

第9圖顯示LCM的邏輯儲存區域；

第10圖顯示介於CDS、PM與處理流程間往來的前段部分；

第11圖顯示介於CDS、PM與處理流程間往來的後段部分；以及

第12圖顯示介於CDS、PM與處理流程間的往來。

<較佳實施例的說明 Description of the Preferred Embodiments>

以下將對照附圖詳述本發明的實施例。

五、發明說明（　）[8]

第1圖顯示根據本實施例的著作權保護系統100的構造。

著作權保護系統100保護數位資料的著作權，該數位資料的著作權被電子性的分散或經由錄製媒體使用。如第1所示，著作權保護系統100包含：一以販賣機的形式經由網際網路電子性分散音樂內容的內容分散系統1(CDS)、一用以儲存音樂內容的的錄製媒體13(以下稱可攜式媒體PM13)、一在錄製音樂內容到PM13與從PM13回放音樂內容的可攜式錄製/回放裝置12(以下稱可攜式裝置PD)、以及一管理錄製、回放及傳輸音樂內容的內容使用控制系統21(以下稱特許依從模組LCM)。

CD1、PM13與PD12配備了一個上述能更新失效資料的功能或構造，即使在CD1、PM13與PD12已被製造後，才發現未經授權電器的存在，也能防止未經授權電子裝置不適當地進入數位產品。

第2圖為一顯示CD1構造的一方塊圖。架構40呈現一電子音樂分配器(EMD)，如一音樂伺服器或廣播站。架構41呈現一失效資料特許實體(RLE)。當剛發現一未經授權電子裝置時，RLE41為此電子裝置核發包括鑑別資料的新失效資料。

CDS1能藉由一專業的終端機(如配電亭終端機)施行，並能在一錄製商店找到。此CDS1經由傳輸路徑連接到EMD40與RLE41，同時包含一保全音樂伺服器2(SMS2)、一EMD_I/F(介面)部件3、一PD_I/F部件5、一媒體_I/F部

五、發明說明（　）[9]

件6、一隱式區域驅動器7、一登錄儲存部件8、一特許儲存部件9、一音樂數據儲存部件10、一失效資料接收部件14、一使用者I/F部件15、以及一失效資料儲存部件16。

CDS1的功能如下。

(1) 功能錄製（購買）功能 Contents Recording (Purchasing) Function

CDS1在PM13上錄製使用者所要的內容並載入CDS1中。這與使用者購買內容相對應。

(2) 失效資料更新功能 Revocation Information Updating Function

CDS1在PM13上更新失效資料並載入CDS1中。此失效資料顯示了何項電子裝置應該被取消。

EMD_I/F部件3為一連結CDS1與數個EMD40的通信配接器。PD_I/F部件5為一連結PD12與CDS1的通用串列匯流排(UBS)。媒體_I/F部件6為載入PM13至CDS1的PCMCIA(個人電腦記憶卡國際協會)卡擴充槽。失效資料接收部件14為一通信配接器，其接收即將登錄的失效資料。使用者I/F部件15包括液晶顯示器(LCD)、開關、鈕扣式鑰匙碼等。音樂數據儲存部件10為一儲存加密音樂內容的快閃記憶體。登錄儲存部件8是在音樂數據儲存部件10中儲存音樂內容的儲存屬性資料的記憶體。

特許儲存部件9為一儲存鑰匙碼或其他資料的記憶體，其使用在解密儲存在音樂數據儲存部件10中的加密音樂內容。失效資料儲存部件16為一記憶體，其暫時儲存失

五、發明說明（　）

效資料，如從RLE41接收的失效資料。

隱式區域驅動器7為一控制電路，其利用一部未開放的隱密程序進入登錄儲存部件8中的受保護儲存區域(以下將詳述)。SMS2為一中央處理器(CPU)，其執行處理控制其他組件，進以達成以上所述的二項功能。

上述(1)與(2)所賦予的CDS1組件功能與SMS2控制功能將在以下分開詳述。

(1)功能錄製(購買)功能 Contents Recording (Purchasing) Function

在CDS1中，利用每一個錄製媒體(PM13)的鑑別資料加密與解密內容能保護內容免於被未授權的使用。

CDS1包含三個接收部件#1~#3，其與EMD40#1~#3互相對應。由三個EMD分配的加密內容(即音樂內容)與特許資料(使用情況、加密內容與解密鑰匙碼等)，藉由對應的接收部件#1~#3接收。利用不同的加密方法與不同的音頻編碼方法能製造EMD40分配的加密內容。每一個接收部件#1~#3也具備回放已接收音頻的功能與向使用者收費的功能。此收費功能使得使用者能購買想要的內容。

SMS2透過EMD_I/F部件3接收使用者購買的已加密內容。必要時，EMD_I/F部件3解密已加密內容，該已加密內容被不同的EMD以音頻編碼及加密方法加密，EMD_I/F部件3同時也利用一音頻編碼格式與加密格式傳送(再加密)內容，該內容曾被CDS1利用。

在接收到一加密內容時，SMS2在音樂數據儲存部件10

五、發明說明（　）[11]

中儲存加密內容，並同時儲存一用以在特許儲存部件9中解密已加密內容的鑰匙碼(加密內容解密鑰匙碼)。SMS2可備置一回放功能以允許使用者聆聽一已被分散的音樂內容。在這樣的情況下，由SMS2所管理的音樂內容可能在CDS1上被重新製造。

SMS2備置一項功能，其透過媒體_I/F部件6，輸出儲存在將音樂數據儲存部件10中的加密內容(音樂內容)到PM13，如記憶卡，該記憶卡被載入媒體_I/F部件6中。

藉由在PD12中設立PM13，使用者能將PD12所解密並回放的加密內容(音樂內容)錄製到PM13上。SMS12能直接地透過媒體_I/F部件6或間接地透過PD12在PM13上錄製內容。

使用者也能在LCM21中設立PM13。LCM13解密並回放已錄製在PM13上的加密(音樂)內容。或者，使用者能將PM13上的加密(音樂)內容傳輸到LCM21上，以便之後在LCM21上儲存。

(2) 失效資料更新功能 Revocation Information Updating Function

此失效資料用來鑑別電子裝置(如PD與LCM)，該電子裝置(如PD與LCM)應該被取消使用PM13的資格，以便保護PM13上的內容。在此，"使用PM13"表示錄製內容到PM13上或是讀取或回放內容錄製在PM13上的內容。此失效資料在製造過程中已事先錄製在PM13上。

一電子裝置執行失效資料更新功能，該電子裝置有特

五、發明說明（　）[12]

殊的許可(如本例中的CD1)。必要時，此功能利用新的失效資料更新在製造過程中就已經錄製在PM13的失效資料。此失效資料在發現新的未經授權電子裝置並必須使其無效時，需要被更新。

CD1配備了失效資料接收部件14，該部件能從RLE41接收新的失效資料。加密從RLE41傳輸到CD1的新失效資料，能避免玩弄二裝置之間的傳輸路徑。例如，可利用RLE41與CD1事先共享的加密鑰匙碼來加密。

SM2透過失效資料接收部件14接收由RLE41核發的已加密新失效資料。該SM2解密該已加密新失效資料，並在失效資料儲存部件16中儲存所得的新失效資料。當一PM13 ，如一記憶卡，被載入媒體_I/F部件6(即在媒體_I/F部件6檢測到PM13已被插入時)，SMS2所備置的功能透過媒體_I/F部件6輸出失效資料儲存部件16中的失效資料到PM13。該SMS2能直接透過媒體_I/F部件6或間接透過PD12在PM13上錄製新的失效資料。

以下將敘述各種不同的失效資料。要注意的是，錄製媒體(此為PM13)不限於儲存數位化音樂，並且也能被另用來作為錄製一應用系統，即所謂的"電子書"。這樣一來，失效資料為每個應用系統核發的。因此，電子裝置能分別地為了各個應用系統而被取消，只有備有特殊許可的電子裝置能為一特定的應用系統被准許更新對應於該應用系統的更新失效資料。在此例中，CD1只能為主管數位化音樂的電子裝置(如PD與LCM)更新失效資料。

五、發明說明（　）[13]

以這樣的配置，即使一位使用者玩弄CD1的失效資料更新功能，也不會影響其他應用系統，因為使用者仍將無法更新其他應用系統中的失效資料。

同時，要取消一有特殊許可的電子裝置(如CD1)，該電子裝置有著特殊許可，能利用登錄在PM13上的特殊失效資料(以下稱主失效資料)的來更新失效資料。換句話說，顯示特殊電子裝置有特殊許可以更新失效資料的的主失效資料，也能被引導入著作權保護系統，作為一未經授權電子裝置的黑名單，而能另外改變失效資料。

例如，假設改變了一特定CDS1的失效資料更新功能，以允許未經授權的使用。鑑別此種CDS1的資料可以被加諸在主失效資料中，以防止已修正的CDS1進入失效資料。這便可能防止未經授權者玩弄失效資料。

在本實例中，要注意的是，假設利用不同於本發明所揭示的方法來更新主失效資料。利用另外核發的一錄有新主失效資料的錄製媒體以更新主失效資料，並利用該錄製媒體以取代錄有舊主失效資料的舊錄製媒體。

第2圖為一個顯示PD12構造的方塊圖。這是一個可以錄製及回放的裝置。

第3圖為一個顯示PM13構造的功能性方塊圖。從此圖中可看出，該PM13包含一控制器130，以及由一開放區域131與一隱式區域134所構成的錄製媒體部分。

此隱式區域134為一邏輯儲存區，唯有利用一私密程序藉由控制器130才能進入該邏輯儲存區。該隱式區域134

五、發明說明（　）[14]

用來儲存解密時所需要的資料。如第3圖所示，隱式區域134由一儲存著秘密常數的隱式ROM區域135(如以下將敘述的獨特主媒體鑰匙碼KM-M)與儲存著私密變數的隱式可逆寫RW區域136(如以下將敘述的特許可者提供的特許解密鑰匙碼、一已加密的的內容解密鑰匙碼、與一獨特媒體鑰匙碼KM-1)所組成。此已被加密的內容解密鑰匙碼(以下稱加密內容鑰匙碼)是利用加密內容鑰匙碼KC產生的，該內容鑰匙碼KC則利用對PM13獨特的獨特媒體鑰匙碼KM-1來解密內容C。

此獨特主媒體鑰匙碼KM-M與獨特媒體鑰匙碼KM-1必須為每個PM13被設定在不同的數值上，如此才有可能為每個PM13使用不同的鑑別資料，如一序號或一產品編號(每個PM13的產品編號或生產抽籤號)。然而，KM-M與KM-1可另從PM13的獨特鑑別資料與特許解密鑰匙碼製造。舉例來說，隱式ROM區域135可實體地備置在ROM中(即唯讀非依電性記憶體)，而隱式RW區域136可備置在一快閃記憶體中(即可逆寫非依電性記憶體)。

開放區域131與隱式區域分開，且祇能被傳統的程序進入。此開放區域131包括一唯讀開放區域132(以下稱開放ROM區域)與一可逆寫開放區域133(以下稱開放RM區域)。如第4圖所示，假設開放ROM區域132同時也包含一僅能根據私密程序被寫入的區域(以下稱開放ROM-W區域132a)。

第4圖顯示PM13中開放ROM區域132及其儲存內容的

五、發明說明（　）[15]

組成。舉例來說，該開放ROM區域132能實體地備置在ROM中，例如，開放RW區域133與開放ROM-W區域132a能實體地備置在一快閃記憶體中。該開放ROM區域132、開放RW區域133、與開放ROM-W區域132a能個別地備置在同一ROM中作為隱式ROM區域315，並且在同一快閃記憶體中作為隱式RW區域136。

主失效資料(RL-M)是在PM13從工廠出貨前，事先就登錄在開放ROM區域132(以下意指開放ROM區域132的部分，但不是開放ROM-W區域132a)。一組或多組的失效資料(RL-1, RL-2.....)從工廠出貨前，也事先就登錄在開放ROM-W區域132a中。利用執行CD1的失消資料更新功能可替代(更新)該多組的失效資料，並能根據一私密程序藉由PM13的控制器130將新的失效資料寫入開放ROM-W區域132a。要注意的是，不需根據本發明所揭示的方法而更新的一組或多組失效資料，也必須事先登錄在開放ROM區域132中。

在本實施例中，主失效資料與一組或多組的失效資料便是必須被取消的電子裝置鑑別資料(64位元的裝置ID)的表單。因此，在以下的解釋中，每組的失效資料即為"失效表單RL"。主失效資料即為"RL-1"與"RL-2"等。在本例中，失效表單RL-1用來取消錄製或回放數位化音樂的電子裝置(如PD或LCM)。

已被加密的內容(以下簡稱為加密內容)與其他數據則必須儲存在開放RW區域133。這些內容以內容鑰匙碼(KC)

五、發明說明（　）[16]

加密。

第5圖顯示CDS1的邏輯儲存區域。CDS1有一開放區域111，其由開放ROM區域112與開放RW區域113組成，以及一個僅能根據私密鑰匙碼進入的隱式區域114。顯示在第2圖的音樂數據儲存部件10備置在開放RW區域113中。該開放ROM區域112包含一開放ROM-W區域(未顯示)，第2圖中所示的失效資料儲存部件16便備置在開放ROM-W區域中。在此實施例中，第2圖中所示的SMS2解密從接收自RLE41的加密的新失效資料，並利用一私密程序在該開放ROM-W上儲存該已解密新失效資料。

鑑別資料(裝置ID)ID_CDS被事先儲存在隱式區域114中。每個內容的內容鑰匙碼(KC)也同樣必要地儲存在隱式區域114中。隱式區域114同時備置了如第2圖所示的登錄儲存部件8。所有儲存在音樂數據儲存部件10(開放RW區域113)中且用SMS2管理的音樂內容，都有一內容ID(TID)與其它相同的鑑別資料作為它的屬性。此屬性資料被稱為”登錄”，且被儲存在登錄儲存部件8中(備置在隱式區域114中)。

CDS1有一隱式區域驅動器7，其執行一特殊的私密程序以使SMS2能進入隱式區域114中的登錄儲存部件8，並隨後從登錄儲存部件8讀取數據。要注意的是，該登錄與本發明應無直接相關性，因此它的用途並未詳述。

PD12包含一開放區域121，其由開放ROM區域122與開放RW區域123所組成，以及一個僅能用私密程序進入

五、發明說明（　）[17]

的隱式區域124。PD12的鑑別資料ID_PD永久地登錄在隱式區域124 。每個內容中的內容鑰匙碼KC也都儲存在隱式區域124中。

第6圖為顯示PD12的方塊圖。第7圖顯示PD中的邏輯儲存區域。

PD12為一半導體音頻回放裝置或類似之裝置。如第6圖所示，PD12的硬體結構包含了一個中央處理器CPU12a、一個隨機快取記憶體RAM12b、一個唯讀記憶體ROM12c、一個快閃記憶體12d、一個外部用品I/F部件12e、一個媒體I/F部件12f、一個用以解密加密的音樂內容或其他相關內容的解調部件12g、一個解碼器部件12h與一個用以解碼及處理壓縮音頻內容的D/A變頻器部件12i。如第7圖所示，PD12備置了一開放區域132與一隱式區域124。

如第6圖所示，PM13被使用在PD12的媒體I/F部件12f上。當CDS1透過PD12讀寫數據時，備置在CDS1中的PD I/F部件5透過PD12的外部用品I/F部件12e與媒體I/F部件12f進入PM13中的隱式區域134(詳見第3圖)。

該媒體I/F部件12f有一隱式區域存取部件(未標示)，用以進入PM13中的隱式區域134。例如，PD12的開放RW區域123與隱式區域124備置於一快閃記憶體。一個能用PM13施行相互鑑別的程式便寫入ROM12c中。在CPU12a的控制下，PD12與此程式一同運作，用PM13施行相互鑑別。

第8圖為顯示LCM21構造的方塊圖。LCM21實施於個人電腦，有著更新失效資料的特殊功能，基本上與CDS1

五、發明說明（　）[18]

有著相同的結構。換句話說，LCM21包含一SMS22、一EMD_I/F部件23、一PD_I/F部件25、一媒體I/F部件26、一隱式區域驅動器27、一登錄儲存部件28、一特許儲存部件29、一音樂數據儲存部件30、一CD_I/F部件31以及一使用者I/F部件35。與CDS1相同，LCM21有以下的功能。LCM21能自一EMD40接收一加密內容，並儲存該內容於LCM21中。該LCM21能將儲存於LCM21的一加密內容錄製到PM13上，或能從PM13上讀取一音樂內容，隨後便在LCM21中儲存內容。

第9圖顯示備置於LCM21中的邏輯儲存區域。與PM13、CDS1、PD12相同，LCM21備置了一開放區域211，該開放區域由一開放ROM區域122與一開放RW區域213組成，也備置了一僅能用特殊程序進入的隱式區域214。LCM21的鑑別資料ID_LCM事先被儲存在隱式區域214中，且不能改變。此隱式區域214也必要地為每一內容儲存了一內容鑰匙碼KC。

PM13用來載入LCM21中的媒體I/F部件26中。當從PM13讀取數據或寫入數據至PM13時，PM13的隱式區域134便被LCM21透過其中的媒體I/F部件26進入。此媒體I/F部件26包含一個用以進入PM13中隱式區域134的隱式區域讀取部件(未顯示)。例如，LCM21的開放RW區域213與隱式區域214可以被備置在一快閃記憶體中。

此開放ROM區域212備置在一個唯讀記憶體ROM中。一個能在PM13中施行相互鑑別的程式被寫入該ROM中。

五、發明說明（　）[19]

在中央處理器CPU(未顯示)的控制下，LCM21與此程式一同運作，與PM13施行相互鑑別。

本實施例的著作權保護系統100將於以下敘述。在本例中，使用者將PM13插入CDS13中，並選擇一由EMD40錄製音樂內容到PM13的過程。這與使用者購買音樂內容的動作相對應。在此例中，同時，由RLE核發並事先儲存在CDS1中的新失效資料隨著音樂內容一同錄製在PM13上。

第10與11圖個別地顯示介於CDS1、PM13與處理流程間往來的前後部分。舉例來說，當使用者透過CDS1的使用者I/F部件15表示有購買音樂內容的意圖而PM13已被載入媒體I/F部件6時，CDS1的媒體I/F部件6能與PM13(步驟S101)的控制器130施行相互鑑別(又叫做主要的識別與鑰匙碼交換AKE-M)。以下CDS1與PM13將施行此AKE-M程序。

首先，CDS1確認PM13的身分。一被允許更新失效資料的CDS1備置了一鑑別鑰匙碼K1-M，也就如同PM13(這些未顯示出來的鑰匙碼儲存在隱式區域ROM中)。CDS1製造一隨機數R1並將它傳送至PM13。當收到由CDS1所製造的隨機數R1時，PM13利用鑑別鑰匙碼K1-M加密此隨機數R1，並將所得的加密隨機數R1(K1-M[R1])傳送至CDS1。CDS1利用鑑別鑰匙碼K1-M來解密K1-M[R1])，並且，如果結果與隨機數R1相等時，它便判定PM13為一適當裝置。

五、發明說明（　）[20]

此後，PM13為CD S1施行相同的過程以完成互相鑑別的工作。為了完成該工作，CDS1與PM13都有一鑑別鑰匙碼K2-M，CDS1利用該鑑別鑰匙碼K2-M加密自PM13接收的隨機數R2，且PM13解密並確認所得結果等於隨機數R2。

在本例中，鑑別鑰匙碼K1-M與K2-M只提供給一特別的電子裝置(在此為CDS1)，該電子裝置允許更新失效資料，因此普通的電子裝置(如LCM21)便禁止執行鑑別過程AKE-M。

在上述步驟S101的互相鑑別過程中，當CDS1與PM13都發現彼此為適當裝置時，CDS1的媒體I/F部件6與PM13的控制器130交換鑰匙碼以共享相同的對話鑰匙碼(KY1)。例如，該對話鑰匙碼(KY1)成為一數值，其為了在互相鑑定過程製造的隨機數R1與R2的邏輯XOR所發現，隨後並將結果輸出至事先備置在CDS1與PM13中的一私密鑰匙碼製造演算法中。如此一來，對話鑰匙碼KY1則為一個時變鑰匙碼，其數值隨每一對話而改變。

CDS1的媒體I/F部件6為CDS1讀取隱密地儲存在隱式區域114中的主鑑別資料ID-M、利用對話鑰匙碼KY-1加密該資料ID-M、並傳送所得加密ID-M到PM13(步驟S102)。

PM13的控制器130利用對話鑰匙碼(KY1)解密自CDS1接收的KY1[ID-M]，該對話鑰匙碼(KY1)在前導鑰匙碼交換過程中接收，以取得ID-M(步驟S103)。

隨後，PM13的控制器130使用已解密的CDS1的主鑑別

五、發明說明（　）[21]

資料ID-M參照對開放ROM區域132的主失效表單RL-M。控制器130藉著檢查是否有符合ID-M的鑑別資料存在於主失效資料表單RL-M中，來判斷CDS1是否應該禁止使用PM13(步驟S104)。

如果符合主失效資料表單RL-M的ID-M的鑑別資料存在的話，控制器130利用CDS1取消PM13的使用權，並在此時結束執行。

另一方面而言，如果符合主失效資料表單RL-M的ID-M的鑑別資料並不存在的話，控制器130判定CDS1可使用PM13(及更新失效資料)，且讀取並輸出秘密儲存在隱式ROM區域135的獨特媒體鑰匙碼KM-M(步驟S105)。控制器130隨後與CDS1的媒體I/F部件6交換鑰匙碼，以共享相同的對話鑰匙碼KY-2，並在利用該對話鑰匙碼KY-2加密已讀取的獨特主媒體鑰匙碼KM-M之前，傳送所得已加密鑰匙碼KM-M(=KY2[KM-M])到CDS1(步驟S106)。

例如，當前述對話鑰匙碼KY-1輸入至事先備置在CDS1與PM13的一私密鑰匙碼產生演算法中時，所得到的結果為該對話鑰匙碼KY-2。

CDS1的媒體I/F部件6利用對話鑰匙碼(KY2)解密自PM13接收的KY2[KM-M]，該對話鑰匙碼(KY1)在前導鑰匙碼交換過程中接收，並因此取得獨特主媒體鑰匙碼KM-M(步驟S107)。

隨後，CDS1的媒體I/F部件6加密儲存在開放ROM-W區域與新獨特媒體鑰匙碼KM-1N的新失效資料表單RL-

五、發明說明（　）[22]

1，該開放ROM-W區域與新獨特媒體鑰匙碼KM-1N利用獨特主媒體鑰匙碼KM-M由媒體I/F部件6製造，CDS1的媒體I/F部件6並傳送所得加密KM-M[RL-1]與KM-M[KM-1N]到PM13(步驟S108)。

例如，此處參照的獨特媒體鑰匙碼KM-1N能做為輸出數值，其由在前述的對話鑰匙碼KY2輸入至一秘密儲存在CDS1的鑰匙碼產生演算法中製造。

PM13的控制器130利用儲存在隱式ROM區域135的KM-M解密自CDS1接收的KM-M[RL-1與KM-M[KM-1N]，並因此取得RL-1與KM-1N(步驟S109)。

隨後，CDS1的媒體I/F部件6與PM13的控制器130對上述的相互鑑別(AKE-M)施行相似的互相鑑別(AKE-1)(步驟S110)。

如此一來，CDS1首先鑑別PM13。為了要如此，CDS1與PM13都儲存相同的鑑別鑰匙碼K1-1(並未顯示，儲存在個別的隱式ROM區域中)。CDS1製造一隨機數R3並將它傳送至PM13。當收到由CDS1所製造的隨機數R3時，PM13利用鑑別鑰匙碼K1-1加密此隨機數R3，並將所得的加密隨機數(K1-1[R3])傳送至CDS1。CDS1利用鑑別鑰匙碼K1-1來解密K1-1[R3])，並且，如果結果與先前製造的隨機數R3相等的話，它便判定PM13為一適當裝置。

此後，PM13為CDS1施行相同的過程以完成互相鑑別的工作。為了完成該工作，CDS1與PM13都有一鑑別鑰匙碼K2-1，CDS1利用該鑑別鑰匙碼K2-1加密自PM13接收的

五、發明說明（　）[23]

隨機數R4，且PM13解密並確認所得結果等於隨機數R4。這些鑑別鑰匙碼K1-1與K2-1只備置於電子裝置(如PD12與LCM16)中，該電子裝置允許使用音樂內容，因此可防止對應於其他應用系統的電子裝置執行鑑別過程AKE-1。

在上述步驟S110的互相鑑別過程中AKE-1，當CDS1與PM13都發現彼此為適當裝置時，CDS1的媒體I/F部件6與PM13的控制器130施行鑰匙碼交換，以共享相同的對話鑰匙碼(KX1)。例如，該對話鑰匙碼(KX1)為一數值，其為了在互相鑑定過程製造的隨機數R3與R4的邏輯XOR所發現，隨後並將結果輸出至事先備置在CDS1與PM13中的一私密鑰匙碼製造演算法。如此一來，對話鑰匙碼KX1則為一個時變鑰匙碼，其數值隨每一時間而改變。

CDS1的媒體I/F部件6為CDS1讀取隱密地儲存在隱式區域114中的主鑑別資料ID-1、利用對話鑰匙碼KX-1加密該資料ID-1、並傳送所得加密ID-1(=KX1[ID-1])到PM13(步驟S111)。

PM13的控制器130利用對話鑰匙碼(KX1)解密自CDS1接收的KX1[ID-1]，該對話鑰匙碼(KX1)在前導鑰匙碼交換過程中接收，並因此取得ID-1(步驟S112)。

隨後，PM13的控制器130使用已解密的CDS1的主鑑別資料ID-1參照對開放ROM區域132的主失效表單RL-1。控制器130藉著檢查是否有符合ID-1的鑑別資料存在於主失效資料表單RL-1中，來判斷CDS1是否應該禁止使用PM13(步驟S113)。

五、發明說明（　）[24]

如果符合主失效資料表單RL-1的ID-1的鑑別資料存在的話，控制器130利用CDS1取消PM13的使用權，並在此時結束執行。

另一方面而言，如果符合主失效資料表單RL-1的ID-1的鑑別資料不存在的話，控制器130判定CDS1可使用PM13(即錄製一內容)，並利用自步驟S109收到的新失效資料RL-1N與新獨特媒體鑰匙碼KM-1N，來更新RL-1與KM-1(步驟S114)。

控制器130隨後與CDS1的媒體I/F部件6交換鑰匙碼，以共享相同的對話鑰匙碼KX-2，並在從CDS1的隱式區域114讀取鑑別資料ID-1之前，傳送所得ID-1(=KX2[ID-1])到PM13(步驟S115)。例如，當對話鑰匙碼KX-1輸入至事先備置在CDS1與PM13的一私密鑰匙碼產生演算法中時，所得到的數值便為該對話鑰匙碼KX-2。

PM13的控制器130利用對話鑰匙碼(KX2)解密自CDS1接收的KX-2[ID-1]，該對話鑰匙碼(KX2)在前導鑰匙碼交換過程中接收，並因此取得獨特ID-1(步驟S116)。

隨後，PM13的控制器130使用已解密的CDS1的解密鑑別資料參照對開放ROM區域的新失效表單RL-1N，並根據是否有符合ID-1的鑑別資料存在於失效資料表單RL-1，來判斷是否應該阻止CDS1使用PM13(步驟S117)。

如果符合ID-M的鑑別資料存在於主失效資料表單RL-1N的話，控制器130判斷CDS1應禁止使用PM13，並在此時結束執行。

五、發明說明（　）[25]

另一方面而言，符合ID-M的鑑別資料不存在於主失效資料表單RL-1N的話，控制器130判定CDS1可使用PM13(即錄製一內容)，並讀取且輸出秘密儲存在隱式ROM區域135的獨特媒體鑰匙碼KM-1N(步驟S118)。控制器130隨後與CDS1的媒體I/F部件6交換鑰匙碼，以共享相同的對話鑰匙碼KX-3，並在利用該對話鑰匙碼KX-3加密已讀取的獨特主媒體鑰匙碼KM-1N之前，傳送所得已加密鑰匙碼KM-1N(=KX3[KM-1N])到CDS1(步驟S119)。例如，當前述對話鑰匙碼KX2輸入至事先備置在CDS1與PM13的一私密鑰匙碼產生演算法中時，所得到的結果為該對話鑰匙碼KX3。

CDS1的媒體I/F部件6利用對話鑰匙碼(KX2)解密自PM13接收的KX3[KM-1N]，該對話鑰匙碼(KX3)在前導鑰匙碼交換過程中接收，並因此取得獨特主媒體鑰匙碼KM-1N(步驟S120)。

隨後，CDS1的媒體I/F部件6使用獨特媒體鑰匙碼KM-1N來加密秘密儲存在隱式區域114的內容鑰匙碼KC，並傳送並傳送所得加密KM-1N[KC]到PM13的隱式RW區域(步驟S121)。

CDS1的媒體I/F部件6傳送儲存在開放RW區域113的已加密內容鑰匙碼KC到PM13的開放RW區域(步驟S122)。

如此一來，本實施例的方法在只有CDS1根據主失效表單RL-M為無效時，允許CDS1自PM13接收已加密主媒體鑰匙碼KM-M。儲存在開放ROM區域114與獨特媒體鑰

五、發明說明（　）[26]

匙碼KM-1N的新失效資料RL-1利用該獨特媒體鑰匙碼KM-M加密，並傳送到PM13。

因此，根據主失效表單RL-M(即嘗試更新PM13的失效資料的電子裝置)而應該被取消的CDS裝置將無疑地被取消(排除在外)。如果一裝置已根據失效表單RL-1無效的話，PM13將無法更新該新失效表單RL-1或獨特媒體鑰匙碼KM-1N。同樣的，如果CDS1根據新失效表單RL-1N不為失效的話，只有已加密的獨特媒體鑰匙碼KM-1N能從PM13被傳輸到CDS1。儲存CDS1的隱式區域114的內容鑰匙碼KC隨後利用獨特媒體鑰匙碼KM-1N被加密並傳送到PM13。如此一來，根據新失效表單RL-1N(即嘗試使用PM13的電子裝置)而應該被取消的CDS裝置將無疑地被取消(排除在外)。

以下將敘述當PD12解密並回放一儲存在PM13的已加密內容的運作方式。以下的解說將著重於PD12所解密與回放的內容，相同的程序也用在LCM21解密與回放內容之情況下。

第12圖顯示介於PM13、PD12與處理流程間的往來。

當使用者指示PD12從PM13回放一內容時，該內容被載入PD12的媒體I/F部件12f，PD12的CPU12a與PM13的控制器130對步驟S110施行一相似的相互鑑別(AKE-1)(步驟S201)。當CDS1與PM13在步驟S201的相互鑑別中發現彼此都為適當的裝置時，PD12的CPU12a與PM13的控制器130交換鑰匙碼以分享相同的對話鑰匙碼KX4。

五、發明說明（　）[27]

PD12的CPU12a讀取PD12的鑑別資料ID-PD，該鑑別資料隱藏在隱式區域124中，並利用對話鑰匙碼KX4解密該鑑別資料ID-PD。媒體I/F部件12f隨後傳送已加密的ID-PD(=KX4[PD])到PM13(步驟S202)。

PM13的控制器130解密利用對話鑰匙碼KX4自PD12接收的KX4[ID-PD]，該對話鑰匙碼KX4自前導鑰匙碼交換中接收，以取得ID-PD(步驟S203)。

PM13的控制器130搜尋開放ROM-W區域中失效表單RL-1N之PD12的已解密鑑別資料ID-PD，並根據符合ID-PD的鑑別資料是否存在，來判定是否應該禁止PD12使用PM13(步驟S204)。

在失效表單RL-1N中找到符合ID-PD的鑑別資料時，控制器130判斷PD12應禁止使用PM13(即被取消)，並在此時結束執行。

另一方面而言，符合ID-PD的鑑別資料不存在於失效資料表單RL-1N的話，控制器130判定PD12可使用PM13，並讀取且輸出秘密儲存在隱式ROM區域135的獨特媒體鑰匙碼KM-1N(步驟S205)。控制器130隨後與PD12的CPU12a(藉由PD12的媒體I/F部件12f)交換鑰匙碼，以共享相同的對話鑰匙碼KX-5。控制器130利用該對話鑰匙碼KX5加密已讀取的獨特主媒體鑰匙碼KM-1N，並傳送所得已加密鑰匙碼KM-1N(=KX5[KM-1N])到PD12(步驟S206)。當前述對話鑰匙碼KX4輸入至事先備置在PD12與PM13的一私密鑰匙碼產生演算法中時，所得到的結果為該對話鑰

五、發明說明（　）[28]

匙碼KX5。

PD12的CPU12a利用在前導鑰匙碼交換過程取得的對話鑰匙碼KX5解密PM13接收的KX5[KM-1N]，而取得獨特媒體鑰匙碼KM-1N(步驟S207)。

隨後，PD12的CPU12a讀取儲存在PM13的隱式RW區域136的加密內容鑰匙碼KC，並利用自步驟S207取得的獨特媒體鑰匙碼KM-1N解密該加密內容鑰匙碼KC。隨後，PD12的CPU12a讀取儲存在PM13的開放RW區域133的加密內容C (=KC[C])、利用自步驟S208取得的加密內容鑰匙碼KC解密該加密內容KC[C]、並回放該內容(步驟S209)。

如此一來，只有在PD12不因著失效表單RL-1N而成為無效時，本實施例中的方法允許PD12自PM13接收加密獨特媒體鑰匙碼KM-1N。保密在PM13的隱式區域RW區域的加密內容鑰匙碼(KM-1N[KC])隨後便利用獨特媒體鑰匙碼KM-1N解密，並被PD12利用以解密加密內容。如此一來，應該因著新失效表單RL-1N而無效的PD(即嘗試著利用PM13的電子裝置)便絕對會失效。

當本發明的著作權保護系統100已根據以上實施例解釋時，本發明很明顯地不受以上所述細節所限制。

例如，當音樂性著作權數位內容受到本實施例保護時，電影的影像數據或電腦程式的數據，如遊戲軟體等，同時也受到保護。

要注意的是，本實施例敘述對話鑰匙碼(KYI或KXI)被用來加密將要或應該保密在隱式區域的訊息的一事件時，

五、發明說明（　）[29]

當在CDS1與PM13之間或在PD12與PM13之間傳輸資料時，加密術便不具備絕對的必要性。然而，利用對話鑰匙碼的加密術更能增加內容被保護的安全性。

在本實施例所敘述的主失效表單RL-M與失效表單RL-1與RL-1N登錄在開放ROM區域132或開放ROM-W區域中，即使失效表單可能儲存在任一無法被改變的區域中。舉例而言，表單可能儲存在只有利用一個特殊程序才能進入的隱式區域134中。

以上實施例所敘述的儲存在隱式RW區域的加密內容鑰匙碼(KM-1N[KC])的一事中，該鑰匙馬可另儲存在開放RW區域133中。

當上述實施例所敘述的一個電子裝置中的鑑別資料從電子裝置傳輸到錄製媒體，該傳輸並不限於此方向。也就是說，一錄製媒體可傳輸鑑別資料到一電子裝置中。

例如，一錄製媒體可事先儲存數值E(ID,K1)與數值E(ID,K2)作為失效資料。該數值E(ID,K1)的取得乃是利用電子裝置的鑑別資料ID來加密事先決定的第一鑰匙碼K1，該電子裝置允許進入錄製媒體上的內容。相反地，該數值E(ID,K2)的取得則是利用電子裝置的鑑別資料ID來加密事先決定的第二鑰匙碼K2，該電子裝置被禁止進入錄製媒體上的內容。

當錄製媒體連接到一電子裝置時，錄製媒體傳送上述的失效資料E與一隨機數R到該電子裝置。

在接收到失效資料E與一隨機數R時，電子裝置利用自

五、發明說明（　）[30]

己的鑑別資料解密失效資料E。當電子裝置還未被取消時，該解密動作導致電子裝置取得第一鑰匙碼K1。相反地，當電子裝置已被取消，該解密動作導致電子裝置取得第一鑰匙碼K2。該電子裝置隨後利用加密結果的鑰匙碼K(K1或K2)來加密隨機數R，並傳送所得數值E(K,R)到錄製媒體。

該錄製媒體解密收到的數值E(K,R)，並比較結果(即隨數R')與傳送到電子裝置的隨機數R。當這些數值相符合時，錄製媒體允許電器用進入內容。此主失效資料可能有相同的內容且利用相同的程序檢驗，而傳輸電子裝置的鑑別資料的方向則可被反轉。

五、發明說明（　）[31]

元件標號對照表

第1圖		12	可攜式錄製/回放裝置(稱可攜式裝置)
1	內容分散系統	13	儲存媒體
12	可攜式錄製/回放裝置(稱可攜式裝置)	14	失效資料接收部件
13	內容使用控制系統(可攜式媒體)	15	使用者I/F部件
		16	失效資料儲存部件
21	內容使用控制系統(特許依從模組)	40	電子音樂分配器
		41	失效資料特許實體
100	著作權保護系統	第3圖	
第2圖		PM	錄製媒體
CDS	內容分散系統	13	儲存媒體
EMD	電子音樂分配器	130	控制器
PM	儲存媒體	131	開放區域
PD	錄製/回放裝置	132	唯讀開放區域
SMS	保全音樂伺服器	133	可逆寫開放區域
2	保全音樂伺服器SMS	134	隱式區域
3	EMD_I/F(介面)部件	135	隱式ROM區域
5	PD_I/F部件	136	隱式可逆寫RW區域136
6	媒體_I/F部件	CDS/PD	內容分散系統/錄製與回放裝置
7	隱式區域驅動器		
8	登錄儲存部件	第4圖	
9	特許儲存部件	132	唯讀開放區域
10	音樂數據儲存部件	132a	開放ROM-W區域

五、發明說明（　　）32

RL-M	主失效資料	第7圖	
RL-1	第一組失效資料	PD	可攜式錄製/回放裝置(稱可攜式裝置)
RL-2	第二組失效資料	12	可攜式錄製/回放裝置(稱可攜式裝置)
第5圖		121	開放區域
CDS	內容分散系統	122	開放ROM區域
1	內容分散系統	123	開放RW區域
111	開放區域	124	隱式區域
112	開放ROM區域	第8圖	
113	開放RW區域	LCM	特許依從模組
114	隱式區域	12	可攜式錄製/回放裝置(稱可攜式裝置)
第6圖		13	儲存媒體PM
PD	錄製/回放裝置(可攜式裝置)	21	內容使用控制系統(特許依從模組)
12a	中央處理器CPU	22	保全音樂伺服器SMS
12b	隨機快取記憶體RAM	23	EMD_I/F部件
12c	唯讀記憶體ROM	25	PD_I/F部件
12d	快閃記憶體	26	媒體I/F部件
12e	外部用品I/F部件	27	隱式區域驅動器
12f	媒體I/F部件	28	登錄儲存部件
12g	解調部件	29	特許儲存部件
12h	解碼器部件	30	音樂數據儲存部件
12i	D/A變頻器部件		
CDS1	內容分散系統		
PM13	錄製媒體		

五、發明說明（　）[33]

31　CD_I/F部件

EMD　電子音樂分配器

第9圖

LCM　特許依從模組

21　內容使用控制系統(特許依從模組)

211　開放區域

212　開放ROM區域

213　開放RW區域

214　隱式區域

第10圖

CDS　內容分散系統

PM　錄製媒體

ID-M　主鑑別資料

ID-1　主鑑別資料

RL-M　主失效資料

RL-1　失效資料

RL-1N 新失效資料

K1-M　鑑別鑰匙碼

KM-1N 新獨特媒體鑰匙碼

KM-M 鑑別鑰匙碼

AKE-M 主要識別與鑰匙碼交換

AKE-1 相互鑑別

KY1　對話鑰匙碼

KY2　對話鑰匙碼

KX1　對話鑰匙碼

E　數值

S101　步驟101

S103　步驟103

S104　步驟104

S105　步驟105

S106　步驟106

S107　步驟107

S108　步驟108

S109　步驟109

S110　步驟110

S111　步驟111

S112　步驟112

S113　步驟113

S114　步驟114

A5
B5

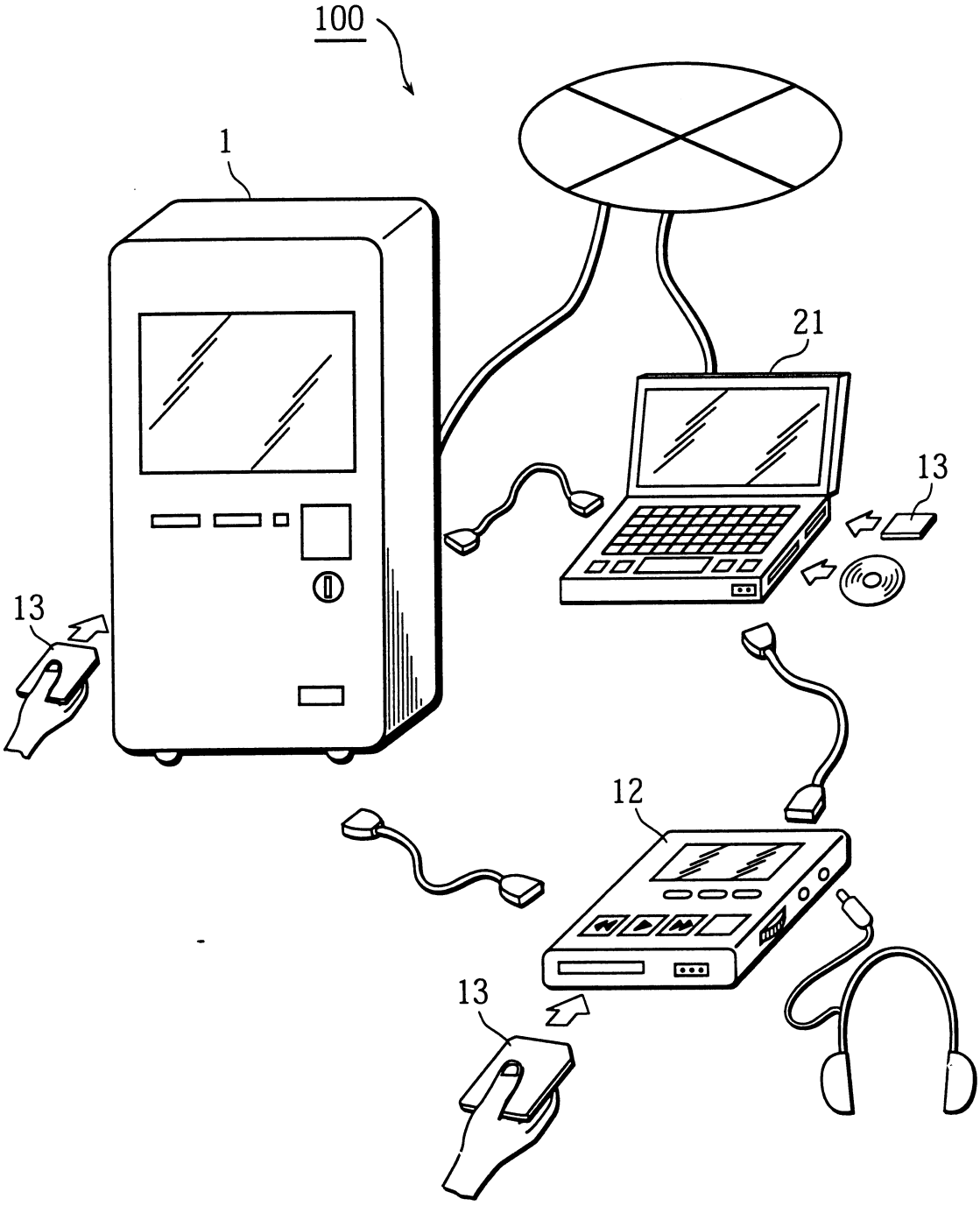
四、中文發明摘要（發明之名稱：失效資訊更新方法與裝置及儲存媒體）

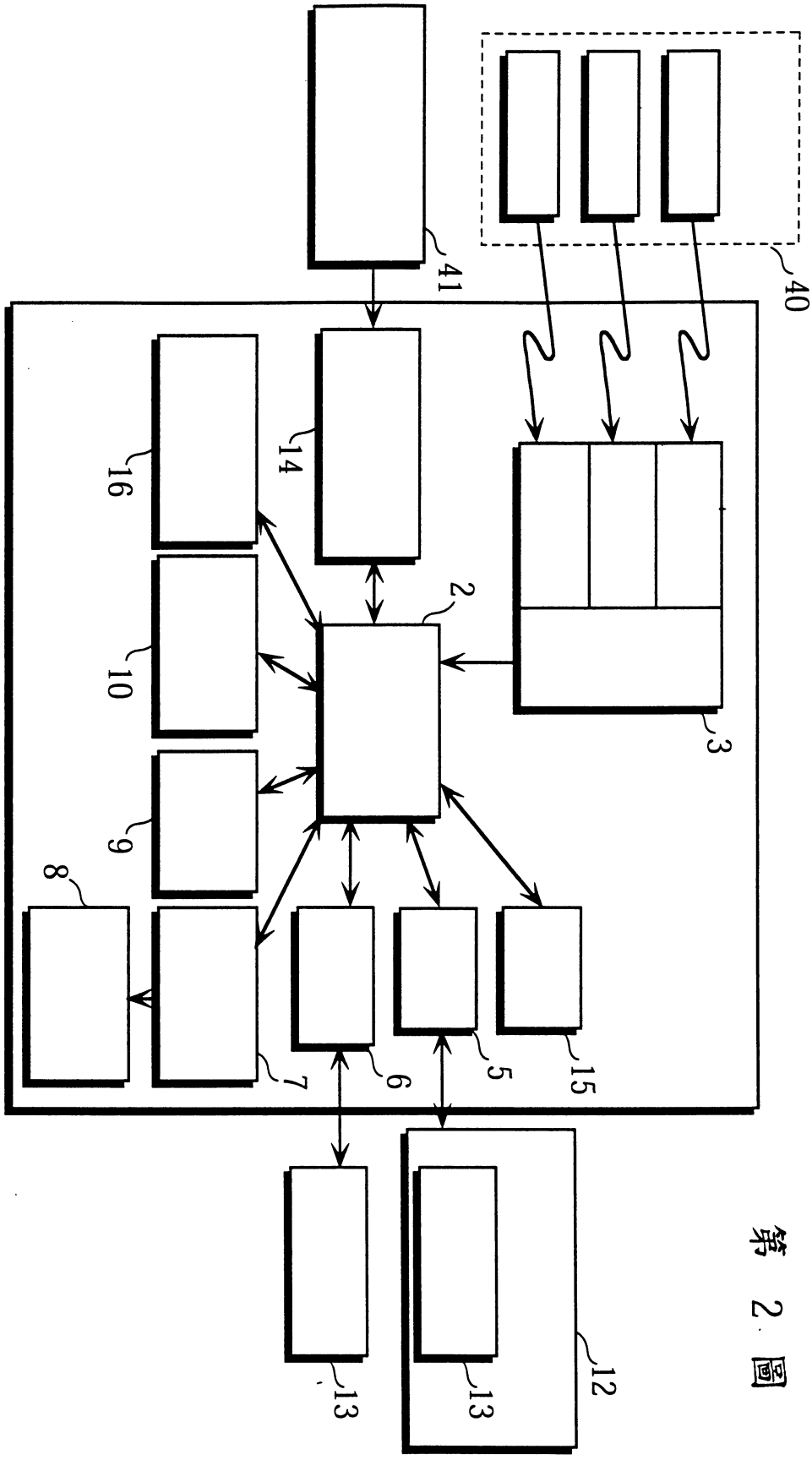
一儲存媒體(PM)13包含一控制器130與二種儲存區域，即隱式區域134與開放區域131。開放區域131包含儲存數位內容的一開放RW區域133；儲存電子裝置之鑑別資料作為失效資料的一開放ROM-W區域132a，該電子裝置被禁止存取數位內容；以及儲存電子裝置之鑑別資料作為主失效資料的一開放ROM區域132，該電子裝置被禁止更新此失效資料。當儲存媒體載入登錄在公開ROM區域132的具鑑別資料的電子裝置時，控制器130可防止電子裝置更新失效資料。

英文發明摘要（發明之名稱：Revocation Information Updating Method, Revocation Information Updating Apparatus and Storage Medium）

A storage medium (PM) 13 includes a controller 130 and two types of storage regions, the concealed region 134 and the open region 131. The open region 131 includes an open RW 133 storing a digital content, an open ROM-W region 132a storing, as revocation information, identification information of an electronic appliance that is prohibited from accessing the digital content, and an open ROM region 132 storing, as master revocation information, identification information of an electronic appliance that is prohibited from updating the revocation information. When the storage medium is loaded into an electronic appliance that has identification information which is registered in the open ROM region 132, the controller 130 prohibits the electronic appliance from updating the revocation information.

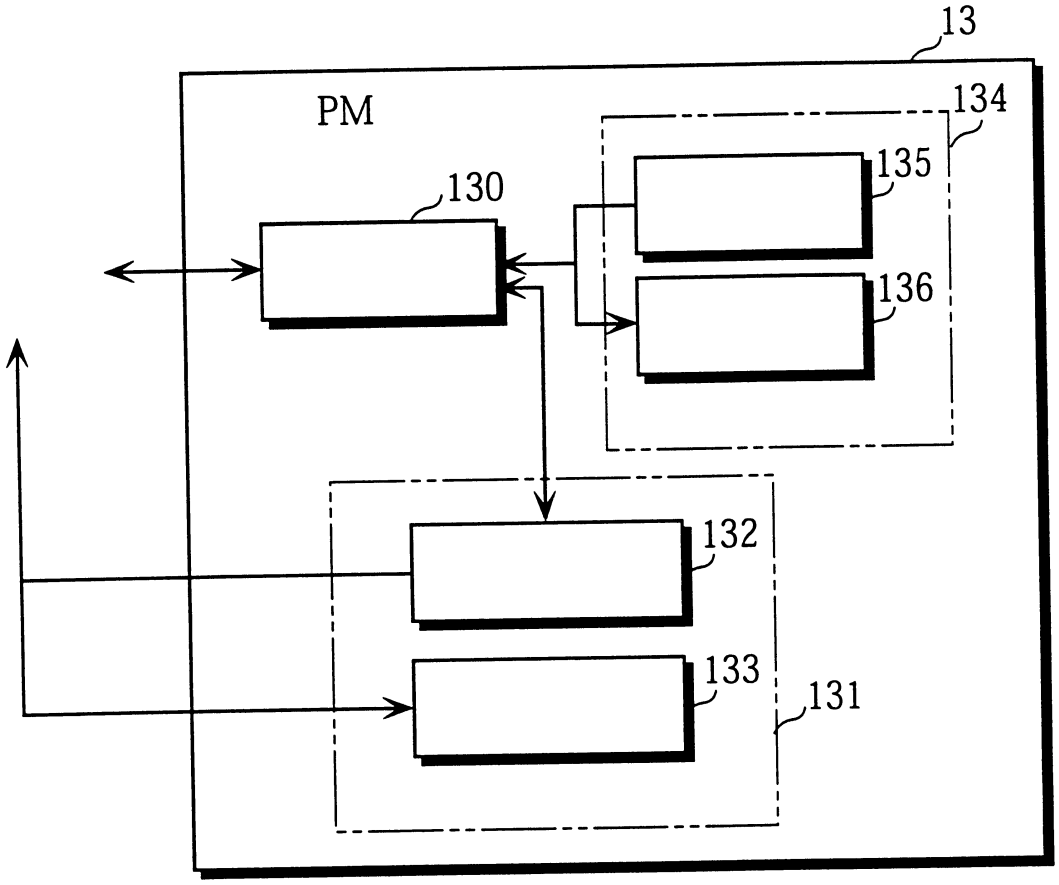
第 1 圖



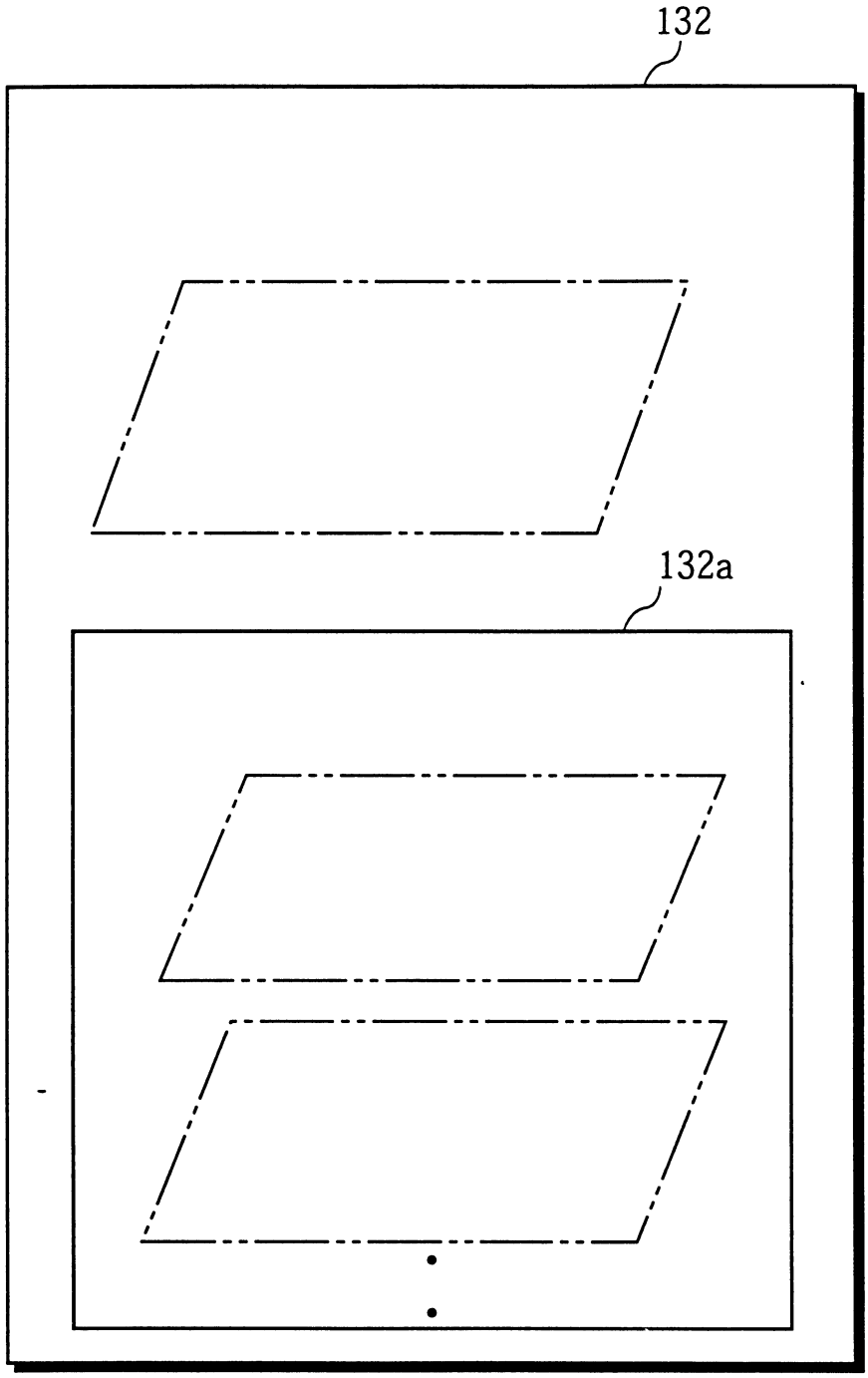


第 2 圖

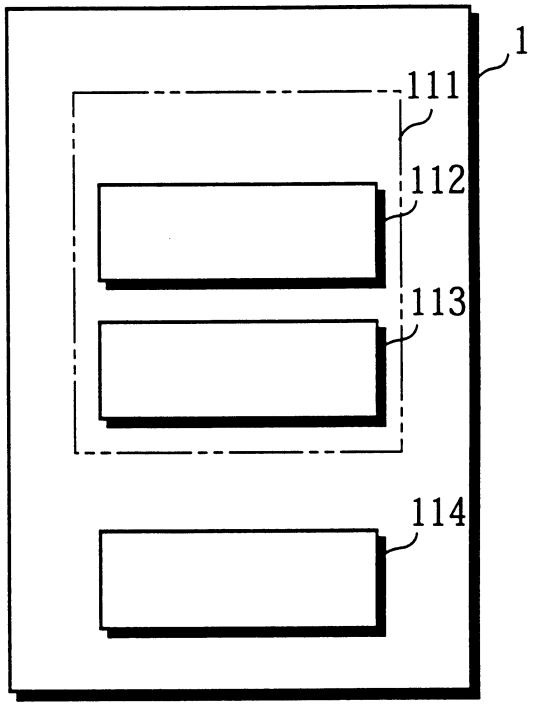
第 3 圖



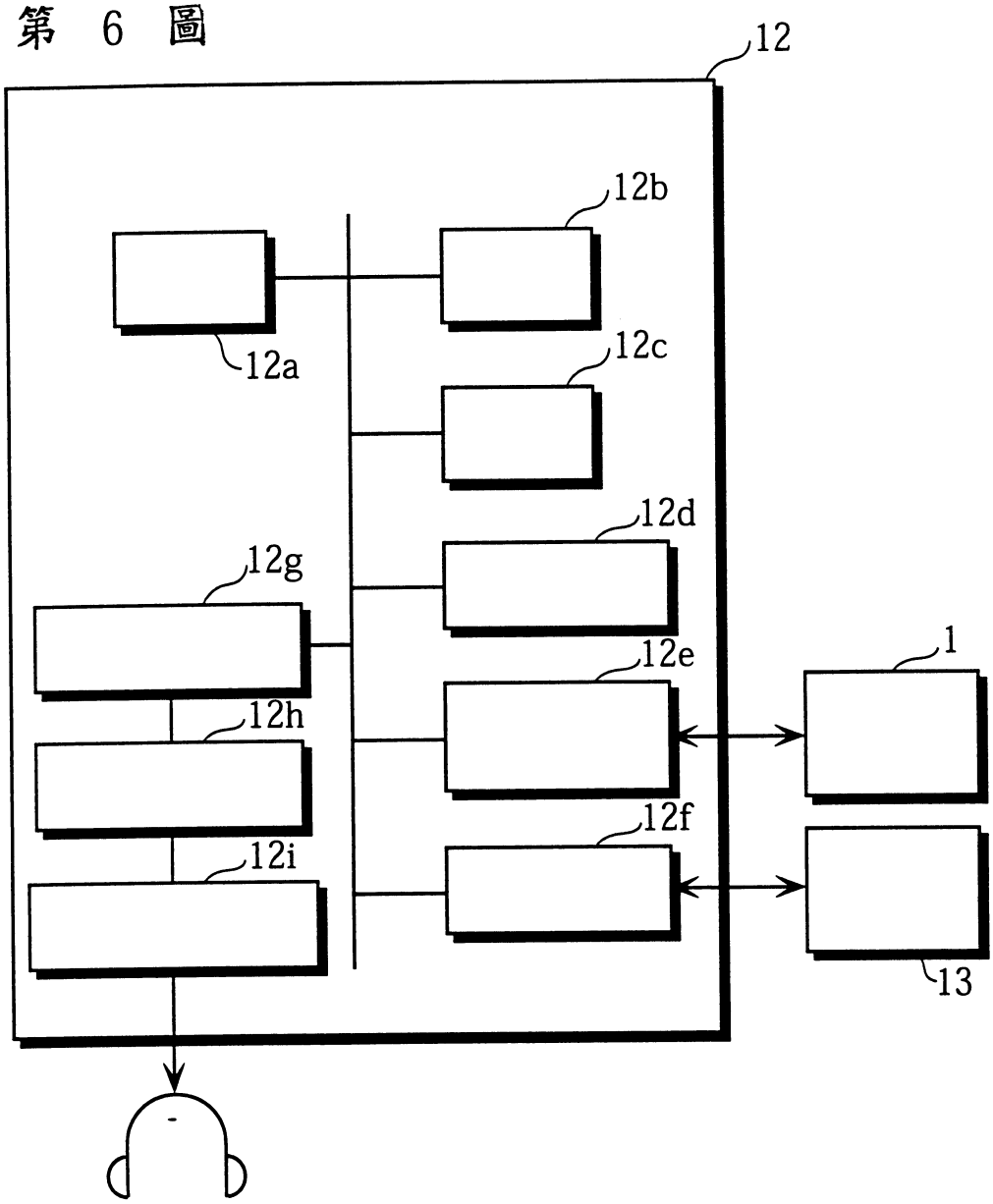
第 4 圖



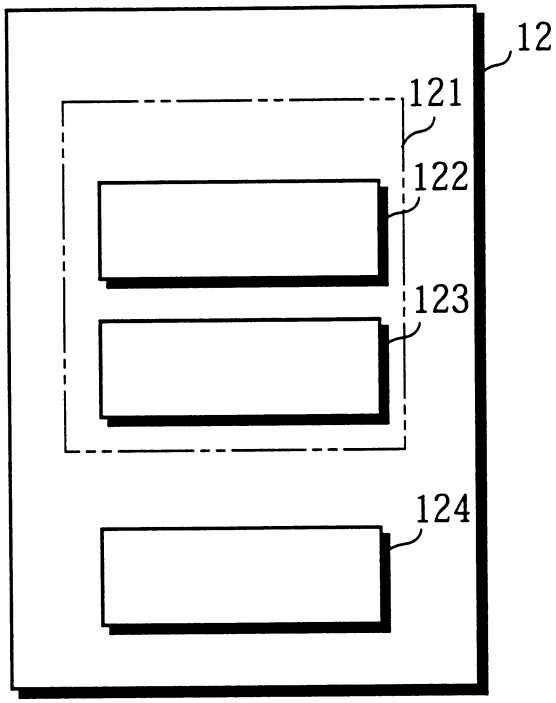
第 5 圖

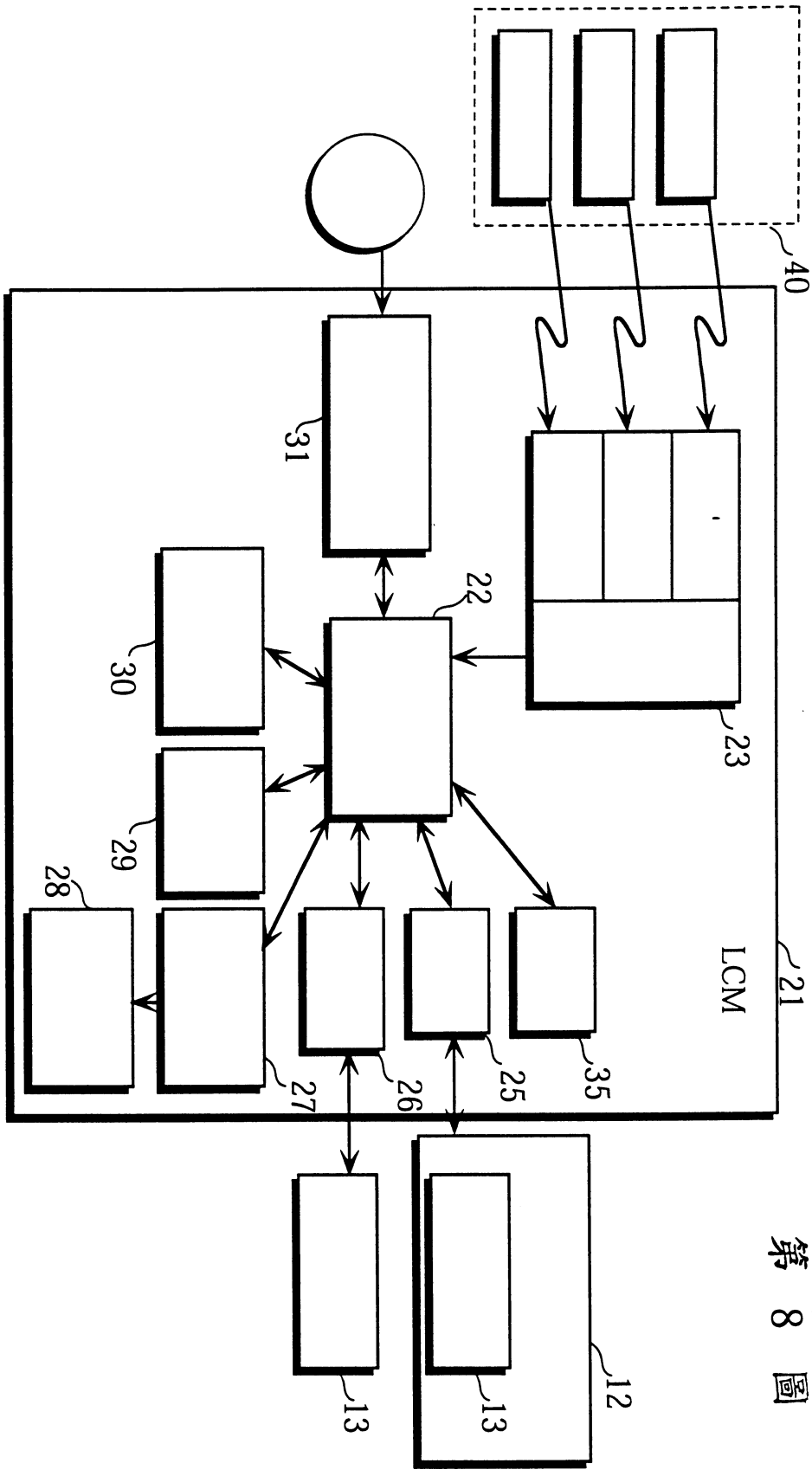


第 6 圖



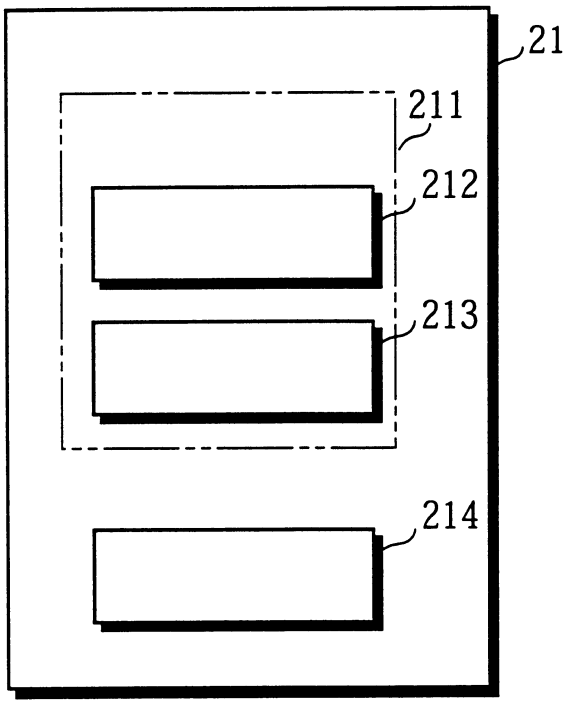
第 7 圖

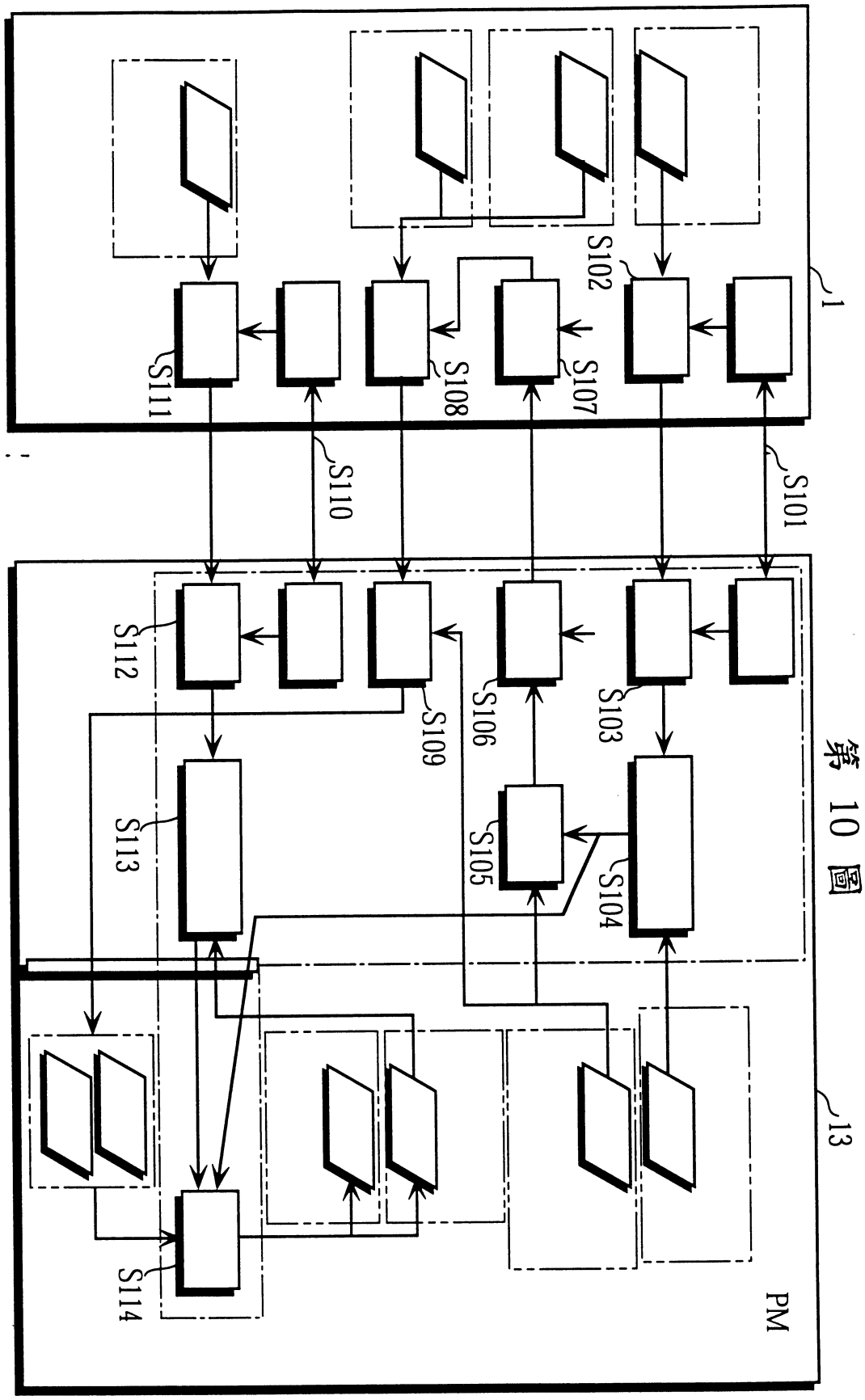




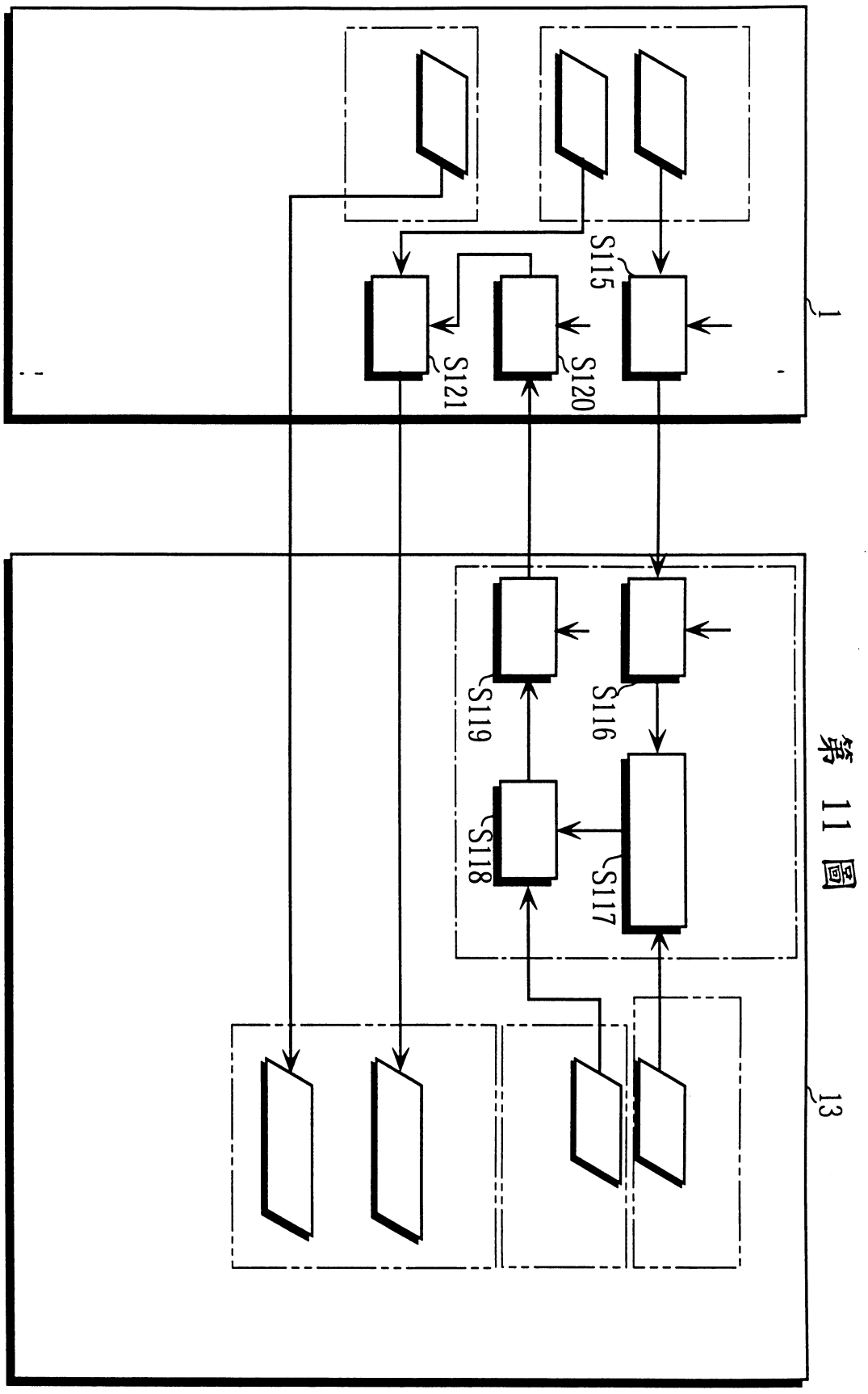
第 8 圖

第 9 圖

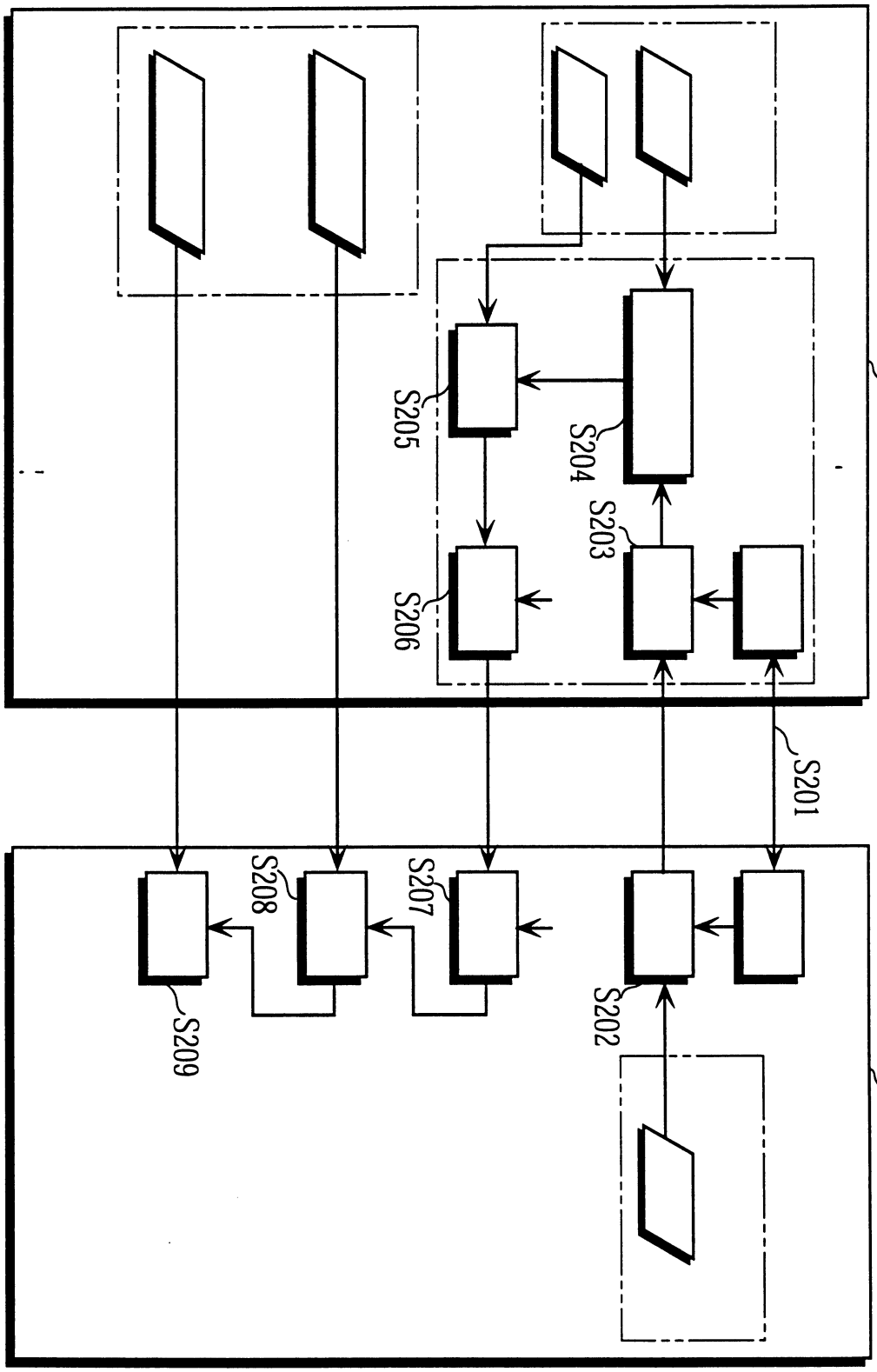



1
S101
S102
S103
S104
S105
S106
S107
S108
S109
S110
S111
S112
S113
S114
13
PM

第 10 圖



第 11 圖



第 12 圖

六、申請專利範圍

第 89122735 號申請案申請專利範圍修正本　　92.3.3.

1. 一種供載入電子裝置使用之儲存媒體，該儲存媒體包含：

一用以儲存數位內容的內容儲存區；

一用以儲存對應於電子裝置之識別資料的資料作為失效資料的失效資料儲存區，該識別資料防止存取儲存於內容儲存區中的數位內容；以及

一用以儲存對應於一電子裝置的識別資料的資料的主失效資料儲存區，該識別資料防止更新儲存於失效資料儲存區中的失效資料。

2. 根據申請專利範圍第 1 項之儲存媒體，其另包含：

一用以執行第一判斷的內容保護方法，它判斷已安裝儲存媒體的一電子裝置是否擁有對應儲存於失效資料儲存區的失效資料的鑑別資料，當第一判斷的結果呈否定時，該內容保護部件允許電子裝置進入儲存在內容儲存資料區的數位內容；以及

一用以執行第二判斷的失效資料更新方法，它判斷已安裝儲存媒體的一電子裝置是否擁有對應儲存於主失效資料儲存區的主失效資料的鑑別資料，當第二判斷結果呈否定時，該更新部件允許電子裝置更新儲存在失效資料儲存資料區的失效資料。

3. 根據申請專利範圍第 2 項之儲存媒體，主失效資料儲存區可備置在 ROM(唯讀記憶體)，其中該主失效資料已事先被儲存。

六、申請專利範圍

4. 根據申請專利範圍第 2 項之儲存媒體，其另包含：

一用以在失效資料更新部件執行第二判斷前，利用已安裝儲存媒體的一電子裝置執行互相鑑別的互相鑑別部件，並且當互相鑑別成功時，該互相鑑別部件也製造一能與電子裝置共享的私密鑰匙碼，其中，該失效資料更新部件利用以互相鑑別部件製造的私密鑰匙碼更新失效資料。

5. 根據申請專利範圍第 2 項的儲存媒體，其中，唯有當第二判斷結果呈否定時，失效資料更新部件可傳送電子裝置必須更新失效資料的一私密鑰匙碼到該電子裝置。

6. 根據申請專利範圍第 2 項之儲存媒體，其中失效資料可分類成數個群組，而失效資料儲存區可包含多個儲存區，每個群組被儲存在不同的儲存區中，而失效資料更新部件可判斷以下情況做為第二判斷：

(1) 安裝了儲存媒體的電子裝置是否擁有不對應於儲存於主失效資料儲存區域的主失效資料的識別資料；

(2) 該電子裝置是否擁有不對應於電子裝置希望更新的失效資料的特定組群中的識別資料；

只有在當(1)與(2)都是肯定的答案時，第二判斷才是否定的，而失效資料更新部件只允許電子裝置更新特定群組中的失效資料。

7. 根據申請專利範圍第 2 項之儲存媒體，該儲存媒體的

六、申請專利範圍

失效資料區域儲存一剛利用加密之事先決定的私密鑰匙碼而被製造的資料作為作為失效資料，該私密鑰匙碼利用被禁止進入數位內容之電子裝置中的鑑別資料作為一鑰匙碼，

內容保護構件傳輸儲存於失效資料儲存區域的失效資料到電子裝置上，該電子裝置已載入儲存媒體，並且判斷電子裝置回覆的資料是否發揮了一事先決定的正規，以決定該電氣用品是否擁有對應儲存於失效資料儲存區的失效資料的鑑別資料，

主失效資料區域儲存一剛利用加密之事先決定的私密鑰匙碼而被製造的資料作為作為主失效資料，該私密鑰匙碼利用被禁止更新失效資料之電子裝置中的鑑別資料作為一鑰匙碼，

該失效資料更新構件傳輸儲存於主失效資料儲存區域的主失效資料到電子裝置上，並且判斷電子裝置回覆的資料是否發揮了一事先決定型態的正規，以決定該電氣用品是否擁有對應儲存於主失效資料儲存區的主失效資料的鑑別資料。

8. 一種更新儲存媒體上的失效資料之失效資料更新方法，該儲存媒體係供載入一電子裝置使用並且包括：(1)一用以儲存數位內容的內容儲存區；(2)一用以儲存對應於電子裝置的識別資料的資料的失效資料儲存區，該電子裝置被禁止存取儲存於內容儲存區中的數位內容；以及(3)一用以儲存對應於一電子裝置的識別

六、申請專利範圍

資料的資料的主失效資料儲存區，該電子裝置被禁止更新儲存於失效資料儲存區中的失效資料；

該方法包含：

一用以檢測儲存媒體是否已安裝到電子裝置的檢測步驟，

一用以判斷電子裝置的第一鑑別資料是否不對應於儲存在儲存媒體的主失效資料儲存區的主失效資料的第一判斷的步驟；以及

唯有當第一判斷結果呈肯定時，一用以更新儲存在失效資料儲存區的失效資料的更新步驟。

9. 如申請專利範圍第 8 項之失效資料更新方法，其中更新步驟有一種對應於一電子裝置的第二鑑別資料的資料，該第二鑑別資料儲存在失效資料儲存區域，作為新失效資料。

10. 如申請專利範圍第 9 項之失效資料更新方法，其另包含：

一相互鑑別步驟，其中在電子裝置與儲存媒體之間執行互相鑑別，只有互相鑑別成功時，一即將被電子裝置與儲存媒體共享的私密鑰匙碼才能被製造，

其中更新步驟利用相互鑑別步驟所產生的私密鑰匙碼更新該失效資料。

11. 如申請專利範圍第 10 項之失效資料更新方法，其中更新步驟包含：

當第一判斷結果呈肯定時，利用相互鑑別步驟所產生

六、申請專利範圍

的私密鑰匙碼來加密對應於一電子裝置之第二鑑別資料的資料並使被加密資料自電子裝置傳輸置儲存媒體的傳輸子步驟；以及

利用私密鑰匙碼，用以解密被傳輸已加密資料的儲存子步驟，以及用以在失效資料儲存區域中儲存資料作為新失效資料的儲存子步驟。

12. 如申請專利範圍第 9 項之失效資料更新方法，其中判斷步驟包含了一用以對判斷第二鑑別資料是否對應於儲存於失效資料儲存區域中執行第三判斷的判斷子步驟，以及

當第一判斷結果呈肯定時而第三判斷呈否定時，更新步驟中有第二鑑別資料，該第二鑑別資料儲存在失效資料儲存區中作為新失效資料。

13. 如申請專利範圍第 9 項之失效資料更新方法，其中主失效資料區域儲存一剛利用加密之特別私密鑰匙碼而被製造的資料作為作為主失效資料，該特別私密鑰匙碼利用被禁止更新失效資料之電子裝置中的鑑別資料作為一鑰匙碼，並且

判斷步驟傳輸儲存於主失效資料儲存區域的主失效資料到電子裝置上，該電子裝置已被載入儲存媒體，也判斷電子裝置的鑑別資料是否對應於儲存儲存媒體中的主失效資料限制區的主失效資料，更判斷自電子裝置接收的回覆是否發揮了一事先決定型態的正規。

14. 一種用以更新儲存媒體上的失效資料之失效資料更新

六、申請專利範圍

裝置，該儲存媒體係供載入電子裝置使用且包含：(1)一用以儲存數位內容的內容儲存區；(2)一用以儲存對應於電子裝置的識別資料的資料的失效資料儲存區，該電子裝置被禁止存取儲存於內容儲存區中的數位內容；以及(3)一用以儲存對應於一電子裝置的識別資料的資料的主失效資料儲存區，該電子裝置被禁止更新儲存於失效資料儲存區中的失效資料；

該失效資料更新裝置包含：

一用以儲存不對應於儲存在儲存媒體之主失效資料儲存區的主限制區域的第一鑑別資料儲存構件；

一用以取得與使用對應於儲存在第一鑑別資料區域構件中的第一鑑別資料的許可取得構件，該許可來自儲存媒體以更新儲存在儲存媒體上的失效資料；以及

一更新構件，用以根據許可取得構件取得之許可更新儲存在儲存媒體的失效資料。

15. 如申請專利範圍第 14 項之失效資料更新裝置，其中更新構件利用事先儲存且對應於第二鑑別資料的資料來更新失效資料。

16. 如申請專利範圍第 15 項之失效資料更新裝置，其另包含：

在許可取得構件試著取得更新失效資料的許可前，一用以與儲存媒體執行互相鑑別的相互鑑別構件；只有互相鑑別已成功時，該相互鑑別構件可製造能被儲存媒體共享的私密鑰匙碼，

六、申請專利範圍

在該儲存媒體中，更新步驟利用相互鑑別步驟所產生的私密鑰匙碼更新該失效資料。

17. 如申請專利範圍第 16 項之失效資料更新裝置，其另包含：

該更新構件利用相互鑑別步驟所產生的私密鑰匙碼，藉由加密對應於第二鑑別資料的新失效資料來更新失效資料，並且將已加密資料從電子裝置傳輸到儲存媒體。

18. 如申請專利範圍第 15 項之失效資料更新裝置，

其中該失效資料被分成多個組群，且失效資料儲存區包含多個儲存區，每個儲存區儲存一種不同的組群，該更新構件只更新一組群中的失效資料，其對應於第二鑑別資料。

19. 如申請專利範圍第 15 項之失效資料更新裝置，其中主失效資料區域儲存一藉由加密事先決定之私密鑰匙碼而被製造的資料作為作為主失效資料，該事先私密鑰匙碼利用被禁止更新失效資料之電子裝置中的鑑別資料作為一鑰匙碼，並且

許可取得構件藉由接收傳送自儲存媒體的主失效資料來取得許可、利用一電子裝置中的第一鑑別資料來解密主失效資料，並傳送發揮一事先決定型態的正規的一已解密結果與資料到該儲存媒體。