

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 日本；2004年05月10日；特願2004-140210

2. 日本；2004年06月07日；特願2004-168489

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係關於一種資訊處理裝置、資訊處理方法以及電腦程式。進而，更詳細的是關於一種防止非法利用內容之資訊處理裝置、資訊處理方法以及電腦程式。

【先前技術】

近年來，DVD、藍色雷射光碟(Blu-ray Disc)等可儲存大容量資料之資訊記錄媒體不斷普及，將例如高精細圖像資料或高品質音聲資料等數位內容於碟片等記錄媒體上上述錄再生之利用形態亦成為一般化。

作為再生、記錄處理來自資訊記錄媒體之內容的態樣，存在利用將驅動資訊記錄媒體(碟片)之驅動器與再生/記錄處理機能一體化之裝置的態樣，以及以匯流排等連接驅動器與作為執行再生處理或記錄處理程式之主機的資訊處理裝置例如PC等，於驅動器與主機之間執行資料轉送的處理態樣。

例如，作為執行驅動器與主機間之資料轉送的情形時之問題點，存在非法利用、流出內容之可能性變大之問題。音樂資料、圖像資料等眾多內容一般會由其作成者或銷售者保存發佈權等。因此，於發佈該等內容時，一般會構成一定利用限制，即僅對正規用戶允許利用內容，且未經許可無法複製等。

根據數位記錄裝置以及記錄媒體，可不劣化圖像或音聲地重複記錄、再生，因此被非法複製之內容介以網際網路

的發送或將內容複製於CD-R、DVD等記錄媒體之盜版碟片的流通已成為較大問題。

於DVD或藍色雷射光碟等大容量型記錄媒體中，可將影像資訊、音樂資訊作為數位資料而儲存。於使此種數位資料記錄媒體流通至市場時，必需實現防止非法複製且保護著作權者之構成。目前，為防止此種數位資料之非法複製，於數位記錄裝置以及記錄媒體方面已試用有用以防止違法複製之多種技術。

例如，於DVD播放器中採用有內容加密系統(CSS：Content Scramble System)。內容加密系統中，於記錄媒體例如DVD-ROM(Read Only Memory，唯讀記憶體)中加密記錄有視頻資料或聲頻資料等，且將用於解碼該經加密之資料的密鑰僅賦予接受到許可證之播放器。許可證僅賦予不進行非法複製等遵從特定動作規定而設計之播放器。因此，接受許可證之播放器中，利用賦予之密鑰，藉由解碼記錄於資訊記錄媒體之加密資料，可再生圖像或音聲。

另一方面，未接受許可證之播放器因不具有用以解碼經加密之資料的密鑰，故而無法對記錄於資訊記錄媒體之加密資料加以解碼。如此，內容加密系統(CSS)可提供僅允許具有正規許可證之播放器利用內容的系統。

然而，該內容加密系統(CSS)存在無法確實排除內容之非法利用的問題。特別是，自安裝有資訊記錄媒體之驅動器將內容輸出至PC等資訊處理裝置而進行再生之處理中，會產生可非法利用內容之問題。以下，參照圖式就該問題加

以說明。

圖1表示採用內容加密系統(CSS)之儲存有內容的資訊記錄媒體之儲存資料例以及再生機器(播放器)之處理。

圖1所示之資訊記錄媒體10為例如DVD視頻碟片，於資訊記錄媒體10儲存有加密碟片密鑰(Secured Disc Key)11、相應於儲存於資訊記錄媒體10之內容標題的加密標題密鑰12、以及作為依據CSS方式實行加密處理之內容的加密MPEG資料13。

安裝資訊記錄媒體10實行內容再生之再生機器20、例如DVD播放器使用儲存於再生機器20之主密鑰，於步驟S11中實行自資訊記錄媒體10取得之加密碟片密鑰(Secured Disc Key)11的解碼處理，取得碟片密鑰，於步驟S12中使用所取得之碟片密鑰，實行自資訊記錄媒體10取得之加密標題密鑰12的解碼處理，取得標題密鑰，使用所取得之標題密鑰，於步驟S13中實行加密MPEG資料13之解密處理後，於步驟S14中實行MPEG解碼處理而再生音聲/影像資料25。

接著，自連接於執行作為內容再生處理程式之播放器應用程式的主機(例如PC)之驅動器，將內容輸入至主機(PC)側，相應主機之播放器應用程式而再生內容，關於該處理流程，參照圖2加以說明。

如圖2所示，於安裝有資訊記錄媒體之驅動器30與主機側之播放器應用程式40之間，於如圖所示之步驟S31、S41中，執行相互認證以及密鑰共有(AKE: Authentication and Key Exchange)。相互認證處理係根據例如公開密鑰密碼方式之

算法而執行。於相互認證中產生通話密鑰，驅動器30與PC側之播放器應用程式40共有通話密鑰。

驅動器30於步驟S32中，使用通話密鑰對自資訊記錄媒體10取得之加密碟片密鑰11實行再加密，發送至播放器應用程式40，又，於步驟S33使用通話密鑰，對自資訊記錄媒體取得之加密標題密鑰12實行再加密，發送至播放器應用程式40。驅動器30與作為播放器應用程式40之執行裝置的PC藉由連接匯流排例如ATAPI-BUS而連接，該等加密密鑰資訊介以連接匯流排發送至主機(PC)之播放器應用程式40側。

進而，驅動器30將自資訊記錄媒體取得且作為依據CSS方式執行加密處理之內容即加密MPEG資料13介以驅動器與PC間之連接匯流排而輸出至PC側。

PC側之播放器應用程式40於步驟S42中，使用通話密鑰解碼自驅動器30接收之加密碟片密鑰11的使用通話密鑰之再加密資料，取得加密碟片密鑰11，進而，於步驟S43中，解碼自驅動器30接收之加密碟片密鑰12的使用通話密鑰之再加密資料，取得加密標題密鑰12。

其後之步驟S51~S55之處理與先前參照圖1說明之處理(S11~S14)為相同的處理。

圖3表示於該圖2所示之處理中之驅動器側之處理的流程圖。當於步驟S61中判定插入有資訊記錄媒體(碟片)時，於步驟S62中，與主機即執行圖2所示之播放器應用程式40的PC執行相互認證以及密鑰共有(AKE: Authentication and

Key Exchange)。

當相互認證以及密鑰共有(AKE)成功(步驟S63: Yes)時，移動至安裝於驅動器之資訊記錄媒體之儲存內容即CSS加密資料之輸出被許可的狀態，該CSS加密資料之輸出許可狀態繼續至退出資訊記錄媒體為止或電源斷開為止。

如此，驅動器於與內容輸出對象之機器之相互認證成立前，設定為CSS加密資料之輸出未被許可之狀態，於與內容輸出對象之機器之相互認證成立以後，設定為CSS加密資料之輸出被許可的狀態，該輸出許可狀態繼續至退出資訊記錄媒體為止或電源斷開為止。

因此一種允許自驅動器輸出內容之狀態，會產生如圖4所示之非法利用內容之情形。

圖4(1)表示通過切換作為自驅動器輸出內容之對象的PC等主機側之應用程式而迂回利用內容的例。

就主機(PC)60側之處理(步驟S71~S73)加以說明。於步驟S71中，於安裝有資訊記錄媒體之驅動器50與主機(PC)60之正規播放器應用程式間執行相互認證。通過成立該相互認證，驅動器50設定為允許輸出CSS加密資料之狀態。

於步驟S72中，自驅動器50讀出含有CSS加密資料之音聲/影像(Audio/Video)資料，並儲存於硬碟中。

於步驟S73中，切換應用程式，使用CSS解除軟體，對儲存於硬碟之CSS加密資料執行解密處理。

藉由如此之處理可實現解密，所解密之正常內容可被無限制地利用。

圖 4(2)所示之處理表示通過主機(PC)與驅動器間之連接匯流排例如 ATAPI-BUS 之竊聽處理而非法利用內容的例。

就主機(PC)60側之處理(步驟S81~S83)加以說明。於步驟S81中，於安裝有資訊記錄媒體之驅動器50與主機(PC)60之正規播放器應用程式間執行相互認證，獲得內容且實行再生。

內容作為CSS加密資料，介以主機(PC)與驅動器間之連接匯流排例如 ATAPI-BUS 而被輸入。

主機60於步驟S82中，對主機(PC)與驅動器間之連接匯流排實行監控，將藉由監控獲得之資料即CSS加密資料儲存於硬碟。

於步驟S63中，使用CSS解除軟體，對儲存於硬碟之CSS加密資料執行解密處理。

藉由如此之處理可獲得解密之內容，所解密之正常內容可被無限制地利用。

如此，現行之內容加密系統(CSS)無法確實地排除內容被非法利用之可能。特別是，如上所述，自安裝有資訊記錄媒體之驅動器將內容輸出至PC等資訊處理裝置而進行再生之處理中，易產生非法利用內容之問題。

[發明所欲解決之問題]

本發明係鑒於上述問題開發而成者，其目的在於提供一種於伴隨驅動器與主機等兩個不同裝置間之資料轉送而再生或記錄處理內容時，藉由對使用於實行資料轉送之裝置間之相互認證的公開密鑰證書之有效性執行嚴格判定，而

可排除非法利用內容的資訊處理裝置、資訊處理方法、以及電腦程式。

進而，更詳細的是，於自數位內容之發送側(源)裝置向接收側(同步)裝置轉送內容時，於裝置間實施以公開密鑰密碼為基礎之相互認證，為判斷相互認證中所使用之各裝置之公開密鑰證書的有效性，參照證書(認定裝置群證書)。此時，本發明之目的在於提供一種為排除過期證書(認定裝置群證書)之使用，藉由依據例如登錄裝置數、或無效(Revoke)裝置數等資料判定證書有無過期，而可排除依據使用過期證書之非法認證處理而非法利用內容的可能性，進而於主機計算與驅動器之認證次數，於認證次數到達預先設定之上限值時停止認證處理之實行，促使用戶獲得證書，藉此可排除過期證書之繼續利用的資訊處理裝置、資訊處理方法、以及電腦程式。

【發明內容】

本發明之第一方面係一種資訊處理裝置，其特徵在於：
具有

證書記憶部，其儲存認定裝置證書，

認證實行部，其執行裝置之認證處理，且於該認證處理中，使用上述認定裝置證書執行處理，以及

計算值記憶部，其計算介以上述認證實行部執行之認證次數，且儲存計算值；

上述認證實行部構成，以認證次數計算值未到達預先設定之認證次數上限值為條件，執行認證處理。

進而，於本發明之資訊處理裝置之一實施態樣中，上述資訊處理裝置之構成為進而具有更新執行部，該更新執行部於儲存於上述計算值記憶部之認證次數計算值到達預先設定之認證次數上限值時，藉由介以通信部獲得認定裝置證書之處理，執行儲存於上述證書記憶部之認定裝置證書的更新處理。

進而，於本發明之資訊處理裝置之一實施態樣中，上述資訊處理裝置構成為，伴隨上述更新執行部之認定裝置證書之更新處理，對上述計算值記憶部之認證次數計算值執行重設處理。

進而，於本發明之資訊處理裝置之一實施態樣中，上述資訊處理裝置構成為，通過上述更新執行部之認定裝置證書之獲得作為自連接網路之伺服器的獲得處理而執行。

進而，於本發明之資訊處理裝置之一實施態樣中，上述資訊處理裝置構成為，具有更新執行部，上述更新執行部對自外部獲得之認定裝置證書執行正當性確認處理，且於確認為正當時，對儲存於上述證書記憶部之認定裝置證書執行更新處理。

進而，於本發明之資訊處理裝置之一實施態樣中，上述資訊處理裝置構成為，於認證次數計算值到達預先設定之認證次數上限值時，上述資訊處理裝置對用戶執行通知處理。

進而，於本發明之資訊處理裝置之一實施態樣中，上述資訊處理裝置構成為，將上述更新執行部自外部獲得之證

書之至少一部分證書資料作為儲存於認證處理對象即驅動器之證書資料而輸出至驅動器。

進而，於本發明之資訊處理裝置之一實施態樣中，上述資訊處理裝置構成爲，儲存於上述驅動器之證書資料為含有使用於認定裝置證書之新舊比較的資料之證書。

進而，於本發明之資訊處理裝置之一實施態樣中，上述資訊處理裝置構成爲，使用於上述認定裝置證書之新舊比較的資料為記錄於認定裝置證書之序列號、登錄裝置數、或無效(Revoke)裝置數中之任一種資料。

進而，本發明之第二態樣係一種資訊處理方法，其特徵在於包含：

比較步驟，其對儲存於記憶部之認證次數計算值與預先設定之認證次數上限值執行比較處理；以及

認證步驟，其以獲得認證次數計算值未到達預先設定之認證次數上限值的比較結果為條件，執行認證處理。

進而，於本發明之資訊處理方法之一實施態樣中，上述資訊處理方法進而具有伴隨上述認證步驟之結束，執行計算出儲存於記憶部之認證次數計算值的處理之步驟。

進而，於本發明之資訊處理方法之一實施態樣中，上述資訊處理方法進而具有更新步驟，其於儲存於上述計算值記憶部之認證次數計算值到達預先設定之認證次數上限值時，介以通信部執行認定裝置證書之獲得處理，對儲存於證書記憶部之認定裝置證書執行更新處理。

進而，於本發明之資訊處理方法之一實施態樣中，伴隨

上述更新步驟之認定裝置證書之更新處理，對上述計算值記憶部之認證次數計算值執行重設處理。

進而，於本發明之資訊處理方法之一實施態樣中，上述更新步驟中認定裝置證書之獲得作為自連接網路之伺服器之獲得處理而執行。

進而，於本發明之資訊處理方法之一實施態樣中，上述更新步驟執行自外部獲得之認定裝置證書之正當性確認處理，於確認為正當時對儲存於上述證書記憶部之認定裝置證書執行更新處理。

進而，於本發明之資訊處理方法之一實施態樣中，上述資訊處理方法進而於認證次數計算值到達預先設定之認證次數上限值時，對用戶執行通知處理。

進而，於本發明之資訊處理方法之一實施態樣中，上述資訊處理方法進而具有將上述更新步驟中自外部獲得之證書之至少一部分證書資料作為儲存於認證處理對象即驅動器之證書資料而輸出至驅動器的步驟。

進而，於本發明之資訊處理方法之一實施態樣中，儲存於上述驅動器之證書資料為包含用以對認定裝置證書執行新舊比較的資料之證書。

進而，於本發明之資訊處理方法之一實施態樣中，用以對上述認定裝置證書加以新舊比較之資料為記錄於認定裝置證書之序列號、登錄裝置數、或無效(Revoke)裝置數中之任一種資料。

進而，本發明之第三態樣係一種電腦程式，其特徵在於

包含：

比較步驟，其對儲存於記憶部之認證次數計算值與預先設定之認證次數上限值執行比較處理；以及

認證步驟，其以獲得認證次數計算值未到達預先設定之認證次數上限值的比較結果為條件，執行認證處理。

再者，本發明之電腦程式為例如可對於可執行各種程式・代碼之電腦系統，藉由以電腦可讀之形式而提供之記錄媒體、通信媒體例如CD或FD、MO等記錄媒體、或網路等通信媒體而提供之電腦程式。藉由以電腦可讀之形式提供該種程式，可於電腦系統上執行相應程式之處理。

本發明之進而其他目的、特徵或益處，可藉由下述本發明之實施例或隨附之圖式而加以更詳細之說明。再者，於本說明書中，所謂系統係指複數個裝置之邏輯性集合構成，並非限定為各構成裝置位於同一框體內者。

[發明之效果]

根據本發明之構成，於伴隨驅動器與主機等兩個不同裝置間之資料轉送而再生或記錄處理內容時，於執行資料轉送之裝置間之相互認證中，計算認證次數，於到達預先設定之認證次數上限值時，停止認證處理，設定為必須更新用以認證之證書，故而可排除使用過期證書繼續認證處理而利用內容之可能性，並促使用戶獲得最新證書。

本發明之構成中，於連接裝置間，自內容之發送側(源)裝置向接收側(同步)裝置轉送內容時實行之公開密鑰密碼方式的相互認證中，為判斷所使用之各裝置之公開密鑰證

書的有效性，使用認定裝置群證書。進而構成爲，於判斷該認定裝置群證書有無過期時，使用將作爲認定裝置群證書之集合而設定之認定裝置群列表(登錄列表)之登錄裝置數或無效(Revoke)裝置數等設爲登錄資料的ADGL資訊證書(AIC)，依據將登錄裝置數爲多者作爲最新或將無效裝置數爲多者作爲最新等之登錄資訊之登錄或無效裝置數的變化狀況，判定認定裝置群證書之最新性，使用新認定裝置群證書判定裝置之公開密鑰證書的有效性而執行相互認證，進而計算認證次數，於到達預先設定之認證次數上限值時，停止認證處理，設定爲必須更新用以認證之證書，故而可防止使用過期認定裝置證書實行認證處理，防止非法獲得內容，排除非法利用內容之可能性。

又，因構成爲依據將登錄裝置數或無效(Revoke)裝置數等設定爲登錄資料之ADGL資訊證書(AIC)，適當更新資訊處理裝置保管之認定裝置群列表(登錄列表)，故而可隨時更新實行內容再生或記錄處理之資訊處理裝置的保管列表。

進而，藉由將登錄裝置數或無效裝置數使用於各證書之是否過期的判定，可減少作爲驅動器或主機之證書儲存用之非揮發性記憶體而使用之快閃記憶體的覆寫次數。即，於使用序列號判定有無過期之情形時，因序列號變更時需全部更新，故而快閃記憶體之使用頻率增多，但藉由將登錄裝置數或無效裝置數用於各證書之是否過期的判定，登錄裝置數或無效裝置數無變化之情形時可無需於驅動器或主機更新證書，故而可減少快閃記憶體之覆寫次數。因此

可搭載小型且廉價之記憶體。

【實施方式】

以下，參照圖式，就本發明之資訊處理裝置、資訊處理方法以及電腦程式加以詳細說明。再者，說明根據以下揭示項目而實行。

1. 資訊記錄媒體之儲存資料
2. 內容再生處理概要
3. 伴隨驅動器與主機間之內容轉送的處理
4. 認證次數之計算以及證書更新處理
5. 資訊處理裝置之構成

[1. 資訊記錄媒體之儲存資料]

首先，就資訊記錄媒體之儲存資料加以說明。圖5表示儲存有內容之資訊記錄媒體之一例。

該碟片係例如Blu-ray(藍光)碟片、DVD等資訊記錄媒體，且係於具有正當內容著作權或頒佈權即獲得內容權利者之許可下於碟片製造工場製造的儲存有正當內容之資訊記錄媒體、或可記錄內容之資訊記錄媒體。再者，於以下實施例中，作為資訊記錄媒體之例，以碟片型媒體為例加以說明，但本發明亦可適用於各種態樣之資訊記錄媒體。

如圖5所示，資訊記錄媒體100具有：儲存內容等資料之資料儲存區域101；以及引入區域102，其儲存對應碟片以及儲存內容之附帶資訊、使用於內容之解碼處理的密鑰資訊、以及實行內容之再生或記錄處理的裝置即驅動器或PC等主機、主機應用程式等之登錄資訊等。

於資料儲存區域101中儲存有加密(Scramble)內容111以及單元密鑰產生資訊：Vu112，該單元密鑰產生資訊：Vu112係作為產生用於加密內容之解碼處理的密鑰所必需之資訊的記錄種(REC SEED)。再者，加密處理係加密處理之一態樣，於本說明書中作為加密內容之上位概念使用所謂加密內容之表現。加密內容111區分為特定單元單位，於使用對應單元之單元密鑰而加密的狀態下，儲存於資訊記錄媒體100之資料儲存區域101。單元密鑰產生資訊：Vu112為使用於產生該等各單元密鑰之資訊，亦稱為種資訊。

於引入區域102儲存產生用以解碼加密內容111之密鑰所必需的各種資訊。其中之一為ROM標記：Ve114。ROM標記：Ve114亦稱為物理指數(Physical Index)，為不可覆寫之固定資訊。於引入區域102進而儲存有密碼密鑰資訊120。

密碼密鑰資訊120與上述單元密鑰產生資訊：Vu112、ROM標記：Ve114相同，藉由密鑰資訊(密鑰產生資訊)而構成，該密鑰資訊(密鑰產生資訊)用以產生對儲存於資訊記錄媒體之資料儲存區域101之加密內容111實行解碼處理的密鑰。

即，作為用以對加密內容111實行解碼處理之密鑰，其係含有例如RKB(Renewal Key Block，更新密鑰塊)121以及加密碟片密鑰EKm(Kd)122之資訊，RKB(Renewal Key Block)121係為獲得作為對應儲存於資訊記錄媒體之內容的密鑰而設定之媒體密鑰：Km所必需之密碼密鑰塊，加密碟片密鑰EKm(Kd)122使用碟片密鑰：Kd加密作為適用於加

密內容111之解碼處理的密鑰即媒體密鑰： K_m 。再者， $E_{K_a}(b)$ 係表示使用密鑰： K_a 加密資料： b 的資料。

RKB(Renewal Key Block)¹²¹係依據作為廣播加密系統方式之一態樣而為人所知之樹狀構造之密鑰配信方式而產生的密碼密鑰塊，係可藉由使用配置於資訊處理裝置之裝置密鑰的解碼處理而獲得媒體密鑰： K_m 的密碼密鑰塊，該資訊處理裝置係保存利用資訊記錄媒體實行內容再生/記錄之合法許可證的用戶機器。藉由變換密碼密鑰塊：RKB之構成資料，可篩選可獲得媒體密鑰： K_m 之用戶機器。

管理中心於判定實行內容再生/記錄之裝置(用戶機器或再生應用程式)為非法之情形時，變換RKB之構成，可實現無法通過非法機器獲得媒體密鑰： K_m 。再者，被判定為非法之裝置作為Revoke(無效)裝置而登錄於管理中心。管理中心保持裝置之登錄資訊並適當更新。

於引入區域102進而儲存有登錄資訊130。登錄資訊130係用以判斷對內容實行再生或記錄處理之裝置即驅動器或PC等主機、主機應用程式等之公開密鑰證書有無有效性的資訊，即含有以下證書之資訊：認定裝置群列表(ADGL：ADGC List)¹³²，其設定為作為記錄有裝置之登錄資訊之認定裝置證書的認定裝置群證書(ADGC：Authorized Device Groups Certificate)之集合；以及ADGL資訊證書(AIC：ADGL Information Certificate)¹³¹，其作為儲存有登錄於認定裝置群列表(ADGL)之裝置數或作為無效(Revoke)裝置而登錄之數量、即無效(Revoke)裝置數之至少若干裝置數資

料的裝置數資料證書。

關於 ADGL 資訊證書 (AIC)131 與認定裝置群列表 (ADGL: ADGC List)132 之詳細內容，進而於以下加以說明。再者，ROM 標記：Ve114、密碼密鑰資訊 120、登錄資訊 130 無須一定儲存於引入區域 102，亦可儲存於資料區域 101。

於再生來自資訊記錄媒體 100 之資料或對資訊記錄媒體 100 實行資料記錄處理時，實行內容之記錄或再生處理的裝置具體為：

(a) 安裝有資訊記錄媒體 100 且實行資料記錄或讀取的驅動器；

(b) 實行與驅動器之資料輸出入且再生內容或產生記錄內容之主機。

於上述 (a) 與 (b) 之裝置間實行相互認證，確認各裝置為正當裝置後，允許於裝置間輸出入內容。於該相互認證中實行公開密鑰密碼方式之認證處理。

於公開密鑰密碼方式之認證處理中，必需相互確認驅動器與主機各裝置所保持之公開密鑰證書的有效性。於判定該公開密鑰證書之有效性時，可使用認定裝置群證書 (ADGC) 之登錄資訊。然而，認定裝置群證書 (ADGC) 伴隨裝置登錄資訊之變化適當更新，隨時發行最新版本。

當利用過期之認定裝置群證書 (ADGC) 實行認證處理時，會產生依據將無效 (Revoke) 之裝置判為有效裝置之誤認定，將內容輸出至非法裝置的情形。因此，為排除非法利用內容之可能性，必須利用最新之認定裝置群證書

(ADGC)實行認證處理。於本發明之構成中，為判定認定裝置群證書(ADGC)有無過期，使用ADGL資訊證書(AIC)。關於該處理之詳細內容將於以下加以說明。

接著，關於儲存於資訊記錄媒體100之加密內容111的記錄構成，參照圖6~圖8加以說明。圖6(a)係儲存於資訊記錄媒體之資料記錄構成。18位元組之用戶控制資料(UCD：User Control Data)與含有實際AV內容資料等之2048位元組的用戶資料(User Data)作為一個扇區資料而構成。

如圖6(b)所示，例如用戶資料3扇區份6144位元組之資料作為一個組塊密碼處理單位之1單元(1AU：Aligned Unit)即組塊而設定。6144位元組之資料相當於32TS(傳輸串流)封包。再者，組塊之設定單位並非僅限於設為3扇區份6144位元組之資料的方式，亦可為將1扇區份2048位元組之資料設定為一個密碼處理單位即組塊的方式等各種設定。

如圖6(c)所示，儲存對應內容之複製控制資訊CCI(Copy Control Information)之用戶資料以2 K(2048)位元組單位加密而記錄。

再者，自加密對象中去除18位元組之用戶控制資料(User Control Data)，僅加密記錄用戶資料。

圖7表示一個扇區資料之構成。一個扇區資料含有18位元組之用戶控制資料(UCD：User Control Data)與2048位元組之用戶資料(User Data)。

用戶控制資料(UCD：User Control Data)亦稱為扇區標頭，於其一部分記錄有扇區單位之輸出控制資訊(Output

Control Information)151。

輸出控制資訊151設定為含有匯流排保護旗標(Bus Protection Flag)之資訊，匯流排保護旗標(Bus Protection Flag)係對應之扇區資料(用戶資料)之轉送控制資訊，即例如自安裝有資訊記錄媒體之驅動器向主機(PC)等資訊處理裝置輸出的控制資訊。

圖8表示記錄於用戶控制資料(UCD：User Control Data)中之輸出控制資訊151的詳細構成。輸出控制資訊151記錄於用戶控制資料(UCD：User Control Data)之1位元組(8位元)資料中。

位元6~0之位元為儲備區域，

位元7之1位元設定為匯流排保護旗標(Bus Protection Flag)。匯流排保護旗標(Bus Protection Flag)作為判斷是否控制資訊記錄媒體之讀出內容的判定資訊而利用。具體的是，例如設定為

匯流排保護旗標(Bus Protection Flag)=1：有輸出制限、以及匯流排加密

匯流排保護旗標(Bus Protection Flag)=0：無輸出制限。

再者，匯流排加密為於驅動器與主機間傳送內容時實行之加密處理，具體如下所述。

[2.內容再生處理概要]

接著，關於儲存於上述資訊記錄媒體之內容的再生處理加以說明。儲存於資訊記錄媒體之內容的再生態樣存在兩種態樣。第1態樣係安裝有資訊記錄媒體，自資訊記錄媒體

讀取資料之機器自身實行再生處理的態樣，第2態樣係將自資訊記錄媒體讀取資料之驅動器與實行再生處理之主機(PC)等再生處理裝置作為不同機器而構成，驅動器裝置與再生處理裝置間藉由資料轉送用匯流排而連接，介以連接匯流排實行資料轉送而實行再生處理的態樣。

首先，關於安裝有資訊記錄媒體，自資訊記錄媒體讀取資料之機器自身實行再生處理的處理流程，參照圖9加以說明。

驅動器兼用再生機器300安裝儲存有加密內容206之資訊記錄媒體200，實行資料之讀取、密鑰產生、內容解碼等各種密碼處理而輸出內容。

於資訊記錄媒體200中儲存有先前參照圖5所說明之各種資訊，即：登錄資訊201，其作為用以依據公開密鑰密碼方式之相互認證以及密鑰交換處理(AKE：Authentication and Key Exchange)的登錄裝置列表；RKB202，其作為儲存有媒體密鑰：Km之密碼密鑰塊；加密碟片密鑰：EKm(Kd)203，其以媒體密鑰：Km加密碟片密鑰：Kd；ROM標記：Ve204；單元密鑰產生資訊：Vu205；以及加密內容206。

關於驅動器兼用再生機器300之處理加以說明。驅動器兼用再生機器300於步驟S101中，使用預先儲存於機器內之裝置密鑰：Kdev301，實行作為密碼密鑰塊之RKB202的解碼處理，自RKB202中獲得媒體密鑰：Km。再者，僅被認可利用內容之機器可自RKB202獲得媒體密鑰：Km，如上所述使用作為非法機器而無效之機器所具有之裝置密鑰無法

解碼RKB，無法獲得媒體密鑰：Km。

當於步驟S101中成功獲得媒體密鑰：Km時，接著於步驟S102中使用所獲得之媒體密鑰：Km，對自資訊記錄媒體200獲得之加密碟片密鑰：EKm(Kd)203實行解碼處理，獲得碟片密鑰：Kd。

接著於步驟S103中，依據所獲得之碟片密鑰：Kd與自資訊記錄媒體200獲得之ROM標記：Ve204實行密鑰產生處理例如依據AES密碼算法之密鑰產生處理，產生嵌入密鑰：Ke。

關於依據AES密碼算法之密鑰產生處理之詳細內容，參照圖10加以說明。如圖10所示，依據AES密碼算法之密鑰產生為以下處理：於AES密碼處理組塊311中，對於輸入值實行使用密碼密鑰之AES密碼處理，輸出該輸出與輸入值之排他邏輯和(XOR)演算結果。於圖9之步驟S103中，實行將輸入值設為自資訊記錄媒體200取得之ROM標記：Ve204，將適用密鑰設為碟片密鑰：Kd之密鑰產生處理，獲得作為輸出值之嵌入密鑰：Ke。

接著，於步驟S104中，依據所獲得之嵌入密鑰：Ke與自資訊記錄媒體200獲得之單元密鑰產生資訊：Vu205實行密鑰產生處理，產生單元密鑰：Ku。該密鑰產生處理作為依據參照圖10說明之AES密碼算法的密鑰產生處理而實行。Vu205藉由檔案"Unit__Key__Gen__Value. inf"可對於複數個單元之各單元定義各自之值，此處繼續對於其中之一個單元加以說明。

接著，於步驟S105中，實行使用所產生之單元密鑰Ku之加密內容206的解碼處理，輸出內容。

就步驟S105中使用單元密鑰Ku之加密內容206的解碼處理，參照圖11加以詳細說明。

加密內容206以特定資料單位之組塊單位加密，儲存於資訊記錄媒體200。如圖11所示，例如6144位元組之扇區資料以每16位元組之組塊而加密。

就解碼處理之步驟加以說明。首先，自6144位元組之扇區資料獲得前部之16位元組資料，於AES密鑰產生處理組塊[AES__G]321中，依據AES密碼算法實行密鑰產生處理。接著，與先前參照圖10說明之處理相同。將AES密鑰產生處理組塊321之輸出設為組塊密鑰：Kb，使用該組塊密鑰：Kb，於AES解碼處理組塊[AES__D]322中實行下一16位元組資料之解碼處理。

於AES解碼處理組塊[AES__D]322中，輸入扇區資料之第2個16位元組資料與初期值：IVa之排他邏輯和(XOR)結果，依據使用組塊密鑰：Kb之AES密碼算法實行解碼處理，獲得16位元組組塊資料之解碼資料，並且設為使用於下一組塊之解碼的輸入值。以下，重複實行同樣處理，可獲得解碼扇區資料323。再者，初期值：IVa為預先設定之常數。IVa亦有設定為例如可自對應扇區資料之用戶控制資料或用戶資料獲得之值的情形。

於圖9之步驟S105中，如此使用單元密鑰：Ku，實行組塊單位之解碼處理，輸出經解碼之內容。

如此，於一個機器內對來自資訊記錄媒體之資訊實行讀取與再生處理時，洩漏內容之可能性小，產生侵犯內容之著作權的問題之可能性亦小。然而，先前如參照圖2~4所說明般，於自安裝有資訊記錄媒體之驅動器，介以匯流排向PC等機器輸出內容而實行再生處理時，或自PC等機器向驅動器輸入內容而記錄於資訊記錄媒體之處理構成時，會產生各種問題。

根據本發明之構成，於如此於安裝有資訊記錄媒體之驅動器與介以匯流排連接的PC等主機機器間輸出入內容的構成中，亦可實現安全的資料轉送，防止內容之非法利用。

[3.伴隨驅動器與主機間之內容轉送的處理]

以下，就伴隨驅動器與主機間之內容轉送的處理加以詳細說明。首先，參照圖12，以下就資訊記錄媒體、驅動器、PC等主機機器側實行資料再生或資料記錄之機器或具有應用程式等之主機所保持之各種密鑰資訊以及證書加以說明。

驅動器400、主機500分別儲存有依據公開密鑰密碼方式而儲存有公開密鑰之公開密鑰證書(PKC: Public Key Certificate)以及秘密密鑰(KS)。如圖12所示，驅動器400保持有驅動器之公開密鑰證書(PKC-D)403以及秘密密鑰(KS-D)402，主機500保持有主機對應之公開密鑰證書(PKC-H)503以及秘密密鑰(KS-H)502。

資訊記錄媒體200、驅動器400以及主機500除公開密鑰證書(PKC)以及秘密密鑰(KS)之外，亦具有作為裝置數資料證

書之ADGL資訊列表(AIC：ADGL Information List)。即，資訊記錄媒體200具有AIC-DISC251，驅動器400具有AIC-D411，主機500具有AIC-H511。再者，將資訊記錄媒體之保持資訊表示為(-DISC)，將驅動器之保持資訊表示為(-D)，將主機之保持資訊表示為(-H)。

資訊記錄媒體200與主機500進而儲存有作為認定裝置證書之集合的認定裝置群列表(ADGL：Authorized Device Groop List)。即，資訊記錄媒體200儲存有ADGL-DISC252，主機500保持有ADGL512。認定裝置群列表(ADGL)為由包含複數個認定裝置群證書(ADGC：Authorized Device Groop Certificate)之集合的列表。

再者，圖12所示之各資料於資訊記錄媒體作為資料記錄區域或引入區域之記錄資料而保持，於驅動器400、主機500則保持於非揮發性記憶體。

該等各證書，即，

公開密鑰證書(PKC)、

認定裝置群證書(ADGC)以及認定裝置群列表(ADGL)、

ADGL資訊證書(AIC)

之詳細構成，參照圖13，以下加以說明。圖13(a)表示各證書之共通構成，圖13(b)係說明設定於各證書中之新資訊與證書之對應的圖。

如圖13(a)所示，公開密鑰證書(PKC)、認定裝置群證書(ADGC)、ADGL資訊證書(AIC)皆儲存有

(a)證書型(Certificate Type)

(b)證書資料(Certificate Data)

(c)電子署名(Signature)

之各資料。

(a)證書型(Certificate Type)如圖 13(b)所示，

1：公開密鑰證書(PKC)、

2：認定裝置群證書(ADGC)、

3：ADGL資訊證書(AIC)

一般根據各證書設定不同型編號。依據型編號，可判斷為何種證書。

(b)證書資料(Certificate Data)中儲存有相應公開密鑰證書(PKC)、認定裝置群證書(ADGC)以及ADGL資訊證書(AIC)之各證書的資料。關於該等，以下參照圖 14加以詳細說明。

(c)電子署名(Signature)係作為各證書之發行實體的管理中心之電子署名，即使用管理中心之秘密密鑰而產生之署名資料，係對於(a)證書型(Certificate Type)與(b)證書資料(Certificate Data)，使用管理中心之秘密密鑰而產生之署名資料。

依據署名資料，可對證書執行篡改驗證、正當性確認。即，藉由使用被公開之管理中心之公開密鑰，可對證書執行篡改驗證、正當性確認。

以下，就儲存於各證書之證書資料，參照圖 14~圖 16加以詳細說明。首先，參照圖 14就公開密鑰證書(PKC)之資料構成加以說明。

圖 14(a)表示公開密鑰證書(PKC)之證書資料的例。圖 14(b)

表示使用橢圓密碼之公開密鑰證書(PKC)之資料構成例。

如圖 14(a)所示，於公開密鑰證書(PKC)之證書資料中含有證書ID、公開密鑰以及其他資訊。例如驅動器自管理中心接收儲存有對應驅動器之公開密鑰的公開密鑰證書(PKC-D)，驅動器將其儲存保持於例如快閃記憶體等非揮發性記憶體中。又，亦提供對應公開密鑰之秘密密鑰(KS-D)。對於主機亦提供公開密鑰證書(PKC)與秘密密鑰之組合，且保持於主機內之硬碟或快閃記憶體等非揮發性記憶體中。

公開密鑰證書(PKC)為允許公開之資料，可相應例如其他機器之要求而輸出。接收到其他機器之公開密鑰證書的機器依據附加於所接收之公開密鑰證書中的管理中心之署名，實行公開密鑰證書之篡改驗證，於確認所接收之公開密鑰證書之正當性後，自公開密鑰證書獲得公開密鑰。再者，依據管理中心之署名而執行之公開密鑰證書之篡改驗證係使用管理中心之公開密鑰而執行。管理中心之公開密鑰亦為公開之資料，例如可利用預先儲存於驅動器、主機之非揮發性記憶體等中者或介以網路或記錄媒體而接收。

可與公開密鑰證書一併向驅動器、主機提供秘密密鑰。即，對驅動器、主機分別提供公開密鑰證書(PKC)與秘密密鑰之組合，其保持於各自之記憶體內。儲存有公開密鑰之公開密鑰證書雖為允許公開之資料，但為防止洩漏至外部而將秘密密鑰安全地保持於各裝置中。

圖 14(b)表示使用橢圓密碼之公開密鑰證書(PKC)之資料構成例。儲存參照圖 13(b)說明之證書型(Certificate Type=

1)以及參照圖14(a)說明之證書ID(Certificate ID)、公開密鑰(Public Key)，對應該等儲存資料設定使用管理中心之秘密密鑰而產生之電子署名(Signature)。

圖15表示(a)認定裝置群證書(ADGC)資料、(b)使用橢圓密碼之認定裝置群證書(ADGC)資料例、(c)認定裝置群列表(ADGL)之各資料構成。如上所述，(c)認定裝置群列表(ADGL)設定為儲存有複數個認定裝置群證書(ADGC)資訊之列表。

首先，關於(a)認定裝置群證書(ADGC)資料加以說明。於(a)認定裝置群證書(ADGC)資料中含有[認定裝置群證書(ADGC)資料長]、[認定裝置群列表(ADGL)序列號]、[ADGC內之第1~最終公開密鑰證書ID]以及[認定公開密鑰證書資訊]。

認定裝置群證書(ADGC)係儲存有表示於作為內容利用機器之驅動器或主機等發行之公開密鑰證書(PKC)為有效或無效(Revoke)之資訊的認定裝置證書。即，用以確認作為內容之管理實體是否為經管理中心確認之正當裝置。

執行相互認證之裝置於自認證對象接收之認證對象之公開密鑰證書的ID於認定裝置群證書(ADGC)中作為有效ID而登錄時，判斷為認證對象保持有有效公開密鑰證書。當自認證對象接收之公開密鑰證書之ID於認定裝置群證書(ADGC)中作為無效ID而登錄時，可使認證對象之公開密鑰證書失效，判定裝置為非法。於該情形時，不進行輸出入內容等之處理。

認定裝置群證書(ADGC)亦與公開密鑰證書(PKC)相同，設定為附加管理中心之電子署名，難以篡改之證書。認定裝置群證書(ADGC)針對各群設定為例如驅動器用認定裝置群證書(ADGC)、應用程式用認定裝置群證書(ADGC)、或對應廠家A之機器之認定裝置群證書(ADGC)等。

圖 15(a)所示之認定裝置群證書(ADGC)資料為對應某個群之證書資料，作為屬於該群之證書發行對象的機器或具有應用程式等之各裝置分別儲存有公開密鑰證書ID(PKC-ID)。其為圖 15(a)之證書資料中之[第1~最終公開密鑰證書ID]。進而，儲存有對應於屬於群之裝置的[認定公開密鑰證書資訊]。[認定公開密鑰證書資訊]為可確認提供至屬於群之裝置之公開密鑰證書的有效性之資訊。其係可確認第1~最終公開密鑰證書ID各自之有效性、無效性的資訊。

執行相互認證處理時，獲得對象方之公開密鑰證書，可依據[認定公開密鑰證書資訊]確認對象方之公開密鑰證書之有效性。

認定裝置群證書(ADGC)於作為群內構成成員之裝置之登錄數產生變更，有效性、無效性之登錄資訊產生變更時，於管理中心適當更新，發行最新認定裝置群證書(ADGC)。[認定裝置群證書(ADGC)序列號]為根據每次更新而設定之不同編號。例如設定為每當更新處理則增加數值之序列號。

認定裝置群證書(ADGC)中進而儲存有AIC資料。AIC資料係與參照圖 16說明之儲存於ADGL資訊證書(AIC)中之資

訊相同的資訊，為登錄於作為複數個認定裝置群證書(ADGC)之集合的認定裝置群列表(ADGL)中之全部登錄裝置數或無效化(Revoke)裝置數中之至少一種資料。即，AIC資料為

(A)登錄於ADGL之全部登錄裝置數

(B)登錄於ADGL之全部非法裝置數

中之至少一種資訊。

圖 15(c)之認定裝置群列表(ADGL)為設定為複數個認定裝置群證書(ADGC)之集合的登錄列表，儲存有列表資料長、上述AIC資料、作為列表登錄之認定裝置群證書(ADGC)數，進而儲存有認定裝置群證書(ADGC)資訊。

圖 15(b)表示使用橢圓密碼之認定裝置群證書(ADGC)資料例。儲存參照圖 13(b)說明之證書型(Certificate Type=2)以及參照圖 15(a)說明之[認定裝置群證書(ADGC)資料長]、[認定裝置群證書(ADGC)序列號]、[AIC資料]、[第1~最終公開密鑰證書(PKC)ID]、以及[認定公開密鑰證書資訊]，對應該等儲存資料設定使用管理中心之秘密密鑰而產生之電子署名(Signature)。

(a)認定裝置群證書(ADGC)以及(c)認定裝置群列表(ADGL)相應登錄裝置之變更、登錄裝置之有效化、無效化等變更處理，而於管理中心隨時更新。[ADGL序列號]為根據每次更新而設定之不同編號。

圖 16為說明作為裝置數資料證書發揮機能之ADGL資訊證書(AIC)的圖。圖 16(a)表示ADGL資訊證書(AIC)之證書資

料構成，圖 16(b)表示使用橢圓密碼之 ADGL 資訊證書(AIC)之資料構成例。

如圖 16(a)所示，於 ADGL 資訊證書(AIC)之證書資料中儲存有[ADGL 序列號]與[AIC 資料]。ADGL 序列號為該時刻發行之最新的對應認定裝置群列表(ADGL)之序列號。序列號為以例如相應發行認定裝置群列表(ADGL)每次遞增一個之方式而設定的編號。

[AIC 資料]為該時刻發行之最新的對應認定裝置群列表(ADGL)之

(A)登錄於 ADGL 之全部登錄裝置數

(B)登錄於 ADGL 之全部無效裝置數

中之至少一種資訊。

於利用資訊記錄媒體(碟片)再生或記錄資料時，於輸出入資料之裝置間例如驅動器與主機間執行相互認證。於該相互認證之處理中，必須執行雙方公開密鑰證書(PKC)之有效性判定處理。於該 PKC 有效性判定時，參照包含於認定裝置群列表(ADGL)中之認定裝置群證書(ADGC)的認定公開密鑰證書資訊。

然而，認定裝置群證書(ADGC)以及認定裝置群列表(ADGL)相應登錄裝置之變更、登錄裝置之有效化、無效化等變更處理，而於管理中心隨時更新。因此，使用過期 ADGC 執行有效性判定處理時，會產生向已失效之裝置輸出內容之問題。

為防止此種問題，於本發明中，使用[認定裝置群列表

(ADGL) 序列號] 或 [AIC 資料] 中之任一種對 ADGL 以及 ADGC 執行新舊判定，且根據需要執行更新處理。進而，使用包含於經更新之認定裝置群列表 (ADGL) 中的認定裝置群證書 (ADGC) 執行相互認證處理。

圖 17 表示資訊記錄媒體、驅動器、主機中之各證書的儲存狀況。

資訊記錄媒體將含有一個以上認定裝置群證書 (ADGC) 之認定裝置群列表 (ADGL) 與 ADGL 資訊證書 (AIC) 記錄於引入區域。

驅動器將公開密鑰證書 (PKC) 儲存於非揮發性記憶體中。認定裝置群列表 (ADGL) 自資訊記錄媒體讀出且向主機轉送。進而，於認證處理過程中，自主機輸入儲存有主機之公開密鑰證書 (PKC-H) 登錄資訊的認定裝置群證書 (ADGC)，判定主機之公開密鑰證書 (PKC-H) 之有效性即主機之有效性。進而，驅動器將 ADGL 資訊證書 (AIC) 儲存於非揮發性記憶體中，且根據需要執行更新處理。更新處理係根據自資訊記錄媒體或主機輸入之 ADGL 資訊證書 (AIC)，依據新舊判定而執行。

主機將公開密鑰證書 (PKC)、認定裝置群列表 (ADGL)、ADGL 資訊證書 (AIC) 儲存於非揮發性記憶體中，且根據需要執行 ADGL、AIC 之更新處理。更新處理依據自資訊記錄媒體經由驅動器，或自主機所連接之伺服器的輸入而執行。

以下，就於主機、驅動器執行之 ADGL 資訊證書 (AIC)、認定裝置群列表 (ADGL) 之更新處理的具體態樣加以說明。

再者，驅動器

執行ADGL資訊證書(AIC)之更新，

主機執行

ADGL資訊證書(AIC)與

認定裝置群列表(ADGL)

之更新處理。再者，於認定裝置群列表(ADGL)含有一個以上認定裝置群證書(ADGC)。

再者，以下關於更新處理態樣，就

(1)依據ADGL序列號之更新處理

(2)依據AIC資料＝登錄裝置數之更新處理

(3)依據AIC資料＝無效(Revoke)裝置數之更新處理

之三種態樣，依序加以說明。

(1)依據ADGL序列號之更新處理

首先，就依據ADGL序列號執行之更新處理，參照圖18加以說明。圖18係說明於將儲存於資訊記錄媒體200之內容253介以驅動器400輸出至主機500而再生時，依據ADGL序列號更新ADGL資訊證書(AIC)以及認定裝置群列表(ADGL)，且依據更新資訊執行驅動器400與主機500間之相互認證以及密鑰交換(AKE)的處理之圖。再者，以內容之輸出方為源，內容之輸入對象為同步。該例中，驅動器400為源，主機500為同步。

首先，驅動器400讀取儲存於資訊記錄媒體200之ADGL資訊證書(AIC-DISC)251，於步驟S121中，與自身記憶體中儲存之ADGL資訊證書(AIC-D)411之ADGL序列號加以比

較。

ADGL序列號如上所述於每次更新則賦予新編號(例如遞增1)，藉由比較序列號，可對自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251與儲存於自身記憶體之ADGL資訊證書(AIC-D)411執行新舊比較。例如，

AIC-D序列No.< AIC-DISC序列No.

時，判斷為AIC-DISC新於AIC-D，此時，執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251。

再者，驅動器400於步驟S121之比較更新處理中，首先，驗證賦予至自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251的署名，確認其為未篡改ADGL資訊證書(AIC-DISC)之正當證書。該確認後，執行比較、更新。

步驟S122係於主機500執行之比較更新處理。主機500自驅動器400輸入儲存於驅動器400之記憶體的ADGL資訊證書(AIC-D)411，藉由署名驗證確認為未篡改之證書後，執行與儲存於主機500之記憶體之ADGL資訊證書(AIC-H)511的ADGL序列號之比較處理。

AIC-H序列No.< AIC-D序列No.

時，判斷為AIC-D新於AIC-H，此時，執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-H)511替換為自驅動器400輸入之ADGL資訊證書(AIC-D)411。

再者，AIC-H序列No.< AIC-D序列No.

時，關於主機儲存於記憶體之認定裝置群列表(ADGL-H)

執行更新處理。該更新處理係作為介以驅動器400置換為儲存於資訊記錄媒體200之認定裝置群列表(ADGL-DISC)，或介以網路獲得最新認定裝置群列表(ADGL)而更新等之處理而執行。

接著，驅動器400於步驟S123中輸入保持於主機500之記憶體的ADGL資訊證書(AIC-H)511，與儲存於自身記憶體之ADGL資訊證書(AIC-D)411執行ADGL序列號的比較。

AIC-D序列No. < AIC-H序列No.

時，判斷為AIC-H新於AIC-D，此時，執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自主機500讀取之ADGL資訊證書(AIC-H)511。

再者，驅動器400於步驟S123中之比較更新處理中，驗證賦予至自主機500輸入之ADGL資訊證書(AIC-H)511的署名，確認其為未被篡改之正當證書。該確認後，執行比較、更新。

驅動器400於步驟S123中之比較更新處理中，進而自主機500獲得包含於儲存於主機500之記憶體的認定裝置群列表(ADGL-H)512之儲存有主機之登錄資訊的認定裝置群證書(ADGC-H)，於署名驗證後，比較設定於認定裝置群證書(ADGC-H)之ADGL序列號與儲存於自身記憶體之ADGL資訊證書(AIC-D)411之ADGL序列號。若

ADGC-H序列No. < AIC-D序列No.

時，則判斷為主機僅具有不對應AIC-D序列No.之過期版本之認定裝置群證書，驅動器不進入相互認證處理

(AKE)，而停止處理。

於步驟S123中，驅動器400於判斷為

ADGC-H序列No.AIC-D序列No.

時，進入下一步驟S124。

於步驟S124中，於驅動器400與主機500間執行相互認證以及密鑰交換(AKE)處理，於該處理中產生通話密鑰Ks。進而，作為內容之密碼密鑰，驅動器400產生匯流排密鑰(Kbus)，使用匯流排密鑰(Kbus)加密內容253(步驟S125)，輸出至主機500。進而使用通話密鑰Ks加密匯流排密鑰(步驟S126)，輸出至主機500。

主機500於步驟S127中，使用通話密鑰Ks執行解碼處理，獲得匯流排密鑰(Kbus)，於步驟S128中，藉由使用匯流排密鑰執行解碼處理而獲得內容。再者，關於步驟S124以下之相互認證以及內容之轉送處理，進而於以下加以詳細說明。

於本處理例中，構成為依據賦予至ADGL資訊證書(AIC)以及認定裝置群證書(ADGC)之ADGL序列號判定各證書之新舊，於確認ADGL資訊證書(AIC)或認定裝置群證書(ADGC)新於自身裝置所保持之證書時執行更新，依據被更新之認定裝置群證書(ADGC)判定裝置之有效性，故而可防止依據過期認定裝置群證書(ADGC)之認證，排除非法利用內容之可能性。

(2)依據AIC資料＝登錄裝置數之更新處理

接著，參照圖19，就將AIC資料設定為登錄於認定裝置群

列表(ADGL)之裝置數時，依據登錄裝置數執行更新的處理例加以說明。圖19係說明於將儲存於資訊記錄媒體200之內容253介以驅動器400輸出至主機500再生時，依據AIC資料(登錄裝置數)更新ADGL資訊證書(AIC)以及認定裝置群列表(ADGL)，且依據更新資訊執行驅動器400與主機500間之相互認證以及密鑰交換(AKE)的處理之圖。再者，內容之輸出方為源，內容之輸入對象為同步，該例中，驅動器400為源，主機500為同步。

首先，驅動器400於步驟S131中讀取儲存於資訊記錄媒體200之ADGL資訊證書(AIC-DISC)251，將該AIC資料(登錄裝置數)與自身記憶體中儲存之ADGL資訊證書(AIC-D)411之AIC資料(登錄裝置數)加以比較。

AIC資料(登錄裝置數)基本上設定為隨每次更新而增加，將AIC資料(登錄裝置數)具有較大之值者判定為最新。例如，

AIC-D之AIC資料 < AIC-DISC之AIC資料

時，判斷為AIC-DISC新於AIC-D，驅動器400執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251。

再者，驅動器400於步驟S131之比較更新處理中，首先，驗證賦予至自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251的署名，確認其為未篡改ADGL資訊證書(AIC-DISC)之正當證書。該確認後，執行比較、更新。

步驟S132係於主機500執行之比較更新處理。主機500自驅動器400輸入儲存於驅動器400之記憶體之ADGL資訊證書(AIC-D)411，藉由署名驗證確認為未篡改之證書後，執行與儲存於主機500之記憶體之ADGL資訊證書(AIC-H)511的AIC資料(登錄裝置數)之比較處理。

AIC-H之AIC資料 < AIC-D之AIC資料

時，判斷為AIC-D新於AIC-H，此時，主機500執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-H)511替換為自驅動器400輸入之ADGL資訊證書(AIC-D)411。

再者，AIC-H之AIC資料 < AIC-D之AIC資料

時，主機就儲存於記憶體之認定裝置群列表(ADGL-H)執行更新處理。該更新處理係作為介以驅動器400置換為儲存於資訊記錄媒體200之認定裝置群列表(ADGL-DISC)，或介以網路獲得最新認定裝置群列表(ADGL)而更新等之處理而執行。

進而，驅動器400於步驟S133中輸入保持於主機500之記憶體的ADGL資訊證書(AIC-H)511，與儲存於自身記憶體之ADGL資訊證書(AIC-D)411執行AIC資料(登錄裝置數)的比較。

AIC-D之AIC資料 < AIC-H之AIC資料

時，判斷為AIC-H新於AIC-D，此時，執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自主機500輸入之ADGL資訊證書(AIC-H)511。

再者，驅動器400於步驟S133中之比較更新處理中，驗證

賦予至自主機500輸入之ADGL資訊證書(AIC-H)511的署名，確認其為未被篡改之正當證書。該確認後，執行比較、更新。

驅動器400於步驟S133中之比較更新處理中，進而自主機500獲得包含於儲存於主機500之記憶體之認定裝置群列表(ADGL-H)512之儲存有主機登錄資訊的認定裝置群證書(ADGC-H)，於署名驗證後，比較設定於認定裝置群證書(ADGC-H)之AIC資料(登錄裝置數)與儲存於自身記憶體之ADGL資訊證書(AIC-D)411之AIC資料(登錄裝置數)。於該比較中，

ADGC-H之AIC資料 < AIC-D之AIC資料

時，則判斷為主機僅具有不對應AIC-D之AIC資料的過期版本認定裝置群證書，驅動器不進入相互認證處理(AKE)，而停止處理。

於步驟S133中，驅動器400判斷為

ADGC-H之AIC資料 $\geq$ AIC-D之AIC資料

時，進入下一步驟S134。

步驟S134~S138中，執行驅動器400與主機500間之相互認證以及密鑰交換(AKE)處理、驅動器400側之內容、匯流排密鑰之發送處理、以及主機500側之資料接收、解碼處理的該等處理與圖18相同，以下加以詳細說明。

本處理例中，將登錄裝置數作為賦予至ADGL資訊證書(AIC)以及認定裝置群證書(ADGC)之AIC資料而使用於各證書之新舊判定。作為AIC資料之登錄裝置數隨證書更新而

增加或不變，但多數情形時會增加登錄裝置數，僅於失效(無效)之無效裝置被更新時為不變。不變時無需更新，例如可減少作為驅動器400或主機500之證書儲存用之非揮發性記憶體而使用的快閃記憶體之覆寫次數。根據上述序列號執行新舊判定時，即使登錄裝置數不變，於序列號變更時亦會全部更新，故而會有快閃記憶體之使用頻率增多之問題。

其中，依據該AIC資料即登錄裝置數執行證書之新舊判定的構成中，於例如失效(無效)裝置增加時，若使登錄裝置數不變則不會於驅動器或主機執行更新處理，故而失效(無效)裝置增加時，必然需要增加登錄裝置數之運用管理。於增加無效化(無效)裝置時，即使於登錄裝置數未實際增加時，例如藉由設定虛設登錄裝置等之處理而更新登錄數，使運用成為可能。

(3)依據AIC資料＝無效(Revoke)裝置數之更新處理

接著，參照圖20，將AIC資料設為登錄於認定裝置群列表(ADGL)之裝置中已失效(無效)之無效裝置數時，關於依據AIC資料即無效裝置數執行更新處理時之處理加以說明。圖20係說明於將儲存於資訊記錄媒體200之內容253介以驅動器400輸出至主機500再生時，依據AIC資料(無效裝置數)更新ADGL資訊證書(AIC)以及認定裝置群列表(ADGL)，且依據更新資訊執行驅動器400與主機500間之相互認證以及密鑰交換(AKE)的處理之圖。再者，內容之輸出方為源，內容之輸入對象為同步，該例中，驅動器400為源，主機500為

同步。

首先，驅動器400於步驟S141中讀取儲存於資訊記錄媒體200之ADGL資訊證書(AIC-DISC)251，將該AIC資料(無效裝置數)與自身記憶體中儲存之ADGL資訊證書(AIC-D)411之AIC資料(無效裝置數)加以比較。

AIC資料(無效裝置數)基本上設定為隨每次更新而增加，將AIC資料(無效裝置數)具有較大之值者判定為最新。例如，

AIC-D之AIC資料 < AIC-DISC之AIC資料

時，判斷為AIC-DISC新於AIC-D，此時，驅動器400執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251。

再者，驅動器400於步驟S141之比較更新處理中，首先，驗證賦予至自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251的署名，確認其為未篡改ADGL資訊證書(AIC-DISC)之正當證書。於該確認後，執行比較、更新。

步驟S142係於主機500執行之比較更新處理。主機500自驅動器400輸入儲存於驅動器400之記憶體的ADGL資訊證書(AIC-D)411，藉由署名驗證確認為未篡改之證書後，執行與儲存於主機500之記憶體之ADGL資訊證書(AIC-H)511的AIC資料(無效裝置數)之比較處理。

AIC-H之AIC資料 < AIC-D之AIC資料

時，判斷為AIC-D新於AIC-H，此時，主機500執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-H)511

替換為自驅動器400輸入之ADGL資訊證書(AIC-D)411。

再者，AIC-H之AIC資料 < AIC-D之AIC資料

時，主機關於儲存於記憶體之認定裝置群列表(ADGL-H)執行更新處理。該更新處理係作為介以驅動器400置換為儲存於資訊記錄媒體200之認定裝置群列表(ADGL-DISC)，或介以網路獲得最新認定裝置群列表(ADGL)而更新等之處理而執行。

進而，驅動器400於步驟S143中輸入保持於主機500之記憶體的ADGL資訊證書(AIC-H)511，與儲存於自身記憶體之ADGL資訊證書(AIC-D)411執行AIC資料(無效裝置數)的比較。

AIC-D之AIC資料 < AIC-H之AIC資料

時，判斷為AIC-H新於AIC-D，此時，驅動器400執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自主機500讀取之ADGL資訊證書(AIC-H)511。

再者，驅動器400於步驟S143中之比較更新處理中，驗證賦予至自主機500輸入之ADGL資訊證書(AIC-H)511的署名，確認其為未被篡改之正當證書。該確認後，執行比較、更新。

驅動器400於步驟S143中之比較更新處理中，進而自主機500獲得包含於儲存於主機500之記憶體的認定裝置群列表(ADGL-H)512之儲存有主機之登錄資訊的認定裝置群證書(ADGC-H)，於署名驗證後，比較設定於認定裝置群證書(ADGC-H)之AIC資料(無效裝置數)與儲存於自身記憶體之

ADGL資訊證書(AIC-D)411之AIC資料(無效裝置數)。於該比較中，

ADGC-H之AIC資料 < AIC-D之AIC資料

時，則判斷為主機僅具有不對應AIC-D之AIC資料之過期版本的認定裝置群證書，驅動器400不進入相互認證處理(AKE)，而停止處理。

於步驟S143中，驅動器400於判斷為

ADGC-H之AIC資料 $\geq$ AIC-D之AIC資料

時，進入下一步驟S144。

步驟S144~S148中，執行驅動器400與主機500間之相互認證以及密鑰交換(AKE)處理、驅動器400側之內容、匯流排密鑰之發送處理、以及主機500側之資料接收、解碼處理的該等處理與圖18相同，以下加以詳細說明。

本處理例中，將無效裝置數作為賦予至ADGL資訊證書(AIC)以及認定裝置群證書(ADGC)之AIC資料而使用於各證書之新舊判定。作為AIC資料之無效裝置數會隨證書更新而增加或不變，但多數情形時會僅增加登錄裝置數而無效裝置數不變，僅於失效(無效)之無效裝置被更新時增加。不變時無需更新，例如可減少作為驅動器400或主機500之證書儲存用非揮發性記憶體而使用的快閃記憶體之覆寫次數。根據上述序列號執行新舊判定時，即使無效裝置數不變，於序列號變更時亦會全部更新，故而會有快閃記憶體之使用頻率增多之問題。

參照圖21、圖22，就參照圖19、圖20說明之依據AIC資料

執行 ADGL 資訊證書 (AIC) 以及認定裝置群證書 (ADGC) 之新舊判定處理中，於驅動器以及主機執行之比較更新處理 1~3 (參照圖 19、圖 20) 的處理步驟加以說明。

圖 21(a) 表示驅動器 400 實行之比較更新處理 1，即圖 19 所示之步驟 S131 與圖 20 所示之步驟 S141 之處理流程的流程。驅動器於步驟 S151 中讀出 ADGL 資訊證書 (AIC-DISC)，於步驟 S152 中執行 ADGL 資訊證書 (AIC-DISC) 之署名驗證。無法藉由署名驗證確認證書之正當性時 (S153: No)，停止其後之處理。此時不執行內容轉送處理。

可藉由署名驗證確認證書之正當性 (S153: Yes) 時，於步驟 S154 中，比較自資訊記錄媒體獲得之 ADGL 資訊證書 (AIC-DISC) 之 AIC 資料 (登錄裝置數或無效裝置數) 與儲存於自身記憶體之 ADGL 資訊證書 (AIC-D) 之 AIC 資料 (登錄裝置數或無效裝置數)。

AIC-D 之 AIC 資料 < AIC-DISC 之 AIC 資料

時，判斷為 AIC-DISC 新於 AIC-D，進入步驟 S155，驅動器執行更新處理，將儲存於自身記憶體之 ADGL 資訊證書 (AIC-D) 替換為自資訊記錄媒體讀取之 ADGL 資訊證書 (AIC-DISC)。上述條件無法滿足

AIC-D 之 AIC 資料 < AIC-DISC 之 AIC 資料

時，判定為無需將儲存於自身記憶體之 ADGL 資訊證書 (AIC-D) 更新為自資訊記錄媒體讀取之 ADGL 資訊證書 (AIC-DISC)，不執行更新處理而結束處理。

接著，就圖 21(b) 之驅動器 400 執行之比較更新處理 2，即

圖 19 所示之步驟 S133 與圖 20 所示之步驟 S143 之處理流程加以說明。驅動器於步驟 S161 中，接收到來自主機之 ADGL 資訊證書 (AIC-H) 之轉送要求後，於步驟 S162 中自主機接收 ADGL 資訊證書 (AIC-H)。於步驟 S163 中，執行 ADGL 資訊證書 (AIC-H) 之署名驗證，於無法藉由署名驗證確認證書之正當性 (S164：No) 時，停止其後之處理。此時不執行內容轉送處理。

可藉由署名驗證確認證書之正當性 (S164：Yes) 時，於步驟 S165 中，比較自主機獲得之 ADGL 資訊證書 (AIC-H) 之 AIC 資料 (登錄裝置數或無效裝置數) 與儲存於自身記憶體之 ADGL 資訊證書 (AIC-D) 之 AIC 資料 (登錄裝置數或無效裝置數)。

AIC-D 之 AIC 資料 < AIC-H 之 AIC 資料

時，判斷為 AIC-H 新於 AIC-D，進入步驟 S166，驅動器執行更新處理，將儲存於自身記憶體之 ADGL 資訊證書 (AIC-D) 替換為自主機獲得之 ADGL 資訊證書 (AIC-H)。上述條件無法滿足

AIC-D 之 AIC 資料 < AIC-H 之 AIC 資料

時，判定為無需將儲存於自身記憶體之 ADGL 資訊證書 (AIC-D) 更新為自主機獲得之 ADGL 資訊證書 (AIC-H)，不執行更新處理。

接著，於步驟 S167 中，確認自主機接收到認定裝置群證書 (ADGC-H) 後，於步驟 S168 中，比較設定於認定裝置群證書 (ADGC-H) 之 AIC 資料 (登錄裝置數或無效裝置數) 與儲存

於自身記憶體之ADGL資訊證書(AIC-D)之AIC資料(登錄裝置數或無效裝置數)。若

ADGC-H之AIC資料 < AIC-D之AIC資料

時，則判斷為主機僅具有不對應AIC-D之AIC資料之過期版本的認定裝置群證書，驅動器不進入相互認證處理(AKE)，而停止處理。

ADGC-H之AIC資料 < AIC-D之AIC資料

不成立時，結束比較更新處理2。

接著，就圖22(c)之驅動器500執行之比較更新處理3，即圖19所示之步驟S132與圖20所示之步驟S142之處理流程加以說明。主機於步驟S171中，對於驅動器執行ADGL資訊證書(AIC-D)之轉送要求，於步驟S172中確認自驅動器接收到ADGL資訊證書(AIC-D)，則於步驟S173中執行ADGL資訊證書(AIC-D)之署名驗證，於無法藉由署名驗證確認證書之正當性(S174：No)時，停止其後之處理。此時不執行內容轉送處理。

於步驟S173中，藉由ADGL資訊證書(AIC-D)之署名驗證確認到證書之正當性(S174：Yes)時，於步驟S175中，與儲存於主機記憶體之ADGL資訊證書(AIC-H)執行AIC資料(登錄裝置數或無效裝置數)比較處理。

AIC-H之AIC資料 < AIC-D之AIC資料

時，判斷為AIC-D新於AIC-H，此時進入步驟S176，執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-H)替換為自驅動器輸入之ADGL資訊證書(AIC-D)411。

再者，AIC-H之AIC資料 < AIC-D之AIC資料

時，主機關於儲存於記憶體之認定裝置群列表(ADGL-H)執行更新處理。該更新處理係作為介以驅動器置換為儲存於資訊記錄媒體之認定裝置群列表(ADGL-DISC)，或介以網路獲得最新認定裝置群列表(ADGL)而更新等之處理而執行。

接著，參照圖23，就於驅動器以及主機執行之比較更新處理1~3(參照圖19、圖20)之處理中，於資訊記錄媒體(碟片)、驅動器以及主機間執行之資料通信序列加以說明。

於步驟S181中，驅動器執行資訊記錄媒體(碟片)之檢測，當檢測到資訊記錄媒體時，於步驟S182中自資訊記錄媒體(碟片)之引入區域讀取ADGL資訊證書(AIC-DISC)，於步驟S183中執行比較更新處理1(圖19-S131、圖20-S141)。該比較更新處理1包含

(1)ADGL資訊證書(AIC-DISC)之署名驗證

(2)AIC-DISC之AIC資料 < AIC-D之AIC資料的確認以及依據確認而執行的更新處理。

接著，當於步驟S184中主機自驅動器獲得碟片檢測資訊時，於步驟S185中，主機向驅動器要求ADGL資訊證書(AIC-D)，於步驟S186中，主機自驅動器接收ADGL資訊證書(AIC-D)。接著，於步驟S187中，執行比較更新處理3(圖19-S132、圖20-S142)。該比較更新處理3包含

(1)ADGL資訊證書(AIC-D)之署名驗證

(2)AIC-D之AIC資料 > AIC-H之AIC資料的確認以及依據

確認而執行的更新處理。

進而，

AIC-D之AIC資料 > AIC-H之AIC資料

時，主機於步驟S188中，

為執行認定裝置群列表(ADGL)之更新處理，為獲得來自碟片之認定裝置群列表(ADGL-DISC)，而對驅動器執行認定裝置群列表(ADGL-DISC)之發送要求，驅動器於步驟S189中自碟片讀取認定裝置群列表(ADGL-DISC)，於步驟S190中發送至主機。

於步驟S191中，主機執行更新處理，將儲存於記憶體之認定裝置群列表(ADGL-H)置換為認定裝置群列表(ADGL-DISC)。該處理僅於

AIC-D之AIC資料 > AIC-H之AIC資料

時執行。再者，於主機為可連接網路之構成時，亦可自介以網路連接之伺服器獲得最新認定裝置群列表(ADGL)而更新。

AIC-D之AIC資料 < AIC-H之AIC資料

時，主機於步驟S192中，獲得儲存於記憶體之ADGL資訊證書(AIC-H)，於步驟S193中發送至驅動器。

接著，於步驟S194中，驅動器執行比較更新處理2(圖19-S133、圖20-S143)。該比較更新處理2包含

(1)ADGL資訊證書(AIC-H)之署名驗證

(2)AIC-D之AIC資料 < AIC-H之AIC資料的確認以及依據確認而執行的更新處理。

進而，驅動器於步驟S195中，自主機接收包含於認定裝置群列表(ADGL-H)之儲存有主機登錄資訊的認定裝置群證書(ADGC-H)，於步驟S196中決定

(1)認定裝置群證書(ADGC-H)之署名驗證

(2)AIC-D之AIC資料 > ADGC-H之AIC資料之確認以及依據確認決定認證處理的執行、停止。

AIC-D之AIC資料 > ADGC-H之AIC資料

成立時，成為主機擁有過期認定裝置群證書(ADGC-H)，停止處理。

接著，參照圖24，就匯流排連接驅動器與主機，伴隨內容轉送之再生處理的整體處理流程加以說明。

圖24表示資訊記錄媒體200，安裝資訊記錄媒體200而自資訊記錄媒體200讀取資料之驅動器400，以及介以連接匯流排自驅動器400輸入內容之外的其他資料，且依據應用程式執行內容再生處理之主機500的處理。再者，連接驅動器400與主機500之匯流排可為例如藉由ATAPI-BUS構成之連接匯流排。再者，亦可為USB等其他連接匯流排。

於資訊記錄媒體200中儲存有與先前參照圖9所說明相同的圖5所示之各種資訊，即：登錄資訊201，其作為用以依據公開密鑰密碼方式之相互認證以及密鑰交換處理(AKE: Authentication and Key Exchange)的登錄裝置列表；RKB202，其作為儲存有媒體密鑰：Km之密碼密鑰塊；加密碟片密鑰：EKm(Kd)203，其以媒體密鑰：Km加密碟片密鑰：Kd；ROM標記：Ve204；單元密鑰產生資訊：Vu205；

以及加密內容 206。登錄資訊 201 中含有 ADGL 資訊證書 (AIC-DISC) 與認定裝置群列表 (ADGL-DISC)。

驅動器 400 中儲存有依據公開密鑰密碼方式之管理中心之公開密鑰 [Kp__kic]401，依據公開密鑰密碼方式對應驅動器之秘密密鑰 [Ks__drive]402，儲存有依據公開密鑰密碼方式對應驅動器之公開密鑰的公開密鑰證書 [Cert__drive]403，以及裝置密鑰 [Kdev]404，進而儲存有 ADGL 資訊證書 (AIC-D)411。

另一方面，於主機 500 中儲存有依據公開密鑰密碼方式之管理中心之公開密鑰 [Kp__kic]501，主機秘密密鑰 [Ks__host]502，儲存有主機公開密鑰之主機公開密鑰證書 [Cert__host]503，進而儲存有 ADGL 資訊證書 (AIC-host)511 與認定裝置群列表 (ADGL-host)512。

首先，步驟 S201、S301 中，於驅動器 400 與主機 500 間執行登錄資訊更新、相互認證以及密鑰交換 (AKE : Authentication and Key Exchange) 處理。

登錄資訊更新為先前參照圖 18~圖 23 所說明之處理，ADGL 資訊證書 (AIC) 與認定裝置群列表 (ADGL) 之更新處理以

- (1) 依據 ADGL 序列號之更新處理
- (2) 依據 AIC 資料 = 登錄裝置數之更新處理
- (3) 依據 AIC 資料 = 無效 (Revoke) 裝置數之更新處理

中之任一態樣而實行。

繼續該登錄資訊之更新處理，於驅動器 400 與主機 500 間

執行相互認證以及密鑰交換(AKE: Authentication and Key Exchange)。關於相互認證以及密鑰交換(AKE: Authentication and Key Exchange)處理之詳細序列，參照圖25加以說明。該處理可使用例如利用規定於ISO/IEC9798-3之公開密鑰算法之相互認證、利用規定於ISO/IEC11770-3之公開密鑰算法之密鑰產生處理方式而執行。再者，作為利用公開密鑰之相互認證方式而實際使用之方式，例如有揭示於DTCP(Digital Transmission Content Protection, 數字傳輸內容保護)Specification Volume 1(Informational Version, 資訊版本)中之方法。

如圖25所示，就處理流程加以說明。於步驟S401中，主機對驅動器發送因隨機產生處理而產生之激發資料[C__host]與公開密鑰證書[Cert__host]。公開密鑰證書[Cert__host]為圖14(b)所示之公開密鑰證書。

接收該資料之驅動器側藉由對公開密鑰證書[Cert__host]之署名驗證處理，驗證公開密鑰證書[Cert__host]之正當性。署名驗證處理係使用驅動器所保持之管理中心之公開密鑰[Kp__kic]401(參照圖24)而執行。

當驗證為公開密鑰證書[Cert__host]具有正當性時，自公開密鑰證書[Cert__host]獲得公開密鑰證書ID，參照儲存有主機之登錄資訊之認定裝置群證書(ADGC)之認定公開密鑰證書資訊，確認主機之公開密鑰證書ID是否為未失效(無效)之有效ID。此處使用之認定裝置群證書(ADGC)為於先前之登錄資訊更新處理中，執行各種證書之新舊比較而更

新的證書。

無法確認公開密鑰證書 [Cert__host] 之正當性或依據認定裝置群證書 (ADGC) 判斷為主機未登錄或雖登錄但已失效(無效)時，執行錯誤資訊之通知等，結束處理。停止其後之內容輸出、再生處理。

當確認公開密鑰證書 [Cert__host] 之正當性，主機已登錄，且主機具有未失效(無效)之正當公開密鑰證書時，則於步驟 S402 中，驅動器向主機發送藉由隨機產生處理而產生之激發資料 [C__drive] 與驅動器側之公開密鑰證書 [Cert__drive]。

主機執行驅動器側之公開密鑰證書 [Cert__drive] 之署名驗證。署名驗證處理係使用主機側所保持之管理中心之公開密鑰 [Kp__kic] 501 (參照圖 24) 而執行。

當確認為公開密鑰證書 [Cert__drive] 具有正當性時，自公開密鑰證書 [Cert__drive] 獲得公開密鑰證書 ID，參照儲存有驅動器之登錄資訊之認定裝置群證書 (ADGC) 的認定公開密鑰證書資訊，確認驅動器之公開密鑰證書 ID 是否已登錄，且是否為未失效(無效)之有效 ID。此處使用之認定裝置群證書 (ADGC) 為於先前之登錄資訊更新處理中，執行各種證書之新舊比較而更新的證書。

無法確認公開密鑰證書 [Cert__drive] 之正當性或依據認定裝置群證書 (ADGC) 判斷為驅動器未登錄或雖登錄但已失效(無效)時，執行錯誤資訊之通知等，結束處理。停止其後之內容輸出、再生處理。

於已確認公開密鑰證書[Cert__drive]之正當性時，主機依據自驅動器接收之激發資料[C__drive]執行演算，計算出參數[A__host]，與新產生之隨機數字[R__host]一同發送至驅動器(步驟S403)。

另一方面，驅動器依據自主機接收之激發資料[C__host]執行演算，計算出參數[A__drive]，與新產生之隨機數字[R__drive]一同發送至主機(步驟S404)。

藉由該處理，驅動器、主機雙方會共有隨機數字[R__host]、[R__drive]、參數[A__host]、[A__drive]，驅動器與主機應用程式雙方依據該等共有資料產生共通之通話密鑰Ks(步驟S405)。

驅動器進而於步驟S406中，將使用通話密鑰：Ks對依據隨機而產生之匯流排密鑰：Kbus與匯流排密鑰之序列號：SEQ之連結資料：[Kbus || SEQ]，以及作為該連結資料之篡改驗證用資料而計算出之雜湊值[hash(Kbus || SEQ)]執行加密的資料：EKs[(Kbus || SEQ)、hash(Kbus || SEQ)]，發送至主機應用程式。再者，於該步驟S406之處理中，相當於圖24中步驟S206之匯流排密鑰產生處理(Generate__Kbus)與步驟S207之使用通話密鑰：Ks之匯流排密鑰之加密處理(AES__E)的處理。

匯流排密鑰：Kbus係加密內容於介以自驅動器至主機側之連接匯流排執行轉送處理時作為加密密鑰而使用之密鑰，於驅動器中依據隨機而產生。匯流排密鑰於例如碟片插入檢測後之最初相互認證中隨機產生，存在至退出碟片

或電源停止為止使用相同值之情形，或例如每次相互認證則切換為不同匯流排密鑰之情形。於該等各個相互認證中，為防止匯流排密鑰之冒充，於各匯流排密鑰轉送時附加相應之序列號。

返回圖 24，就驅動器 400 介以連接匯流排將自資訊記錄媒體獲得之內容等資料轉送至主機 500 並再生之處理流程，繼續加以說明。

當驅動器 400 結束與主機 500 之相互認證以及密鑰交換 (AKE) 時，使用保持於驅動器內之裝置密鑰：Kdev404，於步驟 S202 中將自資訊記錄媒體 200 讀出之 RKB202 作為密碼密鑰塊而執行解碼處理，自 RKB202 獲得媒體密鑰：Km。再者，僅被認可利用內容之機器可自 RKB202 獲得媒體密鑰：Km，如上所述使用作為非法機器而無效之機器所具有之裝置密鑰無法解碼 RKB，無法獲得媒體密鑰：Km。

當於步驟 S202 中成功獲得媒體密鑰：Km 時，接著於步驟 S203 中使用所獲得之媒體密鑰：Km，對自資訊記錄媒體 200 獲得之加密碟片密鑰：EKm(Kd)203 實行解碼處理，獲得碟片密鑰：Kd。

接著於步驟 S204 中，依據所獲得之碟片密鑰：Kd 與自資訊記錄媒體 200 獲得之 ROM 標記：Ve204 實行密鑰產生處理，例如依據 AES 密碼算法之密鑰產生處理，產生嵌入密鑰：Ke。依據 AES 密碼算法執行之密鑰產生處理如先前參照圖 10 之說明。

驅動器於步驟 S205 中，以先前相互認證以及密鑰交換處

理(AKE)中產生之通話密鑰： K_s 加密嵌入密鑰： K_e ，且介以連接匯流排發送至主機500。

步驟S206、以及步驟S207之處理與先前參照圖25所說明之相互認證以及密鑰交換處理(AKE)之步驟S406之處理相當，係根據隨機產生匯流排密鑰： K_{bus} (步驟S206)，將以通話密鑰： K_s 加密含有匯流排密鑰： K_{bus} 之資料(步驟S207)而產生的資料介以連接匯流排發送至主機500的處理。發送資料如先前參照圖25所說明般，為使用通話密鑰： K_s 對依據隨機而產生之匯流排密鑰： K_{bus} 與匯流排密鑰之序列號：SEQ之連結資料： $[K_{bus} \parallel \text{SEQ}]$ ，以及作為該連結資料之篡改驗證用資料而計算出之雜湊值 $[\text{hash}(K_{bus} \parallel \text{SEQ})]$ 執行加密的資料： $E_{K_s}[(K_{bus} \parallel \text{SEQ}), \text{hash}(K_{bus} \parallel \text{SEQ})]$ 。

進而，驅動器400於步驟S208中，依據包含於自資訊記錄媒體200讀取之加密內容206之用戶控制資料(UCD)的輸出控制資訊、以及於相互認證以及密鑰交換處理(AKE)處理中自主機500獲得之主機之公開密鑰證書的儲存資料，執行輸出控制，於步驟S209中，相應控制態樣使用匯流排密鑰： K_{bus} 對加密內容206加密，介以連接匯流排將產生之加密資料輸出至主機500。

自資訊記錄媒體200讀出之加密內容206為例如經加密處理之加密資料，驅動器使用匯流排密鑰： K_{bus} 對該經加密處理之資料執行再加密，輸出至主機側。藉由使用該匯流排密鑰： K_{bus} 執行再加密處理而輸出資料，僅保持有匯流排密鑰： K_{bus} 獲得認證之主機可使用匯流排密鑰： K_{bus} 執

行解碼，可藉由解碼處理獲得內容350。

即，如先前參照圖4所說明般，即使藉由通過於輸入內容之PC(主機)側切換應用程式而迂回獲得內容，或竊聽驅動器與主機間通過連接匯流排之轉送資料而獲得內容，所獲得之內容亦為藉由匯流排密鑰：Kbus而加密之資料，僅與驅動器之認證成立之特定主機應用程式保持有匯流排密鑰：Kbus，故而若不使用該特定主機應用程式，則無法對輸入內容執行解碼。僅CSS加密之解除程式無法對使用匯流排密鑰：Kbus加密之資料執行解碼，故而可防止對內容之非法利用。

如此，本發明之驅動器、主機等裝置根據依據上述新舊判定而選擇之新認定裝置群證書，對自認證對象裝置獲得之公開密鑰證書執行有效性判定處理，並且執行與認證對象裝置之相互認證以及密鑰交換(AKE)，以相互認證成立為條件，設定含有內容通信路以及使用於內容之密碼處理的密鑰通信路的安全通信路，介以該通信路執行資料通信。

關於使用匯流排密鑰：Kbus之加密內容206之加密處理態樣，參照圖26加以說明。使用匯流排密鑰：Kbus之加密內容206之加密處理例如圖26所示，係藉由使用AES-CBC模式之組塊加密處理而執行。

驅動器400對自資訊記錄媒體200讀取之加密內容，使用於驅動器中所產生之匯流排密鑰：Kbus，使用特定資料組塊單位(16位元組)執行加密處理。

首先，從自資訊記錄媒體200讀出之加密內容之構成資料

即2048位元組之扇區資料550中獲得前部16位元組資料，將其與初期值：IVb之排他邏輯和(XOR)結果輸入至AES密碼處理部[AES__E]551，依據使用匯流排密鑰：Kbus之AES密碼算法執行密碼處理，產生16位元組組塊資料之加密資料。初期值：IVb為預先設定之常數。IVb亦可自例如對應扇區資料550之用戶控制資料(UCD)中獲得。

進而，該產生資料作為於下一組塊之加密中使用之輸入值而使用。以下，針對各16位元組之組塊資料同樣地重複執行排他邏輯和(XOR)以及AES密碼處理，產生使用匯流排密鑰之加密扇區資料552，介以ATAPI-BUS等連接匯流排將該資料發送至主機500側之應用程式。於主機500側解碼該輸入加密資料，執行再生處理。

返回圖24，就主機500側之處理流程加以說明。主機500首先如上所述於步驟S301中執行與驅動器400之相互認證以及密鑰交換(AKE)，獲得通話密鑰：Ks。

接著，於步驟S302中，對於使用自驅動器介以連接匯流排而輸入之通話密鑰：Ks執行加密的嵌入密鑰：Ke即[EKs(Ke)]，執行使用通話密鑰：Ks之解碼處理，獲得嵌入密鑰：Ke。

進而，於步驟S303中，對於自驅動器介以連接匯流排而輸入之單元密鑰產生資訊：Vu，執行使用嵌入密鑰：Ke之AES密鑰產生處理(參照圖10)，產生單元密鑰：Ku。

接著，於步驟S304中，對於使用自驅動器介以連接匯流排而輸入之通話密鑰：Ks執行加密的匯流排密鑰：Kbus即

$[EKs(Kbus)]$ ，執行使用通話密鑰： Ks 之解碼處理，獲得匯流排密鑰： $Kbus$ 。

再者，如先前參照圖25所說明般，含有自驅動器發送之匯流排密鑰： $Kbus$ 之資料為使用通話密鑰： Ks 對匯流排密鑰： $Kbus$ 與匯流排密鑰之序列號： SEQ 之連結資料： $[Kbus \parallel SEQ]$ ，以及作為該連結資料之篡改驗證用資料而計算出之雜湊值 $[hash(Kbus \parallel SEQ)]$ 執行加密的資料： $EKs[(Kbus \parallel SEQ)、hash(Kbus \parallel SEQ)]$ 。

主機500之應用程式於步驟S304中，使用通話密鑰： Ks 對資料： $EKs[(Kbus \parallel SEQ)、hash(Kbus \parallel SEQ)]$ 解碼，獲得匯流排密鑰： $Kbus$ 以及匯流排密鑰之序列號： SEQ 的連結資料： $[Kbus \parallel SEQ]$ ，以及作為該連結資料之篡改驗證用資料而計算出之雜湊值 $[hash(Kbus \parallel SEQ)]$ 。

接著，於步驟S305中，計算連結資料： $[Kbus \parallel SEQ]$ 之雜湊值，與包含於來自驅動器之輸入資料中之雜湊值 $[hash(Kbus \parallel SEQ)]$ 執行比較。當兩雜湊值一致時，則判斷為連結資料： $[Kbus \parallel SEQ]$ 未被篡改，移至步驟S306之使用匯流排密鑰： $Kbus$ 之內容解碼處理。

於步驟S306中，對使用自驅動器400輸入之匯流排密鑰： $Kbus$ 再加密之加密內容執行解碼處理。

關於使用匯流排密鑰： $Kbus$ 再加密之加密內容的解碼處理，參照圖27加以詳細說明。使用匯流排密鑰： $Kbus$ 之加密內容之解碼處理例如圖27所示，係藉由使用AES-CBC模式之組塊解碼處理而執行。

主機500之應用程式對於自驅動器400介以連接匯流排而輸入之加密內容，使用自驅動器輸入之匯流排密鑰：Kbus，執行以特定資料組塊單位(16位元組)解碼之處理。

首先，自驅動器400介以連接匯流排輸入之加密內容的構成資料即2048位元組之扇區資料550中獲得前部16位元組資料，輸入至AES解碼處理部[AES__D]571，執行使用匯流排密鑰：Kbus之依據AES密碼算法之解碼處理，進而，執行與初期值：IVb之排他邏輯和(XOR)演算，獲得解碼結果。初期值：IVb為預先設定之常數。IVb亦可自例如對應扇區資料570之用戶控制資料(UCD)中獲得。

進而，16位元組單位之解碼結果資料作為於下一組塊之解碼處理中使用之輸入值而使用。以下，針對各16位元組之組塊資料同樣反覆執行AES解碼處理以及排他邏輯和(XOR)，獲得使用匯流排密鑰解除加密之扇區資料，即作為儲存於資訊記錄媒體200內之資料狀態的加密(Scramble)扇區資料572。

進而，主機500於圖24所示之步驟S307中，使用單元密鑰：Ku，對作為儲存於資訊記錄媒體200中之資料狀態的加密內容執行解碼處理。該解碼處理作為與先前參照圖11說明之處理相同的處理而執行。

根據以上處理，主機500獲得解碼內容520，對揚聲器、顯示器等輸出部執行輸出處理，執行內容再生。

如此，於對資訊記錄媒體執行資料讀取之驅動器中，構成使用匯流排密鑰：Kbus對自資訊記錄媒體讀出之經加

密處理的資料執行再加密，而輸出至主機側，因此僅於保持有匯流排密鑰：Kbus之主機側應用程式即與驅動器之相互認證成立的主機應用程式可使用匯流排密鑰：Kbus執行解碼，且可使用解碼處理利用加密內容。

因此，即使藉由通過於輸入內容之PC(主機)側切換應用程式而迂回獲得內容，或竊聽驅動器與主機間通過連接匯流排之轉送資料而獲得內容，僅與驅動器之相互認證成立且具有相同匯流排密鑰：Kbus之唯一應用程式可對藉由匯流排密鑰：Kbus而加密之資料執行解碼，故而其他應用程式例如CSS加密之解除程式無法對使用匯流排密鑰：Kbus加密之資料執行解碼，故而可防止對內容之非法利用。

接著，參照圖28、圖29，關於內容再生處理中驅動器以及主機各自之處理流程加以說明。

首先，參照圖28，就控制自驅動器向主機輸出內容的流程加以說明。

關於圖28之流程之各步驟加以說明。首先，於步驟S511中檢測資訊記錄媒體(碟片)對驅動器之插入，於步驟S512中，檢測執行經匯流排連接之主機側的內容再生處理之主機應用程式是否啟動。當以檢測到該等為條件，進入步驟S513，使來自主機側之相互認證要求待機，接收相互認證要求時，則於步驟S514執行先前說明之登錄資訊之更新處理、依據公開密鑰密碼方式之相互認證以及密鑰交換(AKE)處理。再者，登錄資訊之更新處理亦可於自驅動器接收相互認證要求之前執行。

於步驟S515中，當確認相互認證以及密鑰交換(AKE)處理結束時，進入步驟S516，驅動器執行對應匯流排密鑰： K_b 之隨機數 R 的產生處理，將該產生隨機數 R 作為匯流排密鑰： K_b 。該處理相當於圖24之步驟S206之處理。再者，於匯流排密鑰： K_b 中對應序列號，以防止匯流排密鑰之冒充。

當於步驟S517中，自主機側接收到匯流排密鑰之轉送要求時，於步驟S518中將匯流排密鑰： K_b 轉送至主機側。該處理相當於圖24之步驟S207之處理。再者，該匯流排密鑰轉送為相當於圖25之相互認證以及密鑰交換(AKE)處理之最終步驟S406的處理，驅動器產生使用通話密鑰： K_s 對匯流排密鑰： K_{bus} 與匯流排密鑰之序列號： SEQ 之連結資料： $[K_{bus} \parallel SEQ]$ ，以及作為該連結資料之篡改驗證用資料而計算出之雜湊值 $[\text{hash}(K_{bus} \parallel SEQ)]$ 執行加密的資料： $EK_s[(K_{bus} \parallel SEQ)、\text{hash}(K_{bus} \parallel SEQ)]$ ，且發送至主機側。

接著，於步驟S519中，確認無新相互認證要求，又，於步驟S520中，確認未退出資訊記錄媒體，於步驟S521中，待機至收到主機側之內容取得要求即扇區資料之讀取要求。

再者，於步驟S519中，產生新相互認證要求時，返回步驟S514執行相互認證以及密鑰交換(AKE)處理，產生新通話密鑰，發送匯流排密鑰。此時產生之匯流排密鑰為序列號：2之匯流排密鑰，成為與先前產生之匯流排密鑰(序列號1)相同的匯流排密鑰。

再者，於步驟S520中，判斷為已自驅動器退出碟片時，

返回步驟S511，設定為初期狀態，重設即刪除已產生之匯流排密鑰、通話密鑰等所有資料。

當於步驟S521中，自主機側產生對扇區資料之讀出要求時，驅動器於步驟S522中，自對應讀出對象之扇區資料的扇區標頭(用戶控制資料)讀取輸出控制資訊，判斷[匯流排保護旗標：BPF]之值。該處理相當於圖24之步驟S208之處理。

匯流排保護旗標：BPF如先前參照圖8所說明般，為

BPF = 1：有輸出制限，有匯流排加密，

BPF = 0：無輸出制限

之設定資訊。

當於步驟S522中，判定對應讀出對象之扇區資料之扇區標頭(用戶控制資料)之輸出控制資訊中的匯流排保護旗標：BPF設定為[1]時，進入步驟S523，使用匯流排密鑰：Kbus對自資訊記錄媒體讀出之扇區資料加密，於步驟S524中輸出至主機側。再者，步驟S523中之扇區資料之加密處理作為例如使用先前參照圖26所說明之AES-CBC模式的加密處理而實行。

當於步驟S522中，判定對應讀出對象之扇區資料之扇區標頭(用戶控制資料)的輸出控制資訊中匯流排保護旗標：BPF設定為[0]時，跳過步驟S523，不使用匯流排密鑰：Kbus對自資訊記錄媒體讀出之扇區資料加密，而於步驟S524中將自資訊記錄媒體讀出之內容直接輸出至主機側。再者，該讀出內容為例如播放列表或檔案系統資訊等。

如此，驅動器依據對應讀出對象之扇區資料之扇區標頭(用戶控制資料)的輸出控制資訊中匯流排保護旗標：BPF為[0]或[1]而判斷是否需要使用匯流排密鑰執行加密，於判斷為需要使用匯流排密鑰執行加密之資料時，對輸出內容使用匯流排密鑰而執行加密並輸出。

接著，參照圖29，就主機側之處理加以說明。於步驟S551中，啟動再生應用程式，當於步驟S552中接收到碟片被插入至驅動器之通知時，執行登錄資訊之更新處理以及與驅動器之相互認證、通話密鑰之共享處理。

當於步驟S554中，確認相互認證以及密鑰交換(AKE)處理結束時，進入步驟S555，主機對於驅動器要求嵌入密鑰：Ke。嵌入密鑰：Ke係藉由依據碟片密鑰：Kd與自資訊記錄媒體獲得之ROM標記：Ve執行之密鑰產生處理、例如根據AES密碼算法之密鑰產生處理，而於驅動器產生之密鑰，藉由通話密鑰Ks而加密並發送至主機。

當於步驟S556中，自驅動器接收到經加密之嵌入密鑰：Ke時，於步驟S557中，使用通話密鑰Ks執行解碼，獲得嵌入密鑰：Ke。進而，主機於步驟S558中，對驅動器要求轉送作為產生使用於加密內容之解碼處理的密鑰所必需之資訊的記錄種(REC SEED)即單元密鑰產生資訊：Vu，當於步驟S559中接收到單元密鑰產生資訊：Vu時，於步驟S560中依據嵌入密鑰：Ke與單元密鑰產生資訊：Vu產生單元密鑰：Ku。該處理相當於圖24之步驟S303之處理。

接著，主機於步驟S561中對驅動器輸出匯流排密鑰：Kbus

之發送要求，當於步驟S562中獲得通過介以連接匯流排輸入之通話密鑰：Ks而加密之匯流排密鑰：Kbus時，於步驟S563中使用通話密鑰：Ks執行解碼處理，獲得匯流排密鑰：Kbus。該處理相當於圖24之步驟S305之處理。

繼而，於確認PC之再生軟體未結束(S564)，碟片未退出(S565)之情形後，當根據用戶指示等判斷為讀取扇區資料的情形(S566：Yes)時，於步驟S567中向驅動器輸出扇區資料之轉送要求。

當自驅動器接收扇區資料(S568)且資料為加密資料之情形(S569：Yes)時，於步驟S570中對藉由匯流排密鑰：Kbus加密之加密內容執行解碼處理。

對藉由匯流排密鑰：Kbus加密之加密內容執行之解碼處理如先前參照圖27所說明般，例如可藉由使用AES-CBC模式之組塊解碼處理而執行。

進而，主機於步驟S571中，使用單元密鑰：Ku對加密內容執行解碼處理。該解碼處理作為與先前參照圖11說明之處理相同的處理而執行。藉由以上處理，主機獲得解碼內容，執行內容再生。

於上述說明中，以來自資訊記錄媒體之資料的再生處理為中心加以了說明，但於主機將產生或自外部獲得之資料介以驅動器而記錄於資訊記錄媒體時，亦可於驅動器與主機間執行相互認證。該情形時亦執行上述登錄資訊之更新，即ADGL資訊證書(AIC)與認定裝置群列表(ADGL)之更新處理。作為更新處理態樣，可執行

(1)依據ADGL序列號之更新處理

(2)依據AIC資料＝登錄裝置數之更新處理

(3)依據AIC資料＝無效(Revoke)裝置數之更新處理

之三態樣中之任一種。

參照圖30，作為對資訊記錄媒體200執行資料記錄處理時之登錄資訊的更新處理例，就依據AIC資料＝無效(Revoke)裝置數之更新處理流程加以說明。

圖30係說明於將內容253介以驅動器400自主機500輸入而記錄於資訊記錄媒體200時，依據AIC資料(無效裝置數)更新ADGL資訊證書(AIC)以及認定裝置群列表(ADGL)，且依據更新資訊執行驅動器400與主機500間之相互認證以及密鑰交換(AKE)的處理之圖。再者，內容之輸出方為源，內容之輸入對象為同步。該例中，主機500為源，驅動器400為同步。

首先，驅動器400於步驟S601中讀取儲存於可寫入資料之資訊記錄媒體200中之ADGL資訊證書(AIC-DISC)251，將該AIC資料(無效裝置數)與自身記憶體中所儲存之ADGL資訊證書(AIC-D)411之AIC資料(無效裝置數)加以比較。

AIC-D之AIC資料 < AIC-DISC之AIC資料

時，判斷為AIC-DISC新於AIC-D，此時，驅動器400執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251。

再者，驅動器400於步驟S601之比較更新處理中，首先，

驗證賦予至自資訊記錄媒體200讀取之ADGL資訊證書(AIC-DISC)251的署名，確認其為未篡改ADGL資訊證書(AIC-DISC)之正當證書。該確認後，執行比較、更新。

步驟S602係於主機500執行之比較更新處理。主機500自驅動器400輸入儲存於驅動器400之記憶體之ADGL資訊證書(AIC-D)411，藉由署名驗證確認為未篡改之證書後，執行與儲存於主機500之記憶體中之ADGL資訊證書(AIC-H)511的AIC資料(無效裝置數)之比較處理。

AIC-H之AIC資料 < AIC-D之AIC資料

時，判斷為AIC-D新於AIC-H，此時，執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-H)511替換為自驅動器400輸入之ADGL資訊證書(AIC-D)411。

再者，AIC-H之AIC資料 < AIC-D之AIC資料

時，主機關於儲存於記憶體之認定裝置群列表(ADGL-H)執行更新處理。該更新處理係作為介以驅動器400置換為儲存於資訊記錄媒體200之認定裝置群列表(ADGL-DISC)，或介以網路獲得最新認定裝置群列表(ADGL)而更新等之處理而執行。

驅動器400於步驟S603中輸入保持於主機500之記憶體中的ADGL資訊證書(AIC-H)511，與儲存於自身記憶體之ADGL資訊證書(AIC-D)411執行AIC資料(無效裝置數)的比較。

AIC-D之AIC資料 < AIC-H之AIC資料

時，判斷為AIC-H新於AIC-D，此時，執行更新處理，將

儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自主機500輸入之ADGL資訊證書(AIC-H)511。

再者，驅動器400於步驟S603中之比較更新處理中，驗證賦予至自主機500輸入之ADGL資訊證書(AIC-H)511的署名，確認其為未被篡改之正當證書。該確認後，執行比較、更新。

驅動器400於步驟S603中之比較更新處理中，自主機500獲得包含於儲存於主機500之記憶體中的認定裝置群列表(ADGL-H)512之儲存有主機之登錄資訊的認定裝置群證書(ADGC-H)，於署名驗證後，比較設定於認定裝置群證書(ADGC-H)之AIC資料(無效裝置數)與儲存於自身記憶體之ADGL資訊證書(AIC-D)411之AIC資料(無效裝置數)。若

ADGC-H之AIC資料 < AIC-D之AIC資料

時，則判斷為主機僅具有不對應AIC-D之AIC資料之過期版本的認定裝置群證書，驅動器不進入相互認證處理(AKE)，而停止處理。

於步驟S603中，驅動器400判斷為

ADGC-H之AIC資料 $\geq$ AIC-D之AIC資料

時，進入下一步驟S604。

步驟S604~S608之處理為

S604：驅動器400與主機500間之相互認證以及密鑰交換(AKE)處理；

S605：使用通話密鑰：Ks對於驅動器400側產生之匯流排密鑰：Kbus執行加密以及發送；

S606：於主機500使用通話密鑰：Ks執行解碼處理，獲得
匯流排密鑰：Kbus；

S607：於主機500使用匯流排密鑰：Kbus對內容執行加密
發送處理；

S608：於驅動器400使用匯流排密鑰：Kbus對內容執行加
密處理以及記錄處理。

圖30所示之例為AIC資料為無效(Revoke)裝置數時的更
新處理，依據ADGL序列號之更新處理、AIC資料＝登錄裝
置數之更新處理亦執行與以上說明之內容再生時之登錄資
訊的更新大致相同之處理。

上述各處理例中，就於驅動器側比較自主機側輸入之設
定為認定裝置群證書(ADGC-H)之AIC資料與驅動器所保持
之ADGL資訊證書(AIC-D)的AIC資料中，當自主機側輸入之
認定裝置群證書(ADGC-H)舊於驅動器所保持之ADGL資訊
證書(AIC-D)時，不移至相互認證處理，而停止處理之設定
加以說明，但該情形時，關於向主機側賦予新認定裝置群
證書(ADGC-H)之獲得機會，驅動器對主機所獲得之新認定
裝置群證書(ADGC-H)反覆特定次數，比較新舊之構成例，
參照圖31、圖32加以說明。

圖31表示作為對來自資訊記錄媒體200之資料執行再生
處理時之登錄資訊的更新處理例，依據AIC資料＝無效
(Revoke)裝置數實施之更新處理流程。

首先，驅動器400於步驟S621中，讀取儲存於資訊記錄媒
體200之ADGL資訊證書(AIC-DISC)251，驗證署名，確認

ADGL 資訊證書 (AIC-DISC) 為未經篡改之正當證書後，比較該 AIC 資料 (無效裝置數) 與儲存於自身記憶體之 ADGL 資訊證書 (AIC-D) 411 之 AIC 資料 (無效裝置數)。

AIC-D 之 AIC 資料 < AIC-DISC 之 AIC 資料

時，判斷為 AIC-DISC 新於 AIC-D，此時，驅動器 400 執行更新處理，將儲存於自身記憶體中之 ADGL 資訊證書 (AIC-D) 411 替換為自資訊記錄媒體 200 讀取之 ADGL 資訊證書 (AIC-DISC) 251。

接著，於步驟 S622 中，主機 500 自驅動器 400 輸入儲存於驅動器 400 之記憶體中的 ADGL 資訊證書 (AIC-D) 411，藉由署名驗證確認為未篡改之證書後，執行與儲存於主機 500 之記憶體中之 ADGL 資訊證書 (AIC-H) 511 的 AIC 資料 (無效裝置數) 之比較處理。

AIC-H 之 AIC 資料 < AIC-D 之 AIC 資料

時，判斷為 AIC-D 新於 AIC-H，此時，執行更新處理，將儲存於自身記憶體之 ADGL 資訊證書 (AIC-H) 511 替換為自驅動器 400 輸入之 ADGL 資訊證書 (AIC-D) 411。

再者，AIC-H 之 AIC 資料 < AIC-D 之 AIC 資料

時，主機關於儲存於記憶體中之認定裝置群列表 (ADGL-H) 執行更新處理。該更新處理係作為介以驅動器 400 置換為儲存於資訊記錄媒體 200 中之認定裝置群列表 (ADGL-DISC)，或介以網路獲得最新認定裝置群列表 (ADGL) 而更新等之處理而執行。

驅動器 400 於步驟 S623 中輸入保持於主機 500 之記憶體中

的ADGL資訊證書(AIC-H)511，確認署名後，與儲存於自身記憶體中之ADGL資訊證書(AIC-D)411執行AIC資料(無效裝置數)的比較。

AIC-D之AIC資料 < AIC-H之AIC資料

時，判斷為AIC-H新於AIC-D，此時，執行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)411替換為自主機500輸入之ADGL資訊證書(AIC-H)511。

進而，驅動器400於步驟S623中之比較更新處理中，自主機500獲得包含於儲存於主機500之記憶體中的認定裝置群列表(ADGL-H)512之儲存有主機之登錄資訊的認定裝置群證書(ADGC-H)，於署名驗證後，比較設定於認定裝置群證書(ADGC-H)之AIC資料(無效裝置數)與儲存於自身記憶體中之ADGL資訊證書(AIC-D)411之AIC資料(無效裝置數)。於該比較處理中，

ADGC-H之AIC資料 < AIC-D之AIC資料

時，驅動器判斷主機僅保持有不對應AIC-D之AIC資料的過期版本之認定裝置群證書，對主機要求新認定裝置群證書(ADGC-H)之獲得以及發送，並且將計數412之值遞增1。該認定裝置群證書(ADGC-H)之再獲得要求設定有最大重複次數，例如最大重複次數=5時，計數412之值為5時，執行再獲得要求。於該允許次數內自主機輸入之認定裝置群證書(ADGC-H)滿足

ADGC-H之AIC資料 $\geq$ AIC-D之AIC資料

時，進入其後之處理即相互認證處理(AKE)。於允許次數

之再獲得處理中獲得之證書皆為

ADGC-H之AIC資料 < AIC-D之AIC資料

時，不進入相互認證處理(AKE)，而停止處理。

允許次數(例如5次)以內自主機輸入之認定裝置群證書(ADGC-H)滿足

ADGC-H之AIC資料 $\geq$ AIC-D之AIC資料

時，執行步驟S624~S628之處理即驅動器400與主機500間之相互認證以及密鑰交換(AKE)處理，執行驅動器400之匯流排密鑰、內容之發送，主機500之內容解碼。

參照圖32，就驅動器400執行之圖31之步驟S623之處理，即主機側督促再獲得含有認定裝置群證書(ADGC-H)之認定裝置群列表(ADGL-H)的處理，加以詳細說明。

驅動器於步驟S701中，接收到來自主機之ADGL資訊證書(AIC-H)之轉送要求後，於步驟S702中自主機接收ADGL資訊證書(AIC-H)。於步驟S703中，執行ADGL資訊證書(AIC-H)之署名驗證，於無法藉由署名驗證確認證書之正當性(S704：No)時，停止其後之處理。此時不執行內容轉送處理。

可藉由署名驗證確認證書之正當性(S704：Yes)時，於步驟S705中，比較自主機獲得之ADGL資訊證書(AIC-H)之AIC資料(無效裝置數)與儲存於自身記憶體中之ADGL資訊證書(AIC-D)之AIC資料(無效裝置數)。

AIC-D之AIC資料 < AIC-H之AIC資料

時，判斷為AIC-H新於AIC-D，進入步驟S706，驅動器執

行更新處理，將儲存於自身記憶體之ADGL資訊證書(AIC-D)替換為自主機獲得之ADGL資訊證書(AIC-H)。上述條件無法滿足

AIC-D之AIC資料 < AIC-H之AIC資料

時，判斷為儲存於自身記憶體之ADGL資訊證書(AIC-D)更新於自主機獲得之ADGL資訊證書(AIC-H)，不執行更新處理。

接著，於步驟S707中，確認自主機接收到認定裝置群證書(ADGC-H)後，於步驟S708中，比較設定於認定裝置群證書(ADGC-H)之AIC資料(無效裝置數)與儲存於自身記憶體之ADGL資訊證書(AIC-D)之AIC資料(無效裝置數)。

ADGC-H之AIC資料 < AIC-D之AIC資料

不成立時，判斷認定裝置群證書為對應AIC-D之AIC資料之新版本，於步驟S711中執行計數 = 0之重設處理，結束比較更新處理，移至下一處理即相互認證處理。

另一方面，ADGC-H之AIC資料 < AIC-D之AIC資料

時，判斷為主機僅保持有不對應AIC-D之AIC資料之過期版本的認定裝置群證書，進入步驟S709，判斷計數是否為允許再獲得次數以下。

計數為允許再獲得次數以下時，於步驟S710中將計數遞增1，對主機要求再次發送認定裝置群證書(ADGC-H)，重複執行步驟S707以下步驟。

於步驟S709中，計數到達允許再獲得次數時，不進入相互認證處理(AKE)，而停止處理。

根據本處理例，向主機提供自身保持之認定裝置群列表 (ADGL-H) 之更新機會，故而可自外部獲得認定裝置群列表 (ADGL)，對內容執行再生或記錄。

再者，參照圖 31 所說明之處理係 AIC 資料為無效 (Revoke) 裝置數時之更新處理，可執行與依據 ADGL 序列號之更新處理、依據 AIC 資料 = 登錄裝置數之更新處理相同的允許再取得處理之處理。

[4. 認證次數之計算以及證書更新處理]

通過上述複數個實施例之說明可知，為使主機能以驅動器存取於資訊記錄媒體，必須自主機向驅動器輸出認定裝置群證書，於驅動器中比較自主機輸入之設定於認定裝置群證書之 AIC 資料與驅動器所保持之 ADGL 資訊證書 (AIC-D) 之 AIC 資料，以自主機輸入之認定裝置群證書 (ADGC-H) 之 AIC 資料不舊於驅動器所保持之 ADGL 資訊證書 (AIC-D) 為條件，實行相互認證，而認證成立。

因此，主機被要求必須獲得更新的認定裝置群證書。作為獲得更新認定裝置群證書之方法，有購買新發售之碟片而自碟片中獲得之方法，以及將主機連接至管理並發佈認定裝置群證書之伺服器，經由伺服器而獲得之方法。

藉由碟片而更新時，會存在用戶必須購買儲存有新認定裝置群證書之新碟片的問題。又，於驅動器為可裝卸於作為主機之 PC 等裝置的裝置時，驅動器可與各種主機 (PC) 連接。驅動器可自所安裝之資訊記錄媒體獲得更新的 AIC 資料，於自資訊記錄媒體獲得新 AIC 資料時，驅動器所連接之

主機(PC)亦可獲得且保存對應該新版本之認定裝置群證書。然而，當驅動器之後連接於其他主機(PC)，安裝不同碟片實行主機-驅動器間之認證時，於此時連接之主機(PC)所保持之認定裝置群證書之AIC資料舊於驅動器之AIC資料，該主機會無法利用碟片。

如此，會產生利用主機之用戶必須經常考慮更新儲存於主機之認定裝置群證書的問題。持有作為複數個主機裝置之例如PC的用戶必須更加注意並實行複數個PC之認定裝置群證書的更新。

以下，關於減輕用戶負擔，確實更新主機之證書的構成例加以說明。

參照圖33就本實施例加以說明。本實施例之概要總結如下。

(1)主機(例如PC)計算與驅動器之相互認證之次數，到達某次數則實行伺服器與網路之連接，更新登錄列表。亦會有自碟片更新登錄列表之情形。

(2)主機(例如PC)與驅動器之相互認證的計算值到達預先設定之上限次數時，不實行與驅動器之相互認證，且通知用戶必須實行登錄列表更新處理。或自動移至登錄列表更新處理。

如上所述，認定裝置群證書之更新步驟為具體者，因此可作為主機側應保守之遵守原則而對照相互認證之許可證，根據合同契約對獲准者加以限制。

圖33表示可安裝資訊記錄媒體200之驅動器400以及介以

驅動器400對資訊記錄媒體200實行存取之PC等主機500。主機500可介以通信部627連接於外部伺服器632。伺服器632介以管理中心631獲得並管理儲存有最新認定裝置群證書(ADGC)之認定裝置群列表(ADGL)、ADGL資訊證書(AIC)，並介以網路發佈該等各證書。

參照圖33就本實施例之概要加以說明。關於詳細處理流程，參照圖34~圖36之流程說明如下。主機500於介以驅動器400對資訊記錄媒體200實行存取時，根據需要實行相互認證處理。主機500於主機500之認證實行部622與驅動器400之認證實行部612間介以雙方之通信部611、612實行認證處理。認證處理如先前參照圖25之流程圖所說明般，使用儲存於雙方之記憶體615、626的公開密鑰證書(PKC)。

主機500具有由非揮發性記憶體(NV-RAM)構成之認證次數計算記憶體623。認證次數計算記憶體623係記錄與驅動器之認證處理之執行結束而算出之認證次數的記憶體。再者，認證次數計算記憶體623之初期值為0。

主機500於開始與驅動器400之認證處理時，於比較部624讀出儲存於認證次數計算記憶體623之認證次數計算值，與預先設定之上限臨界值實行比較。

當儲存於認證次數計算記憶體623之認證次數計算值未滿上限臨界值時，執行與驅動器400之認證處理。當儲存於認證次數計算記憶體623之認證次數計算值到達上限臨界值時，停止與驅動器400之認證處理。此時，通過顯示器等執行將認證次數計算值到達上限臨界值之情形通知用戶的

處理。

當認證次數計算值到達上限臨界值時，依據用戶之指示，自伺服器632獲得證書並執行更新處理。再者，亦可構成以認證次數計算值到達上限臨界值為條件，自動執行自伺服器632獲得證書以及更新處理。

主機500之更新執行部625對伺服器632實行存取，自伺服器632獲得儲存有認定裝置群證書(ADGC)之認定裝置群列表(ADGL)、ADGL資訊證書(AIC)，儲存於記憶體(NV-RAM)626。

當藉由主機500之更新執行部625，將最新認定裝置群列表(ADGL)、ADGL資訊證書(AIC)儲存於記憶體626時，認證次數計算記憶體623之計算值重設，設定為[0]。

其後，認證實行部622執行與驅動器400之認證處理，以認證成立為條件，可對資訊記錄媒體200執行存取。

進而，主機500通過認證處理介以主機500與驅動器400間之介面，將自伺服器632獲得之ADGL資訊證書(AIC)輸出至驅動器400。驅動器400介以通信部611獲得最新ADGL資訊證書(AIC-H)。此時，主機500保持之證書為ADGL資訊證書，故而表示為AIC-H。

驅動器400於比較部613，比較自主機500獲得之ADGL資訊證書(AIC-H)與儲存於自身記憶體615之ADGL資訊證書(AIC-D)的新舊，當判斷為自主機500獲得之ADGL資訊證書(AIC-H)較新時，更新執行部614執行更新處理，將記憶體615之儲存資料置換為自主機500獲得之ADGL資訊證書

(AIC-H)。再者，比較部613之比較係依據記錄於各證書之登錄裝置數、無效裝置數或序列號等而執行。

藉由主機500將自伺服器632獲得之最新證書亦儲存於驅動器400，主機、驅動器之雙方可更新為最新證書。本實施例中，構成為對於主機實行之與驅動器之認證處理次數設定上限臨界值，於到達臨界值時通知用戶必須更新證書，或執行更新處理，因此用戶無需執行更新時序之管理，可減少用戶負擔地適當地實現證書更新處理。

接著，參照圖34~圖36，就伴隨於與驅動器連接之主機所執行之與驅動器的認證處理以及自伺服器獲得證書以及更新處理的一系列處理，加以說明。

於圖34之步驟S801中，主機啟動對應儲存於碟片之內容的再生應用程式。當於步驟S802中自驅動器收到插入碟片之檢測通知時，於步驟S803中，自驅動器獲得碟片資訊。例如，主機向驅動器發送[READ DVD STRUCTURE command]，利用所獲得之資料可確認該碟片是否為經加密記錄之碟片。該指令揭示於SCSI(Small Computer System Interface，小型電腦系統介面)規格中之指令規格INCITS T10, Multimedia Commands-4(MMC-4)中。作為其他判斷方法，亦可構成為解釋使用於碟片記錄之檔案系統，根據所獲得之目錄資訊而判斷之方法。

於步驟S804中，依據於步驟S803中獲得之碟片資訊，判斷安裝於驅動器之碟片是否為加密資料之記錄碟片。當為非加密碟片時，進入圖35之步驟G，實行通常之資料再生處

理，即於步驟S829中確認碟片未退出(S830)後，於判定為根據用戶指示等讀取扇區資料時(S831：Yes)，於步驟S832對於驅動器輸出扇區資料之轉送要求，於步驟S833中至判定為扇區資料結束為止，執行資料再生。

返回圖34，於步驟S804中判定為加密資料之記錄碟片時，於步驟S805判定認證次數計算(SAC計算)之計算值有無到達預先設定之上限值。此處理相當於圖33之於認證次數計算記憶體623之比較部624執行之處理。再者，主機之認證次數計算記憶體623之初期值為0。

步驟S805中認證次數計算(SAC計算)之計算值到達預先設定之上限值時，進入圖36之步驟I。此處理相當於自伺服器獲得更新證書之處理。

於步驟S841中，判斷主機有無連接網路，於未連接網路時，為再生碟片必須更新裝置登錄列表，但因未連接網路故而於畫面上顯示無法更新裝置登錄列表，且結束處理。用戶依據畫面顯示，瞭解到為再生安裝於驅動器之碟片，必須獲得儲存有經更新之認定裝置群證書(ADGC)的認定裝置群列表(ADGL)。

於步驟S841中，當判斷為主機連接有網路時，進入步驟S843，於畫面上顯示正在實行儲存有認定裝置群證書(ADGC)之認定裝置群列表(ADGL)的更新處理，於步驟S844中，與主機上正在啟動之應用程式所指定之伺服器相連接。於主機啟動中之應用程式(內容再生應用程式)中記錄有更新認定裝置群列表(ADGL)時必須連接之伺服器的

URL，使用該URL連接至伺服器。

於步驟S845中確認伺服器連接已結束，於連接失敗時，進入步驟S846，因無法發現指定URL，故而於畫面顯示裝置登錄列表之更新失敗以及若不更新則無法再生碟片，並且結束處理。

當連接成功時，進入步驟S847，自連接之伺服器下載儲存有最新認定裝置群證書(ADGC)之認定裝置群列表(ADGL)。例如依據HTTP或FTP執行下載處理。認定裝置群列表(ADGL)如圖36右下部所示，於認定裝置群列表(ADGL)中添加有篡改驗證值(電子署名、MAC等)，成為篡改防止構成。再者，本處理流程中表示僅下載認定裝置群列表(ADGL)之處理例，但較好的是如上所述構成為一同下載ADGL資訊證書(AIC)。

於步驟S848中確認下載是否結束。於下載無法完成時，進入步驟S849，於畫面顯示自伺服器下載裝置登錄列表之處理失敗而無法更新、以及若不更新則無法再生碟片，並且結束處理。

當於步驟S848中確認下載結束時，於步驟S850中依據附加至ADGL檔案之驗證值實行驗證處理，確認並未篡改。於確認處理完成且無法確認未篡改時，進入步驟S852，於畫面顯示自伺服器下載裝置登錄列表之處理失敗而無法更新、以及若不更新則無法再生碟片，並且結束處理。

於可確認無篡改之情形時，進入步驟S861，自下載之ADGL檔案中獲得認定裝置群列表(ADGL)，於步驟S862

中，於畫面顯示認定裝置群列表(ADGL)之完了通知。進而，於步驟S863中，執行將認證次數計算(SAC計算)記憶體之計算值重設為0之處理。再者，如參照圖33所說明般，如上所述，於S847中一同下載ADGL資訊證書(AIC)時，於S850使用ADGL資訊證書(AIC)之署名驗證確認完全性，且於S861儲存ADGL資訊證書(AIC)，此時亦可介以介面對驅動器實行輸出處理。

接著返回圖34，就步驟S806之後之步驟加以說明。步驟S806中，實行與驅動器之相互認證以及通話密鑰之共享處理。

於步驟S807中，當確認相互認證以及密鑰交換(AKE)處理結束時，於步驟S808中將認證次數計算(SAC計算)記憶體之計算值增加一個。接著，進入步驟S809，主機向驅動器要求嵌入密鑰：Ke。嵌入密鑰：Ke係藉由依據碟片密鑰：Kd與自資訊記錄媒體獲得之ROM標記：Ve執行之密鑰產生處理、例如根據AES密碼算法之密鑰產生處理，而於驅動器產生之密鑰，藉由通話密鑰Ks加密並發送至主機。

於步驟S810中，當自驅動器接收到經加密之嵌入密鑰：Ke時，於步驟S811中，使用通話密鑰Ks執行解碼，獲得嵌入密鑰：Ke。進而，主機於步驟S812中，對驅動器要求轉送作為產生使用於加密內容之解碼處理的密鑰所必需之資訊的記錄種(REC SEED)即單元密鑰產生資訊：Vu，於步驟S813中接收到單元密鑰產生資訊：Vu時，於步驟S814中依據嵌入密鑰：Ke與單元密鑰產生資訊：Vu產生單元密鑰：

Ku。該處理相當於例如圖 24 之步驟 S303 之處理。

接著，主機於步驟 S815 中對驅動器輸出匯流排密鑰：Kbus 之發送要求，當於步驟 S816 中獲得通過介以連接匯流排輸入之通話密鑰：Ks 而加密之匯流排密鑰：Kbus 時，於步驟 S817 中使用通話密鑰：Ks 執行解碼處理，獲得匯流排密鑰：Kbus。該處理相當於例如圖 24 之步驟 S305 之處理。

接著，移至圖 35 之步驟 S821。於確認 PC 之再生軟體未結束 (S821)，碟片未退出 (S822) 之情形後，當判斷為根據用戶指示等讀取扇區資料的情形 (S823：Yes) 時，於步驟 S824 中向驅動器輸出扇區資料之轉送要求。

當自驅動器接收扇區資料 (S825)，且資料為加密扇區資料之情形 (S826：Yes) 時，於步驟 S827 中對藉由匯流排密鑰：Kbus 加密之加密內容執行解碼處理。

對藉由匯流排密鑰：Kbus 加密之加密內容執行之解碼處理如先前參照圖 27 所說明般，例如可藉由使用 AES-CBC 模式之組塊解碼處理而執行。

進而，主機於步驟 S828 中，使用單元密鑰：Ku 對加密內容執行解碼處理。該解碼處理作為與先前參照圖 11 說明之處理相同的處理而執行。藉由以上處理，主機獲得解碼內容執行內容再生。

於上述說明中，以來自資訊記錄媒體之資料的再生處理為中心加以了說明，但於主機將產生或自外部獲得之資料介以驅動器記錄於資訊記錄媒體時，亦可於驅動器與主機間執行相互認證。此時亦可執行上述相互認證計算值之遞

增處理、與上限值之比較處理、對到達上限值時來自伺服器之證書的更新即對ADGL資訊證書(AIC)與認定裝置群列表(ADGL)之更新處理。作為更新處理態樣，可執行

(1)依據ADGL序列號之更新處理

(2)依據AIC資料＝登錄裝置數之更新處理

(3)依據AIC資料＝無效(Revoke)裝置數之更新處理

三態樣中之任一種。

[5.資訊處理裝置之構成]

接著，參照圖37、圖38，關於主機以及驅動器裝置之資訊處理裝置構成例加以說明。

首先，參照圖37就作為主機之資訊處理裝置之構成加以說明。資訊處理裝置800具有：依據OS、內容再生或記錄應用程式、或相互認證處理程式等各種程式執行資料處理的CPU809，作為程式、參數等之記憶區域的ROM808，記憶體810，輸出入數位信號之輸出入I/F802，輸出入類比信號且具有A/D、D/A轉換器805之輸出入I/F804，執行MPEG資料之編碼、解碼處理之MPEG編碼/解碼器803，執行TS(Transport Stream，傳輸串流)・PS(Program Stream，節目串流)處理之TS・PS處理機構806，執行相互認證、加密內容之解碼處理等各種密碼處理的密碼處理機構807，硬碟等記錄媒體812，以及對於記錄媒體812執行驅動、輸出入資料記錄再生信號之驅動器811；且各組塊連接於匯流排801。

資訊處理裝置(主機)800藉由例如ATAPI-BUS等連接匯流

排而與驅動器連接，藉由上述匯流排密鑰而加密之內容自數位信號用輸出入I/F802輸入，根據需要藉由加密處理機構807執行例如使用AES-CBC模式之解碼處理。

再者，執行內容再生或記錄處理之程式保管於例如ROM808內，程式之執行處理中根據需要使用記憶體810作為參數、資料之保管、工作區域。

ROM808或記錄媒體812中儲存有先前參照圖24所說明之管理中心之公開密鑰、主機對應秘密密鑰、對應主機之公開密鑰證書，進而儲存有認定裝置群列表(ADGL-H)、ADGL資訊證書(AIC-H)之登錄資訊。

接著，參照圖38就資訊記錄媒體之儲存內容之讀取以及記錄、以及作為與主機執行資料轉送之驅動器的資訊處理裝置之構成加以說明。驅動器850具有依據內容讀取、內容記錄、轉送處理程式、相互認證處理程式等各種程式執行資料處理的CPU852，作為程式、參數等之記憶區域的ROM855，記憶體856，輸出入數位信號之輸出入I/F853，執行相互認證、匯流排密鑰之產生、輸出資料之加密處理等各種密碼處理的密碼處理機構854，輸出入DVD、Blu-ray碟片等資訊記錄媒體858之驅動、資料記錄再生信號的記錄媒體I/F857；且各組塊連接於匯流排851。

驅動器850藉由例如ATAPI-BUS等連接匯流排而與主機連接，例如使用匯流排密鑰：Kbus將儲存於資訊記錄媒體858之加密(scramble)內容再加密，自輸出入I/F853輸出。使用匯流排密鑰：Kbus對內容之加密藉由加密處理機構854，

例如以 AES-CBC 模式而執行。

再者，於 ROM855 或記憶體 856 中，儲存有先前參照圖 24 說明之管理中心之公開密鑰、對應驅動器之秘密密鑰、對應驅動器之公開密鑰證書、以及用以密碼密鑰塊 RKB 之處理的裝置密鑰：Kdev，進而儲存有 ADGL 資訊證書 (AIC-D)。又，儲存有執行內容之讀取、獲得以及相互認證處理的程式等。

以上，參照特定實施例，關於本發明加以詳細說明。但業者應瞭解，可於不脫離本發明要旨之範圍內修正或代用該實施例。即，例示之形態為說明本發明者，並非有所限定者。為判斷本發明之要旨，應參照專利請求範圍之內容。

再者，於說明書中說明之一系列處理可藉由硬體、軟體或兩者之複合構成而執行。於藉由軟體執行處理時，可將記錄有處理流程之程式安裝於組裝入專用硬體之電腦內之記憶體而實行，或於可執行各種處理之通用電腦上安裝程式而實行。

例如，程式可預先記錄於作為記錄媒體之硬碟或 ROM (Read Only Memory，唯讀記憶體)。或，程式可暫時或永久儲存 (記錄) 於軟碟、CD-ROM (Compact Disc Read Only Memory，緊密磁碟 - 唯讀記憶體)、MO (Magneto optical，磁光) 碟片、DVD (Digital Versatile Disc，數位化通用磁碟)、磁碟、半導體記憶體等抽取式記錄媒體。此種抽取式記錄媒體可作為所謂封裝軟體而提供。

再者，程式除可自如上所述之抽取式記錄媒體安裝於電

腦以外，可自下載點無線轉送至電腦，或介以LAN(Local Area Network，區域網路)、網際網路之網路有線轉送至電腦，於電腦接收如此轉送來之程式，可安裝於內置之硬碟等記錄媒體。

再者，說明書中揭示之各種處理並非僅如揭示般依據時序系列執行，亦可根據執行處理之裝置之處理能力或需要，並列或單獨執行。又，本說明書中所謂系統係指複數個裝置之邏輯集合構成，各構成之裝置並非限定同一框體內者。

[產業上之可利用性]

如上所述，根據本發明之構成，於伴隨驅動器與主機等兩個不同裝置間之資料轉送而再生或記錄內容時，於執行資料轉送之裝置間之相互認證中，計算認證次數，於到達預先設定之認證次數上限值時，停止認證處理，設定為必須更新用以認證之證書，故而可排除使用過期證書繼續認證處理而利用內容之可能性，並促使用戶獲得最新證書。

本發明之構成中，於連接裝置間自內容之發送側(源)裝置向接收側(同步)裝置轉送內容時實行之公開密鑰密碼方式的相互認證中，為判斷使用之各裝置之公開密鑰證書的有效性，使用認定裝置群證書。進而構成為，於判斷該認定裝置群證書有無過期時，使用將作為認定裝置群證書之集合而設定之認定裝置群列表(登錄列表)之登錄裝置數或無效(Revoke)裝置數等設為登錄資料的裝置數資料證書(AIC)，依據將登錄裝置數為多者作為最新或將無效裝置數

為多者作為最新等之登錄資訊之登錄或無效裝置數的變化狀況，判定認定裝置群證書之最新性，使用新認定裝置群證書判定裝置之公開密鑰證書的有效性而執行相互認證，進而計算認證次數，於到達預先設定之認證次數上限值時，停止認證處理，設定為必須更新用以認證之證書，故而可防止使用過期認定裝置證書實行認證處理，防止非法獲得內容，排除非法利用內容之可能性。

又，因構成為依據將登錄裝置數或無效(Revoke)裝置數等設定為登錄資料之裝置數資料證書(AIC)，適當更新資訊處理裝置保管之認定裝置群列表(登錄列表)，故而可隨時更新實行內容再生或記錄處理之資訊處理裝置的保管列表。

進而，藉由將登錄裝置數或無效裝置數使用於各證書之是否過期的判定，可減少作為驅動器或主機之證書儲存用非揮發性記憶體而使用之快閃記憶體的覆寫次數。即，於使用序列號判定有無過期之情形時，因序列號變更時需全部更新，故而快閃記憶體之使用頻率增多，但藉由將登錄裝置數或無效裝置數用以各證書之是否過期的判定，登錄裝置數或無效裝置數無變化之情形時可無需於驅動器或主機更新證書，故而可減少快閃記憶體之覆寫次數。因此可搭載小型且廉價之記憶體。

【圖式簡單說明】

圖1係用以說明先前之資訊記錄媒體儲存內容之再生序列的圖。

圖2係用以說明先前之資訊處理裝置之驅動器輸出內容

之再生序列的圖。

圖3係用以說明來自驅動器之內容輸出序列的流程圖。

圖4(1、2)係用以說明伴隨先前之於主機驅動器間轉送內容之處理構成而非法利用內容之例的圖。

圖5係用以說明本發明之資訊記錄媒體之儲存資料的圖。

圖6(a、b、c)係用以說明本發明之資訊記錄媒體之儲存資料之構成的圖。

圖7係用以說明作為本發明之資訊記錄媒體之儲存資料的扇區資料以及扇區標頭之構成的圖。

圖8係用以說明記錄於本發明之資訊記錄媒體之扇區標頭的輸出控制資訊之詳細內容的圖。

圖9係用以說明實行資訊記錄媒體之儲存內容之讀取、再生的再生機器之處理流程的圖。

圖10係用以說明於資訊記錄媒體之儲存內容之再生中依據所實行之AES密碼算法而實行之密鑰產生處理的圖。

圖11係用以說明於資訊記錄媒體之儲存內容之再生中依據所實行之AES密碼算法而實行之資料解碼處理的圖。

圖12係用以說明儲存於資訊記錄媒體、驅動器與資訊處理裝置之資料的圖。

圖13(a、b)係用以說明證書之資料構成以及種類的圖。

圖14(a、b)係用以說明公開密鑰證書之資料構成的圖。

圖15(a、b)係用以說明認定裝置群證書(ADGC)、認定群列表(ADGL)之資料構成的圖。

圖16(a、b)係用以說明ADGL資訊證書(AIC)之資料構成的

圖。

圖 17 係用以說明儲存於資訊記錄媒體、驅動器與資訊處理裝置之證書的圖。

圖 18 係用以說明依據 ADGL 序列號更新登錄資訊之處理的圖。

圖 19 係用以說明依據 AIC 資料 = 登錄裝置數而更新登錄資訊之處理的圖。

圖 20 係用以說明依據 AIC 資料 = 無效裝置數而更新登錄資訊之處理的圖。

圖 21(a、b)係用以說明依據 AIC 資料而更新登錄資訊之處理之詳細序列的圖。

圖 22(c)係用以說明依據 AIC 資料而更新登錄資訊之處理之詳細序列的圖。

圖 23 係用以說明依據 AIC 資料而更新登錄資訊之處理中，資訊記錄媒體、驅動器與資訊處理裝置間之通信序列的圖。

圖 24 係用以說明伴隨驅動器、資訊處理裝置間之內容轉送而再生內容時之登錄資訊之更新處理、相互認證、內容再生序列的圖。

圖 25 係用以說明於驅動器與資訊處理裝置間實行之相互認證以及密鑰交換(AKE)處理流程的圖。

圖 26 係用以說明於驅動器實行之內容依據匯流排密鑰：Kbus 之加密處理構成的圖。

圖 27 係用以說明於資訊處理裝置實行之內容依據匯流排

密鑰：Kbus之解碼處理構成的圖。

圖28係用以說明於伴隨自驅動器對主機轉送內容之再生處理中，於驅動器實行之處理流程的流程圖。

圖29係用以說明於伴隨自驅動器對主機轉送內容之再生處理中，於主機實行之處理流程的流程圖。

圖30係用以說明於內容之記錄處理中依據AIC資料＝無效裝置數而更新登錄資訊的圖。

圖31係用以說明於主機允許再獲得ADGL之情形時，依據AIC資料＝無效裝置數更新登錄資訊之處理的圖。

圖32係用以說明於主機允許再獲得ADGL之情形時，依據AIC資料＝無效裝置數而更新登錄資訊之處理時驅動器之處理的圖。

圖33係用以說明主機之認證處理次數之計算處理與依據計算值而獲得ADGL之處理的圖。

圖34係用以說明主機之認證處理次數之計算處理與依據計算值而獲得ADGL之處理的流程圖。

圖35係用以說明主機之認證處理次數之計算處理與依據計算值而獲得ADGL之處理的流程圖。

圖36係用以說明主機之認證處理次數之計算處理與依據計算值而獲得ADGL之處理的流程圖。

圖37係表示作為本發明之主機的資訊處理裝置之構成例的圖。

圖38係表示作為本發明之驅動器的資訊處理裝置之構成例的圖。

【主要元件符號說明】

10, 812, 857	記錄媒體
11, 122, 203	加密碟片密鑰
12	加密標題密鑰
13	加密 MPEG 資料
20	再生機器
25	音聲/影像資料
30, 50, 400, 811, 850	驅動器
40	播放器應用程式
60, 500	主機
100, 200, 858	資訊記錄媒體
101	資料儲存區域
102	引入區域
111, 206	加密內容
112, 205	單元密鑰產生資訊
114, 204	ROM標記
120	密碼密鑰資訊
121	RKB
130, 201	登錄資訊
131, 251, 411, 511	ADGL 資訊證書
132, 512	認定裝置群列表
151	輸出控制資訊
202	登錄裝置列表
252	ADGL-DISC

253	內 容
300	驅動器兼用再生機器
301	裝置密鑰
311	AES密碼處理組塊
321	AES密鑰產生處理組塊
322	AES解碼處理組塊
323, 552, 572	加密扇區資料
402, 502	秘密密鑰
403, 503	公開密鑰證書
550, 570	扇區資料
551	AES密碼處理部
571	AES解碼處理部
611, 627	通信部
612, 622	認證實行部
613, 624	比較部
614, 625	更新執行部
615, 626, 810, 856	記憶體
623	認證次數計算記憶體
631	管理中心
632	伺服器
800	資訊處理裝置
801, 851	匯流排
802	數位信號用輸出入I/F
803	MPEG編碼/解碼器

804, 853

輸 出 入 I/F

805

A/D、D/A 轉 換 器

806

TS・PS 處 理 機 構

807, 854

密 碼 處 理 機 構

808, 855

ROM

809, 852

CPU

五、中文發明摘要：

本發明提供一種關於防止繼續使用過期之認定裝置證書的認證處理、以及防止非法利用內容的構成。於伴隨驅動器與主機等兩個不同裝置間進行資料轉送而對內容實行再生或記錄處理時，於實行資料轉送之裝置間的相互認證中計算認證次數，設定為於到達預先規定之認證次數上限值時，停止認證處理，必須更新適用於認證之證書。根據本構成，可排除藉由應用過期證書繼續認證處理而利用內容，並促使用戶取得最新證書。

六、英文發明摘要：

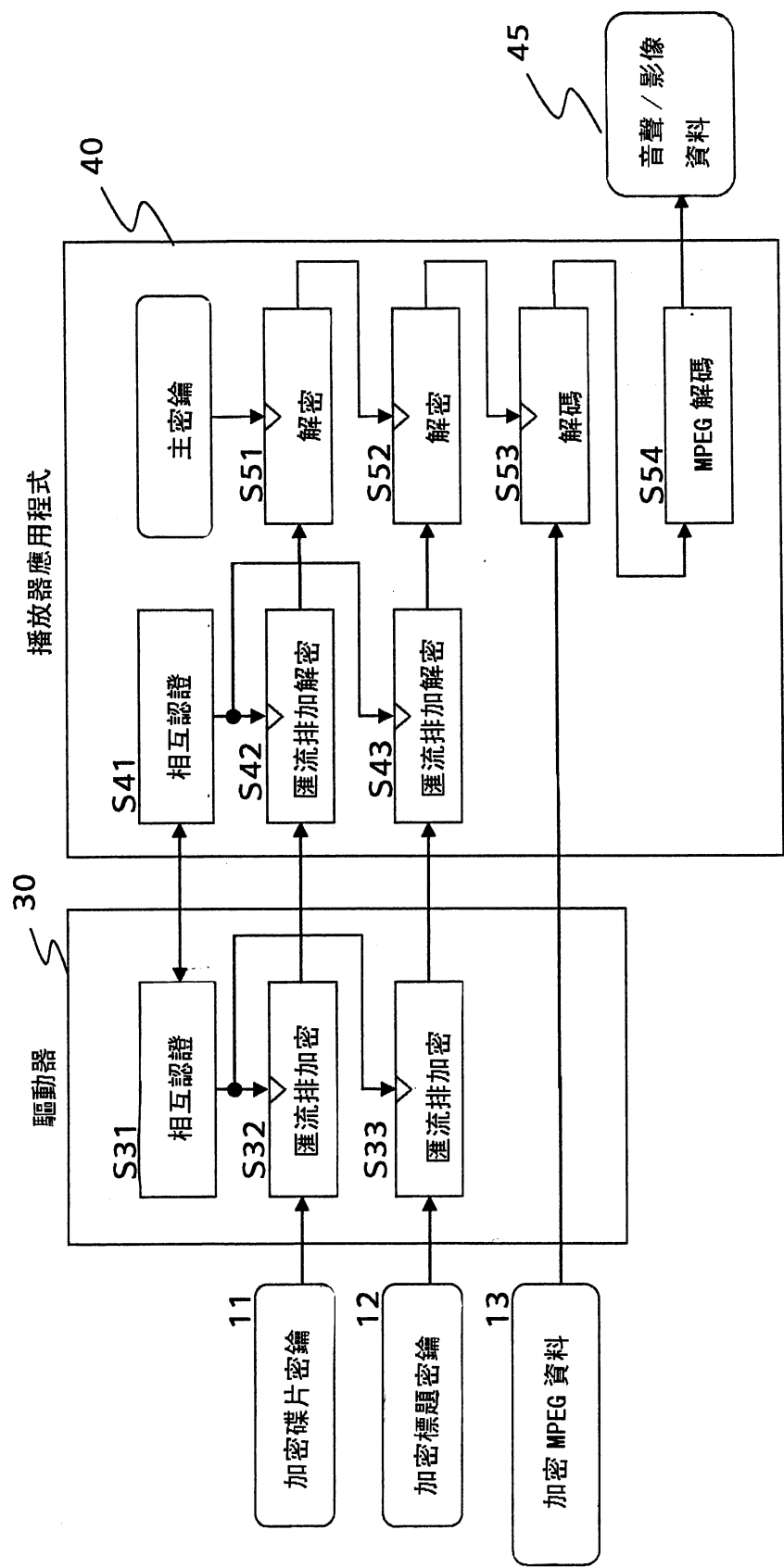


圖 2

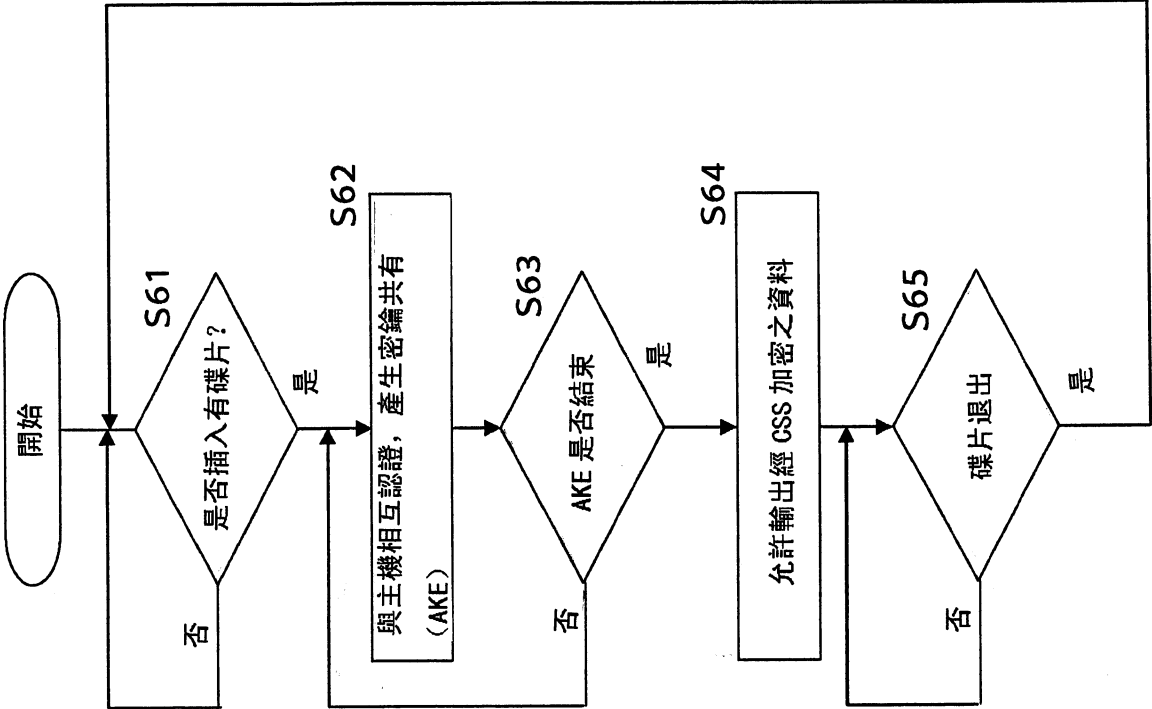


圖 3

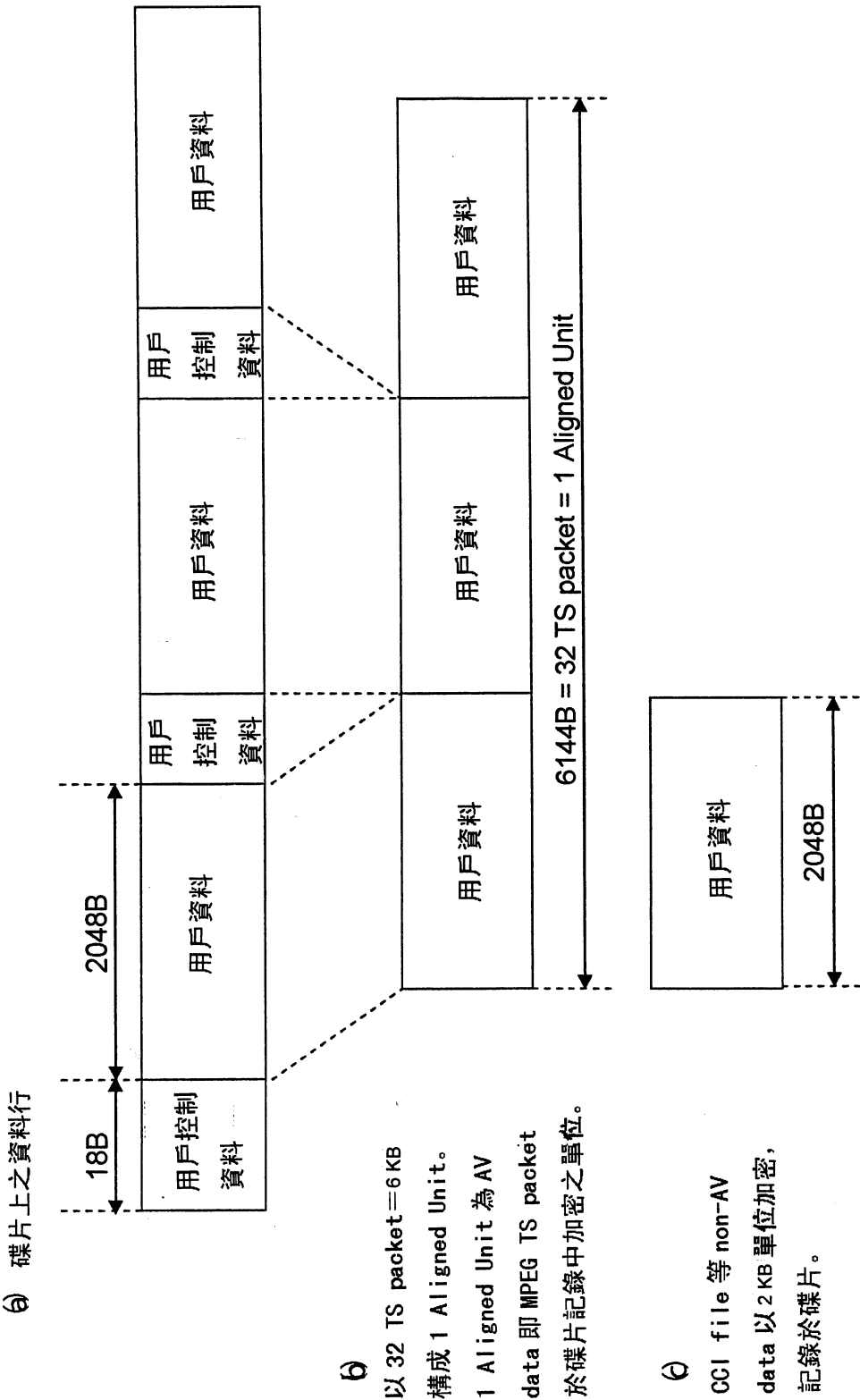


圖 6

扇區標頭 (用戶控制資料: User Control Data)

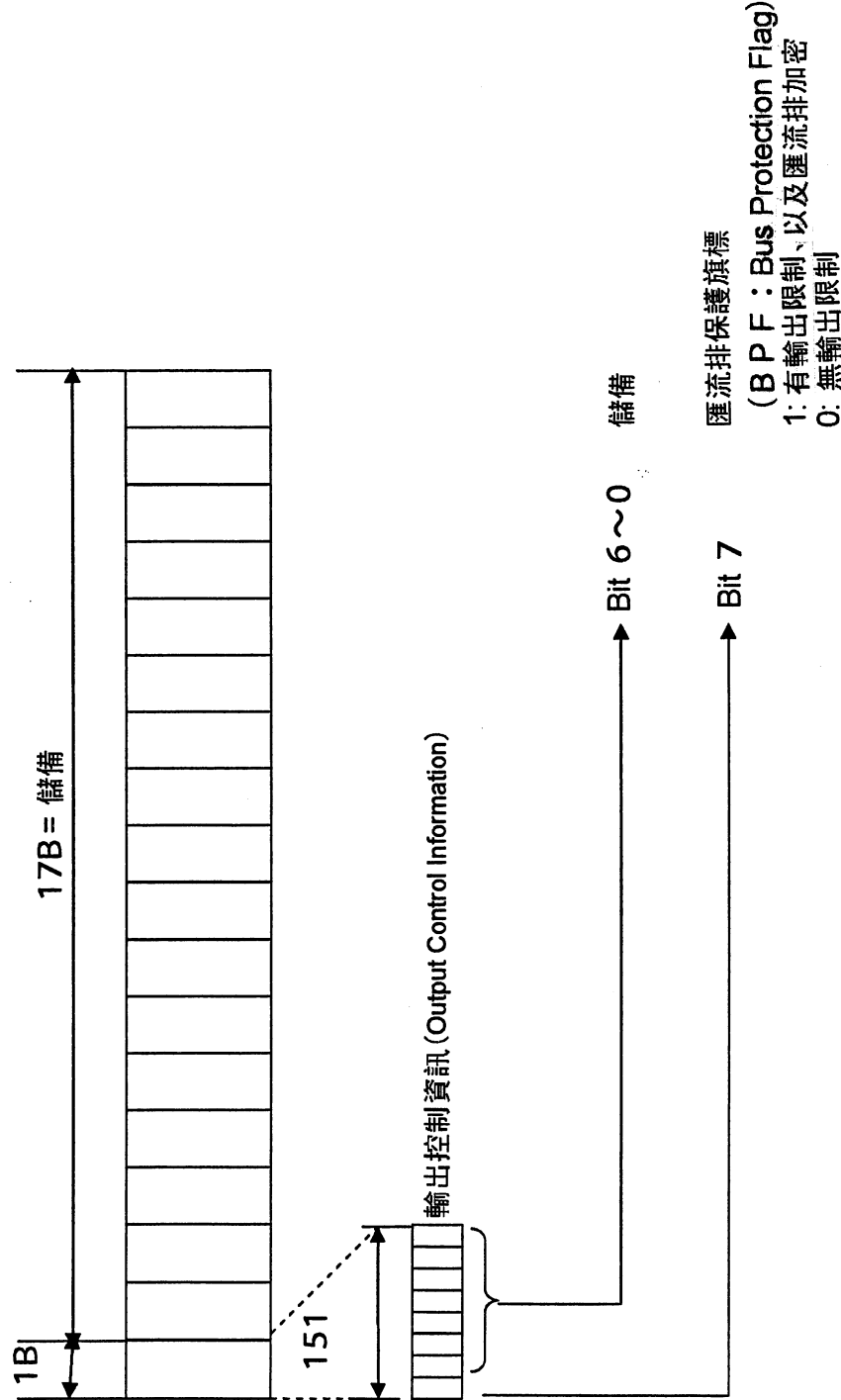


圖 8

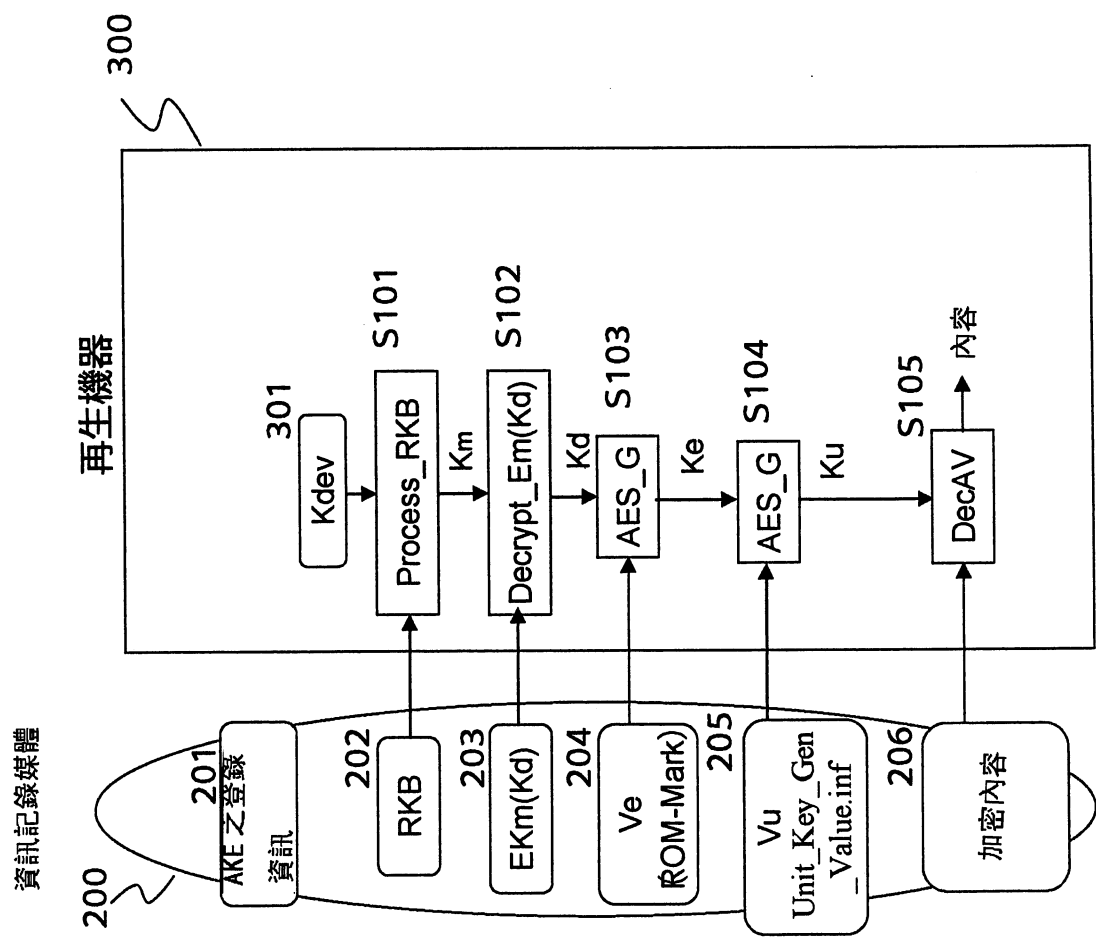


圖 9

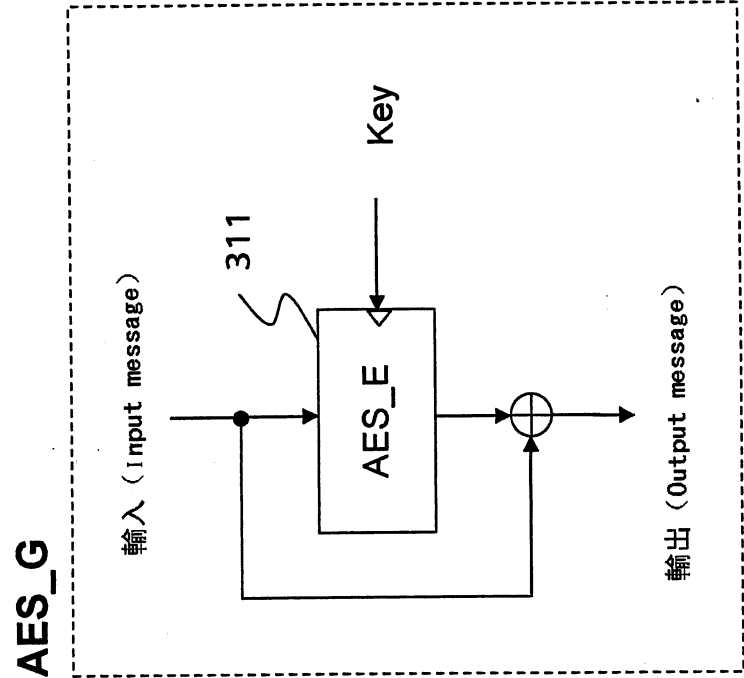


圖 10

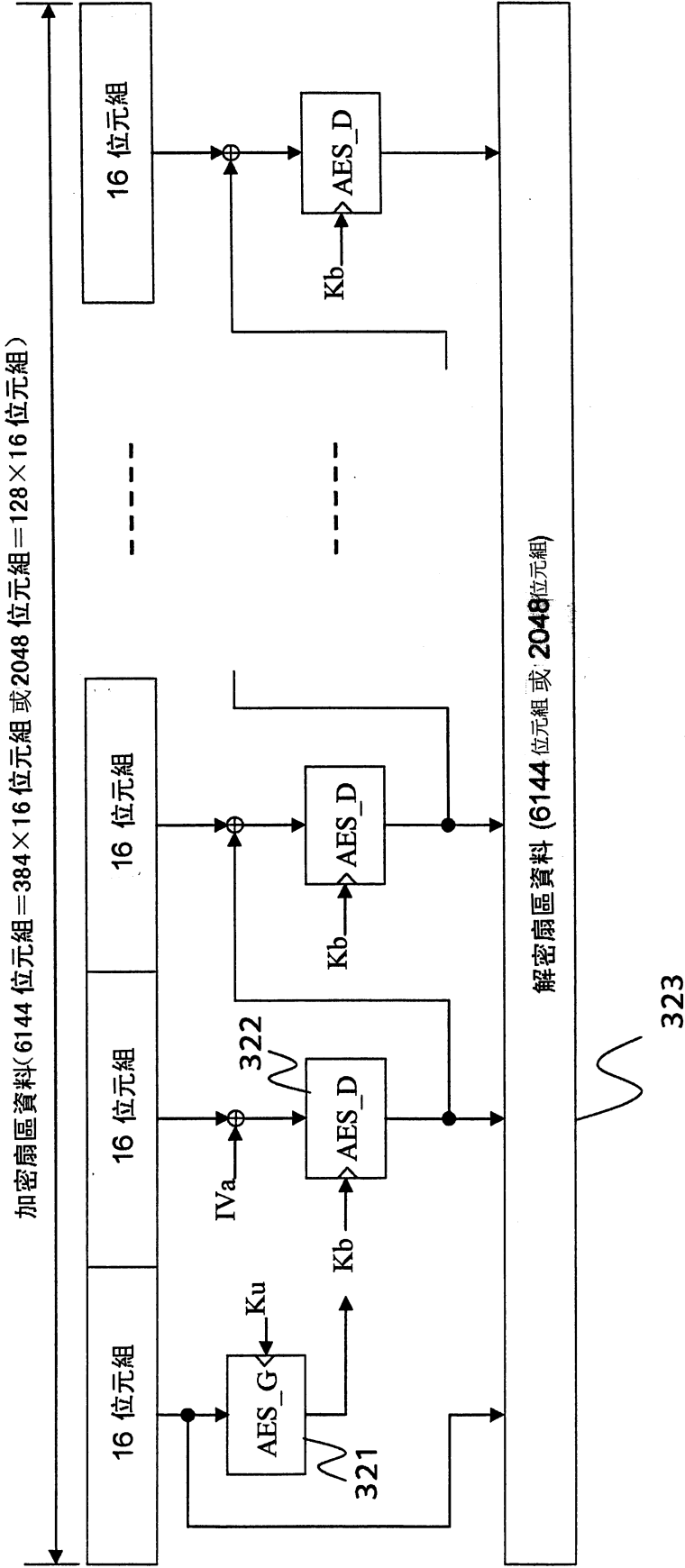


圖 11

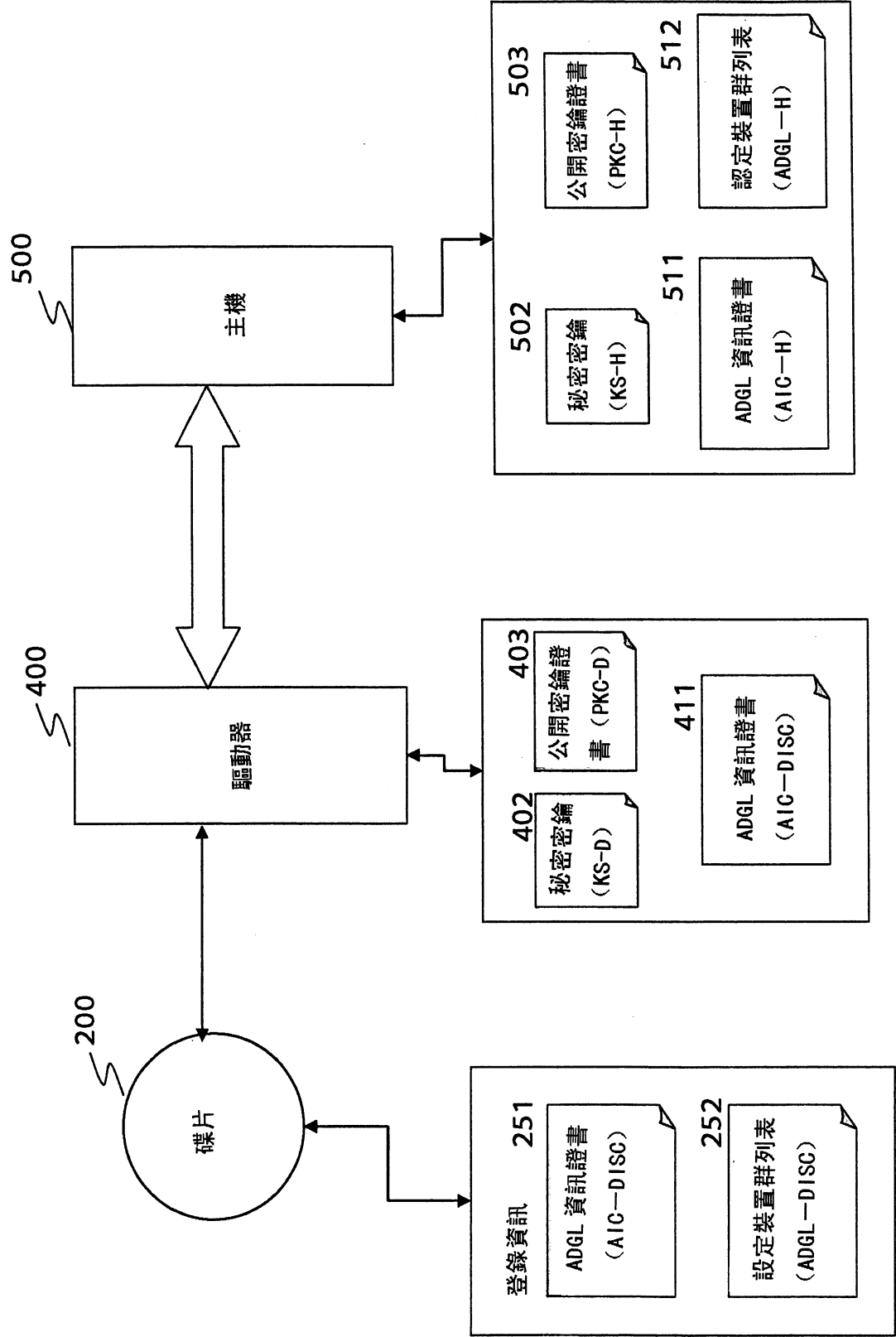
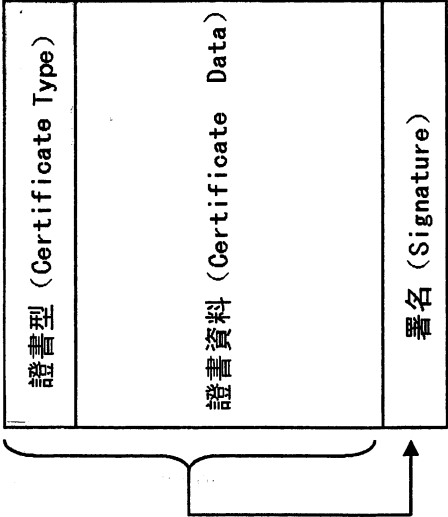


圖 12

a) 證書 (Certificate)



b) 證書型與證書之對應

證書型 (Certificate Type)	證書 (Certificate Data)
1	公開密鑰證書 (PKC: Public Key Certificate)
2	認定裝置群證書 (ADGC: Authorized Device Group Certificate)
3	ADGL 資訊證書 (AIG: ADGL Information Certificate)
其他	預留

圖 13

6) 公開密鑰證書 (PKC) 資料

證書 ID (Certificate ID)
公開密鑰 (Public Key)
其他資訊 Other information (e.g. version, issuer)

6) 使用橢圓密碼之公開密鑰證書 (PKC) 之構成例

(Public Key Certificate)

位元組	7	6	5	4	3	2	1	0
位元	證書型 = 1							
0								
1	預留							
2								
3								
:	證書 ID (40 位元)							
7								
8	公開密鑰 (320 位元)							
:								
47								
48	署名 (320 位元)							
:								
87								

圖 14

a) 認定裝置群證書 (ADGC) 資料 (Certificate Data)

認定裝置群證書資料長 (ADGC Length)
ADGL 序列號 (ADGL Sequence Number)
AIC 資料 (AIC Data)
ADGC 內之第 1 公開密鑰證書 ID (First PKC-ID in A DGC)
ADGC 內之最終公開密鑰證書 ID (Last PKC-ID in A DGC)
認定公開密鑰證書資訊 (Authorized Public Key Certificate Information)

c) 認定裝置群列表 (ADGL, Authorized Device Group List)

列表資料長 (ADGL Length)
AIC 資料 (AIC Data)
ADGCs (n) 號
ADGC_1
ADGC_2
:
ADGC_n

b) 使用橢圓密碼時認定裝置群證書構成例 (ADGC, Authorized Device Group Certificate) 資料例

位元組	7	6	5	4	3	2	1	0
位元								
0	證書型 = 2							
1	ADGC 長 (N+12 位元組)							
2								
3	ADGL 序列號							
4								
5	AIC 資料							
6								
7	ADGC 內之第 1 公開密鑰證書 ID (40 位元)							
:								
11	ADGC 內之最終公開密鑰證書 ID (40 位元)							
12								
:								
16	認定公開密鑰證書資訊 (N 位元組)							
17								
:								
N+16								
N+17								
:								
N+56	簽名 (320 位元)							

圖 15

b) 使用橢圓密碼時 ADGL 資訊證書例
(ADGL Information Certificate)

位元組		7	6	5	4	3	2	1	0
位元		證書型 = 3							
0		ADGL 序列號							
1									
2									
3		AIC 資料							
4									
5									
:		預留 (40 位元)							
9									
10									
:		簽名 (320 位元)							
49									

a) ADGL 資訊證書資料 (Certificate Data)

ADGL 序列號
AIC 資料
預留

圖 16

證書型	資訊記錄媒體	驅動器	主機
1 公開密鑰證書 (PKC)	不記錄	產品發貨時儲存於非揮發性記憶體內	產品發貨時儲存於非揮發性記憶體內
2 認定裝置群證書 (ADGC) = ADGL	向 Lead-in Area 記錄	自 Disc 讀出並向主機轉送。 自主機轉送獲得登錄有主機公開密鑰證書 之 ADGC, 利用其缺人主機之登錄。	通過驅動器獲得記錄於 Disc 之 ADGL 或 ADGC。或亦可自網絡連接之伺服器 獲得。 儲存至非揮發性記憶體 (ADGL _{HT})。
3 ADGL 資訊證書 (AIC)	向 Lead-in Area 記錄	自 Disc 讀出。或自 Host 獲得。 儲存至非揮發性記憶體 (AIC _D)。	自驅動器獲得。或亦可自連接於網絡 之伺服器獲得。 儲存至非揮發性記憶體 (AIC _H)。

圖 17

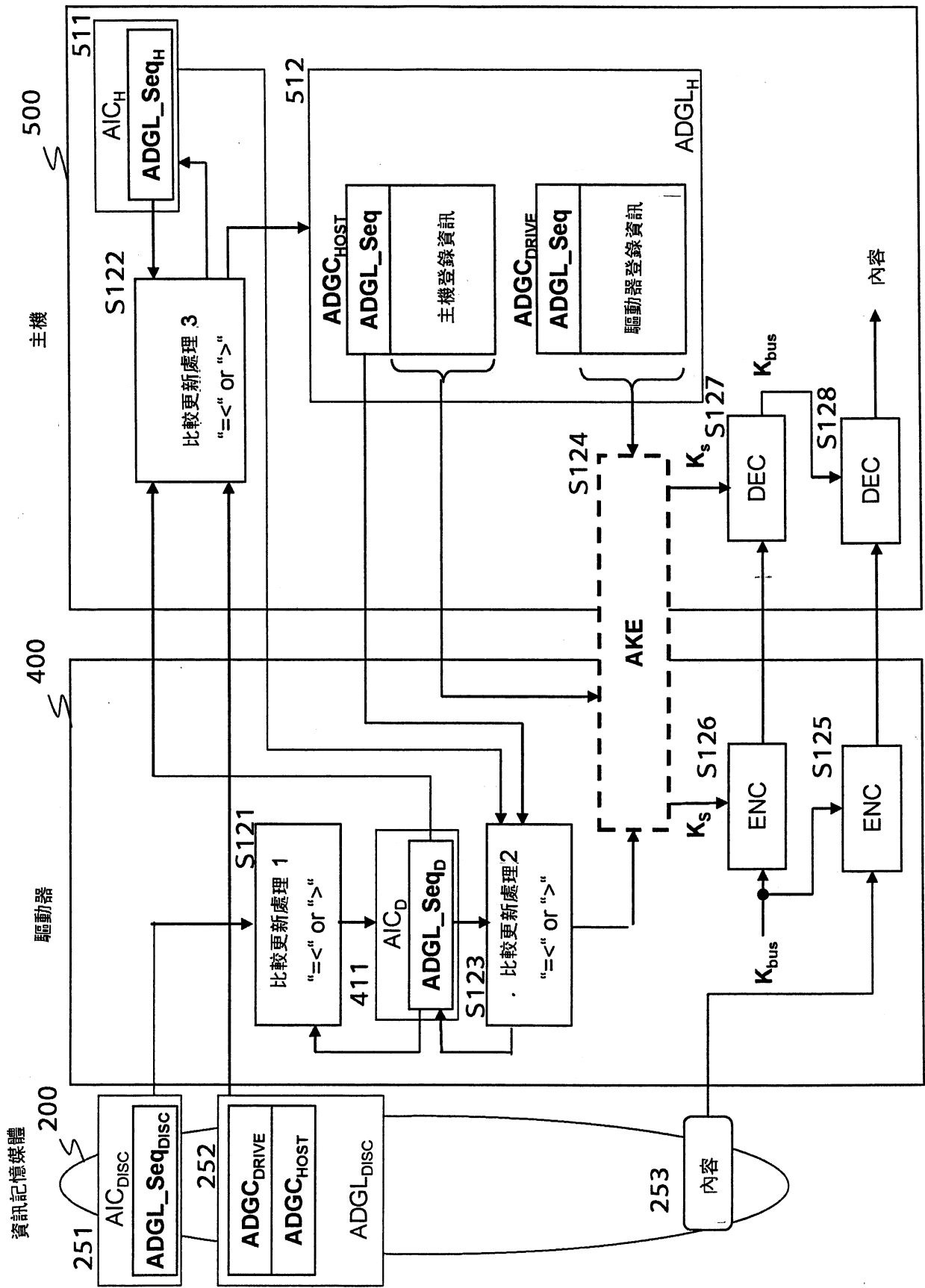


圖 18

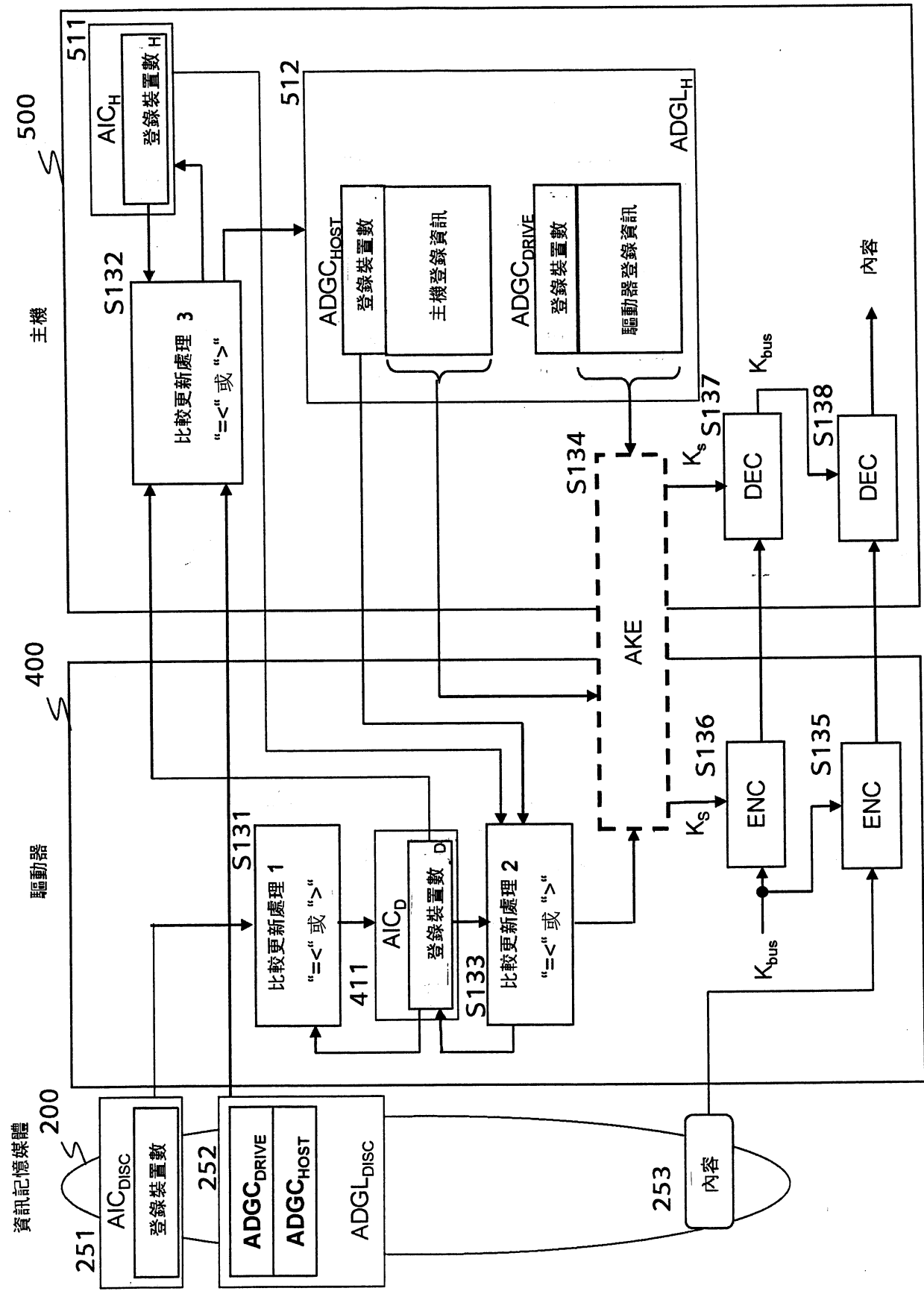


圖 19

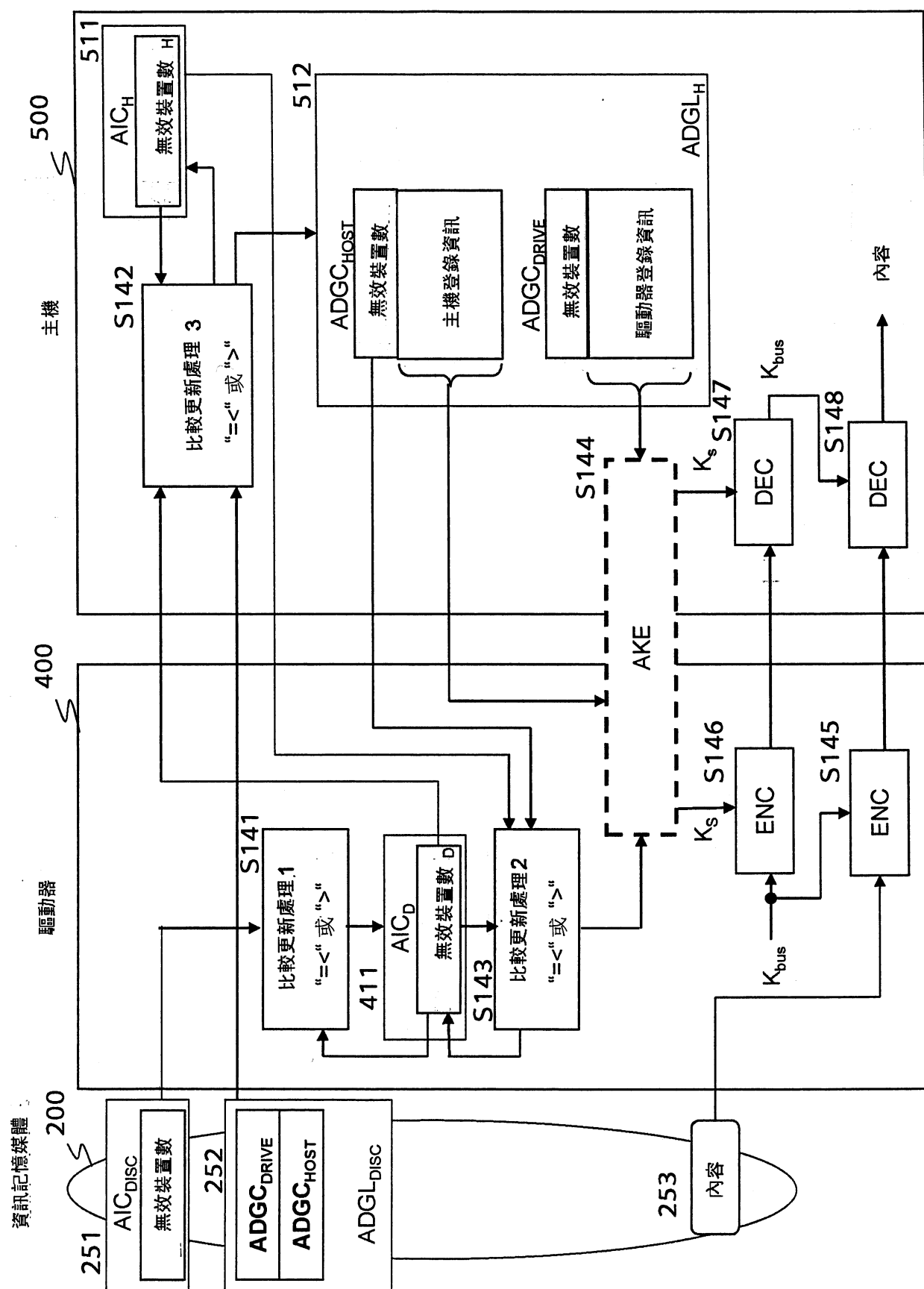
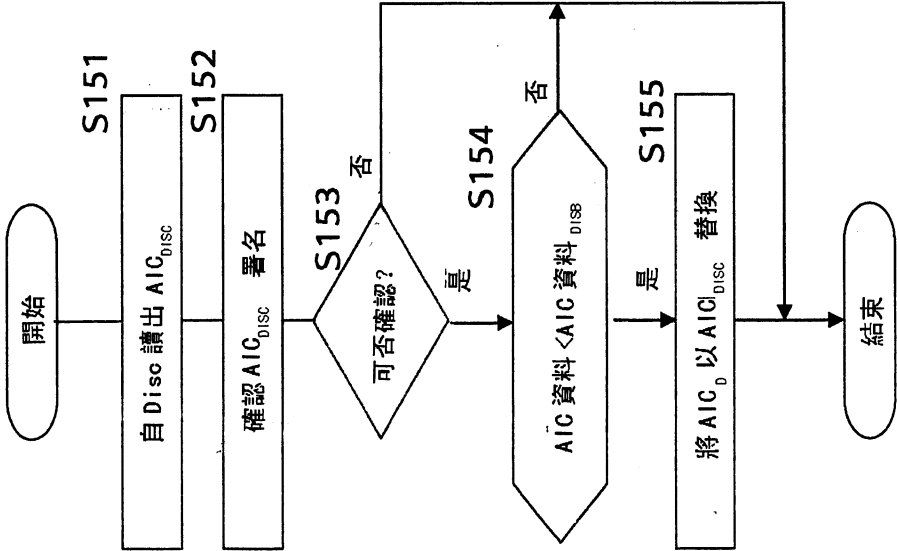


圖 20

a)

比較更新處理 1



b)

比較更新處理 2

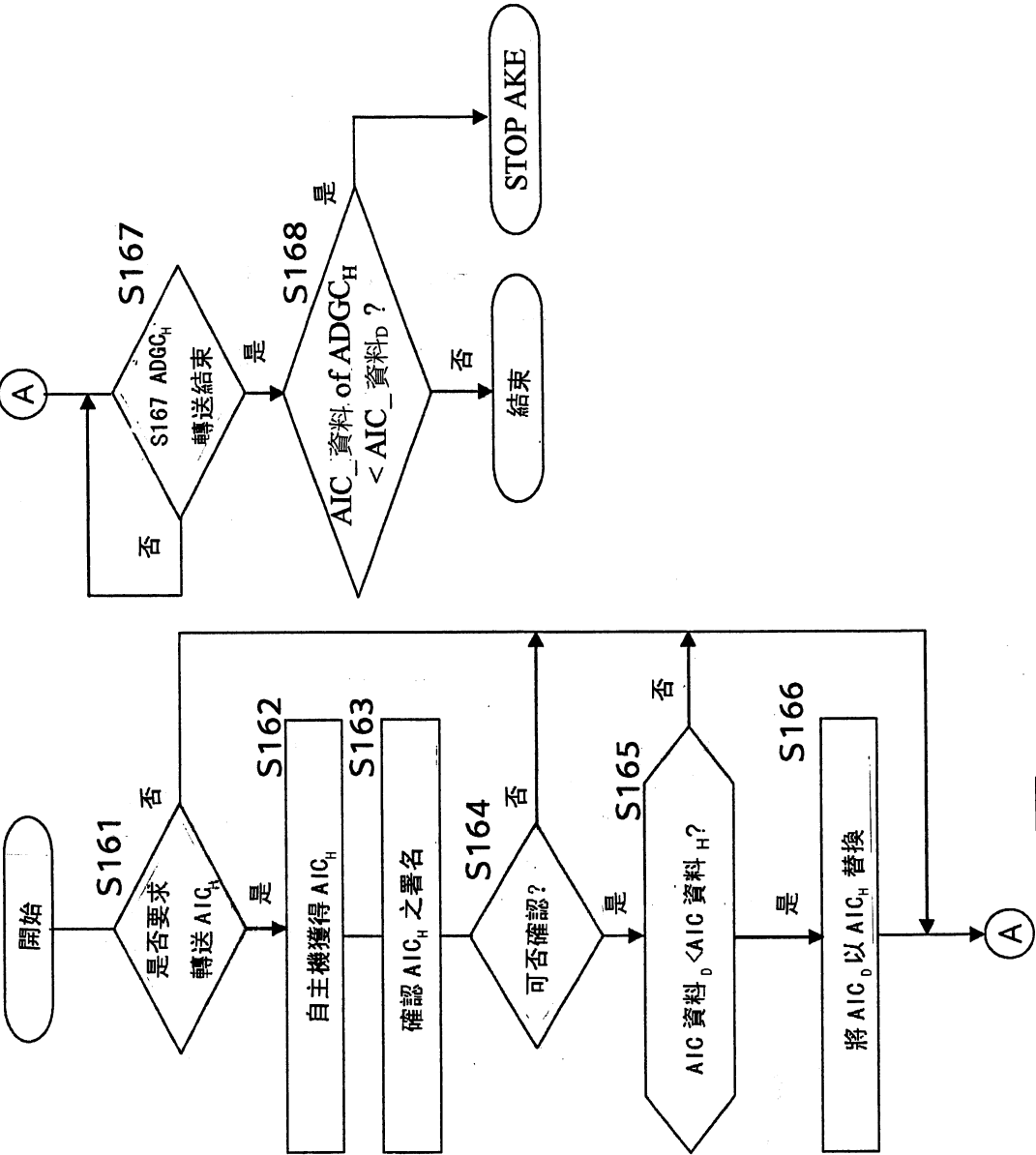


圖 21

6

比較更新處理 3

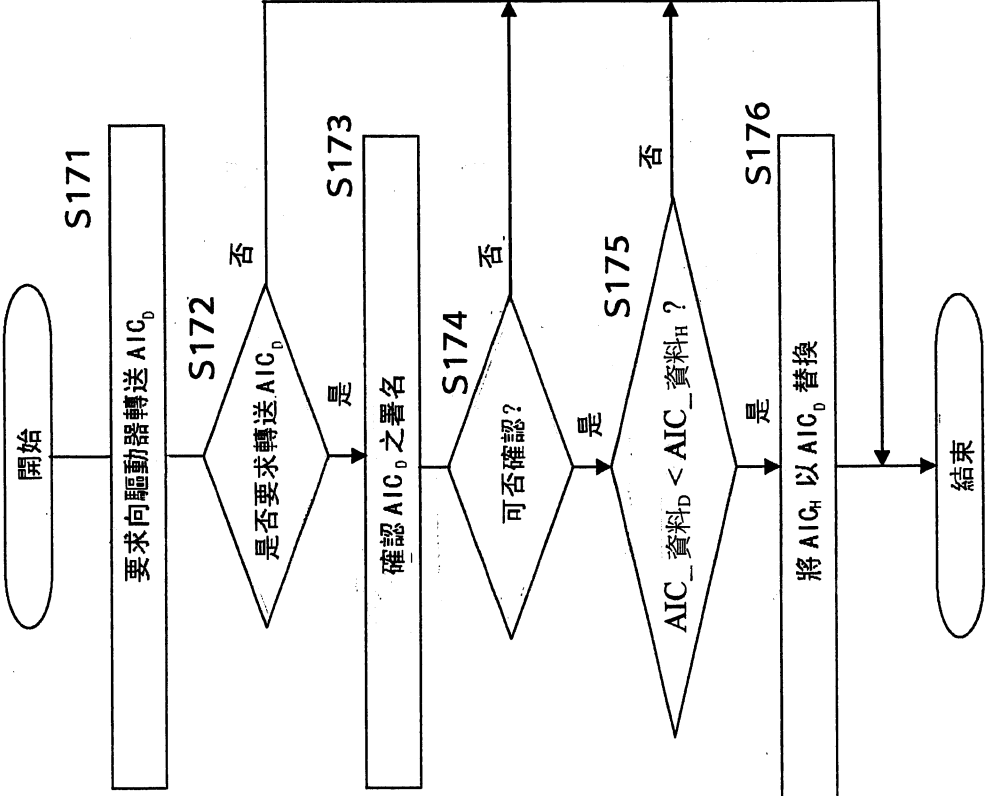


圖 22

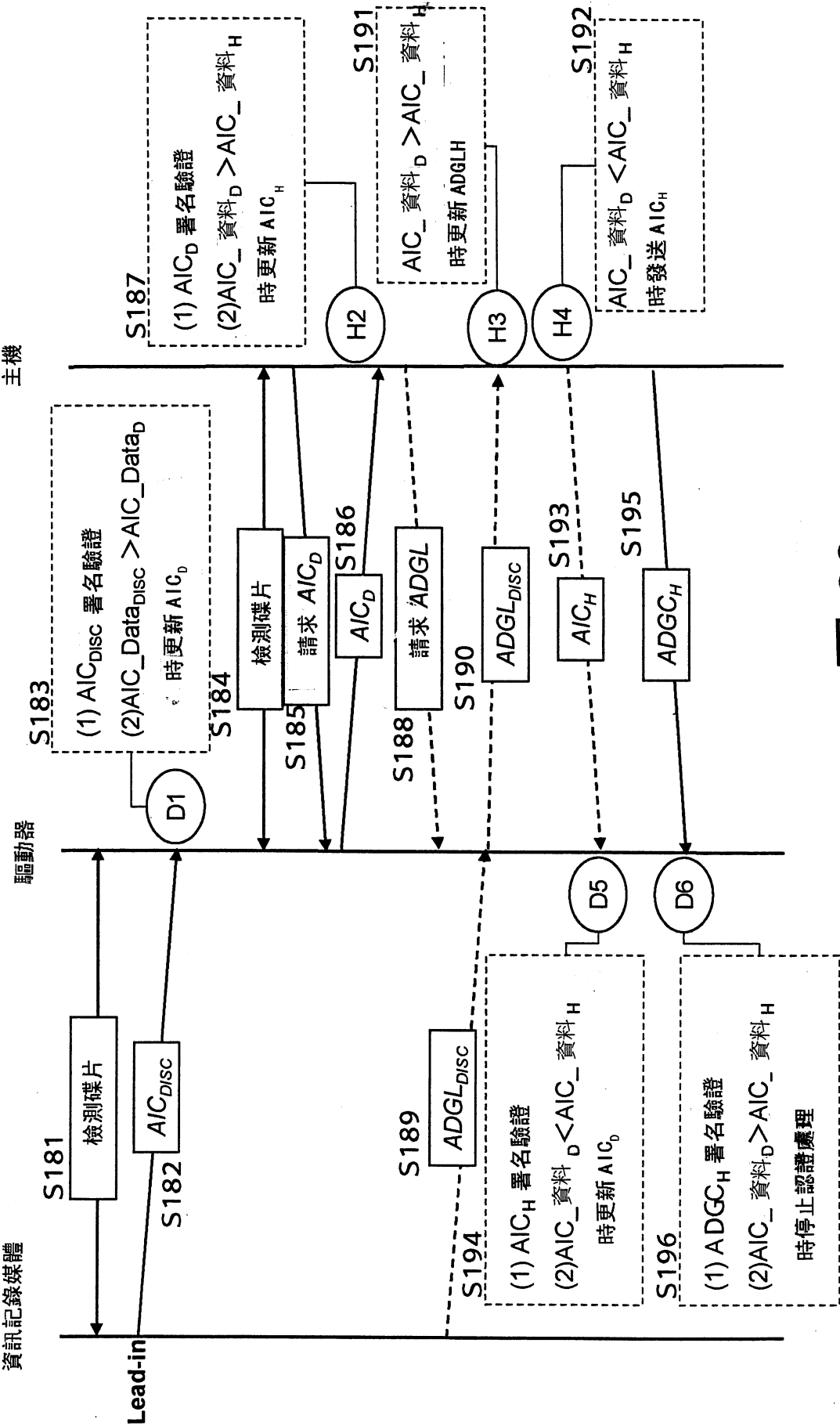


圖 23

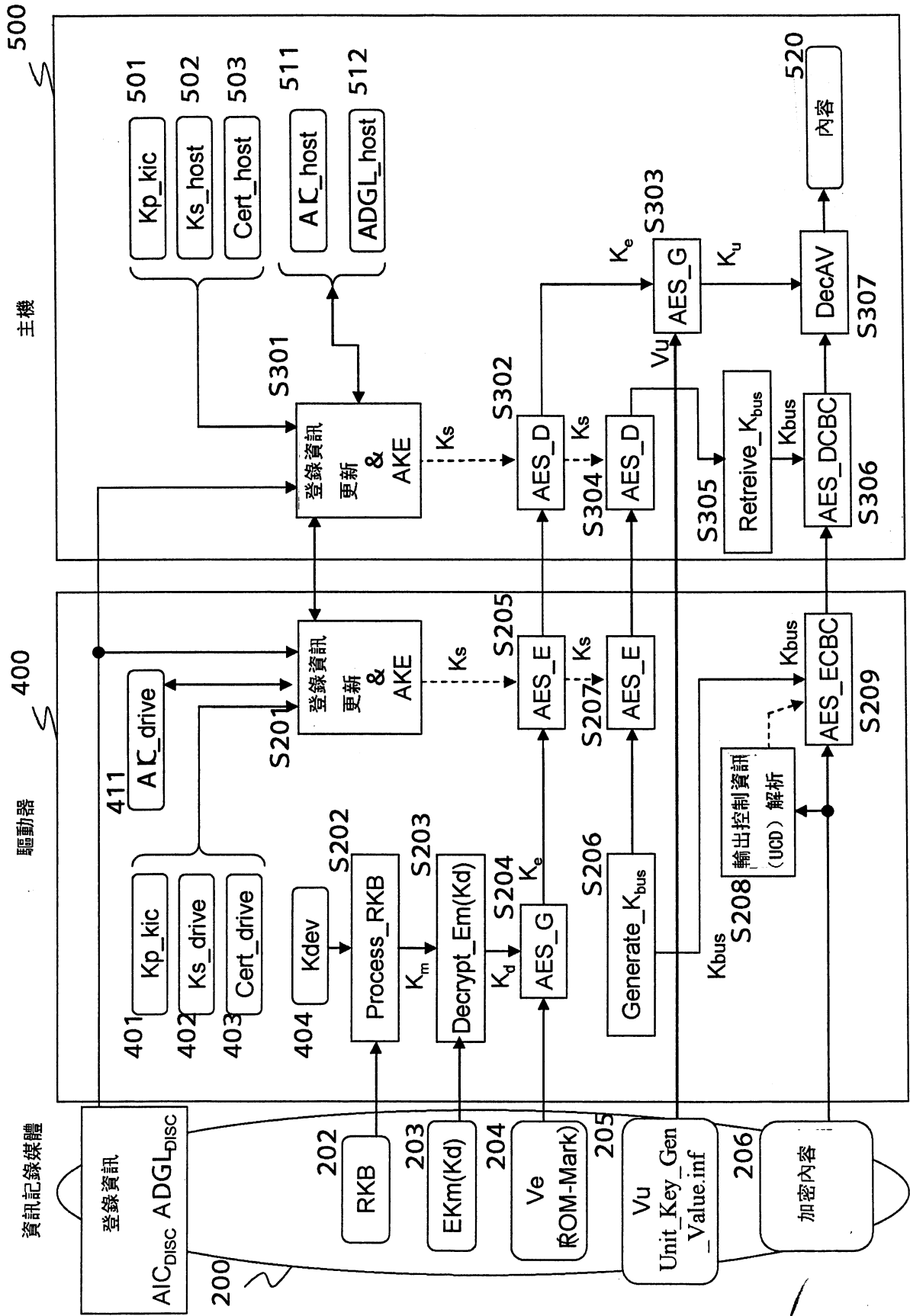


圖 24

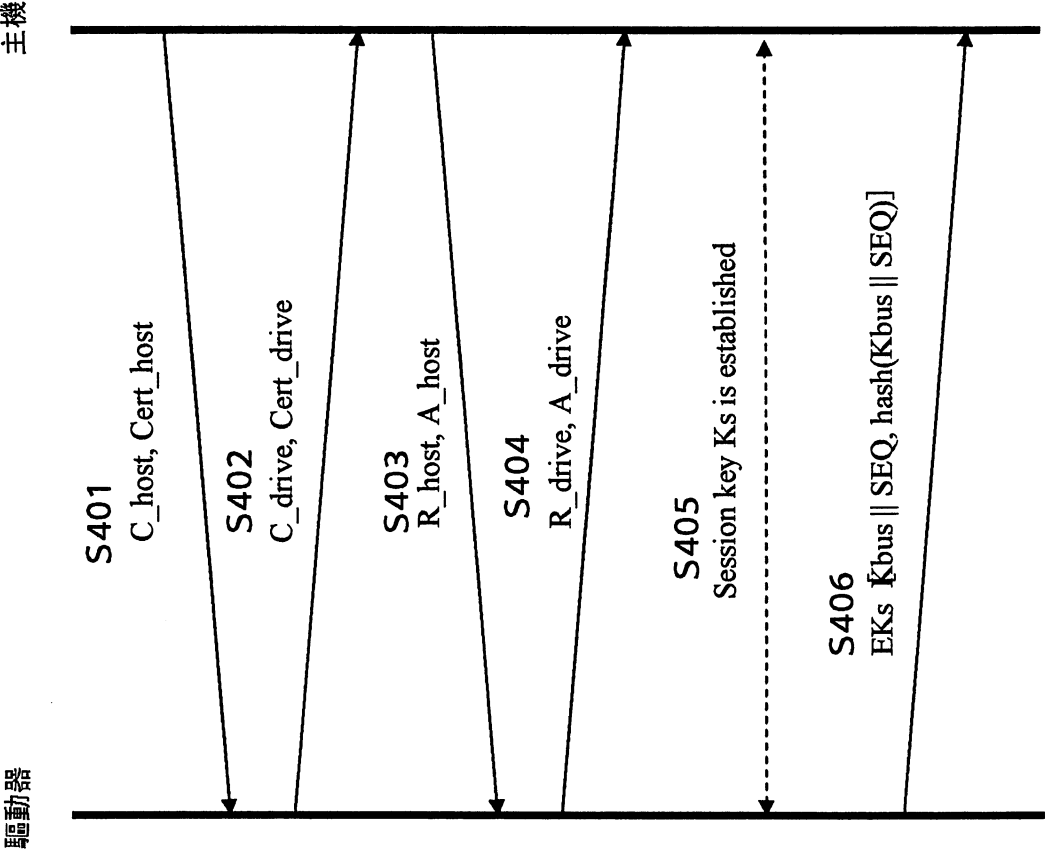
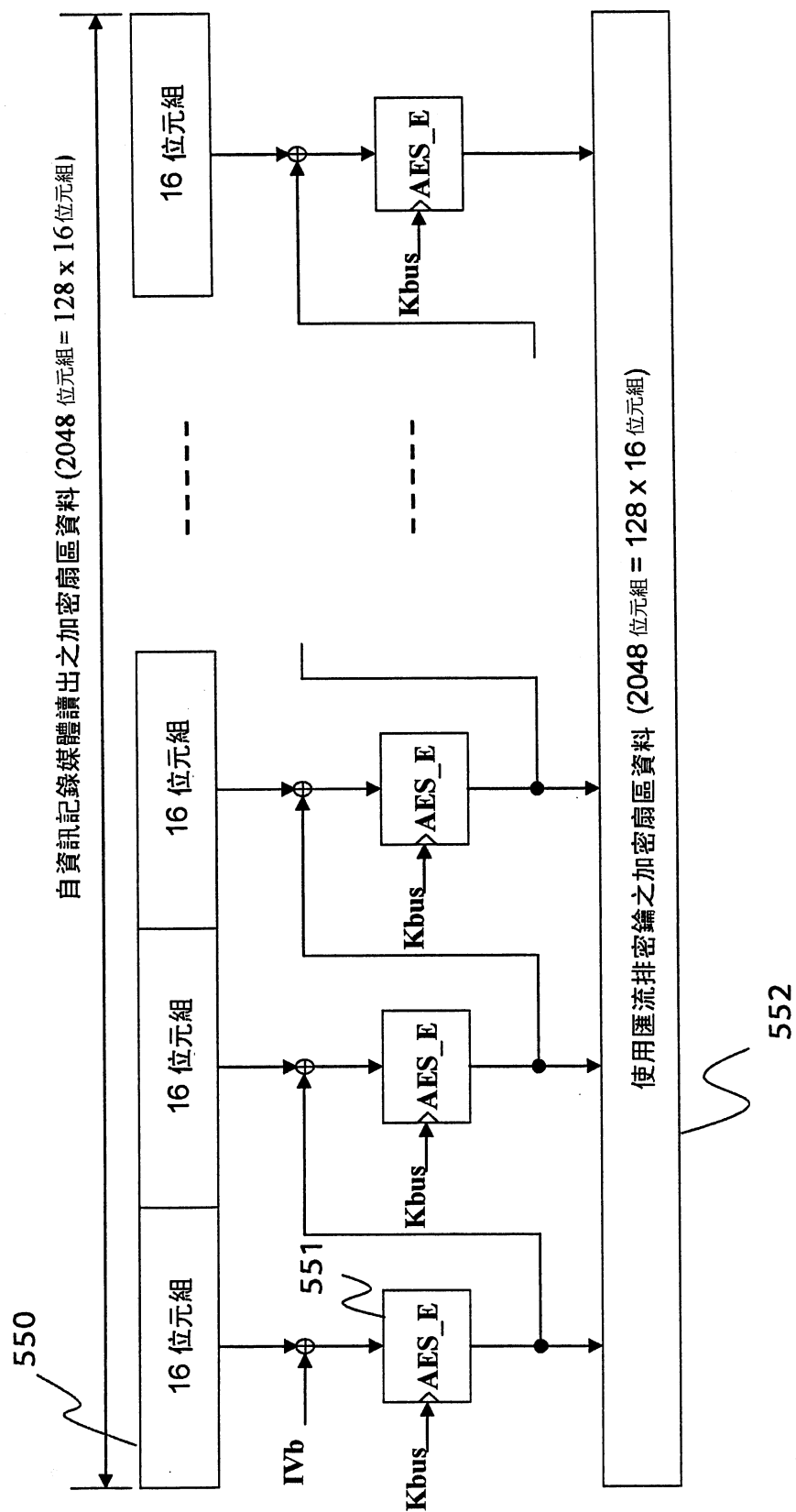


圖 25



26

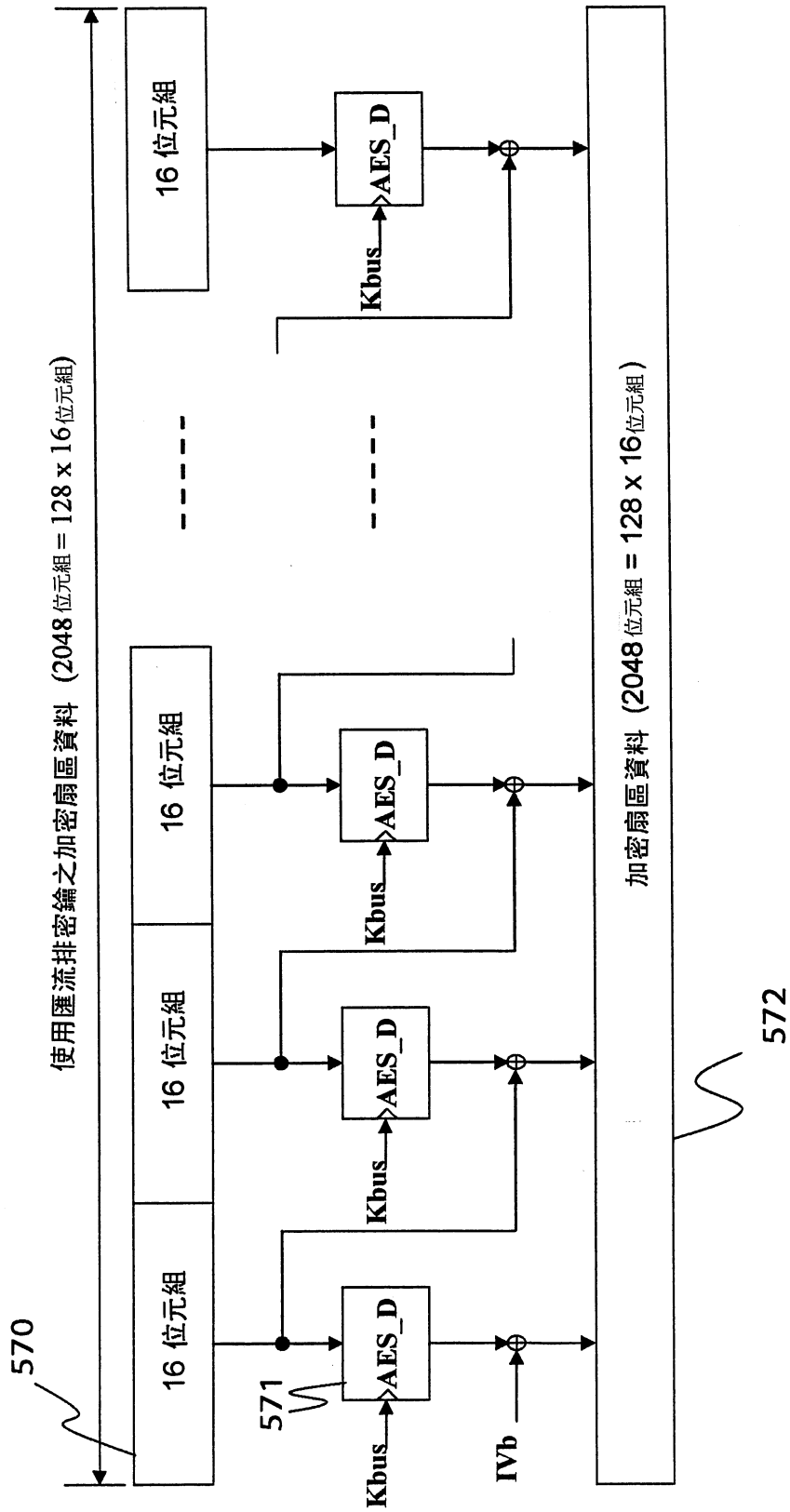


圖 27

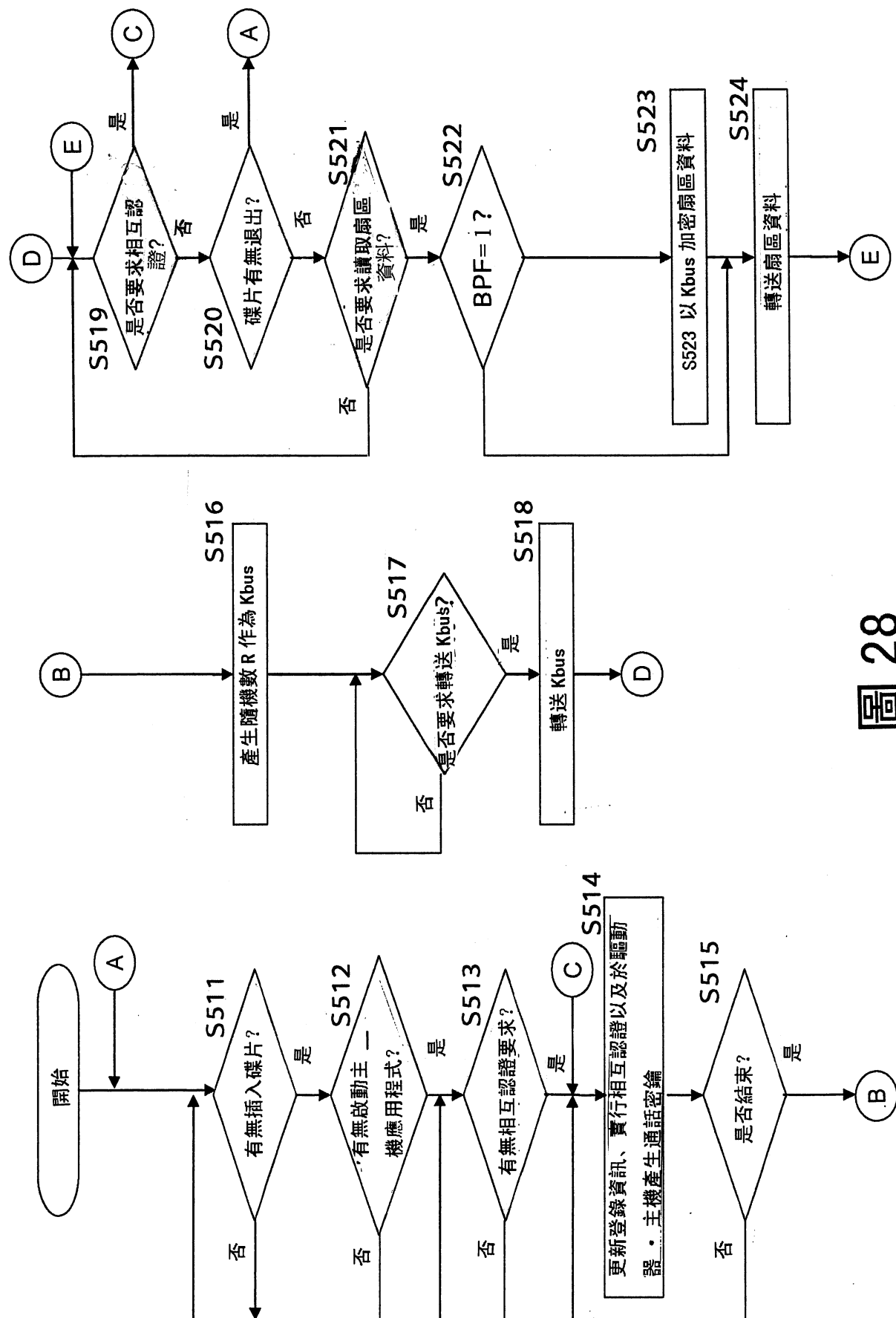


圖 28

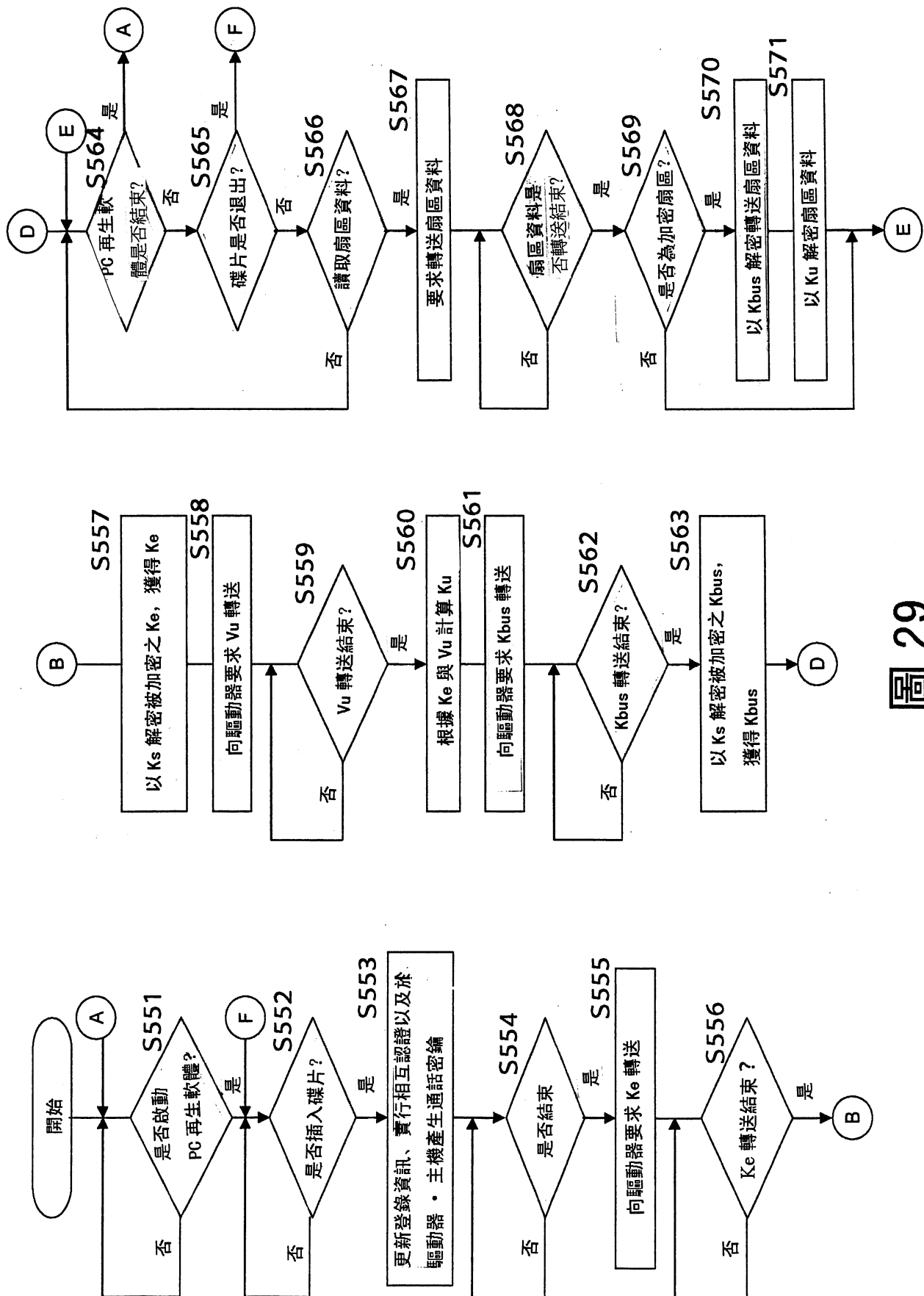


圖 29

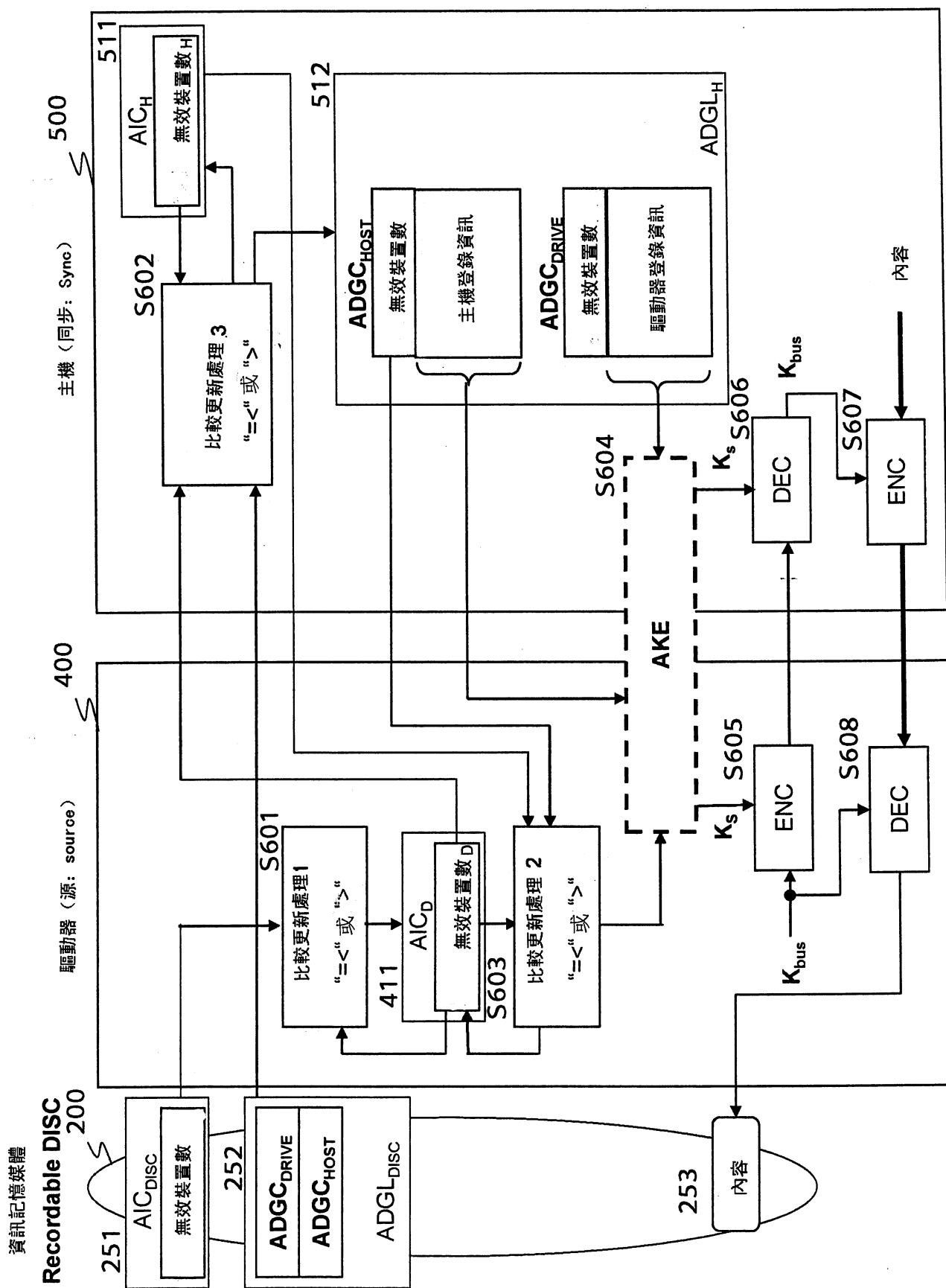


圖 30

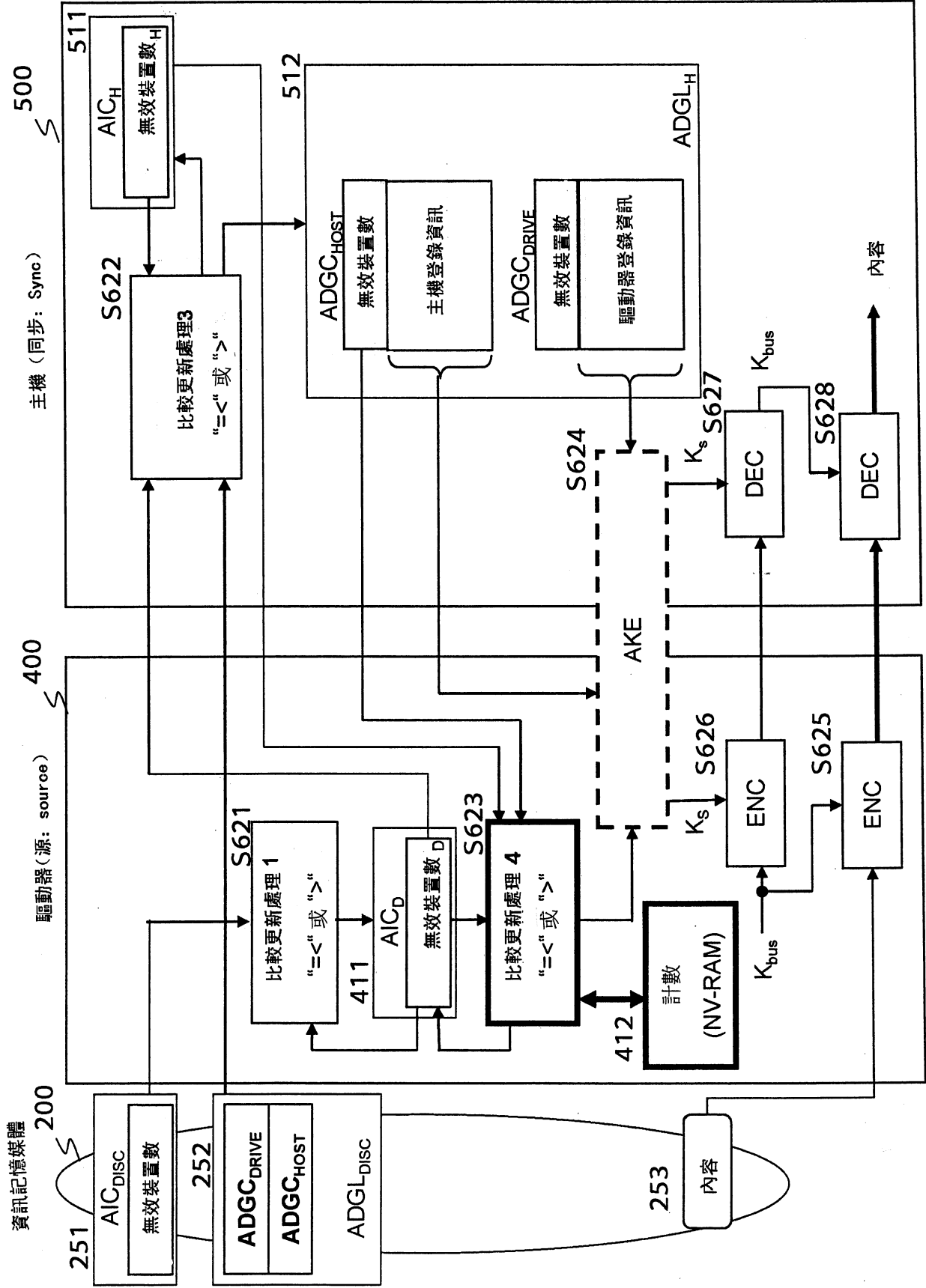


圖 31

比較更新 4

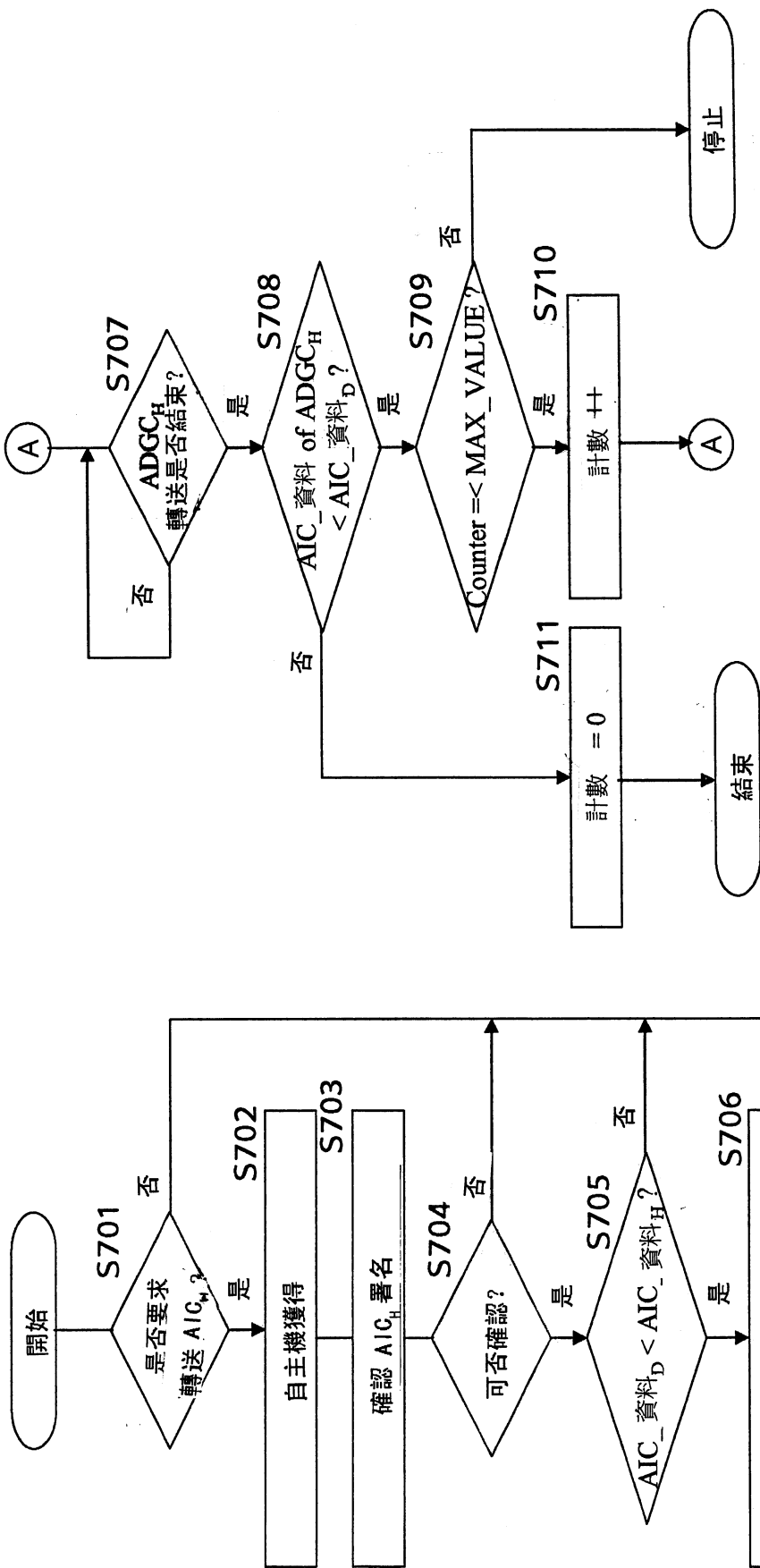


圖 32

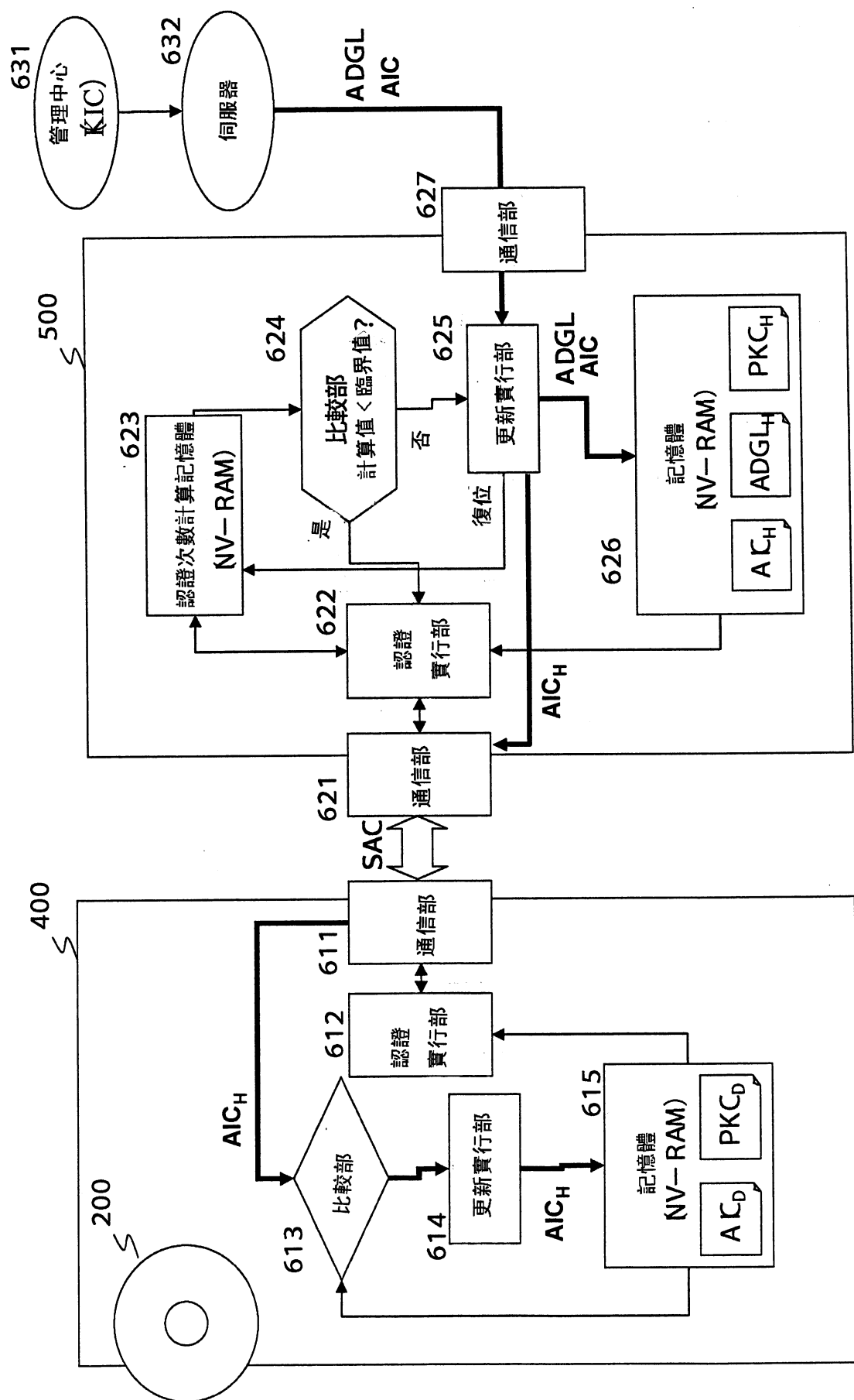


圖 33

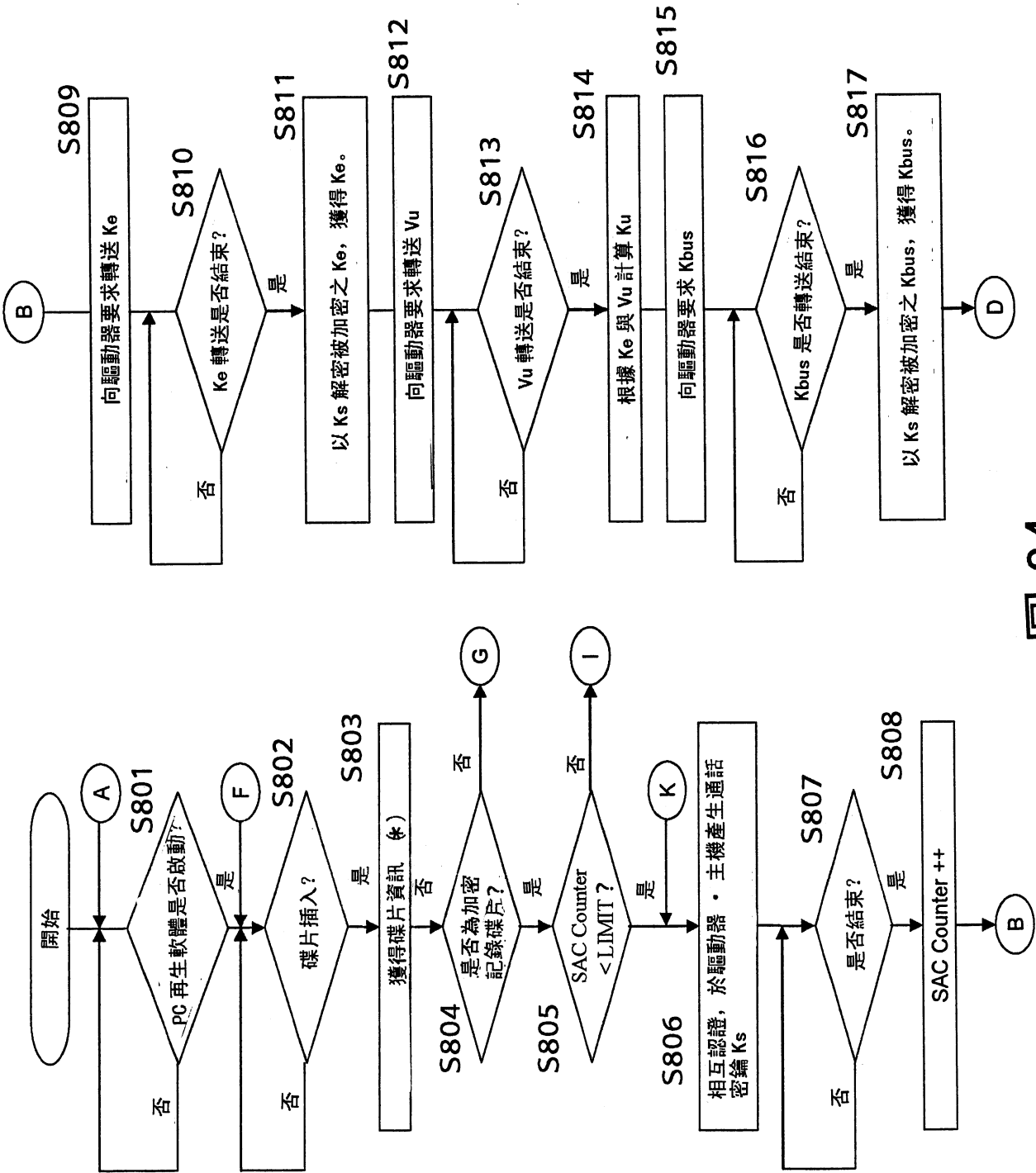


圖 34

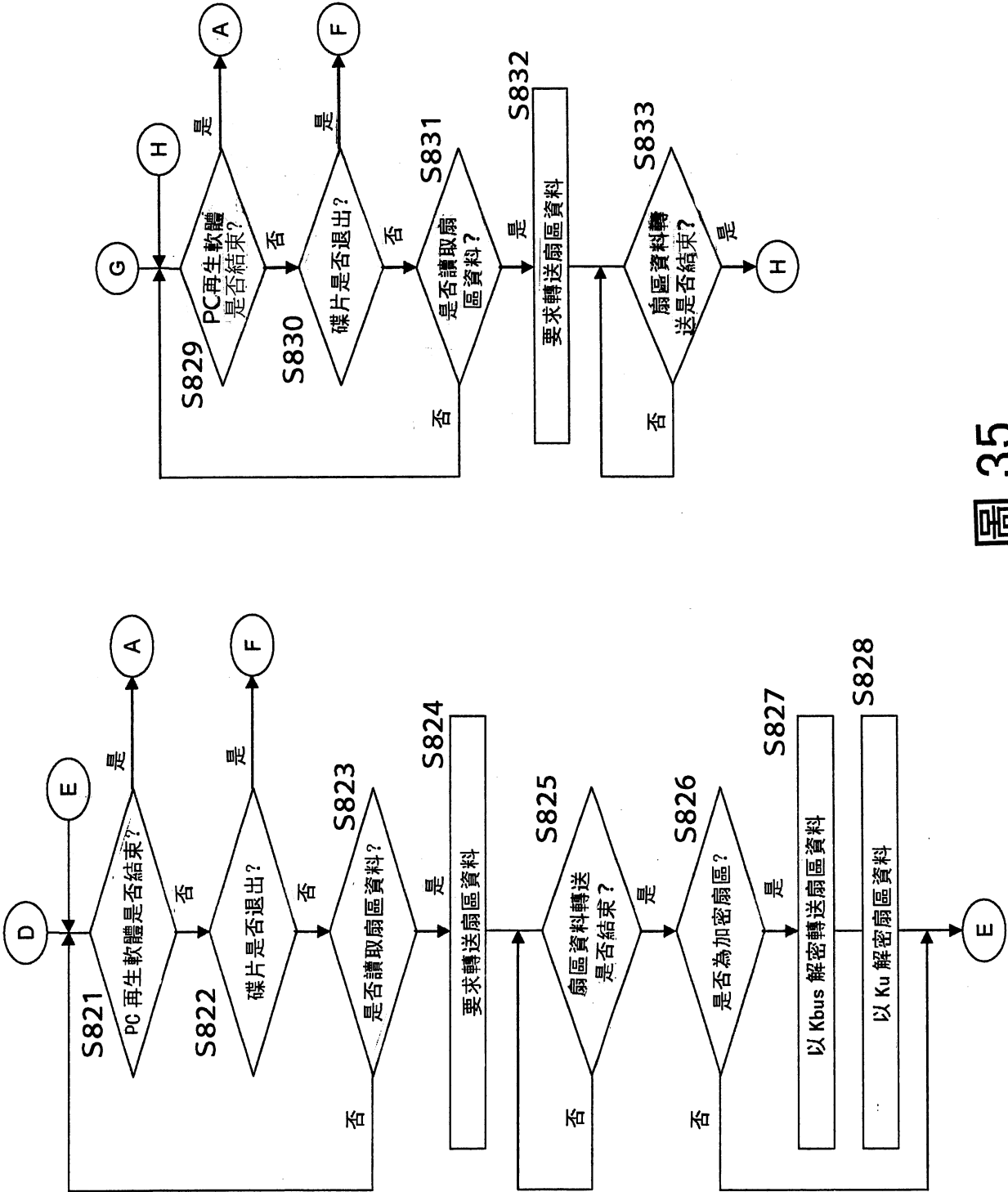


圖 35

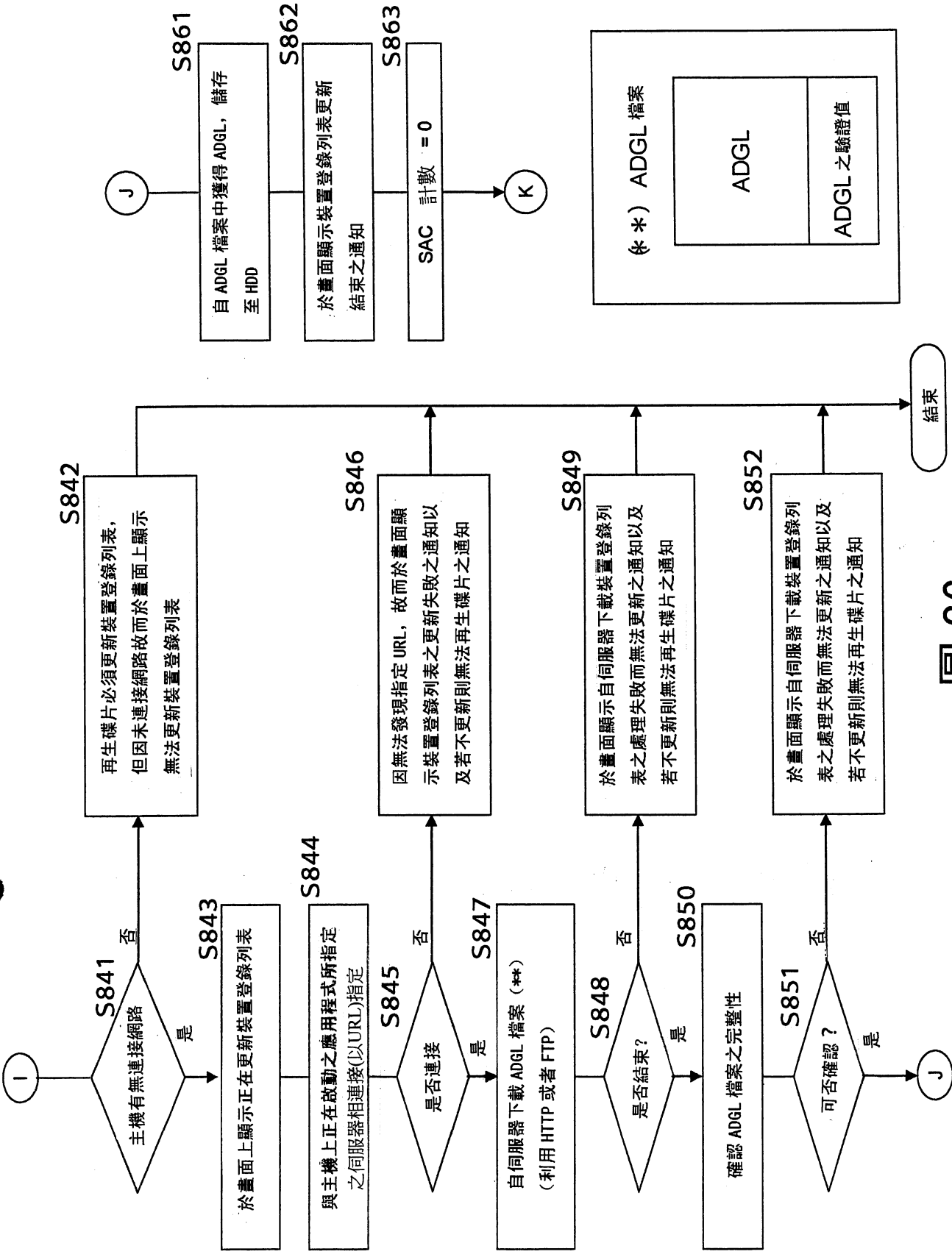


圖 36

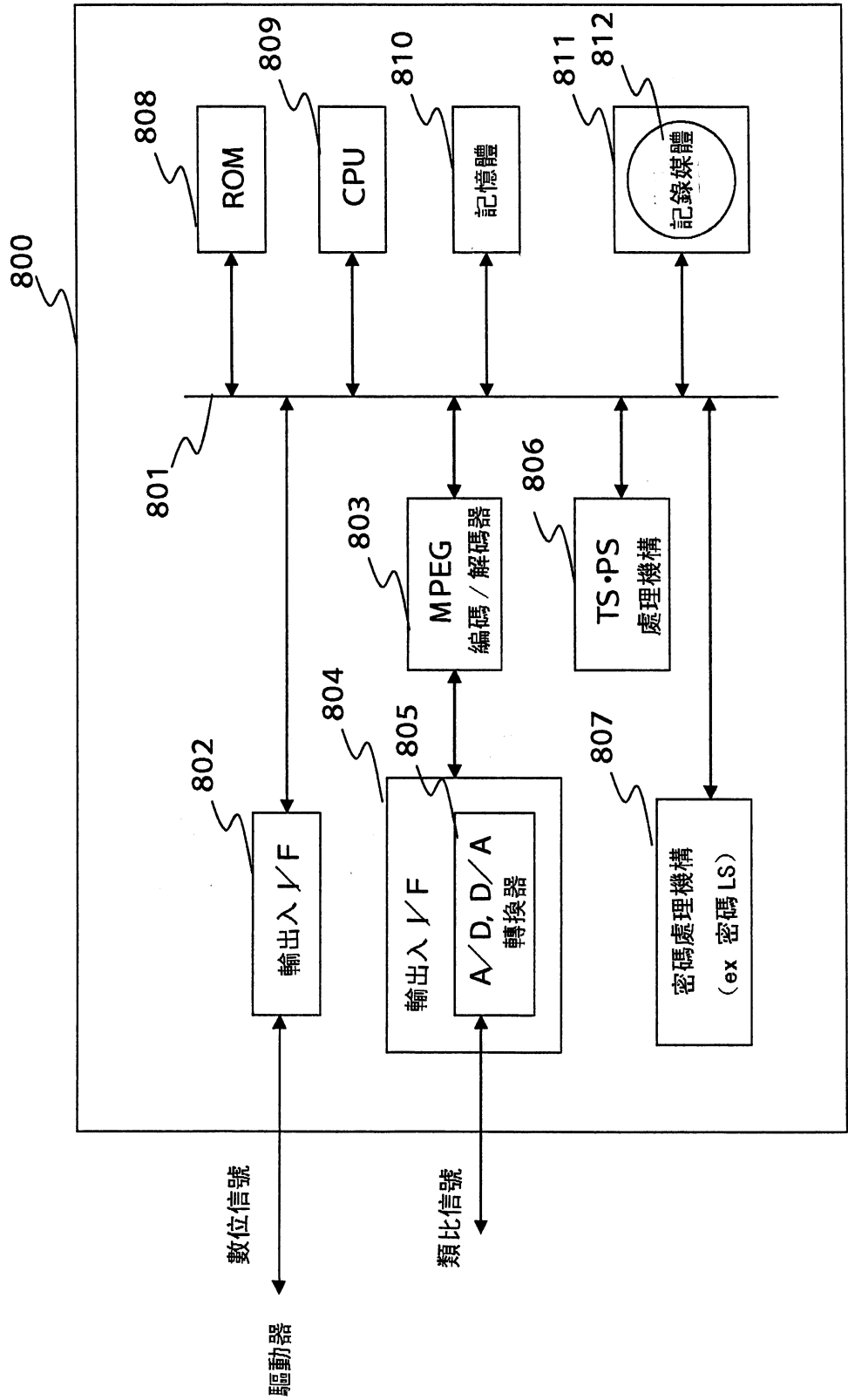


圖 37

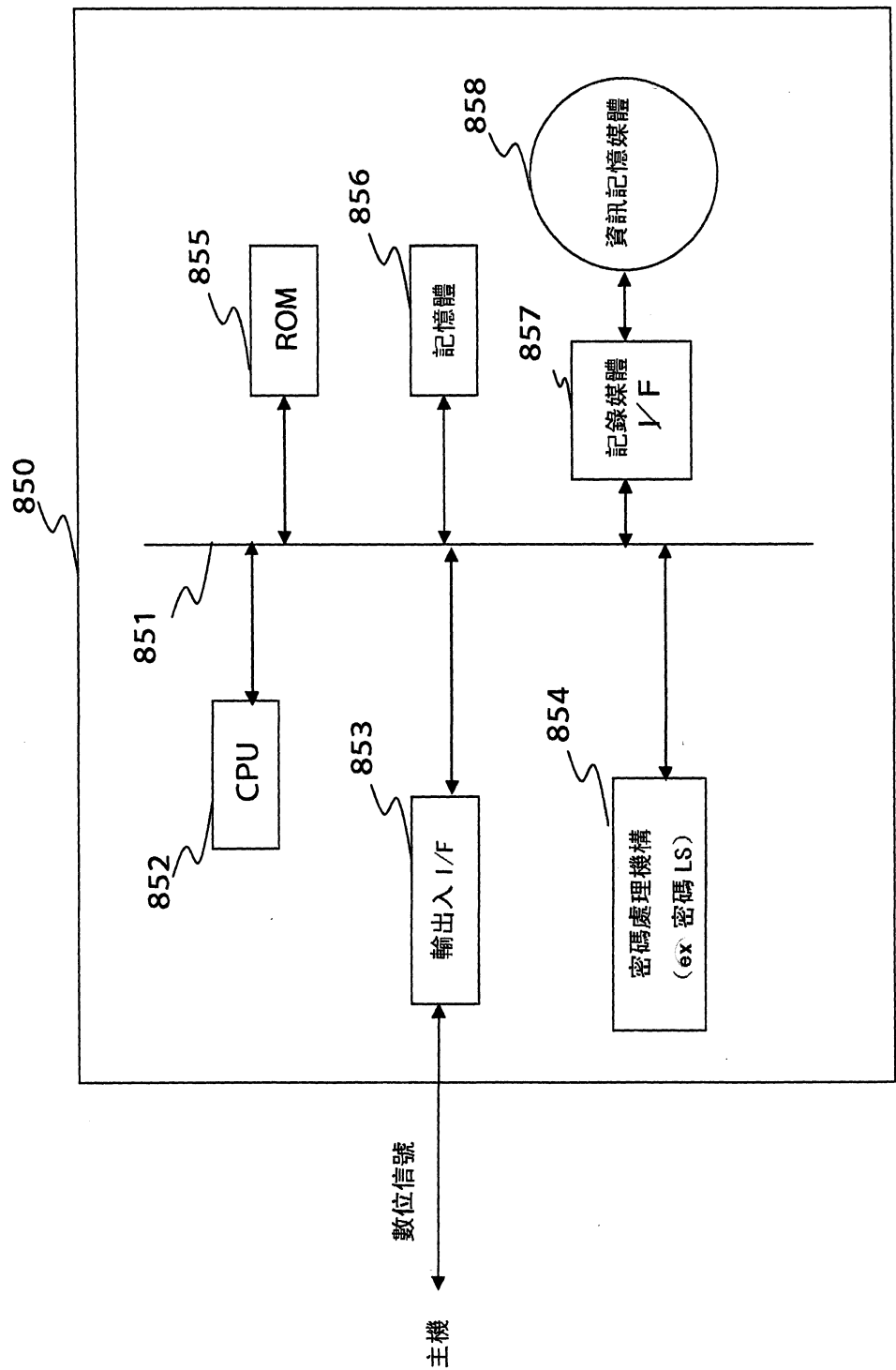


圖 38

七、指定代表圖：

(一)本案指定代表圖為：第 (32) 圖。

(二)本代表圖之元件符號簡單說明：

(無元件符號說明)

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

發明專利說明書

96年8月7日修正替換頁

中文說明書替換頁(96年8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)

公告本

※ 申請案號：094112602

※ 申請日期：94.04.20

※IPC 分類：G11B 7/00 (2006.01)

一、發明名稱：(中文/英文)

資訊處理裝置，及資訊處理方法及記錄媒體

二、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

ANDO, KUNITAKE

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

三、發明人：(共 1 人)

姓 名：(中文/英文)

木谷 聰

KITANI, SATOSHI

國 籍：(中文/英文)

日本 JAPAN

十、申請專利範圍：

1. 一種資訊處理裝置，其特徵在於：具有

證書記憶部，其儲存認定裝置證書，

認證實行部，其執行裝置之認證處理，且於該認證處理中，執行應用上述認定裝置證書之處理，以及

計算值記憶部，其計算介以上述認證實行部執行之認證次數，且儲存計算值；

上述認證實行部構成爲，以認證次數計算值未到達預先設定之認證次數上限值爲條件，執行認證處理；

且上述資訊處理裝置，進而構成爲具有更新執行部，

該更新執行部於儲存於上述計算值記憶部之認證次數計算值到達預先設定之認證次數上限值時，藉由介以通信部獲得認定裝置證書之處理，執行儲存於上述證書記憶部之認定裝置證書的更新處理。

2. 如請求項1之資訊處理裝置，其中構成爲，伴隨上述更新執行部之認定裝置證書之更新處理，對上述計算值記憶部之認證次數計算值執行重設處理。

3. 如請求項1之資訊處理裝置，其中構成爲，通過上述更新執行部之認定裝置證書之獲得，係作爲自網路連接之伺服器的獲得處理而執行。

4. 如請求項1之資訊處理裝置，其中構成爲，具有更新執行部，上述更新執行部對自外部獲得之認定裝置證書執行正當性確認處理，且於確認為正當性時，對儲存於上述證書記憶部之認定裝置證書執行更新處理。

5. 如請求項1之資訊處理裝置，其中構成為，上述資訊處理裝置於認證次數計算值到達預先設定之認證次數上限值時，對用戶執行通知處理。
6. 如請求項1之資訊處理裝置，其中構成為，上述更新執行部將自外部獲得之證書之至少一部分證書資料作為儲存於認證處理對象的驅動器之證書資料而輸出至驅動器。
7. 如請求項6之資訊處理裝置，其中構成為，儲存於上述驅動器之證書資料為含有使用於認定裝置證書之新舊比較的資料之證書。
8. 如請求項7之資訊處理裝置，其中構成為，使用於上述認定裝置證書之新舊比較的資料為記錄於認定裝置證書之序列號、登錄裝置數、或無效(Revoke)裝置數中之任一種資料。
9. 一種資訊處理方法，其特徵在於包含：
比較步驟，其對儲存於計算值記憶部之認證次數計算值與預先設定之認證次數上限值執行比較處理；
認證步驟，其以獲得認證次數計算值未到達預先設定之認證次數上限值的比較結果為條件，執行認證處理；
以及
更新步驟，其於儲存於上述計算值記憶部之認證次數計算值到達預先設定之認證次數上限值時，介以通信部對認定裝置證書執行獲得處理，對儲存於證書記憶部之認定裝置證書執行更新處理。
10. 如請求項9之資訊處理方法，其中進而具有伴隨上述認證

步驟結束，執行計算出儲存於計算值記憶部之認證次數計算值的處理之步驟。

11. 如請求項9之資訊處理方法，其中伴隨上述更新步驟之認定裝置證書之更新處理，對上述計算值記憶部之認證次數計算值執行重設處理。
12. 如請求項9之資訊處理方法，其中上述更新步驟中認定裝置證書之獲得作為自網路連接之伺服器獲得的處理而執行。
13. 如請求項9之資訊處理方法，其中上述更新步驟執行自外部獲得之認定裝置證書之正當性確認處理，於確認為正當性時對儲存於上述證書記憶部之認定裝置證書執行更新處理。
14. 如請求項9之資訊處理方法，其中進而於認證次數計算值到達預先設定之認證次數上限值時，對用戶執行通知處理。
15. 如請求項9之資訊處理方法，其中進而具有
將上述更新步驟中自外部獲得之證書之至少一部分證書資料作為儲存於用作認證處理對象的驅動器之證書資料而輸出至驅動器的步驟。
16. 如請求項15之資訊處理方法，其中儲存於上述驅動器之證書資料為含有應用於對認定裝置證書執行新舊比較的資料之證書。
17. 如請求項16之資訊處理方法，其中應用於對上述認定裝置證書加以新舊比較之資料為記錄於認定裝置證書之序

列號、登錄裝置數、或無效(Revoke)裝置數中之任一種資料。

18. 一種電腦可讀取之記錄媒體，其特徵在於記錄程式，該程式含有：

比較步驟，其對儲存於記憶部之認證次數計算值與預先設定之認證次數上限值執行比較處理；

認證步驟，其以獲得認證次數計算值未到達預先設定之認證次數上限值的比較結果為條件，執行認證處理；以及

更新步驟，其於儲存於上述記憶部之認證次數計算值到達預先設定之認證次數上限值時，介以通信部對認定裝置證書執行獲得處理，對儲存於證書記憶部之認定裝置證書執行更新處理。