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03月05日；特願2004-062959

2.

☐ 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、認證處理方法及電腦程式。更詳細而言，係關於實現防止內容不正當利用之資訊處理裝置、認證處理方法及電腦程式。

【先前技術】

近年來，利用、開發出DVD及藍色雷射光碟(Blu-ray Disc)等可儲存大容量資料之光碟，可保存及重現大容量資料之高精密度圖像及高品質聲音。此外，此等大容量記錄媒體之重現環境，除先前之家庭用記錄重現裝置之外，亦開發出各種搭載高性能之CUP及視訊卡之個人電腦(PC)及其他資訊重現裝置來利用。

如在PC中進行內容重現時之問題，如有內容之著作權保護。音樂資料及圖像資料等許多內容，通常其製作者或販賣者擁有頒發權等。因此，此等內容分發時，通常係採取一定之利用限制，亦即僅對正式之使用者，許可利用內容，不進行未經許可之複製等之構造。

特別是藉由數位記錄裝置及記錄媒體，不致使圖像及聲音惡化而可重複記錄及重現，而發生不正當複製之內容經由網際網路傳送，及在CD-R、DVD等記錄媒體中複製內容之海盜版光碟流通之問題。

DVD及藍色雷射光碟等之大容量型記錄媒體中儲存有著作權保護對象之各種影像資訊及音樂資訊作為數位資料，而在市場上流通。使記錄此種數位資料之媒體在市場上流

通情況下，必須採取謀求防止不正當複製之著作權人保護之構造。最近，為了防止此種數位資料之不正當複製，而開發出在數位記錄裝置及記錄媒體中防止違法複製用之各種技術。

如DVD播放機採用內容攪拌系統(CSS：Content Scramble System)。內容攪拌系統系在記錄媒體，如DVD-ROM(唯讀記憶體)中，將視頻資料及聲頻資料等予以加密來記錄，而將用於其加密資料解碼之鍵，僅供給獲得執照之播放機。執照僅供給以遵照不進行不正當複製等之特定動作規定之方式設計之播放機。因此，獲得執照之播放幾可利用供給之鍵，藉由將記錄於資訊記錄媒體中之加密資料予以解碼，來重現圖像及聲音。

另外，未獲得執照之播放機，由於並無將加密之資料解碼用之鍵，因此無法進行記錄於資訊記錄媒體中之加密資料之解碼。如此，內容攪拌系統(CSS)提供僅擁有正式執照之播放機許可利用內容之系統。

但是，該內容攪拌系統(CSS)存在無法確實排除內容之不正當利用之問題。特別是自安裝資訊記錄媒體之驅動器輸出內容至PC等之資訊處理裝置而重現之處理中，會發生可進行內容之不正當利用之問題。以下參照圖式來說明該問題。

圖1顯示儲存採用內容攪拌系統(CSS)之內容之資訊記錄媒體之儲存資料例與重現機器(播放機)之處理。

圖1所示之資訊記錄媒體10如為DVD光碟，資訊記錄媒體

10中儲存有：加密光碟鍵(Secured Disc Key)11，儲存於資訊記錄媒體10中之內容標題對應之加密標題鍵12及依據CSS方式經過攪拌處理之內容之攪拌MPEG資料13。

安裝資訊記錄媒體10來執行內容重現之重現機器20，如DVD播放機，應用儲存於重現機器20之主鍵，於步驟S11中，執行自資訊記錄媒體10取得之加密光碟鍵(Secured Disc Key)11之解碼處理，而取得光碟鍵，於步驟S12中，應用取得之光碟鍵執行自資訊記錄媒體10取得之加密標題鍵12之解碼處理，而取得標題鍵，應用取得之標題鍵，於步驟S13中，執行攪拌MPEG資料13之攪拌解除處理後，於步驟S14中，執行MPEG解碼處理，來重現聲音/影像資料25。

其次，參照圖2說明自附設或連接於PC等主機裝置之驅動器，將內容輸入主機(PC)側，並藉由主機側之播放機應用程式進行內容重現之處理程序。

如圖2所示，在安裝資訊記錄媒體之驅動器30與主機(PC)側之播放機應用程式40間，於圖式之步驟S31, S41中，執行相互認證及鍵共用(AKE：Authentication and Key Exchange)。相互認證處理如按照公用鍵密碼方式或共用鍵密碼方式之十進制來執行。於相互認證中產生對話鍵，驅動器30與主機側之播放機應用程式40共有對話鍵。

驅動器30於步驟S32中，應用對話鍵，執行自資訊記錄媒體10取得之加密光碟鍵11之再加密，並傳送至播放機應用程式40，此外，於步驟S33中，應用對話鍵，執行自資訊記錄媒體取得之加密標題鍵12之再加密，並傳送至播放機應

用程式40。驅動器30及作為播放機應用程式40之執行裝置之PC藉由連接匯流排，如藉由ATAPI匯流排(AT Attachement with Packet Interface BUS)連接，此等加密鍵資訊經由連接匯流排而傳送至PC之播放機應用程式40側。

再者，驅動器30將自資訊記錄媒體取得，依據CSS方式進行攪拌處理之內容之攪拌MPEG資料13，經由驅動器與PC間之連接匯流排而輸出至PC側。

主機(PC)側之播放機應用程式40於步驟S42中，使用對話鍵，將自驅動器30接收之加密光碟鍵11之藉由對話鍵而再加密資料予以解碼，取得加密光碟鍵11，再者，於步驟S43中，將自驅動器30接收之加密標題鍵12之藉由對話鍵而再加密資料予以解碼，取得加密標題鍵12。

而後之步驟S51~S55之處理，為與前述參照圖1而說明之處理(S11~S14)相同之處理。

圖3顯示以流程顯示該圖2所示之處理中之驅動器側之處理圖。於步驟S61中，判定插入有資訊記錄媒體(光碟)時，於步驟S62中，執行與主機，亦即與執行圖2所示之播放機應用程式40之PC之相互認證及鍵共有(AKE：Authentication and Key Exchange)。

相互認證及鍵共用(AKE)中成功(步驟S63：Yes)時，轉移至許可輸出安裝於驅動器之資訊記錄媒體之儲存內容之CSS攪拌資料之狀態，該CSS攪拌資料之輸出許可狀態持續至排出資訊記錄媒體，或是持續至斷開電源。

如此，自附設或連接於PC等主機裝置之驅動器輸入內容

至主機(PC)側，並藉由主機側之播放機應用程式重現內容情況下，係在主機側之播放機應用程式與驅動器之間執行認證，進行安全之資料傳送。對資訊記錄媒體(光碟)記錄資料時，亦係在主機側之播放機應用程式與驅動器之間執行認證，進行安全之資料傳送。

但是，相互認證處理係執行按照特定程序之處理，藉由發現特定之條件而認證成立。如按照公用鍵密碼方式之相互認證十進制，係藉由執行相互認證之機器滿足具有有效公用鍵與機密鍵之對的條件而認證成立。

公用鍵儲存於特定之管理中心發行之公用鍵證明中，並賦予管理中心之電子簽署，竄改困難。此外，發現不正當複製鍵之流出等不正當處理情況下，進行使管理中心管理下所發行之公用鍵證明無效化(撤銷)處理。該無效化(撤銷)處理中，管理中心表列無效化之公用鍵證明之辨識符(ID)，而發行撤銷表(CRL：Certificate Revocation List)。

執行按照公用鍵密碼方式之相互認證之機器，經由網路及記錄媒體等而獲得最新更新之撤銷表，執行認證處理時，參照獲得之撤銷表，判定認證對方之公用鍵證明之有效性，撤銷表中記錄有對方機器之公用鍵證明之ID時，判定係不正當之公用鍵證明，可進行使認證不成立之處置。

但是，依據撤銷表來排除不正當之鍵資訊之利用相當費時，其間存在無法防止內容不正當利用之問題。如因公用鍵與機密鍵洩漏等，進行利用不正當之公用鍵與機密鍵之不正當處理後，須經管理中心進行不正當處理之確認，而

後進行對撤銷表之登錄處理予以更新，並對各裝置分發撤銷表，在而後之認證處理中，方可藉由更新之撤銷表來排除不正當鍵。

在此等處理完成前，往往需要數個月。此外，亦有可能管理中心未確認洩漏，而放任不正當流通之鍵資訊。

因此，上述之將驅動器與主機應用程式間之認證成立作為條件之內容利用構造中，驅動器或主機應用程式之任何一方具有不正當獲得之公用鍵證明與機密鍵之對，於認證處理中，無法藉由撤銷表作不正當確認情況下，會發生相互認證成立，擁有不正當鍵之驅動器或主機應用程式不正當獲得內容來利用之情形。

參照圖4及圖5說明具體之例。圖4顯示在驅動器60與主機側之播放機應用程式70之間，依據公用鍵密碼十進制執行相互認證，將相互認證之成立作為條件，而自安裝於驅動器60之資訊記錄媒體60讀取內容，在播放機應用程式70中進行重現、利用之處理。

此時，主機側之播放機應用程式70具有包含不正當獲得之公用鍵PH與機密鍵SH之不正當鍵71。另外，公用鍵PH儲存於公用鍵證明中。但是，尚未登錄於管理中心發行之撤銷表中，而形成無法依據撤銷表來排除之狀態。

在該狀態下，於驅動器60與主機側之播放機應用程式70之間，依據公用鍵密碼十進制執行相互認證及鍵交換處理(AKE：Authentication and Key Exchange)(步驟S81)。相互認證及鍵交換處理(AKE)係相互認證處理與進行對話鍵(Ks)

之共有之處理。對話鍵(Ks)用作在認證機器間執行之資料通訊時之密碼鍵。

步驟S81之相互認證及鍵交換處理(AKE)中，驅動器60與主機側之播放機應用程式70兩者交換儲存公用鍵之公用鍵證明，進行公用鍵證明之簽署驗證，及依據撤銷表之撤銷確認，來確認正當性。

驅動器60依據播放機應用程式70接收之公用鍵證明之簽署驗證及撤銷表，進行撤銷確認，來確認正當性。雖然播放機應用程式70之公用鍵係不正當鍵，但是由於此時尚未記錄於撤銷表中，因此驅動器60判斷係正當之公用鍵，而相互認證成立。

而後，驅動器60於步驟S82及步驟S83中，以對話鍵(Ks)加密自資訊記錄媒體50讀取之加密內容與加密內容之加密鍵之內容鍵(Kc)，並輸出至播放機應用程式70。

播放機應用程式70於步驟S84與步驟S85中，應用對話鍵(Ks)將來自驅動器60之接收資料予以解碼，取得加密內容與內容鍵(Kc)，於步驟S86中，應用內容鍵(Kc)執行加密內容之解碼，而可取得內容。

如此，即使係不正當獲得之鍵，在未登錄於撤銷表期間，由於不知道係不正當，因此認證成立，而導致藉由不正當之應用程式不正當讀取儲存於資訊記錄媒體50中之有著作權管理及利用管理之內容來利用。

圖5顯示驅動器60側具有不正當之鍵資訊[SD, PD]61時之內容之不正當利用例。

於步驟S91之相互認證及鍵交換處理(AKE)中，驅動器60與主機側之播放機應用程式70兩者，交換儲存公用鍵之公用鍵證明，並依據公用鍵證明之簽署驗證及撤銷表進行撤銷確認，來確認正當性。播放機應用程式70依據自驅動器60接收之公用鍵證明之簽署驗證及撤銷表進行撤銷確認，而確認正當性。雖然驅動器60之公用鍵係不正當鍵，但是由於此時尚未記錄於撤銷表中，因此播放機應用程式70判斷係正當之公用鍵，而相互認證成立。

而後，播放機應用程式70於步驟S92中，應用仍然以正式手續取得之內容鍵(Kc)加密自網路以正式手續取得之內容，再者，於步驟S93及步驟S94中，以對話鍵(Ks)加密加密內容與加密內容之加密鍵之內容鍵(Kc)，並輸出至驅動器60。

驅動器60於步驟S95及步驟S96中，應用對話鍵(Ks)將來自播放機應用程式70之接收資料予以解碼，而取得加密內容與內容鍵(Kc)，於步驟S97中，應用內容鍵(Kc)執行加密內容之解碼，而取得內容，並記錄內容於如CD-R等記錄媒體中。

如此，即使係不正當獲得之鍵，在未登錄於撤銷表期間，由於不知道係不正當，因此認證成立，不正當之驅動器獲得播放機應用程式70以正式手續自外部取得之內容，可產生CD-R等不正當之內容記錄媒體。

如此，目前僅依據目前之撤銷表排除不正當鍵之構造，不易完全防止內容之不正當利用。

【發明內容】

有鑑於上述問題，本發明之目的在提供一種即使無法藉由撤銷表驗證鍵資訊時，仍可嚴格審查認證對象之鍵資訊之正當性，而可排除內容之不正當利用之資訊處理裝置、認證處理方法及電腦程式。

本發明之第一態樣之資訊處理裝置之特徵為具有：

進行資料傳送處理之介面，及

執行資料處理之資料處理部，

前述資料處理部之構造為：

隨伴經由前述介面之資料傳送之資料處理之執行條件，係執行與資料傳送對象之認證處理，於該認證處理中，依據認證對象保持之公用鍵證明之儲存資料，確認在資料傳送中應用之通道型式，並依據該通道型式來判定認證能否成立。

再者，本發明之資訊處理裝置之一種實施態樣之特徵為：前述資料處理部之構造為依據作為認證對象保持之公用鍵證明之儲存資料之安全認證通道(SAC)型式資訊，確認設定於公用鍵證明之通道型式是否為進行資料處理之主機-裝置型式，該資料處理係應用執行主機應用程式主導之資料處理之安全認證通道(SAC)，並依據該確認來判定認證能否成立。

再者，本發明之資訊處理裝置之一種實施態樣之特徵為：前述資料處理部之構造為依據作為認證對象保持之公用鍵證明之儲存資料之安全認證通道(SAC)型式資訊，確認

設定於公用鍵證明之通道型式是否為應用ATAPI匯流排連接，或是USB匯流排連接或是應用IEEE1394中之串聯匯流排協定(SBP)之安全通道進行資料處理之主機-裝置型式，並依據該確認來判定認證能否成立。

再者，本發明之資訊處理裝置之一種實施態樣之特徵為：前述資料處理部之構造為在前述認證處理中，依據認證對象保持之公用鍵證明之儲存資料，進一步確認認證對象之裝置型式，並依據該裝置型式來判定認證能否成立。

再者，本發明之資訊處理裝置之一種實施態樣之特徵為：前述裝置型式係顯示作為應用程式執行機器之主機，或是對資訊記錄媒體執行資料記錄處理或重現處理之驅動器之任何一個之資訊，前述資料處理部之構造為：依據作為預定認證條件之裝置型式來判定認證能否成立。

再者，本發明之資訊處理裝置之一種實施態樣之特徵為：前述資訊處理裝置係進行與驅動器之連接，來執行應用程式之主機機器，前述資料處理部之構造為：於前述認證處理中，依據自驅動器接收之公用鍵證明之儲存資料，執行確認前述驅動器係應用執行主機應用程式主導之資料處理之安全認證通道(SAC)，而執行主機-裝置型式之資料處理之驅動器之SAC型式確認，確認裝置型式係驅動器之裝置型式確認，及將上述兩者確認作為認證成立條件之認證處理。

再者，本發明之資訊處理裝置之一種實施態樣之特徵為：前述資訊處理裝置係與執行應用程式之主機機器連

接，而執行對資訊記錄媒體記錄或讀取資料之驅動器，前述資料處理部之構造為：於前述認證處理中，依據自執行應用程式之主機接收之公用鍵證明之儲存資料，執行前述應用程式係應用執行主機應用程式主導之資料處理之安全認證通道(SAC)，而執行主機-裝置型式之資料處理之應用程式之SAC型式確認，裝置型式係主機之確認之裝置型式確認，及將上述兩個確認作為認證成立條件之認證處理。

再者，本發明第二態樣之認證處理方法之特徵為具有：

公用鍵證明取得步驟，其係取得認證對象保持之公用鍵證明；

資訊取得步驟，其係自前述公用鍵證明之儲存資料取得通道型式資訊；

通道型式確認步驟，其係依據前述通道型式資訊，確認在與認證對象之資料傳送中應用之通道型式；及

認證能否判定步驟，其係依據在前述通道型式確認步驟中確認之通道型式，來判定認證能否成立。

再者，本發明之認證處理方法之一種實施態樣之特徵為：前述通道型式確認步驟係依據作為公用鍵證明之儲存資料之安全認證通道(SAC)型式資訊，確認設定於公用鍵證明之通道型式是否為應用執行主機應用程式主導之資料處理之安全認證通道(SAC)，而進行資料處理之主機-裝置型式。

再者，本發明之認證處理方法之一種實施態樣之特徵為：前述通道型式確認步驟係依據作為公用鍵證明之儲存

資料之安全認證通道(SAC)型式資訊，確認設定於公用鍵證明之通道型式是否為應用ATAPI匯流排連接，或是USB匯流排連接或是應用IEEE1394中之串聯匯流排協定(SBP)之安全通道進行資料處理之主機-裝置型式之步驟。

再者，本發明之認證處理方法之一種實施態樣之特徵為：前述認證處理方法進一步具有裝置型式確認步驟，其係依據認證對象保持之公用鍵證明之儲存資料，進一步確認認證對象之裝置型式，前述認證能否判定步驟係依據在前述通道型式確認步驟中確認之通道型式，與前述裝置型式確認步驟中確認之裝置型式，來判定認證能否成立之步驟。

再者，本發明之認證處理方法之一種實施態樣之特徵為：前述裝置型式係顯示是否為作為應用程式執行機器之主機，或是對資訊記錄媒體執行資料記錄處理或重現處理之驅動器之任何一個之資訊，前述認證能否判定步驟依據預定認證條件之裝置型式來判定認證能否成立。

再者，本發明之認證處理方法之一種實施態樣之特徵為：前述認證處理係與驅動器連接，在執行應用程式之主機機器中執行之認證處理，前述主機機器依據自驅動器取得之公用鍵證明之儲存資料，執行確認前述驅動器係應用執行主機應用程式主導之資料處理之安全認證通道(SAC)，而執行主機-裝置型式之資料處理之驅動器之SAC型式確認，確認裝置型式係驅動器之裝置型式確認，及將上述兩個確認作為認證成立條件之認證處理。

本發明之另外目的、特徵及優點，從後述之本發明之實施例及依據附圖之更詳細說明即可明瞭。另外，本說明書中所謂系統，係數個裝置之邏輯性集合構造，並不限定於各構造之裝置在同一個框體內者。

本發明之構造如形成在內容重現處理及記錄處理等之機器間執行隨伴資料傳送之資料處理時，係在資料傳送機器間執行認證處理，在該認證處理中，自認證對象機器之公用鍵證明之儲存資料取得通道型式資訊，依據通道型式資訊確認應用之通道型式，並依據確認之通道型式來判定認證能否成立之構造，因此可排除不正當之應用程式及驅動器連接，藉由不正當取得之鍵使認證成立，而進行內容傳送之處理。如將確認進行執行主機應用程式主導之資料處理之安全認證通道(SAC)應用之資料處理之主機-裝置型式作為認證成立之條件，因此，可排除如應用其他型式之通道之應用程式及驅動器具有不正當之鍵資訊而使認證成立，而不正當獲得內容等之處理。

再者，本發明之構造，係形成依據作為公用鍵證明之儲存資料之安全認證通道(SAC)型式資訊，確認設定於公用鍵證明之通道型式是否為應用ATAPI匯流排連接，或是USB匯流排連接或是應用IEEE1394中之串聯匯流排協定(SBP)之安全通道進行資料處理之主機-裝置型式，進行將此等確認處理作為條件之認證之構造，因此，可排除僅於執行應用特定之安全通道之資料處理之應用程式與驅動器之對應成立時，允許隨伴通道間之資料傳送之資料處理，藉由不正

當之應用程式及驅動器之連接而不正當取得內容。

再者，本發明之構造，係形成依據認證對象之公用鍵證明之儲存資料，確認認證對象之裝置型式。具體而言，係確認是否作為應用程式執行機器之主機，或是對資訊記錄媒體執行資料記錄處理或重現處理之驅動器之任何一個，並依據通道型式與裝置型式來判定認證能否成立之構造，因此可更嚴格認證，可排除藉由不正當之應用程式及驅動器之連接而不正當取得內容。

【實施方式】

以下，參照圖式詳細說明本發明之資訊處理裝置、認證處理方法及電腦程式。另外，說明係按照以下記載之項目來進行。

1.資訊記錄媒體之儲存資料構造

2.內容對應之資料處理

3.構成主機及驅動器之資訊處理裝置之構造

[1.資訊記錄媒體之儲存資料構造]

首先，說明資訊記錄媒體之儲存資料構造。圖6顯示儲存有內容之一種資訊記錄媒體。此時，係顯示儲存內容後之光碟之ROM光碟之資訊儲存例。

該ROM光碟如係Blu-ray光碟及DVD等資訊記錄媒體，且係在具有正當之內容著作權或頒發權之所謂內容權利人許可下，在光碟製造工廠中製造之儲存正當之內容之資訊記錄媒體。另外，以下之實施例中，資訊記錄媒體係以光碟型之媒體為例作說明，不過，本發明可適用於各種態樣之

資訊記錄媒體。

如圖6所示，資訊記錄媒體100具有：資料儲存區域101，其係儲存內容等之資料；及讀入區域102，其係儲存光碟及對應於儲存內容之附帶資訊，及應用於內容之解碼處理之鍵資訊等。

資料儲存區域101中儲存：加密(攪拌)內容111，應用於加密內容之解碼處理之鍵之產生上需要之資訊之記錄種(REC SEED)之單元鍵產生資訊：Vu112，及撤銷資訊113。另外，攪拌處理係加密處理之一種態樣，本說明書中，攪拌內容之上階概念係使用稱為加密內容之表現。加密內容111區分成特定之單元單位，在形成應用對應於單元之單元鍵之加密狀態下，儲存於資訊記錄媒體100之資料儲存區域101。單元鍵產生資訊：Vu112係應用於此等各單元鍵之產生之資訊，亦稱為種資訊。有關撤銷資訊113於後述。

讀入區域102中儲存應用於加密內容111之解碼處理之鍵產生上需要之各種資訊。其中之一為ROM符號：Ve114。ROM符號：Ve114亦稱為實體索引(Physical Index)，係無法重寫之固定資訊。於讀入區域102中進一步儲存密碼鍵資訊120。另外，ROM符號：Ve114及密碼鍵資訊120無須儲存於讀入區域102中，亦可儲存於資料區域101中。

密碼鍵資訊120與前述之單元鍵產生資訊：Vu112及ROM符號：Ve114相同，係藉由產生應用於儲存在資訊記錄媒體之資料儲存區域101中之加密內容111解碼處理之鍵用之鍵資訊(鍵產生資訊)而構成。

亦即，應用於加密內容111之解碼處理之鍵，如係包含：RKB(更新鍵區塊)121，其係為了取得作為對應於儲存在資訊記錄媒體之內容之鍵而設定之媒體鍵：Km而需要之密碼鍵區塊；及加密光碟鍵eKm(Kd)122，其係應用媒體鍵：Km，將作為應用於加密內容111之解碼處理之鍵之光碟鍵：Kd予以加密之資訊。另外eKa(b)係表示以鍵：Ka將資料：b予以加密之資料者。

RKB(更新鍵區塊)121係依據廣播加密方式之一種態樣而熟知之樹形結構之鍵發訊方式而產生之密碼鍵區塊，且係藉由分發至作為保有執行資訊記錄媒體重現之正當執照之使用者機器之資訊處理裝置之裝置鍵之解碼處理，可取得媒體鍵：Km之密碼鍵區塊。藉由變更密碼鍵區塊：RKB之構成資料，可選擇可取得媒體鍵：Km之使用者機器。

管理中心判定特定之使用者機器或重現應用程式係不正當時，變更RKB之構造，可使不正當機器無法取得媒體鍵：Km。另外，判定為不正當之使用者機器或重現應用程式作為撤銷(排除)機器而登錄於管理中心。管理中心保持將撤銷之使用者機器或重現應用程式之識別資訊予以表列之撤銷表，並適切更新。使用者可經由資訊記錄媒體或網路獲得包含最新撤銷表之撤銷資訊。

圖6所示之撤銷資訊113係包含將撤銷之使用者機器或重現應用程式之識別資訊予以表列之撤銷表之資訊。使用者機器如可藉由驗證自機器輸入之機器識別符(ID)有無記錄於撤銷表中，來判定輸出內容之機器是否為不正當機器，

為揭示於撤銷表中之不正當機器時，進行中止輸出內容之處理。

其次，參照圖7~圖9詳細說明儲存於資訊記錄媒體100之加密內容111之記錄構造。圖7(a)係儲存於資訊記錄媒體之資料記錄構造。並將18位元組之使用者控制資料(UCD：User Control Data)，與包含實際之AV內容資料等之2048位元組之使用者資料(User Data)作為1個扇區資料而構成。

如圖7(b)所示，如使用者資料3個扇區部分之6144位元組之資料作為1個區塊密碼處理單位之1個單元(1AU：Aligned Unit)，亦即，設定為區塊。6144位元組之資料相當於32TS(傳送流)封包。另外，區塊之設定單位並不限定於形成3個扇區部分6144位元組之資料方式，亦可採用將1個散區部分2048位元組之資料作為1個密碼處理單位，亦即作為區塊而設定之方式等各種設定。

如圖7(c)所示，儲存對應於內容之複製控制資訊CCI(複製控制資訊)之使用者資料以2K(2048)位元組單位加密而記錄。

另外，18位元組之使用者控制資料(User Control Data)自加密對象除去，僅使用者資料加密而記錄。

圖8顯示1個扇區資料之構造。1個扇區資料包含：18位元組之使用者控制資料(UCD：User Control Data)與2048位元組之使用者資料(User Data)。

使用者控制資料(UCD：User Control Data)亦稱為扇區標頭，其一部分中記錄扇區單位之輸出控制資訊(Output

Control Information)151。

輸出控制資訊151係對應之扇區資料(使用者資料)之傳送控制資訊，如係自安裝資訊記錄媒體之驅動器對PC等資訊處理裝置輸出之控制資訊，並包含以下之資訊。

設定為包含：

＊輸出控制旗標(Output Control Flag)

＊安全等級(Security Level)

＊應用程式ID(Application ID)

之資訊。

圖9顯示記錄於使用者控制資料(UCD: User Control Data)中之輸出控制資訊151之詳細構造。輸出控制資訊151記錄成使用者控制資料(UCD：User Control Data)之3位元組(24位元)資料。

首先，位元15~0中，記錄作為最大16位元資訊之應用程式ID(Application ID)。應用程式ID(Application ID)係應用於按照輸出控制資訊(Output Control Information)執行資訊記錄媒體之讀取內容控制時之資訊，且係允許資訊記錄媒體之讀取內容之重現處理之重現應用程式之識別資訊(ID)。如儲存於資訊記錄媒體之內容係藉由應用作為重現應用程式之藍色雷射(Blu-ray)光碟播放機而可重現之MPEG-TS封包為基礎之高度清晰影像內容時，記錄作為重現應用程式之藍色雷射(Blu-ray)光碟播放機之應用程式ID。此外，儲存於資訊記錄媒體之內容為以作為重現應用程式之DVD播放幾可重現之MPEG-PS為基礎之標準畫質之

影像內容時，記錄作為重現應用程式之DVD播放機之識別資訊作為應用程式ID。如此，應用程式ID係指定許可內容重現之重現平台之識別資訊。

在其次之位元19~16中，記錄作為最大4位元資訊之安全等級(Security Level)。安全等級(Security Level)亦係應用於按照輸出控制資訊(Output Control Information)執行資訊記錄媒體之讀取內容控制時之資訊，且係規定允許內容輸出對象之PC等資訊處理裝置之安全等級之資訊。如僅對於具有執行特定之安全資料處理構造之所謂安全PC允許輸出等，規定允許內容輸出對象之PC等之資訊處理裝置之安全等級。

作為4位元資訊，設定安全等級時，可設定達0000~1111之安全等級，將0000作為最低安全等級，將1111作為最高安全等級，自輸出對象機器取得之安全等級資訊，為記錄於資訊記錄媒體之輸出控制資訊151中之安全等級(Security Level)以上時，允許自驅動器輸出內容。

具體而言，如安全等級(Security Level)＝0001，表示係以Microsoft NGSCB及Trusted Computing Group規格制定之在安全PC(Secure PC)環境下動作之應用程式，及僅在安全PC(Secure PC)環境下許可動作之內容。此種設定，亦即記錄有安全等級(Security Level)＝0001之資料，禁止以一般之PC應用程式重現，禁止自驅動器輸出內容。

位元22~20之3位元係保留區域，

位元23之1位元係設定輸出控制旗標(Output Control

Flag)。輸出控制旗標(Output control Flag)係用作是否按照輸出控制資訊(Output Control Information)執行資訊記錄媒體之讀取內容之控制之判定資訊。具體而言如設定成：

輸出控制旗標(Output control Flag)＝1：有輸出限制，及匯流排加密

輸出控制旗標(Output control Flag)＝0：無輸出限制

另外，匯流排加密係於自驅動器輸出內容時執行之加密處理，詳細如後述。

另外，此時說明之各資訊之構成位元數係一種範例，可藉由各個規格作各個設定。

[2.內容對應之資料處理]

其次，說明儲存於上述資訊記錄媒體之內容之重現處理等之內容對應之資料處理。儲存於資訊記錄媒體之內容之重現態樣有兩種態樣。第一態樣係安裝資訊記錄媒體，執行自資訊記錄媒體讀取資料之機器本身執行重現處理之態樣；第二態樣係執行自資訊記錄媒體讀取資料之驅動器，及重現處理時執行內容處理之主機(PC)等之資訊處理裝置係構成不同機器，而在驅動裝置與主機(PC)間藉由資料傳送用匯流排連接，執行經由連接匯流排之資料傳送，來進行重現處理及其他內容資料處理之態樣。

首先，參照圖10說明安裝資訊記錄媒體，執行自資訊記錄媒體讀取資料之機器本身執行重現處理之處理程序。

兼用驅動器之重現機器300設置儲存加密內容206之資訊記錄媒體200，執行資料之讀取、鍵產生及內容解碼等各種

密碼處理後，輸出內容。

資訊記錄媒體200中，儲存有先前參照圖5而說明之各種資訊，亦即儲存有：包含作為不正當機器表之撤銷表之撤銷資訊(Revocation info for AKE)201，作為儲存媒體鍵：Km之密碼鍵區塊之RKB202，以媒體鍵：Km將光碟鍵：Kd加密之加密光碟鍵：EKm(Kd)203，ROM符號：Ve204，單元鍵產生資訊：Vu205及加密內容206。

以下說明兼用驅動器之重現機器300之處理。兼用驅動器之重現機器300於步驟S101中，應用預先儲存於機器內之裝置鍵：Kdev301，執行作為加密鍵區塊之RKB202之解碼處理，而自RKB202取得媒體鍵：Km。另外可自RKB202取得媒體鍵：Km者，僅為允許利用內容之機器，如前述，不正當機器之被撤銷之機器具有之裝置鍵無法進行RKB之解碼，而無法取得媒體鍵：Km。

於步驟S101中，成功取得媒體鍵：Km時，其次於步驟S102中，應用取得之媒體鍵：Km，執行自資訊記錄媒體200取得之加密光碟鍵：EKm(Kd)203之解碼處理，而取得光碟鍵：Kd。

其次於步驟S103中，依據取得之光碟鍵：Kd，及自資訊記錄媒體200取得之ROM符號：Ve204，執行鍵產生處理，如執行按照AES密碼十進制之鍵產生處理，而產生嵌入鍵：Ke。

參照圖11詳細說明按照AES密碼十進制之鍵產生處理。如圖11所示，按照AES密碼十進制之鍵產生，係於AES密碼

處理區塊311中，對輸入值執行應用密碼鍵之AES密碼處理，而輸出其輸出與輸入值之排他邏輯和(XOR)運算結果之處理。圖10之步驟S103中，自資訊記錄媒體200取得輸入值之ROM符號：Ve204，係執行將應用鍵作為光碟鍵：Kd之鍵產生處理，而獲得作為輸出值之嵌入鍵：Ke。

其次，於步驟S104中，依據取得之嵌入鍵：Ke及自資訊記錄媒體200取得之單元鍵產生資訊：Vu205，執行鍵產生處理，而產生單元鍵：Ku。該鍵產生處理，亦係按照參照圖11而說明之AES密碼十進制之鍵產生處理來執行。

其次，於步驟S105中，執行應用產生之單元鍵：Ku之加密內容206之解碼處理，而輸出內容。

參照圖12詳細說明步驟S105中應用單元鍵：Ku之加密內容206之解碼處理。

加密內容206以特定資料單位之區塊單位進行加密，並儲存於資訊記錄媒體200中。如圖12所示，如6144位元組之扇區資料係進行各16位元組之區塊之加密。

以下說明解碼處理之順序。首先，自6144位元組之扇區資料取得最前之16位元組資料，而在AES鍵產生處理區塊[AES_G]321中，執行按照AES密碼十進制之鍵產生處理。此與先前參照圖11而說明之處理相同。將AES鍵產生處理區塊321之輸出作為區塊鍵：Kb，應用該區塊鍵：Kb，在AES解碼處理區塊[AES_D]322中執行下一個16位元組之解碼處理。

AES解碼處理區塊[AES_D]322將扇區資料第二個16位元

組資料與初始值：IVa之排他邏輯和(XOR)結果作為輸入，按照應用區塊鍵：Kb之AES密碼十進制執行解碼處理，而取得16位元組區塊資料之解碼資料，並且作為應用於下一個區塊之解碼之輸入值。以下，重複執行相同之處理，可獲得解碼扇區資料323。另外，初始值：IVa係預先設定之常數。IVa如亦有時設定可自對應於扇區資料之使用者控制資料或使用者資料取得者。

因而，圖10之步驟S105應用單元鍵：Ku執行區塊單位之解碼處理，並輸出解碼後之內容。

如此，在1個機器內執行來自資訊記錄媒體之資訊讀取與重現處理情況下，內容洩漏之可能性小，發生侵害內容之著作權之問題可能性小。但是，先前，如參照圖2~圖5之說明，自安裝資訊記錄媒體之驅動器，經由匯流排而輸出內容至PC等主機機器時，及執行將PC等主機機器自外部獲得之內容傳送至驅動器之處理情況下，主機之應用程式或驅動器均進行不正當處理，因而會發生內容不正當利用之問題。

本發明之構造係在此種驅動器與PC等之主機間進行內容傳送，而嚴格進行作為內容之記錄及重現之前步驟而執行之認證處理。即使認證對象如具有未撤銷之鍵(公用鍵證明)時，仍可依據公用鍵證明之儲存資料，進行認證對象正當性之嚴格確認處理，僅於依據該確認而確認出正當性時，執行內容之重現及記錄。藉由本構造來防止不正當利用內容。

具體而言，相互認證時，係在認證機器間交換而相互驗證之公用鍵證明中設定：

(1)SAC型式資訊

(2)裝置型式資訊

之各資訊，並依據此等資訊判斷認證對象機器之正當性。此等資訊詳細內容於後述。

以下詳細說明匯流排連接驅動器與作為應用程式執行機器之PC等之主機，隨伴內容傳送之處理程序。

圖13顯示資訊記錄媒體200，設定資訊記錄媒體200，而進行來自資訊記錄媒體200之資料讀取或記錄之驅動裝置400，及經由連接匯流排連接驅動裝置400，作為執行內容之重現及輸入輸出處理應用程式之PC等資訊處理裝置之主機500之處理。另外，連接驅動裝置400與主機500之匯流排，如係ATAPI BUS、USB匯流排、IEEE1394匯流排等匯流排。

資訊記錄媒體200中，與先前參照圖10而說明同樣地，儲存有圖5所示之各種資訊，亦即儲存有：包含作為不正當機器表之撤銷表之撤銷資訊(Revocation info for AKE)201，作為儲存媒體鍵：Km之密碼鍵區塊之RKB202，以媒體鍵：Km將光碟鍵：Kd加密之加密光碟鍵：EKm(Kd)203，ROM符號：Ve204，單元鍵產生資訊：Vu205及加密內容206。

驅動裝置400中儲存有：按照公用鍵密碼方式之管理中心之公用鍵[Kp_kic]401，按照公用鍵密碼方式之驅動器對應之機密鍵[Ks_drive]402，儲存按照公用鍵密碼方式之驅動

器對應之公用鍵之公用鍵證明[Cert_drive]403及裝置鍵[Kdev]404。

另外，執行主機應用程式之主機500中儲存有：按照公用鍵密碼方式之管理中心之公用鍵[Kp_kic]501，主機執行之主機應用程式對應之按照公用鍵密碼方式之主機應用程式機密鍵[Ks_host]502及儲存主機執行之主機應用程式對應之按照公用鍵密碼方式之公用鍵之主機應用程式公用鍵證明[Cert_host]503。

參照圖14詳細說明驅動器對應之公用鍵證明[Cert_drive]403及主機應用程式對應之公用鍵證明[Cert_host]503。

圖14(a)係驅動器對應之公用鍵證明[Cert_drive]530之資料構造，圖14(b)係主機應用程式對應之公用鍵證明[Cert_host]550之資料構造。

驅動器對應之公用鍵證明[Cert_drive]530中，除與先前之公用鍵證明同樣資料之證明型式、證明識別符、公用鍵及簽署資料外，還儲存前述之

(1)SAC型式資訊531

(2)裝置型式資訊532。

(1)SAC型式資訊531係

安全認證通道(SAC：Secure Authentication Channel)資訊，且係關於PC等之主機執行之應用程式與驅動器間之資料傳送匯流排之通道資訊。在應用程式側之公用鍵證明中儲存作為其應用程式應用之通道資訊之SAC型式資訊，驅

動器側之公用鍵證明中儲存作為驅動器應用之通道資訊之SAC型式資訊。

SAC型式資訊中包含：

(1a)SAC型式＝[Host-Device]

(1b)SAC型式＝[Peer-to-Peer]

之兩種資訊。

(1a)SAC型式＝[Host-Device]表示

主機側應用程式具有動作之主導權，並經由匯流排而對驅動器輸出命令，驅動器側藉由自主機側應用程式輸入之命令而進行從屬性動作之型式。

具體而言，如PC等主機執行之應用程式與驅動器之連接匯流排應用ATAPI匯流排(AT Attachement with Packet Interface BUS)時，或是USB連接應用程式與驅動器時，或是將應用程式與驅動器作為IEEE1394匯流排連接，而執行按照串聯匯流排協定(SBP：Serial Bus Protocol)之資料處理之構造時等，係

SAC型式＝[Host-Device]。

另外，(1b)SAC型式＝[Peer-to-Peer]係

並非主機側應用程式具有動作之主導權之形態，而各裝置具有對等關係來執行資料處理之型式。

具體而言，如PC等主機執行之應用程式與驅動器之連接匯流排使用IEEE1394，而採用AV協定時等。藉由此種構造，在執行資料處理之應用程式及驅動器之公用鍵證明中設定

SAC型式＝[Peer-to-Peer]。

(2)裝置型式資訊係

顯示裝置之型式資訊之資訊，具體而言包含：

(2a)主機

(2b)驅動器

之各設定。

在主機側應用程式之公用鍵證明中設定

(2a)裝置型式＝主機，

在驅動器之公用鍵證明中設定

(2b)裝置型式＝驅動器。

主機側應用程式及驅動器分別具有儲存

(1)SAC型式資訊

(2)裝置型式資訊

之兩個附加資訊之公用鍵證明，於相互認證時，交換此等公開鍵證明，而相互抽出(1)SAC型式資訊與(2)裝置型式資訊進行驗證。

認證處理中，確認在資料傳送中應用之通道型式，並依據確認之通道型式來判定認證能否成立。亦即，依據認證對象保持之公用鍵證明之儲存資料之安全認證通道(SAC)型式資訊，確認設定於公用鍵證明之通道型式是否為應用執行主機應用程式主導之資料處理之安全認證通道(SAC)而進行資料處理之主機-裝置型式，並依據該確認判定認證能否成立。

具體而言，係確認設定於公用鍵證明之通道型式是否為

應用ATAPI匯流排連接，或是USB匯流排連接，或是應用IEEE1394中之串聯匯流排協定(SBP)之安全通道進行資料處理之主機-裝置型式，並依據該確認來判定認證能否成立。並依據認證對象保持之公用鍵證明之儲存資料來確認認證對象之裝置型式，依據確認之裝置型式來判定認證能否成立。亦即，確認係作為應用程式執行機器之主機，或是對資訊記錄媒體執行資料記錄處理或重現處理之驅動器，判定是否對應於預定認證條件之裝置型式，來判定認證能否成立。

主機應用程式對應之公用鍵證明[Cert_host]550除證明型式、證明識別符、公用鍵、簽署資料之外，還設定應用程式安全等級[SLcert]551、應用程式ID[AIDcert]552及

(1)SAC型式資訊553

(2)裝置型式資訊554

作為新增資料。

應用程式安全等級[SLcert]551如係4位元資訊，且係對應於先前參照圖9而說明之資訊記錄媒體之內容構造資料之扇區資料之使用者控制資料(UCD)中儲存之對應於輸出控制資訊(Output Control Information)內之安全等級(Security Level)之資料。

儲存於主機之應用程式對應之公用鍵證明中之應用程式安全等級[SLcert]551設定其應用程式具有之安全等級資訊。如為以安全之PC執行之應用程式時，設定高安全等級之值。

儲存於公用鍵證明之應用程式安全等級[SLcert]551為4位元資料時，設定[0000]~[1111]中之安全等級值之任何一個。0000為最低安全等級，1111為最高安全等級。

應用程式ID[AIDcert]552係對應於先前參照圖9而說明之資訊記錄媒體之內容構造資料之扇區資料之使用者控制資料(UCD)中儲存之對應於輸出控制資訊(Output Control Information)內之應用程式ID之資料。

儲存於公用鍵證明之應用程式ID係公用鍵證明所設定之應用程式之識別資訊。如儲存於資訊記錄媒體之內容為作為重現應用程式之藍色雷射(Blu-ray)光碟播放機應用程式時，儲存可判斷係藍色雷射(Blu-ray)光碟播放機應用程式之識別資訊之應用程式ID。

SAC型式資訊553係安全認證通道(SAC：Secure Authentication Channel)資訊，且係關於PC等主機執行之應用程式與驅動器間之資料傳送匯流排之通道資訊。在應用程式側之公用鍵證明中儲存作為其應用程式應用之通道資訊之SAC型式資訊，在驅動器側之公用鍵證明中儲存作為驅動器應用之通道資訊之SAC型式資訊。

SAC型式資訊553與驅動器之SAC型式資訊513同樣地設定

(1a)SAC型式＝[Host-Device]

(1b)SAC型式＝[Peer-to-Peer]

之兩種資訊之任何一個。

SAC型式＝[Host-Device]係主機側應用程式具有動作之

主導權，並經由匯流排而對驅動器輸出命令，驅動器側藉由自主機側應用程式輸入之命令而進行從屬性動作之型式，具體而言，如PC等主機執行之應用程式與驅動器之連接匯流排應用ATAPI匯流排(AT Attachement with Packet Interface BUS)時，或是USB連接應用程式與驅動器時，或是將應用程式與驅動器作為IEEE1394匯流排連接，而執行按照串聯匯流排協定(SBP：Serial Bus Protocol)之資料處理之構造時。

另外，SAC型式＝[Peer-to-Peer]係並非主機側應用程式具有動作之主導權之形態，而各裝置具有對等關係來執行資料處理之型式。具體而言，如PC等主機執行之應用程式與驅動器之連接匯流排使用IEEE1394，而採用AV協定之構造時等，設定SAC型式＝[Peer-to-Peer]。

裝置型式資訊554係顯示裝置之型式資訊之資訊，具體而言有：

(2a)主機

(2b)驅動器

之各設定，在主機側應用程式之公用鍵證明中設定裝置型式＝主機。

另外，圖14所示之構成公用鍵證明之各資料之構成位元數係一種範例，各資訊之位元數並不限定於圖14所示之態樣者，而可作各種設定。

回到圖13，說明驅動裝置400將自資訊記錄媒體取得之內容等資料經由連接匯流排而傳送至主機500進行重現之處

理程序。

首先，於步驟S201, S301中，在驅動裝置400與主機500之應用程式間，執行相互認證及鍵交換(AKE：Authentication and Key Exchange)處理。參照圖15說明相互認證及鍵交換(AKE：Authentication and Key Exchange)處理之詳細程序。該處理如可應用利用規定於ISO/IEC9798-3之公用鍵十進制之相互認證，及規定於ISO/IEC11770-3之公用鍵十進制之鍵產生處理方式來執行。另外，利用公用鍵之相互認證方式實用化之方式，如揭示於DTCP(數位傳送內容保護)規格第一冊(資訊版)之方法。

說明圖15所示之處理程序。於步驟S401中，主機應用程式對驅動器傳送藉由亂數產生處理而產生之挑戰資料[C_host]及公用鍵證明[Cert_Host]。公用鍵證明[Cert_Host]係圖14(b)所示之公用鍵證明，且係儲存安全等級及應用程式ID、SAC型式及裝置型式各資訊之公用鍵證明。

獲得該資料之驅動器側於步驟S402中，依據主機應用程式之公用鍵證明[Cert_Host]執行驗證處理。

參照圖16(a)之流程說明於步驟S402中，依據驅動器執行之主機應用程式之公用鍵證明[Cert_Host]之驗證處理之詳細程序。

首先，驅動器於步驟S431中，自主機(應用程式)接收公用鍵證明[Cert_Host]。於步驟S432中，驅動器藉由主機(應用程式)公用鍵證明[Cert_Host]之簽署驗證處理，來驗證公用鍵證明[Cert_Host]有無竄改。簽署驗證處理係應用驅動

器保持之管理中心之公用鍵[Kp_kic]401(參照圖13)來執行。

驗證公用鍵證明[Cert_Host]無竄改時，自公用鍵證明[Cert_Host]取得應用程式ID，並依據自資訊記錄媒體取得之撤銷資訊201中含有之撤銷表，執行撤銷確認。

藉由簽署驗證檢測公用鍵證明[Cert_Host]可能遭竄改時，及依據應用程式ID判明主機應用程式被撤銷時(步驟S433：No)，進入步驟S437，執行錯誤訊息之通知等，並結束處理。中止以後之內容、輸出及重現處理。

確認公用鍵證明[Cert_Host]無竄改，並確認主機應用程式係未被撤銷之應用程式時(步驟S433：Yes)，進入步驟S434，讀取記錄於主機應用程式之公用鍵證明[Cert_Host]之SAC型式。

並非SAC型式＝主機裝置[Host-Device]情況下，進入步驟S437，執行錯誤訊息之通知等，並結束處理。中止以後之內容、輸出及重現處理。

所謂並非SAC型式＝主機裝置[Host-Device]，係指為SAC型式＝同級間[Peer-to-Peer]，並非主機側應用程式具有動作之主導權之形態，係指各裝置具有對等之關係，而執行資料處理之型式。具體而言，如PC等主機執行之應用程式與驅動器之連接匯流排使用IEEE1394，而採用AV協定之構造時等，設定有SAC型式＝[Peer-to-Peer]，此種情況下，不作為認證成立，而進入步驟S437，執行錯誤訊息之通知等，並結束處理，中止以後之內容、輸出及重現處理。

為SAC型式＝主機裝置[Host-Device]時(步驟S434：Yes)時，進入步驟S435。

所謂為SAC型式＝主機裝置[Host-Device]，亦即表示係對應於主機側之應用程式具有資料處理中之各種動作的主導權，並經由匯流排對驅動器輸出命令，驅動器側藉由自主機側應用程式輸入之命令，而從屬性進行動作型式之應用程式。

為SAC型式＝主機裝置[Host-Device]時，具體而言，表示應用程式係與驅動器之ATAPI匯流排連接，USB連接或是IEEE1394匯流排連接係應用串聯匯流排協定(SBP：Serial Bus Protocol)之構造中執行資料處理之應用程式。

此種情況下，進一步於步驟S435中，驅動器自主機應用程式之公用鍵證明取得裝置型式，判定是否為裝置型式＝主機。並非裝置型式＝主機時(步驟S435：No)，進入步驟S437，執行錯誤訊息之通知等，而結束處理。中止以後之內容、輸出及重現處理。

為裝置型式＝主機時(步驟S435：Yes)，進入步驟S436，繼續執行而後之認證處理。

如此，驅動器將依據記錄於主機應用程式之公用鍵證明[Cert_Host]之SAC型式，確認應用程式係通過ATAPI之I/F使驅動器動作之[Host-Device]型式之資料處理，亦即係藉由在兩者間應用SAC(Secure Authenticated Channel)傳送資料，執行應用程式主導型之資料處理之應用程式，進一步依據裝置型式，確認應用程式執行裝置係主機作為認證之

成立條件。

其次，於圖15之步驟S403中，驅動器對主機應用程式傳送藉由亂數產生處理而產生之挑戰資料[C_drive]與驅動器側之公用鍵證明[Cert_drive]。

主機應用程式側執行驅動器側之公用鍵證明[Cert_drive]之驗證。

參照圖16(b)之流程說明於步驟S404中，主機應用程式執行之依據驅動器之公用鍵證明[Cert_Drive]之驗證處理詳細程序。

首先，主機應用程式於步驟S451中，自驅動器接收公用鍵證明[Cert_Drive]。於步驟S452中，主機應用程式藉由驅動器公用鍵證明[Cert_Drive]之簽署驗證處理，驗證公用鍵證明[Cert_Drive]有無竄改。簽署驗證處理係應用主機應用程式保持之管理中心之公用鍵[Kp_kic]501(參照圖13)來執行。

驗證公用鍵證明[Cert_Drive]無竄改時，依據撤銷表執行撤銷確認。撤銷資訊自網路或資訊記錄媒體取得，並應用儲存於記憶體之資料。

藉由簽署驗證檢測出公用鍵證明[Cert_Drive]可能被竄改時，及判明驅動器被撤銷時(步驟S453：No)，進入步驟S457，執行錯誤訊息之通知等，並結束處理。中止以後之內容、輸出及重現處理。

確認公用鍵證明[Cert_Drive]無竄改，並確認係未被撤銷之驅動器時(步驟S453：Yes)，進入步驟S454，讀取記錄於

驅動器之公用鍵證明[Cert_Drive]之SAC型式。

並非SAC型式＝主機裝置[Host-Device]時，進入步驟S457，執行錯誤訊息之通知等，並結束處理。中止以後之內容、輸出及重現處理。

所謂並非SAC型式＝主機裝置[Host-Device]，係指驅動器側之公用鍵證明為SAC型式＝同級間[Peer-to-Peer]，並非主機側應用程式具有動作之主導權之形態，係指各裝置具有對等之關係，而執行資料處理之型式。具體而言，如PC等主機執行之應用程式與驅動器之連接匯流排使用IEEE1394，而採用AV協定之構造時等。

此時，設定有SAC型式＝[Peer-to-Peer]，此種情況下，不作為認證成立，而進入步驟S457，執行錯誤訊息之通知等，並結束處理，中止以後之內容、輸出及重現處理。

為SAC型式＝主機裝置[Host-Device]時(步驟S454：Yes)時，進入步驟S455。所謂為SAC型式＝主機裝置[Host-Device]，亦即表示係回應對應於主機側之應用程式具有資料處理中之各種動作的主導權，並經由匯流排對驅動器輸出命令，驅動器側藉由自主機側應用程式輸入之命令，而從屬性進行動作型式之應用程式，而執行處理之驅動器。具體而言，表示驅動器係與應用程式之ATAPI匯流排連接，USB連接或是IEEE1394匯流排連接係應用串聯匯流排協定(SBP：Serial Bus Protocol)之構造中執行資料處理之驅動器。

此種情況下，進一步於步驟S455中，主機應用程式自驅

動器之公用鍵證明取得裝置型式，判定是否為裝置型式＝驅動器。並非裝置型式＝驅動器時(步驟S455：No)，進入步驟S457，執行錯誤訊息之通知等，而結束處理。中止以後之內容、輸出及重現處理。

為裝置型式＝驅動器時(步驟S455：Yes)，進入步驟S456，繼續執行而後之認證處理。

如此，主機應用程式將依據記錄於驅動器之公用鍵證明[Cert_Drive]之SAC型式，確認驅動器係通過ATAPI之I/F依據來自應用程式之命令而動作之[Host-Device]型式之資料處理，亦即係藉由在兩者間應用SAC(Secure Authenticated Channel)執行應用程式主導型之資料處理之驅動器，進一步依據裝置型式，確認驅動器係正確之驅動器作為認證之成立條件。

確認公用鍵證明[Cert_drive]之正當性時，主機應用程式依據自驅動器接收之挑戰資料[C_drive]執行運算，算出參數[A_host]，並與新產生之亂數[R_host]一起傳送至驅動器(步驟S405)。

另外，驅動器依據自主機應用程式接收之挑戰資料[C_host]執行運算，算出參數[A_drive]，並與新產生之亂數[R_drive]一起傳送至主機應用程式(步驟S406)。

藉由該處理，主機及主機應用程式兩者共有：亂數[R_host]、[R_drive]、參數[A_host]、[A_drive]，驅動器及主機應用程式兩者依據此等之共有資料，產生共用之對話鍵Ks(步驟S407)。

驅動器進一步於步驟S408中，在依據亂數產生之匯流排鍵：Kbus及與匯流排鍵之程序編號：SEQ之連結資料：[Kbus||SEQ]中，使用對話鍵：Ks將作為該連結資料之竄改驗證用資料而算出之散列值[hash(Kbus||SEQ)]加密之資料：EKs[(Kbus||SEQ), hash(Kbus||SEQ)]傳送至主機應用程式。另外該步驟S408之處理相當於圖13中步驟S206之匯流排鍵產生處理(Genarate_Kbus)與步驟S207之對話鍵：Ks之匯流排鍵之加密處理(AES_E)之處理。

匯流排鍵：Kbus係用作加密內容之自驅動器至主機側之經由連接匯流排傳送處理時之加密鍵之鍵，係於驅動器中依據亂數而產生。匯流排鍵適切切換，與依據各匯流排鍵之程序編號相對應。如在主機側應用各個應用程式執行應用數個應用程式重現儲存於資訊記錄媒體之不同內容情況下，係將各應用程式應用之匯流排鍵設定為不同鍵。

回到圖13，繼續說明驅動裝置400將自資訊記錄媒體取得之內容等資料經由連接匯流排傳送至主機500進行重現之處理程序。

驅動裝置400與主機500之相互認證及鍵交換(AKE)結束時，應用保持於驅動器內之裝置鍵：Kdev404，於步驟S202中，執行自資訊記錄媒體200讀取之密碼鍵區塊之RKB202之解碼處理，並自RKB202取得媒體鍵：Km。另外，可自RKB202取得媒體鍵：Km，僅為允許利用內容之機器，如前述作為不正當機器而被撤銷之機器具有之裝置鍵無法進行RKB之解碼，而無法取得媒體鍵：Km。

於步驟S202中，取得媒體鍵：Km成功時，其次於步驟S203中，應用取得之媒體鍵：Km，執行自資訊記錄媒體200取得之加密光碟鍵：EKm(Kd)203之解碼處理，而取得光碟鍵：Kd。

其次於步驟S204中，執行依據取得之光碟鍵：Kd及自資訊記錄媒體200取得之ROM符號：Ve204之鍵產生處理，如執行按照AES密碼十進制之鍵產生處理，而產生嵌入鍵：Ke。按照AES密碼十進制之鍵產生處理如先前參照圖11之說明。

驅動器於步驟S205中，將嵌入鍵：Ke以先前相互認證及鍵交換處理(AKE)中產生之對話鍵：Ks予以加密，並經由連接匯流排傳送至主機500。

步驟S206及步驟S207之處理相當於先前參照圖15而說明之相互認證及鍵交換處理(AKE)之步驟S408之處理，係依據亂數產生匯流排鍵：Kbus(步驟S206)，將以對話鍵：Ks將包含匯流排鍵：Kbus之資料予以加密(步驟S207)而產生之資料，經由連接匯流排而傳送至主機500之處理。傳送資料如先前參照圖15之說明，係使用對話鍵：Ks將依據亂數而產生之匯流排鍵：Kbus，及與匯流排鍵之程序編號：SEQ之連結資料：[Kbus||SEQ]與作為該連結資料之竄改驗證用資料而算出之散列值[hash(Kbus||SEQ)]予以加密之資料：EKs[(Kbus||SEQ), hash(Kbus||SEQ)]。

再者，驅動裝置400於步驟S208中，依據自資訊記錄媒體200讀取之加密內容206之使用者控制資料(UCD)中含有之

輸出控制資訊，及在相互認證及鍵交換處理(AKE)處理中自主機500取得之主機之公用鍵證明之儲存資料執行輸出控制，於步驟S209中，依據控制態樣而使用匯流排鍵：Kbus將加密內容206予以加密，產生之加密資料經由連接匯流排而輸出至主機500。

自資訊記錄媒體200讀取之加密內容350，如係經過攪拌處理之加密資料，驅動器應用匯流排鍵：Kbus將該攪拌處理後之資料再度加密後輸出至主機側。藉由執行應用該匯流排鍵：Kbus之再度加密處理之資料輸出，僅保持匯流排鍵：Kbus之經過認證之主機側唯一之應用程式可應用匯流排鍵：Kbus解碼，而可藉由解碼處理取得加密內容350。

藉由形成此種構造，即使在輸入內容之PC(主機)側藉由切換應用程式而迂迴取得內容，及藉由竊聽驅動器與主機之連接匯流排之傳送資料而取得內容，取得之內容係藉由匯流排鍵：Kbus加密之資料，而擁有匯流排鍵：Kbus者僅為與驅動器之認證成立之特定之應用程式，只要不應用其特定之應用程式，即無法執行輸入內容之解碼。僅CSS攪拌之解除程式，無法執行藉由匯流排鍵：Kbus而加密之資料之解碼，可防止內容之不正當利用。

參照圖17說明應用匯流排鍵：Kbus之加密內容206之加密處理態樣。應用匯流排鍵：Kbus之加密內容206之加密處理如圖17所示，係藉由應用AES-CBC模式之區塊加密處理來執行。

驅動裝置400對於自資訊記錄媒體200讀取之加密內容，

應用於驅動器中產生之匯流排鍵：Kbus，執行以特定資料區塊單位(16位元組)加密之處理。

首先，從自資訊記錄媒體200讀取之加密內容之構成資料之2048位元組之扇區資料350取得最前之16位元組資料，將與初始值：IVb之排他邏輯和(XOR)結果輸入AES密碼處理部[AES_E]351，執行按照應用匯流排鍵：Kbus之AES密碼十進制之密碼處理，產生16位元組區塊資料之加密資料。初始值：IVb係預先設定之常數。IVb如亦有時係自對應於扇區資料350之使用者控制資料(UCD)取得。

再者，該產生資料用作應用於下一個區塊之加密之輸入值。以下，各16位元組之區塊資料同樣地重複執行排他邏輯和(XOR)及AES密碼處理，而產生匯流排鍵之加密扇區資料352，將該資料經由ATAPI-BUS等之連接匯流排，而向主機500側之應用程式傳送。在主機500側將該輸入加密資料予以解碼，進行重現處理。

回到圖13，說明主機500側之處理程序。主機500首先如前述，於步驟S301中，執行與驅動裝置400之相互認證及鍵交換(AKE)，而取得對話鍵：Ks。

其次，於步驟S302中，對於藉由自驅動器經由連接匯流排而輸入之對話鍵：Ks而加密之嵌入鍵：Ke，亦即對[EKs(Ke)]，執行應用對話鍵：Ks之解碼處理，而取得嵌入鍵：Ke。

再者，於步驟S303中，對於自驅動器經由連接匯流排而輸入之單元鍵產生資訊：Vu，執行應用嵌入鍵：Ke之AES

鍵產生處理(參照圖11)，而產生單元鍵：Ku。

再者，於步驟S304中，對於自驅動器經由連接匯流排而輸入之對話鍵：Ks加密之匯流排鍵：Kbus，亦即對[EKs(Kbus)]，執行應用對話鍵：Ks之解碼處理，而取得匯流排鍵：Kbus。

另外，如先前參照圖15之說明，包含自驅動器傳送之匯流排鍵：Kbus之資料，係使用對話鍵：Ks將匯流排鍵：Kbus及與匯流排鍵之程序編號：SEQ之連結資料：[Kbus||SEQ]與作為該連結資料之竄改驗證用資料而算出之散列值[hash(Kbus||SEQ)]予以加密之資料：EKs[(Kbus||SEQ), hash(Kbus||SEQ)]。

主機500之應用程式於步驟S304中，以對話鍵：Ks將資料：EKs[(Kbus||SEQ), hash(Kbus||SEQ)]予以解碼，而取得匯流排鍵：Kbus及與匯流排鍵之程序編號：SEQ之連結資料：[Kbus||SEQ]與作為該連結資料之竄改驗證用資料而算出之散列值[hash(Kbus||SEQ)]。

其次，於步驟S305中，算出連結資料：[Kbus||SEQ]之散列值，執行與來自驅動器之輸入資料中含有之散列值[hash(Kbus||SEQ)]之比較。兩散列值一致時，判定連結資料：[Kbus||SEQ]未被竄改，轉移至步驟S306中之應用匯流排鍵：Kbus之內容解碼處理。

於步驟S306中，執行藉由自驅動裝置400輸入之匯流排鍵：Kbus再度加密之加密內容之解碼處理。

參照圖18詳細說明藉由匯流排鍵：Kbus再度加密之加密

內容之解碼處理。應用匯流排鍵：Kbus之加密內容之解碼處理，如圖18所示，係藉由應用AES-CBC模式之區塊解碼處理。

主機500之應用程式對於自驅動裝置400經由連接匯流排而輸入之加密內容，應用自驅動器輸入之匯流排鍵：Kbus，執行以特定資料區塊單位(16位元組)解碼之處理。

首先，從自驅動裝置400經由連接匯流排而輸入之加密內容之構成資料之2048位元組之扇區資料370取得最前之16位元組資料，並輸入AES解碼處理部[AES_D]371，執行按照應用匯流排鍵：Kbus之AES密碼十進制之解碼處理，再者，執行與初始值：IVb之排他邏輯和(XOR)運算，而獲得解碼結果。初始值：IVb係預先設定之常數。IVb如亦有時係自對應於扇區資料370之使用者控制資料(UCD)取得。

再者，16位元組單位之解碼結果資料用作應用於下一個區塊之解碼處理之輸入值。以下，各16位元組之區塊資料同樣地重複執行AES解碼處理及排他邏輯和(XOR)，而取得藉由匯流排鍵解除加密之扇區資料，亦即取得作為儲存於資訊記錄媒體200之資料狀態之加密(攪拌)扇區資料372。

再者，主機500之主機應用程式在圖13所示之步驟S307中，應用單元鍵：Ku執行作為儲存於資訊記錄媒體200之資料狀態之加密內容之解碼處理。該解碼處理係執行與先前參照圖12說明之相同處理。

藉由以上之處理，主機500之主機應用程式取得解碼內容520，進行對揚聲器、顯示裝置等輸出部之輸出處理，執行

內容重現。

如此，由於本發明之構造，係於執行資訊記錄媒體之資料讀取之驅動器中，應用匯流排鍵：Kbus將自資訊記錄媒體讀取之經過攪拌處理之資料再度加密而輸出至主機側，因此僅在保持匯流排鍵：Kbus之主機側應用程式，亦即僅在與驅動器之相互認證成立之主機應用程式中，可應用匯流排鍵：Kbus解碼，藉由解碼處理可利用加密內容。

因此，即使在輸入內容之PC(主機)側藉由切換應用程式而迂迴取得內容，及藉由竊聽驅動器與主機之連接匯流排之傳送資料而取得內容，僅與驅動器之相互認證成立，具有同一個匯流排鍵：Kbus之唯一應用程式可進行藉由匯流排鍵：Kbus而加密之資料之解碼，因此其他應用程式，如CSS攪拌之解除程式，無法執行藉由匯流排鍵：Kbus而加密之資料之解碼，可防止內容之不正當利用。

其次，參照圖19~圖21，說明圖13所示之步驟S208及步驟S209中執行之輸出控制資訊分析及內容之輸出控制之數個態樣。

首先，如參照圖9之說明，說明儲存於資訊記錄媒體之加密內容之扇區標頭(使用者控制資料)中，自驅動器對PC等資訊處理裝置輸出之控制資訊設定有：

(1)輸出控制旗標(Output control Flag)

(2)安全等級(Security Level)

(3)應用程式ID(Application ID)

之各資訊。

亦可為設定此等(1)~(3)之三種資訊之全部作為輸出控制資訊之態樣，不過亦可為僅設定(1)輸出控制旗標(Output control Flag)，或僅設定(1)輸出控制旗標(Output control Flag)及(3)應用程式ID(Application ID)等各種態樣。此外，設定資訊即使設定有(1)~(3)之全部時，於驅動器中之輸出控制資訊之分析時，亦可執行僅應用其一部分之解釋。以下，就此等數個處理態樣，參照圖19~圖21說明驅動器側之處理程序例。

圖19~圖21分別係說明以下處理之程序。

圖19：僅依據輸出控制資訊中之「輸出控制旗標」之輸出控制程序

圖20：依據輸出控制資訊中之「輸出控制旗標」與「應用程式ID」之輸出控制程序

圖21：依據輸出控制資訊中之「輸出控制旗標」與「應用程式ID」與「安全等級」之輸出控制程序

首先，參照圖19說明僅依據輸出控制資訊中之「輸出控制旗標」控制自驅動器對主機輸出內容之程序。

說明圖19之流程各步驟。首先，於步驟S511中，檢測對驅動器插入資訊記錄媒體(光碟)，於步驟S512中，檢測在匯流排連接之主機側執行內容重現處理之主機應用程式之啟動。將檢測有此等作為條件，而進入步驟S513，等待自主機側要求相互認證，而接收相互認證要求時，於步驟S514中，首先按照先前參照圖15及圖16而說明之公用鍵密碼方式執行相互認證及鍵交換(AKE)處理。

該認證處理中，如參照圖16之說明，抽出公用鍵證明內之SAC型式及裝置型式。依據SAC型式確認在與認證對象之資料傳送中應用之通道型式，確認設定於公用鍵證明之通道型式是否為應用執行主機應用程式主導之資料處理之安全認證通道(SAC)而進行資料處理之主機-裝置型式，並依據該確認判定認證能否成立。如確認設定於公用鍵證明之通道型式是否為應用ATAPI匯流排連接，或USB匯流排連接，或應用IEEE1394中之串聯匯流排協定(SBP)之安全通道進行資料處理之主機-裝置型式，並依據該確認來判定認證能否成立。

此外，依據認證對象之公用鍵證明之儲存資料確認認證對象之裝置型式，並依據該裝置型式判定認證能否成立。具體而言，係確認裝置型式係主機或驅動器，並依據預定之認證條件之裝置型式來判定認證能否成立。

於步驟S515中，確認相互認證及鍵交換(AKE)處理完成時，進入步驟S516，驅動器執行對應於匯流排鍵：Kb之亂數R之產生處理，並將該產生亂數R作為匯流排鍵：Kb。該處理相當於圖13中之步驟S206之處理。另外如前述，匯流排鍵：Kb與程序編號相對應。驅動器亦有時保持對應於數個不同程序編號之不同匯流排鍵，並依據主機側之執行應用程式切換而應用。

於步驟S517中，自主機側接收匯流排鍵之傳送要求時，於步驟S518中，將匯流排鍵：Kb傳送至主機側。該處理相當於圖13中之步驟S207。另外，該匯流排鍵傳送係相當於

圖15之相互認證及鍵交換(AKE)處理之最後步驟S408之處理，驅動器產生使用對話鍵：Ks將匯流排鍵：Kbus，及與匯流排鍵之程序編號：SEQ之連結資料：[Kbus||SEQ]與作為該連結資料之竄改驗證用資料而算出之散列值[hash(Kbus||SEQ)]予以加密之資料：EKs[(Kbus||SEQ), hash(Kbus||SEQ)]，並傳送至主機側。

其次，於步驟S519中，確認並無新的相互認證要求，此外，在步驟S520確認未排出資訊記錄媒體，於步驟S521中，待機至主機側之內容取得要求，亦即扇區資料之讀取要求。

另外，於步驟S519中，有新的相互認證要求時，回到步驟S514，執行相互認證及鍵交換(AKE)處理，並執行新匯流排鍵之產生及傳送。此時產生之匯流排鍵係程序編號：2之匯流排鍵，成為與先前產生之匯流排鍵(程序編號1)不同之匯流排鍵。此等係對應於主機側之不同應用程式之匯流排鍵，驅動器對主機側之每個啟動應用程式執行相互認證及鍵交換(AKE)處理，並執行新匯流排鍵之產生及傳送，於內容傳送時，應用對應於主機側每個啟動應用程式之匯流排鍵產生加密資料並傳送。

另外，於步驟S520中，判定自驅動器排出光碟時，回到步驟S511，設定成初始狀態，重設亦即刪除所產生之匯流排鍵及對話鍵等全部資料。

於步驟S521中，有自主機側要求讀取資料時，驅動器於步驟S522中，自對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)讀取輸出控制資訊，判定[輸出控制旗標：

OCF]之值。該處理相當於圖13之步驟S208之處理。

輸出控制旗標：OCF如先前參照圖9之說明，係

OCF＝1：有輸出限制，有匯流排加密，

OCF＝0：無輸出限制

之設定資訊。

於步驟S522中，判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制旗標(OCF)設定成[1]時，進入步驟S523，以匯流排鍵：Kbus將自資訊記錄媒體讀取之扇區資料予以加密，並於步驟S524中輸出至主機側。另外，步驟S523中之扇區資料之加密處理，如執行應用先前參照圖17而說明之AES-CBC模式之加密處理。

於步驟S522中，判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制旗標(OCF)設定成[0]時，跳過步驟S523，不執行將自資訊記錄媒體讀取之扇區資料以匯流排鍵：Kbus之加密處理，而於步驟S524中，將來自資訊記錄媒體之讀取內容照樣輸出至主機側。另外，該讀取內容如係按照CSS規定而加密(攪拌)內容。

如此，驅動器依據對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制旗標(OCF)為[0]或[1]，判定是否需要以匯流排鍵加密，為需要以匯流排鍵加密之資料時，執行將輸出內容以匯流排鍵加密後輸出。

其次，參照圖20，說明依據輸出控制資訊中之[輸出控制旗標]與[應用程式ID]，控制自驅動器對主機輸出內容之程序。

說明圖20之流程各步驟。首先，於步驟S611中，初始設定處理係將對話ID[SID]與匯流排鍵：Kbus之值設定為初始值[0]。對話ID係對應於在驅動器主機間設定之對話之識別符，對於在主機驅動器間所設定之對話，於主機驅動器間之相互認證及鍵交換(AKE)處理中，與驅動器自主機接收之主機之應用程式對應之公用鍵證明(參照圖14)取得之應用程式ID[AIDcert]相同之值作為對話ID。亦即，作為SID＝AIDcert來決定對話ID。

步驟S612~S616之處理係與圖19中說明之處理步驟S511~515相同之處理，因此省略說明。

步驟S617係在主機驅動器間之相互認證及鍵交換(AKE)處理中，驅動器判定自主機接收之主機之應用程式對應之公用鍵證明(參照圖14)取得之應用程式ID[AIDcert]與對話ID[SID]是否一致。

為SID＝AIDcert時，即是已成立之對話，由於對話對應之匯流排鍵存在，因此不執行匯流排鍵產生處理，而進入步驟S620。

為SID≠AIDcert時，即是新的對話，而於步驟S618中執行對話對應之匯流排之產生處理。其係執行藉由產生亂數而產生匯流排鍵。另外，匯流排鍵與程序編號相對應。並分別記憶、利用各個對話對應之匯流排鍵。

匯流排鍵：Kbus之產生完成時，於步驟S619中，驅動器在主機驅動器間之相互認證及鍵交換(AKE)處理中，設定對於新對話之對話識別符為自主機接收之主機之應用程式對應之公用鍵證明(參照圖14)而取得之應用程式ID[AIDcert]，亦即設定為SID＝AIDcert。

步驟S620~S624之處理由於與先前說明之圖19之流程中之步驟S517~521之處理相同，因此省略說明。

於步驟S624中，有自主機側要求讀取扇區資料時，驅動器於步驟S625中，自對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)讀取輸出控制資訊，判定[輸出控制旗標：OCF]之值。該處理相當於圖13之步驟S208之處理。

輸出控制旗標：OCF如先前參照圖9之說明，係

OCF＝1：有輸出限制，有匯流排加密，

OCF＝0：無輸出限制

之設定資訊。

於步驟S625中，判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制旗標(OCF)設定成[1]時，進入步驟S626，判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之應用程式ID[AIDucd]，與在主機驅動器間之相互認證及鍵交換(AKE)處理中，驅動器自主機接收之主機之應用程式對應之公用鍵證明(參照圖14)而取得之應用程式ID[AIDcert]是否一致，亦即判定

AIDucd＝AIDcert

是否成立。

如前述，輸出控制資訊中之應用程式ID[AIDucd]係表示允許輸出之應用程式之識別資訊，驅動器僅於主機之應用程式與輸出控制資訊中之應用程式ID[AIDucd]一致時，允許輸出內容。

於步驟S626中，判定

AIDucd＝AIDcert

不成立時，於步驟S629中，自驅動器傳送錯誤訊息至主機側，而結束處理。此時，不執行內容之傳送。

於步驟S626中，判定

AIDucd＝AIDcert

成立時，於步驟S627中，以匯流排鍵：Kbus將自資訊記錄媒體讀取之扇區資料加密，並於步驟S628中輸出至主機側。另外，步驟S627中之扇區資料之加密處理，係執行如先前參照圖17而說明之應用AES-CBC模式之加密處理。

於步驟S625中，判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制旗標(OCF)設定成[0]時，跳過步驟S626, S627，不執行應用程式ID之判定處理，及藉由匯流排鍵：Kbus對自資訊記錄媒體讀取之扇區資料之加密處理，而進入步驟S628，將來自資訊記錄媒體之讀取內容照樣輸出至主機側。另外，該讀取內容如係按照CSS規定之加密(攪拌)內容。

本實施例中，驅動器判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制

旗標(OCF)係[0]或[1]，來判定是否執行輸出控制，並且依據輸出控制旗標(OCF)，需要輸出控制情況下，進一步進行應用程式ID之驗證，亦即判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之應用程式ID[AIDucd]，與在主機驅動器間之相互認證及鍵交換(AKE)處理中，驅動器自主機接收之主機之應用程式對應之公用鍵證明而取得之應用程式ID[AIDcert]是否一致，亦即判定

AIDucd＝AIDcert

是否成立，一致時允許輸出內容，執行將輸出內容藉由匯流排鍵加密而輸出。

藉由形成該構造，依據主機側執行之應用程式之確認，實現內容輸出。另外，應用程式ID係儲存於公用鍵證明之資料，且係依據管理中心之簽署，於相互認證時執行竄改驗證之資料，因此，可依據確保可靠性之資料來確認應用程式。

其次，參照圖21，說明依據輸出控制資訊中之[輸出控制旗標]、[應用程式ID]及[安全等級]，控制自驅動器對主機輸出內容之程序。

說明圖21之流程各步驟之處理。圖21之流程中，步驟S631~S644係與先前說明之圖20之流程中之步驟S611~S624相同之處理，因此省略說明。

於步驟S644中，有自主機側要求讀取資料時，驅動器於步驟S645中，自對應於讀取對象之扇區資料之扇區標頭(使

用者控制資料)讀取輸出控制資訊，判定[輸出控制旗標：OCF]之值。該處理相當於圖13之步驟S208之處理。

輸出控制旗標：OCF如先前參照圖9之說明，係

OCF＝1：有輸出限制，有匯流排加密，

OCF＝0：無輸出限制

之設定資訊。

於步驟S645中，判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制旗標(OCF)設定成[1]時，進入步驟S646，執行對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之安全等級[SLucd]，與在主機驅動器間之相互認證及鍵交換(AKE)處理中，驅動器自主機接收之主機之應用程式對應之公用鍵證明(參照圖14)而取得之安全等級[SLcert]之值之比較。

記錄於扇區標頭(使用者控制資料)之輸出控制資訊中之安全等級[SLucd]，係設定允許內容輸出之應用程式之安全等級之資訊，並記錄允許之最低安全等級之值。如設定1111(最高等級)~0000(最低等級)之任何一個值。記錄於主機應用程式對應之公用鍵證明之安全等級[SLcert]，係主機應用程式對應之安全等級之值。

驅動器於主機應用程式對應之安全等級[SLcert]之值，為記錄於輸出控制資訊中之安全等級[SLucd]之值以上時，判定係允許輸出內容之應用程式。亦即係

SLucd≦SLcert

時，判定係允許輸出內容之應用程式。

於步驟S646中，判定

SLucd≦SLcert

不成立時，於步驟S650中，自驅動器傳送錯誤訊息至主機側，而結束處理。此時不執行內容之傳送。

於步驟S646中，判定

SLucd≦SLcert

成立時，進一步於步驟S647中，判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之應用程式ID[AIDucd]，與自主機接收之主機之應用程式對應之公用鍵證明(參照圖14)而取得之應用程式ID[AIDcert]是否一致，亦即判定

AIDucd＝AIDcert

是否成立。

該處理與圖20中說明之步驟S626之處理相同。

於步驟S647中，判定

AIDucd＝AIDcert

不成立時，於步驟S650中，自驅動器傳送錯誤訊息至主機側，而結束處理。此時，不執行內容之傳送。

於步驟S647中，判定

AIDucd＝AIDcert

成立時，於步驟S648中，以匯流排鍵：Kbus將自資訊記錄媒體讀取之扇區資料加密，並於步驟S649中輸出至主機側。另外，步驟S627中之扇區資料之加密處理，係執行如

先前參照圖17而說明之應用AES-CBC模式之加密處理。

另外，於步驟S645中，判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制旗標(OCF)設定成[0]時，跳過步驟S646~S648，不執行安全等級之判定處理，應用程式ID之判定處理，及藉由匯流排鍵：Kbus對自資訊記錄媒體讀取之扇區資料之加密處理，而進入步驟S649，將來自資訊記錄媒體之讀取內容照樣輸出至主機側。另外，該讀取內容如係按照CSS規定之加密(攪拌)內容。

本實施例中，形成驅動器判定對應於讀取對象之扇區資料之扇區標頭(使用者控制資料)之輸出控制資訊中之輸出控制旗標(OCF)係[0]或[1]，來判定是否執行輸出控制，並且依據輸出控制旗標(OCF)，需要輸出控制情況下，進一步執行安全等級之驗證與應用程式ID之驗證之構造。

本構造依據在主機側執行之應用程式之安全等級與應用程式確認，來實現內容輸出。另外，安全等級與應用程式ID係儲存於公用鍵證明之資料，且係依據管理中心之簽署，於相互認證時執行竄改驗證之資料，因此可依據確保可靠性之資料來確認安全等級及應用程式。

[3. 構成主機及驅動器之資訊處理裝置之構造]

其次，參照圖22及圖23，說明資訊處理裝置之構造例，其係如構成：主機，其係藉由進行資訊記錄媒體之儲存內容之重現，自外部輸入內容及對驅動器輸出內容等各種處理之PC等構成；及驅動裝置，其係執行資訊記錄媒體之儲

存內容之讀取及輸出。

首先參照圖22說明作為主機之資訊處理裝置之構造。資訊處理裝置(主機)600具有：CPU670，其係按照OS及內容重現應用程式、相互認證處理程式等各種程式執行資料處理；ROM660，其係作為程式及參數等之記憶區域；記憶體680；輸入輸出數位訊號之輸入輸出I/F610；輸入輸出I/F640，其係輸入輸出類比訊號，並具有A/D, D/A轉換器641；MPEG編碼譯碼器630，其係執行MPEG資料之編碼及解碼處理；TS‧PS處理手段620，其係執行TS(傳送流)‧PS(程式流)處理；密碼處理手段650，其係執行相互認證、加密內容之解碼處理等各種密碼處理；硬碟等之記錄媒體691；及驅動器690，其係進行記錄媒體691之驅動及資料記錄重現訊號之輸入輸出；匯流排601上連接有各區塊。

資訊處理裝置(主機)600如藉由ATAPIBUS等之連接匯流排與驅動器連接，上述藉由匯流排鍵加密之內容自數位訊號用輸入輸出I/F610輸入，並依需要藉由密碼處理手段650，如以參照圖18而說明之AES-CBC模式執行解碼處理。

另外，執行內容重現處理之程式如保管於ROM660內，程式之執行處理中，依需要使用記憶體680作為參數及資料之保管及工作區域。

ROM660或記錄媒體691中，儲存有先前參照圖13而說明之管理中心之公用鍵，對應於主機應用程式之機密鍵，及對應於主機應用程式之公用鍵證明。另外，保持有數個主機應用程式時，儲存對應於各個之機密鍵與公用鍵證明。

其次，參照圖23說明資訊記錄媒體之儲存內容之讀取及對於資訊處理裝置(主機)執行輸出之驅動器之構造。驅動裝置700具有：CPU702，其係執行內容讀取及按照傳送處理程式、相互認證處理程式等各種程式之資料處理；ROM705，其係作為程式及參數等之記憶區域；記憶體706；輸入輸出數位訊號之輸入輸出I/F703；密碼處理手段704，其係執行相互認證匯流排之產生及輸出資料之加密處理等各種密碼處理；及記錄媒體I/F707，其係進行DVD、Blu-ray光碟等資訊記錄媒體708之驅動、資料記錄重現訊號之輸入輸出；匯流排701上連接有各區塊。

驅動裝置700如藉由ATAPIBUS等連接匯流排與資訊處理裝置(主機)連接，如以匯流排鍵：Kbus將儲存於資訊記錄媒體708之加密(攪拌)內容再度加密，而自輸入輸出I/F703輸出。應用匯流排鍵：Kbus之內容加密係藉由密碼處理手段704，如以參照圖17而說明之AES-CBC模式執行。

另外，ROM705或是記憶體706中儲存有先前參照圖13而說明之管理中心之公用鍵，對應於驅動器之機密鍵，對應於驅動器之公用鍵證明及應用於密碼鍵區塊RKB之處理用之裝置鍵：Kdev。此外，儲存有執行內容之讀取、取得及相互認證處理之程式等。

以上，參照特定之實施例詳細說明本發明。但是，在不脫離本發明要旨之範圍內，熟悉本技藝者當然可形成該實施例之修正及代用。亦即，係以例示之形態揭示本發明，而不應作限定性之解釋。為了判斷本發明之要旨，須參酌

申請專利範圍項。

另外，說明書中說明之一連串處理，可藉由硬體、軟體或兩者之複合構造來執行。藉由軟體來執行處理時，可使記錄處理程序之程式安裝於組裝在專用硬體之電腦內之記憶體來執行，或是可在可執行各處理之通用電腦中安裝程式來執行。

如程式可預先記錄於作為記錄媒體之硬碟及ROM(唯讀記憶體)中。或是程式可暫時或永久性儲存(記錄)於軟式磁碟、CD-ROM(唯讀記憶光碟)、MO(光磁)碟、DVD(多樣化數位光碟)、磁碟、半導體記憶體等可移式記憶媒體中。此種可移式記錄媒體可作為所謂封包軟體來提供。

另外，程式除上述自可移式記錄媒體安裝於電腦之外，亦可自下載側無線傳送至電腦，或是經由LAN(區域網路)及網際網路等網路，以有線傳送至電腦，電腦接收如此送達之程式，而安裝於內藏之硬碟等記錄媒體中。

另外，說明書中記載之各種處理，除按照記載時間序列地執行之外，亦可依執行處理之裝置之處理能力或依需要並列或個別地執行。此外，本說明書中所謂系統，係數個裝置之邏輯集合構造，並不限定於各構成裝置在同一個框體內者。

以上，如說明，由於本發明之構造係形成如執行隨伴內容重現處理及記錄處理等機器間之資料傳送之資料處理時，於資料傳送機器間執行認證處理，於該認證處理中，自認證對象機器之公用鍵證明之儲存資料取得通道型式資

訊，依據通道型式資訊確認適用之通道型式，並依據確認之通道型式來判定認證成立與否之構造，因此，可排除不正當之應用程式及驅動器連接，藉由不正當取得之鍵使認證成立，而進行內容傳送之處理。由於將確認係應用執行主機應用程式主導之資料處理之安全認證通道(SAC)之進行資料處理之主機-裝置型式作為認證成立條件，因此可排除如應用其他型式之通道之應用程式及驅動器具有不正當之鍵資訊而使認證成立，不正當獲得內容等之處理。

再者，由於本發明之構造係形成依據作為公用鍵證明之儲存資料之安全認證通道(SAC)型式資訊，確認設定於公用鍵證明之通道型式是否為應用ATAPI匯流排連接，或是USB匯流排連接或是應用IEEE1394中之串聯匯流排協定(SBP)之安全通道進行資料處理之主機-裝置型式，進行將此等確認處理作為條件之認證，因此僅於執行應用特定之安全通道之資料處理之應用程式與驅動器之對應成立時，允許隨伴通道間之資料傳送之資料處理，可排除藉由不正當之應用程式及驅動器之連接而不正當取得內容。

再者，由於本發明之構造係形成依據認證對象之公用鍵證明之儲存資料，確認認證對象之裝置型式。具體而言，係確認是否為作為應用程式執行機器之主機，或是對資訊記錄媒體執行資料記錄處理或重現處理之驅動器之任何一個，依據通道型式與裝置型式判定認證成立與否之構造，因此可更嚴格認證，而可排除藉由不正當之應用程式及驅動器之連接而不正當取得內容。

【圖式簡單說明】

圖1係先前之資訊記錄媒體儲存內容之重現程序之說明圖。

圖2係先前之資訊處理裝置(主機)中之驅動器輸出內容之重現程序之說明圖。

圖3係說明自驅動器之內容輸出程序之流程圖。

圖4係先前之隨伴主機驅動器間之內容傳送之處理構造中之內容不正當利用例之說明圖。

圖5係先前之隨伴主機驅動器間之內容傳送之處理構造中之內容不正當利用例之說明圖。

圖6係本發明之資訊記錄媒體之儲存資料之說明圖。

圖7(a), (b), (c)係本發明之資訊記錄媒體之儲存資料構造之說明圖。

圖8係本發明之作為資訊記錄媒體之儲存資料之扇區資料及扇區標頭構造之說明圖。

圖9係本發明之記錄於資訊記錄媒體之扇區標頭之輸出控制資訊之詳細說明圖。

圖10係執行資訊記錄媒體之儲存內容之讀取、重現之重現機器之處理程序之說明圖。

圖11係按照資訊記錄媒體之儲存內容重現中執行之AES密碼十進制之鍵產生處理之說明圖。

圖12係按照資訊記錄媒體之儲存內容重現中執行之AES密碼十進制之資料解碼處理之說明圖。

圖13係隨伴本發明之驅動裝置與資訊處理裝置(主機)中

執行之內容傳送之重現程序之說明圖。

圖14(a), (b)係儲存於驅動裝置與資訊處理裝置(主機)之公用鍵證明之資料構造之說明圖。

圖15係在驅動裝置與資訊處理裝置(主機)間執行之相互認證及鍵交換(AKE)處理程序之說明圖。

圖16(a), (b)係說明在驅動裝置與資訊處理裝置(主機)間執行之相互認證時之公用鍵證明之驗證處理程序之流程圖。

圖17係說明驅動裝置執行之內容之依據匯流排鍵：Kbus之加密處理構造圖。

圖18係說明資訊處理裝置(主機)執行之內容之依據匯流排鍵：Kbus之解碼處理構造圖。

圖19係顯示說明驅動裝置執行之內容之輸出控制處理例1之流程圖。

圖20係顯示說明驅動裝置執行之內容之輸出控制處理例2之流程圖。

圖21係顯示說明驅動裝置執行之內容之輸出控制處理例3之流程圖。

圖22係顯示本發明之資訊處理裝置(主機)之構造例圖。

圖23係顯示本發明之驅動裝置之構造例圖。

【主要元件符號說明】

10	資訊記錄媒體
11	加密光碟鍵
12	加密標題鍵

13	攪拌MPEG資料
20	重現機器
25	聲音/影像資料
30	驅動器
40	播放機應用程式
45	聲音/影像資料
60	驅動器
61	鍵資訊
70	主機側播放機應用程式
71	鍵資訊
100	資訊記錄媒體
101	使用者資料區域
102	讀入區域
111	加密內容
112	單元鍵產生資訊
113	撤銷資訊
114	ROM符號
120	密碼鍵資訊
121	密碼鍵區塊(RKB)
122	加密光碟鍵
151	輸出控制資訊
200	資訊記錄媒體
201	撤銷資訊
202	密碼鍵區塊(RKB)

203	加密光碟鍵
204	ROM符號
205	單元鍵產生資訊
206	加密內容
300	兼用驅動器之重現機器
301	裝置鍵
311	AES密碼處理區塊
321	AES鍵產生處理區塊
322	AES解碼處理區塊
323	解碼扇區資料
350	扇區資料
351	AES密碼處理部
352	匯流排鍵之加密扇區資料
370	匯流排鍵之加密扇區資料
371	AES解碼處理部
372	加密(攪拌)扇區資料
400	驅動裝置
401	管理中心公用鍵
402	驅動器機密鍵
403	驅動器公用鍵證明
404	裝置鍵
500	資訊處理裝置(主機)
501	管理中心公用鍵
502	主機應用程式機密鍵

503	主機應用程式公用鍵證明
520	內容
530	驅動器公用鍵證明
531	SAC型式
532	裝置型式
550	主機應用程式公用鍵證明
551	安全等級
552	應用程式ID
553	SAC型式
554	裝置型式
600	資訊處理裝置(主機)
601	匯流排
610	輸入輸出I/F
620	TS・PS處理手段
630	MPEG編碼譯碼器
640	輸入輸出I/F
641	A/D, D/A轉換器
650	密碼處理手段
660	ROM
670	CPU
680	記憶體
690	驅動器
691	記錄媒體
700	驅動裝置

701	匯流排
702	CPU
703	輸入輸出I/F
704	密碼處理手段
705	ROM
706	記憶體
707	記錄媒體I/F
708	資訊記錄媒體

五、中文發明摘要：

本發明提供一種可防止隨伴機器間之資料傳送之資料處理時內容之不正當取得及利用，而執行認證之裝置及方法。本發明係自認證對方機器之公用鍵證明之儲存資料，取得安全認證通道(SAC)型式資訊，確認在與認證對方之資料傳送中適用之通道型式，並依據通道型式判定認證能否成立。如將屬於進行執行主機應用程式主導之資料處理之安全認證通道(SAC)適用之資料處理之主機-裝置型之確認作為認證成立之條件。藉由本構造，可排除如應用其他型式之通道之應用程式及驅動器具有不正當之鍵資訊，而使認證成立，不正當獲得內容等之處理。

六、英文發明摘要：

十一、圖式：

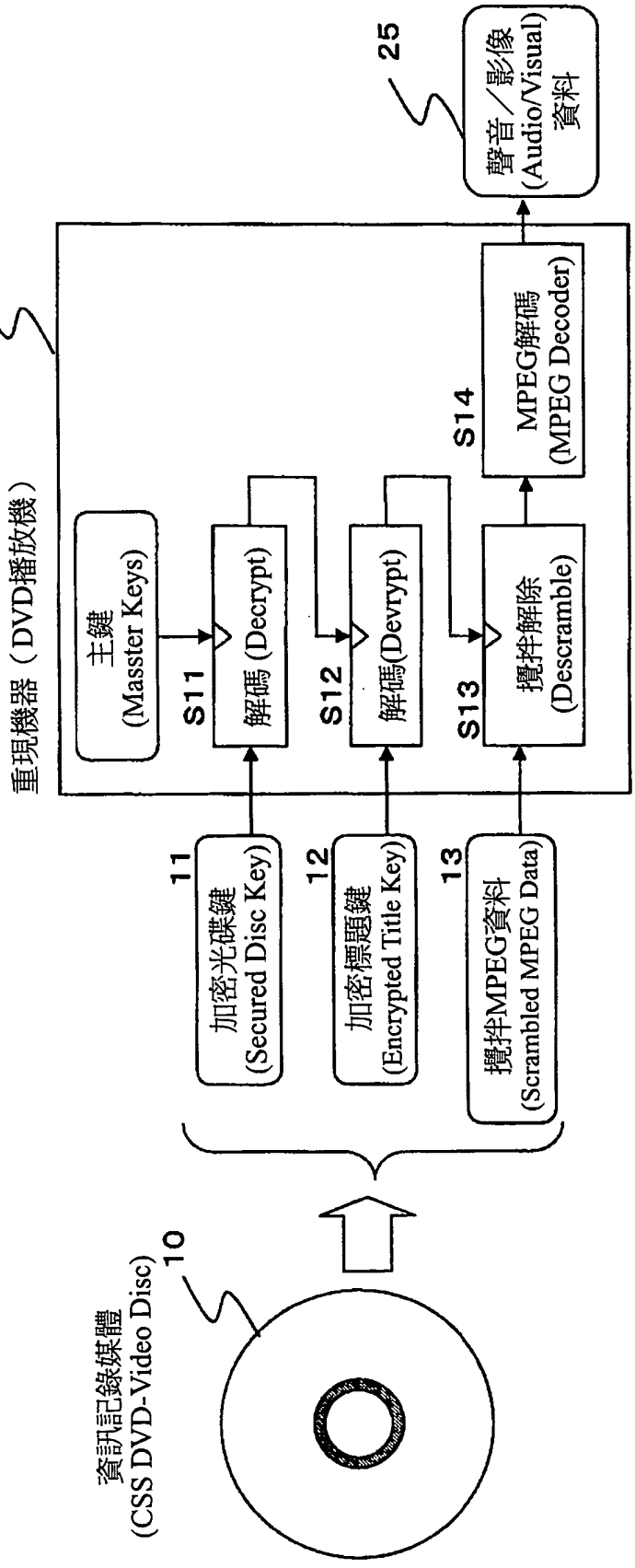

資訊記錄媒體
(CSS DVD-Video Disc)
10
重現機器（DVD播放機）
20
加密光碟鍵
(Secured Disc Key)
11
加密標題鍵
(Encrypted Title Key)
12
攪拌MPEG資料
(Scrambled MPEG Data)
13
主鍵
(Masster Keys)
S11
解碼 (Decrypt)
S12
解碼(Devrypt)
S13
攪拌解除
(Descramble)
S14
MPEG解碼
(MPEG Decoder)
25
聲音／影像
(Audio/Visual)
資料

圖 1

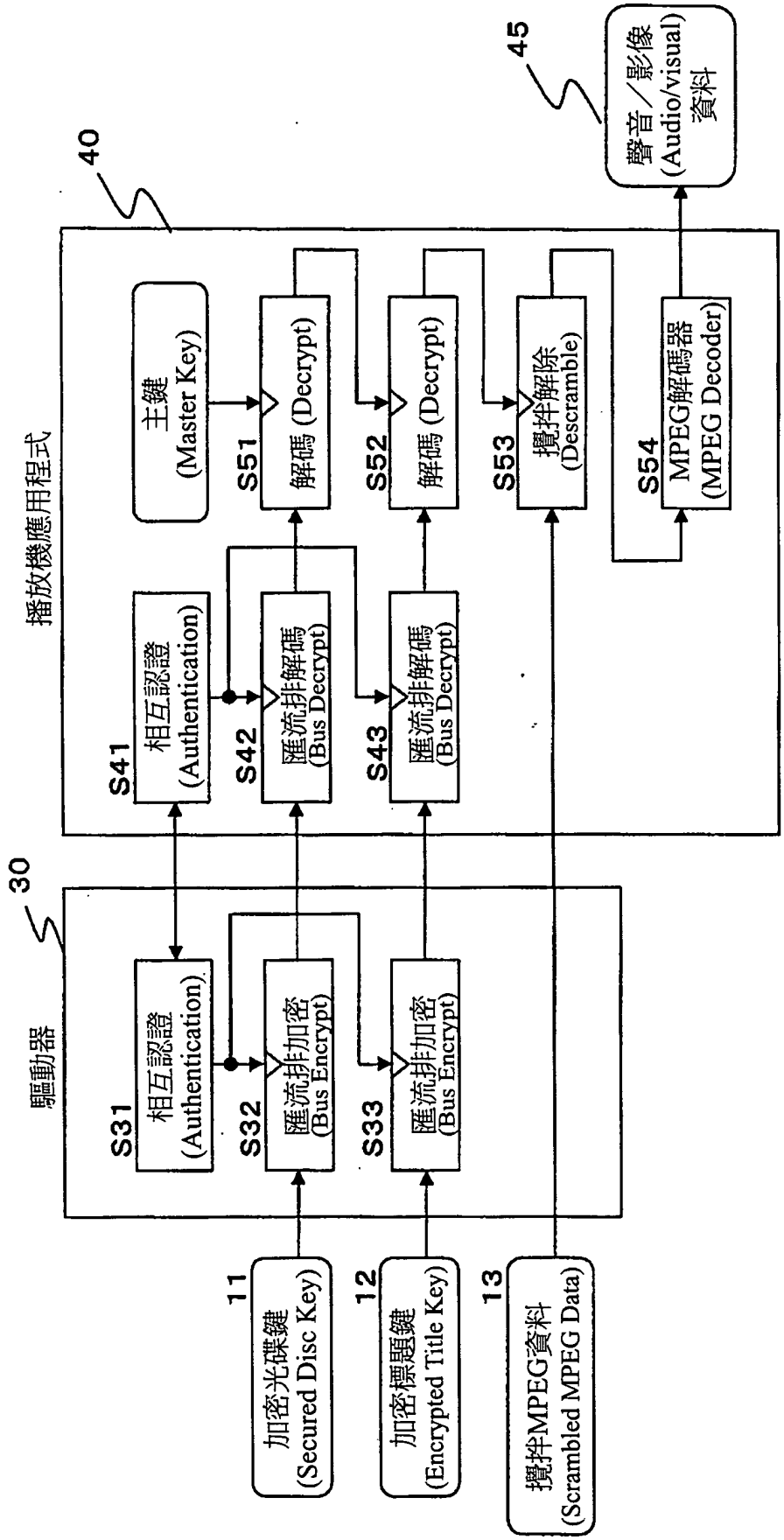

11
加密光碟鍵
(Secured Disc Key)
12
加密標題鍵
(Encrypted Title Key)
13
攪拌MPEG資料
(Scrambled MPEG Data)
30
驅動器
S31
相互認證
(Authentication)
S32
匯流排加密
(Bus Encrypt)
S33
匯流排加密
(Bus Encrypt)
40
播放機應用程式
S41
相互認證
(Authentication)
S42
匯流排解碼
(Bus Decrypt)
S43
匯流排解碼
(Bus Decrypt)
主鍵
(Master Key)
S51
解碼 (Decrypt)
S52
解碼 (Decrypt)
S53
攪拌解除
(Descramble)
S54
MPEG解碼器
(MPEG Decoder)
45
聲音／影像
(Audio/visual)
資料

圖 2

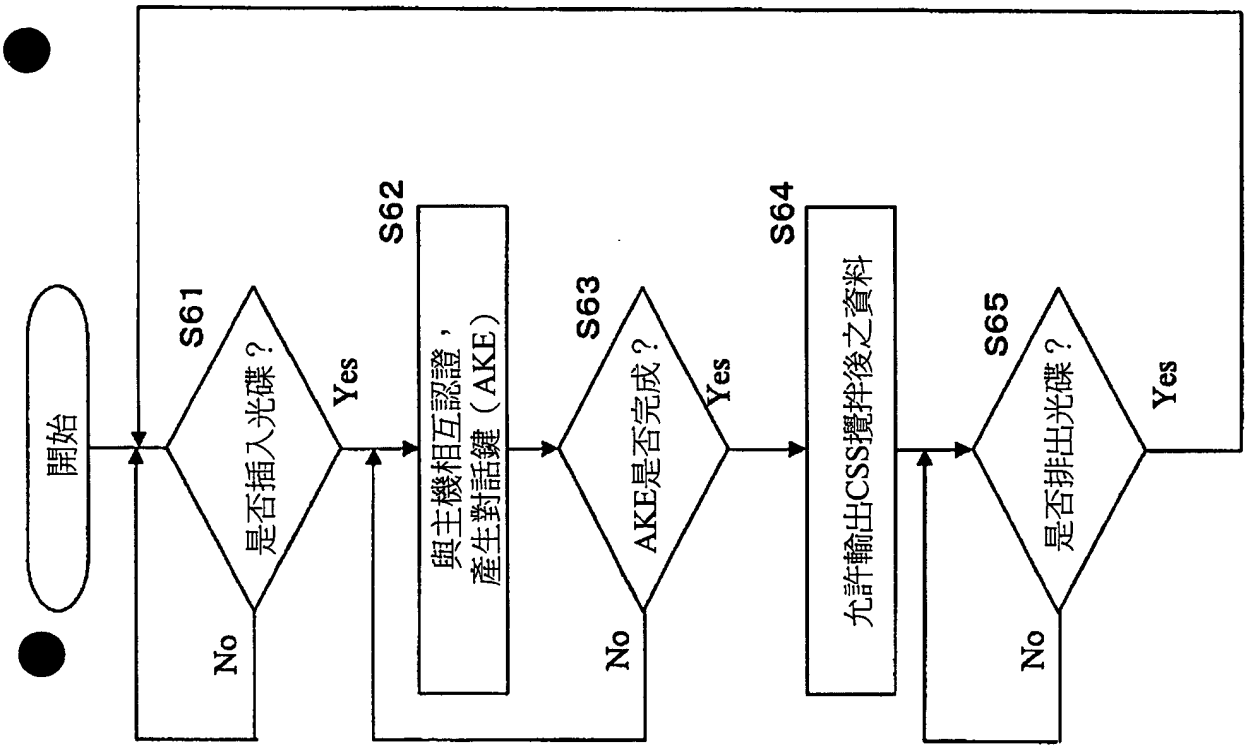

開始
S61
是否插入光碟？
Yes
No
S62
與主機相互認證，
產生對話鍵（AKE）
S63
AKE是否完成？
Yes
No
S64
允許輸出CSS攪拌後之資料
S65
是否排出光碟？
Yes
No

圖 3

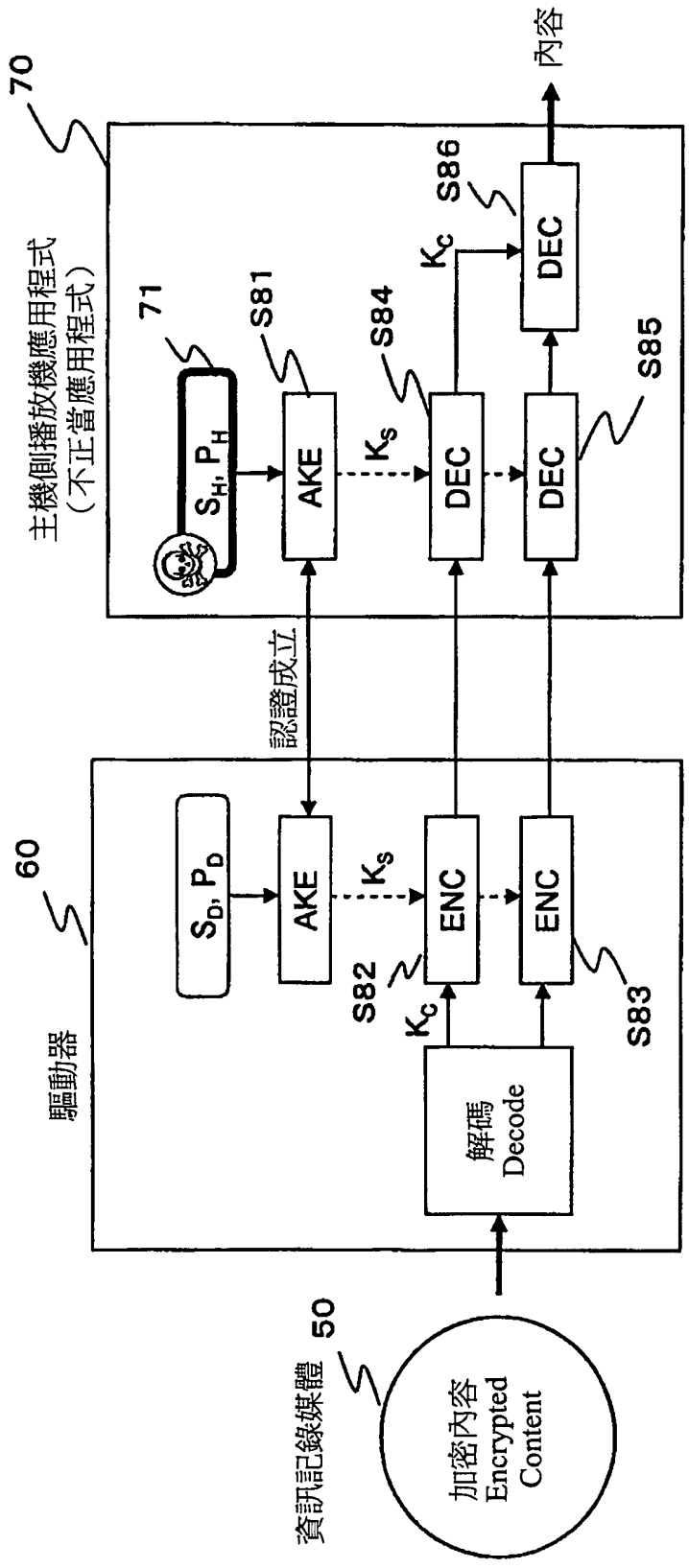

70
主機側播放機應用程式
（不正當應用程式）
71
S_H, P_H
S81
AKE
K_S
S84
DEC
K_C
S86
DEC
DEC
S85
內容
認證成立
60
驅動器
S_D, P_D
AKE
K_S
ENC
ENC
S82
K_C
S83
解碼
Decode
50
資訊記錄媒體
加密內容
Encrypted
Content

圖 4

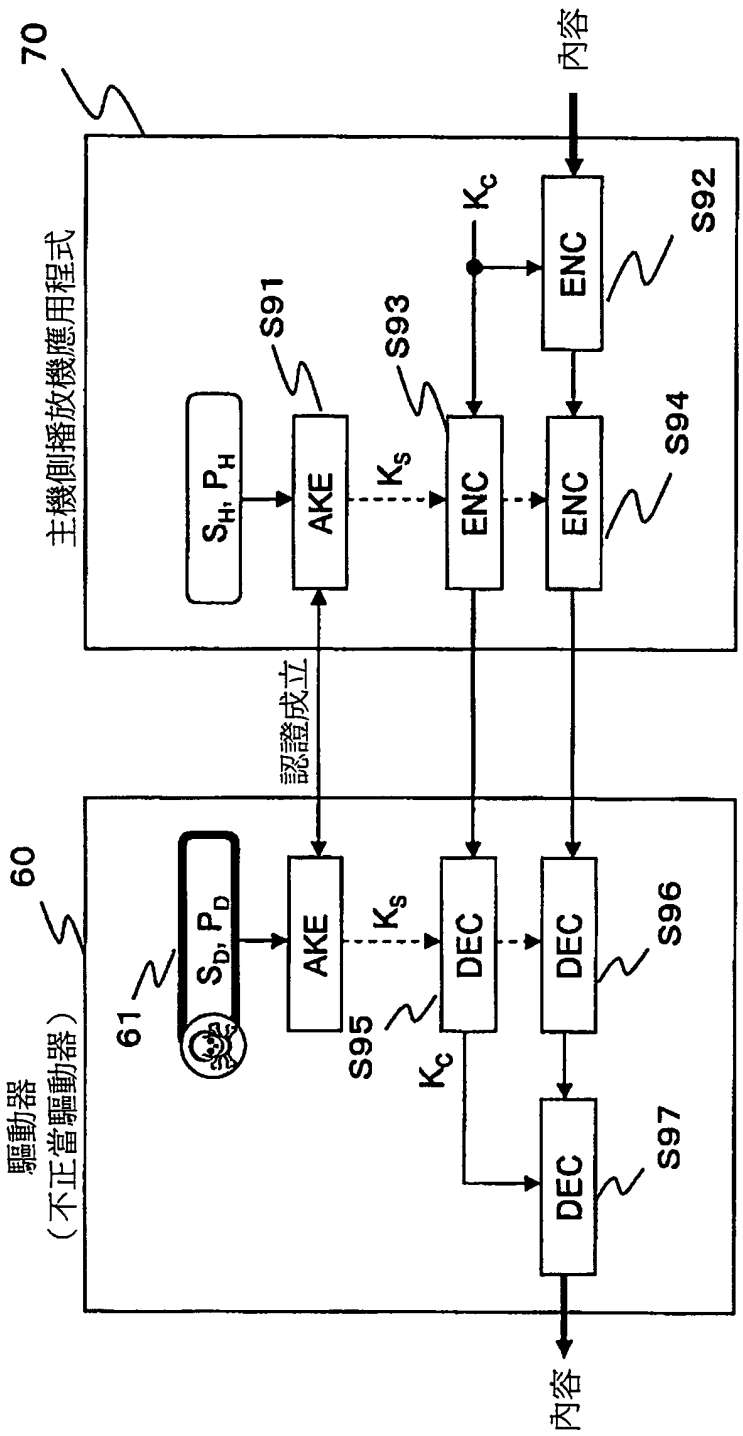

70
主機側播放機應用程式
內容
K_c
S92
ENC
S91
S93
S_H, P_H
AKE
K_s
ENC
S94
ENC
認證成立
60
驅動器
（不正當驅動器）
61
S_D, P_D
AKE
K_s
S95
DEC
S96
DEC
K_c
S97
DEC
內容

圖 5

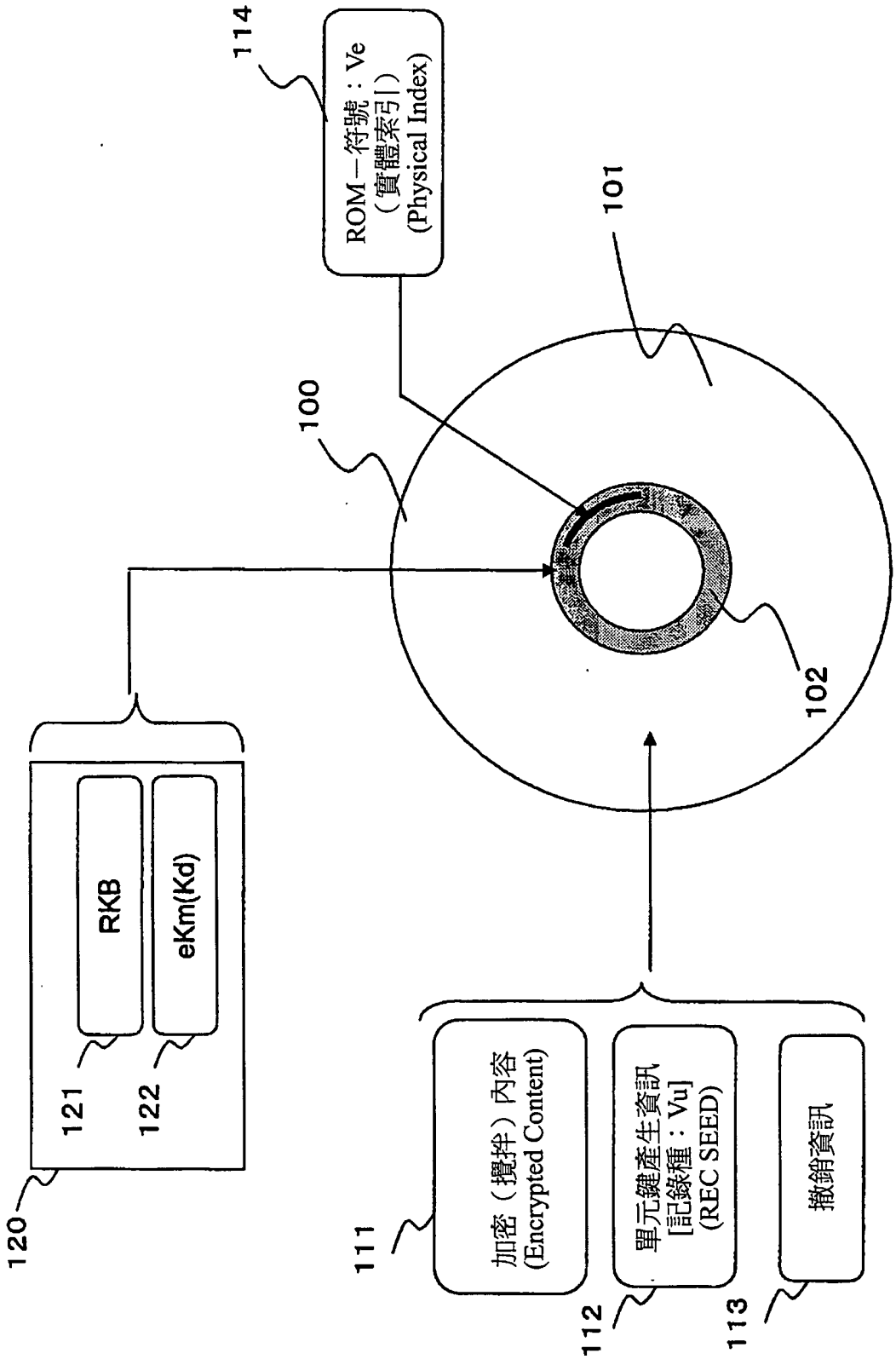
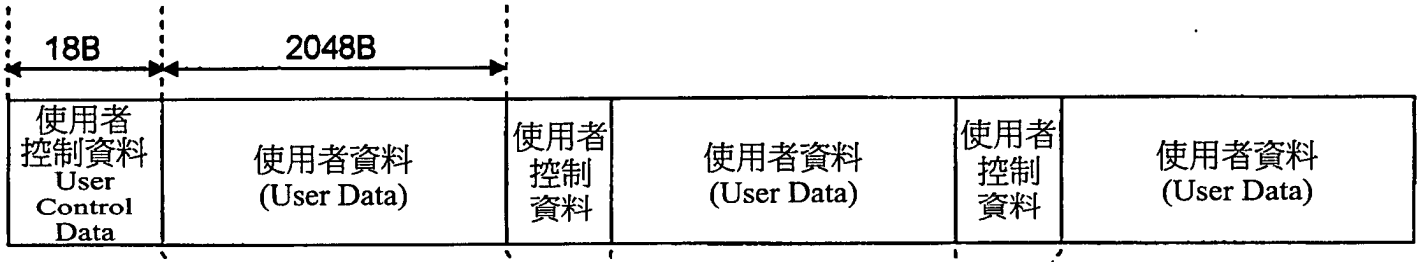
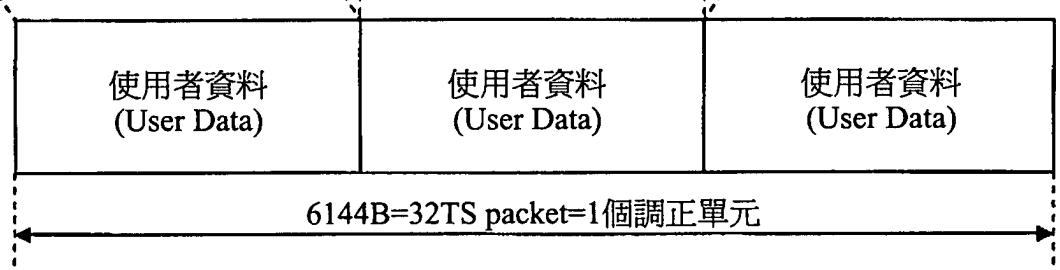

114
ROM－符號：Ve
（實體索引）
(Physical Index)
101
100
102
120
121
RKB
122
eKm(Kd)
111
加密（攪拌）內容
(Encrypted Content)
112
單元鍵產生資訊
[記錄種：Vu]
(REC SEED)
113
撤銷資訊

圖 6

(a)光碟上之資料行



(b)
以32TS packet=6KB構成1個調正單元。1個調正單元係AV資料，亦即MPEG TS packet之光碟記錄中加密之單位。



(c)
CCI檔等之non-AV資料以2KB單位加密進行光碟記錄。

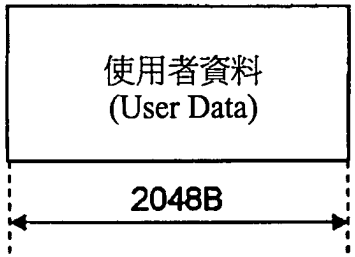


圖 7

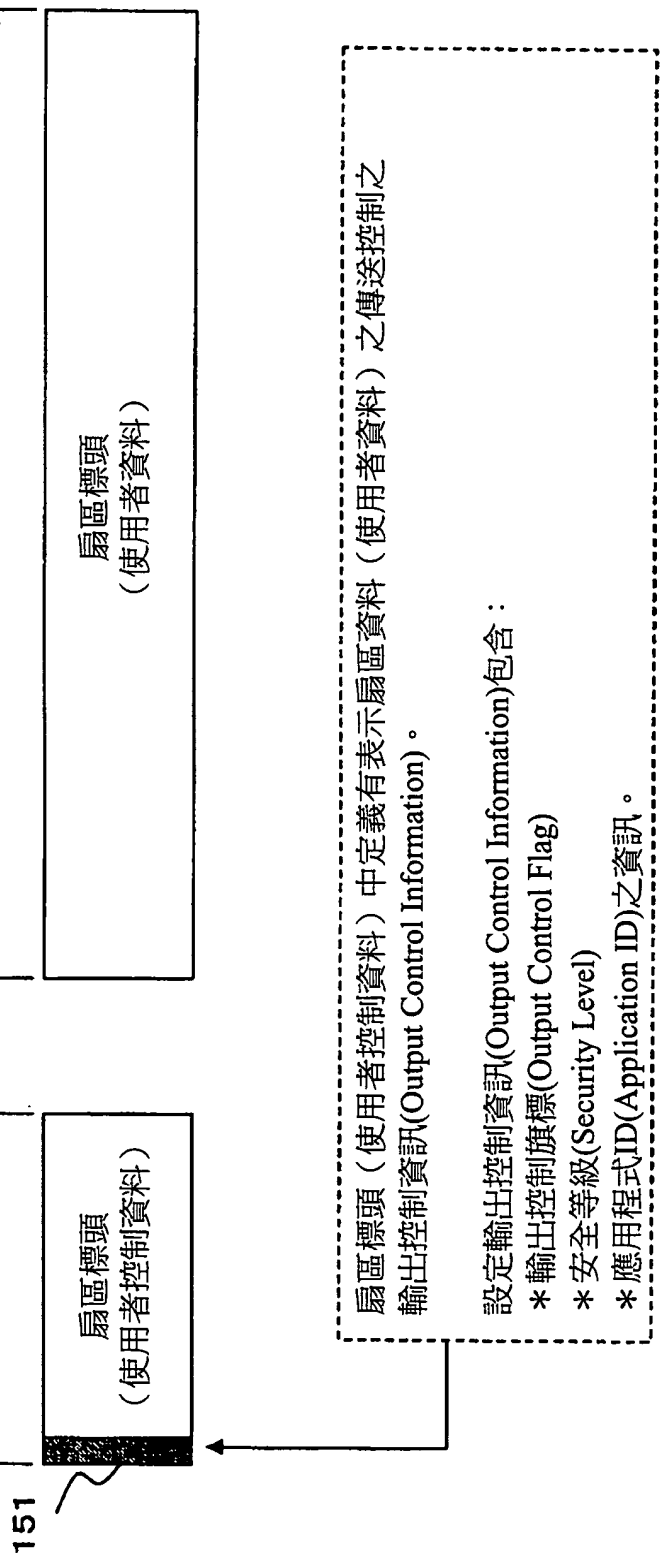

2048B
扇區標頭
（使用者資料）
18B
扇區標頭
（使用者控制資料）
151
扇區標頭（使用者控制資料）中定義有表示扇區資料（使用者資料）之傳送控制之輸出控制資訊(Output Control Information)。
設定輸出控制資訊(Output Control Information)包含：
＊輸出控制旗標(Output Control Flag)
＊安全等級(Security Level)
＊應用程式ID(Application ID)之資訊。

圖 8

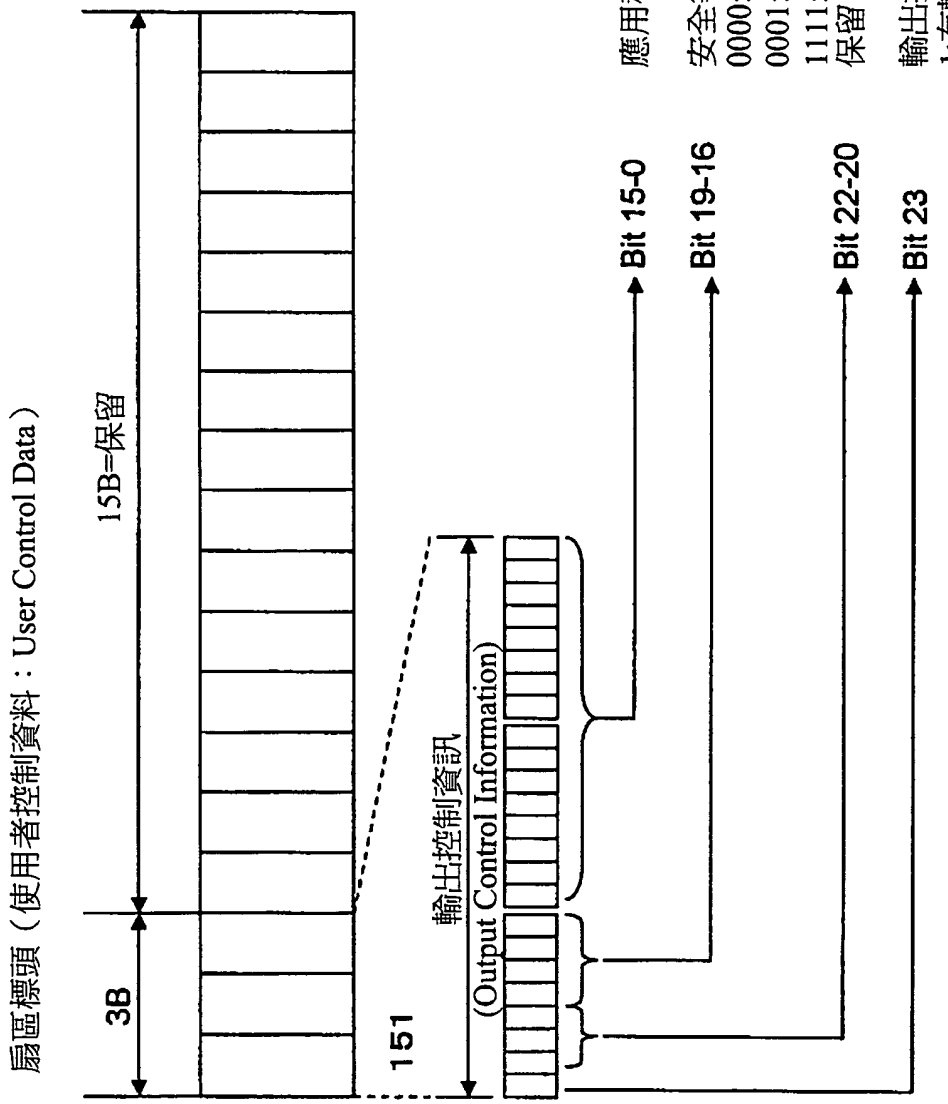

扇區標頭（使用者控制資料：User Control Data）
3B
15B=保留
151
輸出控制資訊
(Output Control Information)
Bit 15-0
Bit 19-16
Bit 22-20
Bit 23
應用程式ID(Application ID)
安全等級(Security Level)
0000:最低安全等級
0001:TCG規格等級
1111:最高安全等級
保留
輸出控制旗標(Output Control Flag)
1:有輸出限制及匯流排加密
0:無輸出限制

圖 9

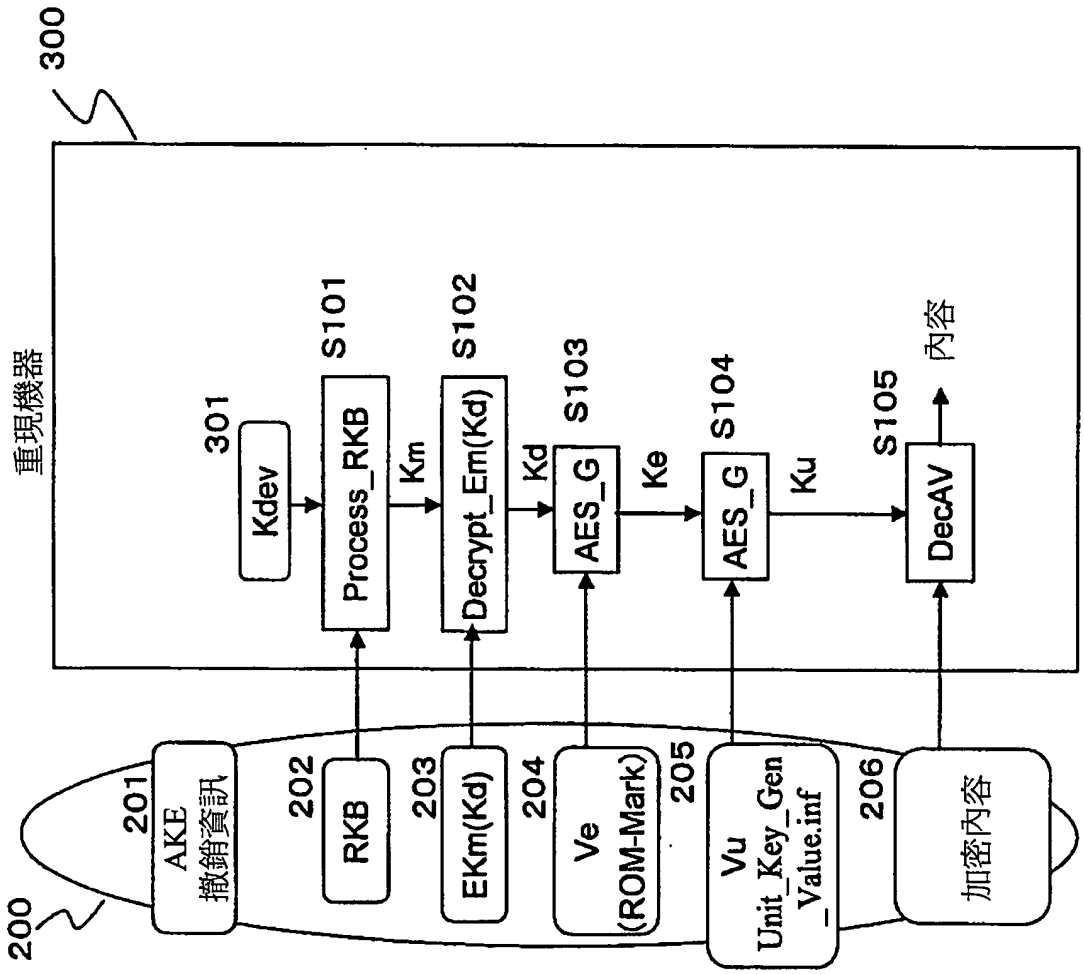

資訊記錄媒體
200
201
AKE
撤銷資訊
202
RKB
203
EKm(Kd)
204
Ve
(ROM-Mark)
205
Vu
Unit_Key_Gen
_Value.inf
206
加密內容
重現機器
300
301
Kdev
S101
Process_RKB
Km
S102
Decrypt_Em(Kd)
Kd
S103
AES_G
Ke
S104
AES_G
Ku
S105
DecAV
內容

圖 10

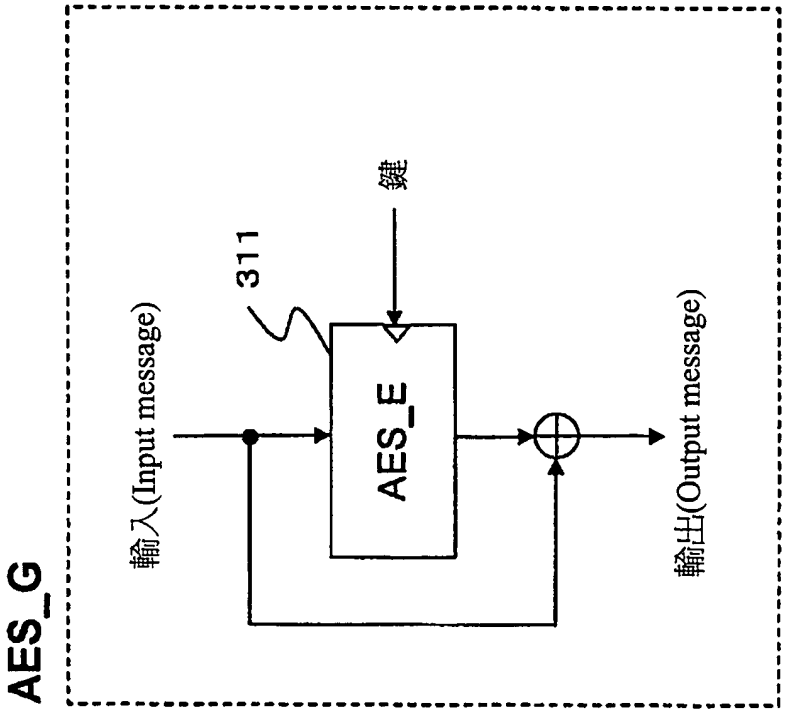


圖 11

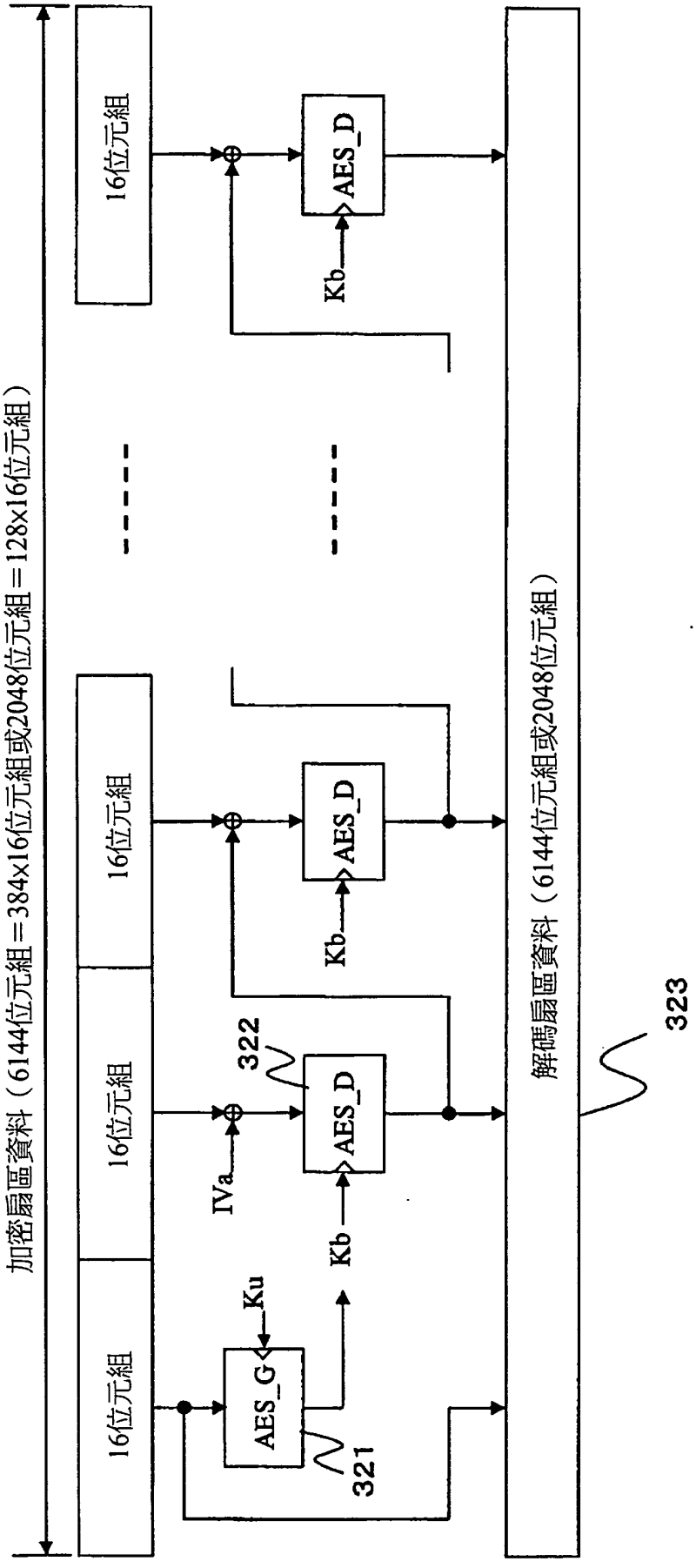

加密扇區資料（6144位元組＝384x16位元組或2048位元組＝128x16位元組）
16位元組
16位元組
16位元組
16位元組
AES_G
AES_D
AES_D
AES_D
Ku
Kb
Kb
Kb
IVa
321
322
323
解碼扇區資料（6144位元組或2048位元組）

圖 12

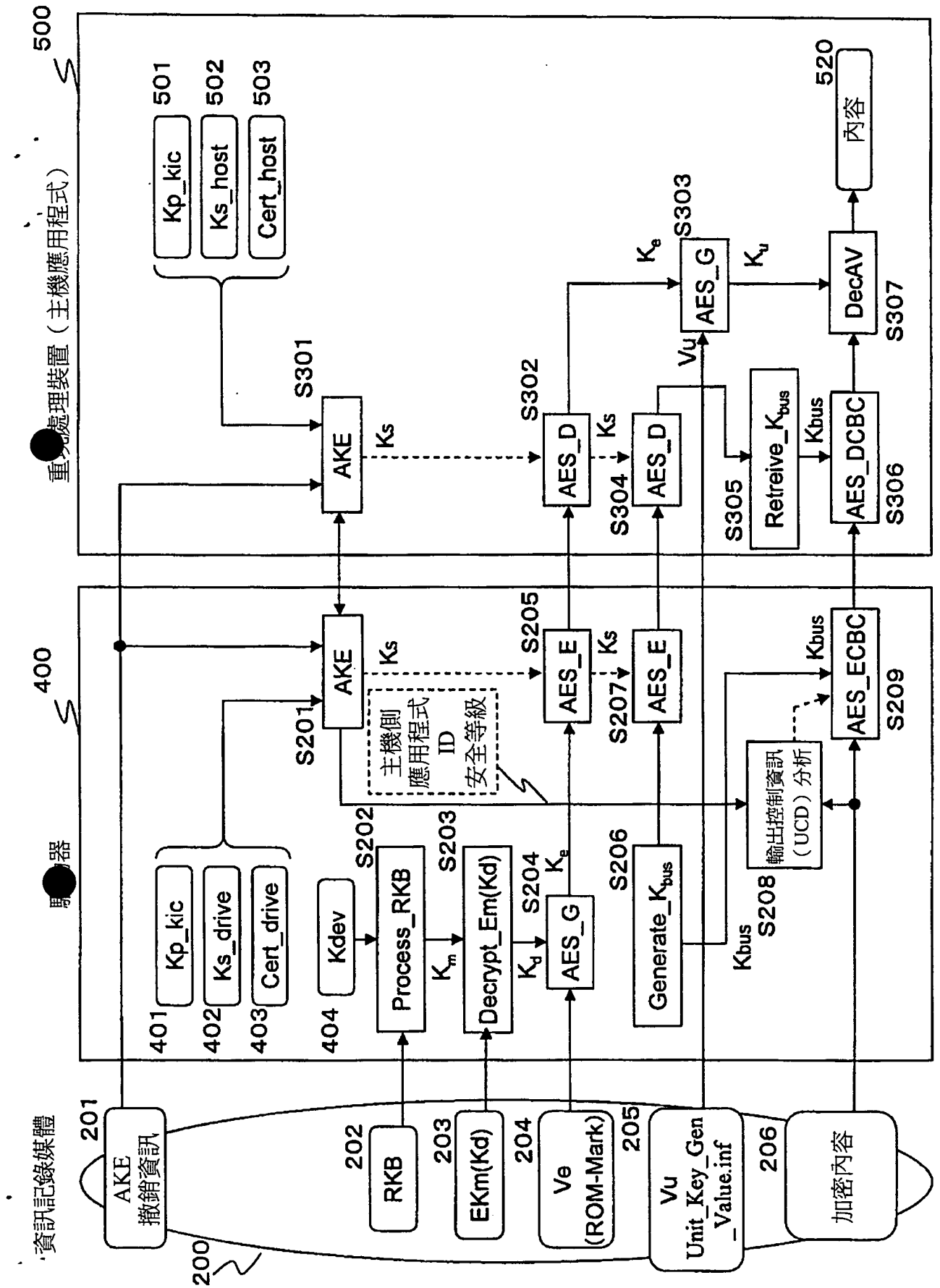

資訊記錄媒體
200
201
AKE
撤銷資訊
202
RKB
203
EKm(Kd)
204
Ve
(ROM-Mark)
205
Vu
Unit_Key_Gen
_Value.inf
206
加密內容
400
401
Kp_kic
402
Ks_drive
403
Cert_drive
404
Kdev
S201
AKE
Ks
主機側
應用程式
ID
安全等級
S202
Process_RKB
Km
S203
Decrypt_Em(Kd)
Kd
S204
AES_G
Ke
S205
AES_E
Ks
S206
Generate_Kbus
S207
AES_E
Kbus
S208
輸出控制資訊
(UCD) 分析
Kbus
S209
AES_ECBC
500
501
Kp_kic
502
Ks_host
503
Cert_host
S301
AKE
Ks
S302
AES_D
Ks
S304
AES_D
Vu
S305
Retreive_Kbus
Kbus
S306
AES_DCBC
S303
Ke
AES_G
Ku
S307
DecAV
520
內容

圖 13

(a) 驅動器公用鍵證明 Drive Certificate (Cert_drive) 530

位元組 \ 位元	7	6	5	4	3	2	1	0
0	證明型式 Certificate Type							
1	保留 Reserved							
2	SAC型式 (SAC Type)				裝置型式 (Device type)			
3	證明識別符 Certificate ID (40 bits) 531 532							
:								
7								
8	公用鍵 Public Key (320 bits)							
:								
27								
28	簽署 Signature (320 bits)							
:								
47								

(b)主機應用程式公用鍵證明 Host Certificate (Cert_host) 550

位元組 \ 位元	7	6	5	4	3	2	1	0
0	證明型式 Certificate Type				安全等級 SLCERT 551			
1	應用程式ID (Application ID AIDCERT) 552							
2	SAC型式 (SAC Type)				裝置型式 (Device type)			
3	證明識別符 Certificate ID (40 bits) 553 554							
:								
7								
8	公用鍵 Public Key (320 bits)							
:								
27								
28	簽署 Signature (320 bits)							
:								
47								

SAC Type — 'Host-Device', 'Peer-to-Peer', reserved

Device Type — 'HOST', 'DRIVE', reserved (where Device Class = Host-Device)

圖 14

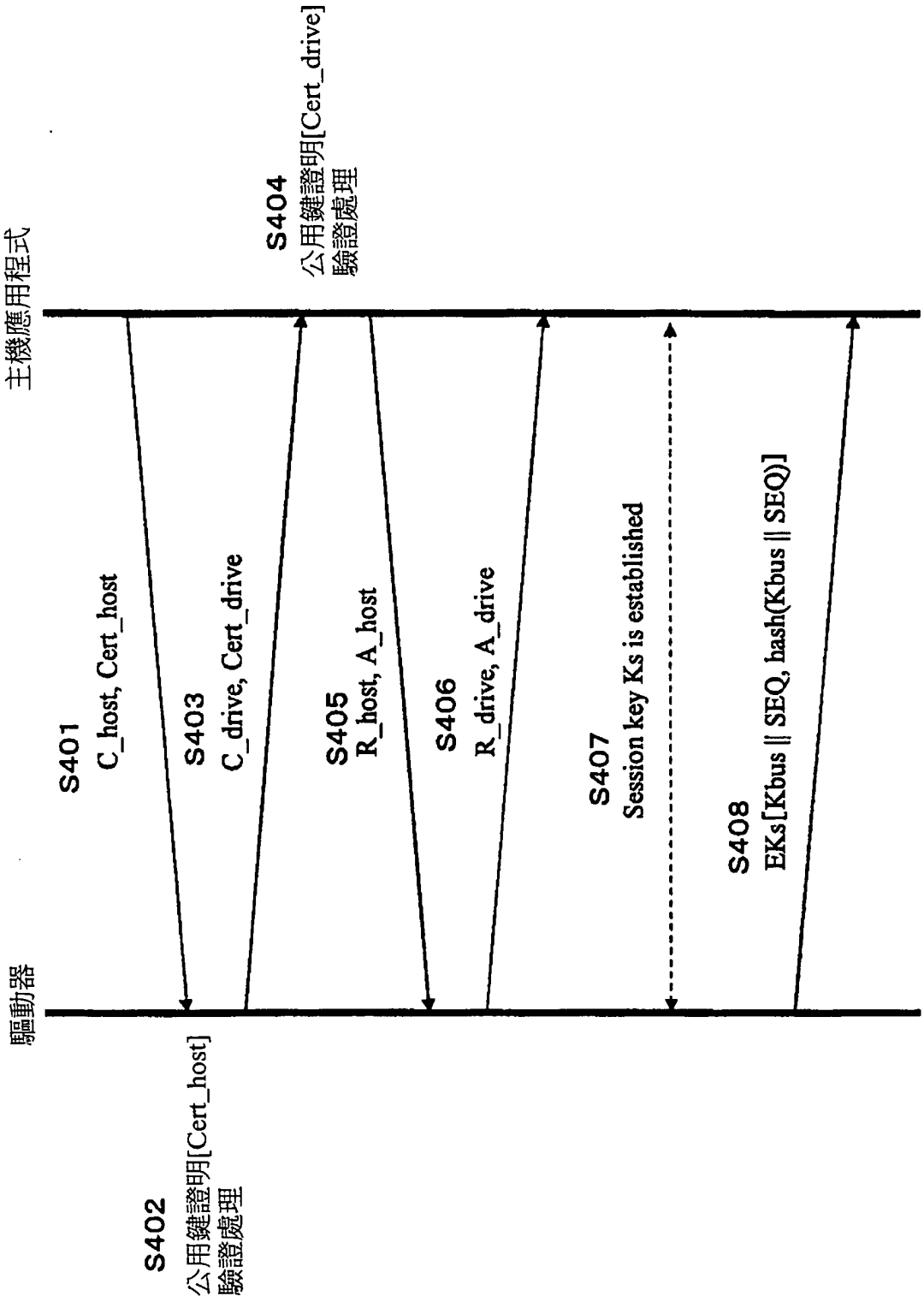

主機應用程式
驅動器
S401
C_host, Cert_host
S402
公用鍵證明[Cert_host]
驗證處理
S403
C_drive, Cert_drive
S404
公用鍵證明[Cert_drive]
驗證處理
S405
R_host, A_host
S406
R_drive, A_drive
S407
Session key Ks is established
S408
EKs[Kbus || SEQ, hash(Kbus || SEQ)]

圖 15

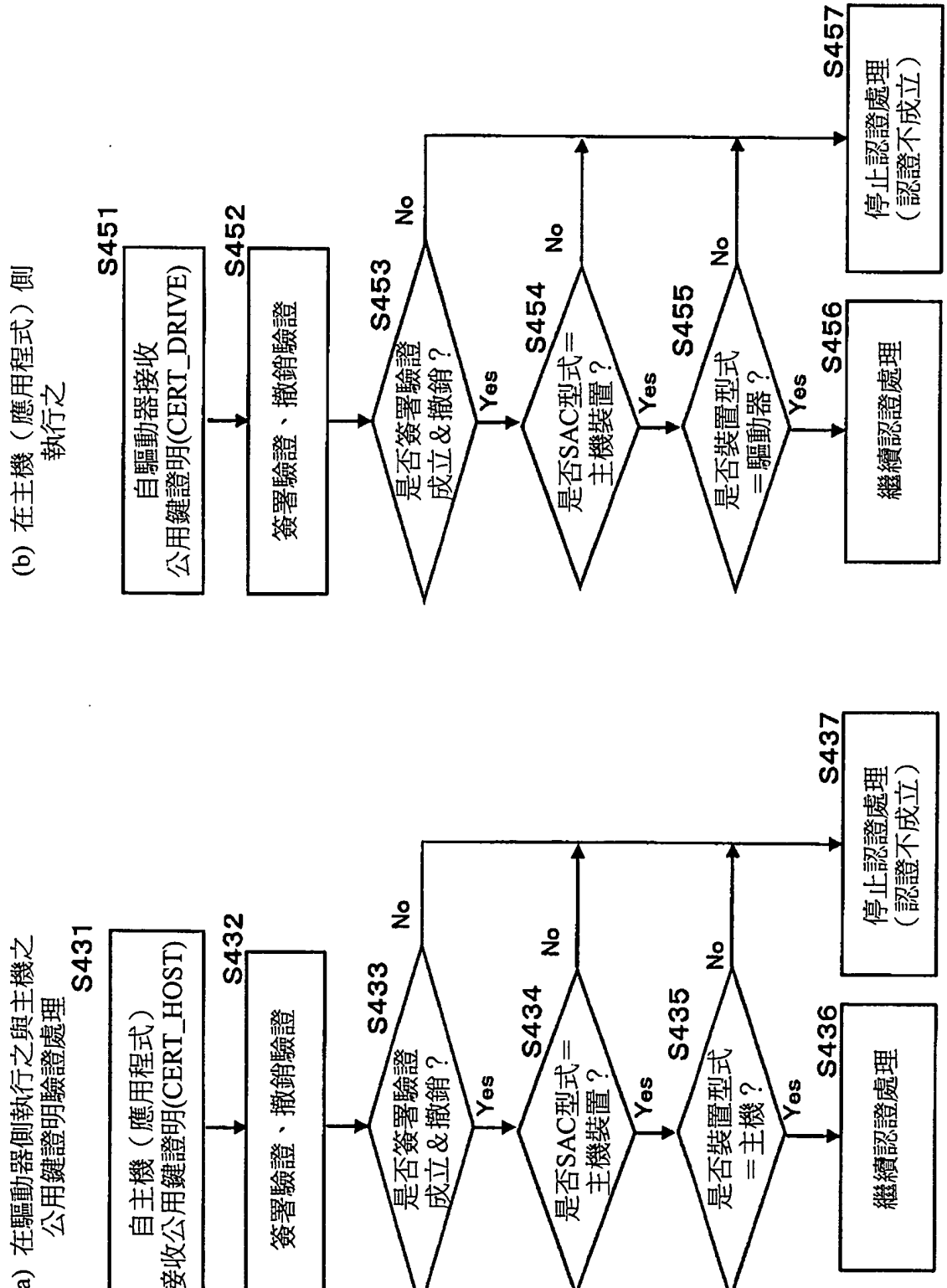

(a) 在驅動器側執行之與主機之公用鍵證明驗證處理
S431
自主機（應用程式）接收公用鍵證明(CERT_HOST)
S432
簽署驗證、撤銷驗證
S433
是否簽署驗證成立&撤銷？
No
Yes
S434
是否SAC型式＝主機裝置？
No
Yes
S435
是否裝置型式＝主機？
No
Yes
S436
繼續認證處理
S437
停止認證處理（認證不成立）
(b) 在主機（應用程式）側執行之
S451
自驅動器接收公用鍵證明(CERT_DRIVE)
S452
簽署驗證、撤銷驗證
S453
是否簽署驗證成立&撤銷？
No
Yes
S454
是否SAC型式＝主機裝置？
No
Yes
S455
是否裝置型式＝驅動器？
No
Yes
S456
繼續認證處理
S457
停止認證處理（認證不成立）

圖 16

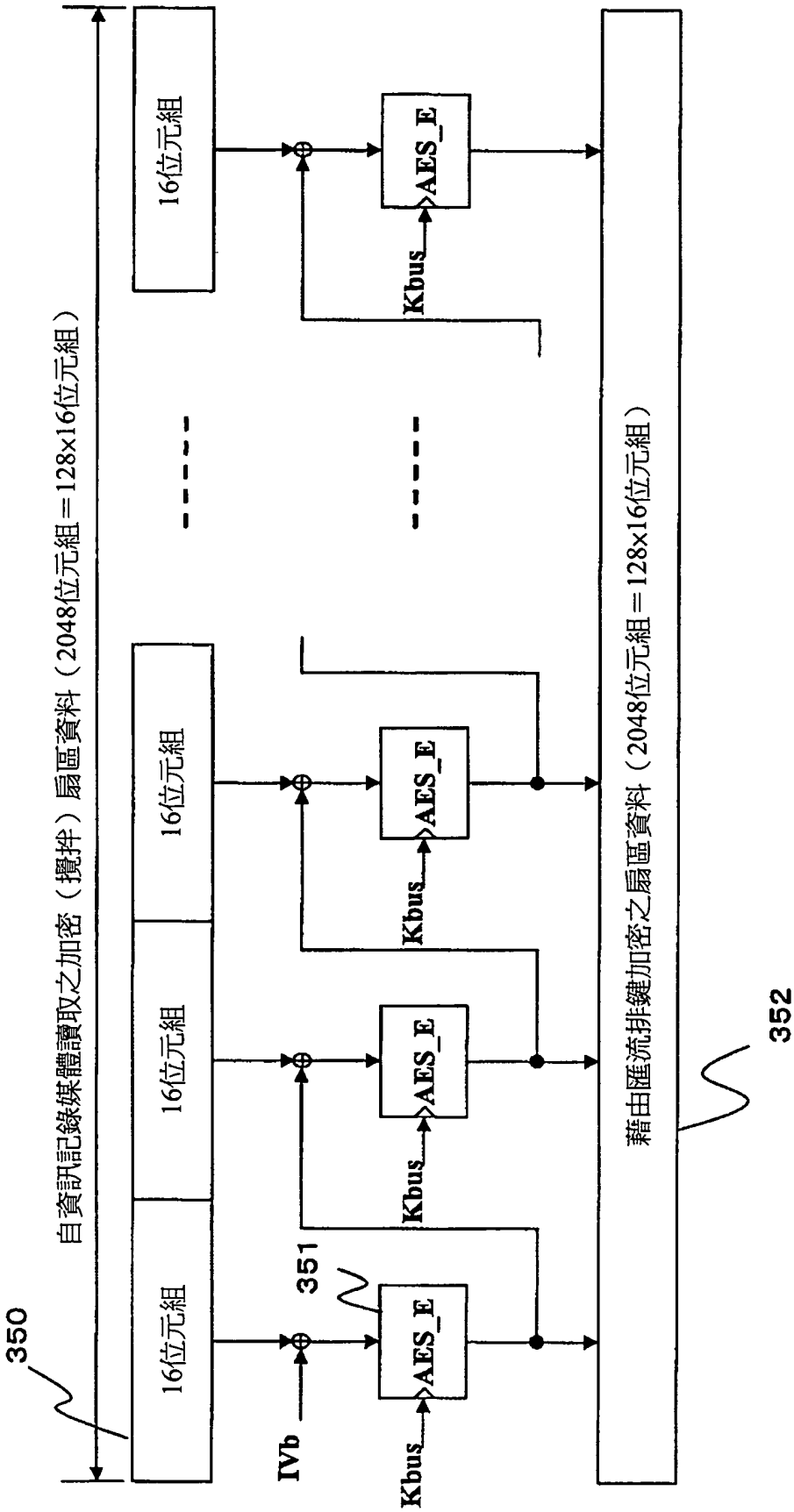

350
自資訊記錄媒體讀取之加密（攪拌）扇區資料（2048位元組＝128×16位元組）
16位元組
16位元組
16位元組
16位元組
351
IVb
Kbus
AES_E
Kbus
AES_E
Kbus
AES_E
Kbus
AES_E
352
藉由匯流排鍵加密之扇區資料（2048位元組＝128×16位元組）

圖 17

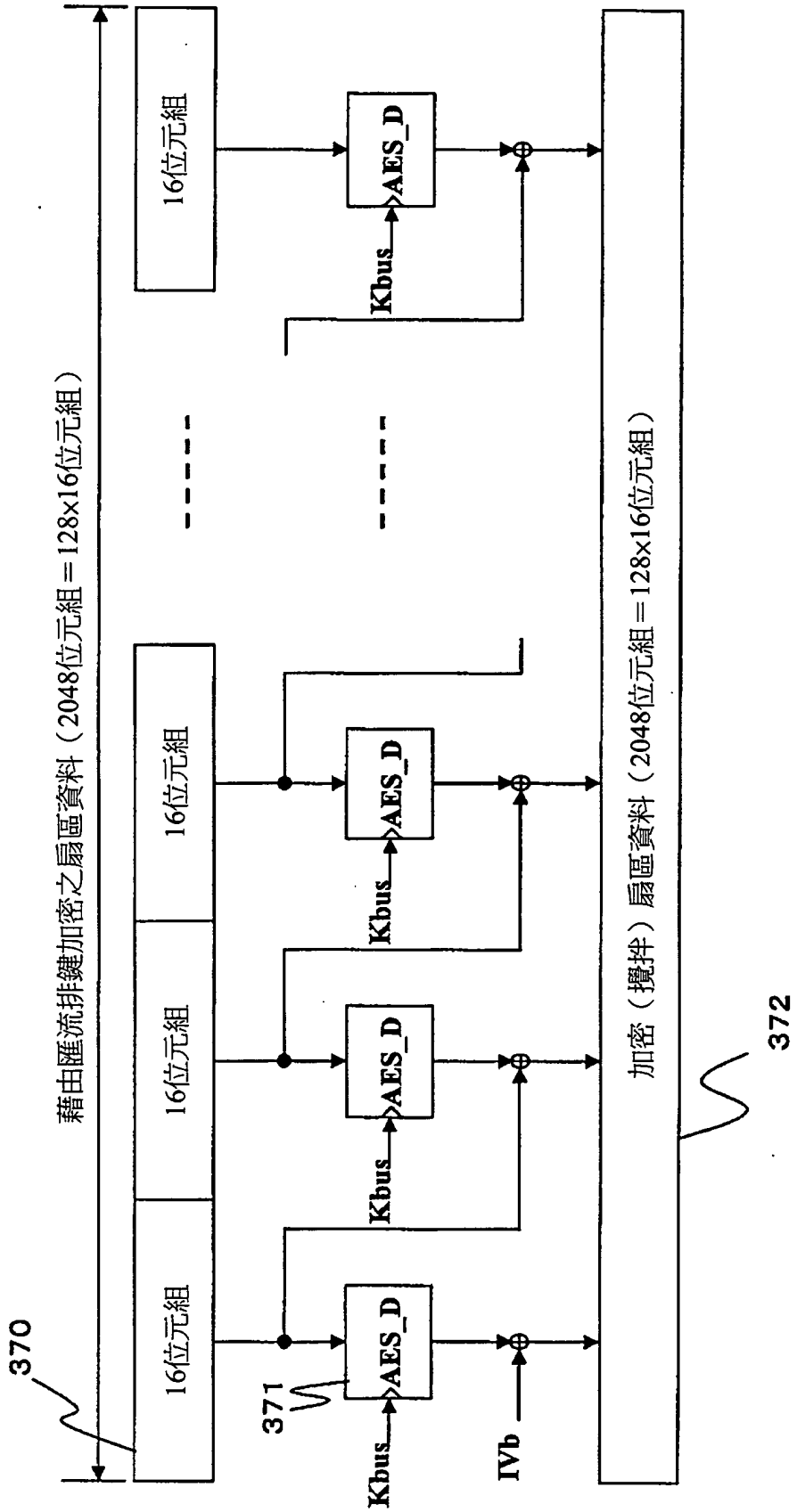

藉由匯流排鍵加密之扇區資料（2048位元組＝128x16位元組）
370
16位元組
371
AES_D
Kbus
IVb
372
加密（攪拌）扇區資料（2048位元組＝128x16位元組）

圖 18

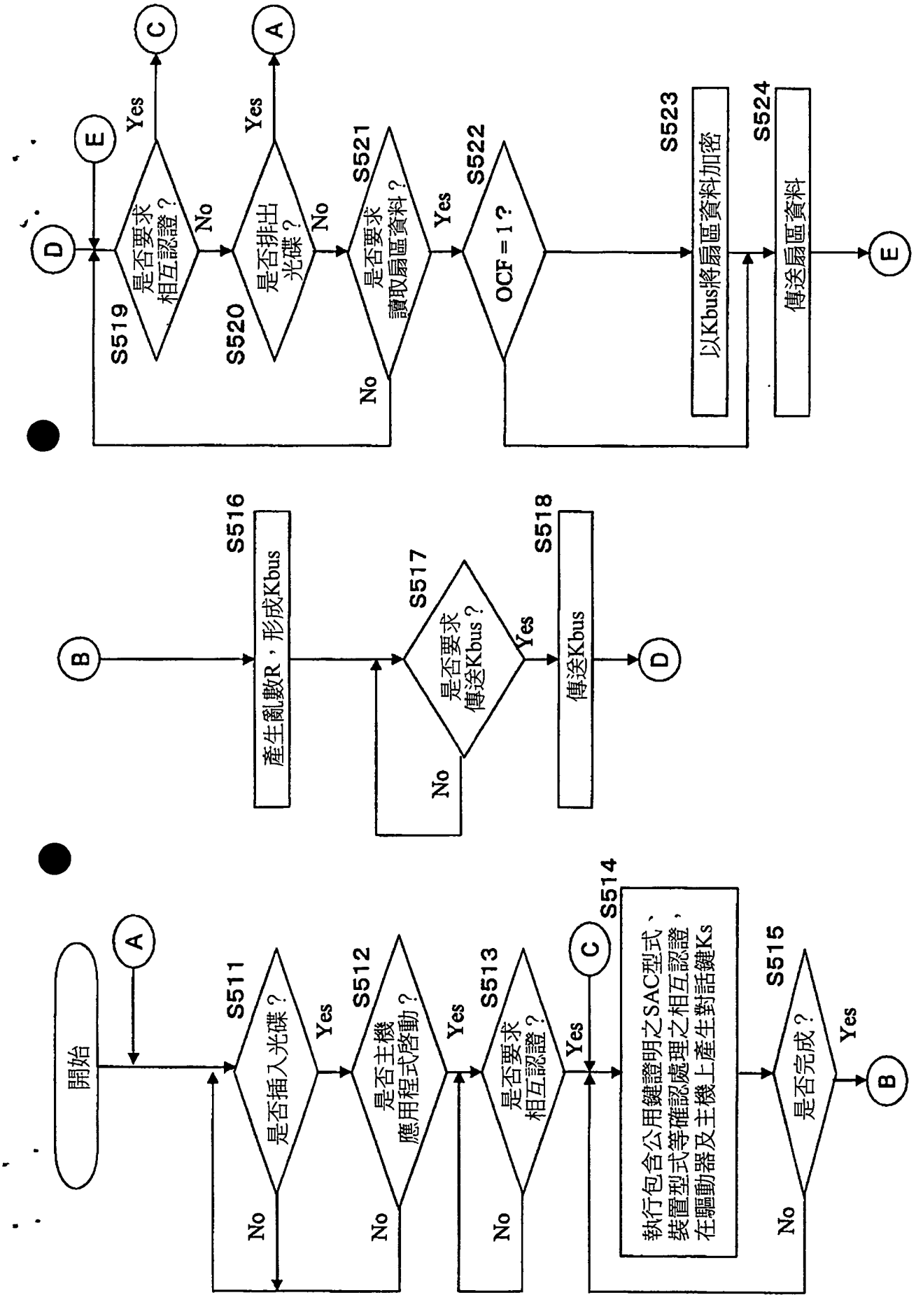

開始
A
S511
是否插入光碟？
No
Yes
S512
是否主機
應用程式啓動？
No
Yes
S513
是否要求
相互認證？
No
Yes
C
S514
執行包含公用鍵證明之SAC型式、
裝置型式等確認處理之相互認證，
在驅動器及主機上產生對話鍵Ks
S515
是否完成？
No
Yes
B
B
S516
產生亂數R，形成Kbus
S517
是否要求
傳送Kbus？
No
Yes
S518
傳送Kbus
D
D
E
S519
是否要求
相互認證？
No
Yes
C
S520
是否排出
光碟？
No
Yes
A
S521
是否要求
讀取扇區資料？
No
Yes
S522
OCF = 1？
S523
以Kbus將扇區資料加密
S524
傳送扇區資料
E

圖 19

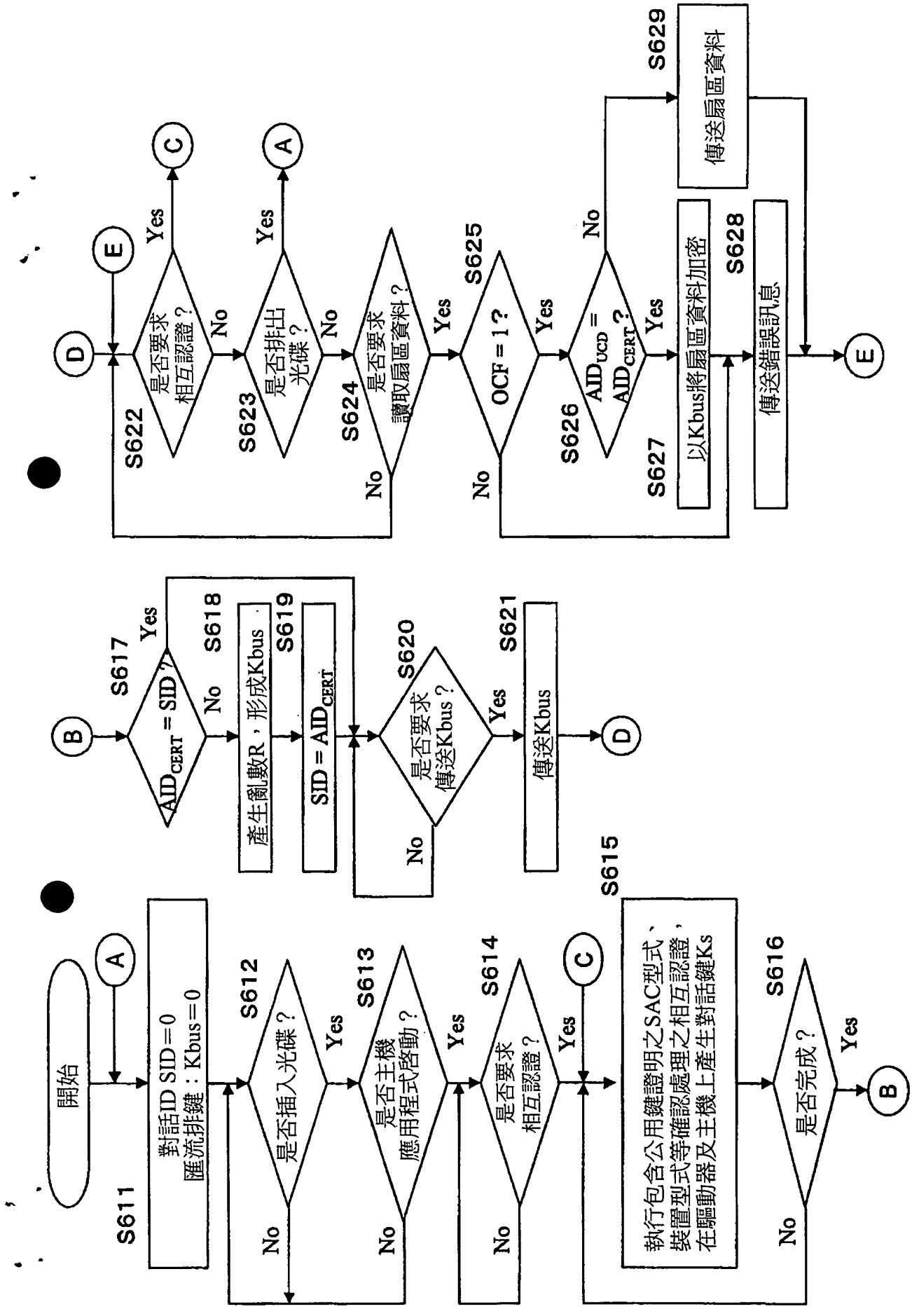

開始
A
S611
對話ID SID＝0
匯流排鍵：Kbus＝0
S612
是否插入光碟？
No
Yes
S613
是否主機
應用程式啓動？
No
Yes
S614
是否要求
相互認證？
No
Yes
C
S615
執行包含公用鍵證明之SAC型式、
裝置型式等確認處理之相互認證，
在驅動器及主機上產生對話鍵Ks
S616
是否完成？
No
Yes
B
B
S617
AIDCERT = SID ?
Yes
No
S618
產生亂數R，形成Kbus
S619
SID = AIDCERT
S620
是否要求
傳送Kbus？
No
Yes
S621
傳送Kbus
D
D
S622
是否要求
相互認證？
No
Yes
C
S623
是否排出
光碟？
No
Yes
A
S624
是否要求
讀取扇區資料？
No
Yes
S625
OCF = 1？
No
Yes
S626
AIDUCD =
AIDCERT ?
No
Yes
S627
以Kbus將扇區資料加密
S628
傳送錯誤訊息
S629
傳送扇區資料
E
E

圖 20

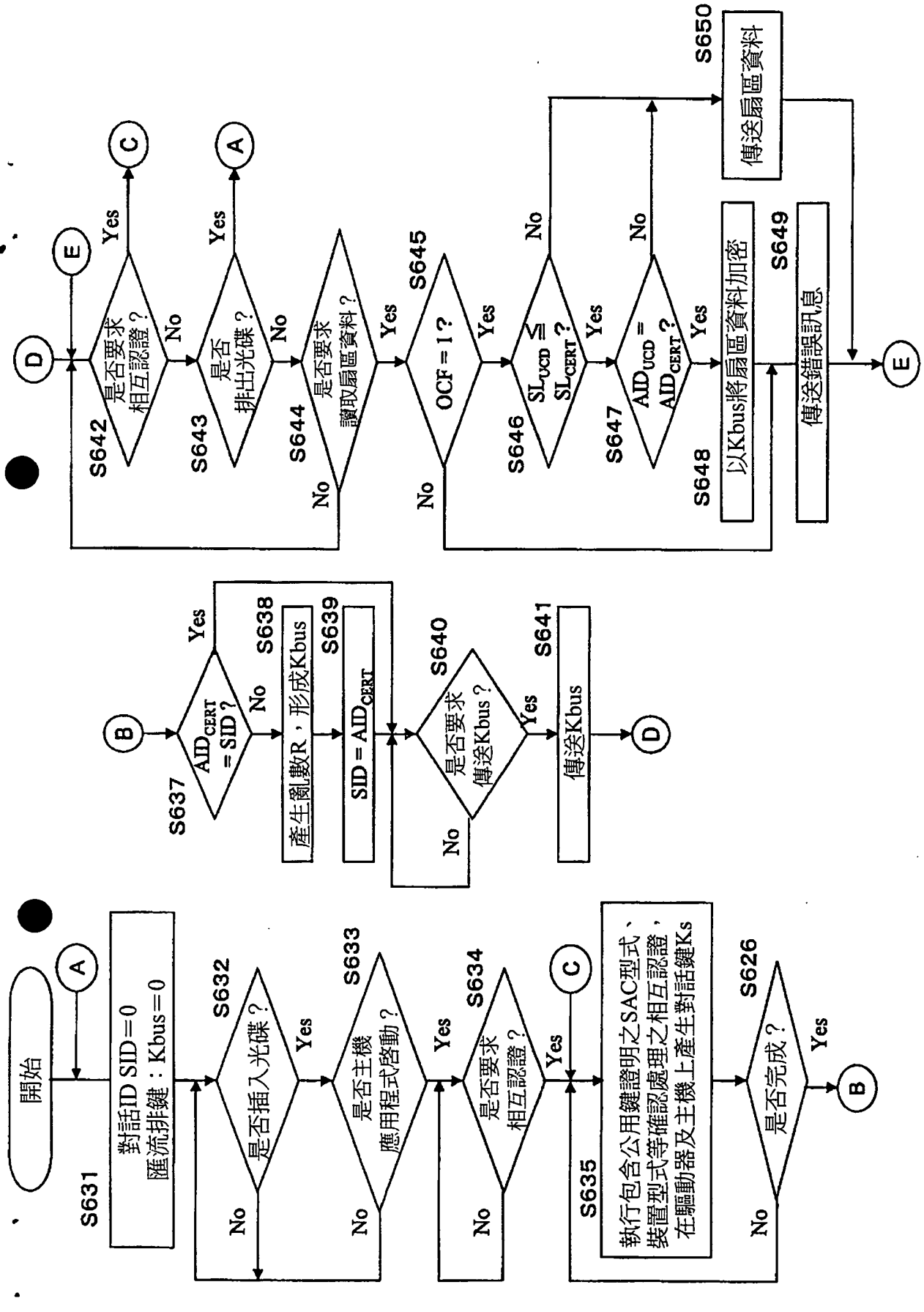

開始
A
S631
對話ID SID=0
匯流排鍵：Kbus=0
S632
是否插入光碟？
No
Yes
S633
是否主機
應用程式啓動？
No
Yes
S634
是否要求
相互認證？
No
Yes
C
S635
執行包含公用鍵證明之SAC型式、
裝置型式等確認處理之相互認證，
在驅動器及主機上產生對話鍵Ks
S626
是否完成？
No
Yes
B
B
S637
AID_CERT = SID？
Yes
No
S638
產生亂數R，形成Kbus
S639
SID = AID_CERT
S640
是否要求
傳送Kbus？
No
Yes
S641
傳送Kbus
D
D
E
S642
是否要求
相互認證？
No
Yes
C
S643
是否
排出光碟？
No
Yes
A
S644
是否要求
讀取扇區資料？
No
Yes
S645
OCF = 1？
No
Yes
S646
SL_UCD ≦ SL_CERT？
No
Yes
S647
AID_UCD = AID_CERT？
No
Yes
S648
以Kbus將扇區資料加密
S649
傳送錯誤訊息
S650
傳送扇區資料
E

圖 21

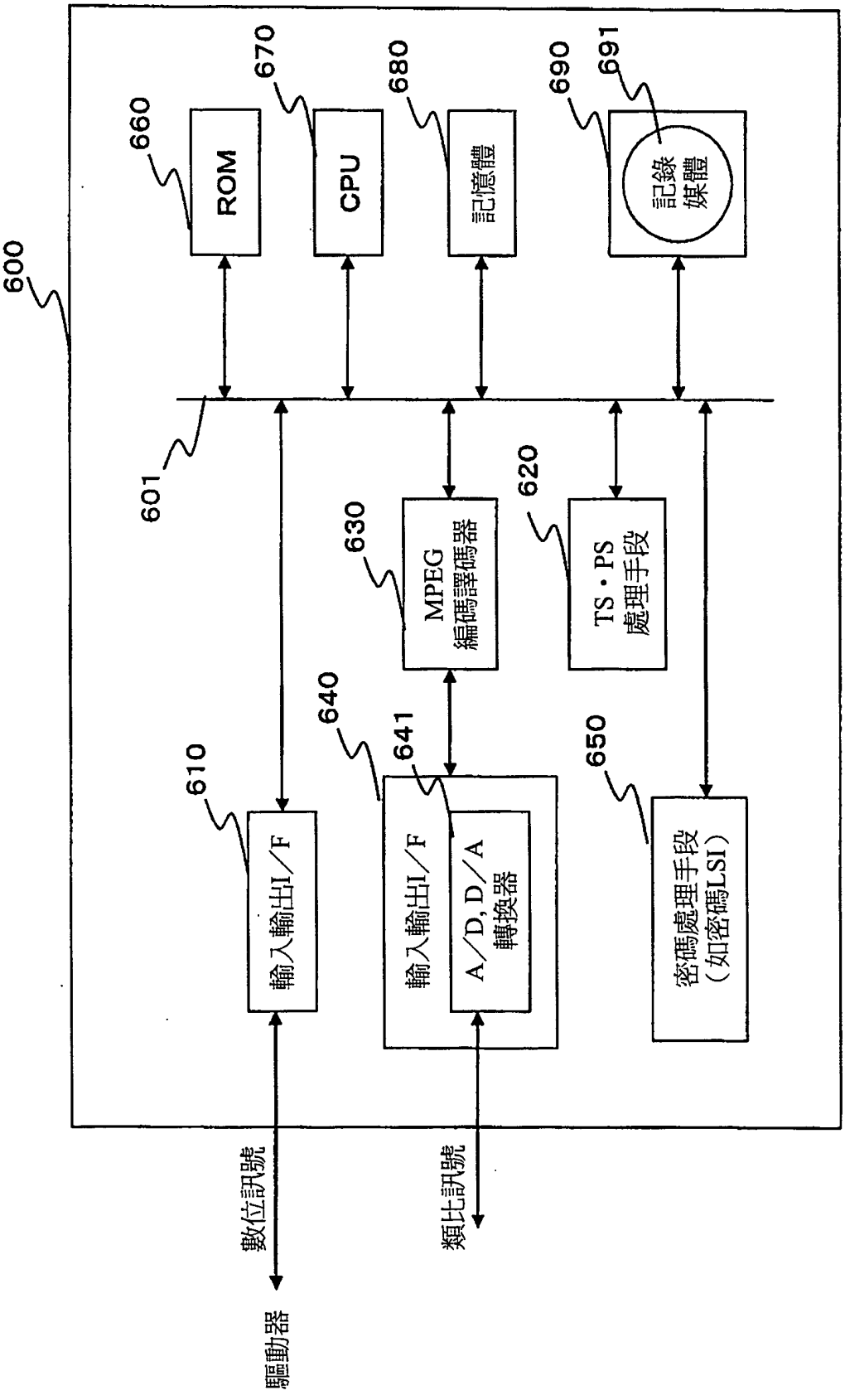

600
601
660
ROM
670
CPU
680
記憶體
690
691
記錄媒體
620
TS・PS處理手段
630
MPEG編碼譯碼器
640
641
輸入輸出I／F
A／D, D／A轉換器
610
輸入輸出I／F
650
密碼處理手段（如密碼LSI）
數位訊號
類比訊號
驅動器

圖 22

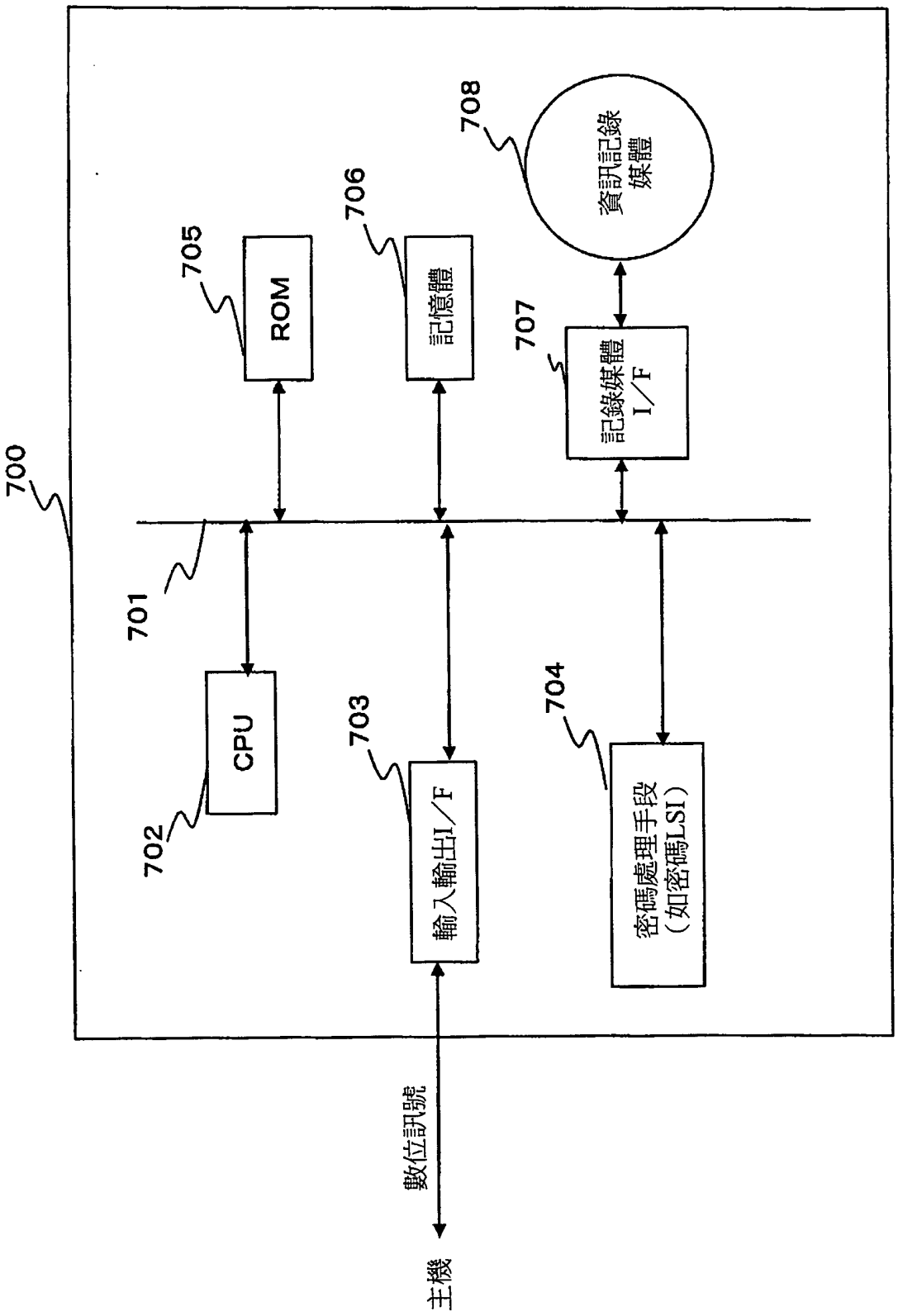

700
701
CPU
702
703
輸入輸出I／F
704
密碼處理手段
（如密碼LSI）
705
ROM
706
記憶體
707
記錄媒體
I／F
708
資訊記錄
媒體
數位訊號
主機

圖 23

七、指定代表圖：

(一)本案指定代表圖為：第(16)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)

公告本

99年1月22日修正替換頁

發明專利說明書

中文說明書替換頁(99年1月)

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：094106682

※ 申請日期：94.3.4　　※IPC 分類：G11B 7/00 (2006.01)

G06F 13/10 (2006.01)

一、發明名稱：（中文/英文）

資訊處理裝置、及認證處理方法及機器可讀媒體

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

再者，本發明之認證處理方法之一種實施態樣之特徵為：前述認證處理係與執行應用程式之主機機器連接，執行對資訊記錄媒體記錄或讀取資料之驅動器中執行之認證處理，前述驅動器依據自執行應用程式之主機接收之公用鍵證明之儲存資料，執行前述應用程式係應用執行主機應用程式主導之資料處理之安全認證通道(SAC)，而執行主機-裝置型式之資料處理之應用程式之SAC型式確認，確認裝置型式係主機之裝置型式確認，及將上述兩個確認作為認證成立條件之認證處理。

再者，本發明第三態樣之電腦程式之特徵為：係執行認證處理之電腦程式，且具有：

公用鍵證明取得步驟，其係取得認證對象保持之公用鍵證明；

資訊取得步驟，其係自前述公用鍵證明之儲存資料取得通道型式資訊；

通道型式確認步驟，其係依據前述通道型式資訊，確認在與認證對象之資料傳送中應用之通道型式；及

認證能否判定步驟，其係依據在前述通道型式確認步驟中確認之通道型式，來判定認證能否成立。

另外，本發明之電腦程式如係對於可執行各種程式碼之電腦系統，藉由以電腦可讀取之型式提供之記錄媒體、通訊媒體，如CD、FD及MO等記錄媒體，或是網路等通訊媒體可提供之電腦程式。藉由可以電腦可讀取之型式提供此種程式，而在電腦系統上實現依據程式之處理。

99年1月22日修正本

十、申請專利範圍：

1. 一種資訊處理裝置，其包含：

介面，其進行資料傳送處理；及

資料處理部，其執行資料處理；

其中前述資料處理部係：

(a)執行與資料傳送之對象之認證處理，以作為執行資料處理之條件，並以此作為利用該介面之資料傳送之結果；

(b)確認：

(i)在用於該認證處理之資料傳送中被應用之通道型式，其係依據儲存在被認證對象保持之公用鍵證明中之第一資料，且儲存在該公用鍵證明中之該第一資料包含該通道型式，及

(ii)該認證對象之裝置型式，其係依據儲存在被該認證對象保持之該公用鍵證明中之第二資料，且儲存在該公用鍵證明中之該第二資料包含該裝置型式；及

(c)判定認證是否成立，其係依據：

(i)儲存在該公用鍵證明中之該通道型式，及

(ii)儲存在該公用鍵證明中之該裝置型式。

2. 如請求項1之資訊處理裝置，其中前述資料處理部：

依據作為認證對象保持之公用鍵證明之儲存資料之安全認證通道(SAC)資訊，來確認設定於該公用鍵證明中之該通道型式是否為用以應用執行主機應用程式主導之資料處理之安全認證通道(SAC)而進行資料處理之主機-裝

置型式，；及

依據該通道型式是否為應用執行主機應用程式主導之資料處理之安全認證通道(SAC)而進行資料處理之主機-裝置型式，來判定認證能否成立。

3. 如請求項1之資訊處理裝置，其中前述資料處理部：

依據作為認證對象保持之公用鍵證明之儲存資料之安全認證通道(SAC)資訊，確認設定以作為公用鍵證明之通道型式是否為應用ATAPI匯流排連接，或是USB匯流排連接或是應用IEEE1394中之串聯匯流排協定(SBP)之安全通道進行資料處理之主機-裝置型式；及

依據該通道型式是否為應用該ATAPI匯流排連接，或是該USB匯流排連接或是應用該IEEE1394中之該串聯匯流排協定(SBP)之安全通道的主機-裝置型式，來判定認證是否成立。

4. 如請求項1之資訊處理裝置，其中

該裝置型式包含指示下列中任一者之資訊：

(a)主機作為應用程式執行機器；及

(b)驅動器，其用於執行下列中任一者：

(i)資料記錄處理，及

(ii)對於資訊記錄媒體之資料回覆處理。

5. 如請求項1之資訊處理裝置，其進一步包含主機機器，其執行應用程式並與驅動器連接，其中前述資訊處理部依據從該驅動器接收之公用鍵證明中的儲存資料，來執行認證處理，並將下列作為認證成立條件：

安全認證通道型式確認，其藉由應用執行被主機應用程式主導之資料處理的安全認證通道(SAC)，來確認前述驅動器是否包含用於執行主機-裝置型式之資料處理的驅動器，裝置型式確認，其確認該裝置型式是否係驅動器。

6. 如請求項1之資訊處理裝置，其進一步包含驅動器，其用於連接執行應用程式之主機機器，並記錄資料到資訊記錄媒體或從該資訊記錄媒體讀取資料，其中前述資訊處理部係

依據從執行應用程式之主機接收之公用鍵證明中的儲存資料，來執行認證處理，並將下列作為認證成立條件：

安全認證通道型式確認，其藉由應用被主機應用程式主導之資料處理的安全認證通道(SAC)，而確認是否前述應用程式係包含用於執行主機-裝置型式之資料處理的應用程式，及

裝置型式確認，其確認該裝置型式是否係主機。

7. 一種認證處理方法，其包含：

公用鍵證明取得步驟，其係取得被認證對象保持之公用鍵證明，其中該公用鍵證明包含(i)包含通道型式之第一資料，及(ii)包含裝置型式之第二資料；通道型式資訊取得步驟，其係自儲存於前述公用鍵證明之該第一資料取得通道型式資訊；

裝置型式資訊取得步驟，其係自儲存於前述公用鍵證明之該第二資料取得裝置型式資訊；

通道型式確認步驟，其係依據取得之前述通道型式資

訊，確認在與該認證對象之資料傳送中應用之該通道型式；

裝置型式確認步驟，其係依據取得之前述裝置型式資訊，確認在與該認證對象之資料傳送中應用之該裝置型式；及

判定認證是否成立步驟，其係依據(i)該確認之通道型式(ii)該確認之裝置型式，來判定認證是否成立。

8. 如請求項7之認證處理方法，其進一步包含

依據作為在公用鍵證明中之儲存資料之安全認證通道(SAC)資訊，來確認設定於該公用鍵證明之通道型式是否為應用執行主機應用程式主導之資料處理之安全認證通道(SAC)，而進行資料處理之主機-裝置型式之步驟。

9. 如請求項7之認證處理方法，其進一步包含

依據作為公用鍵證明之儲存資料之安全認證通道(SAC)資訊，來確認設定於該公用鍵證明之通道型式是否為應用ATAPI匯流排連接，或是USB匯流排連接或是應用IEEE1394中之串聯匯流排協定(SBP)之安全通道進行資料處理之主機-裝置型式之步驟。

10. 如請求項7之認證處理方法，其中

該裝置型式包含指示下列中任一者之資訊：

(a)主機，其作為執行應用程式之機器，及

(b)驅動器，其用於執行下列中任一者

(i)資料記錄處理，及

(ii)對於資訊記錄媒體之資料重現處理。

11. 如請求項7之認證處理方法，其中前述認證處理包含在主機機器執行之認證處理，該主機機器進行與驅動器之連接且執行應用程式，其中該主機機器係

依據從該驅動器接收之公用鍵證明中的儲存資料，來執行認證處理，

並將下列作為認證成立條件：

安全認證通道型式確認，其藉由應用執行被主機應用程式主導之資料處理的安全認證通道(SAC)，來確認該驅動器是否包含用於執行主機-裝置型式之資料處理的驅動器，及

裝置型式確認，其確認該裝置型式是否係驅動器。

12. 如請求項7之認證處理方法，其中前述認證處理包含在驅動器執行之認證處理，該驅動器用於與主機機器連接且執行應用程式並記錄資料到資訊記錄媒體或從該資訊記錄媒體讀取資料，其中該驅動器係

依據從執行應用程式之主機接收之公用鍵證明中的儲存資料，來執行認證處理，

並將下列作為認證成立條件：

安全認證通道型式確認，其藉由應用被主機應用程式主導之資料處理的安全認證通道(SAC)，而確認是否前述應用程式係包含用於執行主機-裝置型式之資料處理的應用程式，及

裝置型式確認，其確認該裝置型式是否係主機。

13. 一種機器可讀媒體，其存有指令以使得一設備係架構以：

取得被認證對象保持之公用鍵證明，其中該公用鍵證明包含(i)包含通道型式之第一資料及(ii)包含裝置型式之第二資料；

自儲存於前述公用鍵證明之該第一資料取得通道型式資訊；

自儲存於前述公用鍵證明之該第二資料取得裝置型式資訊；

依據取得之前述通道型式資訊，確認在與該認證對象之資料傳送中應用之該通道型式；

依據取得之前述裝置型式資訊，確認在與該認證對象之資料傳送中應用之該裝置型式；及

依據(i)該確認之通道型式(ii)該確認之裝置型式來判定認證是否成立。