公告本

739098

G09C
1/04
G06F

申請日期	89 年 12 月 8 日
案號	89126284
類別	G06F15/00, G09C 1/06

A4
C4

559705

（以上各欄由本局填註）

發明 新型 專利說明書

一、發明 新型 名稱	中文	資料處理裝置，資料處理系統及資料處理方法
	英文	Data processing apparatus, data processing system, and data processing method therefor
二、發明 創作 人	姓名	(1) 野中聰 (2) 江崎正
	國籍	(1) 日本　　(2) 日本
	住、居所	(1) 日本國東京都品川區北品川六－七－三五 蘇妮股份有限公司 (2) 日本國東京都品川區北品川六－七－三五 蘇妮股份有限公司
三、申請人	姓名（名稱）	(1) 蘇妮股份有限公司 ソニー株式会社
	國籍	(1) 日本
	住、居所（事務所）	(1) 日本國東京都品川區北品川六丁目七番三五號
	代表人 姓名	(1) 出井伸之

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有　□無主張優先權
日本	1999 年 12 月 20 日	11-361225	☑有主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

經濟部智慧財產局員工消費合作社印製

五、發明說明（１）

發明背景：

１、發明領域

本發明係關於一種資料處理裝置及系統，用於執行提供內容資料之處理，與一種資料處理方法，用於此裝置及系統。

２、相關技藝之敘述

有一種資料提供系統，用於分布加密內容資料至使用者之資料處理裝置，使用者做成預定的合約，且此資料提供系統用於使資料處理裝置能解碼內容資料並讀取及記錄。一種型式的此資料提供系統是習知電子音樂分布（ＥＭＤ）系統，用於分布音樂資料。

圖１０６是一圖形，指出一習知ＥＭＤ系統７００。在ＥＭＤ系統７００中，內容提供者７０１ａ與７０１ｂ加密內容資料７０４ａ、７０４ｂ與７０４ｃ，及著作權資訊７０５ａ、７０５ｂ與７０５ｃ，藉著使用執行相互證明之後所得到的連續鑰匙資料，然後提供加密資料至服務提者７１０線上或離線。著作權資訊７０５ａ、７０５ｂ與７０５ｃ可包括系列拷貝管理系統（ＳＣＭＳ）資訊，用於將著作權資訊嵌入內容資料之數位水記資訊，及用於將著作權資訊嵌入服務提供者之傳輸協定之資訊。

服務提供者７１０解碼接收的內容資料７０４ａ、７０４ｂ與７０４ｃ，及著作權資訊７０５ａ、７０５ｂ

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（２）

與７０５ｃ，藉著使用連續鑰匙資料。

然後服務提供者７１０將著作權資訊７０５ａ、７０５ｂ與７０５ｃ嵌入解碼的內容資料７０４ａ、７０４ｂ與７０４ｃ，其已被線上或離線接收，以產生內容資料７０７ａ、７０７ｂ與７０７ｃ。在此情形中，作爲部份著作權資訊７０４ａ、７０４ｂ與７０４ｃ，服務提供者７１０將數位水記資訊嵌入內容資料７０４ａ、７０４ｂ與７０４ｃ，藉著改變預定頻域，並將ＳＣＭＳ資訊嵌入使用於傳送內容資料７０４ａ、７０４ｂ與７０４ｃ至使用者之網路協定。

服務提供者７１０亦加密內容資料７０７ａ、７０７ｂ與７０７ｃ，藉著使用分別從鑰匙資料庫７０６讀取之內容鑰匙資料Ｋｃａ、Ｋｃｂ與Ｋｃｃ。隨後，服務提供者７１０加密一安全容器７２２，其儲存加密的內容資料７０７ａ、７０７ｂ與７０７ｃ，藉著使用在執行相互證明之後得到的連續鑰匙資料，並送出加密的安全容器７２２至儲存於使用者之終端裝置７０９中的狀態存取（ＣＡ）模組７１１。

ＣＡ模組７１１解碼安全容器７２２，藉著使用連續鑰匙資料。ＣＡ模組７１１亦接收來自服務提供者７１０的鑰匙資料庫７０６之內容鑰匙資料Ｋｃａ、Ｋｃｂ與Ｋｃｃ，藉著使用會計功能，例如電子解決系統或ＣＡ，並藉著使用連續鑰匙資料將它解碼。使得終端裝置７０９能解碼內容資料７０７ａ、７０７ｂ與７０７ｃ，藉著分

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（３）

別使用內容鑰匙資料Ｋｃａ、Ｋｃｂ與Ｋｃｃ。

ＣＡ模組７１１執行各內容之會計處理，以產生會計資訊７２１，並使用連續鑰匙資料將其加密，且將它送至服務提供者７１０之權利處理模組７２０。

在此情形中，ＣＡ模組７１１執行關於由服務提供者７１０提供的服務之項目的處理，換句話說，由服務提供者７１０管理的項目，例如使用者之合約（更新）資訊，收集例如使用網路所發生之月基本費，各內容之會計處理，及確保網路之基層的安全性。

於從ＣＡ模組７１１接收會計資訊時，服務提供者７１０分配服務提供者７１０和內容提供者７０１ａ、７０１ｂ與７０１ｃ之間的利潤。在此情形中，利潤從服務提供者７１０經由媒介例如日本作者、作曲家和出版商協會（ＪＡＳＲＡＣ），被分配至內容提供者７０１ａ、７０１ｂ與７０１ｃ。ＪＡＳＲＡＣ亦分配內容提供者７０１ａ、７０１ｂ與７０１ｃ之利潤至內容資料之著作權擁有者、藝術家、作曲家、作者及製造公司。

記錄分別以內容鑰匙資料Ｋｃａ、Ｋｃｂ與Ｋｃｃ解碼的內容資料７０７ａ、７０７ｂ與７０７ｃ於記錄媒體７２３上時，記錄媒體例如隨機存取記憶體（ＲＡＭ），終端裝置７０９執行拷貝控制，藉著重寫著作權資訊７０５ａ、７０５ｂ與７０５ｃ之ＳＣＭＣ位元。亦即，使用者執行拷貝控制，根據嵌入內容資料７０７ａ、７０７ｂ與７０７ｃ之ＳＣＭＣ位元，藉以實施著作權保

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（４）

護。

ＳＣＭＣ禁止內容資料之拷貝操作，例如兩次或以上的拷貝（免費拷貝），但允許無限制的一次拷貝，於是對於著作權保護是不夠的。

在上述ＥＭＤ系統７００中，內容提供者７０１需要監視服務提供者７１０之動作，服務提供者７１０在技術上能自由地處理未加密的內容資料，內容提供者７０１ａ、７０１ｂ與７０１ｃ之利潤會被不公平地剝削。

此外，在ＥＭＤ系統７００中，很難限制使用者之終端裝置７０９之非法動作，例如著作從服務提供者７１０分布的內容資料，並將其重新分布至另一終端裝置，因而亦不公平地剝削內容提供者７０１ａ、７０１ｂ與７０１ｃ之利潤。

發明節要：

因此，欲解決在相關技藝中之固有的上述問題，本發明之目的在於提供資料處理裝置、資料處理系統及資料處理方法，用於減小保護例如內容提供者之內容權利擁有者之利潤之負載。

欲達成上述目的，依據本發明之觀點，提供一資料處理裝置，用於根據使用控制政策（ＵＣＰ）資料，執行以內容鑰匙資料加密的內容資料之權利處理，且用於解密加密的內容鑰匙資料。資料處理裝置在一抗干預電路模組（tamper-resistant circuit module）內包括：一第一匯流排；

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 5 ）

一算術處理電路，連接至第一匯流排，用於根據ＵＣＰ資料執行內容資料之權利處理；一儲存電路，連接至第一匯流排；一第二匯流排；一第一介面電路，插置於第一匯流排與第二匯流排之間；一加密處理電路，連接至第二匯流排，用於解密內容鑰匙資料；及一外部匯流排介面電路，連接至第二匯流排。

依據前述資料處理裝置，內容資料、對應內容鑰匙資料及對應ＵＣＰ資料被分布，且用於解密內容鑰匙資料之執照鑰匙資料亦被分布。執照鑰匙資料被儲存於例如上述儲存電路中。

然後，響應經由外部匯流排介面電路來自外部算術處理裝置執行權利處理之指令，根據ＵＣＰ資料之內容資料的權利處理被執行於上述算術處理電路中。隨後，藉著使用從儲存電路讀取的執照鑰匙資料，內容鑰匙資料被解密於算術處理電路中。

前述資料處理裝置以另一解碼裝置執行相互證明，並藉著使用由相互證明所得到連續鑰匙資料，加密解密的內容鑰匙資料及內容資料，並將它們送至解碼裝置。

前述資料處理裝置可進一步包括在抗干預電路模阻內的第二介面電路。第一匯流排可包括第三匯流排，連接至算術處理電路及儲存電路，及一第四匯流排，連接至第一介面電路，且第二介面電路可被插置於第三匯流排與第四匯流排之間。

前述資料處理裝置可進一步在抗干預電路模阻內包括

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 6 ）

：第五匯流排；第三介面電路，連接至第五匯流排，用於執行與具有證明功能之資料處理電路之通訊，資料處理電路被負載在記錄媒體與積體電路卡的其中之一上；及一第四介面電路，插置於第四匯流排與第五匯流排之間。

在前述樣品處理裝置中，加密處理電路可包括一公開鑰匙加密電路及一共同鑰匙加密電路。

在前述資料處理裝置中，儲存電路可儲存資料處理裝置之私人鑰匙資料，及第二資料處理裝置之公開鑰匙資料。公開鑰匙加密電路可證明簽名資料之完整，簽名資料證明內容資料、內容鑰匙資料及ＵＣＰ資料之完整，藉著使用對應公開鑰匙資料。當記錄內容資料、內容鑰匙資料及ＵＣＰ資料於一記錄媒體上時，或當將它們送至第二資料處理裝置時，公開鑰匙加密電路可產生簽名資料，其藉著使用私人鑰匙資料證明內容資料、內容鑰匙資料及ＵＣＰ資料之完整。共同鑰匙加密電路可解密內容鑰匙資料，且當將內容資料、內容鑰匙資料及ＵＣＰ資料送至線上的第二資料處理裝置時，共同鑰匙加密電路可加密及解密內容資料、內容鑰匙資料及ＵＣＰ資料，藉著使用以第二資料處理裝置執行相互證明所得到的連續鑰匙資料。

前述資料處理裝置可進一步在抗干預電路模阻內包括一雜亂值產生電路，用於產生內容資料、內容鑰匙資料及ＵＣＰ資料之雜亂值。公開鑰匙加密電路可證明簽名資料之完整，且可藉著使用雜亂值而產生簽名資料。

前述資料處理裝置可進一步在抗干預電路模阻內包括

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（７）

一隨機數產生電路。隨機數產生電路可被連接至第二匯流排，用於產生一隨機數，當將內容資料、內容鑰匙資料及ＵＣＰ資料送至線上的第二資料處理裝置時，以第二資料處理裝置執行相互證明。

在前述資料處理裝置中，外部匯流排介面電路可被連接至外部儲存電路，用於儲存至少內容資料、內容鑰匙資料及ＵＣＰ資料的其中之一。

資料處理裝置可進一步包括一儲存電路控制電路，依據來自算術處理電路之命令，經由外部匯流排介面電路，用於控制至儲存電路之存取及至外部儲存電路之存取。

在前述資料處理裝置中，外部匯流排介面電路可被連接至主算術處理裝置，用於集中地控制其上負載資料處理裝置之系統。

前述資料處理裝置可進一步包括一儲存管理電路，用於管理儲存電路之位址空間，及外部儲存電路之位址空間。

在前述資料處理裝置中，算術處理電路可根據由ＵＣＰ資料表示的處理政策，決定內容資料的購買模式與使用模式的至少其中之一，且可產生表示決定的模式之結果的登錄資料（log data）。

在前述資料處理裝置中，在決定購買模式之後，算術處理電路可依據決定的購買模式產生使用控制狀態資料，且可根據使用控制狀態資料控制內容資料之使用。

在前述資料處理裝置中，於記錄內容資料於記錄媒體

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（８）

上時，內容資料決定購買模式，共同鑰匙加密電路可藉著使用對應記錄媒體之媒體鑰匙資料，加密內容鑰匙資料及使用控制狀態資料。

在前述資料處理裝置中，內容鑰匙資料可使用具有有效周期之執照鑰匙資料被加密。儲存電路可儲存執照鑰匙資料。資料處理裝置可進一步包括一即時時鐘，用於產生即時。算術處理電路可根據由即時時鐘表示的即時，讀取來自儲存電路之有效執照鑰匙資料。共同鑰匙加密電路可藉著使用讀取的執照鑰匙資料加密內容鑰匙資料。

在資料處理裝置中，儲存電路能以區塊爲單位寫入及消除資料。資料處理裝置在抗干預電路模阻內包括，一寫入鎖住控制電路，在算術處理電路的控制之下，用於以區塊爲單位控制資料從儲存電路之寫入與消除。

依據本發明之另一觀點，提供一資料處理裝置，根據ＵＣＰ資料用於執行以內容鑰匙資料加密的內容資料之權利處理。資料處理裝置在抗干預電路模阻內包括：一第一匯流排；一算術處理電路，連接至第一匯流排，根據ＵＣＰ資料用於執行內容資料之權利處理；一儲存電路，連接至第一匯流排；一第二匯流排；一介面電路，插置於第一匯流排與第二匯流排之間；一加密處理電路，連接至第二匯流排，用於解密內容鑰匙資料；及一外部匯流排介面電路，連接至第二匯流排。經由外部匯流排介面電路，於接收來自外部電路之中斷時，算術處理電路成爲外部電路之奴役，以執行由中斷指定的處理，並報告處理之結果

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 9 ）

至外部電路。

在前述資料處理裝置中，算術處理電路可藉著輸出中斷至外部電路而報告處理之結果。

在前述資料處理裝置中，外部匯流排可包括一共同記憶體，用於算術處理電路及外部電路。算術處理電路可將處理之結果寫入共同記憶體。外部電路可藉著投票得到處理之結果。

在前述資料處理裝置中，外部匯流排介面可包括：一第一狀態暫存器，指出從算術處理電路中之外部電路要求的處理之執行狀態，且包括一旗標，由算術處理電路設定且由外部電路讀取；一第二狀態暫存器，指出外部電路是否已要求算術處理電路執行處理，且包括一旗標，由外部電路設定且由算術處理電路讀取；及共同記憶體，用於儲存處理之結果。

在前述資料處理裝置中，儲存電路可儲存一中斷程式，敘述由中斷指定的處理，且算術處理電路可藉著執行從儲存電路讀取的中斷程式而執行處理。

在資料處理裝置中，儲存電路可儲存許多中斷程式，及當執行中斷程式時欲被讀取的許多副常式。當執行從儲存電路讀取的中斷程式時，算術處理電路可適當地讀取及執行來自儲存電路之副常式。

依據本發明之另一觀點，提供一資料處理系統，包括：一算術處理裝置，用於執行預定程式，且用於藉著作爲主人，輸出依據預定狀態之中斷；及一資料處理裝置，用

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 10）

於藉著作爲算術處理裝置之奴役，響應來自算術處理裝置而執行預定處理，且用於報告處理之結果至算術處理裝置。資料處理裝置在抗干預電路模阻內包括：一決定單元，用於根據由ＵＣＰ資料指出的處理政策，決定內容資料之購買模式及使用模式的至少其中之一；一登錄資料產生器，用於產生指出決定的模式之結果的登錄資料；及一解密單元，用於解密內容鑰匙資料。

在前述資料處理系統中，於接收指出中斷型式之中斷時，算術處理裝置可輸出指出指令之中斷至資料處理裝置，以執行對應中斷型式之中斷常式。資料處理裝置可執行對應從算術處理裝置接收的中斷之中斷型式的中斷常式。

在前述資料處理系統中，資料處理裝置可藉著輸出一中斷至算術處理裝置而報告處理之結果。

在前述資料處理系統中，資料處理裝置可包括一共同記憶體，其可由資料處理裝置及算術處理裝置存取。算術處理裝置可藉著經由投票存取共同記憶體而得到處理之結果。

在前述資料處理系統中，資料處理裝置可包括：一第一狀態暫存器，指出從算術處理裝置要求的處理之執行狀態，且包括一旗標，由算術處理裝置讀取；一第二狀態暫存器，指出算術處理裝置是否已要求資料處理裝置執行中斷之處理，且包括一旗標，由算術處理裝置設定；及共同記憶體，用於儲存處理之結果。

前述資料處理系統可進一步包括一匯流排，用於連接

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 11）

算術處理裝置與資料處理裝置。

在前述資料處理系統中，資料處理裝置可在完成啓始程式與中斷常式的其中之一之執行後，輸入一低電力狀態。

在前述資料處理系統中，根據從算術處理裝置接收的中斷，資料處理裝置可依據決定內容資料的購買模式與使用模式之處理，再生內容資料之處理，及從證明授權下載資料之處理的至少其中之一之處理，執行中斷常式。

在前述資料處理系統中，算術處理裝置可執行預定的使用者程式。

依據本發明之另一觀點，提供一資料處理系統，其中由資料提供裝置提供的內容，從資料分布裝置被接收，且被一管理裝置管理。資料處理系統包括：一第一處理模組，用於從資料分布裝置接收一模組，其中儲存以內容鑰匙資料加密的內容資料，加密的內容鑰匙資料，指出內容資料之處理政策之ＵＣＰ資料，及由資料分布裝置決定的內容資料之價格資料，且用於藉著使用共同鑰匙資料解密接收的模組，並藉著資料分布裝置執行模組之分布服務的會計處理。算術處理裝置執行預定程式，並藉著作爲一主人依據預定狀態輸出一中斷。資料處理裝置藉著作爲算術處理裝置之奴役，響應來自算術處理裝置之中斷，執行預定處理，並報告處理之結果至算術處理裝置。資料處理裝置在抗干預電路模阻內包括：一決定單元，用於根據由儲存於接收的模組中之ＵＣＰ資料指出的處理政策，決定內容

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 12）

資料之購買模式及使用模式的至少其中之一。登錄資料產生器產生指出決定的模式之結果的登錄資料。當決定內容資料之購買模式時，輸出單元將價格資料及登錄資料輸出至管理裝置。解密單元解密內容鑰匙資料。

依據本發明之另一觀點，提供一資料處理系統，包括：一算術處理裝置，用於執行預定程式，用於藉著作爲一主人輸出依據預定狀態之中斷；第一抗干預資料處理裝置，用於藉著作爲算術處理裝置之主人，響應來自算術處理裝置之中斷，執行以內容鑰匙資料加密內容資料之權利處理，且用於報告處理之結果至算術處理裝置。第二抗干預資料處理裝置藉著使用以第一抗干預資料處理裝置執行相互證明所得到的內容鑰匙資料，解密內容資料，且藉著作爲算術處理裝置或第一抗干預資料處理裝置之奴役，響應來自算術處理裝置或第一抗干預資料處理裝置之中斷，壓縮或解壓縮內容資料。

前述資料處理系統可進一步包括一匯流排，用於連接算術處理裝置，第一抗干預資料處理裝置，及第二抗干預資料處理裝置。

依據本發明之另一觀點，提供一資料處理系統，包括：一算術處理裝置，用於執行預定程式，且藉著作爲一主人依據預定狀態輸出一中斷。第一抗干預資料處理裝置藉著作爲算術處理裝置之奴役，響應來自算術處理裝置之中斷，執行以內容鑰匙資料加密的內容資料之權利處理，並報告處理之結果至算術處理裝置。第二抗干預資料處理裝

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 13）

置以算術處理裝置執行相互證明，並響應從算術處理裝置輸出之中斷，從記錄媒體讀取及寫入內容資料。

在前述資料處理系統中，第二抗干預資料處理裝置可藉著使用對應記錄媒體之鑰匙資料，解密及加密內容資料。

在前述資料處理系統中，當記錄媒體設有具有相互證明功能之處理電路時，第二抗干預資料處理裝置能以處理電路執行相互證明。

依據本發明之另一觀點，提供一資料處理系統，包括：一算術處理裝置，用於執行預定程式，且藉著作爲一主人依據預定狀態輸出一中斷。第一抗干預資料處理裝置以算術處理裝置執行相互證明，且響應來自算術處理裝置之中斷從記錄媒體讀取並寫入內容資料。第二抗干預資料處理裝置藉著使用內容鑰匙資料解密內容資料，且藉著作爲算術處理裝置之奴役，響應來自算術處理裝置之中斷，壓縮或解壓縮內容資料。

前述資料處理系統進一步包括一儲存電路，用於暫時地儲存藉著第一抗干預資料處理裝置從記錄媒體讀取之內容資料，並輸出儲存的內容資料至第二抗干預資料處理裝置。

在前述資料處理系統中，儲存電路可利用抗震動儲存電路之部份儲存區域。

前述資料處理系統可進一步包括第三抗干預資料處理裝置，藉著作爲算術處理裝置之奴役，響應來自算術處理

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 14）

裝置之中斷，用於執行以內容鑰匙資料加密的內容資料之權利處理，且用於報告處理之結果至算術處理裝置。

依據本發明之另一觀點，提供一資料處理方法，使用算術處理裝置及資料處理裝置。資料處理方法包括以下步驟：在算術處理裝置中，執行預定程式，並藉著作爲一主人依據預定狀態輸出一中斷；及在資料處理裝置中，根據ＵＣＰ資料之處理政策，決定內容資料的購買模式與使用模式的至少其中之一，產生指出決定的模式之結果的登錄資料，並藉著作爲算術處理裝置之奴役，響應來自算術處理裝置之中斷，在抗干預電路模阻內，解密內容鑰匙資料。

依據本發明之另一觀點，提供一資料處理方法，使用算術處理裝置，第一資料處理裝置，及第二資料處理裝置。資料處理方法包括以下步驟：在算術處理裝置中，執行預定程式，並藉著作爲一主人依據預定狀態輸出一中斷；在第一資料處理裝置中，藉著作爲算術處理裝置之奴役，響應來自算術處理裝置之中斷，在抗干預電路模阻內，執行以內容鑰匙資料加密的內容資料之權利處理，並報告處理之結果至算術處理裝置；及在第二資料處理裝置中，藉著使用以第一資料處理裝置執行相互證明所得到的內容鑰匙資料，解密內容資料，並藉著作爲算術處理裝置或第一資料處理裝置之奴役，響應來自算術處理裝置或第一資料處理裝置之中斷，在抗干預模組內，壓縮或解壓縮內容資料。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 15）

依據本發明之另一觀點，提供一資料處理方法，使用算術處理裝置，第一資料處理裝置，及第二資料處理裝置。資料處理方法包括以下步驟：在算術處理裝置中，執行預定程式，並藉著作爲一主人依據預定狀態輸出一中斷；在第一資料處理裝置中，藉著作爲算術處理裝置之奴役，響應來自算術處理裝置之中斷，在抗干預電路模阻內，執行以內容鑰匙資料加密的內容資料之權利處理，並報告處理之結果至算術處理裝置；及在第二資料處理裝置中，以算術處理裝置執行相互證明，並響應來自算術處理裝置之中斷，在抗干預模組內，從記錄媒體讀取及寫入內容資料。

依據本發明之另一觀點，提供一資料處理方法，使用算術處理裝置，第一資料處理裝置，及第二資料處理裝置。資料處理方法包括以下步驟：在算術處理裝置中，執行預定程式，並藉著作爲一主人依據預定狀態輸出一中斷；在第一資料處理裝置中，以算術處理裝置執行相互證明，並響應來自算術處理裝置之中斷，在抗干預模組內，讀取及寫入內容資料；及在第二資料處理裝置中，藉著使用內容鑰匙資料，解密內容資料，並藉著作爲算術處理裝置之奴役，響應來自算術處理裝置之中斷，在抗干預模組內，壓縮或解壓縮內容資料。

圖形之簡要敘述：

圖 1 是一方塊圖，指出依據本發明之第一實施例之

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 16）

ＥＭＤ系統的整個造形；

圖２指出使用於本發明中之安全容器的觀念；

圖３Ａ、３Ｂ與３Ｃ指出從內容提供者送至圖１中之安全應用模組（ＳＡＭ）之安全容器的格式；

圖４指出包含於圖３Ａ中之內容檔的資料之細節；

圖５指出包含於圖３Ｂ中所示之鑰匙檔中之資料的細節；

圖６指出圖１所示的電子音樂分布（ＥＭＤ）中心與內容提供者之間的鑰匙檔之登記與轉移；

圖７指出包含於內容檔中的標頭資料；

圖８指出一內容ＩＤ；

圖９指出安全容器之目錄構造；

圖１０指出安全容器之超鏈構造；

圖１１指出使用於第一實施例中之記錄媒體（ＲＯＭ）的一個例子；

圖１２指出使用於第一實施例中之記錄媒體（ＲＯＭ）的另一個例子；

圖１３指出使用於第一實施例中之記錄媒體（ＲＯＭ）的另一個例子；

圖１４指出使用於第一實施例中之記錄媒體（ＲＡＭ）的另一個例子；

圖１５指出使用於第一實施例中之記錄媒體（ＲＡＭ）的另一個例子；

圖１６指出使用於第一實施例中之記錄媒體（ＲＡＭ

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 17）

）的另一個例子；

圖１７、１８與１９是流程圖，指出藉著內容提供者用於產生安全容器之處理；

圖２０指出圖１所示之ＥＭＤ服務中心之功能；

圖２１指出圖１所示的使用登錄資料；

圖２２是一方塊圖，指出在圖１所示的使用者家庭網路內的網路裝置之造形的一個例子；

圖２３指出圖２２所示的ＳＡＭ與主ＣＰＵ之間的關係；

圖２４指出實施ＳＡＭ之軟體造形；

圖２５指出欲被輸出至主ＣＰＵ之外部中斷；

圖２６指出欲從主ＣＰＵ輸出之內部中斷；

圖２７指出從主ＣＰＵ輸出之功能呼叫；

圖２８指出ＳＡＭ之ＣＰＵ的處理狀態；

圖２９指出ＳＡＭ與主ＣＰＵ之記憶體空間；

圖３０是圖１所示的使用者家庭網路內之ＳＡＭ的功能區塊，且亦指出當解碼從內容提供者接收的安全容器時之資料流；

圖３１指出欲被儲存於圖２２所示的外部記憶體中之資料；

圖３２指出欲被儲存於工作記憶體中的資料；

圖３３是一方塊圖，指出圖１所示的使用者家庭網路內之網路裝置的造形的另一個例子；

圖３４指出欲被儲存於圖３０所示的儲存單元中的資

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 18）

料；

圖３５是一流程圖，指出由用於從ＥＭＤ服務中心接收執照鑰匙資料之ＳＡＭ執行的處理；

圖３６是一流程圖，指出由用於接收安全容器之ＳＡＭ執行的處理；

圖３７是圖１所示的使用者家庭網路內之ＳＡＭ的功能方塊圖，且亦指出當使用及購買內容資料時之資料流；

圖３８是一流程圖，指出用於決定內容資料之購買模式的ＳＡＭ之處理；

圖３９Ａ至３９Ｄ指出購買模式決定的安全容器；

圖４０是一流程圖，指出由用於播放內容資料之ＳＡＭ執行的處理。

圖４１是一方塊圖，指出轉移決定購買模式的內容檔之操作，被下載進入圖２２所示的網路裝置之下載記憶體至音頻－視覺（Ａ／Ｖ）機器之ＳＡＭ，並重新購買Ａ／Ｖ機器中之內容檔；

圖４２指出圖４１所示的接收器ＳＡＭ內之資料流；

圖４３是一流程圖，指出圖４２所示的處理；

圖４４Ａ至４４Ｄ指出在圖４１中欲被轉移的安全容器之格式；

圖４５指出當圖４１所示的接收器ＳＡＭ中之接收的內容檔被寫入一記錄媒體（ＲＯＭ或ＲＡＭ）時之資料流；

圖４６與４７是流程圖，指出圖４１所示的接收器

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 19）

ＳＡＭ之處理；

圖４８指出圖１所示的使用者家庭網路內之ＳＡＭ中的不同購買模式；

圖４９指出當沒有決定購買模式，圖１１所示的記錄媒體（ＲＯＭ）被離線分布至使用者家庭網路，且由Ａ／Ｖ機器決定內容檔之購買模式，在Ａ／Ｖ機器內的資料流；

圖５０指出圖４９所示之Ａ／Ｖ機器之ＳＡＭ內的資料流；

圖５１是一流程圖，指出由圖４９所示的Ａ／Ｖ機器之ＳＡＭ執行的處理；

圖５２指出處理，用於從使用者家庭網路內的Ａ／Ｖ機器之記錄媒體（ＲＯＭ），讀取沒有決定購買模式之安全容器，且用於轉移安全容器至另一Ａ／Ｖ機器並將它寫入一記錄媒體（ＲＡＭ）；

圖５３指出圖５２所示的接收器ＳＡＭ內之資料流；

圖５４Ａ至５４Ｄ指出從送出器ＳＡＭ轉移至圖５２所示的接收器ＳＡＭ之安全容器的格式；

圖５５與５６是一流程圖，指出由圖５２所示的接收器ＳＡＭ與送出器ＳＡＭ執行之處理；

圖５７指出圖５２所示的接收器ＳＡＭ內之資料流；

圖５８指出經由使用者家庭網路內的匯流排之裝置的連接模型之例子；

圖５９指出由ＳＡＭ產生的ＳＡＭ登記列表之資料格

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 20）

式；

圖６０指出由ＥＭＤ服務中心產生的公共鑰匙證書撤銷列表之格式；

圖６１指出由ＥＭＤ服務中心產生的ＳＡＭ登記列表之資料格式；

圖６２指出ＳＡＭ之安全功能；

圖６３指出圖１所示的使用者家庭網路之網路裝置中的不同ＳＡＭ之負載模型的一個例子；

圖６４指出圖６３所示的周邊電路與下載記憶體之詳細電路造形；

圖６５指出圖６３所示的ＳＡＭ與主ＣＰＵ之間的關係；

圖６６指出圖６３所示的主ＣＰＵ、ＳＡＭ、Ａ／Ｖ壓縮／解壓縮ＳＡＭ與記錄媒體之間的關係；

圖６７指出圖６３所示的主ＣＰＵ、媒體驅動ＳＡＭ與Ａ／Ｖ壓縮／解壓縮ＳＡＭ之間的關係；

圖６８指出權利處理ＳＡＭ之電路模組的一個例子；

圖６９指出作爲圖６８所示的電路模組之ＳＡＭ內的硬體造形之例子；

圖７０指出權利處理ＳＡＭ之位址空間；

圖７１指出主ＣＰＵ之位址空間；

圖７２指出權利處理ＳＡＭ之電路模組的另一個例子；

圖７３指出媒體ＳＡＭ之電路模組；

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 21）

圖７４指出當ＲＯＭ被運出時記錄媒體（ＲＯＭ）之媒體ＳＡＭ中的儲存資料；

圖７５指出在進行登記之後的記錄媒體（ＲＯＭ）之媒體ＳＡＭ中的儲存資料；

圖７６指出當ＲＡＭ被運出時記錄媒體（ＲＡＭ）之媒體ＳＡＭ中的儲存資料；

圖７７指出當進行登記時記錄媒體（ＲＡＭ）之媒體ＳＡＭ中的儲存資料；

圖７８指出Ａ／Ｖ壓縮／解壓縮ＳＡＭ之電路模組的一個例子；

圖７９指出媒體驅動ＳＡＭ之電路模組的一個例子；

圖８０是一流程圖，指出圖１所示的ＥＭＤ系統之整個操作；

圖８１指出第一實施例之ＥＭＤ系統中所使用的安全容器之分布協定的例子；

圖８２是一方塊圖，指出依據本發明之第二實施例之ＥＭＤ系統的整個造形；

圖８３是一流程圖，指出用於產生服務提供者中之安全容器的處理；

圖８４Ａ至８４Ｄ指出從服務提供者送出至圖８２所示的使用者家庭網路之安全容器的格式；

圖８５指出儲存於圖８４Ａ至８４Ｄ所示的安全容器中之內容檔的送出格式；

圖８６指出儲存於圖８４Ａ至８４Ｄ所示的安全容器

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 22）

中之鑰匙檔的送出格式；

圖８７指出圖８２所示的ＥＭＤ服務中心之功能；

圖８８是一方塊圖，指出圖８２所示的網路裝置；

圖８９是一功能方塊圖，指出圖８８所示的ＣＡ模組；

圖９０是一功能方塊圖，指出圖８２所示的ＳＡＭ，且亦指出當安全容器被接收且被解碼時之資料流；

圖９１指出欲儲存於圖９０所示的工作記憶體中之資料；

圖９２是一功能方塊圖，指出圖８２所示的ＳＡＭ，且亦指出當內容之購買及使用模式被決定時之資料流；

圖９３是一流程圖，指出以圖８２所示的ＳＡＭ接收安全容器之處理；

圖９４是一方塊圖，指出轉移內容檔之操作，購買模式被決定，下載進入圖８２所示的網路裝置之下載記憶體至Ａ／Ｖ機器之ＳＡＭ；

圖９５指出圖９４所示的接收器ＳＡＭ內之資料流；

圖９６是一流程圖，指出由圖９５所示的送出器ＳＡＭ執行的處理；

圖９７Ａ至９７Ｅ指出從送出器ＳＡＭ轉移至圖９４所示的接收器ＳＡＭ之安全容器的格式；

圖９８指出圖９４所示的接收器ＳＡＭ內之資料流；

圖９９與１００是一流程圖，指出由圖９４所示的接收器ＳＡＭ執行的處理；

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 23）

圖１０１指出圖８２所示的使用者家庭網路內之ＳＡＭ的連接模型之例子；

圖１０２與１０３是一流程圖，指出圖８２所示的ＥＭＤ系統之整個操作；

圖１０４指出圖８２所示的ＥＭＤ系統之服務模型的一個例子；

圖１０５指出圖８２所示的ＥＭＤ系統中使用的安全容器之分布協定；及

圖１０６是一方塊圖，指出一習知ＥＭＤ系統。

主要元件符號說明：

９０　給付閘道

９１　處理組織

１００　ＥＭＤ系統

１０１　內容提供者

１０２　ＥＭＤ服務中心

１０３　使用者家庭網路

１０４　安全容器

１０４ｐ　安全容器

１０４ｘ　安全容器

１０４ｙ　安全容器

105_1　安全應用模組

105_2　安全應用模組

105_3　安全應用模組

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 24）

105$_4$ 安全應用模組

106 UCP資料

107 處理報告資料

108 使用登錄資料

114 加密單元

118b 鑰匙檔資料庫

119 儲存單元

130$_1$ 記錄媒體（ROM）

130$_2$ 記錄媒體（ROM）

130$_3$ 記錄媒體（ROM）

130$_4$ 記錄媒體（RAM）

130$_5$ 記錄媒體（RAM）

130$_6$ 記錄媒體（RAM）

131 ROM區域

132 安全RAM區域

133 媒體SAM

134 不安全RAM區域

152 處理要求資料

160$_1$ 網路裝置

160$_2$ A／V機器

160$_3$ A／V機器

160$_4$ A／V機器

162 通訊模組

163 A／V壓縮／解壓縮SAM

（請先閱讀背面之注意事項再填寫本頁）
裝
訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 25）

165 操作單元

166 UCS資料

166a UCS資料

166b UCS資料

166c UCS資料

167 下載記憶體

169 播放模組

170 相互證明單元

171 加密／解密（解碼）單元

172 加密／解密（解碼）單元

173 加密／解密（解碼）單元

180 內容提供者管理器

182 下載記憶體管理器

184 A／V壓縮／解壓縮SAM管理器

185 EMD服務中心管理器

186 使用監視器

187 會計處理器

189 簽名處理器

190 SAM管理器

191 匯流排

192 儲存單元

196 使用者數位資訊資料

197 媒體SAM管理器

199 部份揭示參數資料

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 26）

２００　工作記憶體

２０１　外部記憶體

２１１　下載記憶體

２２１　解碼器

２２２　解碼器

２２３　解壓縮單元

２２４　數位水記資訊處理器

２２５　部份揭示處理器

２６０　媒體驅動ＳＡＭ

３０８　使用登錄資料

３１０　服務提供者

５８０　服務提供者管理器

５８７　會計處理器

５８９　簽名處理器

７００　ＥＭＤ系統

７０１ａ　內容提供者

７０１ｂ　內容提供者

７０１ｃ　內容提供者

７０４ａ　內容資料

７０４ｂ　內容資料

７０４ｃ　內容資料

７０５ａ　拷貝資訊

７０５ｂ　拷貝資訊

７０５ｃ　拷貝資訊

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 27）

７０７ａ　內容資料

７０７ｂ　內容資料

７０７ｃ　內容資料

７０９　終端裝置

７１０　服務提供者

７１１　ＣＡ模組

７２０　權利處理模組

７２１　會計資訊

７２２　安全容器

８１０　中央處理單元（ＣＰＵ）

８１１　外部記憶體管理器

８５５　媒體驅動ＡＭ管理器

９００　使用者喜愛檔案資料

９０５　解碼模組

９０６　相互證明單元

９０７　儲存單元

９０８　加密／解密單元

９０９　ＳＰ購買登錄資料產生器

９１０　解碼器

９１１　安全容器選定單元

９１２　ＩＣ卡

１０００　主ＣＰＵ匯流排

１００１　驅動ＣＰＵ匯流排

１００２　資料匯流排

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 28）

１００３　驅動ＣＰＵ

１００４　防震記憶體

１００６　ＲＦ放大器

１００７　媒體ＳＡＭ介面

１０１０　直接記憶體存取

１０１１　直接記憶體存取

１０２０　記憶體Ｉ／Ｏ位址解碼器

１１００　中央處理單元

１１０１　直接記憶體存取

１１０２　記憶體管理單元

１１０３　Ｉ／Ｏ模組

１１０４　罩ＲＯＭ

１１０５　非依電性記憶體

１１０６　工作ＲＡＭ

１１０７　公開鑰匙加密模組

１１０８　共同鑰匙加密模組

１１０９　雜亂功能模組

１１１０　隨機數目產生器

１１１１　即時時鐘模組

１１１２　外部匯流排Ｉ／Ｆ

１１１５　匯流排介面

１１１６　匯流排Ｉ／Ｆ電路

１１１７　匯流排介面

１１２０　內部匯流排

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 29）

1121　內部匯流排

1122　內部匯流排

1123　外部匯流排

1130　I^2C介面

1131　媒體ＳＡＭ介面

1132　記憶棒（ＭＳ）介面

1133　ＩＣ卡介面

1141　ＩＣ卡

1155　靜態隨機存取記憶體

1156a　第一ＳＡＭ狀態暫存器

1156b　第二ＳＡＭ狀態暫存器

1200　中央處理單元

1201　直接記憶體存取

1203　Ｉ／Ｏ模組

1204　罩ＲＯＭ

1205　非依電性記憶體

1206　工作ＲＡＭ

1207　公開鑰匙加密模組

1208　共同鑰匙加密模組

1209　雜亂功能模組

1210　隨機數目產生器

1300　中央處理單元

1301　資料記憶體

1304　罩ＲＯＭ

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 30）

１３０５　非依電性記憶體

１３０６　工作ＲＡＭ

１３０８　共同鑰匙加密模組

１３１０　隨機數目產生器

１３２０　壓縮／解壓縮模組

１３２１　數位水記嵌入／偵測模組

１３２２　部份資訊揭示控制模組

１４００　中央處理單元

１４０１　直接記憶體存取

１４０４　罩ＲＯＭ

１４０５　非依電性記憶體

１４０６　工作ＲＡＭ

１４０８　共同鑰匙加密模組

１４０９　雜亂功能模組

１４１０　隨機數目產生器

１４２０　編碼／解碼模組

１４３０　儲存鑰匙資料產生模組

１４４０　媒體獨特ＩＤ產生模組

較佳實施例之詳細敘述：

以下首先敘述依據本發明之實施例的電子音樂分布（ＥＭＤ）系統。

第一實施例

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（31）

圖１是一方塊圖，指出依據本發明之實施例做成的ＥＭＤ系統１００。

在此實施例中，欲被分布至使用者之”內容資料”是具有意義資訊之數位資料，以下以音樂資料作爲例子來敘述。

ＥＭＤ系統１００包括，如圖１所示，內容提供者１０１、ＥＭＤ服務中心（以下可簡稱爲”ＥＳＣ”）１０２及使用者家庭網路１０３。

內容提供者１０１、ＥＭＤ服務中心１０２及安全應用模組（ＳＡＭ）105_1至105_4分別對應本發明之資料提供裝置、資料管理裝置及資料處理裝置。

首先討論整個ＥＭＤ系統１００。ＥＭＤ系統１００將用於加密欲被提供的內容資料Ｃ之內容鑰匙資料Ｋｃ、ＵＣＰ資料１０６、數位水記資訊控制資料及數位水記資訊被嵌入的位置，送至ＥＭＤ服務中心１０２，其是高度可靠的授權組織，ＵＣＰ資料表示例如內容資料Ｃ之執照同意條件。

ＥＭＤ服務中心１０２登記（證明或授權）從內容提供者１０１接收的內容鑰匙資料Ｋｃ、ＵＣＰ資料１０６及數位水記資訊控制資料。

ＥＭＤ服務中心１０２亦產生一鑰匙檔ＫＦ、ＵＣＰ資料１０６、及ＥＭＤ服務中心１０２之簽名資料，鑰匙檔ＫＦ儲存以對應周期之執照鑰匙資料KD_1至KD_6加密的內容鑰匙資料Ｋｃ，且將鑰匙檔ＫＦ送至內容提供者

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 32）

１０１。

簽名資料是用於證明鑰匙檔ＫＦ之完整與鑰匙檔ＫＦ之產生者之辨識，及ＥＭＤ服務中心１０２中之鑰匙檔ＫＦ之正式註冊。

內容提供者１０１產生一內容檔ＣＦ，藉著使用內容鑰匙資料K_c加密內容資料Ｃ，並經由網路分布安全容器１０４至使用者家庭網路１０３，安全容器１０４對應本發明之模組，其儲存從ＥＭＤ服務中心１０２接收的鑰匙檔ＫＦ、內容檔ＣＦ及內容提供者１０１之簽名資料，網路是例如網際網路、數位廣播或封裝媒體，例如記錄媒體。安全容器１０４中儲存之簽名資料是用於證明對應資料之完整及資料之送出者與產生者之辨識。

使用者家庭網路１０３包括例如網路裝置160_1及音頻－視覺（ＡＶ）機器160_2至160_4。網路裝置106_1具有內建$SAM105_1$。Ａ／Ｖ機器160_2至160_4分別具有內建$SAM105_2$至105_4。$SAM105_1$至105_4經由一匯流排１９１例如ＩＥＥＥ－１３９４串聯介面匯流排，彼此相互連接。

$SAM105_1$至105_4經由例如網路線上解碼從內容提供者１０１接收之安全容器１０４，及／或藉著使用對應周期之執照鑰匙資料KD_1至KD_3，經由記錄媒體離線解碼從內容提供者１０１供給至Ａ／Ｖ機器160_2至160_4之安全容器１０４，然後證明簽名資料。

然後在安全容器１０４之購買／使用模式已由使用者

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 33）

之操作決定之後，被供給至ＳＡＭ１０５$_{1}$至１０５$_{4}$之安全容器１０４可以被播放或記錄在Ａ／Ｖ機器１６０$_{2}$至１６０$_{4}$及網路裝置１６０$_{1}$中之記錄媒體上。

ＳＡＭ１０５$_{1}$至１０５$_{4}$記錄安全容器１０４之購買／使用歷史作爲使用登錄資料１０８，且亦產生表示購買模式之使用控制狀態（ＵＣＳ）資料１６６。

使用登錄資料１０８例如響應來自ＥＭＤ服務中心１０２之要求，從使用者家庭網路１０３被送至ＥＭＤ服務中心１０２。例如每次決定購買模式時，ＵＣＳ資料１６６從使用者家庭網路１０３被送至ＥＭＤ服務中心１０２。

ＥＭＤ服務中心１０２根據使用登錄資料１０８決定（計算）會計內容，並根據計算的會計內容經由給付閘道９０藉著使用例如銀行之處理組織９１來處理賬戶。依據此處理，使用者家庭網路１０３之使用者對處理組織９１之給付，藉著由ＥＭＤ服務中心１０２執行之處理被給至內容提供者１０１。ＥＭＤ服務中心１０２定期地將處理報告資料１０７送至內容提供者１０１。

在此實施例中，ＥＭＤ服務中心１０２具有證明功能、鑰匙－資料管理功能及權利處理（利潤分配）功能。

特別是，ＥＭＤ服務中心１０２作爲位在低於根證明授權９２之層的第二證明授權，其是中立最高授權，且藉著使用ＥＭＤ服務中心１０２之私人鑰匙資料，附著簽名至公開鑰匙資料之公開－鑰匙證明資料而證明公開鑰匙資

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（34）

料。使用公開鑰匙資料以證明ＳＡＭ１０５$_1$至１０５$_4$及內容提供者１０１中之簽名資料的完整。如上所述，ＥＭＤ服務中心１０２登記並授權內容提供者１０１之ＵＣＰ資料１０６，其亦是ＥＭＤ服務中心１０２之部份證明功能。

ＥＭＤ服務中心１０２亦具有管理例如執照鑰匙資料ＫＤ$_1$至ＫＤ$_6$之鑰匙資料的鑰匙－資料管理功能。

ＥＭＤ服務中心１０２亦具有以下權利處理（利潤分配）功能。ＥＭＤ服務中心１０２根據授權ＵＣＰ資料１０６中所述之建議零售價（ＳＲＰ），及從ＳＡＭ１０５$_1$至１０５$_4$輸入之使用登錄資料，處理由使用者做成的內容之使用與購買的賬戶，並分配使用者之給付至內容提供者１０１。

圖２圖形地指出安全容器１０４之觀念。

安全容器１０４如圖２所示，儲存由內容提供者１０１產生的內容檔ＣＦ，及由ＥＭＤ服務中心１０２產生的鑰匙檔ＫＦ。

在內容檔ＣＦ中，儲存包含標頭及內容ＩＤ之標頭資料，以內容鑰匙資料Ｋｃ加密的內容資料Ｃ，及以內容提供者１０１之私人鑰匙資料Ｋ$_{CP,S}$加密的簽名資料。

在鑰匙檔ＫＦ中，儲存包含標頭及內容ＩＤ之標頭資料，內容鑰匙資料Ｋｃ與以執照鑰匙資料ＫＤ$_1$至ＫＤ$_6$加密的ＵＣＰ資料１０６，及以ＥＭＤ服務中心１０２之私人鑰匙資料Ｋ$_{ESC,S}$加密的簽名資料。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（35）

圖２中，ＵＣＰ資料１０６可以不被執照鑰匙資料KD_1至KD_6加密，在此情形中，以內容提供者１０１之私人鑰匙資料$K_{CP,S}$加密的簽名資料被加至ＵＣＰ資料１０６。

以下討論ＥＭＤ系統１００之個別元件之細節。

〔內容提供者１０１〕

在開始與ＥＭＤ服務中心１０２通訊之前，內容提供者１０１離線登記由內容提供者１０１產生之公開鑰匙資料$K_{CP,P}$，及ＥＭＤ服務中心１０２中之內容提供者１０１之銀行賬號（用於處理會計），並得到一獨特辨識（ＩＤ號碼）ＣＰ＿ＩＤ。內容提供者１０１亦從ＥＭＤ服務中心１０２接收ＥＭＤ服務中心１０２之公開鑰匙資料$K_{ESC,P}$及根證明授權９２之公開鑰匙資料$K_{R-CA,P}$。

內容提供者１０１產生安全容器１０４，其儲存圖３Ａ所示之內容檔ＣＦ之簽名資料$SIG_{6,CP}$與內容檔ＣＦ，對應從鑰匙檔資料庫１１８ｂ讀取的內容檔ＣＦ之鑰匙檔ＫＦ，與圖３Ｂ所示之鑰匙檔ＫＦ之簽名資料$SIG_{7,CP}$，從儲存單元１１９讀取的內容提供者１０１之公開－鑰匙證明資料CER_{CP}及圖３Ｃ所示之公開－鑰匙證明資料CER_{CP}之簽名資料$SIG_{1,ESC}$。

內容提供者１０１線上或離線供給安全容器１０４至圖１所示之使用者家庭網路１０３之網路裝置160_1。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 36）

以此方式，依據此實施例，使用頻帶內系統，其中儲存於安全容器１０４中之內容提供者１０１之公開鑰匙資料$K_{CP,P}$之公開－鑰匙證明資料CER_{CP}，被直接送至使用者家庭網路１０３。如此不需要使用者家庭網路１０３與ＥＭＤ服務中心１０２通訊，以取得公開－鑰匙證明CER_{CP}。

另一種方式，在本發明中，可使用頻帶外系統，其中使用者家庭網路１０３可從ＥＭＤ服務中心１０２取得公開－鑰匙證明CER_{CP}，而非將它儲存在安全容器１０４中。

在此實施例中，藉著分別使用私人鑰匙$K_{CP,S}$、$K_{ESC,S}$、K_{SAM1}至K_{SAM4}，雜亂化（ｈａｓｈｉｎｇ）使用於內容提供者１０１、ＥＭＤ服務中心１０２、$SAM1051$至$SAM1054$之簽名之資料，而產生簽名資料。藉著使用雜亂功能而產生雜亂值。依據雜亂功能，使用於簽名之資料被輸入並被壓縮成具有預定位元長度之資料，然後其被輸出作爲雜亂值。很難預測來自雜亂值之輸入值（輸出值），且當輸入資料的一位元改變時，雜亂值之許多位元會改變。亦很難搜尋具有相同雜亂值之輸入資料。

以下爲安全容器１０４中之個別資料之細節。

簽名資料$SIG_{6,CP}$

簽名資料$SIG_{6,CP}$被使用在安全容器１０４之目的

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 37）

地，用於證明內容檔ＣＦ之送出者及產生者之完整。

簽名資料ＳＩＧ$_{7,CP}$

簽名資料ＳＩＧ$_{7,CP}$被使用在安全容器１０４之目的地，用於證明鑰匙檔ＫＦ之送出者之完整。根據鑰匙檔ＫＦ內之簽名資料ＳＩＧ$_{K1,ESC}$，在安全容器１０４之目的地證明鑰匙檔ＫＦ之產生者之完整。簽名資料ＳＩＧ$_{K1,ESC}$亦用於證明ＥＭＤ服務中心１０２中之鑰匙檔ＫＦ之登記。

內容檔ＣＦ

圖４指出圖３Ａ所示之內容檔ＣＦ之細節。

如圖３Ａ與４所示，內容檔ＣＦ儲存以從加密單元１１４輸入的內容鑰匙資料Ｋｃ加密之中間資料Ｍｅｔａ，內容資料Ｃ，Ａ／Ｖ解壓縮軟體Ｓｏｆｔ，及數位水記資訊模組（水記模組）ＷＭ。

圖３Ａ指出內容檔ＣＦ之造形，當一數位信號處理器（ＤＳＰ）被使用作爲用於解壓縮內容資料Ｃ之Ａ／Ｖ壓縮／解壓縮裝置。ＤＳＰ解壓縮安全容器１０４內之內容資料Ｃ，且藉著使用安全容器１０４內之數位水記資訊模組及Ａ／Ｖ解壓縮軟體，嵌入並偵測數位水記資訊。使內容提供者１０１能使用所要的數位水記資訊之壓縮方法及嵌入方法。

如果硬體或預先儲存軟體被使用作爲Ａ／Ｖ壓縮／解

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 38）

壓縮裝置，用於解壓縮內容資料C及用於嵌入並偵測數位水記資訊，A／V解壓縮軟體及數位水記資訊模組可以不儲存於內容檔CF內。

如圖4所示，標頭資料含有一同步信號，一內容ID，用於證明內容ID之由內容提供者101之私人鑰匙資料$K_{CP.S}$得到的簽名資料，目錄資訊，超鏈資訊，關於序號之資訊，內容檔CF之產生者及有效周期，檔案尺寸，加密旗標，加密演算與簽名演算，及用於證明目錄資訊之由內容提供者101之私人鑰匙資料$K_{CP.S}$得到的簽名資料。

如圖4所示，中間資料Meta包括產品之敘述（亦即內容資料C），產品展示之廣告資訊，產品相關資訊，及用於證明以上資訊之內容提供者101之簽名資料。

在本發明中，如圖3A與4所示，當被儲存於內容檔CF中時，中間資料Meta被送出。另一種方式，不是將中間資料Meta儲存於內容檔CF中，中間資料Meta可從內容提供者101被傳送至例如$SAM105_1$，經由與送出內容檔CF之路徑不同之路徑。

以如下之方式得到內容資料C。源數位水記資訊（源水記）W_S，拷貝控制數位水記資訊（拷貝控制水記）W_C，使用者數位水記資訊（使用者水記）W_U，及鏈數位水記資訊（鏈水記）W_L等，被嵌入從例如一內容主人源資料庫讀取的內容資料。然後，依據聲音壓縮方法例如適應轉換

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 39）

聲音寫碼3（ＡＴＲＡＣ３）（品牌名），內容資料被壓縮，且藉著使用內容鑰匙Ｋｃ作爲共同鑰匙，依據共同鑰匙密祕系統例如資料加密標準（ＤＥＳ）或Triple DES被加密。

例如藉著使用隨機數目產生器，產生具有預定數目之位元的隨機數目，而得到內容鑰匙資料Ｋｃ。從與由內容資料提供的音樂片段有關之資料，產生內容鑰匙資料Ｋｃ。內容鑰匙資料Ｋｃ被定期地更新。

出現許多內容提供者１０１時，可使用對於各內容提供者１０１之獨特的內容鑰匙資料Ｋｃ，或者對於全部內容提供者１０１，可使用共同內容資料Ｋｃ。

源數位水記資訊W_S指出關於著作權之資訊，例如內容資料之著作權擁有者之名字、國際標準記錄碼（ＩＳＲＣ）、著作日期、著作機器辨識資料（ＩＤ）、及內容之分布目的地。

拷貝控制數位水記資訊W_C指出包括經由類比介面用於避免拷貝操作之拷貝禁止位元之資訊。

使用者數位水記資訊W_U含有例如用於指定分布源之內容提供者１０１之辨識ＣＰ＿ＩＤ，與安全容器１０４之分布目的地，及使用者家庭網路１０３之$SAM105_1$至105_4之辨識SAM_ID_1至SAM_ID_4。

鏈數位水記資訊W_L包括例如內容資料Ｃ之內容ＩＤ。藉著將鏈數位水記資訊W_L嵌入內容資料Ｃ，甚至經由類比廣播分布之內容資料Ｃ，例如電視廣播或調幅（ＡＭ）／

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 40）

調頻（ＦＭ）無線電廣播，響應來自使用者之要求，ＥＭＤ服務中心１０２能將處理內容資料Ｃ之內容提供者１０１介紹給使用者。亦即，藉著使用數位水記資訊解碼器，內容資料Ｃ之接收側偵測被嵌入內容資料Ｃ之鏈數位水記資訊W_L，並將偵測的內容ＩＤ送至ＥＭＤ服務中心１０２。使ＥＭＤ服務中心１０２能將處理內容資料Ｃ之內容提供者１０１介紹給使用者。

特別是，現在假設使用者在車內聽到一段音樂且感到有興趣，並按下一預定按鈕。然後，收音機內之數位水記資訊解碼器偵測到包含於嵌入於內容資料Ｃ中之鏈數位水記資訊W_L之內容ＩＤ，及登記內容資料Ｃ之ＥＭＤ服務中心１０２之通訊位址。然後數位水記資訊解碼器將偵測的資料記錄在負載於可攜式媒體中之媒體ＳＡＭ，例如Memory Stick（品牌名）之半導體記憶體，或例如迷你光碟（ＭＤ）（品牌名）之光碟。然後可攜式媒體被設在負載有連接至網路之ＳＡＭ之網路裝置中。在執行ＳＡＭ與ＥＭＤ服務中心１０２之間的相互證明之後，儲存於ＳＡＭ與記錄內容ＩＤ中之ＩＤ資訊，從網路裝置被送至ＥＭＤ服務中心１０２。然後，網路裝置從ＥＭＤ服務中心１０２接收處理內容資料Ｃ之內容提供者例如內容提供者１０１的列表。

另一種方式，響應來自使用者之內容ＩＤ，ＥＭＤ服務中心１０２可將使用者之資訊送至內容提供者１０１，其處理對應內容ＩＤ之內容資料Ｃ。於接收上述資訊時，

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（41）

如果發現使用者已與內容提供者１０１有做成合約，則內容提供者１０１可將內容資料Ｃ送至使用者之網路裝置。如果不是，內容提供者１０１可將內容提供者１０１之升級資訊送至使用者之網路裝置。

在本發明之第二實施例（敘述於下）中，根據鏈數位水記資訊W_L，ＥＭＤ服務中心１０２能將處理內容資料Ｃ之服務提供者３１０介紹給使用者。

最好，在第一實施例中，數位水記資訊之嵌入位置及內容，可被定義爲數位水記資訊模組ＷＭ，其可在ＥＭＤ服務中心１０２中被登記及管理。數位水記資訊模組ＷＭ用於證明數位水記資訊，藉著例如網路裝置160_1及使用者家庭網路１０３內之Ａ／Ｖ機器160_2至160_4。

特別是，使用者家庭網路１０３根據由ＥＭＤ服務中心１０２管理之使用者數位水記資訊模組ＷＭ，決定是否由使用者家庭網路１０３偵測之數位水記資訊之嵌入位置及內容，符合由ＥＭＤ服務中心１０２所管理者。如果偵測的資訊符合ＥＭＤ服務中心１０２，則決定數位水記資訊是合法的。於是可以偵測非法的嵌入數位水記資訊。

可以是ＡＴＲＡＣ３解壓縮軟體之Ａ／Ｖ解壓縮軟體Ｓｏｆｔ，用於解壓縮使用者家庭網路１０３之Ａ／Ｖ機器160_2至160_4及網路裝置160_1中之內容檔ＣＦ。

如此使$SAM105_1$至105_4能解壓縮內容資料Ｃ，只要藉著使用儲存於安全容器１０４中之Ａ／Ｖ解壓縮

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 42）

軟體。因此，即使對於個別項目的內容資料C或對於個別內容提供者，設定不同的壓縮／解壓縮方法，解壓縮內容資料C之沈重的負擔不會加在使用者上。

如圖4所示，內容檔CF可含有藉著使用私人鑰匙$K_{CP,S}$用於證明檔案讀者之簽名資料及檔案讀者。如此使SAM105$_1$至105$_4$能有效率地處理儲存不同格式的內容檔CF之許多不同型式的安全容器104。

檔案讀者用於讀取內容檔CF及對應的鑰匙檔KF，並指出這些檔之讀取程序。

在此實施例中，假設檔案讀者已從EMD服務中心102被送至SAM105$_1$至105$_4$，於是安全容器104之內容檔CF不儲存檔案讀者。

在此實施例中，解密的內容資料C被儲存於安全容器104中，不管以下因數，例如壓縮旗標，亦即是否內容資料C被壓縮，內容資料C之壓縮方法，加密方法（包括共同鑰匙密祕系統及公開鑰匙密祕系統），內容資料C之信號源（例如取樣頻率），及簽名－資料產生方法（演算）。亦即，上述因數可單獨於內容提供者101被決定。

鑰匙檔KF

圖5指出圖3B所示之鑰匙檔KF之細節。

在此實施例中，如圖6所示，例如在藉著從內容提供者101將登記模組Mod_2送至EMD服務中心102而執行登記處理之後，六個月之鑰匙檔KF例如從EMD服

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 43）

務中心１０２被送至內容提供者１０１，且被儲存於鑰匙檔資料庫中。送出及接收登記模組Mod_2及鑰匙檔ＫＦ時，在內容提供者１０１與ＥＭＤ服務中心１０２之間執行相互證明，且藉著使用連續鑰匙資料K_{SES}加密及解密鑰匙檔ＫＦ與登記模組Mod_2。

鑰匙檔ＫＦ被提供給各內容資料Ｃ，且被鏈接至對應的內容檔ＣＦ，依據內容檔ＣＦ之標頭內的目錄構造資料ＤＳＤ，詳細討論於下。

如圖３Ｂ與５所示，鑰匙檔ＫＦ儲存標頭、內容鑰匙資料K_C、ＵＣＰ資料（執照同意條件）１０６、ＳＡＭ程式下載容器SDC_1至SDC_3及簽名資料$SIG_{K1,ESC}$。

如圖３Ｂ所示，藉著使用ＥＭＤ服務中心１０２之私人鑰匙$K_{ESC,S}$所得到的簽名資料，可以是儲存於鑰匙檔ＫＦ中之全部資料之簽名資料$SIG_{K1,ESC}$。另一種方式，如圖５所示，簽名資料可被分開地提供給從標頭至鑰匙檔之資訊，內容鑰匙K_C與ＵＣＰ資料１０６，及ＳＡＭ程式下載容器ＳＤＣ。

內容鑰匙資料K_C與ＵＣＰ資料１０６，及ＳＡＭ程式下載容器SDC_1至SDC_3，使用對應周期之執照鑰匙資料KD_1至KD_6被加密。

ＵＣＰ資料１０６可以不儲存於鑰匙檔ＫＦ中，在此情形中，它被提供簽名資料而不需被執照鑰匙資料加密。

如圖５所示，標頭資料含有同步信號，內容ＩＤ，藉

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 44）

著使用ＥＭＤ服務中心１０２之私人鑰匙$K_{ESC,S}$用於證明內容ＩＤ之簽名資料，目錄構造資料，超鏈資料，關於鑰匙檔ＫＦ之資訊，及藉著使用ＥＭＤ服務中心１０２之私人鑰匙$K_{ESC,S}$用於證明目錄構造資料之簽名資料。

不同型式的資訊可包含於標頭資料中，且可依狀態而改變。例如，圖７所示之資訊可被包含。

內容ＩＤ可儲存圖８所示之資訊。內容ＩＤ被產生於ＥＭＤ服務中心１０２或內容提供者１０１中，且如圖８所示，藉著使用ＥＭＤ服務中心１０２之私人鑰匙$K_{ESC,S}$所得到的簽名資料，或以內容提供者１０１之私人鑰匙資料$K_{CP,S}$得到的簽名資料，被附著至內容ＩＤ。內容ＩＤ可被產生於內容提供者１０１或ＥＭＤ服務中心１０２中。

目錄構造資料代表內容檔ＣＦ之間的關係，及安全容器１０４內的鑰匙檔ＫＦ與內容檔ＣＦ之間的關係。

例如，如果內容檔CF_1至CF_3及對應的鑰匙檔KF_1至KF_3被儲存於安全容器１０４中，如圖９所示，藉著目錄構造資料，建立CF_1至CF_3之間的鏈接及KF_1至KF_3之間的鏈接。

超鏈資料代表鑰匙檔ＫＦ之階級組織構造及內容檔ＣＦ與鑰匙檔ＫＦ之間的關係，藉著考慮安全容器１０４之內與外的全部檔案。

特別是，儲存欲被鏈接之位址資訊及其證明值（雜亂值），如圖１０所示，於各鑰匙檔ＫＦ及各內容檔ＣＦ之

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 45）

安全容器１０４中。然後由雜亂功能H（ｘ）得到的一內容檔ＣＦ或一鑰匙檔ＫＦ之雜亂值與欲被鏈接之另一內容檔ＣＦ或另一鑰匙檔ＫＦ比較，藉以證明檔案之間的鏈接。

ＵＣＰ資料１０６是一述語，其定義內容資料Ｃ之操作規則，例如建議零售價（ＳＲＰ），及內容提供者１０１之操作者所要的拷貝規則。

特別是，如圖５所示，ＵＣＰ資料１０６含有內容ＩＤ，內容提供者１０１ＣＰ＿ＩＤ之辨識，ＵＣＰ資料１０６之有效日期，ＥＭＤ服務中心１０２之通訊位址，使用－空間搜尋資訊，ＳＲＰ，使用政策，ＵＣＳ資訊，用於展示產品之ＵＣＳ資訊，及上述資訊之簽名資料。

ＵＣＳ資訊指出從不同購買模式選定之接受的購買模式，例如再分布，使用計費，賣斷，限時賣斷，播放Ｎ次計費，以時間計費，以ＳＣＭＳ裝置之使用計費，以區塊計費等等。

在第二實施例中，討論於下，在將安全容器１０４經由服務提供者３１０送至使用者家庭網路３０３時，ＵＣＰ資料１０６含有服務提供者３１０ＳＰ＿ＩＤ之辨識，其被內容提供者３０１提供安全容器１０４。

如圖５所示，ＳＡＭ程式下載容器SDC_1至SDC_3儲存下載驅動器，指出用於下載$SAM105_1$至105_4內之程式的程序，標籤讀者，例如ＵＣＰ－Ｌ（標籤）·Ｒ（讀者），表示ＵＣＰ資料１０６之句子構造（文法）

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（46）

，用於寫入及消去儲存於儲存單元１９２中各區塊資料之鎖住或解開之鎖鑰匙資料，儲存單元（快閃僅讀記憶體（ＲＯＭ），例如罩ＲＯＭ１１０４或非依電性記憶體１１０５）內建於各ＳＡＭ１０５$_1$至１０５$_4$中，及上述資訊之簽名資料。罩ＲＯＭ１１０４或非依電性記憶體１１０５根據鎖鑰匙資料，控制單位區塊內的儲存資料之寫入及消去。

以下敘述安全容器１０４從內容提供者１０１被供給至使用者家庭網路１０３之模式。

如上所討論，內容提供者１０１線上或離線供給安全容器１０４至使用者家庭網路１０３。

當內容提供者１０１線上供給安全容器１０４至使用者家庭網路１０３之網路裝置１６０$_1$時，採取以下處理。內容提供者１０１與網路裝置１６０$_1$相互證明，以分享連續鑰匙（共同鑰匙）K_{SES}，並藉著使用連續鑰匙K_{SES}加密１０４，且將它送至ＥＭＤ服務中心１０２。每次執行相互證明時，連續鑰匙K_{SES}被更新地產生。

作爲用於送出安全容器１０４之通訊協定，多媒體及超媒體資訊寫碼專家群（ＭＨＥＧ）協定使用於數位廣播，或對於網際網路可使用延伸差額語言（ＸＭＬ），同步多媒體集積語言（ＳＭＩＬ），或超本文差額語言（ＨＴＭＬ）。安全容器１０４被嵌入於對應的協定內，依據通道技術，與寫碼方法無關。

因此，安全容器１０４之格式不需符合通訊協定，藉

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（47）

以增加選定安全容器１０４之格式的彈性。

用於從內容提供者１０１將安全容器１０４送至使用者家庭網路１０３之通訊協定，並不限於上述協定。

在此實施例中，作爲內建於內容提供者１０１，ＥＭＤ服務中心１０２，及用於彼此相通之網路裝置160_1之模組，使用無干預或高防干預通訊閘道，其可免於被監視。

相反地，當內容提供者１０１離線供給安全容器１０４至使用者家庭網路１０３，安全容器１０４被記錄在一記錄媒體（ＲＯＭ或ＲＡＭ）上，討論於下，且然後ＲＯＭ或ＲＡＭ之內容經由一通訊路徑被供給至使用者家庭網路１０３。

圖１１指出使用於此實施例中之記錄媒體（ＲＯＭ）130_1。

記錄媒體（ＲＯＭ）130_1具有ＲＯＭ區域１３１，安全ＲＡＭ區域１３２，及媒體ＳＡＭ１３３。圖３Ａ所示之內容檔ＣＦ被儲存於ＲＯＭ區域１３１中。

安全ＲＡＭ區域１３２是一區域，其取得存取之預定許可（證明），並儲存由使用圖３Ｂ所示的鑰匙檔ＫＦ所產生之簽名資料，圖３Ｃ所示之公開－鑰匙證明資料CER_{CP}，及具有依據機器的型式之獨特值之儲存鑰匙資料K_{STR}，藉著利用訊息證明碼（ＭＡＣ）功能。安全ＲＡＭ區域１３２亦儲存藉著使用具有記錄媒體特有的值之媒體鑰匙資料K_{MED}加密鑰匙檔ＫＦ及公開－鑰匙證明

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（48）

資料$CERT_{CP}$所得到之資料。

安全ＲＡＭ區域１３２亦儲存用於指定內容提供者１０１及$SAM105_1$至$SAM105_4$之公開鑰匙證明撤銷資料，其由於非法已成爲無效。

在此實施例使用的媒體ＳＡＭ與媒體裝置ＳＡＭ２６０之間通訊時，討論於下，一ＳＡＭ比較其撤銷列表與其它的ＳＡＭ，並決定何時產生列表。由其它的撤銷列表來更新先前產生的撤銷列表。

安全ＲＡＭ區域１３２儲存ＵＣＳ資料１６６，其當在使用者家庭網路１０３之$SAM105_1$至$SAM105_4$中決定內容資料Ｃ之購買／使用模式時被產生。藉著儲存ＵＣＳ資料１６６於安全ＲＡＭ區域１３２中，可以提供決定購買／使用模式之記錄媒體（ＲＯＭ）130_1。

媒體ＳＡＭ１３３儲存例如媒體鑰匙資料K_{MED}及是記錄媒體（ＲＯＭ）130_1之辨識的媒體ＩＤ。媒體ＳＡＭ１３３具有如相互證明功能。

此實施例中使用記錄媒體（ＲＯＭ）亦可以是圖１２所示之記錄媒體（ＲＯＭ）130_2或圖１３所示之記錄媒體（ＲＯＭ）130_3。

圖１２所示之記錄媒體（ＲＯＭ）130_2具有ＲＯＭ區域１３１及具有證明功能之媒體ＳＡＭ１３３，但沒有安全ＲＡＭ區域１３２，不像圖１１所示之記錄媒體（ＲＯＭ）130_1。如果使用記錄媒體（ＲＯＭ）130_2，內容檔ＣＦ被儲存於ＲＯＭ區域１３１中，且鑰匙檔

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 49）

ＫＦ被儲存於媒體ＳＡＭ１３３中。

圖１３所示之記錄媒體（ＲＯＭ）１３０$_3$具有ＲＯＭ區域１３１及安全ＲＡＭ區域１３２，但沒有媒體ＳＡＭ１３３，不像圖１１所示之記錄媒體（ＲＯＭ）１３０$_1$。如果使用記錄媒體（ＲＯＭ）１３０$_3$，內容檔ＣＦ被儲存於ＲＯＭ區域１３１中，且鑰匙檔ＫＦ被儲存於安全ＲＡＭ區域１３２中。以對應的ＳＡＭ執行證明。

不是ＲＯＭ記錄媒體，此實施例中可使用ＲＡＭ記錄媒體。

作爲可使用於此實施例中之ＲＡＭ記錄媒體，如圖１４所示，可使用具有媒體ＳＡＭ１３３、安全ＲＡＭ區域１３２及不安全ＲＡＭ區域１３４之記錄媒體（ＲＡＭ）１３０$_4$。

在此記錄媒體（ＲＡＭ）１３０$_4$中，媒體ＳＡＭ１３３具有證明功能，且安全ＲＡＭ區域１３２儲存鑰匙檔ＫＦ。不安全ＲＡＭ區域１３４儲存內容檔ＣＦ。

另一種方式，可使用圖１５所示之記錄媒體（ＲＡＭ）１３０$_5$及圖１６所示之記錄媒體（ＲＡＭ）１３０$_6$。

圖１５所示之記錄媒體（ＲＡＭ）１３０$_5$包括不安全ＲＡＭ區域１３４及具有證明功能之媒體ＳＡＭ１３３，但沒有安全ＲＡＭ區域１３２，不像圖１４所示之記錄媒體（ＲＡＭ）１３０$_4$。使用記錄媒體（ＲＡＭ）１３０$_5$時，內容檔ＣＦ被儲存於不安全ＲＡＭ區域１３４中，且

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 50）

鑰匙檔ＫＦ被儲存於媒體ＳＡＭ１３３中。

記錄媒體（ＲＡＭ）１３０$_6$包括安全ＲＡＭ區域１３２及不安全ＲＡＭ區域１３４，但沒有媒體ＳＡＭ１３３，不像圖１４所示之記錄媒體（ＲＡＭ）１３０$_4$。使用記錄媒體（ＲＡＭ）１３０$_6$時，內容檔ＣＦ被儲存於不安全ＲＡＭ區域１３４中，且鑰匙檔ＫＦ被儲存於安全ＲＡＭ區域１３２中。

如上所述，不管內容資料Ｃ是否經由網被線上分布或離線使用，從內容提供者１０１之記錄媒體１３０$_1$至使用者家庭網路１０３，使用儲存ＵＣＰ資料１０６之安全容器１０４的格式以分布內容資料Ｃ。如此使使用者家庭網路１０３之ＳＡＭ１０５$_1$至１０５$_4$能根據ＵＣＰ資料１０６執行權利處理。

如上所討論，在此實施例中，使用頻帶內系統，其中連同用於解密內容資料Ｃ之內容鑰匙資料Ｋｃ，以內容鑰匙資料Ｋｃ加密的內容資料Ｃ，被儲存於安全容器１０４中。依據此頻帶內系統，不需要分開地分布內容鑰匙資料Ｋｃ，當使用者家庭網路１０３播放內容資料Ｃ，藉以減小網路通訊之負擔。以執照鑰匙資料ＫＤ$_1$至ＫＤ$_6$加密內容鑰匙資料Ｋｃ。然而，執照鑰匙資料ＫＤ$_1$至ＫＤ$_6$被管理於ＥＭＤ服務中心１０２中，且已被分布至使用者家庭網路１０３之ＳＡＭ１０５$_1$至１０５$_4$，當ＳＡＭ１０５$_1$至１０５$_4$首先存取ＥＭＤ服務中心１０２。如此使使用者家庭網路１０３能離線使用內容資料Ｃ，

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 51）

而不需線上存取ＥＭＤ服務中心１０２。

在本發明中，可使用頻帶外系統，其中內容資料Ｃ及內容鑰匙資料Ｋｃ被分開地供給至使用者家庭網路１０３，將討論於下。

由內容提供者１０１產生安全容器１０４之處理如下。

圖１７至１９是一流程圖，指出上述處理。

在步驟Ｓ１７－１（圖１７）中，藉著使用內容提供者１０１之ＩＤ證書或用於處理會計之銀行賬戶，內容提供者１０１離線登記於ＥＭＤ服務中心１０２中，並取得全球獨特辨識ＣＰ＿ＩＤ。內容提供者１０１從ＥＭＤ服務中心１０２已得到內容提供者１０１之公開鑰匙證明ＣＥＲ$_{CP}$。

在步驟Ｓ１７－２中，然後內容提供者１０１將內容主人源數位化，例如欲被授權的內容資料及預先儲存的合法內容資料，並指定內容ＩＤ至此資料。然後內容主人源被儲存於內容主人源資料庫中並被集中地管理。

然後，在步驟Ｓ１７－３中，內容提供者１０１對於各集中管理的內容主人源產生中間資料Ｍｅｔａ，且將它儲存在中間資料庫中。

隨後，在步驟Ｓ１７－４中，內容提供者１０１從內容主人源資料庫讀取內容資料，亦即內容主人源，且將數位水記資訊嵌入內容資料中。

在步驟Ｓ１７－５中，內容提供者１０１儲存內容及

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 52）

在步驟Ｓ１７－４中數位水記資訊嵌入預定資料庫中之嵌入位置。

然後，在步驟Ｓ１７－６中，具有嵌入的數位水記資訊之內容資料被壓縮。

在步驟Ｓ１７－７中，內容提供者１０１藉著解壓縮步驟Ｓ１７－６中壓縮內容資料而產生內容資料。

在步驟Ｓ１７－８中，內容提供者１０１執行壓縮的內容資料上之音頻檢查。

隨後，在步驟Ｓ１７－９中，內容提供者１０１偵測根據內容嵌入內容資料之數位水記資訊，及在步驟Ｓ１７－５中儲存於資料庫中之數位水記資訊的嵌入位置。

如果已成功地執行數位水記資訊之偵測及音頻檢查，內容提供者１０１執行步驟Ｓ１７－１０之處理（圖１８）。如果上述處理失敗，則重覆步驟Ｓ１７－４之處理。

在步驟Ｓ１７－１０中，內容提供者１０１產生一隨機數目，以產生內容鑰匙資料Ｋｃ並保持它。內容提供者１０１藉著使用內容鑰匙資料Ｋｃ亦加密在步驟Ｓ１７－６中被壓縮的內容資料。

在步驟Ｓ１７－１１中，內容提供者１０１產生圖３Ａ所示之內容檔ＣＦ，且將它儲存在內容檔資料庫中。

然後，在步驟Ｓ１７－１２中，內容提供者１０１產生與內容資料Ｃ有關的ＵＣＰ資料１０６。

在步驟Ｓ１７－１３中，內容提供者１０１決定ＳＲＰ，且將它儲存於資料庫中。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（53）

在步驟Ｓ１７－１４中，內容提供者１０１輸出內容ＩＤ、內容鑰匙資料Ｋc及ＵＣＰ資料１０６至ＥＭＤ服務中心１０２。

隨後，在步驟Ｓ１７－１５中，內容提供者１０１從ＥＭＤ服務中心１０２接收以執照鑰匙資料KD_1至KD_3加密的鑰匙檔ＫＦ。

在步驟Ｓ１７－１６中，內容提供者１０１儲存接收的鑰匙檔ＫＦ於鑰匙檔資料庫中。

在步驟Ｓ１７－１７（圖１９）中，內容提供者１０１超鏈接內容檔ＣＦ與鑰匙檔ＫＦ。

在步驟Ｓ１７－１８中，內容提供者１０１藉著使用私人鑰匙資料$K_{CP,S}$從內容檔ＣＦ之雜亂值產生簽名資料$SIG_{6,CP}$。內容提供者１０１亦藉著使用私人鑰匙資料$K_{CP,S}$從鑰匙檔ＫＦ之雜亂值產生簽名資料$SIG_{7,CP}$。

在步驟Ｓ１７－１９中，內容提供者１０１產生儲存內容檔ＣＦ、鑰匙檔ＫＦ、公開－鑰匙證明資料CER_{CP}、簽名資料$SIG_{6,CP}$、$SIG_{7,CP}$及$SIG_{1,ESC}$之安全容器１０４，如圖３Ａ至３Ｃ所示。

最好內容資料是以包括許多安全容器之複合格式被提供，各安全容器１０４是藉由重覆步驟Ｓ１７－１至Ｓ１７－１９之處理而產生。然後，在步驟Ｓ１７－２０中，超鏈接內容檔ＣＦ與鑰匙檔ＫＦ之間的關係，且內容檔ＣＦ之間的關係亦被超鏈接。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 54）

隨後，在步驟Ｓ１７－２１中，內容提供者１０１將產生的安全容器１０４儲存安全容器資料庫中。

〔ＥＭＤ服務中心１０２〕

圖２０指出ＥＭＤ服務中心１０２之基本功能。如圖２０所示，ＥＭＤ服務中心１０２主要供給執照鑰匙資料至內容提供者１０１及ＳＡＭ１０５$_1$至１０５$_4$，發出公開－鑰匙證明資料ＣＥＲ$_{CP}$及ＣＥＲ$_{SAM1}$至ＣＥＲ$_{SAM4}$，產生鑰匙檔ＣＦ，並根據使用登錄資料１０８執行給付處理（利潤分配）。

執照鑰匙資料之供給

首先敘述從ＥＭＤ服務中心１０２送出執照鑰匙資料至使用者家庭網路１０３之ＳＡＭ１０５$_1$至１０５$_4$之處理。

ＥＭＤ服務中心１０２從鑰匙資料庫定期地例如三個月讀取執照鑰匙資料ＫＤ$_1$至ＫＤ$_3$，且藉著使用ＥＭＤ服務中心１０２之私人鑰匙資料Ｋ$_{ESC,S}$，從雜亂值產生簽名資料ＳＩＧ$_{KD1,ESC}$至ＳＩＧ$_{KD3,ESC}$。

然後ＥＭＤ服務中心１０２藉著使用連續鑰匙資料Ｋ$_{SES}$，加密三個月之執照鑰匙資料ＫＤ$_1$至ＫＤ$_3$及簽名資料ＳＩＧ$_{KD1,ESC}$至ＳＩＧ$_{KD3,ESC}$，連續鑰匙資料Ｋ$_{SES}$是藉著以ＳＡＭ１０５$_1$至１０５$_4$執行相互證明而得到，且將加密的資料送至ＳＡＭ１０５$_1$至１０５$_4$。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 55）

類似地，ＥＭＤ服務中心１０２將例如六個月之執照鑰匙資料KD_1至KD_6送至內容提供者１０１。

發出公開－鑰匙證明資料

以下敘述當ＥＭＤ服務中心１０２接收一要求以從內容提供者１０１發出公開－鑰匙證明資料CER_{CP}時執行的處理。

於從內容提供者１０１接收內容提供者１０１ＣＰ＿ＩＤ、公開鑰匙資料$K_{CP,P}$及簽名資料$SIG_{9,CP}$時，ＥＭＤ服務中心１０２藉著使用以內容提供者１０１執行相互證明所得到的連續鑰匙資料K_{SES}而加密此資料。

在證明加密的簽名資料$SIG_{9,CP}$完整之後，ＥＭＤ服務中心１０２根據辨識ＣＰ＿ＩＤ及公開鑰匙資料$K_{CP,P}$，決定已被要求發出公開－鑰匙證明資料之內容提供者１０１是否被登記於ＣＰ資料庫中。

然後，ＥＭＤ服務中心１０２從證書資料庫讀取內容提供者１０１之Ｘ．５０９格式公開－鑰匙證明資料CER_{CP}，並藉著使用ＥＭＤ服務中心１０２之私人鑰匙$K_{ESC,S}$，從公開－鑰匙證明資料CER_{CP}之雜亂值產生簽名資料$SIG_{1,ESC}$。

ＥＭＤ服務中心１０２藉著用以內容提供者１０１由執行相互證明所得到的連續鑰匙資料K_{SES}，而加密公開－鑰匙證明資料CER_{CP}及簽名資料$SIG_{1,ESC}$，並將加密的資料送至內容提供者１０１。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 56）

當ＥＭＤ服務中心１０２接收來自ＳＡＭ１０５$_1$之要求以發出公開－鑰匙證明資料ＣＥＲ$_{SAM1}$時所執行之處理，類似於當從內容提供者１０１接收一要求以發出公開－鑰匙證明資料ＣＥＲ$_{CP}$，除了是以ＳＡＭ１０５$_1$來執行處理。亦以Ｘ．５０９格式來敘述公開－鑰匙證明資料ＣＥＲ$_{SAM1}$。

在本發明中，如果設計成私人鑰匙資料Ｋ$_{SAM1,S}$與公開鑰匙資料Ｋ$_{SAM1,P}$被儲存於ＳＡＭ１０５$_1$之儲存單元中，則ＥＭＤ服務中心１０２可產生公開鑰匙資料Ｋ$_{SAM1,P}$之公開－鑰匙證明資料ＣＥＲ$_{SAM1}$，當運送ＳＡＭ１０５$_1$時。在此情形中，公開－鑰匙證明資料ＣＥＲ$_{SAM1}$可被儲存於ＳＡＭ１０５$_1$之儲存單元中，當運送ＳＡＭ１０５$_1$時。

<u>產生鑰匙檔ＫＦ</u>

在從內容提供者１０１接收圖６所示之登記模組Ｍｏｄ$_2$時，ＥＭＤ服務中心１０２藉著使用以內容提供者１０１進行相互證明所得到的連續鑰匙Ｋ$_{SES}$而解碼登記模組Ｍｏｄ$_2$。

然後ＥＭＤ服務中心１０２藉著使用從鑰匙資料庫讀取的公開鑰匙資料Ｋ$_{CP,P}$，證明簽名資料ＳＩＧ$_{M1,CP}$之完整。

隨後，ＥＭＤ服務中心１０２將ＵＣＰ資料１０６，內容鑰匙資料Ｋｃ，數位水記資訊控制資料ＷＭ，及儲存

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（57）

於登記模組Mod_2中之SRP，登記於UCP資料庫中。

EMD服務中心102藉著使用從鑰匙伺服器讀取的對應周期之執照鑰匙資料KD_1至KD_6，加密內容鑰匙資料K_C、UCP資料106及SAM程式下載容器SDC_1至SDC_3。

然後EMD服務中心102藉著使用EMD服務中心102之私人鑰匙$K_{ESC,S}$，從標頭資料、內容鑰匙資料K_C、UCP資料106與SAM程式下載容器SDC_1至SDC_3之雜亂值產生簽名資料$SIG_{K1,ESC}$。

以此方式，EMD服務中心102產生圖3B所奈之鑰匙檔KF，並將它儲存於KF資料庫中。

隨後，EMD服務中心102從KF資料庫讀取鑰匙檔KF，並藉著使用以內容提供者101進行相互證明所得到的連續鑰匙資料K_{SES}而將它加密，然後將它送至內容提供者101。

給付處理

EMD服務中心102中所執行的給付處理如下。

於從例如使用者家庭網路103之$SAM105_1$接收使用登錄資料108及其簽名資料$SIG_{200,SAM1}$時，EMD服務中心102藉著使用以$SAM105_1$執行相互證明所得到的連續鑰匙資料K_{SES}而加密此資料，藉以證明由$SAM105_1$之公開鑰匙資料K_{SAM1}所產生的簽名資料$SIG_{200,SAM1}$。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（58）

圖２１指出使用登錄資料１０８中敘述的資料。使用登錄資料１０８如圖２１所示，含有例如：ＥＳＣ＿內容ＩＤ，其是由ＥＭＤ服務中心１０２提供的全球獨特辨識，用於儲存於安全容器１０４中之內容資料Ｃ；ＣＰ＿內容ＩＤ，其是由內容提供者１０１提供的全球獨特辨識，用於內容資料Ｃ；使用者ＩＤ，其是已接收安全容器１０４之使用者的辨識；使用者資訊；ＳＡＭ＿ＩＤ，其是由安全容器１０４接收的各ＳＡＭ105_1至105_4之辨識；ＨＮＧ＿ＩＤ，其是對應的ＳＡＭ所屬於之家庭網路群的辨識；打折資訊；追蹤資訊；價格標籤；已提供內容資料Ｃ之內容提供者１０１之ＣＰ＿ＩＤ；服務提供者ＩＤ；硬體提供者ＩＤ；記錄安全容器１０４之記錄媒體＿ＩＤ之辨識；零件ＩＤ，其是預定零件之辨識，例如安全容器１０４之壓縮方法；安全容器１０４之執照擁有者ＬＨ＿ＩＤ之辨識；執安全容器１０４之給付處理之ＥＭＤ服務中心１０２ＥＳＣ＿ＩＤ。

在第二實施例中，討論於下，除了包含於使用登錄資料１０８中之上述資料外，使用登錄資料３０８包括由服務提供者３１０提供用於內容資料Ｃ之辨識ＳＰ＿內容ＩＤ，及已分在內容資料Ｃ之服務提供者３１０ＳＰ＿ＩＤ之辨識。

如果使用者家庭網路１０３之使用者的給付需要被分配至相鄰的權利擁有者而非內容提供者１０１，例如壓縮方法之執照擁有者，記錄媒體等等，ＥＭＤ服務中心

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（59）

１０２決定依據預定分配比率之給付量，並根據決定的給付量產生處理報告資料及處理要求資料。可對於儲存於安全容器１０４中之各內容資料產生分配比率。

隨後，ＥＭＤ服務中心１０２根據包含於從ＵＣＰ資料庫讀取的ＵＣＰ資料１０６中之ＳＲＰ及銷售價格且根據使用登錄資料１０８，執行給付處理，並產生處理要求資料１５２及處理報告資料１０７。

處理要求資料１５２是可以根據前述資料從處理組織９１要求給付之授權資料，且如果使用者之給付欲被分配至許多權利擁有者，對於各權利擁有者產生處理要求資料１５２。

然後ＥＭＤ服務中心１０２經由相互證明及使用連續鑰匙資料K_{SES}而加密處理要求資料１５２及其簽名資料SIG_{99}，然後經由圖１所示之給付閘道９０將它們送至處理組織９１。

因此，處理要求資料１５２所指明的給付量被付給內容提供者１０１。

ＥＭＤ服務中心１０２將處理報告資料１０７送至內容提供者１０１。

〔使用者家庭網路１０３〕

使用者家庭網路１０３如圖１所示具有網路裝置160_1及Ａ／Ｖ機器160_2至160_4。網路裝置160_1具有內建$SAM105_1$。Ａ／Ｖ機器160_2至

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（60）

１６０$_4$分別具有內建ＳＡＭ１０５$_2$至ＳＡＭ１０５$_4$。ＳＡＭ１０５$_2$至ＳＡＭ１０５$_4$經由匯流排１９１例如ＩＥＥＥ－１３９４串聯介面匯流排彼此連接。

雖然不是主要的，對於各Ａ／Ｖ機器１６０$_2$至１６０$_4$可提供網路通訊功能。如果沒有提供網路通訊功能，Ａ／Ｖ機器１６０$_2$至１６０$_4$可經由匯流排１９１只使用網路裝置１６０$_1$之網路通訊功能。另一種方式，使用者家庭網路１０３可只包括不具有網路功能之Ａ／Ｖ機器。

網路裝置１６０$_1$之細節如下。

圖２２是網路裝置１６０$_1$之方塊圖。網路裝置１６０$_1$是由ＳＡＭ１５０$_1$、通訊模組１６２、Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３、操作單元１６５、下載記憶體１６７、播放模組１６９、外部記憶體２０１及主中央處理單元（ＣＰＵ）８１０所組成。

主ＣＰＵ８１０集中地控制網路裝置１６０$_1$內執行的處理，且主ＣＰＵ８１０與ＳＡＭ１０５$_1$具有主人－奴役關係。

參見圖２３，以下詳細討論主ＣＰＵ８１０與ＳＡＭ１０５$_1$間的關係。

如圖２３所示，在網路裝置１６０$_1$中，經由主ＣＰＵ匯流排１０００連接主ＣＰＵ８１０與ＳＡＭ１０５$_1$。

當依據使用者執行在操作單元１６５上之操作選定許多中斷型式的其中之一時，主ＣＰＵ８１０接收指出選定的中斷之外部中斷（硬體中斷）Ｓ１６５。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（61）

如果發現對應中斷Ｓ１６５之工作是由ＳＡＭ１０５$_1$執行，主ＣＰＵ８１０經由主ＣＰＵ匯流排１０００，輸出指出工作之內部中斷（軟體中斷）Ｓ８１０至ＳＡＭ１０５$_1$。

然後，ＳＡＭ１０５$_1$被主ＣＰＵ８１０辨認爲輸入／輸出（Ｉ／Ｏ）裝置，且於從主ＣＰＵ８１０接收是功能呼叫之內部中斷Ｓ８１０時，ＳＡＭ１０５$_1$執行要求的工作並將執行結果送回至主ＣＰＵ８１０。

由ＳＡＭ１０５$_1$執行之主要工作可包括用於購買內容資料之處理（會計處理）、簽名檢查、相互證明、內容資料之播放、更新、登記、下載等等。當被完全與外部源隔離時，這些工作是在ＳＡＭ１０５$_1$內被處理，藉以避免主ＣＰＵ８１０監視處理的結果。

主ＣＰＵ８１０知道依據事件之型式何種工作應被要求至ＳＡＭ１０５$_1$。特別是，於藉著執行在操作單元１６５例如外部鍵裝置上之使用者操作接收中斷Ｓ１６５時，主ＣＰＵ８１０決定中斷Ｓ１６５之工作將由ＳＡＭ１０５$_1$執行。然後，主ＣＰＵ８１０經由主ＣＰＵ匯流排１０００輸出內部中斷Ｓ８１０至ＳＡＭ１０５$_1$，以要求它執行工作。

來自Ｉ／Ｏ裝置例如外部鍵裝置如指令或鍵盤至主ＣＰＵ８１０之中斷，與由主ＣＰＵ８１０執行之使用者程式非同步地發生。此中斷通常稱爲”硬體中斷”或”外部中斷”。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（62）

由主ＣＰＵ８１０接收用於觀看及傾聽內容或購買內容之中斷爲硬體中斷。在此情形中，產生硬體中斷之Ｉ／Ｏ裝置可以是網路裝置１６０₁之鍵裝置，例如按鈕或圖形使用者介面（ＧＵＩ）圖示。在此實施例中，操作單元１６５作爲此Ｉ／Ｏ裝置。

另一方面，由主ＣＰＵ８１０藉著執行使用者程式（程式）所產生之中斷稱爲”軟體中斷”或”內部中斷”。

通常，經由與主ＣＰＵ匯流排１０００分開地提供之外部中斷的特定線，外部中斷Ｓ１６５之中斷信號從操作單元１６５被輸出至主ＣＰＵ８１０。

藉著指定數字至產生中斷之Ｉ／Ｏ裝置，區別一外部中斷Ｓ１６５與另一外部中斷Ｓ１６５。例如，對於一鍵盤，數字被指定至個別按鈕（此數字稱爲”中斷型式”）。於按壓其中一個按鈕時，對應的資訊經由特定線從操作單元１６５被報告至主ＣＰＵ８１０，且按壓的按鈕之數字被儲存於Ｉ／Ｏ介面之記憶體中。響應指出按鈕已被按壓之資訊，主ＣＰＵ８１０存取Ｉ／Ｏ介面之記憶體，且從按鈕之數字辨識中斷型式，藉以控制對應按鈕之數字的中斷常式。

在此情形中，如果中斷常式欲被ＳＡＭ１０５₁執行，主ＣＰＵ８１０將內部中斷Ｓ８１０送至ＳＡＭ１０５₁以要求它執行工作。

如上所述，欲由ＳＡＭ１０５₁執行之工作可包括：

１．購買內容（包括購買鑰匙及內容之展示）；

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 63）

２．內容之播放；及

３．從內容提供者１０１及ＥＭＤ服務中心１０２之下載（更新，接收使用登錄，及程式下載）。

主ＣＰＵ８１０首先經由特定線從操作單元１６５接收對應工作１，２與３之外部中斷Ｓ１６５，且輸出對應的內部中斷Ｓ８１０至ＳＡＭ１０５$_1$，使得ＳＡＭ１０５$_1$執行工作１，２與３。

產生對應工作１與２之中斷的Ｉ／Ｏ裝置爲外部鍵裝置，例如按鈕或網路裝置１６０$_1$之ＧＵＩ。

在工作３的情形中，不是推壓型下載安全容器１０４從內容提供者１０１被送出，而是主動拉型安全容器１０４被送至網路裝置１６０$_1$（客戶），藉著執行投票以存取內容提供者１０１。因此，主ＣＰＵ８１０知道安全容器１０４被儲存於網路裝置１６０$_1$內的下載記憶體１６７中。於是，實際上，主ＣＰＵ８１０只產生內部中斷Ｓ８１０，且將它送至ＳＡＭ１０５$_1$，而沒有從操作單元１６５接收外部中斷Ｓ１６５。

由於ＳＡＭ１０５$_1$作爲主ＣＰＵ８１０之Ｉ／Ｏ裝置（奴役），ＳＡＭ１０５$_1$之主常式當電力打開時被開始，然後輸入備用（等待）模式。

隨後，當從主ＣＰＵ８１０（主人）接收內部中斷Ｓ８１０時，ＳＡＭ１０５$_1$立即開始處理工作，而完全與外部源隔離。然後，ＳＡＭ１０５$_1$報告完成處理工作至主ＣＰＵ８１０，藉著外部中斷（硬體中斷），並要求主

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 64）

ＣＰＵ８１０接收結果。因此，ＳＡＭ１０５１不會含有使用者主要程式（使用者程式）。

ＳＡＭ１０５１執行處理，例如購買內容，內容之播放，及從內容提供者１０１及ＥＭＤ服務中心１０２之下載，作爲中斷常式。ＳＡＭ１０５１通常在備用模式等待，且於從主ＣＰＵ８１０接收內部中斷Ｓ８１０時，ＳＡＭ１０５１執行對應中斷型式（數字）之中斷常式（功能呼叫指令），並要求主ＣＰＵ８１０接收結果。

特別是，依據Ｉ／Ｏ指令，由內部中斷Ｓ８１０要求執行從主ＣＰＵ８１０至ＳＡＭ１０５１之工作，然後ＳＡＭ１０５１根據從主ＣＰＵ８１０接收的功能呼叫指令自行中斷。實際上，藉著執行晶片選定以選定ＳＡＭ１０５１，主ＣＰＵ８１０輸出內部中斷Ｓ８１０至ＳＡＭ１０５１。

如上所討論，雖然主ＣＰＵ８１０接收用於購買或播放內容之外部中斷Ｓ１６５，它要求ＳＡＭ１０５１執行對應的工作。這是因爲工作包含安全性，例如加密處理、產生及檢查簽名，伴隨購買鑰匙之處理。

儲存於ＳＡＭ１０５１中之中斷常式作爲主ＣＰＵ８１０之中斷常式的副常式。

由主ＣＰＵ８１０執行之中斷常式是一工作，其做成指示以將要求對應外部中斷Ｓ１６５之工作的執行之內部中斷（功能呼叫）Ｓ８１０送至ＳＡＭ１０５１之共同記憶體空間。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（65）

如圖２４所示，儲存於ＳＡＭ１０５₁中之各中斷常式含有副常式。能與其它中斷常式分享的程式最好定義爲副常式，藉以節省空間。以類似於由ＣＰＵ執行之方式，執行ＳＡＭ１０５₁之處理，例如同時定義來自中斷常式之副常式或定義來自第一產生副常式之第二產生副常式。

參見圖２３，敘述主ＣＰＵ８１０與ＳＡＭ１０５₁間的關係。如上所討論，主ＣＰＵ８１０經由一特定線接收來自Ｉ／Ｏ裝置之中斷，例如外部鍵裝置，作爲外部中斷（硬體中斷）Ｓ１６５。

對於各特定線提供一數字，且依據此數字，從儲存於主ＣＰＵ８１０之系統記憶體中之中斷向量表取出對應的中斷向量，藉以開始中斷常式。

有兩種中斷型式：一型式是一間接存取，指出向量表中之中斷向量，且另一型式是一直接存取，指出中斷常式之啓始址址。

如果接收的外部中斷指出欲由ＳＡＭ１０５₁執行工作，主ＣＰＵ８１０輸出內部中斷Ｓ８１０至ＳＡＭ１０５₁，並要求它執行工作（Ｉ／Ｏ指令）。

工作的型式是由指令名字定義，且主ＣＰＵ８１０輸出指令基礎的內部中斷Ｓ８１０至ＳＡＭ１０５₁。當正被電力打開時，ＳＡＭ１０５₁啓始程式，並檢查ＳＡＭ１０５₁之完整性，如圖２４所示，然後輸入一睡眠模式（備用模式）。在睡眠模式中，只有ＣＰＵ之操作被停止，且睡眠模式被任意中斷釋放。隨後，ＳＡＭ１０５₁

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（66）

之狀態經由執行處理狀態被移位至程式執行狀態。於接收來自主ＣＰＵ８１０之內部中斷時，ＳＡＭ１０５₁執行對應的工作，並將結果送回至主ＣＰＵ８１０。

響應來自ＳＡＭ１０５₁之結果，主ＣＰＵ８１０開始做另一動作。然而，即使當ＳＡＭ１０５₁正在執行一工作，主ＣＰＵ８１０可執行另一工作。主ＣＰＵ８１０接收來自ＳＡＭ１０５₁之工作的執行結果作爲中斷。

有兩種方式報告來自ＳＡＭ１０５₁之工作的執行結果至主ＣＰＵ８１０。一種方式是輸出一中斷至主ＣＰＵ８１０並要求主ＣＰＵ８１０接收此結果。另一種方式是提供可由主ＣＰＵ８１０存取的ＳＡＭ１０５₁之位址空間中的狀態暫存器（稱爲”ＳＡＭ狀態暫存器”）。（讀取／寫入指令、位址資訊及來自主ＣＰＵ８１０之資料被載送至位址空間）。依據第二種方式，工作的型式，指出是否工作正被等待、執行或完成等等之旗標，可被設定在ＳＡＭ狀態暫存器（ＳＡＭ＿ＳＲ）中，且主ＣＰＵ８１０定期地執行投票（讀取資料）至ＳＡＭ狀態暫存器。

第一ＳＡＭ狀態暫存器設定一旗標，指出由主ＣＰＵ８１０讀取的ＳＡＭ１０５₁之狀態。

第二ＳＡＭ狀態暫存器設定旗標，指定是否來自主ＣＰＵ８１０之工作的執行已被要求。這些旗標是由ＳＡＭ１０５₁內之ＣＰＵ讀取。根據匯流排仲裁之優先順序，主ＣＰＵ８１０與ＳＡＭ１０５₁均被允許存取設定在

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（67）

第一與第二ＳＡＭ狀態暫存器中之旗標。

特別是，在第一ＳＡＭ狀態暫存器中，旗標被設定指出是否ＳＡＭ正在執行工作，已完成工作，或正等待欲被執行之工作。工作之名稱亦被指出於第一ＳＡＭ狀態暫存器中。主ＣＰＵ８１０定期地執行投票以存取第一ＳＡＭ狀態暫存器。

在第二ＳＡＭ狀態暫存器中，旗標被設定指出是否工作的執行已從主ＣＰＵ８１０被要求或是在備用模式。

首先Ｉ／Ｏ寫入指令從主ＣＰＵ８１０被送至ＳＡＭ１０５$_1$，其是一Ｉ／Ｏ裝置，接著是欲被寫入之資料與位址。位址資訊（資料儲存位置）被儲存在由主ＣＰＵ８１０與ＳＡＭ１０５$_1$共享的共同記憶體空間中。

要求ＳＡＭ１０５$_1$內的記憶體位址空間應是由主ＣＰＵ８１０看不到的（抗干預特性）。因此，ＳＡＭ１０５$_1$內的記憶體位址空間應被管理，使得可由主ＣＰＵ８１０只看到部份靜態隨機存取記憶體，或部份外部快閃ＲＯＭ（電消除可程式僅讀記憶體（ＥＥＰＲＯＭ））。於是，大量資料從主ＣＰＵ８１０被寫入部份ＳＲＡＭ或部份ＥＥＰＲＯＭ，且小量資料被寫入可由主ＣＰＵ８１０看到的ＳＡＭ１０５$_1$內之暫存器中。

欲由中斷執行之中斷常式的位址稱爲”中斷向量”。中斷向量依據中斷型式之順序被儲存於向量表中。

於接收一外部中斷時，如圖２５所示，依據中斷型式（數字），主ＣＰＵ８１０執行來自儲存於記憶體中的中

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 68）

斷向量表之中斷向量，且執行從位址（中斷向量）開始之對應常式作爲副常式。

在此實施例中，執行上述工作１至３的其中之一時，由一實質中斷信號從對應的Ｉ／Ｏ裝置發生一外部中斷，且主ＣＰＵ８１０藉著使用內部中斷（軟體中斷）送出一功能呼叫（程序呼叫）至ＳＡＭ１０５１，並要求它執行依據中斷型式（數字）之中斷常式（工作）。然後，主ＣＰＵ８１０接收工作之執行結果，並開始另一動作。

內部中斷是由使用者程式，亦即ＣＰＵ，產生之軟體中斷，如圖２６所示。由機器語言之ＩＮＴ指令的執行產生內部中斷。

功能呼叫（程序呼叫）之細節如下。

中斷常式是由小功能組成，且對於各功能定義一指令名稱。藉著指定指令名稱連同來自使用者程式之中斷指令ＩＮＴ，可完成目標功能。此稱爲”功能呼叫（程序呼叫）”。以此方式，功能呼叫經內部中斷（軟體中斷）被執行。

執行功能呼叫時，用於執行中斷常式之參數被傳送，藉著輸入功能呼叫數字於ＣＰＵ之暫存器中，藉以指定目標功能。結果被送回至暫存器或記憶體，或執行對應的操作。

例如，執行圖２７所示的使用者程式內之碼Ａ時，主ＣＰＵ８１０指定中斷指令ＩＮＴ及指令名稱”ＩＮＴ２１Ｈ”，且ＳＡＭ１０５１之ＣＰＵ存取對應中斷型式”

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 69）

２１Ｈ”之記憶體區域，且亦存取一指令分析，藉以執行功能３之副常式。

參見圖２８以下討論ＳＡＭ１０５１之ＣＰＵ的處理狀態。

如圖２８所示，ＳＡＭ１０５１之ＣＰＵ有五個狀態：重置狀態ＳＴ１、例外處理狀態ＳＴ２、程式執行狀態ＳＴ３、匯流排權利釋放狀態ＳＴ４、低電力狀態ＳＴ５。

個別狀態之細節如下。

重置狀態ＳＴ１是一狀態，其中ＣＰＵ被重置。

例外處理狀態ＳＴ２是一轉移狀態，其中由於外部處理因數ＣＰＵ正在移位處理狀態，例如重置或中斷處理。執行中斷處理時，藉參見堆疊指標（ＳＰ），程式計數器（ＰＣ）之計數值及狀態暫存器（ＳＲ）之值被暫時地儲存於堆疊區域中。然後從例外處理向量表取出開始中斷常式之位址，且常式被分支至此位址，藉以開始程式。然後ＣＰＵ之狀態被移位至程式執行狀態ＳＴ３。

程式執行狀態ＳＴ３是一狀態，其中ＣＰＵ正依序地執行程式。

匯流排權利釋放狀態ＳＴ４是一狀態，其中ＣＰＵ釋放匯流排至一已要求匯流排權利之裝置。

低電力狀態ＳＴ５具有三模式，例如睡眠模式、備用模式及模組備用模式。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 70）

（１）睡眠模式

ＣＰＵ之操作中斷，但保持儲存於ＣＰＵ之內部暫存器中的資料、內建快取記憶體中的資料、內建ＲＡＭ中的資料。ＣＰＵ以外的內建周邊模組之功能仍繼續工作。

由重置、中斷或直接記憶體存取（ＤＭＡ）位址錯誤釋放睡眠模式，且睡眠模式經由例外處理狀態ＳＴ２被移位至程式執行狀態ＳＴ３。

（２）備用模式

備用模式中，ＣＰＵ、內建模組及振盪器之功能完全停止。內建快取記憶體之資料與內建ＲＡＭ之資料沒有被保持。藉由重置或外部非罩中斷（ＮＭＩ）釋放備用模式。在被釋放之後，備用模式在過了穩定振盪所需的周期之後，經由例外處理狀態ＳＴ２被移位至正常程式狀態。在備用模式中，由於振盪器被停止，電力消耗可明顯減小。

（３）模組備用模式

時鐘供給至一內建模組例如ＤＭＡ被中斷。

參見圖２９，經由記憶體空間，以下敘述主ＣＰＵ８１０與ＳＡＭ１０５１之間的關係。

如圖２９所示，經由使用者在按鈕上之操作於接收外部中斷時，主ＣＰＵ８１０之ＣＰＵ８１０ａ中斷使用者程式之執行，且指定中斷型式以存取中斷向量表之硬體中斷區域。然後，ＣＰＵ８１０ａ執行儲存於存取的位址中

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（71）

之中斷常式。中斷常式敘述輸出功能呼叫１－１、１－２、２或３之處理至ＳＡＭ１０５１，以要求ＳＡＭ１０５１執行對應工作，且用於從ＳＡＭ１０５１得到執行結果，然後送回至使用者程式。特別是，ＣＰＵ８１０ａ將用於指定工作之資訊寫入ＳＲＡＭ１１５５，其形成ＳＡＭ１０５１內的部份記憶體１０５１ａ，且其作爲ＳＡＭ１０５１與主ＣＰＵ８１０之共同記憶體。

輸出內部中斷至ＳＡＭ１０５１時，主ＣＰＵ８１０之ＣＰＵ８１０ａ打開ＳＡＭ１０５１內第二ＳＡＭ狀態暫存器１１５６ｂ之工作等待旗標。

ＳＡＭ１０５１之ＣＰＵ１１００檢查第二ＳＡＭ狀態暫存器１１５６ｂ並存取ＳＲＡＭ１１５５，以指定由主ＣＰＵ８１０要求的工作之型式，藉以執行對應的中斷常式。如上所述，藉著讀取副常式而執行中斷常式，其包括例如：使用記錄媒體、Ａ／Ｖ壓縮／解壓縮ＳＡＭ、媒體驅動ＳＡＭ、ＩＣ卡與ＥＭＤ服務中心１０２之相互證明，機器間之相互證明，及產生與檢查簽名資料。

ＳＡＭ１０５１之ＣＰＵ１１００儲存ＳＲＡＭ１１５５中之中斷常式之結果（工作結果），且亦打開ＳＡＭ１０５１內之第一ＳＡＭ狀態暫存器１１５６ａ之工作完成旗標。

在檢查第一ＳＡＭ狀態暫存器１１５６ａ之工作完成旗標是打開之後，主ＣＰＵ８１０從ＳＲＡＭ１１５５讀取工作結果，並送回至使用者程式之處理。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 72）

ＳＡＭ１０５$_{1}$之功能如下。應注意ＳＡＭ１０５$_{2}$至１０５$_{4}$之功能是與ＳＡＭ１０５$_{1}$類似。

ＳＡＭ１０５$_{1}$執行對於各內容之會計處理，且與ＥＭＤ服務中心１０２通訊。可由ＥＭＤ服務中心１０２管理ＳＡＭ１０５$_{1}$之標準及版本。如果家庭電器製造商要求ＳＡＭ１０５$_{1}$被負載在家庭電器中，ＥＭＤ服務中心１０２可給這些製造商執行，以使用ＳＡＭ１０５$_{1}$作爲黑盒會計模組，用於執行單元的內容之會計。例如ＥＭＤ服務中心１０２將ＳＡＭ１０５$_{1}$之ＩＣ例如ＩＣ介面標準化，製造商不用知道，且ＳＡＭ１０５$_{1}$依據標準被負載於網路裝置１６０$_{1}$中。ＳＡＭ１０５$_{2}$至１０５$_{4}$分別被負載於Ａ／Ｖ機器１６０$_{2}$至１６０$_{4}$中。

ＳＡＭ１０５$_{1}$之處理內容完全與外部源隔離，於是被保護免於被外部地監視或干預。ＳＡＭ１０５$_{1}$是一功能模組，其藉由執行抗干預硬體組（例如ＩＣ模組）而被實施，其中ＣＰＵ無法藉執行軟體（私人程式）來干預預先儲存的資料或目前處理的資料。

如果ＳＡＭ１０５$_{1}$之功能是藉由一ＩＣ來實施，一私人記憶體被放置在ＩＣ內，且私人程式與私人資料被儲存於私人記憶體中。如果ＳＡＭ１０５$_{1}$之功能被併入部份機器中，而非藉使用一實體形式例如一ＩＣ被實施，則併入功能的部份可被定義爲ＳＡＭ。

在圖２２所示的網路裝置１６０$_{1}$之例子中，安全容器１０４從通訊模組１６２被輸出至ＳＡＭ１０５$_{1}$，如實線

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（73）

所示。然而，如虛線所示，鑰匙檔ＫＦ可從通訊模組１６２被輸出至ＳＡＭ１０５１，且內容檔ＣＦ可經由一ＣＰＵ匯流排從通訊模組１６２被寫入下載記憶體１６７中。

內容資料Ｃ可藉著跳過ＳＡＭ１０５１直接從下載記憶體１６７被輸出至Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。

參見圖３０之功能區塊，以下特定地敘述ＳＡＭ１０５１之功能。

圖３０指出用於從內容提供者１０１接收安全容器１０４之資料流，及用於解碼安全容器１０４內之鑰匙檔ＫＦ之處理。

如圖３０所示，ＳＡＭ１０５１包括證明單元１７０，加密／解密（解碼）單元１７１、１７２、１７３，內容提供者管理器１８０，下載記憶體管理器１８２，Ａ／Ｖ壓縮／解壓縮ＳＡＭ管理器１８４，ＥＭＤ服務中心管理器１８５，使用監視器１８６，會計處理器１８７，簽名處理器１８９，ＳＡＭ管理器，工作記憶體２００，外部記憶體管理器８１１，及ＣＰＵ１１００。

ＣＰＵ１１００從主ＣＰＵ８１０接收內部中斷Ｓ８１０，且控制ＳＡＭ１０５１內之整個處理。

本發明之元件與ＳＡＭ１０５１之零件之間的關係如下。內容提供者管理器１８０與下載記憶體管理器１８２對應輸入處理機構，會計處理器１８７對應決定機構、登錄資料產生機構、ＵＣＳ資料產生機構，加密／解密（解碼

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 74）

）單元１７２對應解碼機構，且使用監視器單元１８６對應使用控制狀態機構。加密／解密（解碼）單元１７３對應加密機構。圖４５所示之媒體驅動ＳＡＭ管理器８５５，敘述於下，對應記錄控制機構。簽名處理器１８９對應簽名處理機構。

如上所述，ＳＡＭ１０５$_1$之個別功能是由ＣＰＵ藉著執行私人程式或藉著操作預定硬體而實施。ＳＡＭ１０５$_1$之硬體造形討論如下。

如圖３１所示，在網路裝置１６０$_1$之外部記憶體２０１中，儲存使用登錄資料１０８與ＳＡＭ登記列表。

從ＳＡＭ１０５$_1$之外部源（例如主ＣＰＵ８１０）看不到外部記憶體２０１之記憶體空間，只有ＳＡＭ１０５$_1$被允許管理存取至外部記憶體２０１之儲存區域。作爲外部記憶體２０１，可使用快閃記憶體或鐵電記憶體（ＦｅＲＡＭ）。

作爲工作記憶體２００，可使用ＳＲＡＭ。如圖３２所示，工作記憶體２００可包括內容鑰匙資料K_C、ＵＣＰ資料１０６、儲存單元１９２之鎖鑰匙資料K_{LOC}、內容提供者１０１之公開鑰匙證明CER_{CP}、ＵＣＳ資料１６６及ＳＡＭ程式下載容器SDC_1至SDC_3，其被儲存於安全容器１０４中。

作爲ＳＡＭ１０５$_1$的一個功能，參見圖３０，以下敘述當從內容提供者１０１接收（下載）安全容器１０４時功能區塊所執行之處理。此處理被已接收內部中斷

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（75）

ＳＡＭ１０５１送出及接收資料時，相互證明單元１７０以內容提供者１０１與ＥＭＤ服務中心１０２執行相互證明，以產生連續鑰匙資料（內容鑰匙資料）K_{SES}，並將它輸出至加密／解密（解碼）單元１７１。連續鑰匙資料K_{SES}每次進行相互證明時被更新地產生。

加密／解密（解碼）單元１７１加密及解密從內容提供者１０１送出及接收的資料，藉著使用由相互證明單元１７０產生的連續鑰匙K_{SES}。

如果圖２２所示的下載記憶體１６７設有媒體ＳＡＭ１６７ａ，如圖２２所示，於相互證明單元１７０與媒體ＳＡＭ１６７ａ之間執行相互證明。然後，下載記憶體管理器１８２將內容加密，藉著使用由相互證明得到的連續鑰匙資料K_{SES}，並將加密的資料寫入圖２２所示的下載記憶體１６７中。作爲下載記憶體１６７，可使用例如記憶棒之非依電性半導體記憶體。

如果使用沒有相互證明功能之記憶體，例如硬碟機（ＨＤＤ），作爲下載記憶體２１１，下載記憶體２１１是不安全的。因此，內容檔ＣＦ被下載進入下載記憶體２１１，且高度機密鑰匙檔ＫＦ被下載進入例如圖３０所示的工作記憶體２００或圖２２所示外部記憶體２０１。

儲存鑰匙檔ＫＦ於外部記憶體２０１時，

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（76）

ＳＡＭ１０５$_{1}$藉著用ＣＢＣ模式中之訊息證明碼（ＭＡＣ）鑰匙資料Ｋ$_{MAC}$將它加密，且亦儲存部份綴字本文之最終區塊於ＳＡＭ１０５$_{1}$中作爲ＭＡＣ值。從外部記憶體２０１讀取鑰匙檔ＫＦ至ＳＡＭ１０５$_{1}$時，讀取的鑰匙檔ＫＦ以ＭＡＣ鑰匙資料Ｋ$_{MAC}$被加密，然後所得到的ＭＡＣ值與儲存的ＭＡＣ值比較，藉以證明鑰匙檔ＫＦ之完整性。在此情形中，不是ＭＡＣ值，可以使用雜亂值。

加密／解密（解碼）單元１７２解碼內容鑰匙資料Ｋ$_{C}$，ＵＣＰ資料１０６，及儲存於從下載記憶體管理器１８２接收的安全容器１０４中之鑰匙檔ＫＦ內的ＳＡＭ程式下載容器ＳＤＣ$_{1}$至ＳＤＣ$_{3}$，藉著使用從儲存單元１９２讀取的對應周期之執照鑰匙資料ＫＤ$_{1}$至ＫＤ$_{3}$。

解碼的內容鑰匙資料Ｋ$_{C}$、ＵＣＰ資料１０６及ＳＡＭ程式下載容器ＳＤＣ$_{1}$至ＳＤＣ$_{3}$，被寫入工作記憶體２００中。

ＥＭＤ服務中心管理器１８５管理與圖１所示ＥＭＤ服務中心１０２之通訊。

簽名處理器１８９證明安全容器１０４內之簽名資料的完整性，藉著使用ＥＭＤ服務中心１０２之公開鑰匙資料Ｋ$_{ESC,P}$及從儲存單元１９２讀取的內容提供者１０１之公開鑰匙資料Ｋ$_{CP,P}$。

儲存單元１９２具有以下資料，如圖３４所示，作爲被保護免於從ＳＡＭ１０５$_{1}$外側被讀取或寫入之私人資料：具有有效日期之許多執照鑰匙資料ＫＤ$_{1}$至ＫＤ$_{3}$，

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（77）

ＳＡＭ＿ＩＤ，使用者ＩＤ，密碼，ＳＡＭ屬於的家庭網路群之辨識ＨＮＧ＿ＩＤ，資訊參考ＩＤ，ＳＡＭ登記列表，裝置及記錄媒體之撤銷列表，儲存鑰匙資料K_{STR}，路由ＣＡ之公開鑰匙資料$K_{R-CA,P}$，ＥＭＤ服務中心１０２之公開鑰匙資料$K_{ESC,P}$，以驅動ＳＡＭ用於相互證明之源鑰匙資料（當使用共同鑰匙密祕系統時），驅動ＳＡＭ之公開鑰匙證明（當使用私人鑰匙密祕系統時），ＳＡＭ１０５$_1$之私人鑰匙資料$K_{SAM1,S}$（當使用共同鑰匙密祕系統時），其中儲存ＳＡＭ１０５$_1$之公開鑰匙資料$K_{SAM1,P}$之公開鑰匙證明CER_{SAM1}（當用私人鑰匙密祕系統時），藉著使用ＥＭＤ服務中心１０２之私人鑰匙資料$K_{ESC,S}$所得到之公開鑰匙證明CER_{ESC}，以Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３用於相互證明之源鑰匙資料（當使用共同鑰匙密祕系統時），以媒體ＳＡＭ用於相互證明之源鑰匙資料（當使用共同鑰匙密祕系統時），媒體ＳＡＭ之公開－鑰匙證明資料CER_{MEDSAM}（當使用公開鑰匙密祕系統），可被處理之信號源，壓縮方法，欲被連接之監視器的顯示性能，格式轉換功能，位元流記錄器之出現或消失，權利處理（利潤分配）資料，接收利潤之相關實體之ＩＤ等等。

圖３４中，具有符號＊標在左側之資料的項目當運送ＳＡＭ１０５$_1$時被儲存於儲存單元１９２中，且其它項目的資料當在運送ＳＡＭ１０５$_1$之後執行使用者登記時被儲存於儲存單元１９２中。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 78）

用於實施至少部份圖３０所示的功能之私人程式亦被儲存於儲存單元１９２中。

作爲儲存單元１９２，可使用快閃ＥＥＰＥＯＭ。

當接收執照鑰匙資料時欲被執行之處理

參見圖３３與３５，現在敘述當將從ＥＭＤ服務中心１０２接收的執照鑰匙資料KD_1至KD_3儲存於儲存單元１９２時，$SAM105_1$內的處理。

圖３５是一流程圖，指出當將來自ＥＭＤ服務中心１０２之執照鑰匙資料KD_1至KD_3儲存於儲存單元１９２時，$SAM105_1$內之處理。

在步驟Ｓ３５－０中，$SAM105_1$之ＣＰＵ１１００接收指出指令之內部中斷Ｓ８１０，以從主ＣＰＵ８１０接收執照鑰匙資料。

在步驟Ｓ３５－１中，在ＥＭＤ服務中心１０２與$SAM105_1$之相互證明單元１７０之間執行相互證明。

然後，在步驟Ｓ３５－２中，以藉由執行於步驟Ｓ３５－１中之相互證明所得到的連續鑰匙資料K_{SES}加密之對應的簽名資料$SIG_{KD1,ESC}$至$SIG_{KD3,ESC}$及三個月之執照鑰匙資料KD_1至KD_3，從ＥＭＤ服務中心１０２經由ＥＭＤ服務中心管理器１８５被寫入工作記憶體２００。

在步驟Ｓ３５－３中，加密／解密（解碼）單元１７１藉著使用連續鑰匙資料K_{SES}而解密執照鑰匙資料

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（79）

KD_1至KD_3與簽名資料$SIG_{KD1,ESC}$至$SIG_{KD3,ESC}$。

隨後，在步驟S35－4中，簽名處理器189證明儲存於工作記憶體200中之簽名資料$SIG_{KD1,ESC}$至$SIG_{KD3,ESC}$的完整性，然後將解密執照鑰匙資料KD_1至KD_3寫入儲存單元192中。

在步驟S35－5中，CPU1100經由外部中斷報告用於用於接收執照鑰匙資料之處理的結果至主CPU810。

另一種方式，CPU1100可設定一旗標於SAM狀態暫存器中，指出是否上述接收處理已被正確地執行，在此情形中，主CPU810可藉著投票讀取旗標。

<u>當從內容提供者101接收安全容器104時執行之處理</u>

參見圖30與36，現在敘述當從內容提供者101接收安全容器104時，$SAM105_1$內的流程。

在以下敘述的例子中，內容檔CF經由$SAM105_1$被寫入下載記憶體167。然而，在本發明中，內容檔CF可直接被寫入下載記憶體167而不通過$SAM105_1$。

圖36是一流程圖，指出當從內容提供者101接收安全容器104時$SAM105_1$內之處理。

在隨後的例子中，當接收安全容器104時，$SAM105_1$證明不同項目之簽名資料。另一種方式，當

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 80）

決定購買／使用模式時，可證明簽名資料。

在步驟Ｓ３６－０中，圖３０所示之ＳＡＭ１０５$_1$之ＣＰＵ１１００從主ＣＰＵ８１０接收內部中斷Ｓ８１０，指出接收安全容器１０４之指令。

在步驟Ｓ３６－１中，進行內容提供者１０１與ＳＡＭ１０５$_1$的相互證明單元１７０之間的相互證明。

然後，在步驟Ｓ３６－２中，執行下載記憶體１６７的媒體ＳＡＭ１６７ａ與ＳＡＭ１０５$_1$的相互證明單元１７０之間的相互證明。

在步驟Ｓ３６－３中，從內容提供者１０１接收的安全容器１０４被寫入下載記憶體１６７。同時，安全容器１０４在相互證明單元１７０中被加密，並藉著使用步驟Ｓ３６－２中所得到的連續鑰匙資料在媒體ＳＡＭ１６７ａ中被解密。

隨後，在步驟Ｓ３６－４中，使用步驟Ｓ３６－１中所得到的連續鑰匙資料，ＳＡＭ１０５$_1$解碼安全容器１０４。

在步驟Ｓ３６－５中，在證明由圖３Ｃ所指出的簽名資料ＳＩＧ$_{1,ESC}$之後，藉著使用儲存於圖３Ｃ所示的公開鑰匙證明資料ＣＥＲ$_{CP}$中之內容提供者１０１的公開鑰匙資料Ｋ$_{CP,P}$，簽名處理器１８９證明簽名資料ＳＩＧ$_{6,CP}$與ＳＩＧ$_{7,CP}$。

當證明簽名資料ＳＩＧ$_{6,CP}$時，證明內容檔ＣＦ之送出者與產生者的完整性。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 81）

當證明簽名資料ＳＩＧ$_{7,CP}$時，證明鑰匙檔ＫＦ之送出者與產生者的完整性。

隨後，在步驟Ｓ３６－６中，簽名處理器１８９檢查圖３Ｂ中之鑰匙檔ＫＦ內的簽名資料ＳＩＧ$_{K1,ESC}$之完整性，亦即鑰匙檔ＫＦ之產生者的完整性，藉著使用從儲存單元１９２讀取的公開鑰匙資料Ｋ$_{ESC,P}$，且亦檢查是否鑰匙檔ＫＦ被登記於ＥＭＤ服務中心１０２中。

在步驟Ｓ３６－７中，加密／解密（解碼）單元１７２解密（解碼）內容鑰匙資料Ｋｃ、ＵＣＰ資料１０６、及圖３所示之ＳＡＭ程式下載容器ＳＤＣ$_1$至ＳＤＣ$_3$，藉著使用從儲存單元１９２讀取的對應周期之執照鑰匙資料ＫＤ$_1$至ＫＤ$_3$，並將它們寫入工作記憶體２００。

然後，在步驟Ｓ３６－８中，ＣＰＵ１１００經由外部中斷報告至主ＣＰＵ８１０，是否安全容器１０４已被正確地接收。另一種方式，ＣＰＵ１１００可設定旗標於ＳＡＭ狀態暫存器中，指出是否安全容器１０４已被適當地接收，且主ＣＰＵ８１０可藉著投票讀取旗標。

參見圖３７，以下敘述用於購買及使用被下載進入下載記憶體１６７之內容資料Ｃ的個別功能區塊。

功能區塊之處理被ＣＰＵ１１００集中地控制，其從主ＣＰＵ８１０接收內部中斷Ｓ８１０。

使用監視器１８６從工作記憶體２００讀取ＵＣＰ資料１０６與ＵＣＳ資料１６６，且監視狀態以確定內容被

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 82）

購買且使用於由ＵＣＰ資料１０６與ＵＣＳ資料１６６限制的執照內。

參見圖３６，ＵＣＰ資料１０６在被解碼之後，被儲存於工作記憶體２００之鑰匙檔ＫＦ中。

當購買模式被使用者決定時，ＵＣＳ資料１６６被儲存於工作記憶體２００中，如以下所討論。ＵＣＳ資料１６６包括已購買內容資料Ｃ之使用者ＩＤ、追蹤資訊等等，亦即與圖３Ｂ所示之ＵＣＰ資料１０６相同的資料，除了指出決定於購買模式決定處理中之購買模式的ＵＣＳ資訊。

從圖２２所示之主ＣＰＵ８１０接收指出內容的購買模式或使用模式之指令的內部中斷Ｓ８１０時，會計處理器１８７產生對應的使用登錄資料１０８。

如上所述，使用登錄資料１０８指出由使用者做成的安全容器１０４之購買與使用模式之歷史，且當執行處理及決定執照費時，依據安全容器１０４之購買被ＥＭＤ服務中心１０２使用。

如果需要的話，會計處理器１８７通知使用者從工作記憶體２００讀取的ＳＲＰ或銷售價格。銷售價格與ＳＲＰ被包含在儲存於２００中之圖３Ｂ所示的鑰匙檔ＫＦ之解碼ＵＣＰ資料１０６內。

根據由ＵＣＰ資料１０６與ＵＣＳ資料１６６表示之權利例如執照同意條件，在使用監視器１８６的監視下，由會計處理器１８７執行會計處理。亦即，使用者購買及

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 83）

使用權利允許內的內容。

會計處理器１８７根據內部中斷Ｓ８１０，亦產生ＵＣＳ資料１６６，指出由使用者決定的內容之購買模式，並將它寫入工作記憶體２００中。

在此實施例中，在決定購買模式之後，ＵＣＳ資料１６６被儲存於工作記憶體２００中。然而，ＵＣＳ資料１６６與內容鑰匙資料Ｋｃ可被儲存於外部記憶體２０１中。作爲外部記憶體２０１，如上所述可使用快閃記憶體，其是非依電性ＲＡＭ。將ＵＣＳ資料１６６與內容鑰匙資料Ｋｃ寫入外部記憶體２０１時，執行完整性檢查以證明外部記憶體２０１之完整性，在此情形中，外部記憶體２０１之儲存區域被分成許多區塊，且藉著使用ＳＨＡ－１或ＭＡＣ決定各區塊之雜亂值，且決定的雜亂值被控制於ＳＡＭ１０５$_1$中。

不是決定ＳＡＭ１０５$_1$中之購買模式，安全容器１０４可被轉移至另一ＳＡＭ，例如ＳＡＭ１０５$_2$至１０５$_4$，在此情形中，ＵＣＳ資料１６６沒有被產生。

內容之購買模式包括例如，”賣斷”，其中沒有限制施加在購買者之播放操作及購買者之使用的拷貝，”時間限制”，其中限制使用之周期，”以播放付費”，其中每次內容被播放時計費，”以ＳＣＭＳ付費”，其中每次拷貝的內容被播放於ＳＣＭＳ裝置時計費，”賣斷ＳＣＭＳ拷貝”，其中允許ＳＣＭＳ中之拷貝，及”無拷貝看護之以拷貝Ｎ次付費”，其中沒有設定拷貝看護每次內容被播

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 84）

放時計費。

當使用者決定內容之購買模式時，ＵＣＳ資料１６６被產生，且隨後被使用於控制，使得購買者使用決定的購買模式之允許內的內容。ＵＣＳ資料１６６包括內容ＩＤ，購買模式，依據購買模式之價格，已購買內容之ＳＡＭ的ＳＡＭ＿ＩＤ，及已購買內容之使用者的使用者＿ＩＤ。

如果決定的購買模式是”以播放付費”、”以ＳＣＭＳ付費”或”無拷貝看護之以拷貝Ｎ次付費”，於購買內容資料Ｃ時，ＳＡＭ１０５$_1$可即時將ＵＣＳ資料１６６送至內容提供者１０１，且內容提供者１０１可指示ＥＭＤ服務中心１０２以取得決定周期內的使用登錄資料１０８。

如果決定的購買模式是”賣斷”，ＵＣＳ資料１６６可即時被送至內容提供者１０１與ＥＭＤ服務中心１０２。於是，在此實施例中，不管購買模式，ＵＣＳ資料１６６被即時送至內容提供者１０１。

ＥＭＤ服務中心管理器１８５定期地經由外部記憶體管理器８１１，將從外部記憶體２０１讀取的使用登錄資料１０８送至ＥＭＤ服務中心１０２。

在此情形中，簽名處理器１８９藉著使用私人鑰匙資料$K_{SAM1,S}$產生使用登錄資料１０８之簽名資料$SIG_{200,SAM1}$，且ＥＭＤ服務中心管理器１８５將簽名資料$SIG_{200,SAM1}$連同使用登錄資料１０８送至

（請先閱讀背面之注意事項再填寫本頁）

裝 訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 85）

ＥＭＤ服務中心１０２。

ＥＭＤ服務中心管理器１８５亦響應來自ＥＭＤ服務中心１０２之要求，或當使用登錄資料１０８中之歷史資訊超過一預定量時，定期地送出使用登錄資料１０８。依據例如外部記憶體２０１之儲存容量，決定歷史資訊之量。

當ＣＰＵ１１００接收指出指示以從圖２２所示之主ＣＰＵ８１０播放內容之內部中斷Ｓ８１０時，下載記憶體管理器１８２輸出從下載記憶體１６７讀取的內容資料Ｃ，從工作記憶體２００讀取的內容鑰匙資料Ｋｃ及從會計處理器１８７輸入之使用者數位資訊資料，至Ａ／Ｖ壓縮／解壓縮ＳＡＭ管理器１８４。

於接收指出指示以傾聽用於展示之內容的內部中斷Ｓ８１０時，下載記憶體管理器１８２輸出從下載記憶體１６７讀取的內容檔ＣＦ，內容鑰匙資料Ｋｃ及從工作記憶體２００讀取的部份揭示參數資料至Ａ／Ｖ壓縮／解壓縮ＳＡＭ管理器１８４。

部份揭示參數資料１９９敘述於ＵＣＰ資料１０６中，且指出展示模式中之內容的處理。使得Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３能根據部份揭示參數資料１９９播放部份揭示狀態中的加密內容資料Ｃ。作爲部份揭示技術，可用以下技術。藉著利用Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３處理單位預定區塊中之資料（信號），某些區塊藉著使用內容鑰匙資料Ｋｃ被解碼，且某些區塊依據部份揭示參數

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 86）

資料１９９沒有藉著使用內容鑰匙資料Ｋｃ被解碼。或者，限制展示模式中之播放功能，或限制傾聽用於展示之內容的周期。

決定下載安全容器之購買模式之處理

參見圖３７與３８，現在敘述ＳＡＭ１０５１之用於決定從內容提供者１０１下載至下載記憶體１６７之安全容器１０４的購買模式之處理。

在隨後處理中，決定安全容器１０４之購買模式時，安全容器１０４內的簽名資料沒有被證明（如上所述，當接收安全容器１０４時簽名資料被證明）。然而，可在決定購買模式時檢查簽名資料。

圖３８是一流程圖，指出決定從內容提供者１０１下載至下載記憶體１６７之安全容器１０４的購買模式之處理。

在步驟Ｓ３８－０中，圖３７所示的ＳＡＭ１０５１之ＣＰＵ１１００從主ＣＰＵ８１０接收指示ＳＡＭ１０５１決定內容的購買模式之內部中斷Ｓ８１０。

然後ＣＰＵ１１００在步驟Ｓ３８－１中決定是否來自主ＣＰＵ８１０之內部中斷Ｓ８１０指出展示模式，如果是的話，ＣＰＵ１１００執行步驟Ｓ３８－２之處理。如果不是的話，ＣＰＵ１１００執行Ｓ３８－５之處理。

在步驟Ｓ３８－２中，從工作記憶體２００讀取的部份揭示參數資料１９９及內容鑰匙資料Ｋｃ被輸出至圖

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（87）

２２所示之Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。同時，在執行ＳＡＭ１０５$_1$的相互證明單元１７０與Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３的相互證明單元２２０之間的相互證明之後，內容鑰匙資料Ｋｃ及部份揭示參數資料１９９藉著使用連續鑰匙資料K_{SES}被加密及解密。

在步驟Ｓ３８－３中，於接收指出來自主ＣＰＵ８１０之展示模式的內部中斷Ｓ８１０時，經由Ａ／Ｖ壓縮／解壓縮ＳＡＭ管理器１８４，ＣＰＵ１１００輸出儲存於下載記憶體１６７中之內容檔ＣＦ至圖２２所示之Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。

同時，進行下載記憶體１６７的媒體ＳＡＭ１６７ａ與相互證明單元１７０之間內容檔ＣＦ的相互證明，且內容檔ＣＦ以連續鑰匙資料K_{SES}被加密及解碼。又，執行相互證明單元１７０與相互證明單元２２０之間內容檔ＣＦ的相互證明，且內容檔ＣＦ以連續鑰匙資料K_{SES}被加密及解碼。

內容檔ＣＦ在圖２２所示之Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３的解碼器２２１中以連續鑰匙資料K_{SES}被解碼，然後被輸出至解碼器２２２。

然後，在步驟Ｓ３８－４中，解碼的部份揭示參數資料１９９被輸出至Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之部份揭示處理器２２５，在部份揭示處理器２２５的控制之下，解碼器２２２使用內容鑰匙資料Ｋｃ以部份揭示狀態解碼內容資料Ｃ。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 88）

部份揭示解碼的內容資料C在解壓縮單元223中被壓縮，且被輸出至數位水記資訊處理器224。

在數位水記資訊處理器224中，使用者數位資訊資料196被嵌入內容資料C，然後內容資料C在播放模組169中被播放，以輸出對應內容資料C之聲音。

數位水記資訊處理器224亦偵測嵌入於內容資料C中之數位水記資訊，並根據偵測結果決定是否應中斷處理。

在步驟S38－5中，當使用者藉著操作操作單元165而決定購買模式時，對應決定的購買模式之內部中斷S810從主CPU810被輸出至SAM1051。

隨後，在步驟S38－6中，SAM1051之會計處理器187依據決定的購買模式，產生使用登錄資料108及UCS資料166，且經由外部記憶體管理器811將使用登錄資料108寫至外部記憶體201，亦將UCS資料166寫至工作記憶體200。

隨後，使用監視器186控制（監視）狀態，以確定內容之購買與使用被控制在UCS資料166所允許的條件內。

在步驟S38－7中，產生以下討論之圖39C所示的新鑰匙檔KF_1，且新鑰匙檔KF_1經由下載記憶體管理器182被儲存於下載記憶體167或另一記憶體。

儲存於鑰匙檔KF_1中之UCS資料166，藉著利用DES之CBC模式，以儲存鑰匙資料K_{STR}與媒體鑰匙

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 89）

資料K_{MED}被加密，如圖３９Ｃ所示。

儲存鑰匙資料K_{STR}是由機器之型式決定的資料，例如超音頻光碟（ＳＡＣＤ）機器，數位影音光碟（ＤＶＤ）機器，光碟機（ＣＲ－Ｒ），或迷你碟（ＭＤ）機器，且儲存鑰匙資料K_{STR}被使用於對應一種型式的機器至一種型式的記錄媒體。媒體鑰匙資料K_{MED}是記錄媒體之獨特資料。

在步驟Ｓ３８－８中，於簽名處理器１８９中，藉著使用ＳＡＭ１０５$_1$之私人鑰匙資料$K_{SAM1,S}$產生雜亂值H_{K1}，且此雜亂值H_{K1}被寫入工作記憶體２００，對應鑰匙檔KF_1。雜亂值H_{K1}用於證明鑰匙檔KF_1的完整性及鑰匙檔KF_1之產生者的辨識。

線上或經由記錄媒體決定購買模式，於送出內容資料Ｃ時，產生安全容器１０４ｐ，如圖３９Ａ與３９Ｄ所示，其儲存鑰匙檔KF_1與雜亂值H_{K1}，內容檔ＣＦ與簽名資料$SIG_{6,CP}$，鑰匙檔ＫＦ與簽名資料$SIG_{7,CP}$，公開－鑰匙證明資料CER_{CP}與簽名資料$SIG_{1,ESC}$，公開－鑰匙證明資料CER_{CP}與簽名資料$SIG_{22,ESC}$。

如上所討論，於決定安全容器１０４之購買模式時，ＵＣＳ資料１６６被產生並儲存於工作記憶體２００中。如果相同安全容器１０４ｐ之購買模式在ＳＡＭ１０５$_1$中被再決定，儲存於工作記憶體２００中之ＵＣＳ資料１６６依據外部中斷（操作信號）Ｓ１６５被更新。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 90）

然後，在步驟Ｓ３８－９中，ＣＰＵ１１００檢查是否上述購買模式決定處理已被正確地執行，並將對應的資訊經由外部中斷報告至主ＣＰＵ８１０。

另一種方式，ＣＰＵ１１００可設定一旗標於ＳＡＭ狀態暫存器中，指出是否上述購買模式決定處理已被正確地執行，在此情形中，主ＣＰＵ８１０藉著投票讀取旗標。

內容資料之播放處理

以下參見圖４０敘述播放儲存於下載記憶體１６７中的內容資料Ｃ之處理，對於內容資料Ｃ決定購買模式。

執行此處理，假設藉著前述購買模式決定處理，ＵＣＳ資料１６６被儲存於工作記憶體２００中。

在步驟Ｓ４０－０中，圖３７所示之ＳＡＭ１０５１的ＣＰＵ１１００接收內部中斷Ｓ８１０，指出從主ＣＰＵ８１０播放內容之指示。

在步驟Ｓ４０－１中，ＵＣＳ資料１６６從工作記憶體２００被讀取至使用監視器１８６，且使用監視器１８６中斷並證明ＵＣＳ資料１６６中所述之播放條件，並監視狀態使得隨後的播放操作根據ＵＣＳ資料１６６被執行。

然後，在步驟Ｓ４０－２中，執行圖３７所示的相互證明單元１７０與圖２２所示的Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之間的相互證明，且連續鑰匙資料K_{SES}被

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 91）

分享。

在步驟Ｓ４０－３中，步驟Ｓ４０－１之中斷與證明的播放條件，及從工作記憶體２００讀取的內容鑰匙資料Ｋｃ，藉著使用步驟Ｓ４０－２中所得到的連續鑰匙資料K_{SES}被加密，且被輸出至Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。

因此，在圖２２所示之Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３的解碼器２２１中，以連續鑰匙資料K_{SES}解碼播放條件與內容鑰匙資料Ｋｃ。

隨後，在步驟Ｓ４０－４中，從下載記憶體１６７讀取的內容檔ＣＦ，藉著使用連續鑰匙資料K_{SES}被加密，然後被輸出至Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。

因此，在Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３的解碼器２２１中，以連續鑰匙資料K_{SES}解碼內容檔ＣＦ。隨後，內容檔ＣＦ內的內容資料Ｃ在Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３的解壓縮單元２２３中被解壓縮，且使用者數位水記資訊在數位水記資訊處理器２２４中被嵌入解壓縮的內容資料Ｃ中。然後，內容資料Ｃ在播放模組１６９中被播放。

在步驟Ｓ４０－５中，如果需要的話，步驟Ｓ４０－１中讀取的ＵＣＳ資料１６６被更新，且ＵＣＳ資料１６６再度被寫入工作記憶體２００。儲存於外部記憶體２０１中之使用登錄資料１０８被更新。

然後ＣＰＵ１１００在步驟Ｓ４０－６中決定是否內

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（92）

容播放處理已被正確地執行，並經由外部中斷報告結果至主ＣＰＵ８１０。

另一種方式，ＣＰＵ１１００可設定一旗標於ＳＡＭ狀態暫存器中，指出是否內容播放處理已被正確地執行，且主ＣＰＵ８１０可藉著投票讀取旗標。

當一機器之ＵＣＳ資料１６６被用於重新購買另一機器中之內容時所執行之處理

在決定下載進入網路裝置160_1的下載記憶體１６７之內容檔ＣＦ的購買模式之後，如圖４１所示，儲存內容檔ＣＦ之新的安全容器１０４ｘ被產生，且經由匯流排１９１被轉移至網路裝置160_2之$SAM105_2$。參見圖４２與４３，以下討論在上述操作中，欲在$SAM105_1$中被執行之處理。

執行圖４３所示之處理，假設圖４４Ｃ所示之雜亂值H_{K1}與鑰匙檔KF_1藉著上述購買處理，被儲存於$SAM105_1$之工作記憶體２００中。

在步驟Ｓ４３－１中，依據操作單元１６５上執行之使用者操作，圖４２所示之$SAM105_1$的ＣＰＵ１１００接收內部中斷Ｓ８１０，指出轉移安全容器１０４ｘ至$SAM105_2$之指示，對於安全容器１０４ｘ決定購買模式。因此，會計處理器１８７更新儲存於外部記憶體２０１中之使用登錄資料１０８。

然後，在步驟Ｓ４３－２中，$SAM105_1$檢查

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（93）

ＳＡＭ登記列表，討論於下，以證明ＳＡＭ１０５$_2$之正式登記，ＳＡＭ１０５$_2$是欲接收安全容器１０４ｘ。如果是的話，ＳＡＭ１０５$_1$執行步驟Ｓ４３－３之處理。ＳＡＭ１０５$_1$亦決定是否ＳＡＭ１０５$_2$是家庭網路內的ＳＡＭ。

在步驟Ｓ４３－３中，相互證明單元１７０分享在以ＳＡＭ１０５$_2$執行相互證明之後所得到的連續鑰匙資料K_{SES}被。

在步驟Ｓ４３－４中，ＳＡＭ管理器１９０從下載記憶體２１１讀取圖３９Ａ所示之內容檔ＣＦ與簽名資料$SIG_{6,CP}$，並控制簽名處理器１８９以藉著使用ＳＡＭ１０５$_1$之私人鑰匙資料K_{SAM1}而產生簽名資料$_{41,SAM1}$。

然後，在步驟Ｓ４３－５中，ＳＡＭ管理器１９０從下載記憶體２１１讀取圖３９Ｂ所示之簽名資料$_{7,CP}$與鑰匙檔ＫＦ，並藉著使用ＳＡＭ１０５$_1$之私人鑰匙資料K_{SAM1}，控制簽名處理器１８９以產生簽名資料$SIG_{42,SAM1}$。

隨後，在步驟Ｓ４３－６中，ＳＡＭ管理器１９０產生圖４４Ａ、４４Ｂ與４４Ｃ所示之安全容器１０４ｘ。

在步驟Ｓ４３－７中，於加密／解密（解碼）單元１７１中，以步驟Ｓ４３－３中所得到的連續鑰匙資料K_{SES}加密安全容器１０４ｘ。

隨後，在步驟Ｓ４３－８中，ＳＡＭ管理器１９０輸

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 94）

出安全容器１０４ｘ至圖４１所示的網路裝置１６０$_2$之ＳＡＭ１０５$_2$。在此情形中，和ＳＡＭ１０５$_1$與ＳＡＭ１０５$_2$之間的相互證明同時，執行ＩＥＥＥ－１３９４匯流排１９１之相互證明。

然後，在步驟Ｓ４３－９中，ＣＰＵ１１００決定是否決定購買模式之安全容器１０４ｘ已被正確地轉移至ＳＡＭ１０５$_2$，並經由外部中斷報告結果至主ＣＰＵ８１０。

另一種方式，ＣＰＵ１１００可設定一旗標於ＳＡＭ狀態暫存器中，指出是否安全容器１０４ｘ已被正確地轉移至ＳＡＭ１０５$_2$，且主ＣＰＵ８１０可藉著投票讀取旗標。

參見圖４５、４６與４７，現在敘述當從ＳＡＭ１０５$_1$接收之圖４４Ａ至４４Ｄ所示的安全容器１０４ｘ被寫入記錄媒體（ＲＡＭ）１３０$_4$（圖１４）時，如圖４１所示，ＳＡＭ１０５$_2$內執行的處理。

圖４６與４７是一流程圖，指出上述處理。

如圖１４與４１所示，記錄媒體（ＲＡＭ）１３０$_4$具有不安全ＲＡＭ區域１３４、媒體ＳＡＭ１３３及安全ＲＡＭ區域１３２。

參見圖４６，在步驟Ｓ４６－０中，圖４５所示之ＣＰＵ１１００從圖４１所示之網路裝置１６０$_2$之主ＣＰＵ８１０，接收內部中斷Ｓ８１０，指出從網路裝置１６０$_1$接收安全容器１０４ｘ之指示。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 95）

在步驟Ｓ４６－１中，ＳＡＭ１０５$_2$檢查ＳＡＭ登記列表以決定是否送出安全容器１０４ｘ之ＳＡＭ１０５$_1$被正式登記。如果是的話，ＳＡＭ１０５$_2$執行步驟Ｓ４６－２之處理。ＳＡＭ１０５$_2$亦檢查是否ＳＡＭ１０５$_1$是家庭網路內之ＳＡＭ。

響應圖４３所示之上述步驟Ｓ４３－３之處理，ＳＡＭ１０５$_2$分享藉由以ＳＡＭ１０５$_1$執行相互證明所得到的連續鑰匙資料K_{SES}。

在步驟Ｓ４６－３中，如圖４１與４５所示，ＳＡＭ１０５$_2$之ＳＡＭ管理器１９０從網路裝置１６０$_1$之ＳＡＭ１０５$_1$接收安全容器１０４ｘ。

在步驟Ｓ４６－４中，ＳＡＭ１０５$_2$之加密／解密（解碼）單元１７１，藉著使用步驟Ｓ４６－２中所得到的連續鑰匙資料K_{SES}，解碼經由ＳＡＭ管理器１９０接收之安全容器１０４ｘ。

然後，步驟Ｓ４６－５中，由連續鑰匙資料K_{SES}解碼之安全容器１０４ｘ內的內容檔ＣＦ，進行圖４５所示之媒體驅動ＳＡＭ管理器８５５中之處理，例如區格化，加入區格標頭，擾頻，錯誤更正碼（ＥＣＣ）編碼，調變，及同步化，然後被儲存於記錄媒體（ＲＡＭ）１３０$_4$之ＲＡＭ區域１３４中。

在步驟Ｓ４６－６中，簽名資料$SIG_{6,CP}$與$SIG_{41,SAM1}$，鑰匙檔ＫＦ與簽名資料$SIG_{7,CP}$及$SIG_{42,SAM1}$，及鑰匙檔KF_1與其雜亂值H_{K1}，公開

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（96）

鑰匙簽名資料CER_{CP}與其簽名資料$SIG_{1,ESC}$，及安全容器104x內之公開鑰匙簽名資料CER_{SAM1}與簽名資料$SIG_{22,ESC}$，均以連續鑰匙資料K_{SES}被解碼，被寫入工作記憶體200。

隨後，在步驟S46－7中，簽名處理器189藉著使用從儲存單元192讀取的私人鑰匙資料$K_{CP,P}$，證明公開－鑰匙證明資料CER_{CP}與CER_{SAM1}之完整性。簽名處理器189亦藉著使用儲存於公開－鑰匙證明資料CER_{SAM1}中之公開鑰匙資料$K_{CP,P}$，檢查簽名資料$SIG_{6,CP}$之完整性，以證明內容檔CF之產生者的完整性。簽名處理器189亦藉著使用儲存於公開－鑰匙證明資料CER_{SAM1}中之公開鑰匙資料$K_{SAM1,P}$，檢查簽名資料$SIG_{41,SAM1}$之完整性，以證明內容檔CF之送出者的完整性。

在步驟S46－8中，簽名處理器189藉著使用公開鑰匙資料$K_{CP,P}$與$K_{SAM1,P}$，檢查儲存於工作記憶體200中之簽名資料$SIG_{7,CP}$與$SIG_{42,SAM1}$之完整性，以證明鑰匙檔KF之送出者的完整性。

此外，在步驟S46－9中，簽名處理器189藉著使用從192讀取的公開鑰匙資料$K_{ESC,P}$，檢查儲存於圖44B所示的鑰匙檔KF中之簽名資料$SIG_{K1,ESC}$之完整性，以證明鑰匙檔KF之產生者的完整性。

參見圖47，在步驟S46－10中，簽名處理器189檢查雜亂值H_{K1}之完整性，以證明鑰匙檔KF_1送

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（97）

出者與產生者之完整性。

在此例子中，鑰匙檔ＫＦ$_1$之送出者與產生者是相同的。然而，如果它們是不同的，產生者與送出者之簽名資料被產生，且簽名處理器１８９證明兩個簽名資料之完整性。

在步驟Ｓ４６－１１中，使用監視器１８６控制內容資料Ｃ之購買與使用模式，藉著使用步驟Ｓ４６－１０中解碼的鑰匙檔ＫＦ$_1$中儲存之ＵＣＳ資料１６６。

在步驟Ｓ４６－１２中，於使用者藉著操作操作單元１６５決定購買模式時，ＳＡＭ１０５$_2$之ＣＰＵ１１００接收對應的內部中斷Ｓ８１０。

在步驟Ｓ４６－１３中，會計處理器１８７在ＣＰＵ１１００控制下，更新儲存於外部記憶體２０１中之使用登錄資料１０８。每次決定內容資料之購買模式時，會計處理器１８７亦更新ＵＣＳ資料１６６。在此情形中，丟棄送出者ＳＡＭ之ＵＣＳ資料１６６。

然後，在步驟Ｓ４６－１４中，ＳＡＭ１０５$_2$之加密／解密（解碼）單元１７３加密步驟Ｓ４６－１２產生的ＵＣＳ資料１６６，藉著依序地使用儲存鑰匙資料K_{STR}，媒體鑰匙資料K_{MED}及從儲存單元１９２讀取的購買鑰匙資料K_{PIN}，並輸出加密的ＵＣＳ資料１６６至媒體驅動ＳＡＭ管理器８５５。

在步驟Ｓ４６－１５中，媒體驅動ＳＡＭ管理器８５５執行處理於具有更新的ＵＣＳ資料１６６之鑰匙檔

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（98）

KF_1上，例如區格化，加入區格標頭，擾頻，錯誤更正碼（ECC）編碼，調變，及同步化，並將它儲存於記錄媒體（RAM）130_4之安全RAM區域132中。

藉著圖45所示之$SAM105_2$的相互證明單元170與圖41所示之記錄媒體（RAM）130_4的媒體SAM133之間的相互證明，媒體鑰匙資料K_{MED}已被儲存於儲存單元192中。

儲存鑰匙資料K_{STR}是由機器（在此例子爲網路裝置160_2）之型式決定的資料，例如SACD機器，DVD機器，光碟機（CR－R），或MD機器，且儲存鑰匙資料K_{STR}被使用於對應一種型式的機器至一種型式的記錄媒體。SACD與DVD具有相同的碟媒體之實體構造。因此，藉著使用DVD機器，SACD上之資料可被記錄及播放，在此情形中，儲存鑰匙資料K_{STR}作爲避免非法拷貝之功能。在此實施例中，不能執行使用儲存鑰匙資料K_{STR}之加密。

媒體鑰匙資料K_{MED}是記錄媒體（在此例子中爲記錄媒體（RAM）130_4）之獨特資料。

媒體鑰匙資料K_{MED}被儲存於記錄媒體（在此例子中爲圖41所示之記錄媒體（RAM）130_4），且以安全的觀點來看最好藉著使用記錄媒體之媒體SAM中的媒體鑰匙資料K_{MED}執行加密與解密。在此情形中，如果記錄媒體設有媒體SAM，媒體鑰匙資料K_{MED}被儲存於媒體SAM中，且如果不是的話，媒體鑰匙資料K_{MED}被儲存

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 99）

於ＲＡＭ區域中，亦即主ＣＰＵ８１０之控制外的區域（未示）。

此實施例中，在ＳＡＭ１０５$_2$與媒體ＳＡＭ（在此例子中爲媒體ＳＡＭ１３３）之間可執行相互證明，然後經由安全通訊路徑，媒體鑰匙資料K_{MED}可被轉移至ＳＡＭ１０５$_2$，且藉著使用媒體鑰匙資料K_{MED}，可在ＳＡＭ１０５$_2$中執行加密與解密。

在此實施例中，可使用儲存鑰匙資料K_{STR}與媒體鑰匙資料K_{MED}，以保護記錄媒體之實體層的安全性。

購買者鑰匙資料K_{PIN}是資料，指出內容檔ＣＦ之購買者，如果是以”賣斷”模式購買內容，購買者鑰匙資料K_{PIN}從ＥＭＤ服務中心１０２被指定給使用者。由ＥＭＤ服務中心１０２管理購買者鑰匙資料K_{PIN}。

在步驟Ｓ４６－１６中，從工作記憶體２００讀取鑰匙檔ＫＦ，且鑰匙檔ＫＦ經由媒體驅動ＳＡＭ管理器８５５被圖４１所示之媒體驅動ＳＡＭ２６０寫入記錄媒體（ＲＡＭ）１３０$_4$之安全ＲＡＭ區域１３２。

在步驟Ｓ４６－１７中，ＳＡＭ１０５$_2$之ＣＰＵ１１００經由外部中斷，報告接收的安全容器１０４ｘ之處理的結果至主ＣＰＵ８１０。

另一種方式，ＣＰＵ１１００可設定一旗標於ＳＡＭ狀態暫存器中，指出是否上述處理已被正確地執行，且主ＣＰＵ８１０可藉投票讀取旗標。

在上述實施例中，鑰匙檔ＫＦ與K_{F1}經由媒體驅動

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 109

ＳＡＭ２６０被記錄在記錄媒體（ＲＡＭ）１３０$_4$之安全ＲＡＭ區域１３２上。然而，鑰匙檔ＫＦ與ＫＦ$_1$可從ＳＡＭ１０５$_2$被記錄在媒體ＳＡＭ１３３上，如圖４１之虛線所示。

在前述實施例中，安全容器１０４ｘ從ＳＡＭ１０５$_1$被送至ＳＡＭ１０５$_2$。然而，在Ａ／Ｖ機器１０６$_2$與網路裝置１０６$_1$之主ＣＰＵ的控制下，內容檔ＣＦ與ＵＣＰ資料１０６可從１６０$_1$被送至Ａ／Ｖ機器１０６$_2$。

作爲上述實施例之修改，在ＳＡＭ１０５$_1$中決定購買模式，且ＳＡＭ１０５$_2$使用ＵＣＳ資料１６６，而不決定購買模式。在此情形中，使用登錄資料１０８只產生於ＳＡＭ１０５$_1$中，並不產生於ＳＡＭ１０５$_2$中。

購買內容資料Ｃ時，例如可購買由許多內容資料Ｃ組成之簿子。在此情形中，可由不同的內容提供者１０１提供內容資料Ｃ（在第二實施例中，討論如下，可由不同的服務提供者３１０提供內容資料Ｃ）。另一種方式，形成簿子之內容資料Ｃ可被啓始地購買，後來可逐漸地購買其餘的內容資料Ｃ。結果，購買整個簿子。

圖４８指出內容資料Ｃ之不同購買模式之例子。

網路裝置１６０$_1$購買內容資料Ｃ，其藉著使用ＵＣＰ資料１０６從內容提供者１０１被接收，並產生ＵＣＳ資料１６６ａ。

類似地，Ａ／Ｖ機器１６０$_2$購買內容資料Ｃ，其藉著使用ＵＣＰ資料１０６從內容提供者１０１被接收至網路

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 101）

裝置１６０₁，並產生ＵＣＳ資料１６６ｂ。

Ａ／Ｖ機器１６０₃拷貝由Ａ／Ｖ機器１６０₂購買之內容資料Ｃ，並藉著使用產生於Ａ／Ｖ機器１６０₂中之ＵＣＳ資料１６６ｂ決定使用模式。結果，在Ａ／Ｖ機器１６０₃中產生ＵＣＳ資料１６６ｃ。Ａ／Ｖ機器１６０₃亦從ＵＣＳ資料１６６ｃ產生使用登錄資料１０８ｂ。

網路裝置１６０₄接收內容資料Ｃ，其從內容提供者１０１已被接收至網路裝置１６０₁且決定網路裝置１６０₁中之購買模式，然後藉著使用由網路裝置１６０₁產生的ＵＣＳ資料１６６決定購買模式。結果，ＵＣＳ資料１６６ａ被產生於Ａ／Ｖ機器１６０₄中，且使用登錄資料１０８ａ亦從ＵＣＳ資料１６６ａ被產生。

ＵＣＳ資料１６６ａ、１６６ｂ與１６６ｃ分別在Ａ／Ｖ機器１６０₄、１６０₂與１６０₃中被加密，藉著使用機器之獨特的儲存鑰匙資料K_{STR}與記錄媒體之獨特的媒體鑰匙資料K_{MED}，且被記錄在對應的記錄媒體上。

在此實施例中，使用者對於內容資料Ｃ給付執照權利而非財產權利。內容資料的拷貝有助於內容的提升，且以加速銷售之觀點來看滿足內容資料之權利擁有者的要求。

決定記錄媒體（ＲＯＭ）上的內容資料之購買模式的處理

如圖４９所示，圖１１所示之記錄媒體（ＲＡＭ）１３０₁儲存內容且購買模式仍未被決定，記錄媒體（ＲＡＭ）１３０₁經由使用者家庭網路１０３被離線分布至

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 102）

Ａ／Ｖ機器１６０$_2$，且Ａ／Ｖ機器１６０$_2$決定購買模式。參見圖５０與５１，以下討論此處理。

參見圖５１，在步驟Ｓ５１－０中，依據操作單元１６５上執行的使用者操作，圖５０所示之ＳＡＭ１０５$_2$的ＣＰＵ１１００，經由記錄媒體（ＲＯＭ）接收內部中斷Ｓ８１０，指出決定分布的內容之購買模式的指令。

在步驟Ｓ５１－１中，於執行圖５０所示的相互證明單元１７０與圖１１所示之記錄媒體（ＲＡＭ）１３０$_1$的媒體ＳＡＭ１３３之間的相互證明之後，ＳＡＭ１０５$_2$從媒體ＳＡＭ１３３接收媒體鑰匙資料K_{MED}。如果ＳＡＭ１０５$_2$已具有媒體鑰匙資料K_{MED}儲存於其中，不需要接收媒體鑰匙資料K_{MED}。

然後，在步驟Ｓ５１－２中，儲存於記錄在記錄媒體（ＲＡＭ）１３０$_1$之安全ＲＡＭ區域１３２上的安全容器１０４中，鑰匙檔ＫＦ與其簽名資料$SIG_{7,CP}$，及公開－鑰匙證明資料CER_{CP}與簽名資料$SIG_{1,ESC}$，如圖３Ｂ與３Ｃ所示，經由媒體驅動ＳＡＭ管理器８５５被寫入工作記憶體２００。

在步驟Ｓ５１－３中，於證明簽名資料$SIG_{1,ESC}$的完整性之後，簽名處理器１８９從公開－鑰匙證明資料CER_{CP}取出公開鑰匙資料$K_{CP,P}$，並藉著使用公開鑰匙資料$K_{CP,P}$證明簽名資料$SIG_{7,CP}$亦即鑰匙檔ＫＦ之送出者的完整性。

簽名處理器１８９亦藉著使用從儲存單元１９２讀取

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 103）

的公開鑰匙資料$K_{ESC,P}$，證明儲存於鑰匙檔ＫＦ中之簽名資料$SIG_{K1,ESC}$亦即鑰匙檔ＫＦ之產生者的完整性。

隨後，在步驟Ｓ５１－４中，於證明簽名處理器１８９中的$SIG_{K1,ESC}$與簽名資料$SIG_{7,CP}$的完整性之後，鑰匙檔ＫＦ從工作記憶體２００被讀取，且被寫入加密／解密（解碼）單元１７２。

然後，加密／解密（解碼）單元１７２藉著使用對應周期之執照鑰匙資料KD_1至KD_3，解密（解碼）內容鑰匙資料Ｋｃ，ＵＣＰ資料１０６，及儲存於鑰匙檔ＫＦ中之ＳＡＭ程式下載容器SDC_1至SDC_3，並將它們寫入工作記憶體２００。

在步驟Ｓ５１－５中，於進行圖５０所示的相互證明單元１７０與圖４９所示的Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之間的相互證明之後，$SAM105_2$之Ａ／Ｖ壓縮／解壓縮ＳＡＭ管理器１８４從記錄媒體（ＲＯＭ）130_1之ＲＯＭ區域１３１，輸出儲存於工作記憶體２００中之內容鑰匙資料Ｋｃ，儲存於ＵＣＰ資料１０６中之部份揭示參數資料１９９，及儲存於內容檔ＣＦ中之內容資料Ｃ，至圖４９所示之Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。

然後，Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３藉著使用內容鑰匙資料Ｋｃ，解碼及解壓縮部份揭示模式之內容資料Ｃ，並將它輸出至播放模組２７０。然後內容資料Ｃ在播

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 104）

放模組２７０中被播放。

隨後，在步驟Ｓ５１－６中，依據圖４９所示之操作單元１６５的使用者操作，決定內容之購買模式，且指出決定的購買模式之內部中斷Ｓ８１０被輸出至ＳＡＭ１０５$_2$ＣＰＵ１１００。

在步驟Ｓ５１－７中，會計處理器１８７依據操作信號Ｓ１６５產生ＵＣＳ資料１６６，並將它寫入工作記憶體２００。

在步驟Ｓ５１－８中，內容鑰匙資料Ｋ$_C$與ＵＣＳ資料１６６從工作記憶體２００被輸出至加密／解密（解碼）單元１７３。

然後加密／解密（解碼）單元１７３依序地加密內容鑰匙資料Ｋ$_C$與ＵＣＳ資料１６６，藉著使用儲存鑰匙資料Ｋ$_{STR}$，媒體鑰匙資料Ｋ$_{MED}$，及從儲存單元１９２讀取的購買者鑰匙資料Ｋ$_{PIN}$，並將它們寫入工作記憶體２００。

在步驟Ｓ５１－９中，媒體ＳＡＭ管理器１９７從內容鑰匙資料Ｋ$_C$，ＵＣＳ資料１６６及由工作記憶體２００讀取的ＳＡＭ程式下載容器ＳＤＣ$_1$至ＳＤＣ$_3$，產生圖４４Ｃ所示之鑰匙檔ＫＦ$_1$。

在簽名處理器１８９中，圖４４Ｃ所示之鑰匙檔ＫＦ$_1$的雜亂值Ｈ$_{K1}$被產生，且被輸出至媒體驅動ＳＡＭ管理器８５５。

於進行圖５０所示的相互證明單元１７０與圖４９所

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 105

示的媒體ＳＡＭ１３３之間的相互證明之後，媒體驅動ＳＡＭ管理器８５５經由圖４９所示的媒體驅動ＳＡＭ２６０，將鑰匙檔ＫＦ$_1$與雜亂值Ｈ$_{K1}$寫入記錄媒體（ＲＯＭ）１３０$_1$安全ＲＡＭ區域１３２。結果得到決定購買模式之記錄媒體１３０$_1$。

同時，由會計處理器１８７產生的使用登錄資料１０８與ＵＣＳ資料１６６，分別從外部記憶體２０１與工作記憶體２００被送至ＥＭＤ服務中心１０２。

如果鑰匙檔ＫＦ被儲存於記錄媒體（ＲＯＭ）１３０$_1$之媒體ＳＡＭ１３３中，ＳＡＭ１０５$_2$從媒體ＳＡＭ１３３接收產生的鑰匙檔ＫＦ$_1$，如圖４９之虛線所示。在此情形中，ＳＡＭ１０５$_2$將產生的鑰匙檔ＫＦ$_1$寫入媒體ＳＡＭ１３３。

在步驟Ｓ５１－１０中，ＳＡＭ１０５$_2$之ＣＰＵ１１００決定是否決定經由上述記錄媒體（ＲＯＭ）分布的內容之購買模式的處理已被正確地執行，並將結果經由外部中斷報告至主ＣＰＵ８１０。

另一種方式，ＣＰＵ１１００可設定一旗標於ＳＡＭ狀態暫存器中，指出是否上述處理已被正確地執行，且主ＣＰＵ８１０可藉投票讀取旗標。

<u>於已決定記錄媒體（ＲＯＭ）中之內容資料的購買模式之後，用於將內容資料寫入記錄媒體（ＲＡＭ）之處理</u>

如圖５２所示，購買模式仍未被決定之安全容器

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 10θ

１０４，從記錄媒體（ＲＯＭ）１３０₁被讀取，且新的安全容器１０４ｙ被產生於Ａ／Ｖ機器１６０₃中並被轉移至Ａ／Ｖ機器１６０₂。安全容器１０４ｙ之購買模式被決定於Ａ／Ｖ機器１６０₂中，且安全容器１０４ｙ被寫入記錄媒體（ＲＡＭ）１３０₅。參見圖５３、５４與５５，以下敘述此處理之流程。

應注意安全容器１０４ｙ從記錄媒體（ＲＯＭ）１３０₁至記錄媒體（ＲＡＭ）１３０₅之轉移，可在網路裝置１６０₁與圖１所示的Ａ／Ｖ機器１６０₂至１６０₄之間被執行。

參見圖５５之流程圖，在步驟Ｓ５５－０中，依據在操作單元１６５上執行的使用者操作，圖５３所示之ＣＰＵ１１００接收指出轉移安全容器１０４之指示的內部中斷Ｓ８１０，安全容器１０４之購買模式仍未被決定，且從記錄媒體（ＲＯＭ）１３０₁被讀至ＳＡＭ１０５₂。

在步驟Ｓ５５－１中，ＳＡＭ１０５₁檢查ＳＡＭ登記列表，以決定是否欲接數安全容器之ＳＡＭ１０５₂被非正式地登記。如果是的話，ＳＡＭ１０５₃執行步驟Ｓ５５－２之處理。ＳＡＭ１０５₃亦檢查是否ＳＡＭ１０５₂是家庭網路內的ＳＡＭ。

然後，在步驟Ｓ５５－２中，執行ＳＡＭ１０５₃與ＳＡＭ１０５₂之間的相互證明，以分享連續鑰匙資料K_{SES}。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（107）

在步驟S55－3中，進行A／V機器1603的SAM1053與記錄媒體（ROM）1301的媒體SAM1331之間的相互證明，且記錄媒體1301之媒體鑰匙資料K_{MED1}被轉移至SAM1053。

如果在記錄媒體（ROM）1301之媒體SAM1331中執行使用媒體鑰匙資料K_{MED1}之加密，媒體鑰匙資料K_{MED1}沒有被轉移至SAM1053。

然後，在步驟S55－4中，執行A／V機器1602的SAM1052與記錄媒體（RAM）1305的媒體SAM1335之間的相互證明，且記錄媒體1305之媒體鑰匙資料K_{MED2}被轉移至SAM1052。

如果在記錄媒體（RAM）1305之媒體SAM1335中執行使用媒體鑰匙資料K_{MED2}之加密，媒體鑰匙資料K_{MED2}沒有被轉移至SAM1052。

在步驟S55－5中，如圖53所示，SAM1053經由媒體驅動SAM管理器855，從記錄媒體（ROM）1301之ROM區域131讀取內容檔CF與簽名資料$SIG_{6,CP}$，並將它們輸出至SAM管理器190，且亦藉著使用私人鑰匙資料$K_{SAM3,S}$控制簽名處理器189以產生簽名資料$SIG_{350,SAM3}$。

在步驟S55－6中，如圖53所示，SAM1053經由媒體驅動SAM管理器855，從記錄媒體（ROM）1301之安全RAM區域132讀取鑰匙檔KF與簽名資料$SIG_{7,CP}$，並將它們輸出至SAM管理器190，

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 108）

且亦藉著使用私人鑰匙資料$K_{SAM3,S}$控制簽名處理器189以產生簽名資料$SIG_{352,SAM3}$。

然後，在步驟S55－7中，於SAM105_3中，從儲存單元192讀取公開－鑰匙證明資料CER_{SAM3}與簽名資料$SIG_{315,ESC}$至SAM管理器190。

在步驟S55－8中，在例如SAM105_3的SAM管理器190中，產生圖54A至54D所示之安全容器104y。

在步驟S55－9中，SAM105_3之加密／解密（解碼）單元171，藉著使用步驟S55－2所得到的連續鑰匙資料K_{SES}，加密安全容器104y。

隨後，在步驟S55－10中，安全容器104y從SAM105_3的SAM管理器190被送至A／V機器160_2。

然後，SAM105_3之CPU1100決定是否上述處理已被適當地執行，並經由外部中斷報告結果至主CPU810。

另一種方式，CPU1100可設定一旗標於SAM狀態暫存器中，指出是否上述處理已被適當地執行，且主CPU810可藉投票讀取旗標。

在SAM105_2中，於CPU1100的控制之下，依據來自主CPU810之內部中斷S810，如圖57所示，經由SAM管理器190從SAM105_3輸入的圖54A至54D所示之安全容器104y，在加密／解密

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 109

（解碼）單元１７１中被解碼，藉著使用連續鑰匙資料K_{SES}。

然後，在步驟Ｓ５５－１１中，鑰匙檔ＫＦ與簽名資料$SIG_{7,CP}$和$SIG_{350,SAM3}$，公開－鑰匙證明資料CER_{SAM3}與簽名資料$SIG_{351,ESC}$，及安全容器１０４ｙ內的簽名資料$SIG_{1,ESC}$與公開－鑰匙證明資料CER_{CP}，被寫入工作記憶體２００。

在步驟Ｓ５５－１２中，$SAM105_2$之簽名處理器１８９證明儲存於安全容器１０４ｙ中之簽名資料$SIG_{6,CP}$與$SIG_{350,SAM3}$，亦即內容檔ＣＦ之產生者與送出者的完整性。

然後，在步驟Ｓ５５－１３中，內容檔ＣＦ經由媒體驅動ＳＡＭ管理器８５５被寫入記錄媒體（ＲＯＭ）130_5之ＲＡＭ區域１３４。在主ＣＰＵ８１０的控制之下，內容檔ＣＦ可被直接寫入記錄媒體（ＲＯＭ）130_5之ＲＡＭ區域１３４不需要$SAM105_2$。

隨後，在步驟Ｓ５５－１４中，簽名處理器１８９檢查簽名資料$SIG_{351,ECS}$之簽名，以證明公開－鑰匙證明資料CER_{SAM3}之完整性，然後證明簽名資料$SIG_{7,CP}$與簽名資料$SIG_{352,SAM3}$與$SIG_{K1,ESC}$之完整性，亦即鑰匙檔ＫＦ之產生者與送出者的完整性，藉著使用儲存於公開－鑰匙證明資料CER_{SAM3}中之公開鑰匙資料K_{SAM3}與公開鑰匙資料$K_{ESC,P}$。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 110

隨後，在步驟Ｓ５５－１５中，鑰匙檔ＫＦ從工作記憶體２００被讀入加密／解密（解碼）單元１７２，且以執照鑰匙資料ＫＤ1至ＫＤ3被解碼，並再度被寫入工作記憶體２００。

在步驟Ｓ５５－１６中，儲存於工作記憶體２００中之解碼鑰匙檔ＫＦ的ＵＣＰ資料１０６被輸出至使用監視器１８６。然後，購買模式與使用模式根據ＵＣＰ資料１０６在使用監視器１８６中被管理（監視）。

在步驟Ｓ５５－１７中，藉著圖５２所示之操作單元１６５上的使用者操作，決定內容之購買與使用模式，且對應的內部中斷Ｓ８１０被輸出至ＳＡＭ１０５2之ＣＰＵ１１００。

在步驟Ｓ５５－１８中，ＵＣＳ資料１６６與使用登錄資料１０８，根據決定的購買與使用模式，被產生於會計處理器１８７中，且被分別寫入工作記憶體２００與外部記憶體２０１。ＵＣＳ資料１６６與使用登錄資料１０８被適當地送至ＥＭＤ服務中心１０２。

然後，在步驟Ｓ５５－１９中，內容鑰匙Ｋc與ＵＣＳ資料１６６從工作記憶體２００被讀至加密／解密（解碼）單元１７３，且被依序地加密，藉著使用儲存鑰匙資料KSTR，媒體鑰匙資料KMED2，及從儲存單元１９２讀取的購買者鑰匙資料KPIN。然後加密的資料被輸出至媒體ＳＡＭ管理器１９７。鑰匙檔ＫＦ亦從工作記憶體２００被輸出至媒體ＳＡＭ管理器１９７。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 111）

在步驟S55－20中，圖44C所示的鑰匙檔KF$_1$被產生於媒體SAM管理器197中，且經由媒體SAM管理器197被寫入記錄媒體（RAM）1305之媒體SAM1335。鑰匙檔KF亦經由媒體SAM管理器197被寫入記錄媒體（RAM）1305之媒體SAM1335。

在步驟S55－21中，SAM1052之CPU1100決定是否上述處理已被精確地執行，並經由外部中斷報告結果至主CPU810。

另一種方式，CPU1100可設定一旗標於SAM狀態暫存器中，指出是否上述處理已被正確地執行，且主CPU810可藉投票讀取旗標。

SAM1051至SAM1054之實施方法如下。

實施作爲硬體之SAM1051至SAM1054之功能時，使用具有內建記憶體之指定應用IC（ASIC）－型CPU，且安全功能模組，用於執行內容權利處理之程式模組，及例如鑰匙資料之高度機密資料，被儲存於記憶體中，以實施圖30所示之功能。一系列的權利處理程式模組，例如加密圖書館（公開鑰匙加密，共同鑰匙加密，隨機數目產生器，雜亂功能），用於限制內容之使用的程式模組，會計程式模組等等，被實施爲例如軟體。

例如，有鑑於處理速率，如加密／解密（解碼）單元171之模組，被實施作爲ASIC－型CPU內的IP核心。以特性例如時鐘速率或CPU碼系統之觀點，加密

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 112

／解密（解碼）單元１７１可被實施作爲軟體。

作爲儲存單元１９２及一記憶體，用於儲存實施圖３０所示之功能的程式模組與資料，可使用非依電性記憶體（快閃ＲＯＭ），且一快速記憶體例如ＳＲＡＭ可被使用作爲工作記憶體。或者ＦｅＲＡＭ可被使用作爲ＳＡＭ１０５$_1$至１０５$_4$中之集積的記憶體。

ＳＡＭ１０５$_1$至１０５$_4$亦具有一內建時間功能，用於檢查時間及日期，以證明內容之使用的有效周期與合約周期。

如上所述，ＳＡＭ１０５$_1$至１０５$_4$具有高度抗干預構造，其中程式模組、資料與處理內容與外源隔離。各ＳＡＭ設定一位址空間，其是無法由對應的主ＣＰＵ看到的，藉著使用一記憶體管理單元（ＭＭＵ），用於管理主ＣＰＵ之記憶體位址。以此管理，儲存於各ＳＡＭ之ＩＣ的記憶體中之內容與高度私人程式，與ＳＡＭ之系統造形有關的一群暫存器，加密圖書館，及一群時鐘的暫存器，可被保護免於經由主ＣＰＵ匯流排被讀取或寫入。亦即，各ＳＡＭ之上述資料與程式被保護免於在由主ＣＰＵ指定的位址空間中。

ＳＡＭ１０５$_1$至１０５$_4$亦可抵抗來自外源之實體攻擊，例如Ｘ射線與熱。此外，即使藉著使用除錯工具（硬體電路內模倣器（ＩＣＥ）或軟體ＩＣＥ）執行即時除錯，處理內容是看不到的，或者除錯工具本身在製造ＩＣ之後變成無法使用。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 113）

以硬體構造的觀點，ＳＡＭ１０５$_1$至１０５$_4$是具有內建記憶體之ＡＳＩＣ－型ＣＰＵ，且ＳＡＭ１０５$_1$至１０５$_4$是與操作ＣＰＵ之軟體相關的。然而，ＳＡＭ１０５$_1$至１０５$_4$是不同於具有設有加密功能與抗干預之硬體構造之ＡＳＩＣ－型ＣＰＵ。

另一方面，有兩種方式可實施ＳＡＭ１０５$_1$至１０５$_4$之全部功能作爲軟體。一種方式是執行具有高抗干預之完全遮蔽的模組內之軟體處理。另一種方式是執行一般機器中安裝的主ＣＰＵ中之軟體處理，但其中軟體處理很難解碼。在第一種方式中，加密圖書館模組被儲存於記憶體中，作爲一軟體模組，而非智慧財產（ＩＰ）核心，亦即，它可被視爲被實施作爲硬體。另一方面，依據第二種方式，使用抗干預軟體，即使由ＩＣＥ（除錯器）解碼執行內容，工作之執行順序是無意義的（在此情形中，工作被分割使得單一工作是一程式，以不影響之前或以後的工作），或者工作本身可被加密。亦即，功能被實施作爲工作排程者（ＭｉｎＯＳ），用於加強安全性。工作排程者被嵌入於目標程式中。

以下敘述圖２２所示之Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之細節。

如圖２２所示，Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３包括：相互證明單元２２０、解碼器２２１與２２２、解壓縮單元２２３、數位水記資訊處理器２２４及部份揭示處理器２２５。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 114）

當Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３從ＳＡＭ１０５$_1$接收資料時，相互證明單元２２０以圖３０所示之ＳＡＭ１０５$_1$之相互證明單元１７０執行相互證明，並產生連續鑰匙資料K_{SES}。

解碼器２２１藉著使用連續鑰匙資料K_{SES}，解碼內容鑰匙資料Ｋｃ，部份揭示參數資料１９９，使用者數位資訊資料１９６及從ＳＡＭ１０５$_1$接收之內容資料Ｃ。然後解碼器２２１輸出解碼的內容鑰匙資料Ｋｃ與內容資料Ｃ至解碼器２２２，並輸出使用者數位資訊資料１９６至數位水記資訊處理器２２４，且亦輸出部份揭示參數資料１９９至部份揭示處理器２２５。

解碼器２２２在部份揭示處理器２２５之控制下，解碼部份揭示狀態之內容資料Ｃ，藉著使用內容鑰匙資料Ｋｃ，並輸出解碼的內容資料Ｃ至解壓縮單元２２３。解碼器２２２亦以正常操作模式（亦即部份揭示模式以外的模式）中的內容鑰匙資料Ｋｃ，解碼整個內容資料Ｃ。

解壓縮單元２２３解壓縮解碼的內容資料Ｃ，並將它輸出至數位水記資訊處理器２２４。解壓縮單元２２３內容資料Ｃ，藉著使用例如儲存於圖３Ａ之內容檔ＣＦ中的Ａ／Ｖ解壓縮軟體，依據例如ＡＴＲＡＣ３方法。

數位水記資訊處理器２２４依據解碼的使用者數位資訊資料１９６，將使用者數位水記資訊嵌入解碼的內容資料Ｃ，以產生新的內容資料Ｃ。然後數位水記資訊處理器２２４輸出新產生的內容資料Ｃ至播放模組１６９。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 115）

以此方式，當再生內容資料C時，藉著A／V壓縮／解壓縮SAM163，使用者數位水記資訊被嵌入內容資料C。

在本發明中，可決定使用者數位資訊資料196不被嵌入內容資料C。

根據部份揭示參數199，部份揭示處理器225通知解碼器222那些區塊要被解碼及那些區塊不要被解碼。部份揭示處理器225可控制部份揭示模組，藉著例如限制展示之播放功能，或限制傾聽用於展示之內容的周期。

播放模組169依據解碼及解壓縮內容資料C執行播放操作。

登記SAM1051至1054於EMD服務中心102中之處理如下。相同的登記處理在SAM1051至1054中被執行，於是以下只討論SAM1051之登記。

當運送SAM1051時，以下的鑰匙資料經由SAM管理器149被登記於圖30所示之儲存單元192中，藉著EMD服務中心102之鑰匙伺服器141。

當SAM1051被運送時，用於由SAM1051啓始存取至EMD服務中心102之程式，亦被儲存於儲存單元192中。

特別是，SAM1051儲存啓始登記，例如SAM1051之辨識SAM_ID，儲存鑰匙資料KSTR

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 119

，根證明授權９２之公開鑰匙資料K_{R-CA}，ＥＭＤ服務中心１０２之公開鑰匙資料$K_{ESC,P}$，ＳＡＭ１０５$_1$之私人鑰匙資料$K_{SAM1,S}$，公開鑰匙資料CER_{SAM1}及其簽名資料$SIG_{22,ESC}$，及源鑰匙資料，用於產生Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３與媒體ＳＡＭ之間的相互證明，如圖３４所示，全部具有符號”＊”附著在資料之左側。

公開－鑰匙證明資料CER_{SAM1}可從ＥＭＤ服務中心１０２被送至ＳＡＭ１０５$_1$，當ＳＡＭ１０５$_1$在運送之後被登記。

運送ＳＡＭ１０５$_1$時，分別指出圖３Ａ與３Ｂ所示之內容檔ＣＦ與鑰匙檔ＫＦ的讀取格式之檔案讀者，藉著ＥＭＤ服務中心１０２被寫入儲存單元１９２。然後，在ＳＡＭ１０５$_1$中，當讀取儲存於內容檔ＣＦ與鑰匙檔ＫＦ中之資料時，使用儲存於儲存單元１９２中之檔案讀者。

根證明授權９２之公開鑰匙資料K_{R-CA}使用River-Shamir-Adleman（ＲＳＡ）演算，其常使用於網際網路上之電子商務，且資料長度是例如１０２４位元。公開鑰匙資料K_{R-CA}被圖１所示之根證明授權９２發出。

由橢圓曲線密祕系統（elliptic curve cryptosystem）產生ＥＭＤ服務中心１０２之公開鑰匙資料$K_{ESC,P}$，其加密長度可與ＲＳＡ相比或高於ＲＳＡ，且資料長度只有例如１６０位元。然而，考慮加密強度，公開鑰匙資料$K_{ESC,P}$最好具有１９２位元或更大。ＥＭＤ服務中心

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 117）

102登記根證明授權92中之公開鑰匙資料$K_{ESC,P}$。

根證明授權92產生公開鑰匙資料$K_{ESC,P}$之公開－鑰匙證明資料CER_{ESC}。儲存公開鑰匙資料$K_{ESC,P}$之公開－鑰匙證明資料CER_{ESC}，最好當運送$SAM105_1$時被儲存於儲存單元192中。在此情形中，公開－鑰匙證明資料CER_{ESC}被標以根證明授權92之私人鑰匙資料$K_{ROOT,S}$。

EMD服務中心102產生一隨機數目，以產生$SAM105_1$之私人鑰匙資料$K_{SAM1,S}$，且亦產生私人鑰匙資料$K_{SAM1,P}$，與私人鑰匙資料$K_{SAM1,S}$成爲一對。

EMD服務中心102亦從根證明授權92得到一證明，以發出公開鑰匙資料$K_{SAM1,P}$之公開－鑰匙證明資料CER_{SAM1}，並以EMD服務中心102之私人鑰匙資料$K_{SAM1,S}$附著簽名資料。亦即，EMD服務中心102作爲第二證明授權。

獨特辨識SAM_ID在EMD服務中心102之控制下，從EMD服務中心102被指定至$SAM105_1$。獨特辨識SAM_ID被儲存於儲存單元192中，且亦被EMD服務中心102管理。

在運送之後，$SAM105_1$藉著例如使用者，被連接至EMD服務中心102且被登記。然後，執照鑰匙資料KD_1至KD_3從EMD服務中心102被轉移至儲存單元192。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 119

亦即，ＳＡＭ１０５$_1$之使用者被要求在下載內容之前，登記於ＥＭＤ服務中心１０２中。離線例如藉由郵件而執行此登記，使用登記記錄附著至機器（在此例子中爲網路裝置１６０$_1$），其上藉著填寫使用者之特定資訊（使用者姓名，地址，聯絡電話，姓別，處理賬戶，登錄名稱，密碼等等）而負載ＳＡＭ１０５$_1$。直到上述登記已被進行，使用者才能使用ＳＡＭ１０５$_1$。

ＥＭＤ服務中心１０２依據使用者之登記，發出使用者之獨特的辨識ＵＳＥＲ＿ＩＤ，並管理ＳＡＭ＿ＩＤ與ＵＳＥＲ＿ＩＤ之間的關係，其用於處理賬戶。

ＥＭＤ服務中心１０２亦指定一資訊參考辨識ＩＤ及一密碼，其是用於ＳＡＭ１０５$_1$之使用者的啓始使用，並將它們報告至使用者。使用者詢問ＥＭＤ服務中心１０２，關於例如內容資料之目前使用狀態，藉著使用資訊參考辨識ＩＤ及密碼。

ＥＭＤ服務中心１０２詢問例如信用卡公司以檢查使用者之辨識，或離線詢問使用者登記中他／她自己之辨識。

如圖３４所示，現在敘述儲存ＳＡＭ登記列表於ＳＡＭ１０５$_1$內之儲存單元１９２中的處理。

圖１所示之ＳＡＭ１０５$_1$得到與ＳＡＭ１０５$_1$相同系統的ＳＡＭ１０５$_2$至１０５$_4$之ＳＡＭ登記列表，藉著使用當連接至匯流排１９１例如ＩＥＥＥ－１３９４串聯匯流排之機器被打開電力，或當新的機器被連接至匯流排

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 119

１９１時所產生的拓撲圖。

不僅對於ＳＡＭ１０５$_1$至１０５$_4$，亦對於連接至匯流排１９１的Ａ／Ｖ機器１６０$_5$與１６０$_6$之ＳＣＭＳ處理電路１０５$_5$與１０５$_6$，依據匯流排１９１產生拓撲圖。因此，ＳＡＭ１０５$_1$產生圖５９所示之ＳＡＭ登記列表，藉著從拓撲圖取出關於ＳＡＭ１０５$_1$至１０５$_4$之資訊。

然後ＳＡＭ１０５$_1$登記圖５９所示之ＳＡＭ登記列表於ＥＭＤ服務中心１０２中以得到簽名。

藉著利用匯流排１９１之連續，自動地由ＳＡＭ１０５$_1$執行前述處理，且ＳＡＭ１０５$_1$發出ＳＡＭ登記列表之登記命令至ＥＭＤ服務中心１０２。

於從ＳＡＭ１０５$_1$接收圖５９所示之ＳＡＭ登記列表時，ＥＭＤ服務中心１０２檢查有效周期，且亦檢查於登記期間被ＳＡＭ１０５$_1$指定之處理功能。ＥＭＤ服務中心１０２參考圖６０所示之預先儲存撤銷列表（證書撤銷列表），並設定撤銷旗標於ＳＡＭ登記列表內。撤銷列表是由於非法使用被禁止使用（成爲無效）的ＳＡＭ之列表。在執行ＳＡＭ之間的通訊時，各ＳＡＭ檢查撤銷列表，是否對應的ＳＡＭ已變成無效，在此情形中，其間的通訊被中斷。

處理賬戶時，ＥＭＤ服務中心１０２檢查ＳＡＭ１０５$_1$之ＳＡＭ登記列表，是否列表中敘述的ＳＡＭ被包含於撤銷列表中。ＥＭＤ服務中心１０２亦附

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 120

著簽名至ＳＡＭ登記列表。

結果，產生圖６１所示之ＳＡＭ登記列表。

對於相同系統中之ＳＡＭ（亦即連接至匯流排１９１之ＳＡＭ）形成ＳＡＭ撤銷列表，且依據對應的ＳＡＭ之撤銷旗標，指出是否各ＳＡＭ是無效。

撤銷列表ＣＲＬ依據例如從ＥＭＤ服務中心１０２送至ＳＡＭ之更新資料，最好在ＳＡＭ內被自動地更新。ＳＡＭ之安全功能如下。

作爲安全功能，ＳＡＭ處理加密圖書館之ＩＰ成份，例如共同鑰匙密祕系統之ＤＥＳ（Triple DES／進步加密標準（ＡＥＳ）），公開鑰匙密祕系統之橢圓曲線密祕系統（簽名產生／檢查ＥＣ－ＤＳＡ，共同鑰匙產生ＥＣ－Ｄ．Ｈ．，及公開鑰匙密祕系統Ｅｃ－Elgamal），壓縮功能雜亂功能）ＳＨＡ－１，及隨機數目產生器（本質隨機數目）。

公開鑰匙密祕系統（橢圓曲線密祕系統）是用於相互證明，簽名產生，簽名檢查，及共同鑰匙（連續鑰匙）產生（傳送）。共同鑰匙密祕系統（ＤＥＳ）是用於加密及解碼內容，且壓縮功能（雜亂功能）是用於簽名產生及檢查中的訊息證明。

圖６２指出ＳＡＭ之安全功能。由ＳＡＭ管理的有兩種型式之安全功能：（１）應用層中之安全功能，用於加密及解碼內容；及（２）實體層中之安全功能，用於藉著以另一ＳＡＭ執行相互證明而保護通訊路徑。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 121）

在ＥＭＤ系統１００中，欲被分布之內容資料Ｃ被完全加密，且於處理賬戶時購買一鑰匙。由於ＵＣＰ資料１０６依據頻帶內系統連同內容資料Ｃ被送出，在與網路媒體之型式無關的層中來加以管理。於是可以提供一共同權利處理系統，與通訊路徑之型式無關，通訊路徑例如衛星，地面微波，電纜，無線電或記錄媒體。例如，當ＵＣＰ資料１０６被插入一網路之實體層的協定之標頭，即使對於相同型式的ＵＣＰ資料１０６，各網路需要決定在何處插入ＵＣＰ資料１０６之標頭。

在此實施例中，內容資料Ｃ與鑰匙檔ＫＦ被應用層加密而保護。相互證明可被執行於實體層，傳輸層或應用層。將加密功能集積至實體層機構，，將加密功能集積於硬體。相互證明最好被執行於實體層，由於執行相互證明之主要目的是欲確保送出者與接收者之間的通訊路徑。然而，實際上，相互證明通常被施實於傳輸層而與傳輸通道無關。

ＳＡＭ之安全功能包括相互證明，用於證明另一欲通訊的ＳＡＭ之完整性，及內容資料的加密與解密（解碼），其是與應用層中之會計處理有關。

通常，用於執行機器間的通訊之ＳＡＭ間的相互證明被實施於應用層中。然而，它可被實施於另一層中，例如傳輸層或實體層。

欲被實施於實體層中之相互證明利用５Ｃ１３９４ＣＰ（內容保護）。依據１３９４ＣＰ，是

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 122）

共同鑰匙密祕系統之Ｍ６，被實施於1394LINKIC（硬體）之通道中。然後以非同步通道執行相互證明（橢圓曲線密祕系統或使用雜亂功能之共同鑰匙密祕系統），且所得到的連續鑰匙被轉移至Ｍ６。結果，由Ｍ６實施共同鑰匙密祕系統。

如果ＳＡＭ間之相互證明被實施於實體層之硬體中，使用公開鑰匙密祕系統（橢圓曲線密祕系統）藉著執行相互證明所得到的連續鑰匙，經由主ＣＰＵ被轉移至１３９４ＬＩＮＫＩＣ之Ｍ６，藉以藉著使用上述連續鑰匙連同由１３９４ＣＰ所得到的連續鑰匙而加密內容資料Ｃ。

如果ＳＡＭ間之相互證明被執行於應用層中，藉著使用ＳＡＭ內之共同鑰匙密祕系統圖書館（ＤＥＳ／Triple ＤＥＳ／ＡＥＳ）而加密內容資料Ｃ。

例如，在此實施例中，ＳＡＭ間之相互證明被實施於應用層中，且１３９４ＣＰ之相互證明被實施於實體層（硬體）例如１３９４ＬＩＮＫＩＣ中。

在此情形中，與會計處理有關的內容資料Ｃ之加密與解密（解碼）被執行於應用層中。然而，應用層容易由使用者存取，且可被無限制地分析。因此，在此實施例中，會計相關的處理被執行於高抗干預硬體中，其中處理內容被完全保護，免於從外源被監視。這是實施ＳＡＭ作爲高抗干預硬體的主要原因。

如果在主ＣＰＵ內執行會計處理，在ＣＰＵ中實施抗

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 123）

干預軟體。

參見圖６３，現在敘述在例如圖１所示之使用者家庭網路１０３之網路裝置１６０₁內之不同ＳＡＭ的實施之例子。

網路裝置１６０₁如圖６３所示包括，主ＣＰＵ８１０₁，ＳＡＭ１０５₁，下載記憶體１６７，媒體驅動ＳＡＭ２６０，驅動ＣＰＵ１００３，及防震動（抗振動）記憶體，例如動態ＲＡＭ（ＤＲＡＭ）１００４。

部份下載記憶體１６７與部份防震記憶體１００４被使用作爲共同記憶體，其可從ＳＡＭ１０５₁與主ＣＰＵ８１０₁被存取。

防震記憶體１００４儲存經由資料匯流排１００２接收的內容資料Ｃ，然後將它輸出至Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。如此使得可以依序地輸出內容資料Ｃ至Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３，即使由於例如振動，來自記錄媒體１３０之內容資料Ｃ的讀取操作被中斷。於是可有效地避免內容資料Ｃ之播放操作的中斷。

下載記憶體１６７經由模組１００５被連接至主ＣＰＵ匯流排１０００，模組１００５是由記憶體控制器與匯流排仲裁／橋組成。

圖６４指出模組１００５與周邊電路的細部造形。如圖６４所示，模組１００５包括控制器１５００及匯流排仲裁／橋１５０１。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 124）

控制器１５００作爲ＤＲＡＭ介面（Ｉ／Ｆ），當ＤＲＡＭ被使用作爲下載記憶體１６７，且具有一讀取／寫入（ｒ／ｗ）線，位址匯流排，$\overline{\text{ＣＡＳ}}$線，及$\overline{\text{ＲＡＳ}}$線以與下載記憶體１６７通訊。

匯流排仲裁／橋１５０１進行主ＣＰＵ匯流排１０００之仲裁，且具有一資料匯流排與下載記憶體１６７通訊，且亦具有一ｒ／ｗ線，一位址匯流排，一備妥線，並具有一晶片選定（ＣＳ）線，一ｒ／ｗ線，一位址匯流排，一資料匯流排，一備妥線與ＳＡＭ１０５$_1$通訊。匯流排仲裁／橋１５０１被連接至主ＣＰＵ匯流排１０００。

匯流排仲裁／橋１５０１、主ＣＰＵ８１０$_1$及ＳＡＭ１０５$_1$被連接至主ＣＰＵ匯流排１０００。主ＣＰＵ匯流排１０００具有一ＣＳ線，一ｒ／ｗ線，一位址匯流排，一資料匯流排及一備妥線。

下載記憶體１６７與防震記憶體１００４儲存上述內容檔ＣＦ與鑰匙檔ＫＦ。使用作爲共同記憶體以外的防震記憶體１００４之儲存區域，被用於暫時地儲存經由資料匯流排１００２從媒體驅動ＳＡＭ２６０接收的內容資料Ｃ，直到內容資料Ｃ被輸出至Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。

Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３經由主ＣＰＵ匯流排１０００轉移資料至下載記憶體１６７，且亦經由資料匯流排１００２轉移資料至媒體驅動ＳＡＭ２６０。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 125）

不僅下載記憶體１６７，ＳＡＭ１０５$_1$、Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３及ＤＭＡ１０１０亦被連接至主ＣＰＵ匯流排１０００。

依據來自主ＣＰＵ８１０$_1$之命令，ＤＭＡ１０１０集中地控制經由主ＣＰＵ匯流排１０００至下載記憶體１６７之存取。

藉著使用１３９４－串聯介面鏈層，主ＣＰＵ匯流排１０００亦被用於與使用者家庭網路１０３內之其它ＳＡＭ，亦即ＳＡＭ１０５$_2$至１０５$_4$通訊。

驅動ＣＰＵ１００３、媒體驅動ＳＡＭ２６０、ＲＦ放大器１００６、媒體ＳＡＭ介面１００７及ＤＭＡ１０１１被連接至驅動ＣＰＵ匯流排１００１。

驅動ＣＰＵ１００３依據來自主ＣＰＵ８１０$_1$之命令，集中地控制至碟型記錄媒體１３０之存取。在此情形中，主ＣＰＵ８１０$_1$作爲主人，而驅動ＣＰＵ１００３作爲奴役。從主ＣＰＵ８１０$_1$來看，驅動ＣＰＵ１００３被處理作爲Ｉ／Ｏ。

存取至記錄媒體（ＲＡＭ）１３０時，驅動ＣＰＵ１００３編碼及解碼資料。

當記錄媒體（ＲＡＭ）１３０被設定於驅動器中，驅動ＣＰＵ１００３決定是否記錄媒體１３０適合於ＳＡＭ１０５$_1$（ＥＭＤ系統１００）（亦即是否權利處理可被ＳＡＭ１０５$_1$安全地執行在記錄媒體１３０上）。如果是的話，驅動ＣＰＵ１００３報告對應的資訊至主

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 129

ＣＰＵ８１０１，且亦指示媒體驅動ＳＡＭ２６０以媒體ＳＡＭ１３３執行相互證明。

媒體ＳＡＭ介面１００７作爲一介面，用於經由驅動ＣＰＵ匯流排１００１存取記錄媒體１３０之媒體ＳＡＭ１３３。

依據來自驅動ＣＰＵ１００３之命令，ＤＭＡ１０１１集中地控制經由驅動ＣＰＵ匯流排１００１與資料匯流排１００２至防震記憶體１００４之存取。ＤＭＡ１０１１控制例如經由資料匯流排１００２，媒體驅動ＳＡＭ２６０與防震記憶體１００４之間的資料轉移。

依據圖６３所示之造形，例如在執行通訊時，如記錄媒體１３０的媒體ＳＡＭ１３３與ＳＡＭ１０５１之間的相互證明，根據主ＣＰＵ８１０１之控制，經由主ＣＰＵ匯流排１０００，主ＣＰＵ８１０１，驅動ＣＰＵ１００３內的暫存器，驅動ＣＰＵ匯流排１００１及媒體ＳＡＭ介面１００７進行其間的資料轉移。

存取記錄媒體１３０時，在媒體驅動ＳＡＭ２６０與媒體ＳＡＭ１３３之間進行相互證明。

如上所討論，在Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３中壓縮或解壓縮資料以存取下載記憶體１６７或防震記憶體１００４時，在ＳＡＭ１０５１與Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之間執行相互證明。

在此實施例中，於圖６３中，由主ＣＰＵ８１０１來看

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 127）

，ＳＡＭ１０５１與Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３被處理作爲連接至Ｉ／Ｏ介面之裝置。在位址解碼器１０２０與記憶體Ｉ／Ｏ之控制下，以主ＣＰＵ８１０１執行ＳＡＭ１０５１與Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之通訊與資料轉移。在此情形中，主ＣＰＵ８１０１作爲主人，而ＳＡＭ１０５１與Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３作爲奴役。ＳＡＭ１０５１與Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３執行由主ＣＰＵ８１０１指示的處理，如果需要的話，報告結果至主ＣＰＵ８１０１。

由驅動ＣＰＵ１００３來看，媒體ＳＡＭ１３３與媒體驅動ＳＡＭ２６０被處理作爲連接至Ｉ／Ｏ介面之裝置。在位址解碼器１０２１與記憶體Ｉ／Ｏ的控制下，以驅動ＣＰＵ１００３執行媒體ＳＡＭ１３３與媒體驅動ＳＡＭ２６０之通訊與資料轉移。在此情形中，驅動ＣＰＵ１００３作爲主人，而媒體ＳＡＭ１３３與媒體驅動ＳＡＭ２６０作爲奴役。媒體ＳＡＭ１３３與媒體驅動ＳＡＭ２６０執行由驅動ＣＰＵ１００３指示的處理，如果需要的話，報告結果至驅動ＣＰＵ１００３。

可由ＳＡＭ１０５１集中地執行對於儲存於下載記憶體１６７與防震記憶體１００４中之內容檔ＣＦ與鑰匙檔ＫＦ的存取控制。另一種方式，可由主ＣＰＵ８１０１執行對於內容檔ＣＦ之存取控制，且由ＳＡＭ１０５１執行對於鑰匙檔ＫＦ的存取控制。

由驅動ＣＰＵ１００３從記錄媒體１３０讀取的內容

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 128）

資料Ｃ，經由ＲＦ放大器１００６及媒體驅動ＳＡＭ２６０被儲存於防震記憶體１００４中，然後被壓縮於Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３中。壓縮的內容資料在數位－類比（Ｄ／Ａ）轉換器中被轉換成類比資料，且根據轉換的類比資料，從揚聲器輸出聲音。

在此情形中，防震記憶體１００４可暫時地儲存內容資料Ｃ，內容資料Ｃ是由許多軌道組成，其被非連續地從獨立地位在記錄媒體１３０中之儲存區域讀取，然後連續地輸出內容資料Ｃ至Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３。

以下敘述圖６３所示之使用者家庭網路１０３內的不同ＳＡＭ之主人－奴役關係。

例如，當決定購買模式之內容資料Ｃ如圖６５所示被記錄在記錄媒體１３０上時，主ＣＰＵ８１０$_1$輸出一內部中斷以指示作爲Ｉ／Ｏ裝置之ＳＡＭ１０５$_1$決定內容資料Ｃ之購買模式，且亦以記錄媒體１３０之媒體ＳＡＭ１３３執行相互證明，藉以記錄內容資料Ｃ於記錄媒體１３０上。

在此情形中，主ＣＰＵ８１０$_1$作爲主人，而ＳＡＭ１０５$_1$與記錄媒體１３０作爲奴役。由主ＣＰＵ８１０$_1$來看，記錄媒體１３０被處理作爲Ｉ／Ｏ裝置。

響應來自主ＣＰＵ８１０$_1$之內部中斷，ＳＡＭ１０５$_1$與媒體ＳＡＭ１３３通訊，以決定內容資料Ｃ之購買模式，且亦將例如內容鑰匙資料Ｋｃ之預定鑰匙

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 129

資料寫入媒體ＳＡＭ１３３。於完成此處理時，ＳＡＭ１０５$_1$經由外部中斷或藉著主ＣＰＵ８１０$_1$之投票，報告處理結果至主ＣＰＵ８１０$_1$。

播放記錄記錄媒體上且決定購買模式之內容資料Ｃ時，如圖６６所示經由內部中斷，從主ＣＰＵ８１０$_1$給予指示播放內容資料Ｃ至ＳＡＭ１０５$_1$。

響應內部中斷，ＳＡＭ１０５$_1$從記錄媒體１３０之媒體ＳＡＭ１３３讀取例如鑰匙檔ＫＦ之鑰匙資料區塊，並根據鑰匙資料區塊中儲存的ＵＣＳ資料１６６，執行播放內容資料Ｃ之處理。

ＳＡＭ１０５$_1$輸出一內部中斷，以指示Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３解壓縮從記錄媒體１３０讀取的內容資料Ｃ。

於從ＳＡＭ１０５$_1$接收內部中斷時，Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３將從記錄媒體１３０讀取的內容資料Ｃ擾頻，嵌入及偵測數位水記資訊，並解壓縮內容資料。然後，Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３輸出處理的內容資料Ｃ至Ｄ／Ａ轉換器，以播放內容資料Ｃ。

在完成播放操作之後，Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３報告對應的資訊至ＳＡＭ１０５$_1$。

於接收上述資訊時，ＳＡＭ１０５$_1$經由外部中斷將它報告至主ＣＰＵ８１０$_1$。

在此情形中，於主ＣＰＵ８１０$_1$與ＳＡＭ１０５$_1$的關係中，主ＣＰＵ８１０$_1$作爲主人，而ＳＡＭ１０５$_1$作

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 130

爲奴役。於ＳＡＭ１０５１與Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３的關係中，ＳＡＭ１０５１作爲主人，而Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３作爲奴役。

雖然在此實施例中，Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３是ＳＡＭ１０５１之奴役，它可以是主ＣＰＵ８１０１之奴役。

如果如圖６７所示，沒有執行內容資料之權利處理，播放記錄在記錄媒體１３０上的內容資料，主ＣＰＵ８１０１輸出一內部中斷，以指示Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３執行播放處理。主ＣＰＵ８１０１亦輸出一內部中斷，以指示媒體驅動ＳＡＭ２６０從記錄媒體１３０讀取內容資料。

於接收內部中斷時，媒體驅動ＳＡＭ２６０在解碼器中，解碼從記錄媒體１３０讀取的內容資料，然後將它儲存於防震記憶體１００４中。於完成此處理時，媒體驅動ＳＡＭ２６０經由外部中斷報告對應的資訊至主ＣＰＵ８１０。

儲存於防震記憶體１００４中之內容資料被讀入Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３，且進行例如擾頻、嵌入及偵測數位水記資訊、與解壓縮之處理，然後經由Ｄ／Ａ轉換器被播放。

於完成此處理時，Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３經由外部中斷報告此資訊至主ＣＰＵ８１０１。

在此情形中，主ＣＰＵ８１０１作爲主人，而Ａ／Ｖ壓

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 131）

縮／解壓縮ＳＡＭ１６３與媒體驅動ＳＡＭ２６０作爲奴役。

以下敘述實施使用者家庭網路１０３內之ＳＡＭ的上述功能之電路模組。

如上所討論，使用者家庭網路１０３內的ＳＡＭ包括ＳＡＭ１０５（１０５$_1$至１０５$_4$），用於執行權利處理（利潤分配），例如決定購買模式，置於記錄媒體中之媒體ＳＡＭ１３３，Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３，及媒體驅動ＳＡＭ２６０。上述ＳＡＭ所提供的電路模組如下。

權利處理ＳＡＭ之例子

圖６８指出一電路模組，用於權利處理ＳＡＭ１０５ａ。

ＳＡＭ１０５ａ是一抗干預硬體（等於本發明之電路模組），如圖６８所示，包括ＣＰＵ１１００、ＭＭＵ１１０２、Ｉ／Ｏ模組１１０３、罩ＲＯＭ１１０４、非依電性記憶體１１０５、工作ＲＡＭ１１０６、公開鑰匙加密模組１１０７、共同鑰匙加密模組１１０８、雜亂功能模組１１０９、（本質）隨機數目產生器１１１０、即時時鐘模組１１１１及外部匯流排Ｉ／Ｆ１１１２。

權利處理ＳＡＭ１０５ａ的元件與本發明之間的關係如下。ＣＰＵ１１００對應算術處理電路。罩

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 132）

ＲＯＭ１１０４、非依電性記憶體１１０５及工作ＲＡＭ１１０６對應儲存電路。共同鑰匙加密模組１１０８對應加密處理電路。外部匯流排Ｉ／Ｆ１１１２對應外部匯流排介面。

參見圖６９，以下將敘述內部匯流排１１２０與１１２１對應本發明之第一匯流排，且外部匯流排１１２３對應本發明之第二匯流排。

內部匯流排１１２０亦對應第三匯流排，且內部匯流排１１２１亦對應第四匯流排。

外部匯流排Ｉ／Ｆ１１１２對應第一介面電路，且匯流排Ｉ／Ｆ電路１１１６對應第二介面電路。

內部匯流排１１２２對應第五匯流排，Ｉ／Ｏ模組對應第三介面電路，且匯流排Ｉ／Ｆ電路１１１７對應第四介面電路。

以下敘述圖６８所示的電路模組與圖３０所示之ＳＡＭ１０５１的功能模組之間的關係。

ＣＰＵ１１００執行例如儲存於罩ＲＯＭ１１０４與非依電性記憶體１１０５中之程式，以實施圖３０所示之使用監視器１８６、會計處理器１８７、ＣＰＵ１１００之功能。

ＤＭＡ１１０１響應來自ＣＰＵ１１００之命令，集中地控制對圖２２所示之下載記憶體１６７與圖３０所示之儲存單元１９２的存取。

ＭＭＵ１１０２管理圖２２所示之下載記憶體１６７

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 133）

與圖３０所示之儲存單元１９２的位址空間。

Ｉ／Ｏ模組１１０３實施圖３０所示之媒體ＳＡＭ管理器１９７的部份功能。

當製造ＳＡＭ１０５ｉ時，罩ＲＯＭ１１０４儲存固定的程式與資料，例如ＳＡＭ１０５ａ之完整性檢查程式與啓始程式，且實施圖３０所示之儲存單元１９２的部份功能。

非依電性記憶體１１０５儲存可變的程式與資料，例如加密程式與鑰匙資料，並實施圖３０所示之儲存單元１９２的部份功能。

工作ＲＡＭ１１０６對應圖３０所示之工作記憶體２００。

公開鑰匙加密模組１１０７實施圖３０所示之簽名處理器１８９的部份功能，且依據公開鑰匙密祕系統，以媒體ＳＡＭ１３３用於執行相互證明，產生ＳＡＭ１０５之簽名資料，檢查簽名資料（ＥＭＤ服務中心１０２，內容提供者１０１，且在第二實施例中爲服務提供者３１０之簽名資料），欲被轉移之小量資料（例如鑰匙檔ＫＦ）之加密與解密，及分享一鑰匙。公開鑰匙加密模組１１０７可被實施作爲電路模組（硬體（Ｈ／Ｗ）ＩＰ解決），或藉著執行儲存於非依電性記憶體１１０５中之公開鑰匙加密程式，由ＣＰＵ１１００（軟體（Ｓ／Ｗ）解決）實施。

共同鑰匙加密模組１１０８實施簽名處理器１８９與

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 134）

加密／解密（解碼）單元１７１、１７２、１７３之部份功能，且被使用於執行相互證明及加密與解密資料，藉著使用由相互證明所得到的連續鑰匙資料K_{SES}。共同鑰匙密祕系統實施比公開鑰匙密祕系統更快的處理，於是被使用於例如加密與解密大量的內容資料（鑰匙檔ＫＦ）。共同鑰匙加密模組１１０８可被實施作爲電路模組（Ｈ／ＷＩＰ解決），或可由ＣＰＵ１１００藉著執行儲存於非依電性記憶體１１０５中之共同鑰匙加密程式而被實施（Ｓ／Ｗ　ＩＰ解決）。

由加密與解密公開鑰匙加密模組１１０７與共同鑰匙加密模組１１０８的其中之一或兩者而達成相互證明。

共同鑰匙加密模組１１０８以執照鑰匙資料ＫＤ解碼內容鑰匙資料K_C。

雜亂功能模組１１０９實施圖３０所示之簽名處理器１８９的部份功能，且被用於產生欲被產生的簽名資料之資料的雜亂值。特別是，雜亂功能模組１１０９用於檢查內容提供者１０１與ＥＭＤ服務中心１０２的簽名資料，且亦檢查圖４４Ａ至４４Ｄ所示之安全容器１０４ｘ的鑰匙檔KF_1之雜亂值H_{K1}。雜亂功能模組１１０９可被實施作爲一電路模組（Ｈ／Ｗ　ＩＰ解決），或可由ＣＰＵ１１００藉著執行儲存於非依電性記憶體１１０５中之雜亂電路模組程式而被實施（Ｓ／Ｗ　ＩＰ解決）。

隨機數目產生器１１１０實施圖３０所示之相互證明單元１７０的部份功能。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 135

即時時鐘模組１１１１產生即時，其是用於選定具有有效周期之執照鑰匙資料ＫＤ，或決定是否滿足由ＵＣＳ資料１６６指出的有效周期之要求。

外部匯流排Ｉ／Ｆ１１１２實施圖３０所示之ＥＭＤ服務中心管理器１８５、下載記憶體管理器１８２與內容提供者管理器１８０之部份功能。

圖６９指出ＳＡＭ１０５ａ內的硬體造形。在圖６９中，與圖６８相同的元件是以相同的參考數字來表示。

如圖６９所示，在ＳＡＭ１０５ａ內，ＣＰＵ１１００、罩ＲＯＭ１１０４與非依電性記憶體１１０５經由ＳＡＭ／ＣＰＵ匯流排１１２０彼此連接。

ＤＭＡ１１０１被連接至內部匯流排１１２１。I^2C介面１１３０、媒體ＳＡＭ介面１１３１、記憶棒（ＭＳ）介面１１３２與ＩＣ卡介面１１３３被連接至內部匯流排１１２２。

媒體ＳＡＭ介面１１３１從記錄媒體１３０之媒體ＳＡＭ１３３，轉移並接收資料。ＭＳ介面１１３２從記憶棒１１４０轉移並接收資料。ＩＣ卡介面１１３３從ＩＣ卡１１４１轉移並接收資料。

公開鑰匙加密模組１１０７、共同鑰匙加密模組１１０８、雜亂功能模組１１０９、隨機數目產生器１１１０、即時時鐘模組１１１１、外部匯流排Ｉ／Ｆ１１１２與外部記憶體Ｉ／Ｆ１１４２被連接至外部匯流排１１２３。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 139）

圖６３所示之主ＣＰＵ匯流排１０００被連接至外部匯流排Ｉ／Ｆ１１１２，且圖６３所示之外部記憶體２０１被連接至外部記憶體Ｉ／Ｆ１１４２。

內部匯流排１１２０與內部匯流排１１２１經由匯流排介面１１１６被連接。內部匯流排１１２２與１１２１經由匯流排介面１１１７被連接。內部匯流排１１２１與外部匯流排１１２３經由匯流排介面１１１５被連接。

上述ＳＲＡＭ１１５５與ＳＡＭ狀態暫存器１１５６被儲存於匯流排介面１１１５中。

如上所述，ＳＡＭ狀態暫存器１１５６具有第一ＳＡＭ狀態暫存器１１５６ａ及第二ＳＡＭ狀態暫存器１１５６ｂ。指出由主ＣＰＵ８１０₁讀取的ＳＡＭ１０５₁之狀態的旗標，被設定於第一ＳＡＭ狀態暫存器１１５６ａ中。指出是否要求執行工作已從主ＣＰＵ８１０₁被輸出之旗標，被設定於第二ＳＡＭ狀態暫存器１１５６ｂ中，且此旗標是從ＳＡＭ１０５₁之ＣＰＵ１１００被讀取。

ＤＭＡ１１０１響應來自ＣＰＵ１１００之命令，經由內部匯流排１１２１集中地控制罩ＲＯＭ１１０４、非依電性記憶體１１０５及工作ＲＡＭ１１０６。

ＭＭＵ１１１３管理圖６３所示之下載記憶體１６７、工作ＲＡＭ１１０６、非依電性記憶體１１０５、罩ＲＯＭ１１０４之記憶體空間。

當資料在內部匯流排１１２１與外部匯流排１１２３

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 137）

之間被轉移時，位址解碼器１１１４執行位址轉換。

寫入鎖住控制電路１１３５根據ＣＰＵ１１００之鎖住鑰匙資料，控制從快閃ＲＯＭ之各區塊資料的寫入與消除。

以下敘述權利處理ＳＡＭ１０５ａ之位址空間。

圖７０指出權利處理ＳＡＭ１０５ａ之位址空間。位址空間包含：從啓始位址之啓始、開機程式、系統造形、快閃ＲＯＭ、非依電性記憶體之裝置驅動、圖６９所示之工作ＲＡＭ１１０６、預定程式、圖６９所示之ＳＲＡＭ１１５５、外部記憶體２０１、Ｋｅｙ＿ＴＯＣ／Ｆｉｌｅ＿Ｓｙｓｔｅｍ、ＳＡＭ登記列表、使用登錄資料１０８、圖６９所示之共同鑰匙加密模組１１０８的暫存器、圖６９所示之公開鑰匙加密模組１１０７的暫存器、圖６９所示之雜亂功能模組１１０９的暫存器、圖６９所示之隨機數目產生器１１１０的暫存器、圖６９所示之即時時鐘模組１１１１的暫存器、目前時間暫存器、有效周期暫存器、控制暫存器、ＩＣ卡介面、媒體ＳＡＭ介面、記憶棒介面、及Ｉ^{2}Ｃ匯流排介面。

在指定至系統造形之位址空間的欄位中，儲存圖６９所示的ＳＡＭ狀態暫存器１１５６與ＤＭＡ１１０１。

在指定至快閃ＲＯＭ之位址空間的欄位中，儲存主常式（核心）、中斷程式、由中斷程式呼叫的副常式、指令分析（指出中斷程式的啓始位址與指令之間的關係之表）、及中斷向量表。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 138）

在圖７０所示的ＳＡＭ１０５ａ之位址空間中，主ＣＰＵ８１０用ＳＡＭ狀態暫存器１１５６與ＳＲＡＭ１１５５作爲共同記憶體空間。

參見圖７１，以下敘述圖６３所示之主ＣＰＵ８１０₁之位址空間。

主ＣＰＵ８１０₁之位址空間如圖７１所示，包含：從啓始位址之啓始、開機程式、系統造形、碼ＲＯＭ、資料ＲＯＭ、工作ＲＡＭ、與圖６３所示之ＳＡＭ１０５₁分享的共同記憶體、與圖６３所示之Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３分享的共同記憶體、與圖６３所示之媒體驅動ＳＡＭ２６０分享的共同記憶體、及外部裝置。

圖６９所示之ＳＡＭ狀態暫存器１１５６與ＳＲＡＭ１１５５被指定至，與圖６３所示之ＳＡＭ１０５₁分享的共同記憶體。

權利處理ＳＡＭ之另一個例子

圖７２指出權利處理ＳＡＭ１０５ｂ之電路模組。在圖７２中，與圖６９相同之元件是由相同的參考數字來表示。

權利處理ＳＡＭ１０５ｂ如圖７２所示，是由安全記憶體１０５ｂａ、主ＣＰＵ８１０、抗干預軟體１１３０及Ｉ／Ｏ模組１１０３組成。

在ＳＡＭ１０５ｂ中，抗干預軟體１１３０是由主ＣＰＵ８１０執行，以實施與圖６８所示之

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（ 139

ＣＰＵ１１００相同的功能。如上所述，抗干預軟體１１３０是一軟體，其中處理完全與外源隔離，且很難被分析或重寫。

安全記憶體１０５ｂａ是一抗干預硬體，包括罩ＲＯＭ１１０４、非依電性記憶體１１０５、工作ＲＡＭ１１０６、公開鑰匙加密模組１１０７、共同鑰匙加密模組１１０８、雜亂功能模組１１０９、（本質）隨機數目產生器１１１０、即時時鐘模組１１１１及外部匯流排Ｉ／Ｆ１１１２。

公開鑰匙加密模組１１０７、共同鑰匙加密模組１１０８及雜亂功能模組１１０９，可被實施作爲電路模組（Ｈ／Ｗ　ＩＰ解決），或可由主ＣＰＵ８１０藉著執行分別儲存於非依電性記憶體１１０５中之公開鑰匙加密程式、共同鑰匙加密程式、雜亂功能程式而被實施（Ｓ／Ｗ　ＩＰ解決）。

上述媒體ＳＡＭ１３３的造形之例子如下。圖７３指出媒體ＳＡＭ１３３之電路模組。

媒體ＳＡＭ１３３是抗干預硬體，如圖７３所示包括：ＣＰＵ１２００、ＤＭＡ１２０１、Ｉ／Ｏ模組１２０３、罩ＲＯＭ１２０４、非依電性記憶體１２０５、工作ＲＡＭ１２０６、公開鑰匙加密模組１２０７、共同鑰匙加密模組１２０８、雜亂功能模組１２０９、及（本質）隨機數目產生器１２１０。

ＣＰＵ１２００控制抗干預硬體內之個各電路。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（ 140

工作ＲＡＭ１２０６對應圖２０所示之工作記憶體２００。

公開鑰匙加密模組１２０７是用於執行依據公開鑰匙密祕系統之操作，例如：（１）以圖６３所示之驅動ＣＰＵ１００３與ＳＡＭ１０５１執行相互證明；（２）產生媒體ＳＡＭ１３３ａ之簽名資料並檢查簽名資料（ＥＭＤ服務中心１０２、內容提供者１０１及在第二實施例中爲服務提供者３１０之簽名資料）；（３）加密與解密欲被轉移之小量資料；及（４）分享由相互證明所得到的連續鑰匙資料K_{SES}。公開鑰匙加密模組１１０７可被實施作爲電路模組（Ｈ／Ｗ　ＩＰ解決），或可由ＣＰＵ１２００藉著執行儲存於非依電性記憶體１２０５中之公開鑰匙加密程式而被實施（Ｓ／Ｗ　ＩＰ解決）。

共同鑰匙加密模組１２０８是用於執行相互證明，及用於加密與解密例如鑰匙檔ＫＦ與KF_1之資料，藉著使用由執行相互證明所得到的連續鑰匙資料K_{SES}。共同鑰匙加密模組１１０８可被實施作爲電路模組（Ｈ／Ｗ　ＩＰ解決），或可由ＣＰＵ１２００藉著執行儲存於非依電性記憶體１２０５中之共同鑰匙加密程式而被實施（Ｓ／Ｗ　ＩＰ解決）。

藉著以公開鑰匙加密模組１２０７與共同鑰匙加密模組１２０８的其中之一或兩者來加密與解密，可實現相互證明。

雜亂功能模組１２０９是用於產生資料之雜亂功能。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（141）

特別是，雜亂功能模組１２０９是用於證明圖４４Ａ至４４Ｄ所示之安全容器１０４ｘ的鑰匙檔ＫＦ$_1$之雜亂值Ｈ$_{K1}$。雜亂功能模組１１０９可被實施作爲電路模組（Ｈ／Ｗ　ＩＰ解決），或可由ＣＰＵ１２００藉著執行儲存於非依電性記憶體１２０５中之雜亂電路模組而被實施（Ｓ／Ｗ　ＩＰ解決）。

隨機數目產生器１２１０是用於執行例如相互證明。

Ｉ／Ｏ模組１２０３是用於執行與圖６３所示之媒體ＳＡＭ　Ｉ／Ｆ１００７通訊。

罩ＲＯＭ１２０４儲存固定的程式與資料，例如正被運送之媒體ＳＡＭ１３３的完整性檢查程式與啓始程式。

非依電性記憶體１２０５儲存可變的程式與資料，例如加密程式與鑰匙資料。

圖７４指出當運送媒體ＳＡＭ１３３以被安裝於記錄媒體（ＲＯＭ）中時，儲存於罩ＲＯＭ１２０４與非依電性記憶體１２０５中之資料。

當運送記錄媒體（ＲＯＭ）時，媒體ＳＡＭ１３３如圖７４所示儲存媒體ＳＡＭ之辨識（ＩＤ），儲存鑰匙資料Ｋ$_{STR}$（媒體鑰匙資料Ｋ$_{MED}$、ＥＭＤ服務中心１０２之公開鑰匙資料Ｋ$_{ESC,P}$、根證明授權９２之公開鑰匙資料Ｋ$_{R-CA,P}$、媒體ＳＡＭ１３３之公開鑰匙證明資料ＣＥＲ$_{MSAM}$、媒體ＳＡＭ１３３之公開鑰匙資料Ｋ$_{MSAM,P}$、媒體ＳＡＭ１３３之私人鑰匙資料Ｋ$_{MSAM,S}$、撤銷列表、權利處理資料、接收利潤之實體ＩＤ、媒體

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（142）

之型式（媒體型式資訊及指出ＲＯＭ或ＲＡＭ之資訊）、鑰匙檔ＫＦ之實體位址資訊（暫存器空間位址）、各內容資料Ｃ（內容檔ＣＦ）之鑰匙檔ＫＦ、及預定檢查值（ＭＡＣ值）。

使用由ＥＭＤ服務中心１０２管理的執照鑰匙資料ＫＤ，加密鑰匙檔ＫＦ之實體位址資訊（暫存器空間位址）、各內容資料Ｃ（內容檔ＣＦ）之鑰匙檔ＫＦ、及預定檢查值（ＭＡＣ值）。

圖７５指出當進行使用者登記，且在欲被安裝於記錄媒體（ＲＯＭ）中的媒體ＳＡＭ１３３已被運送之後決定購買模式時，儲存於罩ＲＯＭ１２０４與非依電性記憶體１２０５中之資料。

如圖７５所示，藉著使用者登記，使用者ＩＤ、密碼、喜愛資訊、處理資料（例如信用卡號碼）、電子錢包資訊、鑰匙檔KF_1等等被新加至媒體ＳＡＭ１３３。

圖７６指出當欲被安裝於記錄媒體（ＲＡＭ）中之媒體ＳＡＭ１３３被運送時，儲存於罩ＲＯＭ１２０４與非依電性記憶體１２０５中之資料。

如圖７６所示，當運送記錄媒體（ＲＡＭ）時，媒體ＳＡＭ１３３儲存媒體ＳＡＭ１３３之辨識（ＩＤ）、記錄鑰匙資料K_{STR}（媒體鑰匙資料K_{MED}）、ＥＭＤ服務中心１０２之公開鑰匙資料$K_{ESC,P}$、根證明授權９２之公開鑰匙資料$K_{R-CA,P}$、媒體ＳＡＭ１３３之公開－鑰匙證明資料CER_{MSAM}、媒體ＳＡＭ１３３之公開鑰匙資

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（143）

料$K_{MSAM.P}$、媒體ＳＡＭ１３３之私人鑰匙資料$K_{MSAM.S}$、撤銷列表、權利處理資料、接收利潤之實體ＩＤ及媒體之型式（媒體型式資訊及指出ＲＯＭ或ＲＡＭ之資訊）。然而，鑰匙檔ＫＦ之實體位址資訊（暫存器空間位址）、各內容資料Ｃ（內容檔ＣＦ）之鑰匙檔ＫＦ、及預定檢查值（ＭＡＣ值）沒有被儲存。

圖７７指出當進行使用者登記，且在欲被安裝於記錄媒體（ＲＡＭ）中的媒體ＳＡＭ１３３已被運送之後決定購買模式時，儲存於罩ＲＯＭ１２０４與非依電性記憶體１２０５中之資料。

如圖７７所示，藉著使用者登記，除了使用者ＩＤ、密碼、喜愛資訊、處理資料（例如信用卡號碼）及電子錢包資訊之外，鑰匙檔ＫＦ之實體位址資訊（暫存器空間位址）、各內容資料Ｃ（內容檔ＣＦ）之鑰匙檔ＫＦ、及預定檢查值（ＭＡＣ值）被新寫入媒體ＳＡＭ１３３。

鑰匙檔ＫＦ之實體位址資訊（暫存器空間位址）、各內容資料Ｃ（內容檔ＣＦ）之鑰匙檔ＫＦ、及預定檢查值（ＭＡＣ值），以儲存鑰匙資料K_{STR}被加密。

Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３

Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３實施例如圖２２所示之功能。

圖７８指出Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之電路模組。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（144）

Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３是一抗干預硬體，如圖７８所示，包括：ＣＰＵ／ＤＳＰ１３００、ＤＭＡ１３０１、罩ＲＯＭ１３０４、非依電性記憶體１３０５、工作ＲＡＭ１３０６、共同鑰匙加密模組１３０８、（本質）隨機數目產生器１３１０、壓縮／解壓縮模組１３２０、數位水記嵌入／偵測模組１３２１、及部份資訊揭示控制模組１３２２。

ＣＰＵ／ＤＳＰ１３００依據例如來自圖６３所示之ＳＡＭ１０５１之命令，藉著執行儲存於罩ＲＯＭ１３０４與非依電性記憶體１３０５中之程式，集中地控制Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３內之個別電路模組。

ＤＭＡ１３０１依據來自ＣＰＵ／ＤＳＰ１３００之命令，集中地控制對罩ＲＯＭ１３０４、非依電性記憶體１３０５、工作ＲＡＭ１３０６之存取。

當Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３操作時，罩ＲＯＭ１３０４儲存固定的程式，例如Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之完整性檢查程式與啓始程式，及固定的資料，例如Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３之辨識ＡＶＳＡＭ＿ＩＤ。

非依電性記憶體１３０５儲存可變程式與資料，例如加密程式與鑰匙資料。

工作ＲＡＭ１３０６儲存從ＳＡＭ１０５１接收的鑰匙檔ＫＦ。

共同鑰匙加密模組１３０８是用於進行相互證明，及

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（145）

用於加密與解密內容資料C與內容鑰匙資料Kc，藉著使用由相互證明所得到的連續鑰匙資料K_{SES}。共同鑰匙加密模組1308可被實施作爲電路模組（H／W IP解決），或可由CPU／DSP1300藉著執行儲存於非依電性記憶體1305中之共同鑰匙加密程式而被實施（S／W IP解決）。共同鑰匙加密模組1308亦解密內容資料C，藉著使用從$SAM105_1$得到的內容鑰匙資料Kc。

（本質）隨機數目產生器1310是用於以例如$SAM105_1$執行相互證明。

壓縮／解壓縮模組1320實施例如圖22所示之解壓縮單元的功能。特別是，壓縮／解壓縮模組1320解壓縮從圖63所示之防震記憶體1004與下載記憶體167接收的內容資料，並壓縮從A／D轉換器接收的內容資料。

數位水記嵌入／偵測模組1321實施圖22所示之數位水記資訊處理器224的功能。例如，數位水記嵌入／偵測模組1321將預定的數位水記資訊嵌入欲由壓縮／解壓縮模組1320處理之內容資料，並偵測嵌入內容資料之數位水記資訊，亦即決定是否由壓縮／解壓縮模組1320執行的處理是適當。

部份資訊揭示控制模組1322實施圖22所示之部份揭示處理器225的功能，且依據播放模組播放內容資料。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（146）

媒體驅動ＳＡＭ２６０

圖７９指出媒體驅動ＳＡＭ２６０之電路模組。

媒體驅動ＳＡＭ２６０是抗干預硬體，如圖７９所示，包括ＣＰＵ１４００、ＤＭＡ１４０１、罩ＲＯＭ１４０４、非依電性記憶體１４０５、工作ＲＡＭ１４０６、共同鑰匙加密模組１４０８、雜亂功能模組１４０９、（本質）隨機數目產生器１４１０、編碼／解碼模組１４２０、儲存鑰匙資料產生模組１４３０、及媒體獨特ＩＤ產生模組１４４０。

ＣＰＵ１４００依據來自圖６３所示之驅動ＣＰＵ１００３之命令，執行儲存於非依電性記憶體１４０５與罩ＲＯＭ１４０４中之程式，且集中地控制媒體驅動ＳＡＭ２６０內的個別電路模組。

ＤＭＡ１４０１依據來自ＣＰＵ１４００之命令，集中地控制對於罩ＲＯＭ１４０４、非依電性記憶體１４０５、工作ＲＡＭ１４０６之存取。

當媒體驅動ＳＡＭ２６０被運送時，罩ＲＯＭ１４０４儲存固定的程式，例如媒體驅動ＳＡＭ２６０之完整性檢查程式與啓始程式，及固定的資料，例如媒體驅動ＳＡＭ２６０之辨識ＭＤＳＡＭ＿ＩＤ。

非依電性記憶體１４０５儲存可變的程式與資料，例如加密程式與鑰匙資料。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（147）

工作ＲＡＭ１４０６作爲用於執行不同處理之工作記憶體。

共同鑰匙加密模組１４０８是用於執行Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３與媒體ＳＡＭ１３３之間的相互證明，且用於加密與解密內容檔ＣＦ與鑰匙檔ＫＦ，藉著使用連續鑰匙資料K_{SES}，其是由相互證明所得到的共同鑰匙，且亦用於加密內容鑰匙資料Ｋｃ，使用儲存鑰匙資料K_{STR}與媒體鑰匙資料K_{MED}。共同鑰匙加密模組１４０８證明簽名資料並產生簽名資料，藉著使用欲被產生的簽名資料之共同鑰匙資料與雜亂值。

共同鑰匙加密模組１４０８可被實施作爲電路模組（Ｈ／Ｗ　ＩＰ解決），或可由ＣＰＵ１４００藉著執行儲存於非依電性記憶體１４０５中之共同鑰匙加密程式而被實施（Ｓ／Ｗ　ＩＰ解決）。

可由媒體ＳＡＭ模組１３３或媒體驅動ＳＡＭ２６０之共同鑰匙加密模組１４０８，藉著使用儲存鑰匙資料K_{STR}來執行加密內容鑰匙資料Ｋｃ。

雜亂功能模組１４０９是用於證明簽名資料，且用於產生欲被產生的簽名資料之資料的雜亂值。

（本質）隨機數目產生器１４１０是用於以例如媒體ＳＡＭ１３３來執行相互證明。

當存取儲存於記錄媒體１３０的ＲＡＭ區域或ＲＯＭ區域中之內容資料時，編碼／解碼模組１４２０執行處理於內容資料上，例如編碼、解碼、ＥＣＣ、調變、解調變

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（148）

、區格化、及解區格化。

儲存鑰匙資料產生模組1430產生各媒體之獨特的儲存鑰匙資料K_{STR}，藉著使用由媒體獨特ID產生模組1440產生的媒體獨特ID。

媒體獨特ID產生模組1440，從由媒體SAM133的SAM_ID與由媒體驅動SAM260產生的驅動ID，產生各記錄媒體之獨特的媒體獨特ID。

參見圖80之流程圖，以下敘述圖1所示之EMD系統100的整個操作。

在步驟S1中，於內容提供者101執行預定的登記之後，EMD服務中心102送出內容提供者101之公開鑰匙資料$K_{CP,P}$的公開鑰匙證明CER_{CP}。

於$SAM105_1$至105_4執行預定的登記處理之後，EMD服務中心102亦分別送出$SAM105_1$至105_4之公開鑰匙資料$K_{SAM1,P}$至$K_{SAM4,P}$的公開鑰匙證明CER_{CP1}至CER_{CP4}。

在進行相互證明之後，EMD服務中心102送出各具有一個月有效周期之三個月的執照鑰匙資料KD_1至KD_3至使用者家庭網路103之$SAM105_1$至105_4。

以此方式，在EMD系統100中，執照鑰匙資料KD_1至KD_3被事先分布至$SAM105_1$至105_4。如此使得$SAM105_1$至105_4可購買及利用從內容提供

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（149）

者１０１分布之安全容器１０４，藉著解碼安全容器１０４，即使ＳＡＭ１０５$_1$至１０５$_4$與ＥＭＤ服務中心１０２分離。在此情形中，購買與使用登錄被記錄在使用登錄資料１０８中，然後其被自動地送至ＥＭＤ服務中心１０２，當ＳＡＭ１０５$_1$至１０５$_4$被連接至ＥＭＤ服務中心１０２。於是ＥＭＤ服務中心１０２可以執行處理。如果ＥＭＤ服務中心１０２在預定周期中沒有接收使用登錄資料１０８，可以使對應的ＳＡＭ在撤銷列表中失效。ＵＣＳ資料１６６基本上是以即時從ＳＡＭ１０５$_1$至１０５$_4$被傳送至ＥＭＤ服務中心１０２。

在步驟Ｓ２中，於以ＥＭＤ服務中心１０２執行相互證明之後，內容提供者１０１授權ＵＣＰ資料１０６與內容鑰匙資料Ｋｃ，藉著將它們登記於ＥＭＤ服務中心１０２中。ＥＭＤ服務中心１０２亦產生六個月之鑰匙檔ＫＦ，並將它送至內容提供者１０１。

在步驟Ｓ３中，內容提供者１０１產生內容檔ＣＦ與其簽名資料ＳＩＧ$_{6,CP}$，如圖３Ａ所示，及鑰匙檔ＫＦ與簽名資料ＳＩＧ$_{7,CP}$，如圖３Ｂ所示。然後內容提供者１０１離線或線上將安全容器１０４送至ＳＡＭ１０５$_1$至１０５$_4$，在安全容器１０４中儲存上述檔案與資料，及圖３Ｃ所示之公開鑰匙證明資料ＣＥＲ$_{CP}$與其簽名資料ＳＩＧ$_{1,ESC}$。

線上送出安全容器１０４時，使用內容提供者１０１之特定協定以從內容提供者１０１分布安全容器１０４至

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（150）

使用者家庭網路１０３，以獨立於協定之格式（亦即，資料是藉著使用由許多層構成的通訊協定之預定層而被傳送）。離線送出安全容器１０４時，安全容器１０４是儲存於記錄媒體（ＲＯＭ或ＲＡＭ）上，且從內容提供者１０１被送至使用者家庭網路１０３。

然後，在步驟Ｓ４中，使用者家庭網路１０３之ＳＡＭ105_1至105_4檢查從內容提供者１０１分布的安全容器１０４內之簽名資料$SIG_{6,CP}$、$SIG_{7,CP}$、及$SIG_{K1,ESC}$，以證明鑰匙檔ＫＦ與內容檔ＣＦ之送出者與產生者的完整性。隨後，ＳＡＭ105_1至105_4解碼鑰匙檔ＫＦ，藉著使用對應周期的執照鑰匙資料KD_1至KD_6。

隨後，在步驟Ｓ５中，於ＳＡＭ105_1至105_4中，依據圖２２所示之操作單元１８５上之使用者操作，根據來自主ＣＰＵ８１０之內部中斷Ｓ８１０，決定購買與使用模式。

在此情形中，圖３７所示之使用監視器１８６根據儲存於安全容器１０４中之ＵＣＰ資料１０６，管理由使用者選定之內容檔ＣＦ的購買與使用模式。

在步驟Ｓ６中，圖３７所示之ＳＡＭ105_1至105_4的會計處理器１８７，產生其中記錄購買與使用模式之ＵＣＳ資料１６６與使用登錄資料１０８，並將它們送至ＥＭＤ服務中心１０２。

在步驟Ｓ７中，ＥＭＤ服務中心１０２根據使用登錄

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（151）

資料１０８執行會計處理，並產生處理要求資料１５２與處理報告資料１０７。ＥＭＤ服務中心１０２將處理要求資料１５２與其簽名資料ＳＩＧ$_{99}$經由圖１所示之給付閘道９０送至處理組織９１。ＥＭＤ服務中心１０２亦將處理報告資料１０７送至內容提供者１０１。

然後，在步驟Ｓ８中，於證明簽名資料ＳＩＧ$_{99}$之後，處理組織９１分配使用者之給付至內容權利擁有者，例如內容提供者１０１，根據處理要求資料１５２。

如上所述，ＥＭＤ系統１００中，圖３Ａ至３Ｃ所示之安全容器１０４從內容提供者１０１被分布至使用者家庭網路１０３，且安全容器１０４內的鑰匙檔ＫＦ被處理於ＳＡＭ１０５$_1$至１０５$_4$中。

儲存於鑰匙檔ＫＦ中之內容鑰匙資料Ｋ$_C$與ＵＣＰ資料１０６以執照鑰匙資料ＫＤ$_1$至ＫＤ$_3$被加密，且只在擁有執照鑰匙資料ＫＤ$_1$至ＫＤ$_3$之ＳＡＭ１０５$_1$至１０５$_4$中被解密。ＳＡＭ１０５$_1$至１０５$_4$是抗干預硬體，其中根據記錄於ＵＣＰ資料１０６中之內容資料Ｃ的處理內容，決定內容資料Ｃ之購買與使用模式。

所以，依據ＥＭＤ系統１００，內容資料Ｃ可在使用者家庭網路１０３中被購買與使用，根據由內容提供者１０１或內容權利擁有者所產生之ＵＣＰ資料１０６。

因此，在ＥＭＤ系統１００中，內容資料Ｃ可線上或離線從內容提供者１０１被分布至使用者家庭網路１０３，藉著將它儲存於安全容器１０４中。在此情形中，

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（152）

ＳＡＭ１０５$_{1}$至１０５$_{4}$中之內容資料Ｃ的權利處理不會被內容資料Ｃ是線上或離線送出影響。

在ＥＭＤ系統１００中，於使用者家庭網路１０３內的Ａ／Ｖ機器１６０$_{2}$至１６０$_{4}$與網路裝置１６０$_{1}$中，購買、使用、記錄及轉移內容資料Ｃ時，總是根據ＵＣＰ資料１０６執行處理。於是，可以建立與整個使用者家庭網路１０３共同的權利處理規則。

圖８１指出用於分布使用於第一實施例中之安全容器１０４的協定之例子。

在多處理器系統（ＥＭＤ系統）１００中，如圖８１所示，作爲從內容提供者１０１分布安全容器１０４至使用者家庭網路１０３之協定，可使用例如ＴＣＰ／ＩＰ與ＸＭＬ／ＳＭＩＬ。

作爲使用者家庭網路１０３的ＳＡＭ之間或使用者家庭網路１０３與１０３ａ之間，轉移安全容器１０４之協定，使用例如建造在１３９４－串聯匯流排／介面上之ＸＭＬ／ＳＭＩＬ。在此情形中，安全容器１０４可被儲存在記錄媒體（ＲＯＭ或ＲＡＭ）中，並在ＳＡＭ之間分布。

第二實施例

在第一實施例中，內容資料直接從內容提供者１０１被分布至使用者家庭網路１０３之ＳＡＭ１０５$_{1}$至１０５$_{4}$。在第二實施例中，內容資料經由服務提供者從內

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（153）

容提供者被分布至使用者家庭網路之ＳＡＭ。

圖８２是一方塊圖，指出第二實施例之ＥＭＤ系統３００。

ＥＭＤ系統３００如圖８２所示，包括：內容提供者３０１、ＥＭＤ服務中心３０２、使用者家庭網路３０３、服務提供者３１０、給付閘道９０及處理組織９１。

內容提供者３０１、ＥＭＤ服務中心３０２、ＳＡＭ１０５$_1$至１０５$_4$與服務提供者３１０分別對應本發明之資料提供裝置、管理裝置、資料處理裝置與資料分布裝置。

內容提供者３０１類似於第一實施例之內容提供者１０１，除了它供給內容資料至服務提供者３１０。

ＥＭＤ服務中心３０２類似於第一實施例之ＥＭＤ服務中心１０２，除了它不僅對於內容提供者１０１與ＳＡＭ３０５$_1$至３０５$_4$能，亦對於服務提供者３０１，實施證明功能、鑰匙資料管理功能、及權利處理功能。

使用者家庭網路３０３包括：網路裝置３６０$_1$與Ａ／Ｖ機器３６０$_2$至３６０$_4$。網路裝置３６０$_1$集積ＳＡＭ３０５$_1$與ＣＡ模組３１１於其中，且Ａ／Ｖ機器３６０$_2$至３６０$_4$集積ＳＡＭ３０５$_2$至３０５$_4$於其中。

ＳＡＭ３０５$_1$至３０５$_4$分別類似於第一實施例之ＳＡＭ１０５$_1$至１０５$_4$，除了它們從服務提供者３１０接收安全容器３０４，並證明服務提供者３１０與內容提供者３０１之簽名資料，且亦產生服務提供者３１０之服

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（154）

務－提供者（ＳＰ）購買登錄資料（資料分布裝置之資料）３０９。

ＥＭＤ系統３００之整體如下。

在ＥＭＤ系統３００中，內容提供者３０１傳送內容鑰匙資料Ｋｃ與ＵＣＰ資料１０６至ＥＭＤ服務中心３０２，內容鑰匙資料Ｋｃ與ＵＣＰ資料１０６是與第一實施例類似，且其指出內容資料之權利，例如欲被提供之內容資料Ｃ的執照同意條件，ＥＭＤ服務中心３０２是一高度可靠的授權組織。ＵＣＰ資料１０６與內容鑰匙資料Ｋｃ被授權（證明），藉著被登記於ＥＭＤ服務中心３０２中。

內容提供者３０１以內容鑰匙資料Ｋｃ加密內容資料Ｃ，以產生內容檔ＣＦ。內容提供者３０１對於來自ＥＭＤ服務中心３０２之各內容檔ＣＦ，接收六個月之鑰匙檔ＫＦ。

鑰匙檔ＫＦ包含簽名資料，用於證明鑰匙檔ＫＦ之完整性與鑰匙檔ＫＦ之送出者與產生者的完整性。

然後內容提供者３０１經由記錄媒體或線上經由一網路，例如網際網路，數位廣播，或藉著使用非正式協定，供給圖３Ａ至３Ｃ所示之安全容器１０４至服務提供者３１０，在安全容器１０４中儲存內容檔ＣＦ、鑰匙檔ＫＦ與簽名資料。

儲存於安全容器１０４中之簽名資料是用於證明對應的資料之完整性及資料的送出者與產生者之完整性。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（155）

於從內容提供者３０１接收安全容器１０４時，服務提供者３１０檢查簽名資料，以證明安全容器１０４之送出者與產生者的完整性。

然後服務提供者３１０產生價格標籤資料（ＰＴ）３１２至ＳＲＰ，對於服務提供者３１０所給予的服務例如授權服務加上價格而得到價格標籤資料（ＰＴ）３１２，其已被離線報告至服務提供者３１０，由內容提供者３０１所要的。

然後服務提供者３１０從安全容器１０４取出內容檔ＣＦ與鑰匙檔ＫＦ，並產生安全容器３０４，其中儲存內容檔ＣＦ、鑰匙檔ＫＦ、價格標籤資料３１２及其簽名資料$K_{SP,S}$。

以執照鑰匙資料KD_1至KD_6加密鑰匙檔ＫＦ，且服務提供者３１０無法看到鑰匙檔ＫＦ之內容或將它重寫，由於它沒擁有執照鑰匙資料KD_1至KD_6。

ＥＭＤ服務中心３０２亦藉著登記它而授權價格標籤資料３１２。

服務提供者３１０線上或離線分布安全容器３０４至使用者家庭網路３０３。如果安全容器３０４被離線供給，它被記錄在記錄媒體（ＲＯＭ），且直接被供給至$SAM105_1$至105_4。如果安全容器３０４被線上供給，服務提供者３１０首先以ＣＡ模組３１１執行相互證明，並藉著使用連續鑰匙資料K_{SES}加密安全容器３０４且將它送出。ＣＡ模組３１１接收安全容器３０４，且藉

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（156）

著使用連續鑰匙資料K_{SES}將它加密，然後將它轉移至SAM3051至3054。

在此情形中，作爲用於從內容提供者301將安全容器304送至使用者家庭網路303之通訊協定，對於數位廣播使用MHEG，且對於網際網路使用XML／SMIL／HTML。安全容器304被嵌入於對應的協定內，依據通道技術而與通訊協定（寫碼方法）無關。

因此，安全容器304之格式不必符合通訊協定，藉以增加選擇安全容器304之格式的彈性。

隨後，SAM3051至3054檢查儲存於安全容器304中之簽名資料，以證明儲存於安全容器304中之鑰匙檔KF與內容檔CF的完整性。然後SAM3051至3054解碼鑰匙檔KF，藉著使用從EMD服務中心302分布之對應的周期之執照鑰匙資料KD_1至KD_3。

在網路裝置3601與A／V機器3602至3604中，依據使用者操作，決定供給至SAM3051至3054之安全容器304的購買與使用模式，然後安全容器304可以被播放或記錄在記錄媒體上。

SAM3051至3054記錄安全容器304之購買與使用登錄作爲使用登錄資料308。使用登錄資料（登錄資料或管理－裝置登錄資料）308從使用者家庭網路303被送至EMD服務中心302，響應例如來自EMD服務中心302之要求。

於決定內容之購買模式時，SAM3051至3054

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（157）

將指出購買模式之ＵＣＳ資料１６６送至ＥＭＤ服務中心３０２。

ＥＭＤ服務中心３０２根據使用登錄資料３０８，決定（計算）各內容提供者３０１之會計內容，並根據計算的會計內容處理賬戶，藉著經由給付閘道９０使用處理組織９１，例如銀行。依據此處理，使用者家庭網路３０３之使用者對處理組織９１之給付被給至內容提供者３０１與服務提供者３１０，藉著由ＥＭＤ服務中心３０２執行的處理。

在此實施例中，ＥＭＤ服務中心３０２具有證明功能、鑰匙－資料管理功能及權利處理（利潤分配）功能。

特別是，ＥＭＤ服務中心３０２作爲位比根證明授權９２更低層的第二證明授權，其是中立最高授權，且證明公開鑰匙資料，藉著附著簽名至公開鑰匙資料的公開－鑰匙證明資料，藉著使用ＥＭＤ服務中心１０２之私人鑰匙資料。公開鑰匙資料是用於證明內容提供者３０１、服務提供者３１０、ＳＡＭ３０５$_1$至３０５$_4$中之簽名資料的完整性。如上所述，ＥＭＤ服務中心１０２登記並授權內容提供者３０１之ＵＣＰ資料１０６、內容鑰匙資料Ｋｃ及服務提供者３１０之價格標籤資料３１２，其亦是ＥＭＤ服務中心３０２的部份證明功能。

ＥＭＤ服務中心３０２亦具有管理鑰匙資料例如執照鑰匙資料ＫＤ$_1$至ＫＤ$_6$之管理功能。

ＥＭＤ服務中心３０２亦具有以下權利處理（利潤分

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（158）

配）功能。ＥＭＤ服務中心３０２處理使用者購買及使用內容之賬戶，根據由內容提供者３０１登記的ＵＣＰ資料１０６，從ＳＡＭ３０５$_1$至３０５$_4$輸入之使用登錄資料３０８，及由服務提供者３１０登記的價格標籤資料３１２，並分配使用者之給付至內容提供者３０１與服務提供者３１０。

內容提供者３０１之個別元件的細節如下。

〔內容提供者３０１〕

內容提供者３０１是與第一實施例之內容提供者１０１類似，除了它線上或離線供給圖３Ａ至３Ｃ所示的安全容器１０４至服務提供者３１０。

亦即，內容提供者３０１產生安全容器１０４，並依據圖１７至１９所示之處理，將它插入內容提供者之產品分布協定。

然後服務提供者３１０下載安全容器１０４，並從協定將它取出。

〔服務提供者３１０〕

服務提供者３１０產生安全容器３０４，其中儲存從內容提供者３０１供給之鑰匙檔ＫＦ與內容檔ＣＦ及價格標籤資料３１２，並將它線上或離線分布至使用者家庭網路３０３之Ａ／Ｖ機器３６０$_2$至３６０$_4$與網路裝置３６０$_1$。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（159）

服務提供者３１０分布內容之服務被分成兩種型式，亦即獨立服務與相依服務。

獨立服務爲用於個別地分布內容之下載服務。相依服務爲用於分布內容連同程式或商品（ＣＭ）之服務，例如供給戲劇節目之歌曲的內容，藉著將它插入於戲劇節目流中。如此使得使用者可購買儲存於流中之內容，同時觀看戲劇節目。

於從內容提供者３０１接收安全容器１０４時，服務提供者３１０依據以下處理產生安全容器３０４。

參見圖８３之流程圖，現在敘述由內容提供者３０１接收的安全容器１０４產生安全容器３０４，並將它分布至使用者家庭網路３０３之處理。

在步驟Ｓ８３－１中，服務提供者３１０線上或離線從內容提供者３０１接收圖３Ａ至３Ｃ所示之安全容器１０４，並將它儲存。

如果安全容器１０４被線上送出，藉著使用由內容提供者３０１與服務提供者３１０之間的相互證明所得到之連續鑰匙資料K_{SES}解碼安全容器１０４。

在步驟Ｓ８３－２中，服務提供者３１０藉著使用ＥＭＤ服務中心３０２之公開鑰匙資料$K_{ESC,P}$，證明安全容器１０４之圖３Ｃ所示的簽名資料$SIG_{1,ESC}$之完整性，然後從圖３Ｃ所示之公開－鑰匙證明資料CER_{CP}取出公開鑰匙資料$K_{CP,P}$。

然後服務提供者３１０分別檢查安全容器１０４之圖

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（160）

３Ａ與３Ｂ所示的簽名資料ＳＩＧ$_{6,CP}$與ＳＩＧ$_{7,CP}$，藉著使用取出的公開鑰匙資料Ｋ$_{CP,P}$，以證明鑰匙檔ＫＦ與內容檔ＣＦ之送出者與產生者的完整性。

服務提供者３１０亦檢查儲存於圖３Ｂ所示鑰匙檔ＫＦ中的簽名資料ＳＩＧ$_{K1,ESC}$，藉著使用公開鑰匙資料Ｋ$_{ESC,P}$，以證明鑰匙檔ＫＦ之產生者的完整性。此亦證明ＥＭＤ服務中心１０２中之鑰匙檔ＫＦ的正式登記。

隨後，在步驟Ｓ８３－３中，服務提供者３１０產生藉著將服務提供者３１０之服務的價格加至內容提供者３０１所要的ＲＳＰ所得到的價格標籤資料３１２，其已離線地從內容提供者３０１被報告。

藉著使用服務提供者３１０私人鑰匙資料Ｋ$_{SP,P}$，服務提供者３１０亦分別從價格標籤資料３１２、鑰匙檔ＫＦ、內容檔ＣＦ之雜亂值產生簽名資料ＳＩＧ$_{64,CP}$、ＳＩＧ$_{63,CP}$、ＳＩＧ$_{62,CP}$。

簽名資料ＳＩＧ$_{62,CP}$是用於證明內容檔ＣＦ之送出者的完整性，簽名資料ＳＩＧ$_{63,CP}$是用於證明鑰匙檔ＫＦ之送出者的完整性，且簽名資料ＳＩＧ$_{64,CP}$是用於證明價格標籤資料３１２之送出者與產生者的完整性。

然後服務提供者３１０產生安全容器３０４，其中儲存圖８４Ａ所示之簽名資料ＳＩＧ$_{6,CP}$與其簽名資料ＳＩＧ$_{62,CP}$，圖８４Ｂ所示之鑰匙檔ＫＦ與簽名資料ＳＩＧ$_{7,CP}$和簽名資料ＳＩＧ$_{63,ESC}$，圖８４Ｃ所示之價格標籤資料３１２與其簽名資料ＳＩＧ$_{64,SP}$，及圖

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（161）

８４Ｄ所示之公開鑰匙證明資料ＣＥＲ$_{SP}$與其簽名資料ＳＩＧ$_{61,ESC}$和公開鑰匙證明資料ＣＥＲ$_{CP}$與其簽名資料ＳＩＧ$_{1,ESC}$，並儲存產生的安全容器３０４於安全容器資料庫中。

儲存於安全容器資料庫中之安全容器３０４藉著使用例如內容ＩＤ而被服務提供者３１０集中地管理。

圖８４Ａ指出當ＤＳＰ被使用作爲用於解壓縮內容資料Ｃ之Ａ／Ｖ壓縮／解壓縮裝置時，內容檔ＣＦ之造形。ＤＳＰ解壓縮安全容器１０４內的內容資料Ｃ，且亦藉著使用Ａ／Ｖ解壓縮軟體及安全容器３０４內的數位水記資訊模組，嵌入及偵測數位水記資訊。如此使得內容提供者３０１可使用所要的壓縮方法及數位水記嵌入方法。

如果硬體或預先儲存的軟體被使用作爲用於解壓縮內容資料Ｃ及用於嵌入並偵測數位水記資訊之Ａ／Ｖ壓縮／解壓縮裝置，Ａ／Ｖ解壓縮軟體與數位水記資訊模組可不被儲存於內容檔ＣＦ內。

然後，在步驟Ｓ８３－４中，服務提供者３１０響應來自使用者家庭網路３０３之要求，從安全容器資料庫讀取安全容器３０４。

在此情形中，安全容器３０４可以是一複合容器，其中儲存許多內容檔ＣＦ與許多鑰匙檔ＫＦ。例如，在單一安全容器３０４中，可儲存許多關於一首音樂、視訊夾、字卡、筆記之內容檔ＣＦ。許多內容檔ＣＦ可被儲存於目錄構造之安全容器３０４中。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（162）

如果安全容器３０４經由數位廣播被送出，使用ＭＨＥＧ協定。如果安全容器３０４經由網際網路被送出，則使用ＸＭＬ／ＳＭＩＬ／ＨＴＭＬ協定。

在此情形中，安全容器１０４內的內容檔ＣＦ與鑰匙檔ＫＦ被儲存於使用在服務提供者３１０與使用者家庭網路３０３之間的通訊協定之預定層中，而與寫碼方法例如ＭＨＥＧ或ＨＴＭＬ協定無關。

例如，如果安全容器３０４如圖８５所示經由數位廣播被送出，內容檔ＣＦ被儲存作爲ＭＨＥＧ物件內之ＭＨＥＧ內容資料。

是電影之ＭＨＥＧ物件以傳輸層協定被儲存於封包化的基本流（ＰＥＳ）－視頻中，是聲音之ＭＨＥＧ物件是以傳輸層協定被儲存於ＰＥＳ－音頻中，且是靜止影像之ＭＨＥＧ物件被儲存於私人－資料中。

如圖８６所示，鑰匙檔ＫＦ、價格標籤資料３１２與公開鑰匙證明資料CER_{CP}、CER_{SP}被儲存於傳輸層協定之ＴＳ封包內之處理控制訊息（ＥＣＭ）中。

內容檔ＣＦ、鑰匙檔ＫＦ、價格標籤資料３１２與公開鑰匙證明資料CER_{CP}、CER_{SP}，被內容檔ＣＦ之標頭內的目錄構造資料DSD_1鏈接。

然後，服務提供者３１０線上及／或離線供給安全容器３０４至使用者家庭網路３０３。

如果安全容器３０４被分布至使用者家庭網路３０３之網路裝置360_1，服務提供者３１０加密安全容器

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（163）

３０４，藉著在執行相互證明之後使用連續鑰匙資料K_{SES}，然後經由網路將它分布至網路裝置３６０１。

如果經由衛星廣播安全容器３０４，服務提供者３１０以擾頻鑰匙資料K_{SCR}加密安全容器３０４。擾頻鑰匙資料K_{SCR}亦以工作鑰匙資料K_W被加密，且工作鑰匙資料K_W以主人鑰匙資料K_M被加密。

然後經由衛星服務提供者３１０送出擾頻鑰匙資料K_{SCR}與工作鑰匙資料K_W連同安全容器３０４至使用者家庭網路３０３。服務提供者３１０亦離線分布主人鑰匙資料K_M至使用者家庭網路３０３，藉著將它儲存於例如ＩＣ卡中。

於從使用者家庭網路３０３接收關於內容資料Ｃ之ＳＰ購買登錄資料３０９時，服務提供者３１０將它儲存。

於決定未來服務時，服務提供者３１０參考ＳＰ購買登錄資料３０９。服務提供者３１０亦根據ＳＰ購買登錄資料３０９，分析已送出ＳＰ購買登錄資料３０９之ＳＡＭ3051至3054的使用者喜愛，然後產生使用者喜愛檔案資料９００，並將它送至使用者家庭網路３０３之ＣＡ模組３１１。

服務提供者３１０或服務提供者相關組織離線登記於ＥＭＤ服務中心３０２中，並得到全球獨特辨識ＳＰ＿ＩＤ，藉著使用服務提供者３１０之ＩＤ證明，或用於執行處理之銀行賬戶。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（164）

服務提供者３１０亦授權價格標籤資料３１２，藉著將它登記於ＥＭＤ服務中心３０２中。

〔ＥＭＤ服務中心３０２〕

如上所討論，ＥＭＤ服務中心３０２作爲證明授權（ＣＡ）、鑰匙管理授權與權利處理（權利清除）授權。

圖８７指出ＥＭＤ服務中心３０２之主要功能。如圖８７所示，ＥＭＤ服務中心３０２執行處理，例如供給執照鑰匙資料至內容提供者３０１與$SAM305_1$至3054_4，發出公開鑰匙證明資料CER_{CP}、CER_{SP}、及CER_{SAM1}至CER_{SAM4}，產生鑰匙檔ＫＦ，及根據使用登錄資料３０８之處理（利潤分配）。

在上述功能之間，供給執照鑰匙資料，發出公開鑰匙證明資料CER_{CP}與CER_{SAM1}至CER_{SAM4}，及產生鑰匙檔ＫＦ，是與第一實施例之ＥＭＤ服務中心１０２相同。

然而，不像ＥＭＤ服務中心１０２，ＥＭＤ服務中心３０２發出服務提供者３１０之公開鑰匙證明資料CER_{SP}，且亦根據使用登錄資料３０８，分配由$SAM305_1$至3054_4中的內容資料Ｃ之購買所得到的利潤至內容提供者３０１、內容提供者權利擁有者、服務提供者３１０與服務提供者權利擁有者。

使用登錄資料３０８之內容可爲如圖２１所示。

ＥＭＤ服務中心３０２亦產生使用者喜愛檔案資料

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（165）

９００，依據已送出使用登錄資料３０８之ＳＡＭ３０５$_1$至３０５$_4$之使用者喜愛，用於選定內容資料Ｃ，並經由ＳＡＭ管理器１４９將它送至ＳＡＭ３０５$_1$至３０５$_4$。

〔使用者家庭網路３０３〕

如圖８２所示，使用者家庭網路３０３包括網路裝置３６０$_1$及Ａ／Ｖ機器３６０$_2$至３６０$_4$。

網路裝置３６０$_1$將ＣＡ模組３１１與ＳＡＭ３０５$_1$集積於其中。Ａ／Ｖ機器３６０$_2$至３６０$_4$分別集積ＳＡＭ３０５$_1$至３０５$_4$。ＳＡＭ３０５$_1$至３０５$_4$經由匯流排１９１例如１３９４－串聯介面匯流排彼此連接。

Ａ／Ｖ機器３６０$_2$至３６０$_4$可設有網路通訊功能，雖然它不是主要的。如果沒有提供網路通訊功能，Ａ／Ｖ機器３６０$_2$至３６０$_4$可經由匯流排１９１使用網路裝置３６０$_1$之網路通訊功能。另一種方式，使用者家庭網路３０３可只包括不具有網路功能之Ａ／Ｖ機器。

網路裝置３６０$_1$之細節如下。

圖８８是一方塊圖，指出網路裝置３６０$_1$。如圖８８所示，網路裝置３６０$_1$包括通訊模組１６２、ＣＡ模組３１１、解碼模組９０５、ＳＡＭ３０５$_1$、Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３、操作單元１６５、下載記憶體１６７、播放模組１６９、外部記憶體２０１、主ＣＰＵ８１０。與圖２２相同的元件是以相同的參考數字來表示。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（166)

通訊模組１６２執行與服務提供者３１０通訊之處理。特別是，通訊模組１６２經由例如衛星廣播，將從服務提供者３１０接收的安全容器３０４輸出至解碼模組９０５。通訊模組１６２亦經由例如電話線，將從服務提供者３１０接收的使用者喜愛檔案資料９００輸出至ＣＡ模組３１１，且亦經由例如電話線將從ＣＡ模組３１１接收的ＳＰ購買登錄資料３０９送至服務提供者３１０。

圖８９是一功能區塊，指出ＣＡ模組３１１與解碼模組９０５。

如圖８９所示，ＣＡ模組３１１包括：相互證明單元９０６、儲存單元９０７、加密／解密單元９０８、及ＳＰ購買登錄資料產生器９０９。

於經由電話線在ＣＡ模組３１１與服務提供者３１０之間送出及接收資料時，相互證明單元９０６以服務提供者３１０執行相互證明，以產生連續鑰匙資料K_{SES}，並將它輸出至加密／解密單元９０８。

在服務提供者３１０已與使用者做成合約之後，儲存單元９０７儲存從服務提供者３１０離線供給之主人鑰匙資料K_M，藉著被儲存於ＩＣ卡９１２中。

加密／解密單元９０８從解碼模組９０５之解碼器９１０接收加密的擾頻鑰匙資料K_{SCR}與工作鑰匙資料K_W，並藉著使用從儲存單元９０７讀取的主人鑰匙資料K_M來解密工作鑰匙資料K_W。

藉著通訊模組１６２經由例如電話線，加密／解密單

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（167）

元９０８亦解密從服務提供者３１０接收的使用者喜愛檔案資料９００，藉著使用來自相互證明單元９０６之連續鑰匙資料K_{SES}，並將它輸出至解碼模組９０５之安全容器選定單元９１１。

加密／解密單元９０８解密從ＳＰ購買登錄資料產生器９０９接收的ＳＰ購買登錄資料３０９，藉著使用來自相互證明單元９０６之連續鑰匙資料K_{SES}，並經由通訊模組１６２將它送至服務提供者３１０。

ＳＰ購買登錄資料產生器９０９產生ＳＰ購買登錄資料３０９，指出服務提供者３１０之獨特內容資料Ｃ之購買登錄，根據藉著執行使用者操作於圖８８所示之操作單元１６５上所得到的操作信號Ｓ１６５，或根據來自$SAM305_1$之ＵＣＳ資料１６６。然後ＳＰ購買登錄資料產生器９０９輸出ＳＰ購買登錄資料３０９至加密／解密單元９０８。

ＳＰ購買登錄資料３０９包括服務提供者３１０之分布服務上的資訊，反應使用者之意見，月基本費（使用網路所發生），合約（更新）資料及購買登錄資訊。

ＣＡ模組３１１與服務提供者３１０之會計資料庫通訊，如果服務提供者３１０具有會計功能，客戶管理資料庫及市場資訊資料庫。在此情形中，ＣＡ模組３１１將用於分布內容資料Ｃ之服務的會計資料送至服務提供者３１０。

解碼模組９０５包括解碼器９１０及安全容器選定單

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（168）

元９１１。

解碼器９１０從通訊模組１６２接收加密的安全容器３０４、擾頻鑰匙資料K_{SCR}、及工作鑰匙資料K_W。然後解碼器９１０將加密的擾頻鑰匙資料K_{SCR}及工作鑰匙資料K_W輸出至ＣＡ模組３１１之加密／解密單元９０８，並從加密／解密單元９０８接收解密的擾頻鑰匙資料K_{SCR}。解碼器９１０亦解密加密的安全容器３０４，藉著使用擾頻鑰匙資料K_{SCR}，然後將它輸出至安全容器選定單元９１１。

如果依據ＭＰＥＧ２傳輸流方法，安全容器３０４從服務提供者３１０被送出，解碼器９１０從ＴＳ封包取出擾頻鑰匙資料K_{SCR}，並從ＥＭＭ取出工作鑰匙資料K_W。

ＥＣＭ亦包含各通道之節目屬性資訊。ＥＭＭ亦包含各使用者（觀看者）之展示合約資訊。

安全容器選定單元９１１過濾從解碼器９１０接收之安全容器３０４，藉著使用從ＣＡ模組３１１接收之使用者喜愛檔案資料９００，以依據使用者之喜愛選定安全容器１０４，並將它輸出至$SAM305_1$。

以下詳細討論$SAM305_1$。

$SAM305_1$之功能與構造基本上與圖２２至７２所述之第一實施例的$SAM105_1$類似，除了它執行不僅內容提供者３０１之處理，亦執行服務提供者３１０之處理，例如檢查服務提供者３１０之簽名。

$SAM305_1$至$SAM305_4$是模組，用於執行與ＥＭＤ

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（169）

服務中心３０２之通訊及各內容之會計。

圖６３所示之使用者家庭網路１０３的造形可應用於使用者家庭網路３０３內之裝置。圖６８至７９所示之權利處理ＳＡＭ、媒體ＳＡＭ１３３、Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３及媒體驅動ＳＡＭ２６０之造形可應用於使用者家庭網路３０３內之ＳＡＭ３０５$_1$至３０５$_4$。

ＳＡＭ３０５$_2$至３０５$_4$基本上具有與ＳＡＭ３０５$_1$相同的功能。

ＳＡＭ３０５$_1$之功能的細節如下。

圖９０是一方塊圖，指出ＳＡＭ３０５$_1$之功能，且亦指出與從服務提供者３１０接收安全容器３０４之處理相關的資料流。

如圖９０所示，ＳＡＭ３０５$_1$包括：相互證明單元１７０、加密／解密單元１７１、１７２、１７３、下載記憶體管理器１８２、Ａ／Ｖ壓縮／解壓縮ＳＡＭ管理器１８４、ＥＭＤ服務中心管理器１８５、使用監視器１８６、ＳＡＭ管理器１９０、儲存單元１９２、媒體ＳＡＭ管理器１９７、工作記憶體２００、服務提供者管理器５８０、會計處理器５８７、簽名處理器５８９、外部記憶體管理器８１１及ＣＰＵ１１００。

如同在ＳＡＭ１０５$_1$之情形中，圖９０所示之ＳＡＭ３０５$_1$之預定功能，由ＣＰＵ藉著執行私人程式而實施。

圖９０中，與圖３０所示相同的功能區塊是以相同的

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（170）

參考數字表示。

在圖８８所示外部記憶體２０１中，使用登錄資料３０８與ＳＡＭ登記列表被儲存，藉著執行第一實施例中所討論之處理及以下討論之處理。

如圖９１所示，在工作記憶體２００中，儲存內容鑰匙資料K_C、ＵＣＰ資料１０６、儲存單元１９２之鎖鑰匙資料K_{LOC}、內容提供者３０１之公開鑰匙證明資料CER_{CP}、服務提供者３１０之公開鑰匙證明資料CER_{SP}、ＵＣＳ資料１６６、ＳＡＭ程式下載容器SDC_1至SDC_3及價格標籤資料３１２。

在ＳＡＭ305_1的功能區塊之間，以下只說明圖９０中之第二實施例之獨特的功能區塊。

簽名處理器５８９證明安全容器３０４內之簽名資料，藉著使用ＥＭＤ服務中心３０２之公開鑰匙資料$K_{ESC,P}$，內容提供者３０１之公開鑰匙資料$K_{CP,P}$，及服務提供者３１０之公開鑰匙資料$K_{SP,P}$，全部均從工作記憶體２００或儲存單元１９２被讀取。

如圖９２所示，當ＣＰＵ１１００依據使用者之操作，從主ＣＰＵ８１０接收內部中斷Ｓ８１０時，在ＣＰＵ１１００之控制下，會計處理器５８７執行會計處理，根據從工作記憶體２００讀取的價格標籤資料３１２，依據內容的內容購買與使用模式。

指出內容資料之銷售價格至使用者的價格標籤資料３１２，於由使用者決定內容資料之購買模式時，經由預

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（171）

定的輸出機構，被輸出至ＳＡＭ３０５１之外部。

在使用監視器１８６之監視下，根據權利之內容，例如由ＵＣＳ資料１６６與ＵＣＰ資料１０６指出的執照同意條件，執行會計處理器５８７。亦即，使用者能購買及使用權利允許內的內容。

於執行會計處理時，會計處理器５８７產生或更新使用登錄資料３０８，並經由外部記憶體管理器８１１將它寫入外部記憶體２０１。

使用登錄資料３０８以及第一實施例中使用之使用登錄資料１０８，是用於由ＥＭＤ服務中心３０２決定安全容器３０４之執照費用的給付。

會計處理器５８７亦產生ＵＣＳ資料１６６，指出在ＣＰＵ１１００之控制下由使用者決定的內容之購買與使用模式，並將它寫入工作記憶體２００。

內容之購買模式包括”賣斷”，其中購買者之使用的拷貝及購買者之播放操作沒有限制，”以播放付費”，其中每次內容被播放時收費。

於使用者決定購買模式時，產生ＵＣＳ資料１６６，且ＵＣＳ資料１６６是用於控制內容之使用，以確保使用者在權利允許內使用內容。在ＵＣＳ資料１６６中，儲存內容ＩＤ、購買模式、賣斷價格、已購買內容之ＳＡＭ的ＳＡＭ＿ＩＤ、已購買內容之使用者的ＵＳＥＲ＿ＩＤ等等。

如果決定的購買模式是”以播放付費”，”以

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（172）

ＳＣＭＳ付費”或”無拷貝看護之以拷貝Ｎ次付費”，ＳＡＭ３０５１將ＵＣＳ資料１６６即時送至服務提供者３１０，且服務提供者３１０指示ＥＭＤ服務中心３０２從ＳＡＭ３０５１得到使用登錄資料３０８。

如果決定的購買模式是”賣斷”，ＵＣＳ資料１６６即時被送至服務提供者３１０與ＥＭＤ服務中心３０２。

如圖９０所示，在ＳＡＭ３０５１中，經由ＥＭＤ服務中心管理器１８５從ＥＭＤ服務中心３０２接收的使用者喜愛檔案資料９００，被輸出至服務提供者管理器５８０。然後，在服務提供者管理器５８０中，選定已從圖８９所示之解碼模組９０５被接收且根據使用者喜愛檔案資料９００被過濾之安全容器３０４，且選定的安全容器３０４被輸出至下載記憶體管理器１８２。如此使得ＳＡＭ３０５１可選定依據使用者之喜愛之內容資料Ｃ，根據從已與使用者簽約之全部服務提供者３１０得到的內容資料Ｃ之購買。

ＳＡＭ３０５１內之處理流程如下。

當接收執照鑰匙資料時執行之處理

ＳＡＭ３０５１內將從ＥＭＤ服務中心３０２接收的執照鑰匙資料ＫＤ１至ＫＤ３儲存於儲存單元１９２之處理流程是與圖３５所討論之第一實施例類似。

當從服務提供者３１０接收安全容器３０４時執行之處理

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（173）

參見圖９３，以下敘述當從服務提供者３１０接收安全容器３０４時，ＳＡＭ３０５１內之處理流程。

在以下例子中，於ＳＡＭ３０５１中，當接收安全容器３０４時，檢查不同型式之簽名資料。然而，當決定購買與使用模式而非當接收安全容器３０４時，可檢查簽名資料。

在步驟Ｓ９３－０中，圖９０所示之ＳＡＭ３０５１之ＣＰＵ１１００從主ＣＰＵ８１０接收內部中斷Ｓ８１０，指出執行處理以接收安全容器之指示。

在步驟Ｓ９３－１中，圖９０所示之ＳＡＭ３０５１之相互證明單元１７０以服務提供者３１０執行相互證明。

然後，在步驟Ｓ９３－２中，ＳＡＭ３０５１之相互證明單元１７０以下載記憶體１６７之媒體ＳＡＭ１６７ａ進行相互證明。

在步驟Ｓ９３－３中，從服務提供者３１０接收的安全容器３０４被寫入下載記憶體１６７。同時，安全容器３０４在相互證明單元１７０中被加密，且藉著使用步驟Ｓ９３－２中得到之連續鑰匙資料，在媒體ＳＡＭ１６７ａ中加密安全容器３０４。

在步驟Ｓ９３－４中，ＳＡＭ３０５１解碼安全容器３０４，藉著使用步驟Ｓ９３－１中得到之連續鑰匙資料。

同時，在步驟Ｓ９３－５中，簽名處理器５８９證明圖４０Ｄ所示之簽名資料ＳＩＧ$_{61,ESC}$，然後證明簽名

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（174）

資料SIG62,SP、SIG63,SP、SIG64,SP，藉著使用儲存於圖84D所示之公開鑰匙證明資料CERSP中之服務提供者310的公開鑰匙資料KSP,P。

當證明簽名資料SIG62,SP之完整性時，證明內容檔CF之送出者的完整性。當證明簽名資料SIG63,SP之完整性時，證明鑰匙檔KF之送出者的完整性。當證明簽名資料SIG64,SP之完整性時，證明價格標籤資料312之送出者與產生者的完整性。

在步驟S93－6中，簽名處理器589證明圖84D中所示之簽名資料SIG1,ESC，然後證明簽名資料SIG6,CP與SIG7,CP，藉著使用儲存於84D所示之公開鑰匙證明資料CERCP中之內容提供者301的公開鑰匙資料KCP,P。

當證明簽名資料SIG6,CP之完整性時，證明內容檔CF之送出者與產生者的完整性。當證明簽名資料SIG7,CP之完整性時，證明鑰匙檔KF之送出者的完整性。

在步驟S93－7中，簽名處理器589檢查圖84B所示之鑰匙檔KF內的簽名資料SIGK1,ESC，藉著使用從儲存單元192讀取的公開鑰匙資料KESC,P，以證明EMD服務中心302中之鑰匙檔KF的正式登記與鑰匙檔KF之產生者的完整性。

然後，在步驟S93－8中，加密／解密（解碼）單元172解密內容鑰匙資料Kc，UCP資料106及圖

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

五、發明說明（175）

８４Ｂ所示之鑰匙檔ＫＦ內的ＳＡＭ程式下載容器ＳＤＣ$_1$至ＳＤＣ$_3$，藉著使用從儲存單元１９２讀取的對應周期之執照鑰匙資料ＫＤ$_1$至ＫＤ$_3$，並將它們寫入工作記憶體２００。

在步驟Ｓ９３－９中，ＣＰＵ１１００決定是否接收安全容器之上述處理已被正確地執行，並經由外部中斷報告對應資訊至主ＣＰＵ８１０。

另一種方式，ＣＰＵ１１００可設定一旗標於ＳＡＭ狀態暫存器中，指出是否上述處理已被適當地執行，且主ＣＰＵ８１０可藉投票讀取旗標。

決定下載的安全容器之購買模式之處理

決定下載的安全容器之購買模式之處理基本上是與圖３８所述之第一實施例的ＳＡＭ１０５$_1$所執行之處理類似。依據此處理，圖９７Ｃ所示之鑰匙檔ＫＦ$_1$，討論於後，經由工作記憶體２００與下載記憶體管理器１８２被儲存於下載記憶體１６７中。

內容資料之播放處理

儲存於１６７中之決定購買模式之內容資料的播放處理，基本上是與圖４０所述之第一實施例的ＳＡＭ１０５$_1$所執行之處理類似。

當一機器之ＵＣＳ資料１６６被用於重新購買另一機器中

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（176）

之內容時所執行之處理

如圖９４所示，在決定被下載進入網路裝置３６０$_1$之下載記憶體１６７的內容檔ＣＦ之購買模式之後，產生儲存內容檔ＣＦ之新安全容器３０４ｘ，且新安全容器３０４ｘ經由匯流排１９１從ＳＡＭ３０５$_1$至３０５$_4$被轉移至Ａ／Ｖ機器３６０$_2$。參見圖９５與９６以下討論ＳＡＭ３０５$_1$中之此處理。

執行圖９６之流程圖所指示之處理，假設圖９７Ｃ所示之鑰匙檔ＫＦ$_1$與雜亂值Ｈ$_{K1}$依據上述購買處理被儲存於ＳＡＭ３０５$_1$之工作記憶體２００中。

在步驟Ｓ９６－１中，依據在圖８８與９４所示之操作單元１６５上的使用者之操作，做成指示轉移已決定購買模式之安全容器至ＳＡＭ３０５$_2$之內部中斷Ｓ８１０，從主ＣＰＵ８１０被輸出至圖９５所示之ＣＰＵ１１００。會計處理器５８７在ＣＰＵ１１００之控制下，依據決定的購買模式，更新儲存於外部記憶體２０１中之使用登錄資料３０８。

在步驟Ｓ９６－２中，ＳＡＭ３０５$_1$檢查第一實施例所討論之ＳＡＭ登記列表，以決定是否接收安全容器之ＳＡＭ３０５$_2$被正式地登記。如果是的話，ＳＡＭ３０５$_1$執行步驟Ｓ９６－３之處理。ＳＡＭ３０５$_1$亦決定是否ＳＡＭ３０５$_2$是使用者家庭網路３０３內的ＳＡＭ。

然後，在步驟Ｓ９６－３中，相互證明單元１７０分

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（177）

享由ＳＡＭ３０５$_2$之相互證明所得到的連續鑰匙資料K_{SES}。

在步驟Ｓ９６－４中，ＳＡＭ管理器１９０從下載記憶體２１１讀取圖８４Ａ所示之內容檔ＣＦ及簽名資料$SIG_{6,CP}$與$SIG_{7,CP}$，並使簽名處理器１８９產生簽名資料$SIG_{41,SAM1}$，藉著使用ＳＡＭ３０５$_1$之私人鑰匙資料K_{SAM1}。

在步驟Ｓ９６－５中，ＳＡＭ管理器１９０從下載記憶體２１１讀取圖８４Ｂ所示之鑰匙檔ＫＦ及簽名資料$SIG_{7,CP}$與$SIG_{63,SP}$，並使簽名處理器５８９產生簽名資料$SIG_{42,SAM1}$，藉著使用ＳＡＭ３０５$_1$之私人鑰匙資料K_{SAM1}。

隨後，在步驟Ｓ９６－６中，ＳＡＭ管理器１９０產生圖９７Ａ至９７Ｅ所示之安全容器３０４ｘ。

在步驟Ｓ９６－７中，加密／解密單元１７１加密圖９７Ａ至９７Ｅ所示之安全容器３０４ｘ，藉著使用步驟Ｓ９６－３所得到之連續鑰匙資料K_{SES}。

然後，在步驟Ｓ９６－８中，ＳＡＭ管理器１９０輸出安全容器３０４ｘ至圖９４所示之網路裝置３６０$_2$之ＳＡＭ３０５$_2$。在此情形中，執行不僅ＳＡＭ３０５$_1$與３０５$_2$之間的相互證明，亦執行匯流排１９１之相互證明。

在步驟Ｓ９６－９中，ＣＰＵ１１００決定是否用於轉移安全容器３０４ｘ之上述處理已被正確地執行，並經

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（178）

由外部中斷報告對應的資訊至主ＣＰＵ８１０。

另一種方式，ＣＰＵ１１００可設定一旗標於ＳＡＭ狀態暫存器中，指出是否上述處理已被精確地執行，且主ＣＰＵ８１０可藉投票讀取旗標。

參見圖９８，現在敘述當將從ＳＡＭ３０５$_1$輸入之圖９７Ａ至９７Ｅ所示的安全容器３０４ｘ寫入記錄媒體（ＲＡＭ）１３０$_4$，如圖９４所示，在ＳＡＭ３０５$_2$內的處理流程。

圖９９與１００爲流程圖，指出上述處理。如圖１４所示，記錄媒體（ＲＡＭ）１３０$_4$包括不安全ＲＡＭ區域１３４、媒體ＳＡＭ１３３及安全ＲＡＭ區域１３２。

在步驟Ｓ９９－０中，圖９８所示之ＳＡＭ３０５$_2$的ＣＰＵ１１００從主ＣＰＵ８１０接收內部中斷Ｓ８１０，指出記錄決定購買模式之接收的安全容器於記錄媒體上之指示。

然後，在步驟Ｓ９９－１中，ＳＡＭ３０５$_2$檢查ＳＡＭ登記列表，以決定是否已送出安全容器之ＳＡＭ３０５$_1$被正式地登記。如果是的話，ＳＡＭ３０５$_2$執行步驟Ｓ９９－２。ＳＡＭ３０５$_2$亦決定是否ＳＡＭ３０５$_1$是使用者家庭網路３０３內的ＳＡＭ。

在步驟Ｓ９９－２中，作爲對應步驟Ｓ９６－３之處理，ＳＡＭ３０５$_2$分享藉著以ＳＡＭ３０５$_1$執行相互證明所得到的連續鑰匙資料K_{SES}。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（179）

然後，如圖９４所示，在步驟Ｓ９９－３中，ＳＡＭ３０５$_2$之ＳＡＭ管理器１９０從網路裝置３６０$_1$之ＳＡＭ３０５$_1$接收安全容器３０４ｘ。

在步驟Ｓ９９－４中，加密／解密單元１７１解密經由ＳＡＭ管理器１９０接收的安全容器３０４ｘ，藉著使用步驟Ｓ９９－２中分享的連續鑰匙資料K_{SES}。

隨後，在步驟Ｓ９９－５中，藉著圖９４所示之媒體驅動ＳＡＭ２６０，加密的安全容器３０４ｘ內之內容檔ＣＦ進行處理，例如區格化，加入區格標頭，擾頻，ＥＣＣ編碼，調變，及同步化，然後被記錄於記錄媒體（ＲＡＭ）１３０$_4$之ＲＡＭ區域１３４上。

在步驟Ｓ９９－６中，以連續鑰匙資料K_{SES}加密的安全容器３０４ｘ內之簽名資料$SIG_{6,CP}$、$SIG_{62,SP}$與$SIG_{41,SAM1}$，鑰匙檔ＫＦ與簽名資料$SIG_{7,CP}$、$SIG_{63,SP}$與$SIG_{42,SAM1}$，鑰匙檔KF_1與雜亂值H_{K1}，公開鑰匙簽名資料CER_{SP}與簽名資料$SIG_{61,ESC}$，公開鑰匙簽名資料CER_{CP}與簽名資料$SIG_{1,ESC}$，及公開鑰匙簽名資料CER_{SAM1}與簽名資料$SIG_{22,ESC}$，被寫入工作記憶體２００。

在步驟Ｓ９９－７中，於簽名處理器５８９中，藉著使用從儲存單元１９２讀取的公開鑰匙資料$K_{ESC,P}$，檢查從工作記憶體２００讀取的簽名資料$SIG_{61,ESC}$、$SIG_{1,ESC}$與$SIG_{22,ESC}$，以證明公開鑰匙資料CER_{SP}、CER_{CP}、CER_{SAM1}之完整性。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（180）

然後，在簽名處理器589中，藉著使用儲存於公開鑰匙證明資料CER_{CP}中之公開鑰匙資料$K_{CP,P}$，證明簽名資料$SIG_{6,CP}$之完整性，以證明內容檔CF之產生者的完整性。而且在簽名處理器589中，藉著使用儲存於公開鑰匙證明資料CER_{SP}中之公開鑰匙資料$K_{SP,P}$，證明簽名資料$SIG_{62,SP}$之完整性，以證明內容檔CF之送出者的完整性。簽名處理器589藉著使用儲存於公開鑰匙證明資料CER_{SAM1}之公開鑰匙資料$K_{SAM1,P}$，證明簽名資料$SIG_{41,SAM1}$之完整性，以證明內容檔CF之送出者的完整性。

在步驟S99－8中，於簽名處理器589中，分別藉著使用儲存於公開鑰匙證明資料CER_{CP}、CER_{SP}、CER_{SAM1}中之公開鑰匙資料$K_{CP,P}$、$K_{SP,P}$、$K_{SAM1,P}$，證明儲存於工作記憶體200中之簽名資料$SIG_{7,CP}$、$SIG_{63,SP}$、$SIG_{42,SAM1}$之完整性，以證明內容檔CF之產生者的完整性。

然後，在步驟S99－9中，於簽名處理器589中，藉著使用從儲存單元192讀取的公開鑰匙資料$K_{ESC,P}$，證明儲存於圖97B所示之鑰匙檔KF中之簽名資料$SIG_{K1,ESC}$之完整性，以證明鑰匙檔KF之產生者的完整性。

在步驟S99－10中，簽名處理器589檢查雜亂值H_{K1}之完整性，以證明鑰匙檔KF_1之送出者與產生者的完整性。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（181）

在此實施例中，鑰匙檔ＫＦ$_1$之送出者與產生者是相同的。然而，如果它們是不同，產生送出者之簽名資料與產生者之簽名資料，且在簽名處理器５８９中證明兩個簽名資料之完整性。

在步驟Ｓ９９－１１中，使用監視器１８６開始控制內容資料Ｃ之購買與使用模式，藉著使用儲存於步驟Ｓ９９－１０中解密的鑰匙檔ＫＦ$_1$中之ＵＣＳ資料１６６。

然後，在步驟Ｓ９９－１２中，使用者決定購買模式，藉著操作操作單元１６５，且對應的操作信號Ｓ１６５被輸出至會計處理器５８７。

在步驟Ｓ９９－１３中，會計處理器５８７根據操作信號Ｓ１６５，更新儲存外部記憶體２０１中之使用登錄資料３０８。每次決定內容資料Ｃ之購買模式時，依據決定的購買模式，會計處理器５８７亦更新ＵＣＳ資料１６６。

隨後，在步驟Ｓ９９－１４中，加密／解密單元１７３加密步驟Ｓ９９－１２中產生的ＵＣＳ資料１６６，藉著依序地使用從儲存單元１９２讀取的購買者鑰匙資料Ｋ$_{PIN}$、儲存鑰匙資料Ｋ$_{STR}$、媒體鑰匙資料Ｋ$_{MED}$，並將加密的ＵＣＳ資料１６６輸出至媒體驅動ＡＭ管理器８５５。

在步驟Ｓ９９－１５中，媒體驅動ＡＭ管理器８５５在儲存新ＵＣＳ資料１６６之鑰匙檔ＫＦ$_1$上執行處理，例

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（182）

如區格化，加入區格標頭，擾頻，ＥＣＣ編碼，調變，及同步化，然後將它記錄於記錄媒體（ＲＡＭ）１３０$_4$之ＲＡＭ區域１３４上。

隨後，在步驟Ｓ９９－１６中，從工作記憶體２００讀取鑰匙檔ＫＦ，且經由媒體驅動ＡＭ管理器８５５，藉著圖９４所示之媒體驅動ＳＡＭ２６０，鑰匙檔ＫＦ被寫入記錄媒體（ＲＡＭ）１３０$_4$之安全ＲＡＭ區域１３２中。

在步驟Ｓ９９－１７中，ＣＰＵ１１００決定是否上述處理已被正確地執行，並經由外部中斷報告對應的資訊至主ＣＰＵ８１０。

另一種方式，ＣＰＵ１１００可設定一旗標於ＳＡＭ狀態暫存器中，指出是否上述處理已被正確地執行，且主ＣＰＵ８１０可藉投票讀取旗標。

記錄媒體（ＲＯＭ）決定內容資料的購買模式之處理，及在決定內容資料的購買模式之後將內容資料寫入記錄媒體（ＲＡＭ）之處理，是與第一實施例之ＳＡＭ３０５$_1$所執行之處理類似，除了由服務提供者３１０檢查藉著使用私人鑰匙資料$K_{SP,P}$附著的簽名資料SIG_{SP}。

實施ＳＡＭ３０５$_1$之方法是與第一實施例之ＳＡＭ１０５$_1$類似。

第一實施例所討論的使用者家庭網路１０３之造形，可應用於使用者家庭網路３０３所使用之裝置。在此情形中，圖６４至７９所討論之第一實施例的造形可應用於

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（183）

ＳＡＭ３０５$_1$之電路模組、Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３、媒體驅動ＳＡＭ２６０及媒體ＳＡＭ１３３。

類似地，圖６２所述之安全功能可應用於ＥＭＤ系統３００，除了以服務提供者３１０取代內容提供者１０１。

使用者家庭網路３０３中之不同裝置的連接模式如下。

圖１０１指出使用者家庭網路３０３中之裝置的連接模式。

如圖１０１所示，使用者家庭網路３０３中之Ａ／Ｖ機器３６０$_2$、３６０$_3$與網路裝置３６０$_1$經由ＩＥＥＥ－１３９４串聯匯流排１９１彼此連接。

網路裝置３６０$_1$包括：外部記憶體２０１、ＳＡＭ３０５$_1$、ＣＡ模組３１１、Ａ／Ｖ壓縮／解壓縮ＳＡＭ１６３及下載記憶體１６７。

ＣＡ模組３１１經由網路例如公共線路與服務提供者３１０通訊。ＳＡＭ３０５$_1$經由網路例如公共線路與ＥＭＤ服務中心３０２通訊。作爲下載記憶體１６７，可使用設有媒體ＳＡＭ１６７ａ之記憶棒或硬碟機（ＨＤＤ）。下載記憶體１６７儲存服務提供者３１０下載的安全容器３０４。

各裝置集積可與不同的壓縮／解壓縮方法例如ＡＴＲＡＣ３及ＭＰＥＧ相容之Ａ／Ｖ壓縮／解壓縮

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（184）

ＳＡＭ１６３。

ＳＡＭ３０５$_1$可與接觸型或非接觸型ＩＣ卡１１４１通訊。ＩＣ卡１４１１儲存不同型式的資料，例如使用者ＩＤ，且被用於執行ＳＡＭ３０５$_1$中之使用者證明。

Ａ／Ｖ機器３６０$_2$是例如一儲存裝置，且在執行ＳＡＭ３０５$_1$與３０５$_2$之間的預定處理之後，經由ＩＥＥＥ－１３９４串聯匯流排１９１從網路裝置３６０$_1$接收的安全容器被記錄在記錄媒體１３０上。

同樣地，Ａ／Ｖ機器３６０$_3$是例如一儲存裝置，且在執行ＳＡＭ３０５$_2$與３０５$_3$之間的預定處理之後，經由ＩＥＥＥ－１３９４串聯匯流排１９１從Ａ／Ｖ機器３６０$_2$接收的安全容器被記錄在記錄媒體１３０上。

在圖１０１所示的例子中，媒體ＳＡＭ１３３被負載在記錄媒體１３０上。然而，如果媒體ＳＡＭ１３３不是提供於記錄媒體１３０，藉著使用圖１０１之虛線所示的媒體驅動ＳＡＭ２６０，執行ＳＡＭ３０５$_2$與３０５$_3$之間的相互證明。

參見圖１０２與１０３，以下敘述圖８２中所示之ＥＭＤ系統３００的整個操作。

在此情形中，安全容器３０４線上從服務提供者３１０被送至使用者家庭網路３０３。執行圖１０２與１０３之處理，假設完成ＥＭＤ服務中心３０２中之ＳＡＭ３０５$_1$至３０５$_4$、服務提供者３１０、內容提供者３０１之登記。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（185）

參見圖１０２，在步驟Ｓ２１中，ＥＭＤ服務中心３０２將內容提供者３０１之公開鑰匙資料$K_{CP,P}$的公開鑰匙證明CER_{CP}連同ＥＭＤ服務中心３０２之簽名資料$SIG_{1,ESC}$送至內容提供者３０１。

ＥＭＤ服務中心３０２亦將服務提供者３１０之公開鑰匙資料$K_{SP,P}$的公開鑰匙證明CER_{SP}連同ＥＭＤ服務中心３０２之簽名資料$SIG_{61,ESC}$送至服務提供者３１０。

ＥＭＤ服務中心３０２亦將各具有一個有效周期的三個月之執照鑰匙資料KD_1至KD_3，送至使用者家庭網路３０３之$SAM3051$至3054。

在步驟Ｓ２２中，於執行相互證明之後，內容提供者３０１授權ＵＣＰ資料１０６與內容鑰匙資料Ｋｃ，藉著將它們登記於ＥＭＤ服務中心３０２中。ＥＭＤ服務中心３０２產生圖３Ｂ所示之六個月的鑰匙檔ＫＦ，並將它送至內容提供者３０１。

然後，在步驟Ｓ２３中，內容提供者３０１產生圖３Ａ所示之內容檔ＣＦ與簽名資料$SIG_{6,CP}$，及圖３Ｂ所示之鑰匙檔ＫＦ與簽名資料$SIG_{7,CP}$，並線上及／或離線提供安全容器１０４至服務提供者３１０，在安全容器１０４中儲存上述檔案與簽名資料，及公開鑰匙證明資料CER_{CP}與簽名資料$SIG_{1,ESC}$。

在步驟Ｓ中，於檢查圖３Ｃ所示之簽名資料$SIG_{1,ESC}$之後，服務提供者３１０分別證明圖３Ａ與

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（186）

３Ｂ所示之簽名資料ＳＩＧ$_{6,CP}$與ＳＩＧ$_{7,CP}$的完整性，藉著使用儲存於公開鑰匙證明資料ＣＥＲ$_{CP}$中之公開鑰匙資料Ｋ$_{CP,P}$，藉以證明安全容器１０４已從合法內容提供者３０１被送出。

隨後，在步驟Ｓ２５中，服務提供者３１０產生價格標籤資料３１２與簽名資料ＳＩＧ$_{64,SP}$，以產生圖８７所示安全容器３０４，其中儲存上述資料。

在步驟Ｓ２６中，服務提供者３１０授權價格標籤資料３１２，藉著將它登記於ＥＭＤ服務中心３０２中。

在步驟Ｓ２７中，服務提供者３１０將步驟Ｓ２５中產生的安全容器３０４線上或離線送至圖８９所示之網路裝置３６０$_1$的解碼模組９０５，響應例如來自使用者家庭網路３０３之ＣＡ模組３１１的要求。

然後，在步驟Ｓ２８中，ＣＡ模組３１１產生ＳＰ購買登錄資料３０９，並適當地將它送至服務提供者３１０。

參見圖１０３，在步驟Ｓ２９中，於證明圖８４Ｄ所示之簽名資料ＳＩＧ$_{61,ESC}$的完整性之後，ＳＡＭ３０５$_1$至３０５$_4$的其中之一分別證明圖８４Ａ、８４Ｂ、８４Ｃ所示之簽名資料ＳＩＧ$_{62,SP}$、ＳＩＧ$_{63,SP}$、ＳＩＧ$_{64,SP}$的完整性，藉著使用儲存於公開鑰匙證明資料ＣＥＲ$_{SP}$中之公開鑰匙資料Ｋ$_{SP,P}$，藉以決定是否安全容器３０４內的預定資料已被合法服務提供者３１０產生且送出。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（187）

隨後，在步驟S30中，於證明圖84D所示之簽名資料$SIG_{1,ESC}$的完整性之後，$SAM3051$至3054的其中之一分別證明圖84A、84B所示之簽名資料$SIG_{6,CP}$、$SIG_{7,CP}$的完整性，藉著使用儲存於公開鑰匙證明資料CER_{CP}中之公開鑰匙資料$K_{CP,P}$，藉以決定是否安全容器304內的內容檔CF已被合法的內容提供者301產生，及是否鑰匙檔KF已從合法的內容提供者301被送出。

此外，$SAM3051$至3054的其中之一證明圖84B所示之鑰匙檔KF內的簽名資料$SIG_{K1,ESC}$的完整性，藉著使用公開鑰匙資料$K_{ESC,P}$，藉以決定是否鑰匙檔KF已被EMD服務中心302產生。

在步驟S31中，使用者決定內容之購買與使用模式，藉著操作圖88所示之操作單元165。

在步驟S32中，於$SAM3051$至3054中，根據步驟S31中從主CPU810輸出至$SAM3051$至3054之內部中斷S810，產生安全容器304之使用登錄資料308。

使用登錄資料308與簽名資料$SIG_{205,SAM1}$從$SAM3051$至3054被送至EMD服務中心302。每次決定購買模式時，UCS資料166即時$SAM3051$至3054被送至EMD服務中心302。

在步驟S33中，根據使用登錄資料308，EMD服務中心302決定（計算）各內容提供者301與服務

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（188）

提供者３１０之會計內容，並根據會計內容產生處理要求資料１５２ｃ與１５２ｓ。

隨後，在步驟Ｓ３４中，ＥＭＤ服務中心３０２經由給付閘道９０，將處理要求資料１５２ｃ與１５２ｓ連同ＥＭＤ服務中心３０２之簽名資料送至處理組織９１。因此，使用者家庭網路３０３之使用者的給付被分配至內容提供者３０１、內容權利擁有者、服務提供者３１０及服務－提供者權利擁有者。

如上所述，在ＥＭＤ系統３００中，圖３Ａ至３Ｃ所示之安全容器１０４從內容提供者３０１被分布至服務提供者３１０，且儲存安全容器１０４之鑰匙檔ＫＦ與內容檔ＣＦ之安全容器３０４，從服務提供者３１０被送至使用者家庭網路３０３。在ＳＡＭ３０５$_1$至３０５$_4$中執行鑰匙檔ＫＦ之處理。

儲存於鑰匙檔ＫＦ中之內容鑰匙資料Ｋｃ與ＵＣＰ資料１０６以執照鑰匙資料ＫＤ$_1$至ＫＤ$_3$被加密，且只在擁有執照鑰匙資料ＫＤ$_1$至ＫＤ$_3$之ＳＡＭ３０５$_1$至３０５$_4$中被解密。ＳＡＭ３０５$_1$至３０５$_4$爲抗干預模組，其根據ＵＣＰ資料１０６所述之內容資料Ｃ的處理政策，決定內容資料Ｃ之購買與使用模式。

因此，依據ＥＭＤ系統３００，使用者家庭網路３０３中之內容資料Ｃ，根據由內容提供者３０１或內容－提供者相關的組織所產生之ＵＣＰ資料１０６，可被可靠地購買與使用，與服務提供者３１０之處理無關。亦即

（請先閱讀背面之注意事項再填寫本頁）

裝 訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（189）

，在ＥＭＤ系統３００中，ＵＣＰ資料１０６無法被服務提供者３１０管理。

於是，在ＥＭＤ系統３００中，即使當內容資料Ｃ經由許多服務提供者３１０被分布至使用者家庭網路３０３，使用者家庭網路３０３之ＳＡＭ中內容資料Ｃ的權利處理，可根據由內容提供者３０１或內容－提供者相關的組織所產生之共同ＵＣＰ資料１０６被執行。

在ＥＭＤ系統３００中，安全容器１０４與３０４內的檔案與資料可設有簽名資料，其證明檔案與資料之送出者與產生者。於是服務提供者３１０與ＳＡＭ３０５$_1$至３０５$_4$可以檢查檔案與資料之完整性，及其送出者與產生者之完整性，藉以有效地避免內容資料Ｃ之非法使用。

在ＥＭＤ系統３００中，安全容器３０４是用於從服務提供者３１０分布內容資料Ｃ至使用者家庭網路３０３，不論它是被線上或離線送出。如此使得使用者家庭網路３０３之ＳＡＭ１０５$_1$至１０５$_4$可執行相同的權利處理，不論安全容器３０４是線上或離線被送出。

於購買、使用、記錄及轉移使用者家庭網路３０３內之Ａ／Ｖ機器３６０$_2$至３６０$_4$與網路裝置３６０$_1$中之內容資料Ｃ時，總是根據ＵＣＰ資料１０６執行處理。於是，能建立與整個使用者家庭網路３０３共通的權利處理規則。

例如，如圖１０４所示，藉著任何方法（路徑），從內容提供者３０１提供之內容資料Ｃ可從服務提供者

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

五、發明說明（190)

３１０被分布至使用者家庭網路３０３，例如封包分布，數位廣播，網際網路，專線，數位無線電，或行動通訊。即使使用上述方法的其中之一，共同的權利處理規則可被使用於使用者家庭網路３０３與３０３ａ之ＳＡＭ中，根據由內容提供者３０１所產生之ＵＣＰ資料１０６。

依據ＥＭＤ系統３００，ＥＭＤ服務中心３０２具有證明功能，鑰匙－資料管理功能，及權利處理（利潤分配）功能。於是，依據預定比例，使用者之給付能可靠地被分配至內容提供者３０１與ＥＭＤ服務中心３０２。

而且，從相同內容提供者３０１供給之相同內容檔ＣＦ的ＵＣＰ資料１０６，被供給至ＳＡＭ３０５_{1}至３０５_{4}，與服務提供者３１０之服務無關。因此，根據由內容提供者３０１決定的ＵＣＰ資料１０６，在$ＳＡＭ３０５_{1}$至３０５_{4}中可使用內容檔ＣＦ。

亦即，依據ＥＭＤ系統３００，提供內容之服務或由使用者使用內容時，依據技術手段而與習知所需之查賬組織７２５無關，能可靠地保護內容提供者３０１之利潤與權利。

例如使用於第二實施例之ＥＭＤ系統３００中的安全容器之分布協定如下。

內容提供者３０１中產生的安全容器１０４被分布至服務提供者３１０，如圖１０５所示，藉著使用內容－提供者分布協定，例如網際網路（ＴＣＰ／ＩＰ）或專線（ＡＴＭ單元）。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部智慧財產局員工消費合作社印製

五、發明說明（191）

然後服務提供者３１０將從安全容器１０４產生的安全容器１０４分布至使用者家庭網路３０３，藉著使用服務－提供者分布協定，例如數位廣播（ＸＭＬ／ＳＭＩＬｏｎ　ＭＰＥＧ－ＴＳ），網際網路（ＸＭＬ／ＳＭＩＬｏｎ　ＴＣＰ／ＩＰ），或封包分布（記錄媒體）。

藉著使用家庭電子商務（ＥＣ）／分布服務（１３９４－串聯匯流排介面上之ＸＭＬ／ＳＭＩＬ）或記錄媒體，安全容器被轉移於使用者家庭網路３０３或３０３ａ內，或使用者家庭網路３０３與３０３ａ之間，或ＳＡＭ之間。

雖然已參見較佳實施例來加以敘述本發明，應瞭解本發明並不限於所揭示之實施例。

例如，雖然在前面的實施例中，鑰匙檔ＫＦ是產生於ＥＭＤ服務中心１０２或３０２中，它可以被產生於內容提供者１０１或３０１中。

由前面的敘述可以看出本發明之資料處理裝置提供以下優點。根據指出安全環境中之內容資料的處理之ＵＣＰ資料，可執行內容資料之權利處理。結果，如果ＵＣＰ資料是由內容提供者產生，內容資料之利潤可被適當地保護，且可減小內容提供者之監視的負擔。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部智慧財產局員工消費合作社印製

A5
B5

四、中文發明摘要（發明之名稱：資料處理裝置，資料處理系統及資料處理方法）

ＳＡＭ接收一安全容器，其中儲存以內容鑰匙資料加密的內容資料、加密的內容鑰匙資料、及指定內容資料之處理政策的ＵＣＰ資料，並根據ＵＣＰ資料決定至少內容資料之購買模式與使用模式的其中之一。ＳＡＭ作爲主ＣＰＵ之奴役，且亦設有一與主ＣＰＵ分享的共同記憶體。

英文發明摘要（發明之名稱：）

（請先閱讀背面之注意事項再填寫本頁各欄）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

A8
B8
C8
D8

六、申請專利範圍

1、一種資料處理裝置，用於根據使用控制政策資料執行以內容鑰匙資料加密的內容資料之權利處理，及用於解密加密的內容鑰匙資料，該資料處理裝置在抗干預電路模阻內包含：

一第一匯流排；

一算術處理電路，連接至該第一匯流排，用於根據使用控制政策資料執行內容資料之權利處理；

一儲存電路，連接至該第一匯流排；

一第二匯流排；

一第一介面電路，置於該第一匯流排與該第二匯流排之間；

一加密處理電路，連接至該第二匯流排，用於解密內容鑰匙資料；及

一外部匯流排介面電路，連接至該第二匯流排。

2、如申請專利範圍第1項之資料處理裝置，進一步包含該抗干預電路模阻內之第二介面電路，其中該第一匯流排包含一第三匯流排，連接至該算術處理電路與該儲存電路；及一第四匯流排，連接至該第一介面電路，且該第二介面電路置於該第三匯流排與該第四匯流排之間。

3、如申請專利範圍第2項之資料處理裝置，進一步在該抗干預電路模阻內包含：

一第五匯流排；

一第三介面電路，連接至該第五匯流排，用於執行與具有證明功能的資料處理電路之通訊，證明功能被負載記

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

錄媒體與積體電路卡的其中之一上；及

一第四介面電路，置於該第四匯流排與該第五匯流排之間。

4、如申請專利範圍第1項之資料處理裝置，其中該加密處理電路包含一公開鑰匙加密電路及一共同鑰匙加密電路。

5、如申請專利範圍第4項之資料處理裝置，其中：

該儲存電路儲存該資料處理裝置之私人鑰匙資料及第二資料處理裝置之公開鑰匙資料；

該公開鑰匙加密電路證明簽名資料之完整性，其證明內容資料、內容鑰匙資料、使用控制政策資料之完整性，藉著使用對應的公開鑰匙資料，且當記錄內容資料、內容鑰匙資料、使用控制政策資料於記錄媒體上時，或當將它們送至該第二資料處理裝置時，該公開鑰匙加密電路產生簽名資料，其證明內容資料、內容鑰匙資料、使用控制政策資料之完整性，藉著使用私人鑰匙資料；且

該共同鑰匙加密電路解密內容鑰匙資料，且當線上將內容資料、內容鑰匙資料、使用控制政策資料送至該第二資料處理裝置時，該共同鑰匙加密電路加密及解密內容資料、內容鑰匙資料、使用控制政策資料，藉著使用由以該第二資料處理裝置執行相互證明所得到之連續鑰匙資料。

6、如申請專利範圍第5項之資料處理裝置，進一步包含該抗干預電路模阻內之雜亂值產生電路，用於產生內容資料、內容鑰匙資料、使用控制政策資料之雜亂值，其

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

中該公開鑰匙加密電路證明簽名資料之完整性，並藉著使用雜亂值產生簽名資料。

7、如申請專利範圍第1項之資料處理裝置，進一步包含該抗干預電路模阻內之隨機數目產生電路，該隨機數目產生電路被連接至該第二匯流排，用於產生一隨機數目，以該第二資料處理裝置執行相互證明，當線上將內容資料、內容鑰匙資料、使用控制政策資料送至該第二資料處理裝置。

8、如申請專利範圍第1項之資料處理裝置，其中該外部匯流排介面電路被連接至一外部儲存電路，用於儲存至少內容資料、內容鑰匙資料、使用控制政策資料的其中之一。

9、如申請專利範圍第8項之資料處理裝置，進一步包含一儲存電路控制電路，用於經由該外部匯流排介面電路，依據來自算術處理電路之命令，控制對該儲存電路之存取及對該外部儲存電路之存取。

10、如申請專利範圍第1項之資料處理裝置，其中該外部匯流排介面電路被連接至一主算術處理裝置，用於集中地控制負載該資料處理裝置之系統。

11、如申請專利範圍第8項之資料處理裝置，進一步包含一儲存管理電路，用於管理該儲存電路之位址空間及該外部儲存電路之位址空間。

12、如申請專利範圍第1項之資料處理裝置，其中該算術處理電路根據由使用控制政策資料指出的處理政策

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

，決定至少內容資料的購買模式與使用模式的其中之一，並產生指出決定模式之結果的登錄資料。

１３、如申請專利範圍第１２項之資料處理裝置，其中在決定購買模式之後，該算術處理電路依據決定的購買模式產生使用控制狀態資料，並根據使用控制狀態資料控制內容資料之使用。

１４、如申請專利範圍第４項之資料處理裝置，其中在記錄決定購買模式之內容資料於記錄媒體上時，該共同鑰匙加密電路加密內容鑰匙資料及使用控制狀態資料，藉著使用對應該記錄媒體之媒體鑰匙資料。

１５、如申請專利範圍第４項之資料處理裝置，其中當以具有有效周期之執照鑰匙資料加密內容鑰匙資料時，該儲存電路儲存執照鑰匙資料，該資料處理裝置進一步包含一即時時鐘，用於產生即時，該算術處理電路根據由該即時時鐘所指出之即時，從該儲存電路讀取有效的執照鑰匙資料，且該共同鑰匙加密電路藉著使用讀取的執照鑰匙資料解密內容鑰匙資料。

１６、如申請專利範圍第１項之資料處理裝置，其中該儲存電路寫入並消除以區塊爲單位之資料，且該資料處理裝置在該抗干預電路模阻內包含：一寫入鎖住控制電路，用於在該算術處理電路的控制下，以區塊爲單位，控制從該儲存電路寫入及消除資料。

１７、一種資料處理裝置，用於根據使用控制政策資料執行以內容鑰匙資料加密的內容資料之權利處理，及用

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

於解密加密的內容鑰匙資料，該資料處理裝置在抗干預電路模阻內包含：

一第一匯流排；

一算術處理電路，連接至該第一匯流排，用於根據使用控制政策資料執行內容資料之權利處理；

一儲存電路，連接至該第一匯流排；

一第二匯流排；

一介面電路，置於該第一匯流排與該第二匯流排之間；

一加密處理電路，連接至該第二匯流排，用於解密內容鑰匙資料；及

一外部匯流排介面電路，連接至該第二匯流排，

其中於經由該外部匯流排介面電路，從外部電路接收中斷時，該算術處理電路成爲該外部電路之奴役，以執行由中斷指定的處理，並報告處理的結果至該外部電路。

１８、如申請專利範圍第１７項之資料處理裝置，其中該算術處理電路藉著輸出一中斷至該外部電路而報告處理之結果。

１９、如申請專利範圍第１７項之資料處理裝置，其中該外部匯流排介面包含一該算術處理電路與該外部電路之共同記憶體，該算術處理電路將處理之結果寫入該共同記憶體，且該外部電路藉著投票得到處理之結果。

２０、如申請專利範圍第１９項之資料處理裝置，其中該外部匯流排介面包含：

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

第一狀態暫存器，指出從該算術處理電路中之該外部電路要求的處理之執行狀態，且包括一旗標，由該算術處理電路設定且由該外部電路讀取；

第二狀態暫存器，指出是否該外部電路已要求該算術處理電路執行處理，且包括一旗標，由該外部電路設定且由該算術處理電路讀取；及

該共同記憶體，用於儲存處理之結果。

２１、如申請專利範圍第１８項之資料處理裝置，其中該儲存電路儲存一中斷程式，敘述由中斷指定的處理，且該算術處理電路執行處理，藉著執行從該儲存電路讀取的中斷程式。

２２、如申請專利範圍第２１項之資料處理裝置，其中該儲存電路儲存許多該中斷程式，及當執行中斷程式時欲被讀取的許多副常式，且當執行從該儲存電路讀取的中斷程式時，該算術處理電路適當地讀取及執行來自該儲存電路之副常式。

２３、一種資料處理系統，包含：

一算術處理裝置，用於執行預定的程式，及用於藉著作爲一主人依據預定的條件輸出一中斷；及

一資料處理裝置，用於藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，執行預定的處理，且用於報告處理之結果至該算術處理裝置，該資料處理裝置在抗干預電路模阻內包含：

決定機構，用於根據由使用控制政策資料指出的處理

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

政策，決定至少內容資料之購買模式與使用模式的其中之一；

登錄資料產生機構，用於產生指出決定的模式之結果的登錄資料；及

解密機構，用於解密內容鑰匙資料。

２４、如申請專利範圍第２３項之資料處理系統，其中於接收指出中斷型式之中斷時，該算術處理裝置將指出一指示之中斷輸出至該資料處理裝置，以執行對應中斷型式之中斷常式，且該資料處理裝置執行對應來自該算術處理裝置之中斷的中斷型式之中斷常式。

２５、如申請專利範圍第２３項之資料處理系統，其中該資料處理裝置藉著輸出一中斷至該算術處理裝置而報告處理之結果。

２６、如申請專利範圍第２３項之資料處理系統，其中該資料處理裝置包含一共同記憶體，其可由該資料處理裝置及該算術處理裝置取存，且該算術處理裝置藉著經由投票存取該共同記憶體而得到處理之結果。

２７、如申請專利範圍第２６項之資料處理系統，其中該資料處理裝置包含一第一狀態暫存器，指出從該算術處理裝置要求的處理之執行狀態，且包括一旗標，由該算術處理裝置讀取；

一第二狀態暫存器，指出是否該算術處理裝置藉著中斷已要求該資料處理裝置執行處理，且包括一旗標，由該算術處理裝置設定；及

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

該共同記憶體，用於儲存處理之結果。

２８、如申請專利範圍第２３項之資料處理系統，進一步包含一匯流排，用於連接該算術處理裝置與該資料處理裝置。

２９、如申請專利範圍第２４項之資料處理系統，其中該資料處理裝置在完成啓始程式與中斷常式的其中之一之後，進入低電力狀態。

３０、如申請專利範圍第２４項之資料處理系統，其中根據從該算術處理裝置接收的中斷，該資料處理裝置執行中斷常式，依據至少決定內容資料的購買模式與使用模式的其中之一之處理，再生內容資料之處理，從證明授權下載資料之處理的其中之一。

３１、如申請專利範圍第２３項之資料處理系統，其中該算術處理裝置執行一預定的使用者程式。

３２、一種資料處理系統，其中從一資料分布裝置接收由資料提供裝置提供之內容資料，且由管理裝置管理內容資料，該資料處理系統包含：

一第一處理模組，用於從該資料分布裝置接收一模組，其中儲存以內容鑰匙資料加密的內容資料、加密的內容鑰匙資料、指出內容資料之處理政策的使用控制政策資料、及由該資料分布裝置決定的內容資料之價格資料，且用於藉著使用內容鑰匙資料而解密接收的模組，並用於由該資料分布裝置執行模組之分布服務的會計處理；

一算術處理裝置，用於執行預定的程式，及藉著作爲

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

一主人用於輸出依據預定的條件之中斷；及

一資料處理裝置，用於藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，執行預定的處理，且用於將處理之結果報告至該算術處理裝置，該資料處理裝置在抗干預電路模阻內包含：

決定機構，用於根據由儲存於接收的模組中之使用控制政策資料指出的處理政策，決定至少內容資料之購買模式與使用模式的其中之一；

登錄資料產生機構，用於產生指出決定的模式之結果的登錄資料；

輸出機構，用於當決定內容資料之購買模式時，將價格資料與登錄資料輸出至該管理裝置；及

解密機構，用於解密內容鑰匙資料。

３３、一種資料處理系統，包含：

一算術處理裝置，用於執行預定的程式，及藉著作爲一主人用於輸出依據預定的條件之中斷；

一第一抗干預資料處理裝置，用於藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，執行以內容鑰匙資料加密的內容資料之權利處理，且用於將處理之結果報告至該算術處理裝置；及

一第二抗干預資料處理裝置，用於解密內容資料，藉著使用以該第一抗干預資料處理裝置執行相互證明所得到之內容鑰匙資料，且用於藉著作爲該算術處理裝置或該第一抗干預資料處理裝置之奴役，響應來自該算術處理裝置

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

或該第一抗干預資料處理裝置之中斷，壓縮或解壓縮內容資料。

３４、如申請專利範圍第３３項之資料處理系統，進一步包含一匯流排，用於連接該算術處理裝置、該第一抗干預資料處理裝置、及該第二抗干預資料處理裝置。

３５、一種資料處理系統，包含：

一算術處理裝置，用於執行預定的程式，及藉著作爲一主人用於輸出依據預定的條件之中斷；

一第一抗干預資料處理裝置，用於藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，執行以內容鑰匙資料加密的內容資料之權利處理，且用於將處理之結果報告至該算術處理裝置；及

一第二抗干預資料處理裝置，用於以該算術處理裝置執行相互證明，且用於響應從該算術處理裝置輸出的中斷，從記錄媒體讀取及寫入內容資料。

３６、如申請專利範圍第３５項之資料處理系統，其中該第二抗干預資料處理裝置藉著使用對應該記錄媒體之媒體鑰匙資料，而解密及加密內容資料。

３７、如申請專利範圍第３５項之資料處理系統，其中當該記錄媒體設有具有相互證明功能之處理電路時，該第二抗干預資料處理裝置以該處理電路執行相互證明。

３８、一種資料處理系統，包含

一算術處理裝置，用於執行預定的程式，及藉著作爲一主人用於輸出依據預定的條件之中斷；

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

一第一抗干預資料處理裝置，用於以該算術處理裝置執行相互證明，且用於響應來自該算術處理裝置之中斷，從記錄媒體讀取及寫入內容資料；及

一第二抗干預資料處理裝置，用於藉著使用內容鑰匙資料而解密內容資料，且用於藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，而壓縮或解壓縮內容資料。

３９、如申請專利範圍第３８項之資料處理系統，進一步包含一儲存電路，用於暫時地儲存由該第一抗干預資料處理裝置從該記錄媒體讀取的內容資料，且用於將儲存的內容資料輸出至該第二抗干預資料處理裝置。

４０、如申請專利範圍第３９項之資料處理系統，其中該儲存電路使用抗震儲存電路之部份儲存區域。

４１、如申請專利範圍第３８項之資料處理系統，進一步包含一第三抗干預資料處理裝置，用於藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，而執行以內容鑰匙資料加密的內容資料之權利處理，且用於將處理之結果報告至該算術處理裝置。

４２、一種使用算術處理裝置及資料處理裝置之資料處理方法，該資料處理方法包含以下步驟：

在該算術處理裝置中，執行一預定的程式並藉著作爲一主人而輸出依據預定的條件之中斷；及

在該資料處理裝置中，根據使用控制政策資料之處理政策，決定至少內容資料之購買模式與使用模式的其中之

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

一，產生指出決定的模式之結果的登錄資料，並在抗干預電路模阻內，藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，而解密內容鑰匙資料。

４３、如申請專利範圍第４２項之資料處理方法，其中於接收指出中斷型式之中斷時，該算術處理裝置將指出一指示之中斷輸出至該資料處理裝置，以執行對應中斷型式之中斷常式，且該資料處理裝置執行對應由從該算術處理裝置接收的中斷所指定的處理之中斷常式。

４４、如申請專利範圍第４２項之資料處理方法，其中該資料處理裝置藉著輸出一中斷至該算術處理裝置而報告處理之結果。

４５、如申請專利範圍第４２項之資料處理方法，其中該資料處理裝置包含一共同記憶體，其可由該資料處理裝置及該算術處理裝置存取，且該算術處理裝置藉著經由投票存取該共同記憶體而得到處理之結果。

４６、如申請專利範圍第４５項之資料處理方法，其中：

該資料處理裝置設定一旗標於第一狀態暫存器中，指出由來自該算術處理裝置之中斷所要求的處理之執行狀態；

該算術處理裝置從該第一狀態暫存器中之旗標，讀取該資料處理裝置之處理的執行狀態；

該算術處理裝置設定一旗標於第二狀態暫存器中，指出是否該算術處理裝置已要求該資料處理裝置經由中斷而

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

執行處理；且

該資料處理裝置決定是否該算術處理裝置已要求該資料處理裝置執行來自該第二狀態暫存器中之旗標的處理。

４７、如申請專利範圍第４２項之資料處理方法，其中該資料處理裝置於完成啓始程式與中斷常式的其中之一之執行時，進入低電力狀態。

４８、如申請專利範圍第４２項之資料處理方法，其中根據從該算術處理裝置接收的中斷，該資料處理裝置執行中斷常式，依據至少決定內容資料之購買模式與使用模式的其中之一之處理，再生內容資料之處理，與從證明授權下載資料之處理的其中之一。

４９、如申請專利範圍第４２項之資料處理方法，其中該算術處理裝置執行一預定的使用者程式。

５０、一種使用算術處理裝置、第一資料處理裝置及第二資料處理裝置之資料處理方法，該資料處理方法包含以下步驟：

在該算術處理裝置中，執行一預定的程式並藉著作爲一主人而輸出依據預定的條件之中斷；

在該第一資料處理裝置中，藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，而執行以抗干預模組內之內容鑰匙資料加密的內容資料之權利處理，並報告處理之結果至該算術處理裝置；及

在該第二資料處理裝置中，解密內容資料，藉著使用由以該第一資料處理裝置執行相互證明所得到之內容鑰匙

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

資料，及藉著作爲該算術處理裝置或該第一資料處理裝置之奴役，響應來自該算術處理裝置或該第一資料處理裝置之中斷，而壓縮或解壓縮抗干預模組內的內容資料。

５１、一種使用算術處理裝置、第一資料處理裝置及第二資料處理裝置之資料處理方法，該資料處理方法包含以下步驟：

在該算術處理裝置中，執行一預定的程式並藉著作爲一主人而輸出依據預定的條件之中斷；

在該第一資料處理裝置中，藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，而執行以抗干預模組內之內容鑰匙資料加密的內容資料之權利處理，並報告處理之結果至該算術處理裝置；及

在該第二資料處理裝置中，以該算術處理裝置執行相互證明，並響應來自算術處理裝置之中斷，從抗干預模組內的記錄媒體讀取及寫入內容資料。

５２、如申請專利範圍第５１項之資料處理方法，其中該第二資料處理裝置藉著使用對應該記錄媒體之媒體鑰匙資料而解密及加密內容資料。

５３、如申請專利範圍第５１項之資料處理方法，其中當該記錄媒體設有具有相互證明功能之處理電路時，該第二資料處理裝置以該處理電路執行相互證明。

５４、一種使用算術處理裝置、第一資料處理裝置及第二資料處理裝置之資料處理方法，該資料處理方法包含以下步驟：

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

經濟部智慧財產局員工消費合作社印製

六、申請專利範圍

在該算術處理裝置中，執行一預定的程式並藉著作爲一主人而輸出依據預定的條件之中斷；

在該第一資料處理裝置中，以該算術處理裝置執行相互證明，並響應來自該算術處理裝置之要求，從抗干預模組內的記錄媒體讀取及寫入內容資料；及

在該第二資料處理裝置中，解密內容資料，藉著使用內容鑰匙資料，及藉著作爲該算術處理裝置之奴役，響應來自該算術處理裝置之中斷，而壓縮或解壓縮抗干預模組內的內容資料。

５５、如申請專利範圍第５４項之資料處理方法，其中由該第一資料處理裝置從該記錄媒體讀取的內容資料被暫時地儲存於儲存電路中，且從該儲存電路讀取的內容資料被輸出至該第二資料處理裝置。

５６、如申請專利範圍第５５項之資料處理方法，其中該儲存電路使用抗震儲存電路之部份儲存區域。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂

經濟部智慧財產局員工消費合作社印製

559705

739098

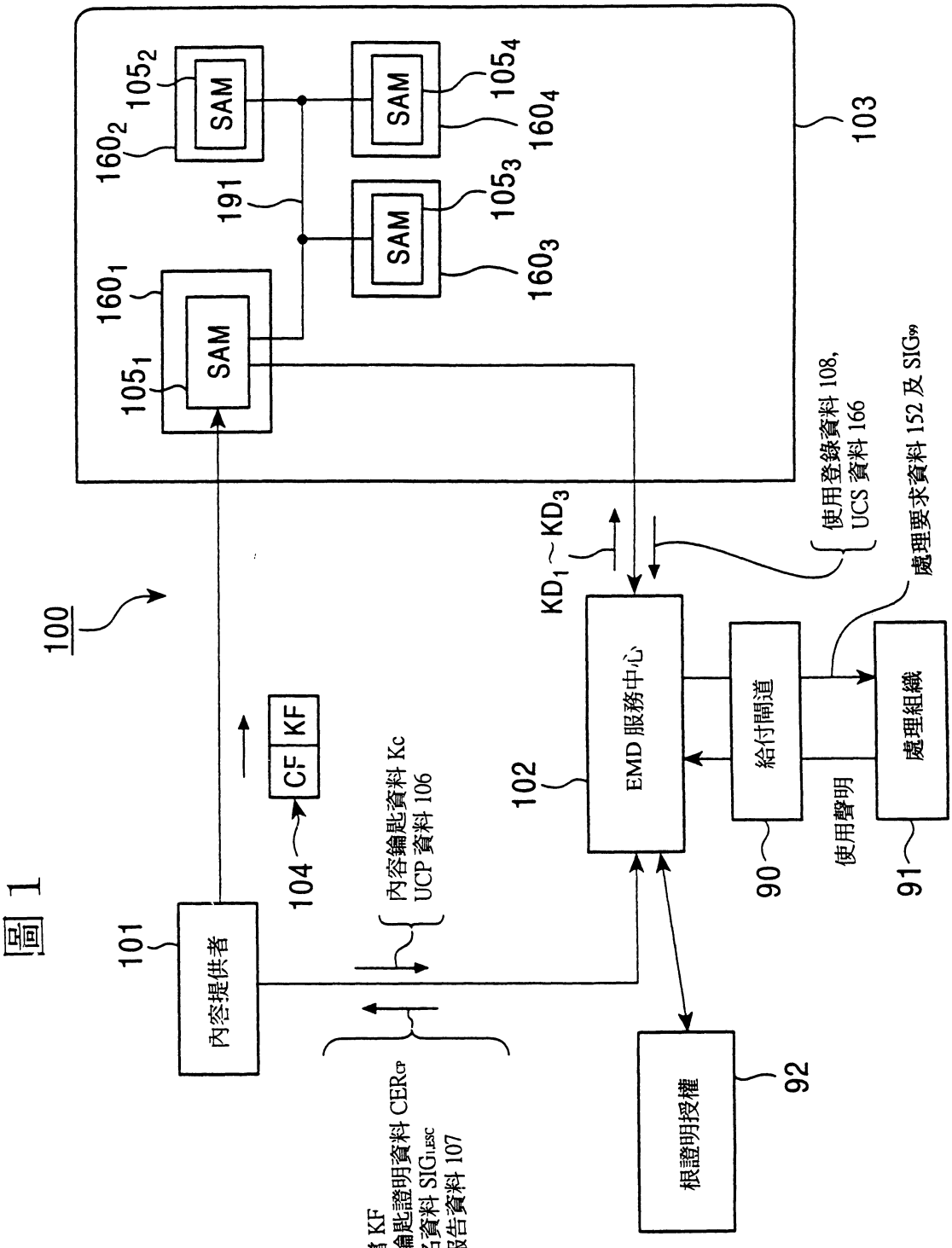
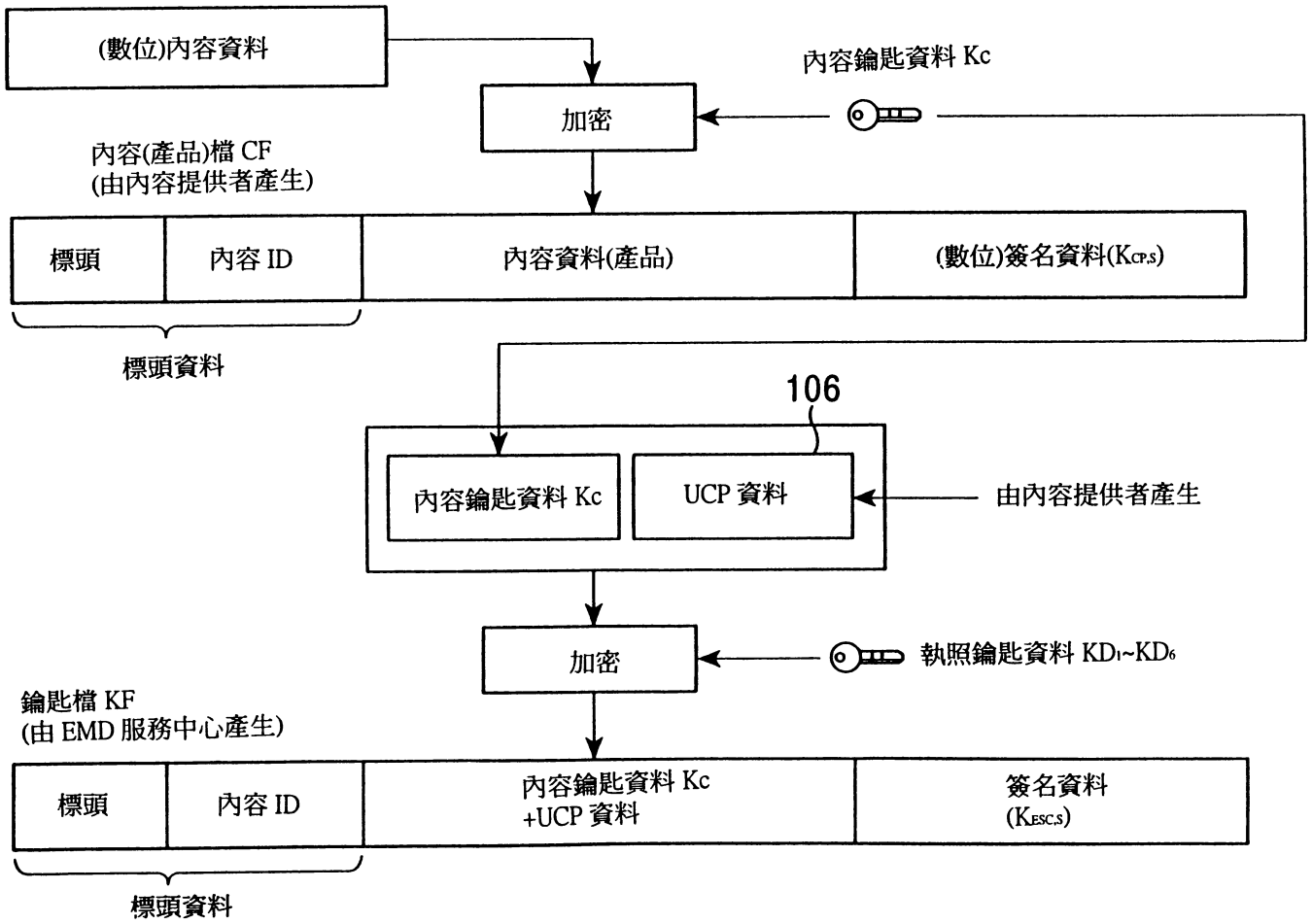


圖 1

圖 2


(數位)內容資料
內容鑰匙資料 Kc
加密
內容(產品)檔 CF
(由內容提供者產生)
標頭
內容 ID
內容資料(產品)
(數位)簽名資料(KCP,S)
標頭資料
106
內容鑰匙資料 Kc
UCP 資料
由內容提供者產生
加密
執照鑰匙資料 KD1~KD6
鑰匙檔 KF
(由 EMD 服務中心產生)
標頭
內容 ID
內容鑰匙資料 Kc
+UCP 資料
簽名資料
(KESC,S)
標頭資料

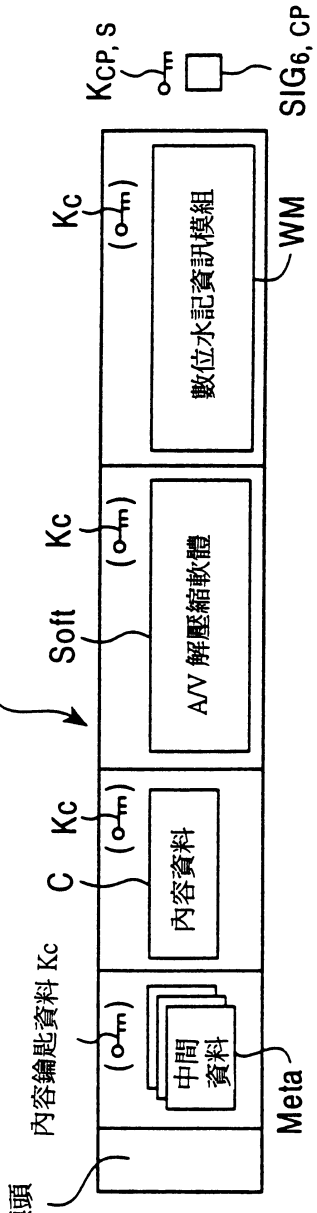

內容檔 CF
標頭
內容鑰匙資料 Kc
C
Kc
Soft
Kc
Kc
KCP, S
SIG6, CP
中間資料
內容資料
A/V 解壓縮軟體
數位水記資訊模組
Meta
WM

圖 3 A

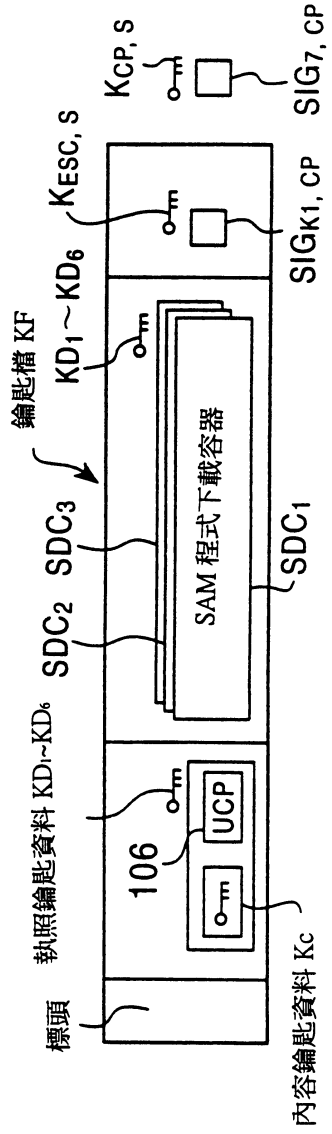

鑰匙檔 KF
標頭
執照鑰匙資料 KD1~KD6
內容鑰匙資料 Kc
106
UCP
SDC2
SDC3
SDC1
KD1～KD6
KESC, S
KCP, S
SIGK1, CP
SIG7, CP
SAM 程式下載容器

圖 3 B

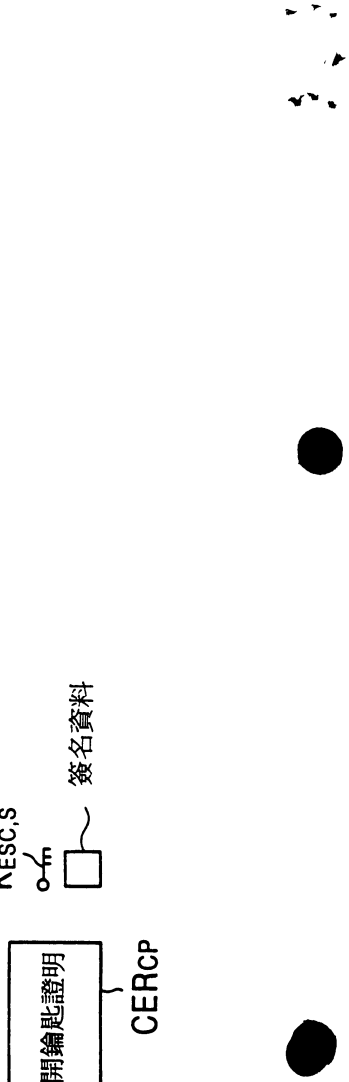

KESC,S
簽名資料
公開鑰匙證明
KCP, P
CERCP

圖 3 C

圖 4

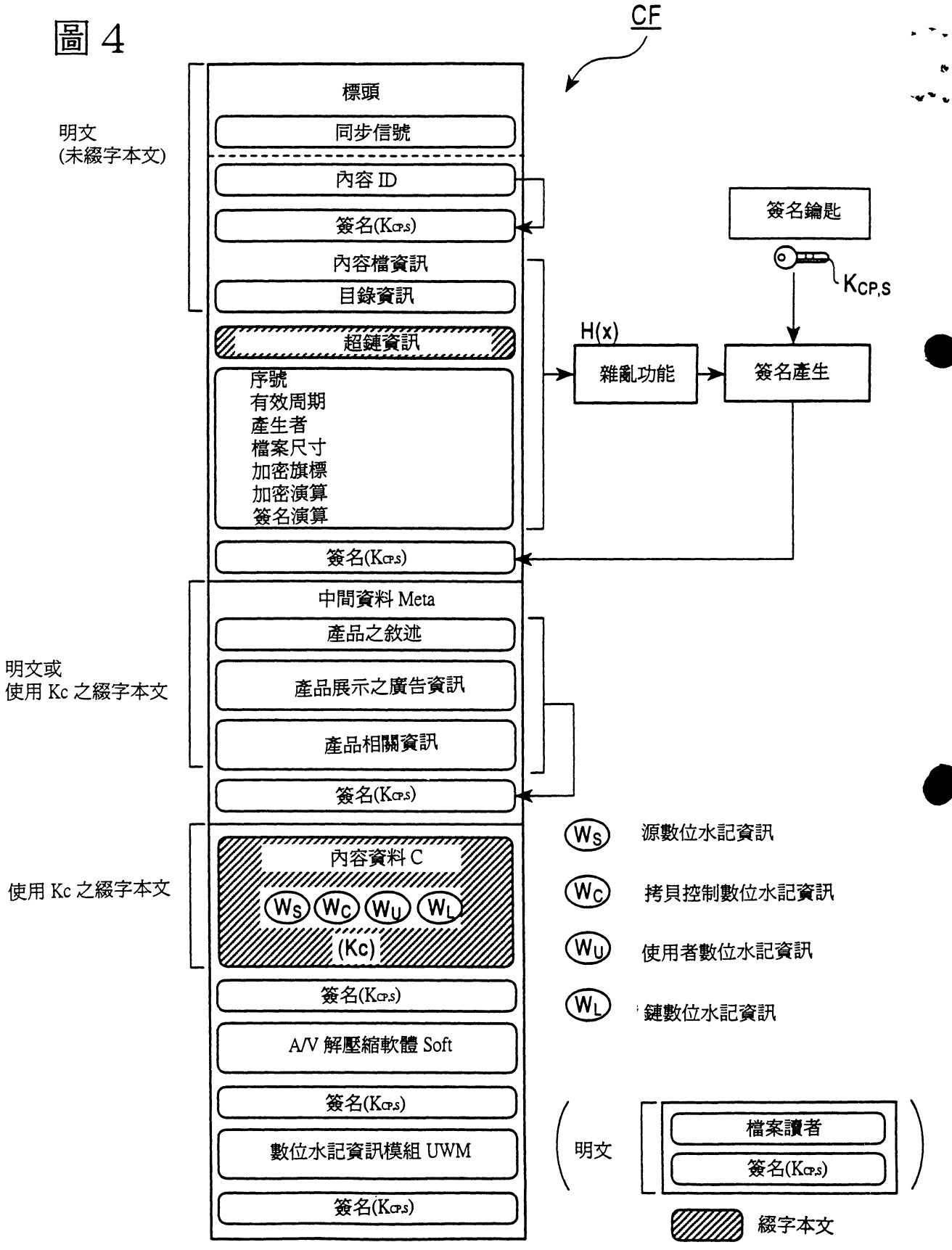

CF
標頭
同步信號
內容 ID
簽名(KCP,S)
內容檔資訊
目錄資訊
超鏈資訊
序號
有效周期
產生者
檔案尺寸
加密旗標
加密演算
簽名演算
簽名(KCP,S)
中間資料 Meta
產品之敘述
產品展示之廣告資訊
產品相關資訊
簽名(KCP,S)
內容資料 C
WS WC WU WL
(Kc)
簽名(KCP,S)
A/V 解壓縮軟體 Soft
簽名(KCP,S)
數位水記資訊模組 UWM
簽名(KCP,S)
明文
(未綴字本文)
明文或
使用 Kc 之綴字本文
使用 Kc 之綴字本文
簽名鑰匙
KCP,S
H(x)
雜亂功能
簽名產生
WS 源數位水記資訊
WC 拷貝控制數位水記資訊
WU 使用者數位水記資訊
WL 鏈數位水記資訊
明文
檔案讀者
簽名(KCP,S)
綴字本文

圖 5

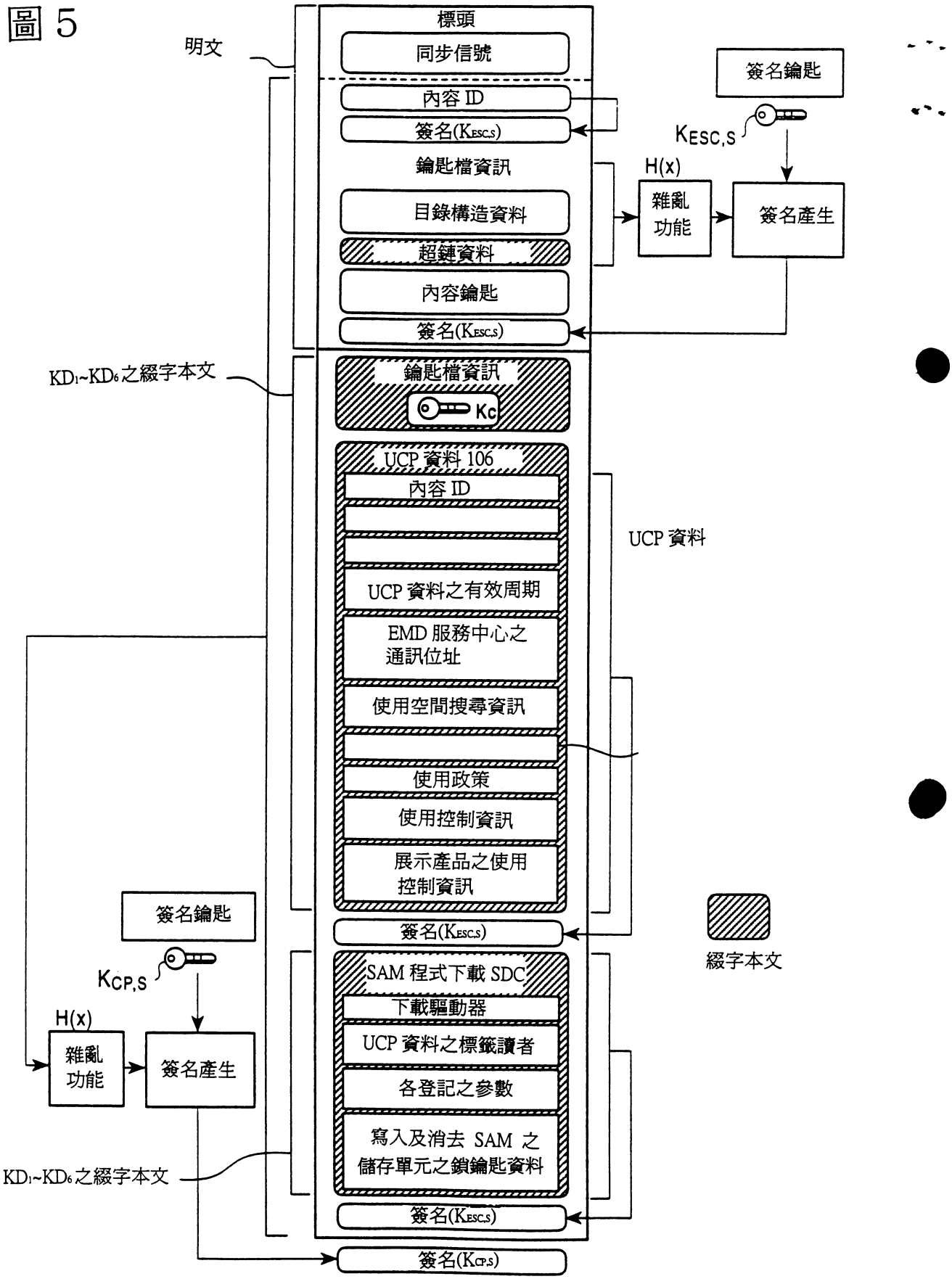

明文
標頭
同步信號
內容 ID
簽名(KESC,S)
鑰匙檔資訊
目錄構造資料
超鏈資料
內容鑰匙
簽名(KESC,S)
KD1~KD6之綴字本文
鑰匙檔資訊
Kc
UCP 資料 106
內容 ID
UCP 資料之有效周期
EMD 服務中心之通訊位址
使用空間搜尋資訊
使用政策
使用控制資訊
展示產品之使用控制資訊
簽名(KESC,S)
SAM 程式下載 SDC
下載驅動器
UCP 資料之標籤讀者
各登記之參數
寫入及消去 SAM 之儲存單元之鎖鑰匙資料
簽名(KESC,S)
簽名(KCP,S)
KD1~KD6之綴字本文
簽名鑰匙
KESC,S
H(x)
雜亂功能
簽名產生
簽名鑰匙
KCP,S
H(x)
雜亂功能
簽名產生
UCP 資料
綴字本文

圖 6

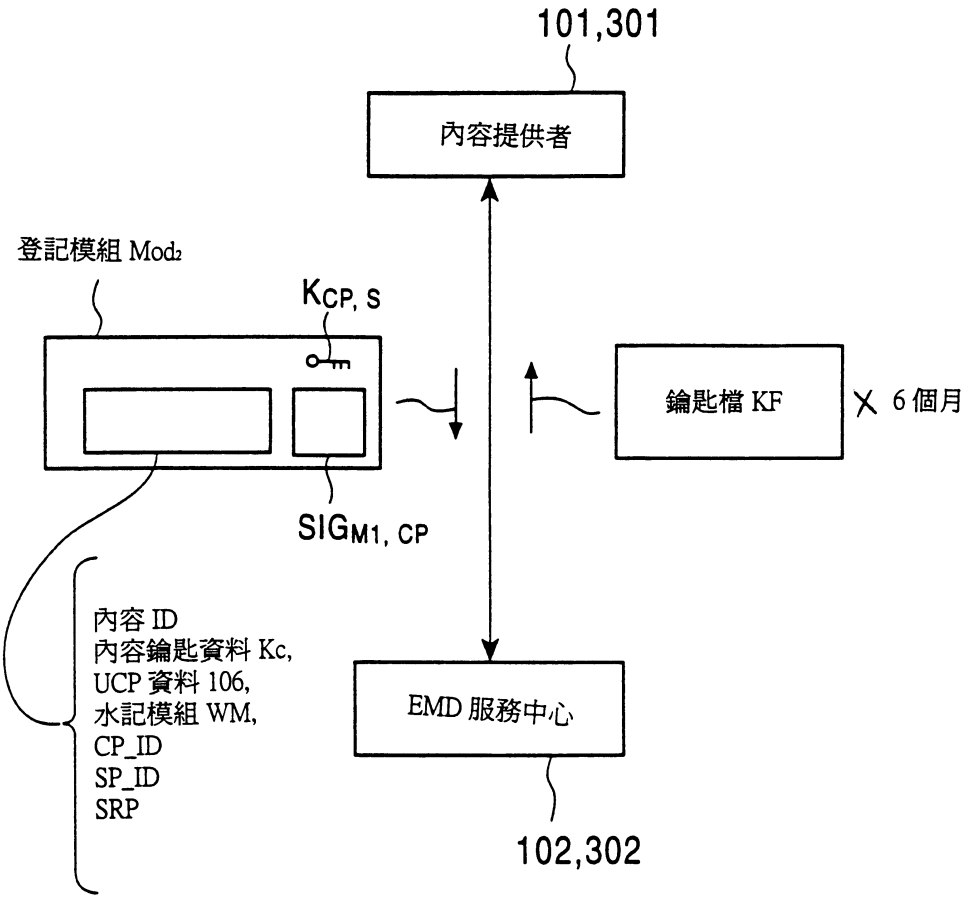

101,301
內容提供者
登記模組 Mod2
KCP, S
鑰匙檔 KF
X 6 個月
SIGM1, CP
內容 ID
內容鑰匙資料 Kc,
UCP 資料 106,
水記模組 WM,
CP_ID
SP_ID
SRP
EMD 服務中心
102,302

圖 7

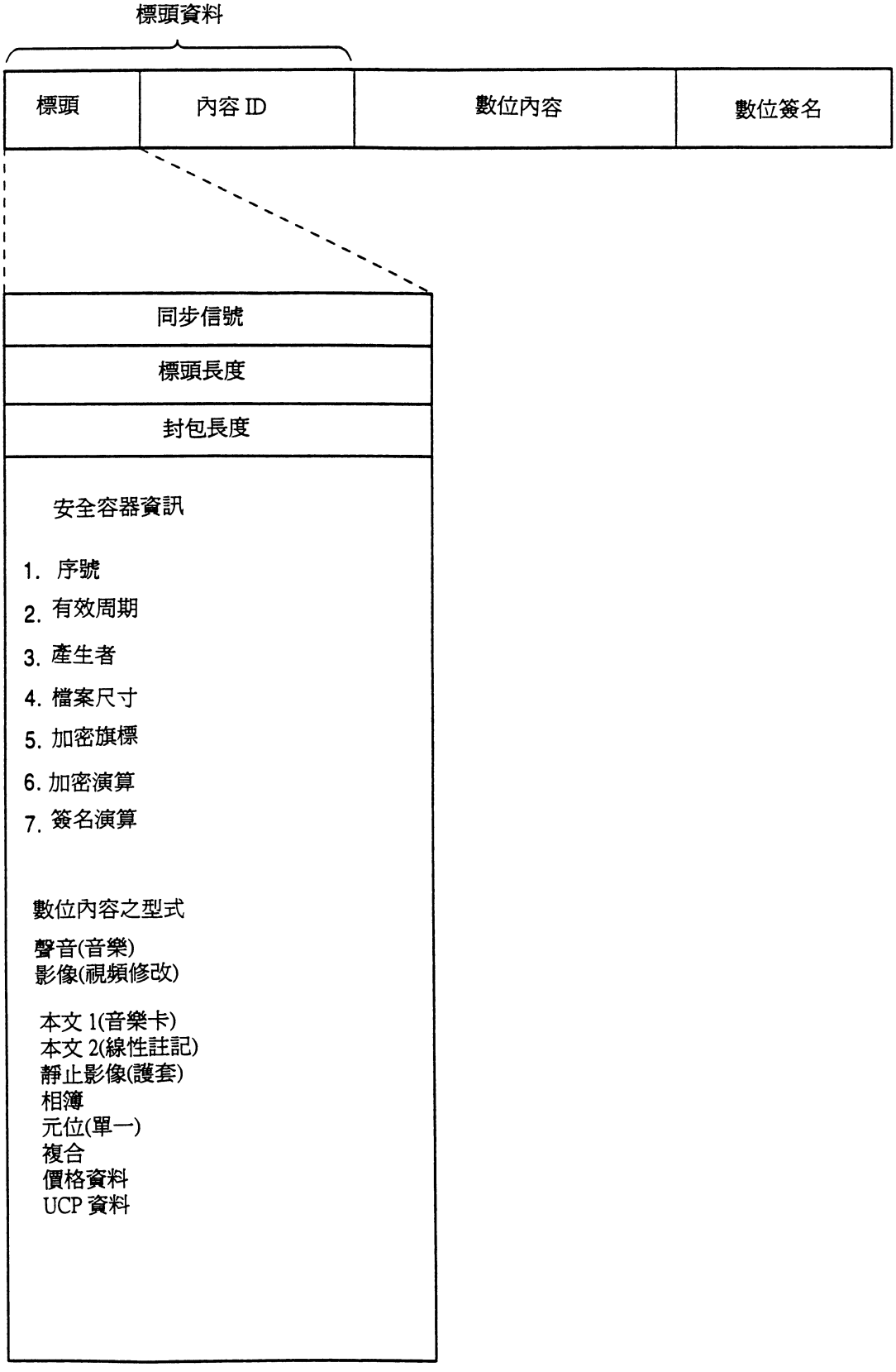

標頭資料
標頭
內容 ID
數位內容
數位簽名
同步信號
標頭長度
封包長度
安全容器資訊
1. 序號
2. 有效周期
3. 產生者
4. 檔案尺寸
5. 加密旗標
6. 加密演算
7. 簽名演算
數位內容之型式
聲音(音樂)
影像(視頻修改)
本文 1(音樂卡)
本文 2(線性註記)
靜止影像(護套)
相簿
元位(單一)
複合
價格資料
UCP 資料

圖 8

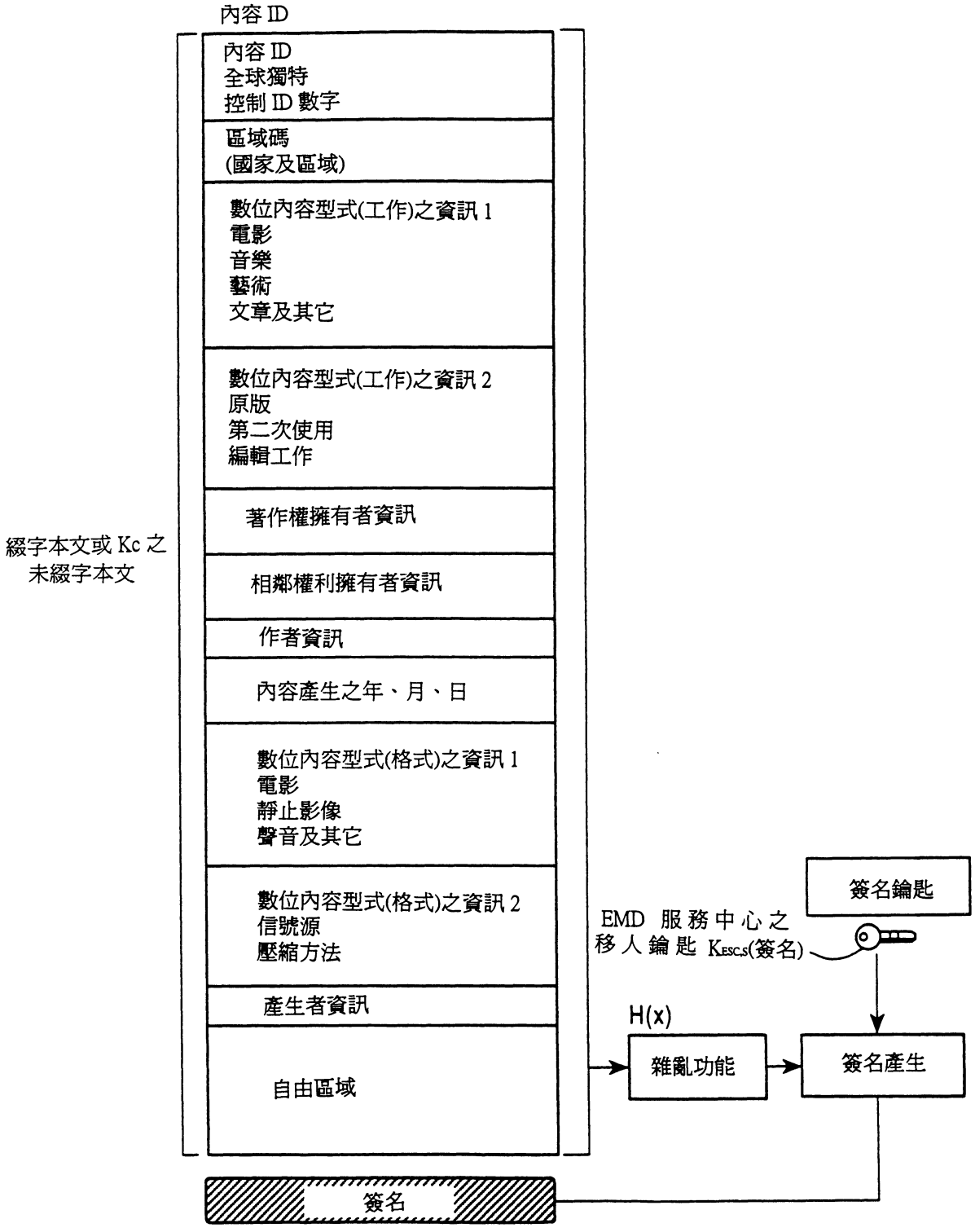

內容 ID
內容 ID
全球獨特
控制 ID 數字
區域碼
(國家及區域)
數位內容型式(工作)之資訊 1
電影
音樂
藝術
文章及其它
數位內容型式(工作)之資訊 2
原版
第二次使用
編輯工作
著作權擁有者資訊
相鄰權利擁有者資訊
作者資訊
內容產生之年、月、日
數位內容型式(格式)之資訊 1
電影
靜止影像
聲音及其它
數位內容型式(格式)之資訊 2
信號源
壓縮方法
產生者資訊
自由區域
綴字本文或 Kc 之
未綴字本文
簽名
簽名鑰匙
EMD 服務中心之
移人鑰匙 KESCS(簽名)
H(x)
雜亂功能
簽名產生

圖 9

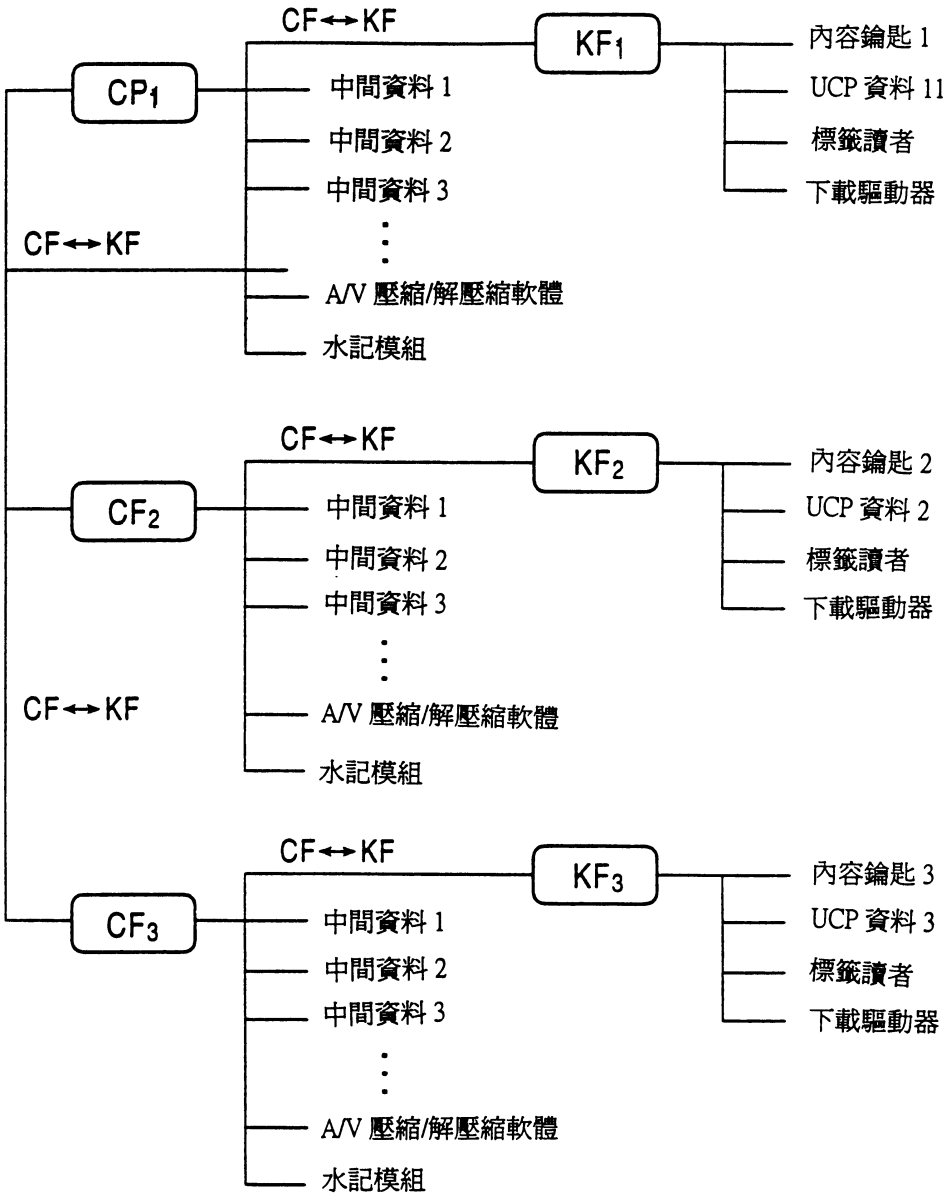

CF↔KF
KF1
內容鑰匙 1
UCP 資料 11
標籤讀者
下載驅動器
CP1
中間資料 1
中間資料 2
中間資料 3
CF↔KF
A/V 壓縮/解壓縮軟體
水記模組
CF↔KF
KF2
內容鑰匙 2
UCP 資料 2
標籤讀者
下載驅動器
CF2
中間資料 1
中間資料 2
中間資料 3
CF↔KF
A/V 壓縮/解壓縮軟體
水記模組
CF↔KF
KF3
內容鑰匙 3
UCP 資料 3
標籤讀者
下載驅動器
CF3
中間資料 1
中間資料 2
中間資料 3
A/V 壓縮/解壓縮軟體
水記模組

圖１０

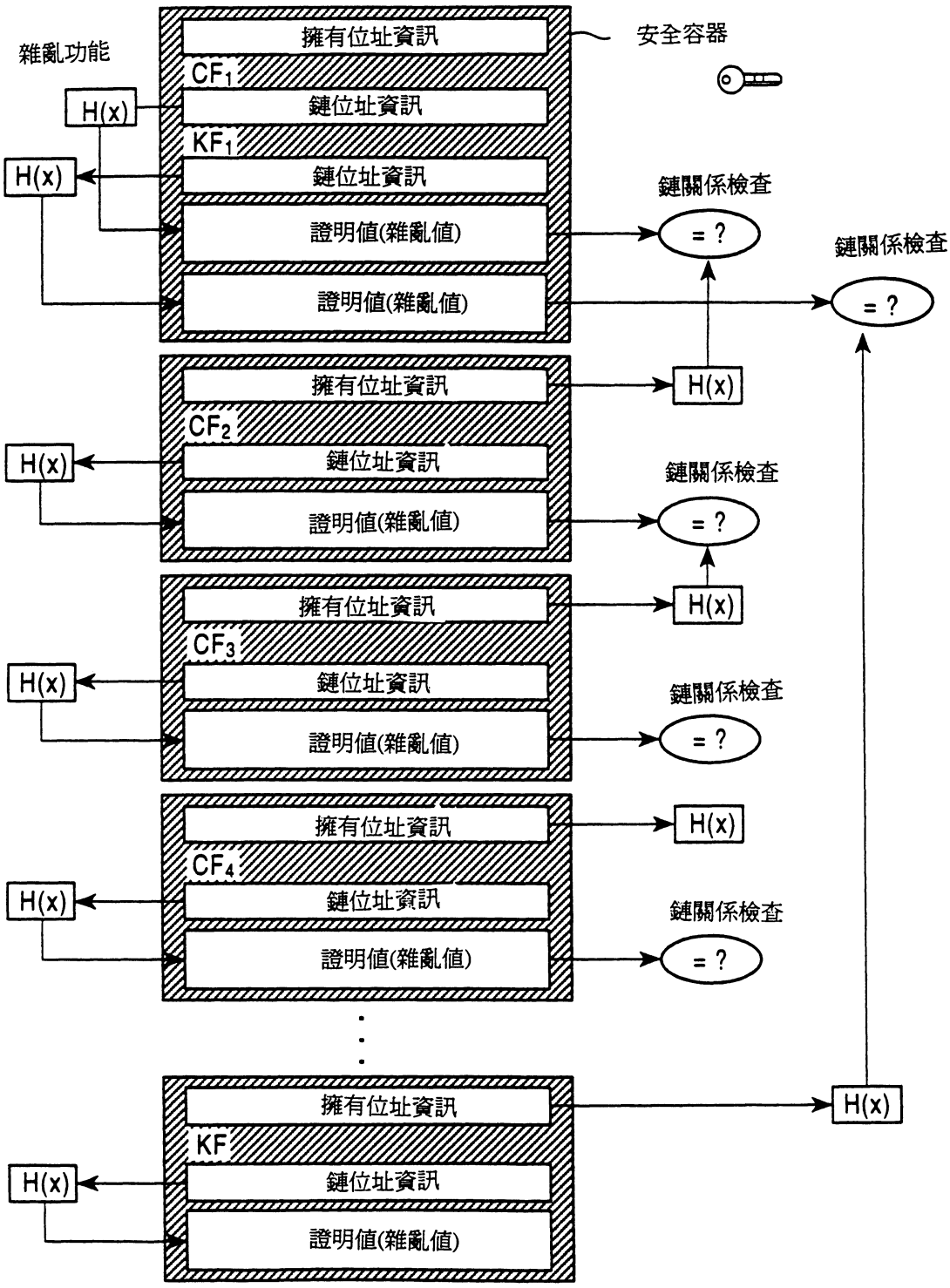

雜亂功能
安全容器
擁有位址資訊
CF1
鏈位址資訊
KF1
鏈位址資訊
證明值(雜亂值)
證明值(雜亂值)
H(x)
鏈關係檢查
= ?
擁有位址資訊
CF2
鏈位址資訊
證明值(雜亂值)
擁有位址資訊
CF3
鏈位址資訊
證明值(雜亂值)
擁有位址資訊
CF4
鏈位址資訊
證明值(雜亂值)
擁有位址資訊
KF
鏈位址資訊
證明值(雜亂值)

圖１１

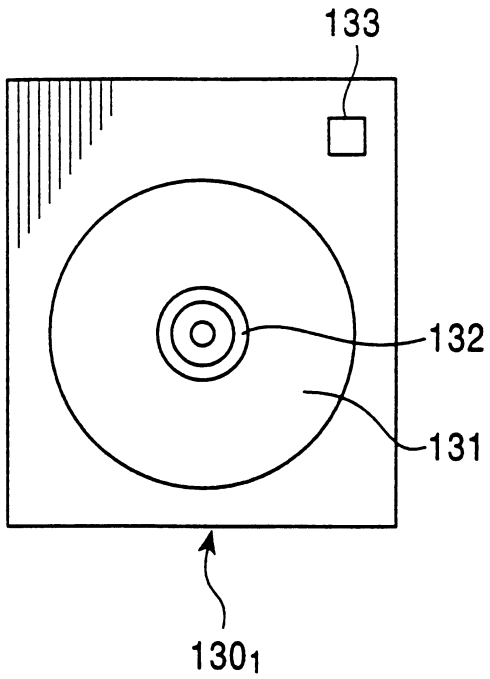


圖１２

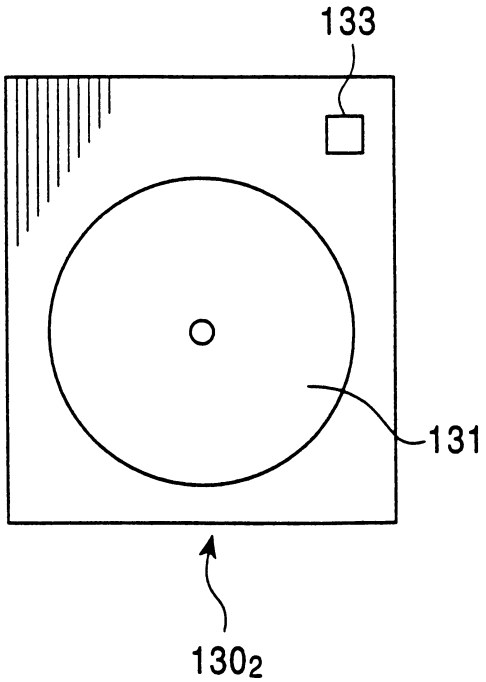


圖１３

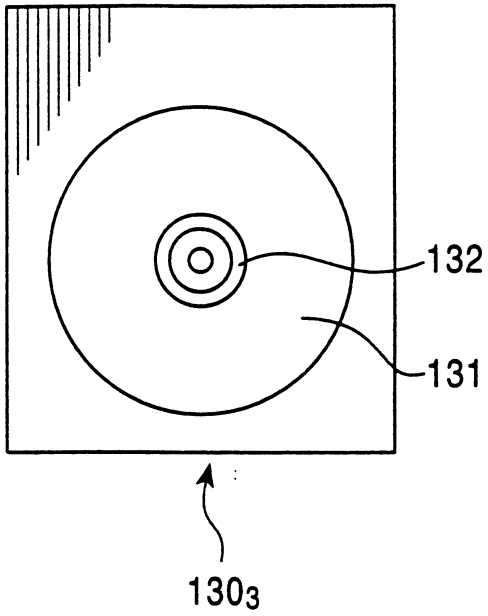


圖１４

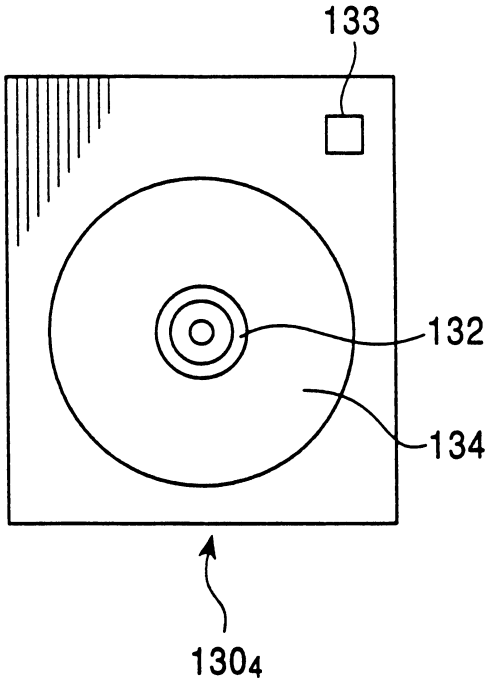


圖１５

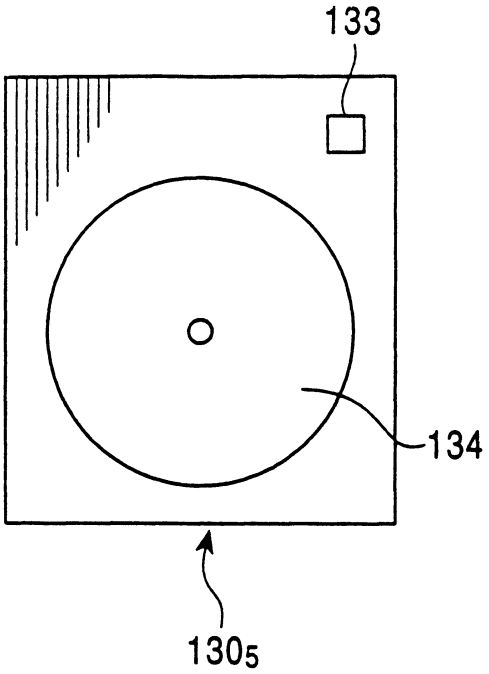


圖１６

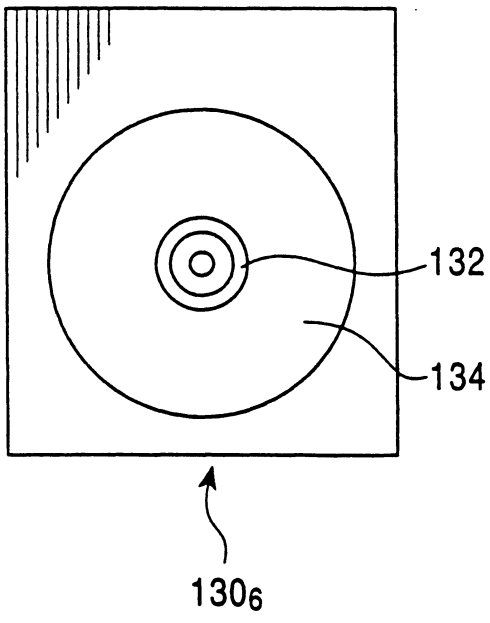


圖１７

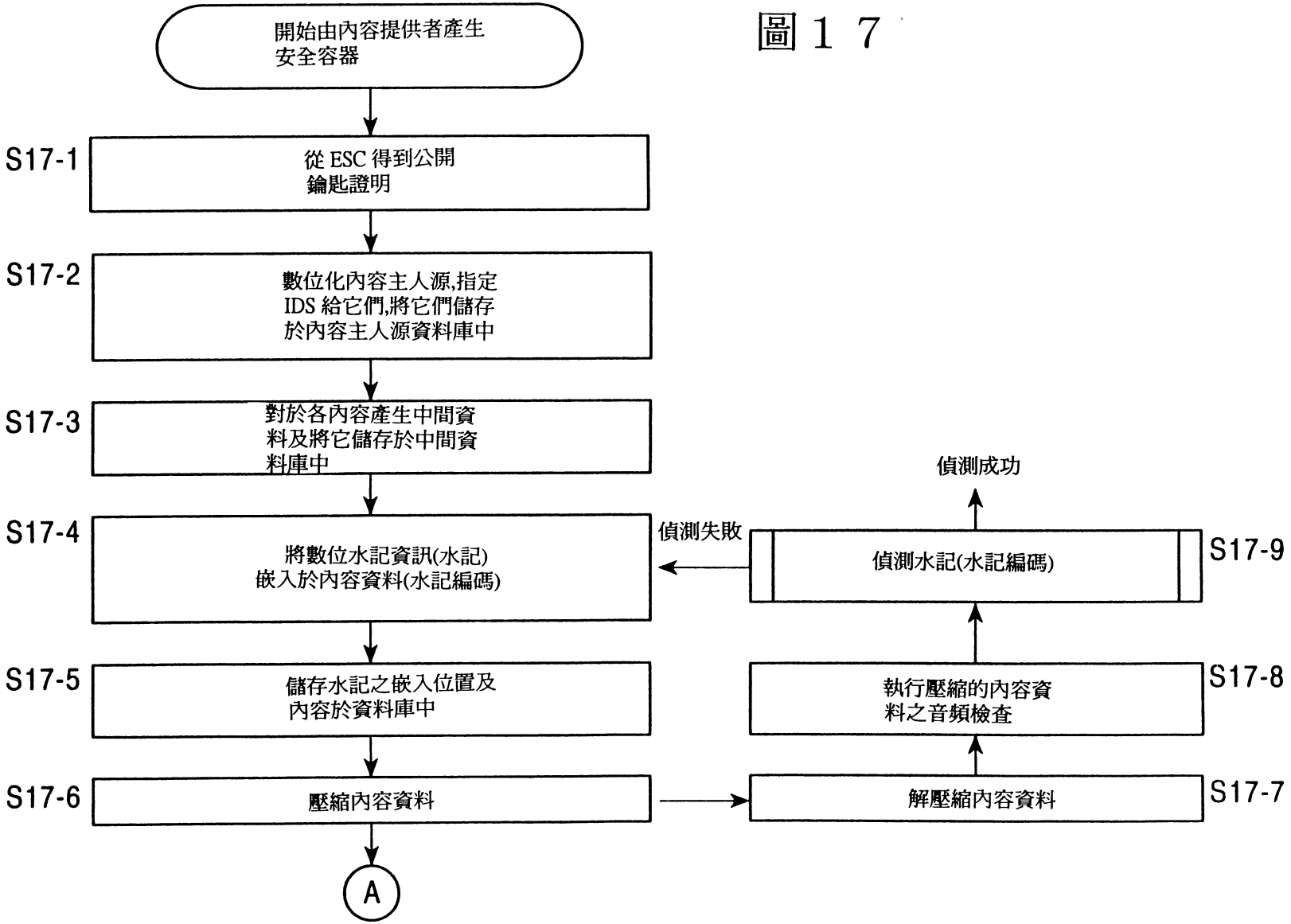

開始由內容提供者產生
安全容器
S17-1
從 ESC 得到公開
鑰匙證明
S17-2
數位化內容主人源,指定
IDS 給它們,將它們儲存
於內容主人源資料庫中
S17-3
對於各內容產生中間資
料及將它儲存於中間資
料庫中
S17-4
將數位水記資訊(水記)
嵌入於內容資料(水記編碼)
S17-5
儲存水記之嵌入位置及
內容於資料庫中
S17-6
壓縮內容資料
A
偵測失敗
偵測成功
偵測水記(水記編碼)
S17-9
執行壓縮的內容資
料之音頻檢查
S17-8
解壓縮內容資料
S17-7

圖１８

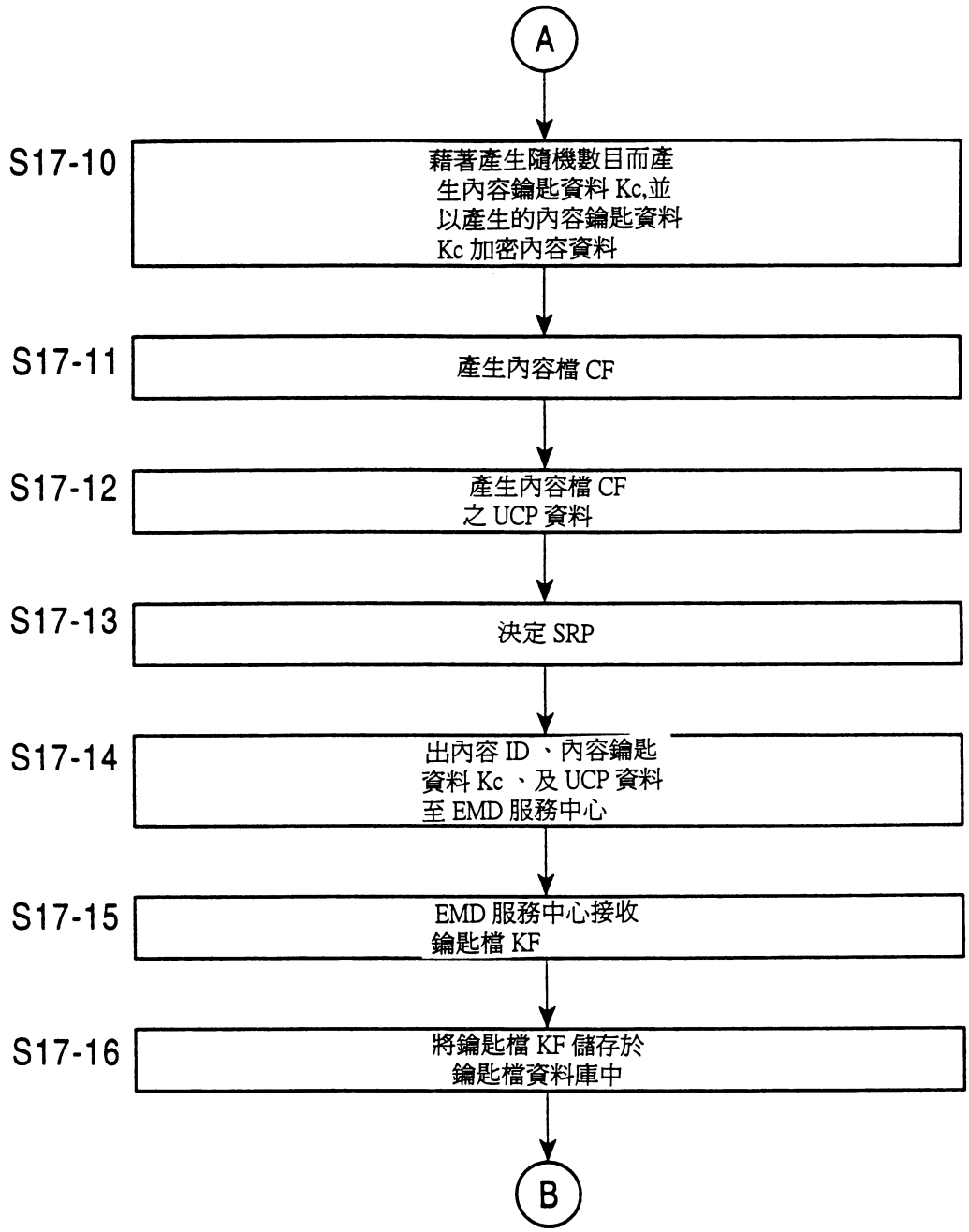

A
S17-10
藉著產生隨機數目而產生內容鑰匙資料 Kc,並以產生的內容鑰匙資料 Kc 加密內容資料
S17-11
產生內容檔 CF
S17-12
產生內容檔 CF 之 UCP 資料
S17-13
決定 SRP
S17-14
出內容 ID、內容鑰匙資料 Kc、及 UCP 資料至 EMD 服務中心
S17-15
EMD 服務中心接收鑰匙檔 KF
S17-16
將鑰匙檔 KF 儲存於鑰匙檔資料庫中
B

圖１９

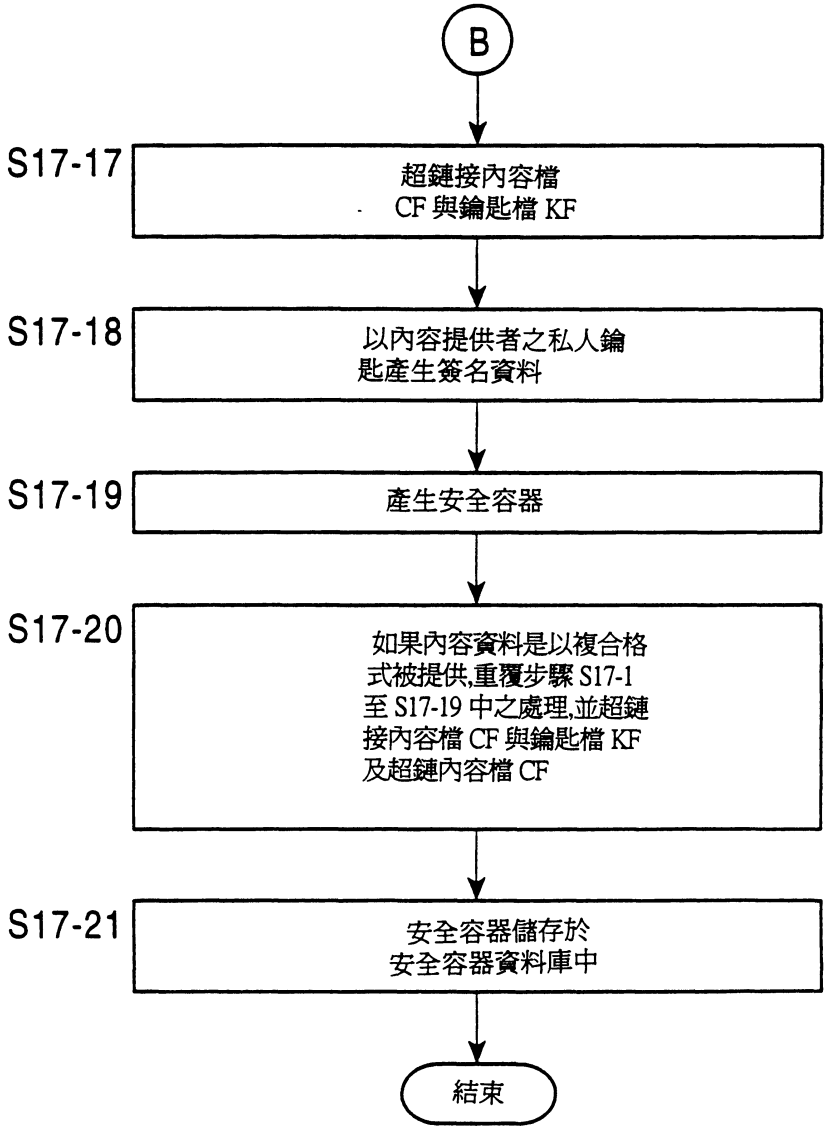

B
S17-17
超鏈接內容檔
CF 與鑰匙檔 KF
S17-18
以內容提供者之私人鑰
匙產生簽名資料
S17-19
產生安全容器
S17-20
如果內容資料是以複合格
式被提供,重覆步驟 S17-1
至 S17-19 中之處理,並超鏈
接內容檔 CF 與鑰匙檔 KF
及超鏈內容檔 CF
S17-21
安全容器儲存於
安全容器資料庫中
結束

圖２０

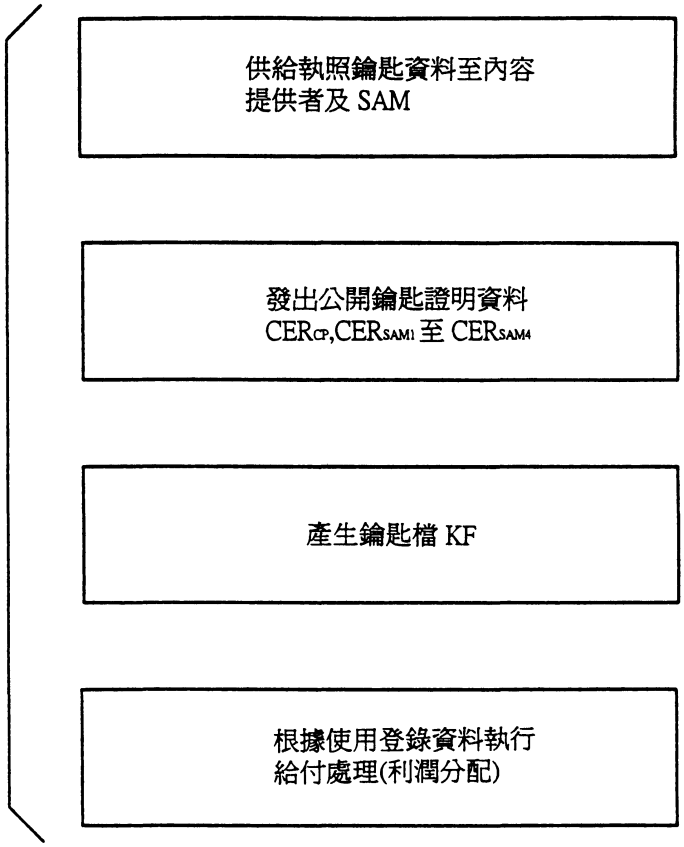

供給執照鑰匙資料至內容
提供者及 SAM
發出公開鑰匙證明資料
CERCP,CERSAM1 至 CERSAM4
產生鑰匙檔 KF
根據使用登錄資料執行
給付處理(利潤分配)

圖２１

ESC_內容 ID
CP_內容 ID
(SP_內容 ID)
使用者 ID
使用者資訊
SAM_ID
HNG_ID
打折資訊
追蹤資訊
(價格資料 PT)
CP_ID
(SP_ID)
服務提供者 ID
硬體提供者
媒體_ID
零件 ID
執照擁有者 LH_ID 之辨識
ESC_ID

圖 2 2

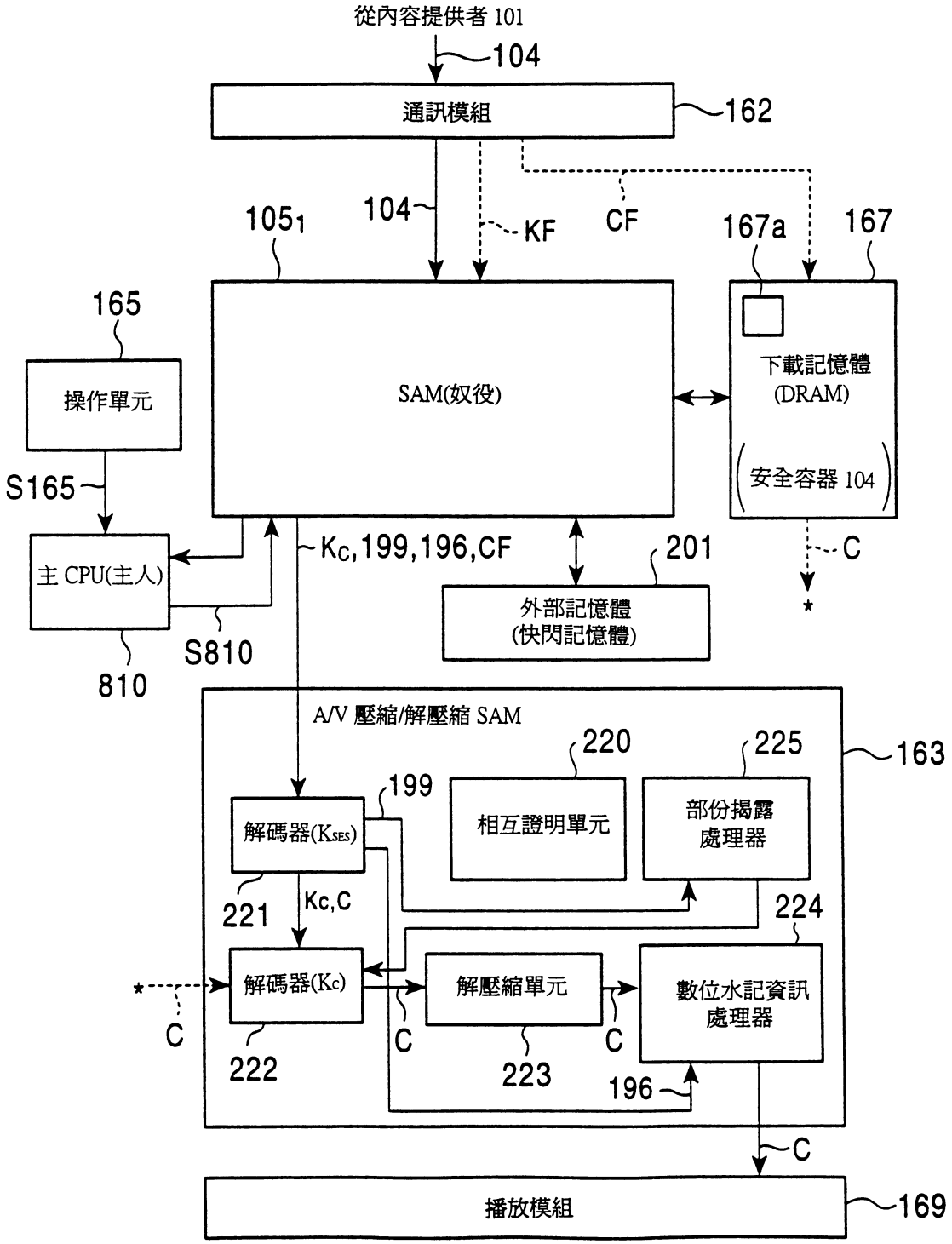

從內容提供者 101
104
通訊模組
162
104
KF
CF
105_1
167a
167
165
操作單元
SAM(奴役)
下載記憶體
(DRAM)
安全容器 104
S165
主 CPU(主人)
K_C,199,196,CF
201
C
外部記憶體
(快閃記憶體)
S810
810
A/V 壓縮/解壓縮 SAM
220
225
163
199
解碼器(K_{SES})
相互證明單元
部份揭露
處理器
221
Kc,C
224
解碼器(K_C)
解壓縮單元
數位水記資訊
處理器
C
C
C
C
222
223
196
播放模組
169

圖２３

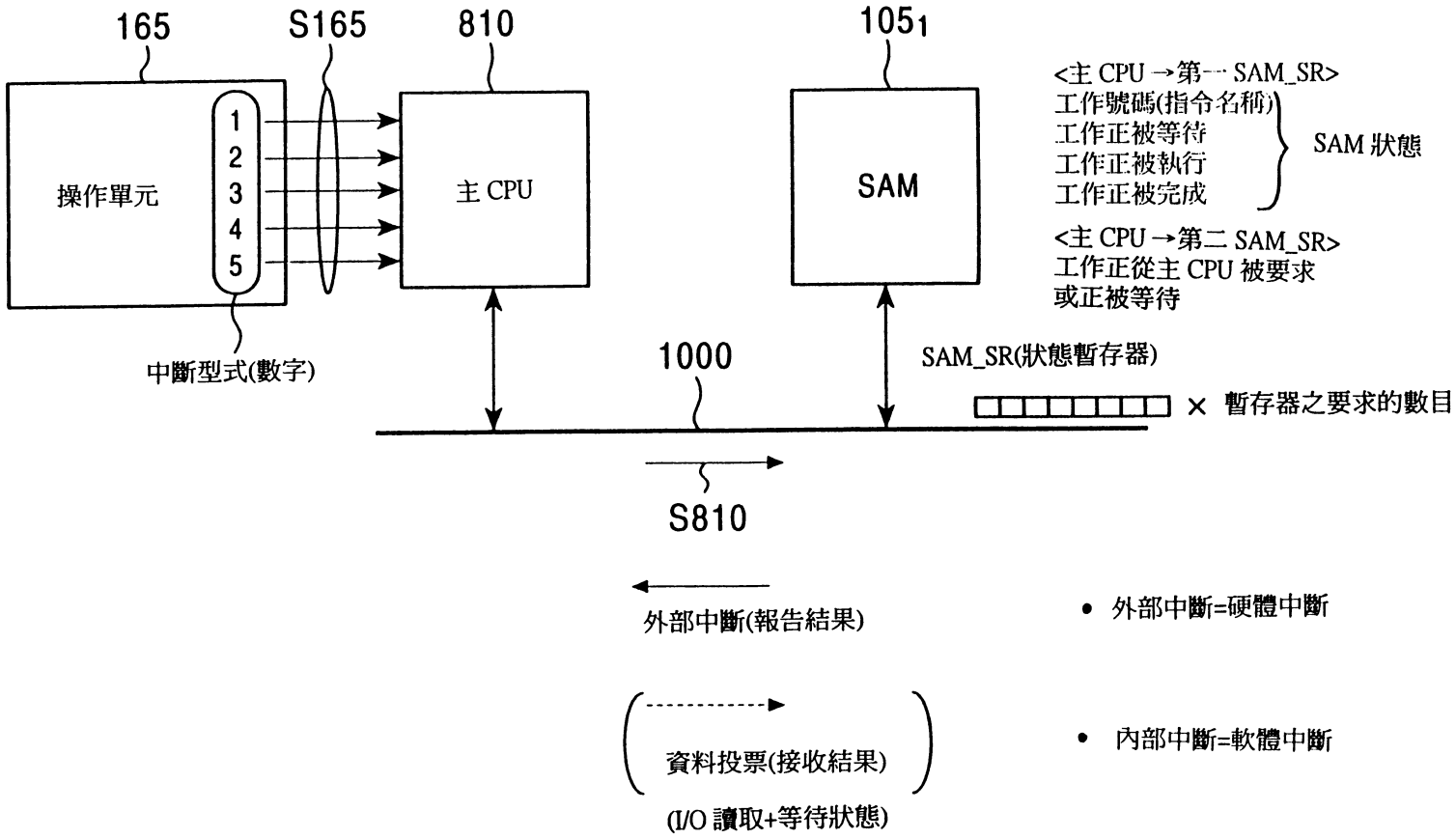

165
S165
810
105_1
操作單元
1
2
3
4
5
主 CPU
SAM
<主 CPU →第一 SAM_SR>
工作號碼(指令名稱)
工作正被等待
工作正被執行
工作正被完成
SAM 狀態
<主 CPU →第二 SAM_SR>
工作正從主 CPU 被要求
或正被等待
中斷型式(數字)
1000
SAM_SR(狀態暫存器)
× 暫存器之要求的數目
S810
外部中斷(報告結果)
• 外部中斷=硬體中斷
資料投票(接收結果)
(I/O 讀取+等待狀態)
• 內部中斷=軟體中斷

圖２４

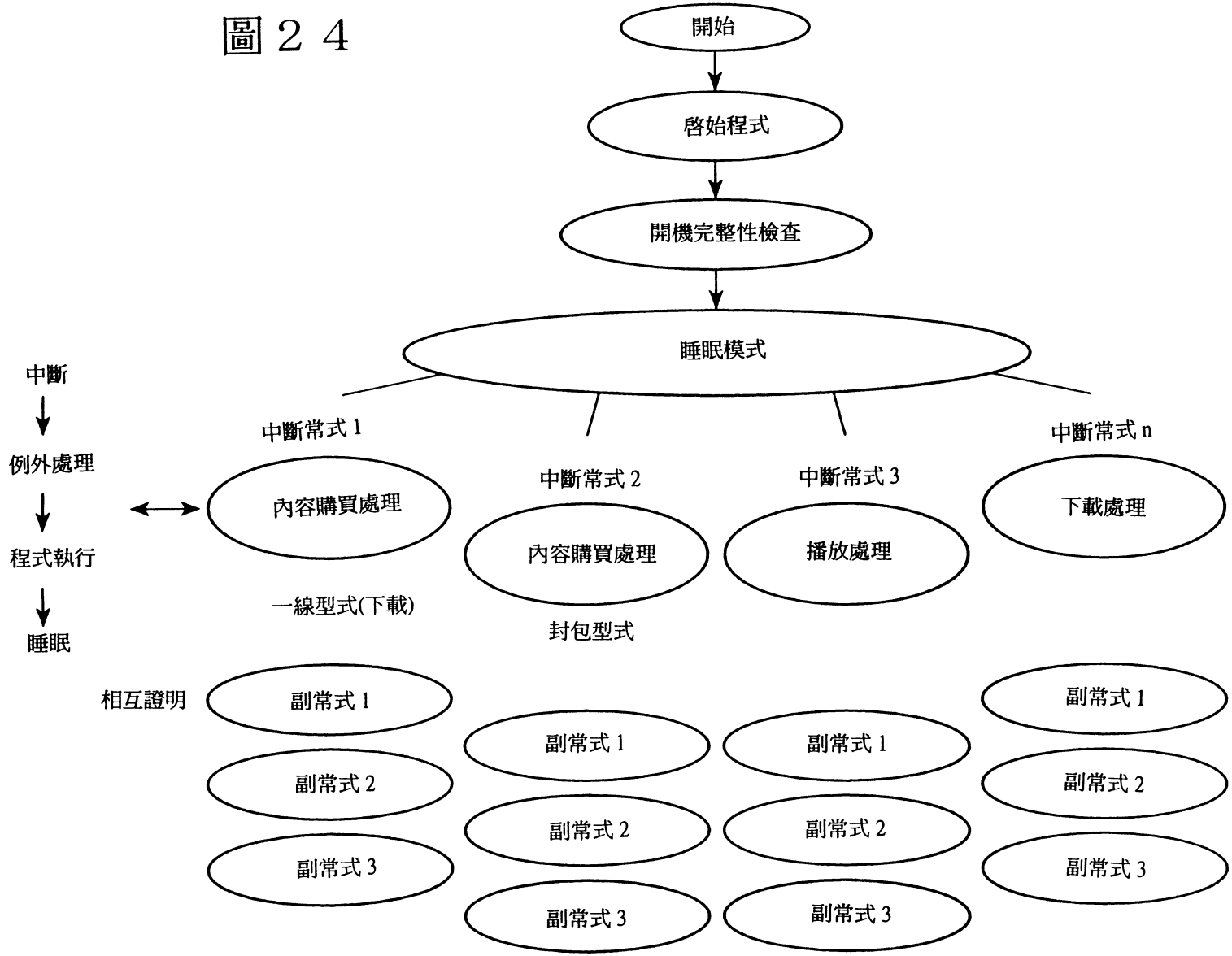

開始
啓始程式
開機完整性檢查
睡眠模式
中斷
例外處理
程式執行
睡眠
中斷常式 1
內容購買處理
一線型式(下載)
中斷常式 2
內容購買處理
封包型式
中斷常式 3
播放處理
中斷常式 n
下載處理
相互證明
副常式 1
副常式 2
副常式 3
副常式 1
副常式 2
副常式 3
副常式 1
副常式 2
副常式 3
副常式 1
副常式 2
副常式 3

圖２５

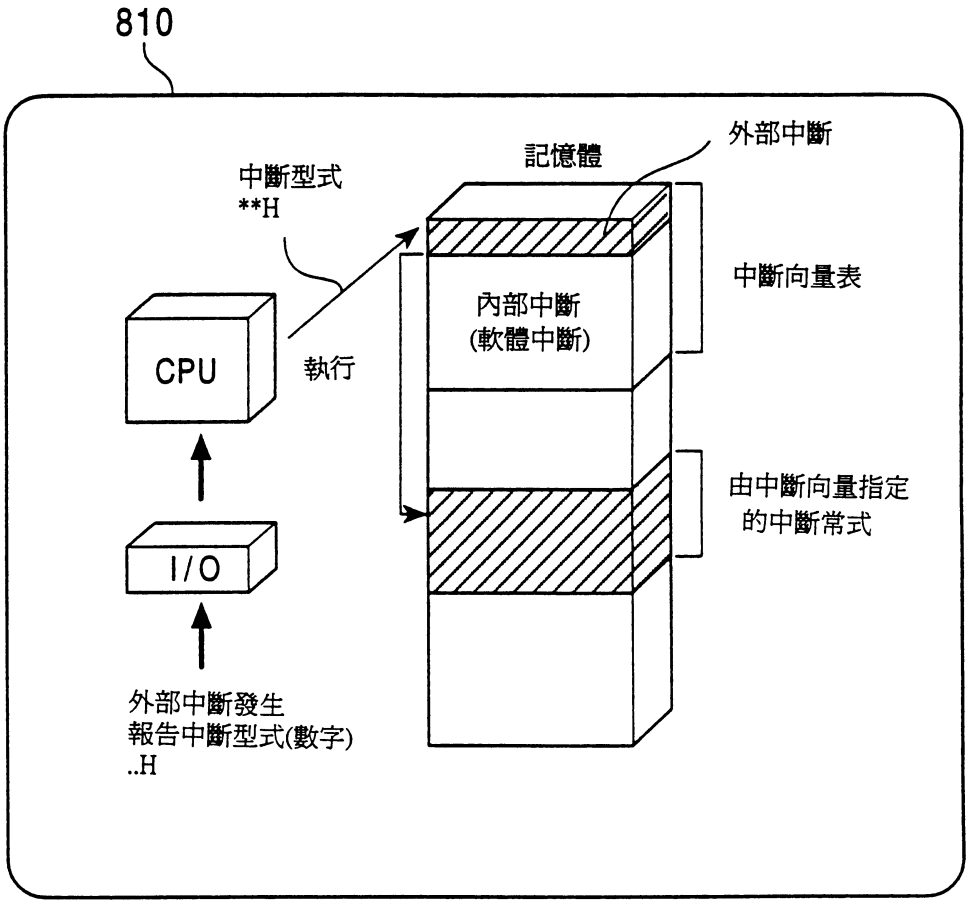

810
記憶體
外部中斷
中斷型式
**H
中斷向量表
內部中斷
(軟體中斷)
CPU
執行
由中斷向量指定
的中斷常式
I/O
外部中斷發生
報告中斷型式(數字)
..H

圖２６

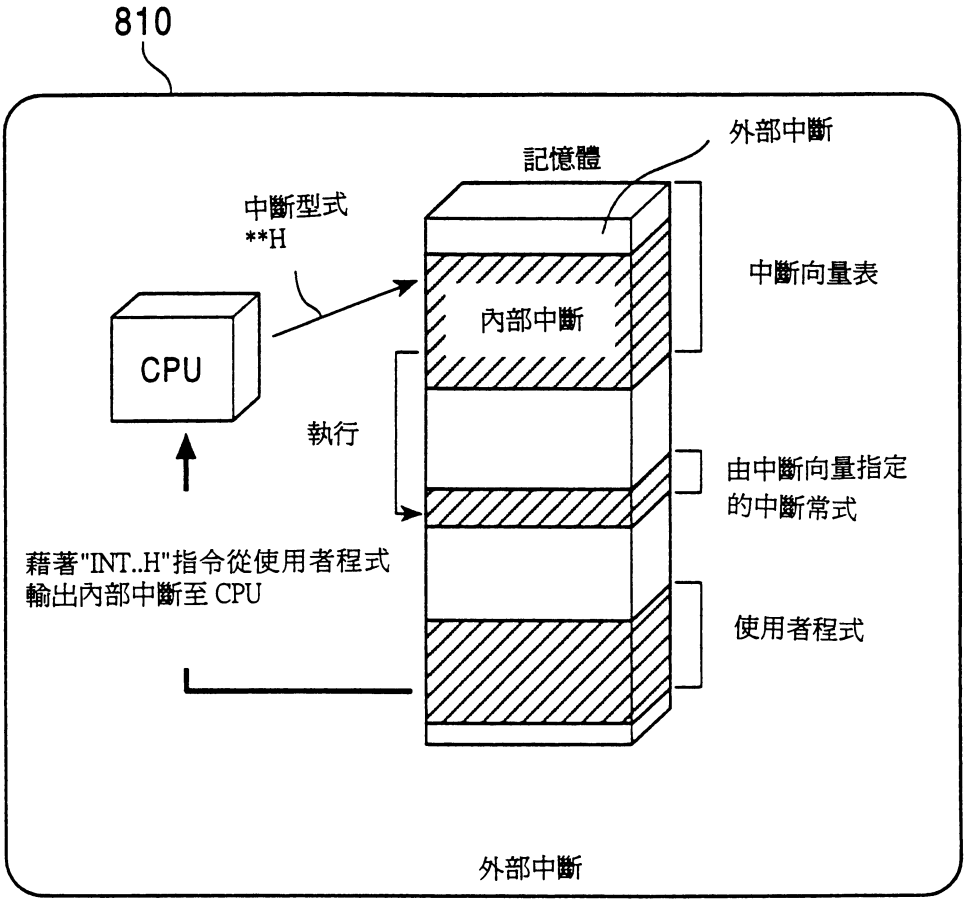

810
記憶體
外部中斷
中斷型式
**H
中斷向量表
內部中斷
CPU
執行
由中斷向量指定
的中斷常式
藉著"INT..H"指令從使用者程式
輸出內部中斷至 CPU
使用者程式
外部中斷

圖 2 7

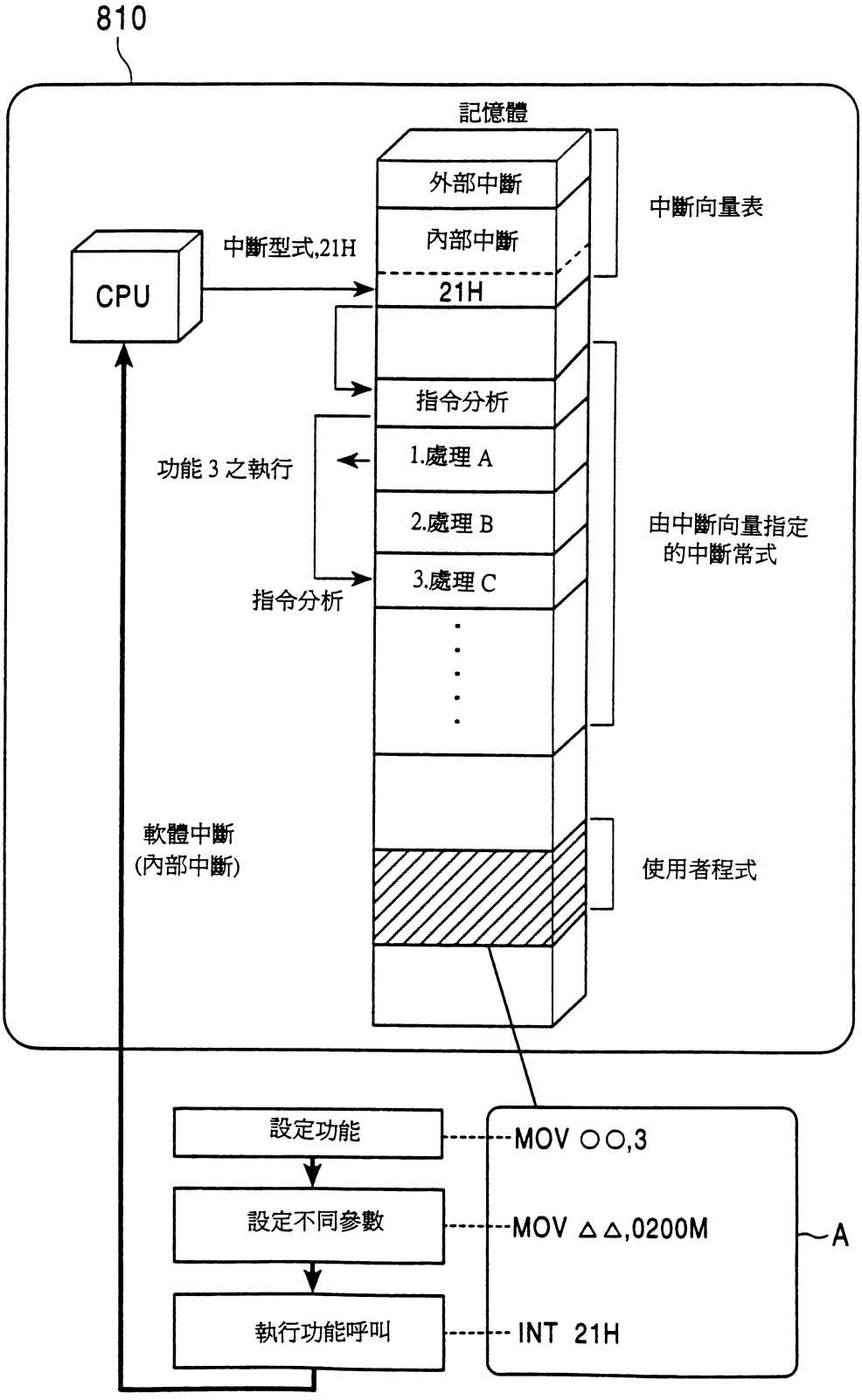

810
記憶體
外部中斷
內部中斷
21H
中斷向量表
CPU
中斷型式,21H
指令分析
功能 3 之執行
1.處理 A
2.處理 B
3.處理 C
指令分析
由中斷向量指定
的中斷常式
軟體中斷
(內部中斷)
使用者程式
設定功能
設定不同參數
執行功能呼叫
MOV ○○,3
MOV △△,0200M
INT 21H
A

圖２８

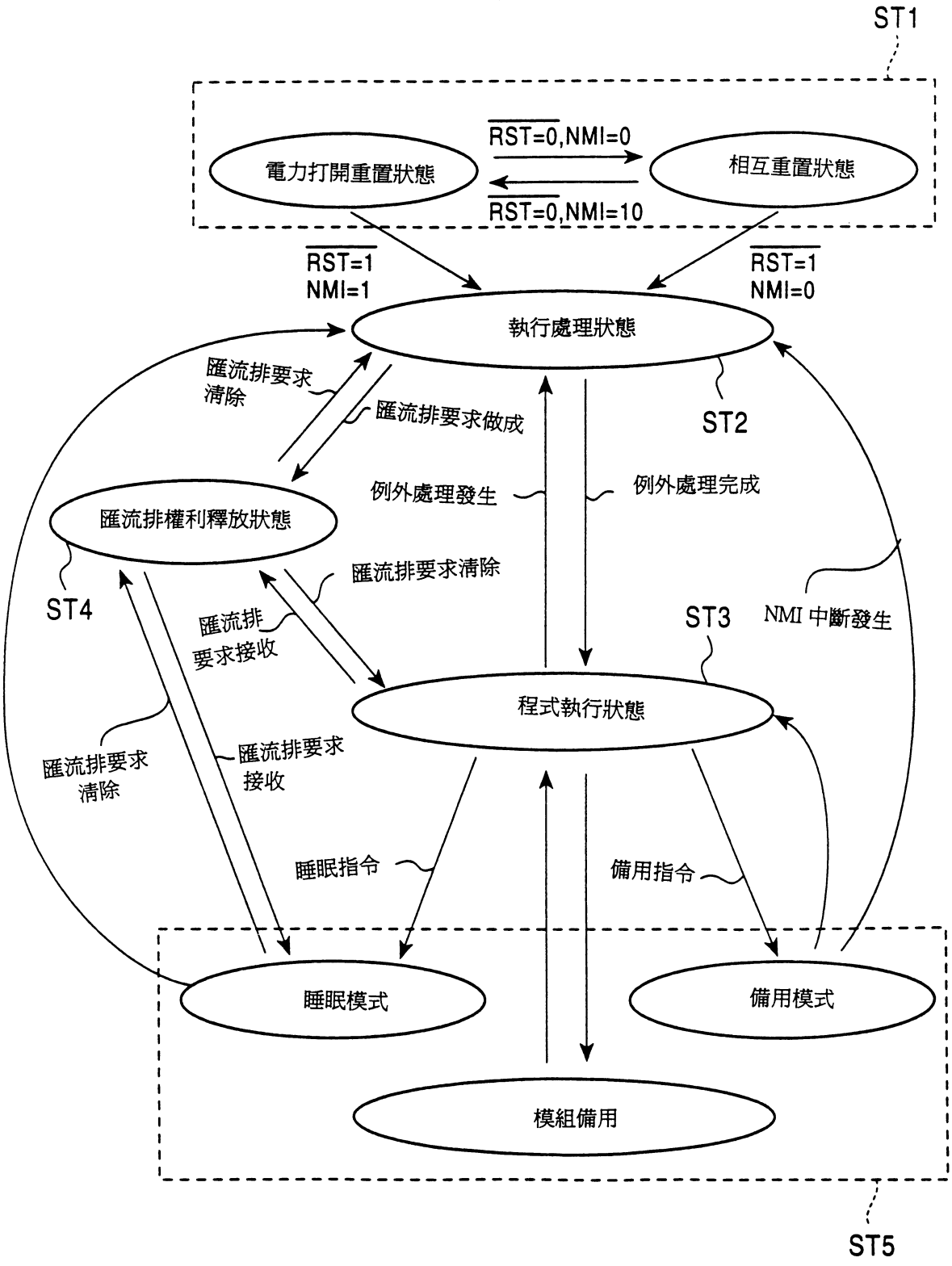

ST1
電力打開重置狀態
RST=0,NMI=0
RST=0,NMI=10
相互重置狀態
RST=1
NMI=1
RST=1
NMI=0
執行處理狀態
匯流排要求
清除
匯流排要求做成
ST2
例外處理發生
例外處理完成
匯流排權利釋放狀態
匯流排要求清除
ST4
匯流排
要求接收
ST3
NMI 中斷發生
程式執行狀態
匯流排要求
清除
匯流排要求
接收
睡眠指令
備用指令
睡眠模式
備用模式
模組備用
ST5

圖 2 9

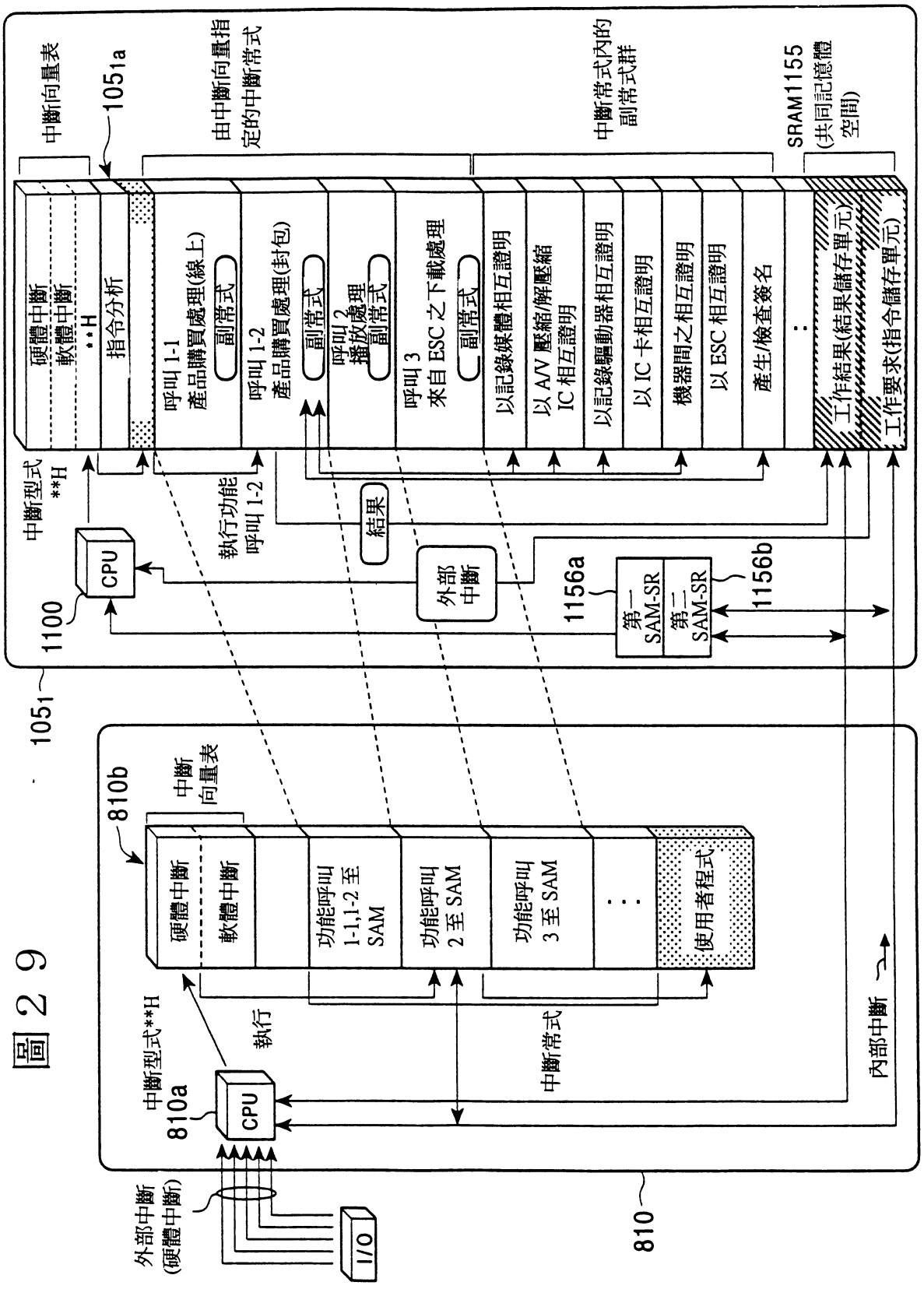

1051
中斷向量表
1051a
由中斷向量指定的中斷常式
中斷常式內的副常式群
SRAM1155
(共同記憶體空間)
硬體中斷
軟體中斷
••H
指令分析
呼叫 1-1
產品購買處理(線上)
副常式
呼叫 1-2
產品購買處理(封包)
副常式
呼叫 2
播放處理
副常式
呼叫 3
來自 ESC 之下載處理
副常式
以記錄媒體相互證明
以 A/V 壓縮/解壓縮
IC 相互證明
以記錄驅動器相互證明
以 IC 卡相互證明
機器間之相互證明
以 ESC 相互證明
產生/檢查簽名
:
工作結果(結果儲存單元)
工作要求(指令儲存單元)
中斷型式
**H
1100
CPU
執行功能
呼叫 1-2
結果
外部中斷
1156a
第一 SAM-SR
第二 SAM-SR
1156b
810b
中斷向量表
硬體中斷
軟體中斷
功能呼叫 1-1,1-2 至 SAM
功能呼叫 2 至 SAM
功能呼叫 3 至 SAM
:
使用者程式
中斷型式**H
810a
CPU
執行
中斷常式
內部中斷
外部中斷
(硬體中斷)
I/O
810

圖 30

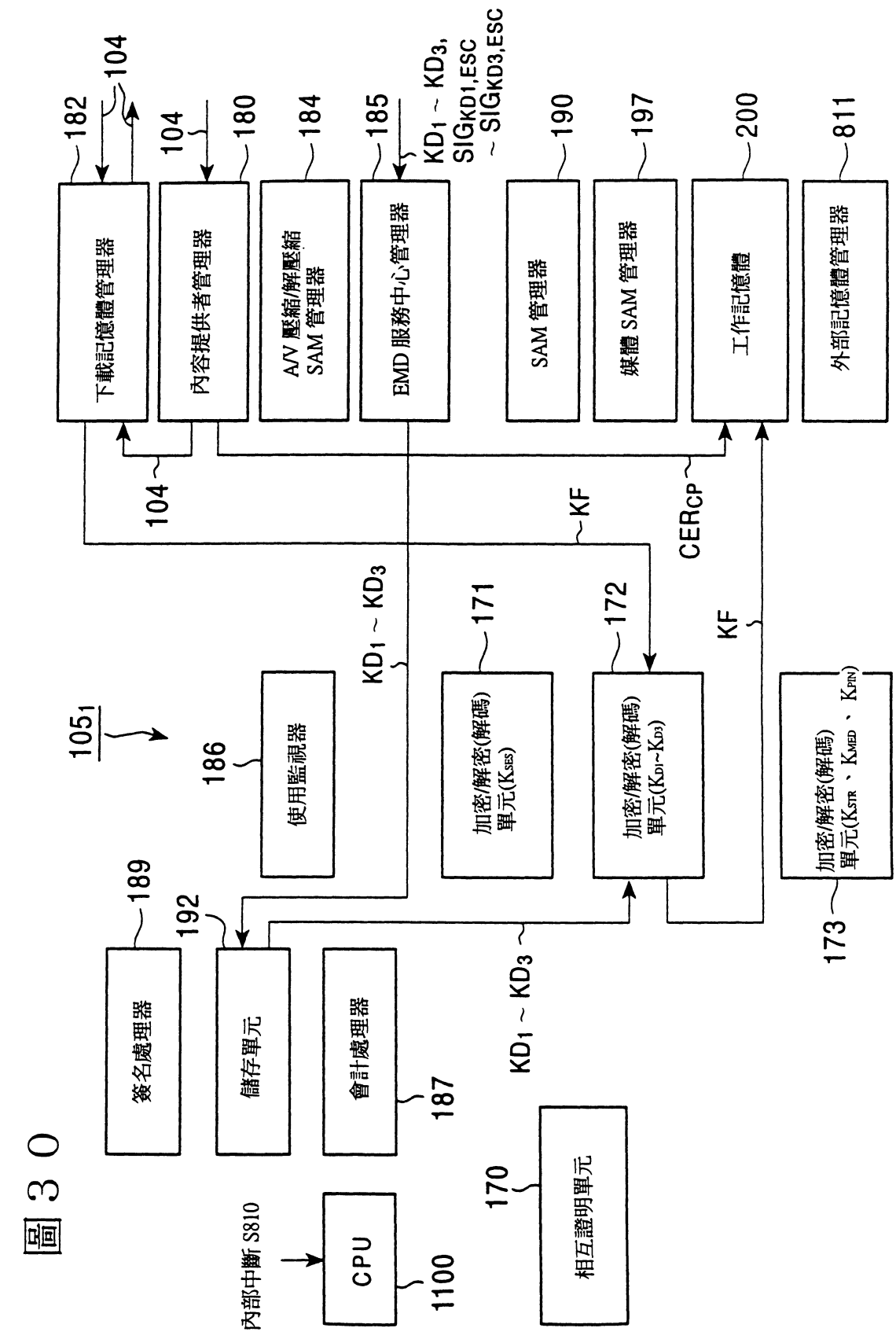

下載記憶體管理器
182
104
內容提供者管理器
104
180
A/V 壓縮/解壓縮 SAM 管理器
184
EMD 服務中心管理器
185
KD1 ~ KD3, SIGKD1,ESC ~ SIGKD3,ESC
SAM 管理器
190
媒體 SAM 管理器
197
工作記憶體
200
外部記憶體管理器
811
104
KF
CERCP
KD1 ~ KD3
1051
使用監視器
186
加密/解密(解碼)單元(KSES)
171
加密/解密(解碼)單元(KD1~KD3)
172
KF
加密/解密(解碼)單元(KSTR、KMED、KPIN)
173
189
簽名處理器
192
儲存單元
會計處理器
187
KD1 ~ KD3
內部中斷 S810
CPU
1100
170
相互證明單元

圖 3 1

第 31 圖
使用登錄資料 108
SAM 登記列表
(KF:當使用下載記憶體而不用
SAM)

圖 3 2

內容鑰匙資料 Kc
UCP 資料 106
儲存單元 192 之鎖鑰匙資料 K_{LOC}
內容提供者之公開鑰匙證明
CER_{CP}
UCS 資料 166
SAM 程式下載容器 SDC_1~SDC_3

圖 3 3

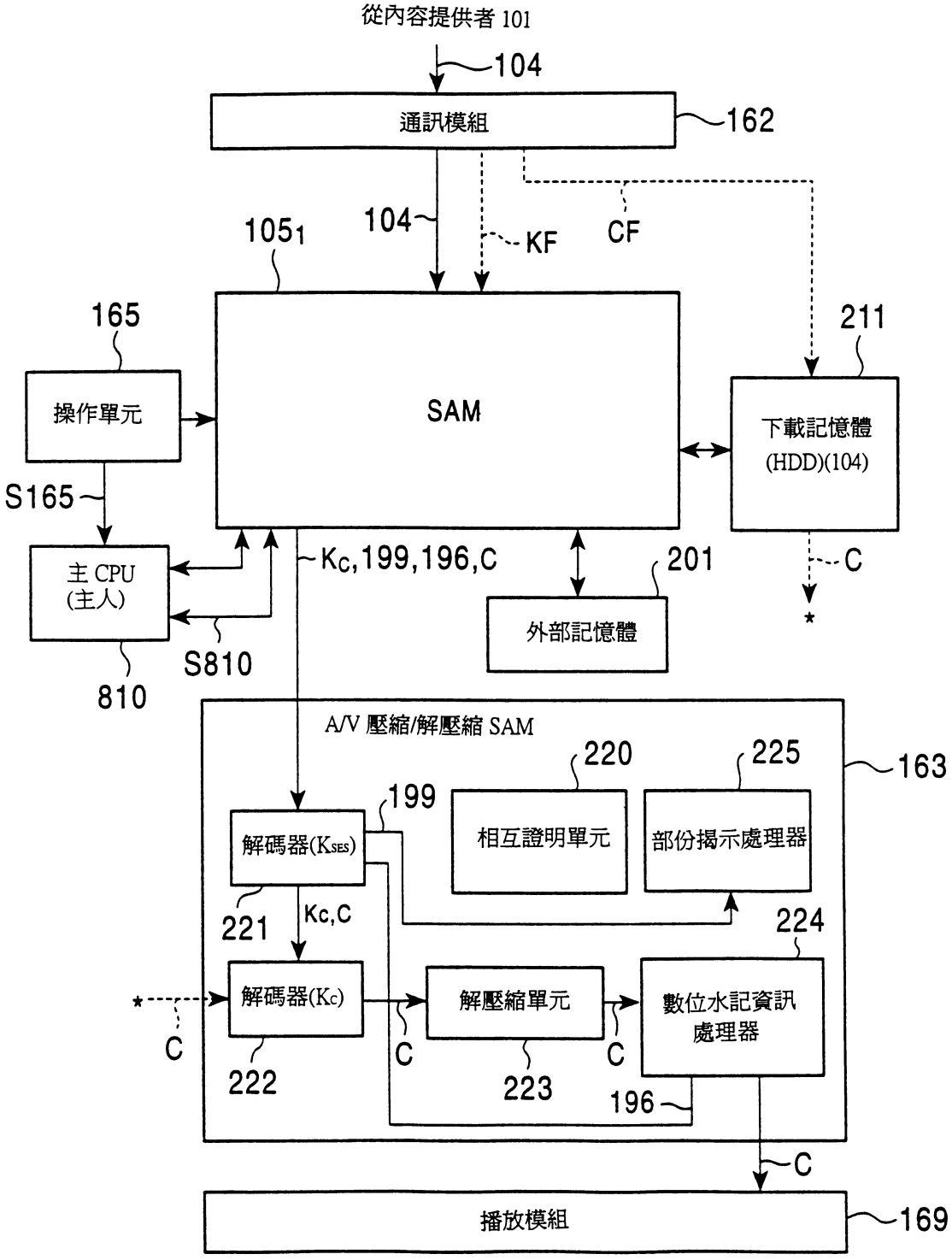

從內容提供者 101
104
通訊模組
162
104
KF
CF
105_1
165
操作單元
SAM
211
下載記憶體
(HDD)(104)
S165
主 CPU
(主人)
K_C,199,196,C
201
外部記憶體
C
S810
810
A/V 壓縮/解壓縮 SAM
220
225
163
199
解碼器(K_{SES})
相互證明單元
部份揭示處理器
221
Kc,C
224
解碼器(K_C)
解壓縮單元
數位水記資訊
處理器
C
C
C
C
222
223
196
播放模組
169

圖 3 4

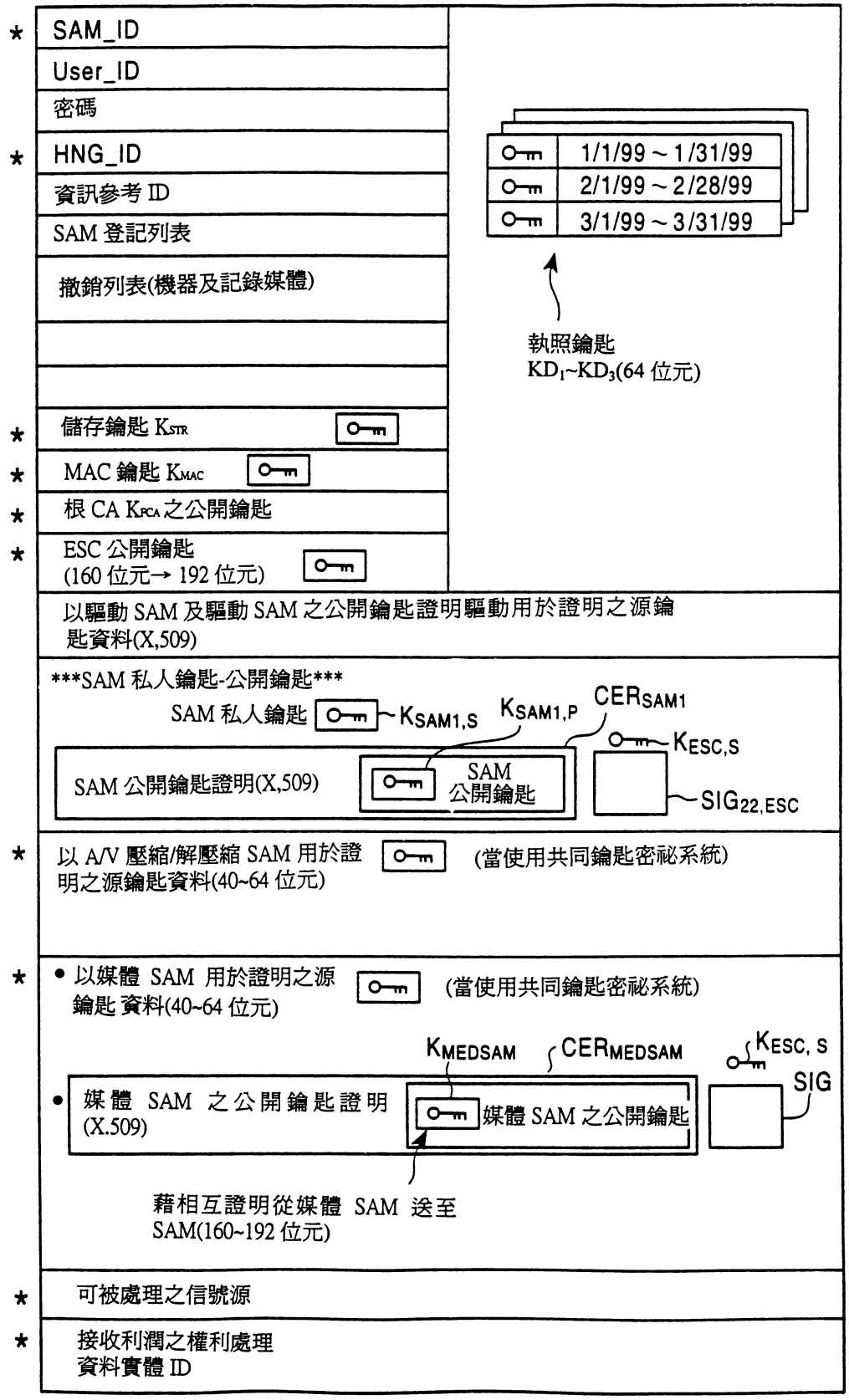

SAM_ID
User_ID
密碼
HNG_ID
資訊參考 ID
SAM 登記列表
撤銷列表(機器及記錄媒體)
儲存鑰匙 KSTR
MAC 鑰匙 KMAC
根 CA KPCA 之公開鑰匙
ESC 公開鑰匙
(160 位元→ 192 位元)
1/1/99 ~ 1/31/99
2/1/99 ~ 2/28/99
3/1/99 ~ 3/31/99
執照鑰匙
KD1~KD3(64 位元)
以驅動 SAM 及驅動 SAM 之公開鑰匙證明驅動用於證明之源鑰匙資料(X,509)
SAM 私人鑰匙-公開鑰匙
SAM 私人鑰匙
KSAM1,S
KSAM1,P
CERSAM1
KESC,S
SAM 公開鑰匙證明(X,509)
SAM 公開鑰匙
SIG22,ESC
以 A/V 壓縮/解壓縮 SAM 用於證明之源鑰匙資料(40~64 位元)
(當使用共同鑰匙密祕系統)
• 以媒體 SAM 用於證明之源鑰匙 資料(40~64 位元)
(當使用共同鑰匙密祕系統)
KMEDSAM
CERMEDSAM
KESC, S
SIG
• 媒體 SAM 之公開鑰匙證明(X.509)
媒體 SAM 之公開鑰匙
藉相互證明從媒體 SAM 送至 SAM(160~192 位元)
可被處理之信號源
接收利潤之權利處理資料實體 ID

圖３５

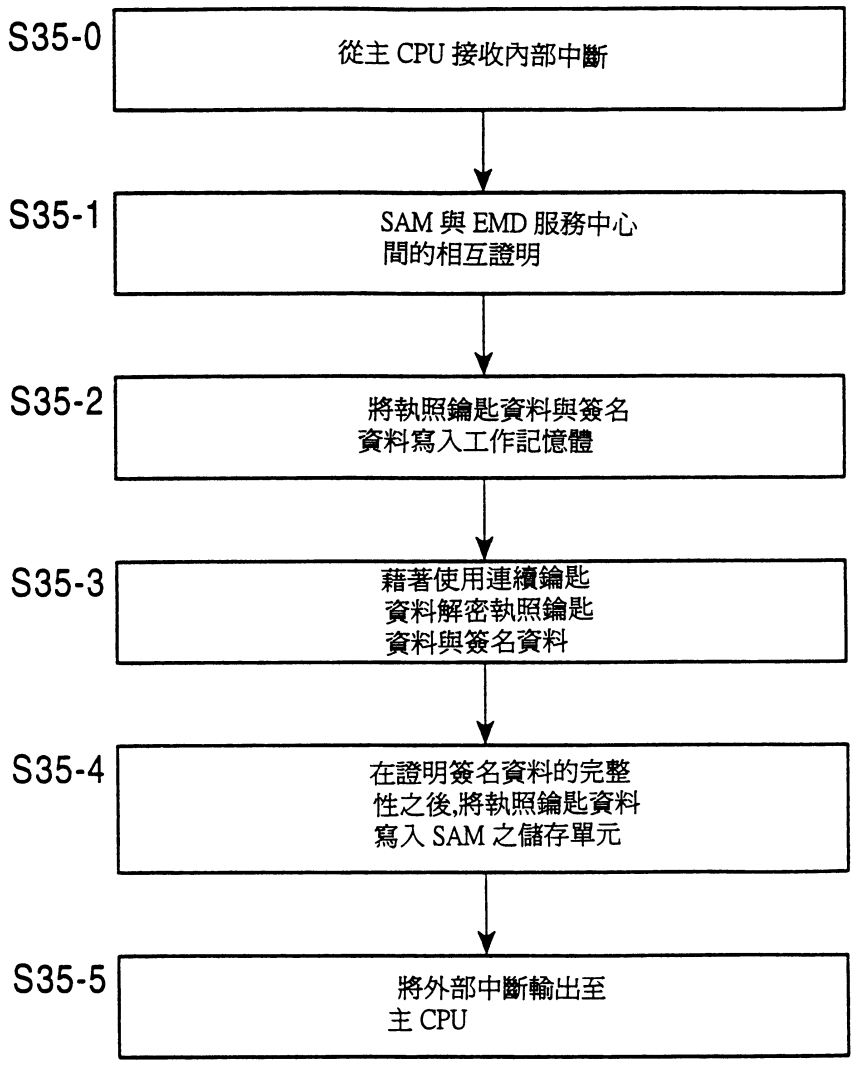
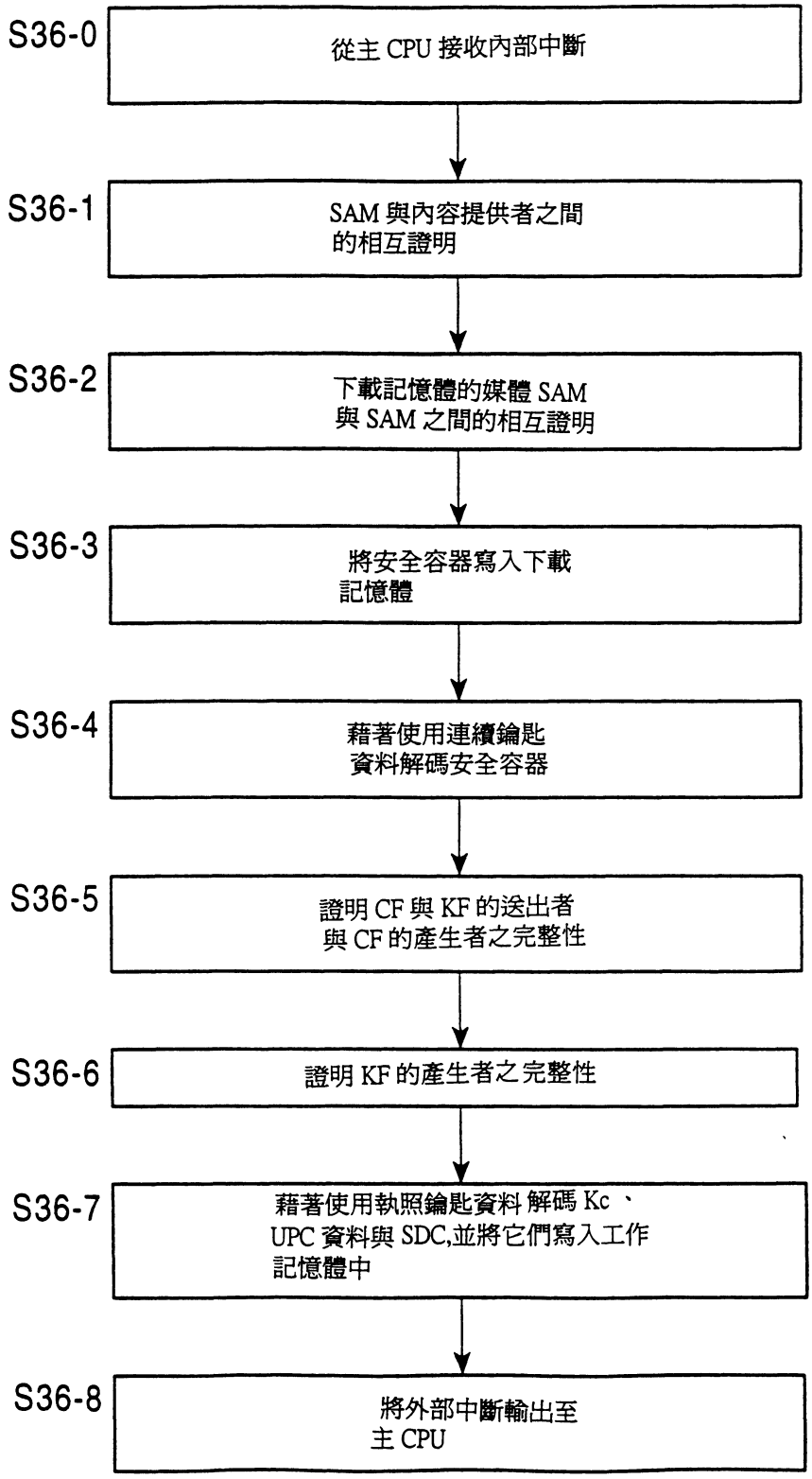

S35-0
從主 CPU 接收內部中斷
S35-1
SAM 與 EMD 服務中心
間的相互證明
S35-2
將執照鑰匙資料與簽名
資料寫入工作記憶體
S35-3
藉著使用連續鑰匙
資料解密執照鑰匙
資料與簽名資料
S35-4
在證明簽名資料的完整
性之後,將執照鑰匙資料
寫入 SAM 之儲存單元
S35-5
將外部中斷輸出至
主 CPU

圖 3 6


S36-0
從主 CPU 接收內部中斷
S36-1
SAM 與內容提供者之間
的相互證明
S36-2
下載記憶體的媒體 SAM
與 SAM 之間的相互證明
S36-3
將安全容器寫入下載
記憶體
S36-4
藉著使用連續鑰匙
資料解碼安全容器
S36-5
證明 CF 與 KF 的送出者
與 CF 的產生者之完整性
S36-6
證明 KF 的產生者之完整性
S36-7
藉著使用執照鑰匙資料解碼 Kc、
UPC 資料與 SDC,並將它們寫入工作
記憶體中
S36-8
將外部中斷輸出至
主 CPU

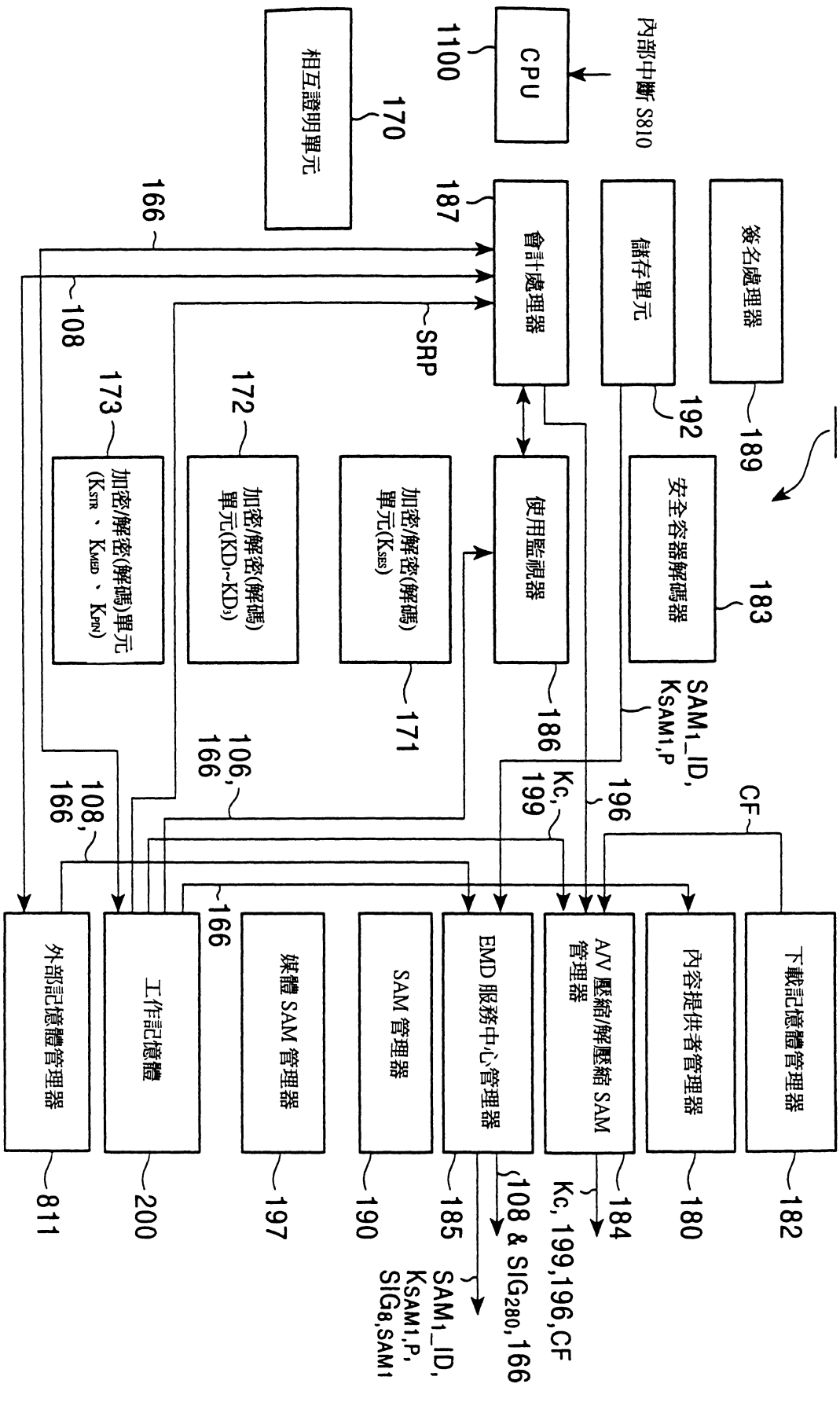

105₁
簽名處理器
189
儲存單元
192
安全容器解碼器
183
SAM₁_ID,
KSAM1,P
196
CF
下載記憶體管理器
182
內容提供者管理器
180
A/V 壓縮/解壓縮 SAM
管理器
184
Kc, 199,196,CF
EMD 服務中心管理器
185
108 & SIG280,166
SAM₁_ID,
KSAM1,P,
SIG8,SAM1
SAM 管理器
190
媒體 SAM 管理器
197
工作記憶體
200
外部記憶體管理器
811
166
內部中斷 S810
CPU
1100
相互證明單元
170
187
會計處理器
166
108
SRP
使用監視器
186
Kc,
199
加密/解密(解碼)
單元(KSES)
171
加密/解密(解碼)
單元(KD1~KD3)
172
加密/解密(解碼)單元
(KSTR、KMED、KPIN)
173
106,
166
108,
166

圖 3 7

圖 3 8

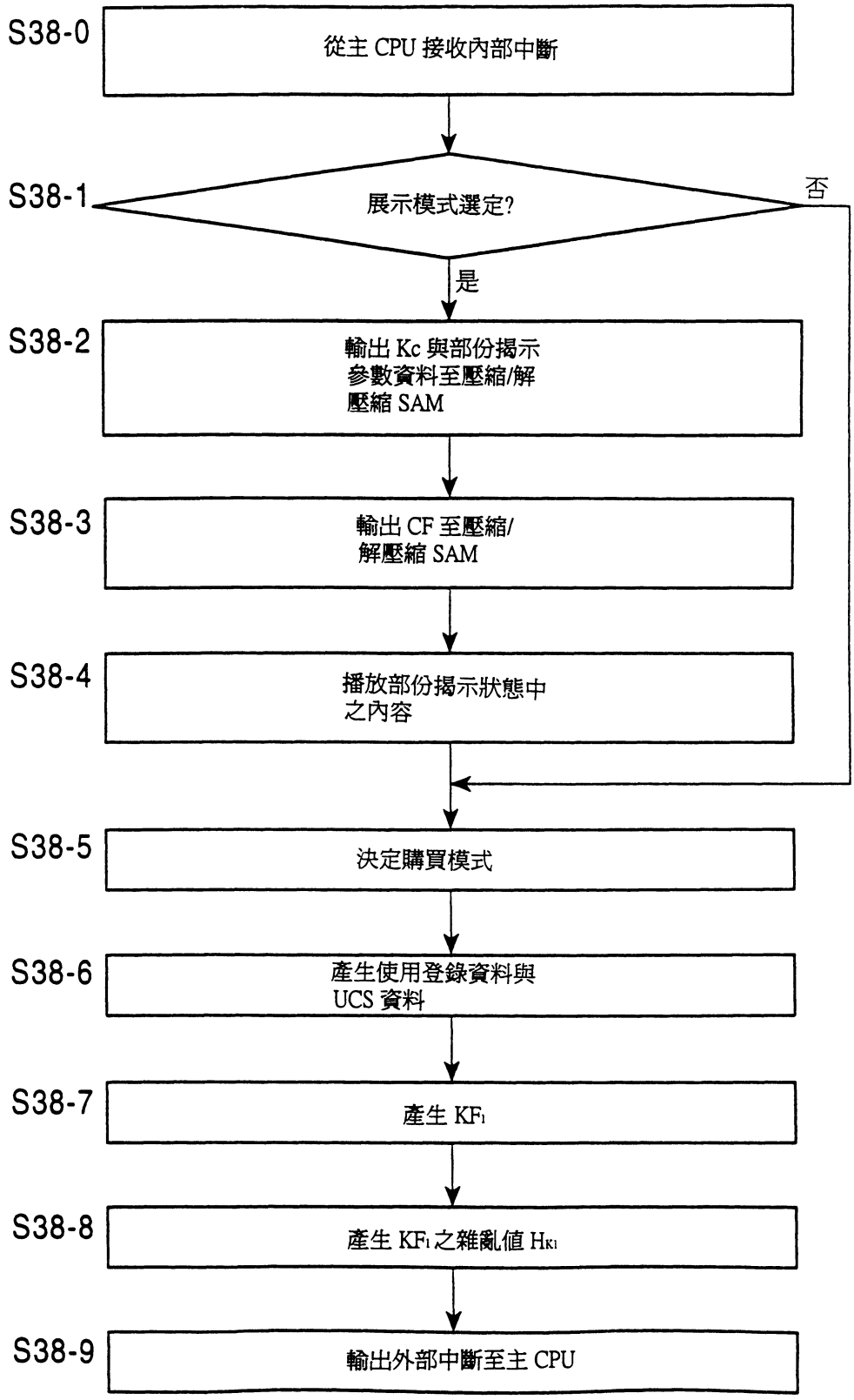

S38-0
從主 CPU 接收內部中斷
S38-1
展示模式選定?
否
是
S38-2
輸出 Kc 與部份揭示
參數資料至壓縮/解
壓縮 SAM
S38-3
輸出 CF 至壓縮/
解壓縮 SAM
S38-4
播放部份揭示狀態中
之內容
S38-5
決定購買模式
S38-6
產生使用登錄資料與
UCS 資料
S38-7
產生 KFi
S38-8
產生 KFi 之雜亂值 HKi
S38-9
輸出外部中斷至主 CPU

圖３９Ａ

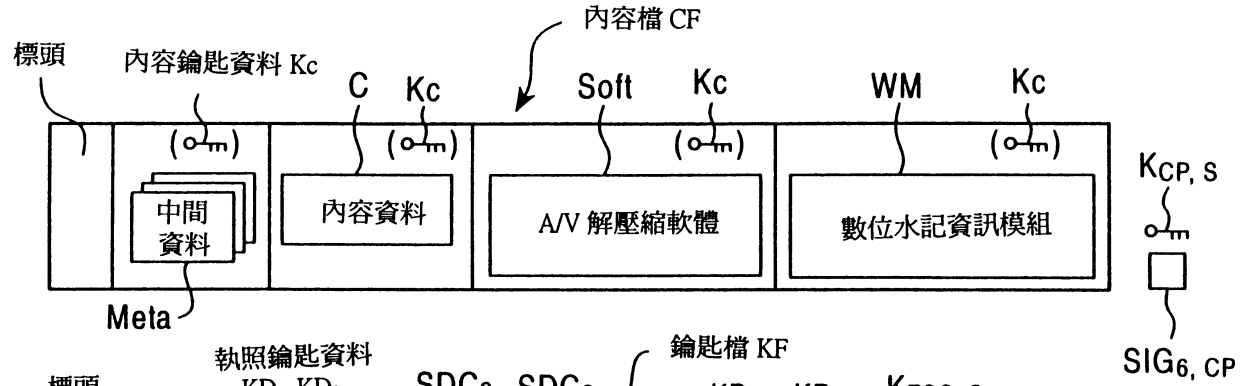


圖３９Ｂ

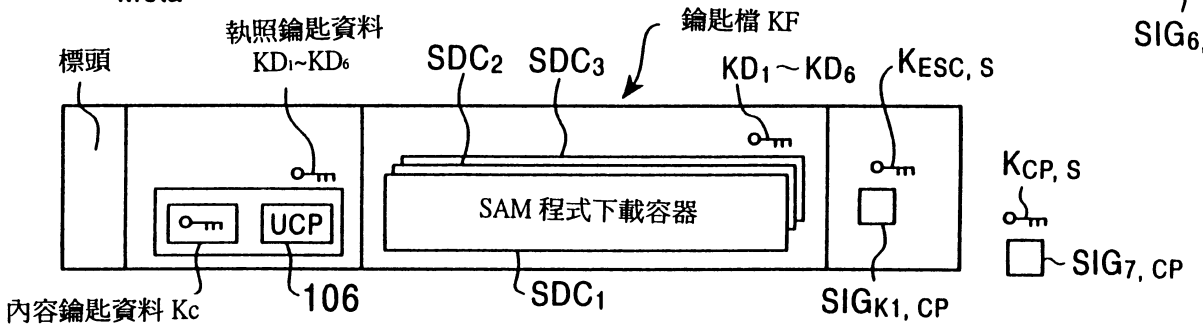


圖３９Ｃ

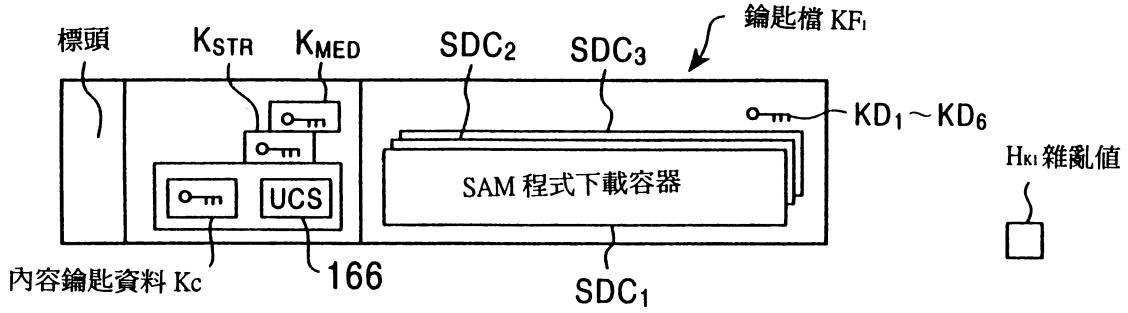


圖３９Ｄ

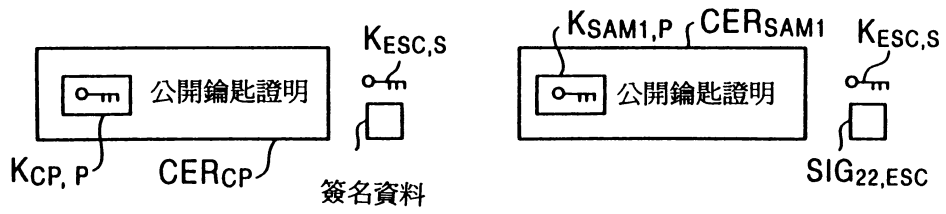


圖４０

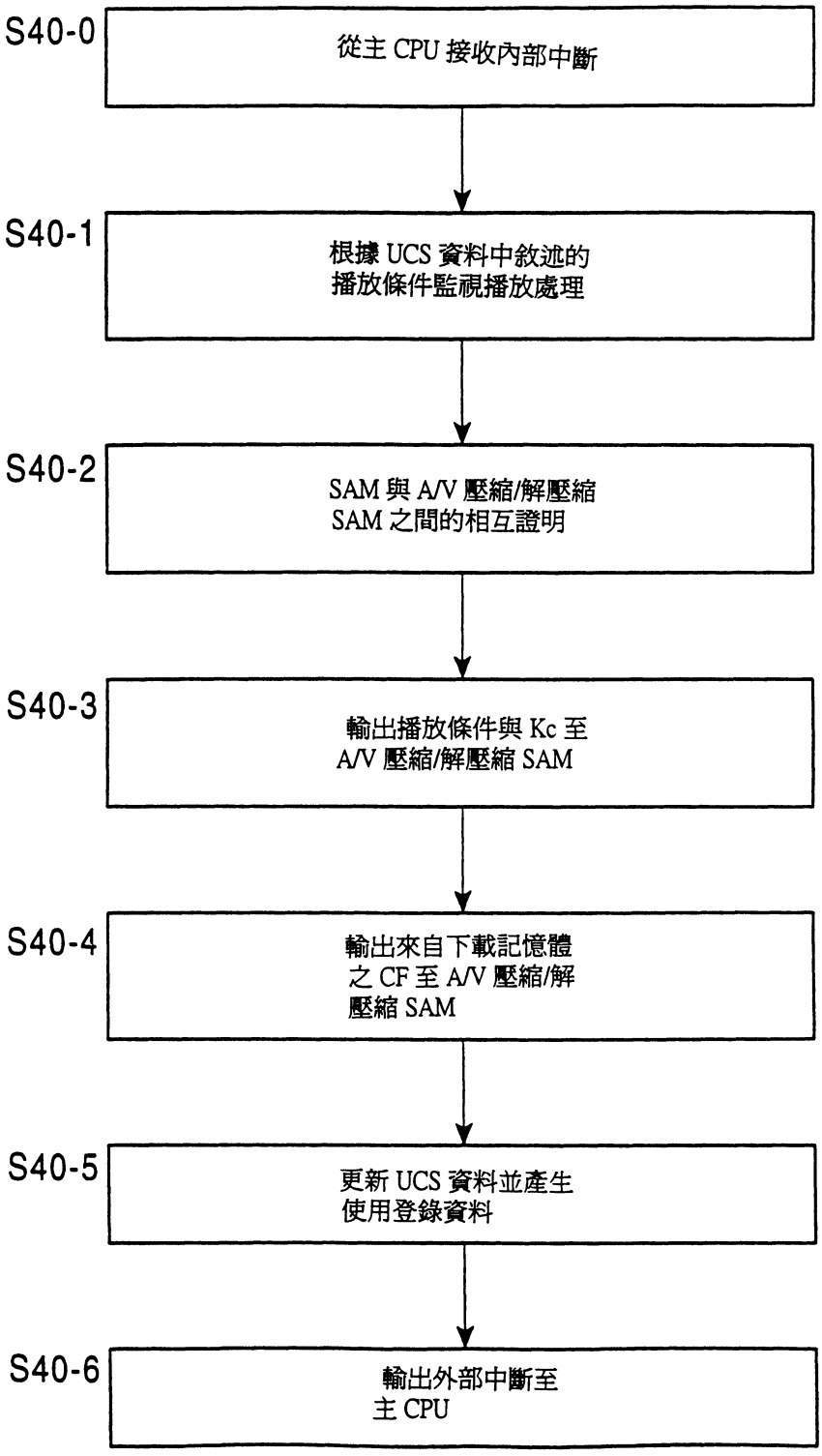

S40-0
從主 CPU 接收內部中斷
S40-1
根據 UCS 資料中敘述的
播放條件監視播放處理
S40-2
SAM 與 A/V 壓縮/解壓縮
SAM 之間的相互證明
S40-3
輸出播放條件與 Kc 至
A/V 壓縮/解壓縮 SAM
S40-4
輸出來自下載記憶體
之 CF 至 A/V 壓縮/解
壓縮 SAM
S40-5
更新 UCS 資料並產生
使用登錄資料
S40-6
輸出外部中斷至
主 CPU

圖 4 1

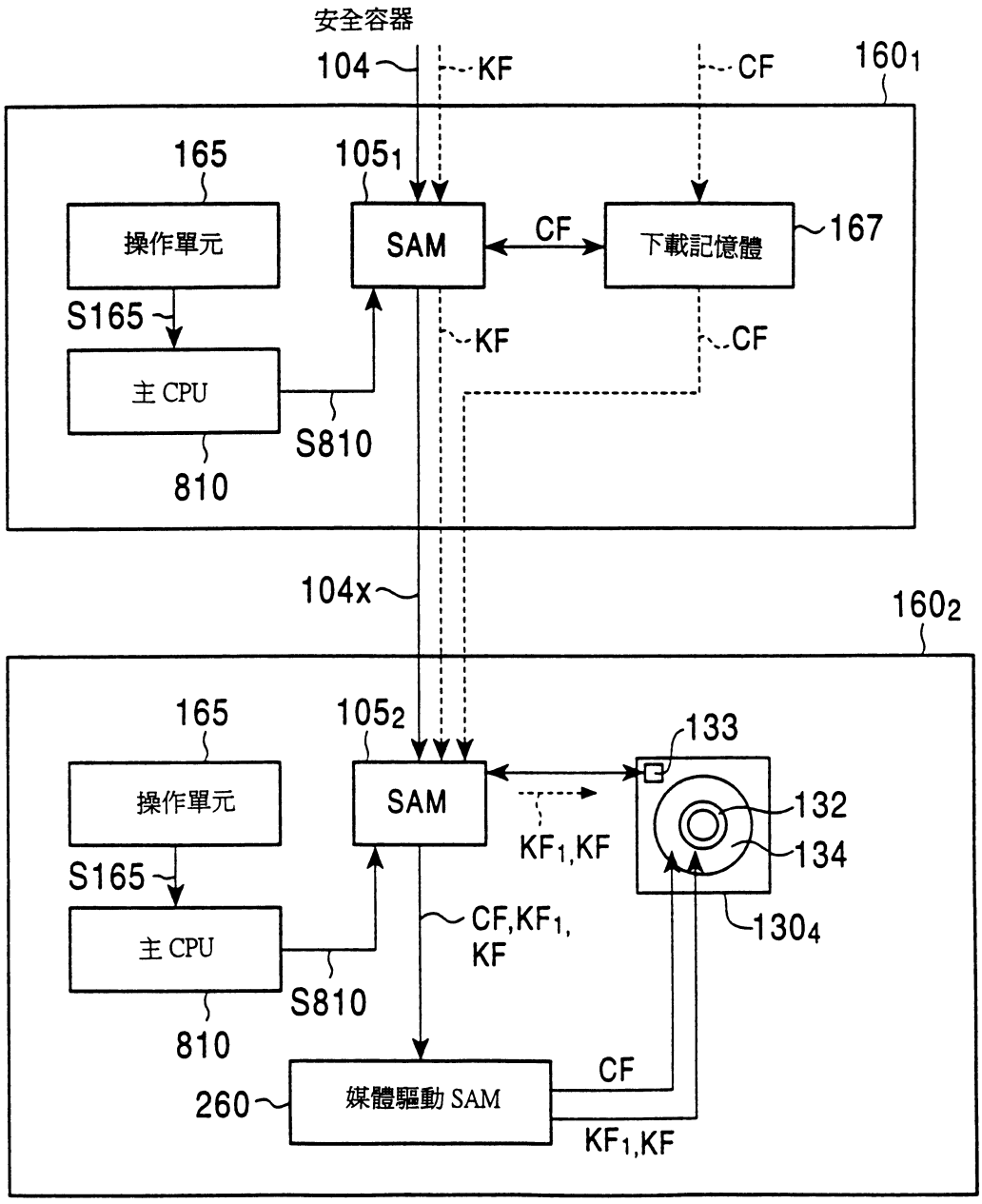

安全容器
104
KF
CF
160_1
165
105_1
操作單元
SAM
CF
下載記憶體
167
S165
KF
CF
主 CPU
S810
810
104x
160_2
165
105_2
133
操作單元
SAM
132
KF_1,KF
S165
134
CF,KF_1,
KF
130_4
主 CPU
S810
810
CF
260
媒體驅動 SAM
KF_1,KF

圖 4 2

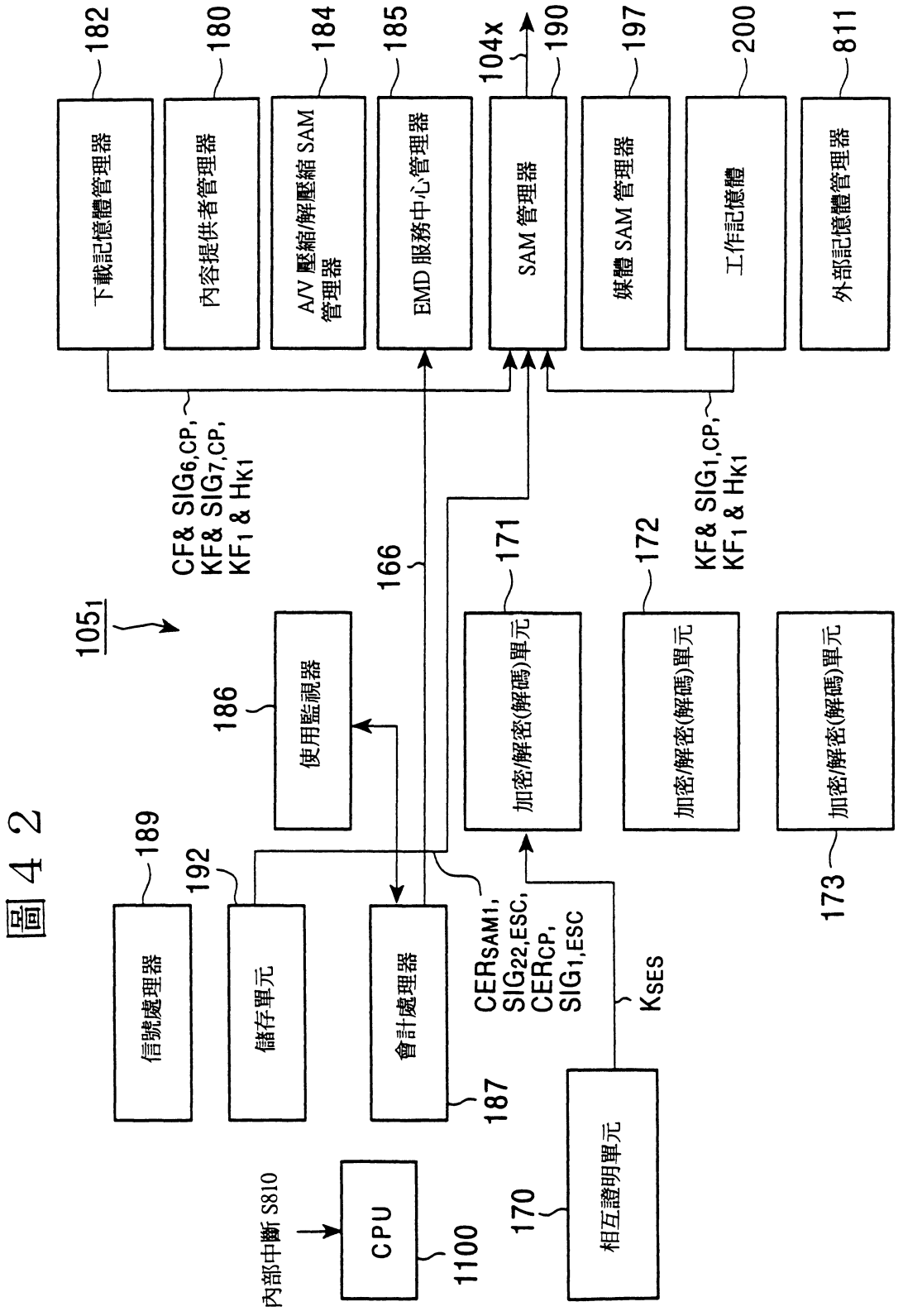

182
下載記憶體管理器
180
內容提供者管理器
184
A/V 壓縮/解壓縮 SAM 管理器
185
EMD 服務中心管理器
104x
190
SAM 管理器
197
媒體 SAM 管理器
200
工作記憶體
811
外部記憶體管理器
CF& SIG6,CP,
KF& SIG7,CP,
KF1 & HK1
KF& SIG1,CP,
KF1 & HK1
1051
166
186
使用監視器
171
加密/解密(解碼)單元
172
加密/解密(解碼)單元
加密/解密(解碼)單元
173
189
信號處理器
192
儲存單元
會計處理器
187
CERSAM1,
SIG22,ESC,
CERCP,
SIG1,ESC
KSES
內部中斷 S810
CPU
1100
170
相互證明單元

圖 4 3

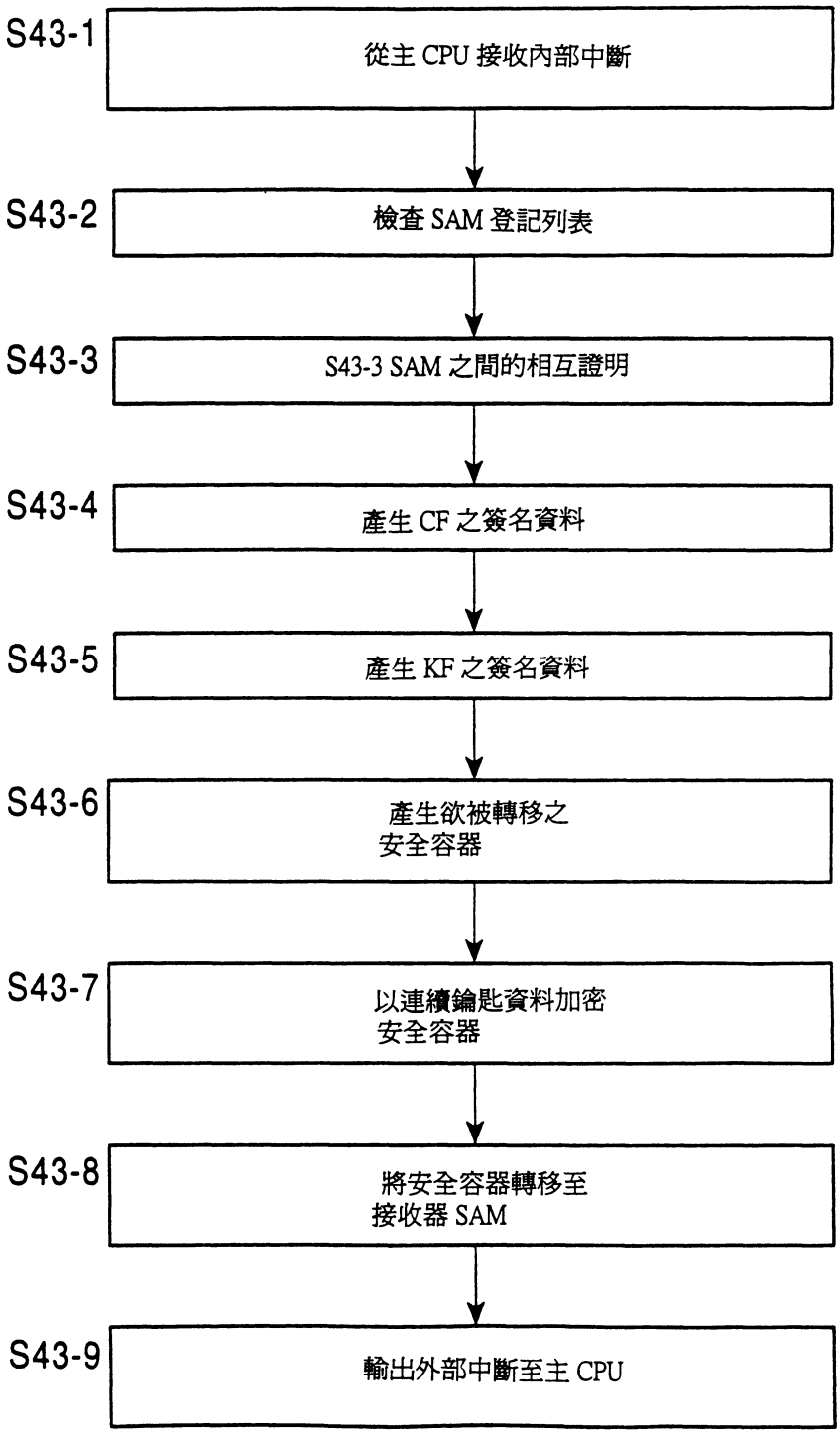

S43-1
從主 CPU 接收內部中斷
S43-2
檢查 SAM 登記列表
S43-3
S43-3 SAM 之間的相互證明
S43-4
產生 CF 之簽名資料
S43-5
產生 KF 之簽名資料
S43-6
產生欲被轉移之
安全容器
S43-7
以連續鑰匙資料加密
安全容器
S43-8
將安全容器轉移至
接收器 SAM
S43-9
輸出外部中斷至主 CPU

圖４４Ａ

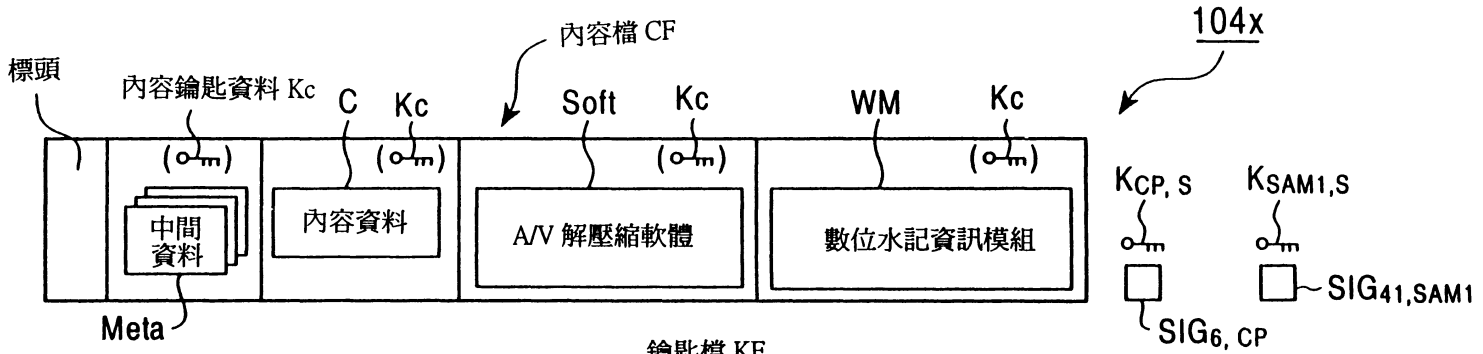


圖４４Ｂ

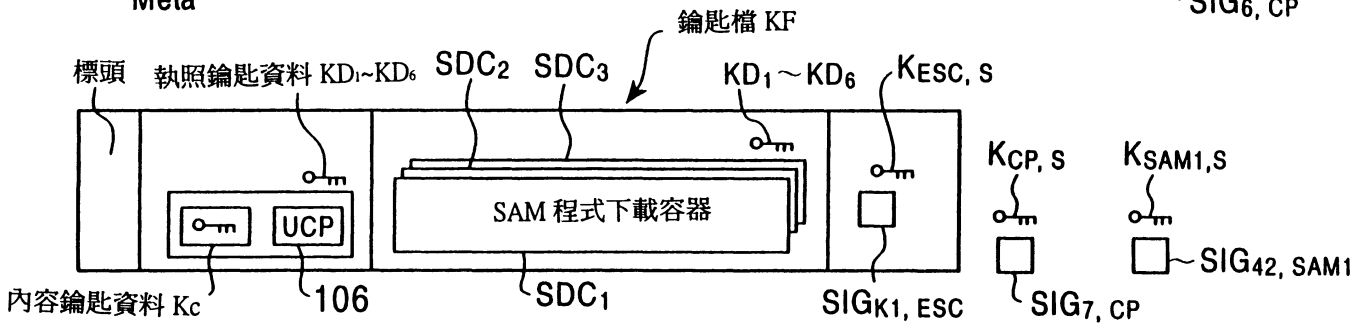


圖４４Ｃ

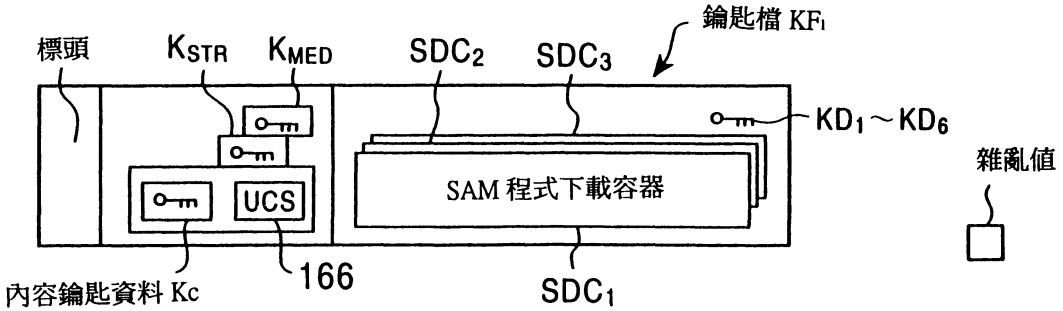


圖４４Ｄ

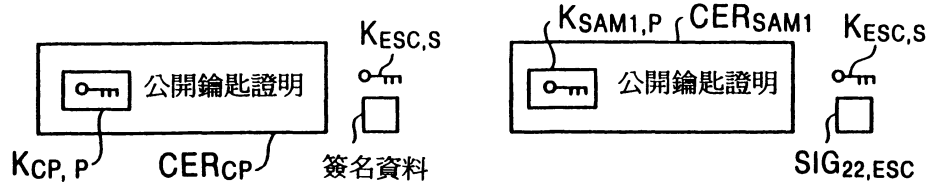


圖 4 5

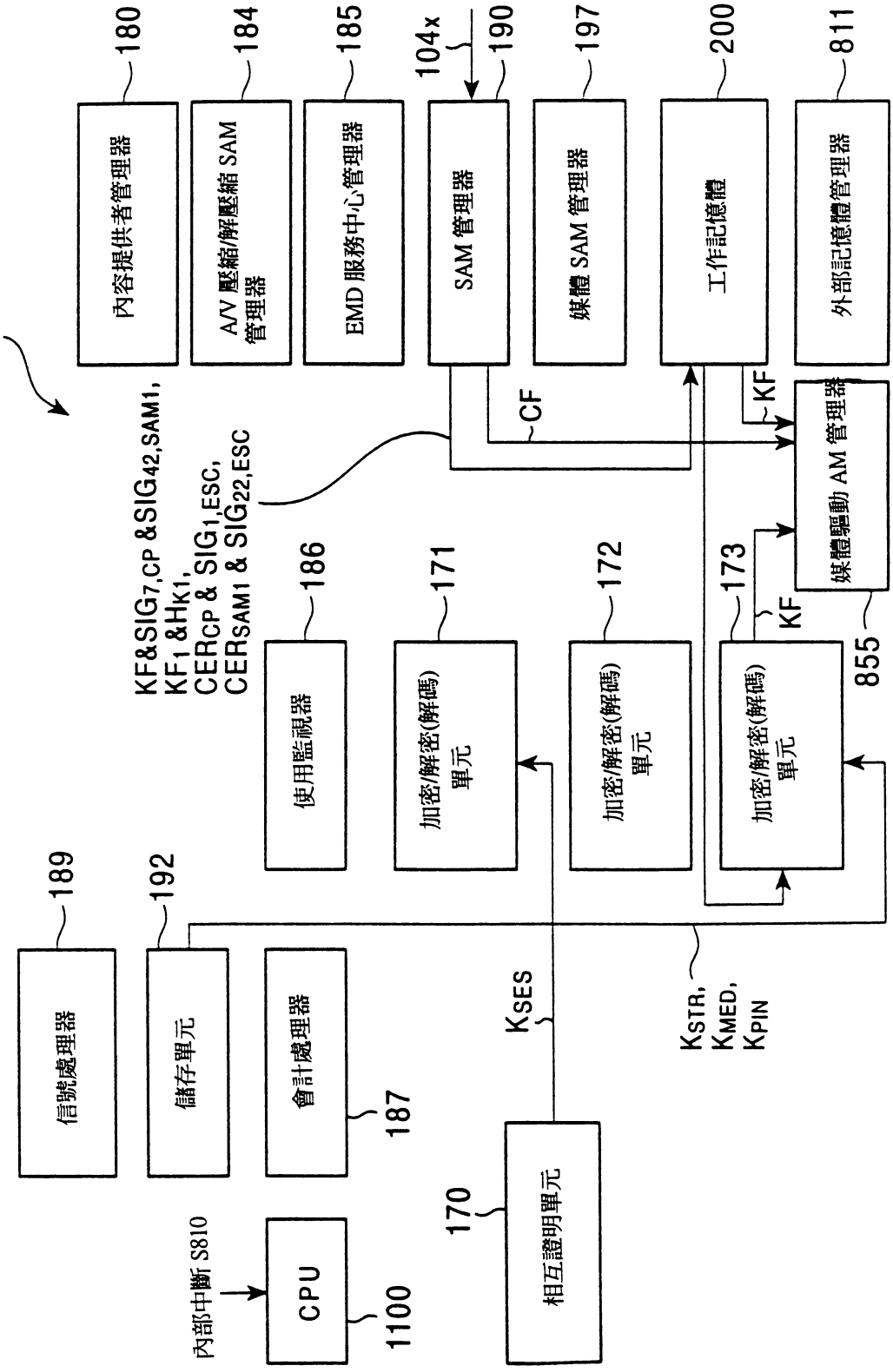

105_2
內容提供者管理器 180
A/V 壓縮/解壓縮 SAM 管理器 184
EMD 服務中心管理器 185
104x
SAM 管理器 190
媒體 SAM 管理器 197
工作記憶體 200
外部記憶體管理器 811
KF&SIG7,CP &SIG42,SAM1,
KF1 &HK1,
CERCP & SIG1,ESC,
CERSAM1 & SIG22,ESC
CF
KF
媒體驅動 AM 管理器
855
使用監視器 186
加密/解密(解碼)單元 171
加密/解密(解碼)單元 172
加密/解密(解碼)單元 173
KF
信號處理器 189
儲存單元 192
會計處理器 187
KSES
KSTR,
KMED,
KPIN
內部中斷 S810
CPU 1100
相互證明單元 170

圖 4 6

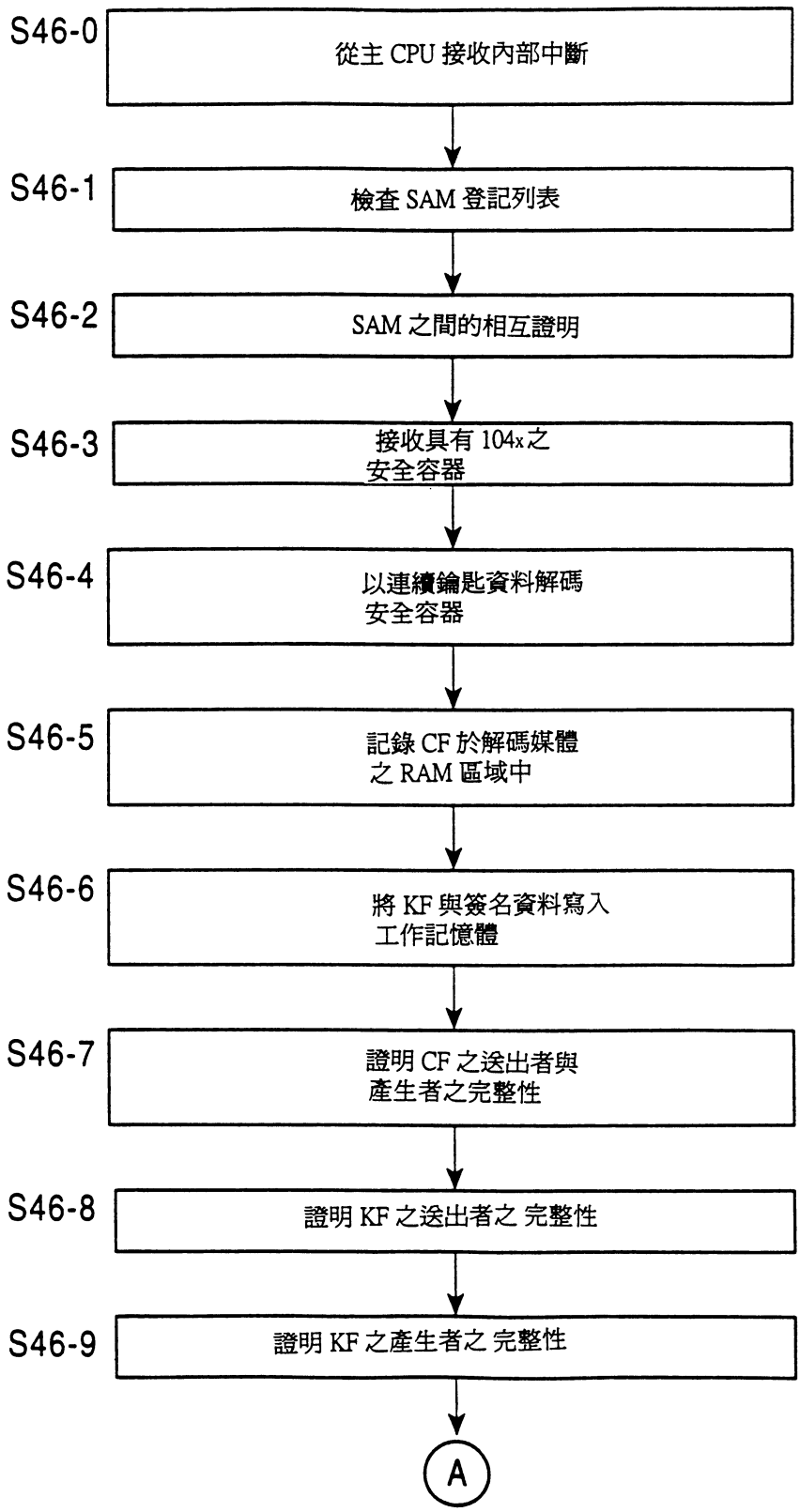

S46-0
從主 CPU 接收內部中斷
S46-1
檢查 SAM 登記列表
S46-2
SAM 之間的相互證明
S46-3
接收具有 104x 之
安全容器
S46-4
以連續鑰匙資料解碼
安全容器
S46-5
記錄 CF 於解碼媒體
之 RAM 區域中
S46-6
將 KF 與簽名資料寫入
工作記憶體
S46-7
證明 CF 之送出者與
產生者之完整性
S46-8
證明 KF 之送出者之 完整性
S46-9
證明 KF 之產生者之 完整性
A

圖 4 7

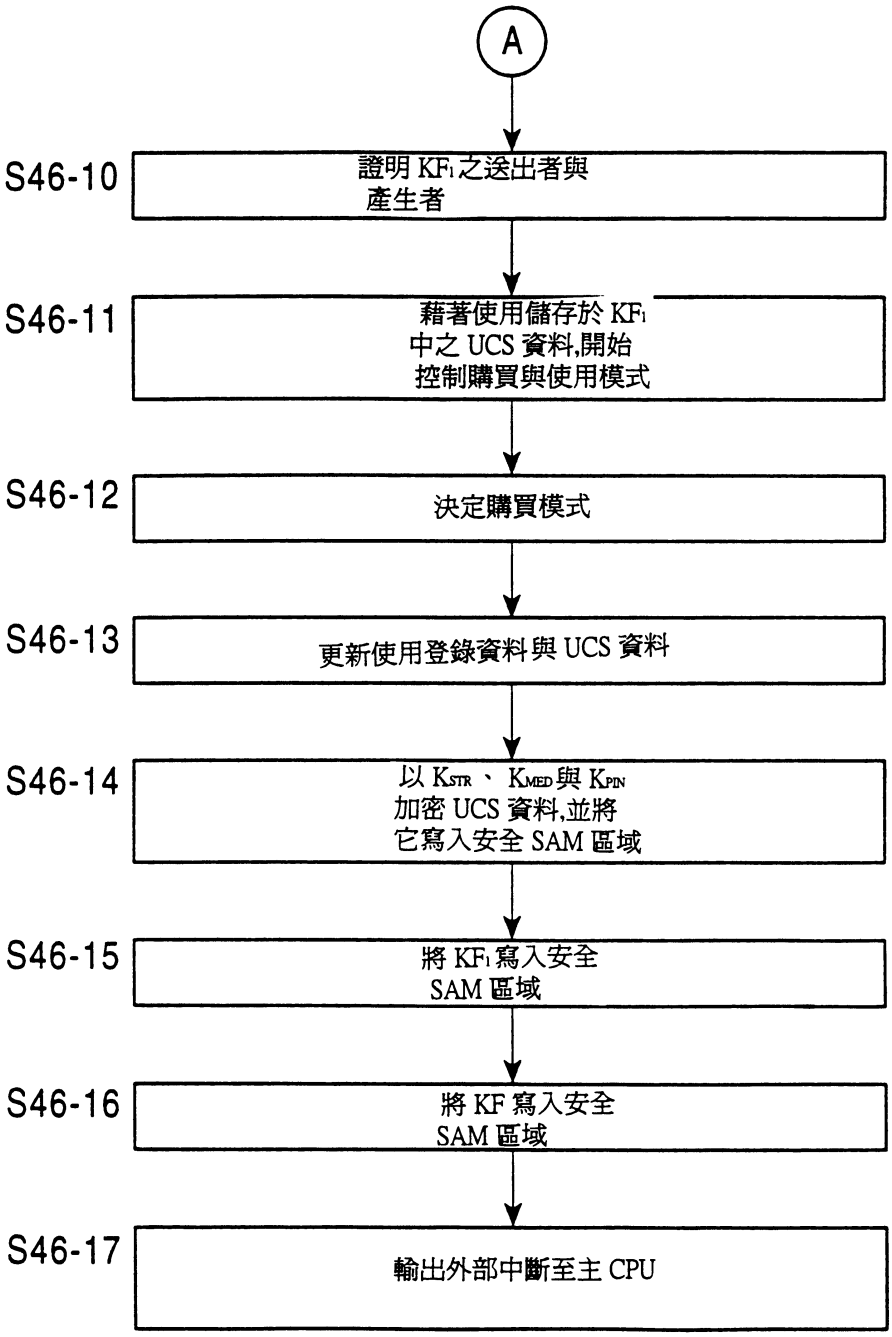

A
S46-10
證明 KF_i 之送出者與產生者
S46-11
藉著使用儲存於 KF_i 中之 UCS 資料,開始控制購買與使用模式
S46-12
決定購買模式
S46-13
更新使用登錄資料與 UCS 資料
S46-14
以 K_{STR}、K_{MED} 與 K_{PIN} 加密 UCS 資料,並將它寫入安全 SAM 區域
S46-15
將 KF_i 寫入安全 SAM 區域
S46-16
將 KF 寫入安全 SAM 區域
S46-17
輸出外部中斷至主 CPU

圖 4 8

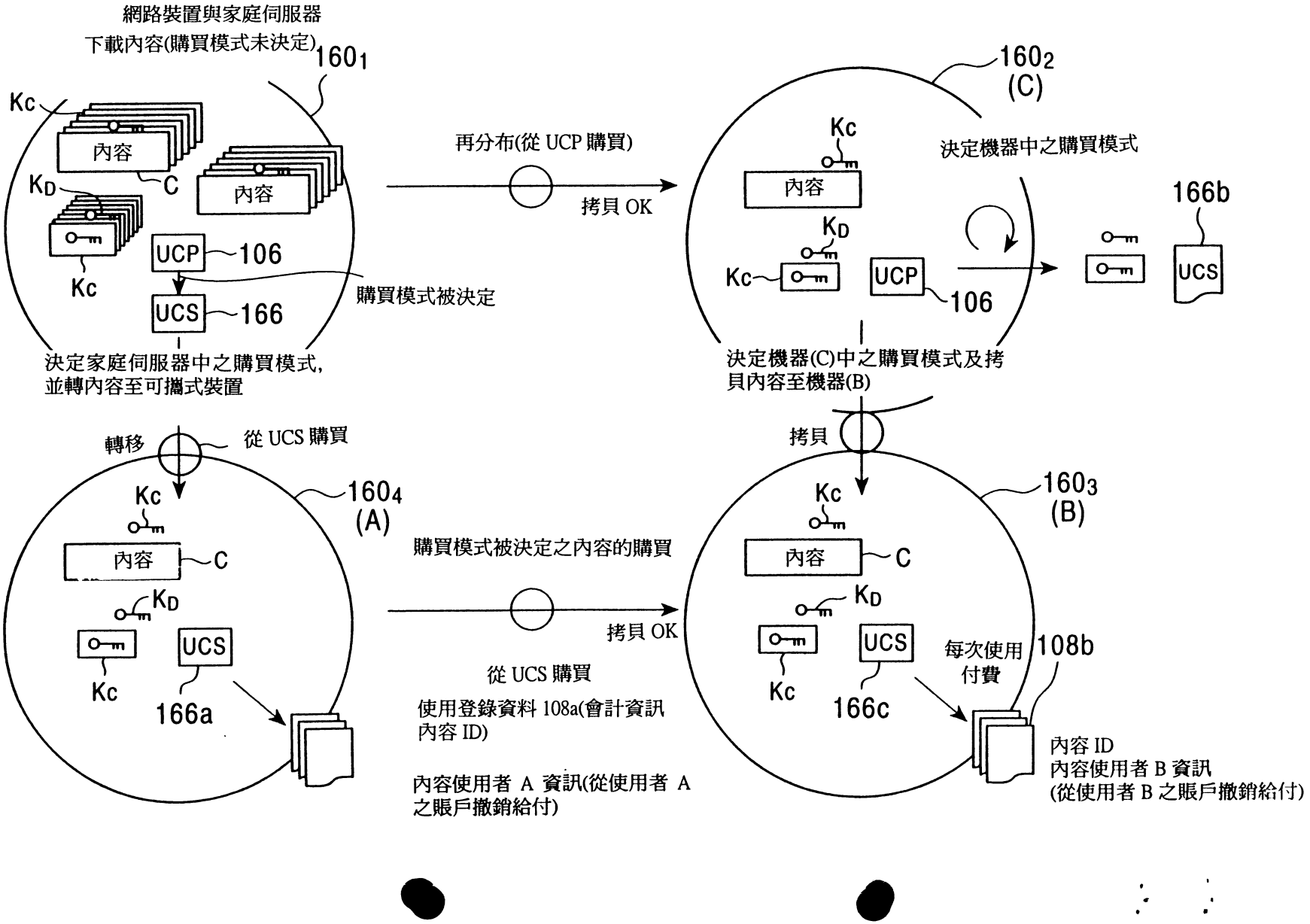
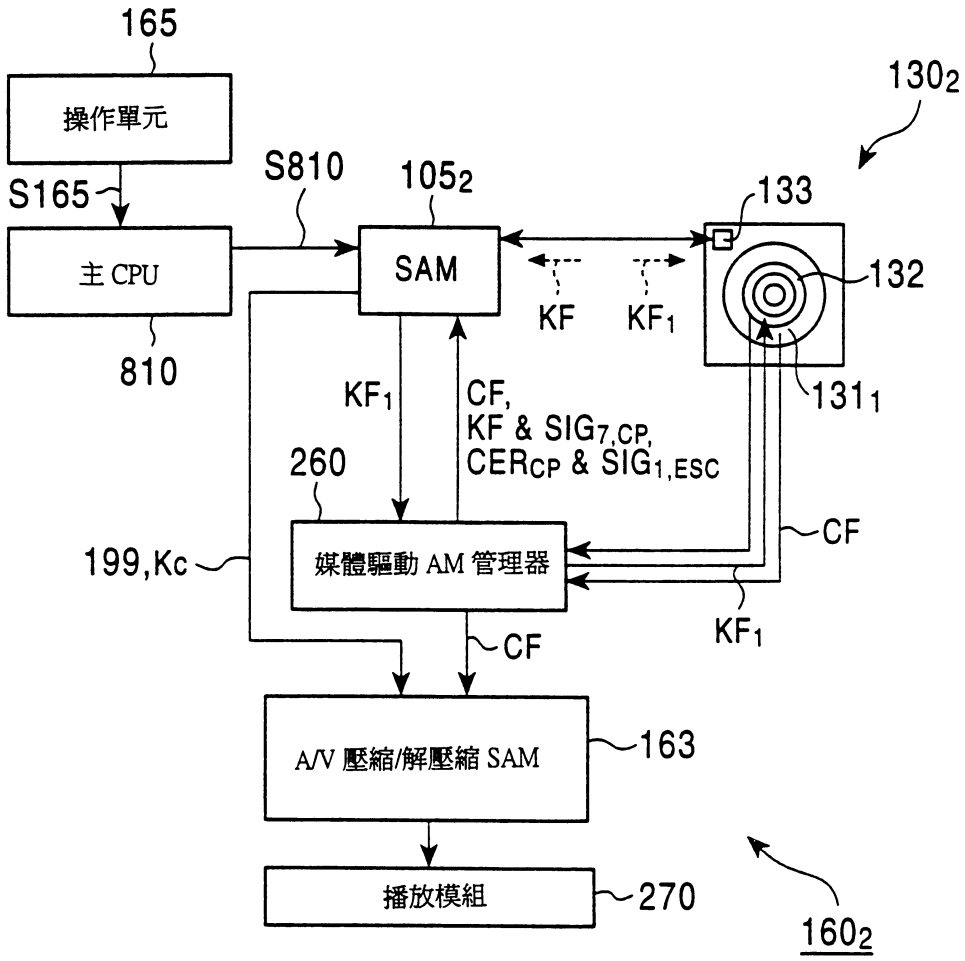

網路裝置與家庭伺服器
下載內容(購買模式未決定)
160_1
Kc
內容
C
K_D
內容
Kc
UCP
106
UCS
166
購買模式被決定
決定家庭伺服器中之購買模式，
並轉內容至可攜式裝置
再分布(從 UCP 購買)
拷貝 OK
160_2
(C)
Kc
內容
K_D
Kc
UCP
106
決定機器中之購買模式
166b
UCS
決定機器(C)中之購買模式及拷
貝內容至機器(B)
轉移
從 UCS 購買
160_4
(A)
Kc
內容
C
K_D
Kc
UCS
166a
購買模式被決定之內容的購買
拷貝 OK
從 UCS 購買
使用登錄資料 108a(會計資訊
內容 ID)
內容使用者 A 資訊(從使用者 A
之賬戶撤銷給付)
拷貝
160_3
(B)
Kc
內容
C
K_D
Kc
UCS
166c
每次使用
付費
108b
內容 ID
內容使用者 B 資訊
(從使用者 B 之賬戶撤銷給付)

圖 4 9


165
操作單元
S165
主 CPU
810
S810
105₂
SAM
KF
KF₁
130₂
133
132
131₁
KF₁
CF,
KF & SIG7,CP,
CERCP & SIG1,ESC
260
199,Kc
媒體驅動 AM 管理器
CF
KF₁
CF
A/V 壓縮/解壓縮 SAM
163
播放模組
270
160₂

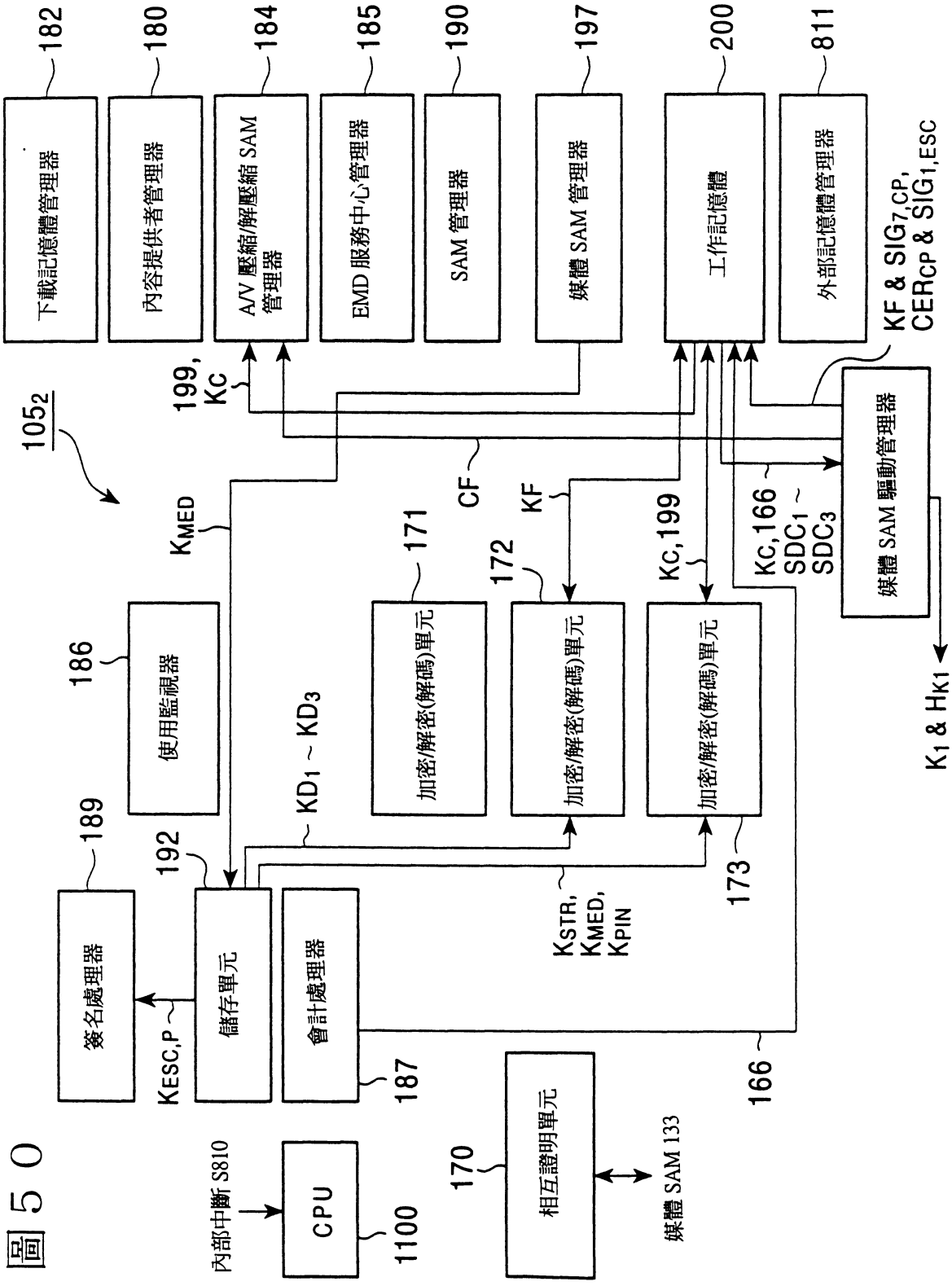

下載記憶體管理器
182
內容提供者管理器
180
A/V 壓縮/解壓縮 SAM 管理器
184
EMD 服務中心管理器
185
SAM 管理器
190
媒體 SAM 管理器
197
工作記憶體
200
外部記憶體管理器
811
KF & SIG7,CP, CERCP & SIG1,ESC
1052
199, KC
KMED
CF
KF
KC,199
KC,166 SDC1 ~ SDC3
媒體 SAM 驅動管理器
K1 & HK1
使用監視器
186
KD1 ~ KD3
加密/解密(解碼)單元
171
加密/解密(解碼)單元
172
加密/解密(解碼)單元
173
簽名處理器
189
KESC,P
儲存單元
192
會計處理器
187
KSTR, KMED, KPIN
166
內部中斷 S810
CPU
1100
相互證明單元
170
媒體 SAM 133

圖 5 0

圖 5 1

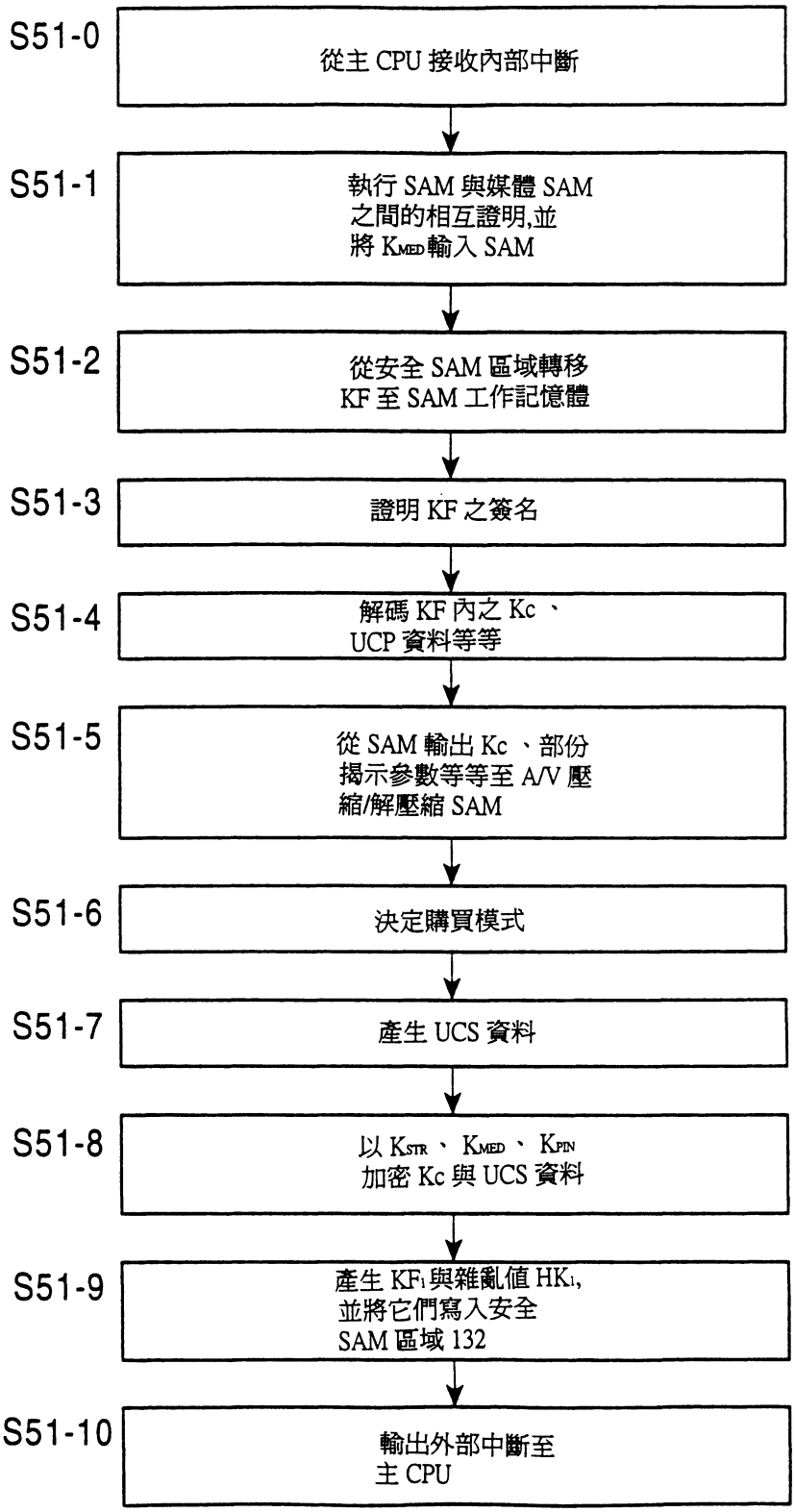

S51-0
從主 CPU 接收內部中斷
S51-1
執行 SAM 與媒體 SAM 之間的相互證明,並將 K_{MED} 輸入 SAM
S51-2
從安全 SAM 區域轉移 KF 至 SAM 工作記憶體
S51-3
證明 KF 之簽名
S51-4
解碼 KF 內之 Kc 、UCP 資料等等
S51-5
從 SAM 輸出 Kc 、部份揭示參數等等至 A/V 壓縮/解壓縮 SAM
S51-6
決定購買模式
S51-7
產生 UCS 資料
S51-8
以 K_{STR} 、 K_{MED} 、 K_{PIN} 加密 Kc 與 UCS 資料
S51-9
產生 KF_1 與雜亂值 HK_1, 並將它們寫入安全 SAM 區域 132
S51-10
輸出外部中斷至主 CPU

圖 5 2

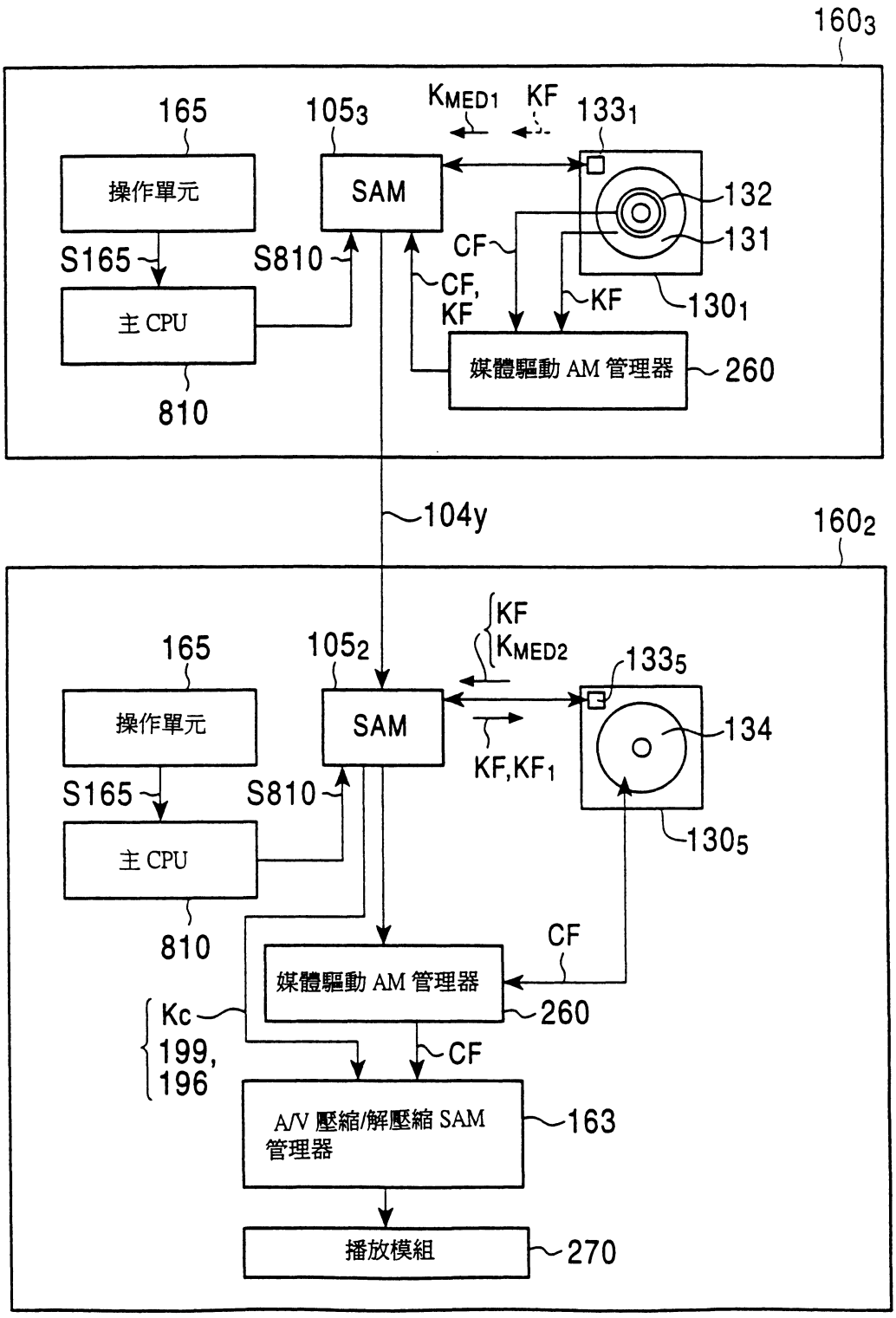

160₃
165
105₃
KMED1
KF
133₁
操作單元
SAM
132
131
S165
S810
CF
主 CPU
CF,
KF
KF
130₁
媒體驅動 AM 管理器
260
810
104y
160₂
165
105₂
KF
KMED2
133₅
操作單元
SAM
134
KF,KF₁
S165
S810
主 CPU
130₅
810
CF
媒體驅動 AM 管理器
260
Kc
199,
196
CF
A/V 壓縮/解壓縮 SAM
管理器
163
播放模組
270

圖 5 3

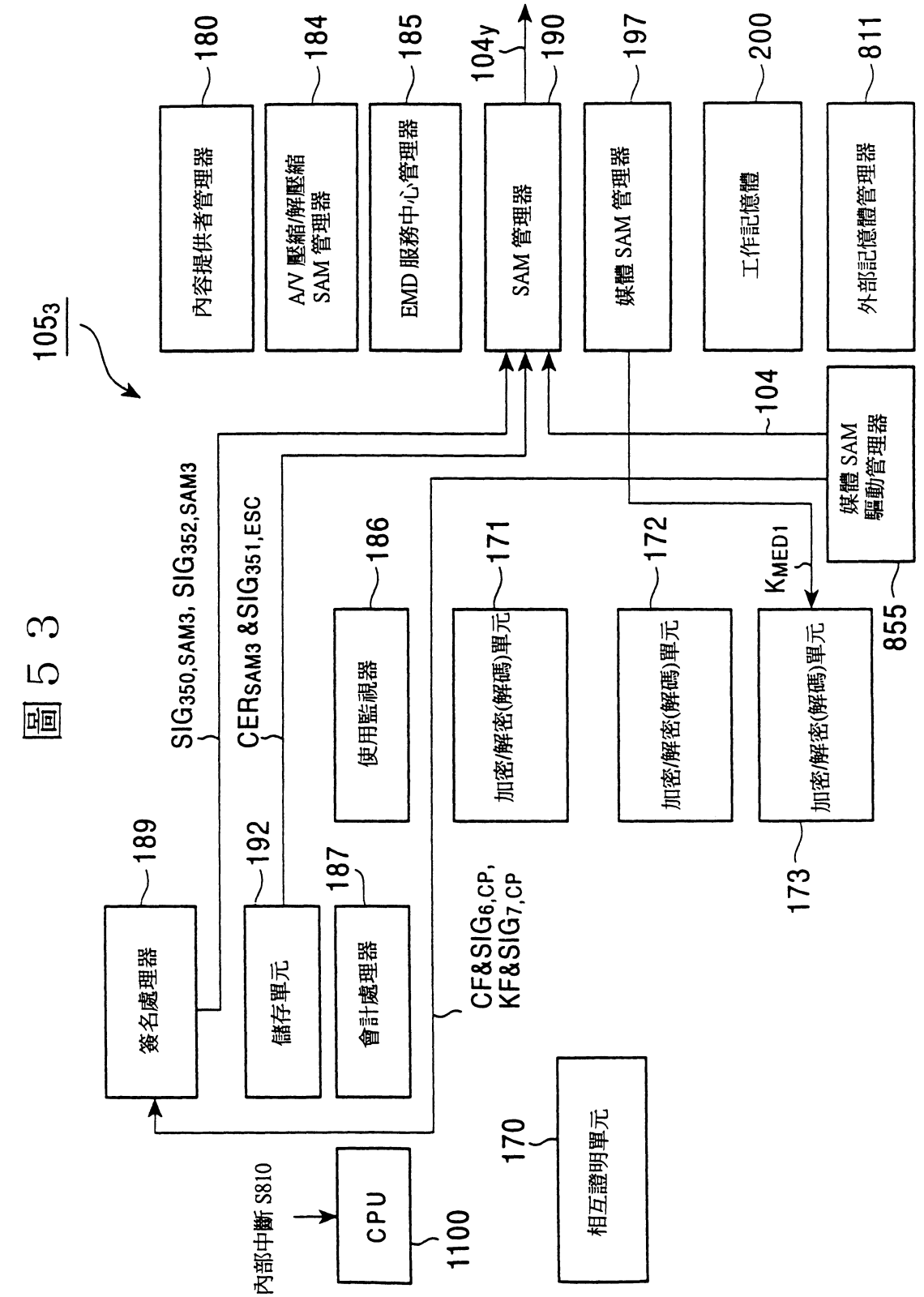

105_3
內容提供者管理器
180
A/V 壓縮/解壓縮 SAM 管理器
184
EMD 服務中心管理器
185
SAM 管理器
104_y
190
媒體 SAM 管理器
197
工作記憶體
200
外部記憶體管理器
811
媒體 SAM 驅動管理器
855
104
$SIG_{350,SAM3}$, $SIG_{352,SAM3}$
CER_{SAM3} &$SIG_{351,ESC}$
$CF\&SIG_{6,CP}$,
$KF\&SIG_{7,CP}$
K_{MED1}
使用監視器
186
加密/解密(解碼)單元
171
加密/解密(解碼)單元
172
加密/解密(解碼)單元
173
簽名處理器
189
儲存單元
192
會計處理器
187
相互證明單元
170
CPU
1100
內部中斷 S810

圖５４Ａ

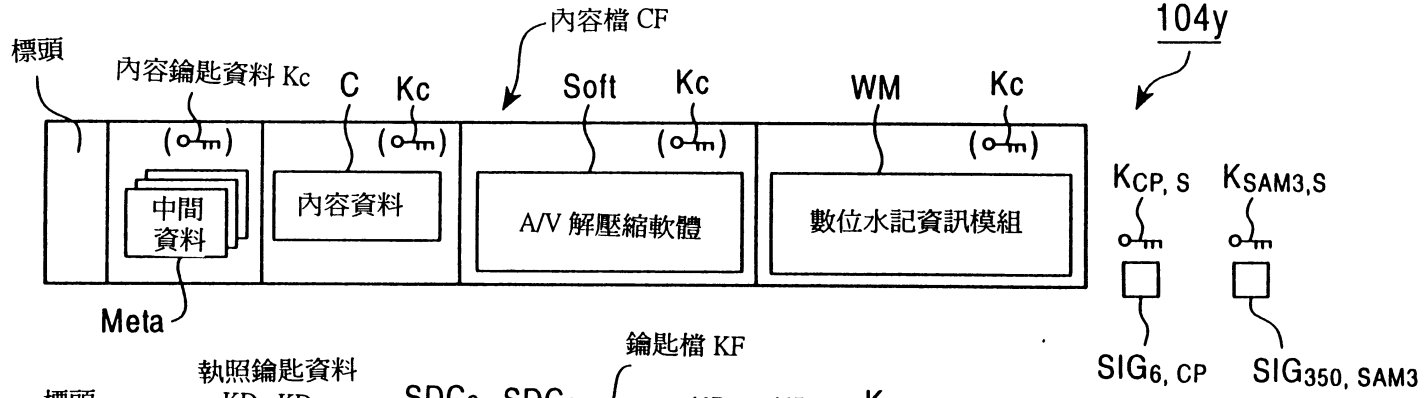


圖５４Ｂ

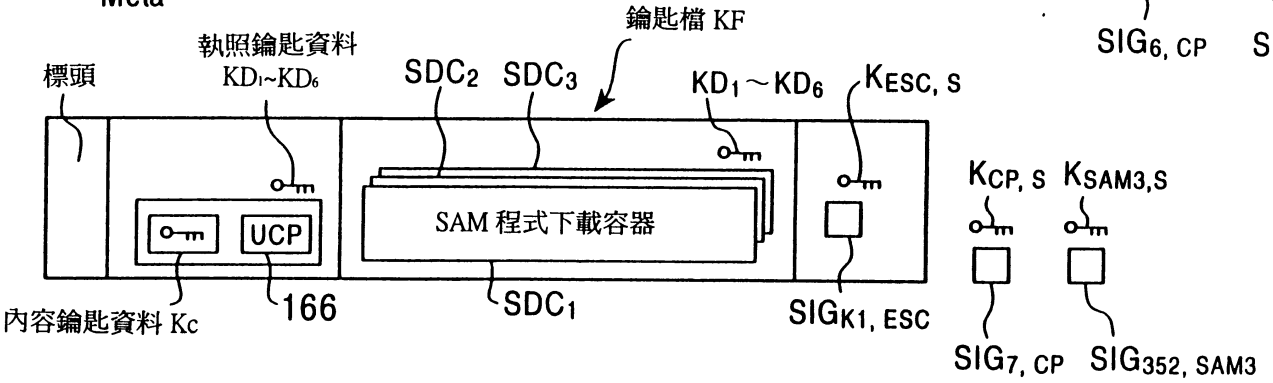


圖５４Ｃ

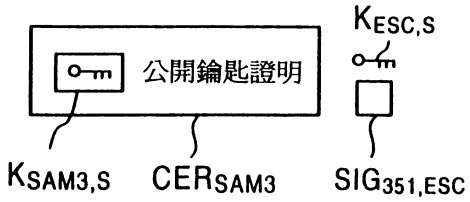


圖５４Ｄ

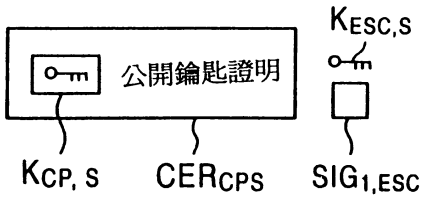


圖 5 5

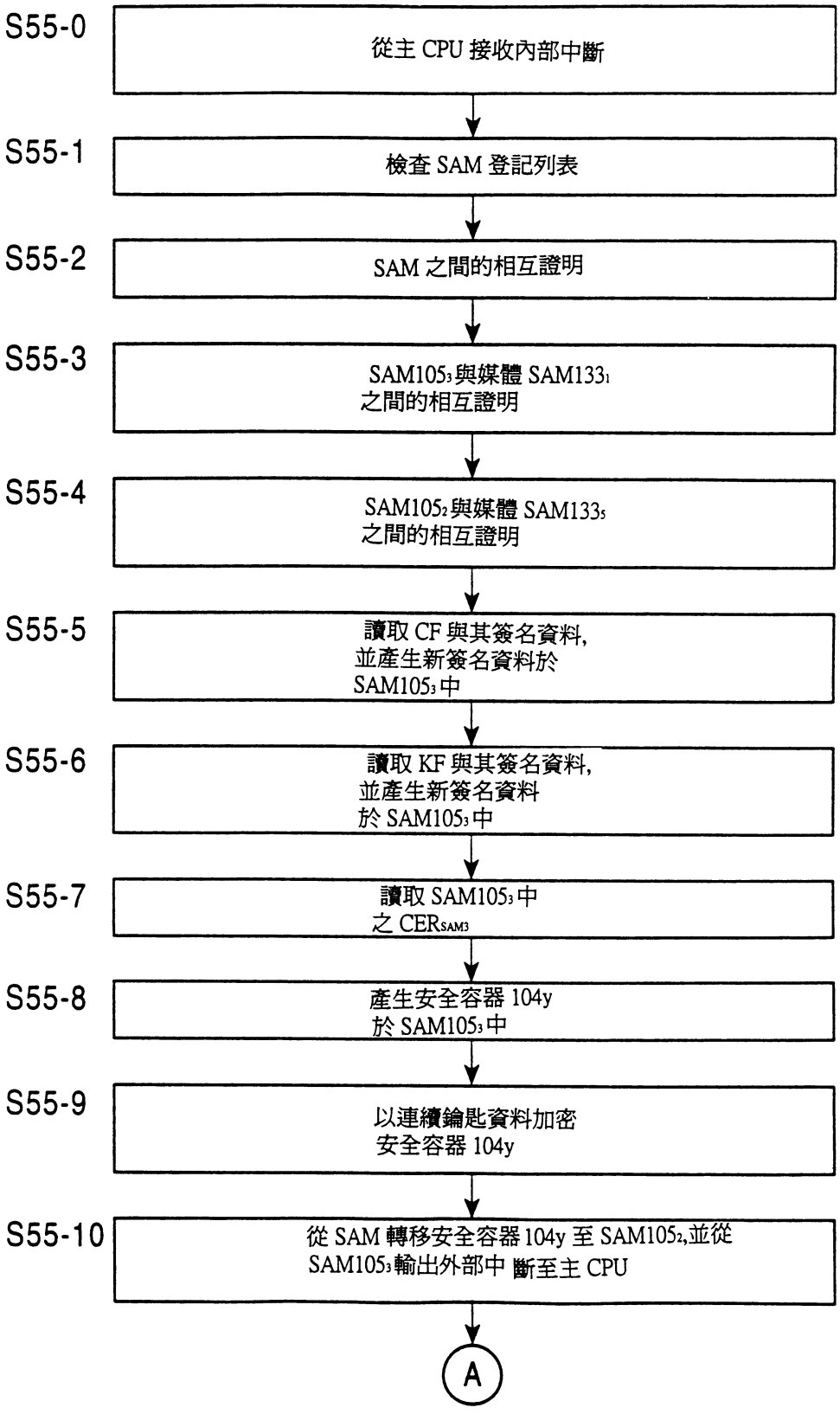

S55-0
從主 CPU 接收內部中斷
S55-1
檢查 SAM 登記列表
S55-2
SAM 之間的相互證明
S55-3
SAM105$_3$與媒體 SAM133$_1$
之間的相互證明
S55-4
SAM105$_2$與媒體 SAM133$_5$
之間的相互證明
S55-5
讀取 CF 與其簽名資料,
並產生新簽名資料於
SAM105$_3$中
S55-6
讀取 KF 與其簽名資料,
並產生新簽名資料
於 SAM105$_3$中
S55-7
讀取 SAM105$_3$中
之 CER$_{SAM3}$
S55-8
產生安全容器 104y
於 SAM105$_3$中
S55-9
以連續鑰匙資料加密
安全容器 104y
S55-10
從 SAM 轉移安全容器 104y 至 SAM105$_2$,並從
SAM105$_3$輸出外部中斷至主 CPU
A

圖 5 6

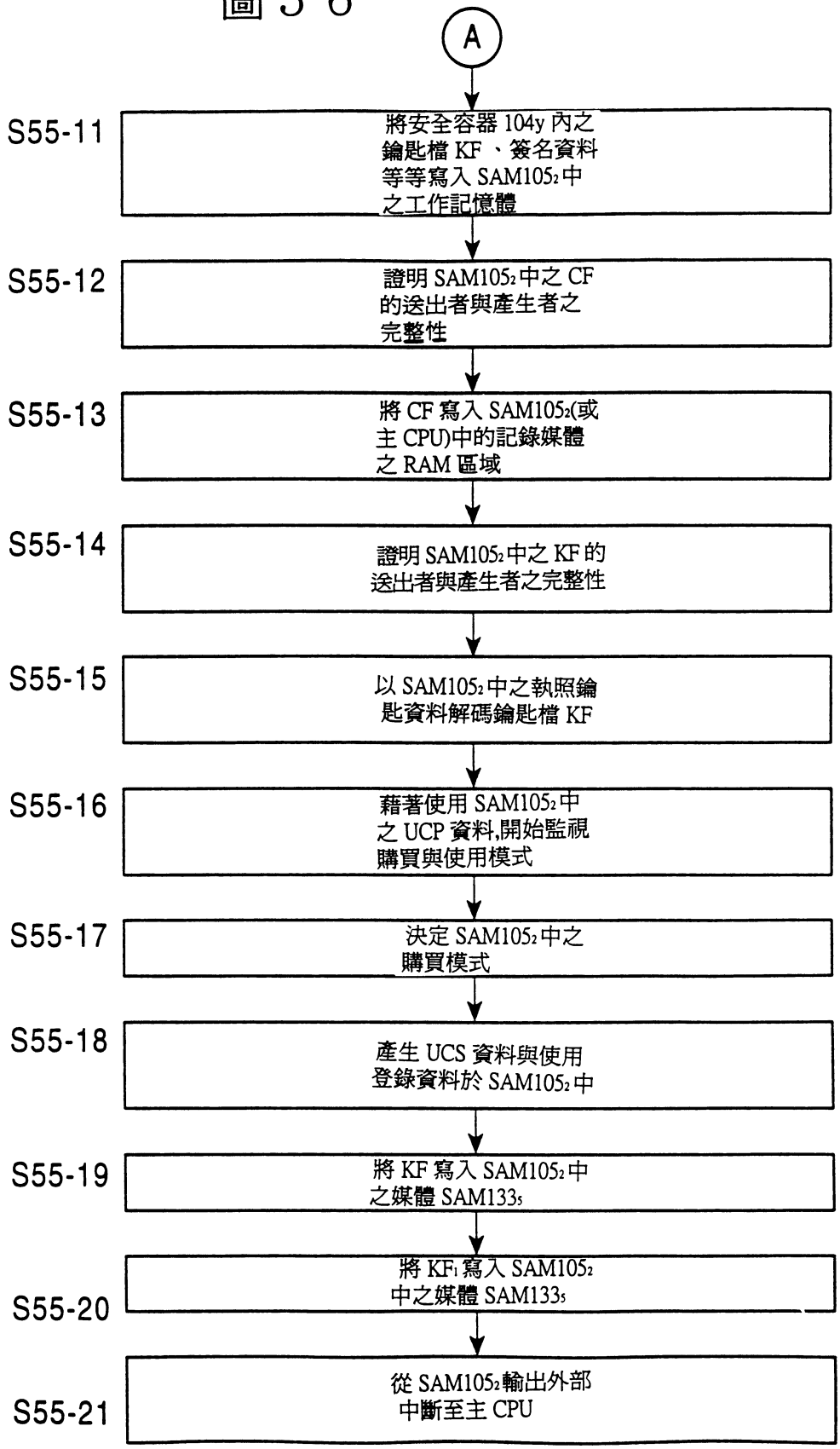

A
S55-11
將安全容器 104y 內之鑰匙檔 KF 、簽名資料等等寫入 SAM105₂ 中之工作記憶體
S55-12
證明 SAM105₂ 中之 CF 的送出者與產生者之完整性
S55-13
將 CF 寫入 SAM105₂(或主 CPU)中的記錄媒體之 RAM 區域
S55-14
證明 SAM105₂ 中之 KF 的送出者與產生者之完整性
S55-15
以 SAM105₂ 中之執照鑰匙資料解碼鑰匙檔 KF
S55-16
藉著使用 SAM105₂ 中之 UCP 資料,開始監視購買與使用模式
S55-17
決定 SAM105₂ 中之購買模式
S55-18
產生 UCS 資料與使用登錄資料於 SAM105₂ 中
S55-19
將 KF 寫入 SAM105₂ 中之媒體 SAM133₅
S55-20
將 KF₁ 寫入 SAM105₂ 中之媒體 SAM133₅
S55-21
從 SAM105₂ 輸出外部中斷至主 CPU

圖 5 7

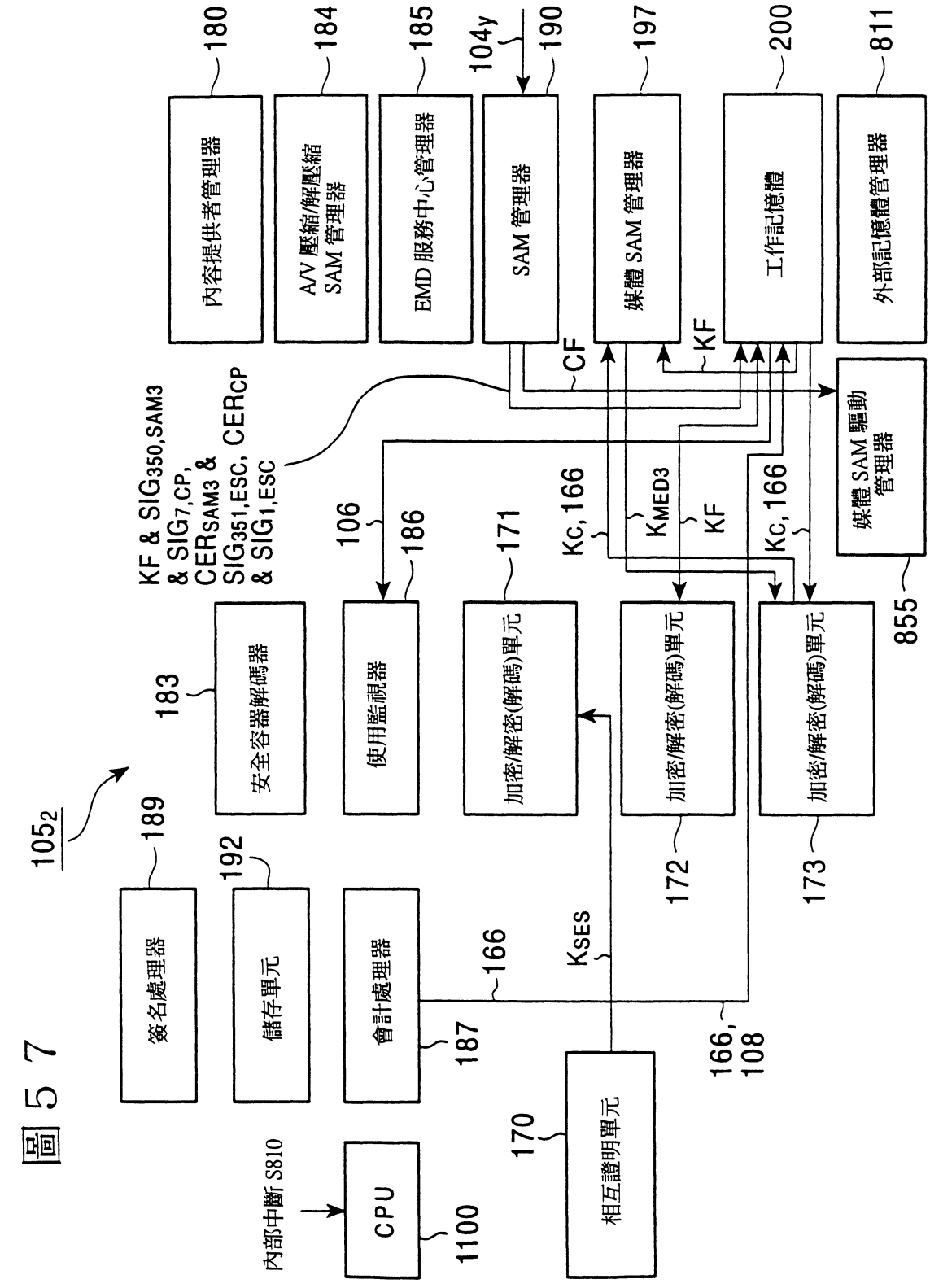

105_2
189
簽名處理器
192
儲存單元
會計處理器
CPU
1100
內部中斷 S810
187
166
K_{SES}
170
相互證明單元
183
安全容器解碼器
106
使用監視器
186
171
加密/解密(解碼)單元
K_C, 166
172
加密/解密(解碼)單元
K_{MED3}
KF
K_C, 166
173
加密/解密(解碼)單元
166, 108
KF & $SIG_{350,SAM3}$ & $SIG_{7,CP}$, CER_{SAM3} & $SIG_{351,ESC}$, CER_{CP} & $SIG_{1,ESC}$
180
內容提供者管理器
184
A/V 壓縮/解壓縮 SAM 管理器
185
EMD 服務中心管理器
104y
190
SAM 管理器
CF
197
媒體 SAM 管理器
KF
200
工作記憶體
811
外部記憶體管理器
媒體 SAM 驅動管理器
855

圖 5 8

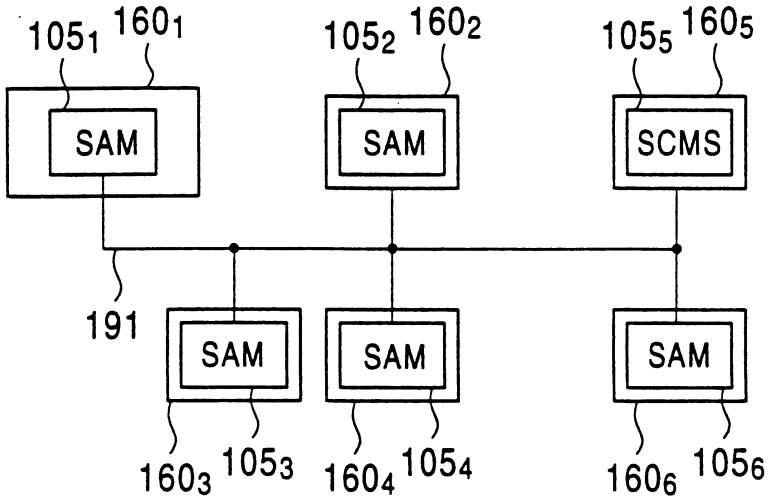

105_1 160_1
105_2 160_2
105_5 160_5
SAM
SAM
SCMS
191
SAM
SAM
SAM
160_3 105_3
160_4 105_4
160_6 105_6

圖 5 9

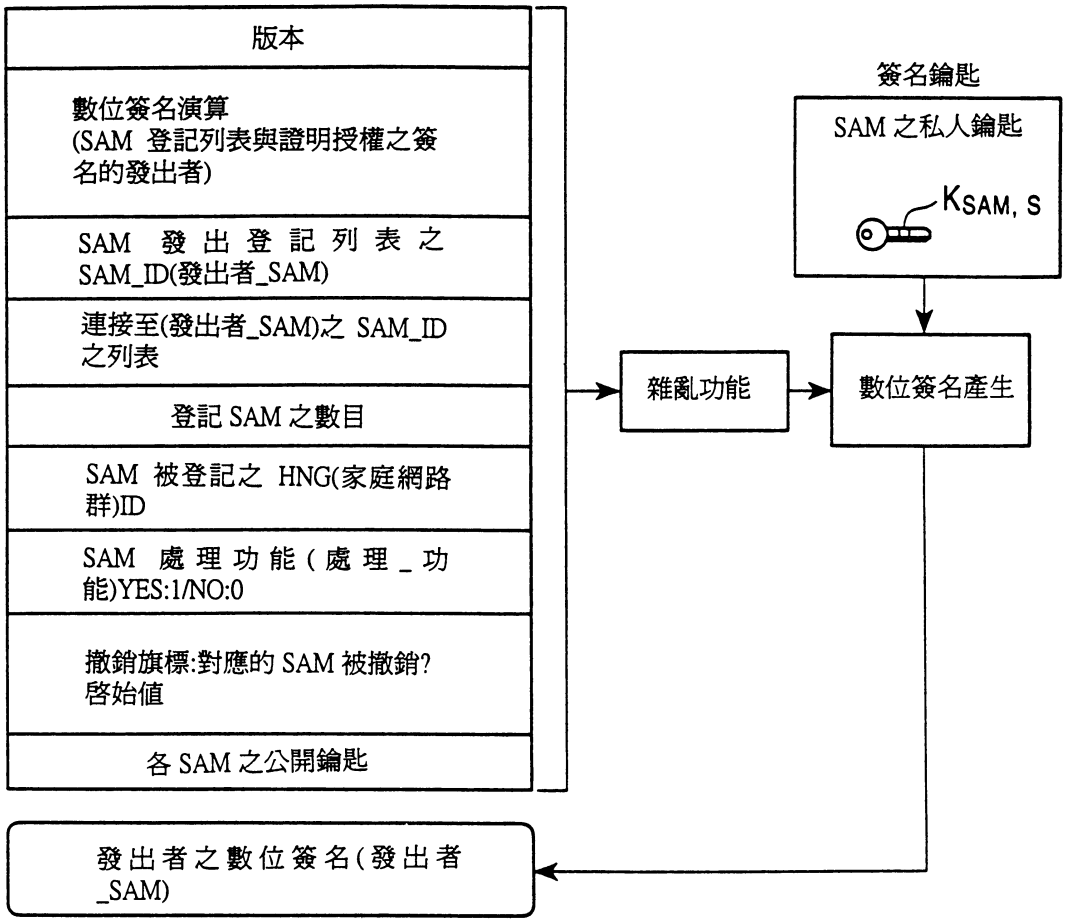

版本
數位簽名演算
(SAM 登記列表與證明授權之簽名的發出者)
SAM 發出登記列表之 SAM_ID(發出者_SAM)
連接至(發出者_SAM)之 SAM_ID 之列表
登記 SAM 之數目
SAM 被登記之 HNG(家庭網路群)ID
SAM 處理功能(處理_功能)YES:1/NO:0
撤銷旗標:對應的 SAM 被撤銷?啓始值
各 SAM 之公開鑰匙
發出者之數位簽名(發出者_SAM)
雜亂功能
簽名鑰匙
SAM 之私人鑰匙
KSAM, S
數位簽名產生

圖 6 0

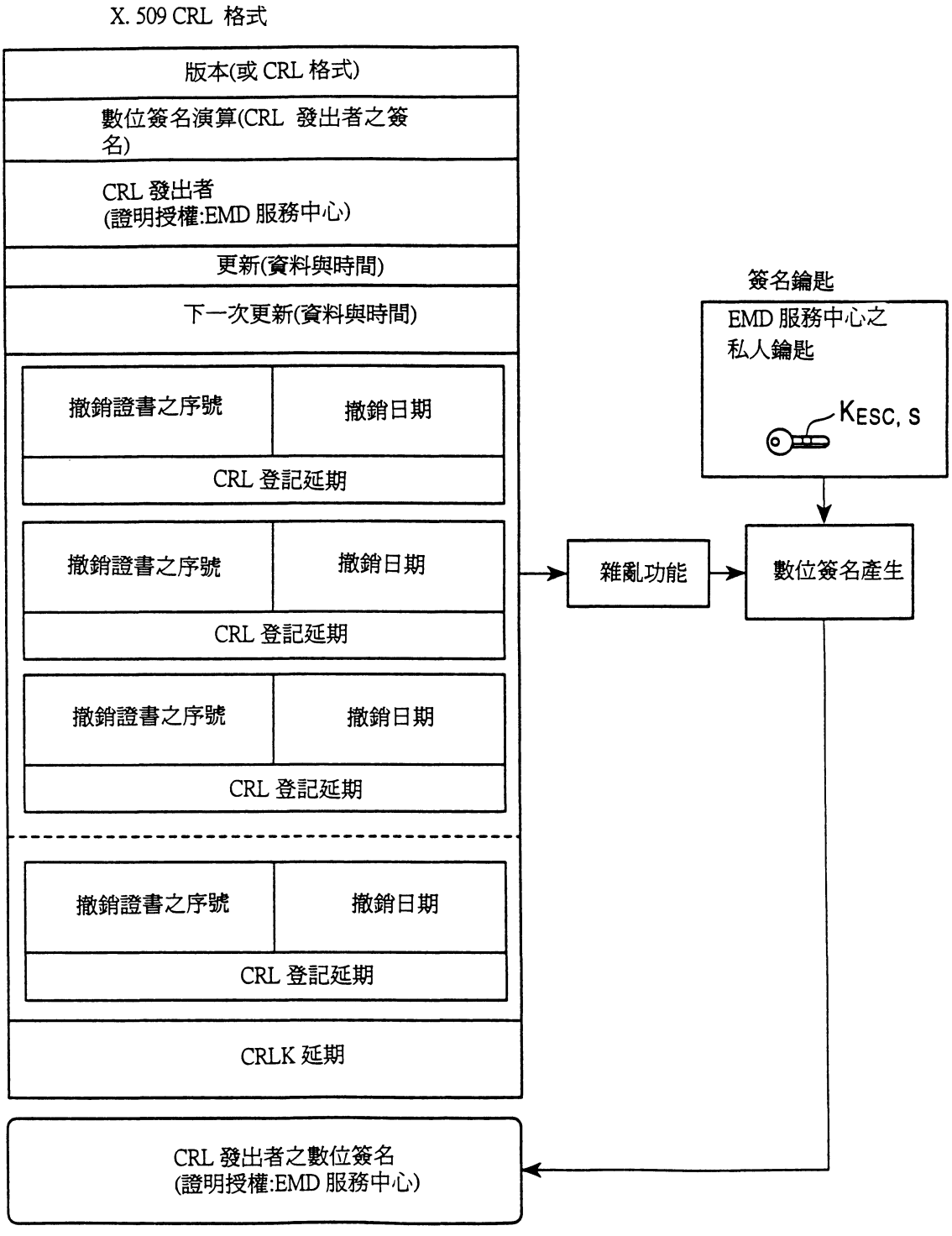

X. 509 CRL 格式
版本(或 CRL 格式)
數位簽名演算(CRL 發出者之簽名)
CRL 發出者
(證明授權:EMD 服務中心)
更新(資料與時間)
下一次更新(資料與時間)
撤銷證書之序號
撤銷日期
CRL 登記延期
撤銷證書之序號
撤銷日期
CRL 登記延期
撤銷證書之序號
撤銷日期
CRL 登記延期
撤銷證書之序號
撤銷日期
CRL 登記延期
CRLK 延期
CRL 發出者之數位簽名
(證明授權:EMD 服務中心)
雜亂功能
簽名鑰匙
EMD 服務中心之
私人鑰匙
KESC, S
數位簽名產生

圖 6 1

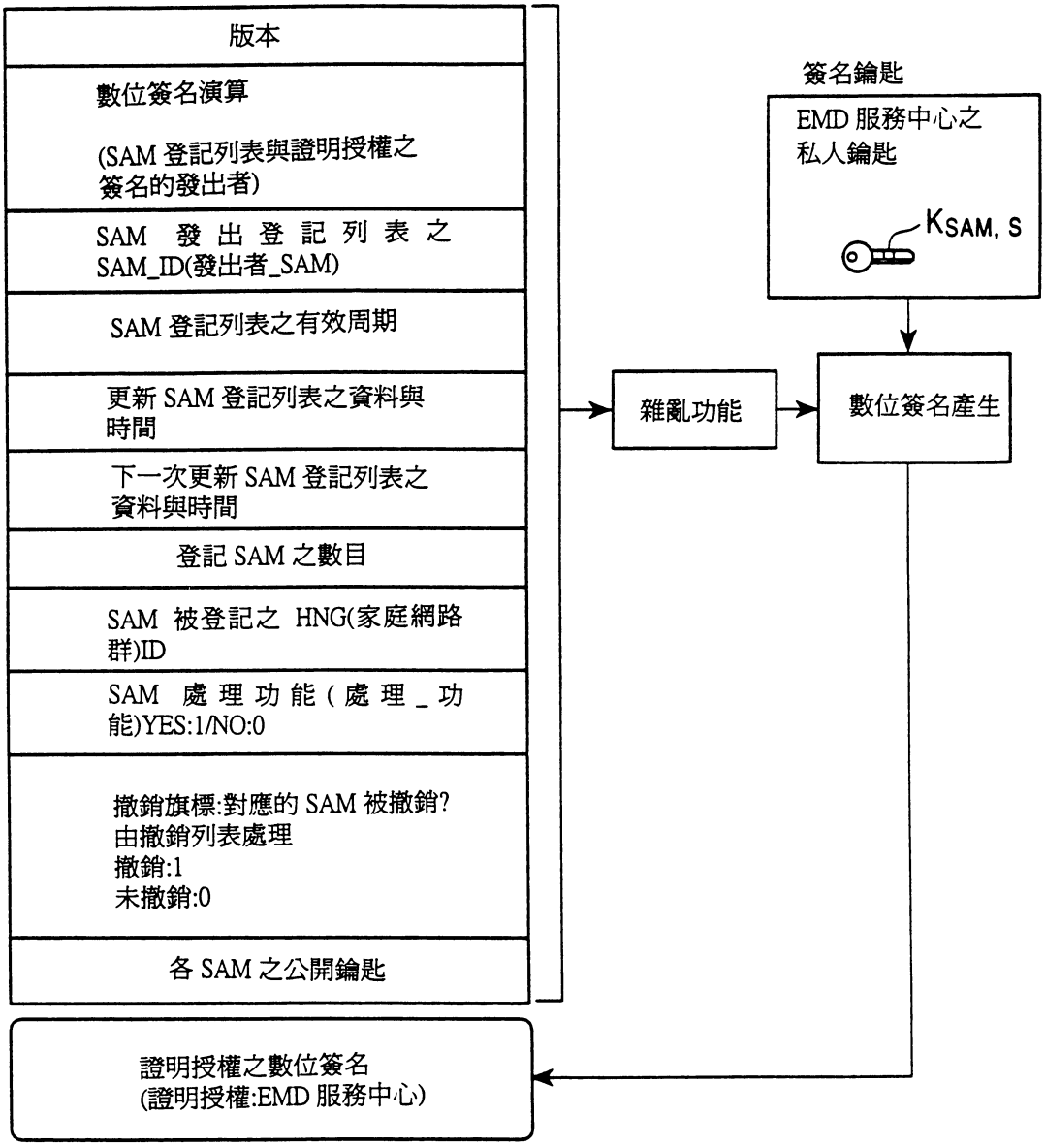

版本
數位簽名演算
(SAM 登記列表與證明授權之簽名的發出者)
SAM 發出登記列表之 SAM_ID(發出者_SAM)
SAM 登記列表之有效周期
更新 SAM 登記列表之資料與時間
下一次更新 SAM 登記列表之資料與時間
登記 SAM 之數目
SAM 被登記之 HNG(家庭網路群)ID
SAM 處理功能(處理_功能)YES:1/NO:0
撤銷旗標:對應的 SAM 被撤銷?
由撤銷列表處理
撤銷:1
未撤銷:0
各 SAM 之公開鑰匙
證明授權之數位簽名
(證明授權:EMD 服務中心)
雜亂功能
簽名鑰匙
EMD 服務中心之私人鑰匙
KSAM, S
數位簽名產生

圖 6 2

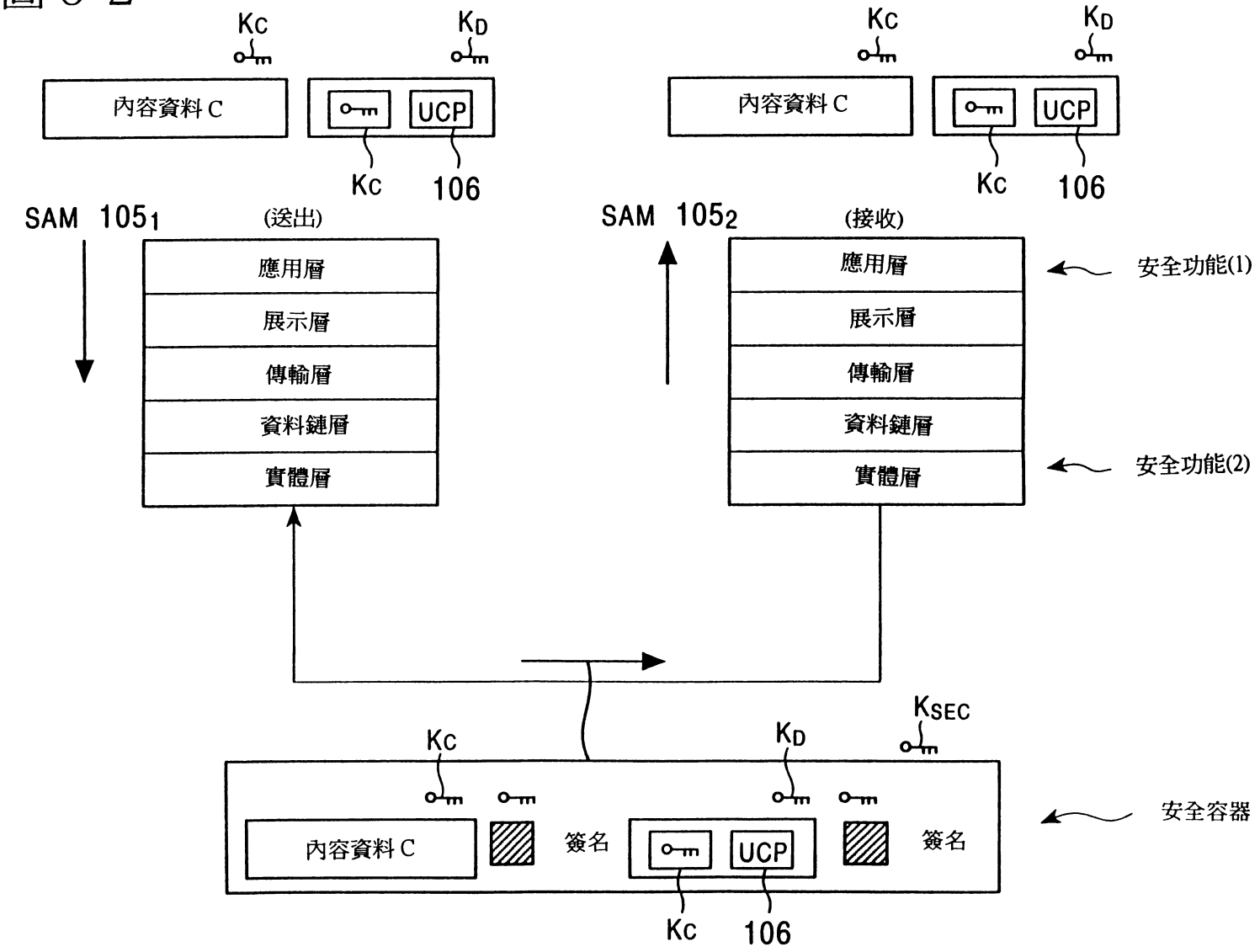

Kc
KD
內容資料 C
UCP
Kc
106
SAM 1051
(送出)
應用層
展示層
傳輸層
資料鏈層
實體層
SAM 1052
(接收)
安全功能(1)
安全功能(2)
KSEC
簽名
安全容器

圖 6 3

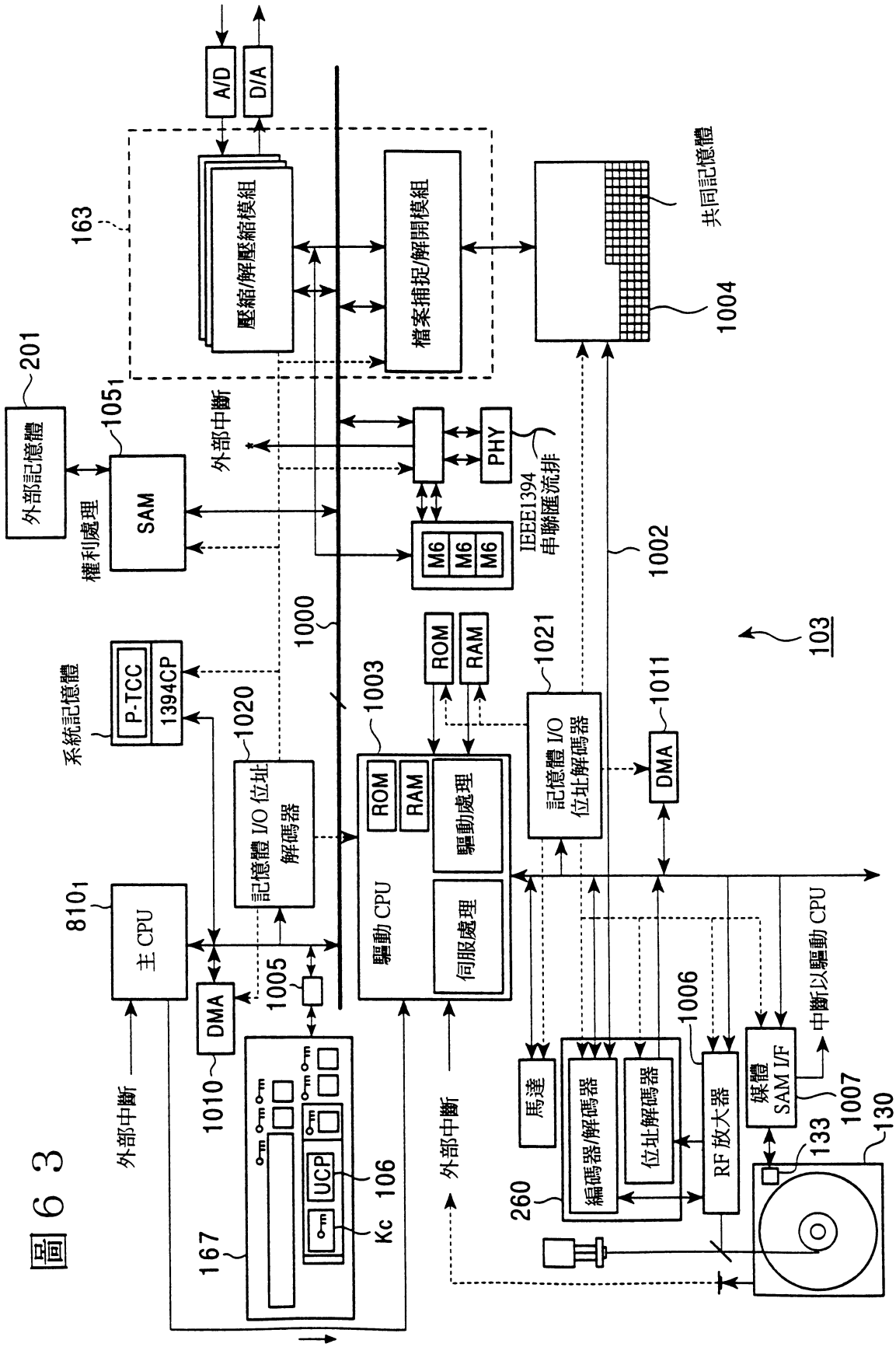

A/D
D/A
163
壓縮/解壓縮模組
檔案捕捉/解開模組
共同記憶體
1004
201
外部記憶體
105₁
SAM
權利處理
外部中斷
PHY
IEEE1394
串聯匯流排
M6
M6
M6
1002
1000
系統記憶體
P-TCC
1394CP
1020
記憶體 I/O 位址
解碼器
ROM
RAM
1003
ROM
RAM
驅動處理
伺服處理
驅動 CPU
1021
記憶體 I/O
位址解碼器
DMA
1011
103
810₁
主 CPU
DMA
1010
1005
外部中斷
UCP
Kc 106
167
外部中斷
馬達
260
編碼器/解碼器
位址解碼器
1006
RF 放大器
媒體
SAM I/F
1007
133
130
中斷以驅動 CPU

圖 6 4

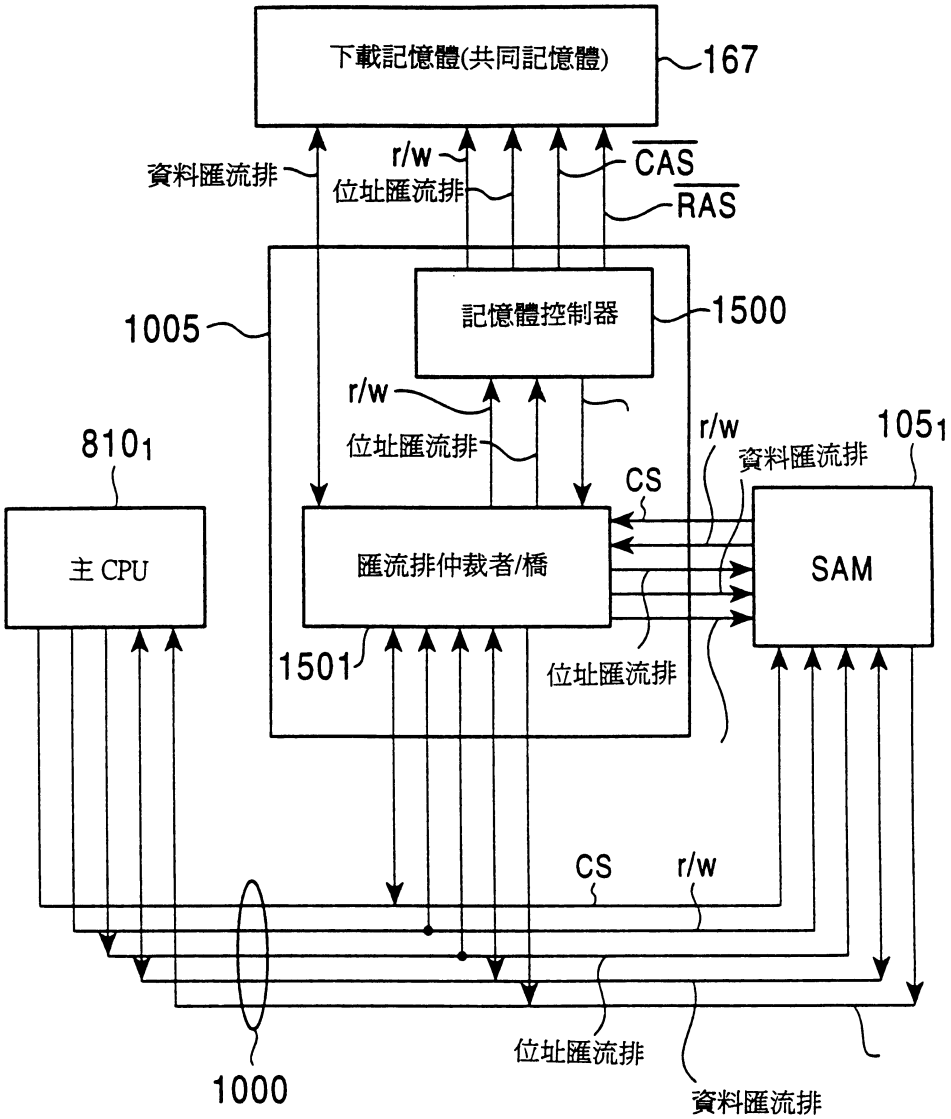

下載記憶體(共同記憶體)
167
資料匯流排
r/w
位址匯流排
CAS
RAS
1005
記憶體控制器
1500
r/w
位址匯流排
810₁
r/w
資料匯流排
105₁
CS
主 CPU
匯流排仲裁者/橋
SAM
1501
位址匯流排
CS
r/w
位址匯流排
資料匯流排
1000

圖 6 5

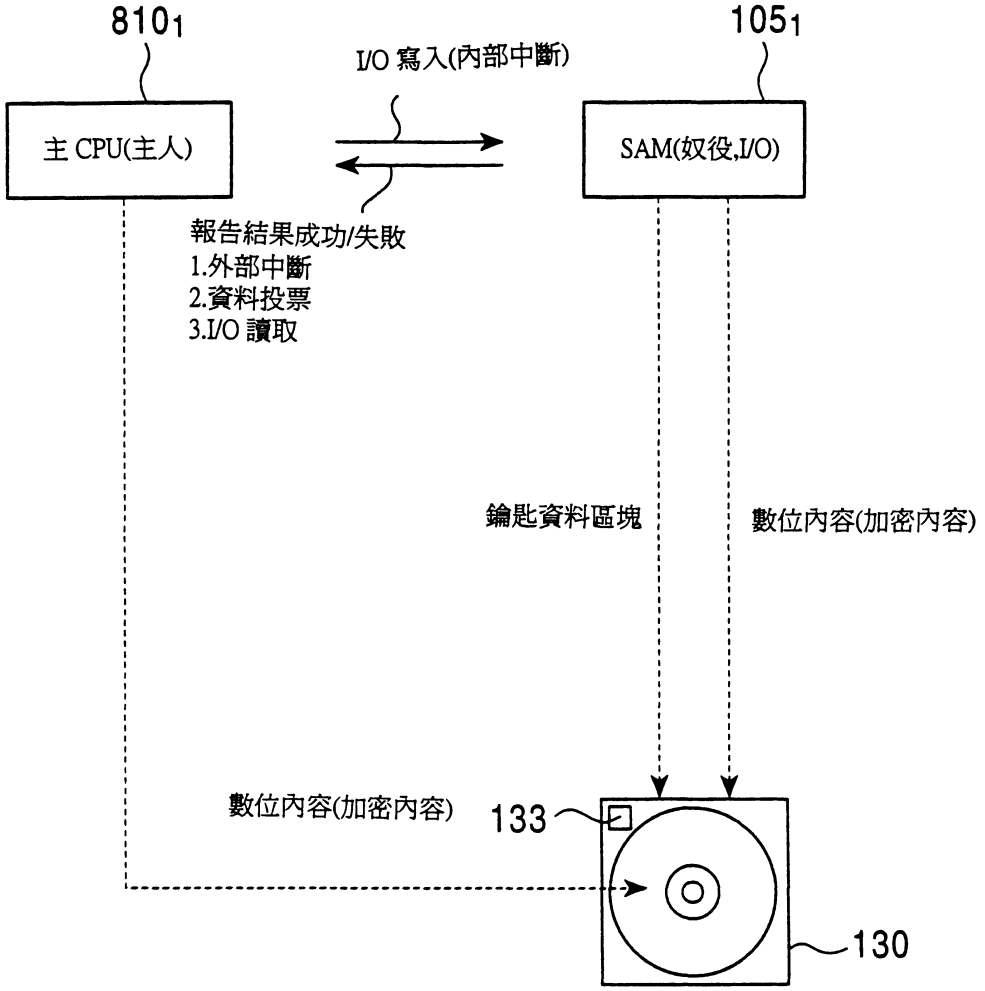

810_1
105_1
I/O 寫入(內部中斷)
主 CPU(主人)
SAM(奴役,I/O)
報告結果成功/失敗
1.外部中斷
2.資料投票
3.I/O 讀取
鑰匙資料區塊
數位內容(加密內容)
數位內容(加密內容)
133
130

圖 6 6

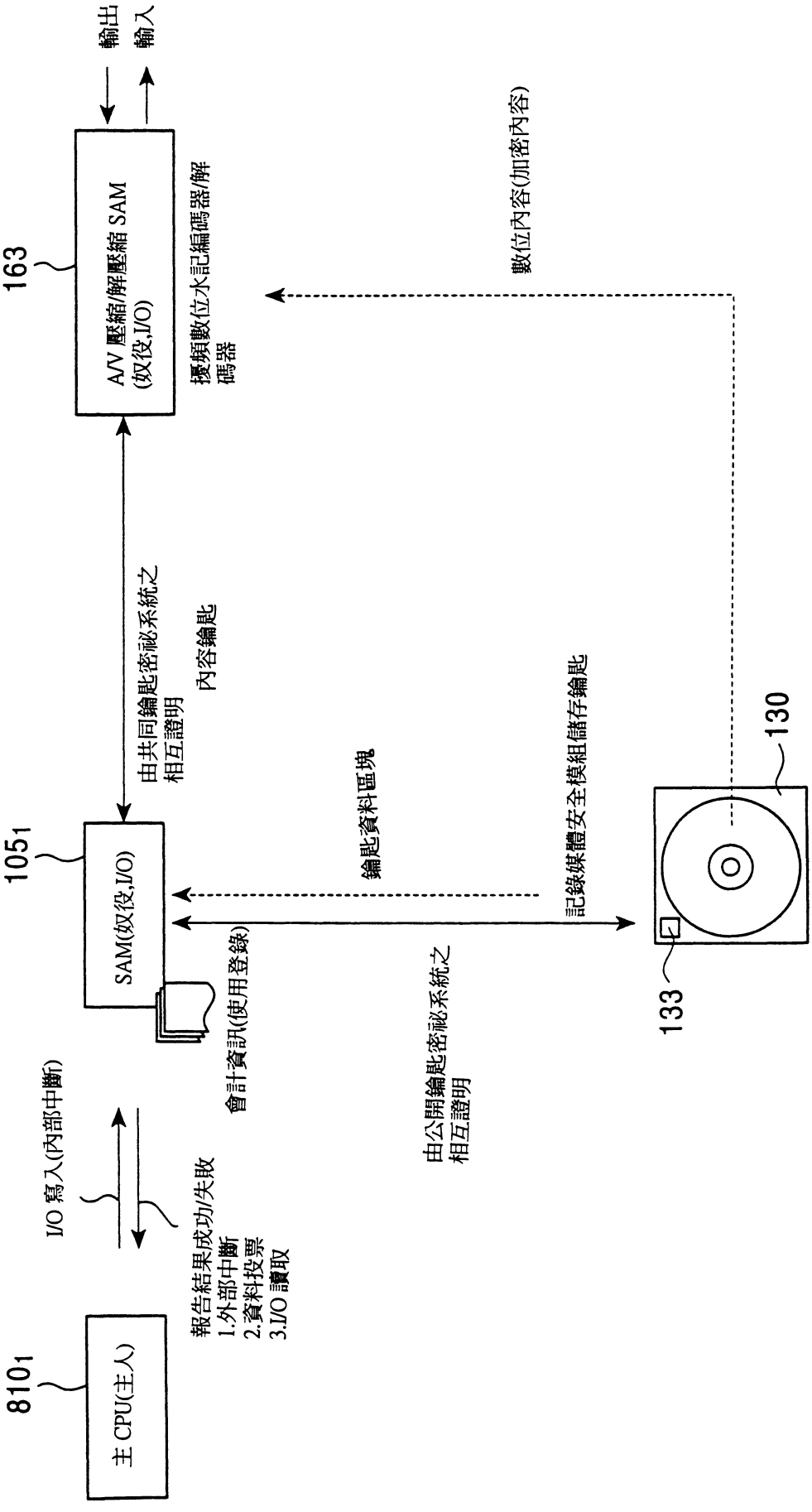

輸出
輸入
163
A/V 壓縮/解壓縮 SAM
(奴役,I/O)
擾頻數位水記編碼器/解
碼器
數位內容(加密內容)
由共同鑰匙密祕系統之
相互證明
內容鑰匙
1051
SAM(奴役,I/O)
鑰匙資料區塊
記錄媒體安全模組儲存鑰匙
130
會計資訊(使用登錄)
由公開鑰匙密祕系統之
相互證明
133
I/O 寫入(內部中斷)
報告結果成功/失敗
1.外部中斷
2.資料投票
3.I/O 讀取
8101
主 CPU(主人)

圖 6 7

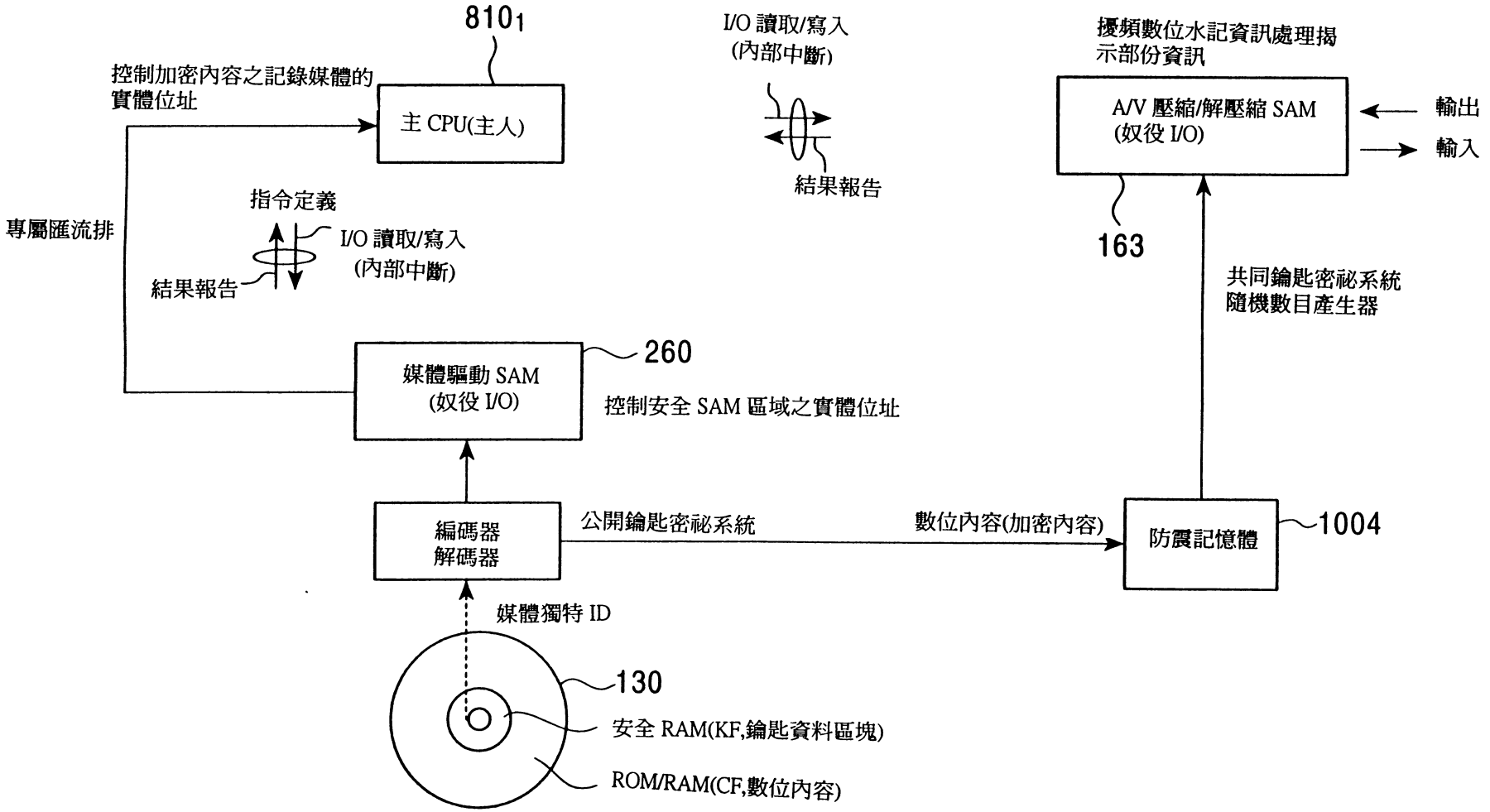

810₁
控制加密內容之記錄媒體的實體位址
主 CPU(主人)
I/O 讀取/寫入
(內部中斷)
結果報告
擾頻數位水記資訊處理揭示部份資訊
A/V 壓縮/解壓縮 SAM
(奴役 I/O)
輸出
輸入
163
指令定義
專屬匯流排
I/O 讀取/寫入
(內部中斷)
結果報告
共同鑰匙密祕系統
隨機數目產生器
媒體驅動 SAM
(奴役 I/O)
260
控制安全 SAM 區域之實體位址
編碼器
解碼器
公開鑰匙密祕系統
數位內容(加密內容)
防震記憶體
1004
媒體獨特 ID
130
安全 RAM(KF,鑰匙資料區塊)
ROM/RAM(CF,數位內容)

圖 6 8

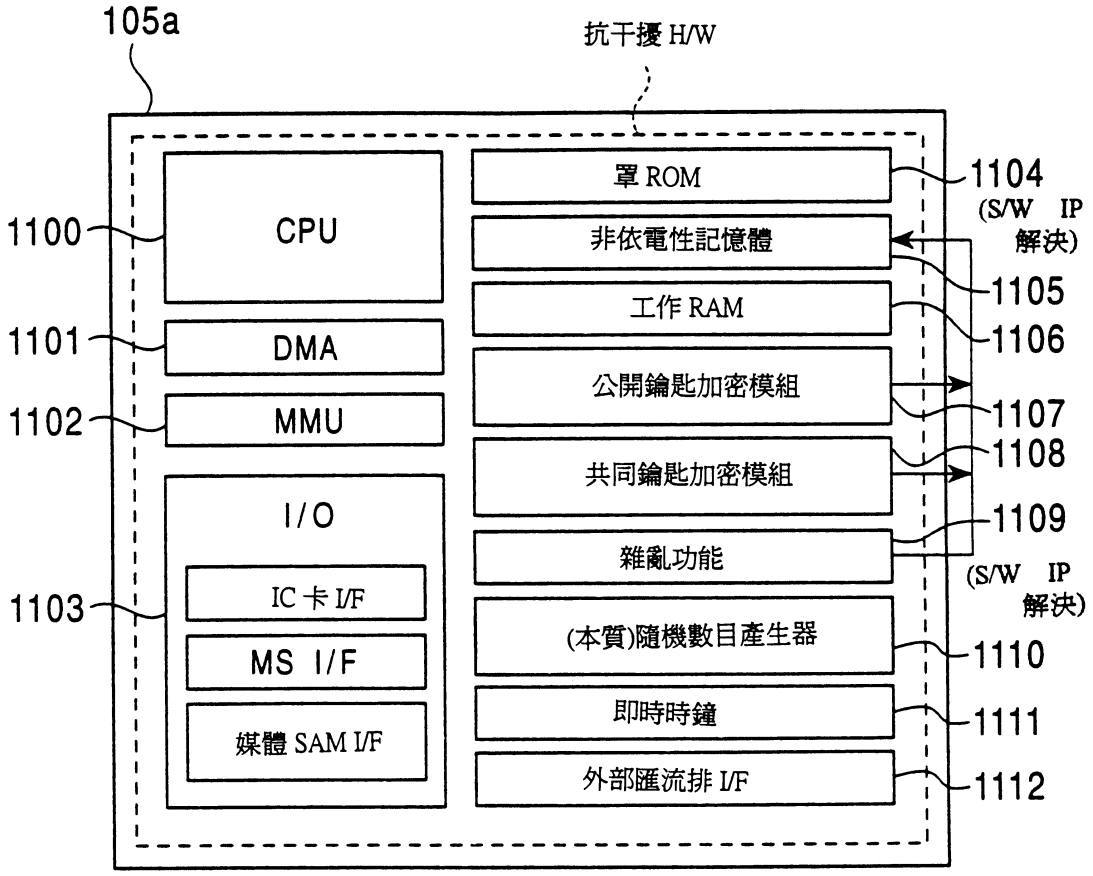

105a
抗干擾 H/W
1100
CPU
1101
DMA
1102
MMU
1103
I/O
IC 卡 I/F
MS I/F
媒體 SAM I/F
罩 ROM
1104
(S/W IP 解決)
非依電性記憶體
工作 RAM
1105
1106
公開鑰匙加密模組
1107
共同鑰匙加密模組
1108
1109
雜亂功能
(S/W IP 解決)
(本質)隨機數目產生器
1110
即時時鐘
1111
外部匯流排 I/F
1112

圖 6 9

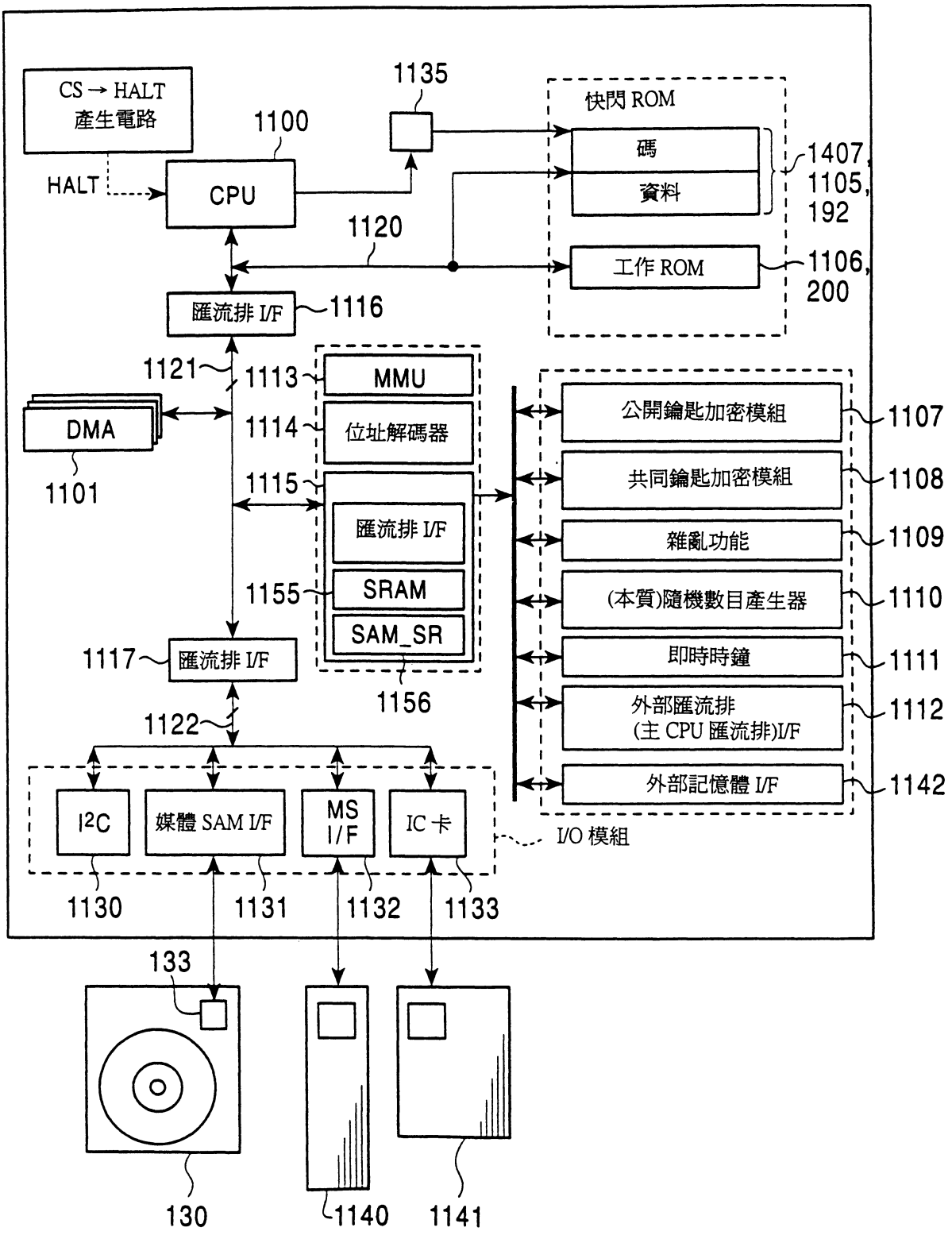

CS → HALT
產生電路
HALT
1100
CPU
1135
快閃 ROM
碼
資料
1407,
1105,
192
1120
工作 ROM
1106,
200
匯流排 I/F
1116
1121
1113
MMU
DMA
1101
1114
位址解碼器
1115
匯流排 I/F
SRAM
1155
SAM_SR
1156
1117
匯流排 I/F
1122
公開鑰匙加密模組
1107
共同鑰匙加密模組
1108
雜亂功能
1109
(本質)隨機數目產生器
1110
即時時鐘
1111
外部匯流排
(主 CPU 匯流排)I/F
1112
外部記憶體 I/F
1142
I²C
媒體 SAM I/F
MS
I/F
IC 卡
I/O 模組
1130
1131
1132
1133
133
130
1140
1141

圖 7 0

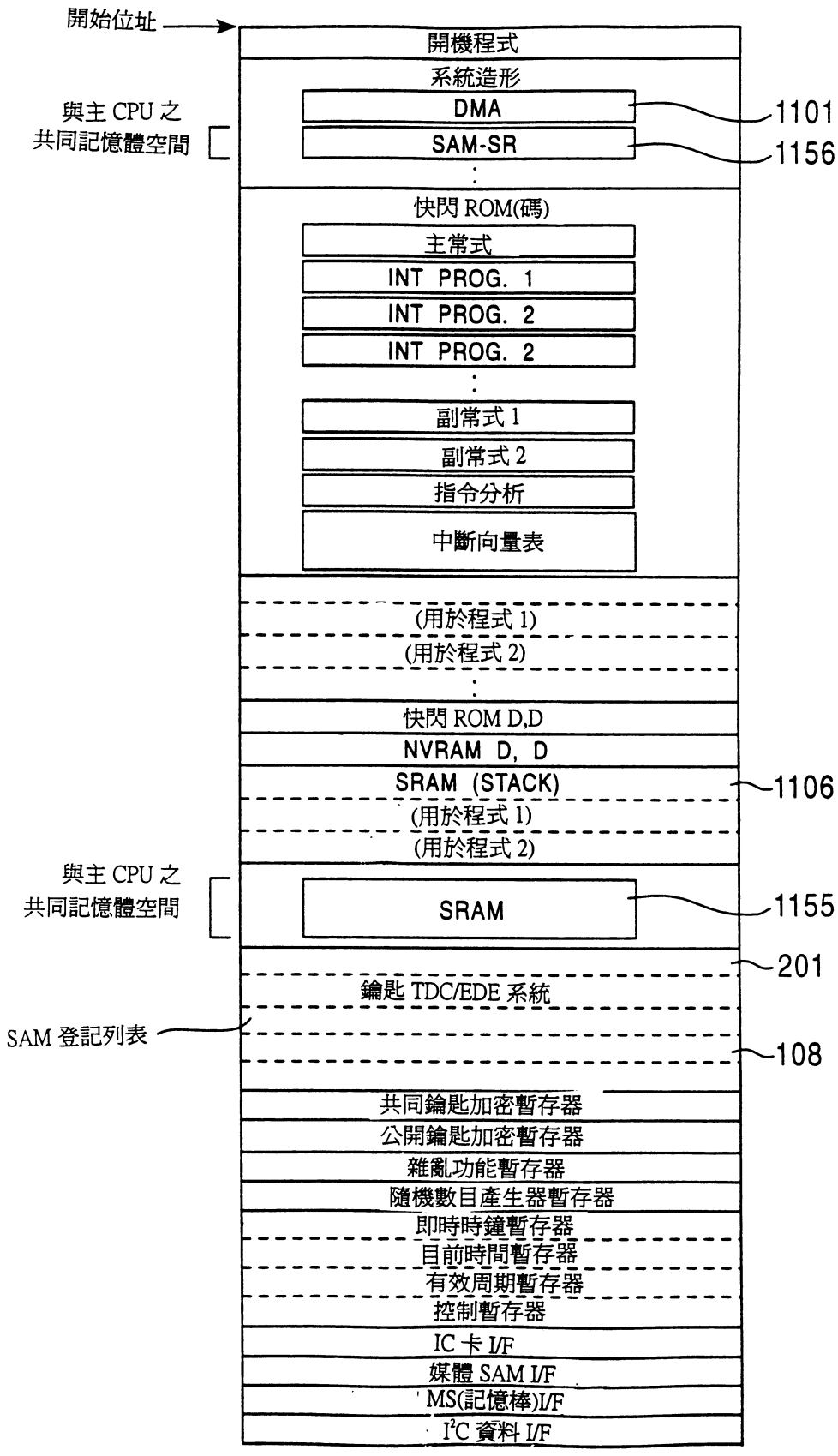

開始位址
開機程式
系統造形
與主 CPU 之
共同記憶體空間
DMA
1101
SAM-SR
1156
快閃 ROM(碼)
主常式
INT PROG. 1
INT PROG. 2
INT PROG. 2
副常式 1
副常式 2
指令分析
中斷向量表
(用於程式 1)
(用於程式 2)
快閃 ROM D,D
NVRAM D, D
SRAM (STACK)
1106
(用於程式 1)
(用於程式 2)
與主 CPU 之
共同記憶體空間
SRAM
1155
201
鑰匙 TDC/EDE 系統
SAM 登記列表
108
共同鑰匙加密暫存器
公開鑰匙加密暫存器
雜亂功能暫存器
隨機數目產生器暫存器
即時時鐘暫存器
目前時間暫存器
有效周期暫存器
控制暫存器
IC 卡 I/F
媒體 SAM I/F
MS(記憶棒)I/F
I²C 資料 I/F

圖 7 1

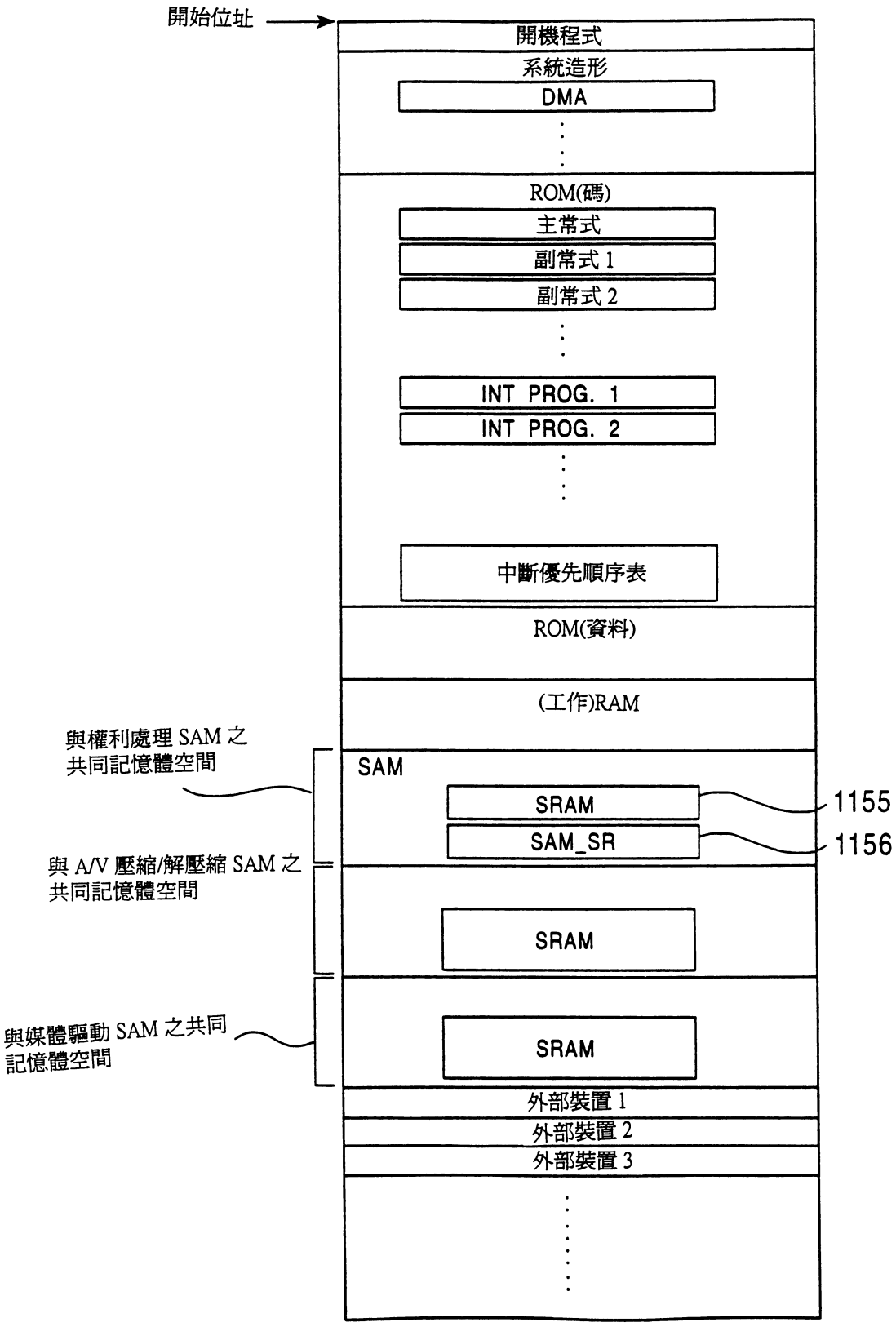

開始位址
開機程式
系統造形
DMA
ROM(碼)
主常式
副常式 1
副常式 2
INT PROG. 1
INT PROG. 2
中斷優先順序表
ROM(資料)
(工作)RAM
與權利處理 SAM 之
共同記憶體空間
SAM
SRAM
SAM_SR
1155
1156
與 A/V 壓縮/解壓縮 SAM 之
共同記憶體空間
SRAM
與媒體驅動 SAM 之共同
記憶體空間
SRAM
外部裝置 1
外部裝置 2
外部裝置 3

圖 7 2

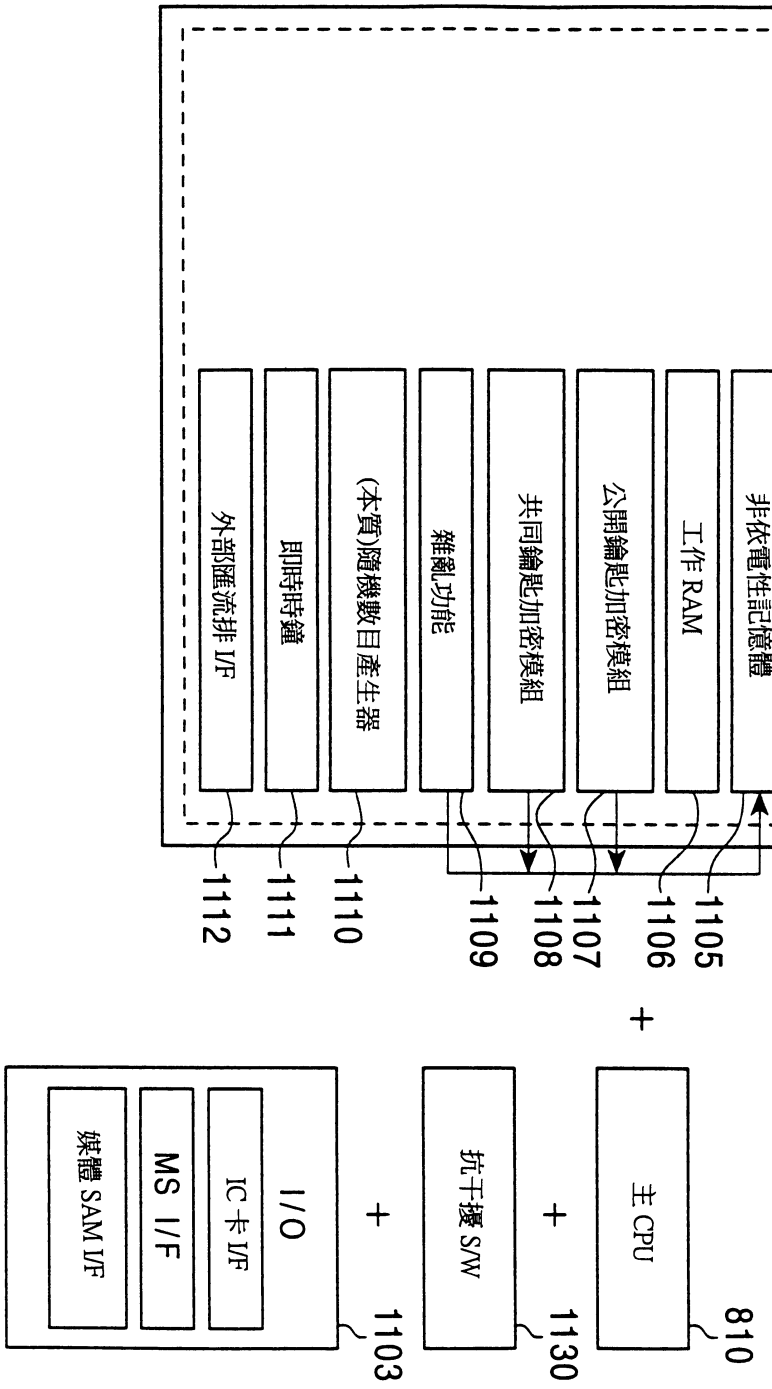

105ba
抗干擾 H/W
罩 ROM
非依電性記憶體
工作 RAM
公開鑰匙加密模組
共同鑰匙加密模組
雜亂功能
(本質)隨機數目產生器
即時時鐘
外部匯流排 I/F
1104
1105
1106
1107
1108
1109
1110
1111
1112
+
主 CPU
810
+
抗干擾 S/W
1130
+
I/O
1103
IC 卡 I/F
MS I/F
媒體 SAM I/F

圖 7 3

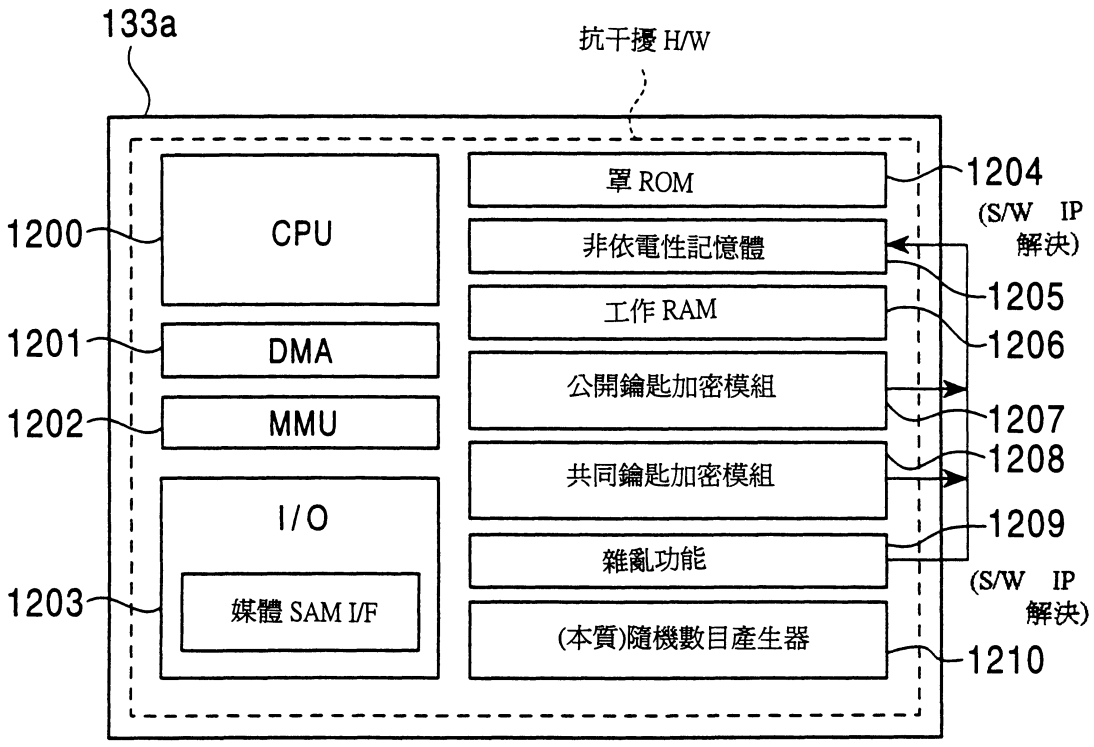

133a
抗干擾 H/W
1200
CPU
1201
DMA
1202
MMU
1203
I/O
媒體 SAM I/F
罩 ROM
非依電性記憶體
工作 RAM
公開鑰匙加密模組
共同鑰匙加密模組
雜亂功能
(本質)隨機數目產生器
1204
(S/W IP 解決)
1205
1206
1207
1208
1209
(S/W IP 解決)
1210

圖 7 4

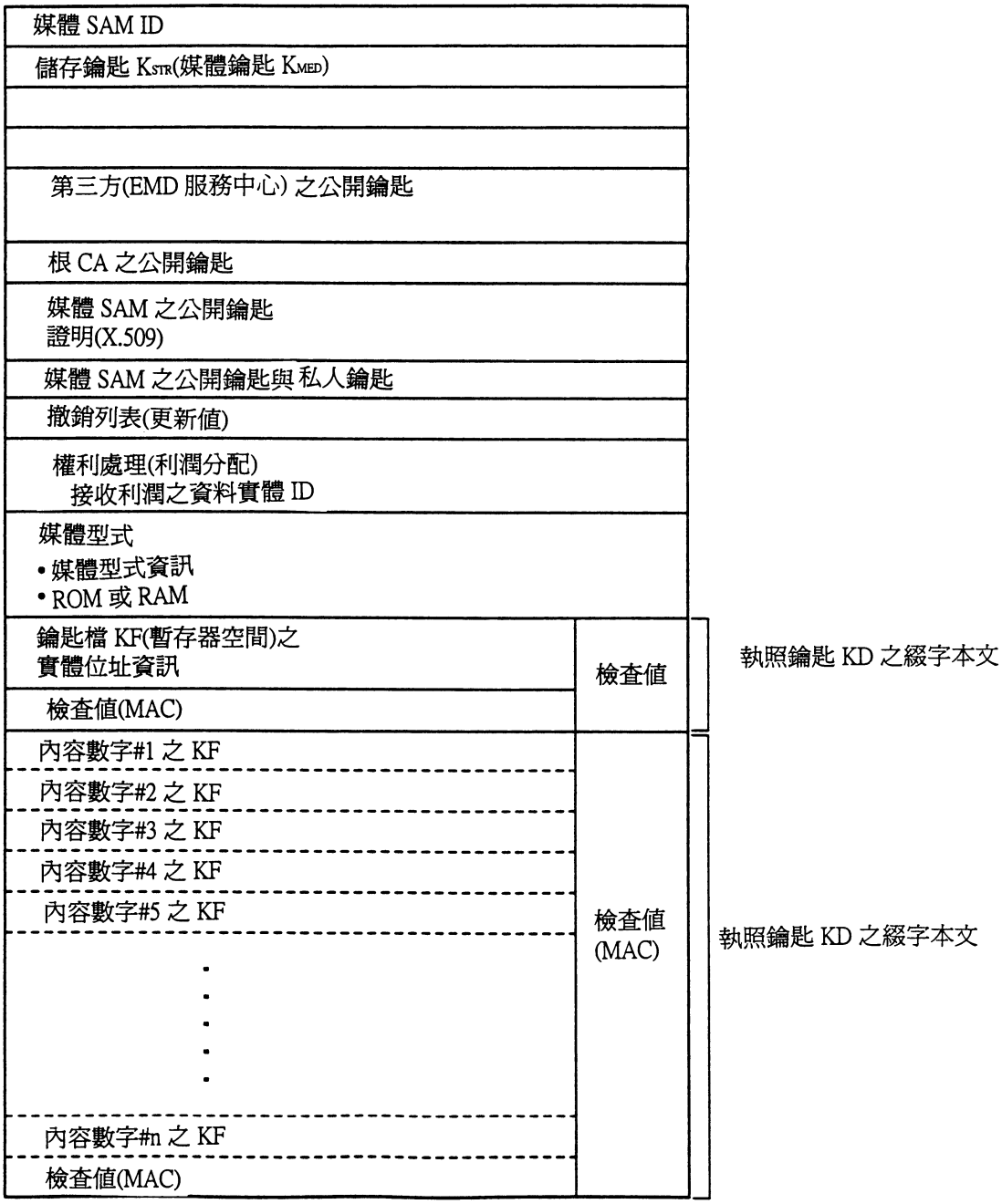

媒體 SAM ID
儲存鑰匙 KSTR(媒體鑰匙 KMED)
第三方(EMD 服務中心) 之公開鑰匙
根 CA 之公開鑰匙
媒體 SAM 之公開鑰匙
證明(X.509)
媒體 SAM 之公開鑰匙與私人鑰匙
撤銷列表(更新值)
權利處理(利潤分配)
接收利潤之資料實體 ID
媒體型式
• 媒體型式資訊
• ROM 或 RAM
鑰匙檔 KF(暫存器空間)之
實體位址資訊
檢查值(MAC)
檢查值
執照鑰匙 KD 之綴字本文
內容數字#1 之 KF
內容數字#2 之 KF
內容數字#3 之 KF
內容數字#4 之 KF
內容數字#5 之 KF
內容數字#n 之 KF
檢查值(MAC)
檢查值
(MAC)
執照鑰匙 KD 之綴字本文

圖 7 5

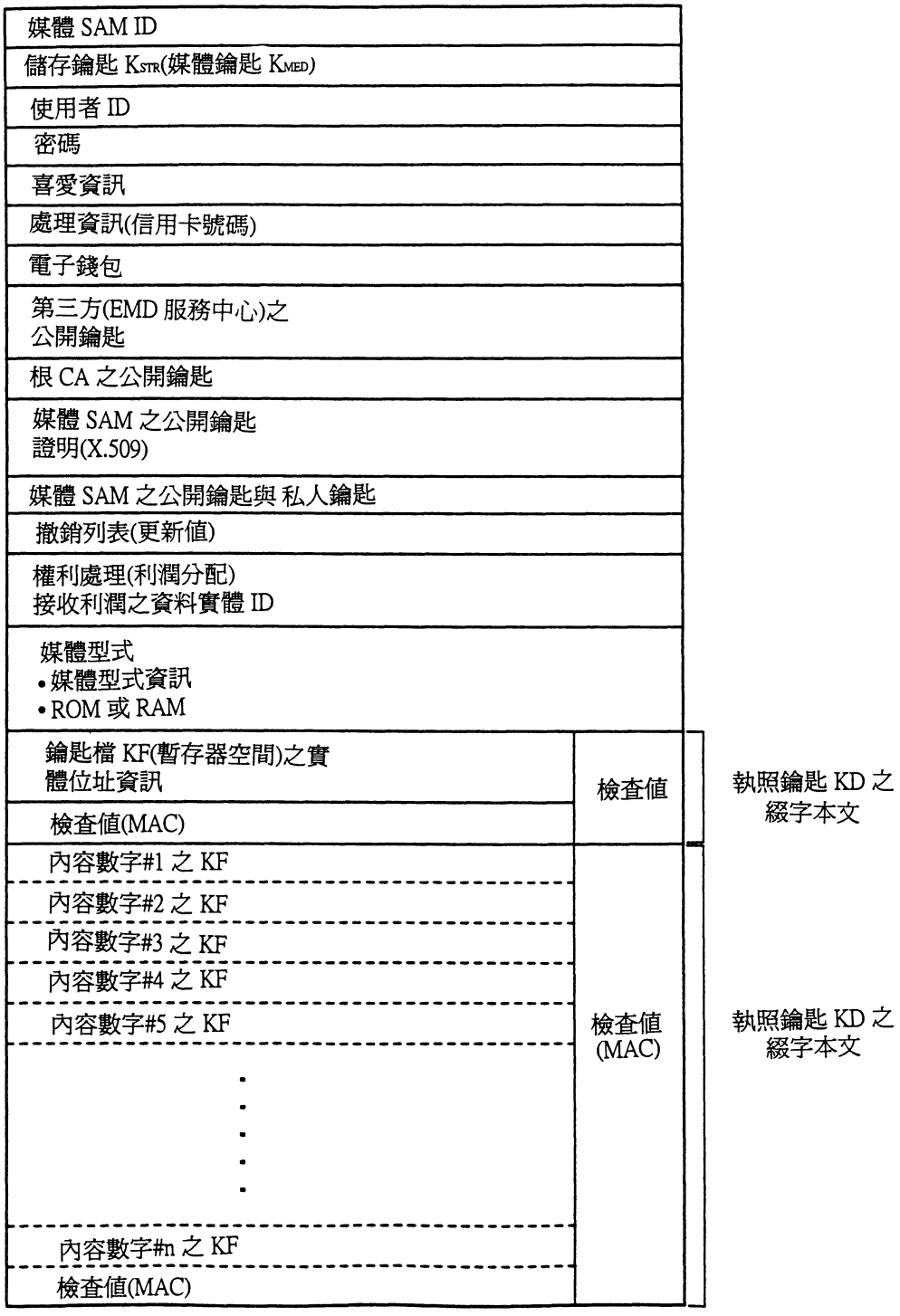

媒體 SAM ID
儲存鑰匙 KSTR(媒體鑰匙 KMED)
使用者 ID
密碼
喜愛資訊
處理資訊(信用卡號碼)
電子錢包
第三方(EMD 服務中心)之
公開鑰匙
根 CA 之公開鑰匙
媒體 SAM 之公開鑰匙
證明(X.509)
媒體 SAM 之公開鑰匙與 私人鑰匙
撤銷列表(更新值)
權利處理(利潤分配)
接收利潤之資料實體 ID
媒體型式
• 媒體型式資訊
• ROM 或 RAM
鑰匙檔 KF(暫存器空間)之實
體位址資訊
檢查值(MAC)
檢查值
執照鑰匙 KD 之
綴字本文
內容數字#1 之 KF
內容數字#2 之 KF
內容數字#3 之 KF
內容數字#4 之 KF
內容數字#5 之 KF
內容數字#n 之 KF
檢查值(MAC)
檢查值
(MAC)
執照鑰匙 KD 之
綴字本文

圖 7 6

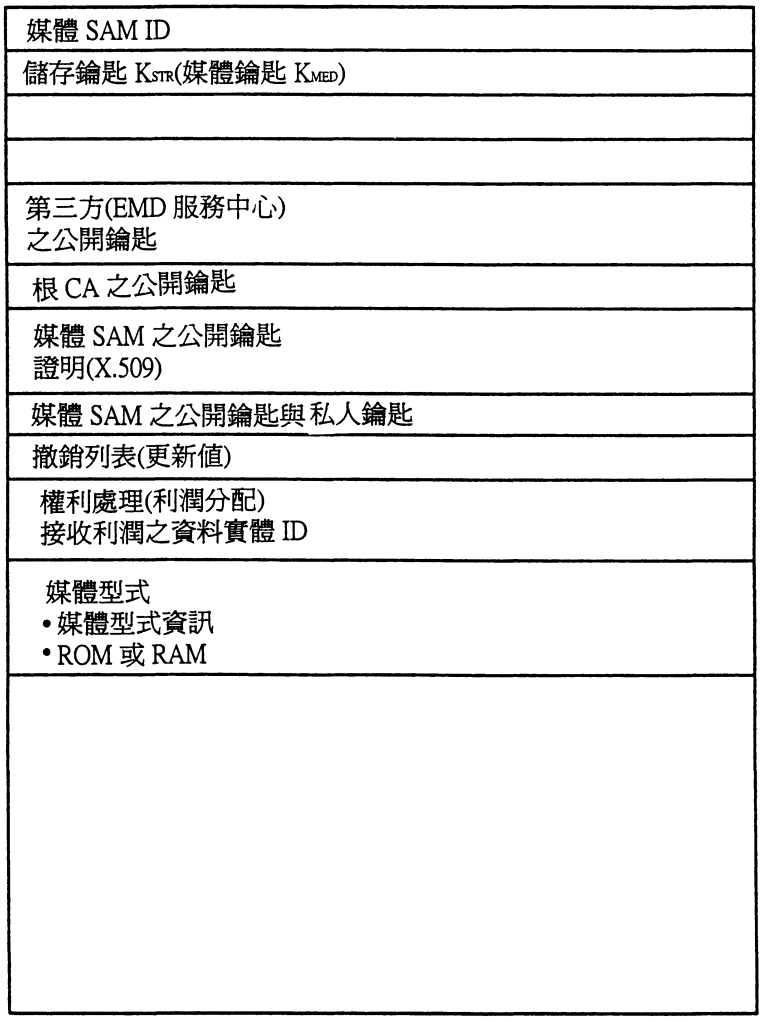

媒體 SAM ID
儲存鑰匙 KSTR(媒體鑰匙 KMED)
第三方(EMD 服務中心)
之公開鑰匙
根 CA 之公開鑰匙
媒體 SAM 之公開鑰匙
證明(X.509)
媒體 SAM 之公開鑰匙與私人鑰匙
撤銷列表(更新值)
權利處理(利潤分配)
接收利潤之資料實體 ID
媒體型式
• 媒體型式資訊
• ROM 或 RAM

圖 7 7

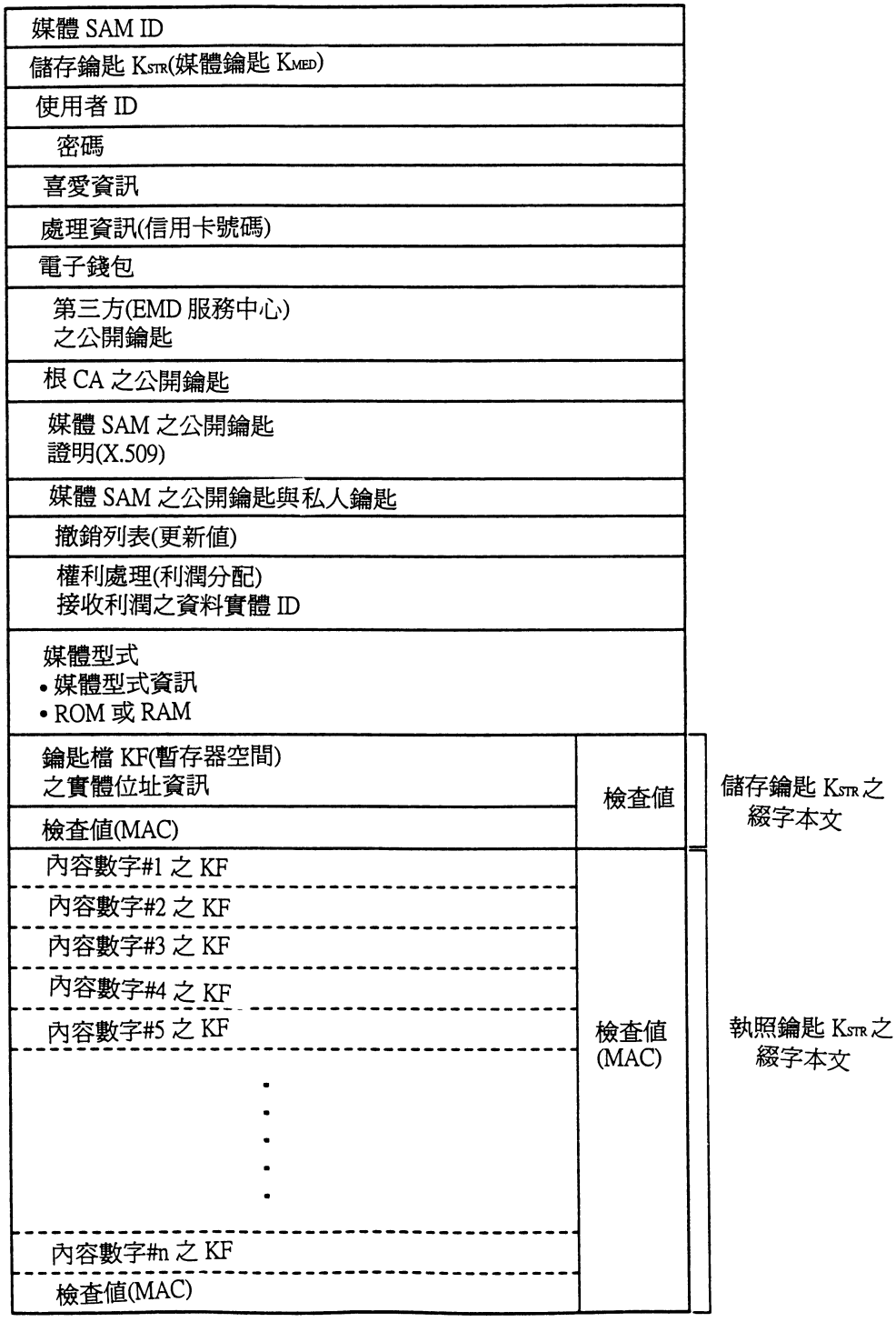

媒體 SAM ID
儲存鑰匙 KSTR(媒體鑰匙 KMED)
使用者 ID
密碼
喜愛資訊
處理資訊(信用卡號碼)
電子錢包
第三方(EMD 服務中心)
之公開鑰匙
根 CA 之公開鑰匙
媒體 SAM 之公開鑰匙
證明(X.509)
媒體 SAM 之公開鑰匙與私人鑰匙
撤銷列表(更新值)
權利處理(利潤分配)
接收利潤之資料實體 ID
媒體型式
• 媒體型式資訊
• ROM 或 RAM
鑰匙檔 KF(暫存器空間)
之實體位址資訊
檢查值
檢查值(MAC)
儲存鑰匙 KSTR 之
綴字本文
內容數字#1 之 KF
內容數字#2 之 KF
內容數字#3 之 KF
內容數字#4 之 KF
內容數字#5 之 KF
檢查值
(MAC)
執照鑰匙 KSTR 之
綴字本文
內容數字#n 之 KF
檢查值(MAC)

圖 7 8

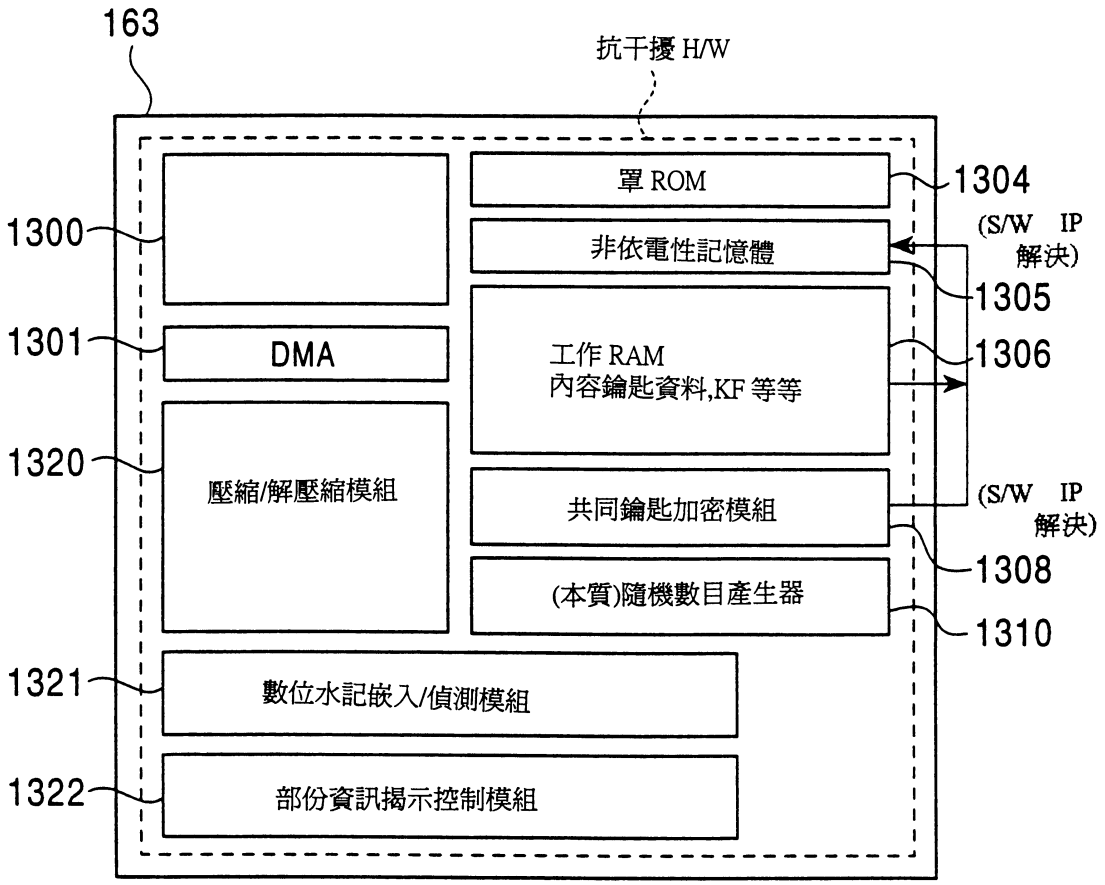

163
抗干擾 H/W
1300
1301
DMA
1320
壓縮/解壓縮模組
1321
數位水記嵌入/偵測模組
1322
部份資訊揭示控制模組
罩 ROM
1304
非依電性記憶體
(S/W IP 解決)
1305
工作 RAM
內容鑰匙資料,KF 等等
1306
共同鑰匙加密模組
(S/W IP 解決)
1308
(本質)隨機數目產生器
1310

圖 7 9

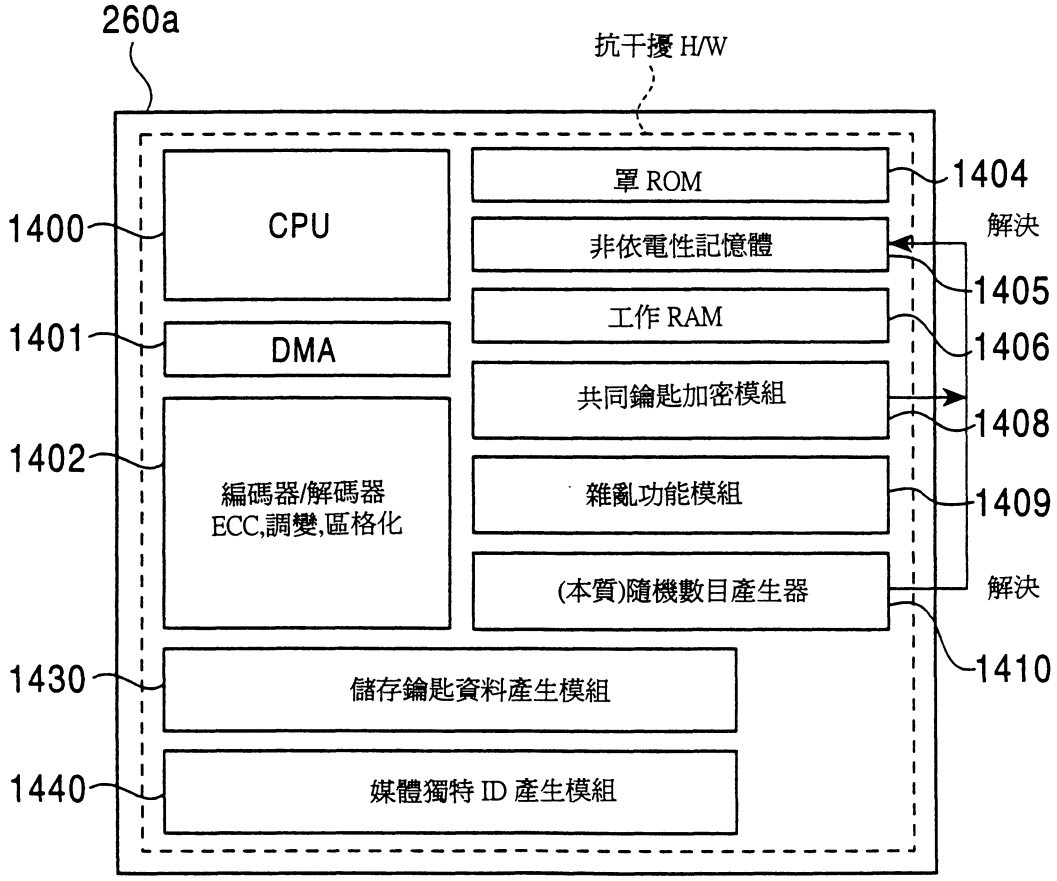
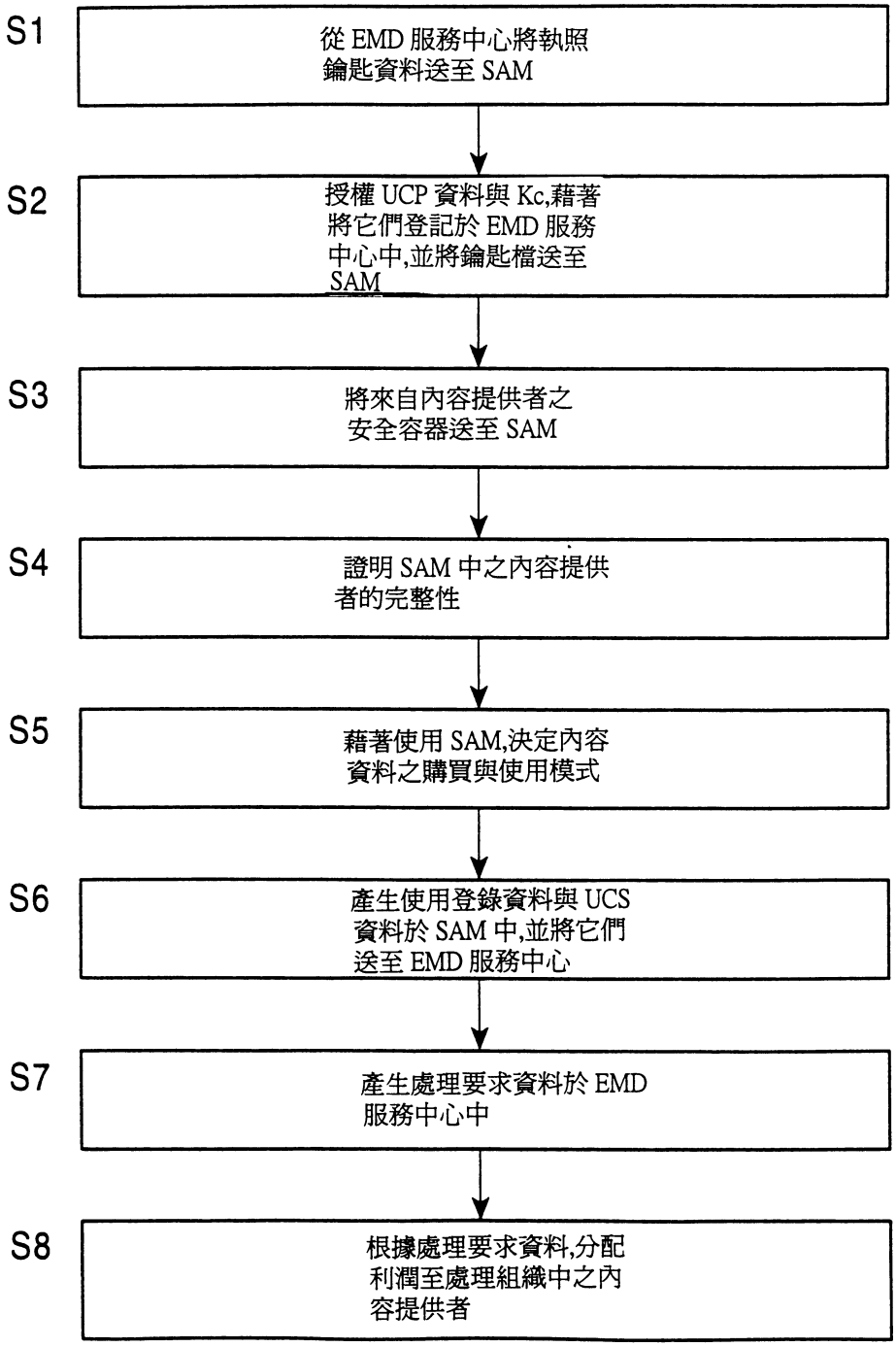

260a
抗干擾 H/W
CPU
1400
DMA
1401
編碼器/解碼器
ECC,調變,區格化
1402
1430
儲存鑰匙資料產生模組
1440
媒體獨特 ID 產生模組
罩 ROM
1404
非依電性記憶體
解決
1405
工作 RAM
1406
共同鑰匙加密模組
1408
雜亂功能模組
1409
(本質)隨機數目產生器
解決
1410

圖８０


S1
從 EMD 服務中心將執照
鑰匙資料送至 SAM
S2
授權 UCP 資料與 Kc,藉著
將它們登記於 EMD 服務
中心中,並將鑰匙檔送至
SAM
S3
將來自內容提供者之
安全容器送至 SAM
S4
證明 SAM 中之內容提供
者的完整性
S5
藉著使用 SAM,決定內容
資料之購買與使用模式
S6
產生使用登錄資料與 UCS
資料於 SAM 中,並將它們
送至 EMD 服務中心
S7
產生處理要求資料於 EMD
服務中心中
S8
根據處理要求資料,分配
利潤至處理組織中之內
容提供者

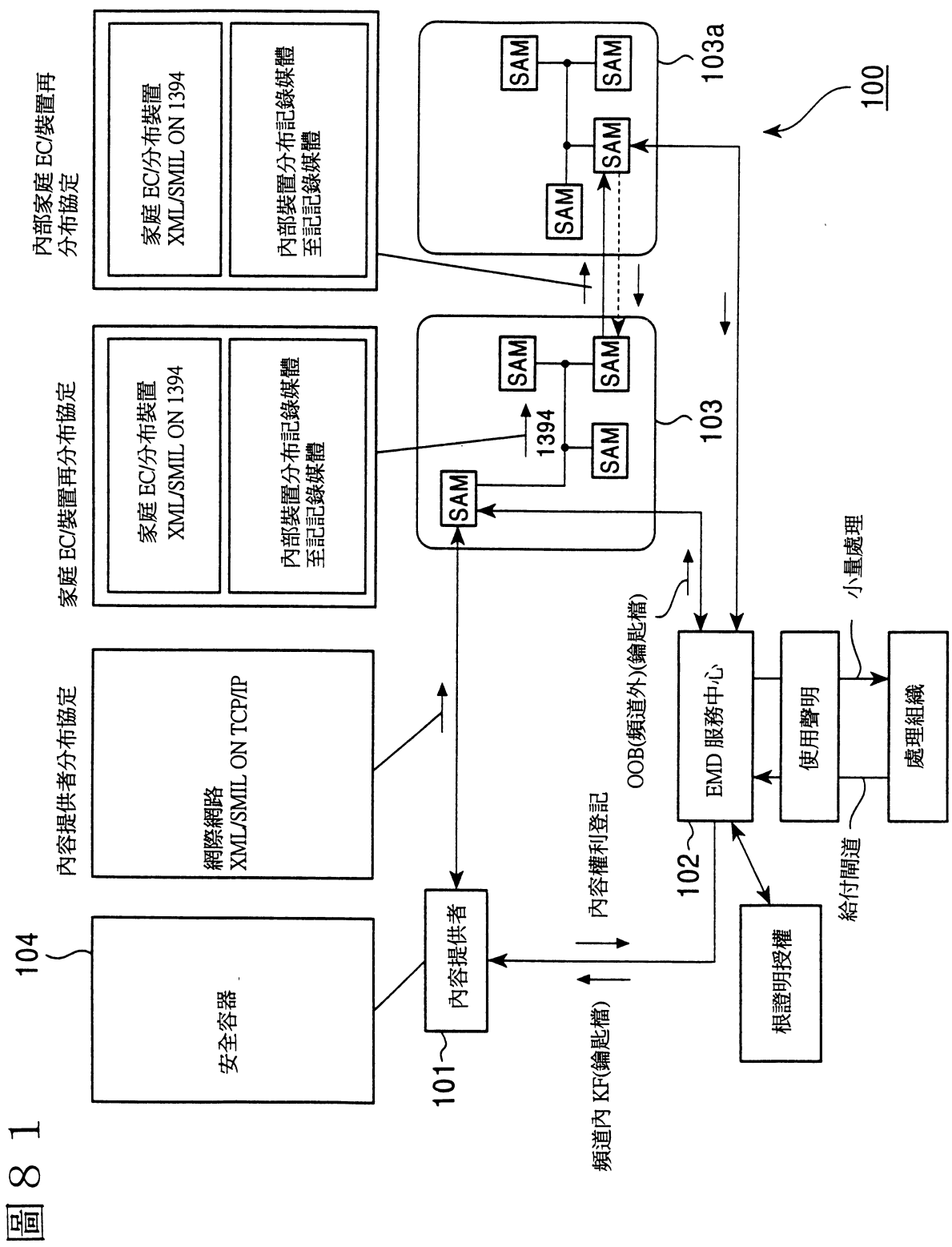

內部家庭 EC/裝置再分布協定
家庭 EC/分布裝置 XML/SMIL ON 1394
內部裝置分布記錄媒體至記記錄媒體
家庭 EC/裝置再分布協定
家庭 EC/分布裝置 XML/SMIL ON 1394
內部裝置分布記錄媒體至記記錄媒體
內容提供者分布協定
網際網路 XML/SMIL ON TCP/IP
安全容器
104
SAM
1394
103
103a
100
101
內容提供者
內容權利登記
頻道內 KF(鑰匙檔)
OOB(頻道外)(鑰匙檔)
102
EMD 服務中心
使用聲明
處理組織
小量處理
給付閘道
根證明授權

圖 8 1

圖 8 2

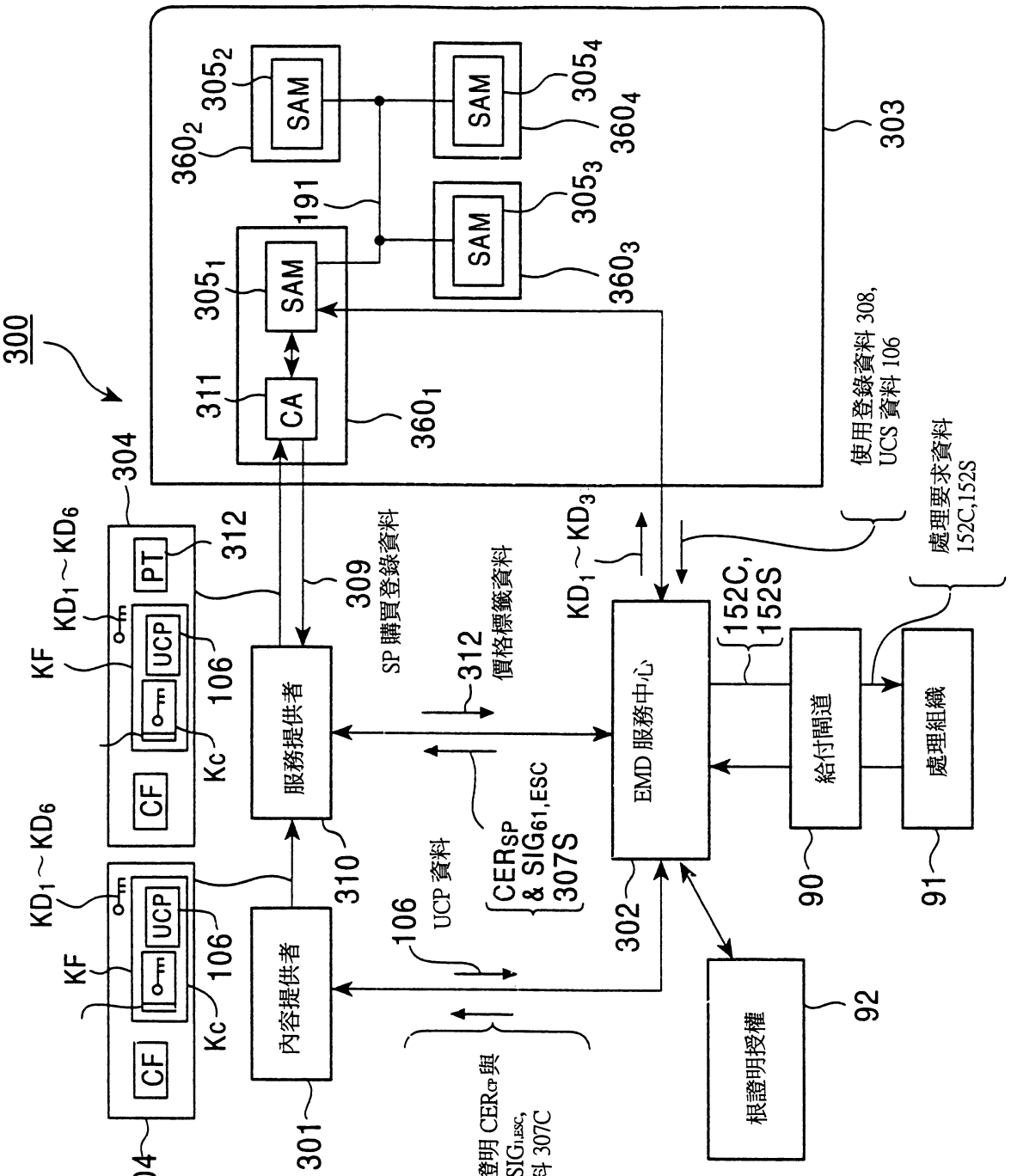

300
304
311
CA
191
SAM
305₁
305₂
305₃
305₄
360₁
360₂
360₃
360₄
303
使用登錄資料 308,
UCS 資料 106
處理要求資料
152C,152S
KD₁～KD₆
KF
CF
UCP
PT
106
312
Kc
104
301
內容提供者
服務提供者
310
309
SP 購買登錄資料
312
價格標籤資料
KD₁～KD₃
EMD 服務中心
302
152C,
152S
給付閘道
90
處理組織
91
106
UCP 資料
CERSP
& SIG61,ESC
307S
鑰匙檔 KF,
公開鑰匙證明 CERCP 與
簽名資料 SIG1,ESC,
處理報告資料 307C
根證明授權
92

圖 8 3

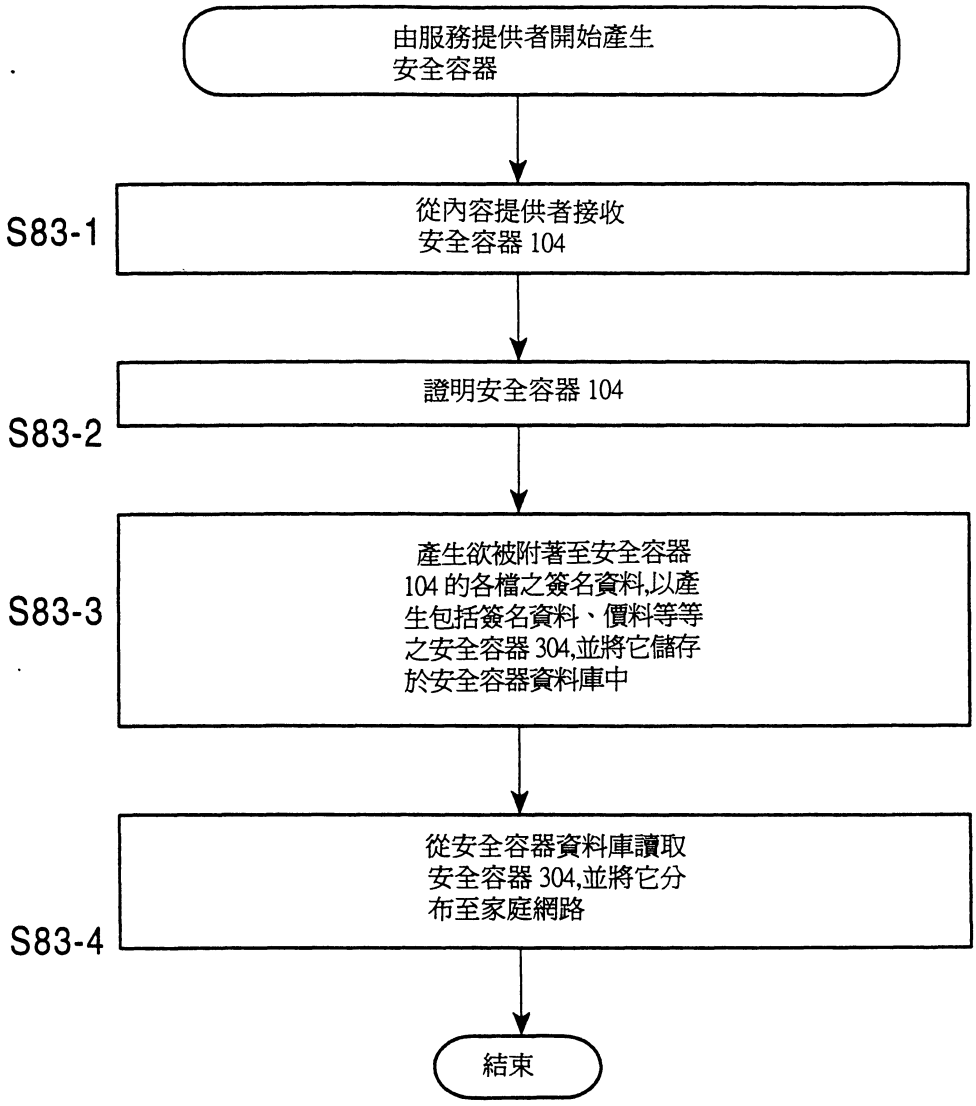

由服務提供者開始產生
安全容器
S83-1
從內容提供者接收
安全容器 104
證明安全容器 104
S83-2
S83-3
產生欲被附著至安全容器
104 的各檔之簽名資料,以產
生包括簽名資料、價料等等
之安全容器 304,並將它儲存
於安全容器資料庫中
從安全容器資料庫讀取
安全容器 304,並將它分
布至家庭網路
S83-4
結束

圖８４Ａ

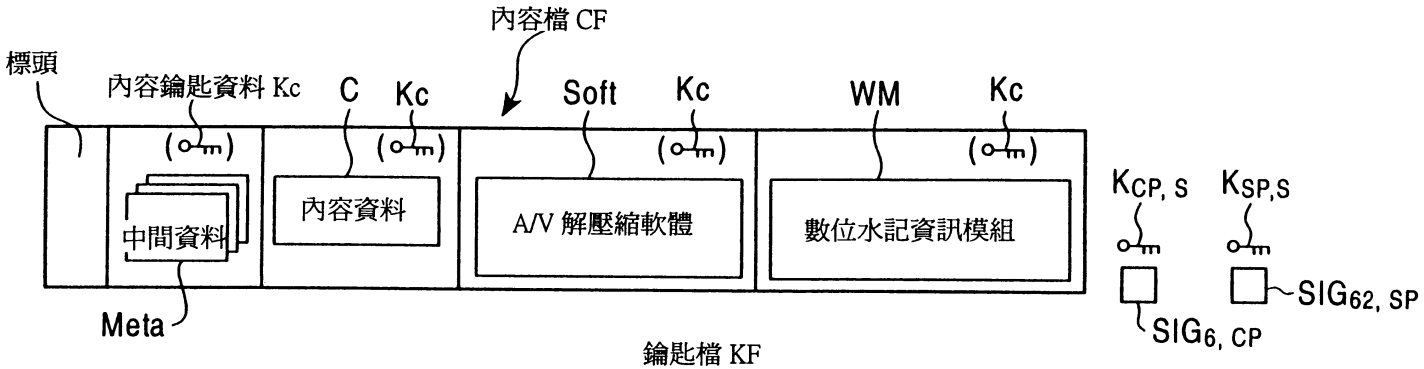


圖８４Ｂ

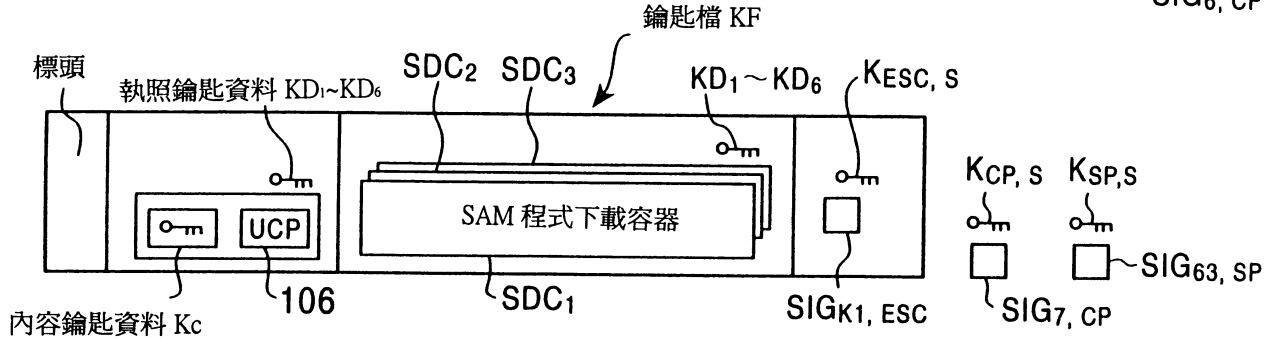


圖８４Ｃ

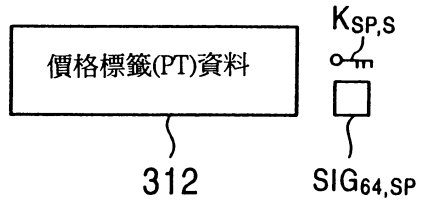


圖８４Ｄ

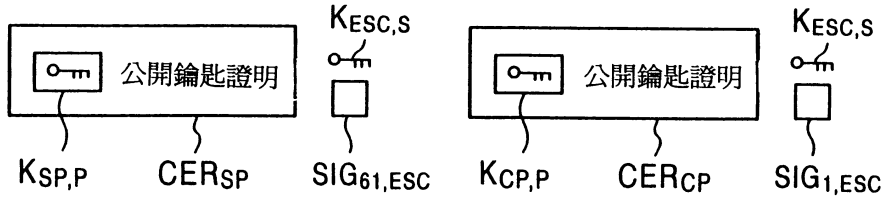


圖 8 5

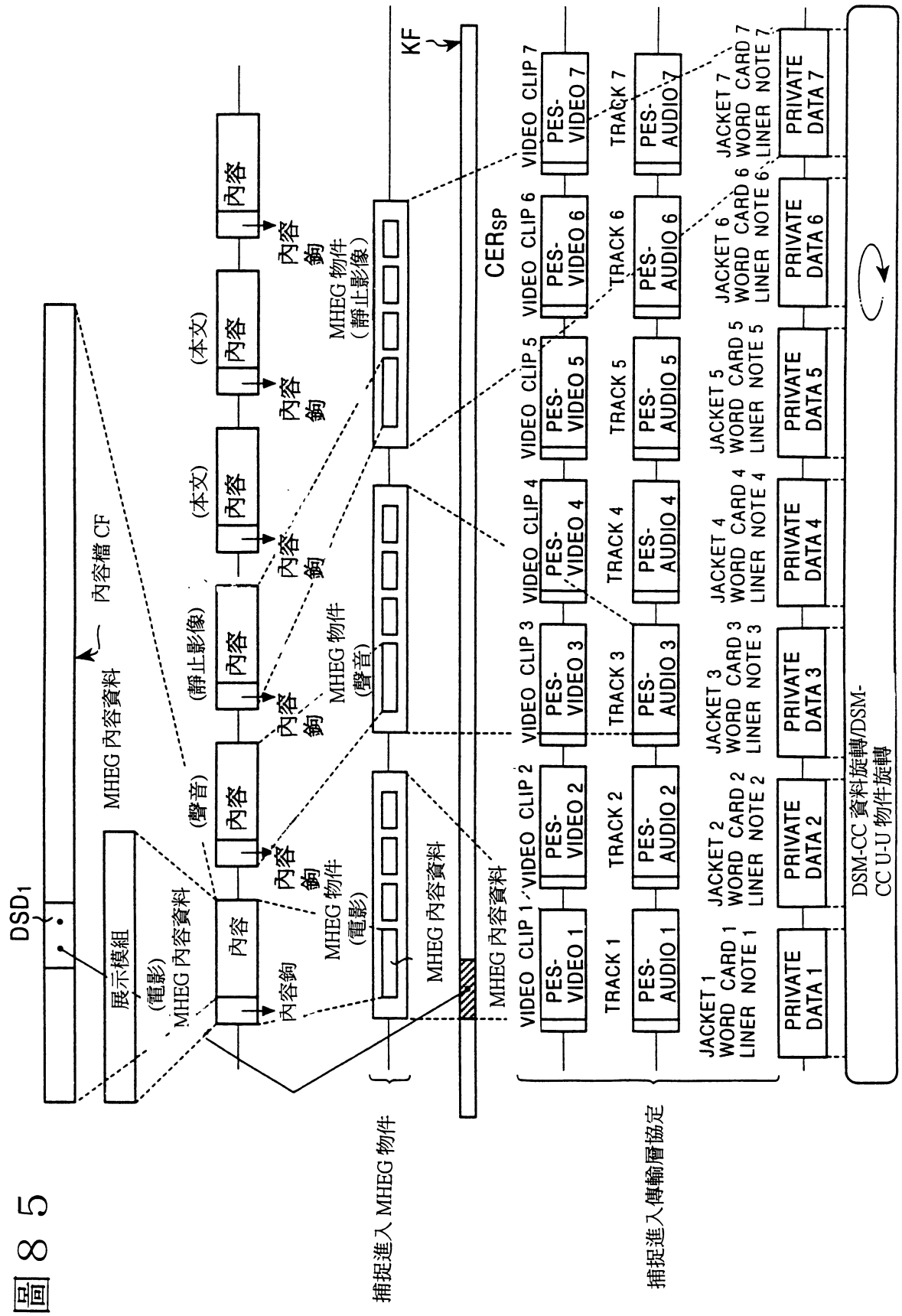

DSD1
展示模組
(電影)
MHEG 內容資料
內容檔 CF
MHEG 內容資料
內容
內容鉤
MHEG 物件
(電影)
(聲音)
內容
內容鉤
MHEG 物件
(聲音)
(靜止影像)
內容
內容鉤
(本文)
內容
內容鉤
(本文)
內容
內容鉤
MHEG 物件
(靜止影像)
內容
KF
CERSP
MHEG 內容資料
MHEG 內容資料
捕捉進入 MHEG 物件
捕捉進入傳輸層協定
VIDEO CLIP 1
PES-VIDEO 1
TRACK 1
PES-AUDIO 1
JACKET 1
WORD CARD 1
LINER NOTE 1
PRIVATE DATA 1
VIDEO CLIP 2
PES-VIDEO 2
TRACK 2
PES-AUDIO 2
JACKET 2
WORD CARD 2
LINER NOTE 2
PRIVATE DATA 2
VIDEO CLIP 3
PES-VIDEO 3
TRACK 3
PES-AUDIO 3
JACKET 3
WORD CARD 3
LINER NOTE 3
PRIVATE DATA 3
VIDEO CLIP 4
PES-VIDEO 4
TRACK 4
PES-AUDIO 4
JACKET 4
WORD CARD 4
LINER NOTE 4
PRIVATE DATA 4
VIDEO CLIP 5
PES-VIDEO 5
TRACK 5
PES-AUDIO 5
JACKET 5
WORD CARD 5
LINER NOTE 5
PRIVATE DATA 5
VIDEO CLIP 6
PES-VIDEO 6
TRACK 6
PES-AUDIO 6
JACKET 6
WORD CARD 6
LINER NOTE 6
PRIVATE DATA 6
VIDEO CLIP 7
PES-VIDEO 7
TRACK 7
PES-AUDIO 7
JACKET 7
WORD CARD 7
LINER NOTE 7
PRIVATE DATA 7
DSM-CC 資料旋轉/DSM-CC U-U 物件旋轉

圖８６

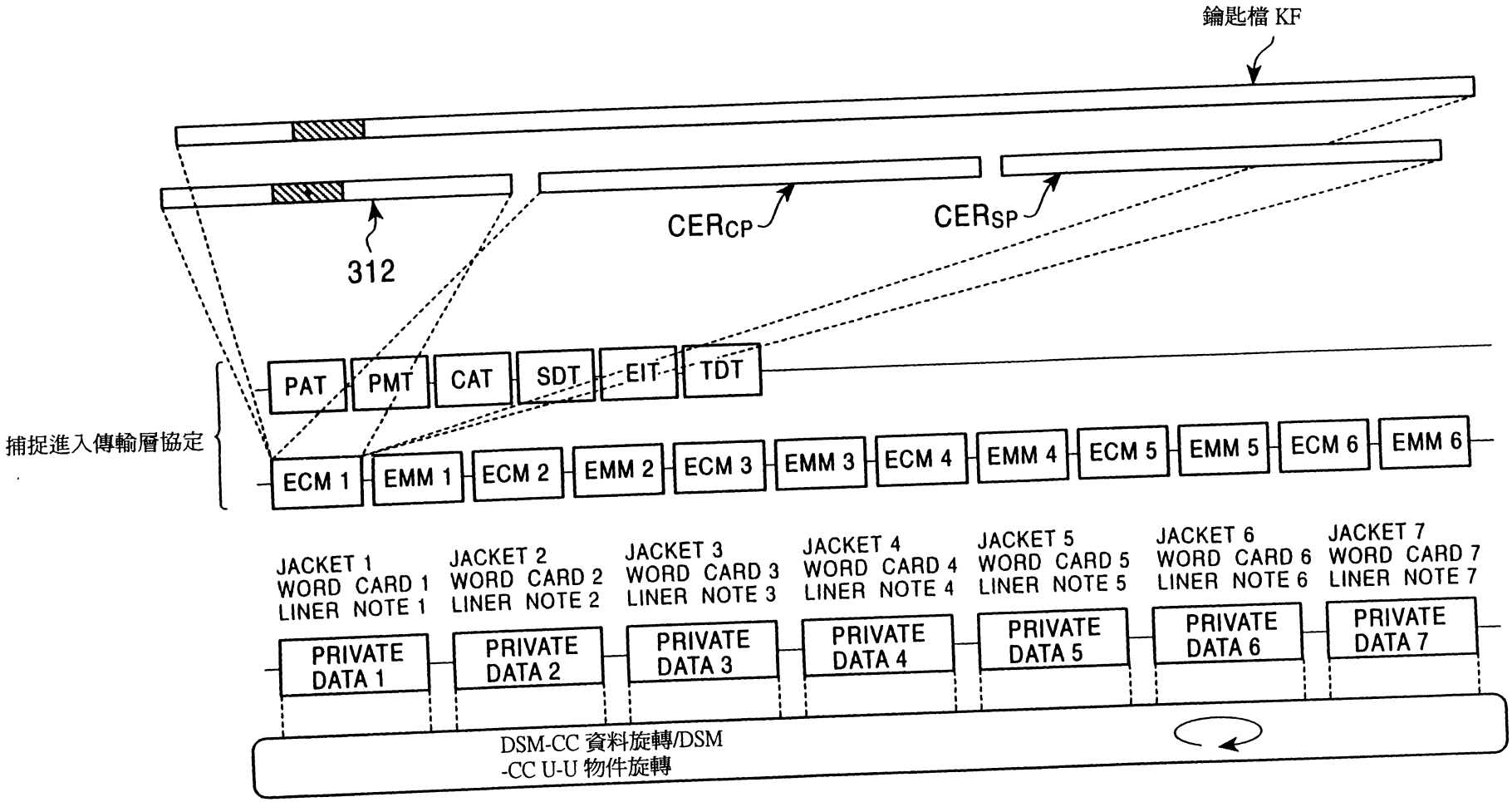

鑰匙檔 KF
312
CERCP
CERSP
捕捉進入傳輸層協定
PAT
PMT
CAT
SDT
EIT
TDT
ECM 1
EMM 1
ECM 2
EMM 2
ECM 3
EMM 3
ECM 4
EMM 4
ECM 5
EMM 5
ECM 6
EMM 6
JACKET 1
WORD CARD 1
LINER NOTE 1
JACKET 2
WORD CARD 2
LINER NOTE 2
JACKET 3
WORD CARD 3
LINER NOTE 3
JACKET 4
WORD CARD 4
LINER NOTE 4
JACKET 5
WORD CARD 5
LINER NOTE 5
JACKET 6
WORD CARD 6
LINER NOTE 6
JACKET 7
WORD CARD 7
LINER NOTE 7
PRIVATE DATA 1
PRIVATE DATA 2
PRIVATE DATA 3
PRIVATE DATA 4
PRIVATE DATA 5
PRIVATE DATA 6
PRIVATE DATA 7
DSM-CC 資料旋轉/DSM
-CC U-U 物件旋轉

圖 8 7

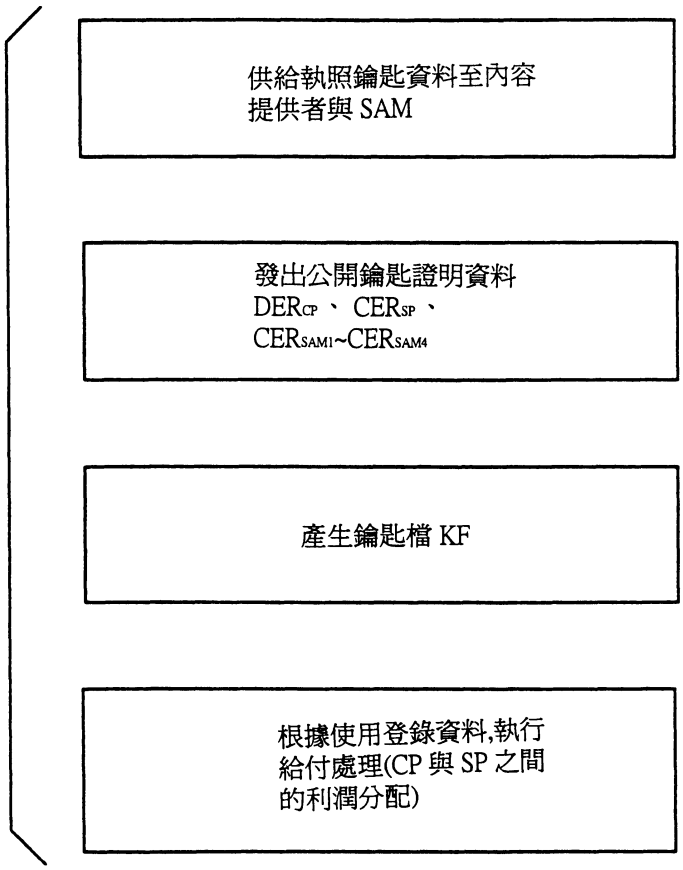

供給執照鑰匙資料至內容提供者與 SAM
發出公開鑰匙證明資料 DER_{CP}、CER_{SP}、CER_{SAM1}~CER_{SAM4}
產生鑰匙檔 KF
根據使用登錄資料,執行給付處理(CP 與 SP 之間的利潤分配)

圖 8 8

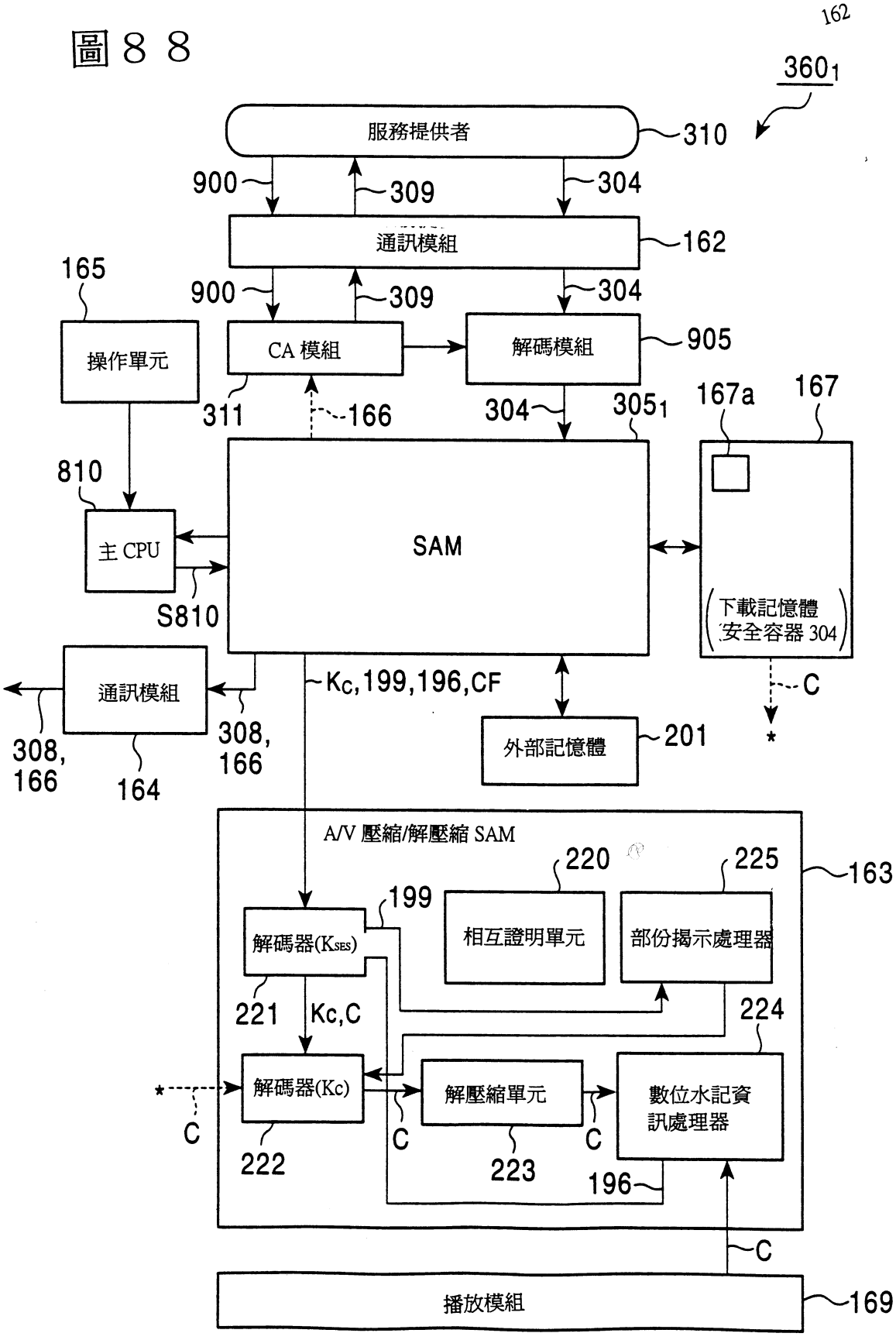

162
360₁
服務提供者
310
900
309
304
通訊模組
162
165
900
309
304
操作單元
CA 模組
解碼模組
905
311
166
304
305₁
167a
167
810
主 CPU
SAM
S810
下載記憶體
安全容器 304
C
Kc,199,196,CF
通訊模組
308,
166
308,
166
164
外部記憶體
201
A/V 壓縮/解壓縮 SAM
220
225
163
199
解碼器(Kses)
相互證明單元
部份揭示處理器
221
Kc,C
224
解碼器(Kc)
解壓縮單元
數位水記資
訊處理器
C
C
C
C
222
223
196
C
播放模組
169

圖 8 9

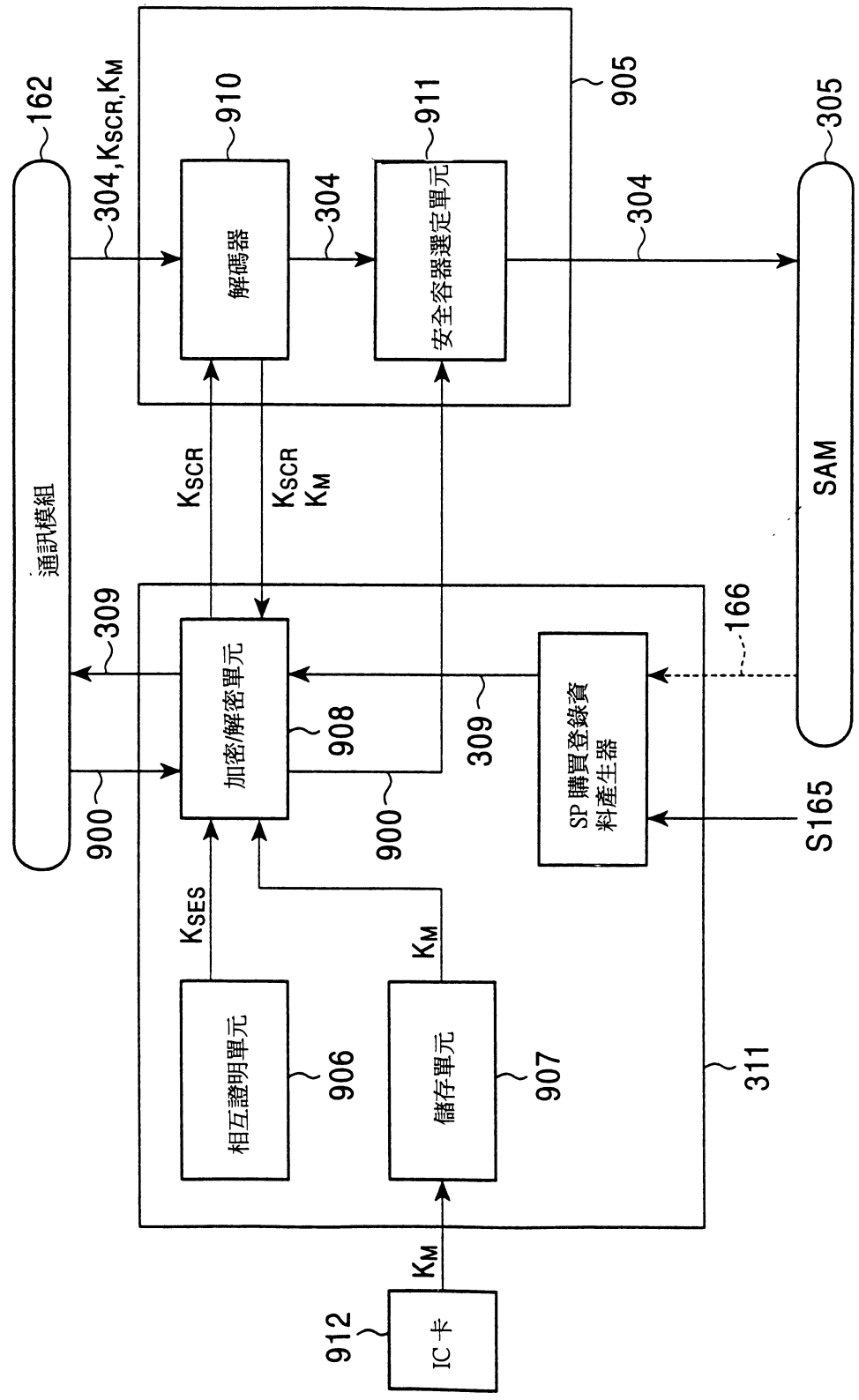

通訊模組
162
304, KSCR, KM
解碼器
910
304
安全容器選定單元
911
905
304
305
SAM
KSCR
KSCR
KM
309
加密/解密單元
908
900
900
309
166
SP 購買登錄資料產生器
S165
KSES
KM
相互證明單元
906
儲存單元
907
311
KM
IC 卡
912

圖 9 0

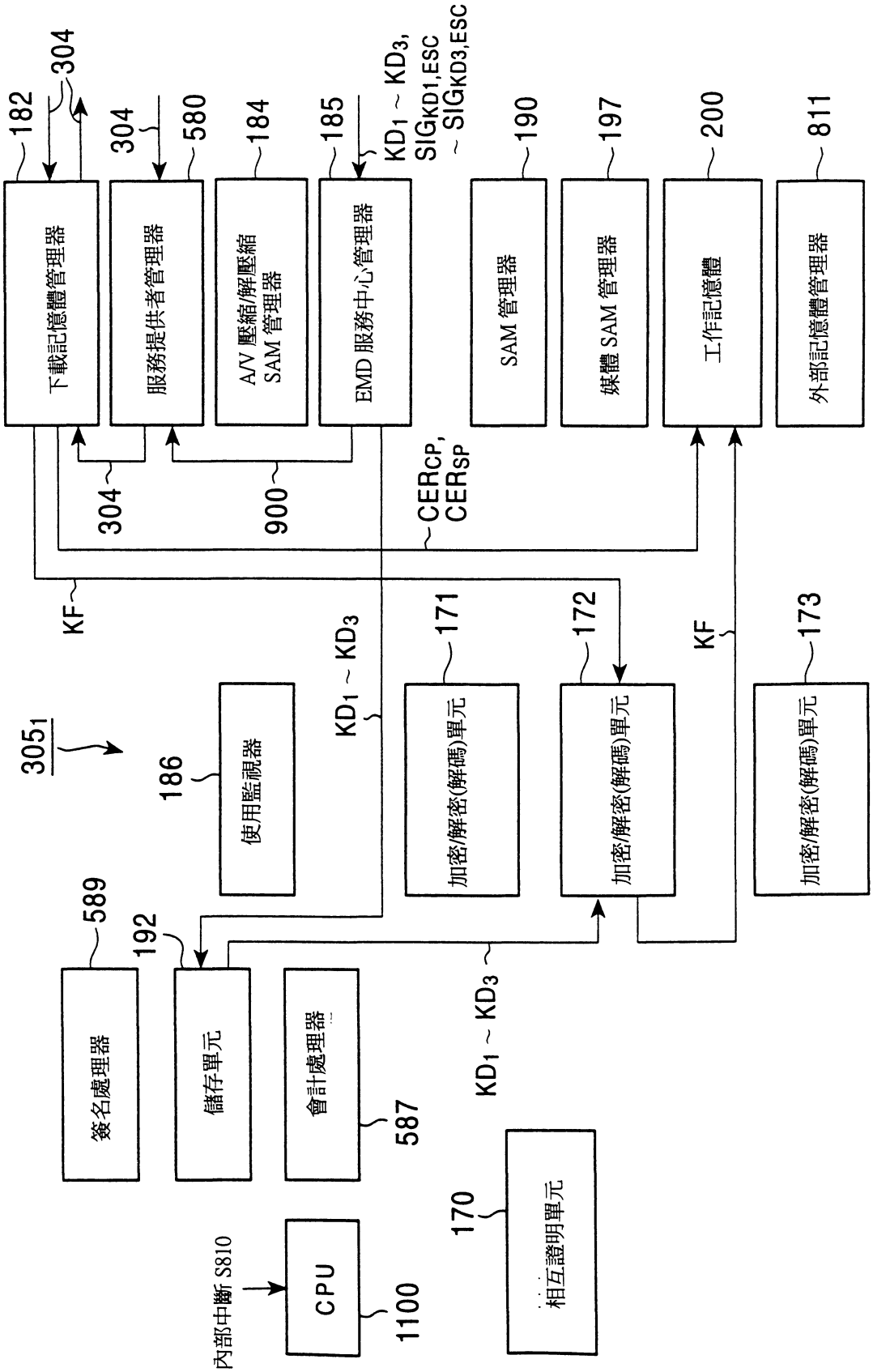

182
304
304
580
184
185
KD1 ~ KD3,
SIGKD1,ESC
~ SIGKD3,ESC
190
197
200
811
下載記憶體管理器
服務提供者管理器
A/V 壓縮/解壓縮
SAM 管理器
EMD 服務中心管理器
SAM 管理器
媒體 SAM 管理器
工作記憶體
外部記憶體管理器
304
900
CERCP,
CERSP
KF
KD1 ~ KD3
171
172
KF
173
3051
186
使用監視器
加密/解密(解碼)單元
加密/解密(解碼)單元
加密/解密(解碼)單元
589
192
簽名處理器
儲存單元
會計處理器
587
KD1 ~ KD3
內部中斷 S810
CPU
1100
170
相互證明單元

圖 9 1

內容鑰匙資料 Kc
UCP 資料 106
非依電性記憶體 210 之鎖鑰匙資料 K_{LOC}
內容提供者 301 之公開鑰匙證明資料 CER_{CP}
內容提供者 301 之公開鑰匙證明資料 CER_{SP}
UCP 資料 166
SAM 程式下載容器 SD_1~SD_3
價格標籤資料 312

圖 9 2

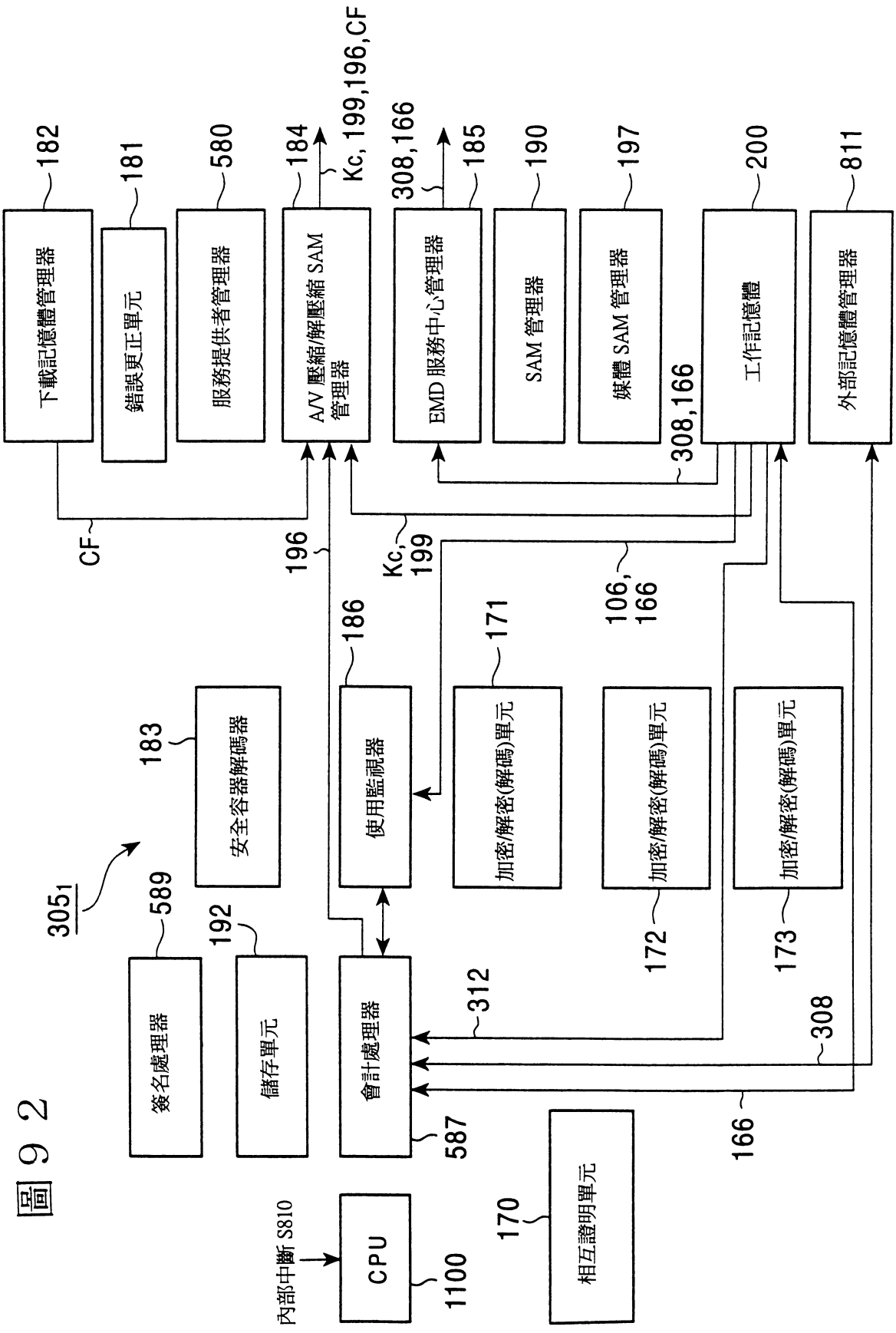

下載記憶體管理器
182
錯誤更正單元
181
服務提供者管理器
580
A/V 壓縮/解壓縮 SAM 管理器
184
Kc, 199,196,CF
EMD 服務中心管理器
308,166
185
SAM 管理器
190
媒體 SAM 管理器
197
工作記憶體
200
外部記憶體管理器
811
CF
196
Kc, 199
106, 166
308,166
簽名處理器
589
安全容器解碼器
183
使用監視器
186
加密/解密(解碼)單元
171
加密/解密(解碼)單元
172
加密/解密(解碼)單元
173
305₁
192
儲存單元
會計處理器
312
308
587
166
內部中斷 S810
CPU
1100
170
相互證明單元

圖 9 3

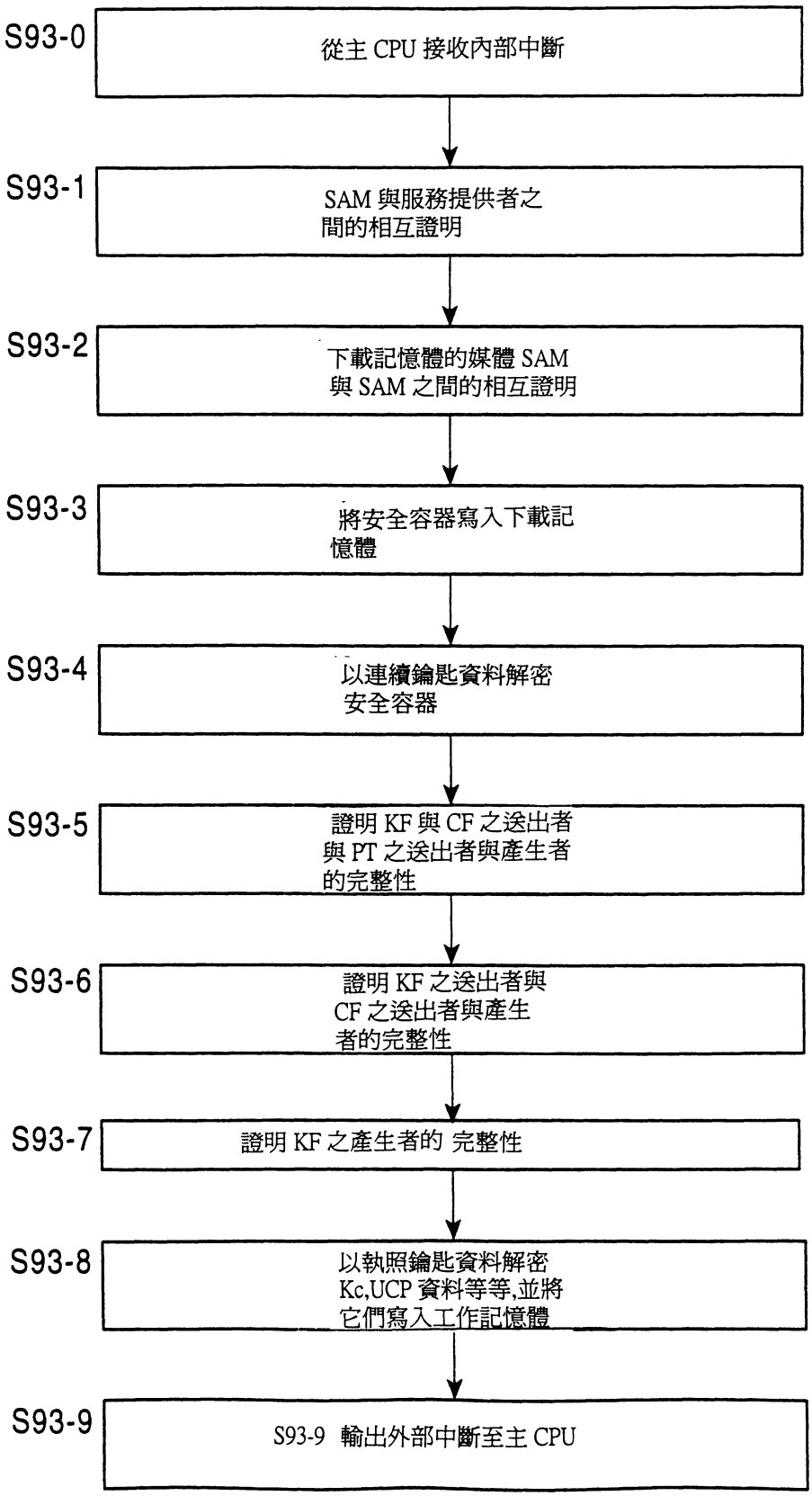

S93-0
從主 CPU 接收內部中斷
S93-1
SAM 與服務提供者之間的相互證明
S93-2
下載記憶體的媒體 SAM 與 SAM 之間的相互證明
S93-3
將安全容器寫入下載記憶體
S93-4
以連續鑰匙資料解密安全容器
S93-5
證明 KF 與 CF 之送出者與 PT 之送出者與產生者的完整性
S93-6
證明 KF 之送出者與 CF 之送出者與產生者的完整性
S93-7
證明 KF 之產生者的 完整性
S93-8
以執照鑰匙資料解密 Kc,UCP 資料等等,並將它們寫入工作記憶體
S93-9
S93-9 輸出外部中斷至主 CPU

圖 9 4

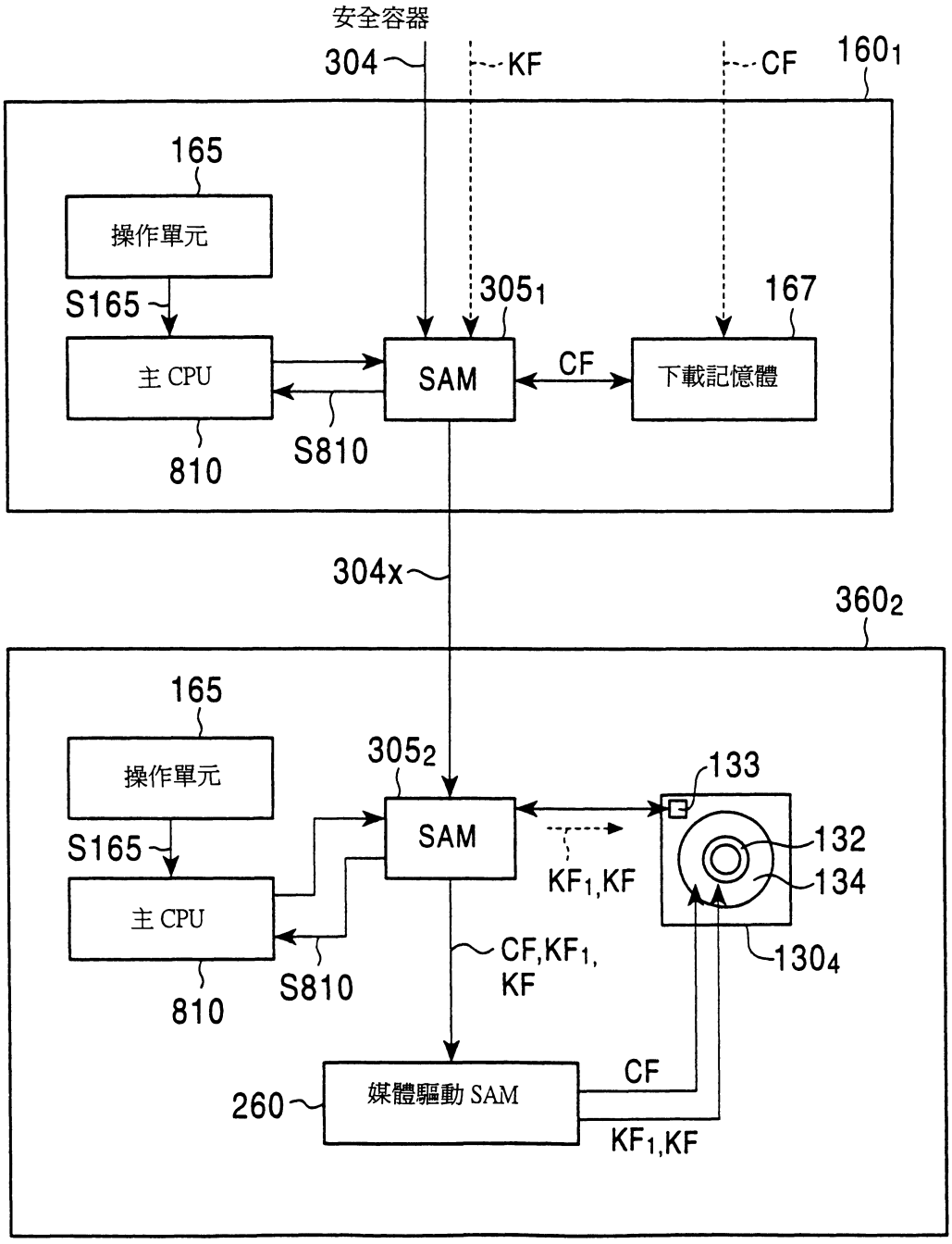

安全容器
304
KF
CF
160_1
165
操作單元
S165
305_1
167
主 CPU
SAM
CF
下載記憶體
S810
810
304x
360_2
165
操作單元
305_2
133
S165
SAM
132
KF_1,KF
134
主 CPU
CF,KF_1,
KF
130_4
S810
810
260
媒體驅動 SAM
CF
KF_1,KF

圖 9 5

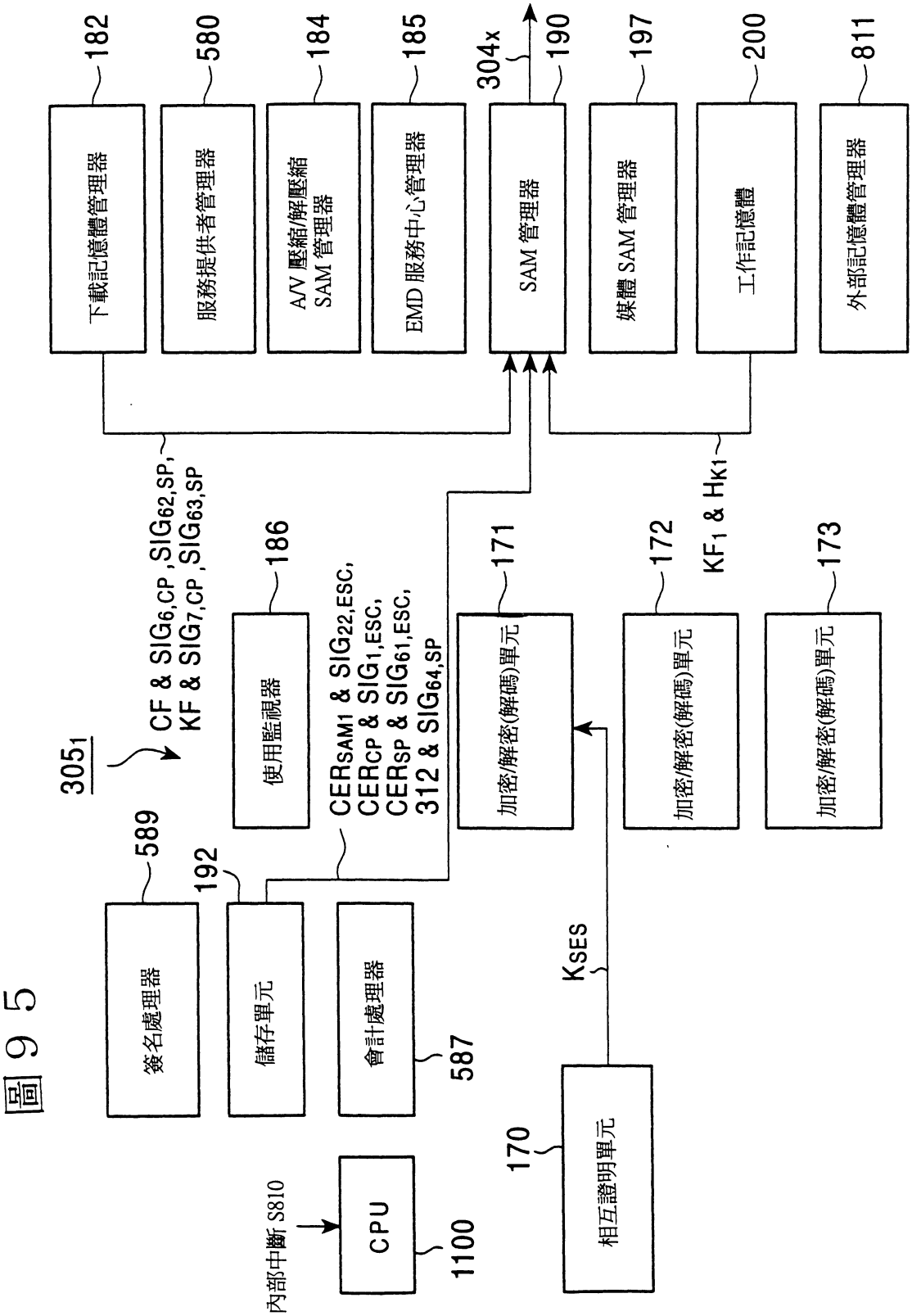

182
下載記憶體管理器
580
服務提供者管理器
184
A/V 壓縮/解壓縮 SAM 管理器
185
EMD 服務中心管理器
304x
190
SAM 管理器
197
媒體 SAM 管理器
200
工作記憶體
811
外部記憶體管理器
CF & SIG6,CP ,SIG62,SP,
KF & SIG7,CP ,SIG63,SP
3051
186
使用監視器
CERSAM1 & SIG22,ESC,
CERCP & SIG1,ESC,
CERSP & SIG61,ESC,
312 & SIG64,SP
171
加密/解密(解碼)單元
172
加密/解密(解碼)單元
KF1 & HK1
173
加密/解密(解碼)單元
589
簽名處理器
192
儲存單元
會計處理器
587
KSES
內部中斷 S810
CPU
1100
170
相互證明單元

圖 9 6

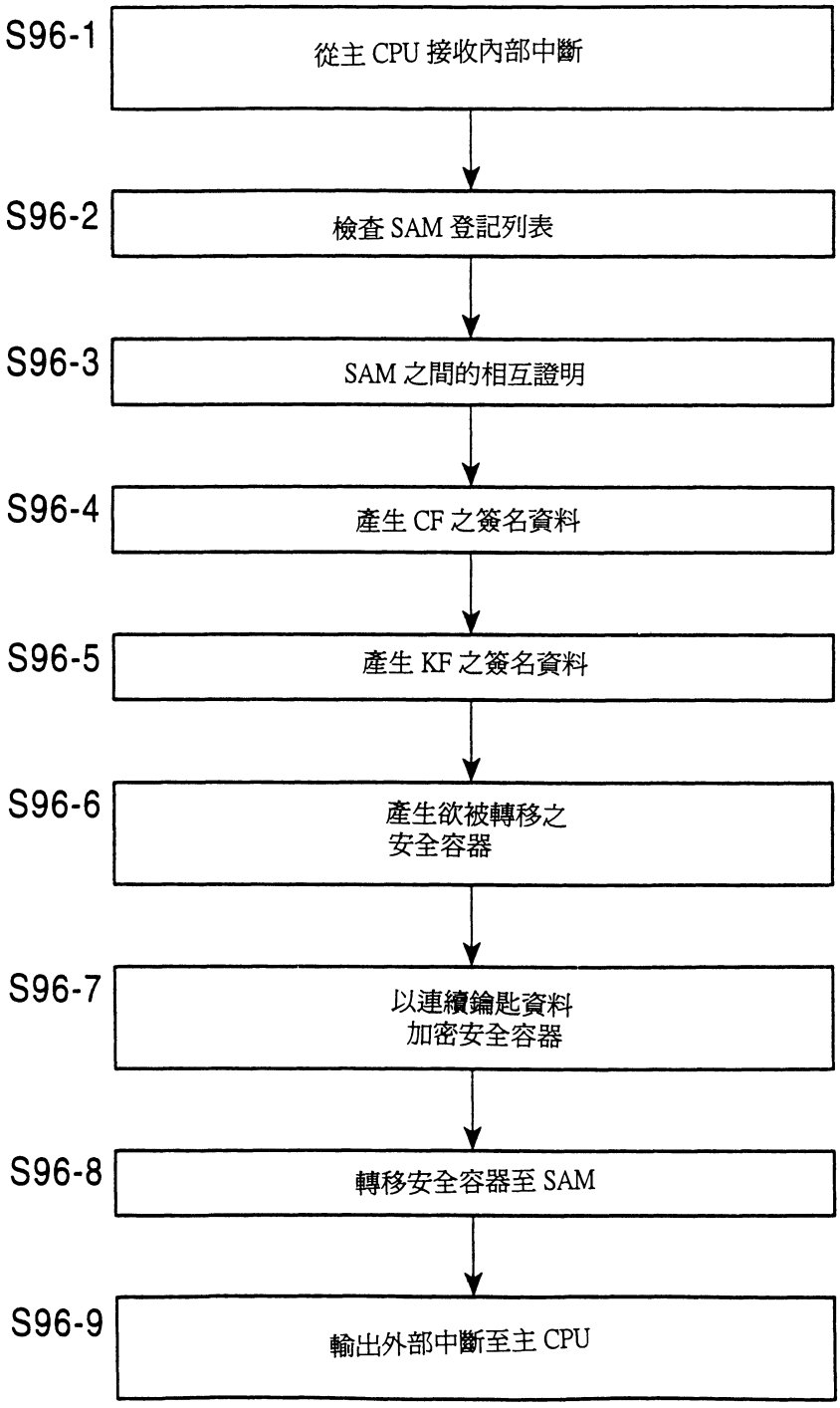

S96-1
從主 CPU 接收內部中斷
S96-2
檢查 SAM 登記列表
S96-3
SAM 之間的相互證明
S96-4
產生 CF 之簽名資料
S96-5
產生 KF 之簽名資料
S96-6
產生欲被轉移之
安全容器
S96-7
以連續鑰匙資料
加密安全容器
S96-8
轉移安全容器至 SAM
S96-9
輸出外部中斷至主 CPU

圖９７Ａ

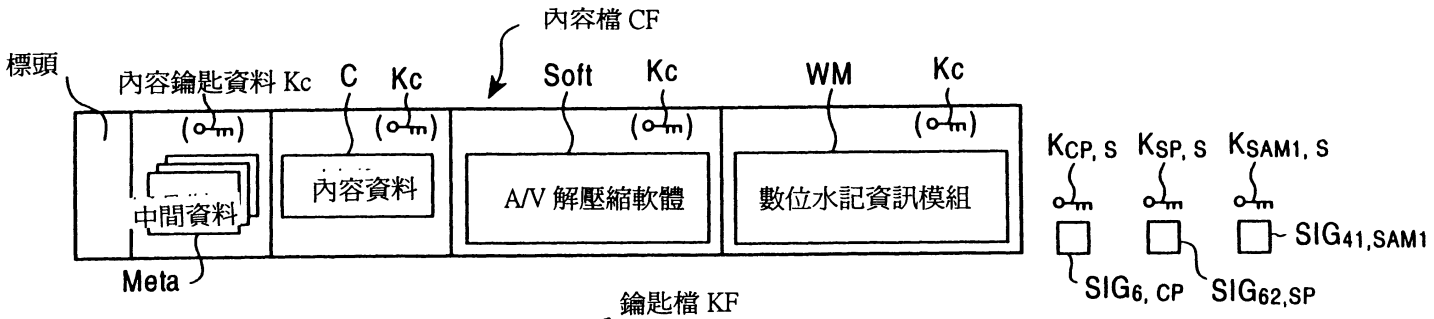


圖９７Ｂ

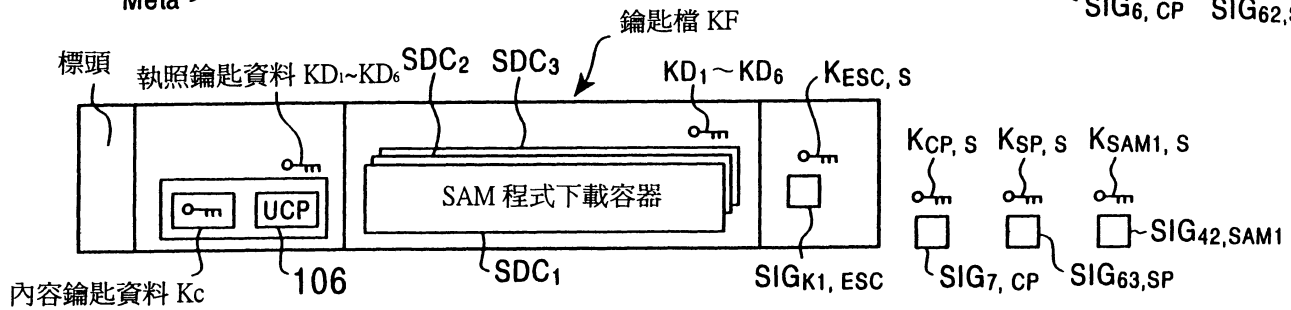


圖９７Ｃ

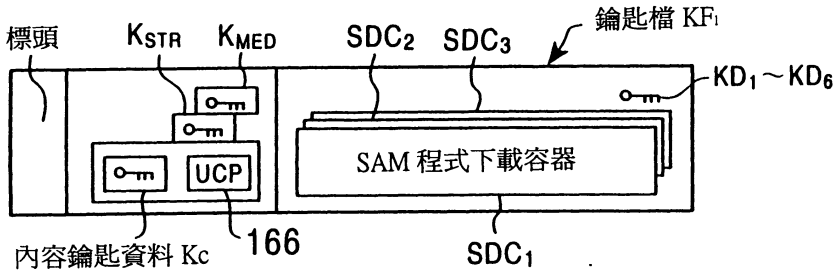


圖９７Ｄ

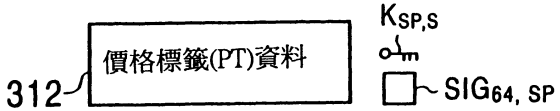


圖９７Ｅ

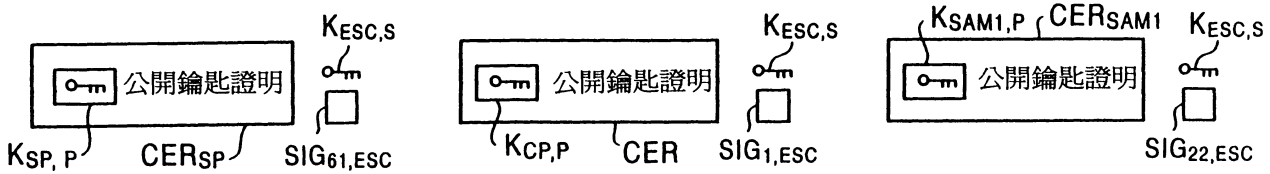


圖 9 8

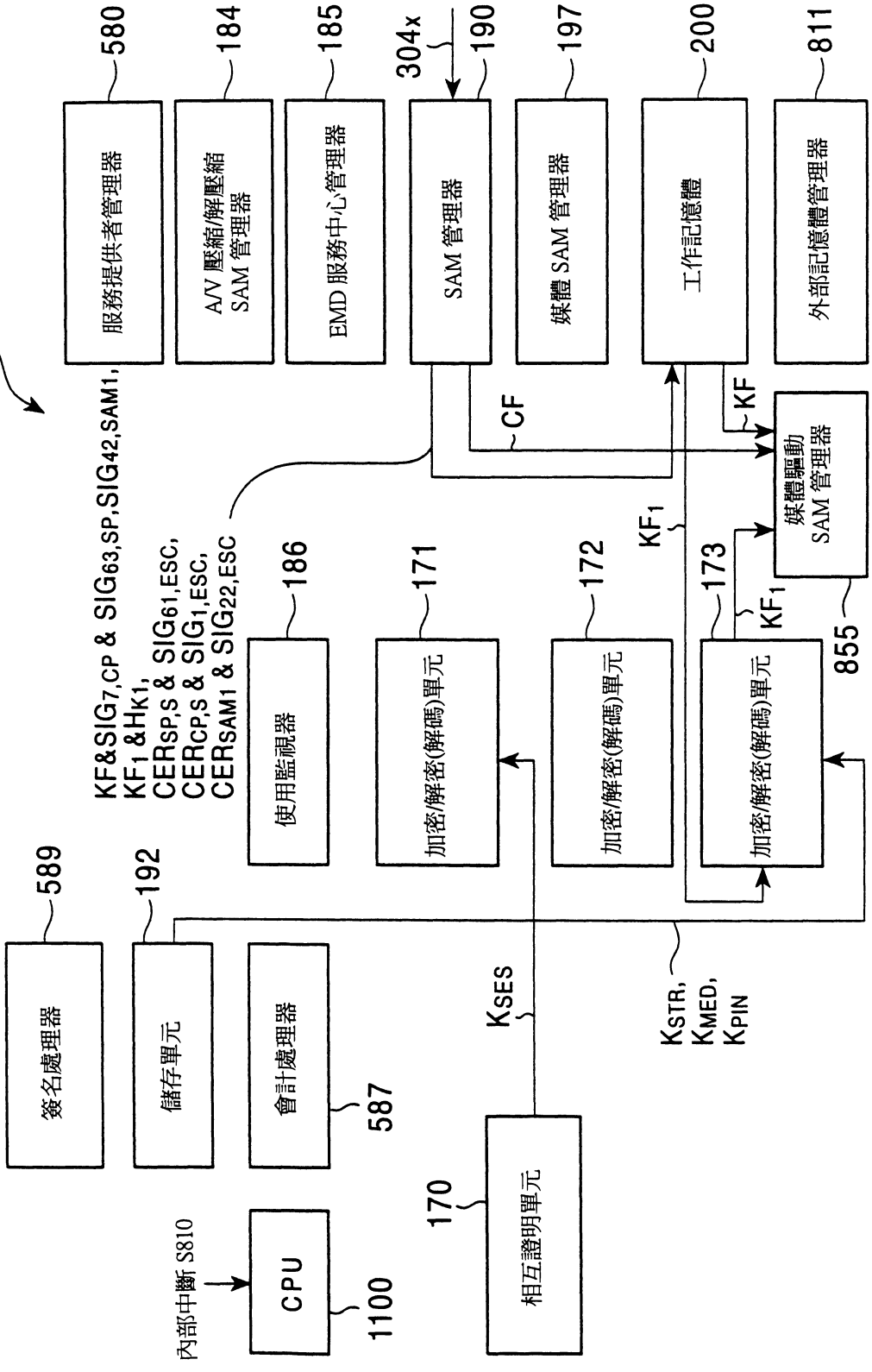

3052
KF&SIG7,CP & SIG63,SP,SIG42,SAM1,
KF1 &HK1,
CERSP,S & SIG61,ESC,
CERCP,S & SIG1,ESC,
CERSAM1 & SIG22,ESC
服務提供者管理器
580
A/V 壓縮/解壓縮
SAM 管理器
184
EMD 服務中心管理器
185
304x
SAM 管理器
190
媒體 SAM 管理器
197
工作記憶體
200
外部記憶體管理器
811
CF
KF
媒體驅動
SAM 管理器
855
KF1
KF1
使用監視器
186
加密/解密(解碼)單元
171
加密/解密(解碼)單元
172
加密/解密(解碼)單元
173
簽名處理器
589
儲存單元
192
會計處理器
587
KSES
KSTR,
KMED,
KPIN
內部中斷 S810
CPU
1100
170
相互證明單元

圖 9 9

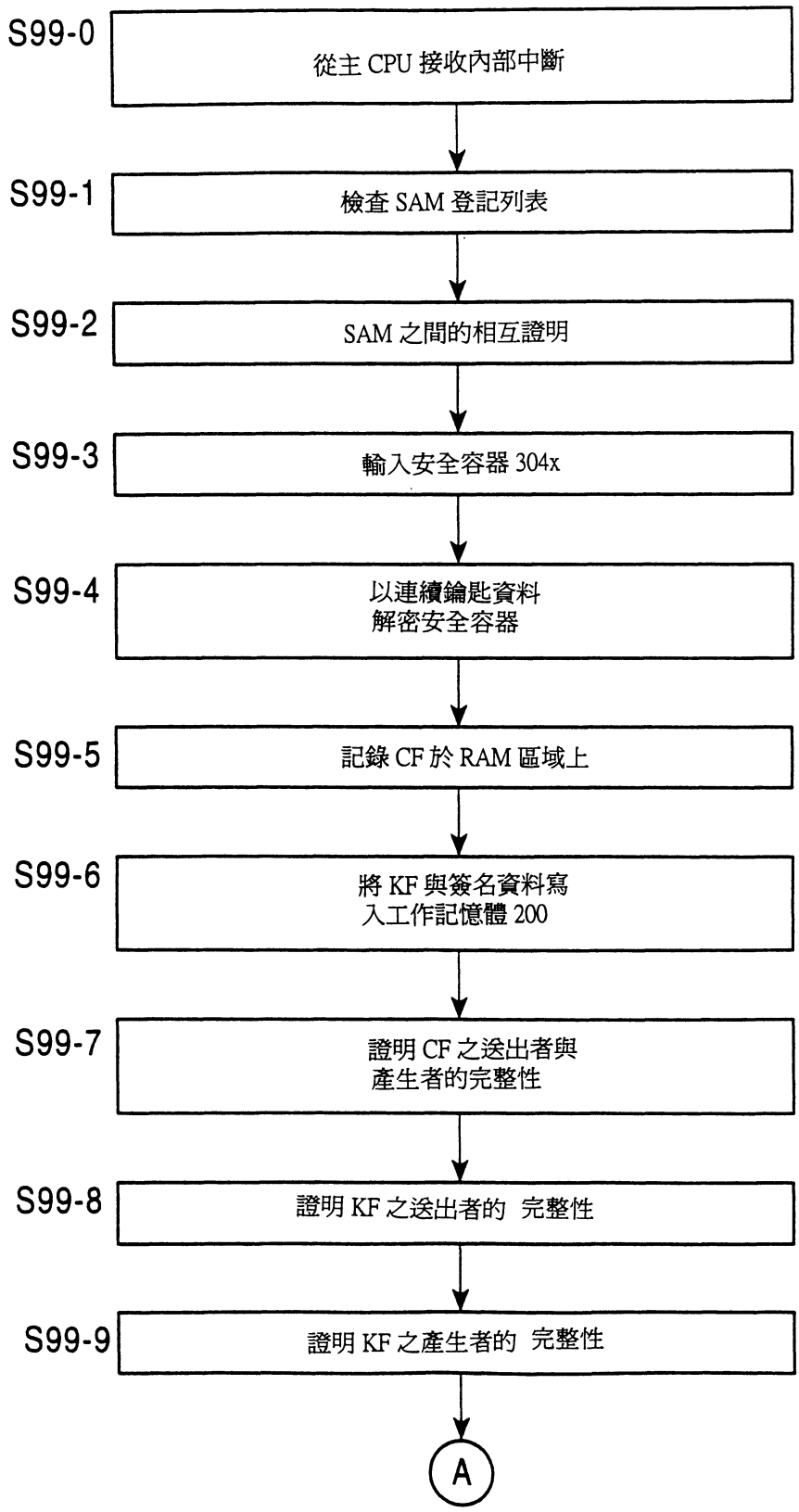

S99-0
從主 CPU 接收內部中斷
S99-1
檢查 SAM 登記列表
S99-2
SAM 之間的相互證明
S99-3
輸入安全容器 304x
S99-4
以連續鑰匙資料
解密安全容器
S99-5
記錄 CF 於 RAM 區域上
S99-6
將 KF 與簽名資料寫
入工作記憶體 200
S99-7
證明 CF 之送出者與
產生者的完整性
S99-8
證明 KF 之送出者的 完整性
S99-9
證明 KF 之產生者的 完整性
A

圖１００

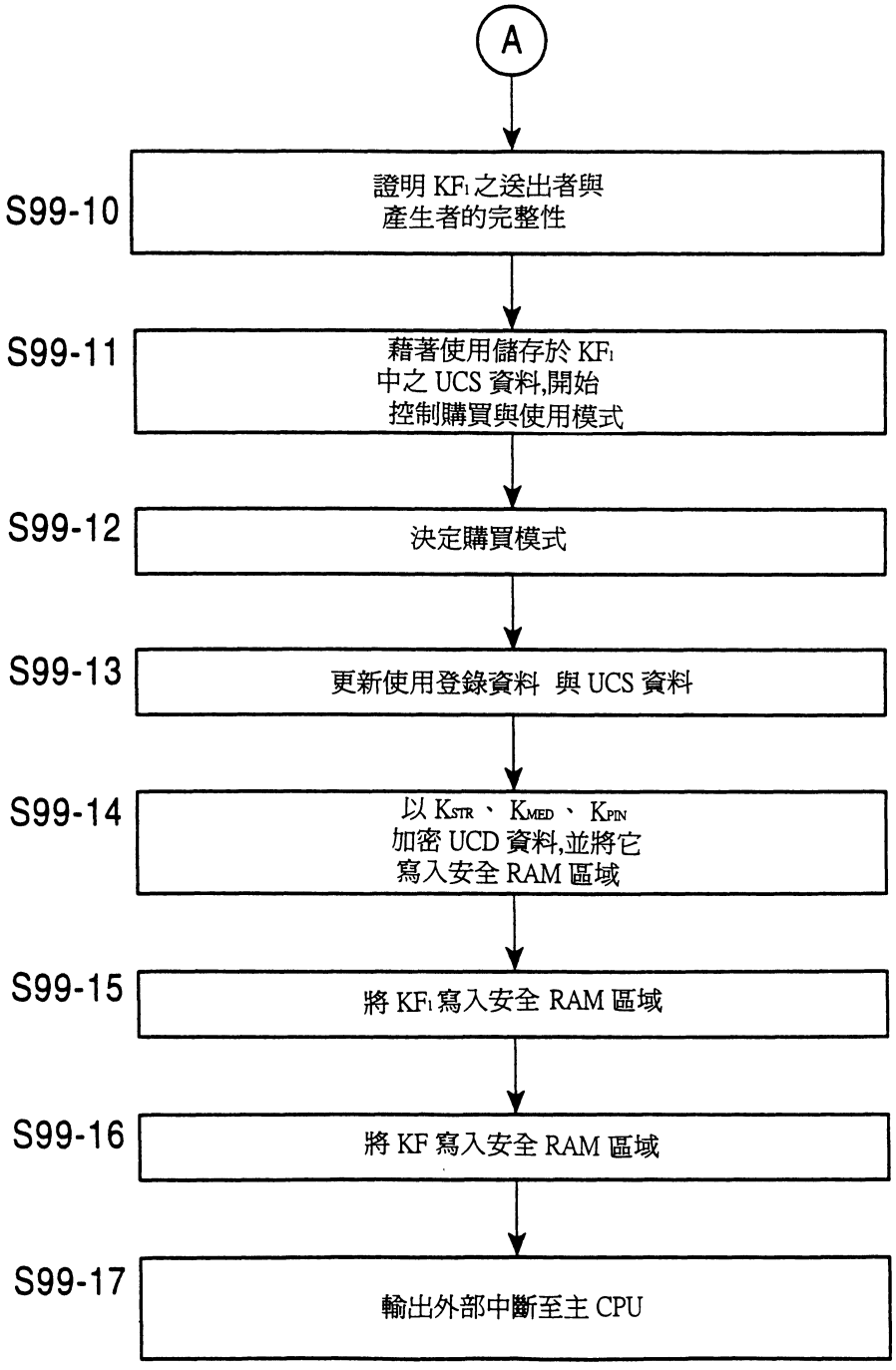

A
S99-10
證明 KF_I 之送出者與
產生者的完整性
S99-11
藉著使用儲存於 KF_I
中之 UCS 資料,開始
控制購買與使用模式
S99-12
決定購買模式
S99-13
更新使用登錄資料 與 UCS 資料
S99-14
以 K_{STR} 、 K_{MED} 、 K_{PIN}
加密 UCD 資料,並將它
寫入安全 RAM 區域
S99-15
將 KF_I 寫入安全 RAM 區域
S99-16
將 KF 寫入安全 RAM 區域
S99-17
輸出外部中斷至主 CPU

圖 1 0 1

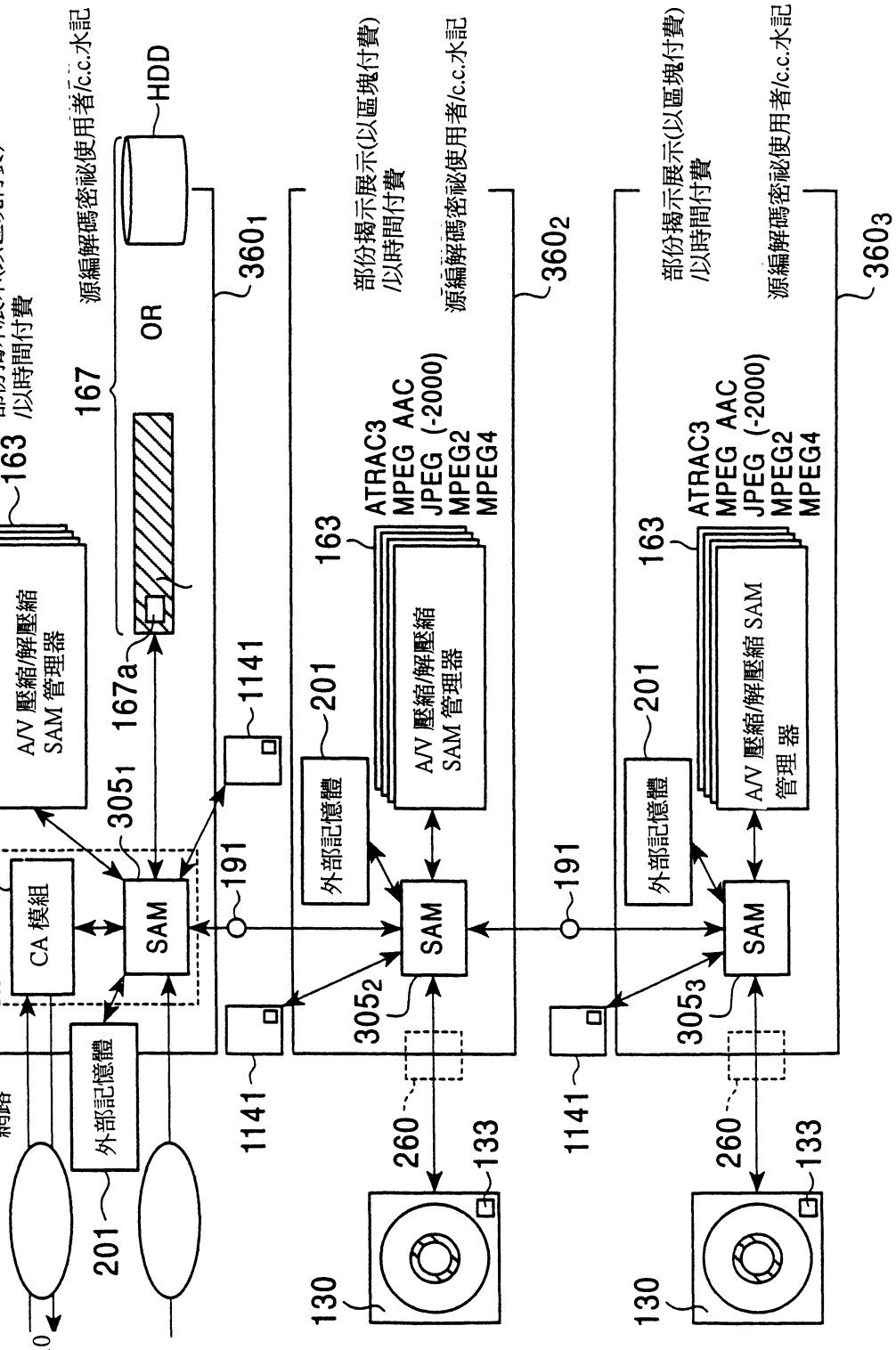

303
網路
服務提供者 310
311
CA 模組
外部記憶體
201
SAM
305_1
167a
167
OR
HDD
源編解碼密祕使用者/c.c.水記
部份揭示展示(以區塊付費)
/以時間付費
163
A/V 壓縮/解壓縮
SAM 管理器
191
1141
360_1
360_2
360_3
外部記憶體
305_2
305_3
ATRAC3
MPEG AAC
JPEG (-2000)
MPEG2
MPEG4
260
133
130

圖１０２

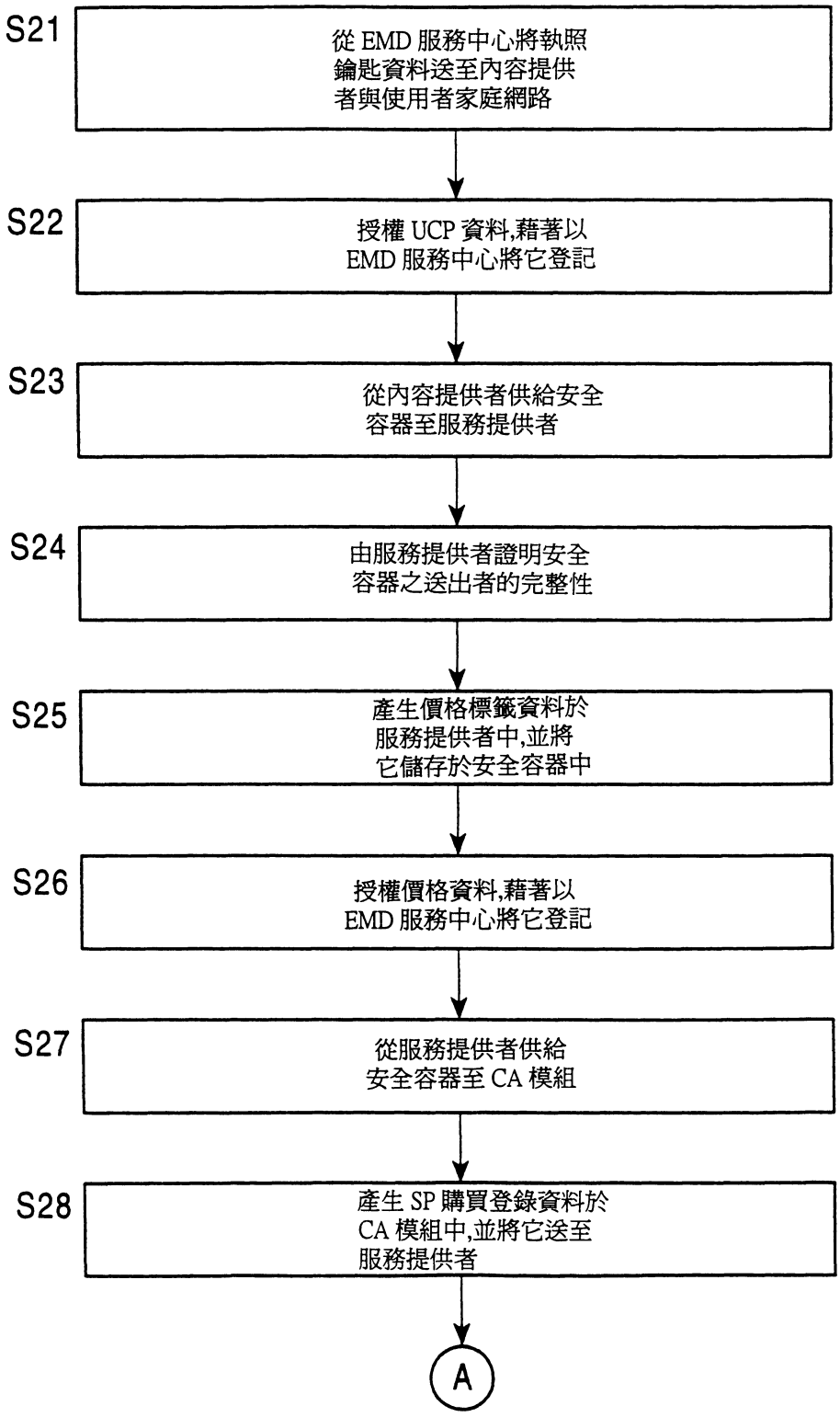

S21
從 EMD 服務中心將執照
鑰匙資料送至內容提供
者與使用者家庭網路
S22
授權 UCP 資料,藉著以
EMD 服務中心將它登記
S23
從內容提供者供給安全
容器至服務提供者
S24
由服務提供者證明安全
容器之送出者的完整性
S25
產生價格標籤資料於
服務提供者中,並將
它儲存於安全容器中
S26
授權價格資料,藉著以
EMD 服務中心將它登記
S27
從服務提供者供給
安全容器至 CA 模組
S28
產生 SP 購買登錄資料於
CA 模組中,並將它送至
服務提供者
A

圖１０３

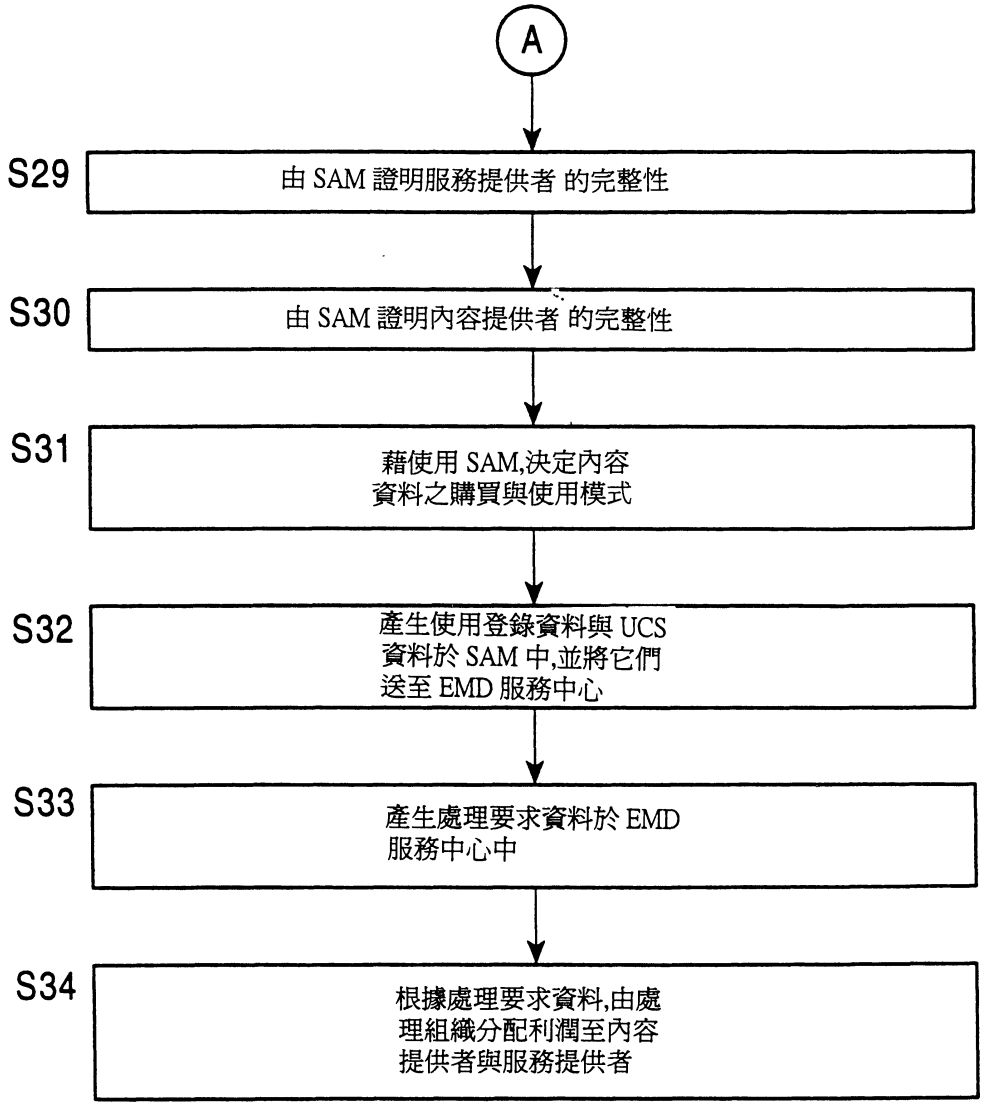

A
S29
由 SAM 證明服務提供者 的完整性
S30
由 SAM 證明內容提供者 的完整性
S31
藉使用 SAM,決定內容
資料之購買與使用模式
S32
產生使用登錄資料與 UCS
資料於 SAM 中,並將它們
送至 EMD 服務中心
S33
產生處理要求資料於 EMD
服務中心中
S34
根據處理要求資料,由處
理組織分配利潤至內容
提供者與服務提供者

圖 1 0 4

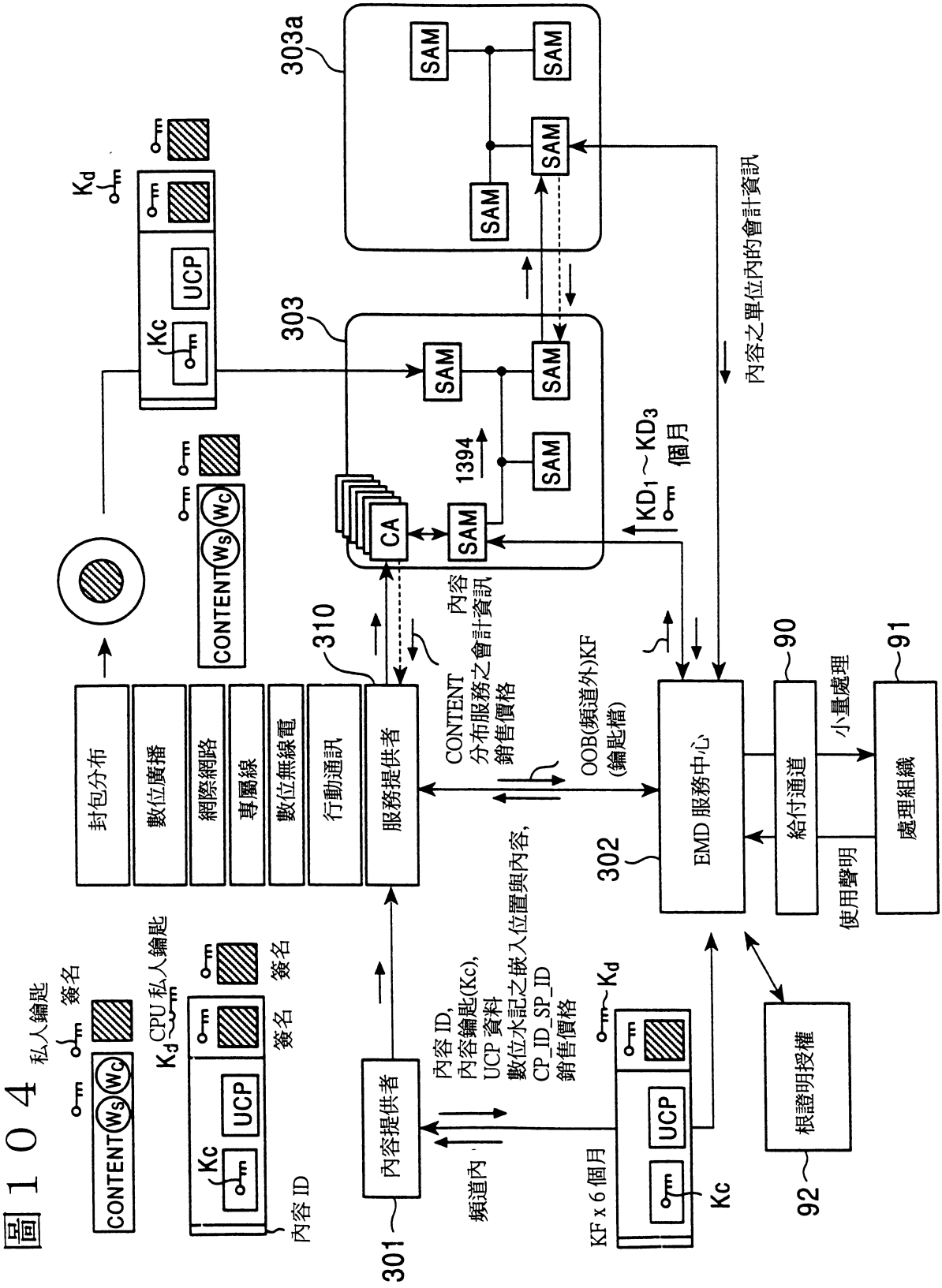

私人鑰匙
簽名
CONTENT Ws Wc
CPU 私人鑰匙
Kd
Kc
UCP
簽名
內容 ID
301
內容提供者
頻道內
內容 ID,
內容鑰匙(Kc),
UCP 資料
數位水記之嵌入位置與內容,
CP_ID_SP_ID
銷售價格
KF x 6 個月
Kd
Kc
UCP
封包分布
數位廣播
網際網路
專屬線
數位無線電
行動通訊
服務提供者
310
CONTENT
分布服務之會計資訊
銷售價格
內容
會計資訊
OOB(頻道外)KF
(鑰匙檔)
302
EMD 服務中心
90
給付通道
小量處理
使用聲明
91
處理組織
92
根證明授權
303
303a
SAM
CA
1394
KD1～KD3
個月
內容之單位內的會計資訊

圖 1 0 5

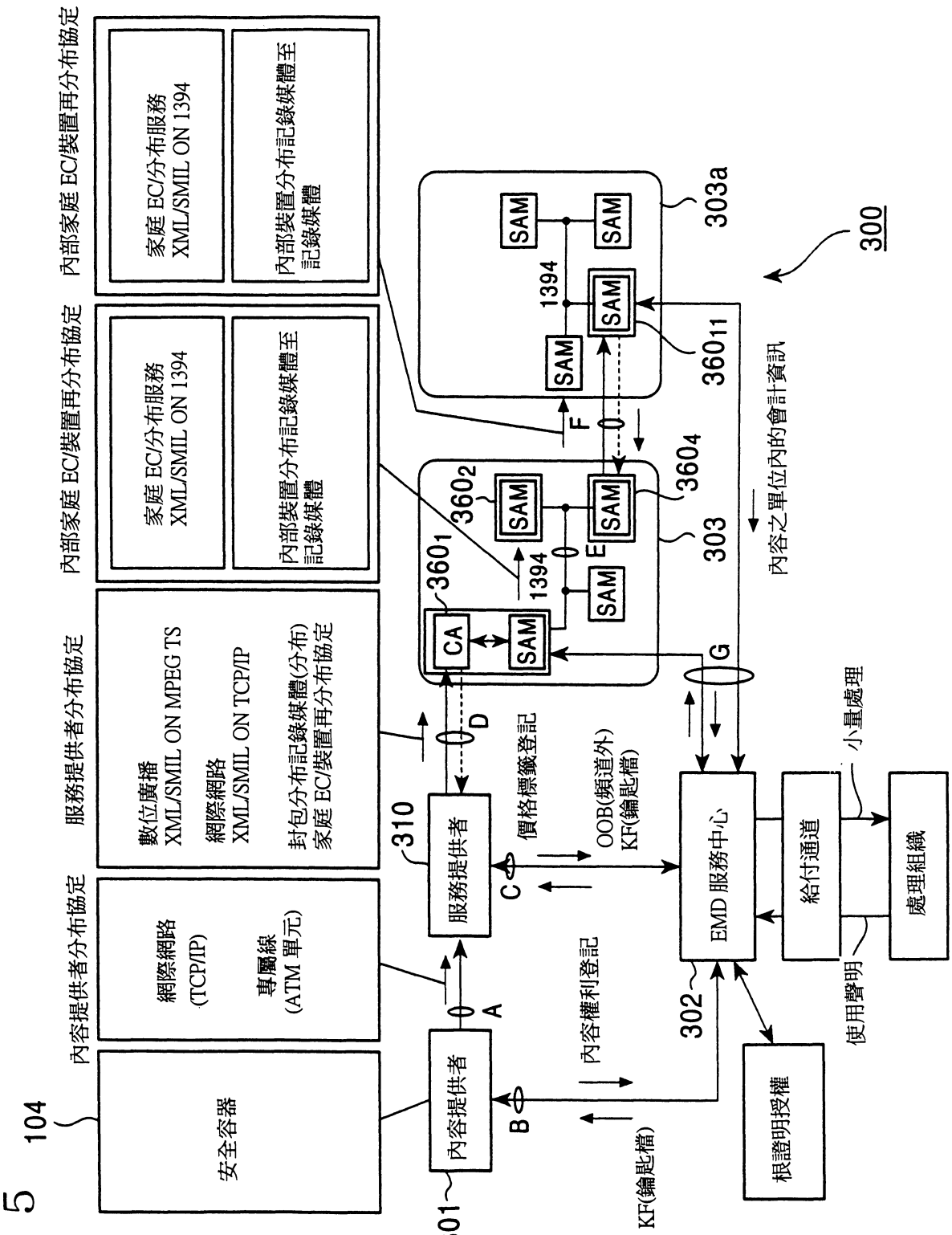
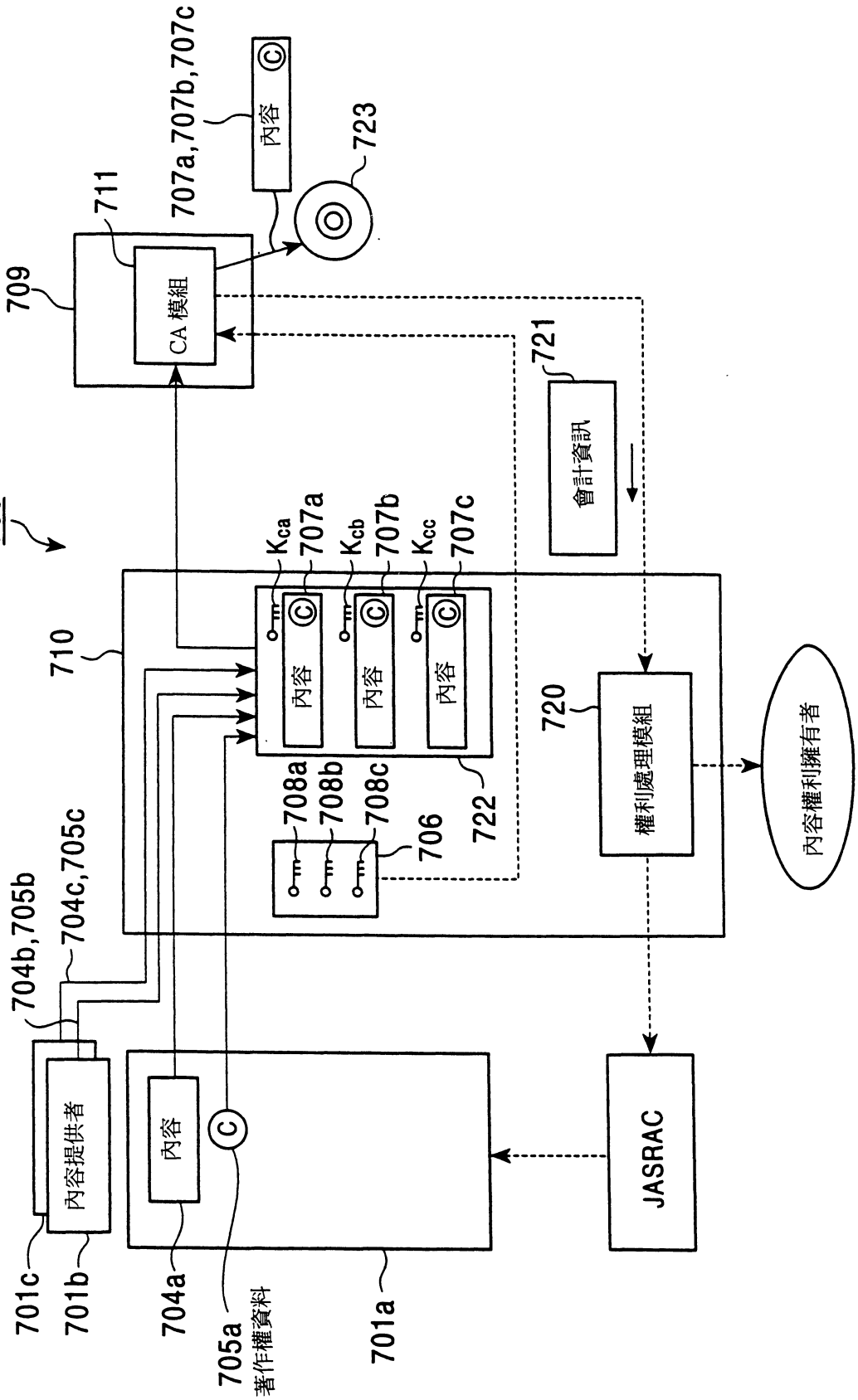

內容提供者分布協定
服務提供者分布協定
內部家庭 EC/裝置再分布協定
內部家庭 EC/裝置再分布協定
104
安全容器
網際網路
(TCP/IP)
專屬線
(ATM 單元)
數位廣播
XML/SMIL ON MPEG TS
網際網路
XML/SMIL ON TCP/IP
封包分布記錄媒體(分布)
家庭 EC/裝置再分布協定
家庭 EC/分布服務
XML/SMIL ON 1394
內部裝置分布記錄媒體至
記錄媒體
家庭 EC/分布服務
XML/SMIL ON 1394
內部裝置分布記錄媒體至
記錄媒體
300
303a
303
360_1
360_2
360_4
360_{11}
SAM
CA
1394
內容之單位內的會計資訊
內容提供者
301
服務提供者
310
A
B
C
D
E
F
G
內容權利登記
價格標籤登記
OOB(頻道外)
KF(鑰匙檔)
頻道內 KF(鑰匙檔)
EMD 服務中心
302
給付通道
小量處理
處理組織
使用聲明
根證明授權

圖１０６


700
701a
701b
701c
704a
704b,705b
704c,705c
705a
著作權資料
706
707a,707b,707c
707a
707b
707c
708a
708b
708c
709
710
711
720
721
722
723
K_{ca}
K_{cb}
K_{cc}
內容
內容提供者
CA 模組
會計資訊
權利處理模組
JASRAC
內容權利擁有者