(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201335782 A1
(43)公開日： 中華民國 102 (2013) 年 09 月 01 日

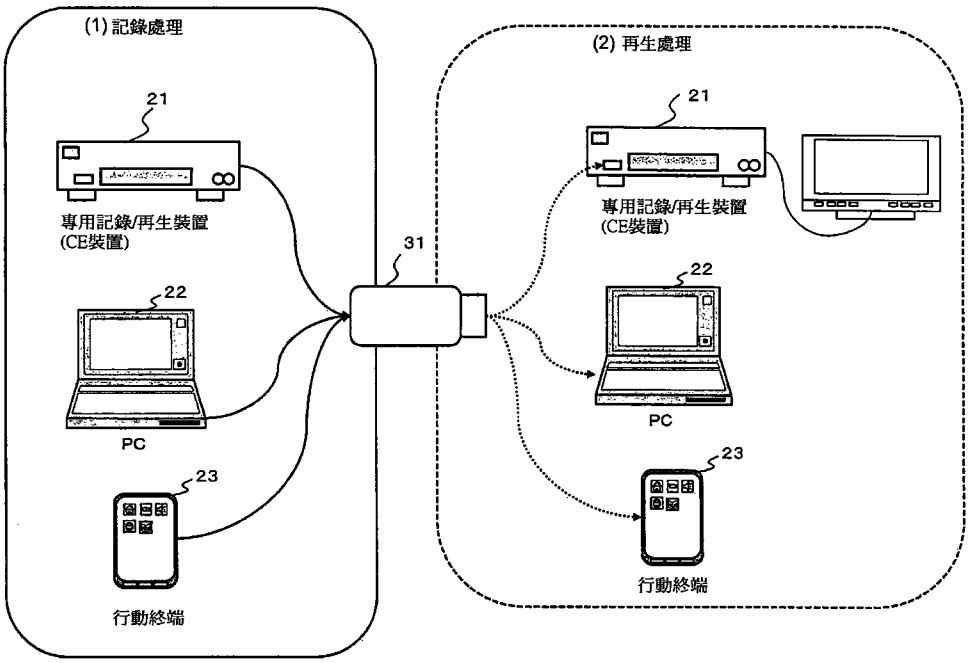
(21)申請案號：101141347 (22)申請日： 中華民國 101 (2012) 年 11 月 07 日
(51)Int. Cl.： *G06F21/10 (2013.01)* *G06F21/62 (2013.01)*
(30)優先權：2011/11/17 日本 2011-251735
(71)申請人：新力股份有限公司 (日本) SONY CORPORATION (JP)
日本
(72)發明人：小林義行 KOBAYASHI, YOSHIYUKI (JP) ；久野浩 KUNO, HIROSHI (JP) ；林隆道 HAYASHI, TAKAMICHI (JP)
(74)代理人：林志剛
申請實體審查：有 申請專利範圍項數：13 項 圖式數：35 共 152 頁

(54)名稱

資訊處理裝置，資訊儲存裝置，資訊處理系統，資訊處理方法及程式
INFORMATION PROCESSING APPARATUS, INFORMATION STORAGE APPARATUS, INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND PROGRAM

(57)摘要

資訊儲存裝置包括儲存單元，該儲存單元被組構成儲存加密內容及欲待應用到該加密內容的解密之加密金鑰，該儲存單元包括：受保護區，在該受保護區中，儲存轉換的加密金鑰及設定存取限制，該轉換的加密金鑰為經由該加密金鑰之轉換所取得的資料項目；以及通用區，其儲存該加密內容及對應於該加密內容所設定之加密內容簽名檔案，該加密內容簽名檔案包含指示在該受保護區的區域中哪一個允許該轉換的加密金鑰之儲存的區塊識別符作為記錄資料項目，以允許再生裝置能夠執行應用該區塊識別符之內容再生可能性判斷，該再生裝置被組構成從該儲存單元讀取該加密內容及執行再生處理。



21：專用記錄/再生裝置
22：個人電腦
23：行動終端
31：記憶卡

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201335782 A1
(43)公開日： 中華民國 102 (2013) 年 09 月 01 日

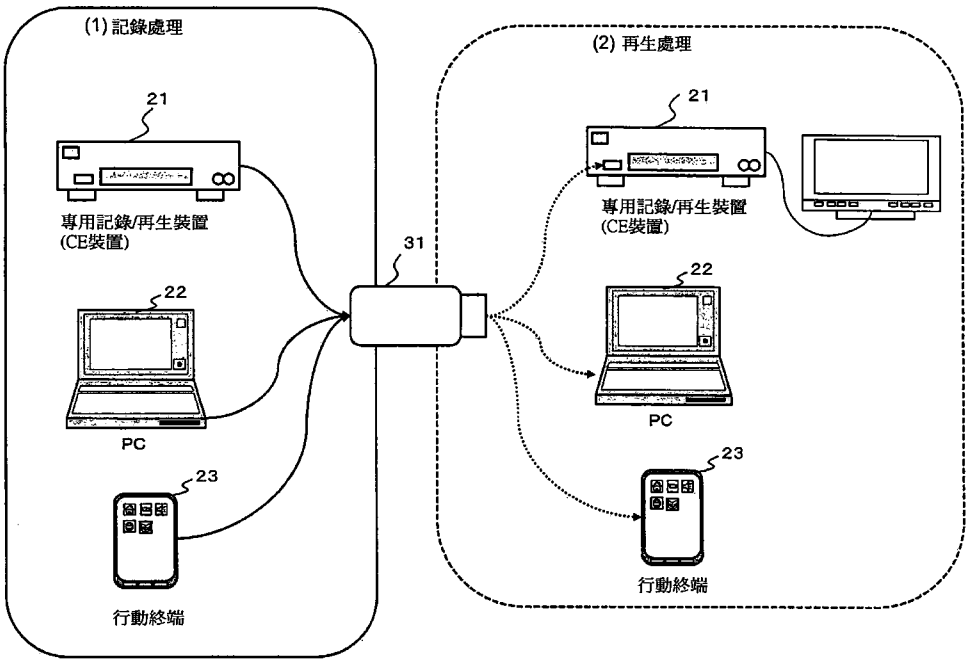
(21)申請案號：101141347 (22)申請日： 中華民國 101 (2012) 年 11 月 07 日
(51)Int. Cl.： *G06F21/10 (2013.01)* *G06F21/62 (2013.01)*
(30)優先權：2011/11/17 日本 2011-251735
(71)申請人：新力股份有限公司 (日本) SONY CORPORATION (JP)
日本
(72)發明人：小林義行 KOBAYASHI, YOSHIYUKI (JP) ；久野浩 KUNO, HIROSHI (JP) ；林隆道 HAYASHI, TAKAMICHI (JP)
(74)代理人：林志剛
申請實體審查：有 申請專利範圍項數：13 項 圖式數：35 共 152 頁

(54)名稱

資訊處理裝置，資訊儲存裝置，資訊處理系統，資訊處理方法及程式
INFORMATION PROCESSING APPARATUS, INFORMATION STORAGE APPARATUS, INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND PROGRAM

(57)摘要

資訊儲存裝置包括儲存單元，該儲存單元被組構成儲存加密內容及欲待應用到該加密內容的解密之加密金鑰，該儲存單元包括：受保護區，在該受保護區中，儲存轉換的加密金鑰及設定存取限制，該轉換的加密金鑰為經由該加密金鑰之轉換所取得的資料項目；以及通用區，其儲存該加密內容及對應於該加密內容所設定之加密內容簽名檔案，該加密內容簽名檔案包含指示在該受保護區的區域中哪一個允許該轉換的加密金鑰之儲存的區塊識別符作為記錄資料項目，以允許再生裝置能夠執行應用該區塊識別符之內容再生可能性判斷，該再生裝置被組構成從該儲存單元讀取該加密內容及執行再生處理。



21：專用記錄/再生裝置
22：個人電腦
23：行動終端
31：記憶卡

發明專利說明書

（本申請書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：101141347

※申請日：101 年 11 月 07 日　　**※IPC 分類：** G06F 21/10 (2006.01)
G06F 21/62 (2006.01)

一、發明名稱：（中文／英文）

資訊處理裝置，資訊儲存裝置，資訊處理系統，資訊處理方法及程式

Information processing apparatus, information storage apparatus, information processing system, information processing method, and program

二、中文發明摘要：

資訊儲存裝置包括儲存單元，該儲存單元被組構成儲存加密內容及欲待應用到該加密內容的解密之加密金鑰，該儲存單元包括：受保護區，在該受保護區中，儲存轉換的加密金鑰及設定存取限制，該轉換的加密金鑰爲經由該加密金鑰之轉換所取得的資料項目；以及通用區，其儲存該加密內容及對應於該加密內容所設定之加密內容簽名檔案，該加密內容簽名檔案包含指示在該受保護區的區域中哪一個允許該轉換的加密金鑰之儲存的區塊識別符作爲記錄資料項目，以允許再生裝置能夠執行應用該區塊識別符之內容再生可能性判斷，該再生裝置被組構成從該儲存單元讀取該加密內容及執行再生處理。

三、英文發明摘要：

An information storage apparatus includes a storage unit configured to store an encrypted content and an encryption key to be applied to decryption of the encrypted content, the storage unit including a protected area in which a converted encryption key is stored and to which access restrictions are set, the converted encryption key being a data item acquired through conversion of the encryption key, and a general purpose area storing the encrypted content and an encrypted content signature file set correspondingly to the encrypted content, the encrypted content signature file containing, as a recorded data item, a block identifier indicating in which of areas in the protected area storage of the converted encryption key is permitted, to permit a reproducing apparatus to execute content reproduction possibility judgment applying the block identifier, the reproducing apparatus being configured to read the encrypted content from the storage unit and execute a reproducing process.

四、指定代表圖：

（一）本案指定代表圖為：第（2）圖。

（二）本代表圖之元件符號簡單說明：

21：專用記錄/再生裝置

22：個人電腦

23：行動終端

31：記憶卡

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無

六、發明說明：

【發明所屬之技術領域】

本揭示係相關於資訊處理裝置，資訊儲存裝置，資訊處理系統，資訊處理方法及程式。尤其是，本揭示係相關於用以防止內容的詐騙使用之資訊處理裝置，資訊儲存裝置，資訊處理系統，資訊處理方法及程式。

【先前技術】

諸如電影及音樂作品等內容係透過諸如 DVD(數位多用途碟)、藍光碟(商標)、及快閃記憶體等各種媒體，諸如網際網路等網路，或廣播提供給使用者。使用者可藉由使用諸如 PC、行動終端、BD 播放器等記錄/再生裝置、或諸如電視等各種資訊處理裝置來再生此種內容。

然而，諸如音樂資料項目及影像資料項目等欲提供給使用者之許多內容的著作權、散佈權等等係由創作者或販售者所擁有。如此，在許多事例中，此種內容的提供商在提供內容給使用者時於內容上設定預定的使用限制。

藉由使用數位記錄裝置及數位記錄媒體，例如影像及聲音可被重複記錄及再生卻不會劣化。如此，已有非法拷貝內容的散佈及使用之問題，尤其是，透過網際網路散佈非法拷貝內容，此種散佈被稱作盜版碟。

爲了防止此種非法資料拷貝，針對數位記錄裝置及數位記錄媒體防止非法拷貝的各種技術已付諸實行。

作爲此種技術的例子，具有內容加密處理，其將加密

資料項目的解密之金鑰只給予具有內容使用權的許可之再生裝置。許可給予所指定的再生裝置，以遵循預定操作規定，諸如禁止非法拷貝的規定等。如此，未曾給予許可之其他再生裝置未具有加密資料項目的解密之金鑰，因此無法解密加密資料項目。

然而，甚至當執行此種內容加密時，仍被詐騙使用內容。

此處，說明內容的詐騙使用之例子。

在此例中，假設內容伺服器散佈加密內容給諸如記錄/再生裝置、PC、及行動終端等使用者裝置之組態。

當散佈加密內容給使用者裝置時，內容伺服器例如透過網路散佈下面資料項目給使用者裝置。

(a)加密內容

(b)加密內容的加密及解密之加密金鑰。

當散佈諸如相同電影等相同內容給大量使用者裝置時，內容伺服器執行例如下面兩處理的任一者。

(A)經由個別不同加密金鑰的應用來產生不同加密內容，及分別將不同加密內容提供給使用者裝置。

(B)產生以相同加密金鑰所加密的相同加密內容，及將相同加密內容提供給複數個使用者裝置的每一個。

考量防止內容的詐騙使用之安全性，上述處理(A)是有利的。

然而，爲了執行上述處理(A)，必須執行分別設定個別加密金鑰給大量使用者及產生個別加密內容之處理。結

果，產生有問題如下：與接收內容的使用者數目成比例，由於例如加密金鑰的產生及管理以及產生加密內容的處理，使得伺服器的處理負載變得更大。

如此，在許多事例中，執行上述處理(B)，換言之，藉由以相同加密金鑰的加密來產生相同內容的相同加密內容以及將相同加密內容提供給複數個使用者的每一個之處理。

例如，一加密金鑰(換言之，標題金鑰)係設定有關具有某些標題的內容，及經由一加密金鑰的應用來產生相同加密內容。然後，下面資料組被散佈給大量使用者的每一個。

(a)加密內容

(b)標題金鑰

此種處理降低內容伺服器的處理負載。

需注意的是，在下面說明中，以內容的標題爲單位所設定之加密金鑰被定義作“標題金鑰”。

需注意的是，標題金鑰係應用到對應於標題之加密及解密加密內容的處理。

然而，當以此方式將相同資料組(換言之，下面資料項目的相同組合：(a)加密內容；以及(b)標題金鑰)散佈給大量使用者時，一些“未授權使用者”可能執行下面處理。

尤其是，執行詐騙如下。

(1)“未授權使用者”讀取接收自伺服器的標題金鑰，及將所讀取的標題金鑰暴露給未指定數目的使用者。

另一選擇是，(2)“未授權使用者”使用對應於某加密內容 A 的標題金鑰 A，以便加密全然不同的內容 B，及散佈下面資料組合給未指定數目的使用者。

(X)標題金鑰 A

(Y)以標題金鑰 A 所加密之加密內容 B。

例如，在執行上述處理(1)之事例中，已取得非法暴露的標題金鑰之大量使用者詐騙地使用以與非法暴露的標題金鑰相同之標題金鑰所加密的內容。

另外，在執行上述處理(2)之事例中，當大量使用者從上述“未授權使用者”取得由“未授權使用者”所產生之非法資料組(換言之，(X)標題金鑰 A，以及(Y)以標題金鑰 A 所加密之加密內容 B)時，加密內容 B 被非法使用。

結果，較少使用者合法購買原有合法資料組(換言之，加密內容 B，以及對應於加密內容 B 之標題金鑰 B)，及著作權擁有人及散佈權擁有人的獲利明顯地損失。

另外，說明詐騙處理的特定例子。

在此特定例子中，假設內容伺服器擁有項目(1)至(3)的加密內容(C)及標題金鑰(Kt)之下面資料組。

(1)(Kt11, C11)

(2)(Kt12, C12)

(3)(Kt13, C13)

需注意的是，Cnn 表示內容檔案，及 Ktnn 表示用於內容的加密之標題金鑰。

(Kt11, C11)表示標題金鑰(Kt11)及以標題金鑰(Kt11)

所加密之內容(C11)的資料組。

例如，假設某一“未授權使用者 Ux”依據“未授權使用者 Ux”的諸如 PC 等使用者裝置與內容伺服器之間的預定合法購買程序已執行此購買處理本身，而購買所有上述三個資料組：

(1)(Kt11, C11)，

(2)(Kt12, C12)，及

(3)(Kt13, C13)。

“未授權使用者 Ux”記錄上述資料組(1)至(3)到諸如作爲使用者裝置之 PC 的硬碟等媒體。

“未授權使用者 Ux”從作爲使用者裝置之 PC 的硬碟等媒體讀取上述資料組(1)至(3)，及以各自標題金鑰解密所有加密內容。以此方式，取得下面資料項目。

標題金鑰：Kt11、Kt12、及 Kt13

加密內容：C11、C12、及 C13

需注意的是，當在授權的再生裝置中使用正規的內容再生程式時，標題金鑰無法被讀取到外面。然而，例如藉由安裝惡意的程式到諸如 PC 等裝置本身可讀取標題金鑰。如此，仍舊難以完善地防止標題金鑰被讀取。

另外，“未授權使用者 Ux”產生經由解密內容 C11 至 C13 的序連所取得之資料項目 C11||C12||C13，及以標題金鑰：Kt11 來加密此序連資料項目。

換言之，“未授權使用者 Ux”產生下面資料組(Kt11, C11||C12||C13)，及透過網路非法散佈此資料組。尤其

是，以低價販售此資料組，或者自由提供給大量使用者。

此種處理使大量一般使用者能夠從上述“未授權使用者 Ux”取得上述非法產生的資料組，換言之，(Kt11, C11||C12||C13)。

此資料組包含下面資料項目：

(a)以標題金鑰 Kt11 加密之加密內容，以及

(b)標題金鑰 Kt11，

及具有與從授權內容提供商提供給使用者之資料組內容的結構相同之結構。

如此，只要具有許可的正規內容再生程式，任何授權的再生裝置可藉由使用標題金鑰 Kt11 沒有問題地解密及再生加密內容[C11||C12||C13]。

結果，在沒有合法購買之下，越來越多詐騙使用內容。在此例中，較少使用者合法購買諸如 C11 至 C13 等內容。最後，合法權利擁有人的獲利會損失。

此處，尤其說明此詐騙處理。例如，假設有關諸如第一集至第 12 集之十二個標題的戲劇等連續內容，內容的購買單位以集數爲單位來設定如下。

第 1 集=(Kt01, C01)

第 2 集=(Kt02, C02)

第 3 集=(Kt03, C03)

...

第 12 集=(Kt12, C12)

在此種事例中，某一“未授權使用者”可執行下面處

理：購買整個系列，換言之，第 1 集至第 12 集之十二個標題全部；序連對應於第 1 集至第 12 集：C01 至 C12 之內容；及藉由以對應於第 1 集之標題金鑰來再加密以產生資料組，換言之，(Kt01, C01||C02||C03...||C12)，以便將此資料組暴露於網路上或非法販售。

在此種事例中，藉由取得由“未授權使用者”所產生之詐騙資料組(Kt01, C01||C02||C03...||C12)，使大量使用者裝置能夠再生及使用內容。

例如，假設上述十二集的每一個之一集的全價爲¥2,000，則購買全部十二集花費如下。

12 x ¥2,000=¥24,000

當“未授權使用者”例如以¥6,000 販售詐騙資料組(Kt01, C01||C02||C03...||C12)時，使大量使用者會購買此低價內容。結果，阻礙合法內容的販售，如此導致侵犯原有著作權擁有人及提供權擁有人的權利及獲利損失。

除了上述例子，以對應於某內容 C11 所設定之標題金鑰 Kt11 可被用於加密各種其他無關的內容 Cxx 作爲下面資料組(Kt11, Cxx)。

內容 Cxx 可包括各種內容，因此產生有所有內容被單一標題金鑰無限制解密及再生之問題。

換言之，甚至當使用禁止再生明文內容之再生裝置時，藉由使用上述詐騙資料組，仍可如解密及再生非法購買的內容一般執行解密及再生。

另外，“未授權使用者”亦被允許提供標題金鑰的更換

及再加密作爲服務，因此被允許像個授權伺服器一般。

如上述，難以僅憑藉此種內容加密處理作爲對策來防止詐騙使用。

作爲除了加密處理以外之消除內容的詐騙使用之方法，具有使再生裝置能夠查驗內容是否已被竄改之方法。藉由利用此方法，在例如散佈內容的處理期間已確認內容有一些變更(竄改)之事例中，可取消竄改內容的使用。

尤其是，可利用下面控制系統：只有在使執行內容的再生之使用者裝置能夠執行查驗內容是否已被竄改之處理及已確認內容無竄改的事例中允許內容的再生；以及在已確認內容有一些竄改之事例中取消內容的再生。

例如，專利文件 1(日本專利申請案先行公開號碼2002-358011)揭示控制系統：從欲待再生的內容之檔案計算雜湊值；執行此雜湊值與準備查驗雜湊值的比較，換言之，依據正規內容資料項目所事先計算的查驗雜湊值；以及在重新計算的雜湊值已匹配查驗雜湊值並且已判斷已確認內容無竄改之事例中位移到再生內容的處理。

然而，在執行依據內容來計算雜湊值的此種處理之事例中，當作爲雜湊值的計算之來源資料項目的內容資料項目量大時，爲了計算需要相當高的處理負載及相當長的處理時間。近年來，移動影像的品質變得更高，因此，在許多事例中，一內容具有十億位元組至幾十個十億位元組之資料量。當使執行內容再生之使用者裝置能夠執行依據此種大量資料來計算內容的雜湊值之處理時，產生有使用者

裝置需要相當高的資料處理能力以及由於內容的查驗需要較長的時間週期導致無法充分執行內容再生處理之問題。

另外，專利文件 2(日本專利號碼 4576936)揭示系統如下：被設定作爲儲存在資訊記錄媒體中之內容的分段資料項目之各自雜湊單位的雜湊值係記錄到內容雜湊表，及連同內容一起儲存在資訊記錄媒體中。

根據專利文件 2 所揭示之系統，執行內容再生之資訊處理裝置依據隨機選擇的雜湊單位中至少一個來執行雜湊值查驗處理。利用此系統，尤其是依據具有少量資料之雜湊單位，不管內容的資料量如何都能夠執行計算及查驗雜湊值之處理。結果，在執行內容再生的使用者裝置中可有效執行內容查驗。

然而，專利文件 2 所揭示之系統係在儲存於資訊記錄媒體的內容上之處理的前提下設計的。換言之，具有問題如下：雖然專利文件 2 所揭示之系統可應用到同時記錄不僅內容而且雜湊值的事例，例如在資訊記錄媒體的製造時，但是此系統難以應用到例如從伺服器所下載的內容。

另外，上述之專利文件 1 及專利文件 2 各個強調查驗內容是否已被竄改，因此具有難以限制非法拷貝內容的散佈之問題。

如上述，在相關技藝中利用加密內容及查驗內容是否已被竄改之處理，仍無法充分防止非法拷貝內容的散佈或內容加密金鑰的漏洩。

【發明內容】

鑑於上述問題，有需要提供有效防止內容的詐騙使用之資訊處理裝置、資訊儲存裝置、資訊處理系統、資訊處理方法，及程式。

根據本揭示的第一實施例，設置有資訊儲存裝置，包括

儲存單元，被組構成儲存加密內容及欲待應用到加密內容的解密之加密金鑰，儲存單元包括

受保護區，在受保護區中，儲存轉換的加密金鑰及設定存取限制，轉換的加密金鑰爲經由加密金鑰之轉換所取得的資料項目，以及

通用區，其儲存加密內容及對應於加密內容所設定之加密內容簽名檔案，加密內容簽名檔案包含指示在受保護區中哪一個區域允許轉換的加密金鑰之儲存的區塊識別符作爲記錄資料項目，以允許再生裝置能夠執行應用區塊識別符之內容再生可能性判斷，再生裝置被組構成從儲存單元讀取加密內容及執行再生處理。

另外，在根據本揭示的第一實施例之資訊儲存裝置中，

加密內容簽名檔案包含 ECS(加密內容簽名)發行人憑證，其儲存來自加密內容簽名檔案的發行人之 ECS 發行人的公用金鑰，ECS 發行人憑證包含作爲在受保護區之各區域中允許轉換的加密金鑰之儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

資訊儲存裝置允許再生裝置能夠判斷記錄在加密內容簽名檔案中之區塊識別符是否落在記錄在 ECS 發行人憑證中的區塊識別符範圍內，及依據判斷的結果來決定是否能夠再生加密內容，再生裝置被組構成從儲存單元讀取加密內容及執行該再生處理。

另外，在根據本揭示的第一實施例之資訊儲存裝置中，

通用區另儲存對應於加密內容之使用控制資訊項目，使用控制資訊項目爲包含指示在哪一個區塊儲存加密金鑰之不同區塊識別符的資訊項目，以及

資訊儲存裝置允許再生裝置能夠判斷記錄在加密內容簽名檔案中之區塊識別符是否匹配記錄在使用控制資訊項目中之不同區塊識別符，及依據判斷的結果來決定是否能夠再生加密內容，再生裝置被組構成從儲存單元讀取加密內容及執行再生處理。

另外，根據本揭示的第二實施例，設置有資訊處理裝置，包括

資料處理單元，被組構成執行記錄在媒體中之加密內容的解密處理及再生處理，資料處理單元被組構成

從媒體讀取對應於加密內容所設定之加密內容簽名檔案，

從加密內容簽名檔案取得區塊識別符，區塊識別符指示在哪一個區域允許欲待應用到加密內容的解密之加密金鑰的儲存，以及

執行應用區塊識別符之內容再生可能性判斷處理。

另外，在根據本揭示的第二實施例之資訊處理裝置中，

加密內容簽名檔案包含 ECS 發行人憑證，其儲存來自加密內容簽名檔案的發行人之 ECS 發行人之公用金鑰，ECS 發行人憑證包含作爲在各區域中允許加密之儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

資料處理單元判斷記錄在加密內容簽名檔案中之區塊識別符是否落在記錄在 ECS 發行人憑證中的區塊識別符範圍內，及依據判斷的結果來決定是否能夠再生加密內容。

另外，在根據本揭示的第二實施例之資訊處理裝置中，

媒體另儲存對應於加密內容之使用控制資訊項目，使用控制資訊項目爲包含指示在哪一個區塊儲存加密金鑰之不同區塊識別符的資訊項目，以及

資料處理單元判斷記錄在加密內容簽名檔案中之區塊識別符是否匹配記錄在使用控制資訊項目中之不同區塊識別符，及依據判斷的結果來決定是否能夠再生加密內容。

另外，根據本揭示的第三實施例，設置有資訊處理裝置，包括

資料處理單元，被組構成輸出欲待記錄到媒體之加密內容及欲待應用到加密內容的解密之加密金鑰，資料處理單元被組構成

取得對應於加密內容所設定之加密內容簽名檔案，

從加密內容簽名檔案取得區塊識別符，區塊識別符指示在哪一個區域允許加密金鑰之儲存，以及

執行應用區塊識別符之內容輸出可能性判斷處理。

另外，在根據本揭示的第三實施例之資訊處理裝置中，

加密內容簽名檔案包含 ECS 發行人憑證，其儲存來自加密內容簽名檔案的發行人之 ECS 發行人之公用金鑰，ECS 發行人憑證包含作爲在各區域中允許加密金鑰之儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

資料處理單元判斷記錄在加密內容簽名檔案中之區塊識別符是否落在記錄在 ECS 發行人憑證中的區塊識別符範圍內，及依據判斷的結果來決定是否能夠輸出加密內容。

另外，在根據本揭示的第三實施例之資訊處理裝置中，資料處理單元被組構成

取得對應於加密內容所設定之使用控制資訊項目，

從取得的使用控制資訊項目取得不同區塊識別符，其指示在哪一個區塊儲存加密金鑰，

判斷記錄在加密內容簽名檔案中之區塊識別符是否匹配記錄在使用控制資訊項目中之不同區塊識別符，以及

依據判斷的結果來決定是否能夠再生加密內容。

另外，根據本揭示的第四實施例，提供有資訊處理方法，係由資訊處理裝置所執行，資訊處理裝置包括資料處理單元，被組構成執行記錄在媒體中之加密內容的解密處理及再生處理，資料處理單元被組構成

從媒體讀取對應於加密內容所設定之加密內容簽名檔案，

從加密內容簽名檔案取得區塊識別符，區塊識別符指示在哪一個區域允許欲待應用到加密內容的解密之加密金鑰的儲存，以及

執行應用區塊識別符之內容再生可能性判斷處理。

另外，根據本揭示的第五實施例，提供有資訊處理方法，係由資訊處理裝置所執行，資訊處理裝置包括資料處理單元，被組構成輸出欲待記錄到媒體之加密內容及欲待應用到加密內容的解密之加密金鑰，資料處理單元被組構成

取得對應於加密內容所設定之加密內容簽名檔案，

從加密內容簽名檔案取得區塊識別符，區塊識別符指示在哪一個區域允許儲存加密金鑰，以及

執行應用區塊識別符之內容輸出可能性判斷處理。

另外，根據本揭示的第六實施例，提供有程式，其使

資訊處理裝置能夠執行資訊處理，資訊處理裝置包括資料處理單元，被組構成執行記錄在媒體中之加密內容的解密處理及再生處理，程式使該資料處理單元能夠執行

讀取處理，從媒體讀取對應於加密內容所設定之加密內容簽名檔案，

取得處理，從加密內容簽名檔案取得區塊識別符，區塊識別符指示在哪一個區域允許欲待應用到加密內容的解密之加密金鑰的儲存，以及

應用區塊識別符之內容再生可能性判斷處理。

另外，根據本揭示的第七實施例，提供有程式，其資訊處理裝置能夠執行資訊處理，資訊處理裝置包括資料處理單元，被組構成輸出欲待記錄到媒體之加密內容及欲待應用到加密內容的解密之加密金鑰，

程式使資料處理單元能夠執行

取得處理，取得對應於加密內容所設定之加密內容簽名檔案，

取得處理，從加密內容簽名檔案取得區塊識別符，區塊識別符指示在哪一個區塊允許加密金鑰之儲存，以及

應用區塊識別符之內容輸出可能性判斷處理。

需注意的是，根據本揭示的實施例之程式包括能夠由記錄媒體或通訊媒體提供給例如資訊處理裝置、電腦、及能夠執行各種程式及碼的系統之程式。藉由提供電腦可讀取形式之此種程式，在資訊處理裝置、電腦、及系統中執

行對應於程式的處理。

此說明書所使用的“系統”一詞意指複數個裝置的邏輯集合組態，因此如上述所組構之這些裝置並不一定設置在同一機殼中。

根據本揭示的一實施例之組態，提供有效防止內容的詐騙使用之裝置及方法。

尤其是，從對應於加密內容所設定之加密內容簽名檔案取得區塊識別符，其指示在哪一個區域允許應用到加密內容的解密之加密金鑰的儲存。然後，執行應用區塊識別符之內容再生可能性判斷處理。加密內容簽名檔案包含從作爲加密內容簽名檔案的發行人之 ECS 發行人所發行的憑證。執行有關記錄在加密內容簽名檔案中之區塊識別符是否落在記錄在 ECS 發行人憑證中之區塊識別符範圍內的判斷，及執行有關記錄在加密內容簽名檔案中之區塊識別符是否匹配記錄在使用控制資訊項目中之不同區塊識別符的判斷。依據這些判斷的結果，決定是否能夠再生內容。

藉由使用從加密內容簽名檔案所取得之區塊識別符資訊項目，依據有關金鑰資訊項目是否記錄在某存取允許區塊中之判斷，能夠執行內容使用控制。

按照如附圖所示之其最佳模式實施例之下面詳細說明，本揭示的這些及其他目的、特徵、及有利點將變得更加明顯。

【實施方式】

在下文中，將參考圖式詳細說明根據本揭示的實施例之資訊處理裝置、資訊儲存裝置、資訊處理系統、資訊處理方法及程式。需注意的是，以下面順序在下面段落中進行說明。

1.內容提供處理及內容使用處理之概要

2.記憶卡的組態例子及使用例子

3.包含有關受保護區之存取允許資訊項目的憑證

4.參考裝置的憑證進行存取到記憶卡之處理的例子

5.使用加密內容簽名(ECS)發行人之內容提供系統

6.ECS 檔案的組態例子

7.ECS 發行人金鑰撤回清單的結構

8.加密內容簽名檔案(ECS)的產生處理

9.應用 ECS 簽名檔案及 ECS 發行人憑證的日期資訊項目之處理

10.使加密金鑰與 ECS 發行人的簽名相關聯之組態

11.應用記錄在加密內容簽名(ECS)檔案中之區塊識別符的處理

12.各個裝置的硬體組態例子

13.本揭示的組態之摘要

[1.內容提供處理及內容使用處理之概要]

在下文中，將參考圖式詳細說明根據本揭示的實施例之資訊處理裝置、資訊處理方法及程式。

首先，將參考圖 1 及隨後圖式說明內容提供處理及內

容使用處理之概要。

圖 1 從其左手側圖解下面的例子。

(a)內容提供裝置

(b)內容記錄/再生裝置(主機)

(c)內容記錄媒體

(c)內容記錄媒體爲使用者記錄內容及使用者用來再生內容的處理之媒體。此處，圖解有記憶卡 31，其爲諸如快閃記憶體等資訊儲存裝置。

需注意的是，在下文的實施例被說明作典型例子之例子中，雖然由內容提供裝置所提供之內容爲加密內容，但是根據本揭示的實施例之組態並不侷限於所提供的內容爲加密內容之事例，及亦可應用到所提供的內容爲未加密的明文內容之事例。

使用者將記憶卡 31 用於記錄各種內容，諸如音樂作品及電影等。這些內容包括在使用上受控制之內容，諸如著作權所適用的內容等。

在使用上受控制之內容包括禁止被無限制拷貝或以拷貝資料形式散佈之內容，及在可使用時間週期上有限制之內容。需注意的是，當將此種使用受控制內容記錄在記憶卡 31 時，同時記錄對應於內容之使用控制資訊項目(使用規則)。

作爲使用控制資訊項目(使用規則)，記錄有有關內容的使用之資訊項目，諸如內容的允許可使用時間週期及內容的拷貝之允許次數等。

內容提供裝置連同內容一起提供對應於內容的此種使用控制資訊項目。

(a)內容提供裝置爲諸如音樂作品及電影等內容的供應之來源。作爲內容提供裝置的例子，圖 1 圖解廣播電台 11 及內容伺服器 12。

諸如電視台等廣播電台 11 在陸地波或透過衛星的衛星波提供各種廣播內容給使用者裝置[(b)內容記錄/再生裝置(主機)]。

內容伺服器 12 爲透過諸如網際網路等網路來提供諸如音樂作品及電影等內容之伺服器。

例如，使用者插入作爲(c)內容記錄媒體之記憶卡 31 到(b)內容記錄/再生裝置(主機)。以此方式，由廣播電台 11 及內容伺服器 12 所提供的內容透過(b)內容記錄/再生裝置(主機)本身的接收單元或連接到內容記錄/再生裝置(主機)的接收裝置來接收，及記錄在記憶卡 31 中。

(b)內容記錄/再生裝置(主機)接受作爲(c)內容記錄媒體之記憶卡 31，以記錄接收自作爲(a)內容提供裝置的廣播電台 11 及內容伺服器 12 之內容在記憶卡 31 中。

(b)內容記錄/再生裝置(主機)包括專用記錄/再生裝置 21(CE 裝置：消費者電子裝置)21，諸如設置有諸如硬碟等碟之 DVD 播放器等、DVD、及 BD 等。另外，(b)內容記錄/再生裝置(主機)包括 PC 22 及行動終端 23，諸如智慧型電話、行動電話、行動播放器、及數位板終端等。它們每一個都是能夠接受作爲(c)內容記錄媒體之記憶卡 31 的

裝置。

藉由使用專用記錄/再生裝置21、PC 22、及行動終端23等等，使用者從廣播電台11及內容伺服器12接收諸如音樂作品及電影等內容，及將這些內容記錄到記憶卡31中。

參考圖2說明如何使用記錄在記憶卡31中之內容。

作爲資訊儲存裝置之記憶卡31爲相對於諸如PC等內容再生裝置可拆卸之記錄媒體，因此能夠從已記錄內容之裝置自由拆卸，並且也能夠插入到其他使用者裝置。

尤其是，如圖2所示，執行下面處理。

(1)記錄處理

(2)再生處理

需注意的是，一些裝置只執行記錄及再生的其中之一。

另外，不需要由同一裝置執行記錄處理及再生處理，因此使用者能夠自由選擇及使用記錄裝置或再生裝置。

需注意的是，在許多事例中，記錄在記憶卡31中之使用受控制內容被記錄作加密內容。諸如專用記錄/再生裝置21、PC 22、及行動終端23等內容再生裝置依據預定序列來執行解密處理，而後再生內容。

另外，以記錄在已對應於內容設定之使用控制資訊項目(使用規則)中之使用允許模式執行再生處理等等。

(b)內容記錄/再生裝置(主機)儲存程式(主機應用程式)，其被組構成依據使用控制資訊項目(使用規則)來執行

內容使用處理及內容解密處理。依據程式(主機應用程式)來再生內容。

[2.記憶卡的組態例子及使用例子]

接著，說明被使用作爲內容記錄的記錄媒體之諸如快閃記憶體等記憶卡的組態例子及使用例子。

圖 3 圖解記憶卡 31 中之儲存區的特定組態例子。

如圖 3 所示，記憶卡 31 中之儲存區係由下面兩區所形成。

(a)受保護區 51

(b)通用區 52

(b)通用區 52 爲從使用者所使用之記錄/再生裝置的自由可存取區，及記錄內容、對應於內容之使用控制資訊項目(使用規則)、其他一般內容管理資料項目等等。

在通用區 52 中，例如藉由伺服器或使用者的記錄/再生裝置可自由寫入及讀取資料。

同時，(a)受保護區 51 爲不允許自由存取之區域。

受保護區 51 被分成作爲複數個區段區之區塊(#0, #1, #2, ...)，及以區塊爲單位來設定存取權。

例如，當例如以藉由使用者所使用的記錄/再生裝置或透過網路所連接之伺服器寫入或讀取資料時，記憶卡 31 的資料處理單元依據預儲存在記憶卡 31 中之程式來決定是否能夠以區塊爲單位來相對應地執行讀取或寫入到裝置。

記憶卡 31 不僅包括被組構成執行預儲存程式之資料處理單元，而且也包括被組構成執行認證處理之認證處理單元。首先，記憶卡 31 執行有關裝置的認證處理，以寫入或讀取有關記憶卡 31 的資料。

在認證處理的階段中，包括公用金鑰憑證等等之裝置憑證係接收自配對裝置，換言之，存取請求裝置。

例如，當存取請求裝置爲伺服器時，接收由伺服器所擁有的伺服器憑證。然後，依據包含在憑證中之資訊來判斷是否允許以受保護區 51 中之區塊(區段區)爲單位來存取。

同時，當存取請求裝置爲作爲被組構成記錄及再生內容之使用者裝置的諸如記錄/再生裝置(主機)等主機裝置時，接收由記錄/再生裝置(主機)所擁有的主機憑證。然後，依據包含在憑證中之資訊來判斷是否允許存取到受保護區 51 的區塊(區段區)。

以圖 3 所示之受保護區 51 中的區塊爲單位(圖 3 所示之區域#0, #1, #2, ...)來執行此種存取權判斷處理。記憶卡 31 使伺服器或主機能夠只執行以區塊爲單位所允許的處理(諸如資料讀取/寫入等處理)。

以裝置爲單位來設定有關媒體的讀取/寫入限制資訊項目(PAD 讀取/PAD 寫入)，以對媒體進行存取，諸如內容伺服器或記錄/再生裝置(主機)等。那些資訊項目被記錄在對應於裝置之伺服器憑證及主機憑證中。

需注意的是，在下文中將“憑證”一詞縮寫成“cert”。

如上述，記憶卡 31 依據預儲存在記憶卡 31 中之管理程式來查驗伺服器憑證及主機憑證中所記錄的資料項目，而後執行只允許存取到存取允許區之處理。

[3.包含有關受保護區的存取允許資訊項目之憑證]

接著，參考圖 4 及 5 說明當作爲使用者裝置之伺服器或主機裝置(換言之，記錄/再生裝置)對記憶卡 31 中的上述受保護區 51 進行存取時需要出示給記憶卡之憑證的組態例子。

如上述，記憶卡 31 執行有關裝置的認證處理，以寫入或讀取有關記憶卡 31 的資料。在認證處理的階段中，諸如包括公用金鑰的伺服器憑證或主機憑證等裝置憑證係接收自配對裝置，換言之，存取請求裝置。然後，依據包含在憑證中之資訊來判斷是否允許存取到受保護區 51 的區段區。

作爲此認證處理所使用的裝置憑證之例子，參考圖 4 說明欲待儲存在諸如圖 1 所示之專用記錄/再生裝置 21、PC 22、及行動終端 23 等使用者裝置(主機裝置)中的主機憑證之組態例子。

例如藉由作爲發行公用金鑰憑證的主體之憑證認證中心將主機憑證提供給對應的使用者裝置(主機裝置)。例如，主機憑證爲從憑證認證中心發行給被憑證認證中心允許執行內容使用處理之使用者裝置(主機裝置)的憑證，換言之，儲存公用金鑰等等之憑證。以憑證認證中心密鑰來

設定主機憑證的簽名。以此方式，主機憑證被組構作爲防竄改資料項目。

需注意的是，在裝置的製造時，依據裝置的類型等等之確認結果，可將裝置憑證預儲存在裝置中的記憶體。在由使用者購買之後，爲了取得憑證，可利用組態如下：依據裝置與憑證認證中心或其他管理站之間的預定序列來執行確認裝置類型、可使用內容類型等等之處理，而後將憑證發行給裝置且儲存在裝置的記憶體中。

需注意的是，對記憶卡 31 中的受保護區進行存取之伺服器擁有具有與主機憑證的結構相同結構之伺服器公用金鑰，及記錄允許存取到記憶卡之資訊項目的伺服器憑證。

圖 4 圖解從憑證認證中心提供給主機裝置(使用者裝置)之主機憑證的特定例子。

如圖 4 所示，主機憑證包含下面資料項目。

(1)類型資訊項目

(2)主機 ID(識別)(使用者裝置 ID)

(3)主機公用金鑰

(4)受保護區存取權資訊項目(有關媒體中的受保護區之讀取/寫入限制資訊項目(PAD 讀取/PAD 寫入))

(5)其他資訊項目

(6)簽名

在下文中，說明項目(1)至(6)的資料項目。

(1)類型資訊項目

類型資訊項目爲指示憑證的類型及使用者裝置的類型之資訊項目。例如，在類型資訊項目中，記錄有指示憑證爲主機憑證之資料項目，及指示裝置的類型之資料項目，尤其是，指示裝置爲 PC、音樂播放器等等。

(2)主機 ID

主機 ID 爲記錄作爲裝置識別資訊項目的裝置 ID 之區域。

(3)主機公用金鑰

主機公用金鑰爲對主機裝置的公用金鑰，及依據公用金鑰加密法連同提供給主機裝置(使用者裝置)的密鑰一起組構金鑰對。

(4)受保護區存取權資訊項目(有關媒體中的受保護區之讀取/寫入限制資訊項目(PAD 讀取/PAD 寫入))

在受保護區存取權資訊項目中，記錄有以設定在被組構成例如記錄圖 3 所示之記憶卡 31 的內容之媒體的儲存區中之受保護區(PDA)51 的區塊(區段區)爲單位之資訊項目，區塊(區段區)中允許資料項目之讀取及寫入。

存取權被記錄作以受保護區中之區塊(區段區)爲單位的存取權。

(5)其他資訊項目及(6)簽名

在主機憑證中，除了在上述資料項目(1)至(4)所說明者以外還記錄有各種其他資訊項目，諸如有關資訊項目(1)至(5)的簽名資料項目等。

以來自憑證認證中心的密鑰來執行簽名。當諸如主機

公用金鑰等記錄在主機憑證中的資訊項目被析取來使用時，首先，應用從憑證認證中心所發行之公用金鑰的簽名查驗處理被執行以確認主機憑證不曾被竄改。倘若已確認未竄改，則使用諸如主機公用金鑰等儲存在憑證中之資料項目。

圖 4 圖示記錄用以允許從使用者裝置(主機裝置)到記憶卡中的受保護區之存取的資訊項目之主機憑證。例如，有關進行存取到受保護區所需之伺服器，諸如被組構成提供內容給記憶卡之內容提供伺服器等，類似於圖 4 所示之主機憑證，提供有記錄用以允許存取到記憶卡中的受保護區之資訊項目的憑證[伺服器憑證(例如，儲存伺服器公用金鑰的公用金鑰憑證)。

參考圖 5 說明欲待提供給伺服器之伺服器憑證的組態例子。需注意的是，在下文的說明中，“伺服器”一詞包括圖 1 所示之所有內容提供裝置，尤其是，被組構成提供內容給使用者裝置之裝置，諸如廣播電台 11 及內容伺服器 12 等。

伺服器憑證係從作爲發行公用金鑰憑證的主體之憑證認證中心提供到裝置，諸如被組構成提供內容之內容伺服器等。例如，伺服器憑證爲從憑證認證中心發行到被憑證認證中心允許能夠執行內容提供處理的伺服器及儲存伺服器公用金鑰等等之憑證。以憑證認證中心密鑰來設定伺服器憑證的簽名。以此方式，伺服器憑證被組構作爲防竄改資料項目。

圖 5 圖解欲待從憑證認證中心提供給內容伺服器之伺服器憑證的特定例子。

如圖 5 所示，伺服器憑證包含類似於參考圖 4 所說明之主機憑證的下面資料項目。

(1)類型資訊項目

(2)伺服器 ID(識別)

(3)伺服器公用金鑰

(4)有關媒體的讀取/寫入限制資訊項目(PAD 讀取/PAD 寫入)

(5)其他資訊項目

(6)簽名

這些資訊項目類似於參考圖 4 所說明之資訊項目，因此此處不詳細說明。

需注意的是，在"(4)有關媒體的讀取/寫入限制資訊項目(PAD 讀取/PAD 寫入)"中，記錄有有關各個伺服器之以記憶卡 31 的受保護區 51 中之區塊(區段區)爲單位的存取權(資料讀取/寫入允許資訊項目)。

需注意的是，當諸如伺服器公用金鑰等記錄在伺服器憑證中之資訊項目被析取來使用時，首先，應用來自憑證認證中心的公用金鑰之簽名查驗處理被執行以確認伺服器憑證不曾被竄改。倘若已確認未竄改，則使用諸如伺服器公用金鑰等儲存在憑證中之資料項目。

[4.參考裝置的憑證來進行存取到記憶卡之處理的例子]

如參考圖 4 及 5 所說明一般，當伺服器或主機裝置(諸如記錄/再生裝置等使用者裝置)進行存取到記憶卡 31 的受保護區 51 中之區塊時，必須出示如圖 4 及 5 所示之憑證給記憶卡。

記憶卡確認如圖 4 及 5 所示之憑證，以便判斷是否允許以如圖 3 所示之記憶卡 31 的受保護區 51 中之區塊爲單位的存取。

主機裝置擁有例如參考圖 4 所說明之主機憑證，及執行內容供應等等之伺服器擁有參考圖 5 所說明之伺服器憑證。

當那些裝置進行存取到記憶卡中之受保護區時，那些裝置必須提供它們的憑證給記憶卡，及依據記憶卡側上的查驗來判斷存取是否被允許。

參考圖 6 說明在有關記憶卡的存取請求裝置爲伺服器或諸如記錄/再生裝置等主機裝置之事例中設定存取限制的例子。

圖 6 從左邊圖示作爲有關記憶卡的存取請求裝置之伺服器 A61、伺服器 B62、及主機裝置 63，及記憶卡 70。

伺服器 A61 及伺服器 B62 提供例如加密內容(Con1、Con2、Con3、...)作爲欲待記錄到記憶卡 70 之內容。

這些伺服器另提供標題金鑰(Kt1、Kt2、...)作爲加密內容的解密之金鑰及對應於內容的使用控制資訊項目(使用規則：UR1、UR2、...)。

主機裝置 63 爲執行再生儲存在記憶卡 70 中之內容的

處理之裝置。

主機裝置 63 讀取儲存在記憶卡 70 之通用區 90 中之加密內容(Con1、Con2、Con3、...)及使用控制資訊項目(使用規則：UR1、UR2、...)。另外，主機裝置 63 從受保護區 80 中之區塊(區段區)81 及 82 讀取欲待應用到內容解密處理之標題金鑰(Kt1、Kt2、...)，而後執行參考標題金鑰的解密處理。以此方式，主機裝置 63 依據使用控制資訊項目(使用規則)來使用內容。

記憶卡 70 包括受保護區 80 及通用區 90。加密內容、使用控制資訊項目(使用規則)等等被記錄在通用區 90 中。

作爲內容再生所需之金鑰的標題金鑰被記錄在受保護區 80 中。

如上面參考圖 3 所說明一般，受保護區 80 被分成複數個區塊(區段區)。

圖 6 所示之例子僅圖示下面兩區塊。

區塊#0(受保護區#0)81

區塊#1(受保護區#1)82

在受保護區 80 中，設定有大量其他區塊。

可利用區塊的各種設定模式。

在圖 6 所示之例子中，區塊#0(受保護區#0)81 被設定作爲伺服器 A61 專用的區塊，換言之，用以儲存從伺服器 A61 所提供之內容的解密之標題金鑰的區域。區塊#1(受保護區#1)82 被設定作爲伺服器 B62 專用的區塊，換言之，用以儲存從伺服器 B62 所提供之內容的解密之標題金

鑰的區域。

在此種設定下，提供內容之伺服器 A61 將解密自此提供之內容所需的標題金鑰記錄在區塊#0(受保護區#0)81中。

在此事例中，將記錄在伺服器 A61 的伺服器憑證中之寫入允許區資訊項目(PAD 寫入)被組構作爲設定有關區塊#0(受保護區#0)81 之寫入允許的憑證。

需注意的是，在圖 6 所示之例子中的設定之下，亦允許有關允許寫入之區塊的讀取。

另外，伺服器 B62 將解密自此提供之內容所需的標題金鑰記錄在區塊#1(受保護區#1)82 中。

在此事例中，將記錄在伺服器 B62 的伺服器憑證中之寫入允許區資訊項目(PAD 寫入)被組構作爲設定有關區塊#1(受保護區#1)82 之寫入允許的憑證。

另外，由作爲被組構成藉由讀取記錄在區塊#0 及#1 中之標題金鑰來執行內容再生的再生裝置之主機裝置 63 所擁有的主機憑證被組構作爲設定有關區塊#0 及#1 之讀取允許的憑證。

在此例中，在主機憑證中並未設定有關區塊#0 及#1 二者之寫入允許。

需注意的是，在刪除內容時，爲了亦能夠刪除對應於欲待刪除的內容之標題金鑰，可設定刪除區塊#0 及#1 二者之處理的允許。

另外，在其他處理中，當主機裝置 63 必須寫入資料

到受保護區時，在主機憑證中可設定寫入允許。

記憶卡 70 中之資料處理單元從諸如提供內容的伺服器或使用內容的主機等存取請求裝置接收有關受保護區 80 的存取請求。然後，資料處理單元參考這些裝置的裝置憑證確認用以允許以區塊爲單位的存取之資訊項目。以此方式，資料處理單元判斷是否允許存取到區塊。

記憶卡 70 區分寫入請求或讀取請求的資料項目類型，以回應來自存取請求裝置之資料寫入或讀取的輸入，及選擇區塊(#0、#1、#2、...)作爲資料寫入目的地或資料讀取來源。

如參考圖 4 及 5 所說明一般，存取控制資訊項目被記錄在存取請求裝置的憑證(伺服器憑證、主機憑證等等)中。記憶卡首先查驗接收自存取請求裝置的這些憑證之簽名，以便確認憑證的有效性。然後，記憶卡讀取包含在憑證中之存取控制資訊項目，換言之，下面資訊項目。

讀取允許區資訊項目(PAD 讀取)

寫入允許區資訊項目(PAD 寫入)

依據這些資訊項目，只有被允許由存取請求裝置執行之處理被允許及執行。

[5.使用加密內容簽名(ECS)發行人之內容提供系統]

如上面參考圖 1 所說明一般，欲待提供給使用者裝置之內容係提供自內容提供裝置。然而，在某些事例中，內容提供裝置本身提供非法拷貝內容。在下文中，說明防止

將以諸如藉由伺服器之詐騙處理等除了使用者裝置的組態以外之組態來執行的詐騙之組態。

參考圖 7，說明被組構成防止內容的詐騙使用之根據本揭示的實施例之資訊處理系統的整體組態。

圖 7 圖解資訊處理系統的整體組態之例子。圖 7 圖示由下面四種類型的裝置所形成之階層式結構。

(A)許可發行人(LA)101

(B)加密內容簽名(ECS)發行人 102-1 至 102-n

(C)內容提供裝置(內容伺服器)103-1 至 103-m

(D)使用者裝置(內容再生裝置)104-1 至 104-f

圖 7 所示之(C)內容提供裝置(內容伺服器)103-1 至 103-m 對應於圖 1 所示之廣播電台 11、內容伺服器 12 等等。

另外，圖 7 所示之(D)使用者裝置(內容再生裝置)104-1 至 104-f 對應於圖 1 所示之諸如專用記錄/再生裝置 21、PC 22、及行動終端 23 等使用者裝置。

(C)內容提供裝置(內容伺服器)103-1 至 103-m 包括各種資訊處理裝置，諸如發送內容的裝置，尤其是，內容伺服器及廣播電台等，及諸如將內容記錄在媒體中之裝置等，及另包括提供諸如儲存內容的碟等媒體之媒體提供公司。這些裝置有很多。

(D)使用者裝置(內容再生裝置)104-1 至 104-f 爲被組構成藉由透過網際網路、廣播波、或諸如碟等媒體從(C)內容提供裝置(內容伺服器)103-1 至 103-m 接收或讀取諸

如電影、音樂作品等內容及其他內容來執行再生處理之裝置。尤其是，(D)使用者裝置(內容再生裝置)104-1 至 104-f 包括能夠內容再生之各種資訊處理裝置，諸如 PC、行動終端、DVD 播放器、BD 播放器、及電視等。

(B)加密內容簽名(ECS)發行人 102-1 至 102-n 產生對應於提供自(C)內容提供裝置(內容伺服器)103-1 至 103-m 的內容之加密內容簽名檔案(ECS 檔案)。

(C)內容提供裝置(內容伺服器)103-1 至 103-m 發出產生有關(B)加密內容簽名(ECS)發行人 102-1 至 102-n 之對應於欲待重新提供給使用者裝置 104 的諸如電影內容等內容之此種加密內容簽名檔案(ECS 檔案)的請求。

回應於這些請求，(B)加密內容簽名(ECS)發行人 102-1 至 102-n 產生及提供加密內容簽名檔案(ECS 檔案)給(C)內容提供裝置(內容伺服器)103-1 至 103-m。

需注意的是，下面詳細說明加密內容簽名檔案(ECS 檔案)的特定組態及產生處理。

(C)內容提供裝置(內容伺服器)103-1 至 103-m 從(B)加密內容簽名(ECS)發行人 102-1 至 102-n 接收加密內容簽名檔案(ECS 檔案)，及連同加密內容一起提供加密內容簽名檔案(ECS 檔案)給(D)使用者裝置(內容再生裝置)104-1 至 104-f。

在內容的再生之前，(D)使用者裝置(內容再生裝置)104-1 至 104-f 各個在加密內容簽名檔案(ECS 檔案)上執行簽名查驗處理。只有在已經由簽名查驗處理確認無竄

改之事例中，允許內容被解密及再生。

需注意的是，倘若在加密內容簽名檔案(ECS 檔案)上已經由簽名查驗確認無竄改，則(D)使用者裝置(內容再生裝置)104-1 至 104-f 各個依據執行內容之解密及再生的序列來儲存再生處理程式。依據再生處理程式，執行諸如加密內容簽名檔案(ECS 檔案)上的簽名查驗等內容再生可能性判斷處理及內容再生。

例如，在經由加密內容簽名檔案(ECS 檔案)上的簽名查驗已確認有一些竄改之事例中，禁止內容的再生。

(A)許可發行人(LA)101 提供作爲發行 ECS 檔案的許可之許可給(B)加密內容簽名(ECS)發行人 102-1 至 102-n。

在經由依據預設的許可發行序列來確認這些加密內容簽名(ECS)發行人是否有效以確認這些加密內容簽名(ECS)發行人的有效性之後，(A)許可發行人(LA)101 發行許可給(B)加密內容簽名(ECS)發行人 102-1 至 102-n。

需注意的是，尤其是，許可爲各個簽名有來自許可發行人(LA)101 的密鑰之公用金鑰憑證。公用金鑰憑證儲存用於(B)加密內容簽名(ECS)發行人 102-1 至 102-n 之公用金鑰。需注意的是，(A)許可發行人(LA)101 亦提供對應於儲存在公用金鑰憑證中之公用金鑰的密鑰給(B)加密內容簽名(ECS)發行人 102-1 至 102-n。

接著，參考圖 8 說明將在下面三個裝置之間所執行的處理。

(A)許可發行人(LA)101

(B)加密內容簽名(ECS)發行人 102

(C)內容提供裝置(內容伺服器)103

圖 8 圖示下面三個裝置及將在這些裝置所執行之主要處理。

(A)許可發行人(LA)101

(B)加密內容簽名(ECS)發行人 102

(C)內容提供裝置(內容伺服器)103

由許可發行人(LA)101 所執行之處理被表示作處理(A1)及(A2)。

尤其是，將由許可發行人(LA)101 所執行之處理(A1)及(A2)的內容如下。

處理(A1)：提供具有截止日期的 ECS 發行人憑證給加密內容簽名(ECS)發行人 102。

處理(A2)：提供 ECS 發行人金鑰撤回清單給內容提供裝置 103。

將由加密內容簽名(ECS)發行人 102 所執行之處理被表示作處理(B1)及(B2)。

尤其是，將由加密內容簽名(ECS)發行人 102 所執行之處理(B1)及(B2)的內容如下。

處理(B1)：產生加密內容簽名檔案(ECS 檔案)。

處理(B2)：提供加密內容簽名檔案(ECS 檔案)給內容提供裝置 103。

將由內容提供裝置 103 所執行之處理被表示作處理

(C1)及(C2)。

尤其是，將由內容提供裝置 103 所執行之處理(C1)及(C2)的內容如下。

處理(C1)：提供 ECS 檔案產生資料項目給加密內容簽名(ECS)發行人 102。例如，提供內容雜湊清單集合、標題金鑰的雜湊值、及區塊識別符。

處理(C2)：執行使用 ECS 檔案之內容供應可能性判斷處理。

[6.ECS 檔案的組態例子]

接著，說明由加密內容簽名(ECS)發行人 102 所產生之 ECS 檔案的組態例子。

圖 9 圖解 ECS 檔案及亦被設定作 ECS 檔案的一構成資料項目之 ECS 發行人憑證的資料項目之組態例子。

ECS 檔案爲由加密內容簽名(ECS)發行人 102 所產生的檔案，及儲存接收自內容提供裝置 103 之內容雜湊清單集合、標題金鑰的雜湊值、及區塊識別符等等作爲構成資料項目。

如圖 9 的(A)所示，ECS 檔案爲包含下面資料項目的檔案。

(1)內容雜湊清單集合(雜湊清單集合)

(2)ECS 發行日期

(3)區塊識別符(PAD 區塊號碼)

(4)ECS 發行人的簽名

(5)ECS 發行人憑證

(6)內容區塊表(所儲存的內容區塊表)

(1)內容雜湊清單集合(雜湊清單集合)爲內容提供裝置(內容伺服器)103 所產生及被加密內容簽名(ECS)發行人 102 接收的資料項目。尤其是，(1)內容雜湊清單集合(雜湊清單集合)爲包含依據欲提供給使用者裝置的內容(尤其是，諸如電影等將由使用者裝置再生的內容)之構成資料項目所產生之雜湊值的資料項目，以及雜湊值的屬性資訊項目(指示例如作爲雜湊值的來源之內容區塊的位置之偏移量、長度等等的資訊項目)。

(2)ECS 發行日期爲產生加密內容簽名(ECS)發行人 102 中之 ECS 檔案的日期之資訊項目。

日期的這資訊項目對應於例如(4)ECS 發行人的簽名之產生日期。

(3)區塊識別符(PAD 區塊號碼)爲欲從內容提供裝置(內容伺服器)103 通知到加密內容簽名(ECS)發行人 102 之資料項目，尤其是，指示在媒體之受保護區中哪一區塊儲存作爲對應於從內容提供裝置 103 提供給使用者裝置 104 的內容之加密金鑰的標題金鑰之識別符。換言之，(3)區塊識別符(PAD 區塊號碼)爲指示內容提供裝置 103 可使用媒體之受保護區中哪一區塊之識別符。

如上面參考例如圖 3 至 6 所說明一般，事先設定內容提供裝置 103 可使用媒體之受保護區中哪一區塊，及記錄此種存取允許區塊的資訊項目。

(4)ECS 發行人的簽名爲 ECS 發行人的電子簽名。

欲待簽名的資料項目包括構成資料項目，諸如內容雜湊清單集合、ECS 發行日期、區塊識別符、及標題金鑰(雜湊值)等。

(5)ECS 發行人憑證爲對應於 ECS 發行人 102 之公用金鑰憑證，及如圖 9 之(B)所示，儲存 ECS 發行人 102 的公用金鑰等等。下面詳細說明此組態。

(6)內容區塊表(所儲存的內容區塊表)被設定作欄位，在欄位中，當對應於複數個內容之雜湊清單被記錄在上述內容雜湊清單集合(雜湊清單集合)中時，記錄雜湊清單與複數個內容之間的對應資訊項目。

接著，說明圖 9 的(B)所示之 ECS 發行人憑證的資料結構。

ECS 發行人憑證係由許可發行人(LA)101 所產生，及提供給 ECS 發行人 102。ECS 發行人 102 藉由提供產生 ECS 發行人憑證所需之資料項目給許可發行人(LA)101 來請求產生 ECS 發行人憑證。

許可發行人(LA)101 產生 ECS 發行人憑證，以回應此請求。

如圖 9 的(B)所示，ECS 發行人憑證爲包含下面資料項目之檔案。

(1)ECS 憑證 ID

(2)區塊識別符起始號碼(起始 PAD 區塊號碼)

(3)區塊識別符範圍(PAD 區塊號碼計數)

(4)發行人憑證截止日期(截止日期)

(5)ECS 發行人公用金鑰

(6)LA 的簽名

(1)ECS 憑證 ID 爲 ECS 憑證的識別符。

(2)區塊識別符起始號碼(起始 PAD 區塊號碼)爲內容提供裝置 103 允許 ECS 發行人 102 能夠進行存取的媒體之受保護區中的存取允許區塊之起始號碼。

(3)區塊識別符範圍(PAD 區塊號碼計數)爲指示從內容提供裝置 103 允許 ECS 發行人 102 能夠進行存取的媒體之受保護區中的存取允許區塊之起始號碼的範圍之資訊項目。

(4)發行人憑證截止日期(截止日期)爲此發行人憑證的截止日期之資訊項目。

(5)ECS 發行人公用金鑰爲 ECS 發行人的公用金鑰。

(6)LA 的簽名爲圖 7 及 8 所示之許可發行人(LA)所發行的電子簽名。尤其是，(6)LA 的簽名爲依據 ECS 發行人憑證的上述構成資料項目(1)至(5)所產生之電子簽名。

圖 10 圖示 ECS 檔案的語法。

圖 11 圖示 ECS 發行人憑證的語法。

需注意的是，記錄在 ECS 發行人憑證中之下面兩資料項目：(2)區塊識別符起始號碼(起始 PAD 區塊號碼)；以及(3)區塊識別符範圍(PAD 區塊號碼計數)如上述爲指示內容提供裝置 103 允許 ECS 發行人 102 能夠進行存取的媒體之受保護區中的存取允許區塊之資訊項目。

尤其是，當設定關係：區塊識別符起始號碼≤N≤區塊識別符起始號碼+區塊識別符範圍時，滿足此關係之所有整數 N 被設定作區塊識別符。

另外，當區塊識別符起始號碼被設定成 0xFFFFFFFF 時，媒體之受保護區中的所有區塊都是存取允許區塊。

需注意的是，雖然在參考圖 9 至 11 所圖解說明的例子中 ECS 檔案包含 ECS 發行人憑證，但是 ECS 檔案不需要包含 ECS 發行人憑證，及 ECS 檔案及 ECS 發行人憑證可被組構成個別檔案。

[7.ECS 發行人金鑰撤回清單的結構]

接著，參考圖 12 說明 ECS 發行人金鑰撤回清單的結構。

如上面參考圖 8 所說明一般，ECS 發行人金鑰撤回清單爲由許可發行人(LA)101 所發行的清單。例如在內容提供裝置 103 中使用此清單。

許可發行人(LA)101 使被判斷是詐騙之儲存 ECS 發行人的公用金鑰之 ECS 發行人憑證(參考圖 9 的(B))無效，而後產生 ECS 發行人金鑰撤回清單作爲登記無效 ECS 發行人的識別符(ID)之清單(尤其是，無效 ECS 發行人憑證)。

如圖 12 所示，ECS 發行人金鑰撤回清單儲存下面資料項目。

(1)版本

(2)實體號碼

(3)撤回(無效)ECS發行人憑證的ID

(4)撤回(無效)ECS發行人憑證的撤回日期

(5)許可發行人(LA)101的電子簽名

(5)許可發行人(LA)101的電子簽名爲有關資料項目(1)至(4)的每一個之電子簽名。

需注意的是，當重新發現詐騙ECS發行人時，藉由添加詐騙ECS發行人的ID，將ECS發行人金鑰撤回清單更新作新的版本，隨後發行以提供給內容提供裝置103。

[8.加密內容簽名檔案(ECS檔案)的產生處理]

接著，參考圖13說明加密內容簽名檔案(ECS檔案)的產生處理。

依據來自內容提供裝置(內容伺服器)103的產生請求，藉由加密內容簽名(ECS)發行人102來產生加密內容簽名檔案(ECS檔案)。

相對於加密內容簽名(ECS)發行人102，內容提供裝置(內容伺服器)103發出產生對應於欲重新提供給使用者裝置104的諸如電影內容等內容之此種加密內容簽名檔案(ECS檔案)的產生之請求。

回應於此請求，加密內容簽名(ECS)發行人102產生及提供加密內容簽名檔案(ECS檔案)給內容提供裝置(內容伺服器)103。

圖13爲在此加密內容簽名(ECS)的產生處理期間將由

內容提供裝置(內容伺服器)103 及加密內容簽名(ECS)發行人 102 所執行之處理的說明圖。

在發出產生新的加密內容簽名檔案(ECS 檔案)之請求時，如圖 13 所示，內容提供裝置(內容伺服器)103 產生包含依據內容 181 的構成資料項目(內容區塊)所產生之雜湊值的內容雜湊清單集合(雜湊清單集合)183。

需注意的是，內容雜湊清單集合(雜湊清單集合)183 被產生作爲儲存依據欲待提供給使用者裝置 104 之加密內容的構成資料項目(內容區塊)所產生之雜湊值的內容雜湊清單集合。

內容提供裝置(內容伺服器)103 提供如此產生的內容雜湊清單集合(雜湊清單集合)183 給加密內容簽名(ECS)發行人 102。

另外，作爲欲待應用到內容 181 的加密之加密金鑰的標題金鑰 182 或標題金鑰的雜湊值亦被提供給加密內容簽名(ECS)發行人 102。

內容雜湊清單集合(雜湊清單集合)183 爲包含依據欲待提供給使用者裝置之內容(尤其是，諸如電影等將由使用者裝置再生的內容)的構成資料項目所產生之雜湊值以及雜湊值的屬性資訊項目的資料項目。

需注意的是，屬性資訊項目包括例如諸如已計算雜湊值之內容區塊的位置資訊等屬性資訊項目。

在圖 13 所示之步驟 S11 中，加密內容簽名(ECS)發行人 102 產生對應於接收自內容提供裝置(內容伺服器)103

之資料項目及ECS檔案的構成資料項目之簽名，尤其是對應於下面資料項目之簽名。

內容雜湊清單集合

ECS發行日期

區塊識別符

標題金鑰(雜湊)

在產生這些簽名的資料項目時，應用由加密內容簽名(ECS)發行人102所擁有的密鑰。例如，依據ECDSA演算法來產生簽名。

如圖13所示，如此產生的簽名被設定作加密內容簽名檔案(ECS檔案)之構成資料項目。

如上面參考圖9的(A)所說明一般，由加密內容簽名(ECS)發行人102所產生之加密內容簽名檔案(ECS檔案)200包含下面資料項目作爲構成資料項目。

(1)內容雜湊清單集合(雜湊清單集合)

(2)ECS發行日期

(3)區塊識別符(PAD區塊號碼)

(4)ECS發行人的簽名

(5)ECS發行人憑證

(6)內容區塊表(所儲存的內容區塊表)

[9.應用ECS檔案及ECS發行人憑證的日期資訊項目之處理]

接著，說明應用ECS檔案及ECS發行人憑證的日期資訊項目之處理。

如參考圖 9 所說明一般，在下面記錄各種日期資訊項目。

(1)由 ECS 發行人 102 所產生及提供給內容提供裝置之 ECS 檔案

(2)由許可發行人(LA)101 所產生及提供給 ECS 發行人 102 之 ECS 發行人憑證

例如，ECS 發行日期被記錄在 ECS 檔案中。

另外，發行人憑證截止日期(截止日期)被記錄在 ECS 發行人憑證。

藉由應用記錄在這些 ECS 檔案及 ECS 發行人憑證中之日期資訊項目，及上面參考圖 12 所說明之 ECS 發行人金鑰撤回清單，內容提供裝置 103 執行判斷有關使用者裝置 104 的內容提供處理之可能性的處理。

同時，藉由應用記錄在 ECS 檔案及 ECS 發行人憑證中之日期資訊項目以及上面參考圖 12 所說明的 ECS 發行人金鑰撤回清單，從內容提供裝置 103 接收內容之使用者裝置 104 執行判斷使用者裝置 104 中的內容再生處理之可能性的處理。

在下文中，說明這些處理。

首先，參考圖 14 及 15 的序列圖來說明加密內容簽名檔案(ECS 檔案)的產生、內容供應、及使用處理序列。

圖 14 從其左手側圖示下面裝置。

許可發行人 101

加密內容簽名(ECS)發行人 102

內容提供裝置 103

以時序處理來圖示步驟 S111 及 S121 至 S128 的處理。

說明這些步驟的處理。

步驟 S111

在步驟 S111 中，許可發行人 101 發行許可(ECS 發行人憑證)給加密內容簽名(ECS)發行人 102。

如上面參考例如圖 8 所說明一般，許可發行人 101 提供許可作爲發行 ECS 檔案之許可，換言之，有關加密內容簽名(ECS)發行人 102 的 ECS 發行人憑證。

在經由依據預定許可發行序列來確認加密內容簽名(ECS)發行人 102 是否有效以確認加密內容簽名(ECS)發行人 102 的有效性之後，許可發行人(LA)101 發行 ECS 發行人憑證給加密內容簽名(ECS)發行人 102。

ECS 發行人憑證爲具有參考圖 9 的(B)所說明之資料結構的公用金鑰憑證。ECS 發行人憑證將公用金鑰儲存到加密內容簽名(ECS)發行人 102。需注意的是，許可發行人(LA)101 亦提供對應於儲存在此 ECS 發行人憑證中之公用金鑰的密鑰給加密內容簽名(ECS)發行人 102。

步驟 S121 至 S124 對應於參考圖 13 所說明之加密內容簽名檔案(ECS 檔案)的產生處理之序列。

針對欲待由內容提供裝置 103 重新提供給使用者裝置之各個內容來連續執行此處理，以便取得對應於欲待重新提供之內容的每一個之加密內容簽名檔案(ECS 檔案)。

在加密內容簽名(ECS)發行人 102 與內容提供裝置 103 之間執行此處理。

首先，在步驟 S121 中，內容提供裝置 103 產生加密內容簽名檔案(ECS 檔案)之產生所需的資料項目。

尤其是，如參考圖 13 所說明一般，執行內容雜湊清單集合(雜湊清單集合)183 等等的產生處理。

如上述，內容雜湊清單集合(雜湊清單集合)爲包含依據欲待提供給使用者裝置之內容(尤其是，諸如電影等將由使用者裝置再生的內容)的構成資料項目所產生之雜湊值以及雜湊值的屬性資訊項目的資料項目。

需注意的是，屬性資訊項目包括例如諸如已計算雜湊值之內容區塊的位置資訊等屬性資訊項目。

需注意的是，內容提供裝置 103 產生將應用到內容的加密處理及解密處理之標題金鑰以及標題金鑰的雜湊值，作爲欲待提供給加密內容簽名(ECS)發行人 102 之資料項目。

接著，在步驟 S122 中，藉由發送所產生的資料項目到加密內容簽名(ECS)發行人 102，內容提供裝置 103 請求產生及發送加密內容簽名檔案(ECS 檔案)。

接著，在步驟 S123 中，加密內容簽名(ECS)發行人 102 執行有關接收自內容提供裝置 103 的資料項目之簽名產生處理。

換言之，加密內容簽名(ECS)發行人 102 執行參考圖 13 所說明之步驟 S11 的簽名產生處理。

另外，加密內容簽名(ECS)發行人 102 產生具有上面參考圖 9 的(A)所說明之資料結構的加密內容簽名檔案(ECS 檔案)，及在步驟 S124 中發送如此產生的加密內容簽名檔案(ECS 檔案)到內容提供裝置 103。

如上面參考圖 9 的(A)所說明一般，加密內容簽名檔案(ECS 檔案)包含下面資料項目。

(1)內容集合(雜湊清單集合)

(2)ECS 發行日期

(3)區塊識別符(PAD 區塊號碼)

(4)ECS 發行人的簽名

(5)ECS 發行人憑證

(6)內容區塊表(所儲存的內容區塊表)

在接收加密內容簽名檔案(ECS 檔案)之後，內容提供裝置 103 在步驟 S125 中執行內容供應可能性判斷處理，其判斷是否允許供應應用加密內容簽名檔案(ECS 檔案)之內容。

在步驟 S126 中，在已判斷允許供應內容之事例中，在步驟 S127 中執行有關使用者裝置之內容提供處理。

同時，在步驟 S126 中，在已判斷不允許供應內容之事例中，流程進行到步驟 S128，以取消內容提供處理。

需注意的是，下面參考圖 16 及隨後圖式更詳細說明步驟 S125 至 S128 的處理。

接著，參考圖 15 說明從內容提供裝置 103 提供內容到使用者裝置 104 以及使用者裝置 104 中的內容再生序

列。

圖 15 從其左手側圖示下面。

使用者提供裝置 103

使用者裝置 104

首先，在步驟 S131 中，內容提供裝置 103 發送下面資料項目給使用者裝置 104。

(1)加密內容

(2)加密內容簽名檔案(ECS 檔案)

(3)標題金鑰

需注意的是，作爲步驟 S131 的處理之預處理，例如，發送內容到使用者裝置 104 之請求已從使用者裝置 104 發出到內容提供裝置 103。內容提供裝置 103 根據來自使用者裝置 104 的請求來提供內容。

需注意的是，在步驟 S131 中欲待從內容提供裝置 103 發送之(1)加密內容爲以對應於內容所設定的上述“(3)標題金鑰”加密之內容。

另外，(2)加密內容簽名檔案(ECS 檔案)爲對應於上述(1)加密內容所產生之檔案，及儲存上面參考圖 9 所說明之加密內容簽名檔案(ECS 檔案)的構成資料項目。

使用者裝置 104 接收及儲存這些資料項目到諸如硬碟等媒體內。

之後，在執行再生內容的處理時，執行圖 15 所示之步驟 S132 及隨後步驟的處理。

在步驟 S132 中，使用者裝置 104 讀取對應於欲待再

生之內容的加密內容簽名檔案(ECS 檔案)，及應用加密內容簽名檔案(ECS 檔案)，以便執行判斷是否允許內容的再生之內容再生可能性判斷處理。

在步驟 S133 中，在已判斷允許內容的再生之事例中，在步驟 S134 中執行內容再生處理。

同時，在步驟 S133 中，在已判斷不允許內容的再生之事例中，流程進行到步驟 S135，以取消內容再生處理。

需注意的是，下面參考圖 18 更詳細說明步驟 S132 至 S135 的處理。

接著，參考圖 16 及 17 所示之流程圖說明參考圖 14 所說明之內容提供裝置中的步驟 S125|S128 之子程式，換言之，應用加密內容簽名檔案(ECS 檔案)之內容供應可能性判斷處理的詳細序列。

作爲圖 16 所示之流程圖中的步驟 S151 之預處理，內容提供裝置執行應用設定在接收自加密內容簽名(ECS)發行人的加密內容簽名檔案(ECS 檔案)之 ECS 發行人的簽名之簽名查驗。

在經由此簽名查驗已確認無竄改之事例中，換言之，已確認加密內容簽名檔案(ECS 檔案)的有效性，執行儲存在加密內容簽名檔案(ECS 檔案)中之 ECS 發行人憑證的另一簽名查驗。倘若在兩簽名查驗處理任一者中已確認無竄改，則執行步驟 S151 及隨後步驟的處理。

在兩簽名查驗處理中的至少一個已確認有些竄改之事

例中，加密內容簽名檔案(ECS 檔案)的有效性或 ECS 發行人憑證的有效性未被確認。如此，不執行步驟 S151 及隨後步驟的處理。在此事例中，也不執行內容提供處理。

在經由加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證之兩簽名查驗處理的任一者已確認無竄改之事例中，換言之，已確認加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證之有效性，內容提供裝置執行步驟 S151 的處理。

內容提供裝置讀取記錄在加密內容簽名檔案(ECS 檔案)中之資料項目的 ECS 發行日期，而後讀取記錄在 ECS 發行人憑證中之資料項目的 ECS 發行人憑證截止日期(截止日期)。

另外，經由這些日期資訊項目的比較，內容提供裝置判斷 ECS 發行人憑證截止日期(截止日期)是否在 ECS 發行日期之前。

在已判斷 ECS 發行人憑證截止日期(截止日期)在 ECS 發行日期之前的事例中(Yes)，流程進行到步驟 S156，以取消加密內容的散佈。

同時，在已判斷 ECS 發行人憑證截止日期(截止日期)未在 ECS 發行日期之前的事例中(No)，流程進行到步驟 S152，以在步驟 S153 及隨後步驟中開始應用記錄在加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證中之日期資訊項目(時間戳記)的內容供應可能性判斷處理。

在步驟 S153 中，ECS 發行人憑證截止日期(截止日期)與內容提供裝置的時間區塊或取得自可靠的時間資訊

提供伺服器之真實時間比較。

在已判斷 ECS 發行人憑證截止日期(截止日期)領先真實時間一天或更多之事例中，流程進行到步驟 S156，以取消內容提供處理。

同時，在已判斷 ECS 發行人憑證截止日期(截止日期)未領先真實時間一天或更多之事例中，流程進行到步驟 S154。

在步驟 S154 中，ECS 發行日期與內容提供裝置的時間區塊或取得自可靠的時間資訊提供伺服器之真實時間比較。

在已判斷 ECS 發行日期領先真實時間一天或更多之事例中，流程進行到步驟 S156，以取消內容提供處理。

同時，在已判斷 ECS 發行日期未領先真實時間一天或更多之事例中，流程進行到步驟 S155。

接著，參考圖 17 所示之流程圖說明將在步驟 S155 及隨後處理執行的應用撤回清單之內容供應可能性判斷處理。

需注意的是，內容提供裝置已事先取得參考圖 12 所說明之 ECS 發行人金鑰撤回清單。例如，可從許可發行人(LA)101 取得 ECS 發行人金鑰撤回清單。

在步驟 S161 中，內容提供裝置從 ECS 發行人憑證取得 ECS 憑證 ID，及判斷此 ID 是否已登記在 ECS 發行人金鑰撤回清單中。

在此 ID 未被登記在 ECS 發行人金鑰撤回清單中之事

例中(No)，確認 ECS 發行人憑證還有效而未使其無效(撤回)。在此事例中，流程進行到步驟 S164 以執行內容提供處理。

同時，在步驟 S161 中，在已判斷 ECS 憑證 ID 被登記在 ECS 發行人金鑰撤回清單中之事例中(Yes)，流程進行到步驟 S162。

在步驟 S162 中，下面兩日期資料項目彼此比較。

使登記在 ECS 發行人金鑰撤回清單中之 ECS 發行人憑證無效(撤回)時的日期，換言之，撤回日期

作爲記錄在加密內容簽名檔案(ECS 檔案)中之資料項目的 ECS 發行日期

在已判斷作爲記錄在加密內容簽名檔案(ECS 檔案)中之資料項目的 ECS 發行日期在撤回日期之前時(Yes)，流程進行到步驟 S164，以執行內容提供處理。

這是因爲內容提供處理可被判斷作依據未撤回有效 ECS 發行人憑證的處理。

同時，在步驟 S162 中，在已判斷作爲記錄在加密內容簽名檔案(ECS 檔案)中之資料項目的 ECS 發行日期未在撤回日期之前時(No)，流程進行到步驟 S163，以取消內容提供處理。

這是因爲內容提供處理可被判斷作依據撤回無效的 ECS 發行人憑證之處理。

接著，參考圖 18 所示之流程圖詳細說明上面參考圖 14 的步驟 S132 至 S135 所說明之應用使用者裝置 104 中

的加密內容簽名檔案(ECS)檔案之內容再生可能性判斷處理。

需注意的是，在圖 18 所示之步驟 S171 之前，使用者裝置執行應用在接收自內容提供裝置的加密內容簽名檔案(ECS 檔案)中所設定之 ECS 發行人的簽名之簽名查驗。

在經由此簽名查驗已確認無竄改之事例中，換言之，已確認加密內容簽名檔案(ECS 檔案)的有效性，執行儲存在加密內容簽名檔案(ECS 檔案)中之 ECS 發行人憑證的另一簽名查驗。倘若在兩簽名查驗處理任一者已確認無竄改，則執行步驟 S171 及隨後步驟的處理。

在兩簽名查驗處理中的至少一個已確認有些竄改之事例中，加密內容簽名檔案(ECS 檔案)的有效性或 ECS 發行人憑證的有效性未被確認。如此，不執行步驟 S171 及隨後步驟的處理。在此事例中，也不執行內容再生處理。

在經由加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證之兩簽名查驗處理的任一者已確認無竄改之事例中，換言之，已確認加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證之有效性，使用者裝置執行步驟 S171 的處理。

在步驟 S171 中，使用者裝置讀取記錄在加密內容簽名檔案(ECS 檔案)中之資料項目的 ECS 發行日期，而後讀取記錄在 ECS 發行人憑證中之資料項目的 ECS 發行人憑證截止日期(截止日期)。

另外，經由這些日期資訊項目的比較，使用者裝置判斷 ECS 發行人憑證截止日期(截止日期)是否在 ECS 發行日

期之前。

在已判斷 ECS 發行人憑證截止日期(截止日期)在 ECS 發行日期之前的事例中(Yes)，流程進行到步驟 S175，以取消內容的解密及再生處理。

這是因爲已確認 ECS 發行人憑證已到期。

同時，在步驟 S171 中，在已判斷 ECS 發行人憑證截止日期(截止日期)未在 ECS 發行日期之前的事例中(No)，流程進行到步驟 S172，以執行應用步驟 S173 及隨後步驟中之撤回清單的內容供應可能性判斷處理。

需注意的是，使用者裝置已事先取得參考圖 12 所說明之 ECS 發行人金鑰撤回清單。例如，可從許可發行人(LA)101 取得 ECS 發行人金鑰撤回清單。

在步驟 S173 中，使用者裝置從 ECS 發行人憑證取得 ECS 憑證 ID，及判斷此 ID 是否已登記在 ECS 發行人金鑰撤回清單中。

在此 ID 未被登記在 ECS 發行人金鑰撤回清單中之事例中(No)，確認 ECS 發行人憑證還有效而未使其無效(撤回)。在此事例中，流程進行到步驟 S176 以執行內容再生處理。

需注意的是，在開始內容再生處理之前，不僅執行取得及產生欲待應用到加密內容的解密之標題金鑰的處理，而且執行應用包含在加密內容簽名檔案中之內容雜湊清單集合的雜湊值查驗處理。在經由雜湊值查驗已確認內容無竄改之事例中，允許內容的再生。

同時，在步驟 S173 中，在已判斷 ECS 憑證 ID 被登記在 ECS 發行人金鑰撤回清單中之事例中(Yes)，流程進行到步驟 S174。

在步驟 S174 中，下面兩日期資料項目彼此比較。

使登記在 ECS 發行人金鑰撤回清單中之 ECS 發行人憑證無效(撤回)時的日期，換言之，撤回日期

作爲記錄在加密內容簽名檔案(ECS 檔案)中之資料項目的 ECS 發行日期

在已判斷作爲記錄在加密內容簽名檔案(ECS 檔案)中之資料項目的 ECS 發行日期在撤回日期之前的事例中(Yes)，流程進行到步驟 S176，以執行內容再生處理。

這是因爲內容再生處理可被判斷作依據未撤回有效 ECS 發行人憑證的處理。

同時，在步驟 S173 中，在已判斷作爲記錄在加密內容簽名檔案(ECS 檔案)中之資料項目的 ECS 發行日期未在撤回日期之前的事例中(No)，流程進行到步驟 S175，以取消內容再生處理。

這是因爲內容再生處理可被判斷作依據撤回無效的 ECS 發行人憑證之處理。

[10.使加密金鑰與 ECS 發行人的簽名有關聯之組態]

接著，說明使加密金鑰與 ECS 發行人的簽名彼此有關聯之組態。

如上面參考圖 3 及 6 所說明一般，在使用者裝置 104

中，在例如由快閃記憶體等等所形成之記憶卡等等中記錄內容的同時使用內容等等。

如上面參考圖 3 所說明一般，記憶卡 31 中之儲存區係由下面兩區所形成。

(a)受保護區 51

(b)通用區 52

(b)通用區 52 爲從使用者所使用之記錄/再生裝置的自由可存取區，及記錄內容、對應於內容之使用控制資訊項目(使用規則)、其他一般內容管理資料項目等等。

在通用區 52 中，例如藉由伺服器或使用者的記錄/再生裝置可自由寫入及讀取資料。

同時，(a)受保護區 51 爲不允許自由存取之區域。

受保護區 51 被分成作爲複數個區段區之區塊(#0, #1, #2, ...)，及以區塊爲單位來設定存取權。

例如，當例如以藉由使用者所使用的記錄/再生裝置或透過網路所連接之伺服器寫入或讀取資料時，記憶卡 31 的資料處理單元依據預儲存在記憶卡 31 中之程式來決定是否能夠以區塊爲單位來相對應地執行讀取或寫入到裝置。

記憶卡 31 不僅包括被組構成執行預儲存程式之資料處理單元，而且也包括被組構成執行認證處理之認證處理單元。首先，記憶卡 31 執行有關裝置的認證處理，以寫入或讀取有關記憶卡 31 的資料。

在認證處理的階段中，包括公用金鑰憑證等等之裝置

憑證係接收自配對裝置，換言之，存取請求裝置。

例如，當存取請求裝置爲伺服器時，接收參考圖 5 所說明之由伺服器所擁有的伺服器憑證。然後，依據包含在憑證中之資訊來判斷是否允許以受保護區 51 中之區塊(區段區)爲單位來存取。

同時，當存取請求裝置爲作爲被組構成記錄及再生內容之使用者裝置的諸如記錄/再生裝置(主機)等主機裝置時，接收參考圖 4 所說明之由記錄/再生裝置(主機)所擁有的主機憑證。然後，依據包含在憑證中之資訊來判斷是否允許存取到受保護區 51 的區塊(區段區)。

以圖 3 所示之受保護區 51 中的區塊爲單位(圖 3 所示之區域#0, #1, #2, ...)來執行此種存取權判斷處理。記憶卡 31 使伺服器或主機能夠只執行以區塊爲單位所允許的處理(諸如資料讀取/寫入等處理)。

參考圖 19 說明在使用者裝置 104 接受媒體來記錄接收自內容提供裝置 103 的內容之事例中的資料之組態例子。

圖 19 圖解作爲內容提供裝置的伺服器 A 201 提供及記錄加密內容到插入作爲使用者裝置之主機 202 的記憶卡 210 之處理的例子。

記憶卡 210 包括

受保護區 211，以及

通用區 212。

在提供加密內容之處理時，作爲內容提供裝置之伺服

器 A 201 記錄欲待應用到欲待提供的內容之加密及解密的標題金鑰到受保護區中之預定區塊。

伺服器 A 201 擁有上面參考圖 5 所說明之伺服器憑證。

首先，伺服器 A 201 執行有關記憶卡 210 的相互認證處理，同時輸出伺服器憑證到記憶卡 210。

記憶卡 210 確認記錄在接收自伺服器 A 201 的伺服器憑證中之受保護區存取權資訊項目。

只有在已經由此確認處理判斷伺服器 A 201 具有到區塊#0 之存取權(執行寫入的權利)的事例中，允許伺服器 A 201 能夠寫入資料到設定在記憶卡 210 之受保護區 211 中的區塊#0。

如圖 19 所示，伺服器 A 201 將欲待應用到欲待提供的內容之加密及解密的標題金鑰儲存在受保護區 211 的區塊#0 221 中。

需注意的是，標題金鑰本身未照原樣儲存在受保護區中，但是由於有關標題金鑰 Kt 之下面資訊項目(a)及(b)的序連資料項目之雜湊值的互斥或操作：

(a)使用控制資訊項目(UR：使用規則)

參考圖 9 的(A)所說明之 ECS 檔案的構成資料項目之(b)ECS 發行人的簽名，

所以例如對應於內容(a1)之標題金鑰：Kt(a1)被儲存作爲受保護區中之下面的標題金鑰轉換資料項目。

Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

需注意的是，

UR(a1)表示對應於內容 a1 之使用控制資訊項目，以及

ECSSig(a1)表示 ECS 發行人的簽名，其爲 ECS 檔案的構成資料項目及對應於內容 a1。

另外，作爲運算子之符號的意義被定義如下。

(+)：互斥或操作

||：資料項目的序連，例如，a||b 表示資料項目 a 及資料項目 b 的序連資料項目。

Hash：雜湊值，例如(a||b)hash 表示資料項目 a 及資料項目 b 的序連資料項目之雜湊值。

在圖 19 所示之例子中，伺服器 A 201 記錄下面內容、使用控制資訊項目、及 ECS 檔案在記憶卡 210 之通用型區 212 中。

內容：Con(a1)、Con(a2)、及 Con(a3)

對應於內容之使用控制資訊項目(使用規則)：UR(a1)、UR(a2)、及 UR(a3)

對應於內容之 ECS 檔案：ECS(a1)、ECS(a2)、及 ECS(a3)

記錄幾組這些內容、使用控制資訊項目、及 ECS 檔案。

另外，伺服器 A 201 記錄下面資料項目在記憶卡 210 的受保護區 211 之區塊#0 221 中，換言之，記錄下面之間的互斥或(XOR)操作之結果。

分別對應於內容的標題金鑰

分別對應於內容之使用控制資訊項目(使用規則)及ECS發行人的簽名(ECSSigs)之序連資料項目的雜湊值。

Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

Kt(a3)(+)(UR(a3)||ECSSig(a3))hash

需注意的是，如同在圖 19 所示之伺服器 A 201 的處理之例子一般，例如，另一伺服器 B 儲存類似的標題金鑰轉換資料項目：

Kt(bx)(+)(UR(bx)||ECSSig(bx))hash

在受保護區的預定區塊中，其被允許作爲用於對應於欲待從伺服器 B 所提供之內容(bx)的標題金鑰之儲存區，例如，在區塊#1 中。

圖 20 圖示使用內容之使用者裝置(主機)202 及儲存內容等等之記憶卡 210。

使用者裝置(主機)202 擁有上面參考圖 4 所說明之主機憑證。

首先，使用者裝置(主機)202 執行有關記憶卡 210 的相互認證處理，同時輸出主機憑證到記憶卡 210。

記憶卡 210 確認記錄在接收自使用者裝置(主機)202 的主機憑證中之受保護區存取權資訊項目。

只有在已經由此確認處理判斷使用者裝置(主機)202 具有到區塊#0 之存取權(執行讀取的權利)的事例中，允許使用者裝置(主機)202 能夠從設定在記憶卡 210 之受保護

區 211 中的區塊#0 讀取資料。

在經由相互認證確認存取權之後，使用者裝置(主機)202 執行下面處理來使用內容。

首先，使用者裝置(主機)202 從記憶卡中的通用區 212 取得使用者目標內容：Con(xy)、對應的使用控制資訊項目：UR(xy)、及對應的 ECS 檔案：ECS(xy)。

接著，使用者裝置(主機)202 參考使用控制資訊項目：UR(xy)，以確認使用者目標內容：Con(xy)的標題金鑰儲存在受保護區的哪一區塊中。

儲存使用者目標內容：Con(xy)的標題金鑰之區塊的識別符記錄在使用控制資訊項目：UR(xy)中。

在指定受保護區 211 的哪一區塊儲存標題金鑰之後，使用者裝置(主機)202 執行讀取記錄在區塊中之資料項目的處理。

例如，從選擇的區塊讀取下面資料項目。

Kt(xy)(+)(UR(xy)||ECSSig(xy))hash

接著，使用者裝置(主機)202 執行序連已從通用區 212 讀取之使用者控制資訊項目：UR(xy)及儲存在 ECS 檔案：ECS(xy)中的 ECS 發行人之簽名(ECSSig(xy))的處理，以及計算其雜湊值的處理。

換言之，使用者裝置(主機)202 計算 (UR(xy)||ECSSig(xy))hash，以獲得計算結果 P(xy)。

之後，經由下面計算取得標題金鑰 Kt(xy)。

[讀取自區塊的資料項目(標題金鑰轉換資料項目)](+)P(xy)

=(Kt(xy)(+)(UR(xy)||ECSSig(xy))hash)(+)P(xy)

=(Kt(xy)(+)(UR(xy)||ECSSig(xy))hash)(+)(UR(xy)||ECSSig(xy))hash)

=Kt(xy)

經由此種計算處理，取得標題金鑰 Kt(xy)，及藉由以如此取得的標題金鑰來解密加密內容以使用加密內容。

參考圖 21 說明記錄在記憶卡中之資料項目的例子。

圖 21 圖示欲由兩不同的伺服器(換言之，伺服器 A 及伺服器 B)寫入到記憶卡之資料項目的例子。

伺服器 A 具有到記憶卡之受保護區中的區塊#0 之存取權。

同時，伺服器 B 具有到到記憶卡之受保護區中的區塊#1 之存取權。

伺服器各個記錄內容及其他資料項目到插入作爲使用者裝置之主機裝置內的記憶卡中。

欲從伺服器 A 提供之內容被表示作 Con(a1)、Con(a2)、及 Con(a3)。

欲從伺服器 B 提供之內容被表示作 Con(b1)及 Con(b2)。

如圖 21 所示，伺服器 A 記錄下面資料項目到記憶卡中的通用區。

內容：Con(a1)、Con(a2)、及 Con(a3)

分別對應於內容之使用控制資訊項目(使用規則)：UR(a1)、UR(a2)、及 UR(a3)

分別對應於內容之 ECS 檔案：ECS(a1)、ECS(a2)、及 ECS(a3)

另外，伺服器 A 記錄下面資料項目到記憶卡之受保護區中的區塊#0。

經由欲待應用到上述內容的解密之標題金鑰： Kt(a1)、Kt(a2)、及 Kt(a3)的轉換所取得之資料項目，換言之，

Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

Kt(a3)(+)(UR(a3)||ECSSig(a3))hash

同時，伺服器 B 記錄下面資料項目到記憶卡中之通用區。

內容：Con(b1)及 Con(b2)

分別對應於內容之使用控制資訊項目(使用規則)：UR(b1)及 UR(b2)

分別對應於內容之 ECS 檔案：ECS(b1)及 ECS(b2)

另外，伺服器 B 記錄下面資料項目到記憶卡之受保護區中的區塊#1。

經由欲待應用到上述內容的解密之標題金鑰：Kt(b1)及 Kt(b2)的轉換所取得之資料項目，換言之，

Kt(b1)(+)(UR(b1)||ECSSig(b1))hash

Kt(b2)(+)(UR(b2)||ECSSig(b2))hash

當伺服器各個記錄資料項目到記憶卡中的受保護區時，記憶卡依據伺服器憑證中的記錄來執行存取權的確認，換言之，執行有關區塊的寫入之權利的確認。只有在

已確認存取權之事例中，執行資料寫入。

圖 22 圖示伺服器 A 及伺服器 B 各個具有到記憶卡的受保護區中之區塊#0 的存取權以及伺服器 C 及伺服器 D 各個具有到記憶卡的受保護區中之區塊#1 的存取權之資料記錄例子。

伺服器 A 記錄下面資料項目到記憶卡中的通用區。

內容：Con(a1)、Con(a2)、及 Con(a3)

分別對應於內容之使用控制資訊項目(使用規則)：UR(a1)、UR(a2)、及 UR(a3)

分別對應於內容之 ECS 檔案：ECS(a1)、ECS(a2)、及 ECS(a3)

另外，伺服器 A 記錄下面資料項目到記憶卡之受保護區中的區塊#0。

經由欲待應用到上述內容的解密之標題金鑰：Kt(a1)、Kt(a2)、及 Kt(a3)的轉換所取得之資料項目，換言之，

Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

Kt(a3)(+)(UR(a3)||ECSSig(a3))hash

伺服器 B 記錄下面資料項目到記憶卡中之通用區。

內容：Con(b1)及 Con(b2)

分別對應於內容之使用控制資訊項目(使用規則)：UR(b1)及 UR(b2)

分別對應於內容之 ECS 檔案：ECS(b1)及 ECS(b2)

另外，伺服器 B 記錄下面資料項目到記憶卡之受保護區中的區塊#0。

經由欲待應用到上述內容的解密之標題金鑰：Kt(b1)及 Kt(b2)的轉換所取得之資料項目，換言之，

Kt(b1)(+)(UR(b1)||ECSSig(b1))hash

Kt(b2)(+)(UR(b2)||ECSSig(b2))hash

伺服器 C 記錄下面資料項目到記憶卡中的通用區。

內容：Con(c1)

對應於內容之使用控制資訊項目(使用規則)：UR(c1)

對應於內容之 ECS 檔案：ECS(c1)

另外，伺服器 C 記錄下面資料項目到記憶卡之受保護區中的區塊#1。

經由欲待應用到上述內容的解密之標題金鑰：Kt(c1)的轉換所取得之資料項目，換言之，

Kt(c1)(+)(UR(c1)||ECSSig(c1))hash

伺服器 D 記錄下面資料項目到記憶卡之通用區。

內容：Con(d1)及 Con(d2)

分別對應於內容之使用控制資訊項目(使用規則)：UR(d1)及 UR(d2)

分別對應於內容之 ECS 檔案：ECS(d1)及 ECS(d2)

另外，伺服器 D 記錄下面資料項目到記憶卡之受保護區中的區塊#1。

經由欲待應用到上述內容的解密之標題金鑰：Kt(d1)及 Kt(d2)的轉換所取得之資料項目，換言之，

Kt(d1)(+)(UR(d1)||ECSSig(d1))hash

Kt(d2)(+)(UR(d2)||ECSSig(d2))hash

需注意的是，當執行內容的再生之使用者裝置(主機)選擇欲從通用區再生之內容時，使用者裝置(主機)必須指定欲待再生的內容之標題金鑰儲存在受保護區中的區塊之哪一個。

從對應於內容的每一個之使用控制資訊項目(UR)取得指定區塊之資訊項目。

參考圖 23 說明使用控制資訊項目的使用例子。圖23(a)圖示對應於記錄在記憶卡之通用區中之內容 a1 的使用控制資訊項目(使用規則)a1 之特定例子。

下面資料項目記錄在使用控制資訊項目(使用規則)

(1)區塊識別符(#0)

(2)標題金鑰識別符(a1)

(3)ECS 檔案識別符(a1)

(1)區塊識別符爲指示儲存對應於使用控制資訊項目(使用規則)UR(a1)之內容：Con(a1)的標題金鑰 Kt(a1)之區塊的資訊項目。

在此例中，區塊識別符爲#0，因此允許執行內容的再生之使用者裝置(主機裝置)選擇區塊#0。

(2)標題金鑰識別符爲指示儲存在區塊#0 中之大量標題金鑰的哪一個爲對應於使用控制資訊項目(使用規則)UR(a1)之內容：Con(a1)的標題金鑰之資訊項目。

在此例中，標題金鑰識別符爲 a1，因此允許使用者裝

置(主機裝置)選擇標題金鑰 Kt(a1)。

(3)ECS 檔案識別符(a1)爲用以識別 ECS 檔案的哪一個對應於內容(a1)之資訊項目。

使用者裝置(主機)參考使用控制資訊項目：UR(a1)，以確認對應於使用者目標內容：Con(a1)之標題金鑰儲存在受保護區中的區塊之哪一個。然後，使用者裝置(主機)從指定區塊讀取下面資料項目。

Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

接著，使用者裝置(主機)執行序連已從通用區讀取之使用控制資訊項目：UR(a1)及儲存在 ECS 檔案：ECS(a1)中的 ECS 發行人之簽名(ECSSig(a1))的處理，及計算其雜湊值的處理。

換言之，使用者裝置(主機)計算下面。

P(a1)=(UR(a1)||ECSSig(a1))hash

之後，使用者裝置(主機)執行下面計算以獲得標題金鑰 Kt(xy)。

[讀取自區塊的資料項目(標題金鑰轉換資料項目)](+)P(a1)

=(Kt(a1)(+)(UR(a1)||ECSSig(a1))hash)(+)P(a1)

=(Kt(a1)(+)(UR(a1)||ECSSig(a1))hash)(+)(UR(a1)||ECSSig(a1))hash)

=Kt(a1)

經由此種計算處理，取得標題金鑰 Kt(a1)，及藉由以如此取得的標題金鑰來解密加密內容以使用加密內容。

如上述，欲待記錄到記憶卡中的受保護區之標題金鑰被儲存作爲使用控制資訊項目(UR)及 ECS 發行人的簽名(ECSSig)及標題金鑰之間的序連資料項目之雜湊值的互斥或(XOR)操作之結果。

甚至在將應用到 ECS 發行人的簽名(ECSSig)之來自 ECS 發行人的簽名金鑰(密鑰)已漏洩之事例中，此種處理仍能夠防止內容的詐騙使用。

例如，此種處理使內容提供伺服器或使用者裝置能夠防止內容被應用從 ECS 發行人所發行的漏洩簽名金鑰(密鑰)之詐騙處理所詐騙使用，尤其是，更換加密內容的處理。

需注意的是，更換意指例如藉由使用對應於某內容(C1)之不同標題金鑰(Kt1)來加密其他內容(C2)、(C3)、(C4)、...以及提供如此加密的內容給使用者之處理。

此種處理使擁有標題金鑰(Kt1)的使用者裝置能夠在未合法購買這些內容之下來解密及再生其他內容(C2)、(C3)、(C4)、...。

藉由儲存欲待記錄到記憶卡中的受保護區之標題金鑰來作爲使用控制資訊項目(UR)及 ECS 發行人的簽名(ECSSig)及標題金鑰之間的序連資料項目之雜湊值的互斥或(XOR)操作之結果，可防止上述之更換。

參考圖 24 及隨後圖式來說明防止更換的此種有利點。

圖 24 的(a)圖示對應於內容(C1)之有效資料儲存結

構，以及

圖 24 的(b)圖示藉由使用對應於內容(C1)之標題金鑰(Kt1)加密內容(C2)所產生的更換資料項目之資料儲存結構。

在圖 24 的(a)所示之有效資料儲存結構中，記憶卡中的通用區儲存下面資料項目。

(a1)以對應於內容(C1)之有效標題金鑰(Kt1)所加密的加密內容(C1(Kt1))

(a2)對應於內容(C1)之有效使用控制資訊項目(UR1)內容(C1)

(a3)對應於內容(C1)之有效 ECS 檔案 ECS1(C1, Kt1)

需注意的是，ECS 檔案儲存 ECS 發行人的簽名(ECSSig)，其如上面參考圖 13 所說明包含依據內容(C1)之雜湊清單集合及標題金鑰(Kt1)的雜湊值之資料項目所產生的電子簽名。爲了釐清此簽名資料項目的來源資料項目，ECS 檔案 ECS1 被表示作(C1, Kt1)。

另外，在圖 24 的(a)所示之有效資料儲存結構中，經由標題金鑰(Kt1)的轉換所取得之資料項目，換言之，下面的資料項目被記錄到記憶卡的受保護區中之區塊 N。

Kt1(+)(UR1||ECS1Sig)hash

需注意的是，

UR1 表示對應於內容(C1)之使用控制資訊項目，以及

ECS1Sig 表示 ECS 檔案的構成資料項目及對應於內容(C1)之 ECS 發行人的簽名。

另外，作爲運算子之符號的意義被定義如下。

(+)：互斥或操作

||：資料項目的序連，例如，a||b 表示資料項目 a 及資料項目 b 的序連資料項目。

Hash：雜湊值，例如(a||b)hash 表示資料項目 a 及資料項目 b 的序連資料項目之雜湊值。

例如，惡意的內容提供伺服器會使用標題金鑰(Kt1)到此內容(C1)作爲另一內容(C2)的加密金鑰，及提供此標題金鑰(Kt1)給使用者。

由於此種非法內容的散佈，圖 24 的(b)所示之“更換資料項目”被儲存在記憶卡中。

在圖 24 的(b)所示之“更換資料”儲存結構中，記憶卡中的通用區儲存下面資料項目。

(b1)以有關內容(C2)的詐騙標題金鑰(Kt1)所加密之詐騙加密內容(C2(Kt1))

(b2)詐騙地對應於內容(C2)之使用控制資訊項目(UR1)[應該對應於內容(C1)之使用控制資訊項目(UR1)]

(b3)對應於內容(C2)所詐騙產生之詐騙 ECS 檔案 ECS2(C2, Kt1)

需注意的是，詐騙的 ECS 檔案 ECS2 儲存 ECS 發行人的簽名(ECSSig)，其包含參考從 ECS 發行人發出的漏洩簽名金鑰(密鑰)，依據內容(C2)的雜湊清單集合及對應於內容(C1)的標題金鑰(Kt1)之雜湊值的資料項目所產生之電子簽名。爲了釐清此簽名資料項目的來源資料項目，ECS 檔

案 ECS2 被表示作(C2, Kt1)。

另外，在圖 24 的(b)所示之“更換資料”儲存結構中，經由標題金鑰(Kt1)的轉換所取得之資料項目，換言之，下面資料項目被記錄到記憶卡的受保護區中之區塊 N。

Kt1(+)(UR1||ECS1Sig)hash

參考圖 25 的流程圖說明圖 24 的(b)所示之這些“更換資料項目”的記錄處理之序列。

需注意的是，圖 25 所示之處理爲藉由使用儲存對應於圖 24 的(a)所示之內容(C1)的有效資料組之記憶卡所執行的處理，尤其是，例如藉由具有執行資料讀取處理之權利作爲有關記憶卡的受保護區中之區塊 N 的存取權之內容提供伺服器或使用者裝置所執行的處理。

首先，在步驟 S201 中，準備新的內容 C2。

接著，在步驟 S202 中，“區塊識別符”及“標題金鑰識別符”係取得自記錄在記憶卡的通用區中之內容(C1)的使用控制資訊項目(UR1)。依據這些取得的資訊項目，對應於下面標題金鑰轉換資料項目之正規內容(C1)係讀取自受保護區中的預定區塊，換言之，標題金鑰儲存區塊。

Kt1(+)(UR1||ECS1Sig)hash

需注意的是，ECS1Sig 表示 Sign(ECS 簽名金鑰，M)，及 M 表示內容 C1 的內容雜湊清單集合及 Kt1 之雜湊值的序連資料項目。

接著，在步驟 S203 中，計算已從通用區讀取之對應於正規內容(C1)的使用控制資訊項目(UR1)及 ECS 檔案

(ECS1(C1, Kt1))之序連資料項目的雜湊值。然後，計算結果與已從受保護區讀取的上述標題金鑰轉換資料項目之間的互斥或(XOR)被執行，以取得對應於內容(C1)之正規標題金鑰(Kt1)。

換言之，依據下面等式取得標題金鑰(Kt1)。

Kt1=(讀取自受保護區的資料項目)(+)(讀取自通用區的資料項目)

=Kt1(+)(UR1||ECS1Sig)hash(+)(UR1||ECS1Sig)hash

需注意的是，(+)表示互斥或操作(XOR)。

接著，在步驟 S204 中，以應用步驟 S203 所取得之標題金鑰(Kt1)來加密新內容 C2。

以此方式，產生加密內容 C2(Kt1)。

接著，在步驟 S205 中，加密內容 C2(Kt1)被記錄到記憶卡中的通用區。

接著，在步驟 S206 中，產生對應於依據內容 C2 所產生之內容雜湊清單集合及 Kt1 的雜湊值之加密內容簽名 ECS2Sig。換言之，產生下面簽名資料項目。

ECS2Sig=Sign(ECS 簽名金鑰，M)

需注意的是，M 表示內容 C2 的內容雜湊清單集合及 Kt1 之雜湊值的序連資料項目。

另外，從加密內容簽名發行人所發行之漏洩簽名金鑰(密鑰)被應用到此簽名產生。

最後，在步驟 S207 中，包含在步驟 S206 所詐騙產生之 ECS 簽名的 ECS 檔案(ECS2Sig(C2, Kt1))被產生及記錄

到記憶卡中的通用區。

藉由圖 25 所示之一連串處理，完成記錄圖 24 的(b)所示之“更換資料項目”的處理。

藉由此種更換處理，產生經由應用對應於不同內容(C1)的標題金鑰(Kt1)所加密之內容 C2(Kt1)。

需注意的是，在此例中，對應於內容 C1 之使用控制資訊項目(UR1)照原樣被使用作爲對應於非法記錄的內容 C2(Kt1)之使用控制資訊項目。

接著，參考圖 26 的流程圖說明使用者裝置如何藉由圖 24 的(b)所示之“更換資料項目”來執行再生內容 C2 的處理。

首先，在步驟 S221 中，使用者裝置從記憶卡的通用區讀取欲待再生之加密內容 C2(Kt1)及對應於此所產生之 ECS 檔案(ECS2(C2, Kt1))。

接著，在步驟 S222 中，指示標題金鑰儲存在區塊的哪一個之區塊識別符係讀取自對應於內容 C2 記錄在記憶卡的通用區中之使用控制資訊項目(UR1)。

如上述，在此例中，對應於內容 C1 之使用資訊項目(UR1)照原樣被使用作爲對應於非法記錄的內容 C2(Kt1)之使用控制資訊項目。

如上面參考圖 23 所說明一般，使用控制資訊項目(UR)記錄指示區塊的哪一個儲存標題金鑰、標題金鑰識別符等等之識別符。

在步驟 S222 中，區塊識別符及標題金鑰識別符係讀

取自對應於內容 C1 之使用控制資訊項目(UR1)。

這些區塊識別符及標題金鑰識別符爲分別對應於儲存對應於內容 C1 的正規標題金鑰 Kt1 之區塊及儲存在同一區塊中之標題金鑰的識別符。

如此，如此讀取的資料項目對應於對應於內容 C1 之標題金鑰轉換資料項目，換言之，

Kt1(+)(UR1||ECS1Sig)hash。

接著，在步驟 S223 中，讀取自通用區之使用控制資訊項目(UR1)與對應於內容 C2 所詐騙產生的 ECS 檔案(ECS2(C2, Kt1))之序連資料項目的雜湊值被計算。然後，執行計算結果與已從受保護區讀取的上述標題金鑰轉換資料項目之間的互斥或(XOR)操作，以便取得對應於內容 C2 的解密標題金鑰 Kt2。

在此事例中，當如此取得之標題金鑰 Kt2 等於 Kt1 時，成功取得標題金鑰。

換言之，試圖依據下面等式來執行標題金鑰計算處理。

Kt2=(讀取自受保護區之資料項目)(+)(讀取自通用區之資料項目)

=Kt1(+)(UR1||ECS2Sig)hash(+)(UR1||ECS1Sig)hash

試圖依據此標題金鑰計算等式來取得標題金鑰(Kt2)。

需注意的是，(+)表示互斥或操作(XOR)。

然而，在上述標題金鑰計算等式中建立關係 ECS2Sig ≠ ECS1Sig。如此，依據上述計算等式所取得之值：Kt2 未

等於 Kt1，換言之，建立下面關係。

Kt2 ≠ Kt1

結果，如步驟 S224 所說明一般，使用者裝置無法取得應用到內容 C2 的加密之標題金鑰 Kt1，及內容 C2 的解密及再生失敗。

另外，在步驟 S225 中，依據預設的再生序列，使用者裝置執行查驗包含在讀取自通用區的 ECS 檔案中之 ECS 發行人的簽名(ECSSig)之處理。

依據下面公式執行簽名查驗處理。

查驗(ECS 發行人公用金鑰，ECS2Sig, M)

需注意的是，查驗(k, S, M)表示以查驗金鑰 k 來查驗對應於資料項目 M 之電子簽名 S 的處理。

M 表示內容 C2 之內容雜湊清單集合及 Kt2 的雜湊值的序連資料項目。

步驟 S223 所計算的值被使用作爲 Kt2。

儲存在 ECS 檔案中之 ECS2Sig 爲在圖 25 所示的流程之步驟 S206 中所產生的詐騙簽名，換言之，下面資料項目。

ECS2Sig=Sign(ECS 簽名金鑰, M)

需注意的是，

M 表示內容 C2 之內容雜湊清單集合及 Kt1 的雜湊值的序連資料項目。

如上述，欲待應用到簽名查驗之資料項目 M 爲包含 Kt2 的雜湊值之資料項目。同時，儲存在 ECS 檔案中之簽

名資料項目 ECS2Sig 係對應於包含 Kt1 的雜湊值之 M 所產生。

如此，如圖 26 的步驟 S226 所說明一般，經由步驟 S225 的簽名查驗已確認一些竄改。

以此方式，甚至當嘗試藉由使用圖 24 的(b)所示之“更換資料項目”來解密及再生內容 C2 時，使用者裝置具有下面結果。

解密內容 C2 失敗

經由 ECS 檔案的簽名查驗所確認的一些竄改

結果，無法使用內容 C2。

參考圖 24 至 26 所說明之處理例子爲嘗試藉由應用對應於內容 C1 的標題金鑰 Kt1 來加密及解密新內容 C2 之處理例子。

接著，參考圖 27 及隨後圖式說明對應於內容 C1 的正規使用控制資訊項目(UR1)被詐騙竄改以產生新的使用控制資訊項目(UR2)之事例的例子。

使用控制資訊項目記錄內容的可使用時間週期、拷貝限制資訊項目等等之資訊項目。如此，可藉由重寫此使用控制資訊項目來執行諸如使用截止日期的延長等詐騙。

類似於上述的圖 24，圖 27 包括下面。

圖 27 的(a)圖示對應於內容(C1)之有效資料儲存結構，以及

圖 27 的(b)圖示藉由使用對應於內容(C1)之標題金鑰(Kt1)加密內容(C2)所產生的更換資料項目之資料儲存結

構。

在圖 27 的(a)所示之有效資料儲存結構中，記憶卡中的通用區儲存下面資料項目。

(a1)以對應於內容(C1)之有效標題金鑰(Kt1)所加密的加密內容(C1(Kt1))

(a2)對應於內容(C1)之有效使用控制資訊項目(UR1)

(a3)對應於內容(C1)之有效 ECS 檔案 ECS1(C1, Kt1)

需注意的是，ECS 檔案儲存 ECS 發行人的簽名(ECSSig)，其如上面參考圖 13 所說明包含依據內容(C1)之雜湊清單集合及標題金鑰(Kt1)的雜湊值之資料項目所產生的電子簽名。爲了釐清此簽名資料項目的來源資料項目，ECS 檔案 ECS1 被表示作(C1, Kt1)。

另外，在圖 27 的(a)所示之有效資料儲存結構中，經由標題金鑰(Kt1)的轉換所取得之資料項目，換言之，下面的資料項目被記錄到記憶卡的受保護區中之區塊 N。

Kt1(+)(UR1||ECS1Sig)hash

需注意的是，

UR1 表示對應於內容(C1)之使用控制資訊項目，以及

ECS1Sig 表示 ECS 檔案的構成資料項目及對應於內容(C1)之 ECS 發行人的簽名。

另外，作爲運算子之符號的意義被定義如下。

(+)：互斥或操作

||：資料項目的序連，例如，a||b 表示資料項目 a 及資料項目 b 的序連資料項目。

Hash：雜湊值，例如(a||b)hash 表示資料項目 a 及資料項目 b 的序連資料項目之雜湊值。

例如，惡意的內容提供伺服器或使用者裝置會重寫對應於此內容(C1)的使用控制資訊項目(UR1)。

由於此種詐騙處理，圖 27 的(b)所示之“更換資料項目”被儲存在記憶卡中。

在圖 27 的(b)所示之“更換資料”儲存結構中，記憶卡中的通用區儲存下面資料項目。

(b1)以有關內容(C1)之詐騙產生的標題金鑰(Kt2)所加密之詐騙加密內容(C1(Kt2))

(b2)對應於內容(C1)所詐騙產生之使用控制資訊項目(UR2)

(b3)對應於內容(C1)所詐騙產生之詐騙 ECS 檔案 ECS2(C1, Kt2)

需注意的是，詐騙 ECS 檔案 ECS2 儲存 ECS 發行人的簽名(ECSSig)，其包含參考從 ECS 發行人發出的漏洩簽名金鑰(密鑰)，依據內容(C1)的雜湊清單集合及詐騙產生的標題金鑰(Kt2)之雜湊值的資料項目所產生之電子簽名。爲了釐清此簽名資料項目的來源資料項目，ECS 檔案 ECS2 被表示作(C1, Kt2)。

另外，在圖 27 的(b)所示之“更換資料”儲存結構中，經由標題金鑰(Kt1)的轉換所取得之資料項目，換言之，下面資料項目被記錄到記憶卡的受保護區中之區塊 N。

Kt1(+)(UR1||ECS1Sig)hash

參考圖 28 的流程圖說明圖 27 的(b)所示之這些“更換資料項目”的記錄處理之序列。

需注意的是，圖 28 所示之處理爲藉由使用儲存對應於圖 27 的(a)所示之內容(C1)的有效資料組之記憶卡所執行的處理，尤其是，例如藉由具有執行資料記錄處理之權利作爲有關記憶卡的受保護區中之區塊 N 的存取權之內容提供伺服器或使用者裝置所執行的處理。

首先，在步驟 S241 中，對應於內容 C1 之使用控制資訊項目 UR1 係讀取自通用區，而後諸如重寫可使用時間週期資訊項目等竄改被執行，以取得詐騙使用控制資訊項目(UR2)。

接著，在步驟 S242 中，“區塊識別符”及“標題金鑰識別符”係取得自記錄在記憶卡的通用區中之內容(C1)的使用控制資訊項目(UR1)。依據這些取得的資訊項目，對應於下面標題金鑰轉換資料項目之正規內容(C1)係讀取自受保護區中的預定區塊，換言之，標題金鑰儲存區塊。

Kt1(+)(UR1||ECS1Sig)hash

需注意的是，ECS1Sig 表示 Sign(ECS 簽名金鑰，M)，及 M 表示內容 C1 的內容雜湊清單集合及 Kt1 之雜湊值的序連資料項目。

接著，在步驟 S243 中，計算已從通用區讀取之對應於正規內容(C1)的使用控制資訊項目(UR1)及 ECS 檔案(ECS1(C1, Kt1))之序連資料項目的雜湊值。然後，計算結果與已從受保護區讀取的上述標題金鑰轉換資料項目之間

的互斥或(XOR)被執行，以取得對應於內容(C1)之正規標題金鑰(Kt1)。

換言之，依據下面等式取得標題金鑰(Kt1)。

Kt1=(讀取自通用區的資料項目)(+)(讀取自受保護區的資料項目)

=(UR1||ECS1Sig)hash(+)Kt1(+)(UR1||ECS1Sig)hash

需注意的是，(+)表示互斥或操作(XOR)。

另外，欲待應用到內容 C2 的加密及解密之標題金鑰 Kt2 係依據下面等式所計算。

Kt2=(Kt1(+)(UR1||ECS1Sig)hash(+)(UR2||ECS1Sig)hash

接著，在步驟 S244 中，步驟 S243 所產生的標題金鑰 Kt1 被應用來解密內容 C1(Kt1)。另外，步驟 S243 所產生的新標題金鑰 Kt2 被應用來加密內容 C1，以產生加密內容 C1(Kt2)。

接著，在步驟 S245 中，加密內容 C1(Kt2)被記錄到記憶卡中的通用區。

接著，在步驟 S246 中，產生對應於依據內容 C1 所產生之內容雜湊清單集合及 Kt2 的雜湊值之加密內容簽名 ECS2Sig。換言之，產生下面簽名資料項目。

ECS2Sig=Sign(ECS 簽名金鑰，M)

需注意的是，M 表示內容 C1 的內容雜湊清單集合及 Kt2 之雜湊值的序連資料項目。

另外，從加密內容簽名發行人所發行之漏洩簽名金鑰(密鑰)被應用到此簽名產生。

接著，在步驟 S247 中，包含在步驟 S246 所詐騙產生之 ECS 簽名的 ECS 檔案(ECS2Sig(C1, Kt2))被產生及記錄到記憶卡中的通用區。

最後，在步驟 S248 中，步驟 S241 所產生之使用控制資訊項目(UR2)被記錄到通用區。

藉由圖 28 所示之一連串處理，完成記錄圖 27 的(b)所示之“更換資料項目”的處理。

藉由此種更換處理，詐騙產生的使用控制資訊項目(UR2)係對應於內容 C1。

需注意的是，內容 C1 在以新的標題金鑰 Kt2 加密的同時被記錄。

接著，參考圖 29 的流程圖說明使用者裝置如何藉由圖 27 的(b)所示之“更換資料項目”來執行再生內容 C1 的處理。

首先，在步驟 S261 中，使用者裝置從記憶卡的通用區讀取欲待再生之加密內容 C1(Kt2)及對應於此所產生之 ECS 檔案(ECS2(C1, Kt2))。

接著，在步驟 S262 中，指示標題金鑰儲存在區塊的哪一個之區塊識別符及標題金鑰識別符係讀取自對應於記憶卡的通用區中的內容 C1 所詐騙產生之新的使用控制資訊項目(UR2)。

這些區塊識別符及標題金鑰識別符被設定成與有效未竄改之使用控制資訊項目(UR1)的那些保持相同。

換言之，這些區塊識別符及標題金鑰識別符爲分別對

應於儲存對應於內容 C1 的正規標題金鑰 Kt1 之區塊及儲存在同一區塊中之標題金鑰的識別符。

如此，如此讀取的資料項目對應於對應於內容 C1 之標題金鑰轉換資料項目，換言之，

Kt1(+)(UR1||ECS1Sig)hash。

在步驟 S263 中，讀取自通用區並且詐騙產生之使用控制資訊項目(UR2)與非法產生的 ECS 檔案(ECS2(C1, Kt2))之序連資料項目的雜湊值被計算。然後，執行計算結果與已從受保護區讀取的上述標題金鑰轉換資料項目之間的互斥或(XOR)操作，以便取得對應於內容 C1 的解密標題金鑰 Kt3。

在此事例中，當如此取得之標題金鑰 Kt3 等於 Kt2 時，成功取得標題金鑰。

接著，在步驟 S263 中，試圖依據下面等式來執行標題金鑰計算處理。

Kt3=(讀取自受保護區之資料項目)(+)(讀取自通用區之資料項目)

=Kt1(+)(UR1||ECS1Sig)hash(+)(UR2||ECS2Sig)hash

依據此標題金鑰計算等式產生標題金鑰(Kt3)。

需注意的是，(+)表示互斥或操作(XOR)。

然而，在上述標題金鑰計算等式中無法取得 Kt2。如此，依據上述計算等式所取得之值：Kt3 未等於 Kt1 或 Kt2，換言之，建立下面關係。

$Kt3 \neq Kt2$

Kt3 ≠ Kt1

結果，如步驟 S264 所說明一般，使用者裝置無法取得應用到內容 C1 的再加密之標題金鑰 Kt2，及內容 C1 的解密及再生失敗。

另外，在步驟 S265 中，依據預設的再生序列，使用者裝置執行查驗包含在讀取自通用區的 ECS 檔案中之 ECS 發行人的簽名(ECSSig)之處理。

依據下面公式執行簽名查驗處理。

查驗(ECS 發行人公用金鑰，ECS2Sig, M)

需注意的是，查驗(k, S, M)表示以查驗金鑰 k 來查驗對應於資料項目 M 之電子簽名 S 的處理。

M 表示內容 C1 之內容雜湊清單集合及 Kt3 的雜湊值的序連資料項目。

步驟 S263 所計算的值被使用作爲 Kt3。

儲存在 ECS 檔案中之 ECS2Sig 爲在圖 28 所示的流程之步驟 S246 中所產生的詐騙簽名，換言之，下面資料項目。

ECS2Sig=Sign(ECS 簽名金鑰, M)

需注意的是，

M 表示內容 C1 之內容雜湊清單集合及 Kt2 的雜湊值的序連資料項目。

如上述，欲待應用到簽名查驗之資料項目 M 爲包含 Kt3 的雜湊值之資料項目。同時，儲存在 ECS 檔案中之簽名資料項目 ECS2Sig 係對應於包含 Kt2 的雜湊值之 M 所

產生。

如此，如圖 29 的步驟 S266 所說明一般，經由步驟 S265 的簽名查驗已確認一些竄改。

以此方式，甚至當嘗試藉由使用圖 27 的(b)所示之“更換資料項目”來解密及再生內容 C1 時，使用者裝置具有下面結果。

解密內容 C1 失敗

經由 ECS 檔案的簽名查驗所確認的一些竄改

結果，無法使用內容 C1。

如上述，當儲存欲待記錄到記憶卡中的受保護區之標題金鑰作爲使用控制資訊項目(UR)及 ECS 發行人的簽名(ECSSig)及標題金鑰之間的序連資料項目之雜湊值的互斥或(XOR)操作之結果時，甚至在欲待應用到 ECS 發行人的簽名(ECSSig)之從 ECS 發行人所發行的簽名金鑰(密鑰)已漏洩之事例中，仍可防止內容的詐騙使用。

例如，此種處理使內容提供伺服器或使用者裝置能夠防止內容被應用從 ECS 發行人所發行的漏洩簽名金鑰(密鑰)之詐騙處理所詐騙使用，尤其是，更換加密金鑰到加密內容及竄改使用者控制資訊項目之處理。

[11.應用記錄在加密內容簽名(ECS)檔案中的區塊識別符之處理]

接著，說明應用記錄在加密內容簽名(ECS)檔案中的區塊識別符(PAD 區塊號碼)之處理。

如上面參考圖 9 的(A)所說明一般，區塊識別符(PAD 區塊號碼)被記錄在加密內容簽名(ECS)檔案中。

如參考圖 13 所說明一般，區塊識別符(PAD 區塊號碼)爲欲從內容提供裝置(內容伺服器)103 通知加密內容簽名(ECS)發行人 102 之資料項目，尤其是，指示媒體中的受保護區之區塊的哪一個儲存作爲對應於從內容提供裝置 103 提供給使用者裝置 104 之內容的加密金鑰之標題金鑰的識別符。換言之，區塊識別符(PAD 區塊號碼)爲指示內容提供裝置 103 可使用媒體中的受保護區之區塊的哪一個之識別符。

如上面參考例如圖 3 及 6 所說明一般，事先設定內容提供裝置 103 可使用媒體中的受保護區之區塊的哪一個，及記錄此種存取允許區塊的資訊項目。

另外，如參考圖 9 的(B)所說明一般，對應於區塊識別符(PAD 區塊號碼)之資訊項目亦被記錄在 ECS 發行人憑證中。

如上面參考圖 9 的(B)所說明一般，記錄下面資料項目。

(a)區塊識別符起始號碼(起始 PAD 區塊號碼)

(b)區塊識別符範圍(PAD 區塊號碼計數)

(a)區塊識別符起始號碼(起始 PAD 區塊號碼)爲內容提供裝置 103 允許 ECS 發行人 102 能夠進行存取的媒體中之受保護區的存取允許區塊之起始號碼。

(b)區塊識別符範圍(PAD 區塊號碼計數)爲指示內容提

供裝置 103 允許 ECS 發行人 102 能夠進行存取的媒體中之受保護區的存取允許區塊之起始號碼的範圍之資訊項目。

另外，如上面參考圖 23 所說明一般，不同區塊識別符亦記錄到對應於內容之使用控制資訊項目(UR)。記錄在使用控制資訊項目(UR)之不同區塊識別符爲指示區塊的哪一個儲存對應於內容之標題金鑰的識別符。

圖 30 圖示下面之間的對應性。

加密內容簽名(ECS)檔案

使用控制資訊項目(UR)

記錄在加密內容簽名(ECS)檔案及使用控制資訊項目(UR)中之區塊識別符

受保護區中之標題金鑰儲存區塊(圖式中的區塊 k)

如圖 30 所示，記憶卡中的通用區儲存對應於內容之下面資料項目。

加密內容簽名(ECS)檔案

使用控制資訊項目(UR)

另外，受保護區中的區塊 k 儲存經由對應於內容之標題金鑰的轉換所取得之資料項目，換言之，

Kt(+)UR||(ECSSig)hash。

提供內容給使用者裝置之內容提供裝置比較作爲記錄在內容提供裝置本身的主機憑證(參考圖 4)中之受保護區存取權資訊項目的區塊識別符與作爲 ECS 發行人憑證中之區塊識別符的寫入允許區資訊項目。

依據此比較的結果，判斷是否能夠提供內容。

另外，執行內容的再生之使用者裝置將使用控制資訊項目中的區塊識別符與 ECS 檔案中的區塊識別符彼此比較。

依據此比較的結果，判斷是否能夠再生內容。

首先，參考圖 31 所示之流程圖說明內容提供裝置如何藉由使用區塊識別符來判斷是否能夠提供內容的序列。

作爲圖 31 所示之流程圖中的步驟 S401 之預處理，內容提供裝置執行應用設定在接收自加密內容簽名(ECS)發行人的加密內容簽名檔案(ECS 檔案)之 ECS 發行人的簽名之簽名查驗。

在經由此簽名查驗已確認無竄改之事例中，換言之，已確認加密內容簽名檔案(ECS 檔案)的有效性，執行儲存在加密內容簽名檔案(ECS 檔案)中之 ECS 發行人憑證的另一簽名查驗。倘若在兩簽名查驗處理二者中已確認無竄改，則執行步驟 S401 及隨後步驟的處理。

在兩簽名查驗處理中的至少一個已確認有些竄改之事例中，加密內容簽名檔案(ECS 檔案)的有效性或 ECS 發行人憑證的有效性未被確認。如此，不執行步驟 S401 及隨後步驟的處理。在此事例中，也不執行內容提供處理。

需注意的是，作爲儲存在加密內容簽名檔案(ECS 檔案)中之內容雜湊清單集合的來源資料之內容雜湊，設定有加密內容的雜湊或未加密內容的雜湊。

在經由加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證之兩簽名查驗處理的二者已確認無竄改之事例中，換言

之，已確認加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證之有效性，內容提供裝置執行步驟 S401 的處理。

首先，在步驟 S401 中，內容提供裝置讀取 ECS 檔案中之 ECS 發行人憑證，以讀取記錄在 ECS 發行人憑證中之區塊識別符的資訊項目。

參考圖 32 所示之流程圖說明此步驟 S401 的細節。

在步驟 S421 中，從 ECS 發行人憑證讀取區塊識別符起始號碼(起始 PAD 區塊號碼)。

區塊識別符起始號碼(起始 PAD 區塊號碼)爲 ECS 發行人 102 允許內容提供裝置 103 能夠進行存取的媒體中之受保護區的存取允許區塊之起始號碼。

接著，在步驟 S422 中，判斷 ECS 發行人憑證中之區塊識別符起始號碼(起始 PAD 區塊號碼)是否爲 0xFFFFFFFF。

需注意的是，當區塊識別符起始號碼(起始 PAD 區塊號碼)爲 0xFFFFFFFF 時，允許存取到所有區塊。

在步驟 S422 中，在已判斷區塊識別符起始號碼(起始 PAD 區塊號碼)爲 0xFFFFFFFF 之事例中，流程進行到步驟 S423，以將媒體中的受保護區之所有區塊視作存取允許區塊。

同時，在步驟 S422 中，在已判斷區塊識別符起始號碼(起始 PAD 區塊號碼)非 0xFFFFFFFF 之事例中，流程進行到步驟 S424。

在步驟 S424 中，從 ECS 發行人憑證讀取區塊識別符範圍(PAD 區塊號碼計數)。

區塊識別符範圍(PAD 區塊號碼計數)爲指示內容提供裝置 103 允許 ECS 發行人 102 能夠進行存取的媒體中之受保護區的存取允許區塊之起始號碼的範圍之資訊項目。

隨後步驟 S425 至 S428 中的處理各個爲增加指示連續從 0 至 1、2、3、...之區塊識別符的變數 I 之反覆常式。

首先，在步驟 S425 中，設定下面等式。

變數：I=1

接著，在步驟 S426 中，區塊識別符起始號碼(起始 PAD 區塊號碼)+ I 被添加到區塊識別符清單(PAD 區塊號碼清單)。

接著，在步驟 S427 中，建立下面等式。

I=I+1

接著，在步驟 S428 中，判斷 I 是否等於區塊識別符範圍(PAD 區塊號碼計數)。

當 I 等於時，完成流程。同時，當 I 不等於時，流程回到步驟 S426 以重複處理。

依據此流程，執行圖 31 所示之流程的步驟 S401 之處理。

在步驟 S401 中，ECS 發行人憑證中之區塊識別符起始號碼(起始 PAD 區塊號碼)及區塊識別符範圍(PAD 區塊號碼計數)被應用來計算由 ECS 發行人憑證所定義的存取允許範圍。然後，存取允許範圍被設定作存取允許區塊識別符清單。

接著，在步驟 S402 中，判斷在步驟 S401 中所產生之

存取允許區塊識別符清單是否包含被說明作記錄在加密內容簽名(ECS)檔案中的資料項目之區塊識別符(PAD 區塊號碼)。

當存取允許區塊識別符清單未包含區塊識別符(PAD區塊號碼)時，流程進行到步驟 S405，不執行提供內容給使用者裝置之處理。

同時，當存取允許區塊識別符清單包含區塊識別符(PAD 區塊號碼)時，流程進行到步驟 S403。

在步驟 S403 中，判斷被說明作記錄在加密內容簽名(ECS)檔案中的資料項目之區塊識別符(PAD 區塊號碼)是否匹配記錄在使用控制資訊項目(UR)中的區塊識別符。

當區塊識別符(PAD 區塊號碼)未匹配不同區塊識別符時，流程進行到步驟 S405，不執行提供內容給使用者裝置之處理。

同時，當區塊識別符(PAD 區塊號碼)匹配不同區塊識別符時，流程進行到步驟 S404，以執行提供內容給使用者裝置之處理。

以此方式，內容提供裝置判斷是否滿足下面條件(a)及(b)二者。

(a)記錄在加密內容簽名(ECS)檔案中之區塊識別符(PAD 區塊號碼)落在記錄在 ECS 發行人憑證中的存取允許區塊範圍內。

(b)記錄在加密內容簽名(ECS)檔案中之區塊識別符(PAD 區塊號碼)匹配記錄在使用控制資訊項目(UR)中的不

同區塊識別符。

只有當滿足條件(a)及(b)二者時，內容被提供給使用者裝置。

接著，參考圖 33 所示之流程圖說明執行內容再生處理的使用者裝置如何執行應用區塊識別符之處理。

需注意的是，在圖 33 所示之步驟 S451 之前，使用者裝置執行應用設定在接收自內容提供裝置的加密內容簽名檔案(ECS 檔案)中之 ECS 發行人的簽名之簽名查驗。

在經由此簽名查驗已確認無竄改之事例中，換言之，已確認加密內容簽名檔案(ECS 檔案)的有效性，執行儲存在加密內容簽名檔案(ECS 檔案)中之 ECS 發行人憑證的另一簽名查驗。倘若在兩簽名查驗處理二者中已確認無竄改，則執行步驟 S451 及隨後步驟的處理。

在兩簽名查驗處理中的至少一個已確認有些竄改之事例中，加密內容簽名檔案(ECS 檔案)的有效性或 ECS 發行人憑證的有效性未被確認。如此，不執行步驟 S451 及隨後步驟的處理。在此事例中，也不執行內容再生處理。

在經由加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證之兩簽名查驗處理二者已確認無竄改之事例中，換言之，已確認加密內容簽名檔案(ECS 檔案)及 ECS 發行人憑證之有效性，使用者裝置執行步驟 S451 的處理。

在步驟 S451 中，執行與上面被說明作由內容提供裝置的處理之圖 31 所示的流程中之步驟 S401 的處理相同之處理。換言之，如參考圖 32 所示的流程詳細說明一般，

ECS 發行人憑證中之區塊識別符起始號碼(起始 PAD 區塊號碼)及區塊識別符範圍(PAD 區塊號碼計數)被應用來計算由 ECS 發行人憑證所定義的存取允許範圍。然後，存取允許範圍被設定作存取允許區塊識別符清單。

接著，在步驟 S452 中，判斷步驟 S451 所產生之存取允許區塊識別符清單是否包含被說明作記錄在加密內容簽名(ECS)檔案中的資料項目之區塊識別符(PAD 區塊號碼)。

當存取允許區塊識別符清單未包含區塊識別符(PAD 區塊號碼)時，流程進行到步驟 S455，不執行再生內容之處理。

同時，當存取允許區塊識別符清單包含區塊識別符(PAD 區塊號碼)時，流程進行到步驟 S453。

在步驟 S453 中，判斷被說明作記錄在加密內容簽名(ECS)檔案中的資料項目之區塊識別符(PAD 區塊號碼)是否匹配記錄在使用控制資訊項目(UR)中的區塊識別符。

當區塊識別符(PAD 區塊號碼)未匹配不同區塊識別符時，流程進行到步驟 S455，不執行再生內容之處理。

同時，當區塊識別符(PAD 區塊號碼)匹配不同區塊識別符時，流程進行到步驟 S454，以執行再生內容之處理。

需注意的是，在開始內容再生處理之前，不僅執行取得及產生欲待應用到加密內容的解密之標題金鑰的處理，而且執行應用包含在加密內容簽名檔案中之內容雜湊清單

集合的雜湊值查驗處理。在經由雜湊值查驗已確認內容無竄改之事例中，允許內容的再生。

以此方式，再生內容的使用者裝置判斷是否滿足下面條件(a)及(b)二者。

(a)記錄在加密內容簽名(ECS)檔案中之區塊識別符(PAD區塊號碼)落在記錄在ECS發行人憑證中的存取允許區塊範圍內。

(b)記錄在加密內容簽名(ECS)檔案中之區塊識別符(PAD區塊號碼)匹配記錄在使用控制資訊項目(UR)中的不同區塊識別符。

只有當滿足條件(a)及(b)二者時，使用者裝置再生內容。

[12.各個裝置的硬體組態例子]

最後，參考圖34說明執行上面所說明之處理的裝置之每一個的硬體組態例子。

圖34圖示資訊處理裝置的硬體組態例子，其可應用到圖7及8所示之使用者裝置104、內容提供裝置103、加密內容簽名發行人102、許可發行人101的任一者。

CPU(中央處理單元)701充作依據儲存在ROM(唯讀記憶體)702或儲存單元708中的程式來執行各種處理之資料處理單元。例如，CPU 701依據上述流程圖來執行處理。RAM(隨機存取記憶體)703適當儲存欲待由CPU 701執行之程式、資料項目等等。這些CPU 701、ROM 702、及

RAM 703 以匯流排 704 彼此連接。

CPU 701 透過匯流排 704 連接到輸入/輸出介面 705。具有包括各種開關、鍵盤、滑鼠、及麥克風之輸入單元 706，以及包括顯示器及揚聲器之輸出單元 707 連接到輸入/輸出介面 705。CPU 701 執行各種處理，以回應從輸入單元 706 輸入的命令，及將處理結果輸出給例如輸出單元 707。

連接到輸入/輸出介面 705 之儲存單元 708 包括例如硬碟，及儲存欲待由 CPU 701 執行之程式與各種資料項目。通訊單元 709 透過諸如網際網路及區域網路等網路與外部裝置通訊。

連接到輸入/輸出介面 705 之驅動器 710 驅動諸如磁碟、光碟、磁光碟、及諸如記憶卡等半導體記憶體等可移動媒體 711，與取得儲存在其內之各種資料項目，諸如內容及金鑰資訊項目等。例如，藉由使用內容及金鑰資料項目，依據欲待由 CPU 執行之再生程式，在內容上執行解密處理、再生處理等等。

圖 35 圖示作爲資訊儲存裝置之記憶卡的硬體組態例子。

CPU(中央處理單元)801 充作依據儲存在 ROM(唯讀記憶體)802 或儲存單元 807 中的程式來執行各種處理之資料處理單元。例如，CPU 801 執行到上面實施例所說明之伺服器及主機裝置的通訊處理，諸如有關儲存單元 807 的資料之讀取及寫入，及以儲存單元 807 中的受保護區 811 之

區段區爲單位的存取可能性判斷處理等處理。RAM(隨機存取記憶體)803 適當儲存欲待由 CPU 801 執行之程式、資料項目等等。這些 CPU 801、ROM 802、及 RAM 803 以匯流排 804 彼此連接。

CPU 801 透過匯流排 804 連接到輸入/輸出介面 805。具有通訊單元 806 及儲存單元 807 連接到輸入/輸出介面 805。

連接到輸入/輸出單元 805 之通訊單元 806 執行例如到伺服器及主機的通訊。儲存單元 807 爲資料的儲存區，及如上述包括設定存取限制之受保護區 811 與可自由讀取資料之通用區 812。

在上面實施例所說明的典型例子中，欲待由內容提供裝置提供之內容爲加密內容。然而，根據本揭示的實施例之組態並未侷限於欲待提供的內容爲加密內容之事例，而是可應用到欲待提供的內容爲未加密的明文內容之事例。需注意的是，在內容爲明文內容之事例中，在上面實施例所說明之標題金鑰包括諸如值全都是零的金鑰資料項目等相關技藝中之資料字串前提下，可執行與上面所說明之加密內容提供處理相同的處理。

[13.本揭示的組態之摘要]

在上文中，已參考特定實施例詳細說明本揭示的實施例。然而，事實上，在不違背本揭示的主旨之下，精於本技藝之人士可進行實施例的修改及更換。換言之，本揭示

僅被說明作爲圖解，因此不應被限制性闡釋。應該依據附錄的申請專利範圍來判斷本揭示的主旨。

需注意的是，說明書所揭示的技術可包括下面組態。

(1)資訊儲存裝置，包括儲存單元，被組構成儲存加密內容及欲待應用到加密內容的解密之加密金鑰，儲存單元包括

受保護區，在受保護區中，儲存轉換的加密金鑰及設定存取限制，轉換的加密金鑰爲經由加密金鑰之轉換所取得的資料項目，以及

通用區，其儲存加密內容及對應於加密內容所設定之加密內容簽名檔案，加密內容簽名檔案包含指示在受保護區的區域中哪一個允許轉換的加密金鑰之儲存的區塊識別符作爲記錄資料項目，以允許再生裝置能夠執行應用區塊識別符之內容再生可能性判斷，再生裝置被組構成從儲存單元讀取加密內容及執行再生處理。

(2)根據項目(1)之資訊儲存裝置，其中

加密內容簽名檔案包含 ECS(加密內容簽名)發行人憑證，其儲存來自加密內容簽名檔案的發行人之 ECS 發行人的公用金鑰，ECS 發行人憑證包含作爲在受保護區之各區域中允許轉換的加密金鑰之儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

資訊儲存裝置允許再生裝置能夠判斷記錄在加密內容簽名檔案中之區塊識別符是否落在記錄在 ECS 發行人憑證中的區塊識別符範圍內，及依據判斷的結果來決定是否能

夠再生加密內容，再生裝置被組構成從儲存單元讀取加密內容及執行該再生處理。

(3)根據項目(1)或(2)之資訊儲存裝置，其中

通用區另儲存對應於加密內容之使用控制資訊項目，使用控制資訊項目爲包含指示在哪一個區塊儲存加密金鑰之不同區塊識別符的資訊項目，以及

資訊儲存裝置允許再生裝置能夠判斷記錄在加密內容簽名檔案中之區塊識別符是否匹配記錄在使用控制資訊項目中之不同區塊識別符，及依據判斷的結果來決定是否能夠再生加密內容，再生裝置被組構成從儲存單元讀取加密內容及執行再生處理。

(4)資訊處理裝置，包括

資料處理單元，被組構成執行記錄在媒體中之加密內容的解密處理及再生處理，資料處理單元被組構成

從媒體讀取對應於加密內容所設定之加密內容簽名檔案，

從加密內容簽名檔案取得區塊識別符，區塊識別符指示在哪一個區域允許欲待應用到加密內容的解密之加密金鑰的儲存，以及

執行應用區塊識別符之內容再生可能性判斷處理。

(5)根據項目(4)之資訊處理裝置，其中

加密內容簽名檔案包含 ECS 發行人憑證，其儲存來自加密內容簽名檔案的發行人之 ECS 發行人之公用金鑰，

ECS 發行人憑證包含作爲在各區域中允許加密之儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

資料處理單元判斷記錄在加密內容簽名檔案中之區塊識別符是否落在記錄在 ECS 發行人憑證中的區塊識別符範圍內，及依據判斷的結果來決定是否能夠再生加密內容。

(6)根據項目(4)或(5)之資訊處理裝置，其中

媒體另儲存對應於加密內容之使用控制資訊項目，使用控制資訊項目爲包含指示在哪一個區塊儲存加密金鑰之不同區塊識別符的資訊項目，以及

資料處理單元判斷記錄在加密內容簽名檔案中之區塊識別符是否匹配記錄在使用控制資訊項目中之不同區塊識別符，及依據判斷的結果來決定是否能夠再生加密內容。

(7)資訊處理裝置，包括

資料處理單元，被組構成輸出欲待記錄到媒體之加密內容及欲待應用到加密內容的解密之加密金鑰，資料處理單元被組構成

取得對應於加密內容所設定之加密內容簽名檔案，

從加密內容簽名檔案取得區塊識別符，區塊識別符指示在哪一個區域允許加密金鑰之儲存，以及

執行應用區塊識別符之內容輸出可能性判斷處理。

(8)根據項目(7)之資訊處理裝置，其中

加密內容簽名檔案包含 ECS 發行人憑證，其儲存來自

加密內容簽名檔案的發行人之 ECS 發行人之公用金鑰，ECS 發行人憑證包含作爲在各區域中允許加密金鑰之儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

資料處理單元判斷記錄在加密內容簽名檔案中之區塊識別符是否落在記錄在 ECS 發行人憑證中的區塊識別符範圍內，及依據判斷的結果來決定是否能夠輸出加密內容。

(9)根據項目(7)或(8)之資訊處理裝置，其中

資料處理單元被組構成

取得對應於加密內容所設定之使用控制資訊項目，

從取得的使用控制資訊項目取得不同區塊識別符，其指示在哪一個區塊儲存加密金鑰，

判斷記錄在加密內容簽名檔案中之區塊識別符是否匹配記錄在使用控制資訊項目中之不同區塊識別符，以及

依據判斷的結果來決定是否能夠再生加密內容。

另外，根據本揭示的實施例之組態包括執行處理之方法以及執行上述裝置及系統中的處理之程式。

另外，說明書所說明的一連串處理係可藉由硬體、軟體、或硬體及軟體的合成組態來執行。當由軟體執行處理時，可以儲存處理序列及安裝在結合在專用硬體中之電腦的記憶體或安裝在能夠執行各種處理之通用型電腦中的程式來執行處理。例如，可將程式事先記錄在技藝媒體中，及可從記錄媒體安裝到電腦。另一選擇是，可透過諸如網

際網路或 LAN(區域網路)等網路來接收程式，而後安裝到諸如內建硬碟等記錄媒體。

需注意的是，此說明書所說明的各種處理不僅可以根據說明書之時間序列來執行，而且可以根據執行處理之裝置的處理能力或當需要時來平行或個別執行。另外，此說明書所使用的“系統”一詞意指複數個裝置的邏輯集合組態，因此如上述所組構之這些裝置並不一定設置在同一機殼中。

如上述，根據本揭示的一實施例之組態，提供用以有效防止內容的詐騙使用之裝置及方法。

尤其是，從對應於加密內容所設定之加密內容簽名檔案，取得區塊識別符，其指示在哪一個區域允許欲待應用到加密內容的解密之加密金鑰的儲存。然後，執行應用區塊識別符之內容再生可能性判斷處理。加密內容簽名檔案包含來自作爲加密內容簽名檔案的發行人之 ECS 發行人的憑證。執行有關記錄在加密內容簽名檔案中之區塊識別符是否落在記錄在 ECS 發行人憑證中之區塊識別符範圍內的判斷，及執行有關記錄在加密內容簽名檔案中之區塊識別符是否匹配記錄在使用控制資訊項目中之不同區塊識別符的判斷。依據這些判斷的結果，決定是否能夠再生內容。

藉由使用從加密內容簽名檔案所取得之區塊識別符資訊項目，依據有關金鑰資訊項目是否記錄在某存取允許區塊中之判斷，能夠執行內容使用控制。

本揭示包含有關日本專利局於 2011 年 11 月 19 日所

發表之日本優先權專利申請案 JP 2011-251735 所揭示的主題之主題，藉以併入其全文做爲參考。

精於本技藝之人士應明白，只要它們落在附錄的申請專利範圍或其同等物的範疇內，依據設計要求及其他因素，可出現各種修改、組合、子組合、及變更。

【圖式簡單說明】

圖 1 爲內容提供處理及內容使用處理之概要的說明圖；

圖 2 爲記錄在記憶卡中之內容的使用模式之說明圖；

圖 3 爲記憶卡中之儲存區的特定組態例子之說明圖；

圖 4 爲主機憑證的說明圖；

圖 5 爲伺服器憑證的說明圖；

圖 6 爲記憶卡所儲存的資料之特定組態例子及存取控制處理的例子之說明圖；

圖 7 爲被組構成防止內容的詐騙使用之本揭示的實施例之資訊處理系統的整體組態之說明圖；

圖 8 爲應用來防止裝置之間的內容之詐騙使用的資料項目之交換的說明圖；

圖 9 爲加密內容簽名檔案(ECS 檔案)的組態例子之說明圖；

圖 10 爲加密內容簽名檔案(ECS 檔案)的組態例子之另一說明圖；

圖 11 爲包含在加密內容簽名檔案(ECS 檔案)中之 ECS

發行人憑證的組態例子之說明圖；

圖 12 爲 ECS 發行人憑證撤回清單之組態例子的說明圖；

圖 13 爲加密內容簽名檔案(ECS 檔案)的產生處理及資料結構之概要的說明圖；

圖 14 爲加密內容簽名檔案(ECS 檔案)的產生、內容提供、及使用處理序列的說明序列圖；

圖 15 爲加密內容簽名檔案(ECS 檔案)的產生、內容提供、及使用處理序列的另一說明序列圖；

圖 16 爲有關記錄在加密內容簽名檔案(ECS 檔案)中之日期資料的內容提供可能性判斷處理之序列的說明流程圖；

圖 17 爲有關記錄在加密內容簽名檔案(ECS 檔案)中之日期資料的內容提供可能性判斷處理之另一序列的說明流程圖；

圖 18 爲有關記錄在加密內容簽名檔案(ECS 檔案)中之日期資料的內容再生可能性判斷處理之序列的說明流程圖；

圖 19 爲有關記憶卡之藉由伺服器的資料記錄處理之例子的說明圖；

圖 20 爲有關記憶卡所記錄的資料之藉由主機的讀取處理之例子的說明圖；

圖 21 爲記憶卡所記錄的資料之組態例子的說明圖；

圖 22 爲記憶卡所記錄的資料之另一組態例子的說明

圖；

圖 23 爲記錄在記憶卡的通用區中之使用控制資訊的資料項目之組態例子的說明圖；

圖 24 爲藉由更換處理之內容的詐騙使用之例子的說明圖；

圖 25 爲藉由更換處理之內容的詐騙記錄處理之例子的說明流程圖；

圖 26 爲藉由更換處理所記錄之詐騙內容無法被再生的說明流程圖；

圖 27 爲藉由更換處理之內容的詐騙使用之另一例子的說明圖；

圖 28 爲藉由更換處理之內容的詐騙記錄處理之另一例子的說明流程圖；

圖 29 爲藉由更換處理所記錄之詐騙內容無法被再生的另一說明流程圖；

圖 30 爲記錄在加密內容簽名檔案(ECS 檔案)中之區塊識別符及記錄在使用控制資訊檔案中之不同的區塊識別符之說明圖；

圖 31 爲參考記錄在加密內容簽名檔案(ECS 檔案)中之區塊識別符及記錄在使用控制資訊檔案中之不同的區塊識別符之內容提供可能性判斷序列的說明流程圖；

圖 32 爲從 ECS 發行人憑證讀取區塊識別符之處理序列的說明流程圖；

圖 33 爲參考記錄在加密內容簽名檔案(ECS 檔案)中之

區塊識別符及記錄在使用控制資訊檔案中之不同的區塊識別符之內容再生可能性判斷序列的說明流程圖；

圖 34 爲資訊處理裝置的硬體組態例子之說明圖；以及

圖 35 爲作爲資訊儲存裝置之記憶卡的硬體組態例子之說明圖。

【主要元件符號說明】

11：廣播電台，12：內容伺服器，

21：專用記錄/再生裝置，22：個人電腦，

23：行動終端，31：記憶卡，51：受保護區，

52：通用區，61：伺服器 A，62：伺服器 B，

63：主機裝置，70：記憶卡，80：受保護區，

81：區塊，82：區塊，90：通用區，101：許可發行人，

102：加密內容簽名(ECS)發行人，

102-1：加密內容簽名(ECS)發行人，

102-k：加密內容簽名(ECS)發行人，

102-n：加密內容簽名(ECS)發行人，

103：內容提供裝置(內容伺服器)，

103-1：內容提供裝置(內容伺服器)，

103-m：內容提供裝置(內容伺服器)，

104：使用者裝置，

104-1：使用者裝置(內容再生裝置)，

104-2：使用者裝置(內容再生裝置)，

104-f：使用者裝置(內容再生裝置)，

181：內容，182：標題金鑰，

183：內容雜湊清單集合(雜湊清單集合)，

200：加密內容簽名檔案(ECS檔案)，

201：伺服器A，202：主機，210：記憶卡，

211：受保護區，212：通用區，221：區塊，

701：中央處理單元，702：唯讀記憶體，

703：隨機存取記憶體，704：匯流排，

705：輸入/輸出介面，706：輸入單元，707：輸出單元，

708：儲存單元，709：通訊單元，710：驅動器，

711：可移動媒體，801：中央處理單元，

802：唯讀記憶體，803：隨機存取記憶體，

804：匯流排，805：輸入/輸出介面，806：通訊單元，

807：儲存單元，811：受保護區，812：通用區

七、申請專利範圍：

1.一種資訊儲存裝置，包含

儲存單元，被組構成儲存加密內容及欲待應用到該加密內容的解密之加密金鑰，該儲存單元包括

受保護區，在該受保護區中，儲存轉換的加密金鑰及設定存取限制，該轉換的加密金鑰爲經由該加密金鑰之轉換所取得的資料項目，以及

通用區，其儲存該加密內容及對應於該加密內容所設定之加密內容簽名檔案，該加密內容簽名檔案包含指示在該受保護區中哪一個區域允許該轉換的加密金鑰之儲存的區塊識別符作爲記錄資料項目，以允許再生裝置能夠執行應用該區塊識別符之內容再生可能性判斷，該再生裝置被組構成從該儲存單元讀取該加密內容及執行再生處理。

2.根據申請專利範圍第1項之資訊儲存裝置，其中

該加密內容簽名檔案包含ECS(加密內容簽名)發行人憑證，其儲存來自係該加密內容簽名檔案的發行人之ECS發行人的公用金鑰，該ECS發行人憑證包含作爲在該受保護區之各區域中允許該轉換的加密金鑰之儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

該資訊儲存裝置允許該再生裝置能夠判斷記錄在該加密內容簽名檔案中之該區塊識別符是否落在記錄在該ECS發行人憑證中的該區塊識別符範圍內，及依據該判斷的結果來決定是否能夠再生該加密內容，該再生裝置被組構成

從該儲存單元讀取該加密內容及執行該再生處理。

3.根據申請專利範圍第 1 項之資訊儲存裝置，其中

該通用區另儲存對應於該加密內容之使用控制資訊項目，該使用控制資訊項目爲包含指示在哪一個區塊儲存該加密金鑰之不同區塊識別符的資訊項目，以及

該資訊儲存裝置允許該再生裝置能夠判斷記錄在該加密內容簽名檔案中之該區塊識別符是否匹配記錄在該使用控制資訊項目中之該不同區塊識別符，及依據該判斷的結果來決定是否能夠再生該加密內容，該再生裝置被組構成從該儲存單元讀取該加密內容及執行該再生處理。

4.一種資訊處理裝置，包含

資料處理單元，被組構成執行記錄在媒體中之加密內容的解密處理及再生處理，該資料處理單元被組構成

從該媒體讀取對應於該加密內容所設定之加密內容簽名檔案，

從該加密內容簽名檔案取得區塊識別符，該區塊識別符指示在哪一個區域允許欲待應用到該加密內容的解密之加密金鑰的儲存，以及

執行應用該區塊識別符之內容再生可能性判斷處理。

5.根據申請專利範圍第 4 項之資訊處理裝置，其中

該加密內容簽名檔案包含 ECS 發行人憑證，其儲存來自該加密內容簽名檔案的發行人之 ECS 發行人之公用金鑰，該 ECS 發行人憑證包含作爲在各區域中允許該加密之

儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

該資料處理單元判斷記錄在該加密內容簽名檔案中之該區塊識別符是否落在記錄在該 ECS 發行人憑證中的該區塊識別符範圍內，及依據該判斷的結果來決定是否能夠再生該加密內容。

6.根據申請專利範圍第 4 項之資訊處理裝置，其中

該媒體另儲存對應於該加密內容之使用控制資訊項目，該使用控制資訊項目爲包含指示在哪一個區塊儲存該加密金鑰之不同區塊識別符的資訊項目，以及

該資料處理單元判斷記錄在該加密內容簽名檔案中之該區塊識別符是否匹配記錄在該使用控制資訊項目中之該不同區塊識別符，及依據該判斷的結果來決定是否能夠再生該加密內容。

7.一種資訊處理裝置，包含

資料處理單元，被組構成輸出欲待記錄到媒體之加密內容及欲待應用到該加密內容的解密之加密金鑰，該資料處理單元被組構成

取得對應於該加密內容所設定之加密內容簽名檔案，

從該加密內容簽名檔案取得區塊識別符，該區塊識別符指示在哪一個區域允許該加密金鑰之儲存，以及

執行應用該區塊識別符之內容輸出可能性判斷處理。

8.根據申請專利範圍第 7 項之資訊處理裝置，其中

該加密內容簽名檔案包含 ECS 發行人憑證，其儲存來自係該加密內容簽名檔案的發行人之 ECS 發行人之公用金鑰，該 ECS 發行人憑證包含作爲在各區域中允許該加密金鑰之儲存範圍的區塊識別符範圍作爲記錄資料項目，以及

該資料處理單元判斷記錄在該加密內容簽名檔案中之該區塊識別符是否落在記錄在該 ECS 發行人憑證中的該區塊識別符範圍內，及依據該判斷的結果來決定是否能夠輸出該加密內容。

9.根據申請專利範圍第 7 項之資訊處理裝置，其中

該資料處理單元被組構成

取得對應於該加密內容所設定之使用控制資訊項目，

從該取得的使用控制資訊項目取得不同區塊識別符，其指示在哪一個區塊儲存該加密金鑰，

判斷記錄在該加密內容簽名檔案中之該區塊識別符是否匹配記錄在該使用控制資訊項目中之該不同區塊識別符，以及

依據該判斷的結果來決定是否能夠再生該加密內容。

10.一種資訊處理方法，係由資訊處理裝置所執行，該資訊處理裝置包括資料處理單元，被組構成執行記錄在媒體中之加密內容的解密處理及再生處理，該資料處理單元被組構成，

從該媒體讀取對應於該加密內容所設定之加密內容簽

名檔案，

從該加密內容簽名檔案取得區塊識別符，該區塊識別符指示在哪一個區域允許欲待應用到該加密內容的解密之加密金鑰的儲存，以及

執行應用該區塊識別符之內容再生可能性判斷處理。

11.一種資訊處理方法，係由資訊處理裝置所執行，該資訊處理裝置包括資料處理單元，被組構成輸出欲待記錄到媒體之加密內容及欲待應用到該加密內容的解密之加密金鑰，該資料處理單元被組構成

取得對應於該加密內容所設定之加密內容簽名檔案，

從該加密內容簽名檔案取得區塊識別符，該區塊識別符指示在哪一個區域允許儲存該加密金鑰，以及

執行應用該區塊識別符之內容輸出可能性判斷處理。

12.一種程式，使資訊處理裝置能夠執行資訊處理，該資訊處理裝置包括資料處理單元，被組構成執行記錄在媒體中之加密內容的解密處理及再生處理，該程式使該資料處理單元能夠執行

讀取處理，從該媒體讀取對應於該加密內容所設定之加密內容簽名檔案，

取得處理，從該加密內容簽名檔案取得區塊識別符，該區塊識別符指示在哪一個區域允許欲待應用到該加密內容的解密之加密金鑰的儲存，以及

應用該區塊識別符之內容再生可能性判斷處理。

13.一種程式，使資訊處理裝置能夠執行資訊處理，

該資訊處理裝置包括資料處理單元，被組構成輸出欲待記錄到媒體之加密內容及欲待應用到該加密內容的解密之加密金鑰，該程式使該資料處理單元能夠執行

取得處理，取得對應於該加密內容所設定之加密內容簽名檔案，

取得處理，從該加密內容簽名檔案取得區塊識別符，該區塊識別符指示在哪一個區域允許該加密金鑰之儲存，以及

應用該區塊識別符之內容輸出可能性判斷處理。

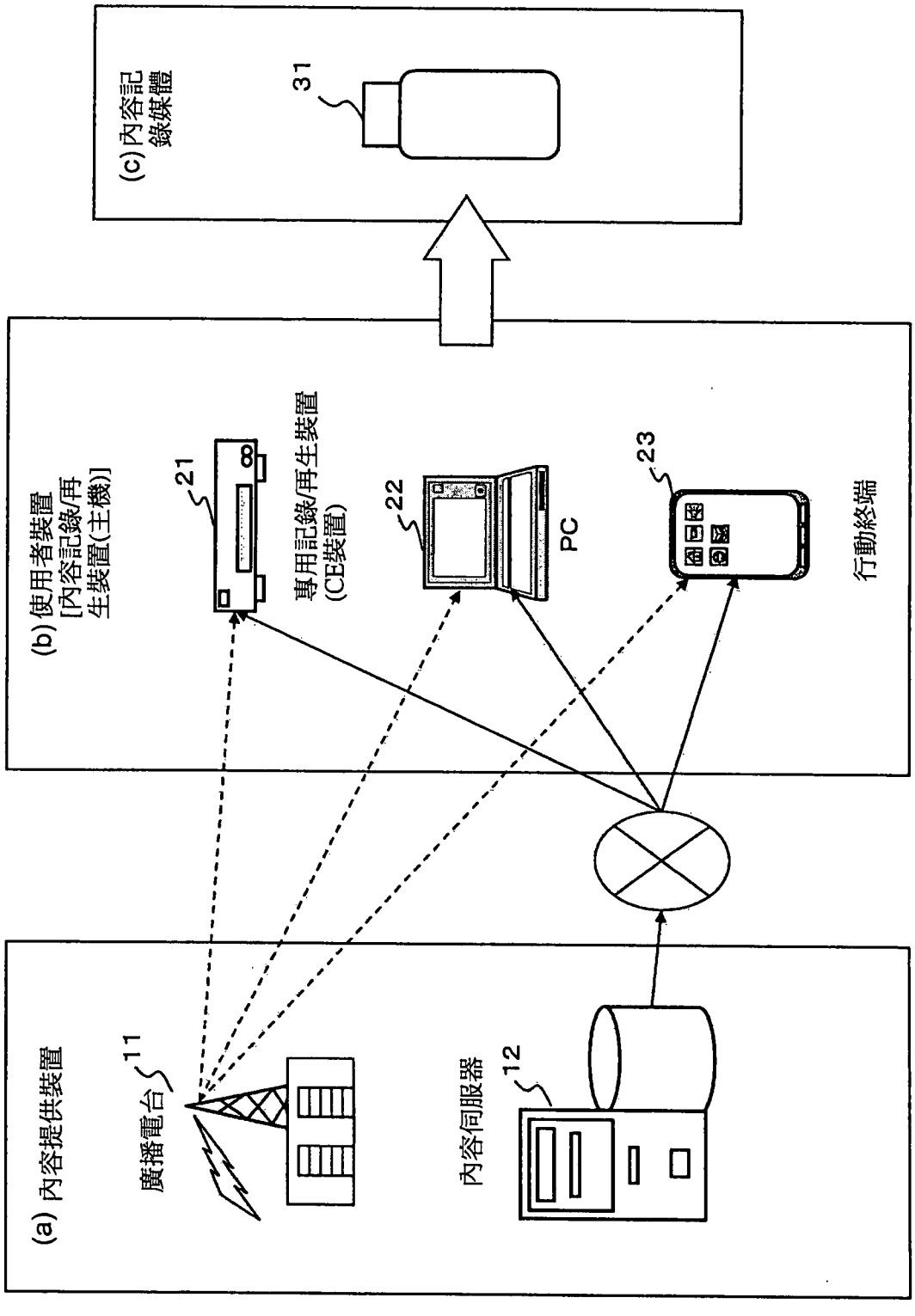

(a) 內容提供裝置
廣播電台
11
內容伺服器
12
(b) 使用者裝置
[內容記錄/再生裝置(主機)]
21
專用記錄/再生裝置
(CE裝置)
22
PC
23
行動終端
(c) 內容記錄媒體
31

圖1

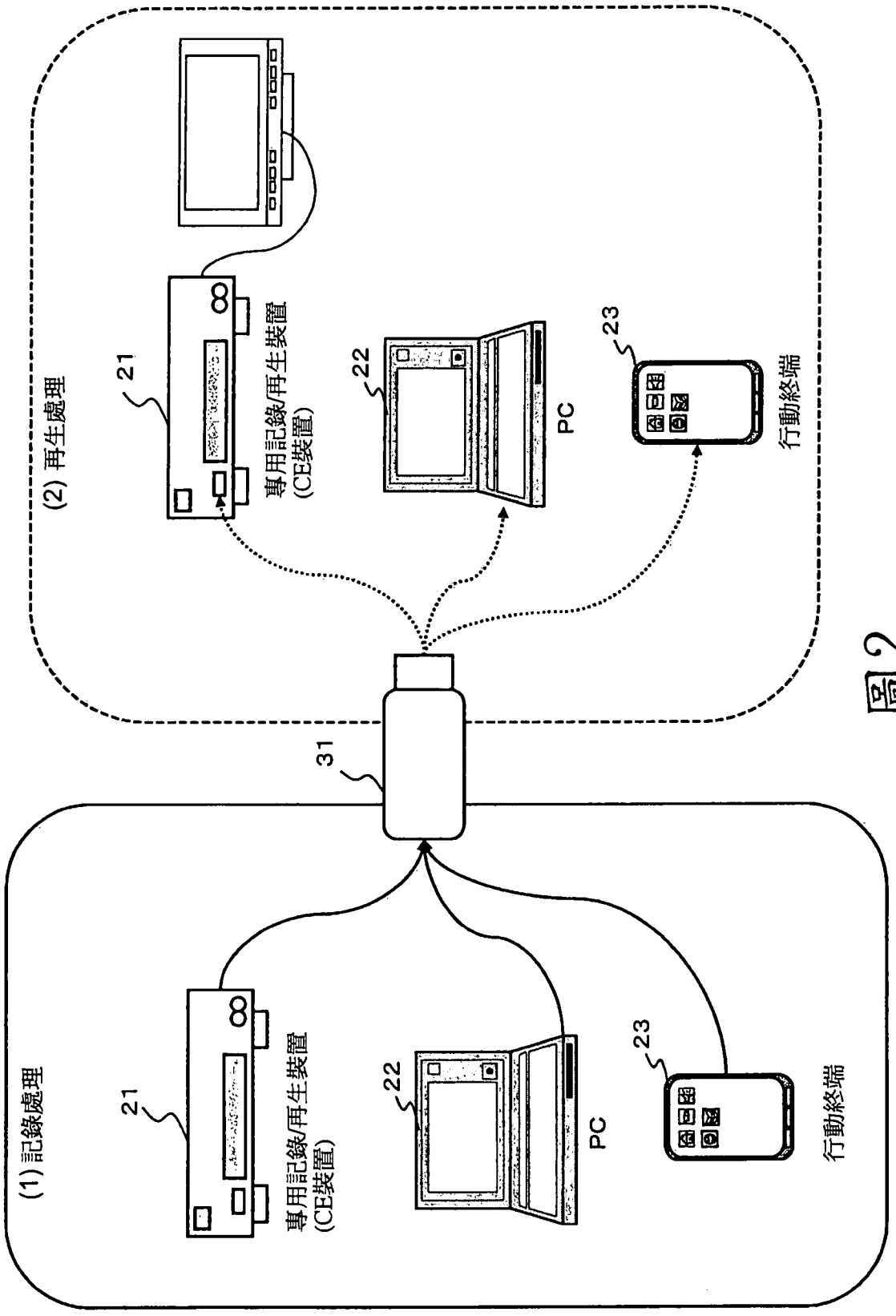

(1) 記錄處理
21
專用記錄/再生裝置
(CE裝置)
22
PC
23
行動終端
31
(2) 再生處理
21
專用記錄/再生裝置
(CE裝置)
22
PC
23
行動終端

圖2

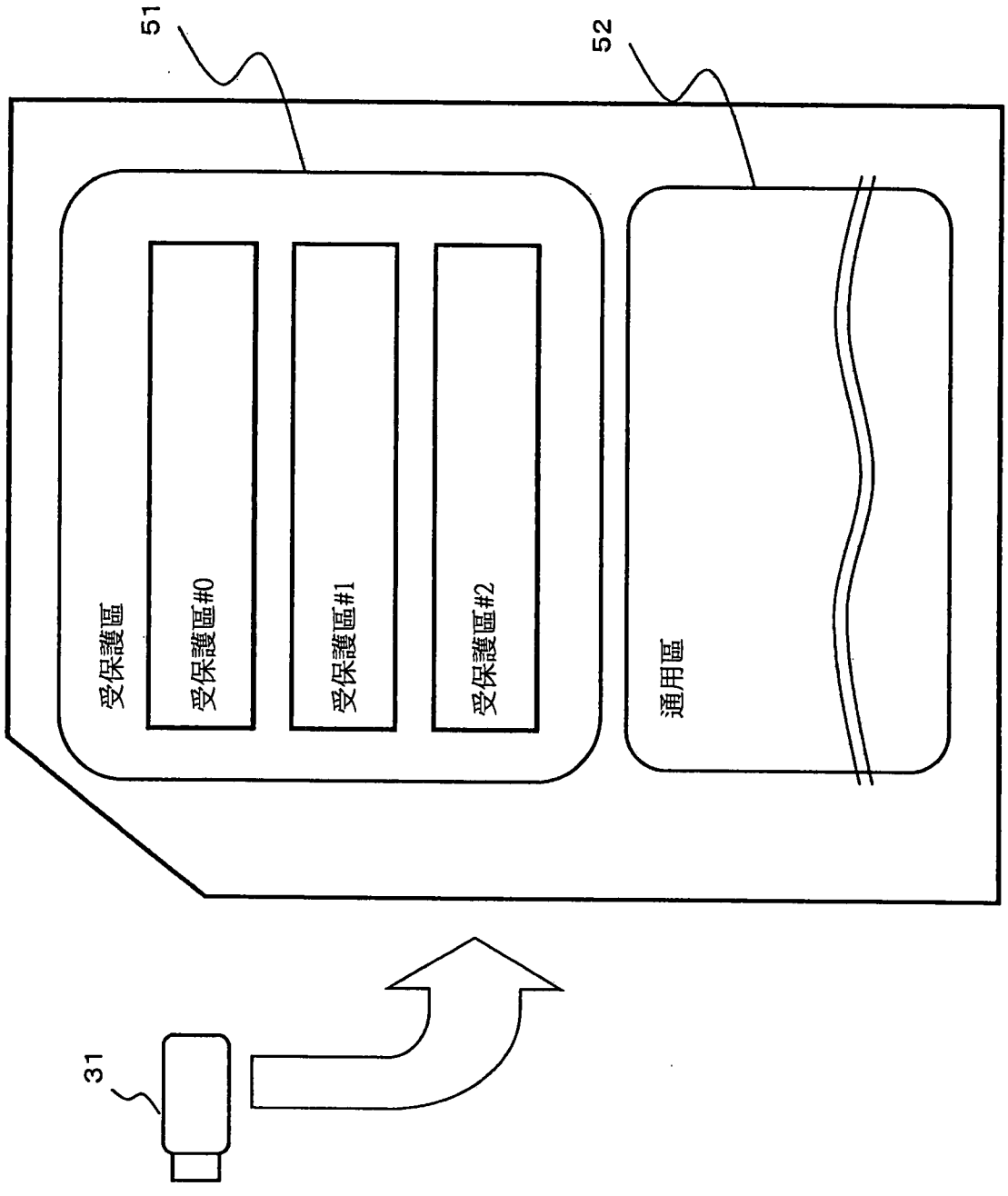


圖3

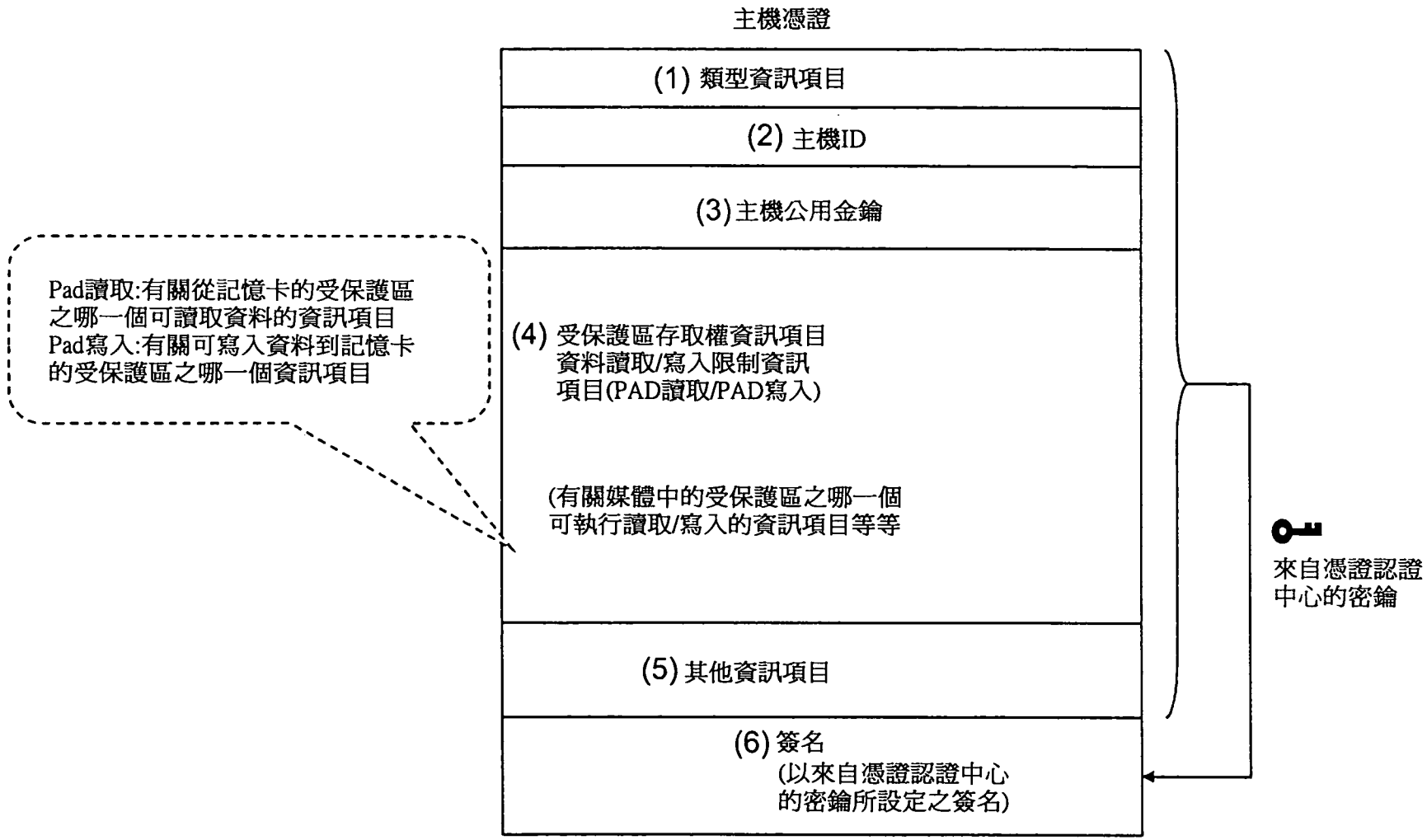

主機憑證
(1) 類型資訊項目
(2) 主機ID
(3) 主機公用金鑰
(4) 受保護區存取權資訊項目
資料讀取/寫入限制資訊
項目(PAD讀取/PAD寫入)
(有關媒體中的受保護區之哪一個
可執行讀取/寫入的資訊項目等等
(5) 其他資訊項目
(6) 簽名
(以來自憑證認證中心
的密鑰所設定之簽名)
Pad讀取:有關從記憶卡的受保護區
之哪一個可讀取資料的資訊項目
Pad寫入:有關可寫入資料到記憶卡
的受保護區之哪一個資訊項目
來自憑證認證
中心的密鑰

圖4

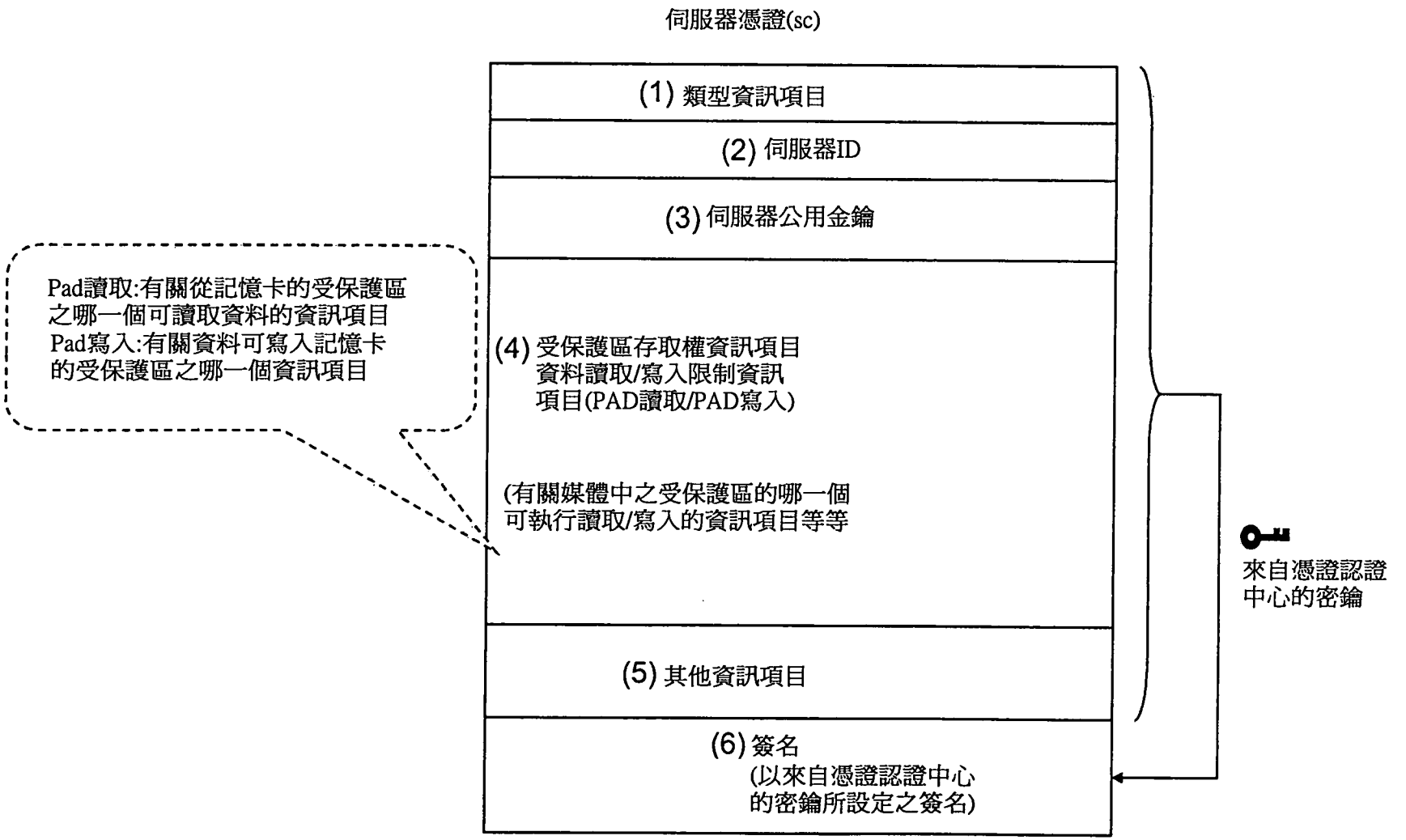

伺服器憑證(sc)
(1) 類型資訊項目
(2) 伺服器ID
(3) 伺服器公用金鑰
Pad讀取:有關從記憶卡的受保護區之哪一個可讀取資料的資訊項目
Pad寫入:有關資料可寫入記憶卡的受保護區之哪一個資訊項目
(4) 受保護區存取權資訊項目
資料讀取/寫入限制資訊項目(PAD讀取/PAD寫入)
(有關媒體中之受保護區的哪一個可執行讀取/寫入的資訊項目等等
(5) 其他資訊項目
(6) 簽名
(以來自憑證認證中心的密鑰所設定之簽名)
來自憑證認證中心的密鑰

圖5

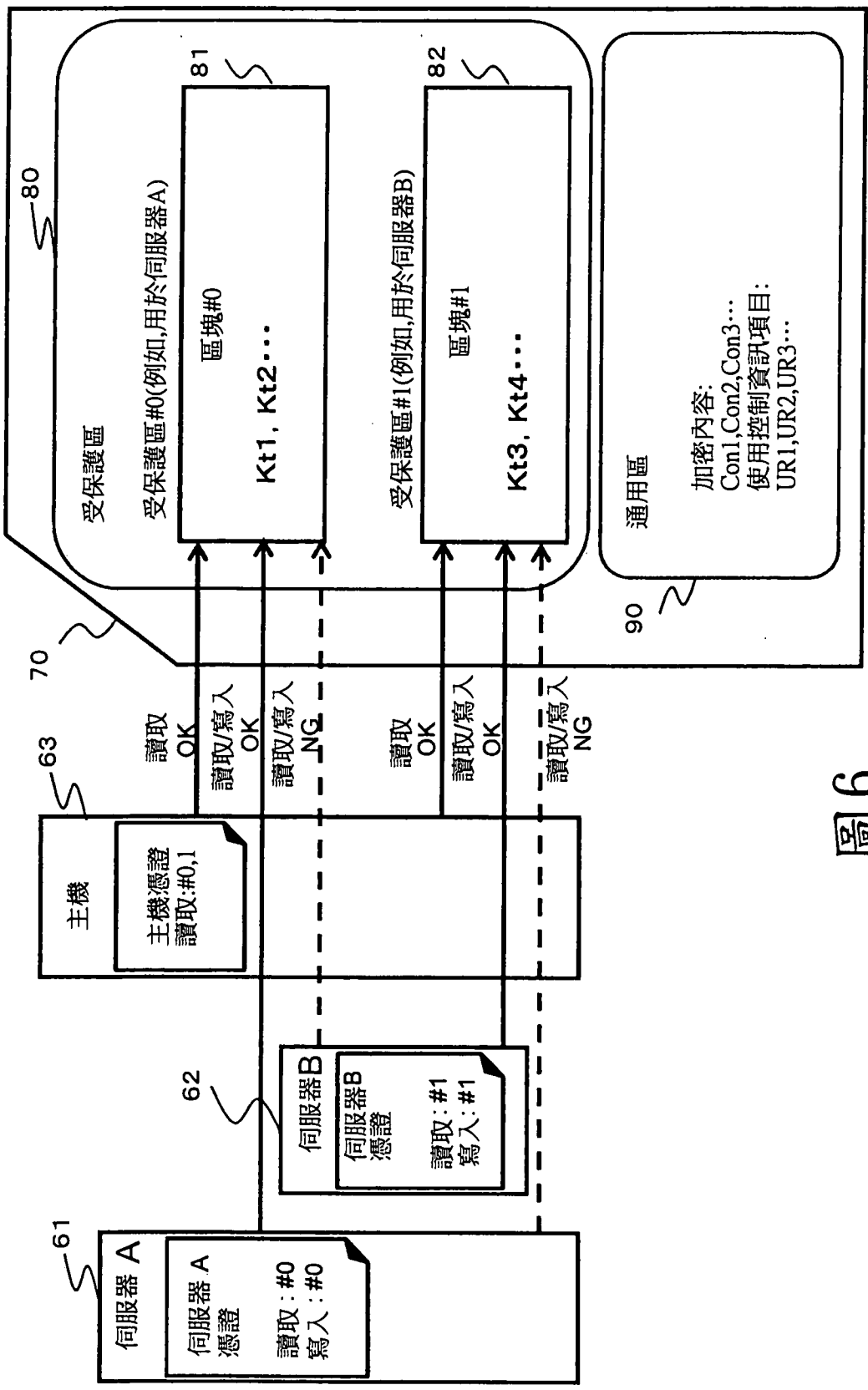

伺服器 A
伺服器 A
憑證
讀取 : #0
寫入 : #0
61
伺服器B
伺服器B
憑證
讀取: #1
寫入: #1
62
主機
主機憑證
讀取:#0,1
63
70
80
受保護區
受保護區#0(例如,用於伺服器A)
區塊#0
Kt1, Kt2…
81
受保護區#1(例如,用於伺服器B)
區塊#1
Kt3, Kt4…
82
通用區
加密內容:
Con1,Con2,Con3…
使用控制資訊項目:
UR1,UR2,UR3…
90
讀取
OK
讀取/寫入
OK
讀取/寫入
NG
讀取
OK
讀取/寫入
OK
讀取/寫入
NG

圖 6

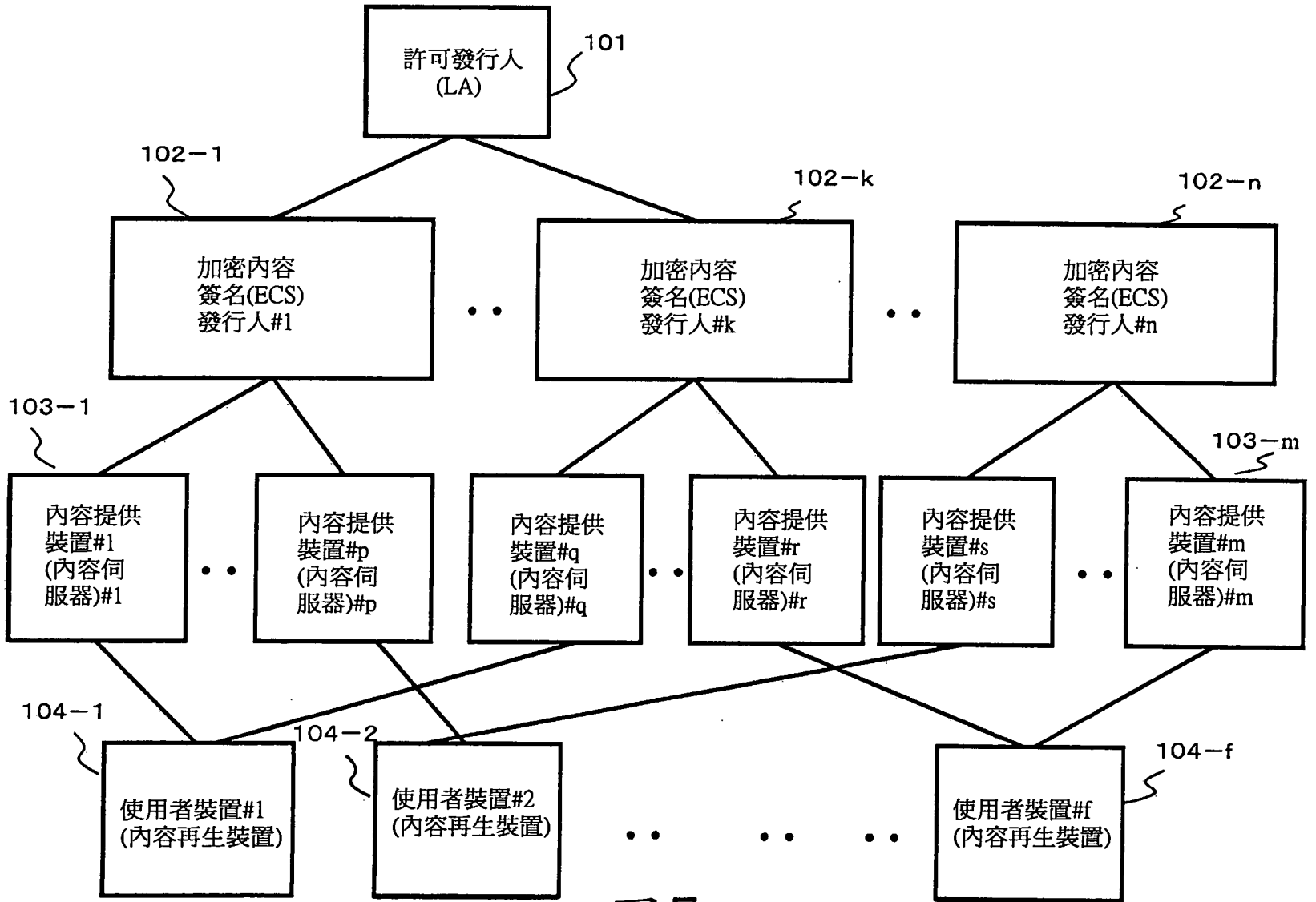

許可發行人
(LA)
101
102－1
102－k
102－n
加密內容
簽名(ECS)
發行人#1
加密內容
簽名(ECS)
發行人#k
加密內容
簽名(ECS)
發行人#n
103－1
103－m
內容提供
裝置#1
(內容伺
服器)#1
內容提供
裝置#p
(內容伺
服器)#p
內容提供
裝置#q
(內容伺
服器)#q
內容提供
裝置#r
(內容伺
服器)#r
內容提供
裝置#s
(內容伺
服器)#s
內容提供
裝置#m
(內容伺
服器)#m
104－1
104－2
104－f
使用者裝置#1
(內容再生裝置)
使用者裝置#2
(內容再生裝置)
使用者裝置#f
(內容再生裝置)

圖7

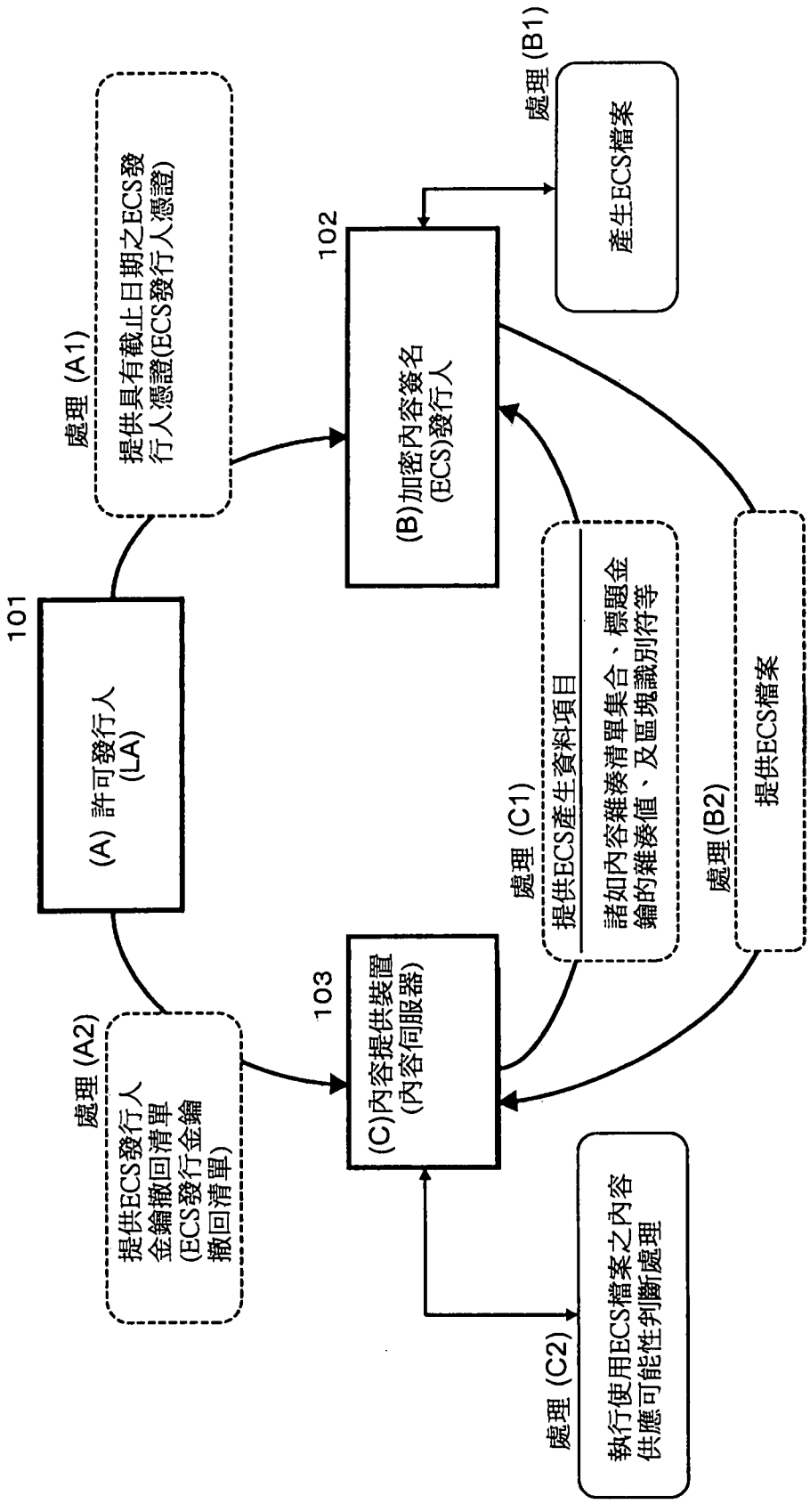

101
(A) 許可發行人
(LA)
處理 (A1)
提供具有截止日期之ECS發
行人憑證(ECS發行人憑證)
102
(B)加密內容簽名
(ECS)發行人
處理 (B1)
產生ECS檔案
處理 (A2)
提供ECS發行人
金鑰撤回清單
(ECS發行金鑰
撤回清單)
103
(C)內容提供裝置
(內容伺服器)
處理 (C1)
提供ECS產生資料項目
諸如內容雜湊清單集合、標題金
鑰的雜湊值、及區塊識別符等
處理 (B2)
提供ECS檔案
處理 (C2)
執行使用ECS檔案之內容
供應可能性判斷處理

圖8

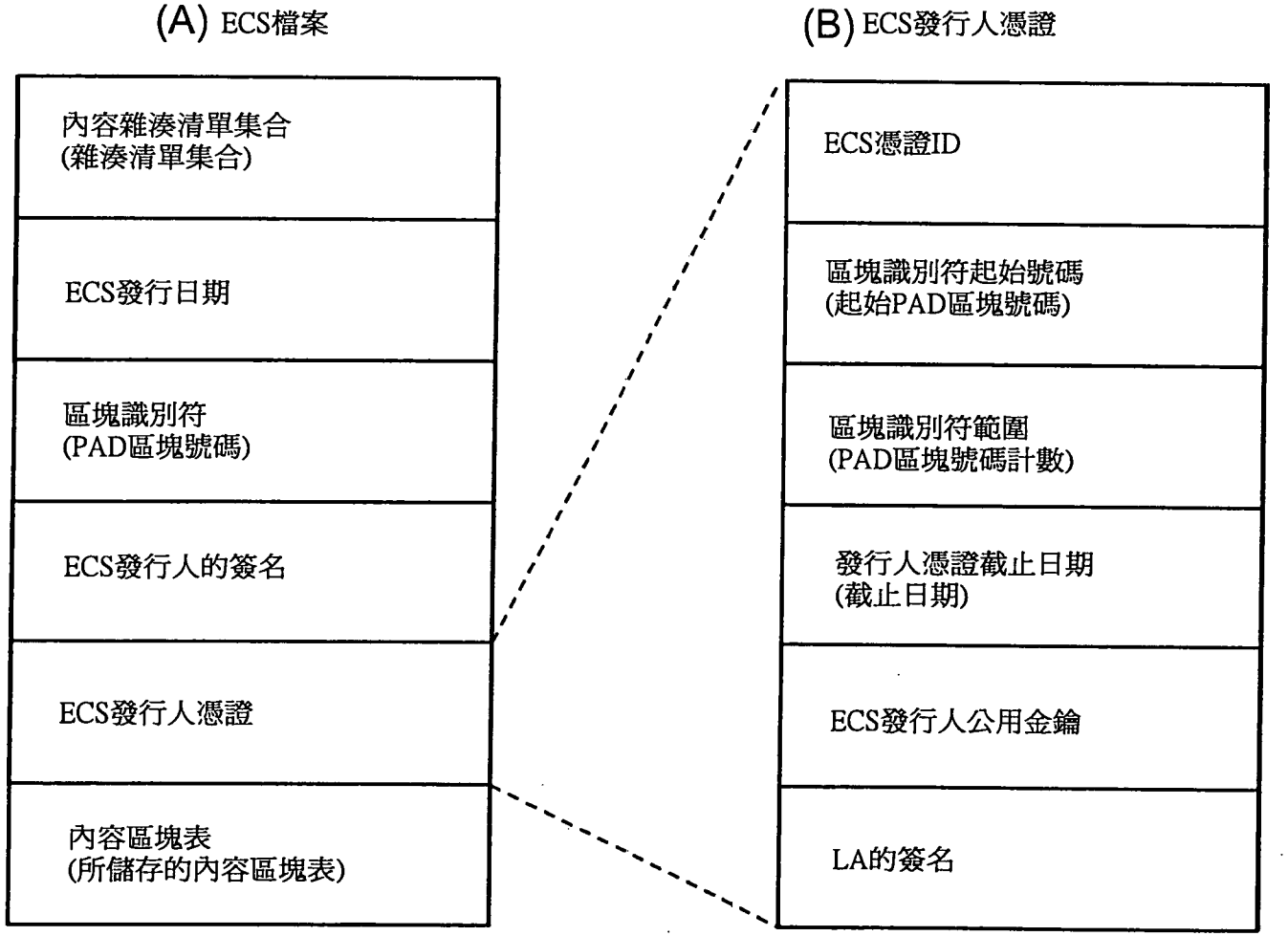

(A) ECS檔案
內容雜湊清單集合
(雜湊清單集合)
ECS發行日期
區塊識別符
(PAD區塊號碼)
ECS發行人的簽名
ECS發行人憑證
內容區塊表
(所儲存的內容區塊表)
(B) ECS發行人憑證
ECS憑證ID
區塊識別符起始號碼
(起始PAD區塊號碼)
區塊識別符範圍
(PAD區塊號碼計數)
發行人憑證截止日期
(截止日期)
ECS發行人公用金鑰
LA的簽名

圖9

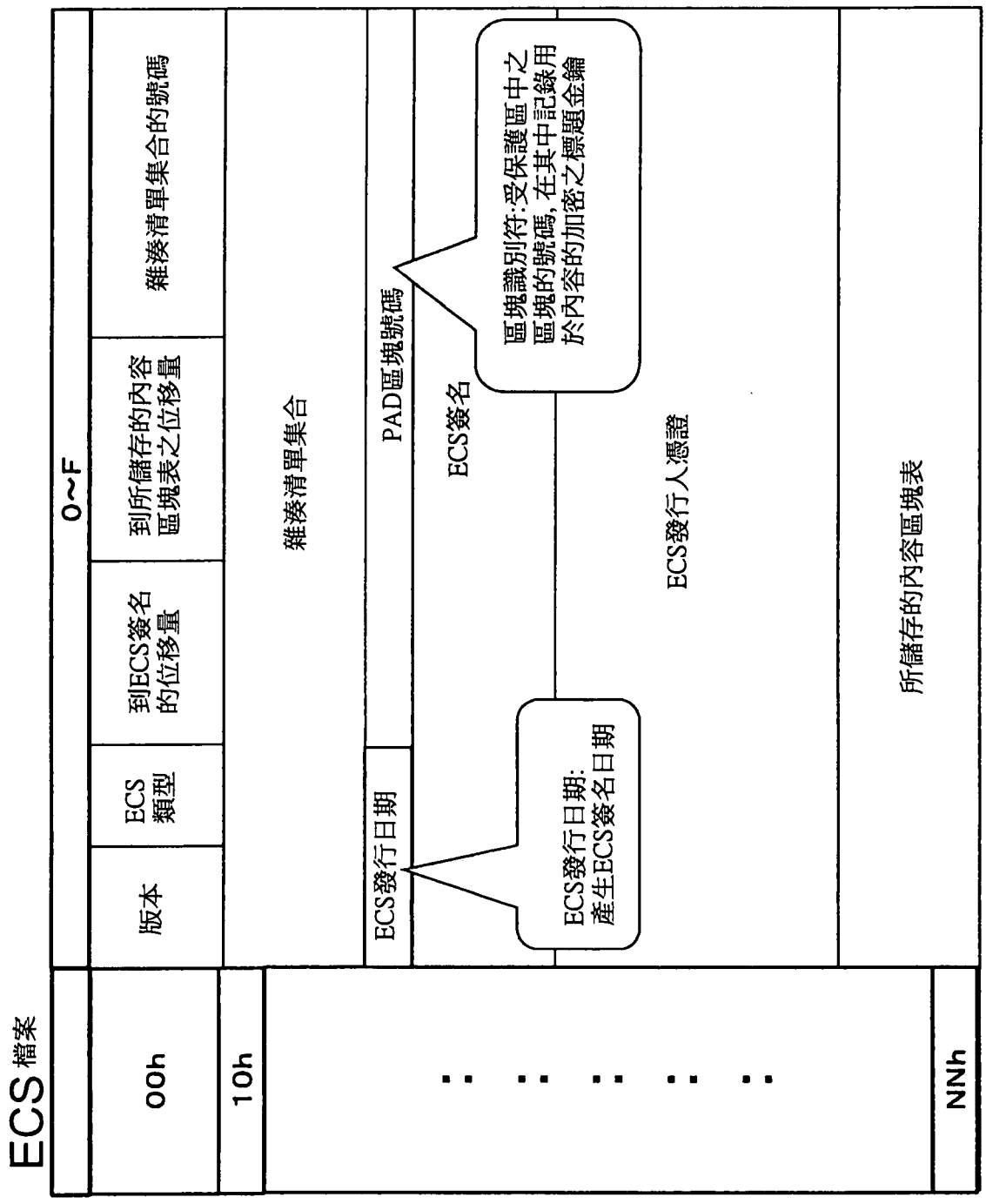
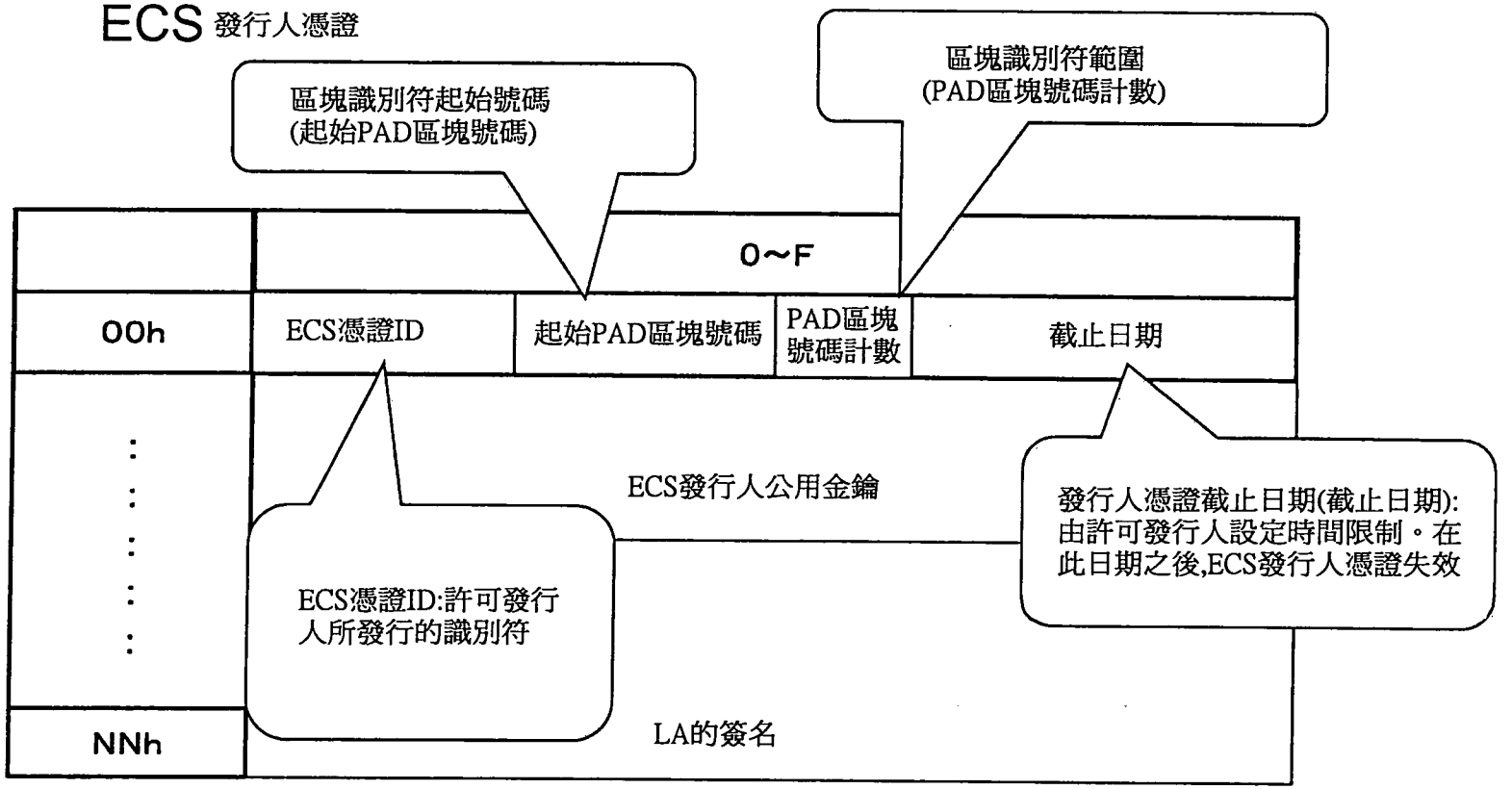

ECS 檔案
0~F
版本
ECS 類型
到ECS簽名的位移量
到所儲存的內容區塊表之位移量
雜湊清單集合的號碼
00h
10h
雜湊清單集合
ECS發行日期
PAD區塊號碼
ECS簽名
區塊識別符:受保護區中之區塊的號碼,在其中記錄用於內容的加密之標題金鑰
ECS發行日期:產生ECS簽名日期
ECS發行人憑證
所儲存的內容區塊表
NNh

圖10



- 滿足關係:起始PAD區塊號碼 ≦ N ≦ 起始PAD區塊號碼+PAD區塊號碼計數之所有整數N被設定作區塊識別符
- 另外,當起始PAD區塊號碼被設成0xFFFFFFFF時,從0至4,294,967,295的所有整數被設定作區塊識別符

圖11

ECS發行人金鑰撤回清單

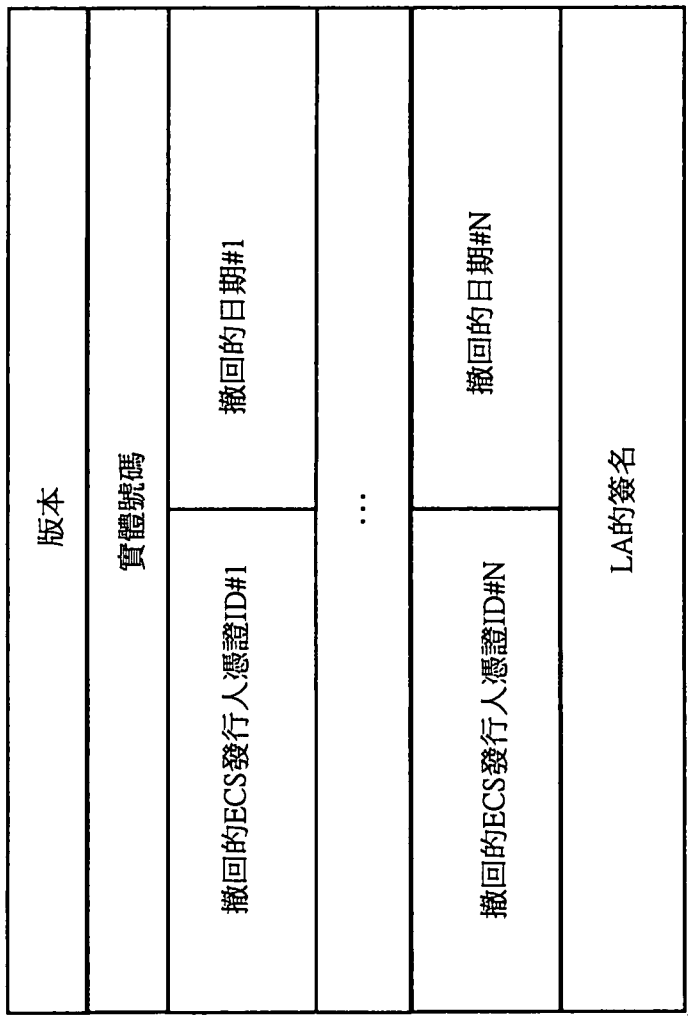


圖12

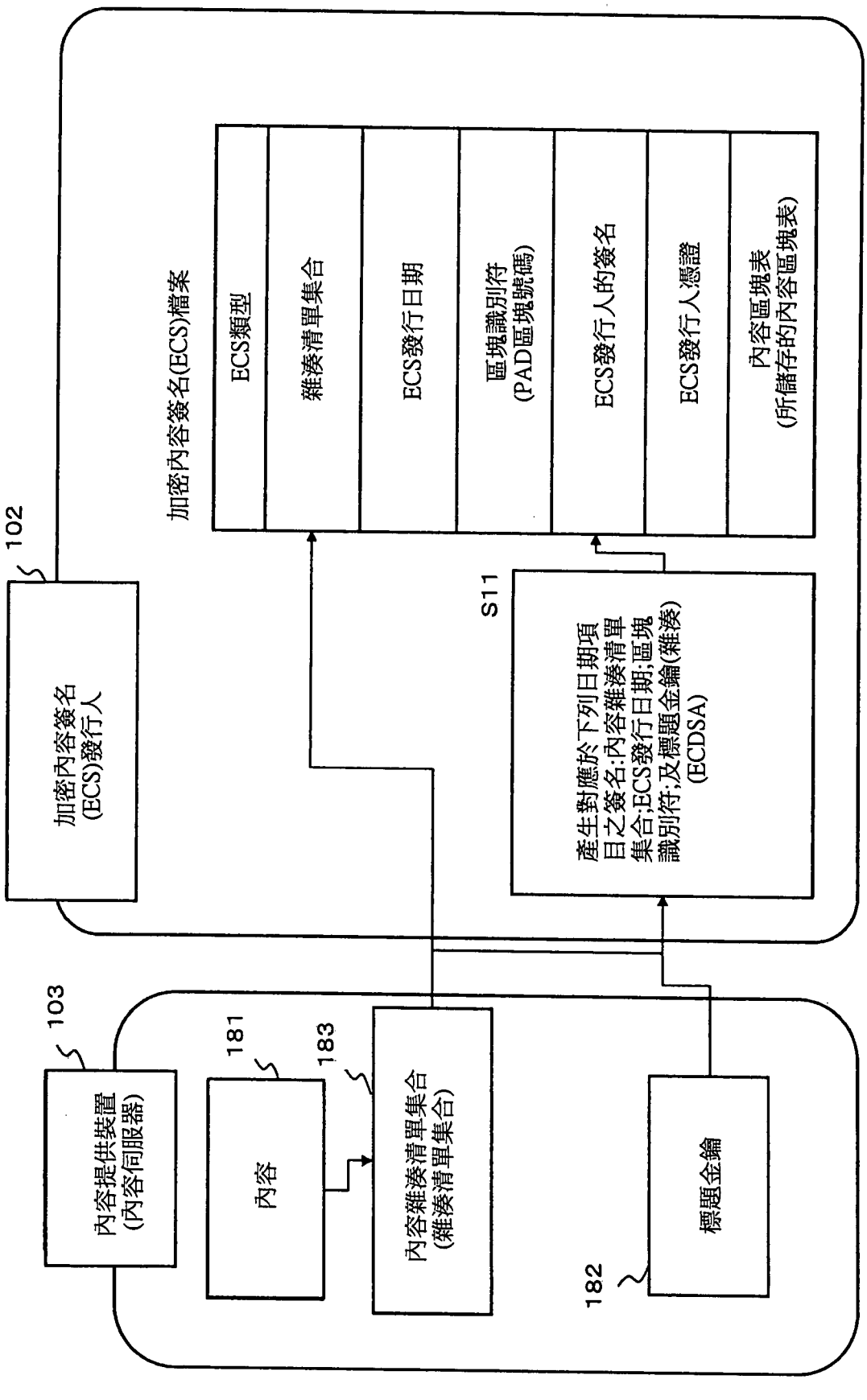

102
加密內容簽名(ECS)發行人
加密內容簽名(ECS)檔案
ECS類型
雜湊清單集合
ECS發行日期
區塊識別符
(PAD區塊號碼)
ECS發行人的簽名
ECS發行人憑證
內容區塊表
(所儲存的內容區塊表)
S11
產生對應於下列日期項目之簽名:內容雜湊清單集合;ECS發行日期;區塊識別符;及標題金鑰(雜湊)
(ECDSA)
103
內容提供裝置
(內容伺服器)
181
內容
183
內容雜湊清單集合
(雜湊清單集合)
182
標題金鑰

圖13

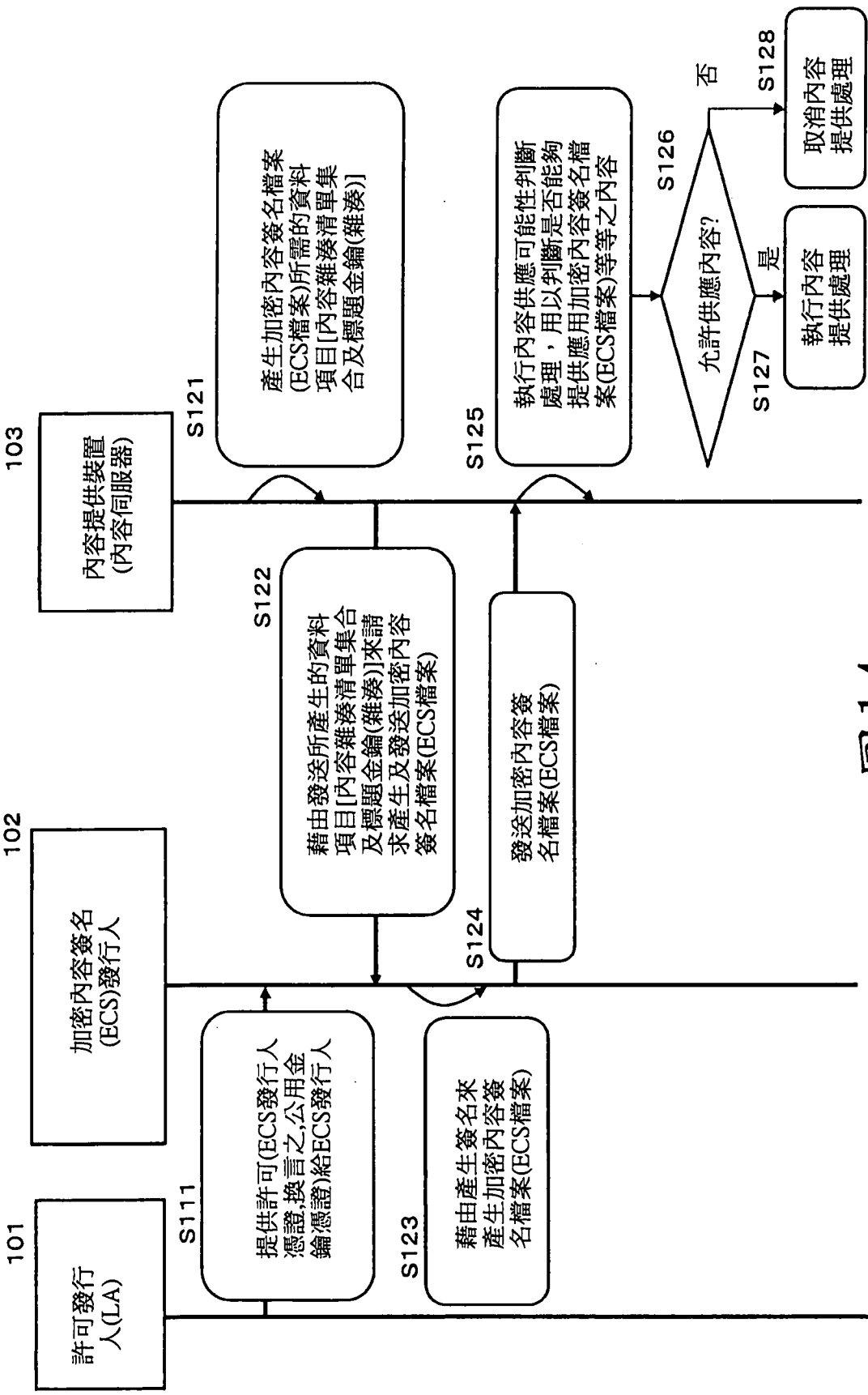

101
許可發行人(LA)
102
加密內容簽名(ECS)發行人
103
內容提供裝置(內容伺服器)
S111
提供許可(ECS發行人憑證,換言之,公用金鑰憑證)給ECS發行人
S121
產生加密內容簽名檔案(ECS檔案)所需的資料項目[內容雜湊清單集合及標題金鑰(雜湊)]
S122
藉由發送所產生的資料項目[內容雜湊清單集合及標題金鑰(雜湊)]來請求產生及發送加密內容簽名檔案(ECS檔案)
S123
藉由產生簽名來產生加密內容簽名檔案(ECS檔案)
S124
發送加密內容簽名檔案(ECS檔案)
S125
執行內容供應可能性判斷處理，用以判斷是否能夠提供應用加密內容簽名檔案(ECS檔案)等等之內容
S126
允許供應內容?
否
是
S127
執行內容提供處理
S128
取消內容提供處理

圖14

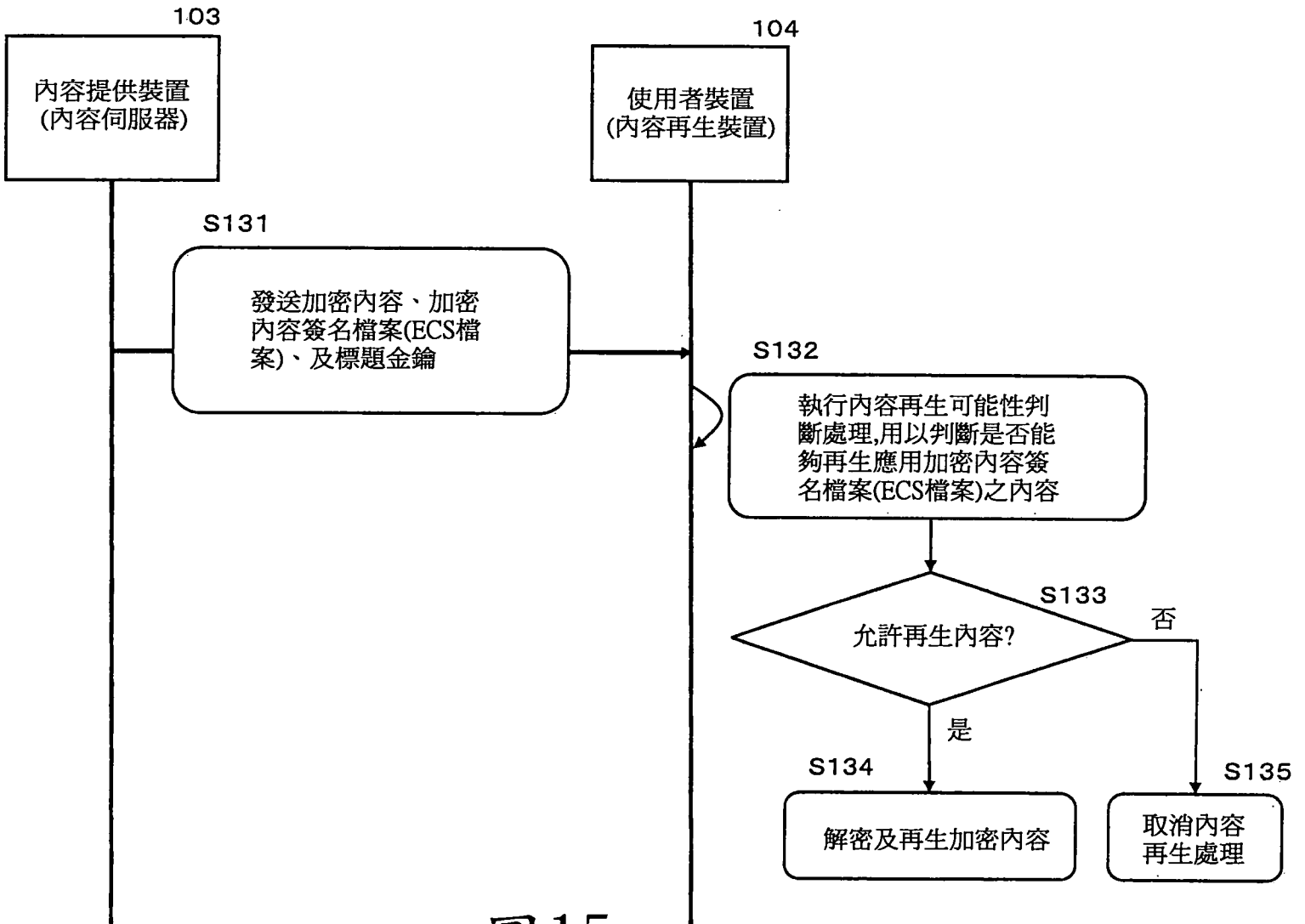

103
內容提供裝置
(內容伺服器)
104
使用者裝置
(內容再生裝置)
S131
發送加密內容、加密內容簽名檔案(ECS檔案)、及標題金鑰
S132
執行內容再生可能性判斷處理,用以判斷是否能夠再生應用加密內容簽名檔案(ECS檔案)之內容
S133
允許再生內容?
否
是
S134
解密及再生加密內容
S135
取消內容再生處理

圖15

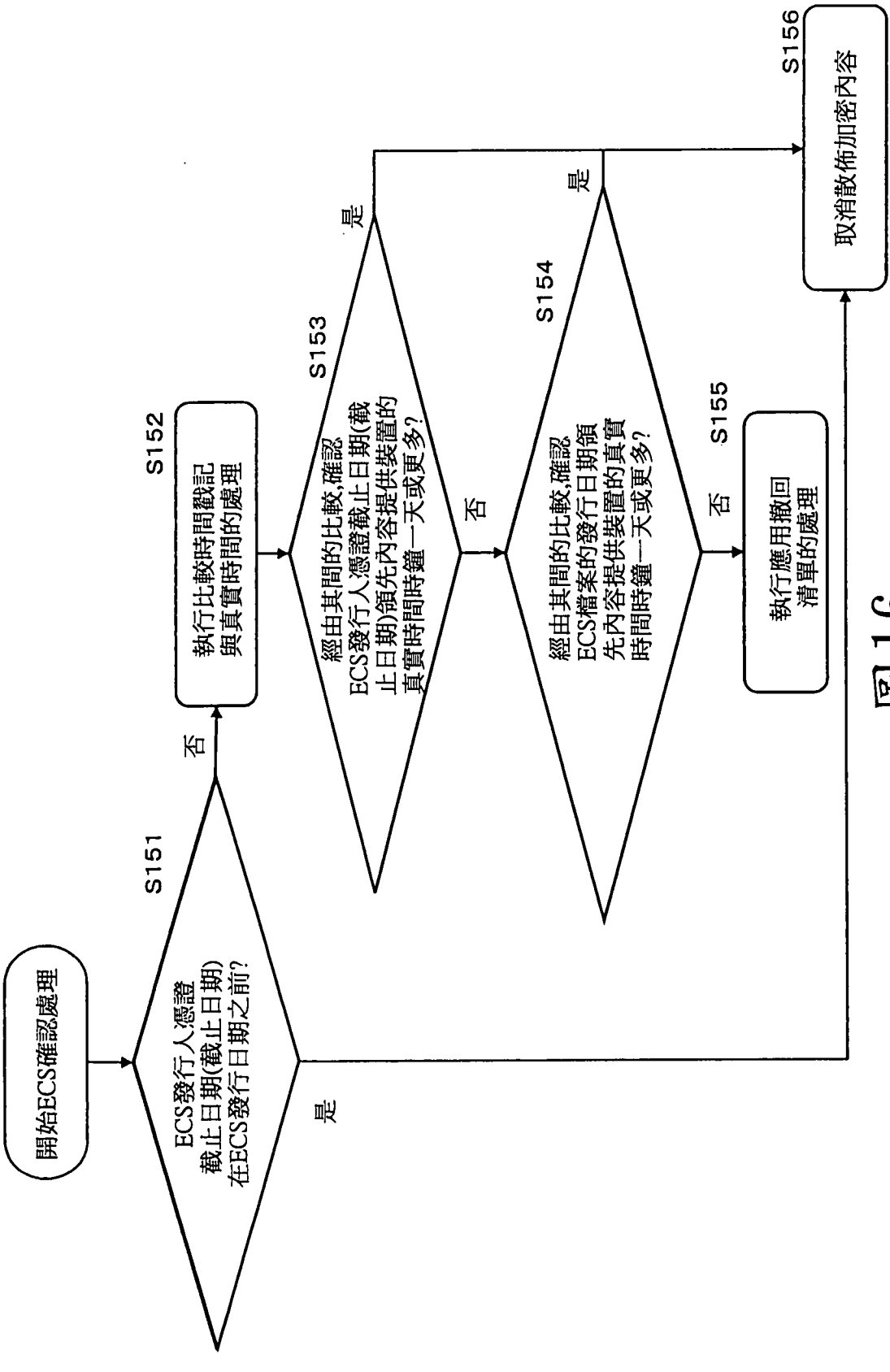

開始ECS確認處理
S151
ECS發行人憑證
截止日期(截止日期)
在ECS發行日期之前?
否
是
S152
執行比較時間戳記
與真實時間的處理
S153
經由其間的比較,確認
ECS發行人憑證截止日期(截
止日期)領先內容提供裝置的
真實時間時鐘一天或更多?
否
是
S154
經由其間的比較,確認
ECS檔案的發行日期領
先內容提供裝置的真實
時間時鐘一天或更多?
否
是
S155
執行應用撤回
清單的處理
S156
取消散佈加密內容

圖16

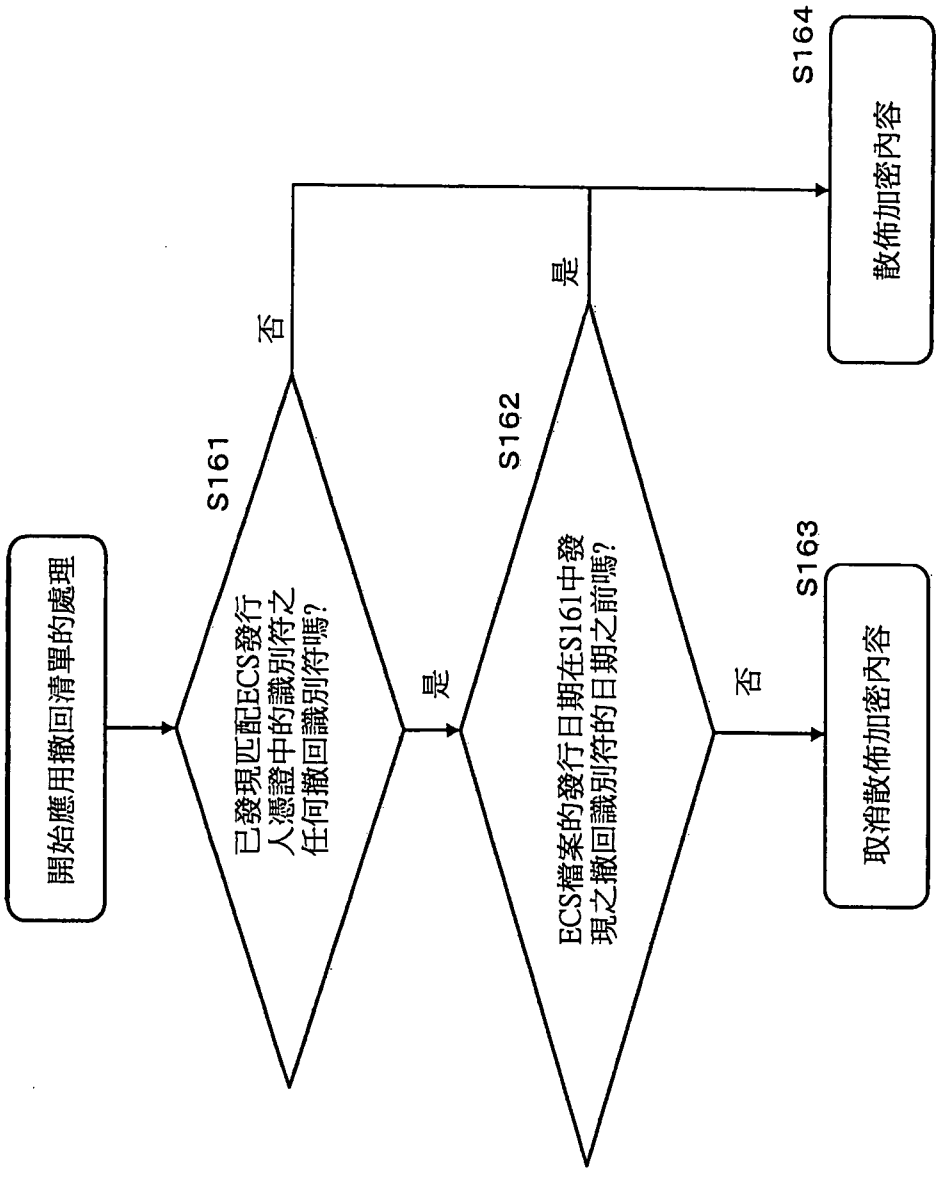

開始應用撤回清單的處理
S161
已發現匹配ECS發行人憑證中的識別符之任何撤回識別符嗎?
否
是
S162
ECS檔案的發行日期在S161中發現之撤回識別符的日期之前嗎?
是
否
S163
取消散佈加密內容
S164
散佈加密內容

圖17

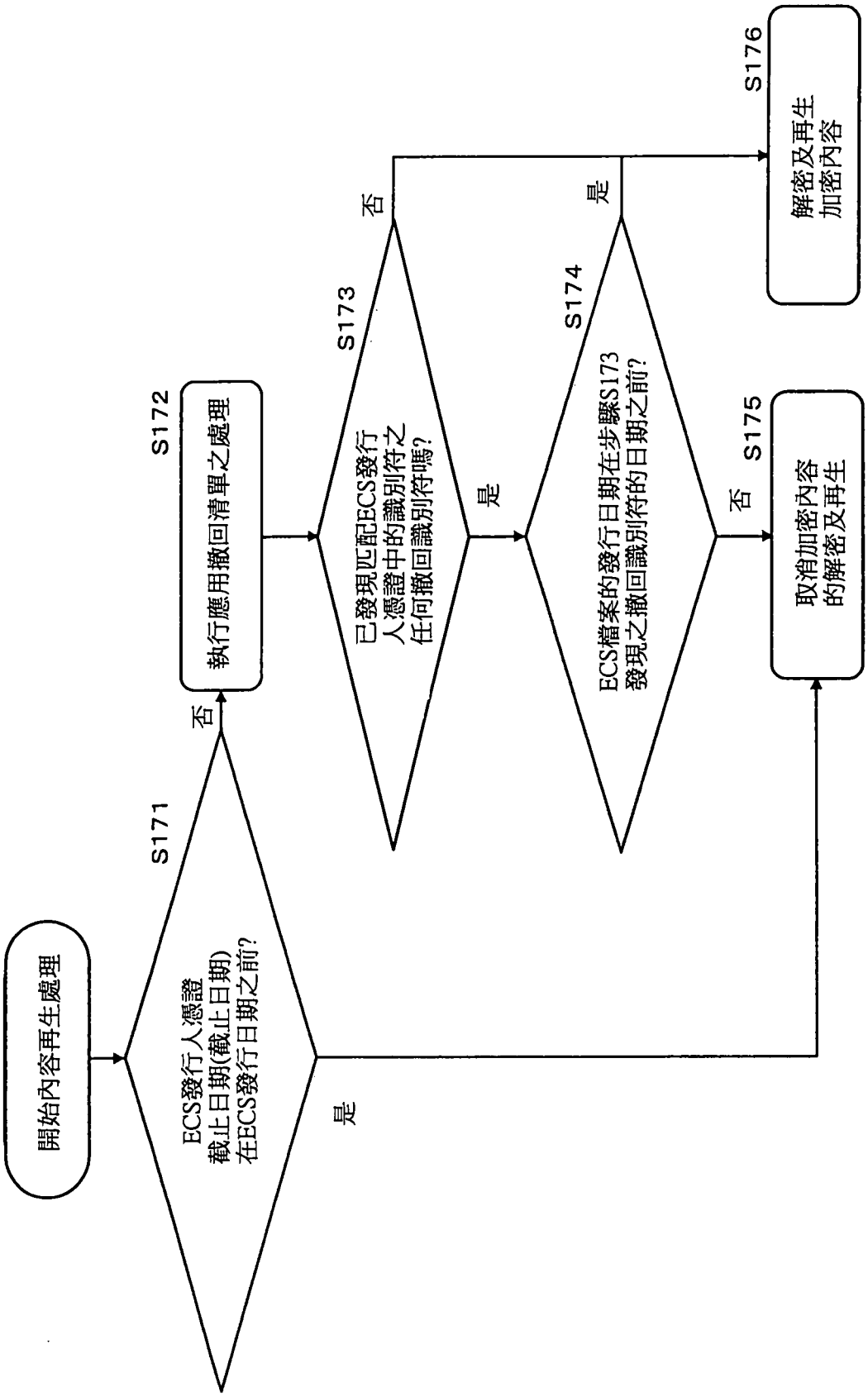

開始內容再生處理
S171
ECS發行人憑證
截止日期(截止日期)
在ECS發行日期之前?
否
是
S172
執行應用撤回清單之處理
S173
已發現匹配ECS發行
人憑證中的識別符之
任何撤回識別符嗎?
否
是
S174
ECS檔案的發行日期在步驟S173
發現之撤回識別符的日期之前?
否
是
S175
取消加密內容
的解密及再生
S176
解密及再生
加密內容

圖18

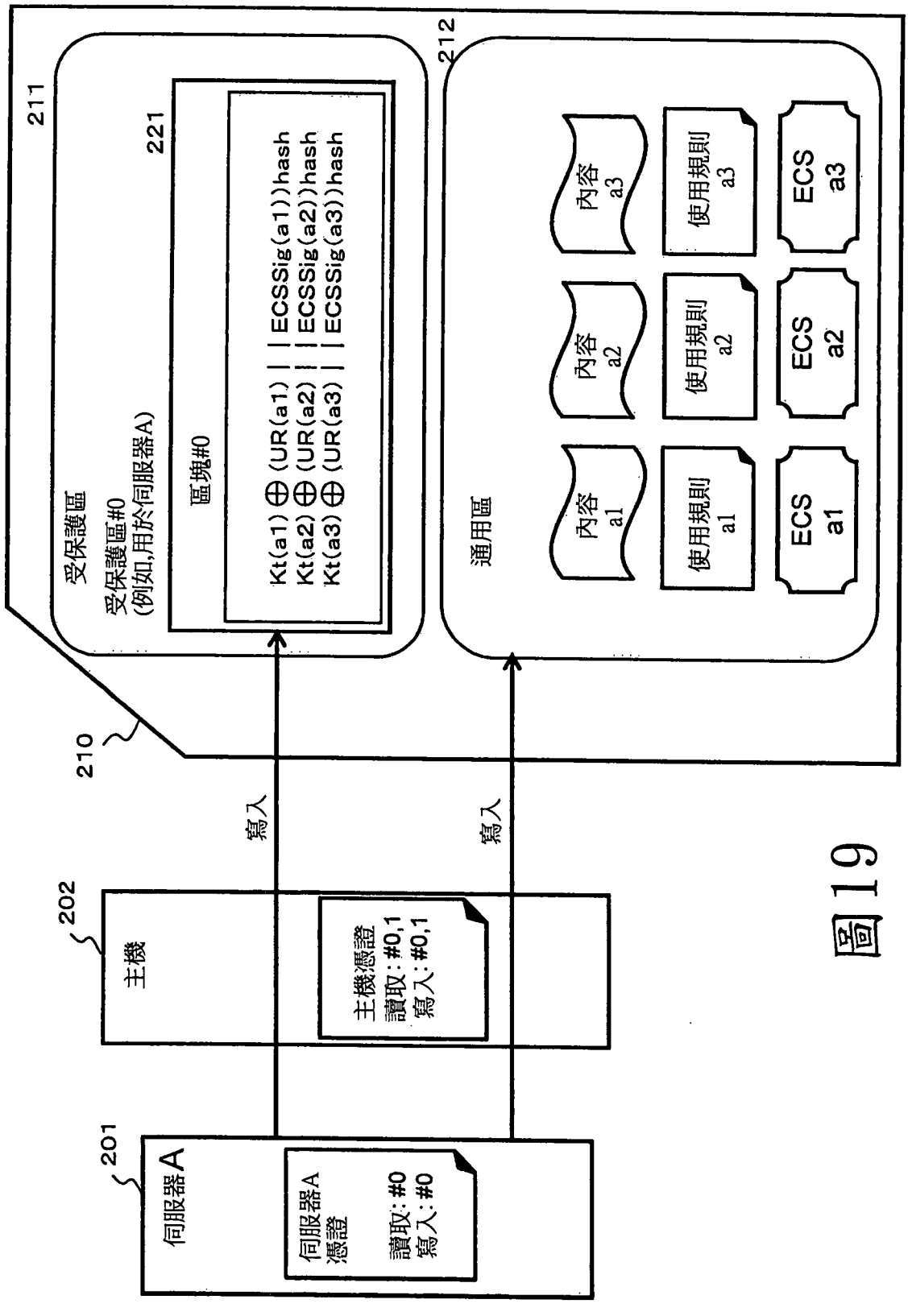

201
伺服器A
伺服器A
憑證
讀取: #0
寫入: #0
202
主機
主機憑證
讀取: #0,1
寫入: #0,1
寫入
寫入
210
211
受保護區
受保護區#0
(例如,用於伺服器A)
221
區塊#0
Kt(a1) ⊕ (UR(a1) | | ECSSig(a1))hash
Kt(a2) ⊕ (UR(a2) | | ECSSig(a2))hash
Kt(a3) ⊕ (UR(a3) | | ECSSig(a3))hash
212
通用區
內容 a1
使用規則 a1
ECS a1
內容 a2
使用規則 a2
ECS a2
內容 a3
使用規則 a3
ECS a3

圖 19

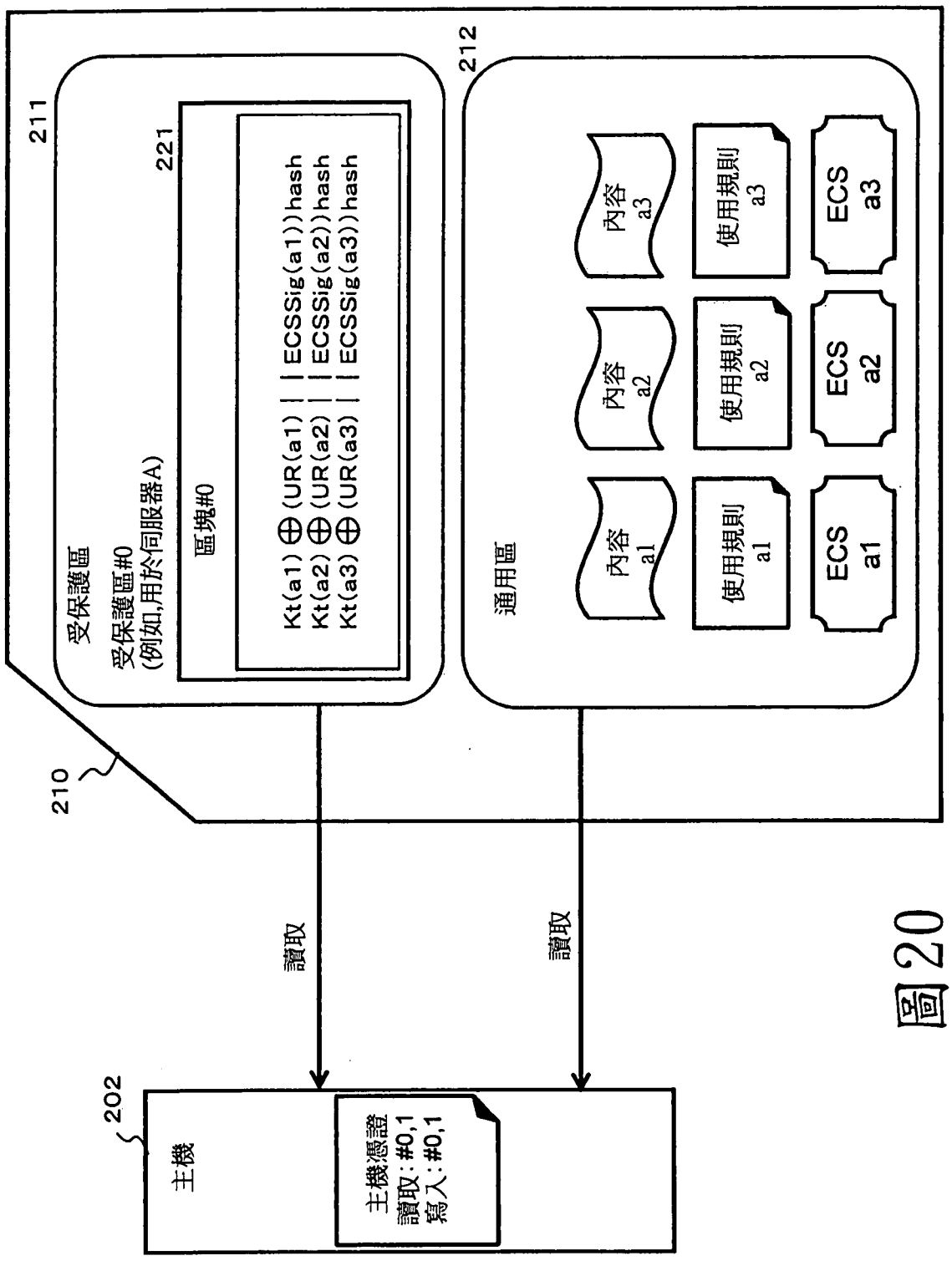

210
211
受保護區
受保護區#0
(例如,用於伺服器A)
221
區塊#0
Kt(a1) ⊕ (UR(a1) | | ECSSig(a1))hash
Kt(a2) ⊕ (UR(a2) | | ECSSig(a2))hash
Kt(a3) ⊕ (UR(a3) | | ECSSig(a3))hash
212
通用區
內容 a1
使用規則 a1
ECS a1
內容 a2
使用規則 a2
ECS a2
內容 a3
使用規則 a3
ECS a3
讀取
讀取
202
主機
主機憑證
讀取: #0,1
寫入: #0,1

圖 20

	受保護區		通用區
	區塊#0	區塊#1	
伺服器 A	Kt(a1)⊕(UR(a1)||ECSSig(a1))hash Kt(a2)⊕(UR(a2)||ECSSig(a2))hash Kt(a3)⊕(UR(a3)||ECSSig(a3))hash	---	Con(a1), UR(a1), ECS(a1) Con(a2), UR(a2), ECS(a2) Con(a3), UR(a3), ECS(a3)
伺服器 B	---	Kt(b1)⊕(UR(b1)||ECSSig(b1))hash Kt(b2)⊕(UR(b2)||ECSSig(b2))hash	Con(b1), UR(b1), ECS(b1) Con(b2), UR(b2), ECS(b2)

圖21

	受保護區		通用區
	區塊#0	區塊#1	
伺服器 A	Kt(a1)⊕(UR(a1)‖ECSSig(a1)) hash Kt(a2)⊕(UR(a2)‖ECSSig(a2))hash Kt(a3)⊕(UR(a3)‖ECSSig(a3))hash	---	Con(a1), UR(a1), ECS(a1) Con(a2), UR(a2), ECS(a2) Con(a3), UR(a3), ECS(a3)
伺服器 B	Kt(b1)⊕(UR(b1)‖ECSSig(b1))hash Kt(b2)⊕(UR(b2)‖ECSSig(b2))hash	---	Con(b1), UR(b1), ECS(b1) Con(b2), UR(b2), ECS(b2)
伺服器 C	---	Kt(c1)⊕(UR(c1)‖ECSSig(c1))hash	Con(c1), UR(c1), ECS(c1)
伺服器 D	---	Kt(d1)⊕(UR(d1)‖ECSSig(d1))hash Kt(d2)⊕(UR(d2)‖ECSSig(d2))hash	Con(d1), UR(d1), ECS(d1) Con(d2), UR(d2), ECS(d2)

圖22

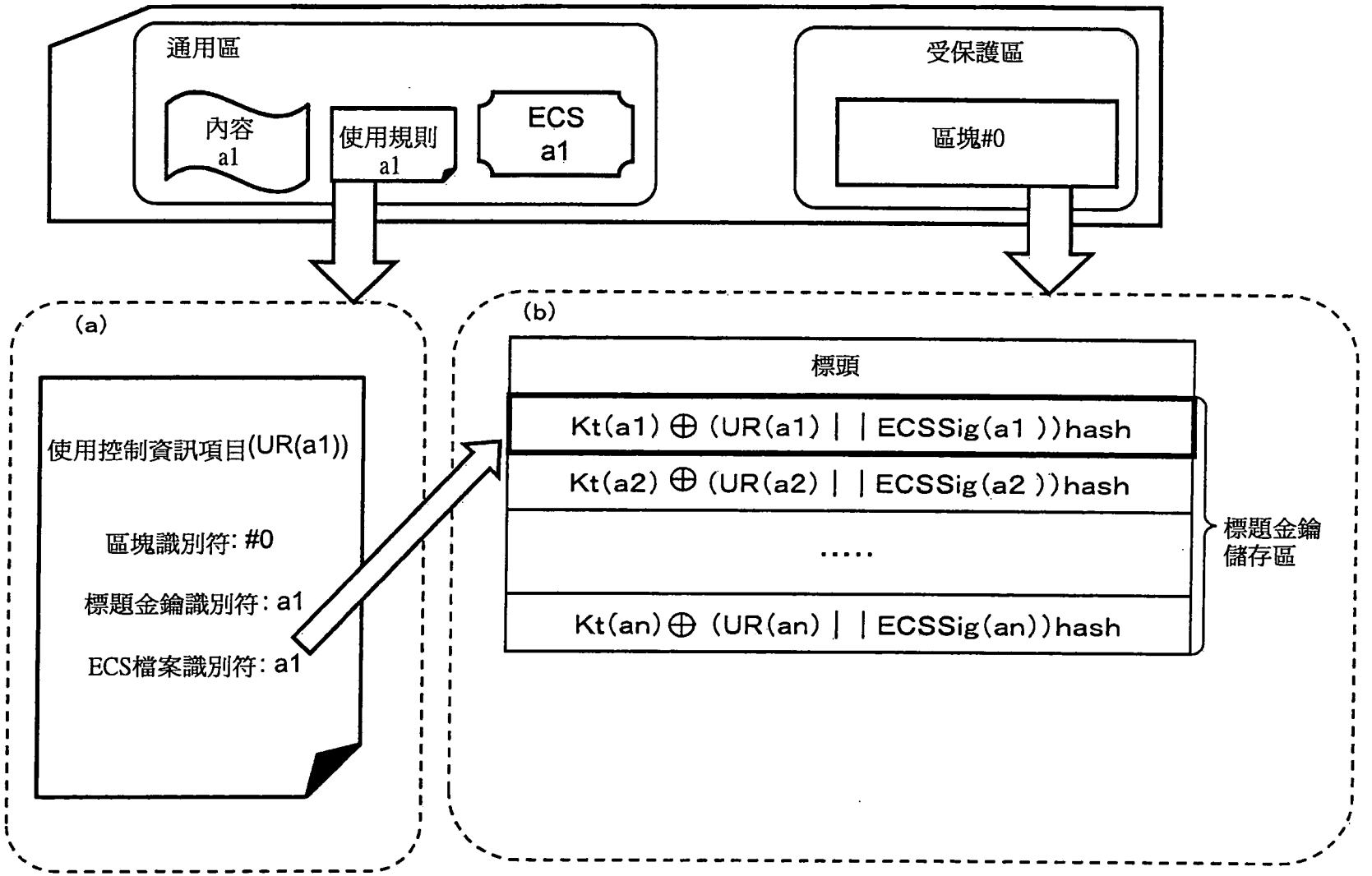

通用區
內容
a1
使用規則
a1
ECS
a1
受保護區
區塊#0
(a)
使用控制資訊項目(UR(a1))
區塊識別符: #0
標題金鑰識別符: a1
ECS檔案識別符: a1
(b)
標頭
Kt(a1) ⊕ (UR(a1) | | ECSSig(a1))hash
Kt(a2) ⊕ (UR(a2) | | ECSSig(a2))hash
.....
Kt(an) ⊕ (UR(an) | | ECSSig(an))hash
標題金鑰
儲存區

圖23

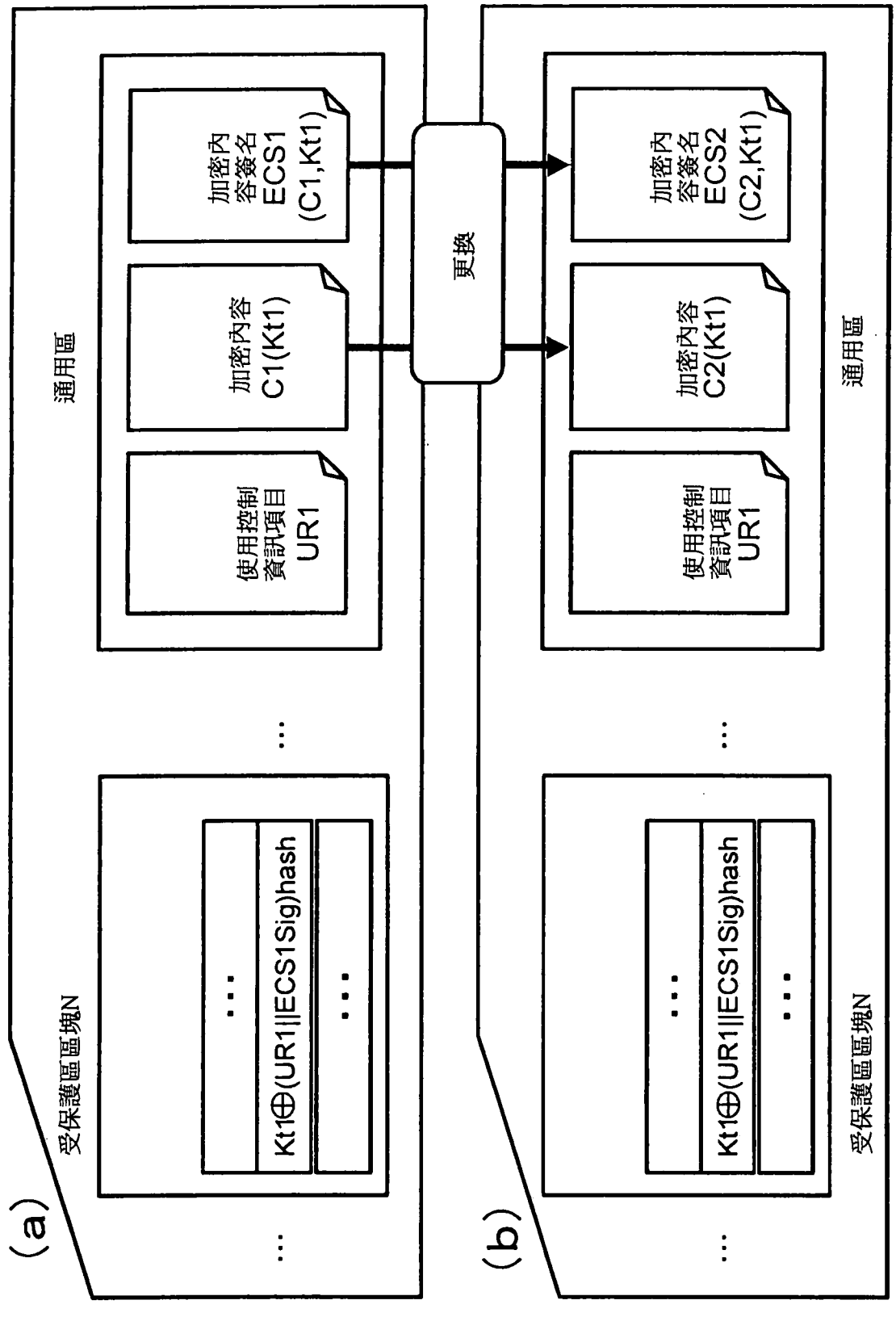

(a)
受保護區區塊N
通用區
使用控制資訊項目 UR1
加密內容 C1(Kt1)
加密內容簽名 ECS1 (C1,Kt1)
Kt1⊕(UR1||ECS1Sig)hash
更換
(b)
受保護區區塊N
通用區
使用控制資訊項目 UR1
加密內容 C2(Kt1)
加密內容簽名 ECS2 (C2,Kt1)
Kt1⊕(UR1||ECS1Sig)hash

圖 24

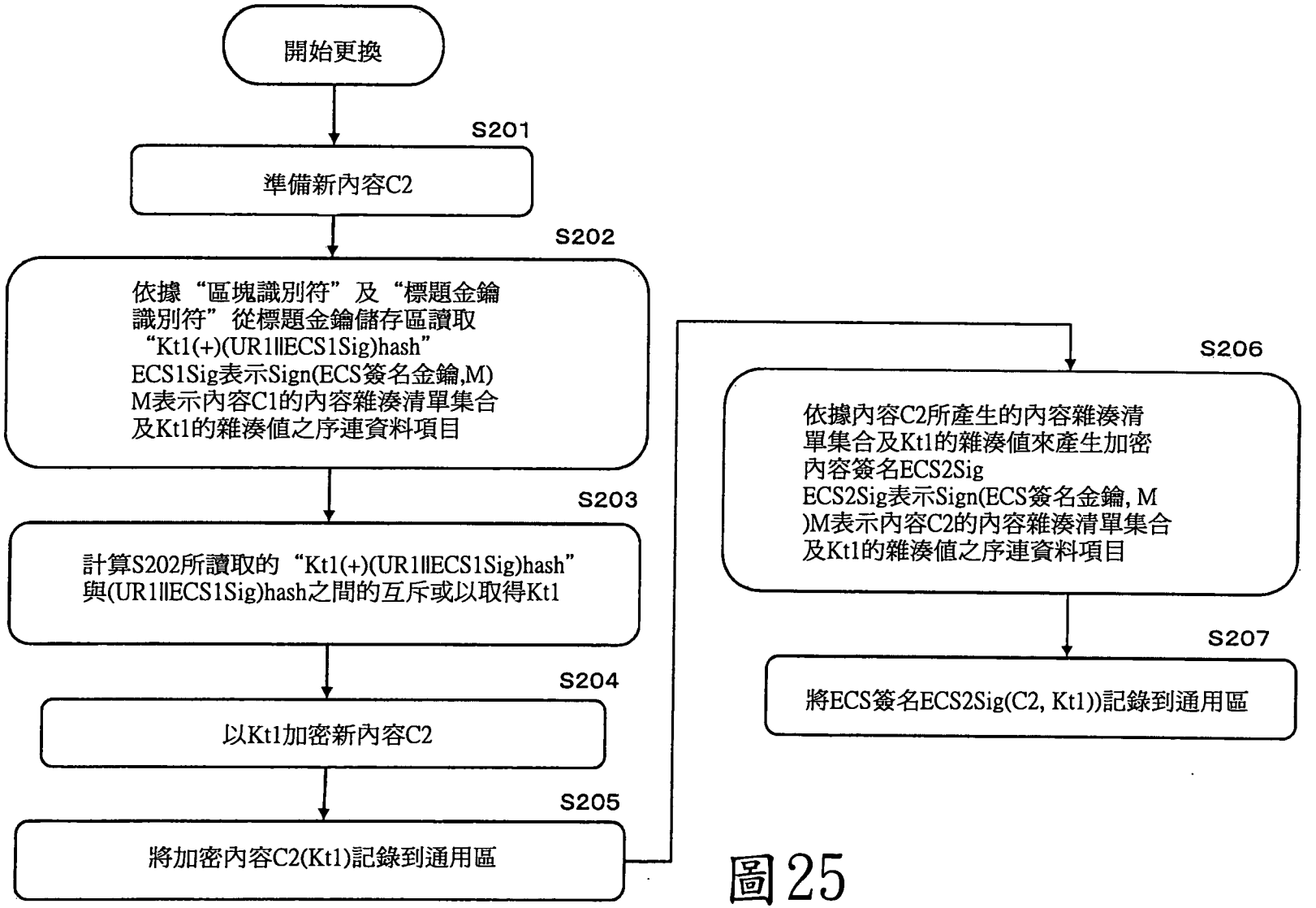

開始更換
S201
準備新內容C2
S202
依據“區塊識別符”及“標題金鑰識別符”從標題金鑰儲存區讀取“Kt1(+)(UR1||ECS1Sig)hash”
ECS1Sig表示Sign(ECS簽名金鑰,M)
M表示內容C1的內容雜湊清單集合及Kt1的雜湊值之序連資料項目
S203
計算S202所讀取的“Kt1(+)(UR1||ECS1Sig)hash”與(UR1||ECS1Sig)hash之間的互斥或以取得Kt1
S204
以Kt1加密新內容C2
S205
將加密內容C2(Kt1)記錄到通用區
S206
依據內容C2所產生的內容雜湊清單集合及Kt1的雜湊值來產生加密內容簽名ECS2Sig
ECS2Sig表示Sign(ECS簽名金鑰, M)M表示內容C2的內容雜湊清單集合及Kt1的雜湊值之序連資料項目
S207
將ECS簽名ECS2Sig(C2, Kt1))記錄到通用區

圖25

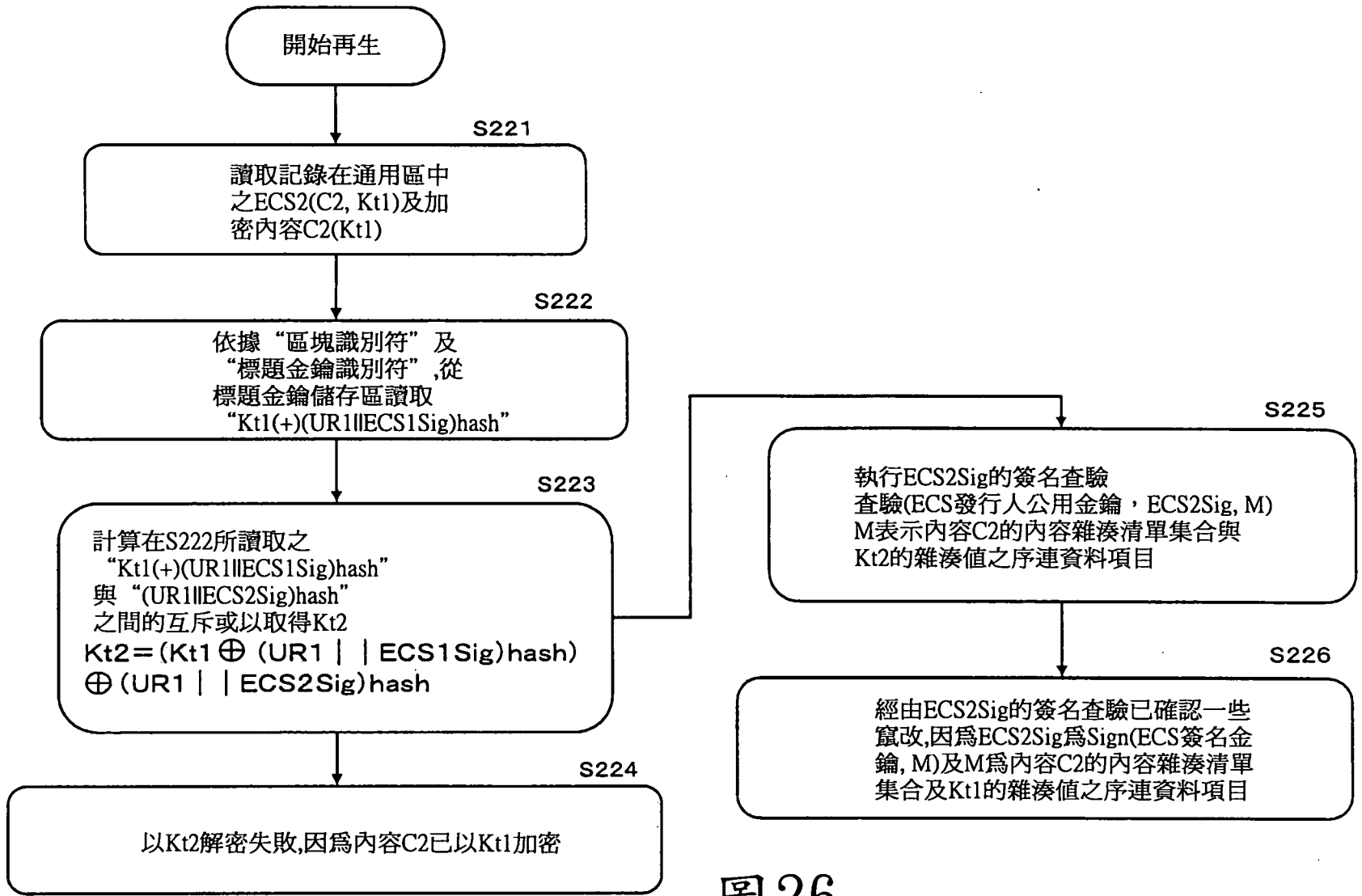

開始再生
S221
讀取記錄在通用區中
之ECS2(C2, Kt1)及加
密內容C2(Kt1)
S222
依據“區塊識別符”及
“標題金鑰識別符”,從
標題金鑰儲存區讀取
“Kt1(+)(UR1||ECS1Sig)hash”
S223
計算在S222所讀取之
“Kt1(+)(UR1||ECS1Sig)hash”
與“(UR1||ECS2Sig)hash”
之間的互斥或以取得Kt2
Kt2＝(Kt1 ⊕ (UR1 | | ECS1Sig)hash)
⊕ (UR1 | | ECS2Sig)hash
S224
以Kt2解密失敗,因爲內容C2已以Kt1加密
S225
執行ECS2Sig的簽名查驗
查驗(ECS發行人公用金鑰，ECS2Sig, M)
M表示內容C2的內容雜湊清單集合與
Kt2的雜湊值之序連資料項目
S226
經由ECS2Sig的簽名查驗已確認一些
竄改,因爲ECS2Sig爲Sign(ECS簽名金
鑰, M)及M爲內容C2的內容雜湊清單
集合及Kt1的雜湊值之序連資料項目

圖26

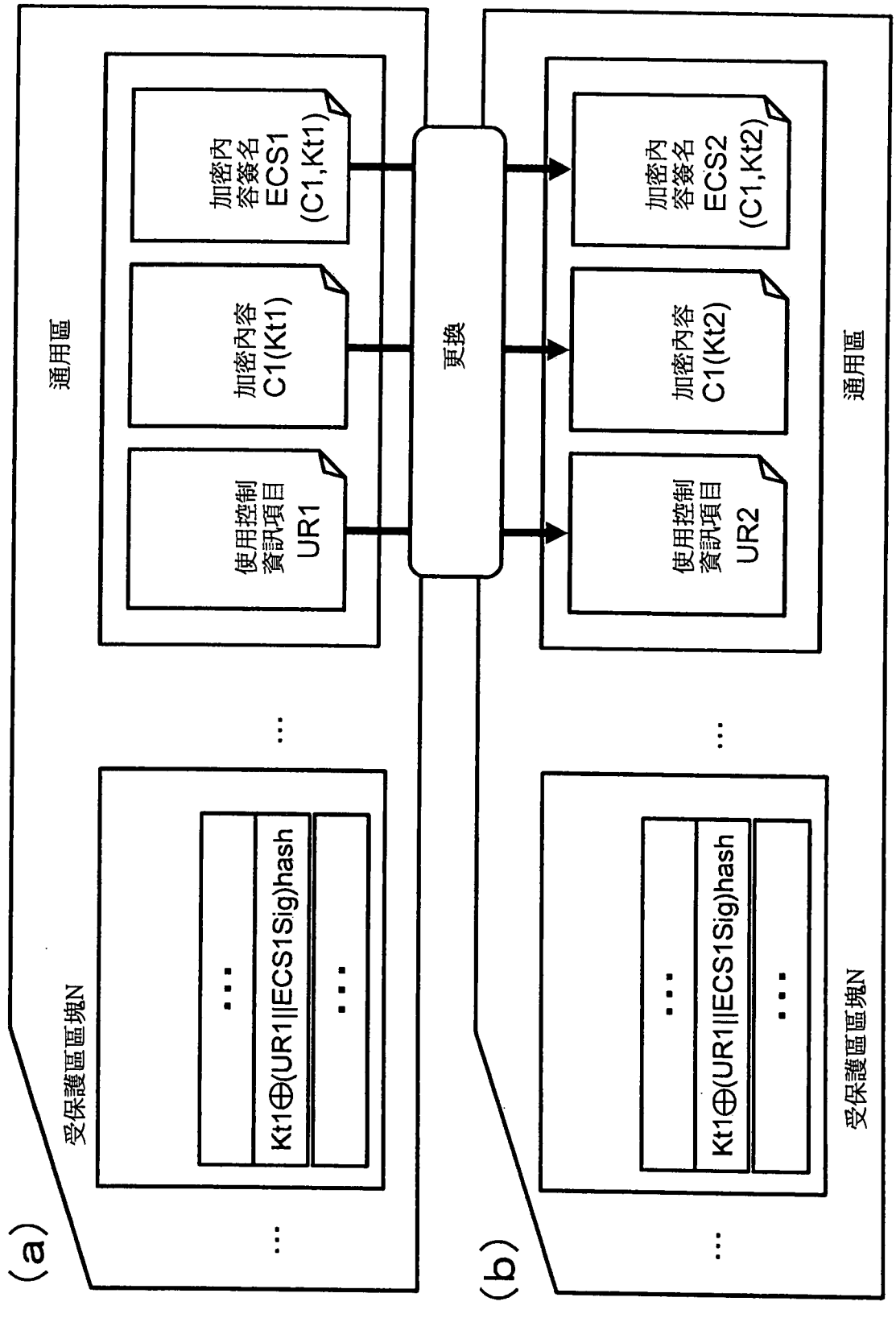

(a)
通用區
受保護區塊N
使用控制資訊項目 UR1
加密內容 C1(Kt1)
加密內容簽名 ECS1 (C1,Kt1)
Kt1⊕(UR1||ECS1Sig)hash
更換
(b)
通用區
受保護區塊N
使用控制資訊項目 UR2
加密內容 C1(Kt2)
加密內容簽名 ECS2 (C1,Kt2)
Kt1⊕(UR1||ECS1Sig)hash

圖27

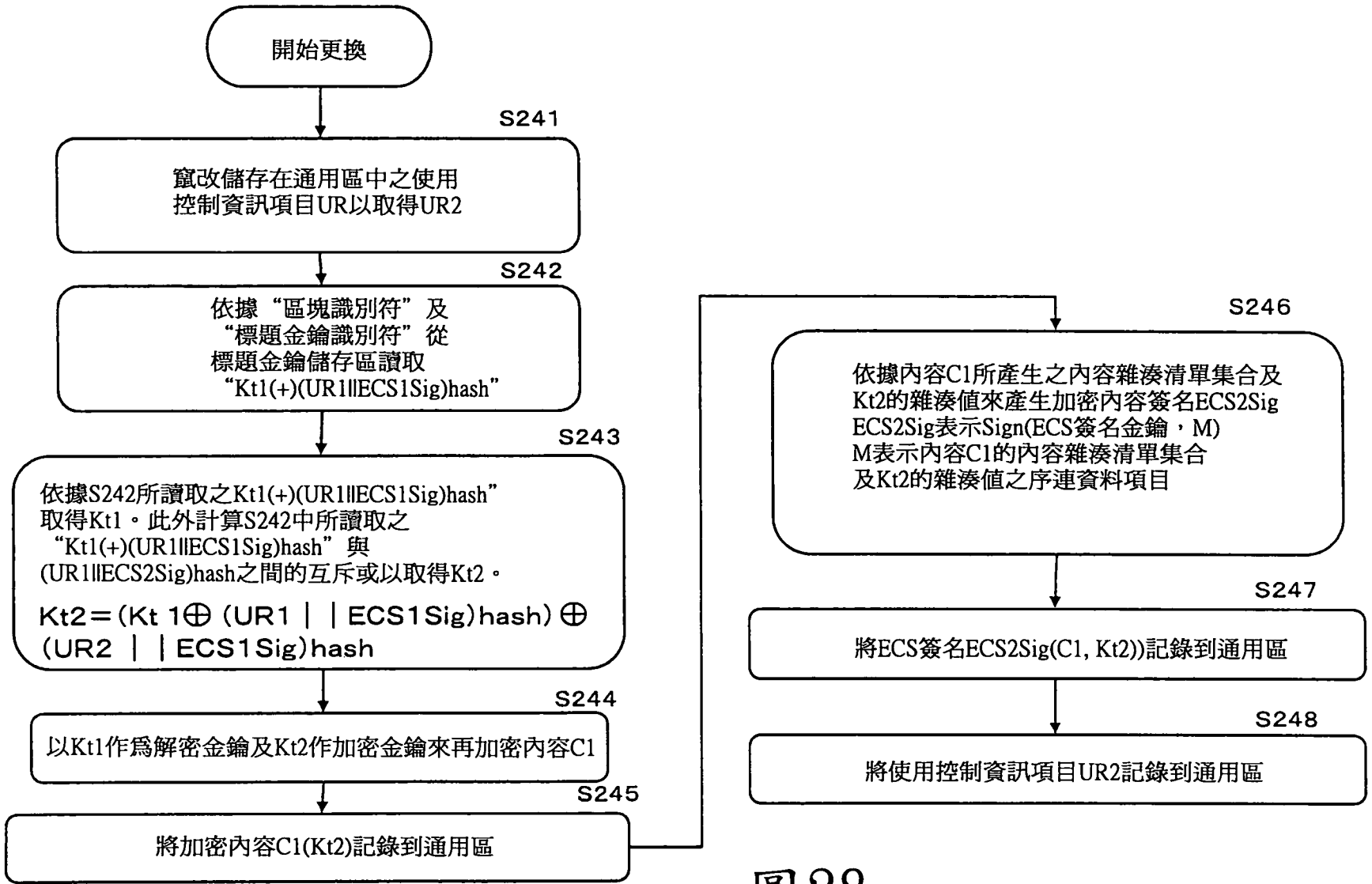

開始更換
S241
竄改儲存在通用區中之使用
控制資訊項目UR以取得UR2
S242
依據“區塊識別符”及
“標題金鑰識別符”從
標題金鑰儲存區讀取
“Kt1(+)(UR1||ECS1Sig)hash”
S243
依據S242所讀取之Kt1(+)(UR1||ECS1Sig)hash”
取得Kt1。此外計算S242中所讀取之
“Kt1(+)(UR1||ECS1Sig)hash”與
(UR1||ECS2Sig)hash之間的互斥或以取得Kt2。
Kt2＝(Kt 1⊕ (UR1 | | ECS1Sig)hash) ⊕
(UR2 | | ECS1Sig)hash
S244
以Kt1作爲解密金鑰及Kt2作加密金鑰來再加密內容C1
S245
將加密內容C1(Kt2)記錄到通用區
S246
依據內容C1所產生之內容雜湊清單集合及
Kt2的雜湊值來產生加密內容簽名ECS2Sig
ECS2Sig表示Sign(ECS簽名金鑰，M)
M表示內容C1的內容雜湊清單集合
及Kt2的雜湊值之序連資料項目
S247
將ECS簽名ECS2Sig(C1, Kt2))記錄到通用區
S248
將使用控制資訊項目UR2記錄到通用區

圖28

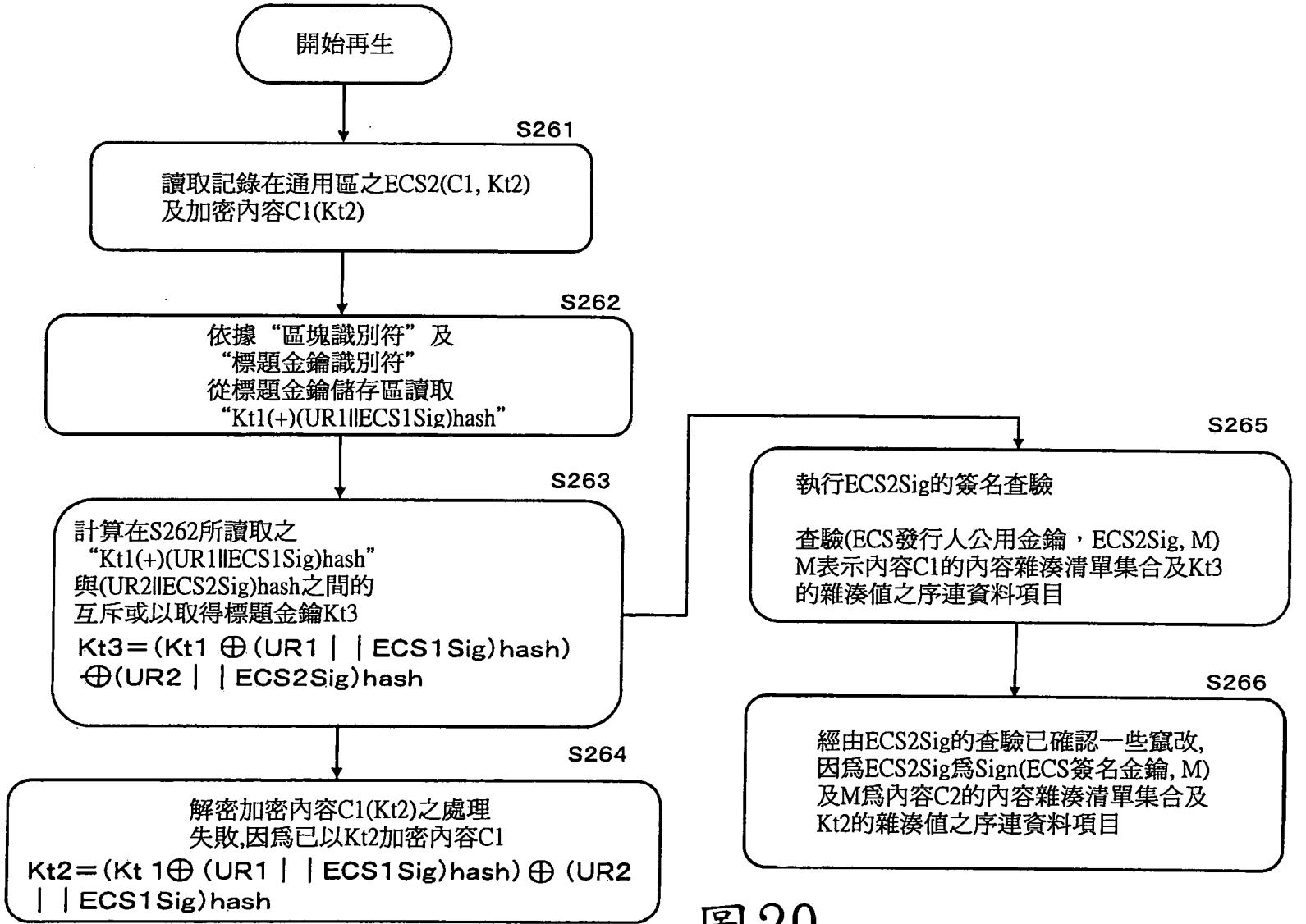

開始再生
S261
讀取記錄在通用區之ECS2(C1, Kt2)
及加密內容C1(Kt2)
S262
依據“區塊識別符”及
“標題金鑰識別符”
從標題金鑰儲存區讀取
“Kt1(+)(UR1||ECS1Sig)hash”
S263
計算在S262所讀取之
“Kt1(+)(UR1||ECS1Sig)hash”
與(UR2||ECS2Sig)hash之間的
互斥或以取得標題金鑰Kt3
Kt3＝(Kt1 ⊕(UR1｜｜ECS1Sig)hash)
⊕(UR2｜｜ECS2Sig)hash
S264
解密加密內容C1(Kt2)之處理
失敗,因爲已以Kt2加密內容C1
Kt2＝(Kt 1⊕(UR1｜｜ECS1Sig)hash)⊕(UR2
｜｜ECS1Sig)hash
S265
執行ECS2Sig的簽名查驗
查驗(ECS發行人公用金鑰，ECS2Sig, M)
M表示內容C1的內容雜湊清單集合及Kt3
的雜湊值之序連資料項目
S266
經由ECS2Sig的查驗已確認一些竄改,
因爲ECS2Sig爲Sign(ECS簽名金鑰, M)
及M爲內容C2的內容雜湊清單集合及
Kt2的雜湊值之序連資料項目

圖29

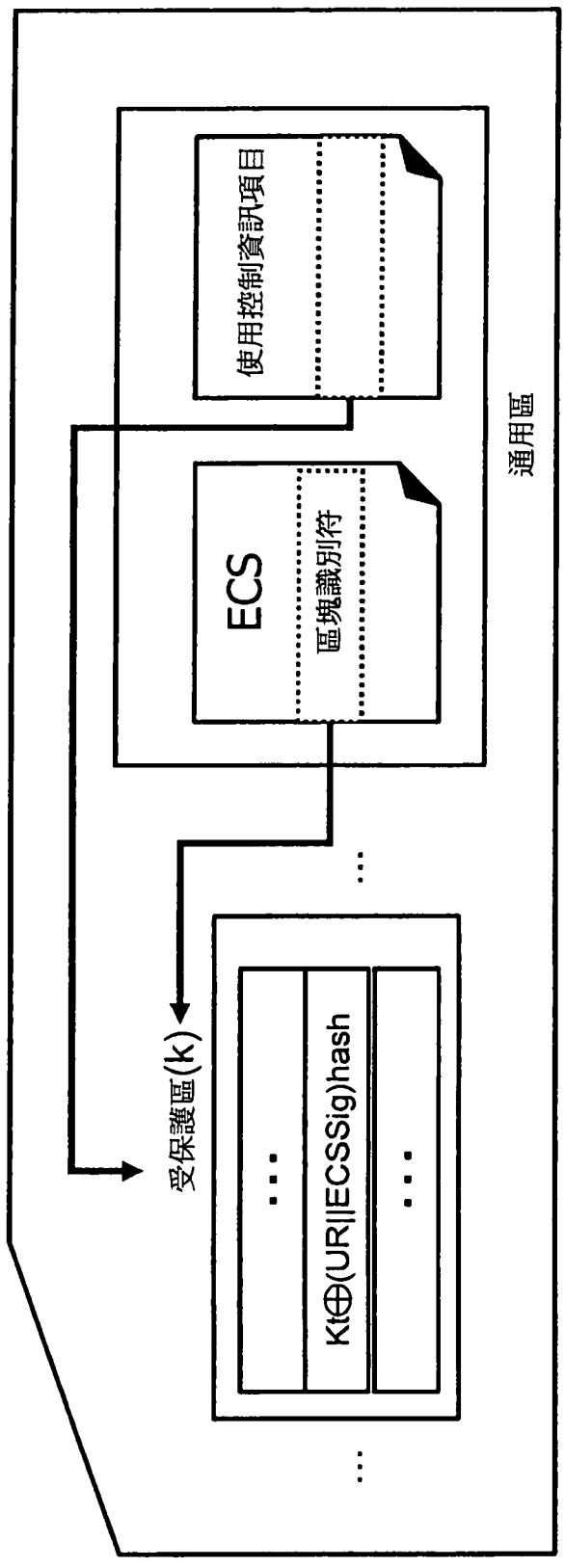


圖30

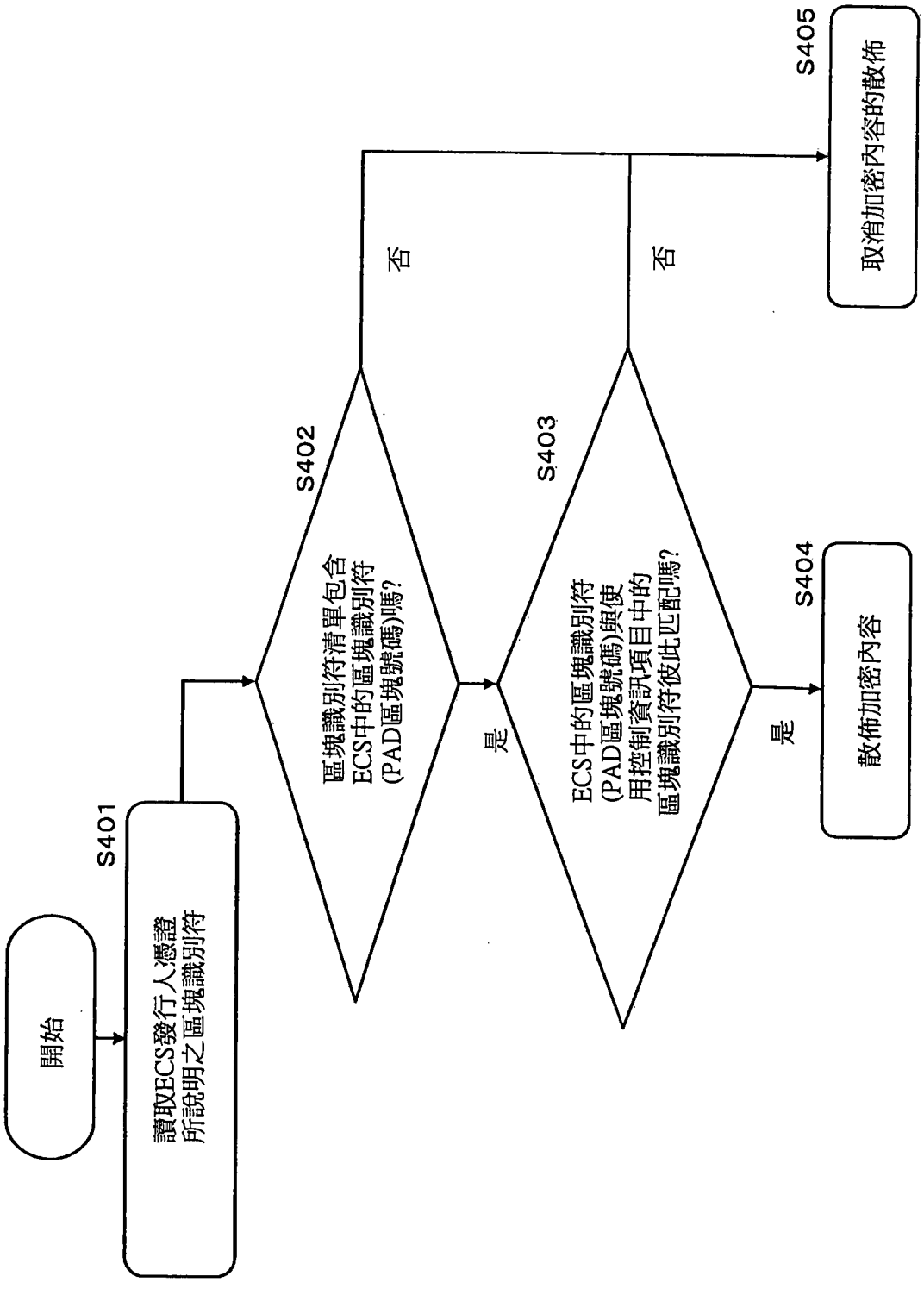

開始
S401
讀取ECS發行人憑證
所說明之區塊識別符
S402
區塊識別符清單包含
ECS中的區塊識別符
(PAD區塊號碼)嗎?
否
S403
ECS中的區塊識別符
(PAD區塊號碼)與使
用控制資訊項目中的
區塊識別符彼此匹配嗎?
否
是
是
S404
散佈加密內容
S405
取消加密內容的散佈

圖31

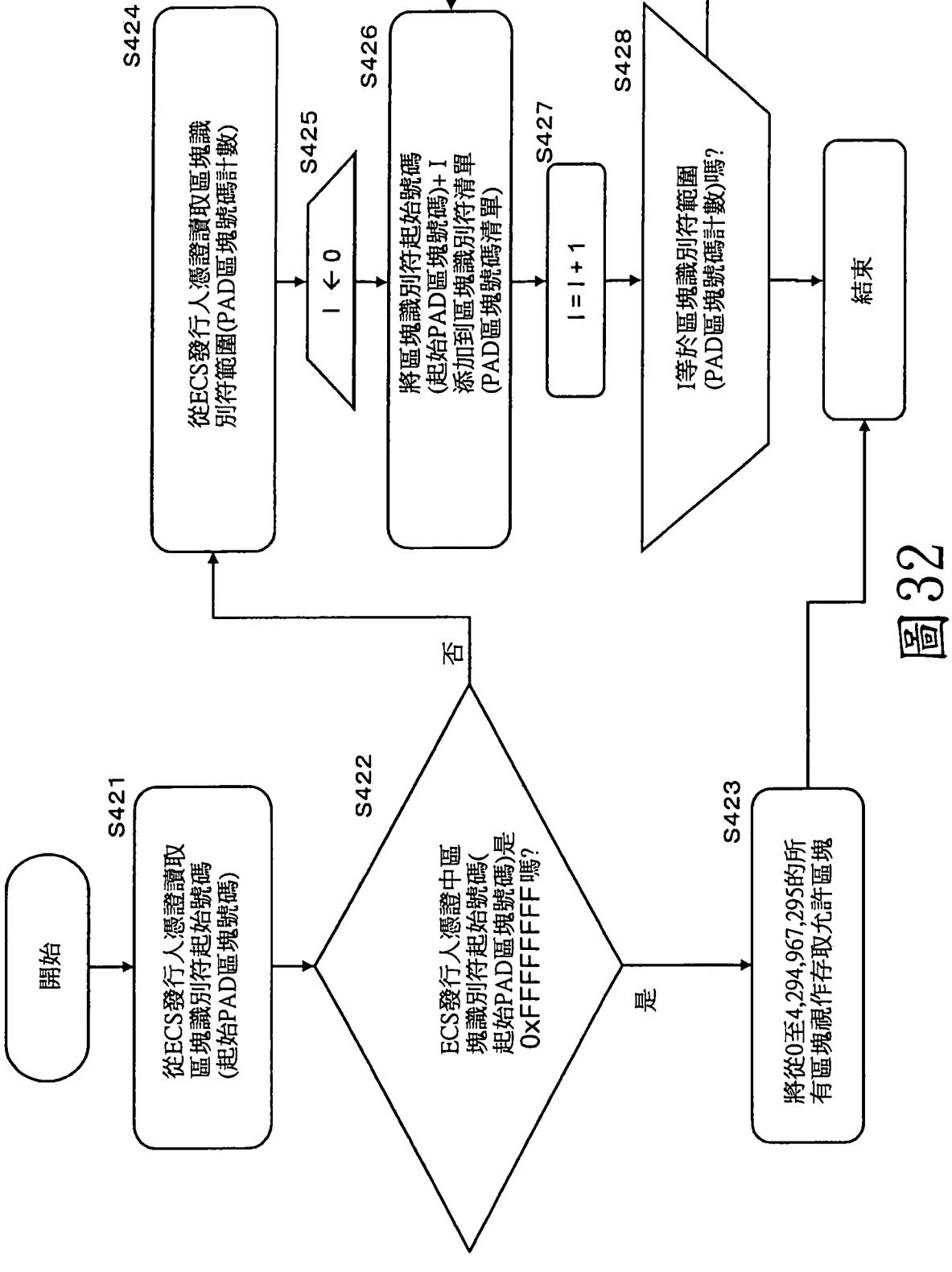

開始
S421
從ECS發行人憑證讀取區塊識別符起始號碼(起始PAD區塊號碼)
S422
ECS發行人憑證中區塊識別符起始號碼(起始PAD區塊號碼)是0xFFFFFFFF嗎?
否
是
S423
將從0至4,294,967,295的所有區塊視作存取允許區塊
結束
S424
從ECS發行人憑證讀取區塊識別符範圍(PAD區塊號碼計數)
S425
I ← 0
S426
將區塊識別符起始號碼(起始PAD區塊號碼)+ I添加到區塊識別符清單(PAD區塊號碼清單)
S427
I = I + 1
S428
I等於區塊識別符範圍(PAD區塊號碼計數)嗎?

圖32

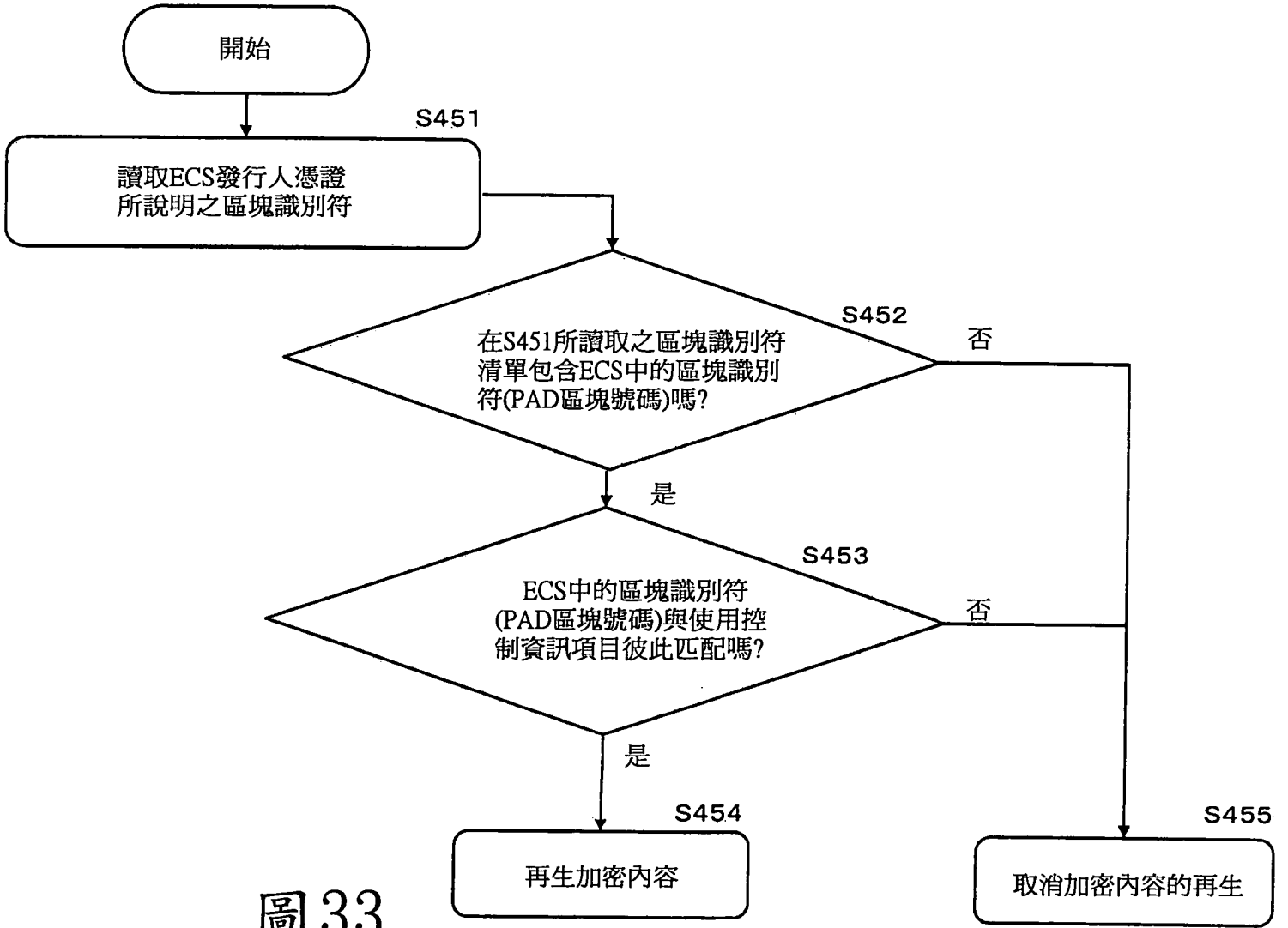

開始
S451
讀取ECS發行人憑證
所說明之區塊識別符
S452
在S451所讀取之區塊識別符
清單包含ECS中的區塊識別
符(PAD區塊號碼)嗎?
否
是
S453
ECS中的區塊識別符
(PAD區塊號碼)與使用控
制資訊項目彼此匹配嗎?
否
是
S454
再生加密內容
S455
取消加密內容的再生

圖33

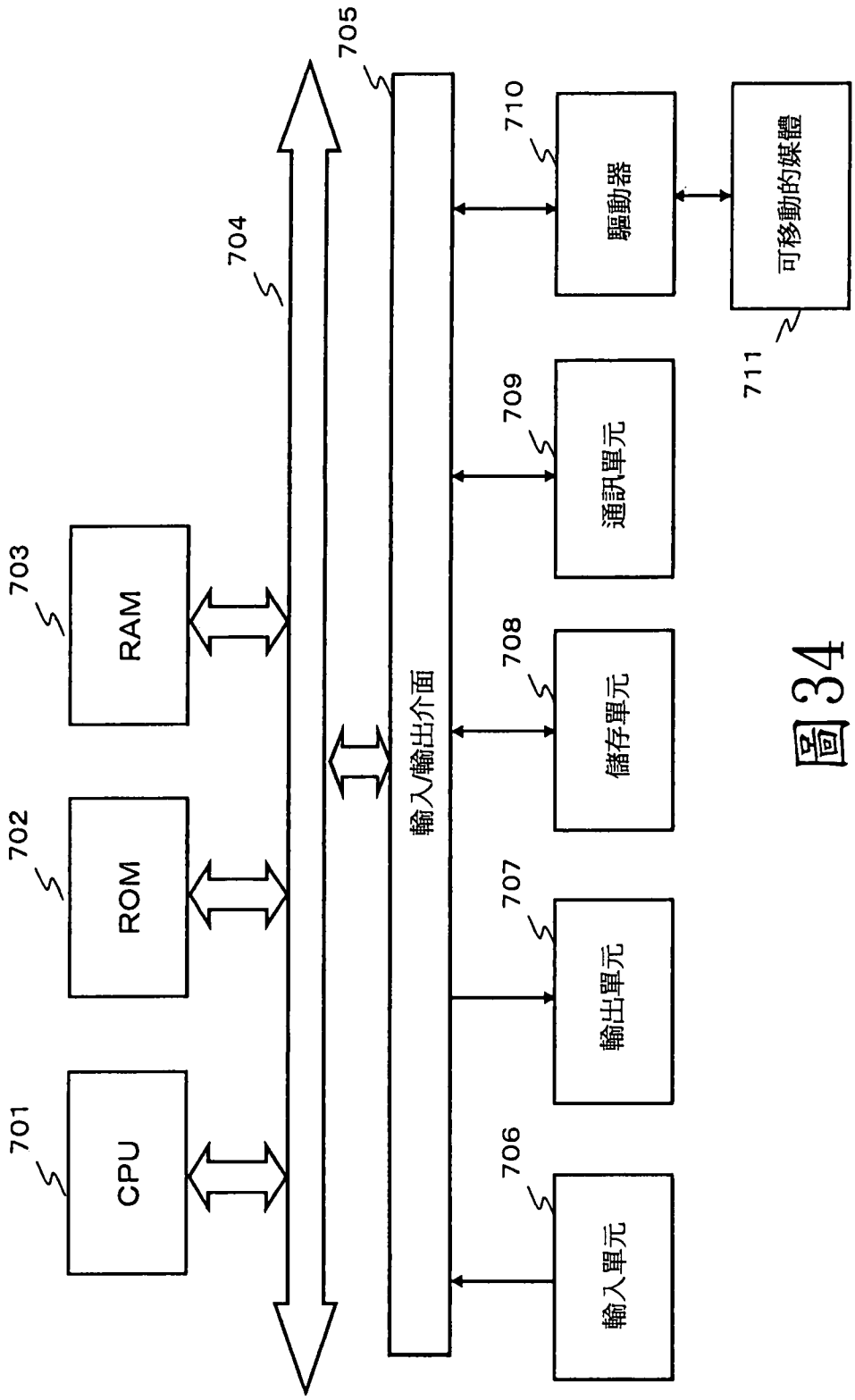

701
CPU
702
ROM
703
RAM
704
705
輸入/輸出介面
706
輸入單元
707
輸出單元
708
儲存單元
709
通訊單元
710
驅動器
711
可移動的媒體

圖34

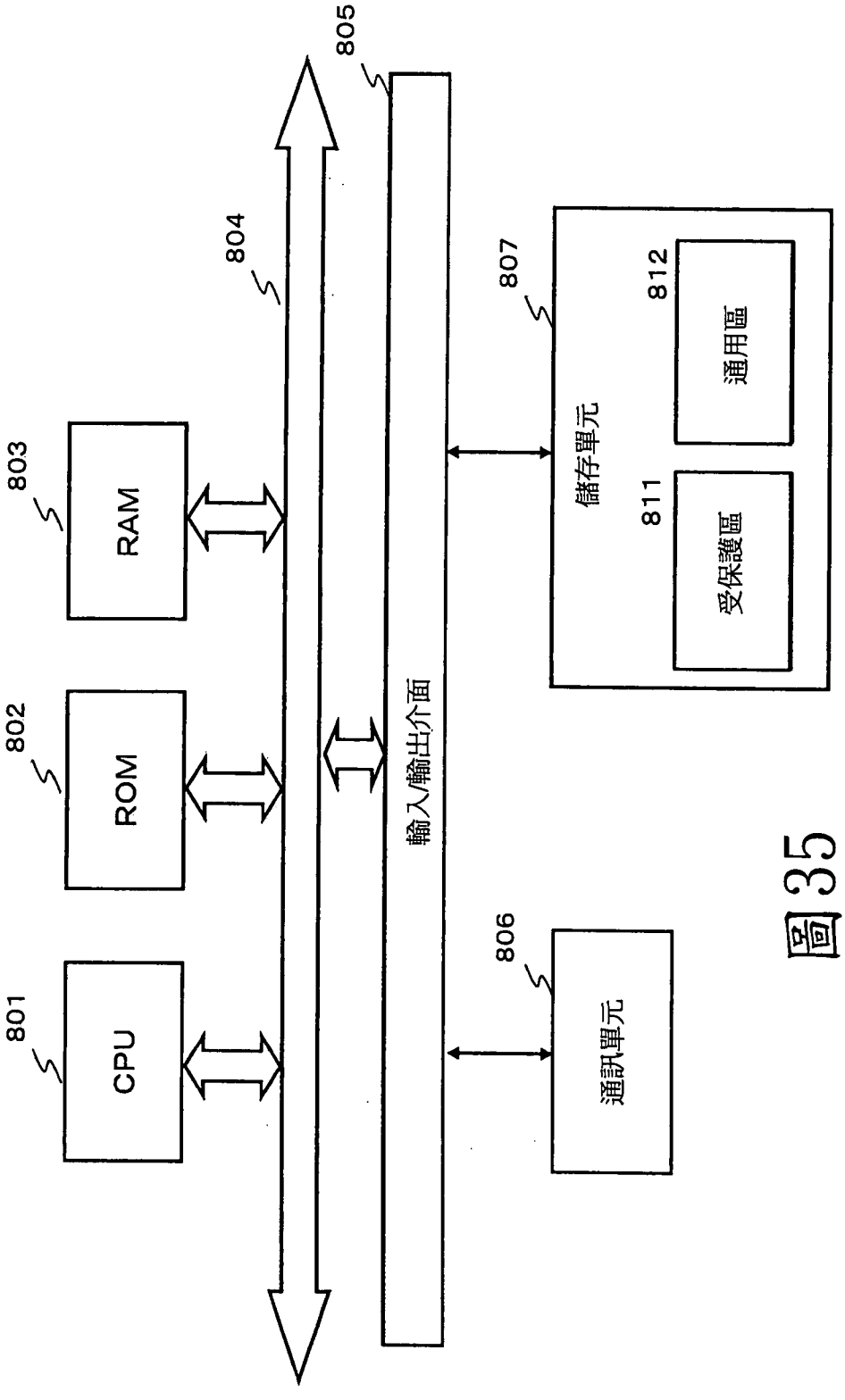

801
CPU
802
ROM
803
RAM
804
805
輸入/輸出介面
806
通訊單元
807
儲存單元
811
受保護區
812
通用區

圖 35