



(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 201313010 A1

(43)公開日：中華民國 102 (2013) 年 03 月 16 日

(21)申請案號：101125196

(22)申請日：中華民國 101 (2012) 年 07 月 12 日

(51)Int. Cl. : *H04N21/83 (2011.01)*

G11B20/10 (2006.01)

H04L9/32 (2006.01)

(30)優先權：2011/08/11 日本

2011-175606

(71)申請人：新力股份有限公司 (日本) SONY CORPORATION (JP)

日本

(72)發明人：上田健二郎 UEDA, KENJIRO (JP)；久野浩 KUNO, HIROSHI (JP)；林隆道
HAYASHI, TAKAMICHI (JP)

(74)代理人：陳長文

申請實體審查：有 申請專利範圍項數：20 項 圖式數：23 共 109 頁

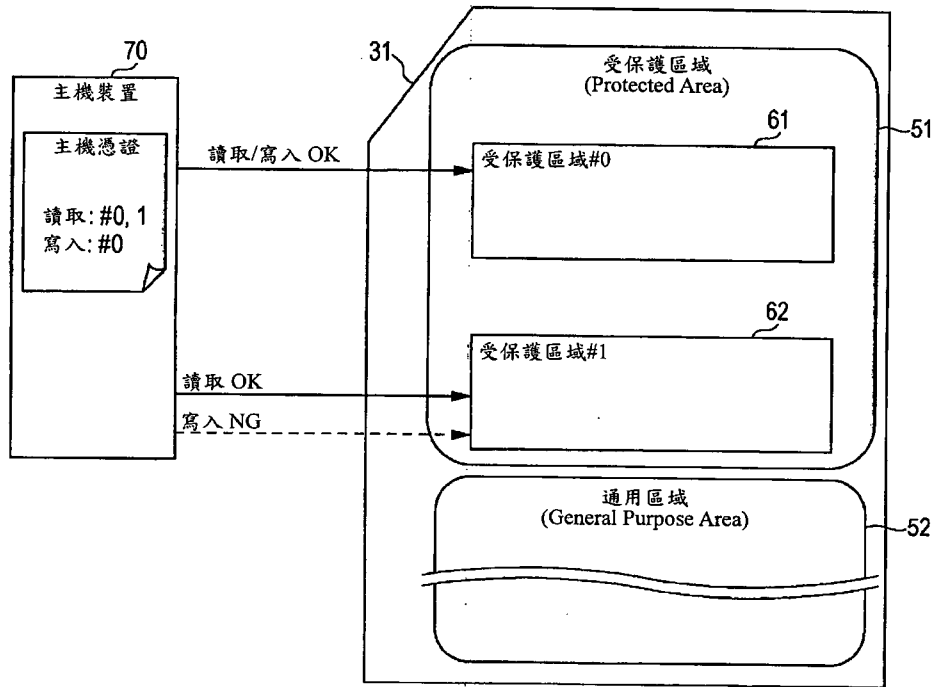
(54)名稱

資訊處理裝置及資訊處理方法，以及程式

INFORMATION PROCESSING DEVICE AND INFORMATION PROCESSING METHOD, AND
PROGRAM

(57)摘要

一種資訊處理系統包括：一媒體，其處儲存有將播放之一內容；及一播放設備，其用於播放儲存於該媒體中之一內容；其中該播放設備經組態以根據將播放之一內容類型選擇性地啟動一播放程式，藉由執行該播放程式自儲存裝置獲得與該播放程式相關之一裝置憑證，且將該所獲得裝置憑證傳輸至該媒體；其中該裝置憑證係其中記錄有在其處該裝置憑證可用之內容類型資訊之內容類型之一裝置憑證；且其中該媒體判定自該播放設備請求讀取之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。



31: 記憶卡

51: 受保護區域

52: 通用區域

61: 區段區域#0(受保護區域#0)

62: 區段區域#1(受保護區域#1)

70: 主機(記錄/播放設備)



(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 201313010 A1

(43)公開日：中華民國 102 (2013) 年 03 月 16 日

(21)申請案號：101125196

(22)申請日：中華民國 101 (2012) 年 07 月 12 日

(51)Int. Cl. : *H04N21/83 (2011.01)*

G11B20/10 (2006.01)

H04L9/32 (2006.01)

(30)優先權：2011/08/11 日本

2011-175606

(71)申請人：新力股份有限公司 (日本) SONY CORPORATION (JP)

日本

(72)發明人：上田健二郎 UEDA, KENJIRO (JP)；久野浩 KUNO, HIROSHI (JP)；林隆道
HAYASHI, TAKAMICHI (JP)

(74)代理人：陳長文

申請實體審查：有 申請專利範圍項數：20 項 圖式數：23 共 109 頁

(54)名稱

資訊處理裝置及資訊處理方法，以及程式

INFORMATION PROCESSING DEVICE AND INFORMATION PROCESSING METHOD, AND
PROGRAM

(57)摘要

一種資訊處理系統包括：一媒體，其處儲存有將播放之一內容；及一播放設備，其用於播放儲存於該媒體中之一內容；其中該播放設備經組態以根據將播放之一內容類型選擇性地啟動一播放程式，藉由執行該播放程式自儲存裝置獲得與該播放程式相關之一裝置憑證，且將該所獲得裝置憑證傳輸至該媒體；其中該裝置憑證係其中記錄有在其處該裝置憑證可用之內容類型資訊之內容類型之一裝置憑證；且其中該媒體判定自該播放設備請求讀取之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：101/25196.

※ 申請日：101.7.12

※IPC 分類

H64N 21/83

(2011.01)

G11B 20/10

(2006.01)

H64L 9/32

(2006.01)

一、發明名稱：(中文/英文)

資訊處理裝置及資訊處理方法，以及程式

INFORMATION PROCESSING DEVICE AND INFORMATION
PROCESSING METHOD, AND PROGRAM

二、中文發明摘要：

一種資訊處理系統包括：一媒體，其處儲存有將播放之一內容；及一播放設備，其用於播放儲存於該媒體中之一內容；其中該播放設備經組態以根據將播放之一內容類型選擇性地啟動一播程序，藉由執行該播程序自儲存裝置獲得與該播程序相關之一裝置憑證，且將該所獲得裝置憑證傳輸至該媒體；其中該裝置憑證係其中記錄有在其處該裝置憑證可用之內容類型資訊之內容類型之一裝置憑證；且其中該媒體判定自該播放設備請求讀取之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

三、英文發明摘要：

An information processing system including a medium where a content to be played is stored; and a playing apparatus for playing a content stored in the medium; with the playing apparatus being configured to selectively activate a playing program according to a content type to be played, to obtain a device certificate correlated with the playing program from storage by executing the playing program, and to transmit the obtained device certificate to the medium; with the device certificate being a device certificate for content types in which content type information where the device certificate is available is recorded; and with the medium determining whether or not an encryption key with reading being requested from the playing apparatus is an encryption key for decrypting an encrypted content matching an available content type recorded in the device certificate, and permitting readout of the encryption key only in the case of matching.

四、指定代表圖：

(一)本案指定代表圖為：第 (5) 圖。

(二)本代表圖之元件符號簡單說明：

31	記憶卡
51	受保護區域
52	通用區域
61	區段區域#0 (受保護區域#0)
62	區段區域#1 (受保護區域#1)
70	主機(記錄/播放設備)

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】

本發明係關於一種資訊處理裝置及一種資訊處理方法以及一種程式，且特定而言係關於有效地阻止對記錄於一記錄媒體(舉例而言，諸如一記憶卡或諸如此類)中之內容之未經授權使用的一種資訊處理裝置及一種資訊處理方法以及一種程式。

【先前技術】

近年來，諸如DVD(數位通用光碟)、Blu-ray Disc(註冊商標)、快閃記憶體等各種媒體已用作資訊記錄媒體。特定而言，近年來，使用諸如USB記憶體等具有一大容量快閃記憶空間之記憶卡已變得普遍。一使用者可藉由將一內容(諸如音樂、電影等)記錄於此等各種資訊記錄媒體中且將此等安裝於一播放設備(播放器)上而執行內容之播放。

然而，關於諸如音樂資料、影像資料等諸多內容，版權及分配權利等由一作者或其銷售者處理。因此，在提供一內容至使用者之情形下，通常提供一特定使用限制，亦即，執行控制以便僅准許具有合法使用權利之一使用者使用該內容，且以便阻止不規範使用，諸如未經准許之複製等。

舉例而言，AACs(進階存取內容系統)已用作與內容的使用控制相關之一標準。舉例而言，AACs之標準定義關於Blu-ray Disc(註冊商標)之一所記錄內容之使用控制組態。特定而言，舉例而言，AACs之標準規定用於把將記

錄於Blu-ray Disc(註冊商標)中之一內容視為一經加密內容及使得能夠將可獲得其加密密鑰之使用者限制為規則使用者等之一演算法。

然而，關於當前AACS規定，儘管存在有關關於一光碟所記錄內容(諸如Blu-ray Disc(註冊商標)或諸如此類)之使用控制組態之一規定，但不存在有關將記錄於快閃記憶體(舉例而言，諸如一記憶卡或諸如此類)中之一內容之充分規定。因此，有關此一記憶卡中之一所記錄內容，對一版權之保護可能不充分，且因此，已請求建立有關使用諸如一記憶卡或諸如此類之一媒體之內容使用之一使用控制組態。

舉例而言，關於AACS規定，關於一光碟所記錄內容(諸如Blu-ray Disc(註冊商標)或諸如此類)存在以下規定作為一使用控制組態。

(a)關於自其中已經記錄有一內容之一媒體(例如，ROM光碟)複製至諸如Blu-ray Disc(註冊商標)之一光碟之一內容之使用規定

(b)關於自一伺服器下載且記錄於諸如Blu-ray Disc(註冊商標)之一光碟中之一內容之使用規定

舉例而言，規定此等內容之使用控制。

關於AACS，舉例而言，在執行以上(a)中之媒體之間之一內容之複製之情形下，規定以自一管理伺服器獲得複製准許資訊作為一條件之受管理複製(MC：Managed Copy)。

此外，作為以上(b)中一內容自一伺服器之下載處理，關於AACS，規定各種類型之下載模式，諸如使用一使用者裝置(諸如一PC或諸如此類)之EST(電子銷售影片服務)、使用安裝於一便利商店中之一共用終端機之MoD(按需製造)或諸如此類，且在藉由此等下載處理中之每一下載處理將一內容記錄於一光碟中且亦使用此之情形下，必需根據一預定規則執行處理。注意，舉例而言，此等程序闡述於日本未經審查專利申請公開案第2008-98765號中。

然而，如上文所闡述，關於AACS規定，存在一問題係，規定假定執行光碟所記錄內容(諸如，關於Blu-ray Disc(註冊商標)或諸如此類)之使用控制，且不存在關於有關記錄於記憶卡(諸如一快閃記憶體類型，包括USB記憶體等)中之內容之充分使用控制之規範。

【發明內容】

已發現需要提供在將一內容記錄於一資訊記錄媒體(諸如快閃記憶體或諸如此類)中及使用此來阻止對內容之未經授權使用之情形下建立使用控制組態之一種資訊處理裝置、一種資訊處理方法以及一種程式。

根據本發明之一實施例，一種資訊處理系統包括：一媒體，其中儲存有用作將播放之一物件之一內容；及一播放設備，其經組態以播放儲存於該媒體中之一內容；其中該播放設備經組態以根據被選定為將播放之一物件之一內容類型選擇性地啟動一播放程式，藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與該播放程式相關之一裝置

憑證，且將該所獲得裝置憑證傳輸至該媒體；其中該裝置憑證係其中記錄有可利用該裝置憑證之內容類型資訊之一內容類型對應裝置憑證；且其中該媒體判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

此外，關於本發明之該資訊處理系統之一實施例，該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構；其中該媒體判定已請求自該播放設備讀取其之一加密密鑰是否係用於解密匹配係記錄於該裝置憑證中之一可用內容類型之一高附加價值內容或正常內容之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

此外，關於本發明之該資訊處理系統之一實施例，該播放設備將一所獲得裝置憑證傳輸至該等媒體以執行鑑認處理；其中該媒體以建立該鑑認處理作為一條件而執行對來自該播放設備之一加密密鑰讀出請求之准許判定處理。

此外，關於本發明之該資訊處理系統之一實施例，該播放設備藉由根據與被選定為將播放之一物件之一內容相關之屬性資訊識別一選定內容之類型而選擇性地啟動一播程式。

此外，關於本發明之該資訊處理系統之一實施例，該媒

體將一加密密鑰儲存於在其處基於對一播放設備之存取權限之確認而准許存取之一受保護區域中，且基於記錄於將自該播放設備接收之一裝置憑證中之受保護區域存取權限資訊而確認在其處儲存有該加密密鑰之該受保護區域之存取權限，且在確認該播放設備之該等存取權限之情形下准許該播放設備讀出一加密密鑰。

此外，關於本發明之該資訊處理系統之一實施例，該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結構；其中該媒體根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該播放設備；且其中該播放設備伴隨藉由根據對應於該設備本身之裝置類型之一解碼演算法解碼自該媒體接收之一經編碼媒體ID而獲得之一媒體ID已應用於其之資料處理而執行對一內容之解碼或播放。

根據本發明之一實施例，一種資訊處理裝置包括：一資料處理單元，其經組態以執行對儲存於一媒體中之一內容之讀出及回放處理；其中該資料處理單元經組態以根據被選定為將播放之一物件之一內容類型選擇性地啟動一播放程式，藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與此播放程式相關之一裝置憑證以將該所獲得裝置憑證傳輸至該媒體，且亦將一經加密內容及對將應用於對此經加密內容之解密之一加密密鑰之一讀出請求輸出至該媒體，且以該媒體做出確認作為一條件而自該媒體獲得一加

密密鑰，其中已執行對其之該讀出請求之一加密密密鑰係匹配記錄於該裝置憑證中之可使用之一內容類型之一內容之一加密密密鑰以藉由將該所獲得加密密密鑰應用於一經加密內容而執行對該經加密內容之解密。

此外，關於本發明之該資訊處理裝置之一實施例，該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構。

此外，關於本發明之該資訊處理裝置之一實施例，該資料處理單元將一所獲得裝置憑證傳輸至該媒體以執行鑑認處理。

此外，關於本發明之該資訊處理裝置之一實施例，該資料處理單元藉由根據與被選定為將播放之一物件之一內容相關之屬性資訊識別一選定內容之類型而選擇性地啟動一播放程式。

此外，關於本發明之該資訊處理裝置之一實施例，該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結構；其中該媒體根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該資訊處理裝置；且其中該資訊處理裝置之一資料處理單元伴隨藉由根據對應於該設備本身之裝置類型之一解碼演算法解碼自該媒體接收之一經編碼媒體ID而獲得之一媒體ID已應用於其之資料處理而執行對一內容之解碼或播放。

根據本發明之一實施例，一種資訊處理裝置包括：一儲存單元，其中儲存有用作將在一播放設備中播放之一物件之一經加密內容及將應用於對該經加密內容之解密之一加密密鑰；及一資料處理單元；其中該資料處理單元經組態以自該播放設備接收一裝置憑證，且亦接收對將應用於對用作將播放之一物件之一經加密內容之解密之一加密密鑰的一讀出請求，且判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

此外，關於本發明之該資訊處理裝置之一實施例，該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構；其中該資料處理單元判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配具有記錄於該裝置憑證中之一可用內容類型之一高附加價值內容或正常內容之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

此外，關於本發明之該資訊處理裝置之一實施例，該加密密鑰儲存於在其處基於對一播放設備之存取權限之確認而准許存取之一儲存單元內之一受保護區域中；其中該資料處理單元基於記錄於將自該播放設備接收之一裝置憑證中之受保護區域存取權限資訊而確認在其處儲存有該加密密鑰之該受保護區域之存取權限，且在確認該播放設備之

該等存取權限之情形下准許該播放設備讀出一加密密鑰。

此外，關於本發明之該資訊處理裝置之一實施例，該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結構；其中該資料處理單元根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該播放設備。

本發明之一實施例係一種將在一資訊處理系統中執行之資訊處理方法，該資訊處理系統具有：一媒體，其中儲存有用作將播放之一物件之一內容，及一播放設備，其經組態以播放儲存於該媒體中之一內容，其中該播放設備經組態以根據被選定為將播放之一物件之一內容類型選擇性地啟動一播放程式，且藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與該播放程式相關之一裝置憑證以將該所獲得裝置憑證傳輸至該媒體；其中該裝置憑證係其中記錄有可利用該裝置憑證之內容類型資訊之一裝置憑證；且其中該媒體判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

本發明之一實施例係一種將在一資訊處理裝置中執行之資訊處理方法，其中一資料處理單元經組態以根據被選定為將播放之一物件之一內容類型選擇性地啟動一播放程式，且藉由執行該選擇性地啟動之播放程式自一儲存單元

獲得與此播放程式相關之一裝置憑證以將該所獲得裝置憑證傳輸至該媒體，且亦將一經加密內容及對將應用於對此經加密內容之解密之一加密密鑰之一讀出請求輸出至該媒體，且以該媒體做出確認作為一條件而自該媒體獲得一加密密鑰，其中已執行對其之該讀出請求之一加密密鑰係匹配記錄於該裝置憑證中之可使用之一內容類型之一內容之一加密密鑰以藉由將該所獲得加密密鑰應用於一經加密內容而執行對該經加密內容之解密。

本發明之一實施例係一種將在一資訊處理裝置中執行之資訊處理方法，其中該資訊處理裝置包括：一儲存單元，其中儲存有用作將在一播放設備中播放之一物件之一經加密內容及將應用於對該經加密內容之解密之一加密密鑰；及一資料處理單元；其中該資料處理單元經組態以自該播放設備接收一裝置憑證，且亦接收對將應用於對用作將播放之一物件之一經加密內容之解密之一加密密鑰之一讀出請求，且判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

本發明之一實施例係一種致使一資訊處理裝置執行資訊處理且致使一資料處理單元進行以下操作之程式：根據被選定為將播放之一物件之一內容類型選擇性地啟動一播放程式，藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與此播放程式相關之一裝置憑證以將該所獲得裝置憑

證傳輸至該媒體，且亦將一經加密內容及對將應用於對此經加密內容之解密之一加密密鑰之一讀出請求輸出至該媒體，且以該媒體做出確認作為一條件而自該媒體獲得一加密密鑰，其中已執行對其之該讀出請求之一加密密鑰係匹配記錄於該裝置憑證中之可使用之一內容類型之一內容之一加密密鑰以藉由將該所獲得加密密鑰應用於一經加密內容而執行對該經加密內容之解密。

本發明之一實施例係一種致使一資訊處理裝置執行資訊處理之程式，其中該資訊處理裝置包括：一儲存單元，其中儲存有用作將在一播放設備中播放之一物件之一經加密內容及將應用於對該經加密內容之解密之一加密密鑰；及一資料處理單元；其中該程式致使該資料處理單元自該播放設備接收一裝置憑證，且亦接收對將應用於對用作將播放之一物件之一經加密內容之解密的一加密密鑰的一讀出請求，且判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

注意，舉例而言，根據本發明之程式係可藉助一儲存媒體或通信媒體提供且將以關於可執行各種程式碼之一資訊處理裝置或電腦系統之一電腦可讀格式提供之一程式。此一程式係以一電腦可讀格式提供，且因此，實現根據該資訊處理裝置或電腦系統上之該程式之處理。

本發明之其他目的、特徵及優點根據本發明之稍後闡述

之實施例及附圖將變得顯而易見。注意，如本說明書中所使用之系統係多個裝置之一邏輯群組組態，且不限於每一組成裝置在同一殼體內。

根據本發明之一實施例，實現用於根據儲存於一媒體中之一內容之內容類型實現內容使用控制之一裝置及方法。

特定而言，一播放設備根據一內容之類型(例如，諸如一高附加價值內容(諸如公開之後不久之一電影)及除該高附加價值內容外之一正常內容之一內容類型)保持對應於一可用內容類型之一裝置憑證。該播放設備根據將在針對其中儲存有一內容之媒體進行鑑認處理時播放之一內容之類型啟動一播放程式，獲得對應於將與該經啟動程式相關地播放之該內容類型之一裝置憑證，將此裝置憑證提供至該媒體，且執行鑑認處理。該媒體確認記錄於該裝置憑證中之對應內容類型資訊，且僅在由該播放設備請求之一標題密鑰係對應於匹配記錄於該裝置憑證中之對應內容類型之一內容之一標題密鑰之情形下准許讀出該標題密鑰。

根據此等程序，可執行根據內容類型之標題密鑰讀出控制，且因此實現根據內容類型之內容使用控制。

【實施方式】

下文中，將參考圖式有關根據本發明之一資訊處理裝置及一資訊處理方法及一程式之細節做出說明。注意，將根據以下項目做出說明。

- 1.內容提供處理及使用處理之概述
- 2.記憶卡之組態實例及使用實例

3.具有關於受保護區域之存取准許資訊之憑證

4.關於每一裝置憑證已應用於其之記憶卡之存取處理實例

5.主機(播放設備)與媒體(記憶卡)之間的處理實例

5-1.(第一實施例)根據內容類型使用裝置憑證之主機與媒體之間的處理實例

5-2.(第二實施例)選擇由播放程式應用之裝置憑證之處理實例

5-3.(第三實施例)根據播放裝置之類型改變媒體(記憶卡)之識別符(媒體ID)之轉換模式之處理實例

6.每一裝置之硬體組態實例

7.本發明之組態之概述

1.內容提供處理及使用處理之概述

下文中，將參考圖式有關根據本發明之一資訊處理裝置及一資訊處理方法及一程式之細節做出說明。

首先，將參考圖1且在其後闡述內容提供處理及使用處理之概述。

圖1自左邊圖解說明以下實例。

(a)內容提供源

(b)內容記錄/播放設備(主機)

(c)內容記錄媒體

(c)內容記錄媒體係將用於對已由一使用者記錄之一內容之回放處理之一媒體。此處，舉例而言，此指示係諸如快閃記憶體或諸如此類之一資訊記錄設備之一記憶卡31。

該使用者將各種內容(諸如音樂、電影等)記錄於記憶卡

31中且使用此等內容。舉例而言，用作使用控制之一物件之一內容(諸如用作將管理之一版權物件之一內容或諸如此類)包括於彼等內容中。

用作此處所提及之使用控制之一物件之該內容係禁止其未經授權之複製、所複製資料之分配或諸如此類之一內容。注意，在將一使用控制內容記錄於記憶卡31中之情形下，對應於其內容之使用控制資訊(使用規則)(特定而言，其中規定複製限制資訊(諸如可允許之複製次數等)之使用控制資訊(使用規則))亦一起記錄於記憶卡31中。

(a)內容提供源係諸如音樂、電影或諸如此類之一內容之一提供源。舉例來說，圖1圖解說明一廣播站11及一內容伺服器12作為內容提供源。舉例而言，廣播站11係一電視站，且經由一衛星透過地面波或衛星波為使用者裝置[(b)內容記錄/播放設備(主機)]提供各種廣播內容。內容伺服器12係用於經由諸如網際網路或諸如此類之一網路提供諸如音樂、電影等內容之一伺服器。

舉例而言，可做出一配置，其中使用者將作為(c)內容記錄媒體之記憶卡31安裝於(b)內容記錄/播放設備(主機)上，經由(b)內容記錄/播放設備(主機)本身之接收單元或連接至(b)內容記錄/播放設備(主機)之一接收裝置接收自廣播站11或內容伺服器12提供之內容，且將該內容記錄於記憶卡31中。

(b)內容記錄/播放設備(主機)安裝作為(c)內容記錄媒體之記憶卡31，且將自作為(a)內容提供源之廣播站11或內容

伺服器12接收之內容記錄於記憶卡31中。

(b)內容記錄/播放設備(主機)之實例包括僅用於記錄/播放之一裝置(CE裝置：消費型電子裝置)21，包括一硬碟或者諸如DVD、BD或諸如此類之一光碟，舉例而言，諸如一DVD播放器或諸如此類，且進一步包括一PC 22、一可攜式終端機23，諸如一智慧電話、蜂巢式電話、可攜式播放器、平板終端機或諸如此類。此等全部係其上可安裝作為(c)內容記錄媒體之記憶卡31之裝置。

使用者使用僅用於記錄/播放之裝置21、PC 22、可攜式終端機23或諸如此類自廣播站11或內容伺服器12接收諸如音樂、一電影或諸如此類之一內容且記錄於記憶卡31中。

將參考圖2闡述記錄於記憶卡31中之一內容之使用模式。記憶卡31係關於一內容播放器(諸如一PC或諸如此類)附接/拆卸之一記錄媒體，且可自己執行對一內容之記錄之一裝置自由地拆卸且安裝於另一使用者裝置上。

特定而言，如圖2中所圖解說明，以下程序之執行裝置不必相同，且使用者可自由地選擇性地使用一記錄裝置及一播放裝置。

(1)記錄處理

(2)回放處理

注意，在諸多情形下，記錄於記憶卡31中之一使用控制內容記錄為一經加密內容，且一內容播放設備(諸如僅用於記錄/播放之裝置21、PC 22、可攜式終端機23等)在根據一預定序列執行解密處理之後執行內容回放。

2.記憶卡之組態實例及使用實例

接下來，將有關將用作一內容記錄媒體之一記憶卡(諸如快閃記憶體或諸如此類)之一組態實例及一使用實例做出說明。記憶卡31之儲存區域之一特定組態實例圖解說明於圖3中。

如圖3中所圖解說明，記憶卡31之儲存區域由以下兩個區域組態。

(a)受保護區域(Protected Area) 51及

(b)通用區域(General Purpose Area) 52

(b)通用區域(General Purpose Area) 52係可由使用者使用之一記錄/播放設備自由地存取之一區域，其中記錄有內容、一般內容管理資料等，例如，在其處一伺服器或使用者之記錄/播放設備可自由地執行對資料之寫入或讀取之一區域(舉例而言)。

另一方面，(a)受保護區域(Protected Area) 51係不准許對其之自由存取之一區域。舉例而言，在嘗試使用使用者使用之一記錄/播放設備或將經由一網路連接之一伺服器或諸如此類執行對資料之寫入或讀取之情形下，記憶卡31之一資料處理單元根據預先儲存於記憶卡31中之一程式根據每一設備判定是否可執行讀取(Read)或寫入(Write)。

記憶卡31包括用於執行預先儲存之程式之一資料處理區段及用於執行鑑認處理之一鑑認處理區段，且首先針對嘗試執行關於記憶卡31之對資料之寫入或讀取之一裝置執行鑑認處理。

關於此鑑認處理之一階段，記憶卡31自一夥伴終端機(亦即，存取請求設備)接收一裝置憑證，諸如一公共密鑰憑證或諸如此類。舉例而言，在該存取請求設備係一伺服器之情形下，記憶卡31接收該伺服器處理之一伺服器憑證(Server Certificate)，且使用其憑證中所描述之資訊而判定是否准許對受保護區域(Protected Area) 51之每一分段區域之存取。此外，舉例而言，在該存取請求裝置係用作執行對一內容之記錄/播放之一使用者機器之一記錄/播放設備(主機)之情形下，記憶卡31接收由記錄/播放設備(主機)處理之一主機憑證(Host Certificate)，且使用其憑證中所描述之資訊而判定是否准許對受保護區域(Protected Area) 51之每一區段區域之存取。

此存取權限判定處理係在圖3中所圖解說明之受保護區域(Protected Area) 51內按區段區域(圖式中所圖解說明之區#0、#1、#2等)之遞增序執行，且記憶卡31僅准許所准許區段區域中所准許之處理(諸如對資料之讀取/寫入之處理等)，且致使伺服器或主機執行對其之處理。

關於此媒體之讀取/寫入限制資訊(PAD讀取/PAD寫入)係按裝置之遞增序設定以執行存取，例如，內容伺服器或記錄/播放設備(主機)。此資訊記錄於對應於每一裝置之一伺服器憑證(Server Certificate)或主機憑證(Host Certificate)中。注意，下文中，「Certificate(憑證)」將以一簡化方式稱作「Cert」。

以此方式，記憶卡31根據預先儲存於記憶卡31中之一所

規定程式驗證伺服器憑證(Server Cert)或主機憑證(Host Cert)之所記錄資料，且執行處理以僅准許有關一存取准許區域之存取。

3.具有關於受保護區域之存取准許資訊之憑證

接下來，將參考圖4有關一憑證之一組態實例做出說明，在執行關於上文所闡述之記憶卡31之受保護區域(Protected Area) 51之存取之情形下涉及關於記憶卡對該憑證之呈現。

如上文所闡述，記憶卡31針對嘗試執行關於記憶卡31之對資料之寫入或讀取之一裝置執行鑑認處理。關於此鑑認處理之一階段，記憶卡31自夥伴裝置(亦即，存取請求設備)接收一裝置憑證，諸如一公共密鑰憑證或諸如此類(例如，伺服器憑證(Server Cert)或主機憑證(Host Cert))，且使用其憑證中所描述之資訊而判定是否准許對受保護區域(Protected Area) 51之每一區段區域之存取。

將參考圖4有關作為用於此鑑認處理之一裝置憑證之一實例之將儲存於一使用者機器(主機機器)(諸如圖1中所圖解說明之記錄/播放設備21、PC 22、可攜式終端機23或諸如此類)中之一主機憑證(Host Cert)之一組態實例做出說明。

舉例而言，該主機憑證(Host Cert)由作為一公共密鑰憑證發行者之憑證授權單位提供至每一使用者機器(主機機器)。舉例而言，主機憑證(Host Cert)係將發行至對其之內容使用處理已被憑證授權單位容許之一使用者機器(主機

機器)之一使用者機器之一憑證，且係其中儲存有一公共密鑰等之一憑證。主機憑證(Host Cert)組態為其中已藉由一憑證授權單位秘密密鑰設定一簽章以阻止篡改之資料。注意，裝置憑證可在一裝置之製造時基於裝置確認(諸如裝置之類型等)而預先儲存於裝置內之記憶體中。在於使用者之購買之後獲得一裝置憑證之情形下，可做出一配置，其中執行根據裝置、憑證授權單位或另一管理授權單位之間的一預定序列之對一裝置類型、一可用內容之類型等之確認處理以發行一裝置憑證至每一裝置，且儲存於裝置內之記憶體中。

注意，執行對記憶卡31之受保護區域之存取之一伺服器保持一伺服器憑證(Server Cert)，其中記錄有具有與主機憑證相同之組態之一伺服器公共密鑰及記憶卡之存取准許資訊。

圖4指示主機憑證(Host Cert)之一特定實例，憑證授權單位為每一主機機器(使用者機器)提供該主機憑證。

該主機憑證(Host Cert)如圖4中所指示包括以下資料。

- (1)類型資訊
- (2)主機ID(使用者機器ID)
- (3)主機公共密鑰(Host Public Key)
- (4)受保護區域存取權限資訊(關於媒體之受保護區域之讀取/寫入限制資訊(PAD讀取/PAD寫入))
- (5)其他資訊
- (6)簽章

下文中，將闡述以上(1)至(6)之每一資料。

(1)類型資訊

類型資訊係指示憑證之類型或使用者機器之類型之資訊，其中記錄有指示目前憑證係一主機憑證之資料及指示機器之類型(例如，諸如一PC或音樂播放器等機器之類型)之資訊。

(2)主機ID

主機ID係其處記錄有用作裝置識別資訊之一裝置ID之一區域。

(3)主機公共密鑰(Host Public Key)

主機公共密鑰係一主機機器之一公共密鑰。此根據公共密鑰密碼系統連同將提供至主機機器(使用者機器)之一秘密密鑰一起組成一密鑰對。

(4)受保護區域存取權限資訊(關於媒體之受保護區域之讀取/寫入限制資訊(PAD讀取/PAD寫入))

關於受保護區域存取權限資訊，舉例而言，記錄有關其中記錄有一內容之一媒體(例如，將在圖3中所圖解說明之記憶卡31之儲存區域中設定受保護區域(PDA：Protected Area) 51內的進行對其之資料之讀取(Read)及寫入(Write)之一區段區域)之資訊。

(5)其他資訊，(6)簽章

關於主機憑證，記錄除以上(1)至(4)外之各種類型之資訊，且記錄關於(1)至(5)中之資訊之簽章資料。藉由憑證授權單位之一秘密密鑰執行簽章。在提取及使用記錄於主

機憑證中之資訊(例如，一主機公共密鑰)之情形下，首先執行憑證授權單位之公共密鑰已應用於其之簽章驗證處理以確認不存在對主機憑證之篡改，且以執行對其之確認作為一條件而使用諸如一主機公共密鑰之憑證所儲存資料。

注意，儘管圖4係其處記錄有關於記憶卡之受保護區域之一使用者機器(主機機器)之存取准許資訊之一主機憑證，但以與圖4中所指示之主機憑證相同之方式將其處記錄有關於記憶卡之受保護區域之存取准許資訊之一憑證[伺服器憑證(例如，其中儲存有一伺服器公共密鑰之公共密鑰憑證)]提供至必須做出對受保護區域之存取之一伺服器。

4.關於每一裝置憑證已應用於其之記憶卡之存取處理實例

如參考圖4所闡述，在執行對記憶卡31之受保護區域(Protected Area) 51之存取之情形下，必須將如圖4中所指示之一憑證呈現至記憶卡。記憶卡確認圖4中所指示之憑證，且判定是否執行對圖3中所圖解說明之記憶卡31之受保護區域(Protected Area) 51之存取。

舉例而言，主機機器保持參考圖4所闡述之一主機憑證(Host Cert)，且執行提供內容之一伺服器保持對應於該伺服器之一憑證(伺服器憑證：Server Certificate)。

在此等裝置中之每一者執行對記憶卡之受保護區域(Protected Area)之存取之情形下，每一裝置必須為記憶卡提供其一經處理憑證以接收有關是否可執行存取之基於記憶卡側之驗證之判定。

將參考圖5在關於記憶卡之存取請求設備係諸如一記錄/播放設備或諸如此類之一主機機器之情形下有關一存取限制設定實例做出說明。

圖5自左邊圖解說明作為關於記憶卡之一存取請求裝置之一主機(記錄/播放設備) 70及記憶卡31。主機(記錄/播放設備) 70係諸如僅用於記錄/播放之裝置21、PC 22、可攜式終端機23(展示於圖1中)或諸如此類之一使用者機器，且係執行關於記憶卡31之內容記錄處理或對記錄於記憶卡31中之一內容之播放之一裝置。

在將自一播放站或伺服器接收之一內容或儲存於裝置本身之一儲存單元中之一內容輸出至記憶卡31用於記錄時，主機(記錄/播放設備) 70執行用於將將應用於對一內容之加密或解密處理之一標題密鑰或者一標題密鑰之經加密或經轉換資料寫入於記憶卡31之受保護區域(Protected Area) 51中之處理。

此外，在播放記錄於記憶卡31中之一經加密內容之情形下，主機(記錄/播放設備) 70執行用於獲得寫入於記憶卡31之受保護區域(Protected Area) 51中之一標題密鑰或者一標題密鑰之一經加密或經轉換資料之處理。主機(記錄/播放設備) 70必須以此方式在內容記錄/回放處理中執行對記憶卡31之受保護區域(Protected Area) 51之存取。

記憶卡31包括受保護區域(Protected Area) 51及通用區域(General Purpose Area) 52，且經加密內容等記錄於通用區域(General Purpose Area) 52中。作為用於內容回放之一密

鑰之一標題密鑰記錄於受保護區域(Protected Area) 51中。

如先前參考圖3所闡述，受保護區域(Protected Area) 51劃分成多個區域。關於圖5中所圖解說明之一實例，圖解說明具有以下兩個區段區域之一實例。

區段區域#0(受保護區域#0) 61及

區段區域#1(受保護區域#1) 62，

可執行各種設定以用於設定此等區段區域之模式。圖5指示主機(記錄/播放設備) 70保持之一主機憑證(Host Cert)之受保護區域存取權限資訊。

關於圖5中所指示之主機憑證之存取控制資訊，執行以下設定。關於區段區域#0(受保護區域#0)准許對資料之寫入(Write)及讀取(Read)程序兩者。

關於區段區域#1(受保護區域#1)僅准許讀取(Read)程序。

關於圖5中所指示之主機憑證(Host Cert)，未設定關於區段區域#1(受保護區域#1)之寫入(Write)准許。舉例而言，將其處記錄有此受保護區域存取權限資訊之一憑證提供至一使用者機器。

嘗試存取記憶卡31之受保護區域(Protected Area) 51之一裝置將其處記錄有此受保護區域存取權限資訊之一憑證輸出至記憶卡。記憶卡基於記憶卡內之資料處理區段中之憑證驗證處理而判定是否可執行存取。主機(記錄/播放設備) 70根據判定資訊存取記憶卡31之受保護區域(Protected Area) 51。

以此方式，記憶卡之受保護區域(Protected Area)組態為在其處已按存取請求設備之遞增序且亦按區段區域(#0、#1、#2等)之遞增序設定準許或不准許對資料之寫入(Write)及讀取(Read)之一存取控制區域。

如參考圖4所闡述，受保護區域存取權限資訊記錄於每一存取請求設備之憑證(伺服器憑證、主機憑證等)中，且記憶卡首先執行有關自存取請求設備接收之憑證之簽章驗證，且在確認有效性之後讀取憑證中所描述之存取控制資訊，亦即，以下資訊。

讀取准許區域資訊(PAD讀取)，及

寫入准許區域資訊(PAD寫入)

基於此資訊，記憶卡僅准許並執行關於存取請求設備所容許之處理。

注意，亦對於主機機器，存在各種類型之機器，舉例而言，諸如CE裝置(諸如記錄器、播放器等)、PC等。裝置憑證係由此等裝置個別地保持之憑證，且可具有根據此等裝置之類型之一不同設定。

此外，基於記錄於一裝置憑證中之以下資訊，亦即，

讀取准許區域資訊(PAD讀取)及寫入准許區域資訊(PAD寫入)，且此外不僅此等資訊而且包括於參考圖4所闡述之憑證中之類型資訊(Type)，記憶卡之資料處理區段可接受保護區域之區段區域之遞增序執行存取准許判定。

5. 主機(播放設備)與媒體(記憶卡)之間的處理實例

接下來，將有關執行對儲存於一媒體(記憶卡)中之一內

容之回放處理之一主機(播放設備)與該媒體(記憶卡)之間的一處理實例做出說明。

5-1.(第一實施例)根據內容類型使用裝置憑證之主機與媒體之間的處理實例

首先，對於主機(播放設備)與媒體(記憶卡)之間的一處理實例之一第一實施例，將闡述根據內容類型採用一裝置憑證之一處理實例。

存在自一廣播站或內容伺服器提供至一使用者機器之各種類型之內容。

舉例而言，存在諸如電影內容、音樂內容、移動影像內容及靜止影像內容之各種內容。

此外，舉例而言，又在電影內容當中，存在公開之後不久之電影內容及有關其在公開之後已過去一特定時間量之電影內容。

在一新內容(諸如在公開放映之後不久之一新電影)之未經授權複製之情形下，出現一問題，其中其內容價值迅速降低，且其一版權持有者及分配權利持有者之收益顯著下降。另一方面，關於舊內容(諸如在公開之後已過去若干年且有關其之DVD或諸如此類之銷售高峰已過去、版權持有者及分配權利持有者之收益水平已經降低之一舊電影)，因此即使產生未經授權之複製，其影響亦將相當小。

以此方式，價值根據內容之類型而不同，且存在應具有更嚴格保護以防止非法使用之高附加價值內容及除此等高

附加價值內容外之內容。關於以下說明，將經受更嚴格保護以防止非法使用之內容將稱作高附加價值內容(增強之內容)，且除高附加價值內容外之內容將稱為正常內容(基本內容)。

回應於其中存在此等各種類型之內容之本情形，至於用於增強對高附加價值內容(增強之內容)之保護之一對策之一實例，將闡述根據內容類型採用一裝置憑證之一處理實例。舉例而言，裝置憑證應係先前參考圖4所闡述之一主機憑證(Host Cert)。如參考圖4及圖5所闡述，關於裝置憑證，按記憶卡之受保護區域(Protected Area)之區段區域(#0、#1、#2等)之遞增序記錄存取權限，且特定而言，各種類型之存取權限資訊，諸如僅准許讀取(Read)、僅准許寫入(Write)、准許讀取/寫入(Read/Write)等。

根據內容類型發行複數個此裝置憑證，且一個內容憑證應被視為可僅用於一特定類型之內容之一內容憑證。

圖6圖解說明記錄於一記憶卡100中之一經加密內容及將應用於對該經加密內容之解密之一標題密鑰之一儲存實例。

如上文所闡述，記憶卡100劃分成以下兩個區域。

受保護區域(Protected Area) 101，及

通用區域(General Purpose Area) 102

經加密內容記錄於通用區域(General Purpose Area) 102中。如圖式中所圖解說明，內容劃分成以下兩種類型。

(a)正常內容(基本內容)

(b)高附加價值內容(增強之內容)

內容記錄為可藉以區分內容類型之設定，例如可區分係(a)正常內容(基本內容)或是(b)高附加價值內容(增強之內容)。舉例而言，內容係連同其中記錄有此等內容之內容類型之後設資料一起記錄。此等內容係經加密內容，且在內容回放時，必須執行使用對應於每一內容(標題)之一標題密鑰之解密處理。

標題密鑰記錄於受保護區域(Protected Area) 101中。注意，一標題密鑰可記錄為經加密或經轉換資料。此係對抗洩漏之對策中之一者。

如圖6中所圖解說明，記錄於受保護區域(Protected Area) 101中之標題密鑰亦以與經加密內容之類型相同之方式簡單地分類為以下兩種類型。

(a)正常內容之標題密鑰(基本內容之標題密鑰)

(b)高附加價值內容之標題密鑰(增強之內容之標題密鑰)

標題密鑰記錄為可藉以區分由標題密鑰解密之內容類型之設定，例如可區分係(a)正常內容(基本內容)或是(b)高附加價值內容(增強之內容)。舉例而言，標題密鑰係連同其中記錄有此等內容之內容類型之後設資料一同記錄。注意，此兩種類型之標題密鑰可經設定以儲存於針對每一類型之一不同區段區域中，且可經設定以便基於一所記錄區段而區分對應內容類型。在此情形下，可根據具有不同區段遞增序之存取權限執行存取控制。

在執行內容回放之情形下，執行內容回放處理之播放設

備(主機)(例如，諸如僅用於記錄/播放之一裝置、PC、可攜式終端機或諸如此類之一播放設備)必須自記憶卡之受保護區域讀出對應於將播放之內容之一標題密鑰。為執行此標題密鑰讀出處理，播放設備(主機)將裝置憑證(Cert)呈現至記憶卡。

此處，如上文所闡述，裝置憑證根據內容類型設定為一裝置憑證。根據內容類型之主機憑證(Host Cert)之一組態實例圖解說明於圖7中。

圖7圖解說明以下兩種類型之主機憑證(Host Cert)之一實例。

(A)可用於播放高附加價值內容及正常內容兩者之主機憑證(Host Cert)

(B)可僅僅用於播放正常內容之主機憑證(Host Cert)

圖7中所圖解說明之主機憑證(Host Cert)係其處記錄有以下資料之憑證(以與先前參考圖4所闡述相同之方式)。

(1)類型資訊

(2)主機ID(使用者裝置ID)

(3)主機公共密鑰(Host Public Key)

(4)受保護區域存取權限資訊(關於媒體之受保護區域之讀取/寫入限制資訊(PAD讀取/PAD寫入))

(5)其他資訊

(6)簽章(Signature)

然而，圖7中所圖解說明之主機憑證之不同之處在於以下資訊記錄於(1)類型資訊中。

(1a)裝置類型資訊

(1b)對應內容類型資訊

「(1a)裝置類型資訊」係指示保持此主機憑證(Host Cert)之主機係何種裝置之資訊。特定而言，舉例而言，此資訊係指示主機係以下裝置類型中之哪一裝置類型之資訊。

*僅用於記錄/播放之裝置，

* PC，或

*可攜式終端機(平板型終端機或諸如此類)

「(1b)對應內容類型資訊」係指示准許使用此主機憑證(Host Cert)自記憶卡獲得之一標題密鑰之內容類型之資訊。特定而言，此資訊係指示此主機憑證是否可用於獲得對應於以下內容中之任一者或兩種內容之一標題密鑰之資訊。

*高附加價值內容(增強之內容)，及

*正常內容(基本內容)

如上文所闡述，關於一裝置憑證，指示裝置本身之裝置類型之裝置類型及指示對應於可藉由應用裝置憑證而獲得之一標題密鑰之一內容之類型之對應內容類型資訊記錄於該裝置憑證中。

將參考圖8闡述以下資訊之組合之一實例。

(1a)裝置類型資訊

(1b)對應內容類型資訊

如圖8中所圖解說明，(1a)裝置類型資訊分類為以下兩種

類型。

僅用於記錄/播放之裝置(碼：0x0001)

PC/可攜式終端機(平板型終端機或諸如此類)(碼：0x0002)

注意，此類型分類係一實例，且可更精細地分類。

此外，(1b)對應內容類型資訊分類為以下三種類型。

僅對應於正常內容(碼：0x0001)

僅對應於高附加價值內容(碼：0x0002)

對應於高附加價值內容及正常內容兩者(碼：0x0003)

注意，此類型分類係一實例，且可更精細地分類。舉例而言，可設定根據各種內容(諸如移動影像內容、電影內容、靜止影像內容、移動影像內容等)之類型之分類。

接下來，將參考圖9至圖11中所圖解說明之流程圖闡述使用對應於一內容類型之裝置憑證之內容回放之序列。

圖9至圖11中所圖解說明之流程圖按順序圖解說明在左側之用於執行內容回放之一主機(播放設備)及在右側之其中儲存有一經加密內容及一標題密鑰之一媒體(記憶卡)，且按順序圖解說明由此兩個裝置執行之程序。將闡述步驟之處理之細節。

其上安裝有媒體(記憶卡)之主機(播放設備)在S111步驟中輸入將播放之一內容之選擇資訊。舉例而言，主機(播放設備)在主機之一顯示器上顯示儲存於記憶卡中之一內容清單，且使用者自所顯示內容清單選擇將播放之一內容，且因此主機之資料處理區段識別使用者之所指定選定內容。

在步驟S112中，主機根據選定內容之類型啟動一播放程式。

關於本處理實例，內容之類型係以下(a)及(b)中之一者。

(a)正常內容，及

(b)高附加價值內容

注意，關於每一內容，指示一內容類型之資訊與該內容相關地記錄於屬性資訊(後設資料)中，且基於此屬性資訊而鑑別內容類型。另一選擇係，可做出一配置，其中一內容檔案記錄為具有根據內容類型之一不同副檔名之一設定，且參考此副檔名而鑑別內容。另一選擇係，可根據副檔名自動選擇將啟動之一程式。

主機保持用於執行對一正常內容之回放處理之一正常內容播放程式及用於執行對一高附加價值內容之回放處理之一高附加價值內容播放程式，且啟動對應於被選定為將播放之一物件之內容之類型之播放程式。注意，儘管主機可僅僅具有正常內容播放程式，但此一主機不能執行對一高附加價值內容之回放處理。此外，該高附加價值內容播放程式可經設定以便僅播放高附加價值內容，或可經設定以成為能夠播放高附加價值內容及正常內容兩者之一程式。

接下來，在步驟S113中，主機自裝置本身之記憶體獲得與根據內容之類型啟動之播放程式相關之一裝置憑證(Host Cert)。此裝置憑證(Host Cert)係先前參考圖7所闡述之一主機憑證(Host Cert)，且係其中以下資訊記錄為類型

資訊之一憑證。

(1a)裝置類型資訊

(1b)對應內容類型資訊

注意，舉例而言，正常內容播放程式可獲得僅僅對應於一正常內容之一主機憑證(指示於圖7中之(B)中)，且高附加價值內容播放程式可獲得僅僅對應於一高附加價值內容及一正常內容之一主機憑證(指示於圖7中之(A)中)。舉例而言，關於用於獲得記錄於每一播放程式中之一主機憑證之資訊(例如，記憶體位址)，僅記錄對應於圖7中之(A)及(B)中之任一者之主機憑證之資訊(位址)，每一播放程式可僅獲得可由程式本身使用之一主機憑證。

接下來，在步驟S114a及S114b中，執行主機(播放設備)與媒體(記憶卡)之間的相互鑑認處理。關於此相互鑑認處理，主機(播放設備)將自主機之記憶體獲得之主機憑證(Host Cert)傳輸至媒體(記憶卡)。

另一方面，媒體(記憶卡)將儲存於媒體(記憶卡)內之記憶體中之媒體之一裝置憑證(Media Cert)傳輸至主機(播放設備)。舉例而言，此鑑認處理作為對此兩個公共密鑰憑證已應用於其之公共密鑰密碼系統之相互鑑認處理而執行。

接下來，將闡述在步驟S115a及S115b中且此後圖解說明於圖10中之處理。在步驟S115a及S115b中，做出有關是否已建立主機(播放設備)與媒體(記憶卡)之間的相互鑑認之判定。

在尚未建立相互鑑認之情形下，做出未能確認兩個裝置之間的可靠性之判定，流程進行至步驟S130，且停止內容回放處理。

在已建立相互鑑認之情形下，流程進行至步驟S116a及S116b。

在步驟S116a中，主機(播放設備)將對應於將播放之內容之一標題密鑰讀取請求傳輸至媒體(記憶卡)。

在步驟S116b中，媒體(記憶卡)接收此標題密鑰讀取請求。

接下來，在步驟S117中，媒體(記憶卡)參考在先前鑑認資訊時自主機(播放設備)接收之主機憑證(Host Cert)之類型資訊而判定自主機(播放設備)接收之主機憑證(Host Cert)是否係其中記錄有對應於對應於主機請求之一標題密鑰之內容之類型之對應內容類型資訊之一主機憑證(Host Cert)。

舉例而言，假定一配置，其中圖7中所圖解說明之兩種類型之主機憑證(Host Cert)可用。在經排程以播放之內容係一正常內容且主機請求之標題密鑰係對應於該正常內容之一標題密鑰之情形下，甚至當自主機接收之主機憑證係圖7中所圖解說明之以下兩個憑證中之任一者時，

(A)可用於播放一高附加價值內容及一正常內容兩者之主機憑證(Host Cert)，及

(B)可僅僅用於播放一正常內容之主機憑證(Host Cert)，
步驟S117中之判定係Yes。

此外，在經排程以播放之內容係一高附加價值內容之情形下，且主機請求之標題密鑰係對應於該高附加價值內容之一標題密鑰時，僅當自主機接收之主機憑證係圖7中所圖解說明之以下憑證時，

(A)可用於播放一高附加價值內容及一正常內容兩者之主機憑證(Host Cert)，

步驟S117中之判定係Yes。

當自主機接收之主機憑證係圖7中所圖解說明之以下憑證時，

(B)可僅僅用於播放一正常內容之主機憑證(Host Cert)，

步驟S117中之判定係No。

在步驟S117中之判定係No之情形下，流程進行至步驟S130，停止對內容之播放。亦即，不執行關於主機之標題密鑰之提供。

在做出自主機(播放設備)接收之主機憑證(Host Cert)係其中記錄有對應於對應於主機請求之一標題密鑰之內容之類型之對應內容類型資訊之一主機憑證(Host Cert)之判定之情形下，步驟S117中之判定係Yes，且流程進行至步驟S118。

接下來，在步驟S118中，媒體(記憶卡)參考在先前鑑認處理時自主機(播放設備)接收之主機憑證(Host Cert)之受保護區域存取權限資訊而確認主機請求之標題密鑰之所儲存區域(亦即，受保護區域之一區段區域)是否已被設定為一資料讀取准許區域。

如先前參考圖4及圖5所闡述，按記憶卡之受保護區域之區段區域之遞增序之存取權限(讀取/寫入)之准許資訊記錄於主機憑證(Host Cert)之受保護區域存取權限資訊區中。媒體(記憶卡)參考此受保護區域存取權限資訊而判定主機請求之標題密鑰之所儲存區域(亦即，受保護區域之區段區域)是否已被設定為資料讀取准許區域。

在於圖11中所圖解說明之步驟S119中其處儲存有主機請求之標題密鑰之受保護區域之區段區域尚未作為資料讀取准許區域記錄於主機憑證(Host Cert)中之情形下，步驟S119中之判定係No。

在此情形下，流程進行至步驟S130，且停止內容回放。亦即，不執行關於主機之標題密鑰之提供。

另一方面，在其處儲存有主機請求之標題密鑰之受保護區域之區段區域已作為資料讀取准許區域記錄於主機憑證(Host Cert)中之情形下，步驟S119中之判定係Yes，且流程進行至步驟S120。

在步驟S120a中，媒體(記憶卡)自受保護區域獲得主機(播放設備)請求之標題密鑰，且進一步自通用區域獲得一經加密內容，且傳輸至主機。

在步驟S120b中，主機(播放設備)自媒體(記憶卡)接收標題密鑰及經加密內容。

接下來，在步驟S121中，主機(播放設備)藉由應用所獲得標題密鑰而執行對經加密內容之解密處理以開始內容回放。

5-2.(第二實施例)選擇由播放程式應用之裝置憑證之處理實例

關於根據參考圖9至圖11中所圖解說明之流程圖而闡述之第一實施例之內容回放序列，已做出一配置，其中根據被選定為將播放之內容之一內容之類型選擇將啟動之播放程式，且使用對應於選定經啟動播放程式而設定之一主機憑證(Host Cert)(亦即，被設定為可由選定經啟動播放程式存取之一個主機憑證(Host Cert))執行處理。

特定而言，已假定一配置，其中根據一內容之類型將播放程式設定為一專用程式，諸如對應於正常內容之播放程式或對應於高附加價值內容之播放程式，且一次一個地為每一播放程式指派一可用主機憑證(Host Cert)。

接下來，將參考圖12至圖14中所圖解說明之流程圖闡述不同於以上第一實施例之執行處理之一第二實施例。關於本第二實施例，在將在主機(播放設備)處執行之播放程式係一個播放程式之情形下(亦即，在將播放之內容係一正常內容或一高附加價值內容之情形下)，執行由同一程式進行之回放處理。關於本實施例，播放程式本身鑑別被選定為將播放之內容之一內容之類型，且根據此鑑別，選擇並使用將使用之一主機憑證(Host Cert)。

特定而言，作為播放程式之處理，鑑別內容類型，且根據所鑑別之內容類型，選擇並使用以下兩種類型之主機憑證(Host Cert)中之一者。

(A)可用於播放一高附加價值內容及一正常內容兩者之主

機憑證(Host Cert)

(B)可僅僅用於播放一正常內容之主機憑證(Host Cert)

將闡述圖12至圖14中所圖解說明之流程圖之步驟中之處理。

圖12至圖14中所圖解說明之流程圖以與圖9至圖11中之流程圖相同之方式按順序圖解說明在左側之用於執行內容回放之一主機(播放設備)及在右側之其中儲存有一經加密內容及一標題密鑰之一媒體(記憶卡)，且按順序圖解說明由此兩個裝置執行之程序。

其上安裝有媒體(記憶卡)之主機(播放設備)在步驟S211中輸入將播放之一內容之選擇資訊。舉例而言，主機在主機之顯示器上顯示儲存於記憶卡中之一內容清單，且使用者自所顯示內容清單選擇將播放之內容，且因此主機之資料處理區段識別使用者之所指定選定內容。舉例而言，以對將播放之內容之選擇作為一觸發器而啟動儲存於主機之記憶體中之內容播程式。

注意，關於先前圖9至圖11中所圖解說明之流程之處理，儘管經啟動程式根據一內容之類型(高附加價值/正常)而不同，但關於本處理實例，不根據選定內容之類型(高附加價值/正常)改變經啟動程式。

在步驟S212中，播程式鑑別由使用者選擇之內容之類型。亦關於本處理實例，內容之類型係以下(a)及(b)中之一者。

(a)正常內容

(b)高附加價值內容

注意，關於每一內容，指示一內容類型之資訊與該內容相關地記錄於屬性資訊(後設資料)中，且基於此屬性資訊而鑑別內容類型。另一選擇係，可做出配置，其中一內容檔案記錄為具有根據內容類型之一不同副檔名之一設定，且參考此副檔名而鑑別內容。

接下來，在步驟S213中，主機根據所判定之內容類型自裝置本身之記憶體選擇且獲得將使用之一裝置憑證(Host Cert)。

此裝置憑證(Host Cert)係先前參考圖7所闡述之主機憑證(Host Cert)，且係其中以下資訊記錄為類型資訊之一憑證。

(1a)裝置類型資訊

(1b)對應內容類型資訊

關於本實例，播放程式本身執行對對應於經排程以播放之內容之類型之一主機憑證(Host Cert)之選擇。在被選定為將播放之內容之內容係一高附加價值內容之情形下，舉例而言，選擇且獲得其中一高附加價值內容在參考圖7所闡述之主機憑證(Host Cert)之(1b)對應內容類型資訊中被設定為一可用內容之一主機憑證(Host Cert)。特定而言，選擇且獲得圖7中之(A)中所圖解說明之主機憑證(舉例而言)。

另一方面，在被選定為將播放之內容之內容係一正常內容之情形下，選擇且獲得其中一正常內容在參考圖7所闡

述之主機憑證(Host Cert)之(1b)對應內容類型資訊中被設定為一可用內容之一主機憑證(Host Cert)。特定而言，選擇且獲得圖7中之(B)中所圖解說明之主機憑證(舉例而言)。注意，在此情形下，圖7中之(A)中所圖解說明之憑證亦可用於播放一正常內容，且因此可選擇圖7之(A)中所圖解說明之憑證。

然而，舉例而言，在主機(播放設備)僅保持圖7中之(B)中所圖解說明之對應於一正常內容之一主機憑證(Host Cert)之情形下，若一高附加價值內容已被選定為將播放之內容，則不能獲得一可用主機憑證(Host Cert)，且因此將不執行內容回放。

以此方式，在步驟S213中，主機(播放設備)根據內容類型選擇性地獲得以下兩種類型之主機憑證(Host Cert)中之任一者。

(A)可用於播放一高附加價值內容及一正常內容兩者之主機憑證(Host Cert)

(B)可僅僅用於播放一正常內容之主機憑證(Host Cert)

接下來，在步驟S214a及S214b中，主機(播放設備)執行主機(播放設備)與媒體(記憶卡)之間的相互鑑認處理。關於此相互鑑認處理，主機(播放設備)將根據內容類型選擇之主機憑證(Host Cert)自主機之記憶體傳輸至媒體(記憶卡)。

另一方面，媒體(記憶卡)將儲存於媒體(記憶卡)內之記憶體中之媒體之主機憑證(Media Cert)傳輸至主機(播放設

備)。舉例而言，鑑認處理作為對此兩個公共密鑰憑證已應用於其之公共密鑰密碼系統之相互鑑認處理而執行。

接下來，將闡述在步驟S215a及S215b中且此後圖解說明於圖13中之處理。

圖解說明於圖13至圖14中之步驟S215a至S221中之處理與先前參考圖9至圖11所闡述之流程之步驟S115a至S121中之處理基本相同。

在步驟S215a及S215b中，做出有關是否已建立主機(播放設備)與媒體(記憶卡)之間的相互鑑認之判定。在尚未建立相互鑑認之情形下，做出未能確認兩個裝置之可靠性之判定，且流程進行至步驟S230，且停止內容回放處理。

在已建立相互鑑認之情形下，流程進行至步驟S216a及S216b。

在步驟S216a中，主機(播放設備)將對應於將播放之內容之一標題密鑰讀取請求傳輸至媒體(記憶卡)。

在步驟S216b中，媒體(記憶卡)接收此標題密鑰讀取請求。

接下來，在步驟S217中，媒體(記憶卡)參考在先前鑑認處理時自主機(播放設備)接收之主機憑證(Host Cert)之類型資訊以判定自主機(播放設備)接收之主機憑證(Host Cert)是否係其中記錄有對應於對應於主機請求之標題密鑰之內容之類型之對應內容類型資訊之一主機憑證(Host Cert)。

舉例而言，假定一配置，其中圖7中所圖解說明之兩種

類型之主機憑證(Host Cert)可用。

在經排程以播放之內容係一正常內容且主機請求之標題密鑰係對應於一正常內容之一標題密鑰、自主機接收之主機憑證係以下兩種類型之主機憑證(Host Cert)中之任一者之情形下，步驟S217中之判定係Yes。

(A)可用於播放一高附加價值內容及一正常內容兩者之主機憑證(Host Cert)

(B)可僅僅用於播放一正常內容之主機憑證(Host Cert)

此外，在經排程以播放之內容係一高附加價值內容且主機請求之標題密鑰係對應於該高附加價值內容之一標題密鑰之情形下，僅當自主機接收之主機憑證係圖7中所圖解說明之以下類型之主機憑證(Host Cert)時，步驟S217中之判定係Yes。

(A)可用於播放一高附加價值內容及一正常內容兩者之主機憑證(Host Cert)

當自主機接收之主機憑證係圖7中所圖解說明之以下類型之主機憑證(Host Cert)時，步驟S217中之判定係No。

(B)可僅僅用於播放一正常內容之主機憑證(Host Cert)

在步驟S217中之判定係No之情形下，流程進行至步驟S230，且停止對內容之播放。亦即，不執行關於主機之一標題密鑰之提供。

當做出自主機(播放設備)接收之主機憑證(Host Cert)係其中記錄有對應於對應於主機請求之標題密鑰之內容之類型之對應內容類型資訊之一主機憑證(Host Cert)之判定

時，步驟S217中之判定係Yes，且流程進行至步驟S218。

接下來，在步驟S218中，媒體(記憶卡)參考在先前鑑認處理時自主機(播放設備)接收之主機憑證(Host Cert)之受保護區域存取權限資訊以判定主機請求之標題密鑰之所儲存區域(亦即，受保護區域之區段區域)是否被設定為資料讀取准許區域。

如先前參考圖4及圖5所闡述，按記憶卡之受保護區域之區段區域之遞增序之存取權限(讀取/寫入)之准許資訊記錄於主機憑證(Host Cert)之受保護區域存取權限資訊區域中。媒體(記憶卡)參考此受保護區域存取權限資訊以判定主機請求之標題密鑰之所儲存區域(亦即，受保護區域之區段區域)是否被設定為資料讀取准許區域。

在於圖14中所圖解說明之步驟S219中其中儲存有主機請求之標題密鑰之受保護區域之區段區域未作為資料讀取准許區域記錄於主機憑證(Host Cert)中之情形下，步驟S219中之判定係No。

在此情形下，流程進行至步驟S230，且停止內容回放。亦即，不執行關於主機之標題密鑰之提供。

另一方面，在其中儲存有主機請求之標題密鑰之受保護區域之區段區域作為資料讀取准許區域記錄於主機憑證(Host Cert)中之情形下，步驟S219中之判定係Yes，且流程進行至步驟S220a及S220b。

在步驟S220a中，媒體(記憶卡)自受保護區域獲得主機(播放設備)請求之標題密鑰，且進一步自通用區域獲得一

經加密內容，且傳輸至主機。

在步驟S220b中，主機(播放設備)自媒體(記憶卡)接收標題密鑰及經加密內容。

接下來，在步驟S221中，主機(播放設備)藉由應用所獲得標題密鑰而執行對經加密內容之解密處理以開始內容回放。

5-3.(第三實施例)根據播放裝置之類型改變媒體(記憶卡)之識別符(媒體ID)之轉換模式之處理實例

接下來，將闡述根據一播放裝置之類型改變媒體(記憶卡)之識別符(媒體ID)之轉換模式之一處理實例作為主機(播放設備)與媒體(記憶卡)之間的一處理實例之一第三實施例。

其中儲存有一經加密內容及將應用於對該經加密內容之解密之一標題密鑰之媒體(記憶卡)保持作為媒體本身之識別資訊之一媒體ID (MID)。如圖15中所圖解說明，一媒體(記憶卡) 300包括在其處基於記錄於每一裝置憑證中之存取權限資訊而准許存取之一受保護區域(Protected Area) 311及一通用區域(General Purpose Area) 312，且將標題密鑰儲存於受保護區域(Protected Area) 311中，且將經加密內容儲存於通用區域(General Purpose Area) 312中。

除經加密內容外，內容使用控制資訊(使用規則)且進一步(如圖式中所圖解說明)一媒體ID (MID) 315及用作其一驗證值之一媒體ID-MAC(訊息鑑認碼) 316亦記錄於通用區域(General Purpose Area) 312中。

媒體ID (MID) 315係媒體(記憶卡)之識別符，且被設定為不同於媒體中之每一者之一值(媒體特徵值)。舉例而言，媒體ID-MAC 316係媒體ID (MID) 315之一篡改驗證值，且組態為管理者之簽章被設定至之資料。

在播放記錄於媒體(記憶卡) 300中之一內容之情形下，媒體ID (MID) 315及媒體ID-MAC 316由播放設備(主機)讀出，且執行採用MAC之驗證處理。根據此驗證處理，處理可進行至採用一標題密鑰對一經加密內容之解密，其中以確認媒體ID (MID) 315之有效性作為一條件。

根據此一預定回放處理序列，預先儲存於播放設備(主機)中之內容播程式執行對媒體ID (MAC)之驗證，且藉由應用一標題密鑰執行對一經加密內容之解密。

將參考圖16有關對一媒體ID (MAC)之驗證及一標題密鑰應用於其之經加密內容解密處理之一序列之一實例做出說明。圖16圖解說明其中儲存有經加密內容等之一媒體(記憶卡) 320及用於執行對儲存於媒體(記憶卡) 320中之一經加密內容之解密及播放之一主機(播放設備) 350。

如圖式中所圖解說明，以下資料儲存於媒體(記憶卡) 320中。

媒體ID-MAC 321，

媒體ID (MID) 322，

轉換標題密鑰(經「互斥或」運算之標題密鑰) 323，

使用控制資訊(使用規則) 324，及

經加密內容(Encrypted Content) 325

注意，儘管各種類型之資料另外儲存於媒體(記憶卡) 320中，但僅圖解說明將應用於對一媒體ID (MAC)之驗證及一標題密鑰應用於其之經加密內容解密處理之序列之資料。

使用控制資訊(使用規則) 324係對應於經加密內容(Encrypted Content) 325之使用控制資訊，且特定而言其中記錄有使用准許資訊(舉例而言，諸如用於複製一內容之准許資訊)之資料。主機(播放設備)在使用經加密內容(Encrypted Content) 325時根據使用控制資訊(使用規則) 324之規定使用內容。

轉換標題密鑰(經「互斥或」運算之標題密鑰) 323係一標題密鑰之經轉換資料，且儲存於記憶卡之受保護區域(Protected Area)中。特定而言，標題密鑰資料與使用控制資訊(使用規則) 324之雜湊值之間的一「互斥或」(XOR)運算結果儲存為轉換標題密鑰。

將闡述主機(播放設備) 350之處理序列。將有關主機(播放設備) 350在圖16中所圖解說明之步驟S301至S305之序列中執行之處理做出說明。

首先，在步驟S301中，主機(播放設備) 350自媒體(記憶卡) 320讀出使用控制資訊(使用規則) 324，且計算其一雜湊值，例如，根據AES加密演算法執行雜湊值計算。

接下來，在步驟S302中，主機(播放設備) 350根據一預定程序(諸如對存取權限之確認等)計算轉換標題密鑰(經「互斥或」運算之標題密鑰) 323與自媒體(記憶卡) 320之

受保護區域(Protected Area)讀出之使用控制資訊(使用規則) 324之雜湊值之間的互斥「或」(XOR)運算。根據此處理，產生一標題密鑰。

接下來，在步驟S303中，主機(播放設備) 350藉由應用在步驟S302中產生之標題密鑰而對自媒體(記憶卡) 320讀出之媒體ID (MID) 322執行MAC計算。

接下來，在步驟S304中，主機(播放設備) 350執行自媒體(記憶卡) 320讀出之媒體ID-MAC 321與在步驟S303中計算之MAC值之間的匹配處理。

關於此匹配處理，當自媒體(記憶卡) 320讀出之媒體ID-MAC 321匹配在步驟S303中計算之所計算MAC值時，確定MAC匹配，做出已確認媒體(記憶卡) 320之有效性之判定，且流程進行至標題密鑰應用於其之經加密內容解密處理。

另一方面，關於該匹配處理，當自媒體(記憶卡) 320讀出之媒體ID-MAC 321不匹配在步驟S303中計算之所計算MAC值時，不確定MAC匹配，做出尚未確認媒體(記憶卡) 320之有效性之判定，且不執行標題密鑰應用於其之經加密內容解密處理。

注意，為描述基於此判定處理之處理之執行/不執行，在圖16中圖解說明一切換器351。此切換器351係圖解說明為用於描述處理演算法，且不必包括為實際硬體上之一組態。

關於步驟S304中之MAC驗證處理，當自媒體(記憶卡)

320讀出之媒體ID-MAC 321匹配在步驟S303中計算之所計算MAC值且確認媒體之有效性時，流程進行至步驟S305。

在步驟S305中，主機(播放設備) 350對自媒體(記憶卡) 320讀出之經加密內容325執行自轉換標題密鑰323產生之標題密鑰應用於其之解密處理以產生一內容(Content) 371，且執行內容使用處理，諸如內容回放或諸如此類。注意，根據自媒體(記憶卡) 320讀出之使用控制資訊(使用規則) 372之規則請求將此內容使用執行為一使用模式。

以此方式，在對儲存於媒體(記憶卡)中之一內容之解密/回放處理時，必須執行使用作為媒體之識別符之媒體ID (MID)之對媒體之有效性確認。

另一方面，存在用於執行內容回放之各種類型之內容裝置。舉例而言，如先前參考圖1及圖2所闡述，存在以下各種裝置。

*僅用於記錄/播放之裝置(CE裝置) 21，諸如DVD播放器、BD播放器或諸如此類

* PC 22

*可攜式終端機23，諸如一智慧電話或平板終端機或諸如此類

下文將闡述之一實施例係其中根據此等各種播放裝置之類型改變媒體(記憶卡)之識別符(媒體ID)之轉換模式之一配置實例。亦即，在將媒體ID (MID)輸出至用於執行內容回放之主機(播放設備)時，媒體(記憶卡)執行根據主機(播放設備)之類型而不同之資料轉換處理(Encode)以提供至主

機(播放設備)。主機(播放設備)關於自媒體(記憶卡)接收之轉換媒體ID (MID)根據裝置之類型執行恢復處理(Decode)以獲得媒體ID (MID)。

將參考圖17闡述一特定實例。圖17係其中用於執行內容回放之裝置(主機)被分類為以下兩種類型之一實例。

(1)主機=僅用於記錄/播放之裝置

(2)主機= PC及可攜式終端機

圖17圖解說明其中裝置(主機)被分類為此兩種類型且根據每一類型執行不同處理之一實例。

關於媒體(記憶卡)，一媒體ID (MID) 401儲存於記憶體中。媒體(記憶卡)確認其上安裝有媒體(記憶卡)以播放媒體內之一內容之主機(播放設備)之類型係以下類型中之哪一者。

(1)主機=僅用於記錄/播放之裝置

(2)主機= PC及可攜式終端機

做出有關主機(播放設備)之類型係以上類型中之哪一者之確認。

注意，可藉由確認(舉例而言)在將在主機(播放設備)與媒體(記憶卡)之間執行之相互鑑認處理時媒體(記憶卡)自主機(播放設備)接收之主機憑證(Host Cert)之類型資訊(見圖7及圖8)而執行對主機類型(播放設備類型)之此確認處理。

在媒體(記憶卡)已確認主機(播放設備)係僅用於記錄/播放之一裝置之情形下，執行圖解說明於圖17之左側之(1)主

機=僅用於記錄/播放之裝置之處理。

另一方面，在媒體(記憶卡)已確認主機(播放設備)係一PC或可攜式終端機之情形下，執行圖解說明於圖17之右側之(2)主機=PC/可攜式終端機之處理。

關於(1)主機=僅用於記錄/播放之裝置之處理，在步驟S321中，媒體(記憶卡)執行對對應於僅用於記錄/播放之一裝置之媒體(MID)之編碼處理(Encode)。將用作此編碼結果之僅用於記錄/播放之一裝置之一經編碼MID 411提供至作為主機(播放設備)之僅用於記錄/播放之裝置。

在步驟S322中，作為主機(播放設備)之僅用於記錄/播放之裝置應用該裝置本身包括之對應於僅用於記錄/播放之裝置之解碼演算法以解碼自媒體(記憶卡)接收之僅用於記錄/播放之一裝置之經編碼MID 411，且獲得一媒體ID (MID) 431。

另一方面，在(2)主機=PC及可攜式終端機之情形下，在步驟S331中，媒體(記憶卡)執行對對應於一PC及可攜式終端機之媒體(MID)之編碼處理(Encode)。將用作此編碼結果之一PC/可攜式終端機經編碼MID 412提供至作為主機(播放設備)之該PC或可攜式終端機。

在步驟S332中，作為主機(播放設備)之PC或可攜式終端機應用該裝置本身包括之對應於PC及可攜式終端機之解碼演算法以解碼自媒體(記憶卡)接收之PC/可攜式終端機經編碼MID 412，且獲得媒體ID (MID) 431。

媒體(記憶卡)經組態以便執行用於執行對媒體(MID)之

編碼處理(Encode)之不同多個編碼演算法，且根據主機(播放設備)之類型選擇性地應用一編碼演算法，例如，

在主機=僅用於記錄/播放之裝置之情形下應用一第一編碼演算法，及

在主機=PC或可攜式終端機之情形下應用一第二編碼演算法。

將參考圖18有關在根據主機(播放設備)之此類型執行媒體ID (MID)編碼處理之情形下之一內容解碼/播放序列做出說明。

圖18係用於以與先前所闡述之圖16相同之方式闡述對媒體ID (MAC)之驗證及一標題密鑰應用於其之經加密內容解密處理之一序列之一圖式。圖18以與圖16相同之方式圖解說明其中儲存有經加密內容等之一媒體(記憶卡) 320及用於執行對儲存於媒體(記憶卡) 320中之一經加密內容之解密/播放之一主機(播放設備) 350。

如圖式中所圖解說明，以下資料儲存於媒體(記憶卡) 320中：媒體ID-MAC 321，媒體ID (MID) 322，轉換標題密鑰(經「互斥或」運算之標題密鑰) 323，使用控制資訊(使用規則) 324，及經加密內容(Encrypted Content) 325。

注意，儘管各種類型之資料另外儲存於媒體(記憶卡) 320中，但僅圖解說明將應用於對一媒體ID (MAC)之驗證及一標題密鑰應用於其之經加密內容解密處理之序列之資料。

以與先前參考圖16所闡述相同之方式，轉換標題密鑰

(經「互斥或」運算之標題密鑰) 323係一標題密鑰之轉換資料，且儲存於記憶卡之受保護區域(Protected Area)中。特定而言，標題密鑰資料與使用控制資訊(使用規則) 324之雜湊值之間的一「互斥或」(XOR)運算結果儲存為轉換標題密鑰。

首先，在步驟S331中，媒體(記憶卡) 320根據用於執行內容回放之主機(播放設備)之類型執行對媒體ID (MID) 322之編碼處理。

注意，作為此處理之一前提，媒體(記憶卡) 320及主機(播放設備) 350已執行相互鑑認處理，且在對此相互鑑認之執行處理時，媒體(記憶卡) 320已自主機(播放設備) 350接收到主機憑證(Host Cert)。關於主機憑證(Host Cert)，如先前參考圖7及圖8所闡述，記錄類型資訊，且指示裝置之類型之裝置類型資訊記錄於其類型資訊中。

媒體(記憶卡) 320參考記錄於自主機(播放設備) 350接收之主機憑證(Host Cert)中之類型資訊(裝置類型資訊)而確認主機(播放設備)之類型。根據對此裝置類型之確認，判定媒體ID (MID)之編碼(Encode)模式(編碼演算法)，且根據所確定之編碼(Encode)模式(編碼演算法)執行對媒體ID (MID)之編碼處理。媒體(記憶卡) 320將在步驟S331中產生之對應於裝置類型之經編碼媒體ID (MID)提供至主機(播放設備) 350。

在步驟S351中，主機(播放設備) 350執行對自媒體(記憶卡) 320接收之經編碼媒體ID (MID)之解碼處理(Decode)。

主機(播放設備) 350包括根據其裝置類型之一解碼程式或解碼器，根據其裝置類型應用該解碼程式或解碼器以執行對經編碼媒體ID (MID)之解碼處理(Decode)。

在主機(播放設備) 350係僅用於記錄/播放之一裝置之情形下，僅用於記錄/播放之該裝置保持與僅用於記錄/播放之該裝置相關之一解碼程式或解碼器，且執行此解碼程式或解碼器已應用於其之處理。此外，在主機(播放設備) 350係一PC或可攜式終端機(諸如一平板終端機或諸如此類)之情形下，該PC或可攜式終端機保持與該PC或可攜式終端機相關之解碼程式或解碼器，且執行此解碼程式或解碼器已應用於其之處理。

主機(播放設備) 350藉由步驟S351中之解碼處理獲得媒體ID (MID)。注意，舉例而言，不管主機(播放設備) 350係一PC，舉例而言，在藉由假扮僅用於記錄/播放之裝置而非法盜用用於記錄/播放之裝置之主機憑證(Host Cert)以執行處理之情形下，PC不能獲得媒體ID (MID)，且不能此後執行內容回放。此係由於，在此一情形下，可僅僅藉由僅用於記錄/播放之裝置僅僅保持之解碼程式或解碼器解碼及獲得媒體(記憶卡)提供之媒體ID (MID)。

在主機(播放設備) 350獲得媒體ID (MID)之後之處理(亦即，步驟S352至S356中之處理)與先前參考圖16所闡述之步驟S301至S305中之處理相同。

在步驟S352中，主機(播放設備) 350自媒體(記憶卡) 320讀出使用控制資訊(使用規則) 324，且計算其一雜湊值，

例如，根據AES加密演算法執行雜湊值計算。

接下來，在步驟S353中，主機(播放設備) 350根據一預定程序(諸如對存取權限之確認等)計算轉換標題密鑰(經「互斥或」運算之標題密鑰) 323與所讀出之使用控制資訊(使用規則) 324之雜湊值之間的「互斥或」(XOR)運算。根據此處理，產生一標題密鑰。

接下來，在步驟S354中，主機(播放設備) 350藉由應用在步驟S353中產生之標題密鑰而對自媒體(記憶卡) 320讀出之媒體ID (MID) 322執行MAC計算。

接下來，在步驟S355中，主機(播放設備) 350執行自媒體(記憶卡) 320讀出之媒體ID-MAC 321與在步驟S354中計算之MAC值之間的匹配處理。

關於此匹配處理，當自媒體(記憶卡) 320讀出之媒體ID-MAC 321匹配在步驟S354中計算之所計算MAC值時，確定MAC匹配，做出已確認媒體(記憶卡) 320之有效性之判定，且流程進行至步驟S356中之標題密鑰應用於其之經加密內容解密處理。

另一方面，關於步驟S355中之匹配處理，當自媒體(記憶卡) 320讀出之媒體ID-MAC 321不匹配在步驟S354中計算之所計算MAC值時，不確定MAC匹配，做出尚未確認媒體(記憶卡) 320之有效性之判定，且不執行步驟S356中之標題密鑰應用於其之經加密內容解密處理。

注意，根據自媒體(記憶卡) 320讀出之使用控制資訊(使用規則) 324之規則請求將此內容使用執行為一使用模式。

以此方式，關於本實施例，媒體(記憶卡)鑑別主機(播放設備)之類型，且根據所鑑別之主機類型，改變媒體ID之轉換模式並提供至主機。主機應用包括於裝置本身中之對應於裝置類型之解密演算法以獲得媒體ID (MID)。根據此一配置，媒體(記憶卡)可根據主機(播放設備)之類型執行處理控制。

接下來，將參考圖19至圖21中所圖解說明之流程圖闡述根據本實施例之一內容回放處理序列。亦即，此等流程圖係用於闡述伴隨根據主機(播放設備)類型對媒體ID (MID)之轉換處理之一內容回放處理序列之流程圖。

圖19至圖21中所圖解說明之流程圖按順序圖解說明在左側之用於執行內容回放之一主機(播放設備)及在右側之其中儲存有一經加密內容及一標題密鑰之一媒體(記憶卡)，且按順序圖解說明由此兩個裝置執行之程序。將闡述步驟之處理之細節。

其上安裝有媒體(記憶卡)之主機(播放設備)在步驟S511中輸入將播放之一內容之選擇資訊。舉例而言，主機(播放設備)在主機之顯示器上顯示儲存於記憶卡中之一內容清單，且使用者自所顯示內容清單選擇將播放之一內容，且因此主機之資料處理區段識別使用者之所指定選定內容。

在步驟S512中，主機根據選定內容之類型啟動一播程式。

關於本處理實例，內容之類型係以下(a)及(b)中之一

者。

(a)正常內容，及

(b)高附加價值內容

特定而言，主機保持用於執行對一正常內容之回放處理之一正常內容播程式及用於執行對一高附加價值內容之回放處理之一高附加價值內容播程式，且啟動對應於被選定為將播放之一物件之內容之類型之播程式。

注意，儘管主機可僅僅具有正常內容播程式，但此一主機不能執行對一高附加價值內容之回放處理。此外，該高附加價值內容播程式可經設定以便僅播放高附加價值內容，或可經設定以成為能夠播放高附加價值內容及正常內容兩者之一程式。

接下來，在步驟S513中，主機自裝置本身之記憶體獲得與根據內容之類型啟動之播程式相關之一裝置憑證(Host Cert)。此裝置憑證(Host Cert)係先前參考圖7所闡述之一主機憑證(Host Cert)，且係其中以下資訊記錄為類型資訊之一憑證。

(1a)裝置類型資訊

(1b)對應內容類型資訊

注意，舉例而言，正常內容播程式可獲得僅僅對應於一正常內容之一主機憑證(指示於圖7中之(B)中)，且高附加價值內容播程式可獲得僅僅對應於一高附加價值內容及一正常內容之一主機憑證(指示於圖7中之(A)中)。舉例而言，關於用於獲得記錄於每一播程式中之一主機憑證

之資訊(例如，記憶體位址)，僅記錄對應於圖7中之(A)及(B)中之任一者之主機憑證之資訊(位址)，每一播放程式可僅獲得可由程式本身使用之一主機憑證。

接下來，在步驟S514a及S514b中，執行主機(播放設備)與媒體(記憶卡)之間的相互鑑認處理。關於此相互鑑認處理，主機(播放設備)將自主機之記憶體獲得之主機憑證(Host Cert)傳輸至媒體(記憶卡)。

另一方面，媒體(記憶卡)將儲存於媒體(記憶卡)內之記憶體中之媒體之一裝置憑證(Media Cert)傳輸至主機(播放設備)。舉例而言，此鑑認處理作為對此兩個公共密鑰憑證已應用於其之公共密鑰密碼系統之相互鑑認處理而執行。

接下來，將闡述在步驟S515a及S515b中且此後圖解說明於圖20中之處理。

在步驟S515a及S515b中，做出有關是否已建立主機(播放設備)與媒體(記憶卡)之間的相互鑑認之判定。在尚未建立相互鑑認之情形下，做出未能確認兩個裝置之間的可靠性之判定，流程進行至步驟S530，且停止內容回放處理。

在已建立相互鑑認之情形下，在步驟S516中，媒體(記憶卡)基於包括於裝置憑證(Host Cert)之類型資訊中之裝置類型資訊而鑑別主機(播放設備)之類型。舉例而言，媒體(記憶卡)鑑別裝置類型，使得主機係僅用於記錄/播放之一裝置、一PC或一可攜式終端機，諸如一平板終端機或諸如此類。

接下來，在步驟S517中，媒體(記憶卡)根據已預先根據基於裝置憑證(Host Cert)而鑑別之主機(播放設備)之類型(例如，僅用於記錄/播放之裝置、PC或可攜式終端機)與裝置類型相關地設定之編碼(Encode)演算法執行對媒體ID (MID)之編碼處理。

媒體(記憶卡)經組態以便選擇性地執行多個編碼演算法，且藉由根據主機(播放設備)之類型自此等多個編碼演算法選擇一者而執行對媒體ID (MID)之編碼(Encode)。

接下來，在步驟S518a中，媒體(記憶卡)將經編碼媒體ID (MID)傳輸至主機(播放設備)。

在步驟S518b中，主機(播放設備)自媒體(記憶卡)接收經編碼媒體ID (MID)。

接下來，在圖21中所圖解說明之步驟S519中，主機(播放設備)應用僅針對一裝置之該裝置本身可執行之解碼演算法以執行對經編碼媒體ID (MID)之解碼(decode)。

在於步驟S520中做出解碼失敗之判定之情形下，流程進行至步驟S530，且停止內容回放處理。

在於步驟S520中做出解碼成功之判定且已成功獲得媒體ID (MID)之情形下，流程進行至步驟S521。

在步驟S521a中，媒體(記憶卡)執行用於提供用於內容回放之資料之處理。特定而言，此資料之實例包括儲存於受保護區域中之一標題密鑰及儲存於通用區域中之一經加密內容。

在步驟S521b中，主機(播放設備)自媒體(記憶卡)接收一

標題密鑰、一經加密內容等。

最後，主機(播放設備)使用自媒體(記憶卡)接收之標題密鑰執行對一經加密內容之解密處理以執行內容回放。

注意，儘管在本流程中以一簡化方式圖解說明步驟S518a至S522中之程序，但此等程序對應於先前參考圖18所闡述之程序，其中執行諸如對媒體ID之MAC驗證處理、藉由基於使用控制資訊而計算一經轉換標題密鑰來獲得一標題密鑰等程序。

以此方式，媒體(記憶卡)藉由根據執行內容回放之主機(播放設備)改變媒體ID (MID)之轉換模式而執行內容回放。根據此處理，僅在已確認主機(播放設備)之類型與主機(播放設備)呈現之主機憑證之類型資訊之間的匹配之情形下，可執行內容回放。

此外，媒體(記憶卡)可基於主機憑證(Host Cert)而確認主機(播放設備)之類型，且亦可根據主機(播放設備)執行內容使用控制。舉例而言，可做出一配置，其中可執行根據主機(播放設備)之類型之內容使用控制，以使得僅僅在僅用於記錄/播放之一裝置處允許對一特定內容之使用，而在一PC及可攜式終端機處不允許。

注意，關於圖19至圖21中之流程圖，以與參考圖9至圖11所闡述相同之方式，儘管做出其中在步驟S512中啟動根據選定內容之類型之播放程式且選擇(S513)與播放程式相關之主機憑證(Host Cert)之一配置，但可做出其中與參考圖12至圖14所闡述之流程相同，內容播放程式本身根據內

容類型選擇一主機憑證之一配置。

此外，以上多項實施例，亦即：(第一實施例)用於根據內容類型選擇性地啟動一播放程式且使用與經啟動播放程式相關之一主機憑證(Host Cert)之一程序；(第二實施例)一播放程式根據內容類型選擇性地使用一主機憑證(Host Cert)之一程序；及(第三實施例)用於根據主機(播放設備)之類型改變媒體ID (MID)之轉換模式之一程序，此等程序可經配置以獨立地執行，或可經配置以作為第一實施例與第三實施例之間的一組合或第二實施例與第三實施例之間的一組合來執行。

6. 每一裝置之硬體組態實例

最後，將參考圖22及圖23闡述用於執行以上程序之裝置之硬體組態實例。

首先，將參考圖22闡述其上安裝有一記憶卡之用於執行資料記錄/回放處理之一主機裝置之一硬體組態實例。

一CPU(中央處理單元) 701用作用於根據儲存於ROM(唯讀記憶體) 702或一儲存單元708中之一程式執行各種類型之處理之一資料處理區段。舉例而言，CPU 701執行自一廣播站或伺服器之內容接收處理、關於一記憶卡(圖式中之可抽換式媒體711)對所接收資料之記錄處理、自記憶卡(圖式中之可抽換式媒體711)之資料回放處理等。CPU 701執行之一程式、資料或諸如此類適當地儲存於RAM(隨機存取記憶體) 703中。此等CPU 701、ROM 702及RAM 703藉由一匯流排704相互連接。

CPU 701經由匯流排704連接至一輸入/輸出介面705，且由各種類型之切換器、鍵盤、滑鼠、麥克風等組成之一輸入單元706及由一顯示器、揚聲器等組成之一輸出單元707連接至輸入/輸出介面705。CPU 701執行對應於來自輸入單元706之一命令輸入之各種類型之處理，且將處理結果輸出至(舉例而言)輸出單元707。

連接至輸入/輸出介面705之儲存單元708由(舉例而言)一硬磁碟或諸如此類組成，且儲存CPU 701執行之一程式及各種類型之資料。一通信單元709經由一網路(諸如網際網路或區域網路或諸如此類)與一外部裝置通信。

連接至輸入/輸出介面705之一磁碟機710驅動一可抽換式媒體711(諸如一磁碟、光碟、磁性-光學碟)或半導體記憶體(諸如一記憶卡或諸如此類)以獲得各種類型之資料，諸如所記錄內容、密鑰資訊等。舉例而言，根據CPU執行之播程式使用所獲得內容及密鑰資料而執行內容解密/回放處理或諸如此類。

圖23圖解說明一記憶卡之一硬體組態實例。一CPU(中央處理單元)801用作用於根據儲存於ROM(唯讀記憶體)802或一儲存單元807中之一程式執行各種類型之處理之一資料處理區段。舉例而言，CPU 801執行一伺服器或主機裝置之間的通信處理、關於儲存單元807對資料之寫入或讀取或諸如此類之處理、按儲存單元807之受保護區域811之區段區域之遞增序之可存取/不可存取判定處理(已關於以上實施例對其予以闡述)等。CPU 801執行之一程式、資

料等適當地儲存於RAM(隨機存取記憶體)803中。此等CPU 801、ROM 802及RAM 803藉由一匯流排804相互連接。

CPU 801經由匯流排804連接至一輸入/輸出介面805，且一通信單元806及儲存單元807連接至輸入/輸出介面805。

舉例而言，連接至輸入/輸出介面805之通信單元804執行與一伺服器或主機之通信。儲存單元807係一資料儲存區域，且包括具有存取權限之一受保護區域(Protected Area)811、在其處可自由地執行資料記錄/讀取之通用區域(General Purpose Area)812，如上文先前所闡述。

注意，舉例而言，可藉助具有與圖22中所圖解說明之主機裝置相同之硬體組態之一裝置實現伺服器。

7.本發明之組態之概述

已參考特定實施例詳細闡述了本發明之實施例。然而，很明顯，熟習此項技術者可在不背離本發明之本質之情形下構想各種修改或替代形式。亦即，已以一例示模式闡述了本發明，其不應以一限制方式來理解。應參考申請專利範圍以便判定本發明之本質。

注意，本說明書中所揭示之技術可具有以下配置。

(1)一種資訊處理系統，其包括：

一媒體，其中儲存有用作將播放之一物件之一內容；及
一播放設備，其經組態以播放儲存於該媒體中之一內容；

其中該播放設備經組態以

根據被選定為將播放之一物件之一內容類型選擇性地

啟動一播放程式，

藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與該播放程式相關之一裝置憑證，且

將該所獲得裝置憑證傳輸至該媒體；

且其中該裝置憑證係其中記錄有可利用該裝置憑證之內容類型資訊之內容類型之一裝置憑證；

且其中該媒體判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

(2)如(1)之資訊處理系統，其中該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構；

且其中該媒體判定已自該播放設備請求讀取之一加密密鑰是否係用於解密匹配係記錄於該裝置憑證中之一可用內容類型之一高附加價值內容或正常內容之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

(3)如(1)或(2)之資訊處理系統，其中該播放設備傳輸一所獲得裝置憑證以執行鑑認處理；

且其中該媒體以建立該鑑認處理作為一條件而執行對來自該播放設備之一加密密鑰讀出請求之准許判定處理。

(4)如(1)至(3)中任一者之資訊處理系統，其中該播放設備藉由根據與被選定為將播放之一物件之一內容相關之屬

性資訊識別一選定內容之類型而選擇性地啟動一播放程式。

(5)如(1)至(4)中任一者之資訊處理系統，其中該媒體將一加密密鑰儲存於在其處基於對一播放設備之存取權限之確認而准許存取之一受保護區域中，且基於記錄於將自該播放設備接收之一裝置憑證中之受保護區域存取權限資訊而確認在其處儲存有該加密密鑰之該受保護區域之存取權限，且在確認該播放設備之該等存取權限之情形下准許該播放設備讀出一加密密鑰。

(6)如(1)至(5)中任一者之資訊處理系統，其中該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結構；

且其中該媒體根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該播放設備；

且其中該播放設備伴隨藉由根據對應於該設備本身之裝置類型之一解碼演算法解碼自該媒體接收之一經編碼媒體ID而獲得之一媒體ID已應用於其之資料處理而執行對一內容之解碼或播放。

(7)一種資訊處理裝置，其包括：

一資料處理單元，其經組態以執行對儲存於一媒體中之一內容之讀出及回放處理；

其中該資料處理單元經組態以

根據被選定為將播放之一物件之一內容類型選擇性地

啟動一播放程式，

藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與此播放程式相關之一裝置憑證以將該所獲得裝置憑證傳輸至該媒體，且亦

將一經加密內容及對將應用於對此經加密內容之解密之一加密密鑰之一讀出請求輸出至該媒體，且

以該媒體做出確認作為一條件而自該媒體獲得一加密密鑰，其中已執行對其之該讀出請求之一加密密鑰係匹配記錄於該裝置憑證中之可使用之一內容類型之一內容之一加密密鑰以藉由將該所獲得加密密鑰應用於一經加密內容而執行對該經加密內容之解密。

(8)如(7)之資訊處理裝置，其中該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構。

(9)如(7)或(8)之資訊處理裝置，其中該資料處理單元將一所獲得裝置憑證傳輸至該媒體以執行鑑認處理。

(10)如(7)至(9)中任一者之資訊處理裝置，其中該資料處理單元藉由根據與被選定為將播放之一物件之一內容相關之屬性資訊識別一選定內容之類型而選擇性地啟動一播放程式。

(11)如(7)至(10)中任一者之資訊處理裝置，其中該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結構；

且其中該媒體根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該資訊處理裝置；

且其中該資訊處理裝置之一資料處理單元伴隨藉由根據對應於該設備本身之裝置類型之一解碼演算法解碼自該媒體接收之一經編碼媒體ID而獲得之一媒體ID已應用於其之資料處理而執行對一內容之解碼或播放。

(12)一種資訊處理裝置，其包括：

一儲存單元，其中儲存有用作將在一播放設備中播放之一物件之一經加密內容及將應用於對該經加密內容之解密之一加密密鑰；及

一資料處理單元；

其中該資料處理單元經組態以

自該播放設備接收一裝置憑證，且亦接收對將應用於對用作將播放之一物件之一經加密內容之解密的一加密密鑰的一讀出請求，且

判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

(13)如(12)之資訊處理裝置，其中該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構；

且其中該資料處理單元判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配具有記錄於該裝置憑證中之一可用內容類型之一高附加價值內容或正常內容之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

(14)如(12)或(13)之資訊處理裝置，其中該加密密鑰儲存於在其處基於對一播放設備之存取權限之確認而准許存取之一儲存單元內之一受保護區域中；

且其中該資料處理單元基於記錄於將自該播放設備接收之一裝置憑證中之受保護區域存取權限資訊而確認在其處儲存有該加密密鑰之該受保護區域之存取權限，且在確認該播放設備之該等存取權限之情形下准許該播放設備讀出一加密密鑰。

(15)如(12)至(14)中任一者之資訊處理裝置，其中該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結構；

且其中該資料處理單元根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該播放設備。

此外，將在以上裝置及系統處執行之一處理方法及致使該裝置及系統執行處理之一程式亦涵蓋於本發明之配置中。

此外，可藉由硬體或軟體或兩者之一複合配置來執行本說明書中所闡述之一系列處理。在根據軟體執行處理之情

形下，其中記錄有一處理序列之一程式可藉由安裝於嵌入於專用硬體中之一電腦內之記憶體中來執行，或可藉由安裝於能夠進行各種類型之處理之一通用電腦中來執行。舉例而言，該程式可預先記錄於一記錄媒體中。除自一記錄媒體將該程式安裝於一電腦中外，亦可經由一網路(諸如LAN(區域網路)或網際網路)接收該程式且安裝於一記錄媒體(諸如一內建硬磁碟或諸如此類)中。

注意，根據本說明書之各種類型之處理不僅包括根據所闡述之序列以時間序列執行之處理，而且包括未必以時間序列執行而是根據執行處理之一裝置之處理能力或需要並行或個別地執行之處理。此外，關於本說明書，術語「系統」係多個裝置之一邏輯群組組態，且不限於其中用作組件之裝置包括於同一殼體中之一組態。

本申請案含有與於2011年8月11日在日本專利局提出申請之日本優先專利申請案JP 2011-175606中所揭示之標的物相關之標的物，該申請案之全部內容據此以引用方式併入。

熟習此項技術者應瞭解，可取決於設計要求及其他因素做出各種修改、組合、子組合及變更，只要其歸屬於隨附申請專利範圍或其等效範圍之範疇內即可。

【圖式簡單說明】

圖1係用於闡述內容提供處理及使用處理之概述之一圖式；

圖2係用於闡述記錄於一記憶卡中之一內容之一使用模

式之一圖式；

圖3係用於闡述該記憶卡之一儲存區域之一特定組態實例之一圖式；

圖4係用於闡述一主機憑證(Host Certificate)之一圖式；

圖5係用於闡述該記憶卡之該儲存區域之一特定組態實例及存取控制處理之一實例之一圖式；

圖6係用於闡述一記憶卡之所儲存資料之一實例之一圖式；

圖7係用於闡述其中記錄有一裝置類型及對應內容類型之類型資訊之該主機憑證(Host Certificate)之一資料組態實例之一圖式；

圖8係用於闡述一裝置類型及將記錄於該主機憑證(Host Certificate)中之對應內容類型之類型資訊之一特定實例之一圖式；

圖9係圖解說明用於闡述將藉由根據內容類型選擇性地啟動一播放程式且使用與該經啟動播放程式相關之主機憑證(Host Certificate)而執行之一內容使用序列之一流程之一圖式；

圖10係圖解說明用於闡述將藉由根據內容類型選擇性地啟動一播放程式且使用與該經啟動播放程式相關之主機憑證(Host Certificate)而執行之該內容使用序列之一流程之一圖式；

圖11係圖解說明用於闡述將藉由根據內容類型選擇性地啟動一播放程式且使用與該經啟動播放程式相關之主機憑

證 (Host Certificate) 而執行之該內容使用序列之一流程之一圖式；

圖 12 係圖解說明用於闡述一序列之一流程之一圖式，其中播放程式根據內容類型選擇性地使用主機憑證 (Host Certificate)；

圖 13 係圖解說明用於闡述該序列之一流程之一圖式，其中播放程式根據內容類型選擇性地使用主機憑證 (Host Certificate)；

圖 14 係圖解說明用於闡述該序列之一流程之一圖式，其中播放程式根據內容類型選擇性地使用主機憑證 (Host Certificate)；

圖 15 係用於闡述一記憶卡之所儲存資料之一實例之一圖式；

圖 16 係用於闡述使用一媒體 ID (MID) 之一內容解碼及播放序列之一圖式；

圖 17 係用於闡述用於根據一主機 (播放設備) 之類型改變一媒體 ID (MID) 之轉換模式之處理之一圖式；

圖 18 係用於闡述在根據一主機 (播放設備) 之類型改變一媒體 ID (MID) 之轉換模式之情形下之內容解碼及回放處理之一圖式；

圖 19 係圖解說明用於闡述在藉由根據一主機 (播放設備) 之類型改變一媒體 ID (MID) 之轉換模式執行內容解碼及回放處理之情形下之一處理序列之一流程之一圖式；

圖 20 係圖解說明用於闡述在藉由根據一主機 (播放設備)

之類型改變一媒體ID (MID)之轉換模式執行內容解碼及回放處理之情形下之該處理序列之一流程的一圖式；

圖 21係圖解說明用於闡述在藉由根據一主機(播放設備)之類型改變一媒體ID (MID)之轉換模式執行內容解碼及回放處理之情形下之該處理序列之一流程的一圖式；

圖 22係用於闡述一主機(播放設備)之一硬體組態實例之一圖式；及

圖 23係用於闡述一記憶卡之一硬體組態實例之一圖式。

【主要元件符號說明】

- 11 廣播站
- 12 內容伺服器
- 21 裝置(CE裝置：消費型電子裝置)/僅用於記錄/
 播放之裝置/記錄/播放設備/僅用於記錄/播放
 之裝置(消費型電子裝置)
- 22 個人電腦
- 23 可攜式終端機
- 31 記憶卡
- 51 受保護區域
- 52 通用區域
- 61 區段區域#0(受保護區域#0)
- 62 區段區域#1(受保護區域#1)
- 70 主機(記錄/播放設備)
- 100 記憶卡
- 101 受保護區域

102	通用區域
300	媒體(記憶卡)
311	受保護區域
312	通用區域
315	媒體ID (MID)
316	媒體ID-訊息鑑認碼
320	媒體(記憶卡)
321	媒體ID-訊息鑑認碼
322	媒體ID (MID)
323	轉換標題密鑰(經「互斥或」運算之標題密鑰)
324	使用控制資訊(使用規則)
325	經加密內容
350	主機(播放設備)
351	切換器
371	內容
372	使用控制資訊(使用規則)
401	媒體ID (MID)
411	經編碼MID
412	個人電腦/可攜式終端機經編碼MID
431	媒體ID (MID)
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	通信單元
710	磁碟機
711	可抽換式媒體
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/通信單元
805	輸入/輸出介面
806	通信單元
807	儲存單元
811	受保護區域
812	通用區域

七、申請專利範圍：

1. 一種資訊處理系統，其包含：

一媒體，其中儲存有用作將播放之一物件之一內容；
及

一播放設備，其經組態以播放儲存於該媒體中之一內容；

其中該播放設備經組態以

根據被選定為將播放之一物件之一內容類型選擇性地啟動一播放程式，

藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與該播放程式相關之一裝置憑證，且

將該所獲得裝置憑證傳輸至該媒體；

且其中該裝置憑證係其中記錄有可利用該裝置憑證之內容類型資訊之內容類型之一裝置憑證；

且其中該媒體判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在匹配之情形中准許讀出該加密密鑰。

2. 如請求項1之資訊處理系統，其中該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構；

且其中該媒體判定已自該播放設備請求讀取之一加密密鑰是否係用於解密匹配係記錄於該裝置憑證中之一可

用內容類型之一高附加價值內容或正常內容之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

3. 如請求項1之資訊處理系統，其中該播放設備傳輸一所獲得裝置憑證以執行鑑認處理；

且其中該媒體以建立該鑑認處理作為一條件而執行對來自該播放設備之一加密密鑰讀出請求之准許判定處理。

4. 如請求項1之資訊處理系統，其中該播放設備藉由根據與被選定為將播放之一物件之一內容相關之屬性資訊識別一選定內容之類型而選擇性地啟動一播程式。

5. 如請求項1之資訊處理系統，其中該媒體將一加密密鑰儲存於在其處基於對一播放設備之存取權限之確認而准許存取之一受保護區域中，且基於記錄於將自該播放設備接收之一裝置憑證中之受保護區域存取權限資訊而確認在其處儲存有該加密密鑰之該受保護區域之存取權限，且在確認該播放設備之該等存取權限之情形下准許該播放設備讀出一加密密鑰。

6. 如請求項1之資訊處理系統，其中該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結構；

且其中該媒體根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該播放設備；

且其中該播放設備伴隨藉由根據對應於該設備本身之裝置類型之一解碼演算法解碼自該媒體接收之一經編碼媒體ID而獲得之一媒體ID已應用於其之資料處理而執行對一內容之解碼或播放。

7. 一種資訊處理裝置，其包含：

一資料處理單元，其經組態以執行對儲存於一媒體中之一內容之讀出及回放處理；

其中該資料處理單元經組態以

根據被選定為將播放之一物件之一內容類型選擇性地啟動一播程序，

藉由執行該選擇性地啟動之播程序自一儲存單元獲得與此播程序相關之一裝置憑證以將該所獲得裝置憑證傳輸至該媒體，且亦

將一經加密內容及對將應用於對此經加密內容之解密之一加密密鑰之一讀出請求輸出至該媒體，且

以該媒體做出確認作為一條件而自該媒體獲得一加密密鑰，其中已執行對其之該讀出請求之一加密密鑰係匹配記錄於該裝置憑證中之可使用之一內容類型之一內容之一加密密鑰以藉由將該所獲得加密密鑰應用於一經加密內容而執行對該經加密內容之解密。

8. 如請求項7之資訊處理裝置，其中該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構。

9. 如請求項7之資訊處理裝置，其中該資料處理單元將一所獲得裝置憑證傳輸至該媒體以執行鑑認處理。
10. 如請求項7之資訊處理裝置，其中該資料處理單元藉由根據與被選定為將播放之一物件之一內容相關之屬性資訊識別一選定內容之類型而選擇性地啟動一播程式。
11. 如請求項7之資訊處理裝置，其中該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結構；

且其中該媒體根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該資訊處理裝置；

且其中該資訊處理裝置之一資料處理單元伴隨藉由根據對應於該設備本身之裝置類型之一解碼演算法解碼自該媒體接收之一經編碼媒體ID而獲得之一媒體ID已應用於其之資料處理而執行對一內容之解碼或播放。

12. 一種資訊處理裝置，其包含：

一儲存單元，其中儲存有用作將在一播放設備中播放之一物件之一經加密內容及將應用於對該經加密內容之解密之一加密密鑰；及

一資料處理單元；

其中該資料處理單元經組態以

自該播放設備接收一裝置憑證，且亦接收對將應用於對用作將播放之一物件之一經加密內容之解密的一

加密密鑰之一讀出請求，且

判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密與記錄於該裝置憑證中之一可用內容類型匹配之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

13. 如請求項12之資訊處理裝置，其中該裝置憑證具有其中一高附加價值內容及除該高附加價值內容外之一正常內容中之至少一者被記錄為可利用該裝置憑證之一內容類型之一結構；

且其中該資料處理單元判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配具有記錄於該裝置憑證中之一可用內容類型之一高附加價值內容或正常內容之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

14. 如請求項12之資訊處理裝置，其中該加密密鑰儲存於在其處基於對一播放設備之存取權限之確認而准許存取之一儲存單元內之一受保護區域中；

且其中該資料處理單元基於記錄於將自該播放設備接收之一裝置憑證中之受保護區域存取權限資訊而確認在其處儲存有該加密密鑰之該受保護區域之存取權限，且在確認該播放設備之該等存取權限之情形下准許該播放設備讀出一加密密鑰。

15. 如請求項12之資訊處理裝置，其中該裝置憑證具有其中記錄有可利用該裝置憑證之播放設備類型資訊之一結

構；

且其中該資料處理單元根據將根據記錄於該裝置憑證中之播放設備類型資訊選擇之一編碼演算法執行對係該媒體之識別資訊之一媒體ID之編碼處理以傳輸至該播放設備。

16. 一種將在一資訊處理系統中執行之資訊處理方法，該資訊處理系統具有

一媒體，其中儲存有用作將播放之一物件之一內容，及一播放設備，其經組態以播放儲存於該媒體中之一內容，其中該播放設備經組態以

根據被選定為將播放之一物件之一內容類型選擇性地啟動一播放程式，且

藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與此播放程式相關之一裝置憑證以將該所獲得裝置憑證傳輸至該媒體；

且其中該裝置憑證係其中記錄有可利用該裝置憑證之內容類型資訊之一裝置憑證；

且其中該媒體判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密與記錄於該裝置憑證中之一可用內容類型匹配之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

17. 一種將在一資訊處理裝置中執行之資訊處理方法，其中一資料處理單元經組態以

根據被選定為將播放之一物件之一內容類型選擇性地

啟動一播放程式，且

藉由執行該選擇性地啟動之播放程式自一儲存單元獲得與此播放程式相關之一裝置憑證以將該所獲得裝置憑證傳輸至該媒體，且亦

將一經加密內容及對將應用於對此經加密內容之解密之一加密密鑰之一讀出請求輸出至該媒體，且

以該媒體做出確認作為一條件而自該媒體獲得一加密密鑰，其中已執行對其之該讀出請求之一加密密鑰係匹配記錄於該裝置憑證中之可使用之一內容類型之一內容的一加密密鑰以藉由將該所獲得加密密鑰應用於一經加密內容而執行對該經加密內容之解密。

18. 一種將在一資訊處理裝置中執行之資訊處理方法，其中該資訊處理裝置包括

一儲存單元，其中儲存有用作將在一播放設備中播放之一物件之一經加密內容及將應用於對該經加密內容之解密之一加密密鑰；及

一資料處理單元；

且其中該資料處理單元經組態以

自該播放設備接收一裝置憑證，且亦接收對將應用於對用作將播放之一物件之一經加密內容之解密的一加密密鑰的一讀出請求，且

判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密匹配記錄於該裝置憑證中之一可用內容類型之一經加密內容之一加密密鑰，且僅在

匹配之情形下准許讀出該加密密鑰。

19. 一種致使一資訊處理裝置執行資訊處理且致使一資料處理單元進行以下操作之程式

根據被選定為將播放之一物件之一內容類型選擇性地啟動一播程式，

藉由執行該選擇性地啟動之播程式自一儲存單元獲得與此播程式相關之一裝置憑證以將該所獲得裝置憑證傳輸至該媒體，且亦

將一經加密內容及對將應用於對此經加密內容之解密之一加密密鑰之一讀出請求輸出至該媒體，且

以該媒體做出確認作為一條件而自該媒體獲得一加密密鑰，其中已執行對其之該讀出請求之一加密密鑰係匹配記錄於該裝置憑證中之可使用之一內容類型之一內容的一加密密鑰以藉由將該所獲得加密密鑰應用於一經加密內容而執行對該經加密內容之解密。

20. 一種致使一資訊處理裝置執行資訊處理之程式，其中該資訊處理裝置包括

一儲存單元，其中儲存有用作將在一播放設備中播放之一物件之一經加密內容及將應用於對該經加密內容之解密之一加密密鑰，及

一資料處理單元；

且其中該程式致使該資料處理單元

自該播放設備接收一裝置憑證，且亦接收對將應用於對用作將播放之一物件之一經加密內容之解密的一

加密密鑰的一讀出請求，且

判定已自該播放設備執行對其之一讀取請求之一加密密鑰是否係用於解密與記錄於該裝置憑證中之一可用內容類型匹配之一經加密內容之一加密密鑰，且僅在匹配之情形下准許讀出該加密密鑰。

八、圖式：

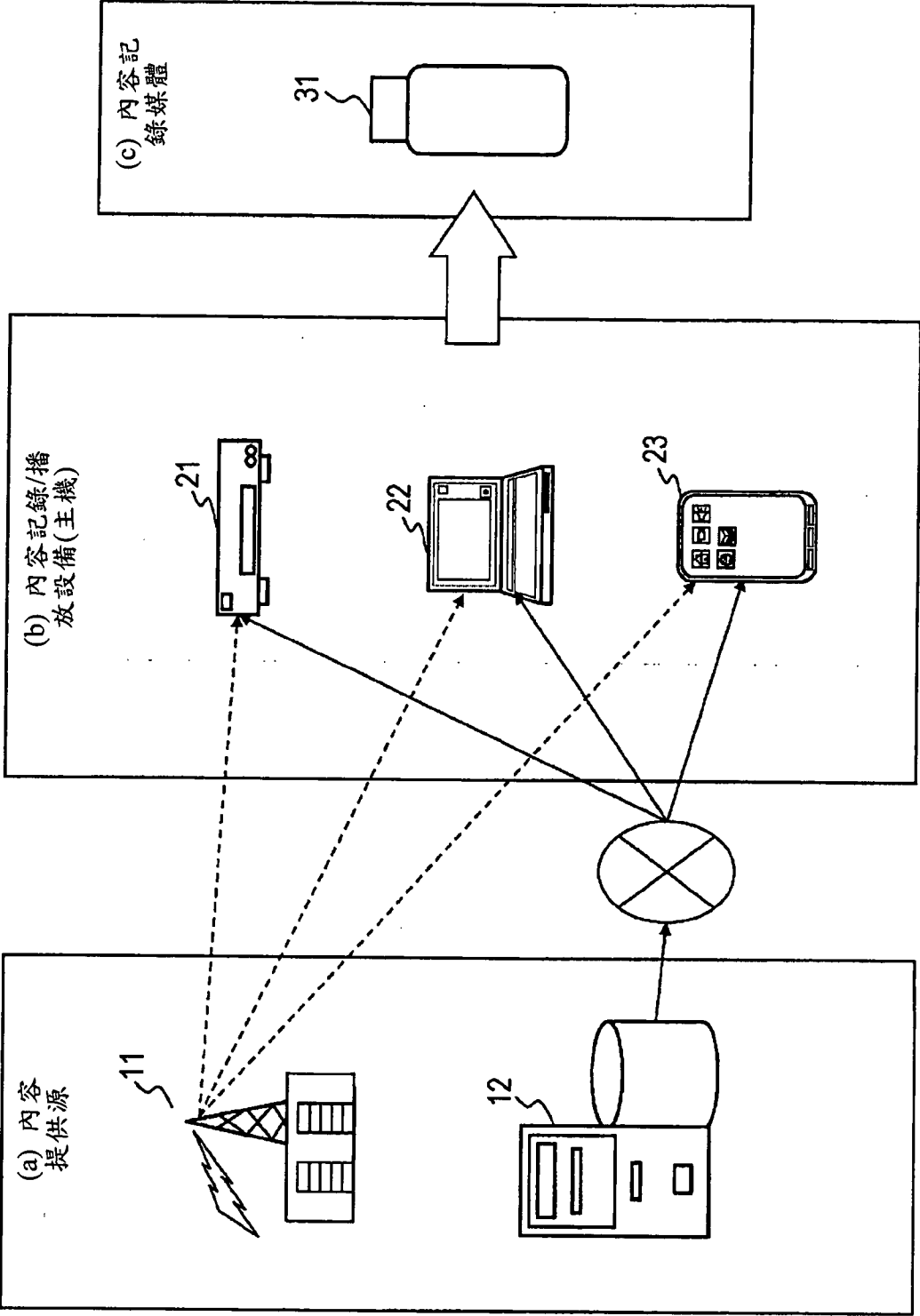


圖 1

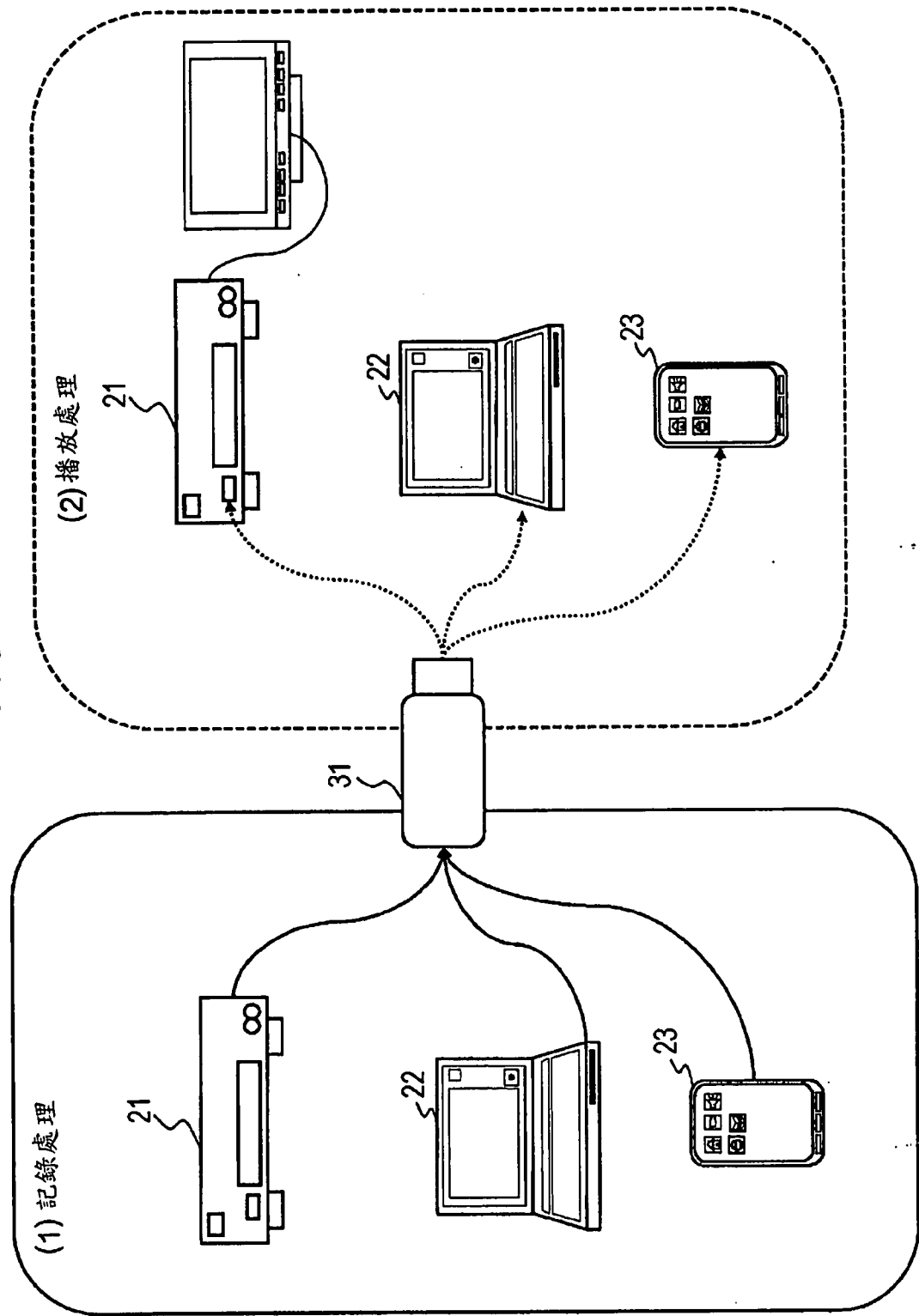


圖 2

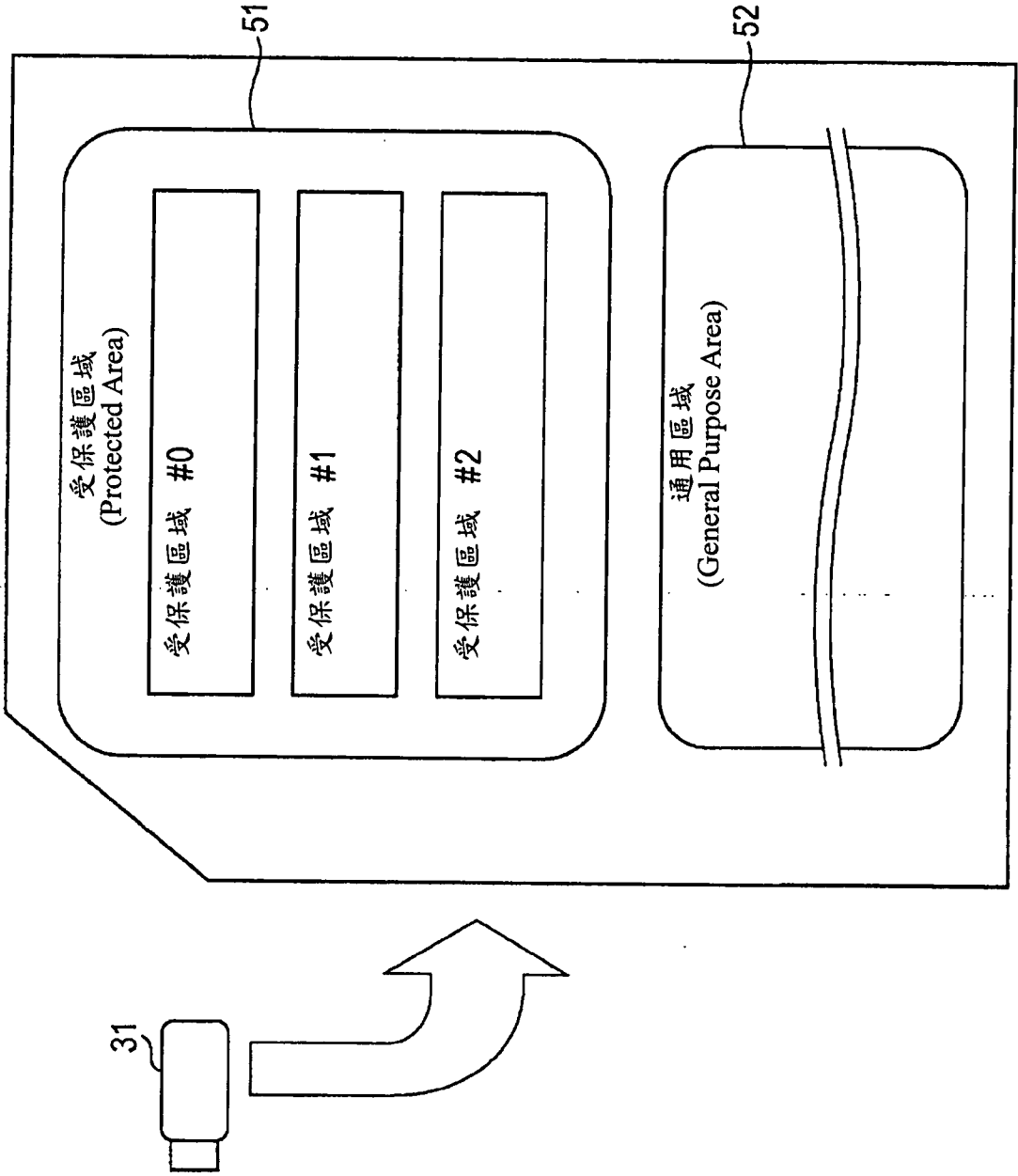


圖 3

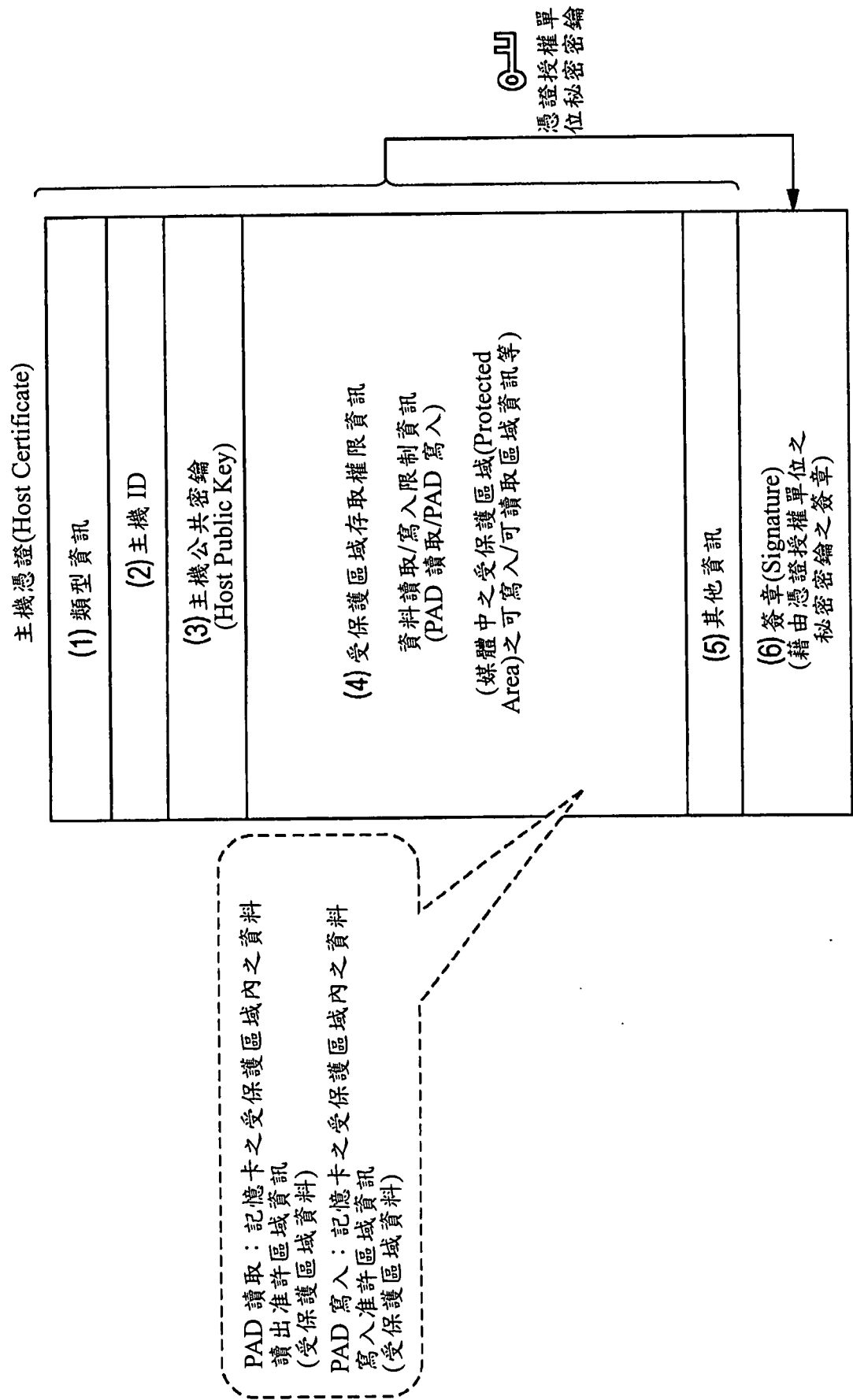


圖 4

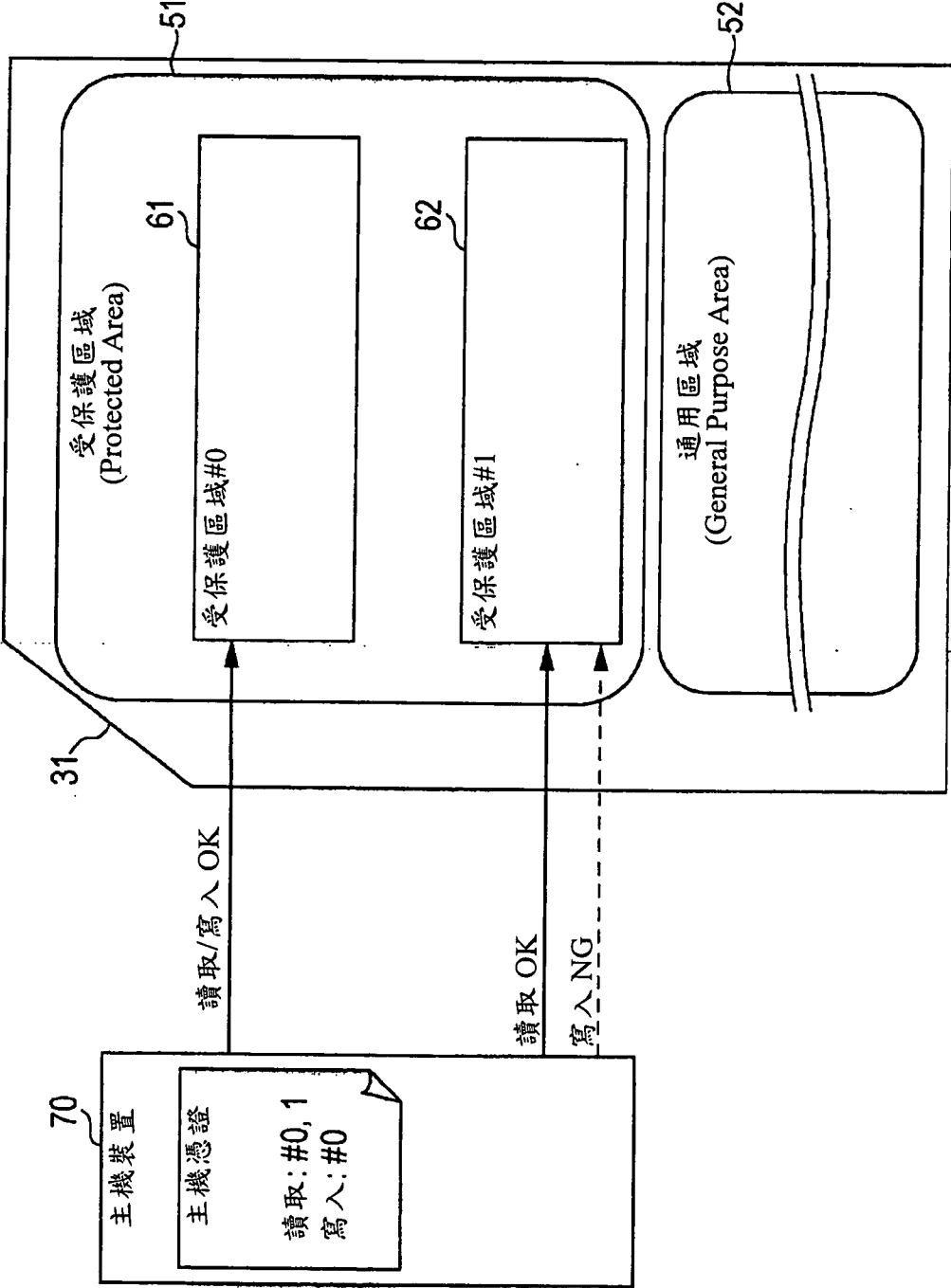


圖 5

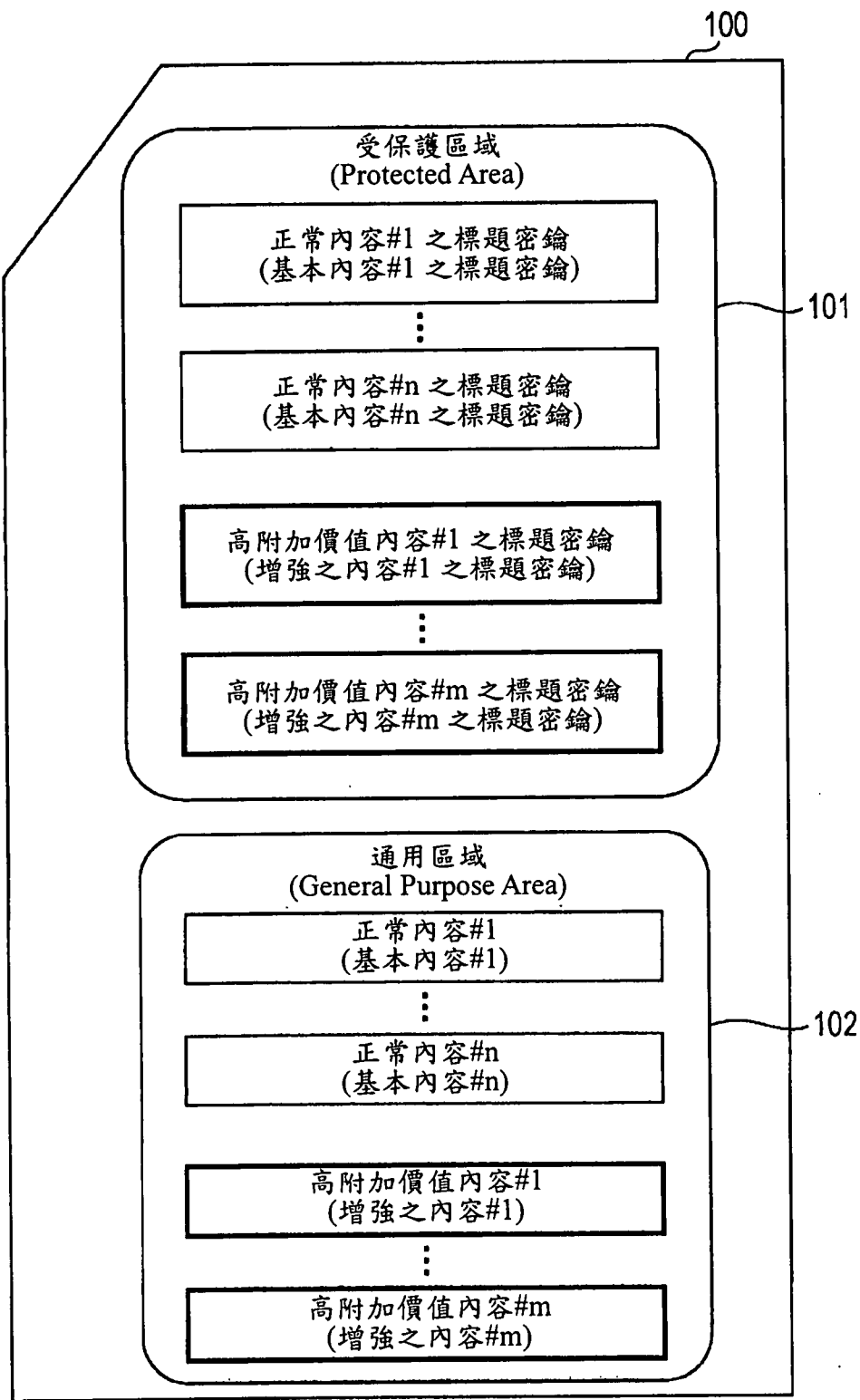


圖 6

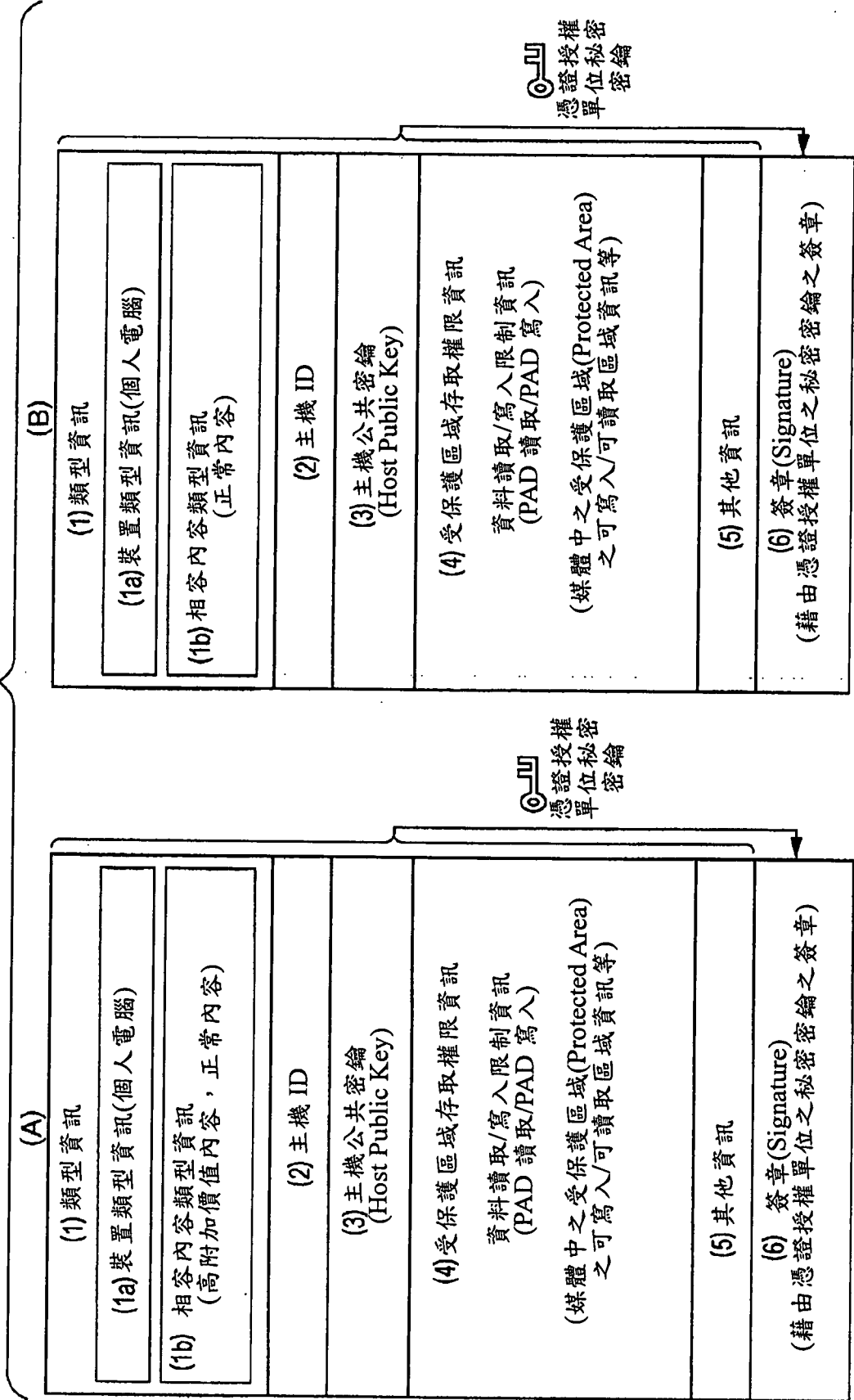


圖 7

(1a) 裝置類型 資訊(個人電腦)	(1b) 相容內容類型資訊 (高附加價值內容，正常內容)
0x0001 (僅用於記錄/播放之裝置)	0x0001 僅僅對應於正常內容
	0x0002 僅僅對應於高附加價值內容
	0x0003 對應於高附加價值內容及正常內容兩者
0x0002 個人電腦/可攜式終端機	0x0001 僅僅對應於正常內容
	0x0002 僅僅對應於高附加價值內容
	0x0003 對應於高附加價值內容及正常內容兩者

圖 8

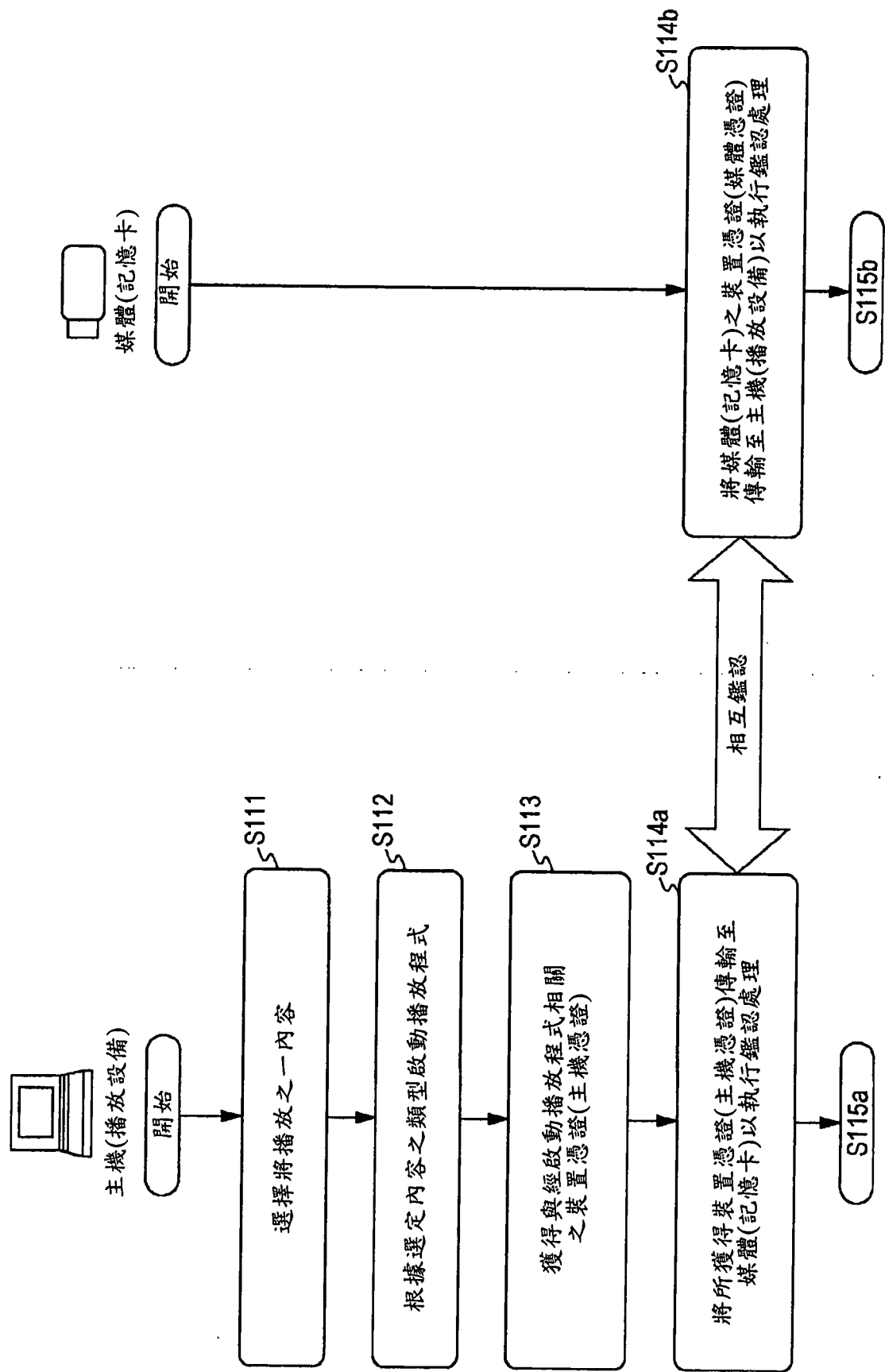


圖 9

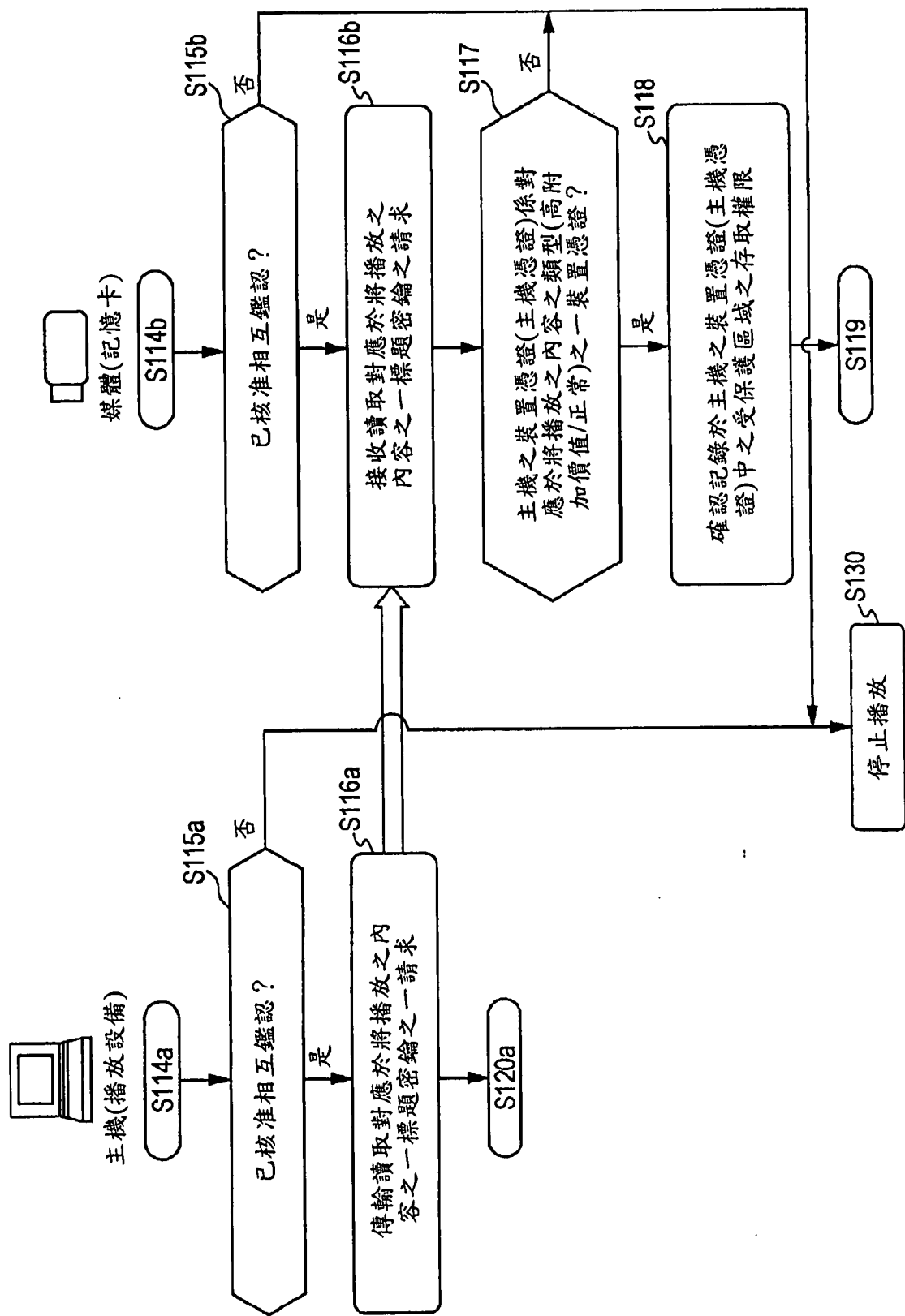


圖 10

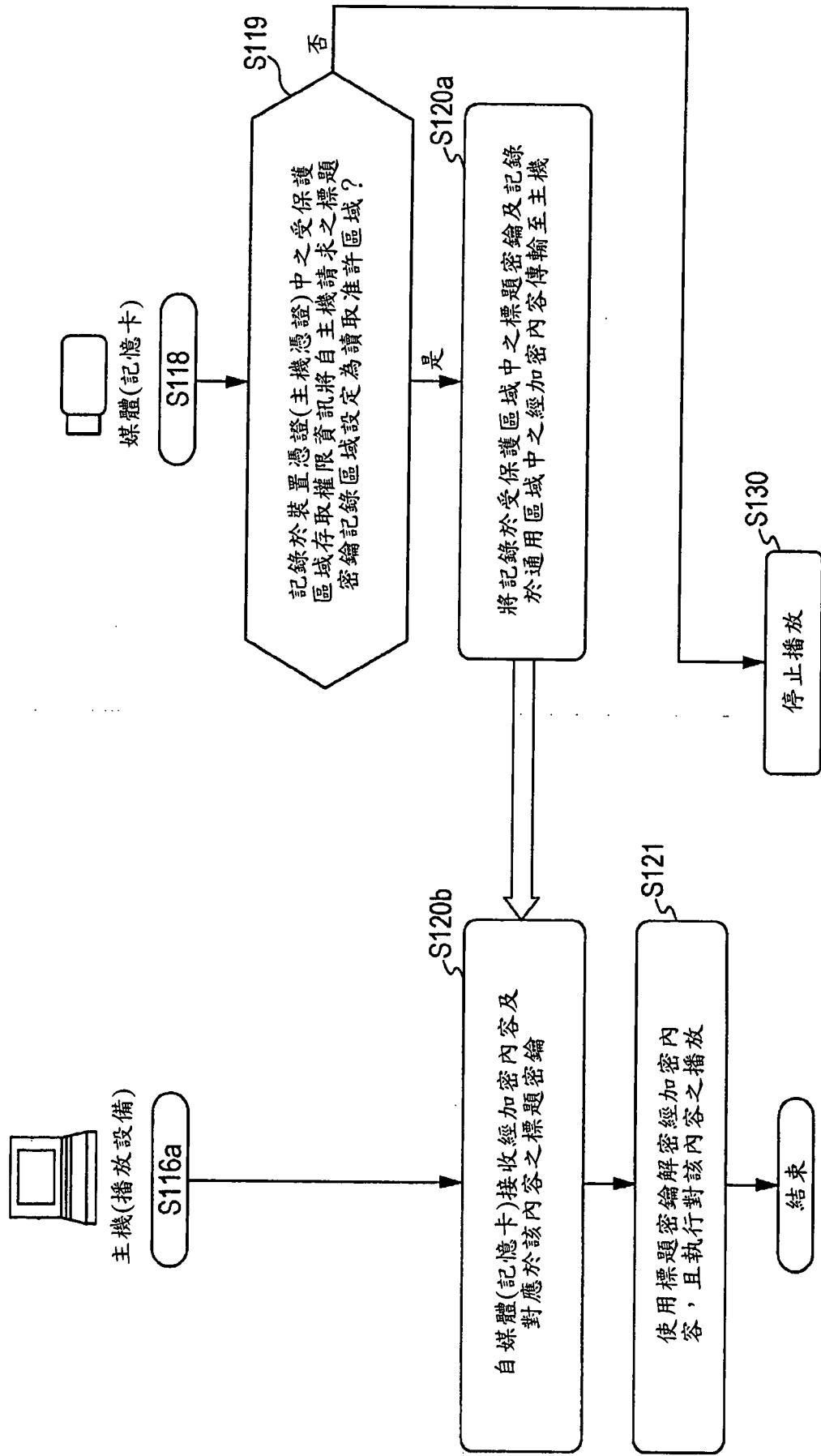


圖 11

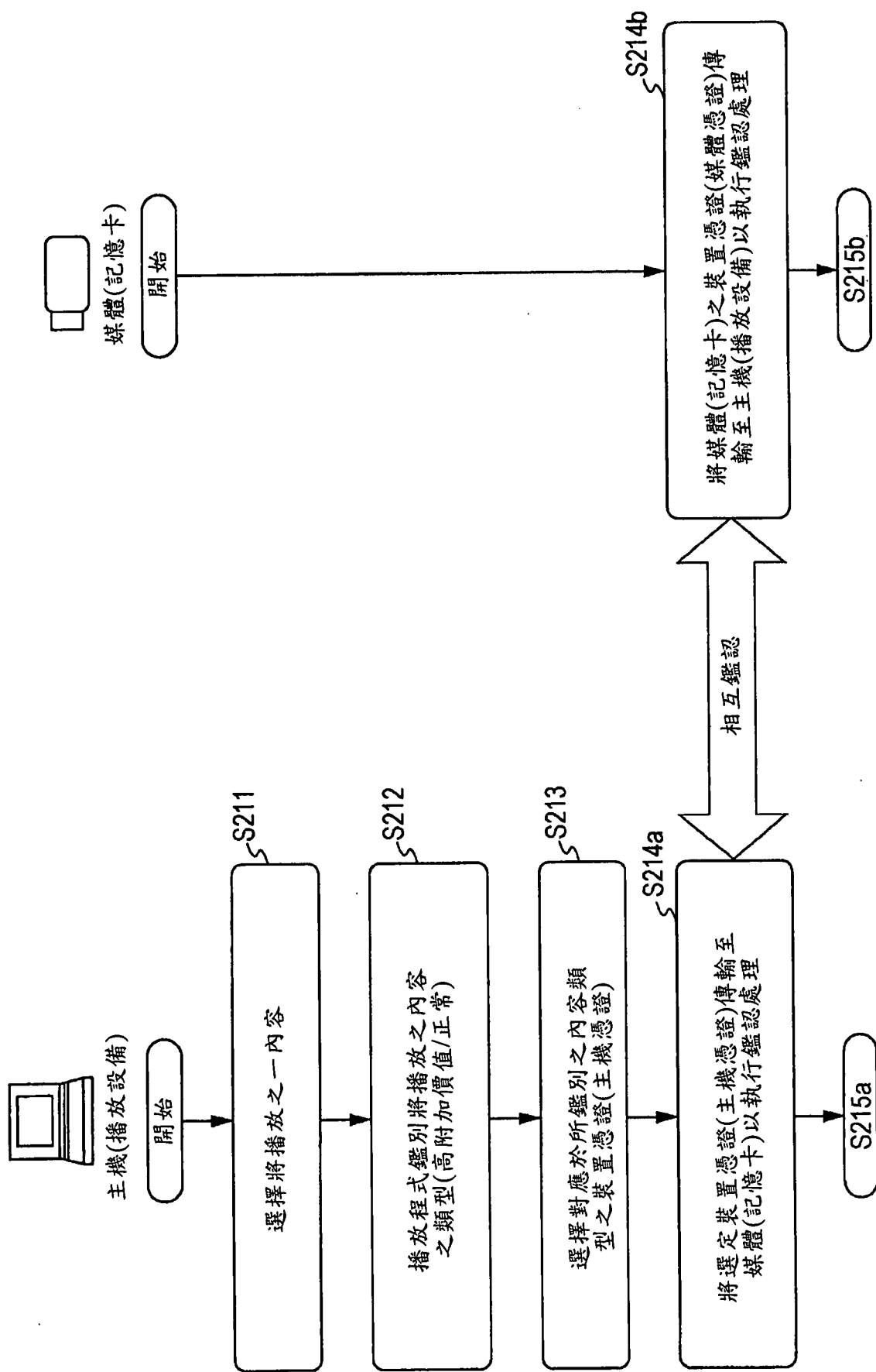


圖 12

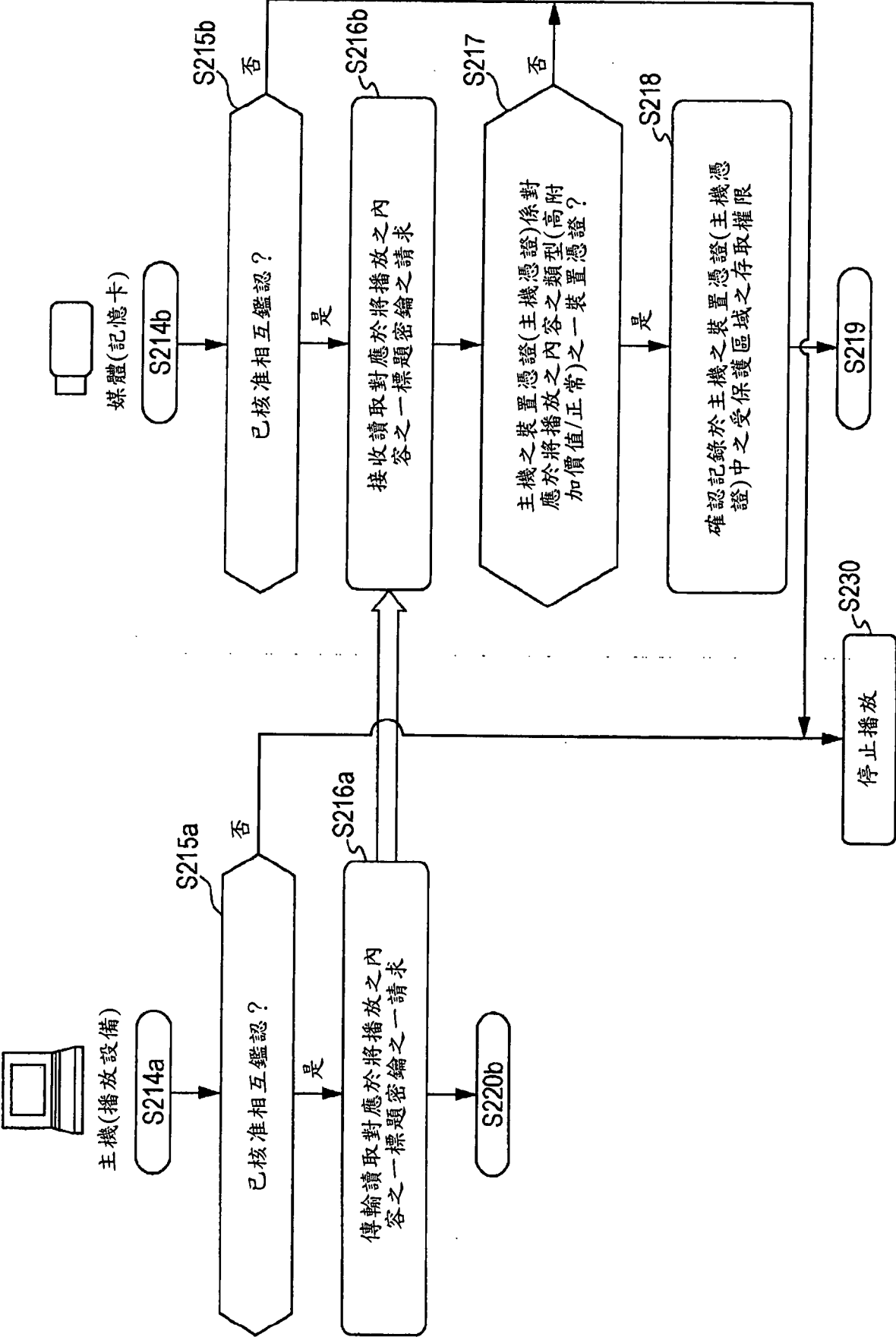


圖 13



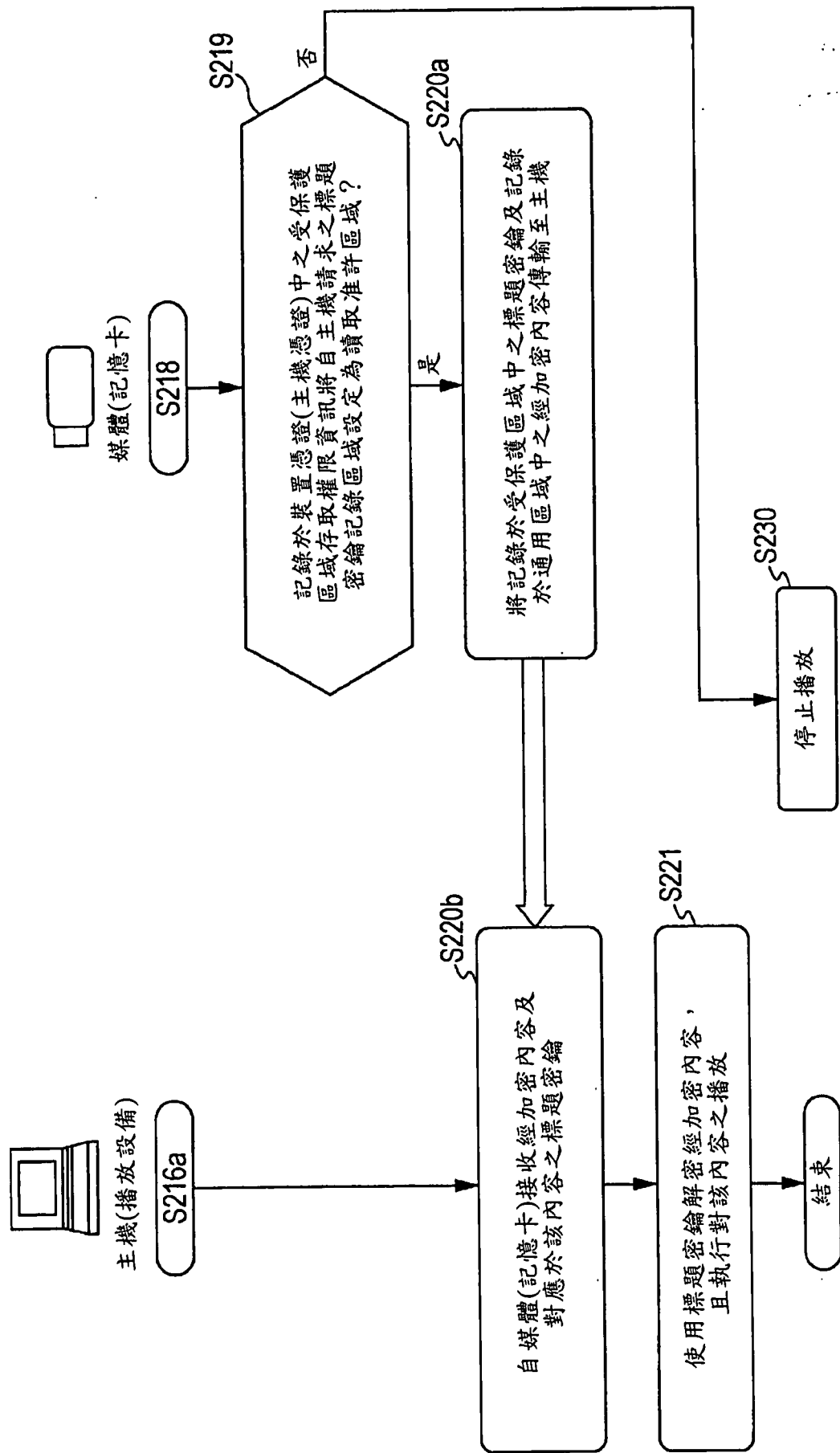


圖 14

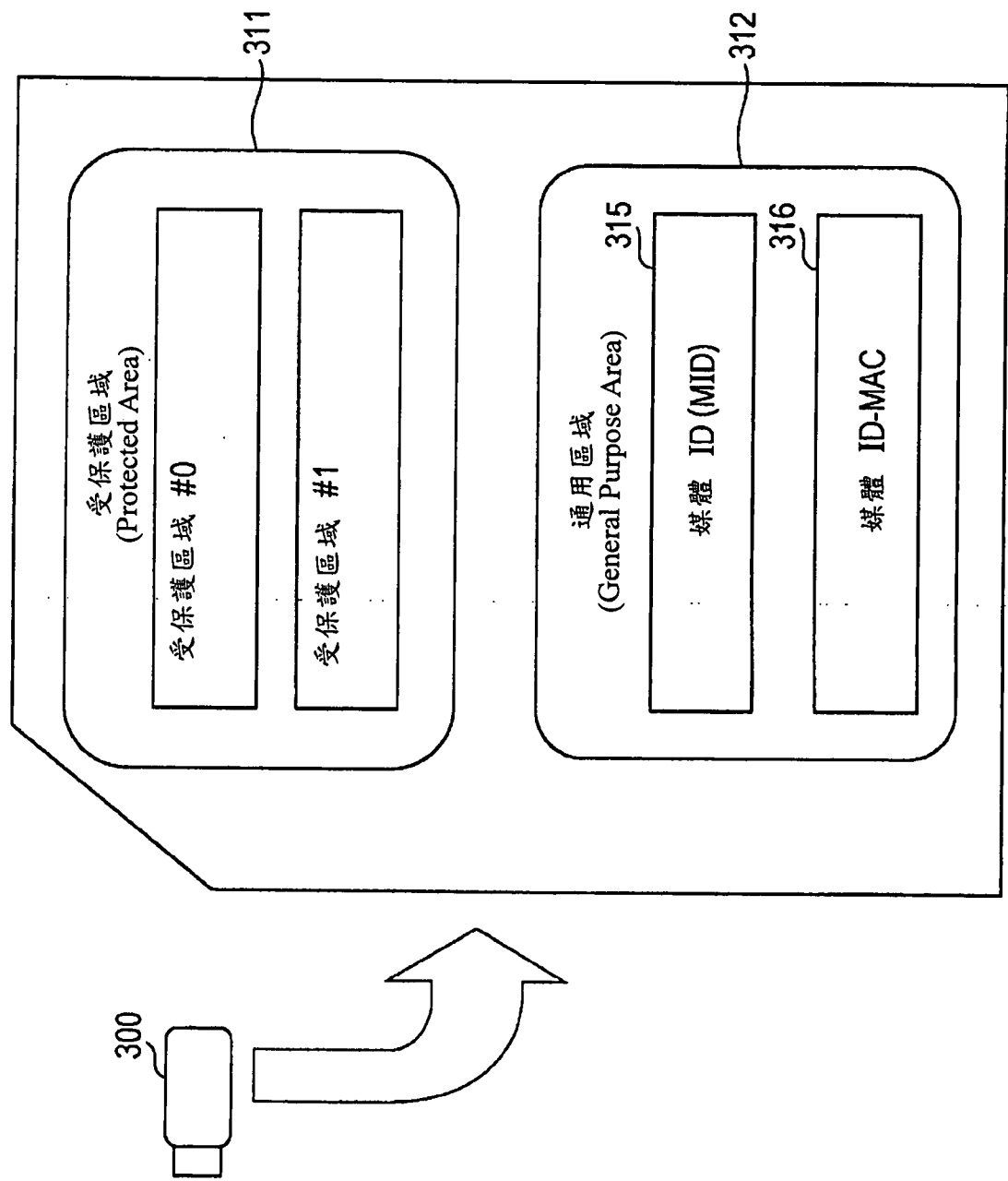


圖 15

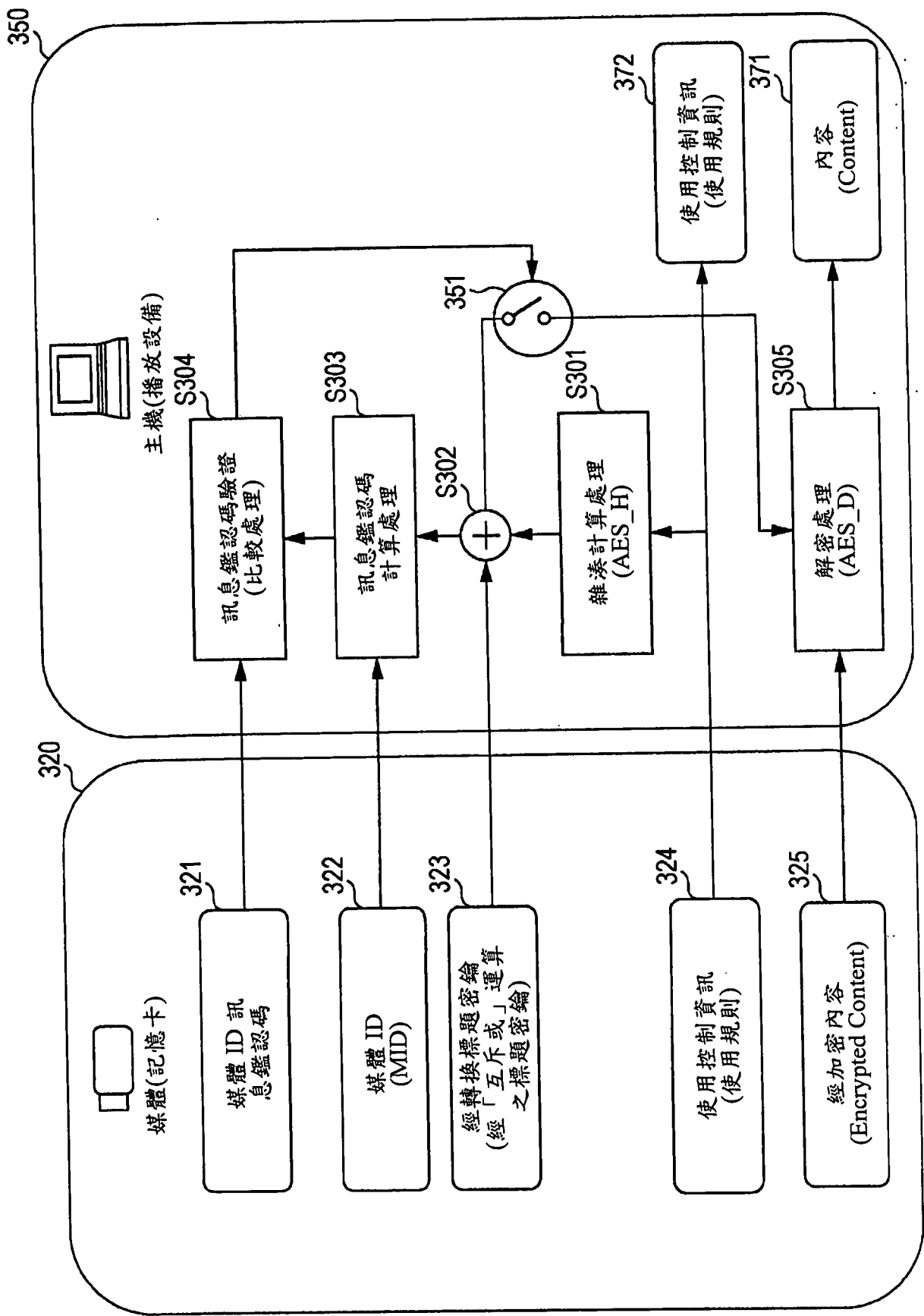


圖 16

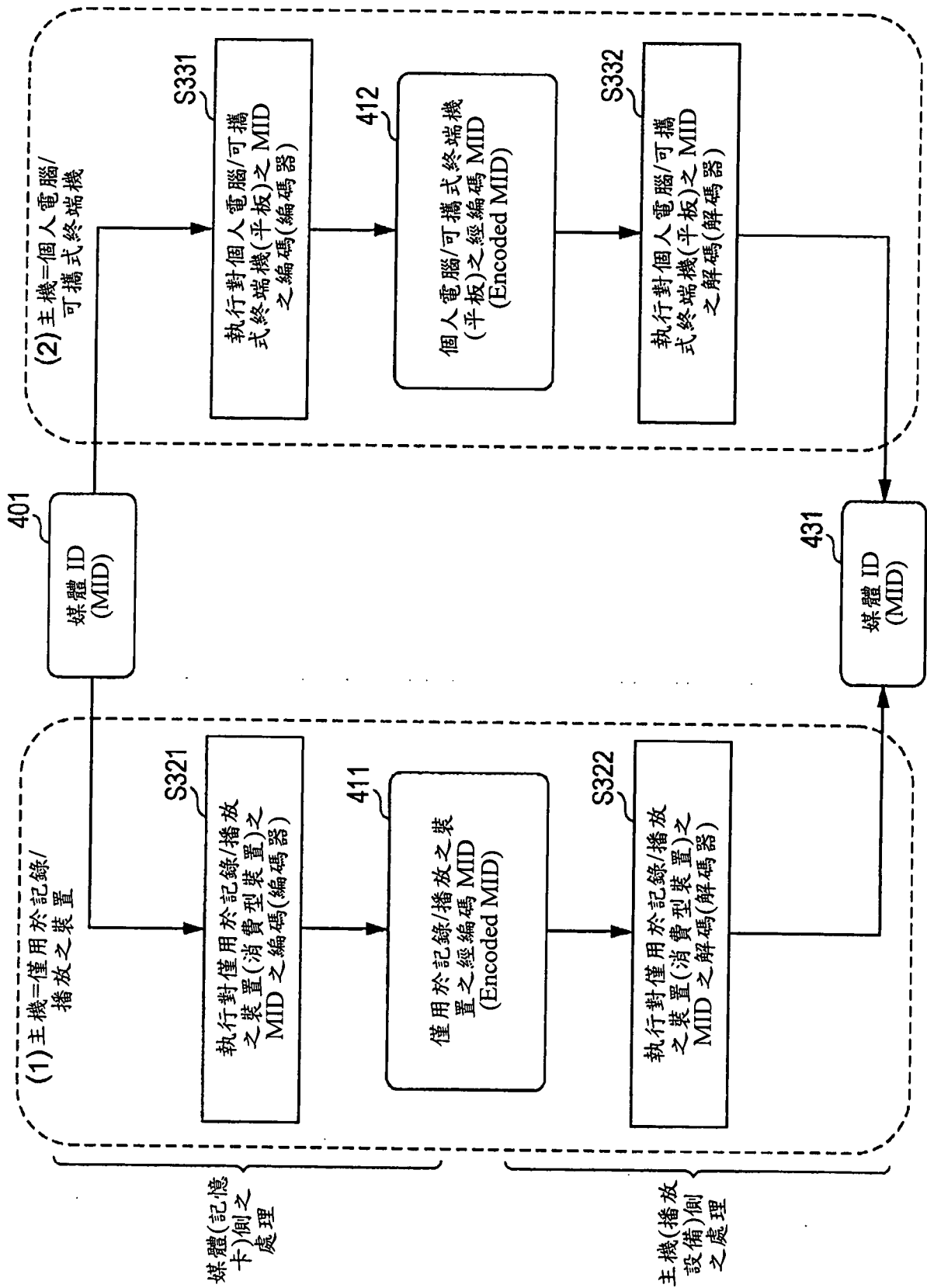
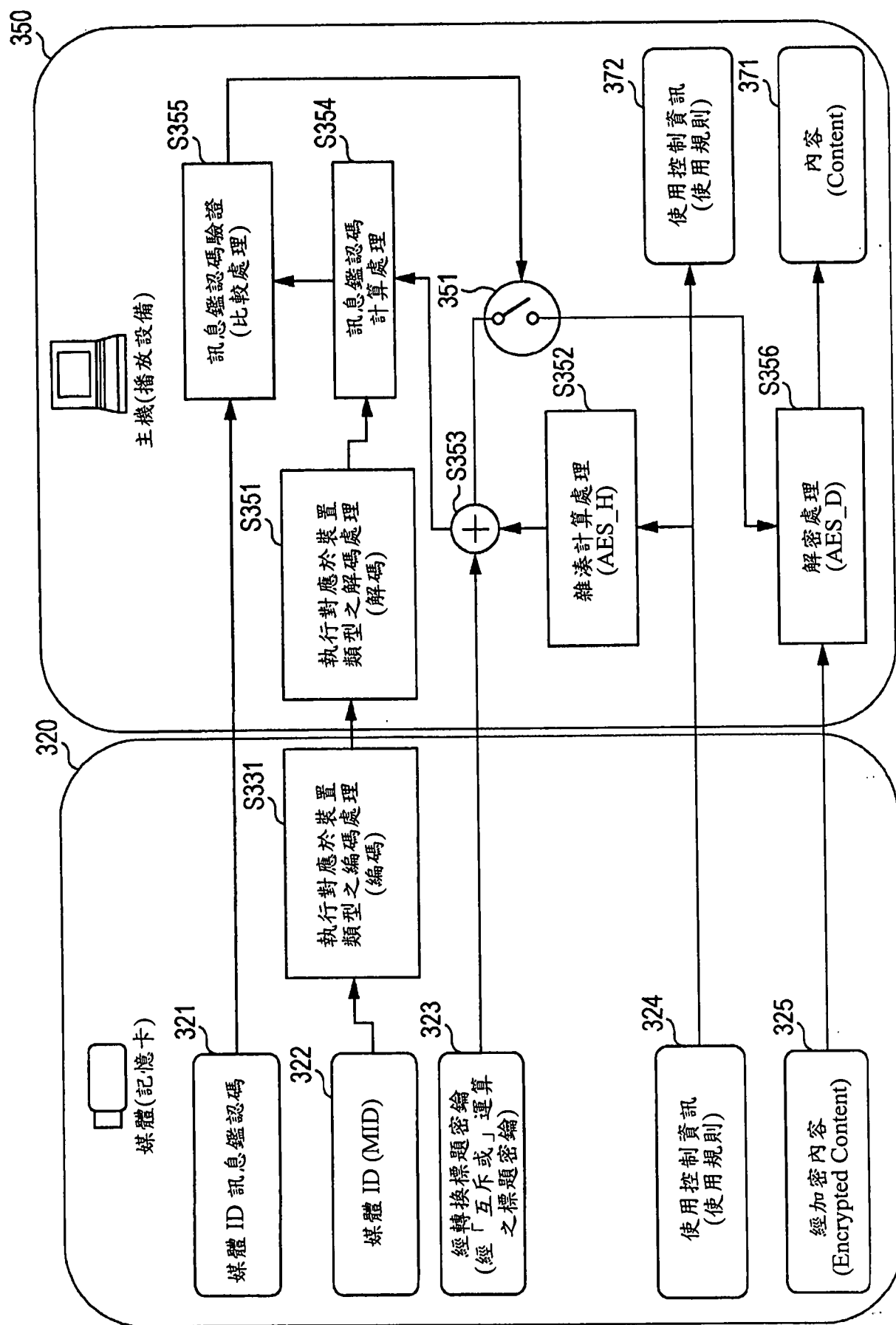


圖 17



18

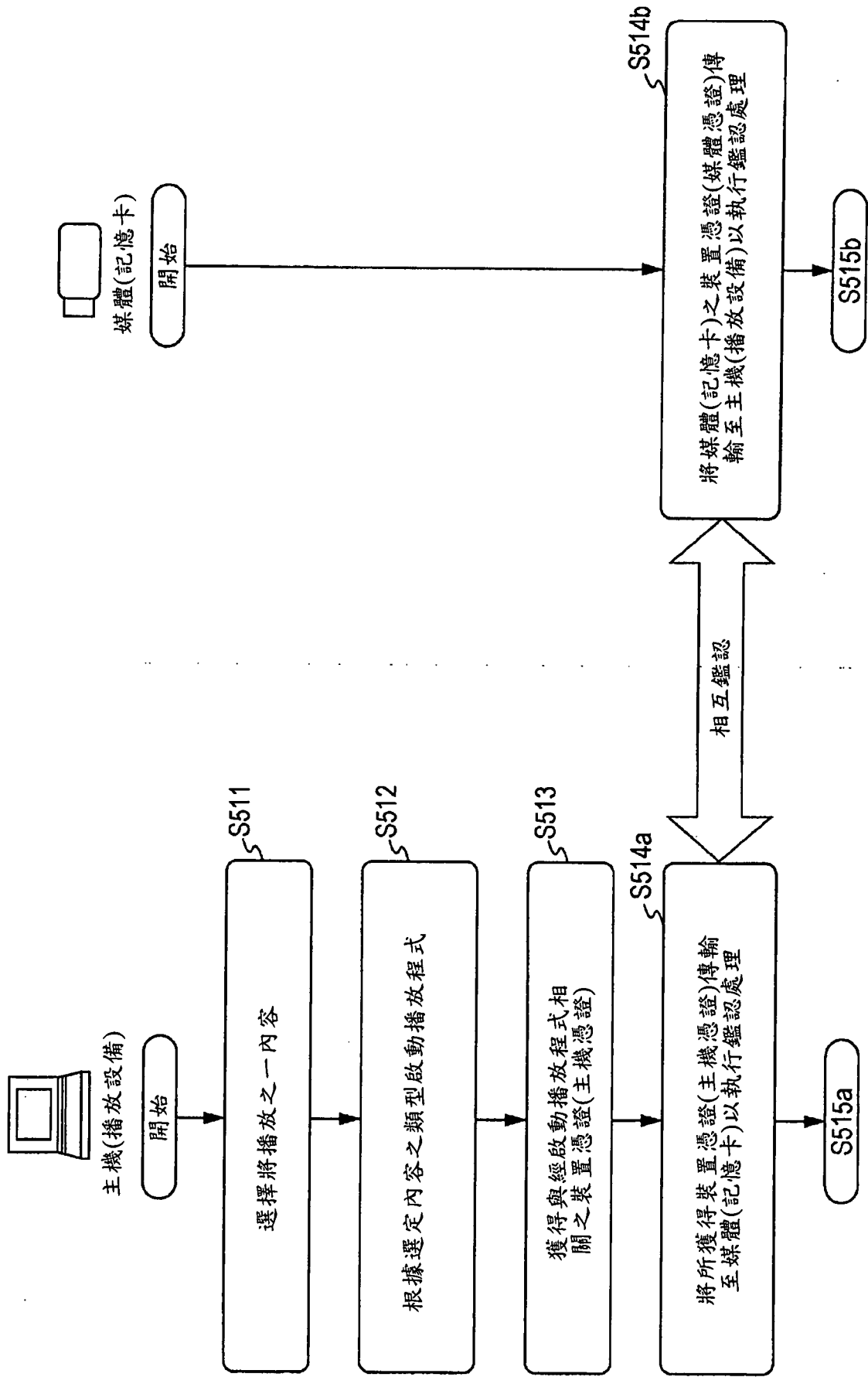


圖 19

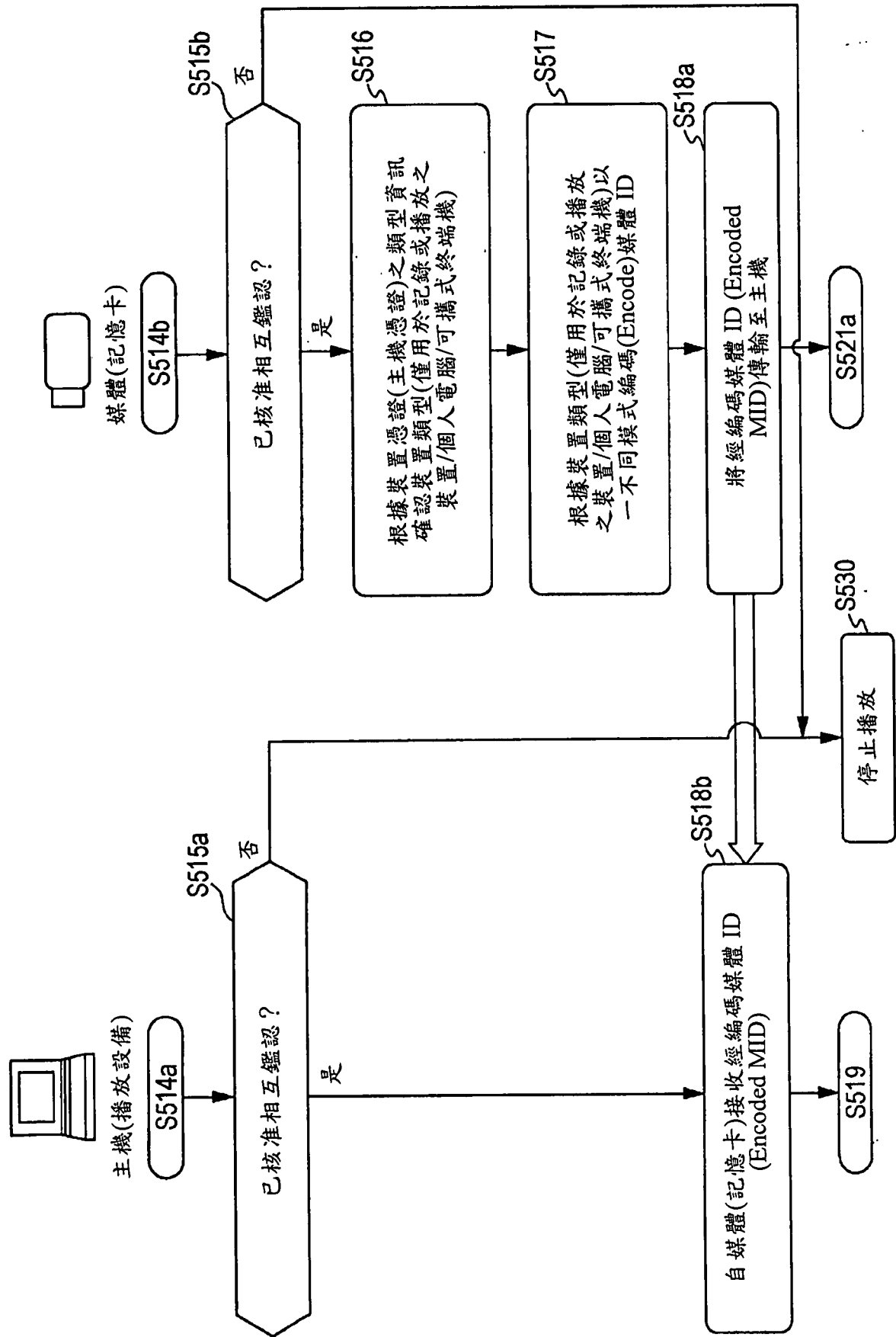


圖 20

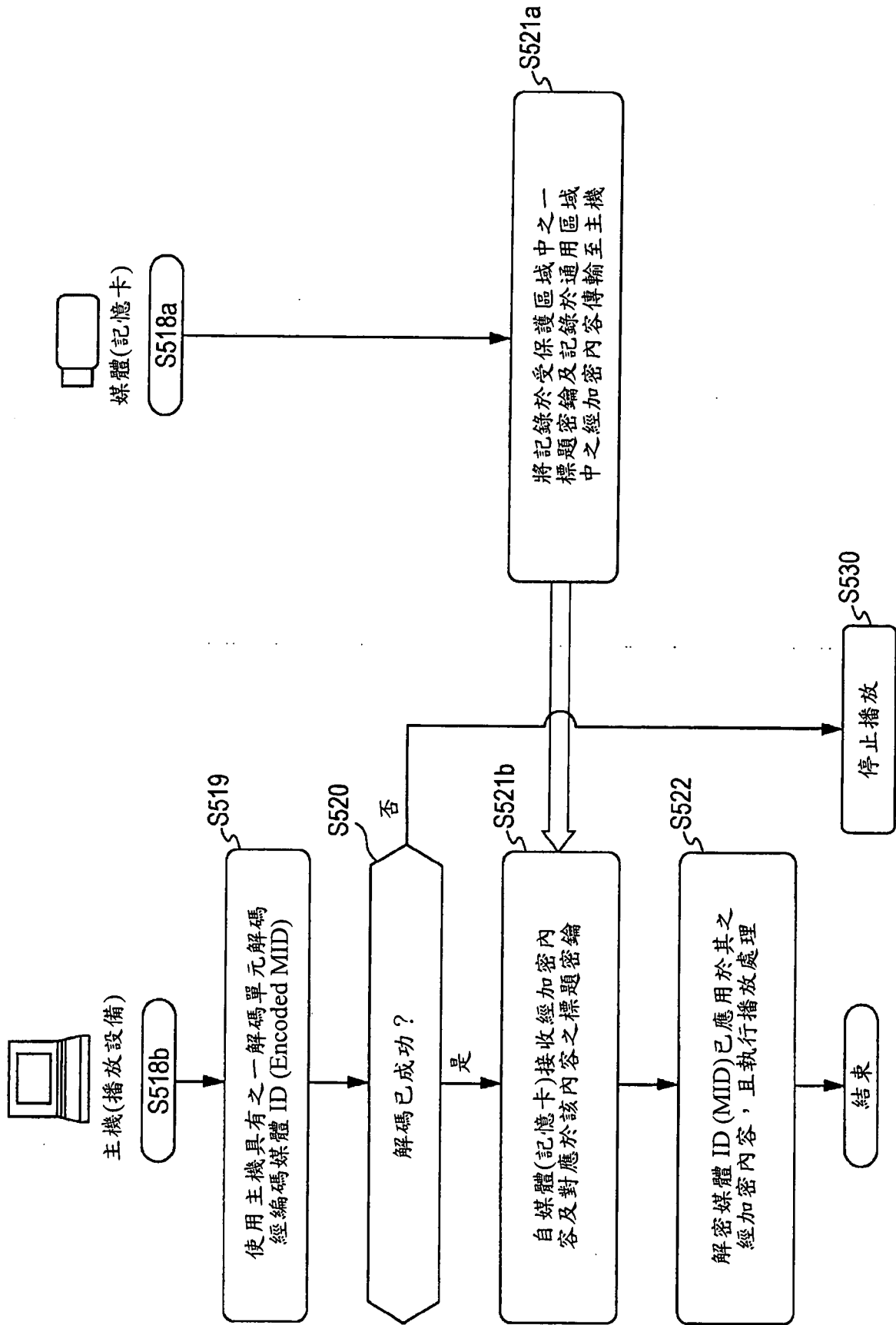


圖 21

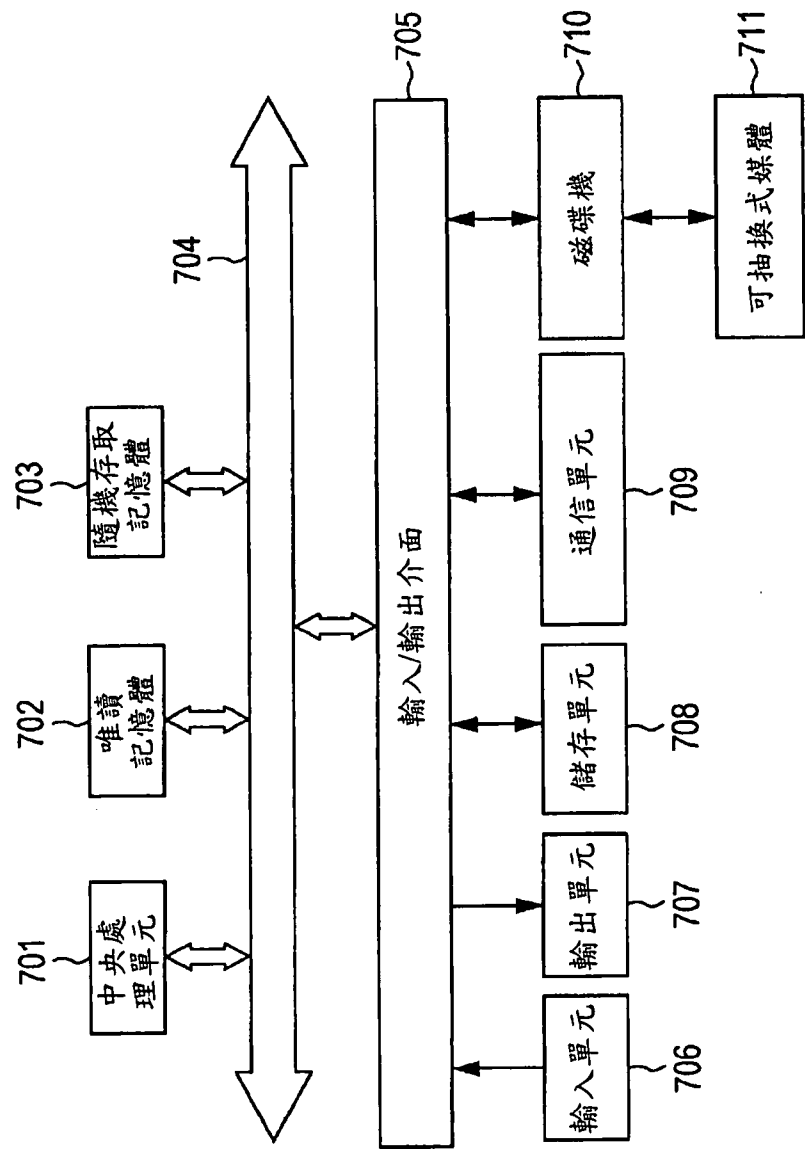


圖 22

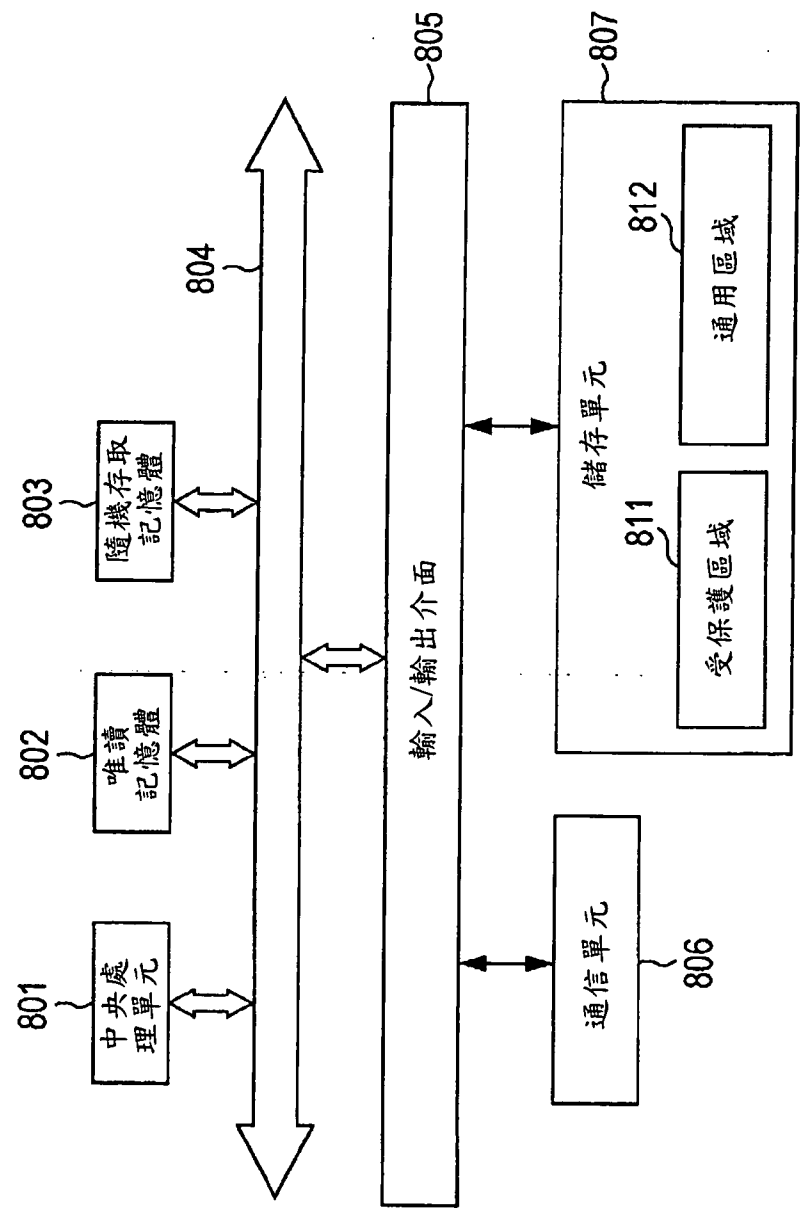


圖 23