

四、聲明事項：

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

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 日本；2004年02月04日；特願2004-027940

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係關於一種服務提供伺服器、資訊處理裝置、資料處理方法及電腦程式。具體為，關於一種可向用戶設備提供與內容相關之服務的服務提供伺服器、資訊處理裝置、資料處理方法及電腦程式，上述用戶設備係實行儲存有內容之碟片等資訊記錄媒體之再生處理者。

【先前技術】

音樂等聲頻資料、電影等圖像資料、遊戲程式、各種應用程式等種種軟體資料(以下將此等稱為內容(Content))係儲存於記錄媒體，例如DVD(Digital Versatile Disc，數位影音光碟)、MD(Mini Disc，迷你光碟)、CD(Compact Disc，光碟)或可使用藍色雷射光進行高密度記錄的碟片[藍光光碟(Blu-ray Disc)]等資訊記錄媒體，提供給用戶，用戶可使用PC(Personal Computer，個人電腦)、碟片播放器等用戶設備即再生裝置，將內容加以再生與利用。

進而，近年來採用有自與用戶設備網絡連接之伺服器向用戶提供與儲存於碟片等資訊記錄媒體之內容相關聯的各種服務之提供服務結構。

例如，碟片儲存內容為外文電影時，可自網絡連接之伺服器將相對於聲音之字幕資料或配音之聲音資料，或內容續集碟片之購買折扣券等各種內容相關服務提供至PC等用戶設備。

自伺服器提供之服務形體有各種各樣，存在對用戶不設

限制之服務形態，亦存在例如設定一定條件之服務提供形態，如一張記錄有服務相關內容之碟片1張僅可利用1次等。

儲存於碟片之內容即音樂資料、圖像資料等，通常多數內容因其作者或銷售商具有其發行權等，此等內容之使用會有一定使用限制，即，通常採取僅允許正規用戶使用內容，而未經允許則不可使用之形式。

因此，關聯內容而提供之服務最好亦構造為一種確認一定使用權限後，例如，以確認購買正規碟片之用戶為前提條件，方可提供服務之系統。

[發明所欲解決之問題]

本發明係鑒於上述問題點而開發完成者，其目的在於提供一種服務提供伺服器、資訊處理裝置、資料處理方法及電腦程式，其可於將內容儲存於DVD、CD、及藍色雷射光記錄媒體等各種資訊記錄媒體中而提供，進而，自網絡連接之服務提供伺服器進行服務提供處理之構造中，確認合法服務使用權限，排除非法之服務使用。

【發明內容】

本發明之第1方面，一種服務提供伺服器，其特徵為對應於來自資訊處理裝置之服務提供要求，實行服務提供處理，且具有資料接收部，其自資訊處理裝置接收帶有資訊記錄媒體ID及服務ID之服務要求，記憶部，其儲存每個上述資訊記錄媒體ID之服務提供狀況資料，作為每個與資訊記錄媒體之儲存內容標題相對應之標題固定值的服務管理

資料，及資料處理部，其實行介以上述資料接收部接收之資訊記錄媒體ID的驗證處理，以確認合法性為前提條件，依據該資訊記錄媒體ID取得標題固有值，自上述記憶部取得相應於標題固有值之服務提供狀況資料，根據上述資訊記錄媒體ID及上述服務ID判斷是否可提供特定之服務，於判定為可提供之前提條件下，實行服務提供處理。

進而，於本發明之服務提供伺服器之一個實施形態中，其中上述資料處理部構造為實行資訊記錄媒體ID中包含之署名資料之驗證處理作為資訊記錄媒體ID之驗證處理，根據資訊記錄媒體ID中所包含之標題固有值，或依據資訊記錄媒體ID中包含之資料進行運算而計算出之標題固有值，實行自上述記憶部取得對應標題固有值之服務提供狀況資料的處理。

進而，於本發明之服務提供伺服器之一個實施形態中，其中上述服務提供伺服器具有儲存非法資訊記錄媒體ID列表之廢止清冊的記憶部，上述資料處理部中資訊記錄媒體ID之驗證處理係藉由將自資訊處理裝置接收之資訊記錄媒體ID與上述廢止清冊中記錄之ID進行對照處理而實行。

進而，於本發明之服務提供伺服器之一個實施形態中，其中上述資訊記錄媒體ID包含與資訊記錄媒體之儲存內容標題相對應之標題固有值，及依據管理裝置之密鑰而產生之每個資訊記錄媒體各不相同的署名資料，上述資料處理部藉由對應上述資訊記錄媒體ID中包含之署名資料，產生適用上述管理裝置之公鑰的訊息並進行對照處理，而實行

上述資訊記錄媒體ID之驗證處理，並自上述記憶部取得與包含於資訊記錄媒體ID之標題固有值相對應之服務提供狀況資料。

進而，於本發明之服務提供伺服器之一個實施形態中，上述資訊記錄媒體ID包含對應於所製造之資訊記錄媒體張數 W 而設定之質數 $p(w)$ ，以及依據質數 $p(w)$ 、標題固有值進行運算而計算出之資料IDKey(w)，上述資料處理部構造為藉由判斷上述資訊記錄媒體ID中包含之資料是否為質數，進行ID驗證處理，並由資訊記錄媒體ID中包含之資料IDKey(w)計算標題固有值，自上述記憶部取得與所計算出之標題固有值相對應的服務提供狀況資料。

進而，本發明之第2方面，一種資訊處理裝置，其特徵為向服務提供伺服器提出服務提供要求，且具有記錄媒體介面，其實行資訊記錄媒體之存取處理，資料處理部，其對介以上述資訊記錄媒體介面，自資訊記錄媒體讀取之資訊記錄媒體ID進行驗證處理，並以已確認合法性為前提條件，向服務提供伺服器發送該資訊記錄媒體ID。

進而，於本發明之資訊處理裝置之一個實施形態中其中，上述資料處理部係藉由資訊記錄媒體ID中所包含之署名資料之驗證處理，實行資訊記錄媒體ID之驗證處理。

進而，於本發明之資訊處理裝置之一個實施形態中，其中上述資料處理部中資訊記錄媒體ID之驗證處理係採取自記憶部或資訊記錄媒體取得非法資訊記錄媒體ID列表之廢止清冊，將取得之廢止清冊中記錄的ID與自資訊處理裝置

接收之資訊記錄媒體ID進行對照處理之方式實行。

進而，於本發明之資訊處理裝置之一個實施形態中，其中上述資訊記錄媒體ID包含與資訊記錄媒體之儲存內容標題相對應之標題固有值，及依據管理裝置之密鑰而產生之每個資訊記錄媒體各不相同的署名資料，上述資料處理部藉由對應上述資訊記錄媒體ID中包含之署名資料，產生適用上述管理裝置之公鑰的訊息並進行對照處理，而實行上述資訊記錄媒體ID之驗證處理。

進而，於本發明之資訊處理裝置之一個實施形態中，其中上述資訊記錄媒體ID包含對應於所製造之資訊記錄媒體張數 W 而設定之質數 $p(w)$ 、以及依據質數 $p(w)$ 與標題固有值進行運算而計算出之資料IDKey(w)，上述資料處理部藉由判斷上述資訊記錄媒體ID中包含之資料是否為質數，從而進行ID驗證處理。

進而，本發明之第3方面，一種資料處理方法，其特徵為對應於來自資訊處理裝置之服務提供要求實行處理，且具有資料接收步驟，其自資訊處理裝置接收帶有資訊記錄媒體ID及服務ID之服務要求，及資料處理步驟，其實行接收之資訊記錄媒體ID的驗證處理，以已確認合法性為前提條件，依據該資訊記錄媒體ID取得標題固有值，自記憶部獲得與取得之標題固有值相對應的服務提供狀況資料，依據上述資訊記錄媒體ID及上述服務ID判斷是否可以提供特定服務，於判定為可提供之前提條件下，實行服務提供處理，上述記憶部儲存上述每個資訊記錄媒體ID之服務提供

狀況資料，作為每個與資訊記錄媒體之儲存內容標題相對應之標題固定值的服務管理資料。

進而，於本發明之資料處理部之一個實施形態中，其構造為，上述資料處理步驟包含以下步驟：藉由資訊記錄媒體ID中包含之署名資料的驗證處理，進行資訊記錄媒體ID之驗證處理，根據資訊記錄媒體ID中所包含之標題固有价值，或依據資訊記錄媒體ID中包含之資料進行運算而計算出之標題固有价值，實行自上述記憶部取得對應標題固有价值之服務提供狀況資料之處理。

進而，本發明之資料處理部之一個實施形態中，其中上述資料處理步驟中之資訊記錄媒體ID的驗證處理包含以下步驟：藉由進行自資訊處理裝置接收之資訊記錄媒體ID與記錄於非法資訊記錄媒體ID列表之廢止清冊之ID的對照處理之方式進行上述資訊記錄媒體ID之驗證處理。

進而，於本發明之資料處理方法之一個實施形態中，其中上述資訊記錄媒體ID包含與資訊記錄媒體之儲存內容標題相對應之標題固有价值，及依據管理裝置之密鑰而產生之每個資訊記錄媒體各不相同的署名資料，上述資料處理步驟包含以下步驟：藉由對應上述資訊記錄媒體ID中包含之署名資料，產生適用上述管理裝置之公鑰的訊息並進行對照處理，而實行上述資訊記錄媒體ID之驗證處理，並且自上述記憶部取得與包含於資訊記錄媒體ID之標題固有价值相對應之服務提供狀況資料。

進而，於本發明之資料處理方法之一個實施形態中，其

中上述資訊記錄媒體ID包含對應於所製造之資訊記錄媒體的張數 W 而設定之質數 $p(w)$ 、以及依據質數 $p(w)$ 與標題固有值進行運算而計算出之資料IDKey(w)，上述資料處理步驟包含以下步驟：藉由判斷上述資訊記錄媒體ID中包含之資料是否為質數，進行ID驗證處理，並由資訊記錄媒體ID中包含之資料IDKey(w)計算標題固有值，自上述記憶部取得與所計算出之標題固有值相對應的服務提供狀況資料。

進而，本發明之第4方面，一種資料處理方法，其特徵為向服務提供伺服器提出服務提供要求，且具有資訊記錄媒體存取步驟，其介以上述媒體介面，實行資訊記錄媒體之存取處理資料處理步驟，其對介以上述資訊記錄媒體之介面，自資訊記錄媒體讀取之資訊記錄媒體ID進行驗證處理，並以已確認合法性為前提條件，向服務提供伺服器發送該資訊記錄媒體ID。

進而，於本發明之資料處理方法之一個實施形態中，上述資料處理步驟係藉由資訊記錄媒體ID中所包含之署名資料之驗證處理進行資訊記錄媒體ID之驗證處理。

進而，於本發明之資料處理方法之一個實施形態中，包含以下步驟：上述資料處理步驟中資訊記錄媒體ID之驗證處理採取自記憶部或資訊處理媒體取得非法資訊記錄媒體ID列表之廢止清冊，將取得之廢止清冊中記錄的ID與自資訊處理裝置接收之資訊記錄媒體ID進行對照處理之方式實行。

進而，於本發明之資料處理方法之一個實施形態中，其

中上述資訊記錄媒體ID包含與資訊記錄媒體之儲存內容標題相對應之標題固有值，及依據管理裝置之密鑰而產生之每個資訊記錄媒體各不相同的署名資料，上述資料處理步驟包含以下步驟：藉由對應上述資訊記錄媒體ID中包含之署名資料，產生適用上述管理裝置之公鑰的訊息並進行對照處理，而實行上述資訊記錄媒體ID之驗證處理。

進而，於本發明之資料處理方法之一個實施形態中，其中上述資訊記錄媒體ID包含對應於所製造之資訊記錄媒體張數 W 而設定之質數 $p(w)$ 、以及依據質數 $p(w)$ 與標題固有值進行運算而計算出之資料IDKey(w)，上述資料處理步驟包含以下步驟：藉由判斷上述資訊記錄媒體ID中包含之資料是否為質數，進行ID驗證處理。

進而，本發明之第5方面，一種電腦程式，其特徵為對應於來自資訊處理裝置之服務提供要求實行處理，且具有資料接收步驟，其自資訊處理裝置接收帶有資訊記錄媒體ID及服務ID之服務要求，及資料處理步驟，其實行接收之資訊記錄媒體ID的驗證處理，於已確認合法性為前提條件，依據該資訊記錄媒體ID取得標題固有值，自記憶部獲得與取得之標題固有值相對應的服務提供狀況資料，根據上述資訊記錄媒體ID及上述服務ID判斷是否可以提供特定服務，於判定為可提供之前提條件下，實行服務提供處理，上述記憶部儲存上述每個資訊記錄媒體ID之服務提供狀況資料，作為每個與資訊記錄媒體之儲存內容標題相對應之標題固定值的服務管理資料。

進而，本發明之第6方面，一種電腦程式，其特徵為向服務提供伺服器提出服務提供要求，且具有資訊記錄媒體存取步驟，其介以記錄媒體介面，實行資訊記錄媒體之存取處理，及資料處理步驟，其對介以上述資訊記錄媒體之介面，自資訊記錄媒體讀取之資訊記錄媒體ID實行驗證處理，並以已確認合法性為條件，向該資訊記錄媒體ID之服務提供伺服器實行發信處理。

另，本發明之電腦程式係例如可藉由記憶媒體、通訊媒體、CD或FD、MO等記錄媒體、或網絡等通訊媒體，以電腦可讀取之形式向各種可實行程式代碼之電腦系統提供的電腦程式。藉由以電腦可讀取之形式提供此種程式，可實現於電腦系統上進行相應於程式之處理。

本發明之進而其他目的、特徵或優點，透過依據以下本發明之實施例或附圖之說明將清楚明瞭。另，本說明書中所謂之系統係指複數個裝置之邏輯集合構造，各構造之裝置並非一定存在於同一框體內。

[發明之效果]

藉由本發明之構造，於將內容儲存至DVD、CD、藍色雷射光記錄媒體等各種資訊記錄媒體而提供，進而自網絡連接之服務提供伺服器進行服務提供處理之構造中，於服務提供伺服器側，驗證由資訊處理裝置(用戶設備)發送之資訊記錄媒體ID，依據每個資訊記錄媒體ID之服務提供狀況資料提供服務，因此發送服務要求之資訊處理裝置係自資訊記錄媒體讀取合法資訊記錄媒體ID之資訊處理裝置，

僅當依據服務提供狀況資料確認該服務提供係允許之服務時，方提供服務。

進而，根據本發明之構造，儲存於資訊記錄媒體中之資訊記錄媒體ID包含可確認管理裝置之署名資料等之合法性的資料，又，包含是否具有或是否可計算出標題固有值之資料，因此於服務提供伺服器中，可依據包含於資訊記錄媒體ID之資料，確認合法性，並取得標題固有值，指定對應於標題固有值而設定之服務提供狀況資料。

【實施方式】

以下，參照圖示，說明本發明之服務提供伺服器、資訊處理裝置及資料處理方法，以及電腦程式之具體內容。

另，說明按照以下項目進行。

1. 資訊記錄媒體之儲存資料
2. 內容儲存資訊記錄媒體之提供及使用管理構造
3. 構成服務提供伺服器及用戶設備之資訊處理裝置的構造
4. 用戶設備處理之具體內容
5. 服務提供伺服器處理之具體內容

[1. 資訊記錄媒體之儲存資料]

圖1表示資訊記錄媒體之資料記錄構造例。圖1係說明CD(Compact Disc，光碟)、DVD(Digital Versatile Disc，數位影音光碟)、MD(Mini Disc，迷你光碟)、藍光碟片(Blu-ray Disc)、快閃記憶體等各種資訊記錄媒體100之儲存資料的圖。圖1係以碟片狀媒體為例表示，但本發明並非僅限於碟片狀媒體，可適用於快閃記憶體等各種資訊記

錄媒體。

資訊記錄媒體100中儲存有圖1所示之資訊，即，碟片ID 101、內容102、碟片ID廢止清冊(DIRL:Disc ID Revocation List)103、密鑰資訊(EKB: Enabling Key Block)104。

碟片ID 101例如係碟片固有之識別符，以難以刪除或改寫之方式儲存。另，於本發明中，碟片ID 101包含對應於資訊記錄媒體100中儲存之內容102之各標題的固有价值(標題固有价值)，每個資訊記錄媒體100之固有价值(碟片固有价值)，以及表示其合法性之資訊，例如署名等資訊(合法性驗證值)等。關於碟片ID之具體內容將稍後說明。

另，於以下說明之實施例中，表示以碟片狀媒體作為內容儲存資訊記錄媒體之例，因此將其識別符作為碟片ID加以說明。當將快閃記憶體等各種資訊記錄媒體作為內容儲存資訊記錄媒體使用時，設定對應於碟片ID之資訊記錄媒體ID。

於資訊記錄媒體100中，進而儲存內容102。內容例如作為加密內容儲存。作為加密內容時，用以解密內容之密鑰資訊儲存於資訊記錄媒體100中，或透過網絡提供。

於資訊記錄媒體100中進而儲存有碟片ID廢止清冊(DIRL:Disc ID Revocation List)103。碟片ID廢止清冊(DIRL:Disc ID Revocation List)103係當發現被認定為非法拷貝等之碟片，例如於市場上發現儲存有非法拷貝內容之CD-R時，自該非法CD-R中將內容以及被拷貝之碟片ID提

取並列表化之資料。碟片ID廢止清冊(DIRL:Disc ID Revocation List)103之產生、管理、對碟片製造者進行列表資訊之提供等由特定之可靠管理局(CA: Central Authority, 中央權威機構)進行。

參照圖2說明碟片ID廢止清冊(DIRL:Disc ID Revocation List)103之資料構造。碟片ID廢止清冊(DIRL:Disc ID Revocation List)150如圖2所示, 包含自創建列表(DIRL:Disc ID Revocation List)時開始單調增加之版本編號151, 羅列應排除之碟片ID的廢止碟片ID清冊152, 以及作為對應於版本編號151與廢止碟片ID清冊152之篡改驗證值153的認證符。篡改驗證值153係用於判斷對象資料, 此處為用以判斷版本編號151與廢止碟片ID清冊152是否被篡改之資料, 使用利用公鑰加密技術之數位署名或利用對稱密鑰加密技術之訊息認證代碼(MAC: Message Authentication Code, 訊息認證碼)。

當採用公鑰加密技術之數位署名作為篡改驗證值153使用時, 再生機器取得可靠機關例如上述管理局(CA: Central Authority, 中央權威機構)之署名驗證密鑰(公鑰), 根據各再生機器所取得之署名驗證密鑰(公鑰), 驗證使用管理局(CA: Central Authority, 中央權威機構)之署名產生鑰(密鑰)而創建的署名, 藉此可判斷版本編號151與廢止碟片ID清冊152有無篡改過。

參照圖3說明使用訊息認證代碼(MAC: Message Authentication Code)作為篡改驗證值153時之MAC產生、

驗證處理。訊息認證代碼(MAC：Message Authentication Code)係作為資料篡改驗證用途之資料而產生者，於MAC產生處理、驗證處理態樣中可表現為各種態樣，圖3所示為其一例，即使用DES加密處理構造之MAC值產生例。

如圖3所示，將對象訊息，此處為圖2所示之版本編號151與廢止碟片ID清冊152以8位元組為單位分割(以下，將分割之訊息表示為M1、M2、．．．、MN)，首先，計算初始值(Initial Value(以下表示為IV))與M1之異或邏輯和(結果表示為I1)。繼而，放置I1至DES加密部，使用密鑰(以下表示為K1)進行加密(輸出表示為E1)。接著，計算E1及M2之異或邏輯和，將其輸出I2放置於DES加密部，使用密鑰K1進行加密(輸出為E2)。之後重複此步驟，對所有訊息進行加密處理。最後輸出之EN即成為訊息認證代碼(MAC：Message Authentication Code)。

MAC值當其產生源資料變更時，便會成為不同值，因此將依據驗證對象之資料(訊息)而產生之MAC與記錄之MAC進行比較，當一致時，則證明驗證對象之資料(訊息)未被變更、篡改。

返回圖1，繼續說明資訊記錄媒體100之儲存資料。資訊記錄媒體100中進而儲存有密鑰資訊(EKB：Enabling Key Block)104。

參照圖式說明使用密鑰資訊(EKB)之秘密資訊提供構造。圖4最下段所示之編號0~15係用戶設備，其例如作為進行內容使用之資訊處理裝置。即，圖4所示之多層樹

(tree)狀結構之各葉部(leaf)相當於各設備。

各設備0~15於製造時、出廠時或出廠之後，於記憶體中儲存密鑰組(設備密鑰(DNK: Device Node Key))，其包含分配於多層樹(tree)狀構造中由自身葉至根之節點的密鑰(節點密鑰)，以及各葉部之葉部密鑰。圖4最下段所示之K0000~K1111係分別分配至各設備0~15之葉部密鑰，自最上段KR(根密鑰)至從最下段往上第2個節(節點)所記載的密鑰：KR~K111為節點密鑰。

於圖4所示之樹狀構造中，例如設備0具有葉部密鑰K0000與節點密鑰：K000、K00、K0、KR作為設備密鑰。設備5具有K0101、K010、K01、K0、KR。設備15具有K1111、K111、K11、K1、KR。另，於圖4之樹中，僅表示有設備0~15之16個，樹狀構造中亦僅僅表示為均衡4段構造之左右對稱結構，但樹中可構造更多之設備，此外，於樹之各部分中，可具有不同之段數構造。

又，圖4之樹狀構造中所包含之各設備中，包含各種記錄媒體，例如使用設備嵌入型或構造為可自由裝卸於設備的DVD、CD、MD、快閃記憶體等的各種類型設備。進而，各種應用服務可共同存在。此種不同設備、不同應用程式共存之構造可使用圖4所示之內容或密鑰分佈構造之多層樹狀構造。

於此等各種設備、應用程式共存之系統中，例如將圖4之虛線範圍內的部分，即設備0、1、2、3作為一個組進行設定。例如，僅此虛線包圍之組中所包含之設備具有儲存

於資訊記錄媒體之加密內容的合法使用權即授權。此時，僅設備0、1、2、3設定有可取得用於內容解密之密鑰的EKB，並將其儲存至存有加密內容之資訊記錄媒體。

由圖4可知，一個組中所包含之三個設備0、1、2、3具有作為儲存於各設備之設備密鑰(DNK：Device Node Key)的共用密鑰K00、K0、KR。

此時，僅設備0、1、2可取得用於內容解密之內容密鑰Kcon的EKB之構造為例如圖5所示之構造。即，EKB將內容及加密資料設定為000、 $\text{Enc}(K000, Kcon)$ 及0010、 $\text{Enc}(K0010, Kcon)$ 。

另， $\text{Enc}(Kx, Ky)$ 代表將資料Ky以密鑰Kx加密之加密資料。此時，設備0、1可使用自身持有之設備密鑰[K000]進行標記[000]之加密資料的解密，又，設備2可使用設備密鑰[K0010]進行上述EKB中標記[0010]之加密資料的解密，藉由分別對加密資料進行解密處理而取得內容密鑰Kcon。其他設備不具備設備密鑰[K000]、[K0010]中任何一者，即使收到具有圖5所示之構造的EKB，亦無法將EKB解密而取得內容密鑰。

如此，EKB藉由使構造資料對應於持有授權之設備，因此可構造為密鑰資訊組塊，該密鑰資訊組塊係將僅可於任意選擇之設備進行處理的內容密鑰等秘密資訊僅向特定設備提供。密鑰資訊(EKB)發佈中心104產生僅於允許使用內容之設備方可進行處理之EKB，並提供至資訊記錄媒體製造實體103。資訊記錄媒體製造實體103將此EKB連同加密

內容一起儲存於資訊記錄媒體110，並向用戶提供。

[2.內容儲存資訊記錄媒體之提供及使用管理構造]

圖6係說明儲存有上述各種資料之資訊記錄媒體200之提供及利用管理構造的圖。

如圖6所示，於內容提供及管理構造中，存在有管理局(CA：Central Authority，中央權威機構)所使用之管理裝置201，內容提供商使用之內容提供裝置203，碟片製造者所使用之碟片製造裝置202，用戶使用之進行內容再生處理之資訊處理裝置(用戶設備)400，以及服務提供伺服器300，該服務提供伺服器300向資訊處理裝置(用戶設備)400實行相應於資訊記錄媒體200中所儲存內容之服務，例如字幕資訊之提供處理等。

管理裝置201產生上述碟片ID與碟片ID廢止清冊(DIRL)並提供至碟片製造裝置202。又，內容提供裝置203將加密內容與有效化密鑰組塊(EKB)提供至碟片製造裝置202。

碟片製造裝置202製造資訊記錄媒體200，該資訊記錄媒體200記錄有自管理裝置201接收之碟片ID及碟片ID廢止清冊(DIRL)、自內容提供裝置203接收之加密內容資料以及有效化密鑰組塊(EKB)。

用戶例如購入資訊記錄媒體200，安裝於資訊處理裝置(用戶設備)400。資訊處理裝置(用戶設備)400驗證記錄於資訊記錄媒體200之碟片ID為合法，並確認該碟片ID不存在於廢止清冊DIRL內後，可依據自身之設備節點密鑰DNK，自有效化密鑰組塊EKB取得適當之內容密鑰資料，

將加密內容資料解密，進行再生。

進而，資訊處理裝置(用戶設備)400將記錄於資訊記錄媒體200之碟片ID以及作為服務識別符之服務ID發送至服務提供伺服器300，於服務提供伺服器300驗證碟片ID之合法性，進而依據服務提供伺服器300所具有之服務提供狀況資料，判斷可否提供服務，當碟片ID合法，並依據服務提供狀況資料判斷可提供服務時，向資訊處理裝置(用戶設備)400實行服務提供處理。

[3.構成服務提供伺服器及用戶設備之資訊處理裝置的構造]

繼而，說明構成服務提供伺服器及用戶設備之資訊處理裝置的構造。

圖7係圖6所示之服務提供伺服器的構造圖。如圖7所示，服務提供伺服器300具有例如包含CPU等之控制器302，實行各種運算處理之運算單元303，向資料輸入裝置或資料輸出裝置進行資料之輸入輸出及用於透過網絡進行資料輸入輸出之作為介面的輸入輸出介面(I/F)304，安全記憶體305，以及主記憶體306。此等介以匯流排301而連接。

主記憶體306將運算單元303及控制器302之處理所用各種資料中的安全級別低之資料加以記憶。安全記憶體305將運算單元303及控制器302之處理所用各種資料中的安全級別高之資料加以記憶。安全記憶體305例如記憶自圖6所示之管理裝置201接收之碟片ID等。

輸入輸出介面304例如連接於未圖示之操作機構或網絡

等，自圖6所示之管理裝置201或內容提供裝置203接收各種資料，並與接受服務提供之資訊處理裝置(用戶設備)400進行通訊，提供服務。

運算單元303依據控制器302之控制，實行各種運算，如產生署名資料之驗證用資料等。控制器302例如實行判斷是否允許向用戶設備提供服務之確認處理程式，以及服務提供程式等各種程式。

服務提供伺服器300介以輸入輸出介面(I/F)304，定期或以事件為單位自管理裝置201、內容提供裝置203或其他裝置接收碟片ID廢止清冊，因而於安全記憶體305總是保存最新版碟片ID廢止清冊。

又，介以輸入輸出介面(I/F)304，自內容提供裝置203或其他裝置接收每個標題之標題固有值，以及用於識別所提供之服務的服務識別資訊，並將以標題為單位管理服务提供狀況資料之服務提供狀況資料庫儲存於安全記憶體305。

所謂標題係指資訊處理裝置(用戶設備)400所安裝之資訊記錄媒體200中儲存的內容所對應之標題。

服務提供狀況資料庫之資料構造例如圖8所示。服務提供狀況資料庫如圖8所示，儲存有與服務提供伺服器300所提供之服務相對應之內容的標題識別資訊，以及設定於每個標題固有值，儲存有該標題之內容的碟片之各碟片ID的各服務提供狀況。

例如圖8(a)所示之服務提供狀況資料係關於

標題識別資訊：aaaa

標題固有值：bbbb

之服務提供狀況資料，

此與標題相應之內容所對應之服務1與服務2將記錄對於服務提供要求此前已提供幾次服務，上述服務提供要求係依據碟片ID1與碟片ID2之各碟片而提出者。

另，於圖8(a)所示之服務提供狀況資料中，固定為服務1係每個碟片ID1僅可提供一次之服務，服務2係每個碟片ID1可提供5次之服務。

服務提供伺服器300將圖8所示之服務提供狀況資料儲存並保持於例如安全記憶體305，對應於資訊處理裝置(用戶設備)400提出之與碟片ID相隨之服務提供要求，服務提供要求設備實行確認處理，判斷其是否為依據合法碟片ID之服務要求，進而僅當依據圖8所示之服務提供狀況資料，判斷未到達服務提供所允許之上限時，方提供服務。

服務提供伺服器300當收到資訊處理裝置(用戶設備)400提出之與碟片ID相隨之服務提供要求時，確認自資訊處理裝置(用戶設備)400發送之碟片ID的合法性，並確認於服務提供伺服器300所具有之廢止清冊中，自資訊處理裝置(用戶設備)400發送之碟片ID未被廢止。

進而，對依據已確認合法性之碟片ID之標題固有值實行確認或取出，及標題固有值之取出等處理。服務提供伺服器300依據取得之標題固有值，自圖8所示之儲存有服務提供狀況資料之資料庫指定相應標題之服務提供狀況資料，

並依據該資料檢查是否可以提供服務。即，依據圖8所示之服務提供狀況資料，僅於未到達服務提供之允許上限之情形下，方提供服務。

另，於圖8所示之服務提供狀況資料之構造例中，係以每個碟片ID均儲存服務提供狀況之資料為例說明，但亦可取代碟片ID，採取使用碟片固有值之構造，該碟片固有值用以識別各碟片。

另，於服務提供伺服器300向資訊處理裝置(用戶設備)400提供服務時，實行圖8所示之更新服務提供狀況資料之處理。

以下，參照圖9說明資訊處理裝置(用戶設備)400之構造。

如圖9所示，資訊處理裝置(用戶設備)400例如具有輸入輸出介面402，產生MPEG(Moving Picture Experts Group，運動圖像專家組)等各種符號化資料及將其解密之編解碼器403，具備A/D·D/A轉換器405之輸入輸出介面404，加密處理部406，ROM(Read Only Memory，唯讀記憶體)407，控制器408，記憶體409，以及用以存取於資訊記錄媒體200之記錄媒體介面410，此等藉由匯流排401互相連接。

輸入輸出介面402接收自網絡等外部供給之數位訊號，輸出至匯流排401上，並接收匯流排401上之數位訊號，輸出至外部。

編解碼器403將介以匯流排401供給之例如MPEG符號化

之資料解碼，輸出至輸入輸出介面404，並將自輸入輸出介面404供給之數位訊號編碼並輸出至匯流排401上。

輸入輸出介面404內置有A/D、D/A轉換器405。輸入輸出介面404接收自外部供給之類比訊號，以A/D、D/A轉換器405進行A/D(Analog Digital，類比數位)轉換，藉此將其作為數位訊號輸出至編解碼器403，並以A/D、D/A轉換器405將來自編解碼器403之數位訊號進行D/A(Digital Analog，類比數位)轉換，藉此將其作為類比訊號輸出至外部。

加密處理部406例如包含1個晶片之LSI，具有將透過匯流排401供給之例如內容等數位訊號加密，或解密，並輸出至匯流排401上之構造。另，加密處理部406並非僅限於1個晶片LSI，亦可藉由組合各種軟體或硬體之構造而實現。

ROM 407例如記憶有每個作為用戶設備之資訊處理裝置所固有的，或每個包含複數個資訊處理裝置(用戶設備)之組所固有的作為設備密鑰資料之葉部密鑰資料，以及複數個再生裝置或複數個組所共用的作為設備密鑰資料之節點密鑰資料。此等適用於上述作為密鑰資訊之有效化密鑰組塊(EKB)的解密處理。

控制器408包含例如CPU等，其實行記憶於記憶體409之程式。控制器408匯總控制資訊處理裝置(用戶設備)400之處理。即，資訊處理裝置(用戶設備)400之功能(處理)由控制器408所實行之程式而定。

記憶體409以自資訊記錄媒體200安全讀取之狀態儲存上述碟片ID廢止清冊(DIRL)。例如，較好的是依據設定於資訊處理裝置(用戶設備)400之ID實施加密並儲存於記憶體，藉此作為具有反篡改之資料加以儲存。如此，可將碟片ID廢止清冊(DIRL)儲存而不易於外部被刪除，或篡改內容，或被替換為舊版本之清冊。記錄媒體介面410用以存取於資訊記錄媒體200。

[4.用戶設備處理之具體內容]

以下說明作為用戶設備之資訊記錄媒體400自服務提供伺服器300接收服務時之處理的具體內容。

圖10係說明圖9所示之資訊處理裝置(用戶設備)400安裝資訊記錄媒體，自服務提供伺服器接受服務時實行之順序的流程圖。

於步驟S101中，當資訊記錄媒體200安裝於特定存取位置時，資訊處理裝置(用戶設備)400介以記錄媒體介面410，自資訊記錄媒體200讀取碟片ID，並將其儲存於記憶體409。

於步驟S102中，資訊處理裝置(用戶設備)400之控制器408讀出儲存於記憶體409中之碟片ID，檢查其合法性以及有無被篡改。關於該檢查處理，將稍後詳細說明。

於步驟S103中，控制器408於步驟S102中判斷上述碟片ID為合法時，進入步驟S105之處理，否則進入步驟S104，於步驟S104中，控制器408停止(禁止)記錄於資訊記錄媒體200之加密內容的解密及再生。

當判定碟片ID合法時，於步驟S105中，控制器408介以記錄媒體介面410，自資訊記錄媒體200讀取碟片ID廢止清冊(DIRL)。接著，當作為該讀取之廢止清冊之篡改驗證值的使用公鑰加密技術之數位署名完成時，控制器408使用署名驗證密鑰(公開密鑰)進行驗證。又，當賦予訊息認證代碼MAC作為篡改驗證值時，首先實行參照圖3說明之MAC驗證處理。

控制器408以判定碟片ID廢止清冊(DIRL)未被篡改為前提條件，進行該碟片ID廢止清冊(DIRL)之版本與記憶體409中已儲存之碟片ID廢止清冊(DIRL)之版本的比較。

當讀出之碟片ID廢止清冊(DIRL)的版本較記憶體409中已儲存之碟片ID廢止清冊(DIRL)新時，控制器408根據所讀出之碟片ID廢止清冊(DIRL)，更新記憶體409內之廢止清冊DIRL。

於步驟S106中，控制器408判斷於步驟S101中讀出之碟片ID是否存在於廢止清冊DIRL內，當判斷存在時進入步驟S107，否則進入步驟S108。於步驟S107中，控制器408停止(禁止)記錄於資訊記錄媒體200之加密內容的解密及再生。

當碟片ID不存在於廢止清冊內時，進入步驟S108，控制器408將步驟S101中讀取之碟片ID發送至服務提供伺服器。進而，於步驟S109中，自服務提供伺服器接受服務。另，服務提供伺服器於步驟S108中，實行自資訊處理裝置(用戶設備)400接收之碟片ID的驗證處理，僅於已確認合

法性之情形下，實行服務之提供處理。

以下，說明於步驟S102中實行之碟片ID的驗證處理。儲存於資訊記錄媒體之碟片ID作為偽造困難性高之識別資訊而設定。碟片ID之構造例如圖11所示。

於圖11中，作為資訊記錄媒體ID(碟片ID)、標題固有值以及碟片固有值之對應例表示有6種碟片ID設定例，上述資訊記錄媒體ID(碟片ID)係作為資訊記錄媒體識別符者，上述標題固有值係對儲存於資訊記錄媒體之內容標題而設定之固有值，上述碟片固有值係作為資訊記錄媒體之固有值而設定者。另，碟片ID、碟片固有值均自管理裝置201產生。標題固有值：M可使用構成儲存於資訊記錄媒體中之內容的部分資訊，或自管理裝置201、內容提供裝置203產生。標題固有值：S自管理裝置201依據標題固有值：M而產生。

圖11所示各記號之意義如下。

M：相應於資訊記錄媒體之儲存內容之標題的固有值。

w： $w = 1, 2, \dots, W$ ，W代表所製造之資訊記錄媒體的張數。

Sig(w)：依據管理裝置之密鑰(例如依據公開密鑰加密方式設定之密鑰)的署名資料，對應於製造之資訊記錄媒體的張數W而產生，每個資訊記錄媒體之署名資料各不相同。Sig(w)表示各碟片之署名係設定為Sig(1)，Sig(2)．．．Sig(W)。

p(w)：相應於製造之資訊記錄媒體的張數W而設定之質

數，相應於製造之資訊記錄媒體的張數 W 而產生之各資訊記錄媒體均不相同的質數資料。

S ：相應於資訊記錄媒體之儲存內容之標題的固有值， $S = K^T \bmod M$ ，其中 T 係由以下算式計算之值。

[數 1]

$$T = \prod_{w=1}^W P_w$$

$$\text{IDKey}(w) : \text{IDKey}(w) = K^{T/p(w)} \bmod M$$

其中， K 係對於各標題設定之值，且係滿足 $K \in Z^*_M$ (K 係遍曆群 Z^*_M 之產生源，另， $X \in Z^*_M$ 表示 X 係 $1 \sim X-1$ 之整數 x 中，以 x 為分母，具有逆元之集合要素)之值。

$e(w)$ ：滿足 $e(w) \in Z^*_M$ ，與對應於碟片製造張數 W 之數字不同的值。

其中， $e(w)$ 與 $\lambda(M)$ 互為質數，即， $e(w)$ 與 $\lambda(M)$ 之最大公約數為1。另， $\lambda(M)$ 係質數 (q_1-1) 與 (q_2-1) 之最小公倍數。 q_1 、 q_2 係用於RSA加密所需之大質數。

$$I(w) : I(w) = S^{d(w)} \bmod M$$

其中， $d(w)$ 係以 $\lambda(M)$ 為分母時， $e(w)$ 之倒數。

Σw ：係使用管理裝置(CA)201之密鑰，將資料 S 與資料 $e(w)$ 之連接資料，即 $M(w)$ 加密後之資料。

以下，說明對應於圖11所示之6個碟片ID設定例之資訊處理裝置(用戶設備)400的碟片ID驗證處理順序。

參照圖12說明設定例1之資訊處理裝置(用戶設備)400的碟片ID驗證處理順序。

設定例1係，

碟片ID = M，Sig(w)

標題固有值 = M

碟片固有值 = Sig(w)

之設定例。

資訊處理裝置(用戶設備)400之控制器408於步驟S201中，取出碟片ID(w)內之署名資料SIG(w)。另，碟片ID當碟片製造張數為W時，根據由 $w = 1, 2, \dots, W$ 表示之各碟片(w)而成為不同的值，因此標記為碟片ID(w)。

於步驟S202中，控制器408依據自記憶體409讀取之管理裝置12(管理局CA)之公鑰及公開之參數，由步驟S201中讀取之署名資料SIG(w)產生訊息M(w)'。訊息之標記亦與碟片ID(w)之標記相同，以M(w)表示對應各碟片互不相同之訊息。

於步驟S203中，控制器408對碟片ID(w)內包含之訊息M(w)與於步驟S202中產生之訊息M(w)'進行比較。

於步驟S204中，控制器408當於步驟S203之比較處理中判斷為一致時，進入步驟S205，否則進入步驟S206。

於步驟S205中，控制器408判斷於步驟S201中取出之碟片ID(w)合法。於步驟S206中，控制器408判斷於步驟S201中取出之碟片ID(w)不合法。

設定例2係

碟片ID = S，Sig(w)

標題固有值 = S

碟片固有值 = $\text{Sig}(w)$

之設定例。

此設定例2僅將設定例1中標題固有值M置換為S，順序與設定例1中資訊處理裝置(用戶設備)400之碟片ID驗證處理順序相同，不同點僅係於步驟S202中，由署名資料產生之資料變為訊息S'(w)，步驟S203中所比較之資料變為碟片ID中包含之資料S(w)。

繼而，參照圖13說明設定例3之資訊處理裝置(用戶設備)400的碟片ID驗證處理順序。

設定例3係

碟片ID = $p(w)$ ，IDKey(w)

標題固有值 = S

碟片固有值 = $p(w)$ 或IDKey(w)

之設定例。

於步驟S301中，資訊處理裝置(用戶設備)400之控制器408取出自資訊記錄媒體200讀取的碟片ID(w)內之資料 $p(w)$ 。

於步驟S302中，控制器408判斷於步驟S302中取出之資料 $p(w)$ 是否為質數。控制器408當判斷資料 $p(w)$ 為質數時，進入步驟S303，否則進入步驟S304。

於步驟S303中，控制器408判斷於步驟S301中取出之碟片ID(w)合法。於步驟S304中，控制器408判斷於步驟S301中取出之碟片ID(w)不合法。

繼而，參照圖14說明設定例4之資訊處理裝置(用戶設

備)400的碟片ID驗證處理順序。

設定例4係

碟片ID = $e(w)$ ， $I(w)$

標題固有值 = S

碟片固有值 = $e(w)$ 或 $I(w)$

之設定例。

於步驟S401中，當資訊記錄媒體200安裝於特定存取位置時，資訊處理裝置(用戶設備)400介以記錄媒體介面410，自資訊記錄媒體200讀取碟片ID，並將其儲存於記憶體409。

於步驟S402中，資訊處理裝置(用戶設備)400之控制器408使用記錄於記憶體409之碟片ID內的資料 $e(w)$ 與 $I(w)$ ，計算出 $I(w)^{e(w)} \bmod M$ ，將其結果作為資料 S' 。即，

$$S' = I(w)^{e(w)} \bmod M$$

於步驟S403中，控制器408介以記錄媒體介面410，自資訊記錄媒體200讀取碟片ID廢止清冊(DIRL)。當作為讀出之碟片ID廢止清冊(DIRL)之篡改驗證值的使用有公鑰加密技術之數位署名完成時，控制器408使用署名驗證密鑰(公開密鑰)進行驗證。又，當賦予訊息認證代碼MAC作為篡改驗證值時，首先實行參照圖3說明之MAC驗證處理。

控制器408以判定碟片ID廢止清冊(DIRL)未被篡改為前提條件，進行該碟片ID廢止清冊(DIRL)之版本與記憶體409中已儲存之碟片ID廢止清冊(DIRL)之版本的比較。當該讀取之碟片ID廢止清冊(DIRL)的版本較記憶體409中儲

存之碟片ID廢止清冊(DIRL)新時，控制器408根據所讀出之碟片ID廢止清冊(DIRL)，更新記憶體409內之廢止清冊DIRL。

於步驟S404中，控制器408判斷於步驟S401中讀取之碟片ID是否存在於廢止清冊內，當判斷存在時進入步驟S405，否則進入步驟S406。

於步驟S405中，控制器408停止(禁止)記錄於資訊記錄媒體200c之內容的再生。於步驟S406中，控制器408將於步驟S401中讀取之碟片ID發送至服務提供伺服器。進而。於步驟S407中，自服務提供伺服器接受服務。另，服務提供伺服器於步驟S406中，實行自資訊處理裝置(用戶設備)400接收之碟片ID的驗證處理，僅於已確認合法性之情形下，實行服務之提供處理。

繼而，參照圖15說明設定例5之資訊處理裝置(用戶設備)400的碟片ID驗證處理順序。

設定例5係

碟片ID = Σw

標題固有值 = S

碟片固有值 = $e(w)$

之設定例。

於步驟S501中，資訊處理裝置(用戶設備)400之控制器408依據管理裝置201(管理局CA)之公鑰資料將自資訊記錄媒體200讀出之碟片ID(w)解碼，並產生訊息M(w)。訊息M(w)如上所述，其係連結資料S與資料 $e(w)$ 之資料。

於步驟S502中，資訊處理裝置(用戶設備)400依據管理裝置201公開之大小 $|S|$ 、以及大小 $|e(w)|$ 、以及資料S與資料 $e(w)$ 之組合樣式，自步驟S501中解碼之訊息 $M(w)$ 取出資料S。

資訊處理裝置(用戶設備)400於上述圖15所示之處理之後，進行圖10所示之步驟S105~S109之處理。此時，資訊處理裝置(用戶設備)400於圖10所示步驟S105、S106之廢止清冊與碟片ID之對照處理中，使用步驟S501中自資訊記錄媒體200讀出之碟片ID(w)作為碟片ID。

資訊處理裝置(用戶設備)400使用步驟S502中取出之資料S作為內容密鑰資料，將內容資料解密。因此，當經過上述步驟S501、S502之處理後，無法取得適當資料S時，便無法正確將內容資料解碼。

設定例6係

碟片ID = $p(w)$ ，IDKey(w)

標題固有值 = S

碟片固有值 = $p(w)$

之設定例，此與設定例3之碟片ID的構造相同，因此首先實行與參照圖13說明之處理相同的碟片ID驗證處理。

[5.服務提供伺服器處理之具體內容]

接著說明服務提供伺服器300自資訊處理裝置(用戶設備)400接收服務提供要求時之處理。

如圖16所示，服務提供伺服器300自資訊處理裝置(用戶設備)400接收碟片ID。此碟片ID係於資訊處理裝置(用戶

設備)400中，藉由驗證處理驗證合法性之碟片ID，上述資訊處理裝置(用戶設備)400係安裝有資訊記錄媒體200，自資訊記錄媒體200讀取碟片ID者。

當服務提供伺服器300自資訊處理裝置(用戶設備)400接收到服務提供要求以及碟片ID時，便驗證碟片ID之合法性，以合法性之確認為前提條件提供服務。

另，自資訊處理裝置(用戶設備)400不僅發送服務提供要求及碟片ID，並且發送作為服務識別符之服務ID至服務提供伺服器300。

服務提供伺服器300介以圖7所示之輸入輸出介面(I/F)304，定期或以事件為單位自管理裝置201、內容提供裝置203或其他裝置接收碟片ID廢止清冊，使安全記憶體305中總是儲存最新版碟片ID廢止清冊，又，介以輸入輸出介面(I/F)304，自內容提供裝置203或其他裝置，接收各標題之標題固有值及用以識別所提供服務之服務識別資訊，將先前參照圖8說明之管理各標題之服務提供狀況資料的服務提供狀況資料庫儲存於安全記憶體305。

服務提供伺服器300將圖8所示之服務提供狀況資料儲存並保持於例如安全記憶體305，對應於資訊處理裝置(用戶設備)400提出之伴隨碟片ID之服務提供要求，服務提供要求設備實行確認處理，判斷其是否為依據合法碟片ID之服務要求，進而僅於依據圖8所示之服務提供狀況資料，判斷未到達服務提供所允許之上限時，方提供服務。

參照圖17，說明服務提供伺服器300自資訊處理裝置(用

戶設備)400接收服務提供要求時之處理順序。

於步驟S701中，服務提供伺服器300介以圖7所示之輸入輸出介面(I/F)304，自資訊處理裝置(用戶設備)400接收服務提供要求。此資訊處理裝置(用戶設備)400提出之服務提供要求中，包含資訊處理裝置(用戶設備)400自資訊記錄媒體200取得之碟片ID，以及要求服務之識別符(服務識別符)。碟片ID係先前參照圖11說明之設定例1~6中任一碟片ID。

於步驟S702中，服務提供伺服器300對接收之碟片ID進行驗證處理。此驗證處理之驗證順序與資訊處理裝置(用戶設備)400所實行之驗證處理相同，即，實行與參照圖12~圖15說明之碟片ID設定例1~6相應的驗證順序。

於步驟S703中，當藉由碟片ID驗證處理確認碟片ID之合法性後，進入步驟S705，當判斷碟片ID非法時，進入步驟S704，中止服務之提供處理。另，亦可構造為，於此中止處理時，向資訊處理裝置(用戶設備)400發送中止服務提供處理之訊息。

當確認碟片ID之合法性，進入步驟S705時，讀取儲存於安全記憶體305(參照圖7)中之碟片ID廢止清冊(DIRL)。

於步驟S706中，判斷已完成合法性確認之碟片ID是否記錄於廢止清冊中。

當接收之碟片ID記錄於廢止清冊中時，判斷為非法ID，進入步驟S711，中止服務之提供處理。另，亦可構造為，於此中止處理時，向資訊處理裝置(用戶設備)400發送中止

服務提供處理之訊息。

當接收之碟片ID未記錄於廢止清冊時，於步驟S707中，依據碟片ID計算標題固有值。碟片ID構造為包含先前參照圖11說明之標題固有值M或S之資料，或可計算出標題固有值M或S之資料，服務提供伺服器300取得接收之碟片ID中包含的標題固有值M或S，或藉由運算單元303之運算處理，由接收之碟片ID計算標題固有值M或S。此標題固有值M或S之取得、計算處理對應於先前參照圖11說明之設定例1~6，採取不同處理方式。

於步驟S707中，進而依據由碟片ID取得之標題固有值M或S，自資料庫取得對應於標題之服務提供狀況資料。即參照圖8說明之服務提供狀況資料，對應於各碟片ID設定有各服務之提供狀況的資料。

於步驟S707中，自服務提供狀況資料中，提取自資訊處理裝置(用戶設備)400接收之碟片ID與服務識別符相應之資料，檢查是否為可提供之服務。

以圖8所示之服務提供狀況資料為例說明，例如當自資訊處理裝置(用戶設備)400接收之碟片ID為(DiscID1)，服務識別符為(服務1)時，服務1之上限為1次，服務提供狀況為[未提供]，因此判斷為可提供。

於步驟S708中，當依據服務提供狀況資料判斷可提供服務時，進入步驟S709，當於步驟S708中，依據服務提供狀況資料判斷不可提供服務時，進入步驟S711。

於步驟S711中，中止服務之提供處理。另，亦可構造

為，於此中止處理時，向資訊處理裝置(用戶設備)400發送中止服務提供處理之訊息。

當依據服務提供狀況資料判斷可提供服務時，於步驟S709中，進行資料庫之更新。

以圖8所示之服務提供狀況資料為例說明，例如當自資訊處理裝置(用戶設備)400接收之碟片ID為(DiscID1)，服務識別符為(服務1)時，服務提供狀況自[未提供]變更為[已提供1次]。

於步驟S710中，服務提供伺服器300向發送服務提供要求之資訊處理裝置(用戶設備)400實行服務提供處理。

例如，碟片儲存內容為外文電影時，相對於聲音之字幕資料、配音之聲音資料或內容續編碟片之購買折扣券等，各種內容相關服務可介以網絡，自服務提供伺服器300提供至資訊處理裝置(用戶設備)400。

另，資訊處理裝置(用戶設備)400與服務提供伺服器300間之通訊較好的是進行使用加密技術之相互認證，及共用會話密鑰，製作安全通訊路徑，再進行通訊。

又，於上述例中，每次接受服務提供要求時，於步驟S705、S706，便會檢查碟片ID廢止清冊(DIRL)，但亦可構造為預先檢查碟片ID廢止清冊(DIRL)，例如可定期檢查，根據其中的碟片ID，更新資料庫，不再向其提供服務。當如此構造時，可省略於接受服務提供要求時之碟片ID廢止清冊(DIRL)的檢查，亦可縮短用以提供服務之時間。

又，於上述實施例中，就每張碟片之碟片ID均不同之情

形為例加以說明，但碟片ID例如以10張、100張、1000張為組單位時亦同樣，可考慮Group之張數而決定對一個碟片ID所提供之服務次數。

以上參照特定實施例詳細說明了本發明。但於不脫離本發明之要旨之範圍內，業者顯然可完成該實施例之修改或代用。即，本發明係以例示之形態加以揭示，不可作限定性之解釋。應參照專利申請範圍之內容判斷本發明之要旨。

另，說明書中說明之一系列處理可藉由硬體、軟體或兩者之複合構造實行。藉由軟體實行處理時，可將記錄有處理順序之程式安裝於裝有專用硬體之電腦內的記憶體後實行，或將程式安裝於可實行各種處理之泛用電腦後實行。

例如，可將程式預先記錄於作為記錄媒體之硬碟或ROM(Read Only Memory，唯讀記憶體)。或者，將程式暫時或永遠儲存(記錄)於軟碟、CD-ROM(Compact Disc Read Only Memory，緊密磁碟-唯讀記憶體)、MO(Magneto optical，磁光盤)碟，DVD(Digital Versatile Disc，數位影音光碟)、磁碟、半導體記憶體等可移動記錄媒體。此種可移動記錄媒體可作為所謂封裝軟體提供。

另，程式除由上述可移動記錄媒體安裝於電腦，亦可由下載網站無線傳送至電腦，或介以所謂LAN(Local Area Network，區域網)、網際網路之網絡，有線傳送至電腦，電腦可接收如此傳送而來之程式，並安裝於內置之硬碟等記錄媒體。

另，揭示於說明書之各種處理並非僅限於按照所揭示之順序進行，可根據實行處理之裝置的處理能力或需要，並列或單獨實行。又，本說明書中所謂系統，係指複數裝置之邏輯集合構造，各構造之裝置並非一定存在於同一框體內。

[產業上之可利用性]

如上所述，藉由本發明之構造，於將內容儲存並提供至DVD、CD、藍色雷射光記錄媒體等各種資訊記錄媒體，進而自網絡連接之服務提供伺服器進行服務提供處理之構造中，於服務提供伺服器側，驗證自資訊處理裝置(用戶設備)發送之資訊記錄媒體ID，依據每個資訊記錄媒體ID之服務提供狀況資料提供服務，因此發送服務要求之資訊處理裝置係自資訊記錄媒體讀取合法資訊記錄媒體ID之資訊處理裝置，僅當依據服務提供狀況資料確認該服務提供係允許之服務時，方進行服務之提供。本發明之構造可於自伺服器提供與內容對應之各種服務資訊的系統等中，嚴格審查服務提供對象，確認合法權限後，提供與內容對應之各種服務資訊，上述服務資訊例如碟片儲存內容為電影內容時之字幕資料以及配音聲音資料等內容相隨的資訊。

進而，藉由本發明之構造，儲存於資訊記錄媒體中之資訊記錄媒體ID包含可確認管理裝置之署名資料等之合法性的資料，又，包含可計算是否具有標題固有值之資料，因此於服務提供伺服器中，可依據包含於資訊記錄媒體ID之資料，確認合法性，並取得標題固有值，指定對應於標題

固有值設定之服務提供狀況資料。因此，可嚴格審查服務提供對象，於確認合法權限後，提供與內容相應之各種服務資訊。

【圖式簡單說明】

圖1係說明資訊記錄媒體之儲存資料的圖。

圖2係說明廢止清冊之構造之圖。

圖3係說明使用訊息認證代碼(MAC：Message Authentication Code)時之MAC產生、驗證處理的圖。

圖4係說明各種鑰、資料之加密處理、分佈處理中所使用之多層樹狀結構的圖。

圖5係表示使用內容鑰之有效化密鑰組塊(EKB)之分佈例與解密處理例的圖。

圖6係說明資訊記錄媒體之構造、管理處理構造的圖。

圖7係說明服務提供伺服器之構造例的圖。

圖8係表示服務提供伺服器所具有之服務提供狀況資料的圖。

圖9係說明資訊處理裝置(用戶設備)之構造例的圖。

圖10係說明碟片ID之設定例的圖。

圖11係說明資訊處理裝置(用戶設備)所實行之處理的流程圖。

圖12係說明資訊處理裝置(用戶設備)所實行之碟片ID驗證順序的流程圖。

圖13係說明資訊處理裝置(用戶設備)所實行之碟片ID驗證順序的流程圖。

圖 14 係說明資訊處理裝置(用戶設備)所實行之碟片 ID 驗證順序的流程圖。

圖 15 係說明資訊處理裝置(用戶設備)所實行之碟片 ID 驗證順序的流程圖。

圖 16 係說明資訊處理裝置(用戶設備)自服務提供伺服器接受服務之處理的圖。

圖 17 係說明服務提供伺服器所實行之處理的流程圖。

【主要元件符號說明】

100	資訊記錄媒體
101	碟片 ID
102	內容
103	碟片 ID 廢止清冊 (DIRL: Disc ID Revocation List)
104	密鑰資訊 (EKB: Enabling Key Block)
150	碟片 ID 廢止清冊 (DIRL: Disc ID Revocation List)
151	版本編號
152	廢止碟片 ID 清冊
153	篡改驗證值
200	資訊記錄媒體
201	管理裝置
202	碟片製造裝置
203	內容提供裝置
300	服務提供伺服器
301	匯流排
302	控制器

303	運算單元
304	輸入輸出介面(I/F)
305	安全記憶體
306	主記憶體
400	資訊處理裝置(用戶設備)
401	匯流排
402	輸入輸出介面
403	編解碼器
404	輸入輸出介面
405	A/D·D/A轉換器
406	加密處理部
407	ROM(Read Only Memory，唯讀記憶體)
408	控制器
409	記憶體
410	記錄媒體介面

五、中文發明摘要：

本發明係提供一種可僅對具有合法資訊記錄媒體之設備提供與儲存於資訊記錄媒體中內容相應之服務的裝置、方法。本發明係於將內容儲存至資訊記錄媒體而提供，進而自網絡連接之服務提供伺服器進行服務提供處理之構造中，由服務提供伺服器驗證自用戶設備發送之資訊記錄媒體ID，依據每個資訊記錄媒體ID之服務提供狀況資料判斷可否提供服務後進行服務提供。本發明係一種資訊處理裝置，其由發送服務要求之資訊處理裝置自資訊記錄媒體讀取合法之資訊記錄媒體ID，僅當依據服務提供狀況資料允許提供服務時，提供服務。

六、英文發明摘要：

十一、圖式：

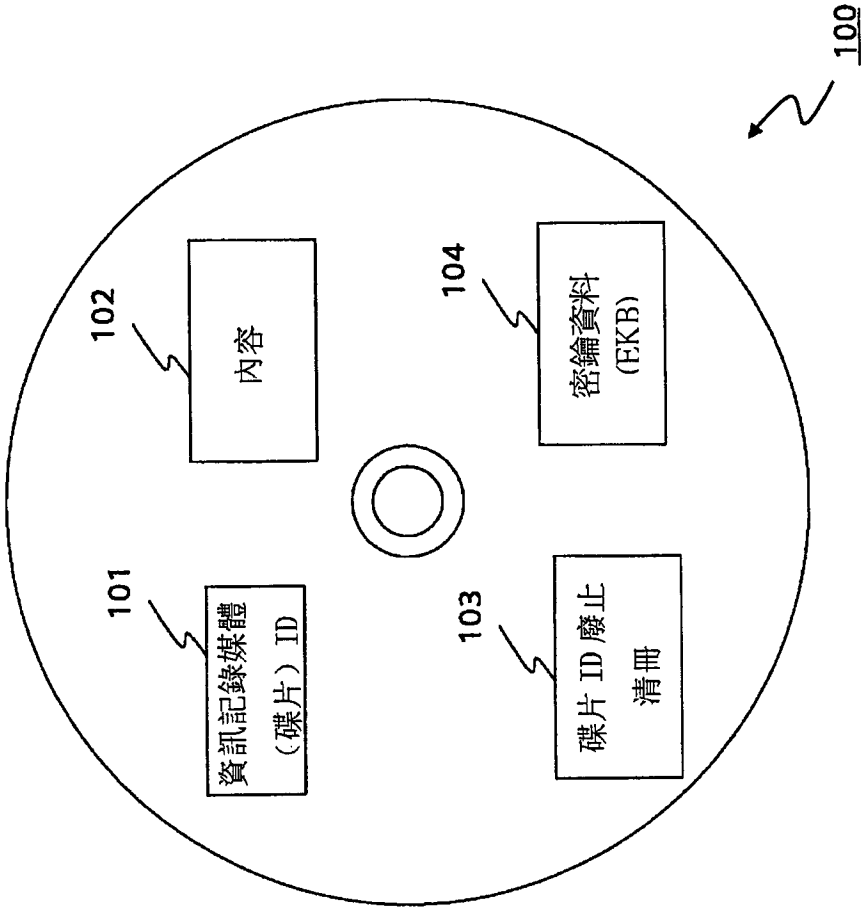


圖 1

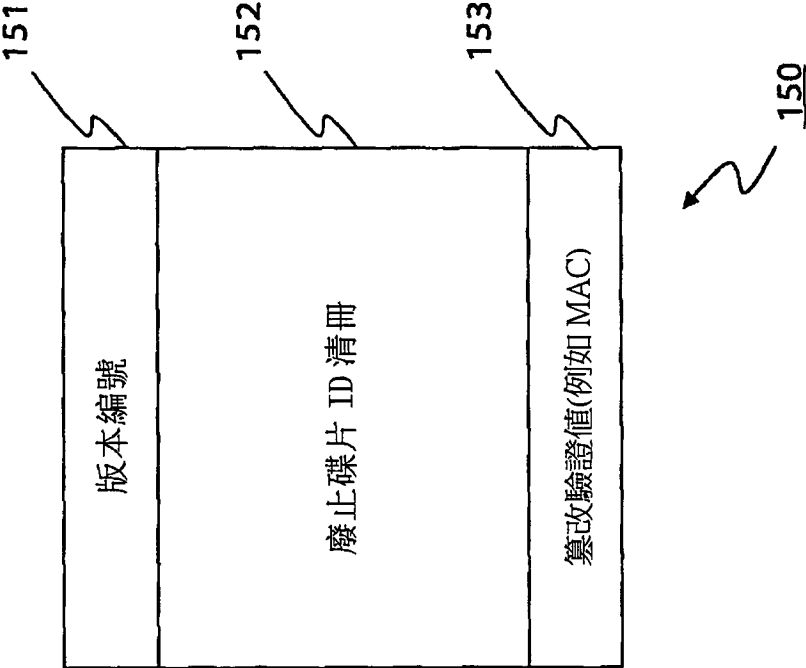


圖 2

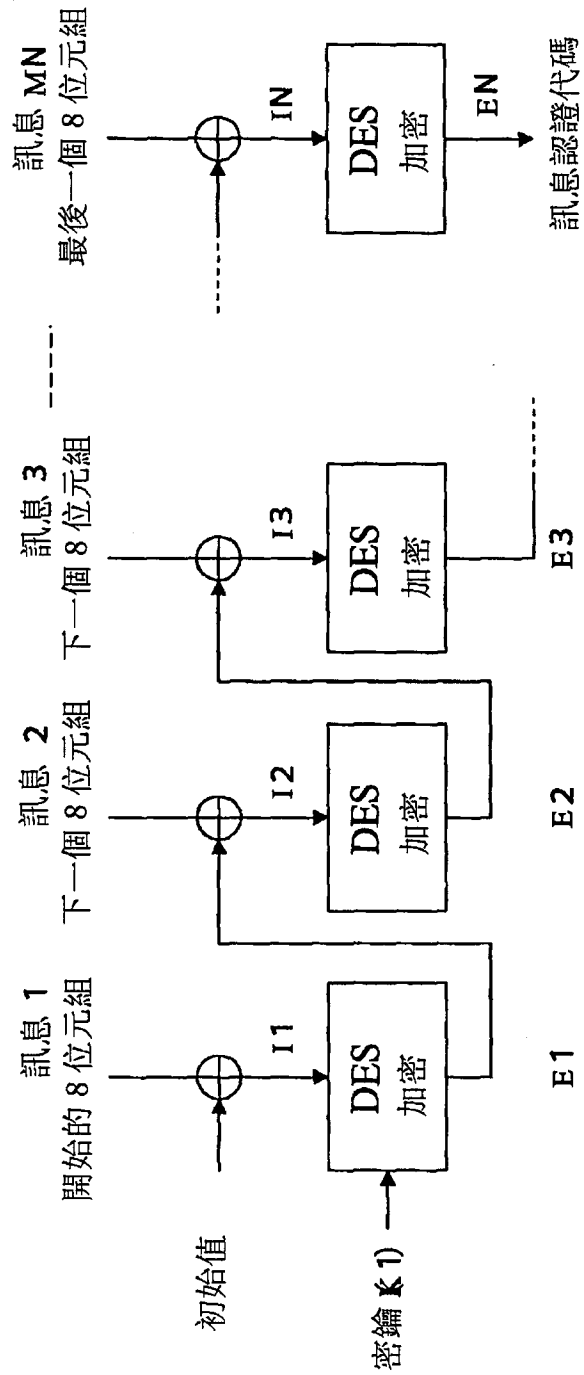


圖 3

$\oplus$ 排他性邏輯和處理(8 位元單元)

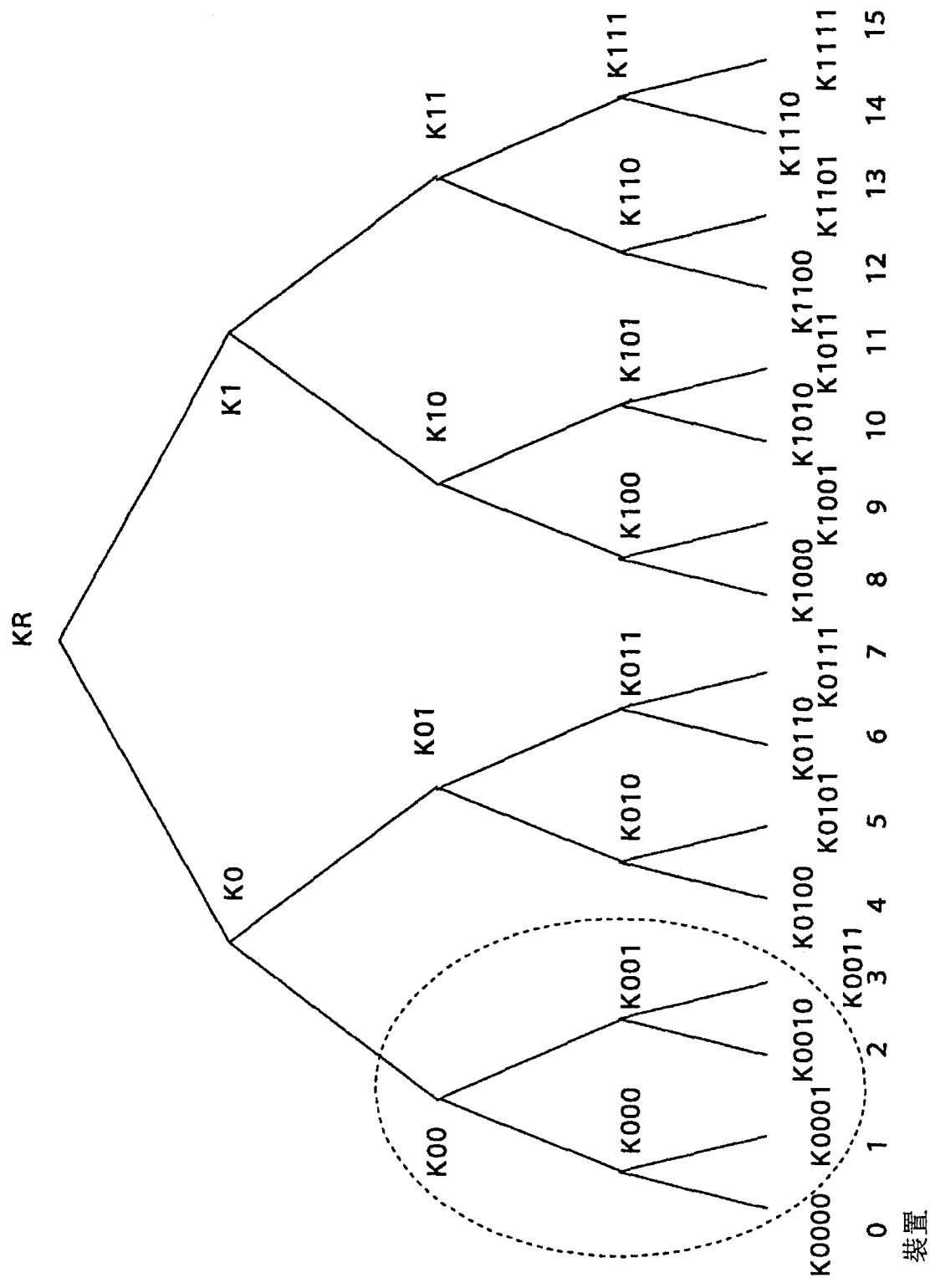
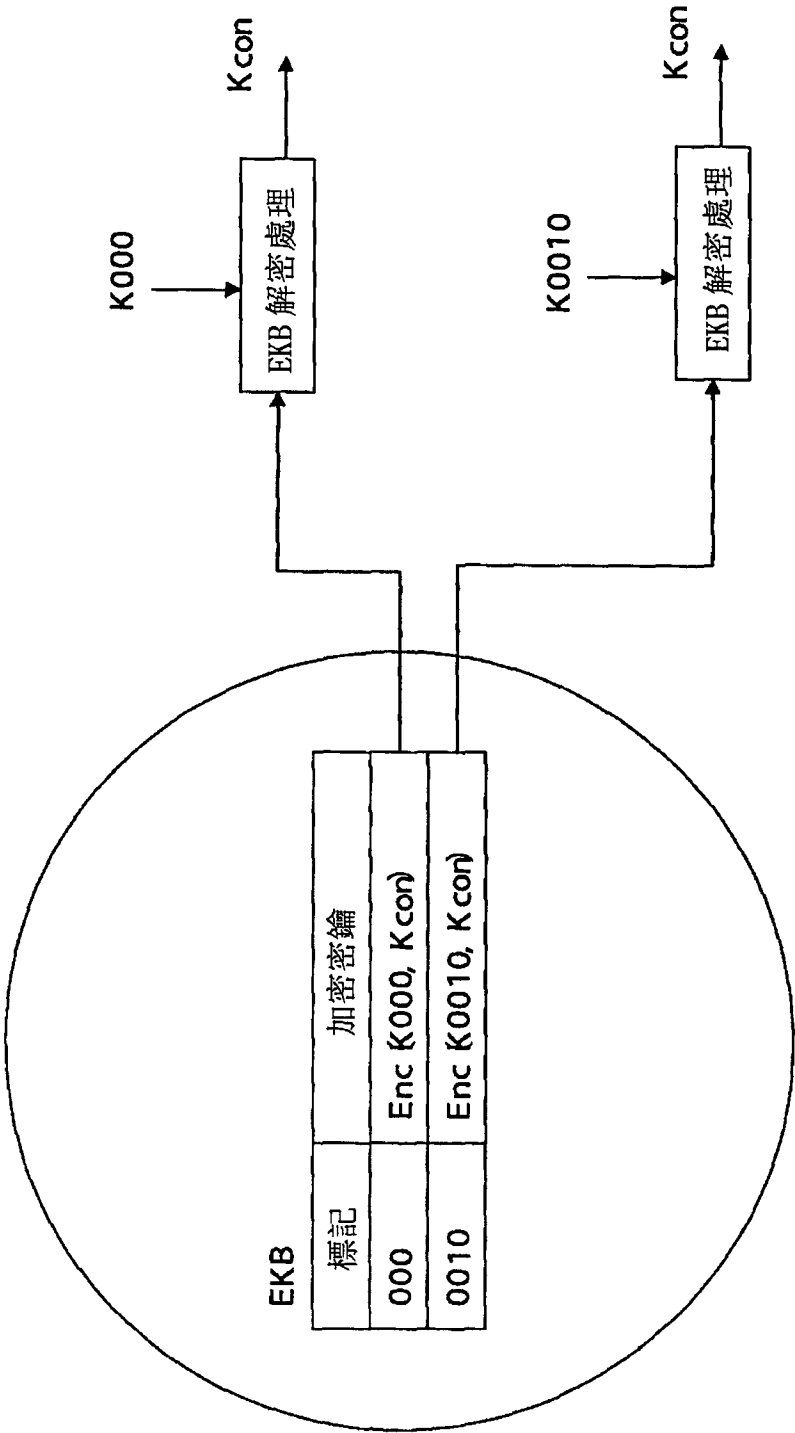


圖 4



記錄媒體

圖 5

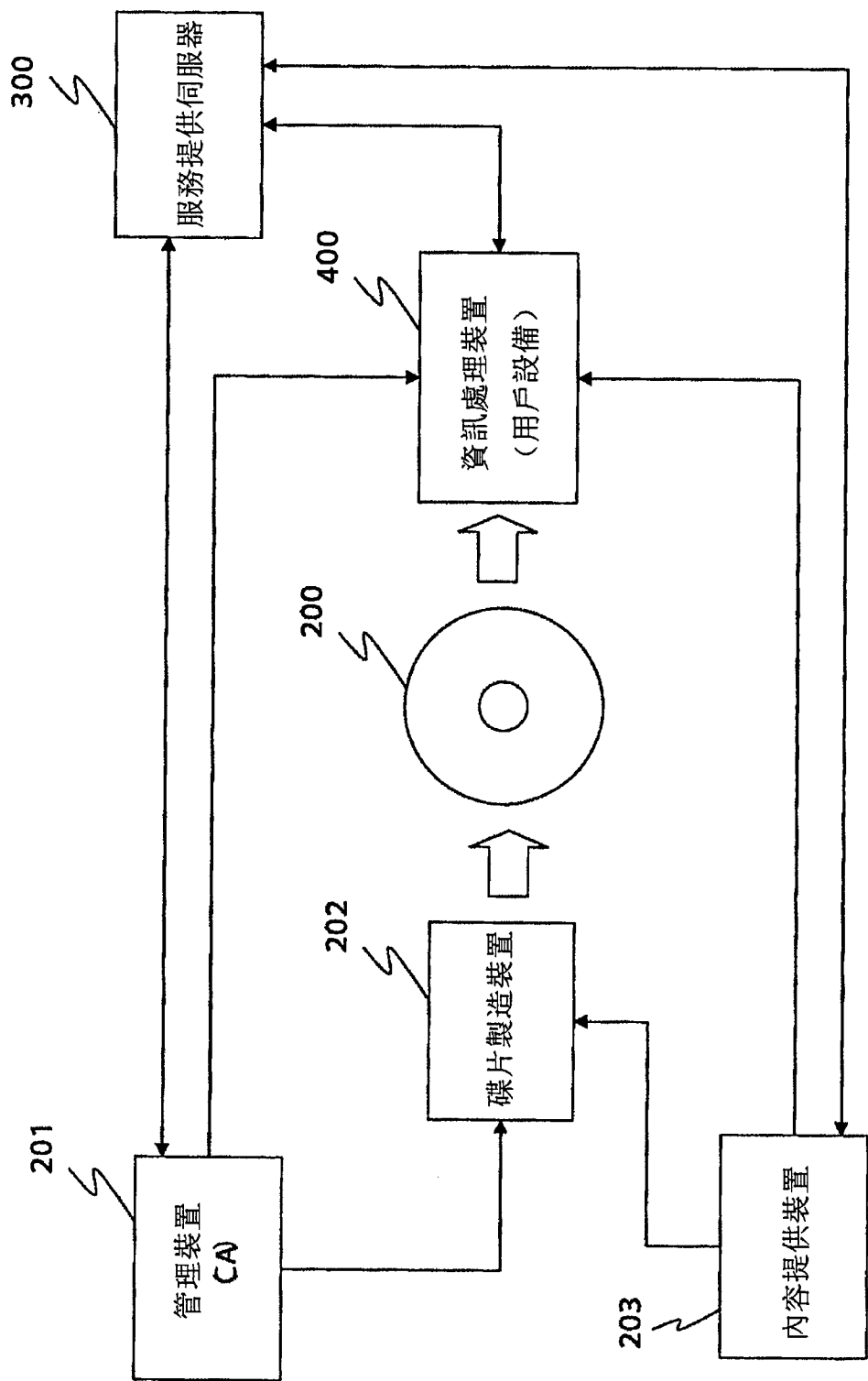


圖 6

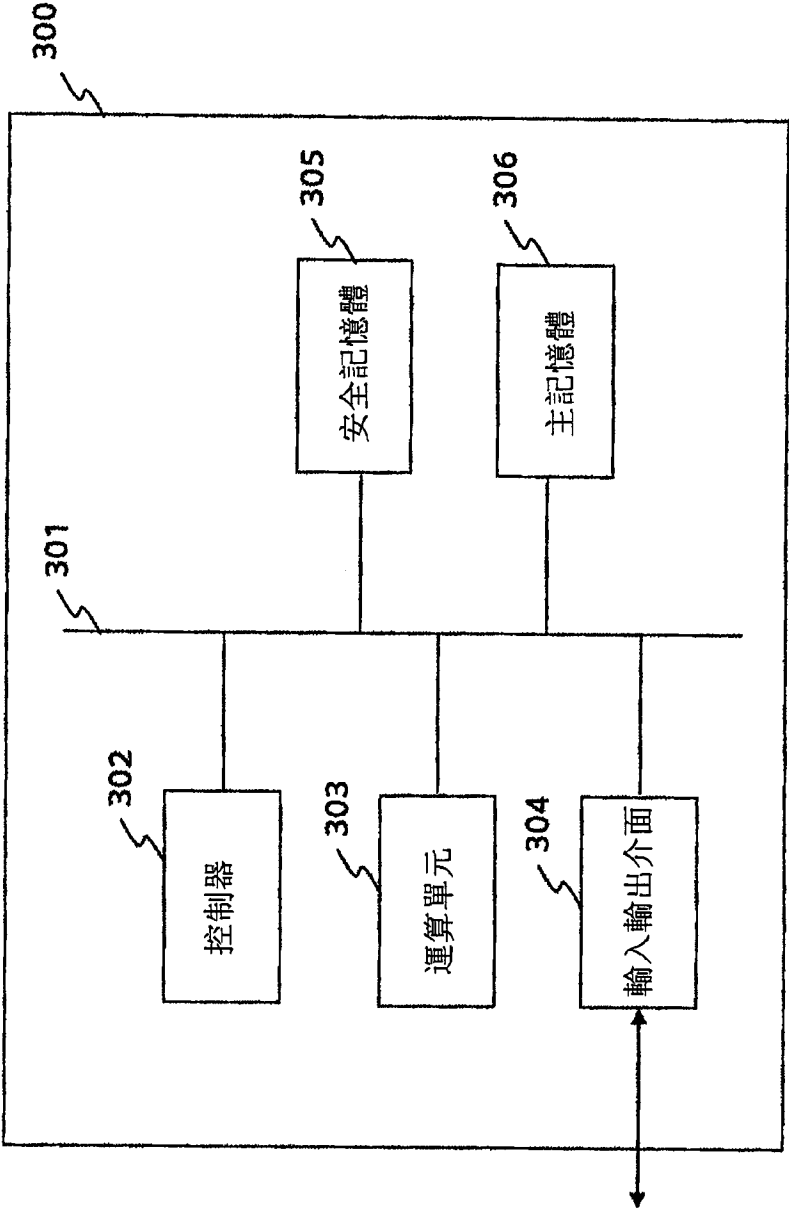


圖 7

標題識別資訊 :aaaa 標題固有值 :bbbb			
	服務 1 (上限為 1 次)	服務 2 (上限為 5 次)	...
Disc ID 1	未提供	已提供 5 次	...
Disc ID 2	已提供	已提供 2 次	...
...	...	...	...

標題識別資訊 :aaaa 標題固有值 :bbbb				...				標題識別資訊 :xxxx 標題固有值 :yyyy			
...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...

圖 8

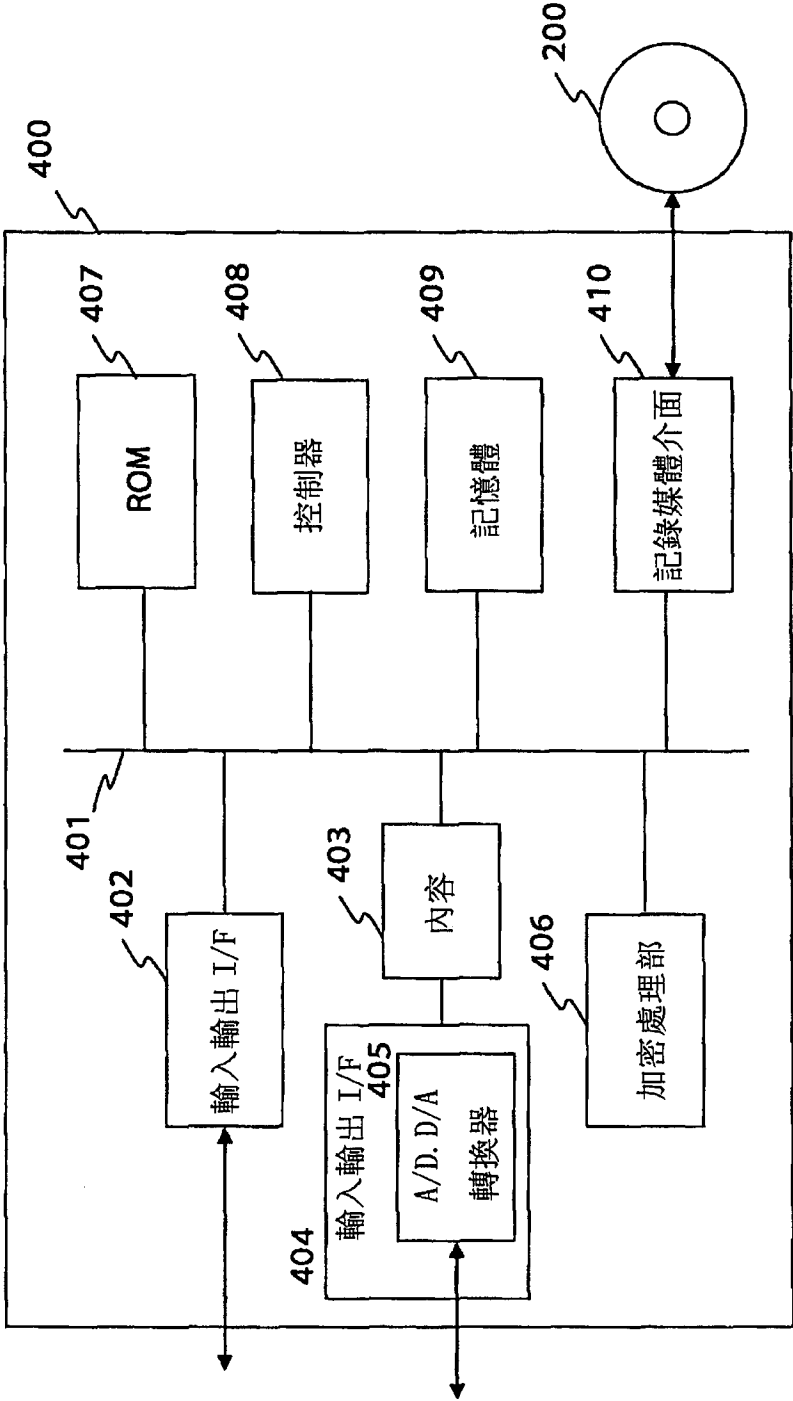


圖 9

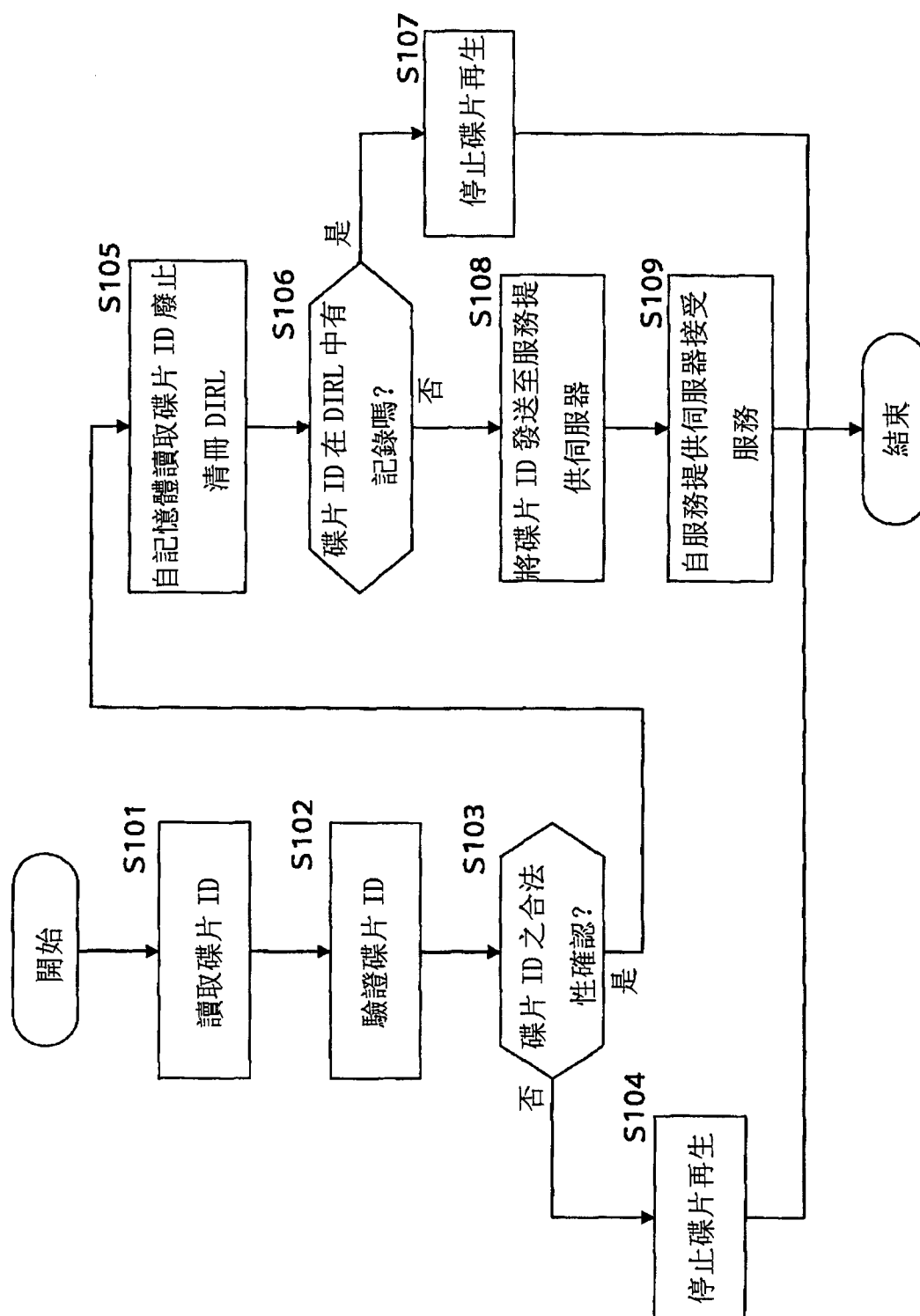


圖 10

	碟片 ID	標題固有值	碟片固有值
碟片 ID 設定例 1	M, S g w	M	S g w
碟片 ID 設定例 2	S, S g w	S	S g w
碟片 ID 設定例 3	p w, DKey w	S	p w 或者、 DKey w
碟片 ID 設定例 4	e w, l w	S	e w 或者、l w
碟片 ID 設定例 5	Σ w	S	e w
碟片 ID 設定例 6	p w, DKey w	S	p w

圖 11

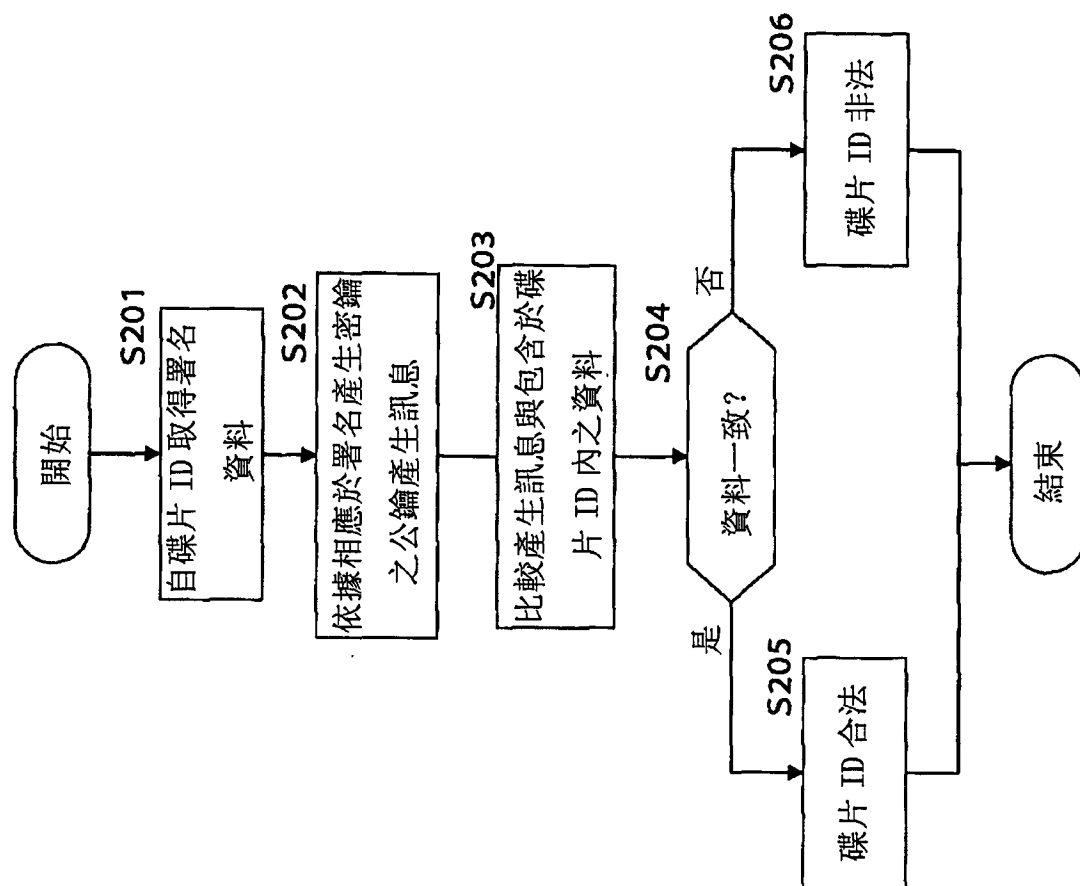


圖 12

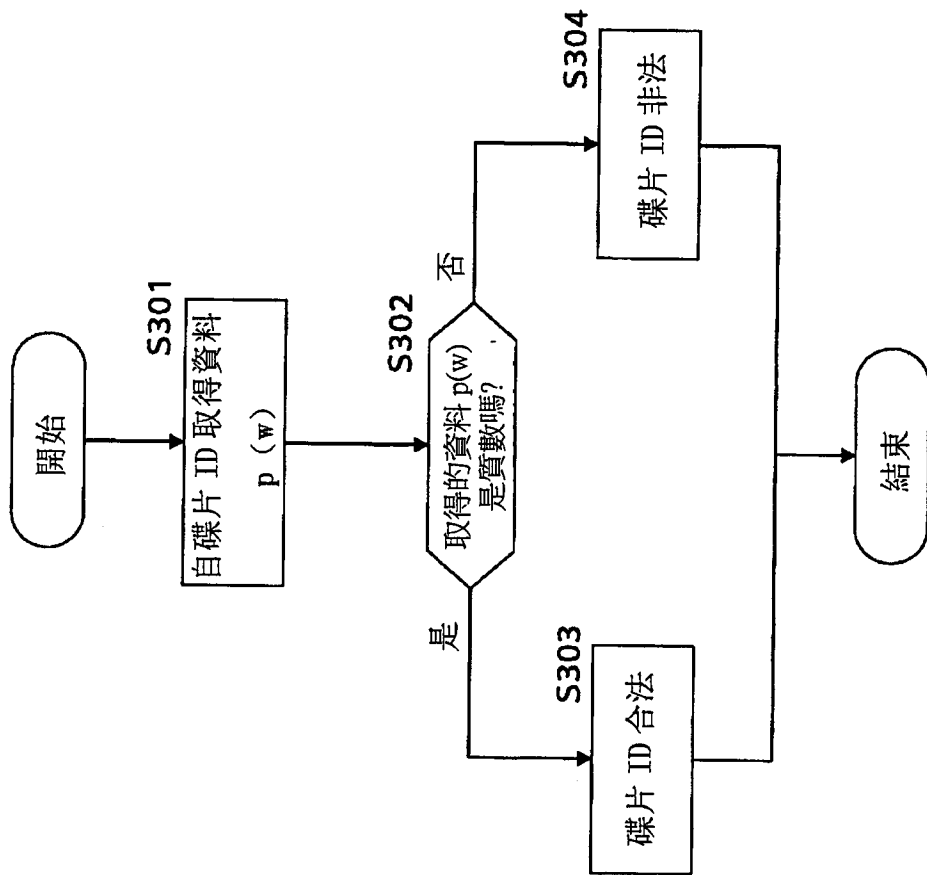


圖 13

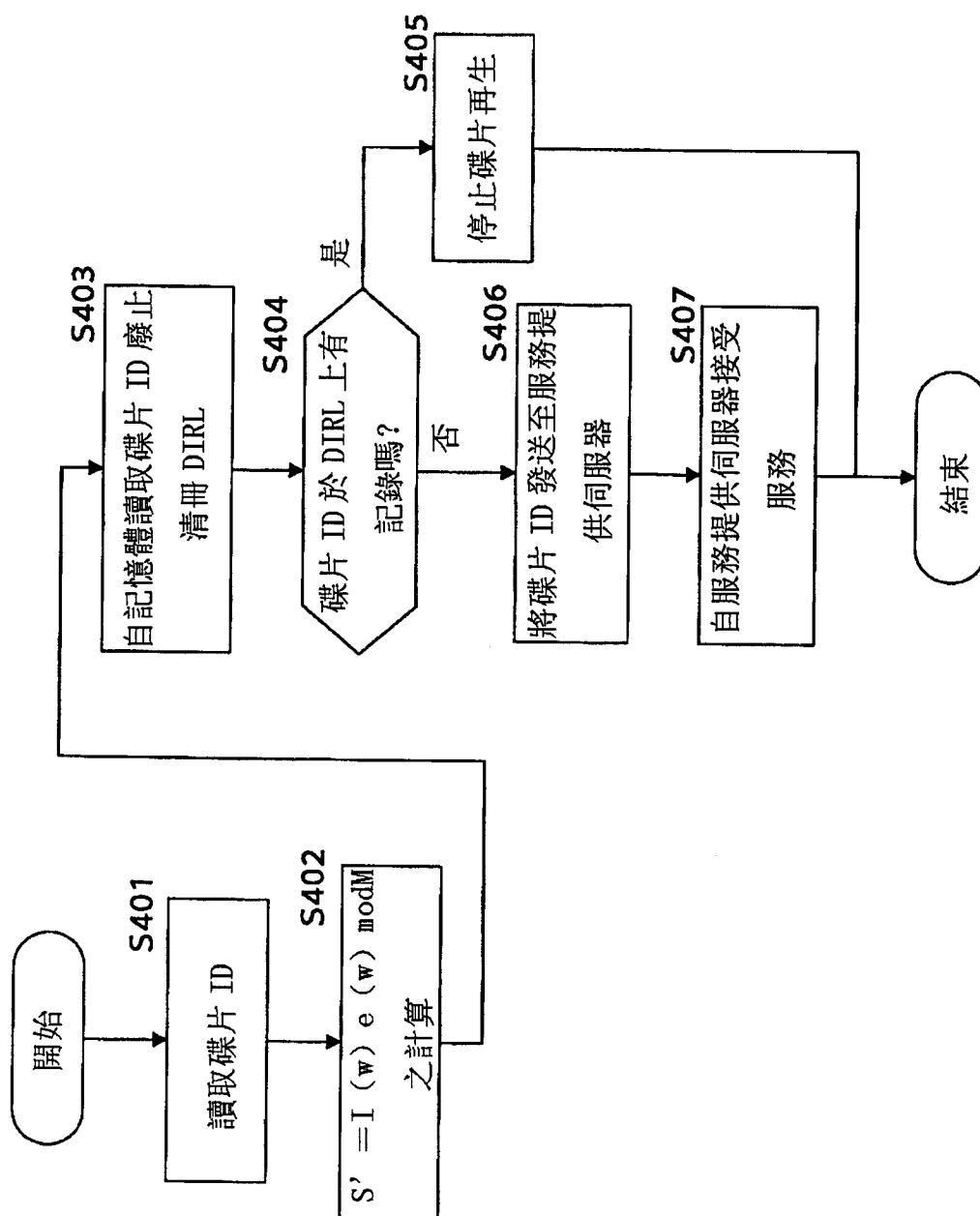


圖 14

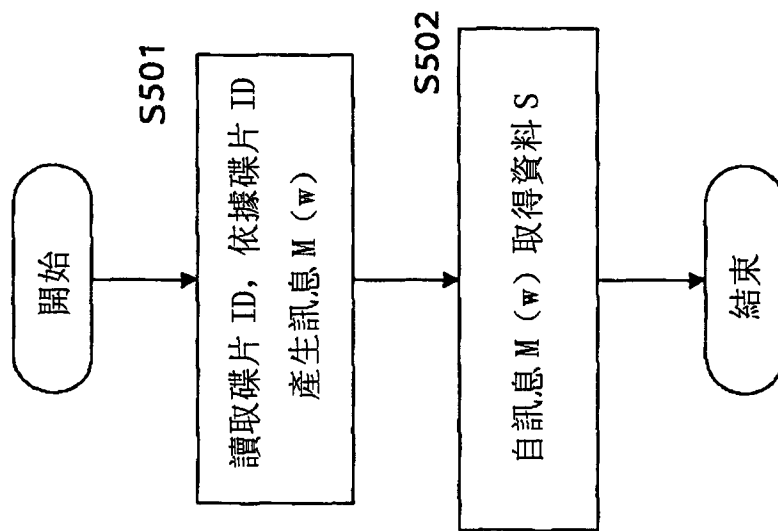


圖 15

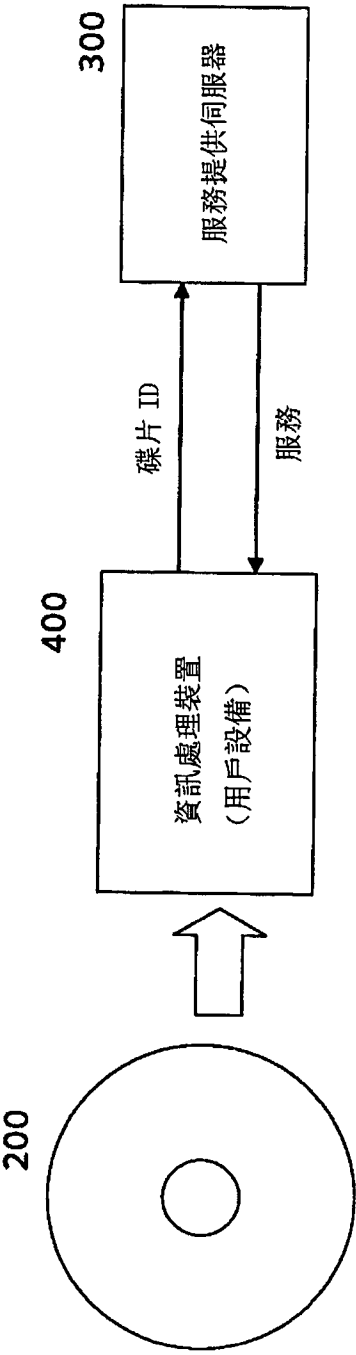


圖 16

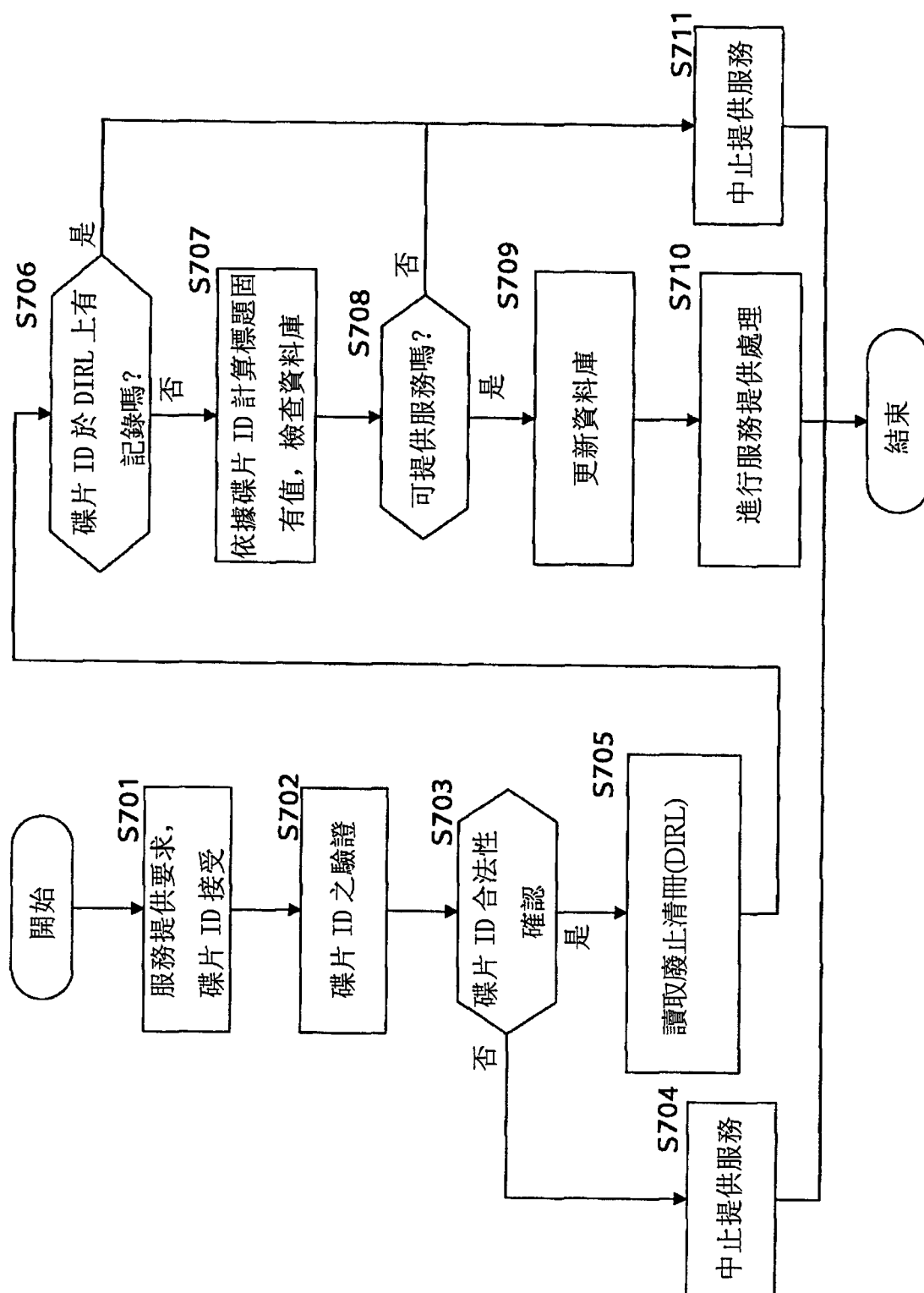


圖 17

七、指定代表圖：

(一)本案指定代表圖為：第 (11) 圖。

(二)本代表圖之元件符號簡單說明：

(無元件符號說明)

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

發明專利說明書

中文說明書替換頁(97年4月)

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：094103530

※申請日期：

※IPC 分類：

G06F 17/40 (2006.01)

H01L 9/30 (2006.01)

一、發明名稱：(中文/英文)

服務提供伺服器、資訊處理裝置、資料處理方法及電腦可讀取之記錄
媒體

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

日商新力股份有限公司

SONY CORPORATION

代表人：(中文/英文)

安藤 國威

ANDO, KUNITAKE

住居所或營業所地址：(中文/英文)

日本東京都品川區北品川六丁目七番35號

7-35, KITASHINAGAWA 6-CHOME SHINAGAWA-KU, TOKYO,

JAPAN

國 籍：(中文/英文)

日本 JAPAN

三、發明人：(共 1 人)

姓 名：(中文/英文)

淺野 智之

ASANO, TOMOYUKI

國 籍：(中文/英文)

日本 JAPAN

十、申請專利範圍：

1. 一種服務提供伺服器，其特徵為，對應於來自資訊處理裝置之服務提供要求，實行服務提供處理，且具有：資料接收部，其自資訊處理裝置接收帶有資訊記錄媒體ID及服務ID之服務要求；記憶部，其儲存每個上述資訊記錄媒體ID之服務提供狀況資料，作為每個與資訊記錄媒體之儲存內容標題相對應之標題固定值的服務管理資料；及資料處理部，其實行介以上述資料接收部接收之資訊記錄媒體ID的驗證處理，以確認合法性為前提條件，依據該資訊記錄媒體ID取得標題固有值，自上述記憶部取得相應於標題固有值之服務提供狀況資料，根據上述資訊記錄媒體ID及上述服務ID判斷是否可提供特定服務，於判定為可提供之前提條件下，實行服務提供處理。
2. 如請求項1之服務提供伺服器，其中上述資料處理部構造為藉由實行資訊記錄媒體ID中包含之署名資料之驗證處理，從而進行資訊記錄媒體ID之驗證處理，根據資訊記錄媒體ID中所包含之標題固有值，或依據資訊記錄媒體ID中包含之資料進行運算而計算出之標題固有值，實行自上述記憶部取得對應標題固有值之服務提供狀況資料的處理。
3. 如請求項1之服務提供伺服器，其中上述服務提供伺服器具有儲存有非法資訊記錄媒體ID列表即廢止清冊的記憶部，上述資料處理部中資訊記錄媒體ID之驗證處理係

藉由將自資訊處理裝置接收之資訊記錄媒體ID與上述廢止清冊中記錄之ID進行對照處理而實行。

4. 如請求項1之服務提供伺服器，其中上述資訊記錄媒體ID包含與資訊記錄媒體之儲存內容標題相對應之標題固有值，及依據管理裝置之密鑰而產生之每個資訊記錄媒體各不相同的署名資料，上述資料處理部藉由對應上述資訊記錄媒體ID中包含之署名資料，產生適用上述管理裝置之公鑰的訊息並進行對照處理，而實行上述資訊記錄媒體ID之驗證處理，並自上述記憶部取得與包含於資訊記錄媒體ID之標題固有值相對應之服務提供狀況資料。

5. 如請求項1之服務提供伺服器，其中上述資訊記錄媒體ID包含對應於所製造之資訊記錄媒體張數 W 而設定之質數 $p(w)$ ，以及

依據質數 $p(w)$ 與標題固有值進行運算，藉此計算出之資料IDKey(w)，上述資料處理部構造為，藉由判斷上述資訊記錄媒體ID中包含之資料是否為質數，進行ID驗證處理，並根據資訊記錄媒體ID中包含之資料IDKey(w)計算標題固有值，自上述記憶部取得與所計算出之標題固有值相對應的服務提供狀況資料。

6. 一種資訊處理裝置，其特徵為實行對於服務提供伺服器之服務提供要求；

且具有記錄媒體介面，其實行資訊記錄媒體之存取處理；

及資料處理部，其對介以上述資訊記錄媒體介面，自資訊記錄媒體讀取之資訊記錄媒體ID進行驗證處理，並以已確認合法性為前提條件，對於服務提供伺服器發送該資訊記錄媒體ID。

7. 如請求項6之資訊處理裝置，其中上述資料處理部構造為，藉由資訊記錄媒體ID中所包含之署名資料之驗證處理，實行資訊記錄媒體ID之驗證處理。
8. 如請求項6之資訊處理裝置，其中上述資料處理部中資訊記錄媒體ID之驗證處理係採取自記憶部或資訊記錄媒體取得非法資訊記錄媒體ID列表即廢止清冊，將取得之廢止清冊中記錄的ID與自資訊處理裝置接收之資訊記錄媒體ID進行對照處理之方式實行。
9. 如請求項6之資訊處理裝置，其中上述資訊記錄媒體ID包含與資訊記錄媒體之儲存內容標題相對應之標題固有价值，及依據管理裝置之密鑰而產生之每個資訊記錄媒體各不相同的署名資料，上述資料處理部構造為，藉由對應上述資訊記錄媒體ID中包含之署名資料，產生適用上述管理裝置之公鑰的訊息並進行對照處理，而實行上述資訊記錄媒體ID之驗證處理。
10. 如請求項6之資訊處理裝置，其中上述資訊記錄媒體ID包含對應於所製造之資訊記錄媒體張數 W 而設定之質數 $p(w)$ 、以及依據質數 $p(w)$ 與標題固有价值進行運算，藉此計算出之資料 $IDKey(w)$ ，上述資料處理部藉由判斷上述資訊記錄媒體ID中包含之資料是否為質數，從而實行ID

驗證處理。

11. 一種資料處理方法，其特徵為對應於來自資訊處理裝置之服務提供要求實行處理，且具有資料接收步驟，其自資訊處理裝置接收帶有資訊記錄媒體ID及服務ID之服務要求，及資料處理步驟，其實行接收之資訊記錄媒體ID的驗證處理，於已確認合法性為前提條件，依據該資訊記錄媒體ID取得標題固有值，自記憶部獲得與取得之標題固有值相對應的服務提供狀況資料，根據上述資訊記錄媒體ID及上述服務ID判斷是否可以提供特定服務，於判定為可提供之前提條件下，實行服務提供處理，上述記憶部儲存有上述每個資訊記錄媒體ID之服務提供狀況資料，作為每個與資訊記錄媒體之儲存內容標題相對應之標題固定值的服務管理資料。
12. 如請求項11之資料處理方法，其中上述資料處理步驟包含以下步驟：藉由實行資訊記錄媒體ID中包含之署名資料之驗證處理，從而進行資訊記錄媒體ID之驗證處理，根據資訊記錄媒體ID中所包含之標題固有值，或依據資訊記錄媒體ID中包含之資料進行運算而計算出之標題固有值，實行自上述記憶部取得對應標題固有值之服務提供狀況資料的處理。
13. 如請求項11之資料處理方法，其中上述資料處理步驟之資訊記錄媒體ID驗證處理包含以下步驟：以進行自資訊處理裝置接收之資訊記錄媒體ID與記錄於非法資訊記錄媒體ID列表之廢止清冊之ID的對照處理之方式進行。

14. 如請求項11之資料處理方法，其中上述資訊記錄媒體ID包含與資訊記錄媒體之儲存內容標題相對應之標題固有价值，及依據管理裝置之密鑰而產生之每個資訊記錄媒體各不相同的署名資料，上述資料處理步驟包含以下步驟：

藉由對應上述資訊記錄媒體ID中包含之署名資料，產生適用上述管理裝置之公鑰的訊息並進行對照處理，而實行上述資訊記錄媒體ID之驗證處理，並自上述記憶部取得與包含於資訊記錄媒體ID之標題固有价值相對應之服務提供狀況資料。

15. 如請求項11之資料處理方法，其中上述資訊記錄媒體ID包含對應於所製造之資訊記錄媒體張數 W 而設定之質數 $p(w)$ ，以及依據質數 $p(w)$ 與標題固有价值進行運算，藉此計算出之資料IDKey(w)，上述資料處理步驟包含以下步驟：藉由判斷上述資訊記錄媒體ID中包含之資料是否為質數，進行ID驗證處理，並根據資訊記錄媒體ID中包含之資料IDKey(w)計算標題固有价值，自上述記憶部取得與所計算出之標題固有价值相對應的服務提供狀況資料。

16. 一種資料處理方法，其特徵為實行對於服務提供伺服器之服務提供要求；

且具有資訊記錄媒體存取步驟，其介以記錄媒體介面，實行資訊記錄媒體之存取處理；

及資料處理步驟，其對介以上述記錄媒體介面，自資訊記錄媒體讀取之資訊記錄媒體ID進行驗證處理，並以

已確認合法性為前提條件，對於服務提供伺服器發送該資訊記錄媒體ID。

17. 如請求項16之資料處理方法，其中上述資料處理步驟藉由資訊記錄媒體ID中所包含之署名資料之驗證處理，實行資訊記錄媒體ID之驗證處理。
18. 如請求項16之資料處理方法，其中上述資料處理步驟中資訊記錄媒體ID之驗證處理包含以下步驟：藉由記憶部或資訊記錄媒體取得非法資訊記錄媒體ID列表即廢止清冊，將取得之廢止清冊中記錄的ID與自資訊處理裝置接收之資訊記錄媒體ID進行對照處理，實行上述資訊記錄媒體ID之驗證處理。
19. 如請求項16之資料處理方法，其中上述資訊記錄媒體ID包含與資訊記錄媒體之儲存內容標題相對應之標題固有值，及依據管理裝置之密鑰而產生之每個資訊記錄媒體各不相同的署名資料，上述資料處理步驟包含以下步驟：藉由對應上述資訊記錄媒體ID中包含之署名資料，產生適用上述管理裝置之公鑰的訊息並進行對照處理，而實行上述資訊記錄媒體ID之驗證處理。
20. 如請求項16之資料處理方法，其中上述資訊記錄媒體ID包含對應於所製造之資訊記錄媒體張數 W 而設定之質數 $p(w)$ 、以及依據質數 $p(w)$ 與標題固有值進行運算，藉此計算出之資料IDKey(w)，上述資料處理步驟包含以下步驟：藉由判斷上述資訊記錄媒體ID中包含之資料是否為質數，從而進行ID驗證處理。

21. 一種電腦可讀取之記錄媒體，其記錄有一電腦程式，其特徵為對應於來自資訊處理裝置之服務提供要求實行處理；且具有資料接收步驟，其自資訊處理裝置接收帶有資訊記錄媒體ID及服務ID之服務要求，及資料處理步驟，其實行接收之資訊記錄媒體ID的驗證處理，以已確認合法性為前提條件，依據該資訊記錄媒體ID取得標題固有值，自記憶部獲得與取得之標題固有值相對應的服務提供狀況資料，根據上述資訊記錄媒體ID及上述服務ID判斷是否可以提供特定服務，於判定為可提供之前提條件下，實行服務提供處理，上述記憶部儲存上述每個資訊記錄媒體ID之服務提供狀況資料，作為每個與資訊記錄媒體之儲存內容標題相對應之標題固定值的服務管理資料。
22. 一種電腦可讀取之記錄媒體，其記錄有一電腦程式，其特徵為實行對於服務提供伺服器之服務提供要求；且具有：資訊記錄媒體存取步驟，其介以上述記錄媒體介面，實行資訊記錄媒體之存取處理，及資料處理步驟，其實行介以上述記錄媒體介面自資訊記錄媒體讀取之資訊記錄媒體ID的驗證處理，並以已確認合法性為前提條件，向服務提供伺服器發送該資訊記錄媒體ID。