I410961

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I410961 B**

**(45)公告日： 中華民國 102 (2013) 年 10 月 01 日**

(21)申請案號：099106011 (22)申請日： 中華民國 99 (2010) 年 03 月 02 日

(51)Int. Cl.： ***G11B20/10 (2006.01)***

(30)優先權：2009/03/27 日本 2009-078663

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

(72)發明人：上田健二朗 UEDA, KENJIRO (JP)；小林昭榮 KOBAYASHI, SHOEI (JP)；村松克美 MURAMATSU, KATSUMI (JP)；御園耕輔 MISONO, KOUSUKE (JP)

(74)代理人：陳長文

(56)參考文獻：

| | | | |
|---|---|---|---|
| TW | 200830323A | JP | 2005-228299A |
| US | 6934851B2 | US | 2008/0005802A1 |

審查人員：林坤隆

申請專利範圍項數：11 項 圖式數：9 共 0 頁

(54)名稱

資訊處理裝置、資訊處理方法及程式

INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND PROGRAM

(57)摘要

本發明揭示一種資訊處理裝置，其包含經組態以對自一資料可記錄光碟讀取之資料執行資料處理之一資料處理單元。該資料處理單元執行用於驗證在製造該光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記是否已記錄在該光碟上的一實體標記驗證過程，及用於自該光碟獲得含有由提供該光碟之所記錄內容之一內容提供伺服器基於每一光碟所特有之一識別符之一媒體 ID 產生之一電子簽名之一符記且用於執行簽名驗證的一簽名驗證過程；且該資料處理單元在其中一實體標記之該記錄在該實體標記驗證過程中已得到確認且簽名驗證在該簽名驗證過程中有效之一條件下複製該光碟之所記錄內容。

An information processing apparatus includes a data processing unit configured to perform data processing on data read from a data recordable disc. The data processing unit performs a physical mark verification process for verifying whether or not a physical mark that is identification data unique to each of mother discs used when the disc was manufactured has been recorded on the disc, and a signature verification process for obtaining, from the disc, a token containing an electronic signature generated on the basis of a medium ID that is an identifier unique to each disc by a content providing server that provided the recorded content of the disc and for performing signature verification, and reproduces recorded content of the disc under a condition in which the recording of a physical mark in the physical mark verification process has been confirmed and signature verification in the signature verification process holds true.

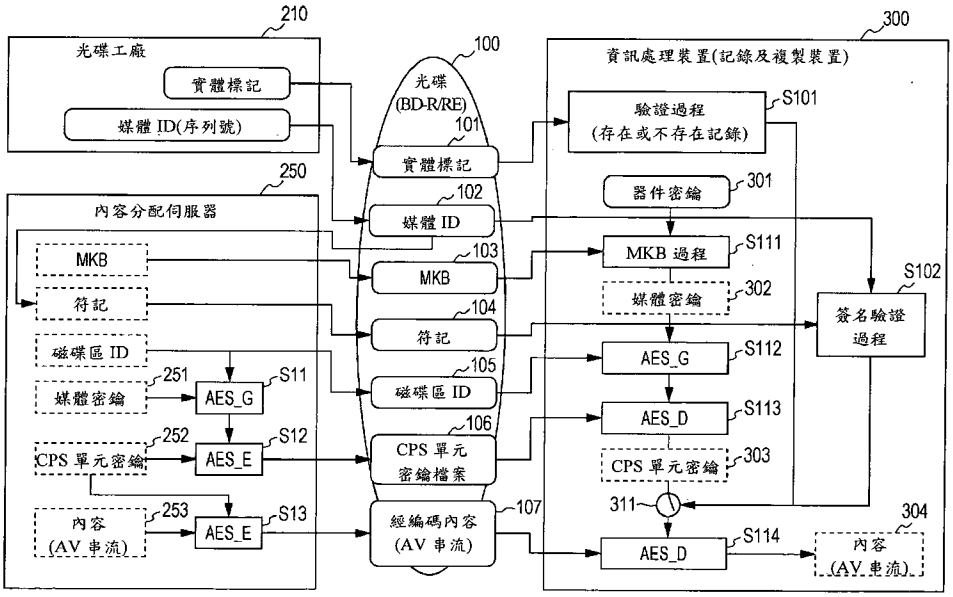


圖 3

100・・・光碟

101・・・實體標記

102・・・媒體 ID

103・・・媒體密鑰區塊(MKB)

104・・・符記

105・・・磁碟區 ID

106・・・CPS 單元密鑰檔案

107・・・經編碼內容

210・・・光碟工廠

250・・・內容提供伺服器

251・・・媒體密鑰

252・・・CPS 單元密鑰

253・・・內容

300・・・資訊處理裝置

301・・・器件密鑰

302・・・媒體密鑰

303・・・CPS 單元密鑰

304・・・內容

311・・・開關

公告本

# 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：99106011

※ 申請日： 99.3.02 ※IPC 分類：

G11B 20/10 (2006.01)

## 一、發明名稱：（中文/英文）

資訊處理裝置、資訊處理方法及程式

INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND PROGRAM

## 二、中文發明摘要：

本發明揭示一種資訊處理裝置，其包含經組態以對自一資料可記錄光碟讀取之資料執行資料處理之一資料處理單元。該資料處理單元執行用於驗證在製造該光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記是否已記錄在該光碟上的一實體標記驗證過程，及用於自該光碟獲得含有由提供該光碟之所記錄內容之一內容提供伺服器基於每一光碟所特有之一識別符之一媒體ID產生之一電子簽名之一符記且用於執行簽名驗證的一簽名驗證過程；且該資料處理單元在其中一實體標記之該記錄在該實體標記驗證過程中已得到確認且簽名驗證在該簽名驗證過程中有效之一條件下複製該光碟之所記錄內容。

## 三、英文發明摘要：

An information processing apparatus includes a data processing unit configured to perform data processing on data read from a data recordable disc. The data processing unit performs a physical mark verification process for verifying whether or not a physical mark that is identification data unique to each of mother discs used when the disc was manufactured has been recorded on the disc, and a signature verification process for obtaining, from the disc, a token containing an electronic signature generated on the basis of a medium ID that is an identifier unique to each disc by a content providing server that provided the recorded content of the disc and for performing signature verification, and reproduces recorded content of the disc under a condition in which the recording of a physical mark in the physical mark verification process has been confirmed and signature verification in the signature verification process holds true.

## 四、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件符號簡單說明：

| | |
|---|---|
| 100 | 光碟 |
| 101 | 實體標記 |
| 102 | 媒體ID |
| 103 | 媒體密鑰區塊(MKB) |
| 104 | 符記 |
| 105 | 磁碟區ID |
| 106 | CPS單元密鑰檔案 |
| 107 | 經編碼內容 |
| 210 | 光碟工廠 |
| 250 | 內容提供伺服器 |
| 251 | 媒體密鑰 |
| 252 | CPS單元密鑰 |
| 253 | 內容 |
| 300 | 資訊處理裝置 |
| 301 | 器件密鑰 |
| 302 | 媒體密鑰 |
| 303 | CPS單元密鑰 |
| 304 | 內容 |
| 311 | 開關 |

## 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】

本發明係關於一資訊處理裝置、一資訊處理方法及一程式。更特定而言，本發明係關於實現對內容之使用控制之一資訊處理裝置、一資訊處理方法及一程式。

【先前技術】

近年來，藍光光碟(注冊商標)、數位多功能光碟(DVD)等已為人們廣泛用作資料記錄媒體(資訊記錄媒體)。此等媒體用於記錄及複製各種內容，諸如，電影及音樂。

媒體類型之實例包含：其上已預先記錄資料但不允許寫入新資料之唯讀媒體，諸如，DVD-ROM媒體及BD-ROM媒體；及一使用者可在其上寫入資料之可重寫媒體，諸如，DVD-RAM/R/RW媒體、DVD+RW/+R媒體及BD-R/RE媒體。

唯讀媒體係在一光碟工廠處記錄有各種內容(諸如，舉例而言，電影及音樂)且被提供給一使用者。此外，可重寫媒體係在一使用者購買之後安裝至一使用者器件(諸如，一PC或一記錄器)中，且經由一網路下載之內容及廣播內容可記錄在其上。另一選擇係，可藉由使用安置在一公共場所之一終端機記錄並使用一使用者選定之內容。

作為使用可重寫媒體之一內容提供形式，舉例而言，電子銷售(EST)及按需製造(MoD)係可用的。EST係其中藉由使用能夠將資料寫入於一媒體上之一使用者器件(諸如，一記錄器或一PC)記錄自一內容提供伺服器等下載之內容

的一內容提供服務。MoD係其中藉由使用位於(舉例而言)一便利店或一公共空間中之一共享終端機將自一伺服器接收到之內容記錄在一媒體上的一內容提供服務。舉例而言，此等內容提供服務揭示於日本未經審查之專利申請案公開案第2008-159233號、日本未經審查之專利申請案公開案第2008-98765號等中。

除事先記錄在媒體上之內容以外，經由一廣播及經由一網路獲得之大部分內容之版權及經銷權為一內容創作者或一銷售商所有。因此，對於欲提供給使用者之大部分內容，需要進行用於防止非法拷貝之使用控制及管理。更具體而言，執行內容編碼、基於內容及媒體之識別資料之使用管理及使用控制等。舉例而言，採用其中僅允許一經授權使用者使用內容複製等以使得不執行未經允許之拷貝等之一控制組態。此外，執行其中若藉由非法拷貝生產之盜版光碟在市場上經銷則可追蹤其拷貝源之管理。

舉例而言，在製造階段將針對每一媒體皆不同之一媒體ID(序列號)寫入於媒體上。舉例而言，在可記錄光碟上將一媒體ID記錄在一燒錄區(BCA)中，該燒錄區係不同於一般資料記錄區之一特殊資料記錄區。該BCA區係不同於一普通資料記錄區之一區，且資料係藉由不同於一普通資料記錄方法之一實體刻錄過程記錄。因此，難以將記錄資料重寫在BCA區中，且在一複製過程期間需要不同於一普通資料複製過程之一特殊讀取過程。舉例而言，在其中經非法拷貝之盜版版本在市場上經銷之一情況下，若識別出一

媒體ID(序列號)，則可追蹤其拷貝源。

由於ROM媒體之媒體ID與所記錄內容之間的對應係固定，因此可識別該內容記錄源之光碟工廠，且可追蹤其拷貝源之媒體製造源。

然而，在R/RE類型媒體之情況下，內容可由一使用者按需記錄在媒體上，且媒體識別符之一媒體ID(序列號)與該內容之間的對應並不固定。因此，當某一內容之盜版版本在市場上經銷時，難以追蹤其拷貝源。因此，需要更嚴格地防止非法內容使用。本發明已揭示了將一序列號寫入至一BCA區之方法。具有某一知識之一未經授權者(諸如，生產一盜版光碟的某人)可應用所揭示之資料寫入方法來寫入一非法媒體ID(序列號)。

【發明內容】

期望提供在其中一使用者將所期望內容記錄在一資料可寫入媒體(諸如，一R/RE類型媒體)並使用該資料之一組態中能夠防止對光碟所記錄內容之未經授權使用且實現對內容之嚴格使用控制之一資訊處理裝置、一資訊處理方法及一程式。

根據本發明之一實施例，提供有一種資訊處理裝置，其包含：經組態以對自一資料可記錄光碟讀取之資料執行資料處理之一資料處理單元，其中該資料處理單元執行用於驗證在製造該資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記是否已記錄在該資料可記錄光碟上的一實體標記驗證過程，及用於自該資料可記

錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器基於每一資料可記錄光碟所特有之一識別符之一媒體ID產生之一電子簽名之一符記並用於執行簽名驗證的一簽名驗證過程；且該資料處理單元在其中一實體標記之該記錄在該實體標記驗證過程中得到確認且該簽名驗證在該簽名驗證過程中有效之一條件下複製該資料可記錄光碟之所記錄內容。

該實體標記及該媒體ID可係在一光碟工廠處記錄在該資料可記錄光碟上之資料。該符記可係含有在對該資料可讀光碟執行一內容記錄過程時由提供內容之內容提供伺服器基於該媒體ID產生之電子簽名之一符記。

根據本發明之另一實施例，提供有一種資訊處理系統，其包含：經組態以執行自一資料可記錄光碟之資料讀取之一驅動器；及包含一資料處理單元之一資訊處理裝置，該資料處理單元獲得經由該驅動器自該資料可記錄光碟讀取之資料且執行資料處理，其中該驅動器執行用於驗證在製造該資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記是否已記錄在該資料可記錄光碟上的一實體標記驗證過程，且在其中該實體標記之該記錄已在該實體標記驗證過程中得到確認之一條件下將該資料可記錄光碟之該所記錄資料輸出至該資訊處理裝置；且其中該資料處理單元執行用於自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器基於每一資料可記錄光碟所特有之一識別符之媒體ID產

生之一電子簽名之一符記且用於執行簽名驗證的一簽名驗證過程，且該資料處理單元在其中該簽名驗證在該簽名驗證過程中有效之一條件下複製該資料可記錄光碟之該所記錄內容。

該實體記錄及該媒體ID可係在一光碟工廠處記錄在一資料可記錄光碟上之資料。該符記可係含有在對該資料可記錄光碟執行一內容記錄過程時由提供內容之內容提供伺服器基於該媒體ID產生之電子簽名之一符記。

根據本發明之另一實施例，提供有一種資訊處理裝置，其包含：經組態以對自一資料可記錄光碟讀取之資料執行資料處理之一資料處理單元，其中該資料處理單元自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器產生之一電子簽名之一符記且執行一簽名驗證過程，且該資料處理單元在其中該簽名驗證在該簽名驗證過程中有效之一條件下複製該資料可記錄光碟之該所記錄內容，且其中該符記係含有基於一實體標記及一媒體ID的一計算運算結果所產生之一電子簽名之一符記，該實體標記係在製造該資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料，該媒體ID係每一資料可記錄光碟所特有之一識別符，該實體標記及該媒體ID皆記錄在該資料可記錄光碟上。

該符記可係含有基於該實體標記及該媒體ID之一互斥OR運算結果所產生之一電子簽名之一符記。該資料處理單元可對記錄在該資料可記錄光碟上之該實體標記及該媒

體ID執行一互斥OR運算且當執行用於驗證該符記中所含有之該簽名之一過程時可執行與該互斥OR運算結果之一比較過程。

該實體標記及該媒體ID可係在一光碟工廠處記錄在一資料可記錄光碟上之資料。該符記可係含有在對該資料可記錄光碟執行一內容記錄過程時由提供內容之內容提供伺服器基於該媒體ID產生之電子簽名之一符記。

根據本發明之另一實施例，提供有一種資訊處理裝置，其包含：經組態以對自一資料可記錄光碟讀取之資料執行資料處理之一資料處理單元，其中該資料處理單元自該資料可記錄光碟獲得在製造該資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記及每一資料可記錄光碟所特有之一識別符之一媒體ID，且將該實體標記及該媒體ID傳輸至一內容提供伺服器，且自該內容提供伺服器接收含有基於該實體標記及該媒體ID之計算運算結果所產生之一電子簽名之一符記及內容，且將該符記及該內容記錄在該資料可記錄光碟上。

該符記係含有基於該實體標記及該媒體ID之互斥OR運算結果所產生之一電子簽名之一符記。

該實體標記及該媒體ID可係在一光碟工廠處記錄在一資料可記錄光碟上之資料。該符記可係含有在對該資料可記錄光碟執行一內容記錄過程時由提供內容之內容提供伺服器基於該媒體ID產生之電子簽名之一符記。

根據本發明之另一實施例，提供有一種用於在一資訊處

理裝置中對自一資料可記錄光碟讀取之資料執行資料處理之資訊處理方法，該資訊處理方法包含以下步驟：藉由使用一資料處理單元驗證在製造該資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記是否已記錄在該資料可記錄光碟上；藉由使用一資料處理單元自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器基於每一資料可記錄光碟所特有之一識別符之一媒體ID產生之一電子簽名之一符記並執行簽名驗證；及藉由使用一資料處理單元在其中該實體標記之該記錄在該實體標記驗證過程中已得到確認且該簽名驗證在該簽名驗證過程中有效之一條件下複製該資料可記錄光碟之所記錄內容。

根據本發明之另一實施例，提供有一種用於在一資訊處理裝置中對自一資料可記錄光碟讀取之資料執行資料處理之資訊處理方法，該資訊處理方法包含以下步驟：藉由使用一資料處理單元對在製造該資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記及每一資料可記錄光碟所特有之一識別符之一媒體ID執行一計算過程；藉由使用一資料處理單元自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器產生之一電子簽名之一符記，且執行包含將基於該電子簽名所產生之資料與該計算運算過程之所得資料進行比較之一過程的一簽名驗證過程；及在其中該簽名驗證在該簽名驗證過程中有效之一條件下複製該資料可記錄光碟

之所記錄內容。

根據本發明之另一實施例，提供有一種用於在一資訊處理裝置中對自一資料可記錄光碟讀取之資料執行資料處理之資訊處理方法，該資訊處理方法包含以下步驟：藉由使用一資料處理單元自該資料可記錄光碟獲得在製造該資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一識別標記及每一資料可記錄光碟所特有之一識別符之一媒體ID，並將該實體標記及該媒體ID傳輸至一內容提供伺服器；及藉由使用該資料處理單元自該內容提供伺服器接收含有基於該實體標記及該媒體ID之計算運算結果所產生之一電子簽名之一符記及內容，且將該媒體ID及該內容記錄在該資料可記錄光碟上。

根據本發明之另一實施例，提供有一種非暫時性記錄媒體，其包含用於處理自一可記錄媒體讀取之資料之一程式，該程式包含以下步驟：致使一資料處理單元驗證在製造一資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記是否已記錄在該資料可記錄光碟上；致使該資料處理單元自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器基於每一資料可記錄光碟所特有之一識別符之一媒體ID產生之一電子簽名之一符記，並執行簽名驗證；及致使該資料處理單元在其中該實體標記之該記錄在該實體標記驗證過程中已得到確認且該簽名驗證在該簽名驗證過程中有效之一條件下複製該資料可記錄光碟之所記錄內容。

根據本發明之另一實施例，提供有一種非暫時性記錄媒體，其包含用於處理自一可記錄媒體讀取之資料之一程式，該程式包含以下步驟：致使一資料處理單元對在製造一資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記及每一資料可記錄光碟所特有之一識別符之一媒體ID執行一計算過程；致使該資料處理單元自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器產生之一電子簽名之一符記，並執行包含用於將基於該電子簽名所產生之資料與該計算運算過程之所得資料進行比較之一過程的一簽名驗證過程；及在其中該簽名驗證在該簽名驗證過程中有效之一條件下複製該資料可記錄光碟之所記錄內容。

根據本發明之另一實施例，提供有一種非暫時性記錄媒體，其包含用於處理自一可記錄媒體讀取之資料之一程式，該程式包含以下步驟：致使一資料處理單元自該資料可記錄光碟獲得在製造一資料可記錄光碟時所使用之母光碟中之每一者所特有之識別資料之一實體標記及每一資料可記錄光碟所特有之一識別符之一媒體ID，並將該實體標記及該媒體ID傳輸至一內容提供伺服器；及致使該資料處理單元自該內容提供伺服器接收含有基於該實體標記及該媒體ID之計算運算結果所產生之一電子簽名之一符記及內容，且將該媒體ID及該內容記錄在該資料可記錄光碟上。

舉例而言，根據本發明之一實施例之一程式係可以使用一儲存媒體或一通信媒體之一電腦可讀形式提供至一資訊

處理裝置或能夠執行各種程式碼之一電腦系統之一程式。藉由提供呈一電腦可讀形式之此一程式，對應於該程式之處理係在電腦系統上實施。

本發明之其他目標、特徵及優點將自稍後欲參照隨附圖式闡述之實施例之一更加詳細說明而變得顯而易見。在本說明書中，該系統表示複數個器件之一邏輯總成，且該等器件是否安置在相同外殼中無關緊要。

根據本發明之一實施例，在一製造階段對應於一光碟之識別資訊之一實體標記及一光碟所特有之識別資訊之一媒體ID記錄在可由一使用者記錄之光碟上。在執行一內容記錄過程時，將一媒體ID或一媒體ID及一實體標記傳輸至一內容提供伺服器，且接收包含簽名資料之一符記並將其與內容一起記錄在光碟上。在執行複製內容時，執行對一符記簽名之驗證及對一實體標記之記錄之確認，且在此等確認之條件下複製該內容。藉助此組態，實現基於對光碟及內容分配伺服器之可靠性確認之嚴格內容使用控制。

【實施方式】

下文將參照圖式詳細闡述根據本發明之實施例之一資訊處理裝置、一資訊處理方法及一程式。將以如下次序給出該等說明。

1.媒體結構之實例

2.資料記錄及複製處理實例1(第一實施例)

3.資料記錄及複製處理實例2(第二實施例)

4.資料記錄及複製處理實例3(第三實施例)

5.資料記錄及複製處理實例4(第四實施例)

6.實體標記之具體實例

7.資訊處理裝置之組態之實例

✓ X

1.媒體結構之實例

首先，將闡述本發明之一實施例中所使用之一媒體結構之一實例。可在根據本發明之一實施例之處理中使用之媒體係一使用者可將任一所期望資料記錄在其上之媒體。其實例包含一使用者可將資料寫入於其上之光碟，諸如，DVD-RAM/R/RW光碟、DVD+RW/+R光碟及BD-R/RE光碟。

圖1顯示(a)製造光碟時(記錄內容之前)之一光碟100及(b)記錄內容之後之光碟100。

(a)製造光碟時(記錄內容之前)之光碟100係在一光碟工廠(光碟製造商)處製造之一光碟。此光碟100被提供給使用者，且該使用者可將任一所期望內容(舉例而言，一電影之內容)記錄在其上。

在光碟製造時(記錄內容之前)之光碟100上，記錄一實體標記101及一媒體ID(序列號)102。此等內容係在光碟工廠處製造光碟時記錄在每一光碟上之識別資訊。更具體而言，實體標記係在製造光碟時所使用之每一母光碟所特有之識別資料。

其上記錄此等識別資訊項之光碟經由一銷售店等被提供給使用者。使用者可將含有一電影等內容之資料記錄在光

碟100上。在此實例中，假定欲記錄在光碟100上之內容係受到使用控制之內容且係如圖1中所示之經編碼內容107。

舉例而言，經編碼內容107係自一內容分配伺服器提供至一使用者之一複製裝置。不僅經編碼內容107而且各種資料皆係自內容分配伺服器提供至使用者之複製裝置，且該各種資料連同該內容記錄在一起。更具體而言，該各種資料係(諸如)用於在複製裝置中執行一內容解碼過程之資料或用於確定該複製裝置是否係其中允許內容使用之一裝置之資料的資料。

顯示於圖1之部分(b)之光碟100中之一媒體密鑰區塊(MKB)103、一符記104、一磁碟區ID 105、一CPS單元密鑰檔案106及經編碼內容107之資料係自內容分配伺服器提供至使用者之複製裝置且記錄在該使用者複製裝置中。稍後將詳細闡述該資料及記錄序列。

下文將參考圖2給出對在記錄內容之前記錄在圖1之部分(a)中所示之光碟100上之一實體標記101及媒體ID(序列號)102之一說明。

圖2顯示實體標記及媒體ID(序列號)中之每一者之(a)資料長度、(b)資料結構及(c)特徵。

實體標記具有16個位元組之一資料長度，且係由等於1個位元組之一標頭、等於2個位元組之一被許可人ID及等於13個位元組之一隨機數字形成。

該標頭係指示相關聯資料係一實體標記之識別符資料。舉例而言，定義標頭等於[0x01]。在其中欲執行解碼及複

製記錄在一光碟上之內容之一過程之一情況下，複製裝置或驅動器驗證一實體標記是否已記錄在光碟上，且在一實體標記已記錄在該光碟上之條件下對該內容執行解碼及複製。該複製裝置或該驅動器根據一預定讀取序列自實體標記記錄位置讀取該實體標記，且確認係一標頭部分之開始1個位元組是否係[0x01]。在其中開始1個位元組係[0x01]之一情況下，確定該光碟係已在其上記錄實體標記之一光碟。稍後將闡述具體處理序列。

該被許可人ID係關於已允許在其處記錄實體標記之一光碟工廠之識別資訊，或係一實體標記記錄器件之識別資訊。一隨機數字係藉助使用其中滿足一預設準則之一隨機數字產生方法所計算之資訊而形成。

該實體標記具有如下特徵：

資料藉由不同於一般資料之方法的一方法記錄在光碟上，

將資料記錄為針對每一壓模係不同之一ID，及

資料可僅由一經特許器件[實體標記記錄器件]寫入。

如上文所闡述，實體標記係藉由不同於一般資料(亦即，經編碼內容等)之記錄形式之記錄方法的一記錄方法記錄。實體標記可僅由一經特許裝置[實體標記記錄裝置]寫入。該許可係由執行內容使用管理之一管理中心給予一光碟工廠等之一許可。將應用於記錄實體標記之一實體標記記錄器件提供給一經許可光碟工廠。該實體標記記錄器件用於記錄係一壓模單元中之識別資訊之一實體標記。

該實體標記係設定在一壓模單元中之一識別符(ID)，其中相同實體標記記錄在自相同壓模製造之一光碟上。

接下來，將闡述媒體ID(序列號)。該媒體ID(序列號)具有16個位元組之一資料長度，且係由等於1個位元組之一標頭、等於2個位元組之一光碟工廠(光碟製造商)ID及等於13個位元組之一唯一值形成。

該標頭係指示相關聯資料係一媒體ID(序列號)之識別符資料。該光碟工廠(光碟製造商)ID係關於光碟製造工廠設定之一識別符(ID)。該唯一值係針對每一光碟係不同之一值，舉例而言，一序列號。

該媒體ID(序列號)係在一燒錄區(BCA)中記錄為針對每一光碟係不同之一ID之資料。如上文所闡述，該BCA區係其中資料係由不同於一典型資料記錄方法之一實體刻錄過程記錄之一區。因此，BCA區之記錄資料難以重寫，且對於該複製過程需要不同於一典型資料複製過程之一特殊讀取過程。

圖2中所示每一資料項之位元組長度及資料結構皆係實例，且可將資料長度設定為不同於圖2中所示之資料長度。此外，關於資料結構，可將每一資料項之資料長度設定為不同且可進一步將其設定為包含其他組成資料。

2.資料記錄及複製過程實例1(第一實施例)

接下來，將參照圖3給出對用於將內容記錄在一光碟上之一過程及用於自一光碟複製內容之一過程之一第一實施例之一說明。

圖3顯示：光碟工廠210，其用於製造一光碟100；一內容提供伺服器250，其用於提供含有欲記錄在光碟100上之內容之所記錄資料；及一資訊處理裝置(記錄及複製裝置)300，其用於執行在光碟100上之一內容記錄過程及讀取記錄在光碟100上之資料以複製內容之一過程。

如先前所闡述，光碟工廠210執行用於將實體標記101及媒體ID(序列號)102記錄在光碟100上之一過程。使用者購買其上已記錄實體標記101及媒體ID(序列號)102之光碟100。

使用者將光碟100裝入資訊處理裝置300中，且執行與提供內容之內容提供伺服器250之通信，且記錄該使用者選定之內容。內容提供伺服器250及資訊處理裝置300經由一網路執行通信。光碟100之記錄資料係自內容提供伺服器250提供至資訊處理裝置300，且資訊處理裝置300在光碟100上執行資料記錄。

當執行內容記錄過程時，內容提供伺服器250提供MKB 103、符記104、磁碟區ID 105、CPS單元密鑰檔案106及經編碼內容107之資料。資訊處理裝置300將自內容提供伺服器250接收到之資料記錄在光碟100上。

MKB 103係一密鑰區塊，其中產生應用於解碼經編碼內容107之一過程之一密鑰所需之一媒體密鑰作為經加密資料儲存。媒體密鑰具有可使用儲存於資訊處理裝置300中之一器件密鑰藉由一MKB過程擷取之一結構。然而，該MKB係以視情況執行一更新過程之此一方式提供且該

MKB更新至一設定，在該設定之情形下，難以藉由儲存於去啟動資訊處理裝置中之一器件密鑰獲得一媒體密鑰。

符記104係由內容提供伺服器250產生。符記104係以當資訊處理裝置300將內容記錄在光碟100上時記錄在光碟100上之媒體ID 102被傳輸至內容提供伺服器250且由內容提供伺服器250執行一簽名過程之此一方式產生之資料。

符記104含有執行(舉例而言)一內容提供過程之內容提供伺服器250之伺服器資訊作為組成資料，諸如，自伺服器之公共密鑰及伺服器識別符(ID)、記錄在光碟100上之媒體ID等形成之伺服器資訊。此外，符記104係其中附有一電子簽名之資料，該電子簽名係針對至少包含媒體ID之組成資料之資料。舉例而言，該簽名係藉由應用內容提供伺服器之一密鑰而產生。

資訊處理裝置300在解碼及複製記錄在光碟100上之經編碼內容107之前執行用於驗證符記104之簽名之一過程。資訊處理裝置300藉由使用內容提供伺服器250之公共密鑰執行對設定於符記104中之簽名之驗證，且對符記104執行一可靠性確認過程。藉助此過程，以確認經編碼內容107之供應源係一合法裝置之後，允許解碼該內容之此一方式形成該組態。稍後將闡述複製處理序列之細節。

磁碟區ID 105係以對應於由內容提供伺服器250提供之一組內容(諸如，舉例而言，某些標題之一組內容或某一週期內所提供之一組內容)之此一方式設定之識別資訊(ID)。磁碟區ID 105係由內容提供伺服器250產生且記錄在

光碟100上。

在圖3中所示之步驟S11中，內容提供伺服器250進一步使用磁碟區ID及儲存於MKB中之媒體密鑰來執行一密鑰產生過程(AES_G)。此外，在步驟S12中，內容提供伺服器250藉由使用所產生之密鑰對係內容之加密密鑰之CPS單元密鑰252執行一加密過程(AES_E)以產生一CPS單元密鑰檔案106。將此CPS單元密鑰檔案106記錄在光碟100上。

此外，在步驟S13中，內容提供伺服器250對內容253執行一加密過程(AES_E)，其中應用CPS單元密鑰252以產生經編碼內容107。將此經編碼內容107記錄在光碟100上。

接下來，將給出對資訊處理裝置300之處理之一說明，該資訊處理裝置執行用於解碼及複製記錄在光碟100上之經編碼內容107之一過程。顯示於圖3之資訊處理裝置300內側之步驟S101至S114之處理係由資訊處理裝置300之資料處理單元執行。資訊處理裝置300經組態以包含其中儲存有欲由資料處理單元執行之程式之一記憶體，且該資料處理單元經組態以包含(舉例而言)根據自該記憶體讀取之一程式執行資料處理之一CPU。

資訊處理裝置300在該記憶體中具有一器件密鑰301。器件密鑰301係用於應用來自MKB 103獲得一媒體密鑰之密鑰資料。

首先，在步驟S101中，資訊處理裝置300執行用於驗證實體標記101是否已記錄在光碟100上之一過程。如先前所闡述，將此驗證過程執行為(舉例而言)其中讀取實體標記

101之開始1個位元組之標頭資訊以確定該標頭資訊是否具有指示一實體標記之資訊的一確定過程。

在其中實體標記101尚未記錄在光碟100上之一情況下，不執行後續處理。亦即，取消對該內容之使用(複製)過程。

若在步驟S101中確認實體標記101已記錄在光碟100上，則過程繼續進行至步驟S102。在步驟S102中，資訊處理裝置300讀取記錄在光碟100上之媒體ID 102及符記104，且執行一簽名驗證過程。如先前所闡述，符記104係含有一簽名之資料，該簽名係針對含有記錄在光碟100上之媒體ID 102之資料。符記104係由內容提供伺服器250產生之一簽名。

在步驟S102中，資訊處理裝置300藉由應用內容提供伺服器250之公共密鑰來執行簽名驗證。對符記104中所含有之簽名執行使用內容提供伺服器250之公共密鑰的資料處理。將該處理結果與記錄在光碟100上之媒體ID 102之組成資料進行比較。當其匹配時，確定該簽名驗證有效。作為簽名驗證有效之一結果，確認符記104之可靠性。此對應於用於確認經編碼內容107之供應源(亦即，內容提供伺服器250)係一合法裝置之一過程。在進行此確認之後，允許解碼該內容。

在其中簽名驗證無效之一情況下，確定符記104係非法的，且內容提供伺服器250確定內容提供伺服器250不係一合法裝置。在此情況下，取消後續處理。亦即，取消內容

使用(複製)過程。

僅當在步驟S101中確認已將實體標記101記錄在光碟100上且在步驟S102中確認簽名驗證過程有效時，該過程才繼續進行至下一過程，亦即，針對記錄在光碟100上之經編碼內容107之一解碼及複製序列(S111至S114)。

將闡述該複製序列。最初，在步驟S111中，藉由使用儲存於資訊處理裝置300之記憶體中之器件密鑰301對自光碟100讀取之MKB 103執行一MKB過程，藉此自MKB 103擷取一媒體密鑰302。

接下來，在步驟S112中，執行使用自光碟100讀取之磁碟區密鑰105及自MKB獲得之媒體密鑰302之一密鑰產生過程(AES_G)以產生應用於解碼儲存於光碟100上之CPS單元密鑰檔案106之一密鑰。

接下來，在步驟S113中，藉由使用所產生之密鑰，執行用於解碼自光碟100讀取之CPS單元密鑰檔案106之一過程(AES_D)以獲得一CPS單元密鑰303。

接下來，在步驟S114中，藉由使用所獲得之CPS單元密鑰303，執行用於解碼自光碟100讀取之經編碼內容107之一過程(AES_D)以獲得並複製內容304。

圖中顯示一開關311以圖解說明僅當在步驟S101之過程中確認實體標記101已記錄在光碟100上時且當符記104之可靠性已在步驟S102之簽名驗證過程中得到確認時，可解碼並複製該內容。亦即，一實體開關不必存在於資訊處理裝置300中，且該開關係概念上顯示允許處理序列繼續或

停止處理序列繼續之一開關。

在圖3中，開關311之位置(亦即，處理之停止位置)顯示於步驟S114之前。然而，舉例而言，開關311之位置可係解碼或複製序列之任一位置，諸如，在步驟S111之MKB過程之前。

亦即，需要在完成對所有步驟S111至S114之處理之前執行對步驟S101及S102之處理，即實體標記101已記錄在光碟100上，且記錄在光碟100上之符記之可靠性得到確認。

如上文所闡述，在該實施例中，記錄在光碟100上之經編碼內容之使用允許條件設定如下：

(1)確認實體標記101已記錄在光碟100上，及

(2)確認記錄在光碟100上之符記104(針對媒體ID 102之簽名)之可靠性。

此兩個確認係允許使用記錄在光碟100上之經編碼內容之條件。若不滿足該等條件中之任一者，則不允許使用該內容。

在確認實體標記101已記錄在光碟100上之情況下，確認光碟100係在一合法工廠生產之一光碟。亦即，確認光碟100係具有藉由使用一經許可實體標記記錄器件記錄之一實體標記之一光碟。此外，在簽名驗證記錄在光碟100上之符記104(針對媒體ID 102之簽名)之情況下，確認內容提供伺服器之可靠性。

符記104含有針對媒體ID 102之簽名資料，且媒體ID 102係在光碟之一製造實體之光碟工廠處記錄。因此，光碟工

廠(其係上面已記錄有媒體ID之光碟之製造實體)與內容分配伺服器(其係內容之提供主體且提供上面記錄有媒體ID之光碟及含有簽名(其針對含有媒體ID之資料)之符記)之間的對應係藉由一符記聯繫起來，從而使該對應清晰。

如上文所闡述，本發明中設定，在確認實體標記101已記錄在光碟100上且記錄在光碟100上之符記104(針對媒體ID 102之簽名)之簽名驗證有效之條件下允許使用記錄在光碟100上之經編碼內容107。

作為確認實體標記101已記錄在光碟100上之一結果，光碟可靠性得到確認，此證明光碟100係在一合法工廠生產。此外，作為符記104之簽名驗證之一結果，確認由合法內容分配伺服器提供之內容已記錄在光碟上。以上述方式確認內容提供源及光碟供應源之可靠性之事實用作允許內容使用之條件。此一內容使用控制組態使得可防止使用一非法光碟或防止使用一非法內容提供伺服器所提供之內容。因此，可實現嚴格的內容使用控制。

3.資料記錄及複製處理實例2(第二實施例)

接下來，將參照圖4給出對根據本發明的用於將內容記錄在一光碟上之一過程及用於自一光碟複製內容之一過程之一第二實施例之一說明。

圖4顯示：一光碟工廠210，其製造一光碟100；內容提供伺服器250，其提供含有欲記錄在光碟100上之內容之資料；一驅動器350，其執行用於將內容記錄在光碟100上之一過程並自光碟100讀取資料；及一資訊處理裝置(記錄複

製裝置)320，其經由驅動器350藉由使用光碟100來執行記錄及複製資料。

參照圖3所闡述之第一實施例係以驅動器包含於資訊處理裝置300中之此一方式組態。然而，圖4中所示之第二實施例係以驅動器350及資訊處理裝置320係分離器件之此一方式組態。

光碟工廠210執行用於將實體標記101及媒體ID(序列號)102記錄在光碟100上之一過程。使用者購買其上已記錄實體標記101及媒體ID(序列號)102之光碟100。

使用者將光碟100裝入驅動器350中。資訊處理裝置320執行與提供內容之內容提供伺服器250之通信且記錄該使用者選定之內容。

在光碟100上之資料記錄過程與先前參照圖3所闡述之處理大致相同。當執行內容記錄過程時，內容提供伺服器250將MKB 103、符記104、磁碟區ID 105、CPS單元密鑰檔案106及經編碼內容107之資料提供至資訊處理裝置320。資訊處理裝置320經由驅動器350將自內容提供伺服器250接收到之此等資料項記錄在光碟100上。

將闡述對記錄在光碟100上之經編碼內容107之解碼過程及複製過程。在該實施例中，將解碼過程及複製過程執行為驅動器350及資訊處理裝置320兩者之處理。

資訊處理裝置320在記憶體中具有一器件密鑰321。器件密鑰321係用於自MKB 103獲得一媒體密鑰之密鑰資料。

最初，在步驟S201中，驅動器350執行對實體標記101是

否已記錄在光碟100上之一驗證過程。如先前所闡述，將此驗證過程執行為其中(舉例而言)讀取實體標記101之開始1個位元組之標頭資訊且確定該標頭資訊是否具有指示一實體標記之資料之一過程。

在其中實體標記101尚未記錄在光碟100上之一情況下，不執行後續處理。亦即，圖中所示之開關351斷開，且不執行步驟S202中及步驟S202之後之處理。類似於上述之第一實施例，開關351係出於圖解說明而顯示，且不必存在一實體開關。亦即，該開關係用於示意性顯示允許處理繼續或停止處理繼續之一開關。

顯示於圖4之驅動器350中之步驟S202之複製控制過程係其中將記錄在光碟100上之MKB 103...經編碼內容107經由驅動器350提供至資訊處理裝置320之一過程。當驅動器350在步驟S201中確定實體標記101尚未記錄在光碟100上時，不執行步驟S202之過程，且不將記錄在光碟100上之資料提供至資訊處理裝置320。因此，不複製該內容。

當驅動器350在步驟S201中確定實體標記101已記錄在光碟100上時，在步驟S202中，驅動器350將記錄在光碟100上之MKB 103...經編碼內容107依序地提供至資訊處理裝置320。

接下來，在步驟S211中，資訊處理裝置320藉由使用經由驅動器350自光碟100讀取之媒體ID 102及符記104執行一簽名驗證過程。如先前所闡述，符記104係由內容分配伺服器250產生之資料，其含有針對記錄在光碟100上之媒

體ID 102之簽名。

資訊處理裝置320對自光碟100讀取之符記104執行一簽名驗證過程。對符記104中所含有之簽名執行使用內容提供伺服器250之公共密鑰的資料處理。執行處理結果與記錄在光碟100上之媒體ID 102之組成資料、其雜湊值等之比較。若其匹配，則確定該簽名驗證有效。

當其不匹配時，確定該簽名驗證無效，亦即，確定記錄在光碟100上之符記104無效，且確定內容提供伺服器250不係一合法裝置。在此情況下，取消後續處理。亦即，取消內容使用(複製)過程。

僅當驅動器350在步驟S211中確認實體標記101已記錄在光碟100上時且當在步驟S201中簽名驗證過程有效時，該過程才繼續進行至下一過程，亦即，對記錄在光碟100上之經編碼內容107之解碼及複製序列(S221至S224)。

步驟S221至S224之處理與第一實施例中參照圖3所闡述之步驟S111至S114之處理相同，且因此省略對其之說明。該圖中所示之開關321類似於上述第一實施例係出於圖解說明而闡述，且不必實體存在。

亦即，開關321係出於圖解說明而顯示，其指示僅當步驟S211之簽名驗證過程有效時才可解碼及複製內容。開關321之位置(亦即，該過程之停止位置)顯示於圖4中之步驟S224之前。另一選擇係，開關321之位置可係內容之解碼及複製序列之任一位置(諸如，舉例而言，在步驟S221之MKB過程之前)。

同樣，在該實施例中，記錄在光碟100上之經編碼內容之使用允許條件設定如下：

(1)確認實體標記101已記錄在光碟100上，及

(2)確認記錄在光碟100上之符記104(針對媒體ID 102之簽名)之可靠性。

此兩個確認係允許使用記錄在光碟100上之經編碼內容之條件。

若不滿足該等條件中之任一者，則不允許使用該內容。

同樣，在該第二實施例中，類似於第一實施例，藉由確認實體標記101已記錄在光碟100上，確認光碟100係在一合法工廠生產之光碟可靠性。此外，作為符記104之簽名驗證之一結果，確認由合法內容分配伺服器提供之內容已記錄在光碟上。以上述方式確認內容提供源及光碟供應源之可靠性之事實用作允許內容使用之條件。此一內容使用控制組態使得可防止使用一非法光碟或防止使用一非法內容提供伺服器所提供之內容。因此，可實現嚴格的內容使用控制。

4.資料記錄及複製處理實例3(第三實施例)

接下來，將參照圖5給出對根據本發明的用於將內容記錄在一光碟上之一過程及用於自一光碟複製內容之一過程之一第三實施例之一說明。

該第三實施例類似於第一實施例具有其中資訊處理裝置300與一驅動器整合在一起之一組態。圖5顯示：一光碟工廠210，其製造光碟100；一內容提供伺服器250，其提供

含有欲記錄在光碟100上之內容之記錄資料；及一資訊處理裝置(記錄複製裝置)300，其在光碟100上執行一內容記錄過程、讀取記錄在光碟100上之資料及複製內容。

如先前所闡述，光碟工廠210執行用於將實體標記101及媒體ID(序列號)102記錄在光碟100上之一過程。使用者購買其上已記錄實體標記101及媒體ID(序列號)102之光碟100。

使用者將光碟100裝入資訊處理裝置300中，且執行與提供內容之內容提供伺服器250之通信，且記錄該使用者選定之內容。內容提供伺服器250及資訊處理裝置300經由一網路執行通信。光碟100之記錄資料係自內容提供伺服器250提供至資訊處理裝置300，且資訊處理裝置300在光碟100上執行資料記錄。內容提供伺服器250及資訊處理裝置300經由一網路執行通信。光碟100之記錄資料係自內容提供伺服器250提供至資訊處理裝置300，且資訊處理裝置300在光碟100上執行資料記錄。

當執行內容記錄過程時，內容提供伺服器250將MKB 103、符記108、磁碟區ID 105、CPS單元密鑰檔案106及經編碼內容107之資料提供至資訊處理裝置320。資訊處理裝置320經由驅動器350將自內容提供伺服器250接收到之資料記錄在光碟100上。

資料處理過程與參照圖3所闡述之第一實施例之差異係符記108之結構。

在先前所闡述之第一實施例中，記錄在光碟100上之符

記104具有針對媒體ID 102之簽名資料。亦即，資訊處理裝置300僅將記錄在光碟100上之媒體ID 102傳輸至內容提供伺服器250。內容提供伺服器250產生含有基於媒體ID之一簽名之符記104且將該簽名提供為光碟100之記錄資料。

與上述情況不同，在該實施例中，資訊處理裝置300將記錄在光碟100上之實體標記101及媒體ID 102之兩個資料項傳輸至內容提供伺服器250。當內容提供伺服器250接收實體標記101及媒體ID 102之兩個資料項時，在圖5中所示之步驟S21中，內容提供伺服器250對實體標記101及媒體ID 102之兩個資料項執行互斥OR運算。

藉由使用該兩個資料之互斥OR運算之結果，產生一簽名。亦即，針對實體標記101及媒體ID 102之兩個資料之互斥OR運算結果或基於自該結果所產生之資料產生一簽名，且產生含有此簽名資料之一符記。內容提供伺服器250將以上述方式產生之符記傳輸至資訊處理裝置300。資訊處理裝置300將自內容提供伺服器250接收到之符記記錄在光碟100上。結果係記錄在圖5之光碟100上之一符記108。

亦即，在該實施例中，記錄在光碟100上之符記108經組態以含有不僅基於媒體ID而且基於實體標記之組成資料所產生之一簽名。

記錄在光碟100上之其他資料(亦即，MKB 103、磁碟區ID 105、CPS單元密鑰檔案106及經編碼內容107)藉由與上述第一實施例相同之處理記錄在光碟100上。

將闡述對記錄在光碟100上之經編碼內容107之一解碼過程及一複製過程。資訊處理裝置300在記憶體中具有一器件密鑰301。器件密鑰301係用於自MKB 103獲得一媒體密鑰之密鑰資料。

最初，在步驟S311中，資訊處理裝置300讀取記錄在光碟100上之實體標記101及媒體ID 102，且對此兩個資料執行一互斥OR運算。

接下來，在步驟S312中，讀取記錄在光碟100上之符記108，且執行一簽名驗證過程。如先前所闡述，符記108係含有針對記錄在光碟100上之實體標記101及媒體ID 102之互斥OR結果之一簽名之資料。符記108係由內容提供伺服器250產生之一簽名。

在步驟S312中，資訊處理裝置300藉由使用內容提供伺服器250之公共密鑰執行簽名驗證。對符記108中所含有之簽名執行使用內容提供伺服器250之公共密鑰的資料處理，且將其處理結果與在步驟S311中所產生之資料進行比較。

在步驟S311中，讀取記錄在光碟100上之實體標記101及媒體ID 102，且計算此兩個資料之一互斥OR結果。將此計算結果與其中已將公共密鑰應用於符記108中所含有之簽名之資料處理結果進行比較。

當其匹配時，確定該簽名驗證有效。作為該簽名驗證有效之一結果，確認符記108之可靠性。此對應於經編碼內容107之供應源(亦即，內容提供伺服器250)係一合法裝置

且光碟製造源之光碟工廠係可靠之確認。在進行此確認之後，允許解碼該內容。

在其中簽名驗證無效之一情況下，確定符記108無效，且確定內容提供伺服器或光碟製造工廠係非法的。在此情況下，取消後續處理。亦即，取消內容使用(複製)過程。

僅在簽名驗證過程在步驟S312中有效之情況下，該過程繼續進行至下一過程，亦即，對記錄在光碟100上之經編碼內容107之一解碼及複製序列(S321至S324)。

步驟S321至S324之處理係與參照圖3所闡述之步驟S111至S114相同之處理，且因此省略對其之說明。圖中所示之一開關311類似於上述第一實施例係出於圖解說明而闡述，且不必實體存在。

亦即，開關311經顯示以闡述僅在步驟S312之簽名驗證過程有效之情況下才可解碼或複製內容。開關311之位置(亦即，過程停止位置)顯示於圖5中之步驟S324之前。另一選擇係，開關311之位置可係內容解碼及複製序列之任一位置(諸如，舉例而言，在步驟S321之MKB過程之前)。

在該實施例中，記錄在光碟100上之經編碼內容之使用允許條件係：

確認(1)記錄在光碟100上之符記108(針對基於實體標記101及媒體ID 102之計算運算結果之簽名)之可靠性。

此簽名驗證過程係包含實體標記101及媒體ID已記錄在光碟100上之確認及已記錄由一合法內容分配伺服器產生其一簽名之一符記之確認的一過程。

亦即，作為符記108之簽名驗證之一結果，確認光碟100係由具有一經許可實體標記記錄器件之一合法工廠所生產之一光碟且由合法內容分配伺服器提供之內容已記錄在該光碟上。

將光碟供應源及內容提供源之可靠性以上述方式得到確認設定為一內容使用允許條件。

藉助此一內容使用控制組態，可防止使用一非法光碟或防止使用一非法內容提供伺服器所提供之內容。因此，可實現嚴格的內容使用控制。

在參照圖5所闡述之處理實例中，將記錄在光碟100上之實體標記101及媒體ID之一互斥OR運算結果用作用於產生符記108中欲含有之簽名資料之資訊。本發明不侷限於一互斥OR運算，亦可使用其他運算。亦即，簽名可基於藉由一計算運算獲得之一計算值而產生，在該計算運算中使用實體標記101及媒體ID作為輸入值。

5.資料記錄及複製處理實例4(第四實施例)

接下來，將參照圖6給出對用於將內容記錄在一光碟上之一過程及用於自一光碟複製內容之一過程之一第四實施例之一說明。

圖6顯示：一光碟工廠210，其製造一光碟100；一內容提供伺服器250，其提供含有欲記錄在光碟100上之內容之資料；一驅動器350，其執行用於將內容記錄在光碟100上之一過程及自光碟100讀取資料；及一資訊處理裝置(記錄複製裝置)320，其經由驅動器350藉由使用光碟100執行資

料記錄及複製。

該實施例類似於先前參照圖4所闡述之組態以驅動器350及資訊處理裝置320係分離器件之此一方式組態。此外，記錄在光碟100上之符記108以與參照圖5所闡述之第三實施例相同之方式經組態以包含針對基於實體標記101及媒體ID 102之計算運算結果之一簽名。

對光碟100之一資料記錄過程係幾乎與先前參照圖5所闡述之第三實施例相同之過程。當執行該內容記錄過程時，內容提供伺服器250將MKB 103、符記108、磁碟區ID 105、CPS單元密鑰檔案106及經編碼內容107之資料提供至資訊處理裝置320。資訊處理裝置320經由驅動器350將自內容提供伺服器250接收到之此等資料記錄在光碟100上。

符記108經組態以包含不僅基於媒體ID而且基於實體標記之組成資料所產生之一簽名。當在光碟100上執行一內容記錄過程時，資訊處理裝置320經由驅動器350讀取記錄在光碟100上之實體標記101及媒體ID 102。資訊處理裝置320將此兩個資料傳輸至內容提供伺服器250。當內容提供伺服器250接收到實體標記101及媒體ID 102之兩個資料時，在圖6中所示之步驟S21中，內容提供伺服器250對實體標記101及媒體ID 102之兩個資料執行一互斥OR運算。

藉由使用此兩個資料之互斥OR運算之一結果產生一簽名。亦即，一簽名係基於實體標記101及媒體ID 102之兩個資料之一互斥OR結果或針對自此結果所產生之資料而產生，且產生含有此簽名資料之一符記。內容提供伺服器

250將以上述方式所產生之符記傳輸至資訊處理裝置320。資訊處理裝置320經由驅動器350將自內容提供伺服器250接收到之符記記錄在光碟100上。此結果係記錄在圖6之光碟100上之符記108。

將闡述用於解碼及複製記錄在光碟100上之經編碼內容107之過程。資訊處理裝置320在記憶體中具有一器件密鑰321。器件密鑰321係用於自MKB 103獲得一媒體密鑰之密鑰資料。

首先，在步驟S401中，資訊處理裝置320經由驅動器350讀取記錄在光碟100上之實體標記101及媒體ID 102，且對此兩個資料執行一互斥OR運算。

接下來，在步驟S402中，經由驅動器350讀取記錄在光碟100上之符記108，且執行一簽名驗證過程。如先前所闡述，符記108係含有針對記錄在光碟100上之實體標記101及媒體ID 102之互斥OR結果之一簽名之資料。符記108係由內容提供伺服器250產生之一簽名。

在步驟S402中，資訊處理裝置320藉由使用內容提供伺服器250之公共密鑰執行簽名驗證。對符記108中所含有之簽名執行使用內容提供伺服器250之公共密鑰的資料處理，且將其處理結果與在步驟S401中所產生之資料進行比較。

在步驟S401中，計算記錄在光碟100上之實體標記101及媒體ID 102之一互斥OR結果。將此計算結果與其中將公共密鑰用於符記108中所含有之簽名之一資料處理結果進行

比較。

當其匹配時，確定該簽名驗證有效。作為該簽名驗證有效之一結果，確認符記108之可靠性。此對應於確認經編碼內容107之供應源(亦即，內容提供伺服器250)係一合法器件且確認一光碟製造源之光碟工廠之可靠性。在進行此確認之後，允許解碼該內容。

在其中簽名驗證無效之一情況下，確定符記108為無效，且確定內容提供伺服器或光碟製造工廠為無效。在此情況下，取消後續處理。亦即，取消內容之使用(複製)過程。

僅在簽名驗證過程在步驟S402中有效之情況下，該過程繼續進行至下一過程，亦即，對記錄在光碟100上之經編碼內容107之一解碼及複製序列(S411至S414)。

步驟S411至S414之處理係與參照圖3所闡述之步驟S111至S114相同之處理，且因此省略對其之一說明。圖中所示之一開關321類似於先前所闡述之實施例係出於圖解說明而闡述，且不必實體存在。其之位置可係步驟S411至S414之前之任一位置，只要該位置係在步驟S414之前。

類似於上文參照圖5所闡述之第三實施例，在該實施例中，其中允許使用記錄在光碟100上之經編碼內容之條件如下：(1)確認記錄在光碟100上之符記108(針對基於實體標記101及媒體ID 102之計算運算結果之簽名)之可靠性。

此簽名驗證過程係包含實體標記101及媒體ID已記錄在光碟100上之一確認及已記錄由一合法內容分配伺服器產

生其一簽名之一符記之一確認的一過程。

亦即，藉由符記108之簽名驗證確認光碟100係在具有一經許可實體標記記錄器件之一合法工廠生產之一光碟且由一合法內容分配伺服器提供之內容已記錄在該光碟上。

光碟供應源及內容提供源之可靠性如上述已得到確認係允許內容使用之條件。

藉助此一內容使用控制組態，可防止使用一非法光碟或使用由一非法內容提供伺服器提供之內容。因此，可實現嚴格的內容使用控制。

在參照圖6所闡述之處理實例中，將記錄在光碟100上之實體標記101及媒體ID之一互斥OR運算結果用作用於產生符記108中欲含有之簽名資料之資訊。本發明不侷限於一互斥OR運算，亦可使用其他運算。亦即，一簽名可經組態以基於藉由執行一計算運算獲得之計算值而產生，在該計算運算中，使用實體標記101及媒體ID作為輸入值。

6.實體標記之具體實例

如上文參照圖2所闡述，一實體標記及一媒體ID(序列號)記錄在一光碟上。舉例而言，媒體ID(序列號)藉由一燒錄過程記錄在一光碟上之一燒錄區(BCA)中。已揭示了此記錄方法。

另一方面，未揭示記錄一實體標記之方法。更具體而言，實體標記僅記錄在由一內容管理中心(諸如，高級存取內容系統(AACS))向一經許可光碟工廠提供之一實體標記記錄器件中。

參照圖7，下文將闡述一實體標記之記錄結構之一實例。一實體標記之記錄之一實例(稍後將闡述)圖解說明可用作一實體標記記錄形式之結構之一實例。本發明中可使用之一實體標記之記錄結構之一實例並不侷限於下文欲闡述之一實體標記。

圖7顯示用於一可記錄光碟之一實體標記之記錄結構之一實例。在一可記錄光碟上，如圖7之部分(a)中所示，沿磁軌寬度方向位移之凹槽(所謂之擺動凹槽(wobble))形成於一預先記錄資料區域中，該預先記錄資料區域在一光碟製造階段形成於該光碟之內周邊側。光碟在出貨時等資訊記錄在此預先記錄資料區域中。舉例而言，該等凹槽係記錄在一可記錄光碟之一導入區中之唯讀凹槽，諸如日本未經審查專利申請案公開案第2003-12332號中所揭示。

假定圖7之部分(a1)顯示一預先記錄資料區域之記錄資料。可藉由使用一預定時脈信號作為一同步化信號來讀取該預先記錄資料區域之記錄資料，可根據圖7之部分(a2)中所示之一時脈信號來讀取該記錄資料。

可以疊加在預先記錄資料區域之記錄資料上之此一方式隱藏實體標記。舉例而言，圖7之部分(b1)顯示其中以疊加在預先記錄資料區域之記錄資料上之此一方式隱藏一實體標記之一結果。

在圖7之部分(b1)中所示之實體標記隱藏資料中，圖7之部分(a1)中所示之原始資料之位移位置自時脈定時偏移。偏移方向係一向前方向(正方向)或一向後方向(反方向)。

根據形成欲記錄之實體標記之位元上之資訊確定此偏移方向。若形成實體標記之位元係[1]，則產生沿正方向之一偏移，且若其係[0]，則產生沿反方向之一偏移，或執行其之一逆過程。然而，由於此偏移係一極小位移，因此可出現若攜帶雜訊則不可複製之情況。因此，期望其中基於沿複數個磁軌之方向形成之類似位移疊加實體標記之一區。當執行一實體標記複製過程時，可藉由如下設定讀取實體標記，其中在其中實體標記疊加之區中偵測位置位移，且在其中偵測到正方向位移(其之數目係一臨限值或更多)之一情況下將邏輯值設定為1，且在其中偵測到反方向位移(其之數目係一臨限值或更多)之一情況下，將邏輯值設定為0。亦即，當製造用於製造一壓模之一母光碟時，在其中關於出貨時之資訊記錄在導入區內之擺動凹槽中，在記錄實體標記時母光碟所特有之位移極小。因此，唯一標記亦轉印至藉由使用母光碟所生產之壓模。此外，類似實體標記轉印至基於壓模大規模生產之可記錄光碟。

除圖7中所示之實體標記之結構以外，各種記錄過程皆可能。然而，設定此記錄方法未被揭示。亦即，實體標記係可僅由被提供至僅一特許光碟工廠之實體標記記錄器件藉由使用一未經揭示之記錄方法記錄之資料。

7.資訊處理裝置之組態實例

參照圖8及圖9，將給出對執行對應於上述實施例之處理之一資訊處理裝置之功能及組態之一說明。圖8顯示一資訊處理裝置之組態之一實例。

如圖8中所示，資訊處理裝置包含一輸入單元711、一資料處理單元712、一通信單元713、一輸出單元714、一記憶體715及一媒體介面716。圖8中所示之資訊處理裝置經由媒體介面716對由(舉例而言)一DVD、一藍線光碟(注冊商標)等形成之一媒體720執行資料記錄或執行自媒體720之資料複製。

輸入單元711接收使用者操作資訊。更具體而言，通信單元713執行與一內容提供伺服器之通信。

在記憶體715中，儲存經由通信單元713接收之充當一器件唯一密鑰之一器件密鑰、資料、程式等。資料處理單元712執行一內容記錄及複製過程且亦經由通信單元713執行對一資料傳輸及接收過程之控制。舉例而言，資料處理單元712根據上述第一實施例至第四實施例之處理執行內容記錄及複製控制過程。

圖9顯示一驅動器件730與其分離之一資訊處理裝置之組態之一實例。驅動器730包含一資料處理單元731及一記憶體732。經由一通信IF 717執行與驅動器730之資料通信。驅動器730內之資料處理單元731根據儲存於記憶體732中之一程式執行處理。更具體而言，其實例包含參照圖4所闡述之一實體標記驗證過程及用於自一光碟讀取的資料之一輸入/輸出控制過程。剩餘組態與參照圖8所闡述之組態相同。

上文雖然已參照具體實施例詳細闡述了本發明。然而，熟悉此項技術者明瞭可在本發明之精神及範疇內對該等實

施例做出修改及替換。亦即，已將本發明揭示為實例性實施例，而不應視為侷限性。為確定本發明之要旨，應慮及申請專利範圍。

說明書中所闡述之該等系列過程可由硬體、軟體或兩者之一組合執行。在其中該等系列過程欲由軟體執行之情況下，記錄處理序列之一程式可安裝在一電腦中嵌於專用硬體中之一記憶體中且被執行。另一選擇係，該程式可安裝在能夠執行各種過程之一通用電腦上且被執行。舉例而言，該程式可預先記錄在一記錄媒體上。除將程式自記錄媒體安裝至一電腦外，該程式可經由一網路(諸如，一區域網路(LAN)或網際網路)被接收，且可安裝至一記錄媒體(諸如，其中所含之一硬碟)中。

說明書中所闡述之各種過程不必以所闡述次序依序執行，且可根據處理效能或根據執行該等過程之一裝置之需要並行或個別地執行。在本說明書中，該系統表示複數個器件之一邏輯總成，且該等器件是否安置於相同外殼中無關緊要。

本申請案含有與2009年3月27日在日本專利局提出申請之日本優先權專利申請案JP 2009-078663中所揭示之標的物相關之標的物，該申請案之全部內容藉此以引用方式併入本文中。

熟習此項技術者應理解，可端視設計需求及其他因素作出各種修改、組合、子組合及變更，只要其在隨附申請專利範圍或其等效範圍之範疇內。

【圖式簡單說明】

圖1圖解說明一光碟及所儲存資料之結構之實例；

圖2圖解說明記錄在一光碟上之識別資料；

圖3圖解說明根據本發明之一實施例使用一光碟之一資料記錄過程及一資料複製過程之實例；

圖4圖解說明根據本發明之一實施例使用一光碟之一資料記錄過程及一資料複製過程之實例；

圖5圖解說明根據本發明之一實施例使用一光碟之一資料記錄過程及一資料複製過程之實例；

圖6圖解說明根據本發明之一實施例使用一光碟之一資料記錄過程及一資料複製過程之實例；

圖7圖解說明一實體標記之一實例；

圖8圖解說明根據本發明之一實施例之一資訊處理裝置之組態之一實例；及

圖9圖解說明根據本發明之一實施例之一資訊處理裝置之組態之一實例。

【主要元件符號說明】

| | |
|---|---|
| 100 | 光碟 |
| 101 | 實體標記 |
| 102 | 媒體ID |
| 103 | 媒體密鑰區塊(MKB) |
| 104 | 符記 |
| 105 | 磁碟區ID |
| 106 | CPS單元密鑰檔案 |

| | |
|---|---|
| 107 | 經編碼內容 |
| 108 | 符記 |
| 210 | 光碟工廠 |
| 250 | 內容提供伺服器 |
| 252 | CPS單元密鑰 |
| 253 | 內容 |
| 300 | 資訊處理裝置 |
| 301 | 器件密鑰 |
| 302 | 媒體密鑰 |
| 303 | CPS單元密鑰 |
| 304 | 內容 |
| 311 | 開關 |
| 320 | 資訊處理裝置 |
| 321 | 器件密鑰 |
| 350 | 驅動器 |
| 351 | 開關 |
| 711 | 輸入單元 |
| 712 | 資料處理單元 |
| 713 | 通信單元 |
| 714 | 輸出單元 |
| 715 | 記憶體 |
| 716 | 媒體介面 |
| 717 | 通信IF |
| 720 | 媒體 |

730 驅動器件/驅動器

731 資料處理單元

732 記憶體

P.1-7

## 七、申請專利範圍：

1. 一種資訊處理裝置，其包括：

一資料處理單元，其經組態以對自一資料可記錄光碟讀取之資料來執行資料處理，

其中該資料處理單元執行

一實體標記驗證過程，其用於驗證一實體標記已記錄在該資料可記錄光碟上，該實體標記為在製造該資料可記錄光碟時所使用之一來源光碟中所特有及對應之識別資料，

一簽名驗證過程，其用於自該資料可記錄光碟獲得一符記，該符記含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器所產生之一電子簽名，其中該符記係由該內容提供伺服器於一寫入該記錄內容之時間點，為用於回應於由該資料可記錄光碟接收之一媒體ID之簽名驗證過程而產生，且該媒體ID為該資料可記錄光碟所特有且為於一製造該資料可記錄光碟之時間點記錄於該資料可記錄光碟之一識別符，及

一重製過程，該重製過程在其中一實體標記之記錄在該實體標記驗證過程中得到確認且該簽名驗證在該簽名驗證過程中為有效之一條件下重製該資料可記錄光碟之所記錄內容。

2. 如請求項1之資訊處理裝置，

其中：

該實體標記及該媒體ID係在該寫入該記錄內容之時間

點前於一光碟工廠處記錄在該資料可記錄光碟上之資料，

該電子簽名包含於在對該資料可記錄光碟執行一內容記錄過程時由提供該內容之該內容提供伺服器基於該媒體ID產生之該符記中，且

當該符記之該電子簽名與該內容提供伺服器之一驗證金鑰相符時，該簽名驗證過程係在有效之一條件下。

3. 如請求項1之資訊處理裝置，其中該媒體ID為一序列號，該序列號係對應於該資料可記錄光碟，且該序列號係於一製造該資料可記錄光碟之時間點被記錄。

4. 如請求項2之資訊處理裝置，其中該媒體ID包含識別該光碟工廠之資訊，使得該簽名驗證過程連結該光碟工廠與該內容提供伺服器，該內容提供伺服器係提供該資料可記錄光碟之該記錄內容。

5. 一種資訊處理裝置，其包括：

一資料處理單元，其經組態以對自一資料可記錄光碟讀取之資料執行資料處理，

其中該資料處理單元

自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器產生之一電子簽名之一符記，並執行包含於該符記之該電子簽名之一簽名驗證過程，及

在該簽名驗證在該簽名驗證過程中為有效之一條件下重製該資料可記錄光碟之該所記錄內容，

該簽名驗證過程係基於驗證一實體標記存在該資料可記錄光碟上之一計算運算結果及一媒體ID而執行，該實體標記係在製造該資料可記錄光碟時所使用之一來源光碟中所特有且對應之識別資料，該媒體ID係該資料可記錄光碟所特有之一識別符，

該符記係由該內容提供伺服器於一寫入該記錄內容之時間點，回應於由該資料可記錄光碟接收該媒體ID及該實體標記而產生，且

該實體標記及該媒體ID皆於一製造該資料可記錄光碟之時間點被記錄在該資料可記錄光碟上。

6. 如請求項5之資訊處理裝置，其中：

該電子簽名係包含於基於該實體標記及該媒體ID之一互斥OR運算結果所產生之該符記中，且

該資料處理單元對記錄在該資料可記錄光碟上之該實體標記及該媒體ID執行一互斥OR運算，且當執行該簽名驗證過程時執行與該互斥OR運算結果之一比較過程。

7. 如請求項5或6之資訊處理裝置，

其中該實體標記及該媒體ID係在一光碟工廠處記錄在一資料可記錄光碟上之資料，

該電子簽名係包含於在對該資料可記錄光碟執行一內容記錄過程時由提供該內容之該內容提供伺服器基於該媒體ID及該實體標記而產生之該符記中，且

當該符記之該電子簽名與該內容提供伺服器之一驗證金鑰相符時，該簽名驗證過程係有效的。

8. 一種用於在一資訊處理裝置中對自一資料可記錄光碟讀取之資料執行資料處理之資訊處理方法，該資訊處理方法包括：

藉由使用一資料處理單元驗證一實體標記已記錄在該資料可記錄光碟上，該實體標記為在製造該資料可記錄光碟時所使用之一來源光碟中所特有及對應之識別資料；

藉由使用一資料處理單元自該資料可記錄光碟獲得一符記，該符記含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器產生之一電子簽名，其中該符記係由該內容提供伺服器於一寫入該記錄內容之時間點，回應於由該資料可記錄光碟接收之一媒體ID而產生，且該媒體ID為該資料可記錄光碟所特有且為於一製造該資料可記錄光碟之時間點記錄於該資料可記錄光碟之一識別符；

藉由使用該資料處理單元執行一簽名驗證過程，該簽名驗證過程使用包含於該符記中之該電子簽名；及

藉由使用該資料處理單元在該實體標記之該記錄在該實體標記驗證過程中已得到確認且該簽名驗證在該簽名驗證過程中係有效之一條件下重製該資料可記錄光碟之所記錄內容。

9. 一種用於在一資訊處理裝置中對自一資料可記錄光碟讀取之資料來執行資料處理之資訊處理方法，該資訊處理方法包括：

藉由使用一資料處理單元執行驗證一實體標記及一媒體ID存在該資料可記錄光碟上之一第一計算過程，該實體標記係製造該資料可記錄光碟時所使用之來源光碟中所特有及對應之識別資料，該媒體ID為該資料可記錄光碟所特有且於一製造該資料可記錄光碟之時間點記錄於該資料可記錄光碟之一識別符；

藉由該資料處理單元自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器產生之一電子簽名之一符記，其中該符記係由該內容提供伺服器於一寫入該記錄內容之時間點，回應於由該資料可記錄光碟接收之一媒體ID之簽名驗證過程而產生；

藉由該資料處理單元執行包含將該電子簽名所包含之資料與該第一計算運算過程之所得資料進行比較之一過程的一簽名驗證過程；及

在其中該簽名驗證在該簽名驗證過程中有效之一條件下重製該資料可記錄光碟之所記錄內容。

10. 一種非暫時性記錄媒體，其具有儲存於其中以用於處理自一可記錄媒體讀取之資料之指令，當該指令被一或多個資料處理單元所執行時使該一或多個資料處理單元執行一方法，該方法包括：

驗證一實體標記已記錄在一資料可記錄光碟上，該實體標記為在製造該資料可記錄光碟時所使用之一來源光碟中所特有及對應之識別資料；

自該資料可記錄光碟獲得一符記，該符記含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器產生之一電子簽名，其中該符記係由該內容提供伺服器於一寫入該記錄內容之時間點，回應於由該資料可記錄光碟接收一媒體ID而產生，且該媒體ID為該資料可記錄光碟所特有且於一製造該資料可記錄光碟之時間點記錄於該資料可記錄光碟之一識別符；

使用含於該符記中之該電子簽名來執行一簽名驗證；及

在其中該實體標記之該記錄在該實體標記驗證過程中已得到確認且該簽名驗證在該簽名驗證過程中有效之一條件下複製該資料可記錄光碟之所記錄內容。

11. 一種非暫時性記錄媒體，其具有儲存於其中以用於處理自一可記錄媒體讀取之資料之指令，當該指令被一或多個資料處理單元所執行時使該一或多個資料處理單元執行一方法，該方法包括：

執行驗證一實體標記及一媒體ID存在該資料可記錄光碟上之一第一計算過程，該實體標記為製造一資料可記錄光碟時所使用之一來源光碟中所特有及對應之識別資料，該媒體ID為該資料可記錄光碟所特有且於一製造該資料可記錄光碟之時間點記錄於該資料可記錄光碟之一識別符；

自該資料可記錄光碟獲得含有由提供該資料可記錄光碟之所記錄內容之一內容提供伺服器所產生之一電子簽

名之一符記，其中該符記係由該內容提供伺服器於一寫入該記錄內容之時間點，回應於由該資料可記錄光碟接收之一媒體ID及該實體標記而產生；

執行一簽名驗證過程，其包含將該電子簽名包含之資料與該第一計算運算過程之所得資料進行比較之一過程；及

在其中該簽名驗證在該簽名驗證過程中為有效之一條件下重製該資料可記錄光碟之所記錄內容。

# 八、圖式：

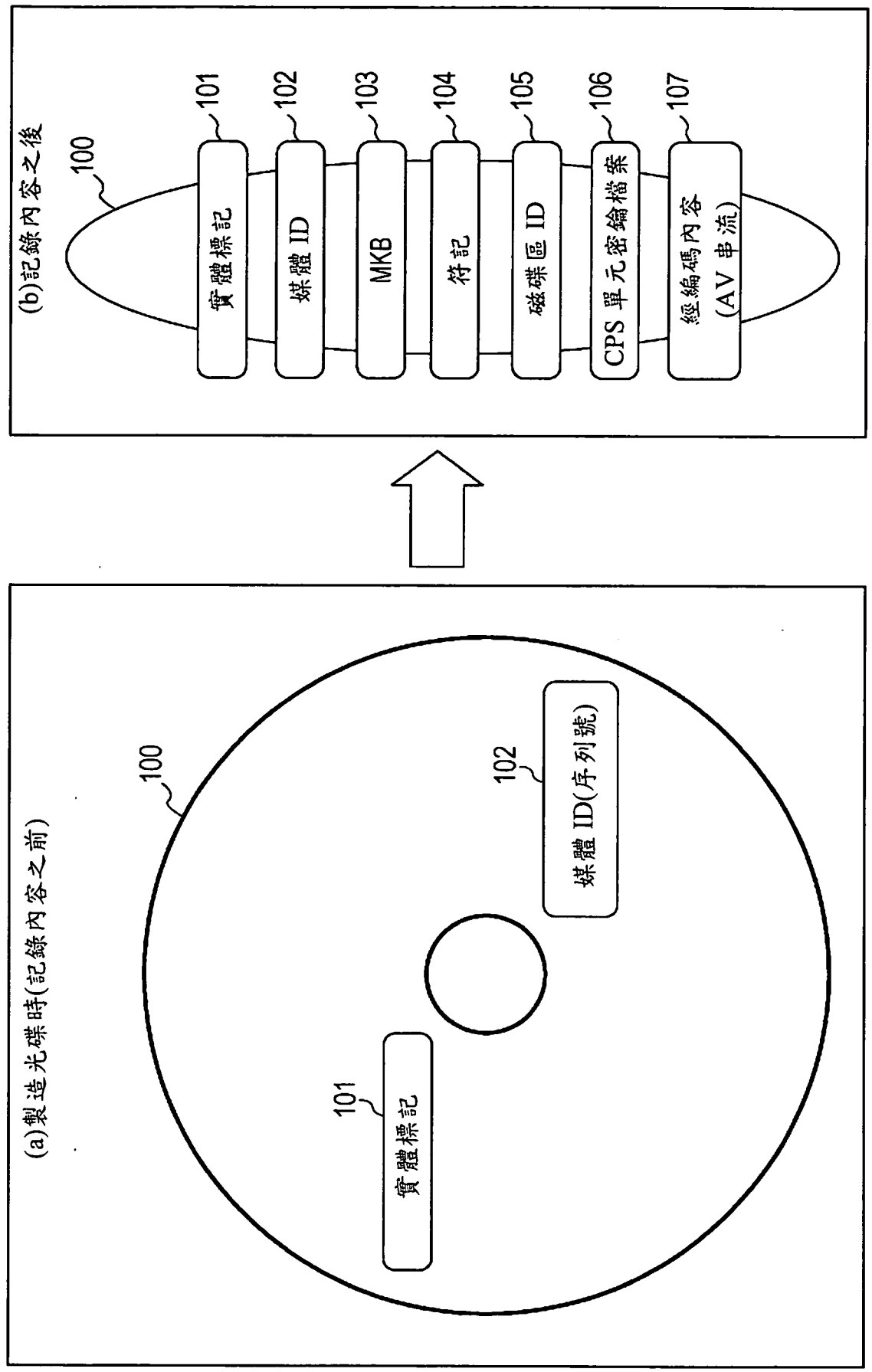
(a)製造光碟時(記錄內容之前)
100
101
實體標記
102
媒體 ID(序列號)
(b)記錄內容之後
100
101
實體標記
102
媒體 ID
103
MKB
104
符記
105
磁碟區 ID
106
CPS 單元密鑰檔案
107
經編碼內容
(AV 串流)

圖 1

| | 實體標記 | 媒體 ID(序列號) |
|---|---|---|
| (a)資料長度 | 16 個位元組 | 16 個位元組 |
| (b)資料結構 | 標頭：1 個位元組<br>經許可人 ID：2 個位元組<br>隨機數字：13 個位元組 | 標頭：1 個位元組<br>光碟工廠 ID：2 個位元組<br>光碟唯一值：13 個位元組 |
| (c)特徵 | 藉由不同於一般資料之方法的方法記錄在光碟上。<br>記錄為針對每一壓模而不同之 ID。<br>(可僅藉由經許可之特定機器寫入) | 舉例而言，記錄為針對每一光碟而不同之 ID 於光碟之燒錄區(BCA)中 |

圖 2

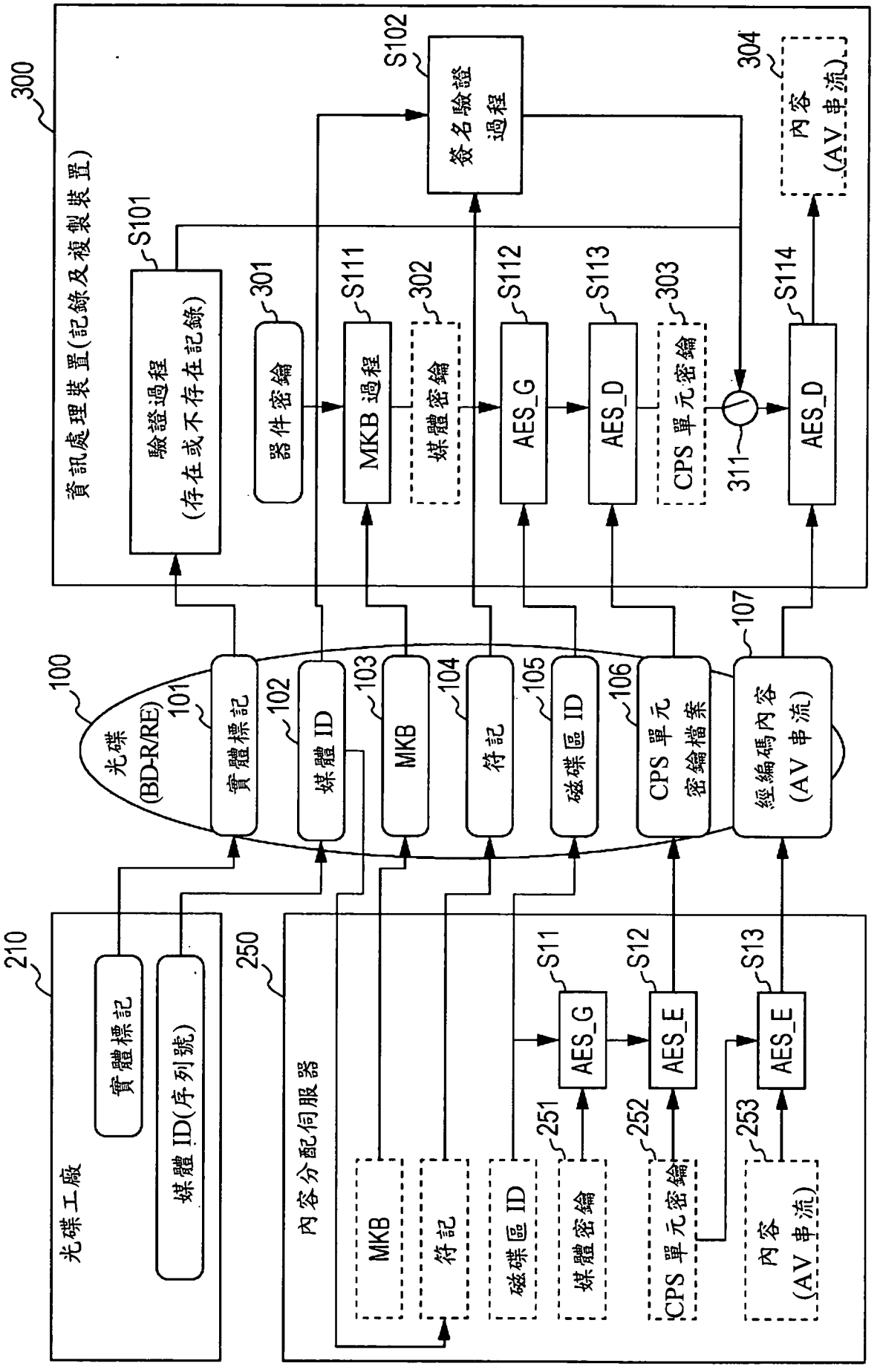
300
資訊處理裝置(記錄及複製裝置)
S101
驗證過程
(存在或不存在記錄)
301
器件密鑰
S102
簽名驗證
過程
304
內容
(AV 串流)
S111
MKB 過程
302
媒體密鑰
S112
AES_G
S113
AES_D
303
CPS 單元密鑰
311
S114
AES_D
100
光碟
(BD-R/RE)
101
實體標記
102
媒體 ID
103
MKB
104
符記
105
磁碟區 ID
106
CPS 單元
密鑰檔案
107
經編碼內容
(AV 串流)
210
光碟工廠
實體標記
媒體 ID(序列號)
250
內容分配伺服器
MKB
符記
磁碟區 ID
S11
AES_G
251
媒體密鑰
S12
AES_E
252
CPS 單元密鑰
S13
AES_E
253
內容
(AV 串流)

圖 3

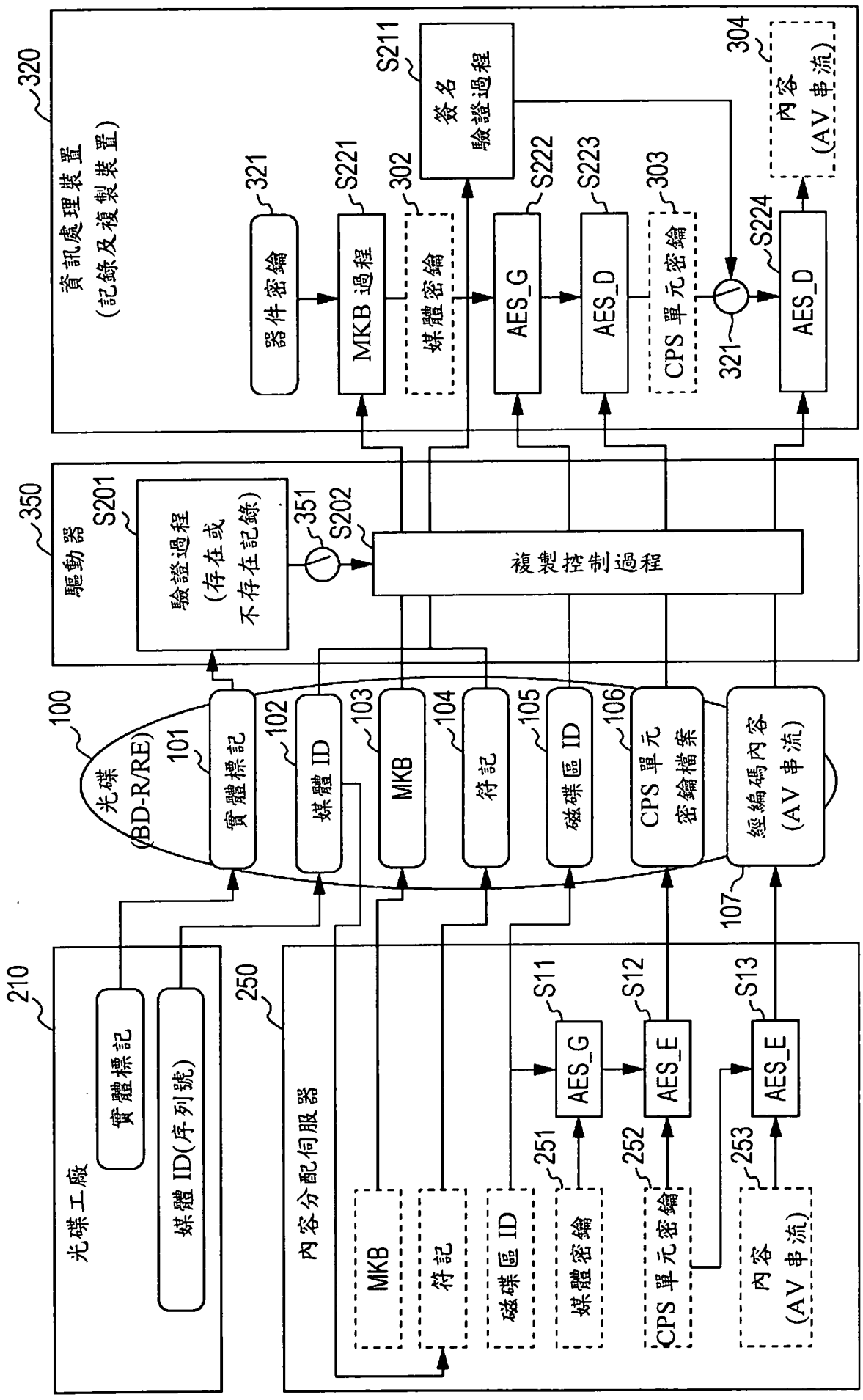
320
資訊處理裝置
(記錄及複製裝置)
321
器件密鑰
S221
MKB 過程
302
媒體密鑰
S211
簽名
驗證過程
S222
AES_G
S223
AES_D
303
CPS 單元密鑰
321
S224
AES_D
304
內容
(AV 串流)
350
驅動器
S201
驗證過程
(存在或
不存在記錄)
351
S202
複製控制過程
100
光碟
(BD-R/RE)
101
實體標記
102
媒體 ID
103
MKB
104
符記
105
磁碟區 ID
106
CPS 單元
密鑰檔案
107
經編碼內容
(AV 串流)
210
光碟工廠
實體標記
媒體 ID(序列號)
250
內容分配伺服器
MKB
符記
磁碟區 ID
251
媒體密鑰
S11
AES_G
S12
AES_E
252
CPS 單元密鑰
S13
AES_E
253
內容
(AV 串流)

圖 4

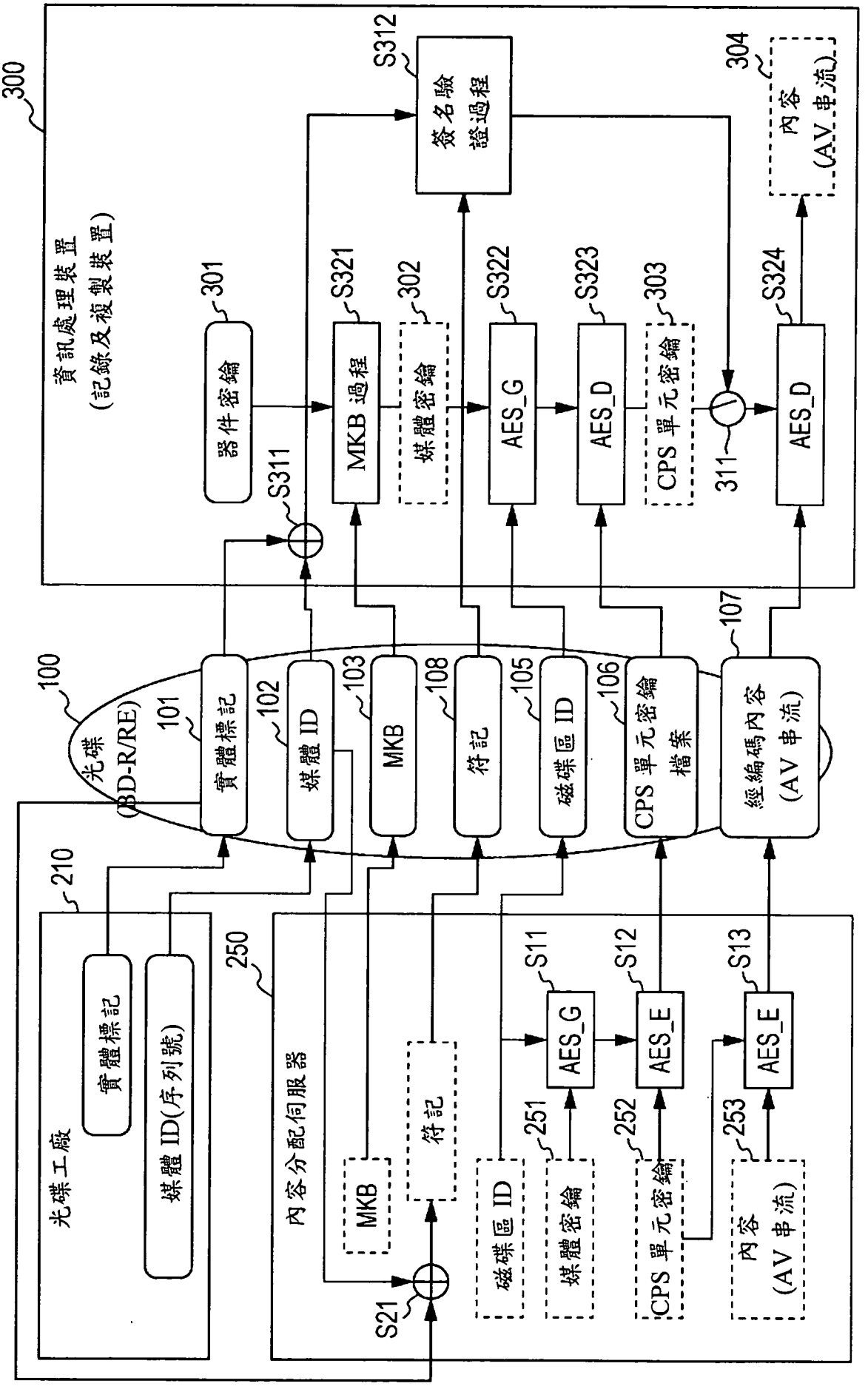
300
資訊處理裝置
(記錄及複製裝置)
S312
簽名驗證過程
304
內容
(AV 串流)
301
器件密鑰
S321
MKB 過程
302
媒體密鑰
S322
AES_G
S323
AES_D
303
CPS 單元密鑰
311
S324
AES_D
S311
100
光碟
(BD-R/RE)
101
實體標記
102
媒體 ID
103
MKB
108
符記
105
磁碟區 ID
106
CPS 單元密鑰
檔案
107
經編碼內容
(AV 串流)
210
光碟工廠
實體標記
媒體 ID(序列號)
250
內容分配伺服器
S11
AES_G
S12
AES_E
S13
AES_E
MKB
符記
磁碟區 ID
251
媒體密鑰
252
CPS 單元密鑰
253
內容
(AV 串流)
S21

圖 5

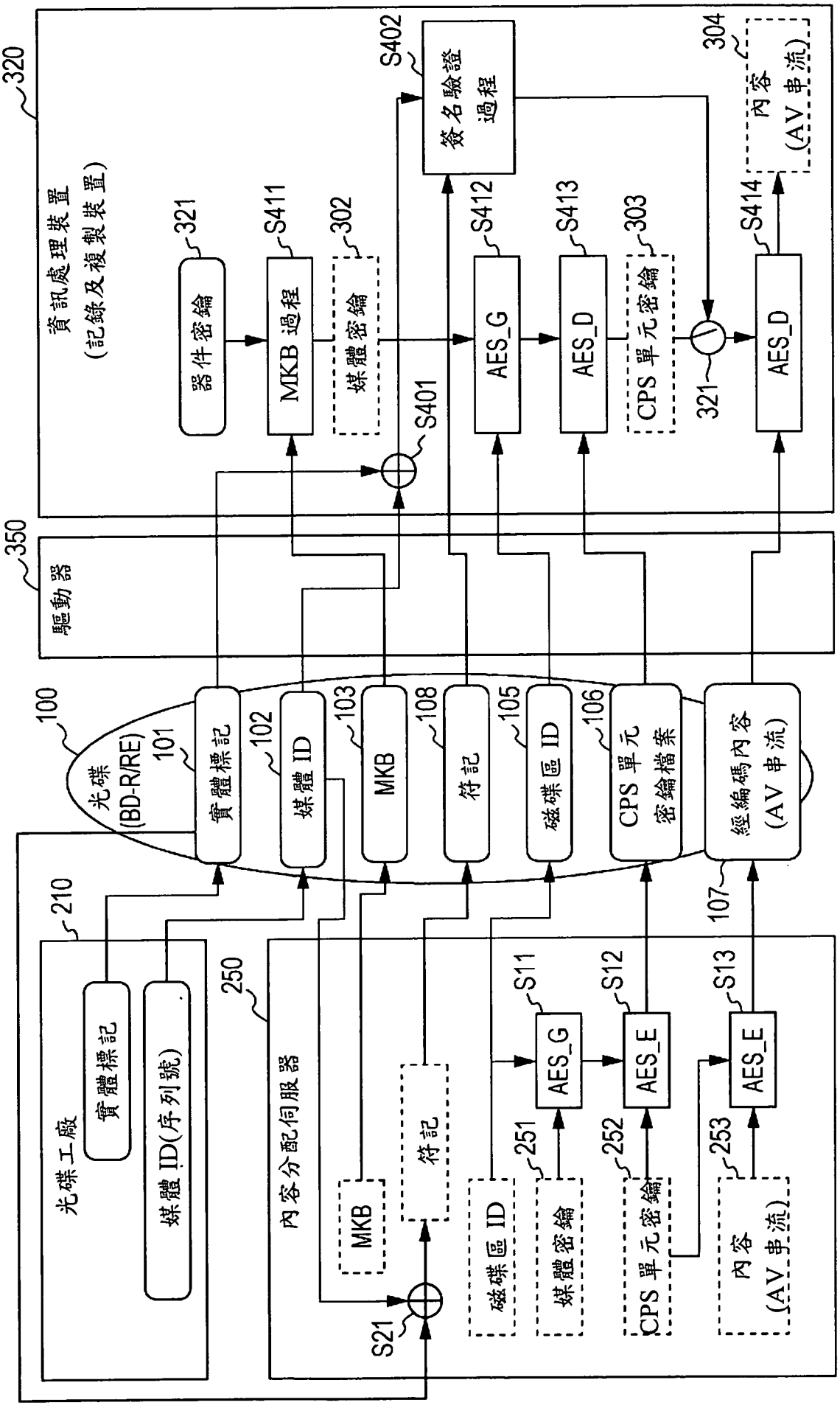
320
資訊處理裝置
(記錄及複製裝置)
350
驅動器
100
光碟
(BD-R/RE)
101
實體標記
102
媒體 ID
103
MKB
108
符記
105
磁碟區 ID
106
CPS 單元
密鑰檔案
107
經編碼內容
(AV 串流)
210
光碟工廠
實體標記
媒體 ID(序列號)
250
內容分配伺服器
MKB
符記
S21
磁碟區 ID
媒體密鑰
CPS 單元密鑰
內容
(AV 串流)
S11
AES_G
S12
AES_E
S13
AES_E
251
252
253
321
器件密鑰
S411
MKB 過程
302
媒體密鑰
S401
S402
簽名驗證
過程
S412
AES_G
S413
AES_D
303
CPS 單元密鑰
321
S414
AES_D
304
內容
(AV 串流)

圖 6

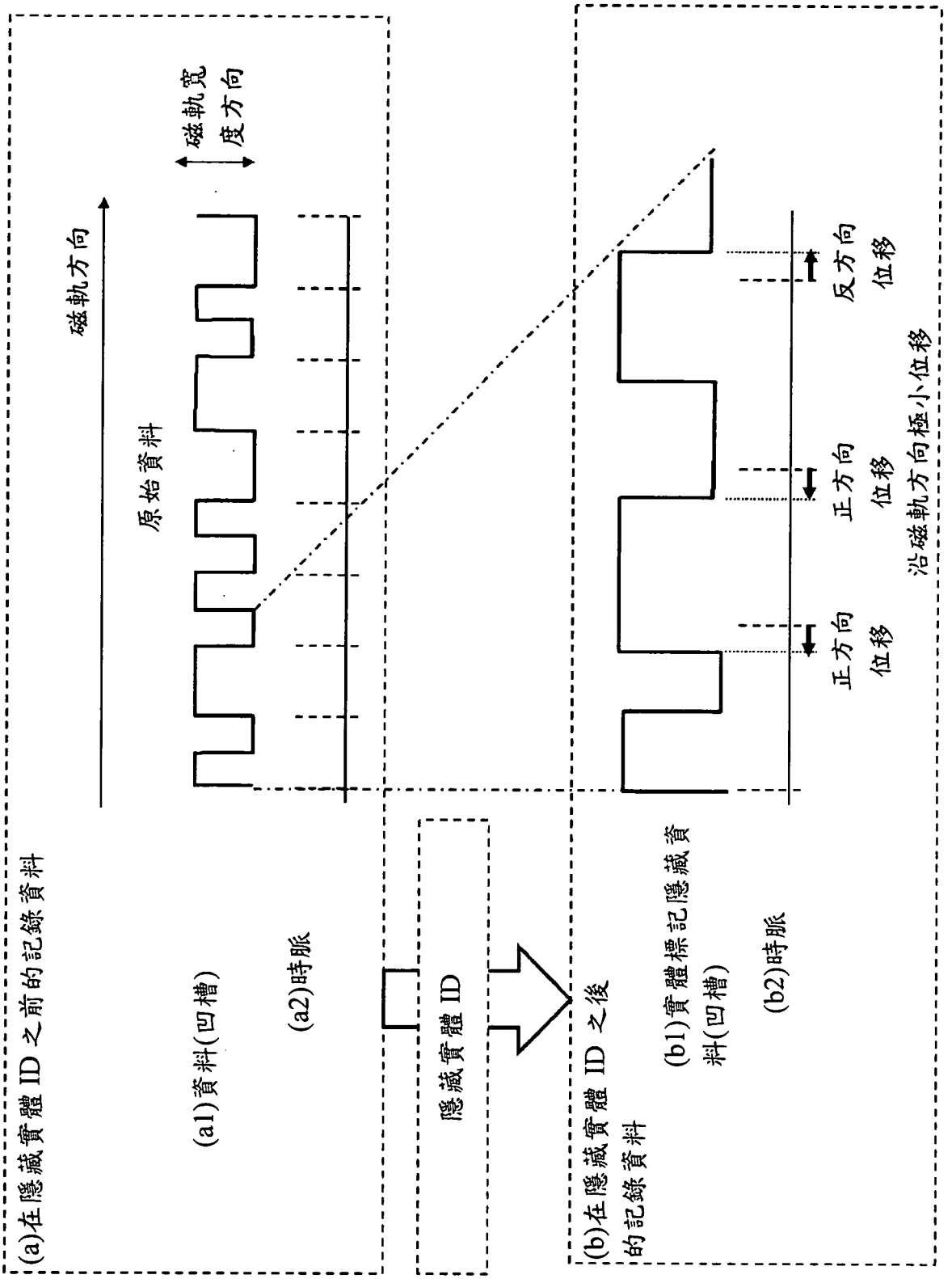
(a)在隱藏實體 ID 之前的記錄資料
磁軌方向
磁軌寬度方向
原始資料
(a1)資料(凹槽)
(a2)時脈
隱藏實體 ID
(b)在隱藏實體 ID 之後的記錄資料
(b1)實體標記隱藏資料(凹槽)
(b2)時脈
正方向位移
反方向位移
沿磁軌方向極小位移

圖 7

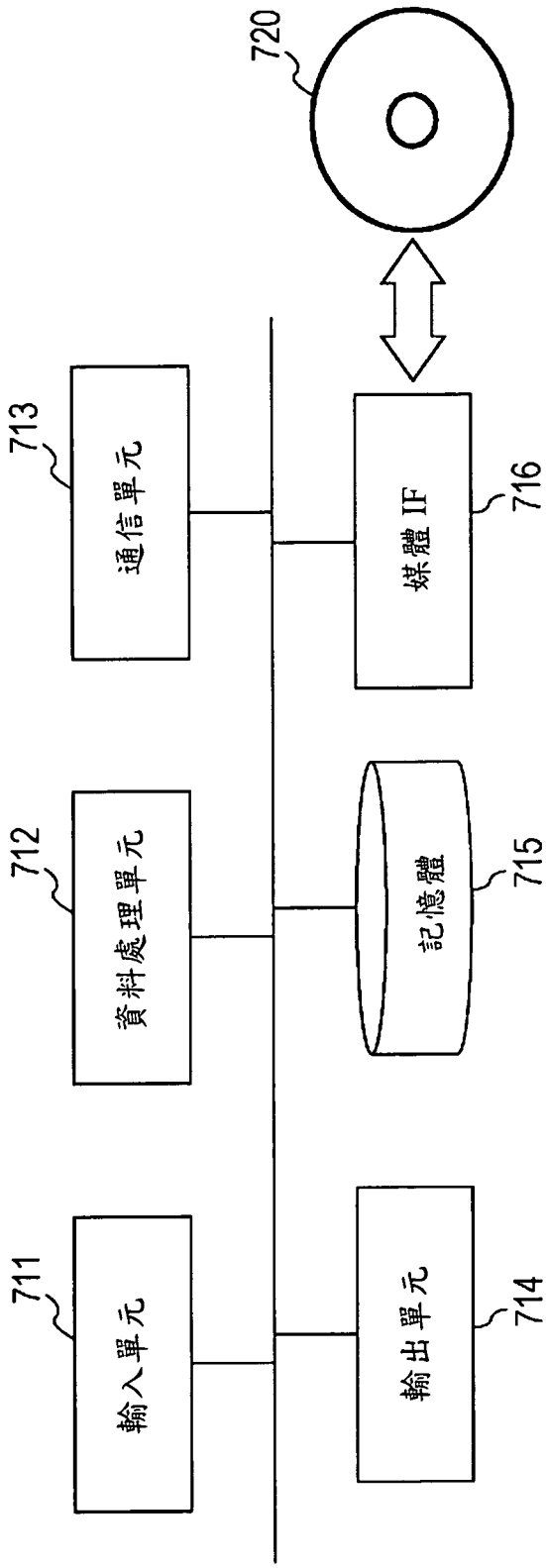


圖 8

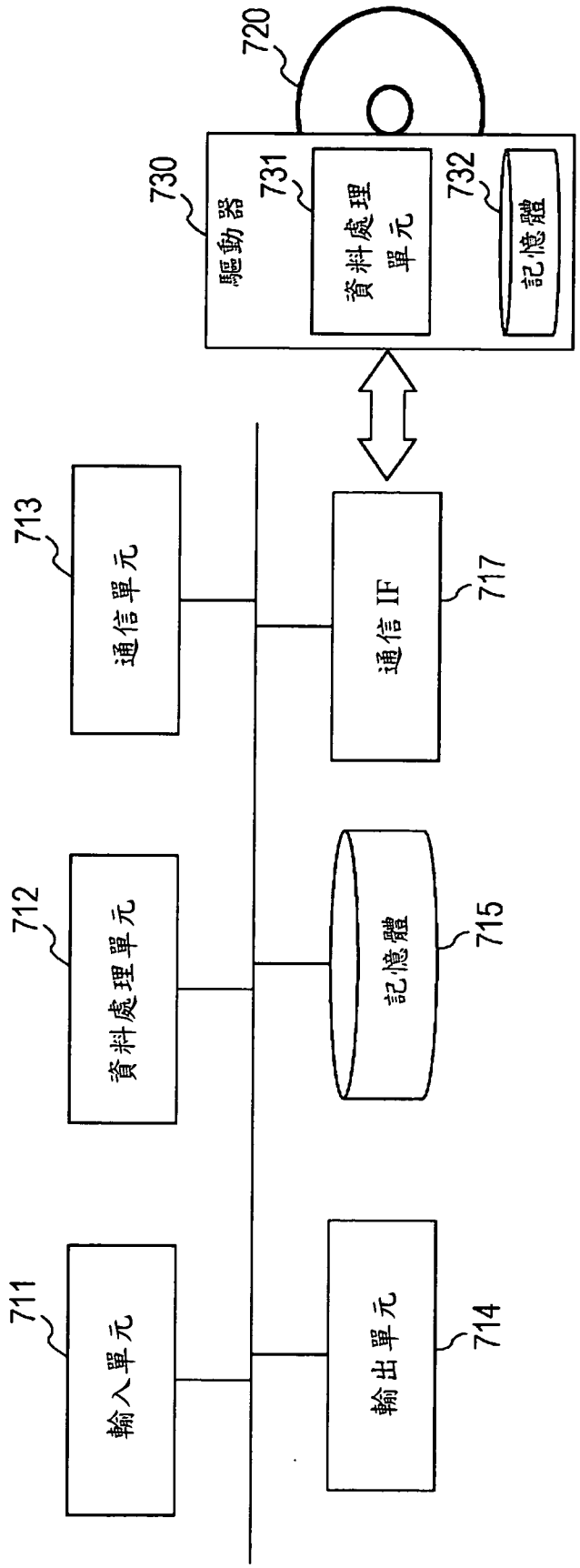
720
730
驅動器
731
資料處理單元
732
記憶體
713
通信單元
通信 IF
717
712
資料處理單元
記憶體
715
711
輸入單元
輸出單元
714

圖 9