三、發明人：（共 6 人）

姓　名：（中文/英文）

1. 上田　健二朗
UEDA, KENJIRO
2. 大石　丈於
OISHI, TATEO
3. 大澤　義知
OSAWA, YOSHITOMO
4. 村松　克美
MURAMATSU, KATSUMI
5. 加藤　元樹
KATO, MOTOKI
6. 高島　芳和
TAKASHIMA, YOSHIKAZU

國　籍：（中文/英文）

1. 日本 JAPAN
2. 日本 JAPAN
3. 日本 JAPAN
4. 日本 JAPAN
5. 日本 JAPAN
6. 日本 JAPAN

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09月02日；特願2004-255153

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】

本發明係關於一種資訊處理裝置、資訊記錄媒體、內容管理系統及資料處理方法、以及電腦程式。進一步詳細而言，係關於可實現內容利用管理要求之各種內容經細分化之各資料單元之管理，且有效且確實執行內容之竄改驗證之資訊處理裝置、資訊記錄媒體、內容管理系統及資料處理方法、以及電腦程式。

【先前技術】

音樂等之聲頻資料、電影等之影像資料、遊戲程式、各種應用程式等各種軟體資料(以下將此等稱為內容(Content))，可作為數位資料，而儲存於記錄媒體，如應用藍色雷射之Blu-ray光碟或DVD(多樣化數位光碟)、MD(迷你光碟)、CD(光碟)中。特別是利用藍色雷射之Blu-ray光碟，係可高密度記錄之光碟，且可記錄大容量之視頻內容等，作為高畫質資料。

在此等各種資訊記錄媒體(記錄媒體)中儲存數位內容而提供使用者。使用者在擁有之PC(個人電腦)及光碟播放機等重現裝置中進行內容之重現及利用。

一般而言，音樂資料及影像資料等許多內容之製作者或販賣者擁有發行權。因此，通常分發此等內容時，有一定之利用限制，亦即，採取僅對正當之使用者同意利用內容，而避免進行未經許可之複製等之構造。

採用數位記錄裝置及記錄媒體，如可不使影像及聲音惡

化地反覆記錄、重現，而發生經由不正當複製內容之網際網路分發，將內容複製於CD-R等之所謂海盜版光碟之流通，及儲存於PC等硬碟之複製內容之利用蔓延等問題。

利用DVD或是近年來進行開發之利用藍色雷射之記錄媒體等大容量型記錄媒體，在一片媒體中可記錄一部～數部電影之大量資料作為數位資訊。如此，可記錄視頻資訊等作為數位資訊時，防止不正當複製，謀求保護著作權者，則成為日益重要之課題。最近為了防止此種數位資料之不正當複製，在數位記錄裝置及記錄媒體中防止非法複製用之各種技術已實用化。

如DVD播放器採用內容攪拌系統(Content Scramble System)。內容攪拌系統係將視頻資料及聲頻資料等加密後記錄於DVD-ROM(唯讀記憶體)中，用於將其加密後之資料予以解碼之鍵，則提供獲得許可證之DVD播放器。許可證對按照不進行不正當複製等之指定之動作規定而設計之DVD播放器提供。因此，獲得許可證之DVD播放器利用提供之鍵，藉由將記錄於DVD-ROM之加密資料予以解碼，即可自DVD-ROM重現影像及聲音。

另外，由於未獲得許可證之DVD播放器沒有將加密後之資料予以解碼用之鍵，因此無法進行記錄於DVD-ROM之加密資料之解碼。因而內容攪拌系統構造，使不滿足許可證時要求之條件之DVD播放器，無法進行記錄數位資料之DVD-ROM之重現，而可防止不正當複製。

排除內容之不正當利用之一種方法，提出有一種控制構

造，其係於執行內容重現之資訊處理裝置(重現裝置)中，驗證內容有無遭竄改，僅於確認內容未遭竄改時，允許內容重現，判明遭竄改時，不執行內容重現之構造。

如在專利文獻1中揭示有一種控制構造，其係自預定重現之內容檔計算散列值，依據預先方便對照用散列值，亦即依據正當之內容資料，與預先計算完成之對照用散列值進行比較，新算出之散列值與對照用散列值一致情況下，判定為內容未遭竄改，並轉移至內容之重現處理。

但是，如此執行依據內容算出散列值之處理時，於作為散列值算出之原來資料之內容資料容量大時，計算時需要之處理負荷及處理時間過大。最近動畫影像資料之高品質化進步，往往一個內容中具有數GB～數十GB之資料量。因而發生使執行內容重現之使用者機器進行依據此種大容量資料之內容之散列值算出處理，要求使用者機器之資料處理能力過大之問題，且發生內容驗證需要時間長，無法有效進行內容重現處理之問題。

專利文獻1：特開2002-358011號

【發明內容】

(發明所欲解決之問題)

有鑑於此種情況，本發明之目的在提供一種於儲存有要求著作權管理等利用管理之各種內容之資訊記錄媒體之內容利用中，可有效執行內容之竄改驗證處理之資訊處理裝置、資訊記錄媒體、內容管理系統及資料處理方法、以及電腦程式。

再者，本發明之目的在提供一種儲存於資訊記錄媒體之內容經細分化之各單元，有效且確實進行竄改驗證處理，來實現內容之利用管理之資訊處理裝置、資訊記錄媒體、內容管理系統及資料處理方法、以及電腦程式。

(解決問題之手段)

本發明第一部分係執行來自資訊記錄媒體之內容重現處理之資訊處理裝置，其特徵為具有：

內容驗證機構，其係驗證內容之正當性；及

內容重現機構，其係將依據前述內容驗證機構之驗證，確認內容之正當性作為條件，來執行內容之重現處理；

前述內容驗證機構具有執行內容驗證處理之構造，其係選擇n個(其中n為1以上整數)作為記錄於資訊記錄媒體之內容之細分化資料而設定之散列單元，執行依據選擇散列單元之算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理，並將選擇之n個全部散列值對照成立作為內容正當性之確認條件。

再者，本發明之資訊處理裝置一種實施態樣之特徵為：前述內容驗證機構之構造係自儲存於資訊記錄媒體之內容散列表之記錄資料，取得儲存於資訊記錄媒體中之散列單元數(HN)，隨機選擇x≦HN之數值x，使該選擇數值x對應於儲存於資訊記錄媒體之散列單元之散列單元編號，來執行對照處理對象之散列單元之選擇處理。

再者，本發明之資訊處理裝置一種實施態樣之特徵為：前述內容驗證機構之構造係依據作為儲存於資訊記錄媒體

之加密內容之構成資料之散列單元，執行算出散列值之處理。

再者，本發明之資訊處理裝置一種實施態樣之特徵為：前述內容驗證機構之構造係執行前述選擇散列單元之解碼處理，算出依據該解碼散列單元之散列值，並執行算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理。

再者，本發明之資訊處理裝置一種實施態樣之特徵為：前述內容驗證機構之構造係於前述選擇散列單元之解碼處理時，取得對應於散列單元所屬之內容管理單元之單元鍵，來執行應用該單元鍵之解碼處理。

再者，本發明第二部分係資訊記錄媒體，其特徵為：具有儲存內容及作為內容之細分化資料而設定之各個散列單元之散列值之構造。

再者，本發明之資訊記錄媒體一種實施態樣之特徵為：前述散列單元之邏輯上尺寸設定成執行內容重現之資訊處理裝置中之資料讀取單位之ECC區塊資料之資料長之整數倍。

再者，本發明之資訊記錄媒體一種實施態樣之特徵為：前述內容之構造係藉由作為內容檔而設定之剪輯檔來區分，並以該剪輯檔之構成資料中，至少剪輯檔之最前資料位置與前述ECC區塊之最前位置一致之方式來記錄。

再者，本發明第三部分係內容管理系統，其特徵為：

具有：管理中心，其係提供內容利用管理用之管理資訊；

內容編輯實體，其係進行內容編輯處理；及資訊記錄媒體製造實體，其係自前述內容編輯實體接收編輯內容，而對資訊記錄媒體記錄內容；

前述內容編輯實體或資訊記錄媒體製造實體之至少任何一個之構造，係算出對應於資訊記錄媒體儲存內容之細分化資料之散列單元之散列值，並生成記錄該算出散列值之內容散列表，作為資訊記錄媒體之儲存資料。

再者，本發明之內容管理系統一種實施態樣之特徵為：前述內容編輯實體或資訊記錄媒體製造實體之至少任何一個之構造，為生成記錄依據儲存於前述內容散列表之散列值而算出之散列摘要值之內容證明書，作為儲存於資訊記錄媒體之資料。

再者，本發明之內容管理系統一種實施態樣之特徵為：前述內容編輯實體或資訊記錄媒體製造實體之至少任何一個之構造，為執行依據儲存於前述內容證明書之資料生成電子簽署，並賦予該內容證明書之處理。

再者，本發明第四部分係生成記錄於資訊記錄媒體之資料之資料處理方法，其特徵為具有：

記錄資料生成步驟，其係執行扇區單位之記錄資料生成處理；

儲存步驟，其係將生成之記錄資料儲存於緩衝器中；

散列值算出步驟，其係於緩衝器儲存資料達到對應於預定之散區單元之資料量時，依據該緩衝器儲存資料算出散列值；及

設定步驟，其係設定於前述散列值算出步驟中算出之各散列單元之散列值，作為記錄於資訊記錄媒體之資料。

再者，本發明之資料處理方法一種實施態樣之特徵為：前述資料處理方法進一步具有：內容散列表生成步驟，其係儲存在前述散列值算出步驟中算出之各散列單元之散列值；及內容證明書生成步驟，其係生成記錄依據儲存於前述內容散列表之散列值算出之散列摘要值之內容證明書，作為儲存於資訊記錄媒體之資料。

再者，本發明之資料處理方法一種實施態樣之特徵為：前述內容證明書生成步驟包含生成依據儲存於內容證明書之資料之電子簽署，並賦予該內容證明書之處理。

再者，本發明之資料處理方法一種實施態樣之特徵為：前述記錄資料生成步驟參照記述各扇區單位之資料處理態樣之輔助檔，依據該輔助檔決定各扇區是否需要加密及加密態樣，進行按照該決定資訊之資料處理，而生成扇區單位之記錄資料。

再者，本發明第五部分係執行來自資訊記錄媒體之內容重現處理之資料處理方法，其特徵為具有：

內容驗證步驟，其係驗證內容之正當性；及

內容重現步驟，其係將依據前述內容驗證步驟中之驗證，確認內容之正當性作為條件，來執行內容之重現處理；

前述內容驗證步驟包含選擇n個(其中n為1以上整數)作為記錄於資訊記錄媒體之內容之細分化資料而設定之散列單元，執行依據選擇散列單元之算出散列值與儲存於資訊

記錄媒體中之對照用散列值之對照處理，並執行將選擇之n個全部散列值對照成立作為內容正當性之確認條件之內容驗證處理之步驟。

再者，本發明之資料處理方法一種實施態樣之特徵為：前述內容驗證步驟包含自儲存於資訊記錄媒體之內容散列表之記錄資料，取得儲存於資訊記錄媒體中之散列單元數(HN)，隨機選擇x≦HN之數值x，使該選擇數值x對應於儲存於資訊記錄媒體之散列單元之散列單元編號，來執行對照處理對象之散列單元之選擇處理之步驟。

再者，本發明之資料處理方法一種實施態樣之特徵為：前述內容驗證步驟包含依據作為儲存於資訊記錄媒體之加密內容之構成資料之散列單元，執行算出散列值之處理之步驟。

再者，本發明之資料處理方法一種實施態樣之特徵為：前述內容驗證步驟包含執行前述選擇散列單元之解碼處理，算出依據該解碼散列單元之散列值，並執行算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理之步驟。

再者，本發明之資料處理方法一種實施態樣之特徵為：前述內容驗證步驟包含於前述選擇散列單元之解碼處理時，取得對應於散列單元所屬之內容管理單元之單元鍵，來執行應用該單元鍵之解碼處理之步驟。

再者，本發明第七部分係在電腦中執行生成記錄於資訊記錄媒體之資料之處理之電腦程式，其特徵為具有：

記錄資料生成步驟，其係執行扇區單位之記錄資料生成處理；

儲存步驟，其係將生成之記錄資料儲存於緩衝器中；

散列值算出步驟，其係於緩衝器儲存資料達到對應於預定之散區單元之資料量時，依據該緩衝器儲存資料算出散列值；及

設定步驟，其係設定於前述散列值算出步驟中算出之各散列單元之散列值，作為記錄於資訊記錄媒體之資料。

再者，本發明第八部分係在電腦中執行來次資訊記錄媒體之內容重現處理之電腦程式，其特徵為具有：

內容驗證步驟，其係驗證內容之正當性；及

內容重現步驟，其係將依據前述內容驗證步驟中之驗證，確認內容之正當性作為條件，來執行內容之重現處理；

前述內容驗證步驟包含選擇n個(其中n為1以上整數)作為記錄於資訊記錄媒體之內容之細分化資料而設定之散列單元，執行依據選擇散列單元之算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理，並執行將選擇之n個全部散列值對照成立作為內容正當性之確認條件之內容驗證處理之步驟。

另外，本發明之電腦程式如係對可執行各種程式碼之電腦系統，可藉由以電腦可讀取之形式，而提供之記憶媒體、通訊媒體，如CD、FD及MO等記錄媒體，或是網路等通訊媒體而提供之電腦程式。藉由以電腦可讀取之形式提供此種程式，而在電腦系統上實現依程式之處理。

本發明之另外目的、特徵及優點，藉由後述之本發明之實施例及依據附加圖式之進一步詳細說明即可明瞭。另外，本說明書中所謂系統，係數個裝置之邏輯性集合構造，各構成之裝置並不限定於在同一個框體內。

(發明效果)

本發明之構造，由於係算出作為資訊記錄媒體之儲存內容之細分化資料而設定之各個散列單元之散列值，將算出散列值記錄於內容散列表，而與內容一起儲存於資訊記錄媒體中，於執行內容重現之資訊處理裝置中，依據自許多散列單元隨機選擇之1個以上之散列單元，執行散列值對照處理，因此，不論內容之資料量為何，可進行依據少資料量而設定之散列單元算出散列值，及對照處理之內容驗證，無須提高執行內容重現之使用者機器之資料處理能力，且亦縮短內容重現前之驗證處理時間，而可進行有效之內容驗證。

再者，本發明之構造，由於係散列單元設定成執行內容重現之資訊處理裝置中之資料讀取單位之ECC區塊資料之資料長之整數倍，因此可藉由更少之資料讀取來實現散列單元之讀取，可進行處理效率高之資料驗證。

【實施方式】

以下，參照圖式詳細說明本發明之資訊處理裝置、資訊記錄媒體、內容管理系統及資料處理方法、以及電腦程式。另外，說明係按照以下記載之項目來進行。

1.資訊記錄媒體之儲存資料構造

2.儲存內容之加密、利用管理構造

3.資訊記錄媒體之資料記錄構造、加密構造及內容散列之詳細內容

4.資訊記錄媒體之製造、資料儲存處理之詳細內容

5.內容重現處理中應用內容散列之驗證處理

6.單元鍵之生成、內容解碼及重現處理

7.資訊處理裝置之構造例

[1.資訊記錄媒體之儲存資料構造]

首先，說明資訊記錄媒體之儲存資料構造。圖1顯示可適用本發明之處理之內容儲存之資訊記錄媒體一種範例。此處顯示內容儲存完成之光碟之ROM光碟之資訊儲存例。

該ROM光碟如係Blu-ray光碟及DVD等資訊記錄媒體，且係儲存在具有正當之內容著作權或分發權之內容權利人許可下，於光碟製造工廠中製造之正當內容之資訊記錄媒體。另外，以下之實施例中，資訊記錄媒體之例係以光碟型之媒體為例做說明，不過本發明亦可適用於使用各種態樣之資訊記錄媒體之構造。

如圖1所示，資訊記錄媒體100具有：儲存內容等資料之資料儲存區域101，及儲存對應於光碟及儲存內容之附帶資訊，與適用於內容之解碼處理之鍵資訊等之引入區域102。

於資料儲存區域101中儲存：加密內容111，作為適用於加密內容之解碼處理之鍵生成時需要之資訊之記錄種(REC SEED)112，作為內容之複製、重現控制資訊之CCI(複製控制資訊)113，作為應用於內容之竄改驗證之內容之散列值

之內容散列114，顯示內容正當性用之內容證明書115，及儲存適用於賦予內容證明書之電子簽署驗證之公開鍵之簽署驗證用公開鍵證明書116。內容散列114作為內容散列表(CHT)而儲存。內容散列表(CHT)之詳細內容於後述。另外，記錄種(REC SEED)112、CCI(複製控制資訊)113及內容散列114用作適用於內容之加密及解碼之密碼鍵(單元鍵)之生成資訊。詳細構造於後述。

於引入區域102中儲存適用於加密內容111之解碼處理之鍵生成時需要之密碼鍵資訊120。密碼鍵資訊120中包含依據作為播放加密方式一種態樣而熟知之樹構造之鍵分發方式而生成之密碼鍵區塊之媒體鍵區塊(MKB：Media Key Block)121。再者，資訊記錄媒體100記錄實際索引(Physical Index)131。以下說明此等各種資訊之概要。

(1)加密內容111

資訊記錄媒體100中儲存各種內容。如包含：高度精密動畫影像資料之HD(高精密度)電影內容等之動畫內容之AV(視聽)流、以特定規格規定之形式之遊戲程式、影像檔、聲音資料、本文資料等之主要內容。此等內容係特定之AV格式規格資料，並按照特定之AV資料格式儲存。具體而言，如Blu-ray光碟ROM規格資料係按照Blu-ray光碟ROM規格格式來儲存。

再者，有時亦儲存如作為服務資料之遊戲程式、影像檔、聲音資料及本文資料等子內容。子內容係具有不按照特定之AV資料格式之資料格式之資料。亦即，Blu-ray光碟ROM

規格以外資料，可以不按照Blu-ray光碟ROM規格格式之任意格式儲存。

主內容與子內容之內容種類均包含：音樂資料、動畫、靜止畫等影像資料、遊戲程式及WEB內容等各種內容，此等內容中包含：僅藉由來自資訊記錄媒體100之資料而可利用之內容資訊，及可合併來自資訊記錄媒體100之資料，與自網路連接之伺服器提供之資料而利用之內容資訊等各種態樣之資訊。

(2)記錄種112

各內容或數個內容之集合，為了內容之利用管理，各自應用個別之密碼鍵(單元鍵)加密後，儲存於資訊記錄媒體100中。亦即，構成內容之AV(視聽)流、音樂資料、動畫、靜止畫等影像資料、遊戲程式及WEB內容等，區分成作為內容利用之管理單位之單元，並對區分之各單元分配不同之記錄種：Vu112。

內容利用時，按照記錄種：Vu112及應用密碼鍵資訊120之指定之密碼鍵生成順序，分配各單元對應之密碼鍵(單元鍵)。將分配1個單元鍵之單位稱為內容管理單元(CPS單元)。亦即，加密內容111區分成CPS單元單位，並以對應於各CPS單元之單元鍵加密後，儲存於資訊記錄媒體100中。

(3)複製控制資訊(CCI)113

複製控制資訊(CCI)113係對應於儲存於資訊記錄媒體100之加密內容111之利用控制用之複製限制資訊及重現限制資訊。該複製控制資訊(CCI)113可於作為CPS單元個別之

資訊而設定時，及對應於數個CPS單元而設定時等之各種情況來設定。該資訊之詳細內容於後段作說明。

(4)內容散列114

內容散列114係依據儲存於資訊記錄媒體100中之內容或加密內容之構成資料之散列值，且適用於內容之竄改驗證。本發明之構造中，係將作為構成CPS單元之AV流實際資料之剪輯檔予以細分化，設定指定資料單位(如192 KB)之散列單元，算出各散列單元之散列值，將各散列單元單位之散列值記錄於內容散列表(CHT)，而儲存於資訊記錄媒體中。

執行來自資訊記錄媒體之內容重現之資訊處理裝置(重現裝置)，算出依據散列單元之散列值，比較算出散列值與記錄於儲存於資訊記錄媒體之內容散列表(CHT)之對應之散列單元之對照用散列值，一致時，判定為內容未遭竄改，而轉移至內容之解碼、重現處理。不一致情況下，判定為內容遭竄改，停止內容之解碼、重現處理。此等處理之詳細內容於後述。

另外，內容散列係亦利用作為適用於內容之密碼處理、解碼處理之密碼鍵生成資訊之資料。就內容散列114之生成及利用態樣，於後段做說明。

(5)內容證明書

內容證明書係顯示儲存於資訊記錄媒體之內容正當性用之證明書，且儲存依據儲存於上述內容散列表(CHT)之對照用散列單元之內容散列摘要等資料，並附加電子簽署。如

附加光碟工廠之資訊記錄媒體製造實體等之電子簽署，成為防止竄改之資料。內容證明書之詳細內容於後段詳細說明。

(6)簽署驗證用公開鍵證明書

簽署驗證用公開鍵證明書係儲存適用於賦予內容證明書之資訊記錄媒體製造實體等之電子簽署驗證之公開鍵之公開鍵證明書。

(7)實際索引131

實際索引131中記錄資訊記錄媒體之種類資訊，如光碟種類等光碟附帶資訊，及對應於儲存於資料區域101中之內容之內容之附帶資訊等。再者，與記錄種112同樣地，有時亦記錄生成適用於儲存於資訊記錄媒體之資料儲存區域101中之加密內容之解碼處理之鍵用之鍵資訊(鍵生成資訊)。另外，亦可構成實際索引113記錄於引入區域102中。

(8)密碼鍵資訊120

密碼鍵資訊120與前述記錄種112同樣地，包含作為取得生成適用於儲存於資訊記錄媒體之資料儲存區域101中之加密內容之解碼處理之鍵用之鍵資訊(鍵生成資訊)用之密碼鍵區塊，亦即，作為依據播放加密方式一種態樣而熟知之樹構造之鍵分發方式而生成之密碼鍵區塊之媒體鍵區塊(MKB：Media Key Block)121。

MKB121係僅藉由依據儲存於具有有效許可證之使用者之資訊處理裝置中之裝置鍵之處理(解碼)，可取得內容解碼時需要之鍵之媒體鍵(Km)之鍵資訊區塊。此因，藉由按照

所謂階層型樹構造之資訊分發方式，使用者裝置(資訊處理裝置)僅於具有有效之許可證時，方可取得鍵，可阻止無效化(Revoke處理)之使用者裝置取得鍵(媒體鍵)。管理中心藉由變更儲存於MKB之鍵資訊，儲存於特定之使用者裝置之裝置鍵無法解碼，亦即，可生成具有無法取得內容解碼時需要之媒體鍵構造之MKB。因此，任何時間均排除(無效化)不正當裝置，而可僅對具有有效之許可證之裝置提供可解碼之加密內容。

[2.儲存內容之加密、利用管理構造]

其次，參照圖2以下，來說明區分儲存於資訊記錄媒體中之內容，而實現各區分內容不同之利用控制之內容管理構造。

如前述，儲存於資訊記錄媒體之內容，為了實現各區分內容不同之利用控制，係分配各區分內容不同之鍵(單元鍵)，並予以加密後儲存。將分配1個單元鍵之單位稱為內容管理單元(CPS單元)。

應用各個單元鍵，將屬於各單元之內容予以加密來利用內容時，取得分配至各單元之鍵(單元鍵)來進行重現。各單元鍵可個別地管理，如對某個單元A分配之單元鍵，係作為可自資訊記錄媒體取得之鍵來設定。此外，對單元B分配之單元鍵，係進入網路連接之伺服器中，將使用者執行指定程序作為條件而可取得之鍵等，各單元對應之鍵之取得及管理構造，可在各單元鍵中形成獨立之態樣。

以下，參照圖2來說明分配1個鍵之單位，亦即內容管理

單元(CPS單元)之設定態樣。

如圖2所示，內容具有：(A)標題210、(B)電影物件220、(C)播放表230及(D)剪輯240之階層構造，指定作為藉由重現應用而存取之索引檔之標題時，係指定與標題相關之重現程式，並按照所指定之重現程式之程式資訊，選擇規定內容之重現順序等之播放表，藉由播放表中規定之剪輯資訊，讀取作為內容實際資料之AV流或是命令，來進行AV流之重現及命令之執行處理。

圖2中顯示2個CPS單元。此等構成儲存於資訊記錄媒體之內容之一部分。CPS單元1, 301、CPS單元2, 302分別係作為包含剪輯之單元而設定之CPS單元，該剪輯包含：作為應用索引之標題、作為重現程式檔之電影物件、播放表及作為內容實際資料之AV流檔。

內容管理單元(CPS單元)1, 301中包含：標題1, 211與標題2, 212、重現程式221, 222、播放表231, 232、剪輯241、剪輯242，此等2個剪輯241, 242中包含之內容之實際資料之AV流資料檔261, 262，應用搭配內容管理單元(CPS單元)1, 301而設定之密碼鍵之單元鍵：Ku1予以加密。

內容管理單元(CPS單元)2, 302中包含：標題3, 213、重現程式224、播放表233及剪輯243，剪輯243中包含之內容之實際資料之AV流資料檔263應用搭配內容管理單元(CPS單元)2, 302而設定之密碼鍵之單元鍵：Ku2予以加密。

如使用者為了執行對應於內容管理單元1, 301之應用檔或內容重現處理，須取得作為搭配內容管理單元(CPS單

元)1, 301而設定之密碼鍵之單元鍵：Ku1，來執行解碼處理，執行解碼處理後，執行應用程式，可進行內容重現。為了執行對應於內容管理單元2, 302之應用檔或內容重現處理，須取得搭配內容管理單元(CPS單元)2, 302而設定之密碼鍵之單元鍵：Ku2，來執行解碼處理。

在重現內容之資訊處理裝置中執行之重現應用程式，識別對應於使用者之重現指定內容之內容管理單元(CPS單元)，並執行對應於識別之CPS管理單元資訊之CPS密碼鍵之取得處理。無法取得CPS密碼鍵情況下，進行無法重現之訊息顯示等。此外，重現應用程式進行內容重現執行時內容管理單元(CPS單元)發生切換之檢測，進行必要鍵之取得及無法重現之訊息顯示等。

重現應用程式依據圖3所示之單元構造及單元鍵管理表執行重現管理。如圖3所示，單元構造及單元鍵管理表係搭配：應用層之索引或應用檔，或是對應於資料群之內容管理單元(CPS單元)，及單元鍵資訊之表。重現應用程式依據該管理表進行管理。

重現應用程式如檢測藉由應用索引之切換，而發生內容管理單元(CPS單元)之切換時，進行藉由內容管理單元(CPS單元)之切換而應用之鍵之切換。或是執行需要取得單元鍵之訊息顯示等之處理。

如在執行內容重現處理之重現裝置中儲存有內容管理單元(CPS單元)1, 301之單元鍵Ku1，亦儲存有內容管理單元(CPS單元)2, 302之單元鍵Ku2時，統籌控制內容重現處理之

重現應用程式於檢測有應用之單元間之切換及內容之切換時，進行對應於內容管理單元(CPS單元)之切換之單元鍵之切換，亦即進行Ku1→Ku2之切換。

此外，在執行內容重現處理之重現裝置中儲存有內容管理單元(CPS單元)1, 301之單元鍵Ku1，而未儲存內容管理單元(CPS單元)2, 302之單元鍵Ku2時，統籌控制內容重現處理之重現應用程式於檢測有應用之單元間之切換及內容之切換時，執行需要取得單元鍵之訊息顯示等之處理。

[3.資訊記錄媒體之資料記錄構造、加密構造及內容散列之詳細內容]

其次，說明資訊記錄媒體之資料記錄構造、加密構造及內容散列之詳細內容。首先，參照圖4說明剪輯檔與ECC區塊之對應。儲存於資訊記錄媒體之資料係以作為執行內容記錄重現之驅動器之最小資料記錄重現單位之ECC區塊單位來記錄資料。本例中，ECC區塊如圖4(a)所示，係設定64KB之資料。圖4(a)顯示實際層中之資料記錄構造，(b)顯示對應於實際層之記錄內容之剪輯檔。

如參照圖2之說明，內容係將剪輯檔作為管理單位來設定。圖4(b)中顯示剪輯AV流記錄有：

剪輯No.=#00003

剪輯No.=#00005

剪輯No.=#00023

之數個剪輯檔之構造例。

圖例中，剪輯：#00001~#00023之各剪輯檔儲存於資訊記

錄媒體中，各剪輯予以細分化，細分化資料作為資料#000nn_x而分散記錄於以UDF(通用光碟格式)管理之1個連續記錄區域(Extent)。

本發明之資訊記錄媒體之資料記錄構造，係使各剪輯之最前資料，亦即剪輯檔之AV流資料之最前資料之資料[#000nn_0]，均與實際層中之ECC區塊(64 KB)之最前一致來記錄。此因，可有效進行對應於各剪輯檔而設定之散列單元之讀取，及自散列單元算出散列值等之處理。此等處理於後段詳細作說明。

本實施例中，與實際層中之ECC區塊(64 KB)之最前一致之記錄者，僅為剪輯檔之AV流資料之最前資料之資料[#000nn_0]，其他後續資料[#000nn_1~]無須與ECC區塊之最前一致。不過，亦可形成使全部之連續記錄區域(Extent)資料之最前與ECC區塊之最前一致來記錄之構造，藉由該構造，可更有效算出散列值。

其次，參照圖5，說明剪輯檔與散列單元之對應。如前述，作為參照圖1而說明之資訊記錄媒體100之儲存資料之內容散列114，係依據儲存於資訊記錄媒體100之內容或加密內容之構成資料之散列值，並適用於內容之竄改驗證。本發明之構造中，將作為構成CPS單元之AV流實際資料之剪輯檔予以細分化，設定指定資料單位(如192 KB)之散列單元，算出各散列單元之散列值，將各散列單元單位之散列值記錄於內容散列表(CHT)，而儲存於資訊記錄媒體中。

顯示於圖5之最上段之(b)顯示對應於圖4所示之(b)之實

際層中之剪輯檔之排列。各剪輯檔之構成資料如前述地可予以細分化而分散記錄於資訊記錄媒體中。此等分散資料如圖5(c)所示，係在邏輯層中依各剪輯檔來管理。執行內容重現處理之資訊處理裝置中之重現應用，按照位址讀取分散記錄於資訊記錄媒體之剪輯檔之構成資料，在邏輯層上構成1個剪輯檔，來執行資料解碼處理及重現處理等。

執行內容重現處理之資訊處理裝置中之重現應用，執行內容之竄改驗證處理。內容之竄改驗證如自作為重現對象而選擇之剪輯檔隨機選擇數個散列單元，算出對應於選出之散列單元之內容資料之散列值，執行此等算出散列值與預先記錄於資訊記錄媒體中之內容散列表(CHT)之儲存值(對照用散列值)之對比。於此等之散列值一致時，判定為內容未遭竄改，並轉移至內容之解碼、重現處理，不一致情況下，判定為內容遭竄改，而中止內容之解碼、重現處理。

如圖5(d)所示，散列單元設定成將邏輯層中之剪輯檔予以細分化之資料單位(192 KB)單位。如圖5(e)所示，各散列單位相當於96個邏輯扇區(2048B)部分之資料。

如圖5(d)所示，對應於各剪輯檔而設定之散列單元中設定散列單元編號(#0, #1, #2・・・)。圖5顯示於剪輯檔(#00003)中包含散列單元#0~#1233，於剪輯檔(#00005)中包含散列單元#1234~之構造例。

儲存於資訊記錄媒體之內容散列表(CHT)中儲存各個散列單元之散列值(對照用散列值)，並且記錄各剪輯檔最前之散列單元編號。藉由該構造，執行散列值驗證之資訊處理

裝置(重現裝置)可依據記錄於內容散列表(CHT)之剪輯檔之最前散列單元編號，有效選擇對應於重現對象之剪輯之驗證對象之散列單元。內容散列表(CHT)之構造及應用CHT之處理詳細內容於後段作說明。

圖6係儲存於資訊記錄媒體之資料之加密處理構造之說明圖。內容之加密係將作為顯示於圖6(f)之密碼處理單位而設定之校正單元(Aligned Unit)作為單位來執行。如圖6(g)所示，1個密碼處理單位(Aligned Unit)係藉由3個扇區資料(2048B(位元組))之6144B(位元組)而構成。1個扇區資料相當於圖5(e)之1個扇區資料。

如圖6(h)所示，1個密碼處理單位(Aligned Unit)係藉由16位元組之非加密部分與6128位元組之加密部分而構成。自非加密部分取得作為區塊鍵生成值之種，藉由與依據自參照圖1而說明之媒體鍵區塊而取得之媒體鍵等各種資訊而生成之單元鍵(unit Key)之密碼處理(AES_E)及配置邏輯和運算，而生成區塊鍵，並執行對明文之加密處理(AES_ECBC)，而生成6128位元組之加密資料。

應用區塊鍵之加密處理係應用AES密碼十進制之CBC模式來執行，該加密處理參照圖7作說明。

圖7(i)顯示儲存於資訊記錄媒體中之內容明文。明文分割成16位元組單位，各分割區塊執行排他邏輯和運算及經由加密部(AES)執行加密，其結果資料與後續之16位元組資料予以排他邏輯和，並反覆處理來執行AES加密。連結加密部(AES)之輸出，而生成顯示於圖7(j)之加密資料。該加密

資料係圖7(h)之資料，其與圖6(h)之資料相同，而成為藉由2048位元組之3個散區資料構成之1個密碼處理單位(Aligned Unit)之6128位元組之加密部分。另外，進行與最前之明文單元16位元組之排他邏輯和運算處理之初始值(IV)，係自顯示於圖6(h)之非加密部份取得之種。

如此生成之加密資料分割成ECC區塊，而記錄於資訊記錄媒體中。另外，執行內容重現處理之資訊處理裝置(重現裝置)執行與按照顯示於圖7之AES密碼十進制之CBC模式相同之解碼處理，並執行自加密資料生成解碼資料(明文)之處理。

其次，參照圖8說明記錄於資訊記錄媒體之ECC區塊排列及散列單元之對應。圖8(a)顯示與圖4(a)相同之實際層中之ECC區塊排列。圖8(m)中，顯示邏輯層上之散列單元之排列。各散列單元如參照圖5之說明，分別對應於任一個剪輯檔之構成資料，各散列單元包含指定之資料長(如192 KB)之資料構造。

散列單元為192 KB，由於一方ECC區塊係64 KB構造，因此1個散列單元係作為與3個ECC區塊相同之資料長來設定。ECC區塊係驅動器中之資料記錄重現之處理單位。執行內容重現之資訊處理裝置(重現裝置)於內容重現之前，讀取屬於重現對象之內容管理單元(CPS單元)之1個以上之散列單元，來算出散列值，並與記錄於內容散列表(CHT)中之對照用散列值對照。

此時，驅動器執行以ECC區塊單位之資料讀取。邏輯層

上之邏輯扇區雖可分散記錄於實際層上之實際扇區中，不過，通常如1個剪輯檔中包含之扇區資料，亦即在邏輯層上連續之扇區資料，在實際層上亦連續記錄。

本發明之資料記錄構造如前述參照圖4之說明，係進行使各剪輯檔之最前與實際層中之ECC區塊最前一致之記錄。再者，各散列單元(192 KB)設定成ECC區塊(64 KB)之整數倍(3倍)之資料長。因而，通常散列單元之讀取係藉由3個ECC區塊之讀取來實現。因而，執行依據散列值之資料驗證之資訊處理裝置通常可藉由最低限度之ECC區塊之讀取來實現散列驗證中之資料讀取處理，而可進行有效之驗證處理。

另外，如圖8(n)所示，散列單元對應於作為資料處理單位(加密處理單位)之校正單元之連結資料。圖8(n)之校正單元係邏輯層上之排列，不過本發明之資料記錄構造中，實際層之排列往往亦顯示相同之排列。

參照圖9說明作為資料處理單位(加密處理單位)之校正單元之邏輯層上之排列與實際層上之排列之對應。圖9(L1)顯示邏輯層上之校正單元排列，圖9(P1)顯示應用本發明之構造時之實際層上之校正單元排列，最上段之圖9(L2)顯示進行先前之資料記錄處理時之實際層上之校正單元排列。

本發明之構造，亦即圖9(L1)之邏輯層上之校正單元排列與圖9(P1)之實際層上之校正單元排列中，至少各剪輯檔最前部分之資料如圖所示地一致排列。此因進行前述參照圖4而說明之資料記錄處理，亦即使剪輯檔之最前部分與實際層上之ECC區塊最前一致之資料記錄。先前由於未進行此

種資料記錄，因此如圖9(P2)所示，在實際層上，作為資料處理單位(加密處理單位)之校正單元往往隔離記錄。現行原則雖禁止將邏輯扇區(2048B)過度細分地分割，不過允許將加密單位之校正單元(6144B=2048B×3)區分成每個扇區(2048B)。因而經常出現如圖9(P2)所示之零零落落之資料。

藉由採用本發明之資料記錄構造(圖9(P1))，不但散列算出時之記錄媒體存取有效率，且儲存於資訊記錄媒體之內容之密碼處理中亦可有效處理。亦即，如圖9(P2)所示，在實際層上分割校正單元來記錄時，執行資料記錄時之加密處理及資料重現時之解碼處理之程式無效率。如前述，內容之加密及解碼時係使用CBC模式。連鎖之單位為6144B(＝校正單元之尺寸)。因此，校正單元#X_1與校正單元#X_2之加密及解碼時，(邏輯上)需要之前之校正單元之最後16B(AES之最小單位)。

亦即，密碼處理如前述參照圖7之說明，包含執行某個單元之運算結果與連續之單元間之運算(排他邏輯和)之處理。因此，分割校正單元內之邏輯扇區時，在將校正單元#1_1予以加密時，於隔離之資料存取期間中，須預先保持校正單元#1_0之最後16B。1個內容中包含許多校正單元，進行資料記錄或重現時，隔離之單元之存取時間保留。此種存取等待時間累積，因而造成資料處理效率降低。反之。採用圖9(P1)之排列時，各單元連續地排列。因而資料記錄、重現時之存取可連續地執行，資料存取時間減少，可進行有效之處理。

其次，說明每散列單元儲存對應於各散列單元之對照用散列值，亦即依據正當之內容資料預先計算完成之散列值之內容散列表(CHT)之構造例。圖10顯示對資訊記錄媒體之1個記錄層(記錄Layer)設定之1個內容散列表(CHT)之資料構造例。

內容散列表(CHT)中，於

全部剪輯數(NC)

全部散列單元數(NH)

之各資料後面，就各剪輯(i)，記錄有：

剪輯(i)之最前散列單元編號，

剪輯(i)之檔名對應編號，及

剪輯(i)之偏置值

之各資料，再者，

各剪輯記錄作為各散列單元之散列值(對照用散列值)之[Hash Value]。

作為各散列單元之散列值(對照用散列值)之[Hash Value]，係藉由執行正當之內容記錄處理之如光碟工廠來記錄。

全部散列單元數(NH)如於資訊處理裝置(重現裝置)中，執行散列值算出及對照處理之內容驗證情況下，隨機選擇散列單元編號時，使用於取得作為其選擇範圍之數量。具體之處理例於後述。

藉由對全部散列編號選擇散列單元，可提高竄改檢測精確度。不應用散列單元數，而採用自全部剪輯編號隨機選

擇剪輯編號，自選出之剪輯內隨機選擇散列單元之方法時，如光碟中記錄「極小尺寸之未遭竄改之剪輯檔999個」與「遭竄改之大尺寸之剪輯檔1個」時，雖檢測竄改之可能性降低，不過藉由對全部散列編號選擇散列單元之構造，可提高竄改檢測知可能性。

剪輯(i)之最前散列單元編號對光碟上之剪輯檔(如最多1000個)，分別賦予0~NC之編號。而後記述屬於各剪輯檔之散列單元之(邏輯性)最前散列單元全體之編號。其如前述參照圖5之說明。

所謂剪輯(i)之偏置值係光碟之層(記錄層)之識別值。層0之偏置值全部為0。層1之偏置值係作為顯示層0中包含之剪輯之散列單元數之值來設定。藉由該值可輕易瞭解層1之表之散列單元之邏輯位址。

執行來自資訊記錄媒體之內容重現之資訊處理裝置(重現裝置)，於資訊記錄媒體重現時，比較自資訊記錄媒體上之內容之任意散列單元計算之散列值與記載於內容散列表之對照用散列值，可進行內容之竄改驗證。

參照圖11說明內容散列表(CHT)之具體構造。圖11(A)顯示具有兩個記錄層(Layer0, 1)之資訊記錄媒體(光碟)之資料記錄構造，圖11(B)顯示對應於該記錄資料之內容散列表之構造。

如圖11(A)所示，具有兩個記錄層(Layer0, 1)之資訊記錄媒體(光碟)中記錄4個剪輯(Clip0~3)，散列單元之總數(NH)為64個。剪輯0具有16個散列單元，此等全部記錄於層0。

剪輯1之8個散列單元記錄於層0，層1中記錄有12個散列單元。層2之8個散列單元記錄於層0，層1中記錄有4個散列單元。層3係16個散列單元記錄於層1之剪輯。

而係

層0之散列單元總數(L0_NH)=32，

層1之散列單元總數(L1_NH)=32。

該構造中，內容散列表(CHT)係以層單位設定，而記錄兩個內容散列表。顯示於圖11(B)者係顯示內容散列表之標頭與本體之各資料。(B1)係層0之內容散列表之標頭資料，就層0中包含之各剪輯(Clip0~2)，儲存：

剪輯(i)之最前散列單元編號＝Start，

剪輯(i)之檔名對應之編號＝Clip#，及

剪輯(i)之偏置值＝Offset

之各值。

(B2)係層0之內容散列表之本體資料，並儲存層0中包含之各散列單元(散列編號0~31)之對照用散列值。

(B3)係層1之內容散列表之標頭資料，

就層1中包含之各剪輯(Clip1~3)，儲存：

剪輯(i)之最前散列單元編號＝Start，

剪輯(i)之檔名對應之編號＝Clip#，及

剪輯(i)之偏置值＝Offset

之各值。

(B4)係層1之內容散列表之本體資料，並儲存層0中包含之各散列單元(散列編號32~63)之對照用散列值。

執行來自資訊記錄媒體之內容重現之資訊處理裝置(重現裝置)，於資訊記錄媒體重現時，比較自資訊記錄媒體上之內容之任意散列單元計算之散列值與記載於內容散列表之對照用散列值，來進行內容之竄改驗證。此等處理於後段作說明。

其次，參照圖12說明內容散列表(CHT)之其他構造例。圖12(A)顯示每個剪輯檔設定1個內容散列表(CHT)時之內容散列表(CHT)之例。並儲存對應於儲存於資訊記錄媒體之剪輯數之內容散列表(CHT)。

顯示於圖12(A)之內容散列表(CHT)中，

包含顯示係對應於哪個剪輯編號之內容散列表(CHT)之識別資訊，而後，就該剪輯(n)之以下資訊，記錄：

全部散列單元數(NH)

剪輯(n)所屬之CPS單元編號

作為每個散列單元之散列值(對照用散列值)之[Hash Value]

之各資訊。

對1個剪輯檔設定1個內容散列表(CHT)之構造，進一步儲存顯示於圖12(B)之內容散列表－剪輯檔相關連表。

內容散列表－剪輯檔相關連表，於

全部剪輯數(NC)

全部散列單元數(NH)

之各資料後面，就各剪輯(i)，記錄有：

剪輯(i)之最前散列單元編號，及

剪輯(i)之檔名對應編號

之各資料。

如圖12(A)所示，對1個剪輯檔設定1個內容散列表(CHT)之構造，如執行內容重現之資訊處理裝置欲存取某個剪輯AV流#xxxxx時，須選擇對應於該剪輯AV流#xxxxx之散列單元，進行散列算出及對照。該選擇處理時，需要剪輯AV流檔編號#xxxxx與散列表之對應資訊，該對應資訊係應用圖12(B)之內容散列表－剪輯檔相關連表。

另外，亦可不應用顯示於圖12(B)之內容散列表－剪輯檔相關連表，如作為在內容散列表(CHT)之資料檔名中設定對應於剪輯AV流檔編號#xxxxx之識別資料之構造，而形成內容散列表(CHT)之資料檔可識別對應於哪個AV流資料檔。如係將內容散列表(CHT)之資料檔名作為[CHT_XXXX.dat]之構造。

[4.資訊記錄媒體之製造、資料儲存處理之詳細內容]

如上述，資訊記錄媒體中，內容及對應於各散列單元而設定之散列值記錄儲存於內容散列表(CHT)中。以下說明具有此種資料紀錄構造之資訊記錄媒體之製造、資料儲存處理之詳細內容。

如圖13所示，在內容編輯實體(AS：編輯室(Authoring Studio))330中編輯儲存於資訊記錄媒體之內容，而後，於資訊記錄媒體製造實體(DM：光碟製造廠)(＝加密實體)350中大量複製(Replica)如CD、DVD、Blu-ray光碟等，來製造資訊記錄媒體100，並提供使用者。資訊記錄媒體100在使

用者之裝置(資訊處理裝置)400中重現。

執行該光碟製造、販賣、使用處理全體之管理者，係管理中心(TC：Trusted Center)(＝許可證實體)310。管理中心(TC：Trusted Center)310對資訊記錄媒體製造實體(DM：光碟製造廠)350提供各種管理資訊，如對應於媒體(資訊記錄媒體)而設定之媒體鍵Km、儲存媒體鍵Km作為加密資料之加密鍵區塊之MKB，資訊記錄媒體製造實體(DM：光碟製造廠)350依據自管理中心(TC：Trusted Center)310接收之管理資訊，進行自內容編輯實體(AS：編輯室)330接收之內容之編輯、加密、鍵資訊之生成、儲存處理等。此外，管理中心(TC：Trusted Center)310亦進行儲存於使用者之資訊處理裝置400之裝置鍵之管理及提供。

參照圖14說明管理中心310、內容編輯實體330及資訊記錄媒體製造實體350執行之處理例。

將編輯前內容303帶到內容編輯實體330，藉由編碼器對MPEG資料等進行編碼處理，及藉由編輯系統進行編輯處理(步驟S11)後，生成作為編輯完成內容之分割主檔(Cutting Master)331。

另外，編輯系統之編輯處理(步驟S11)時，亦生成對應於內容之限制複製資訊及限制重現資訊之CCI資訊(複製、重現控制資訊)，以及使用於內容加密之記錄種，不過圖上並未顯示。如前述，各CPS單元可設定記錄種，編輯完成內容331具有數個內容管理單位(CPS單元)時，記錄種Vu亦生成CPS單元之數量。顯示於圖中之編輯完成內容331中包含

CCI資訊及記錄種Vu，作為編輯完成內容之分割主檔331送至資訊記錄媒體製造實體350。

資訊記錄媒體製造實體350自管理中心310取得內容加密時需要之資訊(管理資訊)。

管理中心310生成媒體鍵Km313，並生成將媒體鍵Km313作為加密資料而儲存之媒體鍵區塊(MKB)311，將此等媒體鍵區塊(MKB)311、媒體鍵Km313以及資訊記錄媒體製造實體350之公開鍵之公開鍵證明書(MF Key Certificate)312提供資訊記錄媒體製造實體350。

如前述，MKB312儲存有僅藉由應用儲存於保持作為正當之內容利用權之許可證之重現裝置中之裝置鍵之解碼處理而可解碼之加密資料，僅保持作為正當內容利用權之許可證之重現裝置可取得媒體鍵Km。

資訊記錄媒體製造實體350自內容編輯實體330接收作為編輯完成內容之切割主檔331，自管理中心310接收媒體鍵區塊(MKB)311、公開鍵證明書(MF Key Certificate)312及媒體鍵Km313，來製造資訊記錄媒體。

首先，於步驟S21中，執行對切割主檔331應用媒體鍵313之加密處理及散列計算。加密處理如執行以按照前述參照圖7而說明之AES密碼十進制之CBC模式之密碼處理。此外，散列計算係執行前述以散列單元單位之散列值算出處理，並執行生成將算出值作為對照用散列值來記錄之內容散列表(CHT)之處理。內容散列表(CHT)具有前述參照圖11、圖12而說明之構造。另外，如前述說明，記錄剪輯單

位之內容散列表(CHT)時，依需要一併生成內容散列表－剪輯檔相關連表。

加密內容與內容散列表(CHT)之生成完成時，於步驟S22中，執行作為記錄資料之光碟影像生成處理。光碟影像中包含記錄於資訊記錄媒體(光碟)之全部資料。除加密內容及內容散列表之外，還包含媒體鍵區塊(MKB)311及公開鍵證明書(MF Key Certificate)312。

光碟影像之生成完成時，於步驟S23中，執行光碟影像之調製處理，生成作為記錄訊號之調製資料，並藉由依據步驟S24中之調製資料之控制處理，生成作為光碟原盤之母盤。再者，於步驟S25中執行複製(Replication)，而生成許多光碟，經過步驟S26中之檢查步驟，於步驟S27中出貨。

另外，內容加密及內容散列表(CHT)之生成，於步驟S24之控制處理前，可以層單位執行。如前述參照圖10、圖11之說明，係因內容散列表(CHT)具有每層獨立之構造。複製(Replication)時，藉由使用各層之母盤進行位元轉印，而生成具有許多層之光碟。

其次，詳細說明資訊記錄媒體製造實體350於步驟S21中執行之加密內容及內容散列表(CHT)之生成處理。首先，參照圖15之流程來說明內容之加密處理與隨伴內容散列表(CHT)之生成之光碟影像生成處理之詳細順序。

首先，於步驟S101中，進行適用於光碟影像生成之輔助資訊檔(MSTBL.DAT)之讀取。該輔助檔包含於作為自內容編輯實體330接收之編輯完成內容之切割主檔331。

圖16顯示光碟影像生成用輔助資訊檔(MSTBL.DAT)之具體例，圖17顯示作為包含於光碟影像生成用輔助資訊檔(MSTBL.DAT)之資料說明之語法。

光碟影像生成用之輔助資訊檔(MSTBL.DAT)中包含自切割主檔331生成光碟影像時需要之資訊。具體而言，包含以下資訊：

UD_START_Location：各層之使用者資料(資料區)之開始點之實際扇區編號(Physical Sector Number)。

UD_END_Location：各層之使用者資料(資料區)之結束點之實際扇區編號。

CHT_Location：CHT之開始點之實際扇區編號。

CHT_Offset：CHT之開始點與散列值(控制設施放入資料)之前之位元數。

Content_Cert_Location：內容證明書開始點之實際扇區編號。

Content_Cert_Offset：內容證明書開始點與內容ID(控制設施放入資料)之前之位元數。

UK_Inf_Location：Unit_Key.inf(參照P.2)之開始點之實際扇區編號。於其層中未記錄Unit_Key.inf時，記述00000000_{16}。

UK_Inf_Offset：Unit_Key.inf之開始點與CPS Unit#1之加密單元鍵之前之位元數。於其層中未記錄Unit_Key.inf時，記述00000000_{16}。

Num_of_UK：光碟全體之單元鍵數(＝CPS單元之數)。

MFK_Cert_Location：MF Key Certificate之開始點之實際扇區編號。尺寸固定。其層中未記錄MFK_Cert時，記述00000000_{16}。

MKB_Location：MKB之開始點之實際扇區編號。其層中未記錄MKB_Cert時，記述00000000_{16}。

N：層i之邏輯扇區數。

Encryption_Flag：是否加密之旗標。

Data_Type：顯示扇區類型之旗標。

CPS_Unit_No：CPS單元編號。

Clip_AV_File_No：剪輯檔編號。用於作成CHT之資訊。

Last_Sector_of_Clip：(無關於層)顯示各剪輯之最後扇區之旗標。

Last_Sector_of_Layer：顯示各層中之各剪輯之最後扇區之旗標。

光碟影像生成用之輔助資訊檔(MSTBL.DAT)中包含扇區單位是否需要加密，及執行應用哪個單元鍵(CPS Unit Key)之加密等之資訊。資訊記錄媒體製造實體350按照輔助資訊檔(MSTBL.DAT)決定各記錄扇區之處理。

回到圖15繼續說明資訊記錄媒體製造實體350執行之處理流程。步驟S101中，進行輔助資訊檔(MSTBL.DAT)之讀取時，於步驟S102中，設定作為處理扇區No.之變數J=0，作為初始設定。

於步驟S103中，執行j＜全部扇區數之判定，j＜全部扇區數之判定為Yes時，進入步驟S104，自分割主檔讀取使用者

扇區資料(j)。於步驟S105中，參照使用者扇區資料(j)之加密旗標，並依據加密旗標之值決定是否需要加密處理。加密旗標(Encryption Flag)如記載於圖16所示之輔助檔，而為[00]時，係不需要加密之扇區，為[1]時，係需要加密之扇區。

加密旗標並非0時，判定為需要密碼處理之扇區，並進入步驟S106。加密旗標為0時，判定為不需要密碼處理之旗標，並進入步驟S115。步驟S106係讀取對應於處理扇區之CPS單元No(j)。其次於步驟S107中判定對應於處理扇區之資料類形式否為1。

資料類型(Data Type)如記載於圖16所示之輔助檔而為[01]時，表示係校正單元(AU)之最初之扇區。此時進入步驟S108，取得前述參照圖7而說明之AES－CBC模式之密碼處理中之初始值(IV)。該初始值如應用自管理中心提供之值。

於步驟S107之判定中，判定資料類型(Data Type)並非1時，表示並非校正單元(AU)之最初之扇區。此時進入步驟S109，而取得已執行AES－CBC模式之處理之前扇區(j－1)之密文單元。其次，於步驟S110中，執行應用單元鍵之AES密碼處理。此等處理相當於前述參照圖7而說明之AES－CBC模式之密碼處理程序。

生成1個密文單元時，於步驟S111中，讀取執行處理之剪輯AV檔No.，於步驟S112中，在剪輯對應之緩衝器中儲存密碼單元(16B)，於步驟S113中判定緩衝器之儲存資料是否

達到192位元組，於達到時，在步驟S114中算出散列值。亦即，於每次達到散列單元之單位之192 KB時算出散列值，並作為儲存於內容散列表之對照用散列值而儲存於記憶體中。

以上之處理於步驟S115中，藉由增加扇區No.，以扇區單位反覆執行。執行全部之扇區處理，於步驟S103之判定中，

j＜全部扇區數？

之判定為No時，進入步驟S121。

步驟S121中，生成於192之該散區單元單位中儲存算出之對照用散列值之內容散列表(CHT)。內容散列表(CHT)具有參照前述圖10~圖12而說明之構造。

再者，於步驟S122中作成內容證明書。就內容證明書之構造，參照圖18作說明。內容證明書係證明儲存於資訊記錄媒體之內容係正當之內容之證明書，如以1層單位設定1個證明書，並儲存於資訊記錄媒體中。

內容證明書中包含以下之資訊。

(a)CC：資訊記錄媒體全體之內容證明書數量

(b)ID：內容ID

(c)NC：記錄於各層之全部剪輯檔數量

(d)各剪輯之內容散列摘要

(e)電子簽署(Signature)

此等中之(b)內容ID係對應於內容之識別資料，且係自管理中心310提供之值。(d), (e)係在資訊記錄媒體製造實體350中生成之資料。

內容散列摘要如記錄藉由以下之算出處理而算出之值。

剪輯(j)之內容散列摘要之算出處理例

記錄於層i之內容散列表之剪輯(j)之散列值，如對

Hash Value(k)||Hash Value(k+1)|| … ||Hash Value(l-1)||Hash Value(l)

如以SHA-1進行散列計算，並將該算出值作為剪輯(j)之內容散列摘要來設定。另外，上述公式中，||表示資料連結。

電子簽署(Signature)係對記錄於內容證明書之資料(CC~Clip(NC-1))之電子簽署。簽署鍵使用資訊記錄媒體製造實體350之機密鍵(SK_MF)。電子簽署函數中如使用RSA。重現資訊記錄媒體之資訊處理裝置，自儲存於資訊記錄媒體之資訊記錄媒體製造實體350之公開鍵證明書取得公開鍵，執行內容證明書之簽署驗證，來驗證資料有無竄改驗證，亦即驗證內容證明書之正當性。

另外，藉由內容編輯實體(編輯設施)計算內容散列時，剪輯之內容散列摘要及簽署藉由內容編輯實體(編輯設施)寫入。

參照圖19說明儲存加密內容之其他資料之資訊記錄媒體製造時之資料流動及資料處理全體。圖19中顯示：管理中心(TC：Trusted Center)(＝許可證實體)510、內容編輯實體(AS：編輯室)(＝編輯設施)530、資訊記錄媒體製造實體(DM：光碟製造廠)(＝加密設施)550及最後製造之資訊記錄媒體(光碟)600。

資訊記錄媒體製造實體550自管理中心510取得儲存媒體

鍵(Km)之媒體鍵區塊(MKB)，取得媒體鍵之同時，自內容編輯實體530取得明文內容532及記述加密處理之詳細資訊之輔助檔(MSTB.DAT)531，並應用單元鍵551，執行內容之加密處理(步驟211)，而生成加密內容552。內容之加密處理，如前述參照圖15之說明，扇區單位之處理係作為AES-CBC模式之密碼處理(參照圖7)來執行。生成之加密內容552係儲存於資訊記錄媒體600之加密內容601。

再者，資訊記錄媒體製造實體550在步驟S212中，於生成之加密內容552之指定資料單位(散列單元)算出散列值。該處理係對應於前述參照圖15而說明之步驟S112~S114之處理，而算出散列單元之資料長之192 KB之資料單位之散列值。生成將此等散列值作為對照用散列值來記錄之內容散列表553，而作為儲存於資訊記錄媒體600之內容散列表602。

再者，資訊記錄媒體製造實體550於步驟S213中，執行內容證明書之生成處理。內容證明書係證明前述參照圖18而說明之具有資料構造之內容之正當性用之資料。此時儲存依據儲存於內容散列表602之散列值之內容散列摘要(參照圖18)，進一步附加對應於儲存資料之電子簽署。

管理中心510保存資訊記錄媒體製造實體550之機密鍵(SK_MF)512及公開鍵(PK_MF)513，並將儲存機密鍵512與公開鍵(PK_MF)513之公開鍵證明書514提供資訊記錄媒體製造實體550。

資訊記錄媒體製造實體550應用自管理中心510接收之機

密鍵(SK_MF)554，執行對內容證明書之電子簽署，而生成附加電子簽署之內容證明書555。其作為儲存於資訊記錄媒體600中之內容證明書603。

再者，資訊記錄媒體製造實體550將自管理中心510接收之公開鍵證明書556記錄於資訊記錄媒體。其成為儲存於資訊記錄媒體600之公開鍵證明書604。

圖19之處理例係按照圖15之處理流程之處理例，各個實體之角色分擔並不限定於圖15及圖19所示之處理例。參照圖20~圖21來說明其他之處理例。

圖20係內容編輯實體(AS：編輯室)(＝編輯設施)530執行散列值算出處理及內容散列表(CHT)之生成處理之處理例。顯示於圖20之虛線部之構造與圖19所示之處理例不同。

內容編輯實體530於步驟231中，依據明文內容532抽出散列單元，算出各散列單元之散列值，而生成記錄此等之內容散列表(CHT)533。此時，以明文資料之指定資料長單位設定之各散列單元求出散列值。

內容散列表(CHT)533提供資訊記錄媒體製造實體550，資訊記錄媒體製造實體550依據儲存於內容散列表(CHT)553之散列值，算出內容散列摘要(參照圖18)，於內容證明書中儲存算出之內容散列摘要，進一步生成對應於儲存資料之電子簽署，而生成附加電子簽署之內容證明書555。其作為儲存於資訊記錄媒體600之內容證明書603。

該處理例係內容編輯實體530執行依據明文內容算出內容散列及生成內容散列表。資訊記錄媒體製造實體550執行

內容證明書之生成及電子簽署附加處理。

其次，參照圖21，說明資訊記錄媒體製造實體550執行依據明文內容之內容散列之算出及內容散列表之生成之處理例。圖21所示之虛線部之構造與圖19所示之處理例不同。

資訊記錄媒體製造實體550於圖21所示之步驟S551中，依據自內容編輯實體530接收之明文內容，抽出散列單元，算出各散列單元之散列值，而生成記錄此等之內容散列表(CHT)553。此時以明文資料之指定資料長單位而設定之各散列單元求出散列值。

資訊記錄媒體製造實體550依據儲存於內容散列表(CHT)553之散列值，算出內容散列摘要(參照圖18)，於內容證明書中儲存算出之內容散列摘要，進一步生成對應於儲存資料之電子簽署，而生成附加電子簽署之內容證明書555。其作為儲存於資訊記錄媒體600之內容證明書603。

該處理例係資訊記錄媒體製造實體550執行依據明文內容之內容散列之算出及內容散列表之生成之處理例。

再者，其他處理例，亦可由內容編輯實體執行如依據明文內容之內容散列之算出、內容散列表之生成以及內容證明書之生成、簽署處理之全部處理。因而，內容散列之算出、內容散列表之生成及內容證明書之生成、簽署，並不限定於資訊記錄媒體製造實體550，亦可構成在內容編輯實體530或資訊記錄媒體製造實體550之任何一個中執行。

[5.內容重現處理中應用內容散列之驗證處理]

其次說明內容重現處理中應用內容散列之驗證處理。

參照圖22~圖24，說明依據於執行來自資訊記錄媒體之內容重現之資訊處理裝置(重現裝置)中執行之散列值之內容驗證處理。

執行來自資訊記錄媒體之內容重現處理之資訊處理裝置具有：內容驗證機構，其係驗證內容之正當性；及內容重現機構，其係依據內容驗證機構之驗證，將確認內容之正當性作為條件，來執行內容之重現處理；內容驗證機構具有執行內容驗證處理之構造，其係選擇n個(其中n為1以上整數)作為記錄於資訊記錄媒體之內容之細分化資料而設定之散列單元，執行依據選擇散列單元之算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理，並將選擇之n個全部散列值對照成立作為內容正當性之確認條件。

圖22顯示資訊處理裝置(重現裝置)中之內容驗證機構執行之處理概要。資訊處理裝置(重現裝置)621安裝記錄內容之資訊記錄媒體622，於內容重現之前，選擇對應於預定重現之內容之散列單元，來執行對散列單元設定之散列值之對照。

首先，於步驟S301中，選擇執行對照處理之散列單元。從前述之說明可知，資訊記錄媒體之儲存內容區分成指定資料長(如192 KB)之散列單元。資訊記錄媒體621執行自此等許多散列單元執行對照處理之單元之選擇。單元選擇處理詳細內容，參照圖24於後段詳細說明。作為對照處理對象而選擇之散列單元，係隨機選擇數個(n個)，如3個散列單元。

選擇之散列單元係：

散列單元#1

散列單元#12345

散列單元#99999

於步驟S302中，自資訊記錄媒體622讀取對應於選出之散列單元之散列單元對應資料，算出各選擇散列單元之散列值。將算出散列值分別作為：

散列單元#1之散列值＝aaa

散列單元#12345之散列值＝bbb

散列單元#99999之散列值＝ccc

另外，於步驟303中，自儲存於資訊記錄媒體622之內容散列表623，讀取在步驟S301中選擇之對照處理對象之內容散列單元之對照用散列值。讀取之對照用散列值係：

散列單元#1之散列值＝AAA

散列單元#12345之散列值＝BBB

散列單元#99999之散列值＝CCC

於步驟S304中，執行在步驟S302中依據內容之散列單元而算出之散列值，與自內容散列表(CHT)讀取之對照用散列值之比較處理。全部對應之散列單元之算出散列值與對照用散列值一致時，亦即，

aaa=AAA

bbb=BBB

ccc=CCC

成立時，判斷為內容未遭竄改，允許內容重現，並轉移

至內容之重現處理。

另外，檢測出對應之散列單元之算出散列值與對照用散列值之任何一個不一致時，亦即，檢測出

aaa≠AAA

bbb≠BBB

ccc≠CCC

之任何一個時，判斷為內容遭竄改，禁止內容重現，並中止而後之轉移至內容重現處理。

其次，參照圖23、圖24之流程，詳細說明執行內容重現之資訊處理裝置中之內容散列之驗證步驟。

圖23之處理流程係將執行對照處理之散列單元數n作為n=3來設定之處理例。

於步驟S501中，執行散列值對照之資訊處理裝置，作為初始設定，而進行執行對照處理之散列單元數之初始值n=0之設定。於步驟502中，判斷是否n≧3。並非n≧3時，未達到規定之對照數(n=3)，因此執行步驟S503以下之對照處理。

於步驟S503中，n=n+1之設定後，於步驟S504中，依據散列單元編號選擇散列單元。散列單元之選擇係隨機執行。

具體而言，讀取記錄於內容散列表(CHT)之[全部散列單元數(NH)]，選擇x＜NH之亂數(x)。將該選擇之數值(x)作為執行對照處理之散列單元編號#x。

於步驟S505中，自儲存於資訊記錄媒體之內容散列表取得散列單元編號#x之對照用散列值。再者，於步驟S506中，自儲存於資訊記錄媒體之內容之散列單元抽出散列單元編

號#x之散列單元，並依據抽出之散列單元算出散列值，於步驟S507中，執行算出散列值與對照用散列值之比較處理。

於步驟S508中，進行算出散列值與對照用散列值之一致判定，一致時，回到步驟S502，進行n≧3之判定，未達到規定之對照數(n=3)時，在步驟S503中更新n後，於步驟S504中進一步執行新的散列單元之選擇，在以下步驟S505~S507中，就不同之散列單元，執行同樣之算出散列值與對照用散列值之對照處理。反覆執行規定次數之該處理，在確認規定數(n=3)全部之散列值一致時，於步驟S502中，n≧3?之判定為Yes，於步驟S510中，允許重現，而轉移至重現處理。

規定次數、n次之散列值驗證處理過程中，步驟S508之算出散列值與對照用散列值之一致判定中，未確認一致時，進入步驟S509，禁止重現，不轉移至內容之重現處理。

對加密內容設定對照對象之散列值時，如上述之處理，可自對應於自資訊記錄媒體讀取之加密內容之散列單元直接算出散列值，不過，對前述說明之明文算出散列值，作為對照用散列值而記錄於內容散列表(CHT)時，算出散列值亦須依據明文算出。

參照圖24，說明進行依據明文之散列值之驗證之處理步驟。顯示於圖24之處理對應於顯示於圖23之處理流程之步驟S504~S507之處理。進行步驟S501~S503之處理後，於圖24之步驟S521中，讀取記錄於內容散列表(CHT)之[全部散列單元數(NH)]，並選擇x＜NH之亂數。

於步驟S522中，自儲存於資訊記錄媒體之內容散列表取得散列單元編號#x之對照用散列值(Hash Value(x))。於步驟S523中，計算散列單元編號#x之單元屬於哪個剪輯。

如前述，內容散列表(CHT)中，於

全部剪輯數(NC)

全部散列單元數(NH)

之各資料後面，就各剪輯(i)，記錄有：

剪輯(i)之最前散列單元編號，

剪輯(i)之檔名對應編號，及

剪輯(i)之偏置值

之各資料，再者，

各剪輯記錄作為各散列單元之散列值(對照用散列值)之[Hash Value]。

依據內容散列表之記錄資料，自散列單元編號算出所屬之剪輯。其次於步驟S524中，生成剪輯AV流所屬之內容管理單元(CPS單元)之單元鍵。如前述參照圖2、圖3之說明，各剪輯屬於任何一個內容管理單元(CPS單元)，各內容管理單元(CPS單元)中搭配單元鍵，藉由單元鍵進行加密。於步驟S524中，生成該單元鍵。另外，單元鍵之生成處理於後述。

其次，於步驟S525中，進入剪輯AV流，於步驟S526中，取得剪輯AV流中包含之散列單元#x，執行解碼處理。再者，於步驟S527中，依據散列單元#x之解碼資料算出散列值。

於步驟S528中，進行算出散列值與對照用散列值之一致判定，一致時，進一步對其他散列單元執行同樣之處理，於達到規定之對照數(如n=3)前，反覆執行對照處理，於確認規定數(n)全部之散列值一致時，允許重現，並轉移至重現處理。在規定次數、n次之散列值驗證處理過程中，出現未確認一致時，此時禁止重現，不轉移至內容之重現處理。

[6.單元鍵之生成、內容解碼及重現處理]

其次，說明執行內容重現之資訊處理裝置(重現裝置)中之單元鍵之生成、內容解碼、重現處理。單元鍵適用於內容之解碼及重現時，不過，如上述，對解碼資料(明文)設定散列值情況下，於依據散列值進行驗證處理時，亦需要生成，來將散列單元予以解碼。參照圖25、圖26，詳細說明單元鍵之生成、內容解碼、重現處理。

首先，參照圖25說明資訊處理裝置之內容驗證機構、內容重現機構執行之單元鍵之生成、內容解碼處理及內容重現機構執行之內容重現處理。首先，執行單元鍵之生成、內容解碼、重現處理之資訊處理裝置(重現裝置)讀取儲存於記憶體之裝置鍵776，裝置鍵776係儲存於接收關於內容利用之許可證之資訊處理裝置之機密鍵。

其次，於步驟S601中，應用裝置鍵776執行儲存資訊記錄媒體780中儲存之媒體鍵Km之密碼鍵區塊之MKB781之解碼處理，而取得媒體鍵Km。

MKB781係僅藉由依據儲存於具有有效許可證之使用者之資訊處理裝置中之裝置鍵之處理(解碼)，而可取得內容解

碼時需要之鍵之媒體鍵(Km)之鍵資訊區塊。其如前述，藉由按照所謂階層型樹構造之資訊分發方式，使用者裝置(資訊處理裝置)僅於具有有效之許可證時，方可取得鍵，可阻止無效化(Revoke處理)之使用者裝置取得鍵(媒體鍵)。管理中心藉由變更儲存於MKB之鍵資訊，儲存於特定之使用者裝置之裝置鍵無法解碼，亦即，可生成具有無法取得內容解碼時需要之媒體鍵構造之MKB。因此，任何時間均排除(無效化)不正當裝置，而可僅對具有有效之許可證之裝置提供可解碼之加密內容。

其次，於步驟S602中，藉由依據步驟S601中之MKB處理而取得之媒體鍵Km與自資訊記錄媒體780讀取之實際索引782之密碼處理(AES_GD)，生成單元鍵生成鍵Ke(embedded Key)。該鍵生成處理如係作為按照AES密碼十進制之處理來執行。另外，圖25中，AES_D表示應用AES密碼處理之資料解碼(Decryption)處理，AES_GD表示應用AES密碼處理之隨伴資料解碼處理之鍵生成(Key Generation)處理，AES_GE表示應用AES密碼處理之隨伴資料密碼處理之鍵生成(Key Generation)處理。

其次，於步驟S603中，藉由依據單元鍵生成鍵Ke(embedded Key)與自資訊記錄媒體780讀取之內容利用控制資訊(複製、重現控制資訊(CCI))783之密碼處理(AES_GD)，生成控制鍵Kc，於步驟S604中，藉由依據控制鍵Kc與資訊記錄媒體780讀取之內容散列784之密碼處理(AES_GD)，生成內容散列鍵Kh。內容散列784係依據儲存

(S)

於資訊記錄媒體之內容或加密內容之構成資料之散列值。

其次，於步驟S605中，對於自資訊記錄媒體780讀取之加密單元鍵Enc(Ku)785，應用內容散列鍵Kh進行解碼(AES_D)，而取得單元鍵Ku。另外，本例中儲存於資訊記錄媒體780中之單元鍵，作為藉由與圖25之步驟S601~S604相同之處理而生成之內容散列鍵Kh之加密資料來儲存。

另外，各CPS單元定義記錄於資訊記錄媒體780中之加密單元鍵Enc(Ku)785，於S605中生成之單元鍵Ku亦同樣地各CPS單元定義。生成之CPS單元鍵之Ku(i)，係對應於重現對象之內容之CPS單元，亦即對應於自儲存於資訊記錄媒體780之CPS單元1~n選擇之CPS單元(i)而設定之CPS單元鍵Ku(i)。

進行加密內容之解碼時，首先於步驟S606中，進行來自由資訊記錄媒體780讀取之加密內容406之區塊種之取出、解碼處理時需要之解碼處理部(加密資料)，及解碼處理不需要之非解碼處理部(明文資料)之資料選擇。

另外，區塊種係對應於作為加密處理單位之區塊而設定之密碼鍵生成資訊。作為CPS單元之內容資料應用以指定資料長之區塊單位而不同之區塊鍵Kb予以加密，解碼時，藉由對應於各區塊資料而設定之區塊種與依據CPS單元鍵Ku之密碼處理(S607：AES_GE)，而生成作為各區塊之解碼處理鍵之區塊鍵Kb，並以生成之區塊鍵Kb進行解碼處理(S608)。

區塊鍵Kb係在特定尺寸之密碼處理單位中，使用於加密

內容之解碼之鍵。加密處理單位之尺寸，如假設為包含6144位元組之User Data者，及包含2048位元組之User Data者。

步驟S609係結合加密內容中包含之如區塊種部分等之非加密資料與在步驟S608中解碼之資料之處理，結果，輸出解碼內容(CPS單元)777。

參照圖26說明於步驟S602~S605, S607中執行之密碼處理具體例。圖26中，AES解碼部(AES_D)791如係具有128位元之鍵長之AES、ECB模式之解密處理部，AES加密部(AES_E)793如係具有128位元之鍵長之AES、ECB模式之加密處理部。排他性邏輯和部792表示在具有相同長度之兩個位元行間進行排他性邏輯和(XOR)處理之運算部。

圖25之步驟S602中之單元鍵生成鍵Ke之生成處理(AES_GD)具體而言如圖26(a)所示，將儲存於資訊記錄媒體780之實際索引輸入AES解碼部791，應用共同鍵密碼方式之AES(高級加密標準)密碼十進制，並使用自MKB取得之媒體鍵Km予以解碼，進一步將AES解碼部791之輸出值與實際索引資料輸入排他性邏輯和部792，執行將執行排他邏輯和運算之結果值作為單元鍵生成鍵Ke之處理。

圖25之步驟S603中之控制鍵Kc之生成，及步驟S604中之內容散列鍵之生成，如圖26(b), (c)所示，亦藉由AES解碼部791及排他性邏輯和部792之運算來進行。如圖26(d)所示，單元鍵Ku之生成係執行將自資訊記錄媒體780取得之加密單元鍵eKh(Ku)應用內容散列鍵Kh，而於AES解碼部791中予以解碼之處理。圖26之步驟S607之區塊鍵Kb之生成，

如圖26(e)所示，係藉由AES解碼部793與排他性邏輯和部792之運算來進行。

另外，本實施例中係顯示應用AES密碼十進制，具有128位元之鍵長之鍵資料之生成例，不過十進制及鍵長並不限定於此等之例，亦可應用其他十進制及鍵長。

如此，適用於內容(CPS單元)之解碼處理之單元鍵，係利用各種資訊生成。依據明文資料執行散列值驗證時，進行按照參照圖25而說明之處理而選出之散列單元之解碼處理後，依據解碼資料算出散列值，進行散出散列值與儲存於內容散列表(CHT)之對照用散列值之比較。

[7.資訊處理裝置之構造例]

其次，參照圖27，說明進行具有上述內容管理單元(CPS單元)構造之主內容、子內容之記錄處理或重現處理之資訊處理裝置之構造例。

資訊處理裝置800具有：進行資訊記錄媒體891之驅動，並進行資料記錄重現訊號之輸入輸出之驅動器890，按照各種程式執行資料處理之CPU870，作為程式及參數等記憶區域之ROM860，記憶體880，輸入輸出數位訊號之輸入輸出I/F810，輸入輸出類比訊號，具有A/D、D/A轉換器841之輸入輸出I/F840，執行MPEG資料之編碼、解碼處理之MPEG編碼解碼器830，執行TS(傳送流)、PS(程式流)處理之TS、PS處理機構820及執行各種密碼處理之密碼處理機構850，匯流排801中連接有各區塊。

首先，說明資料記錄時之動作。進行記錄之資料假設係

數位訊號輸入與類比訊號輸入兩種情況。

為數位訊號時，將自數位訊號用輸入輸出I/F810輸入，依需要藉由加密處理機構850而實施適切之加密處理之資料保存於資訊記錄媒體891中。此外，轉換輸入之數位訊號之資料形式而保存時，係藉由MPEG編碼解碼器830、CPU870及TS、PS處理機構820轉換成保存用之資料形式，而後以加密處理機構850實施適切之加密處理後，保存於資訊記錄媒體891中。

為類比訊號時，對輸入輸出I/F840輸入之類比訊號藉由A/D轉換器841而成為數位訊號，並藉由MPEG編碼解碼器830轉換成記錄時使用之編碼解碼器。而後藉由TS、PS處理機構820轉換成記錄資料形式之AV多重化資料，將依需要藉由加密處理機構850實施適切之加密處理之資料保存於記錄媒體891中。

如進行包含藉由MPEG-TS資料構成之AV流資料之主內容之記錄時，主內容區分成內容管理單元(CPS單元)後，單元鍵之加密處理藉由密碼處理機構850加密，並經由驅動器890而記錄於記錄媒體891中。

子內容亦係區分成各資料群對應之內容管理單元(CPS單元)後，單元鍵之加密處理藉由密碼處理機構850加密，並經由驅動器890而記錄於記錄媒體891中。

其次，說明自資訊記錄媒體重現資料時之處理。如進行包含作為主內容之MPEG-TS資料之AV流資料之重現時，於驅動器890中識別自資訊記錄媒體891讀取之資料作為內容

管理單元時，係執行對應於內容管理單元之單元鍵之取得處理，並依據取得之單元鍵，以加密處理機構850解碼，並藉由TS(傳送流)、PS(程式流)處理機構820區分成視頻、聲頻及字幕等各資料。

於MPEG編碼解碼器830中解碼之數位資料藉由輸入輸出I/F840內之D/A轉換器841轉換成類比訊號後輸出。此外，進行數位輸出時，以加密處理機構850解碼之MPEG-TS資料係通過輸入輸出I/F810作為數位資料而輸出。此時之輸出，如對IEEE1394及乙太網電纜及無線LAN等之數位介面進行。另外，對應於網路連接功能時，輸入輸出I/F810具備網路連接之功能。此外，在重現裝置內，以輸出端機器可接收之形式轉換資料進行輸出時，將對於經TS、PS處理機構820分離之視頻、聲頻及字幕等，於MPEG編碼解碼器830中施加比率轉換及編碼解碼器轉換處理，再度以TS、PS處理機構820於MPEG-TS及MPEG-PS等中進行多重化之資料，自數位用輸入輸出I/F810輸出。此外，亦可使用CPU870轉換成MPEG以外之編碼解碼器及多重化檔，而自數位用輸入輸出I/F810輸出。

子內容時亦是作為內容管理單元來識別時，執行對應於內容管理單元之單元鍵之取得處理，並依據取得之單元鍵，以加密處理機構850解碼，執行重現處理。進行重現時需要之各內容管理單元(CPS單元)之鍵資訊，可自保管於記憶體880上之資料取得。另外，單元鍵未儲存於資訊記錄媒體中時，可藉由自網路連接伺服器進行指定之程序來取得。

如前述，內容管理單元(CPS單元)中搭配有1個單元鍵。統籌地執行內容重現之重現控制之重現應用程式，檢測內容管理單元(CPS單元)發生切換，並依切換執行適用之鍵之切換。未取得鍵時，執行提示促使鍵取得之訊息之處理。

資訊處理裝置中，經由裝置外部之網路而取得需要之資訊時，取得之資料保存於資訊處理裝置內部之記憶體880中。保存之資料包含：內容重現時需要之鍵資訊、配合內容重現時而重現用之字幕、聲音(Audio)資訊、靜止畫等之資料、內容管理資訊及對應於內容管理資訊之重現裝置之動作原則(Usage Rule)等。

另外，執行重現處理及記錄處理之程式預先保管於ROM860內，於程式之執行處理中，依需要使用記憶體880作為參數及資料之保管與工作區域。另外，圖27中係顯示可進行資料記錄、重現之裝置構造作說明，不過亦可構成僅具有重現功能之裝置及僅具有記錄功能之裝置，此等裝置中亦可適用本發明。

以上，係參照特定之實施例來詳細說明本發明。但是，熟悉本技術之業者瞭解在不脫離本發明要旨之範圍內，可進行該實施例之修正及代用。亦即，例示之形態係在揭示本發明，而不應作限定性解釋。為了判斷本發明之要旨，須參酌申請專利範圍項。

另外，說明書中說明之一連串處理，可藉由硬體或軟體或兩者之複合構造來執行。藉由軟體執行處理時，可將記錄處理順序之程式安裝於組裝有專用硬體之電腦內之記憶

體中來執行，或是在可執行各種處理之通用電腦中安裝程式來執行。

如程式可預先記錄於作為記錄媒體之硬碟及ROM(唯讀記憶體)中。或是可將程式暫時性或永久性儲存(記錄)於軟式磁碟、CD-ROM(唯讀記憶光碟)、MO(光磁)碟、DVD(多樣化數位光碟)、磁碟、半導體記憶體等可移式記錄媒體中。此種可移式記錄媒體可作為所謂密封軟體來提供。

另外，程式除自上述之可移式記錄媒體安裝於電腦之外，亦可自下載側無線傳送至電腦，或是經由LAN(區域網路)及網際網路等網路，以有線傳送至電腦，電腦可接收如此送達之程式，並安裝於內藏之硬碟等記錄媒體中。

另外，記載於說明書中之各種處理，除按照記載時間序列地執行之外，亦可依執行處理之裝置之處理能力或需要，並列地或個別地執行。此外，本說明書中所謂系統，係數個裝置之邏輯性集合構造，並不限定於各構成裝置在同一個框體內。

(產業上之利用可行性)

本發明之構造，由於係算出作為資訊記錄媒體之儲存內容之細分化資料而設定之各個散列單元之散列值，將算出散列值記錄於內容散列表，而與內容一起儲存於資訊記錄媒體中，於執行內容重現之資訊處理裝置中，依據自許多散列單元隨機選擇之1個以上之散列單元，執行散列值對照處理，因此，不論內容之資料量為何，可進行依據少資料量而設定之散列單元算出散列值，及對照處理之內容驗

證，無須提高執行內容重現之使用者機器之資料處理能力，且亦縮短內容重現前之驗證處理時間，而可進行有效之內容驗證。

再者，本發明之構造，由於係散列單元設定成執行內容重現之資訊處理裝置中之資料讀取單位之ECC區塊資料之資料長之整數倍，因此可藉由更少之資料讀取來實現散列單元之讀取，可進行處理效率高之資料驗證。

【圖式簡單說明】

圖1係資訊記錄媒體之儲存資料構造之說明圖。

圖2(A)-(D)係對資訊記錄媒體之儲存內容而設定之內容管理單元之設定例之說明圖。

圖3係顯示內容管理單元構造及單元鍵管理表範例之圖。

圖4(a), (b)係資訊記錄媒體之資料記錄構造之說明圖，且係實際層中之ECC區塊與剪輯AV流之對應之說明圖。

圖5(b)~(e)係資訊記錄媒體之資料記錄構造之說明圖，且係實際層中之剪輯AV流、邏輯層中之剪輯AV流及散列單元之對應之說明圖。

圖6(f)~(h)係資訊記錄媒體之資料記錄構造及加密處理構造之說明圖。

圖7(i)~(h)係資訊記錄媒體之儲存內容之加密處理構造之說明圖。

圖8(a), (m), (n)係資訊記錄媒體之資料記錄構造之說明圖，且係散列單元與校正單元(aligned Unit)對應之說明圖。

圖9(P2), (L1), (P1)係資訊記錄媒體之資料記錄構造之說

明圖，且係實際層及邏輯層中之校正單元對應之說明圖。

圖10係內容散列表之構造例之說明圖。

圖11(A), (B)係內容散列表之具體構造例之說明圖。

圖12(A), (B)係剪輯對應之內容散列表之構造例之說明圖。

圖13係資訊記錄媒體之製造步驟中之管理中心、內容編輯實體及資訊記錄媒體製造實體之處理概要之說明圖。

圖14係管理中心、內容編輯實體及資訊記錄媒體製造實體執行之處理例之說明圖。

圖15係說明作為儲存於資訊記錄媒體之資料而生成之光碟影像之生成處理步驟之流程圖。

圖16係儲存於資訊記錄媒體之內容加密處理時應用之輔助檔之資料之說明圖。

圖17係顯示儲存於資訊記錄媒體之內容加密處理時應用之輔助檔之語法圖。

圖18係內容證明書之資料構造之說明圖。

圖19係內容儲存資訊記錄媒體之製造中，管理中心、內容編輯實體及資訊記錄媒體製造實體執行之處理例之說明圖。

圖20係內容儲存資訊記錄媒體之製造中，管理中心、內容編輯實體及資訊記錄媒體製造實體執行之處理例之說明圖。

圖21係內容儲存資訊記錄媒體之製造中，管理中心、內容編輯實體及資訊記錄媒體製造實體執行之處理例之說明

圖。

圖22係依據執行內容重現之資訊處理裝置中之散列值之內容驗證處理順序之說明圖。

圖23係依據執行內容重現之資訊處理裝置中之散列值之內容驗證處理順序之說明圖。

圖24係應用依據執行內容重現之資訊處理裝置中之明文資料之散列值之內容驗證處理順序之說明圖。

圖25係資訊處理裝置中之內容重現中之密碼處理順序之說明圖。

圖26(a)~(e)係資訊處理裝置中之內容重現中適用之鍵生成等之密碼處理之詳細說明圖。

圖27係安裝資訊記錄媒體執行資訊之記錄重現之資訊處理裝置構造例之說明圖。

【主要元件符號說明】

100，600，622，780，891	資訊記錄媒體
101	資料儲存區域
102	引入區域
111	加密內容
112	記錄種
113，783	CCI
114，784	內容散列
115，555，603	內容證明書
116，312，514，556，604	公開鍵證明書
120	密碼鍵資訊

121	媒體鍵區塊
131，782	實際索引
210，211，212，213	標題
220	電影物件
221，222，224	重現程式
230，231，232，233	播放表
240，241，242，243	剪輯
261，262，263	AV流資料檔
301	CPS單元1
302	CPS單元2
303	編輯前內容
310，510	管理中心
311	媒體鍵區塊
313	媒體鍵Km
330，530	內容編輯實體
350，553	資訊記錄媒體製造實體
400，621，800	資訊處理裝置
512，554	機密鍵
513	公開鍵
531	輔助檔
532	明文內容
551	應用單元鍵
552，601	加密內容
602，623	內容散列表

776	裝置鍵
777	解碼內容
781	MKB
785	加密單元鍵
791	AES解碼部
792	排他性邏輯和部
793	AES加密部
801	匯流排
810，840	輸出I/F
820	TS、PS處理機構
830	MPEG編碼解碼器
841	A/D、D/A轉換器
850	密碼處理機構
860	ROM
870	CPU
880	記憶體
890	驅動器

五、中文發明摘要：

本發明提供實現依據散列值之內容驗證處理效率化之構造。將作為資訊記錄媒體之儲存內容之細分化資料而設定之各個散列單元之散列值記錄於內容散列表，而與內容一起儲存於資訊記錄媒體中。執行內容重現之資訊處理裝置依據隨機選擇之1個以上之散列單元，執行散列值對照處理。藉由本構造，不論內容之資料量為何，可依據少資料量之散列單元算出散列值，進行對照處理，並可進行執行內容重現之使用者機器中之有效之內容驗證。

六、英文發明摘要：

十一、圖式：

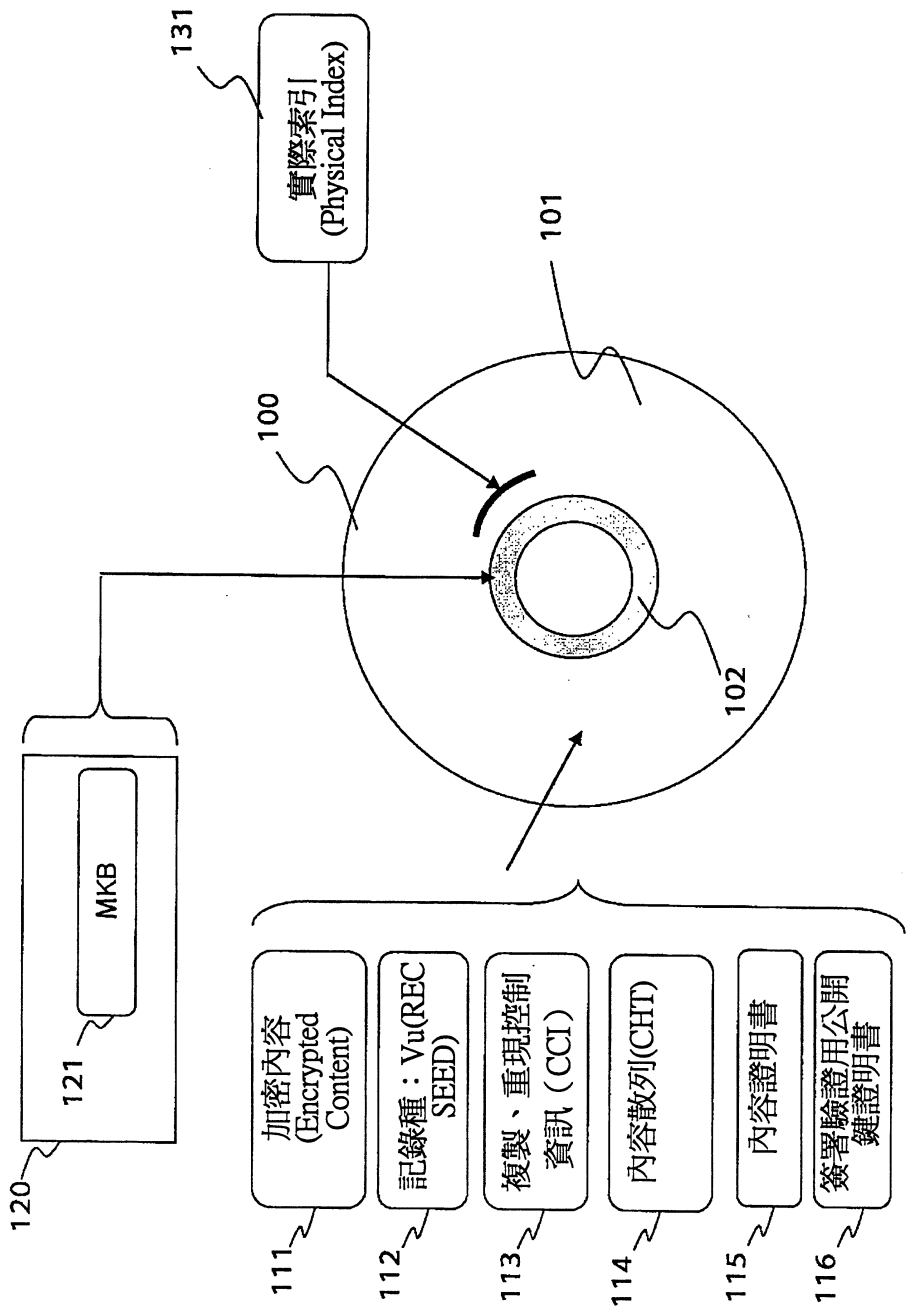
131
實際索引
(Physical Index)
101
100
102
120
121
MKB
111
加密內容
(Encrypted
Content)
112
記錄種：Vu(REC
SEED)
113
複製、重現控制
資訊（CCI）
114
內容散列(CHT)
115
內容證明書
116
簽署驗證用公開
鍵證明書

圖 1

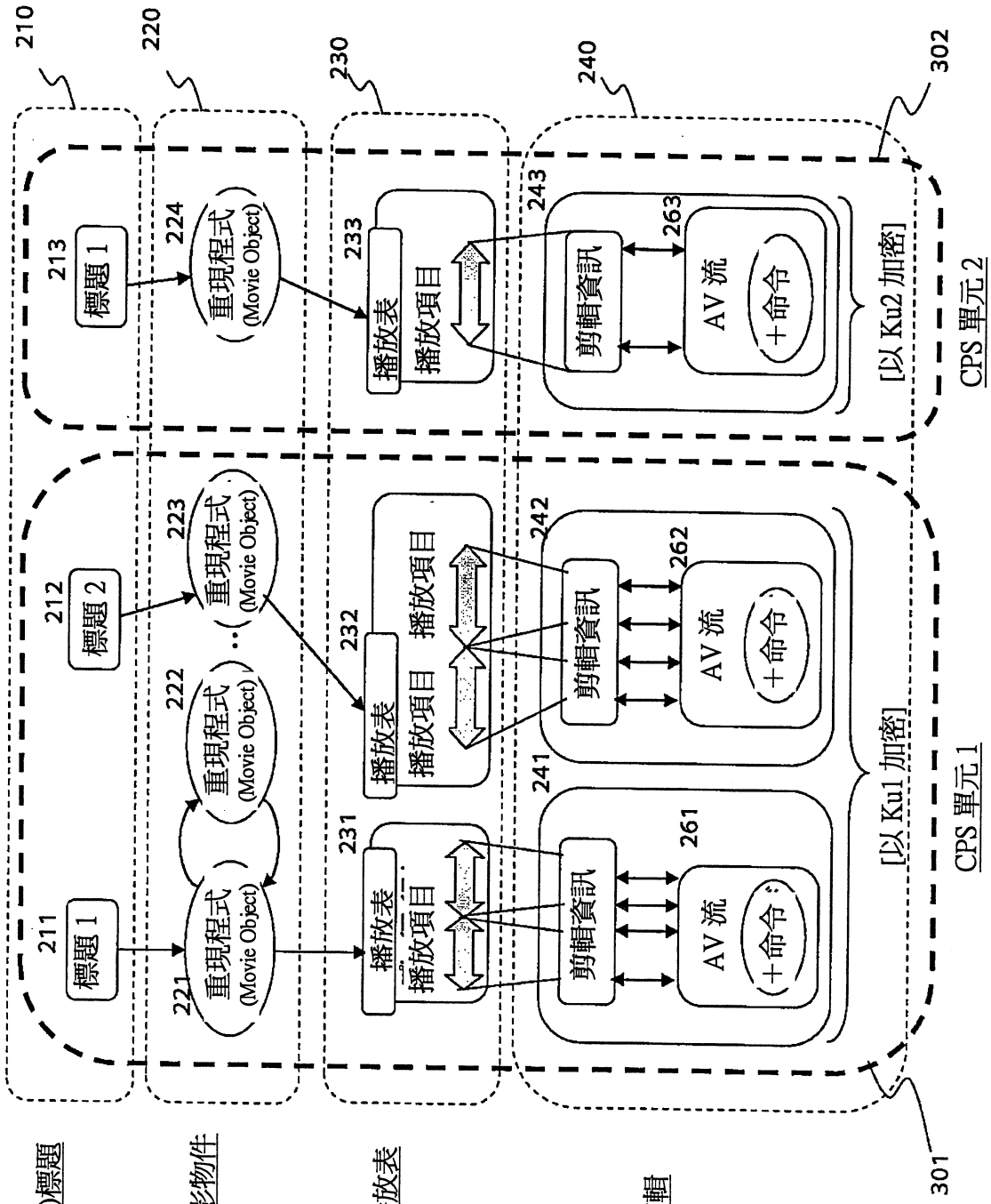
(A)標題
(B)電影物件
(C)播放表
(D)剪輯
210
220
230
240
211
標題 1
212
標題 2
213
標題 1
221
重現程式 (Movie Object)
222
重現程式 (Movie Object)
223
重現程式 (Movie Object)
224
重現程式 (Movie Object)
231
播放表
播放項目
232
播放表
播放項目 播放項目
233
播放表
播放項目
241
剪輯資訊
261
AV 流
(+命令)
242
剪輯資訊
262
AV 流
(+命令)
243
剪輯資訊
263
AV 流
(+命令)
[以 Ku1 加密]
CPS 單元 1
[以 Ku2 加密]
CPS 單元 2
301
302

圖 2

標題等在應用層中可區別之索引	內容管理單元(CPS)	單元鍵(CPS)
標題 1	CPS1	Ku1
標題 2	CPS1	Ku1
應用 1	CPS2	Ku2
應用 2	CPS3	Ku3
⋮	⋮	⋮
資料群 1	CPS4	Ku4
資料群 2	CPS5	Ku5
⋮	⋮	⋮

圖 3

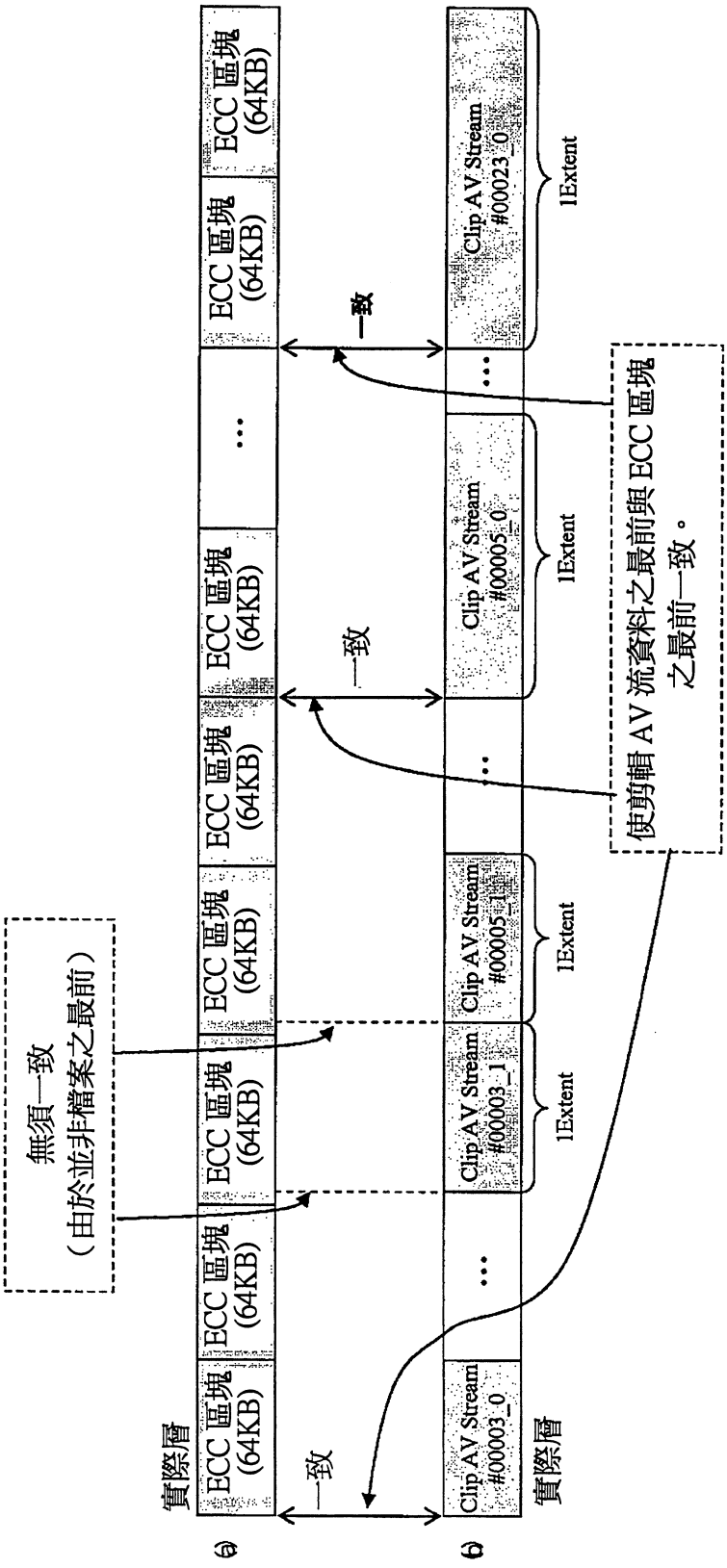
無須一致
（由於並非檔案之最前）
實際層
ECC 區塊 (64KB)
Clip AV Stream #00003_0
Clip AV Stream #00003_1
Clip AV Stream #00005_0
Clip AV Stream #00023_0
1Extent
一致
使剪輯 AV 流資料之最前與 ECC 區塊之最前一致。
(a)
(b)

圖 4

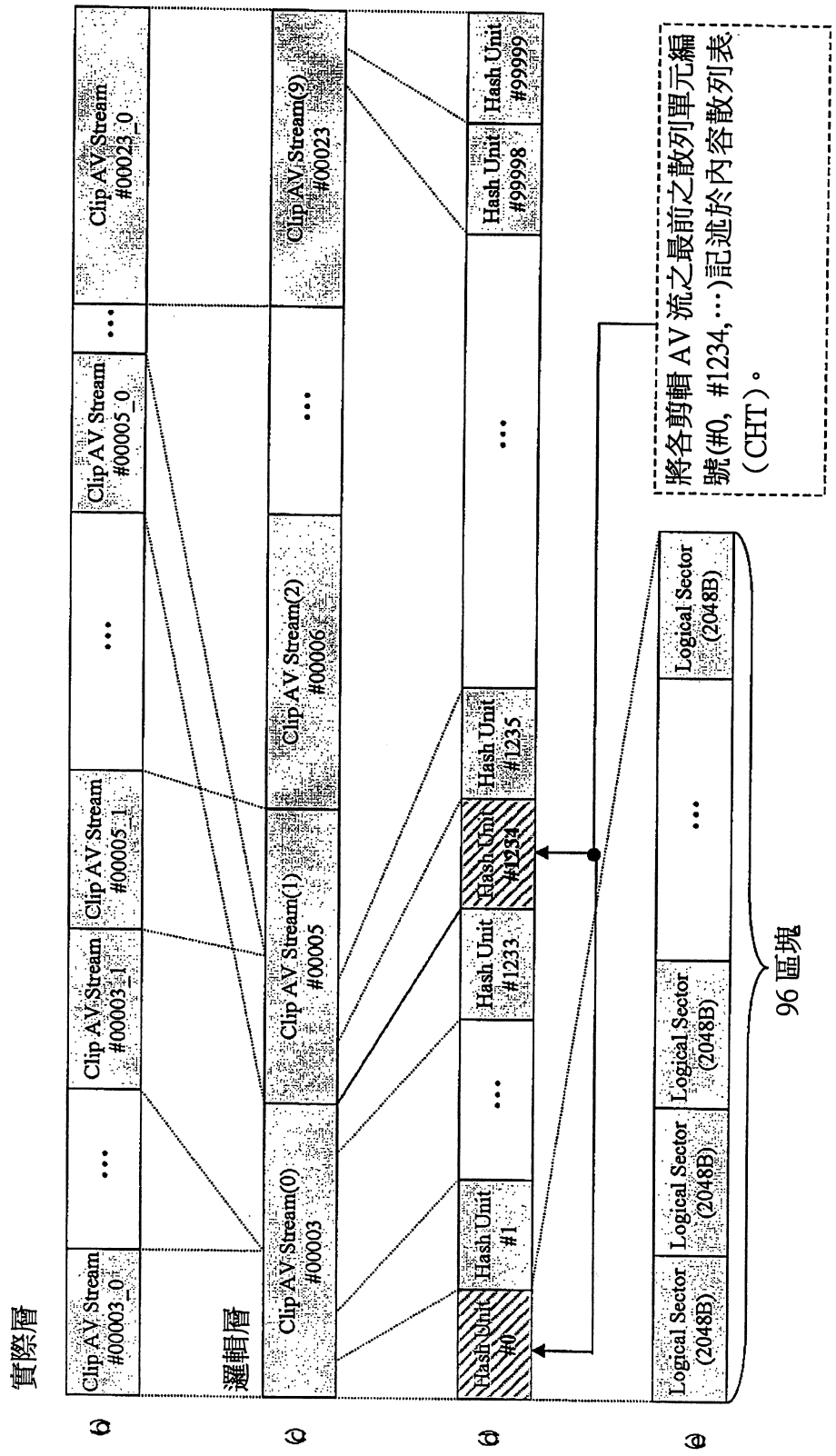
實際層
邏輯層
Clip AV Stream #00003_0
Clip AV Stream #00003_1
Clip AV Stream #00005_1
Clip AV Stream #00005_0
Clip AV Stream #00023_0
Clip AV Stream(0) #00003
Clip AV Stream(1) #00005
Clip AV Stream(2) #00006
Clip AV Stream(9) #00023
Hash Unit #0
Hash Unit #1
Hash Unit #1233
Hash Unit #1234
Hash Unit #1235
Hash Unit #99998
Hash Unit #99999
Logical Sector (2048B)
96 區塊
將各剪輯 AV 流之最前之散列單元編號(#0, #1234, …)記述於內容散列表（CHT）。
a
b
c
d
e

圖 5

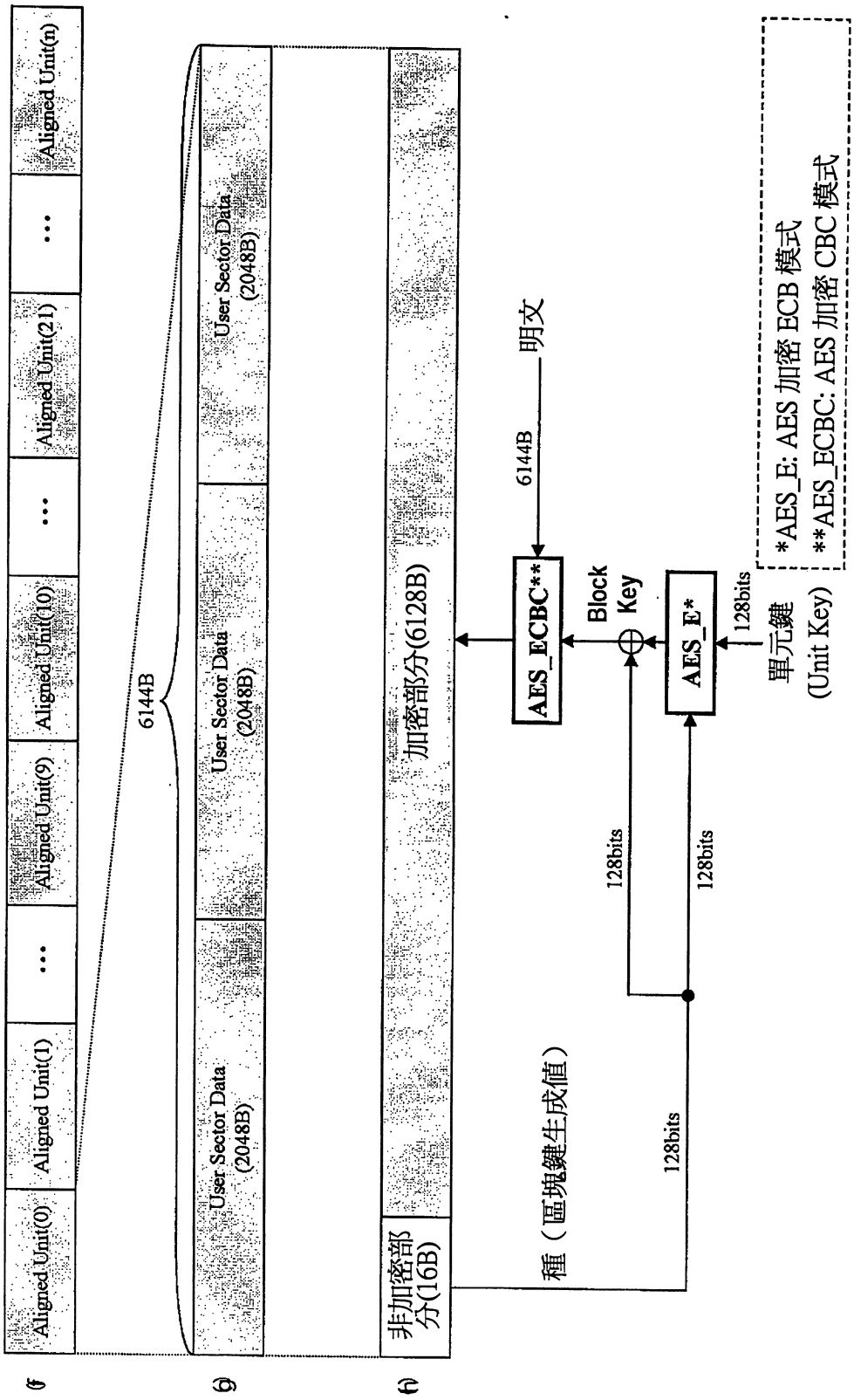
Aligned Unit(0)
Aligned Unit(1)
...
Aligned Unit(9)
Aligned Unit(10)
...
Aligned Unit(21)
...
Aligned Unit(n)
6144B
User Sector Data (2048B)
User Sector Data (2048B)
User Sector Data (2048B)
非加密部分(16B)
加密部分(6128B)
種（區塊鍵生成值）
128bits
128bits
128bits
AES_ECBC**
AES_E*
Block Key
6144B
明文
128bits
單元鍵
(Unit Key)
*AES_E: AES 加密 ECB 模式
**AES_ECBC: AES 加密 CBC 模式

圖 6

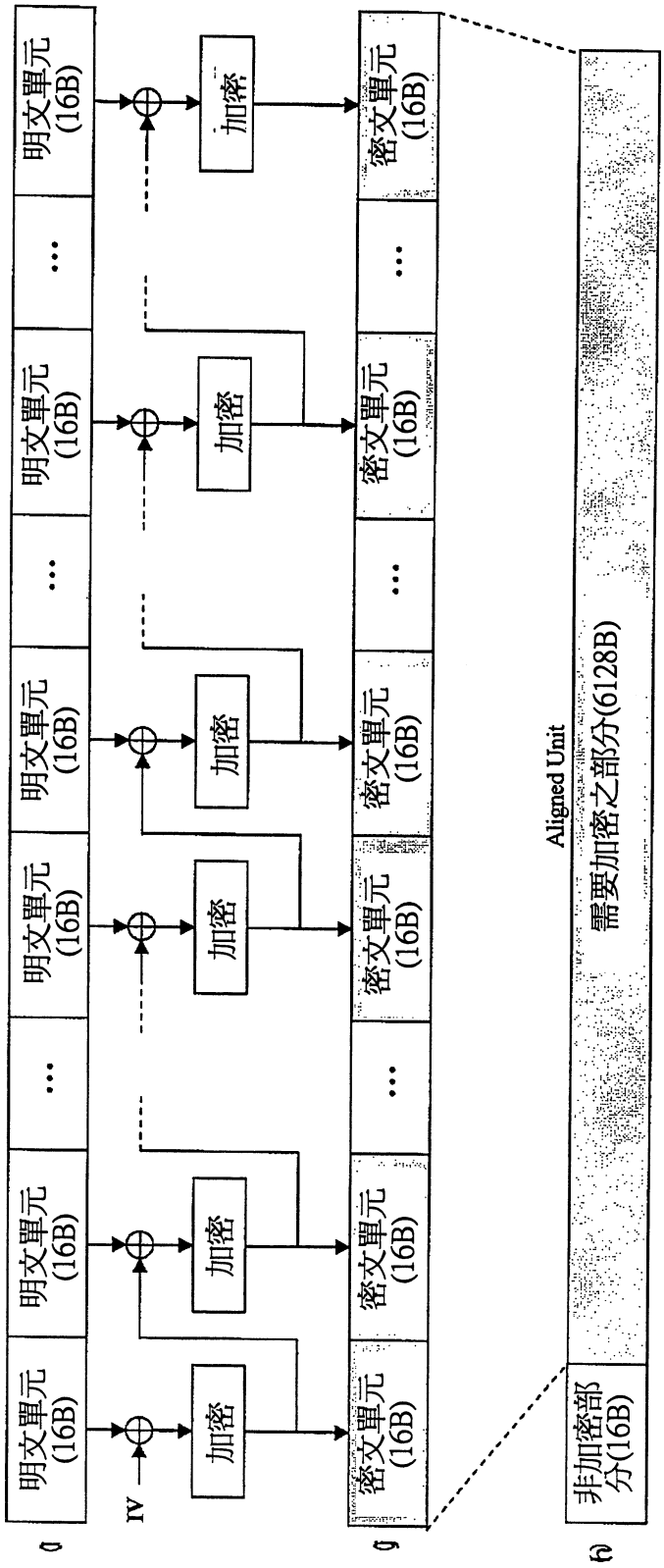

圖 7

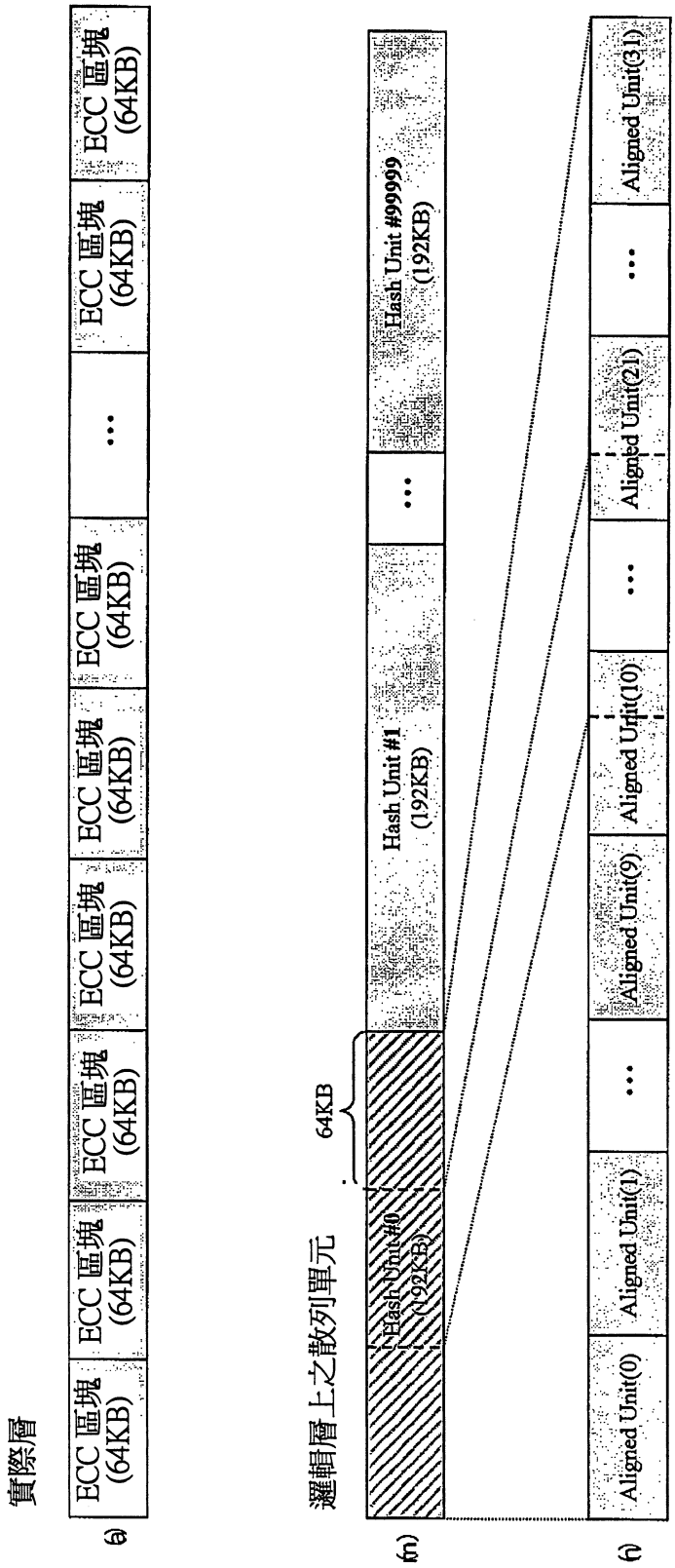
實際層
ECC 區塊 (64KB)
ECC 區塊 (64KB)
ECC 區塊 (64KB)
ECC 區塊 (64KB)
ECC 區塊 (64KB)
...
ECC 區塊 (64KB)
ECC 區塊 (64KB)
(a)
邏輯層上之散列單元
64KB
Hash Unit #0 (192KB)
Hash Unit #1 (192KB)
...
Hash Unit #99999 (192KB)
(b)
Aligned Unit(0)
Aligned Unit(1)
...
Aligned Unit(9)
Aligned Unit(10)
...
Aligned Unit(21)
...
Aligned Unit(31)
(c)

圖 8

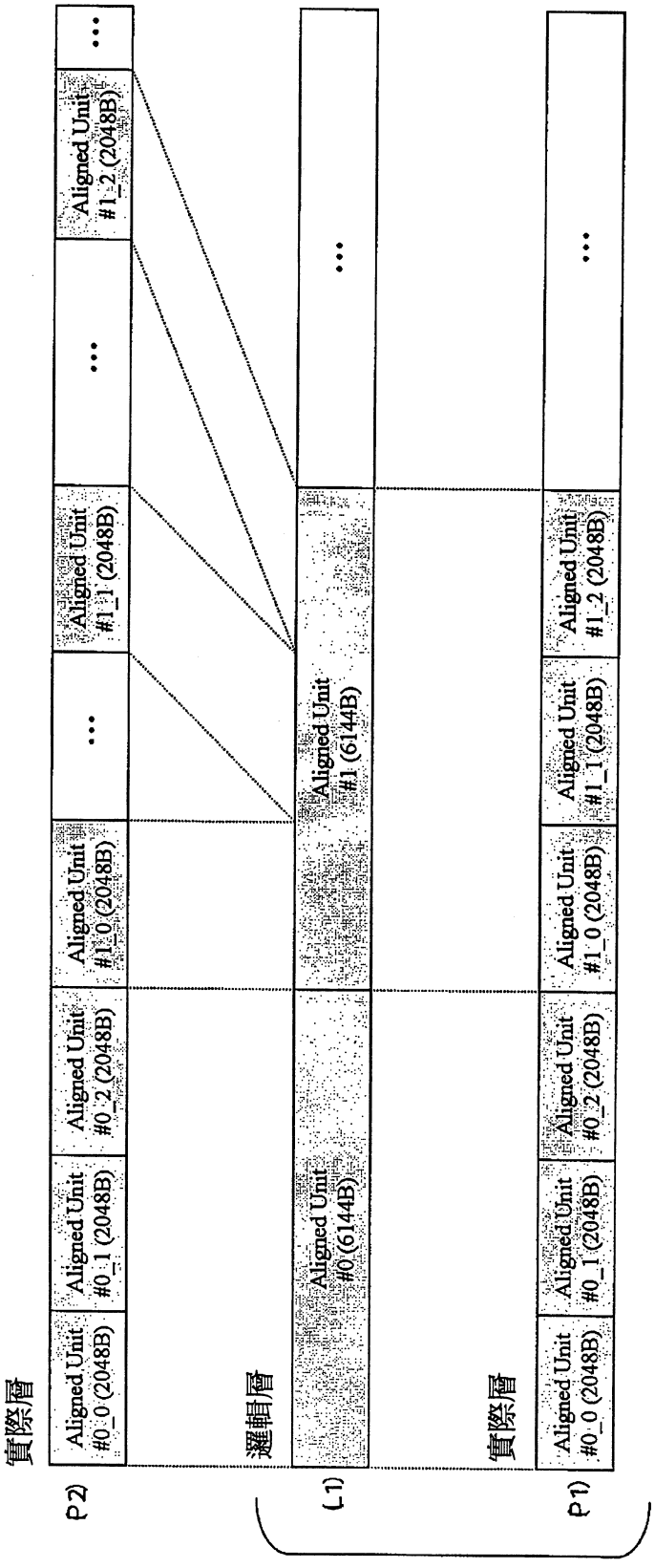
實際層
Aligned Unit #0_0 (2048B)
Aligned Unit #0_1 (2048B)
Aligned Unit #0_2 (2048B)
Aligned Unit #1_0 (2048B)
...
Aligned Unit #1_1 (2048B)
...
Aligned Unit #1_2 (2048B)
...
P2)
邏輯層
Aligned Unit #0 (6144B)
Aligned Unit #1 (6144B)
...
L1)
實際層
Aligned Unit #0_0 (2048B)
Aligned Unit #0_1 (2048B)
Aligned Unit #0_2 (2048B)
Aligned Unit #1_0 (2048B)
Aligned Unit #1_1 (2048B)
Aligned Unit #1_2 (2048B)
...
P1)

圖 9

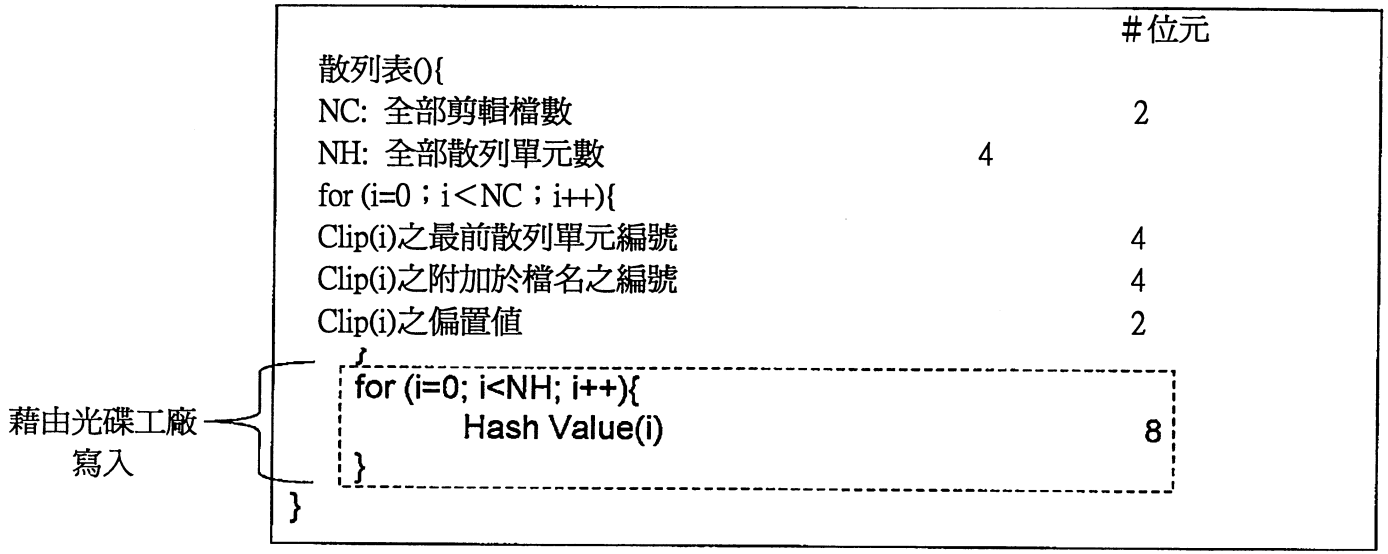
#位元
散列表(){
NC: 全部剪輯檔數 2
NH: 全部散列單元數 4
for (i=0；i＜NC；i++){
Clip(i)之最前散列單元編號 4
Clip(i)之附加於檔名之編號 4
Clip(i)之偏置值 2
}
for (i=0; i<NH; i++){
Hash Value(i) 8
}
}
藉由光碟工廠
寫入

圖 10

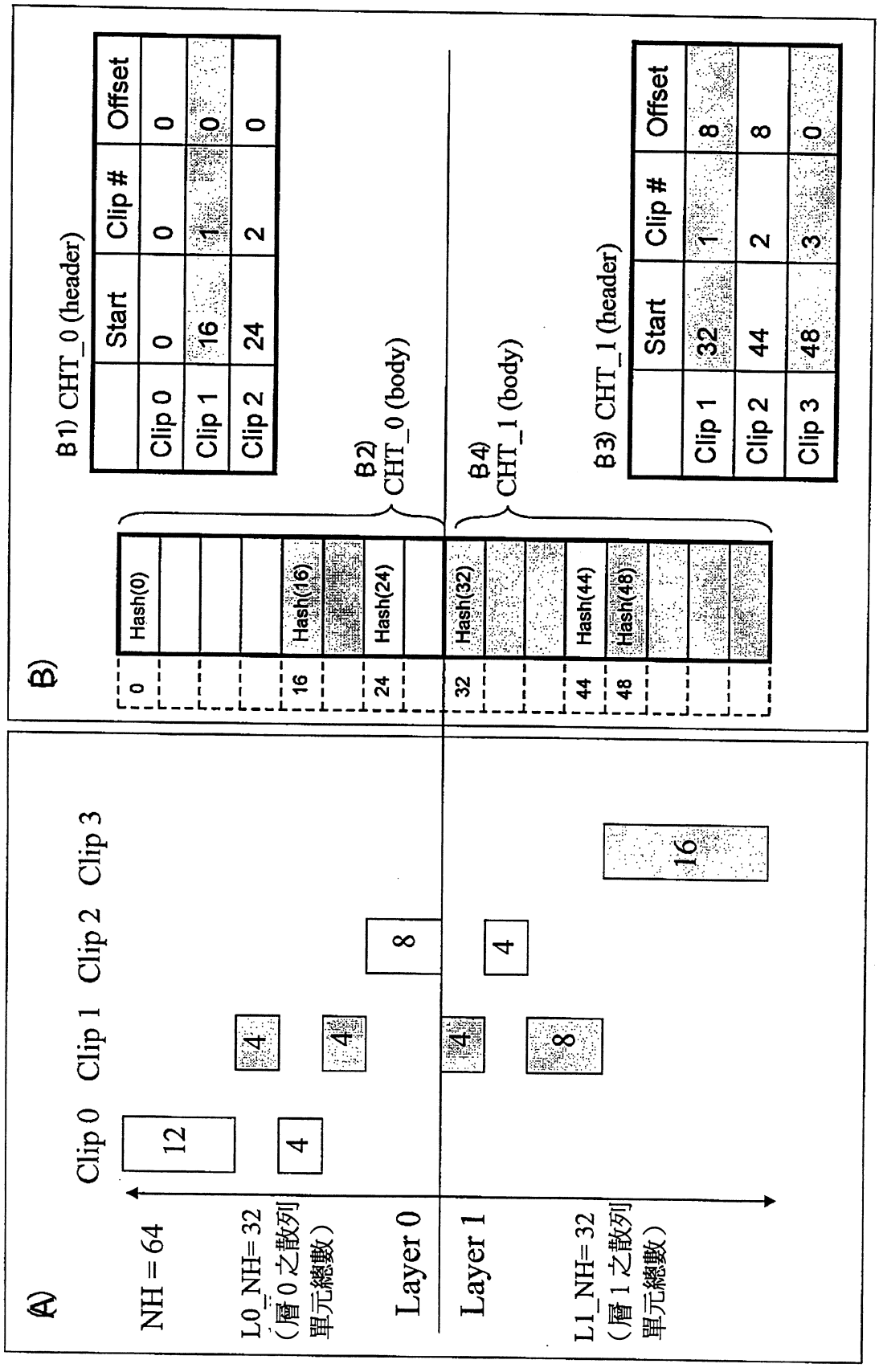
A)
Clip 0
Clip 1
Clip 2
Clip 3
NH = 64
12
4
4
8
4
8
16
Layer 0
Layer 1
L0_NH= 32
（層 0 之散列
單元總數）
L1_NH= 32
（層 1 之散列
單元總數）
B)
B1) CHT_0 (header)
Start
Clip #
Offset
Clip 0
0
0
0
Clip 1
16
1
0
Clip 2
24
2
0
B2)
CHT_0 (body)
B4)
CHT_1 (body)
B3) CHT_1 (header)
Start
Clip #
Offset
Clip 1
32
1
8
Clip 2
44
2
8
Clip 3
48
3
0
Hash(0)
Hash(16)
Hash(24)
Hash(32)
Hash(44)
Hash(48)
0
16
24
32
44
48

圖 11

(A)

	#位元
Clip(n)之散列表	
NH: Clip(n)中之全部散列單元數	4
Clip(n)所屬之 CPS 單元編號	2
for (i=0; i<NH; i++){	
Hash Value(i)	8
}	
}	

(B)

	#位元
相關連表（）{	
NC：全部剪輯檔數	2
NH：全部散列單元數	4
for（i=0；i＜NC；i++）{	
Clip(i)之最前之散列單元編號	4
Clip(i)之附加於檔名之編號	4
}	
}	

圖 12

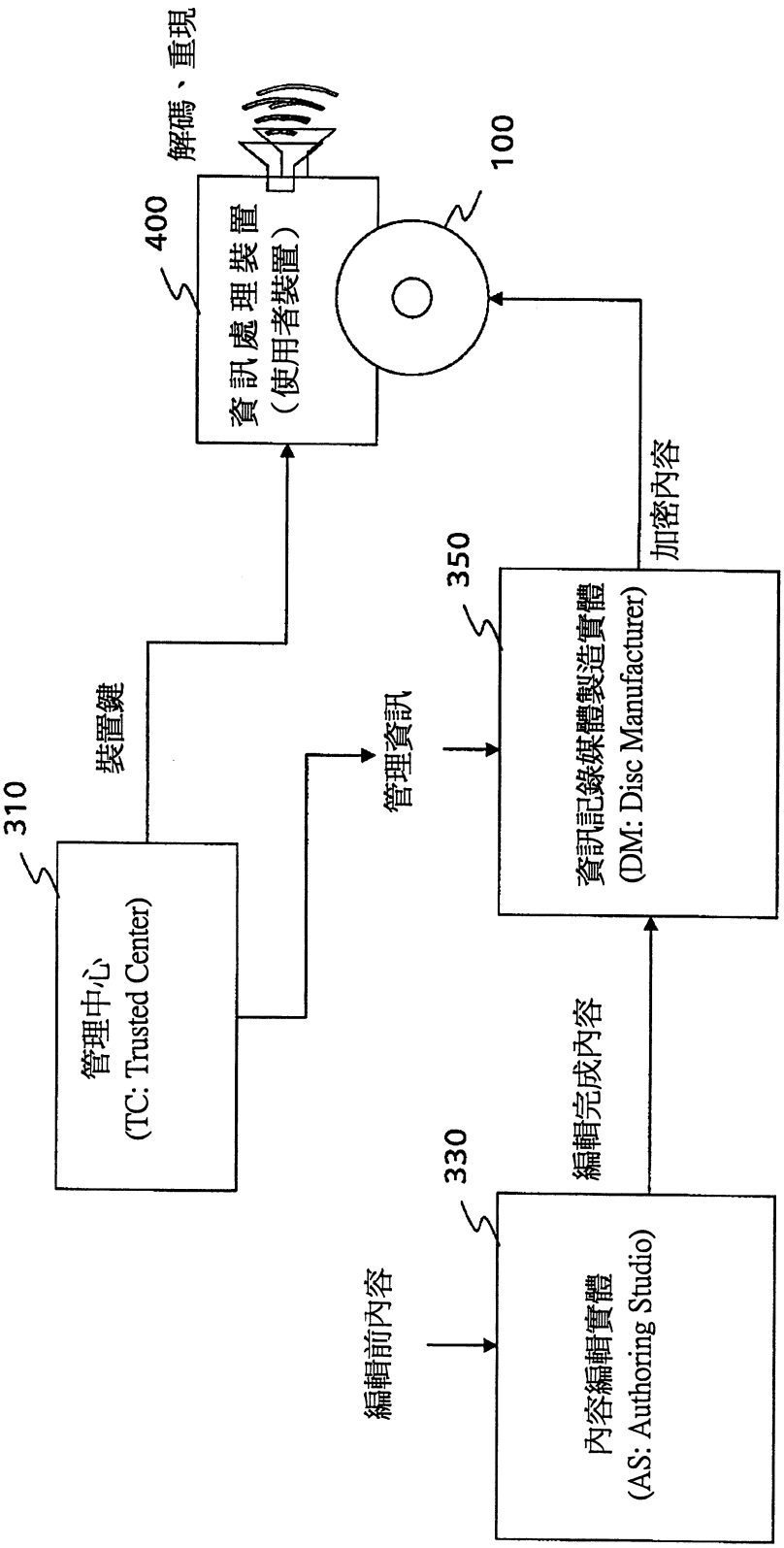
管理中心
(TC: Trusted Center)
310
裝置鍵
管理資訊
資訊記錄媒體製造實體
(DM: Disc Manufacturer)
350
加密內容
資訊處理裝置
（使用者裝置）
400
解碼、重現
100
內容編輯實體
(AS: Authoring Studio)
330
編輯前內容
編輯完成內容

圖 13

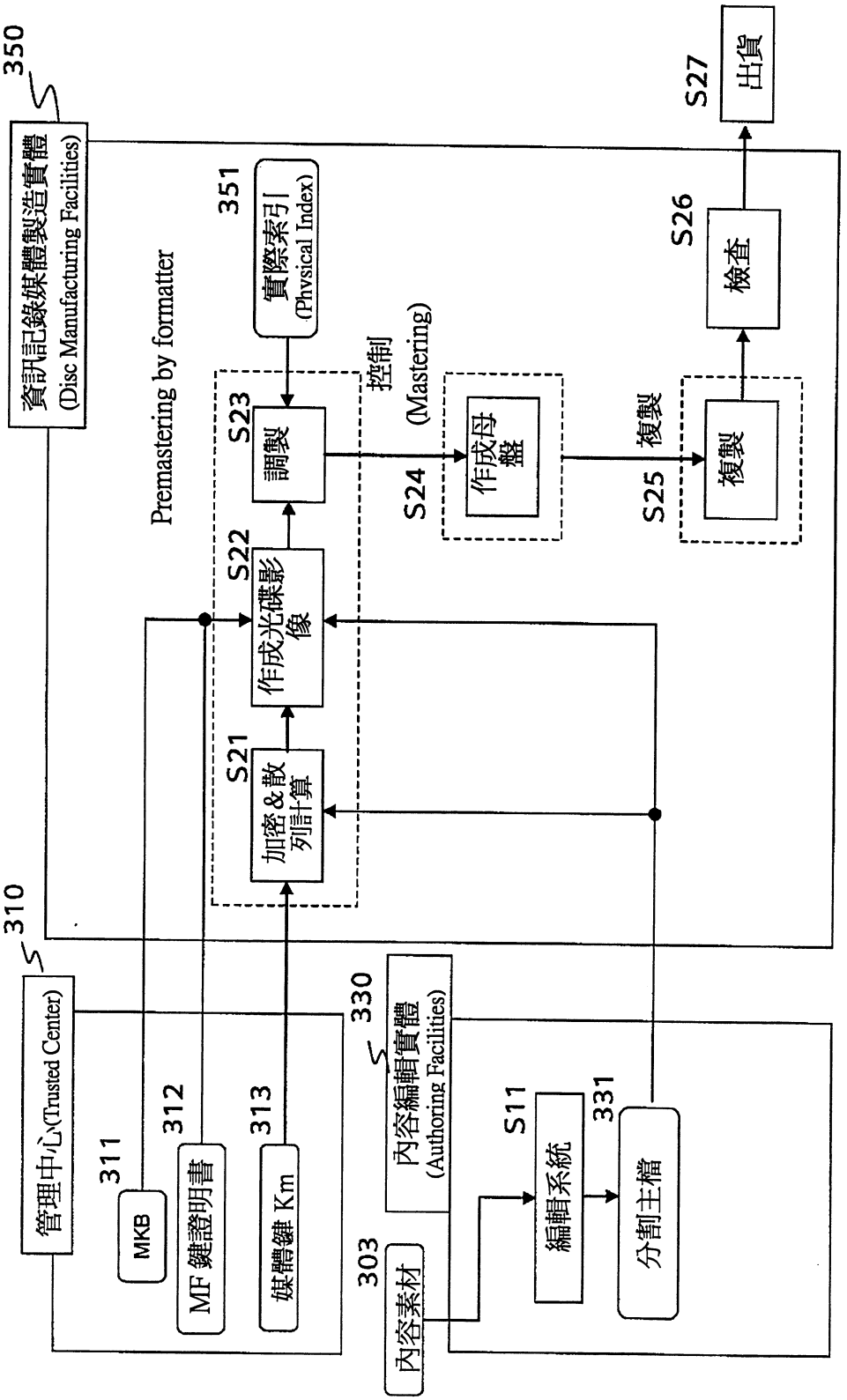
350
資訊記錄媒體製造實體
(Disc Manufacturing Facilities)
S27
出貨
S26
檢查
351
實際索引
(Physical Index)
Premastering by formatter
S23
調製
控制
(Mastering)
S22
作成光碟影像
S24
作成母盤
S25
複製
複製
S21
加密&散列計算
310
管理中心(Trusted Center)
330
內容編輯實體
(Authoring Facilities)
311
MKB
312
MF 鍵證明書
313
媒體鍵 Km
S11
編輯系統
331
分割主檔
303
內容素材

圖 14

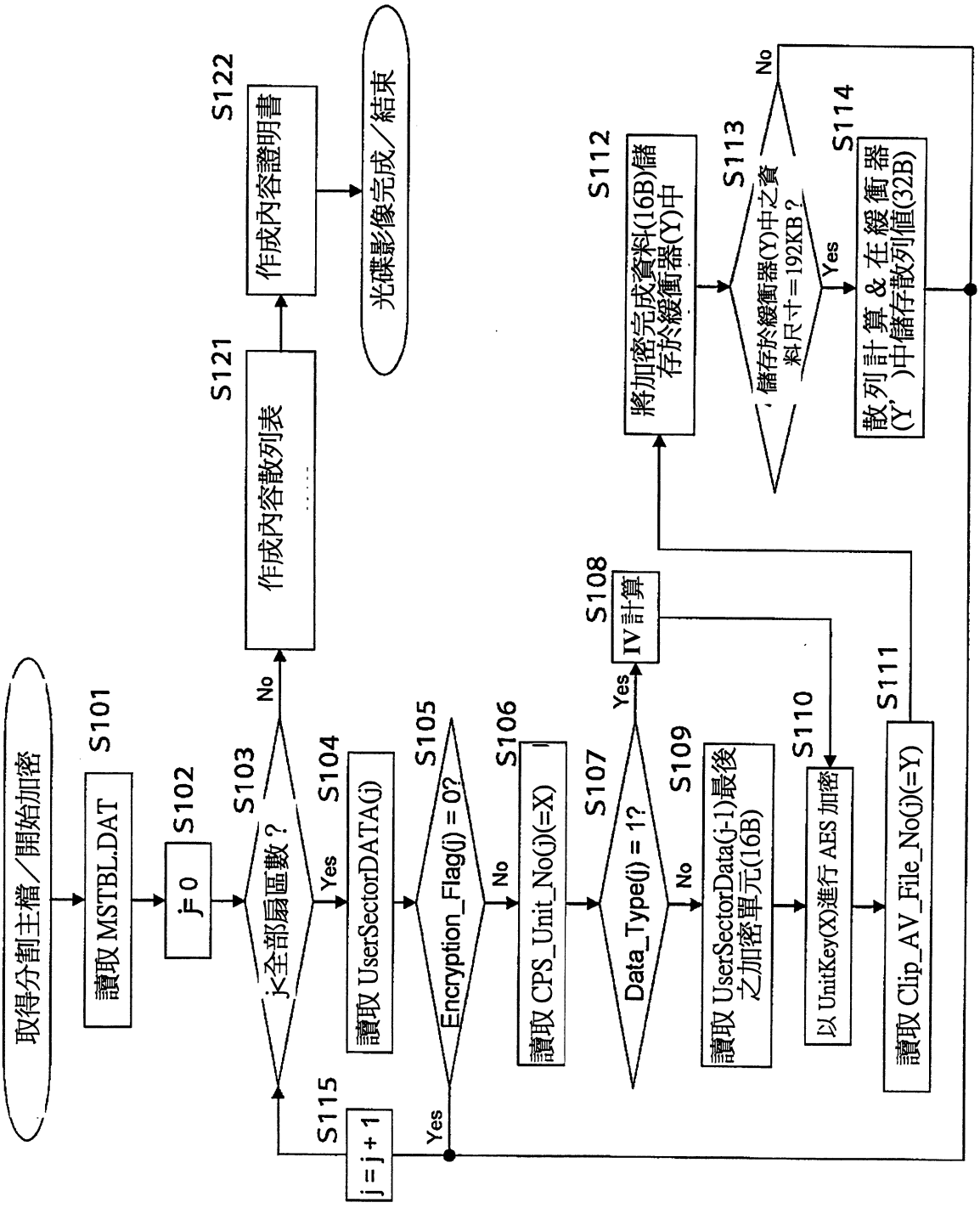
取得分割主檔／開始加密
S101
讀取 MSTBL.DAT
S102
j= 0
S103
j<全部扇區數？
No
S121
作成內容散列表
S122
作成內容證明書
光碟影像完成／結束
Yes
S104
讀取 UserSectorDATA(j)
S105
Encryption_Flag(j) = 0?
No
S106
讀取 CPS_Unit_No(j)(=X)
S107
Data_Type(j) = 1?
Yes
S108
IV計算
No
S109
讀取 UserSectorData(j-1)最後之加密單元(16B)
S110
以 UnitKey(X)進行 AES 加密
S111
讀取 Clip_AV_File_No(j)(=Y)
S112
將加密完成資料(16B)儲存於緩衝器(Y)中
S113
儲存於緩衝器(Y)中之資料尺寸=192KB？
No
Yes
S114
散列計算 & 在緩衝器(Y')中儲存散列值(32B)
S115
j = j + 1
Yes

圖 15

	#bits	value
Li_MSTBL.DAT( ){		
UD_START_Location	32	
UD_END_Location	32	
CHT_Location	32	
CHT_Offset	32	
Content_Cert_Location	32	
Content_Cert_Offset	32	
UK_Inf_Location	32	
UK_Inf_Offset	32	
Num_of_UK	32	
MFK_Cert_Location	32	
MKB_Location	32	
For (j = 1; j =<N, j++) {		
Encryption_Flag(j)	8	00_{16} : not to-be-encrypted 01_{16} : to-be-encrypted
Data_Type(j)	8	01_{16} : 1st sector of AU 02_{16} : 2nd sector of AU 03_{16} : 3rd sector of AU
CPS_Unit_No(j)	16	0000_{16}-$FFFF_{16}$
Clip_AV_File_No(j)	24	00000-99999
Reserved	6	000000_2
Last_Sector_of_Clip(j)	1	0_2 : not Last Sector of each Clip 1_2 : Last Sector of each Clip
Last_Sector_of_Layer(j)	1	0_2 : not Last Sector of each Clip in layer i 1_2 : Last Sector of each Clip in each layer i
}		
}		

圖 16

UD_START_Location：各層之使用者資料（資料區）之開始點之實際扇區編號(Physical Sector Number)。
UD_END_Location：各層之使用者資料（資料區）之結束點之實際扇區編號。
CHT_Location：CHT 之開始點之實際扇區編號。
CHT_Offset：CHT 之開始點與散列值（控制設施放入資料）之前之位元數。
Content_Cert_Location：內容證明書開始點之實際扇區編號。
Content_Cert_Offset：內容證明書開始點與內容 ID（控制設施放入資料）之前之位元數。
UK_Inf_Location：Unit_Key.inf(參照 P.2)之開始點之實際扇區編號。於其層中未記錄 Unit_Key.inf 時，記述 00000000_{16}。
UK_Inf_Offset：Unit_Key.inf 之開始點與 CPS Unit#1 之加密單元鍵之前之位元數。於其層中未記錄 Unit_Key.inf 時，記述 00000000_{16}。
Num_of_UK：光碟全體之單元鍵數（＝CPS 單元之數）。
MFK Cert=Location：MF Key Certificate 之開始點之實際扇區編號。尺寸固定。其層中未記錄 MFK_Cert 時，記述 00000000_{16}。
MKB_Location：MKB 之開始點之實際扇區編號。其層中未記錄 MKB_Cert 時，記述 00000000_{16}。
N：層 i 之邏輯扇區數。
Encryption_Flag：是否加密之旗標。
Data_Type：顯示扇區類型之旗標。
CPS_Unit_No：CPS 單元編號。
Clip_AV_File_No：剪輯檔編號。用於作成 CHT 之資訊。
Last_Sector_of_Clip：（無關於層）顯示各剪輯之最後扇區之旗標。
Last_Sector_of_Layer：顯示各層中之各剪輯之最後扇區之旗標。

圖 17

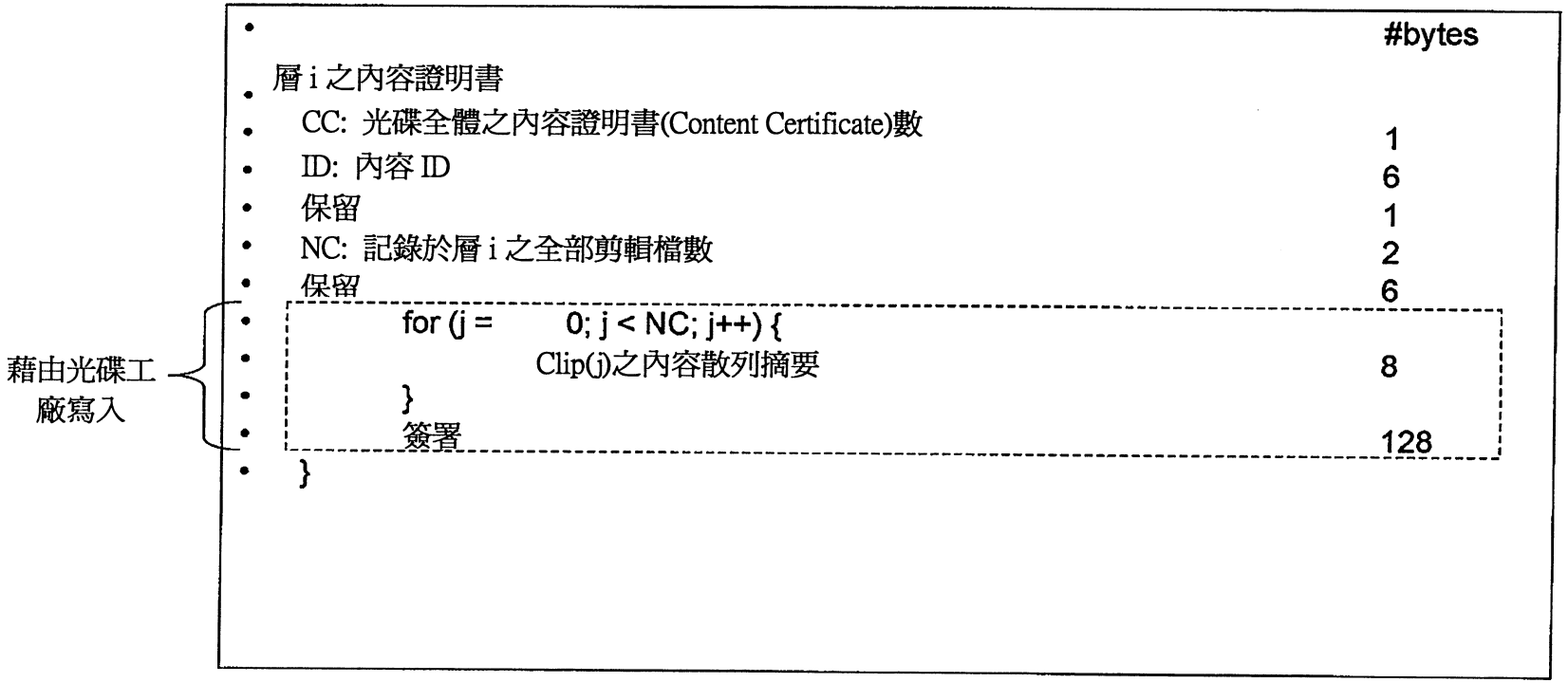
#bytes
層 i 之內容證明書
CC: 光碟全體之內容證明書(Content Certificate)數
1
ID: 內容 ID
6
保留
1
NC: 記錄於層 i 之全部剪輯檔數
2
保留
6
for (j = 0; j < NC; j++) {
Clip(j)之內容散列摘要
8
}
簽署
128
}
藉由光碟工廠寫入

圖 18

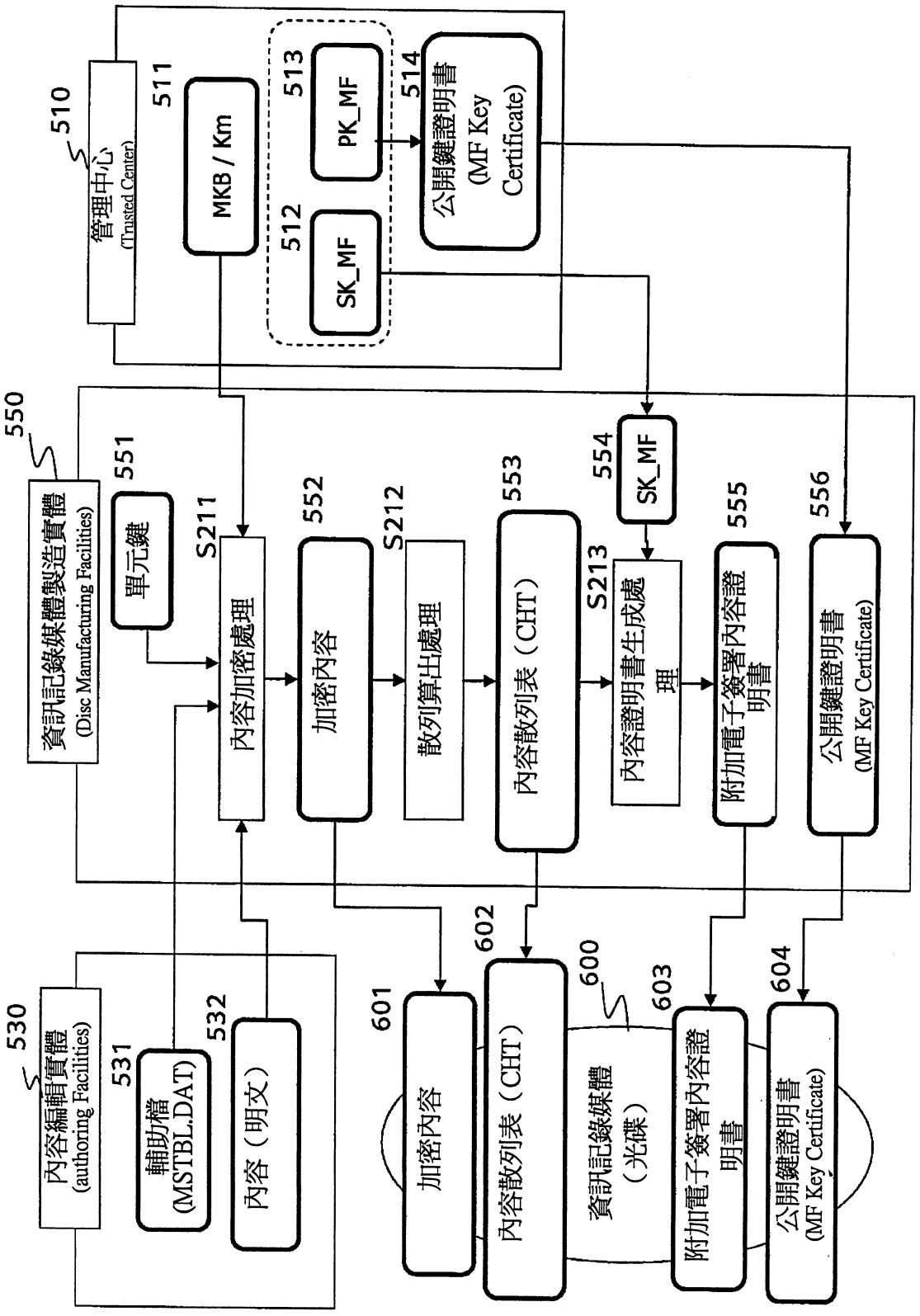
510
管理中心
(Trusted Center)
511
MKB / Km
513
PK_MF
514
公開鍵證明書
(MF Key
Certificate)
512
SK_MF
550
資訊記錄媒體製造實體
(Disc Manufacturing Facilities)
551
單元鍵
S211
內容加密處理
552
加密內容
S212
散列算出處理
553
內容散列表（CHT）
S213
554
SK_MF
內容證明書生成處
理
555
附加電子簽署內容證
明書
556
公開鍵證明書
(MF Key Certificate)
530
內容編輯實體
(authoring Facilities)
531
輔助檔
(MSTBL.DAT)
532
內容（明文）
601
加密內容
602
內容散列表（CHT）
600
資訊記錄媒體
（光碟）
603
附加電子簽署內容證
明書
604
公開鍵證明書
(MF Key Certificate)

圖 19

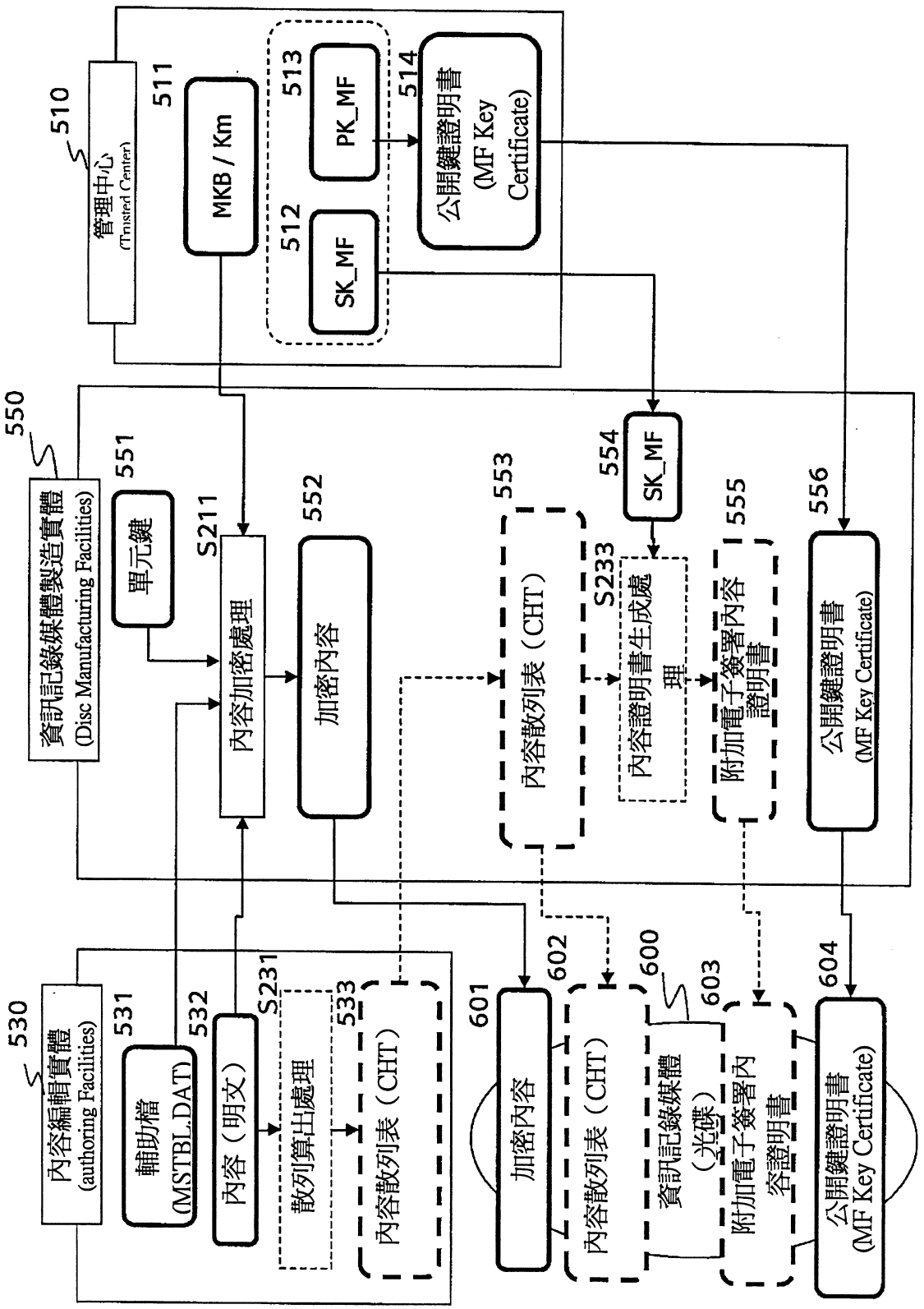
510
管理中心
(Trusted Center)
511
MKB / Km
512
SK_MF
513
PK_MF
514
公開鍵證明書
(MF Key Certificate)
550
資訊記錄媒體製造實體
(Disc Manufacturing Facilities)
551
單元鍵
S211
內容加密處理
552
加密內容
553
內容散列表（CHT）
554
SK_MF
S233
內容證明書生成處理
555
附加電子簽署內容證明書
556
公開鍵證明書
(MF Key Certificate)
530
內容編輯實體
(authoring Facilities)
531
輔助檔
(MSTBL.DAT)
532
內容（明文）
S231
散列算出處理
533
內容散列表（CHT）
601
加密內容
602
內容散列表（CHT）
600
資訊記錄媒體
（光碟）
603
附加電子簽署內容證明書
604
公開鍵證明書
(MF Key Certificate)

圖 20

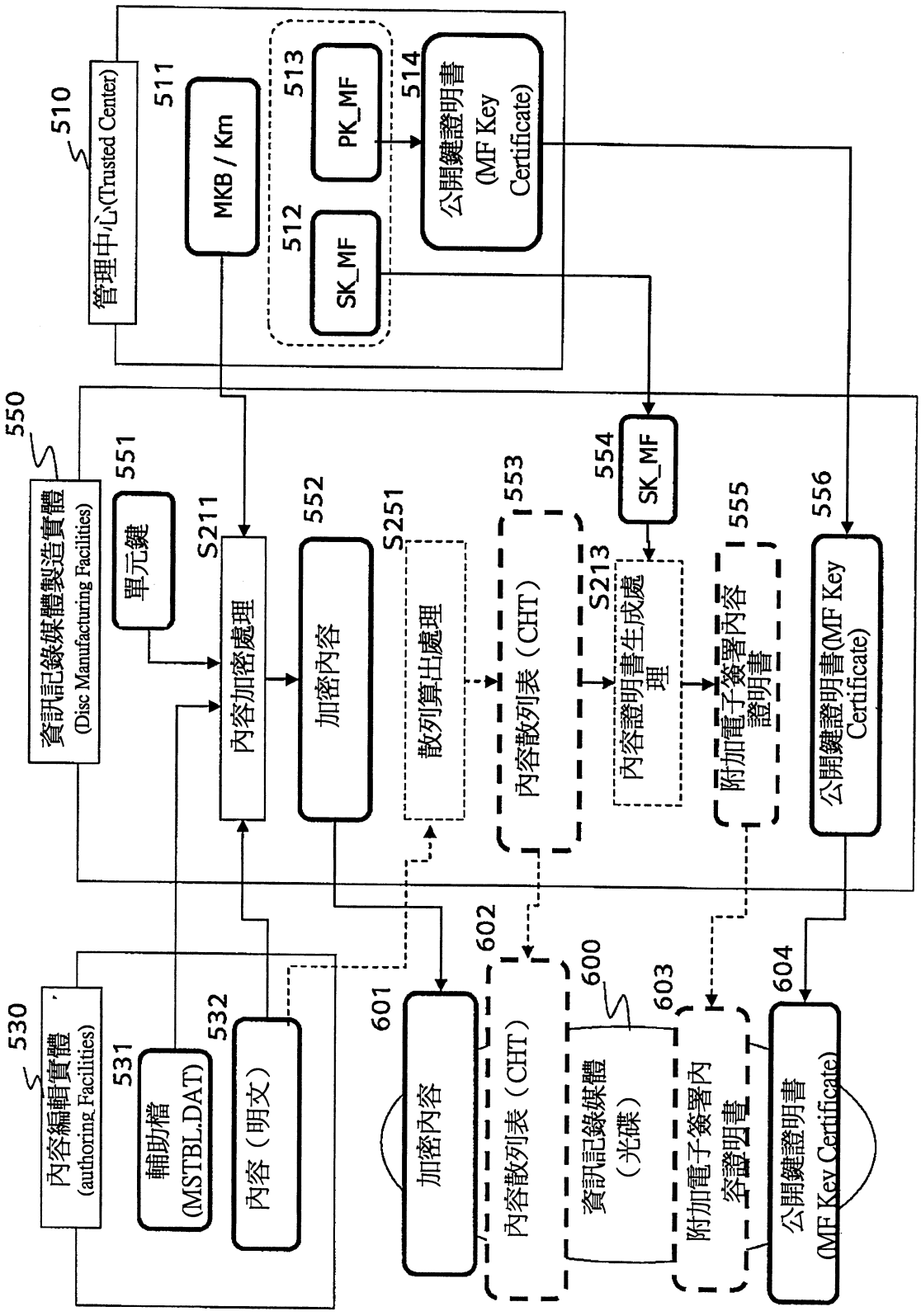
510
管理中心(Trusted Center)
511
MKB / Km
512
SK_MF
513
PK_MF
514
公開鍵證明書
(MF Key
Certificate)
550
資訊記錄媒體製造實體
(Disc Manufacturing Facilities)
551
單元鍵
S211
內容加密處理
552
加密內容
S251
散列算出處理
553
內容散列表（CHT）
554
SK_MF
S213
內容證明書生成處理
555
附加電子簽署內容
證明書
556
公開鍵證明書(MF Key
Certificate)
530
內容編輯實體
(authoring Facilities)
531
輔助檔
(MSTBL.DAT)
532
內容（明文）
601
加密內容
602
內容散列表（CHT）
600
資訊記錄媒體
（光碟）
603
附加電子簽署內
容證明書
604
公開鍵證明書
(MF Key Certificate)

圖 21

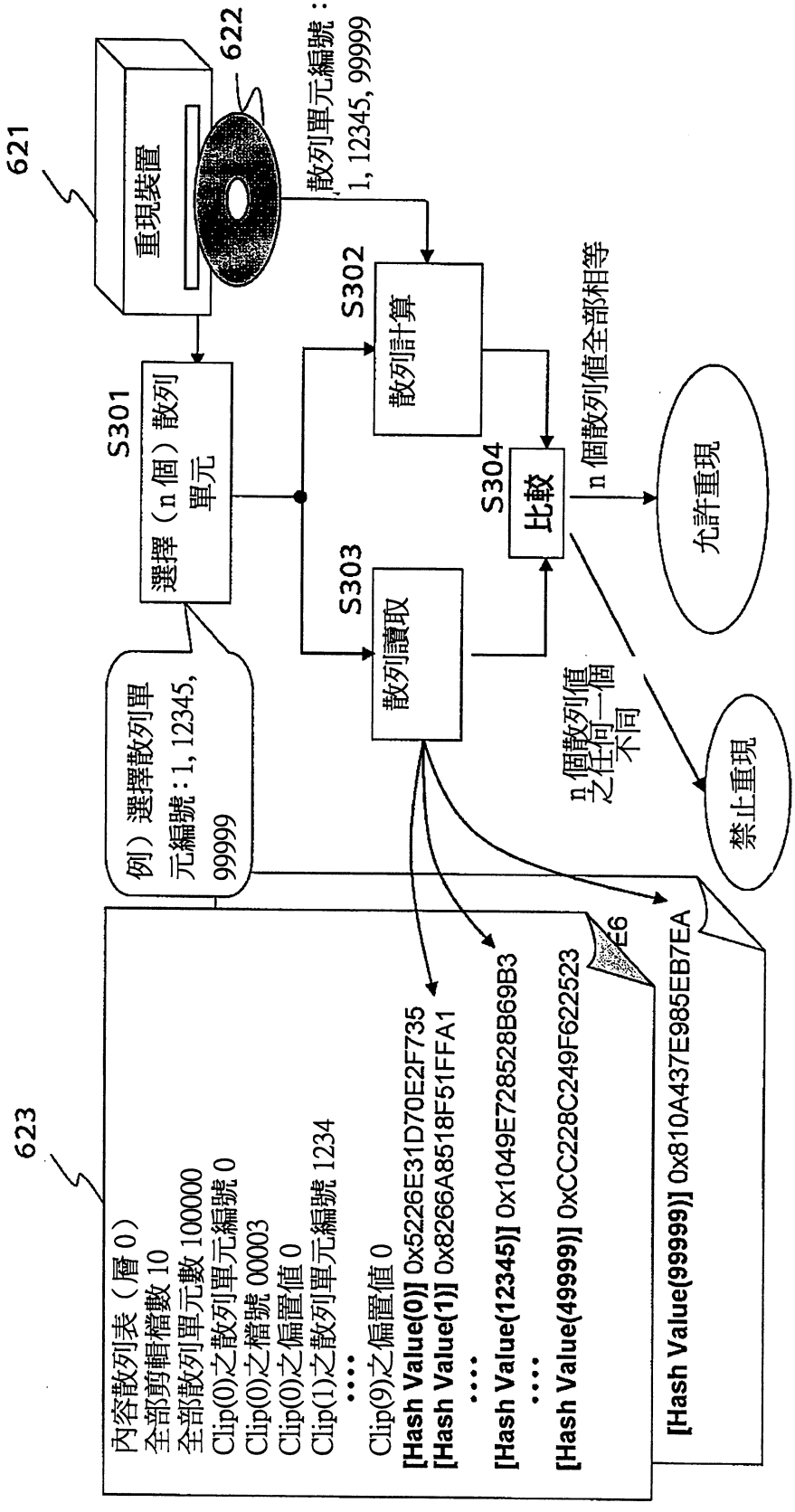
621
重現裝置
622
散列單元編號：
1, 12345, 99999
S301
選擇（n個）散列
單元
S302
散列計算
S303
散列讀取
S304
比較
n個散列值全部相等
允許重現
禁止重現
n個散列值
之任何一個
不同
例）選擇散列單
元編號：1, 12345,
99999
623
內容散列表（層0）
全部剪輯檔數 10
全部散列單元數 100000
Clip(0)之散列單元編號 0
Clip(0)之檔號 00003
Clip(0)之偏置值 0
Clip(1)之散列單元編號 1234
....
Clip(9)之偏置值 0
[Hash Value(0)] 0x5226E31D70E2F735
[Hash Value(1)] 0x8266A8518F51FFA1
....
[Hash Value(12345)] 0x1049E728528B69B3
....
[Hash Value(49999)] 0xCC228C249F622523
....
[Hash Value(99999)] 0x810A437E985EB7EA

圖 22

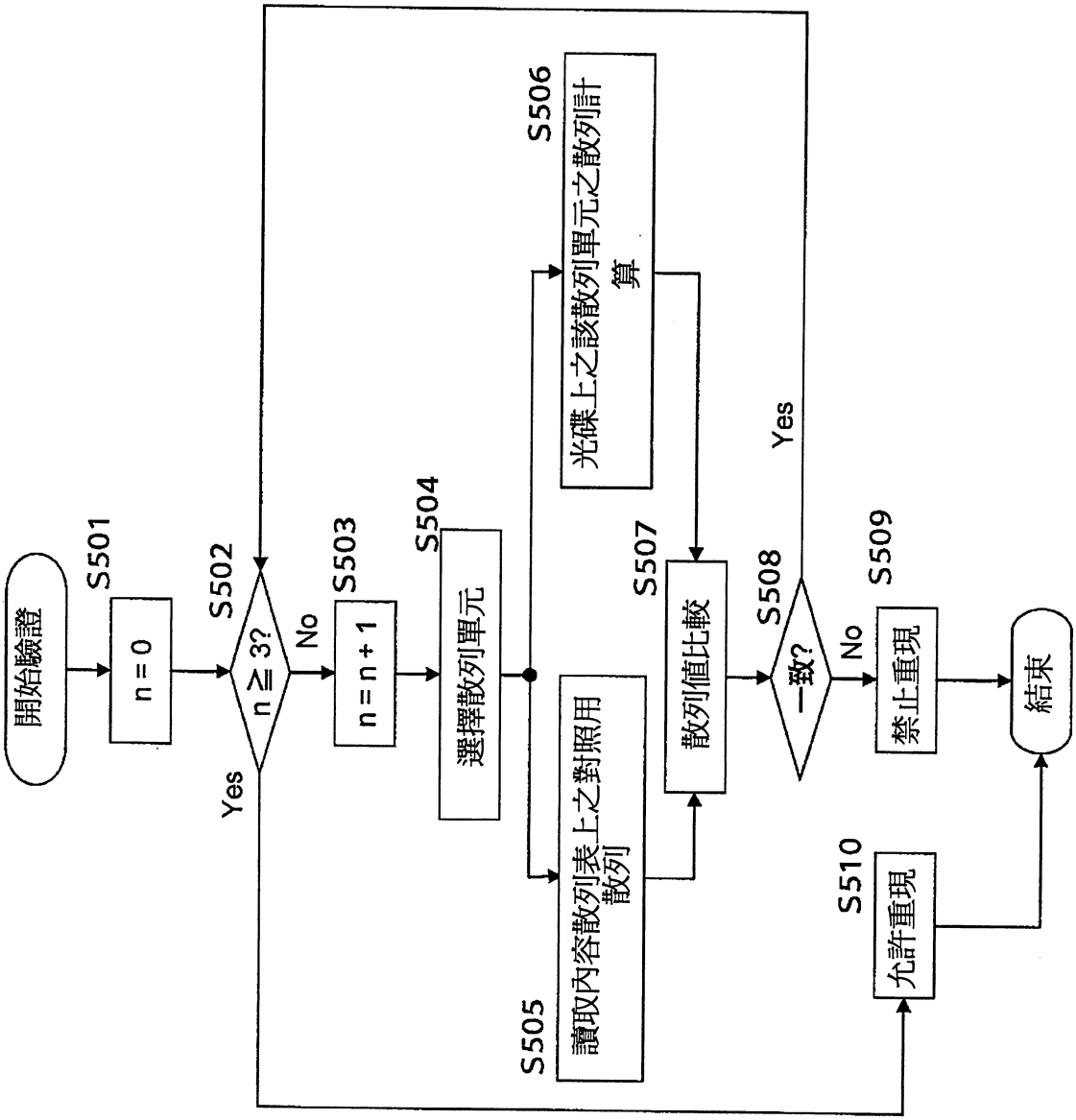
開始驗證
S501
n = 0
S502
n ≧ 3?
Yes
No
S503
n = n + 1
S504
選擇散列單元
S505
讀取內容散列表上之對照用散列
S506
光碟上之該散列單元之散列計算
S507
散列值比較
S508
一致?
Yes
No
S509
禁止重現
S510
允許重現
結束

圖 23

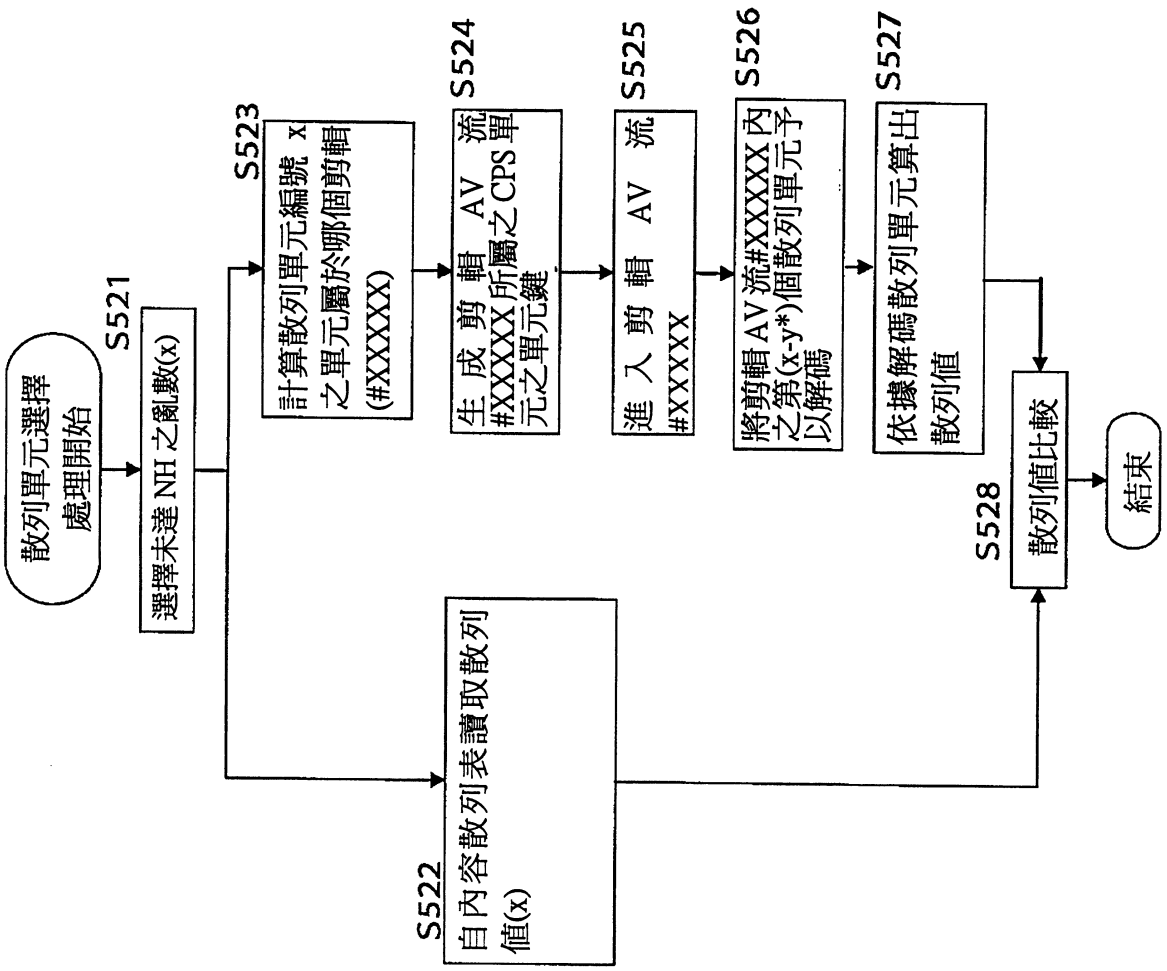
散列單元選擇處理開始
S521
選擇未達 NH 之亂數(x)
S523
計算散列單元編號 x 之單元屬於哪個剪輯(#XXXXX)
S524
生成剪輯 AV 流#XXXXX 所屬之 CPS 單元之單元鍵
S525
進入剪輯 AV 流#XXXXX
S526
將剪輯 AV 流#XXXXX 內之第(x-y*)個散列單元予以解碼
S527
依據解碼散列單元算出散列值
S522
自內容散列表讀取散列值(x)
S528
散列值比較
結束

圖 24

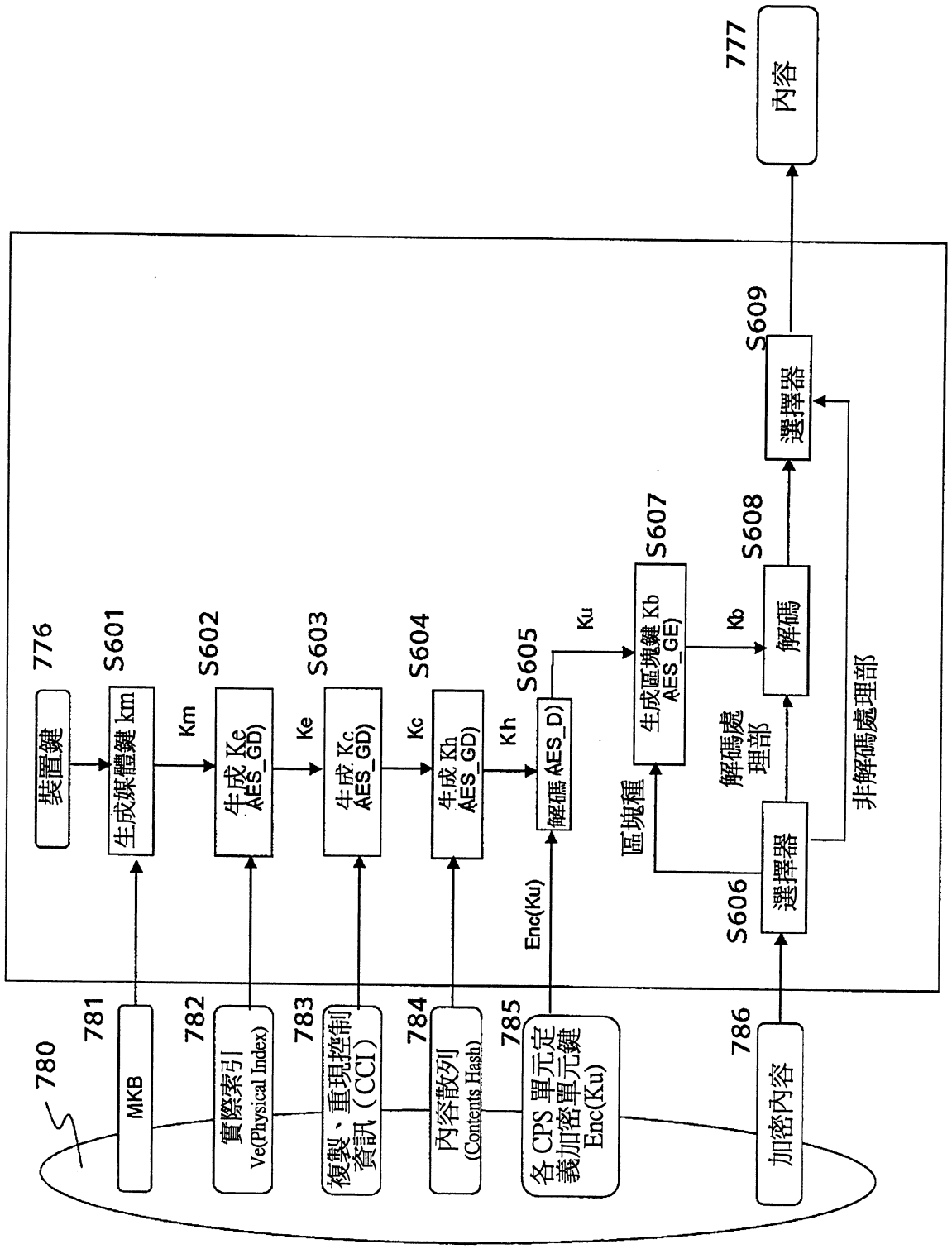
780
781
MKB
782
實際索引
Ve(Physical Index)
783
複製、重現控制
資訊（CCI）
784
內容散列
(Contents Hash)
785
各 CPS 單元定
義加密單元鍵
Enc(Ku)
786
加密內容
776
裝置鍵
S601
生成媒體鍵 km
Km
S602
生成 Ke
AES_GD)
Ke
S603
生成 Kc
AES_GD)
Kc
S604
生成 Kh
AES_GD)
Kh
S605
解碼 AES_D)
Ku
Enc(Ku)
S606
選擇器
區塊種
S607
生成區塊鍵 Kb
AES_GE)
Kb
S608
解碼
解碼處
理部
S609
選擇器
非解碼處理部
777
內容

圖 25

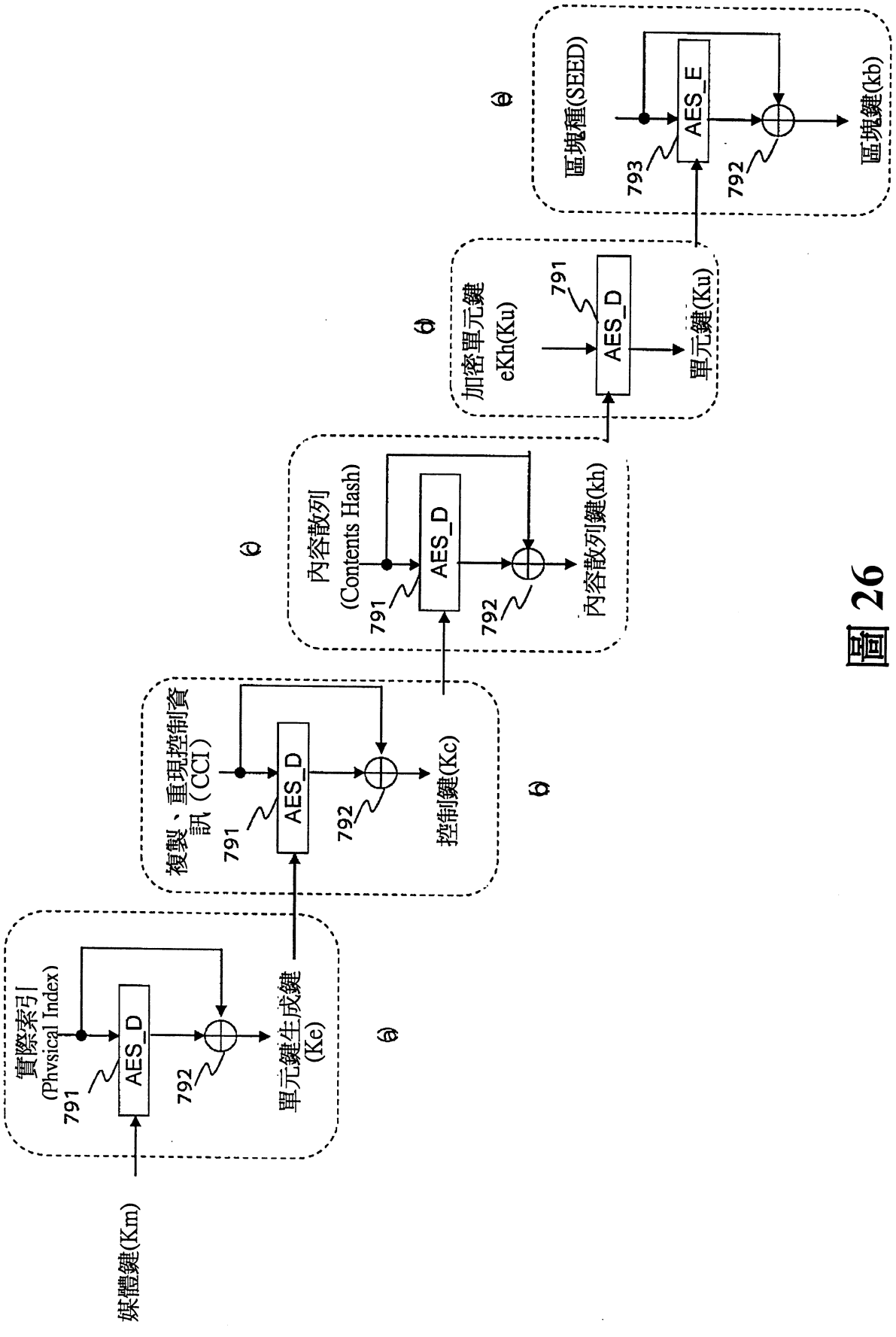
媒體鍵(Km)
實際索引
(Physical Index)
791
AES_D
792
單元鍵生成鍵
(Ke)
複製、重現控制資訊（CCI）
791
AES_D
792
控制鍵(Kc)
內容散列
(Contents Hash)
791
AES_D
792
內容散列鍵(kh)
加密單元鍵
eKh(Ku)
791
AES_D
單元鍵(Ku)
區塊種(SEED)
793
AES_E
792
區塊鍵(kb)

圖 26

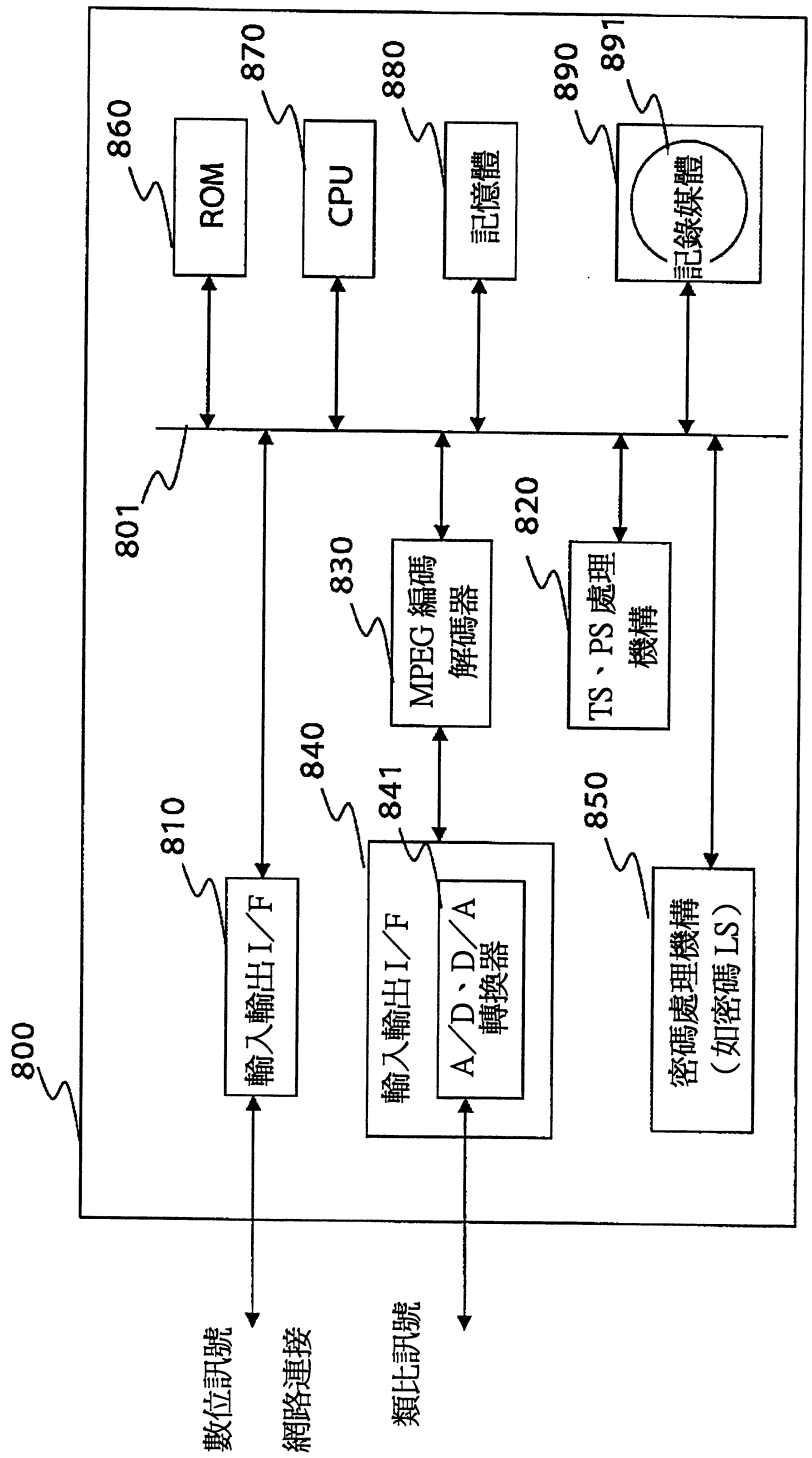
800
801
860
ROM
870
CPU
880
記憶體
890
891
記錄媒體
810
輸入輸出I／F
840
841
輸入輸出I／F
A／D、D／A
轉換器
830
MPEG 編碼
解碼器
820
TS、PS 處理
機構
850
密碼處理機構
（如密碼 LS）
數位訊號
網路連接
類比訊號

圖 27

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100	資訊記錄媒體
101	資料儲存區域
102	引入區域
111	加密內容
112	記錄種
113	CCI
114	內容散列
115	內容證明書
116	公開鍵證明書
120	密碼鍵資訊
121	媒體鍵區塊
131	實際索引

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)

I282055 公告本

發明專利說明書

中文說明書替換頁(95年12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：94129500

※ 申請日期：94.8.29　　※IPC 分類：G06F 12/00 (2006.01)

一、發明名稱：（中文/英文）

資訊處理裝置、資訊記錄媒體、內容管理系統及資料處理方法、以及儲存媒體

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）

中鉢　良治

CHUBACHI, RYOJI

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

十、申請專利範圍：

1. 一種資訊處理裝置，係執行來自資訊記錄媒體之內容重現處理，其特徵為包含：

內容驗證機構，其係驗證內容之正當性；及

內容重現機構，其係將依據前述內容驗證機構之驗證，確認內容之正當性作為條件，來執行內容之重現處理；

前述內容驗證機構包含執行內容驗證處理之構造，其係選擇n個(其中n為1以上整數)作為記錄於資訊記錄媒體之內容之細分化資料而設定之散列單元，執行依據選擇散列單元之算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理，並將選擇之n個全部散列值對照成立作為內容正當性之確認條件。

2. 如請求項1之資訊處理裝置，其中前述內容驗證機構之構造係自儲存於資訊記錄媒體之內容散列表之記錄資料，取得儲存於資訊記錄媒體中之散列單元數(HN)，隨機選擇x≦HN之數值x，使該選擇數值x對應於儲存於資訊記錄媒體之散列單元之散列單元編號，來執行對照處理對象之散列單元之選擇處理。

3. 如請求項1之資訊處理裝置，其中前述內容驗證機構之構造係依據作為儲存於資訊記錄媒體之加密內容之構成資料之散列單元，執行算出散列值之處理。

4. 如請求項1之資訊處理裝置，其中前述內容驗證機構之構造係執行前述選擇散列單元之解碼處理，算出依據該解

碼散列單元之散列值，並執行算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理。

5. 如請求項4之資訊處理裝置，其中前述內容驗證機構之構造係於前述選擇散列單元之解碼處理時，取得對應於散列單元所屬之內容管理單元之單元鍵，來執行應用該單元鍵之解碼處理。

6. 一種資訊記錄媒體，其特徵為：包含儲存內容及作為內容之細分化資料而設定之各個散列單元之散列值之構造。

7. 如請求項6之資訊記錄媒體，其中前述散列單元之邏輯上尺寸設定成執行內容重現之資訊處理裝置中之資料讀取單位之ECC區塊資料之資料長之整數倍。

8. 如請求項7之資訊記錄媒體，其中前述內容包含下述構造：藉由作為內容檔而設定之剪輯檔來區分，並以該剪輯檔之構成資料中，至少剪輯檔之最前資料位置與前述ECC區塊之最前位置一致之方式來記錄。

9. 一種內容管理系統，其特徵為包含：管理中心，其係提供內容利用管理用之管理資訊；內容編輯實體，其係進行內容編輯處理；及資訊記錄媒體製造實體，其係自前述內容編輯實體接收編輯內容，而對資訊記錄媒體記錄內容；

前述內容編輯實體或資訊記錄媒體製造實體之至少任何一個之構造，係算出對應於資訊記錄媒體儲存內容之細分化資料之散列單元之散列值，並生成記錄該算出散

列值之內容散列表，作為資訊記錄媒體之儲存資料。

10. 如請求項9之內容管理系統，其中前述內容編輯實體或資訊記錄媒體製造實體之至少任何一個之構造為，生成記錄依據儲存於前述內容散列表之散列值而算出之散列摘要值之內容證明書，作為儲存於資訊記錄媒體之資料。

11. 如請求項10之內容管理系統，其中前述內容編輯實體或資訊記錄媒體製造實體之至少任何一個之構造為，執行依據儲存於前述內容證明書之資料生成電子簽署，並賦予該內容證明書之處理。

12. 一種資料處理方法，係生成記錄於資訊記錄媒體之資料，其特徵為包含：

記錄資料生成步驟，其係執行扇區單位之記錄資料生成處理；

儲存步驟，其係將生成之記錄資料儲存於緩衝器中；

散列值算出步驟，其係於緩衝器儲存資料達到對應於預定之散區單元之資料量時，依據該緩衝器儲存資料算出散列值；及

設定步驟，其係設定於前述散列值算出步驟中算出之各散列單元之散列值，作為記錄於資訊記錄媒體之資料。

13. 如請求項12之資料處理方法，其中前述資料處理方法進一步包含：

內容散列表生成步驟，其係儲存在前述散列值算出步驟中算出之各散列單元之散列值；及

內容證明書生成步驟，其係生成記錄依據儲存於前述

內容散列表之散列值算出之散列摘要值之內容證明書，作為儲存於資訊記錄媒體之資料。

14. 如請求項13之資料處理方法，其中前述內容證明書生成步驟包含生成依據儲存於內容證明書之資料之電子簽署，並賦予該內容證明書之處理。

15. 如請求項12之資料處理方法，其中前述記錄資料生成步驟參照記述各扇區單位之資料處理態樣之輔助檔，依據該輔助檔決定各扇區是否需要加密及加密態樣，進行按照該決定資訊之資料處理，而生成扇區單位之記錄資料。

16. 一種資料處理方法，係執行來自資訊記錄媒體之內容重現處理，其特徵為包含：

內容驗證步驟，其係驗證內容之正當性；及

內容重現步驟，其係將依據前述內容驗證步驟中之驗證，確認內容之正當性作為條件，來執行內容之重現處理；

前述內容驗證步驟包含選擇n個(其中n為1以上整數)作為記錄於資訊記錄媒體之內容之細分化資料而設定之散列單元，執行依據選擇散列單元之算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理，並執行將選擇之n個全部散列值對照成立作為內容正當性之確認條件之內容驗證處理之步驟。

17. 如請求項16之資料處理方法，其中前述內容驗證步驟包含自儲存於資訊記錄媒體之內容散列表之記錄資料，取得儲存於資訊記錄媒體中之散列單元數(HN)，隨機選擇x

≦HN之數值x，使該選擇數值x對應於儲存於資訊記錄媒體之散列單元之散列單元編號，來執行對照處理對象之散列單元之選擇處理之步驟。

18. 如請求項16之資料處理方法，其中前述內容驗證步驟包含依據作為儲存於資訊記錄媒體之加密內容之構成資料之散列單元，執行算出散列值之處理之步驟。

19. 如請求項16之資料處理方法，其中前述內容驗證步驟包含執行前述選擇散列單元之解碼處理，算出依據該解碼散列單元之散列值，並執行算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理之步驟。

20. 如請求項19之資料處理方法，其中前述內容驗證步驟包含於前述選擇散列單元之解碼處理時，取得對應於散列單元所屬之內容管理單元之單元鍵，來執行應用該單元鍵之解碼處理之步驟。

21. 一種儲存電腦程式之儲存媒體，該電腦程式係在電腦中執行生成記錄於資訊記錄媒體之資料之處理，其特徵為包含：

記錄資料生成步驟，其係執行扇區單位之記錄資料生成處理；

儲存步驟，其係將生成之記錄資料儲存於緩衝器中；

散列值算出步驟，其係於緩衝器儲存資料達到對應於預定之散區單元之資料量時，依據該緩衝器儲存資料算出散列值；及

設定步驟，其係設定於前述散列值算出步驟中算出之

各散列單元之散列值，作為記錄於資訊記錄媒體之資料。

22. 一種儲存電腦程式之儲存媒體，該電腦程式係在電腦中執行來次資訊記錄媒體之內容重現處理，其特徵為包含：

內容驗證步驟，其係驗證內容之正當性；及

內容重現步驟，其係將依據前述內容驗證步驟中之驗證，確認內容之正當性作為條件，來執行內容之重現處理；

前述內容驗證步驟包含選擇n個(其中n為1以上整數)作為記錄於資訊記錄媒體之內容之細分化資料而設定之散列單元，執行依據選擇散列單元之算出散列值與儲存於資訊記錄媒體中之對照用散列值之對照處理，並執行將選擇之n個全部散列值對照成立作為內容正當性之確認條件之內容驗證處理之步驟。