(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4882636号
(P4882636)
(45)発行日　平成24年2月22日(2012.2.22)　(24)登録日　平成23年12月16日(2011.12.16)

(51)Int.Cl.　　F I
G11B 20/10 (2006.01)　　G11B 20/10 H
G06F 21/24 (2006.01)　　G11B 20/10 311
G06F 12/14 560A

請求項の数 19　(全 67 頁)

(21)出願番号　特願2006-263600 (P2006-263600)
(22)出願日　平成18年9月27日 (2006.9.27)
(65)公開番号　特開2008-84445 (P2008-84445A)
(43)公開日　平成20年4月10日 (2008.4.10)
審査請求日　平成21年9月15日 (2009.9.15)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100095496
弁理士　佐々木　榮二
(72)発明者　上田　健二朗
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラム

(57)【特許請求の範囲】
【請求項１】
情報記録媒体（メディア）に対する記録用データを出力するサーバとしての情報処理装置であり、
情報記録媒体に対する記録用データを記憶する記憶部と、
情報記録媒体に対する記録用データを生成するデータ処理部と、
前記記憶部の格納データおよび前記データ処理部の生成データを出力する出力部を有し、
前記記憶部は、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
を含むデータを格納し、
前記データ処理部は、
前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を取得して、取得したメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して自装置対応の秘密鍵を適用して生成した電子署名データを含むユニット対応トークンを生成し、
前記データ出力部は、
前記コンテンツ管理ユニットと、

前記ユニット対応コンテンツ証明書と、
前記ユニット対応使用許諾情報と、
前記ユニット対応トークンを含むデータを情報記録媒体に対する記録データとして出力する処理を実行する構成であることを特徴とする情報処理装置。
【請求項２】
前記記憶部に格納されたユニット対応コンテンツ証明書は、正当なコンテンツ管理ユニットに対応するハッシュ値を照合用ハッシュ値として格納したコンテンツハッシュテーブルのダィジェスト値、および外部機関の電子署名が設定されたコンテンツ証明書であることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記記憶部に格納されたユニット対応コンテンツ証明書は、
情報記録媒体（メディア）に対する記録用データを出力する情報処理装置に対応する公開鍵情報を含む証明書であることを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記データ処理部は、
前記コンテンツ管理ユニットの記録先である情報記録媒体に、既にコンテンツ管理ユニットおよび該コンテンツ管理ユニット対応の鍵情報ファイルが記録されている場合、該記録済みの鍵情報ファイルの更新処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記データ処理部は、
前記コンテンツ管理ユニットの記録先である情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、新たに情報記録媒体に記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項６】
前記データ処理部は、
新たに情報記録媒体に記録するコンテンツ管理ユニットに対応するコンテンツ証明書のファイル名を、前記固有のユニット識別情報を含むファイル名に設定することを特徴とする請求項５に記載の情報処理装置。
【請求項７】
情報記録媒体（メディア）間のコンテンツのコピー記録処理に対する管理処理を実行するサーバとしての情報処理装置であり、
コピー記録対象となるコンテンツ管理ユニットのユニット識別情報を入力するとともに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を入力する入力部と、
前記メディア識別情報と前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書の識別情報とを含むデータに対して自装置対応の秘密鍵を適用して電子署名データを生成して、該電子署名データを含むコンテンツ管理ユニット対応のユニット対応トークンを生成するデータ処理部と、
前記ユニット対応トークンを情報記録媒体記録データとして出力する出力部と、
を有することを特徴とする情報処理装置。
【請求項８】
情報記録媒体（メディア）に対するコンテンツ記録処理を実行する情報処理装置であり、
情報記録媒体に対する記録データを取得または生成するデータ処理部を有し、
前記データ処理部は、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、

前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して外部サーバの秘密鍵を適用して生成された電子署名データを含むユニット対応トークンと、
を含むデータを情報記録媒体に対する記録データとして取得または生成する処理を実行し、
前記コンテンツ管理ユニットの記録先である情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、新たに情報記録媒体に記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行する構成であることを特徴とする情報処理装置。

【請求項９】
第１の情報記録媒体（メディア）の記録コンテンツを読み出し、第２の情報記録媒体（メディア）に対する記録データとして出力する処理を実行する情報処理装置であり、
前記第１の情報記録媒体から読み取られたデータに基づいて、前記第２の情報記録媒体に記録するデータを生成するデータ処理部を有し、
前記データ処理部は、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを前記第１の情報記録媒体から読み出して出力する構成であり、
前記第２の情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、該第２の情報記録媒体に新たに記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行し、
前記第２の情報記録媒体のメディア識別情報と前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書の識別情報とを含むデータに対してサーバの秘密鍵を適用して生成された電子署名を含むコンテンツ管理ユニット対応のユニット対応トークンを前記第２の情報記録媒体への記録データとして出力することを特徴とする情報処理装置。

【請求項１０】
情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理装置であり、
前記情報記録媒体に記録され、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを取得して復号する処理を実行するデータ処理部を有し、
前記データ処理部は、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記情報記録媒体の識別情報であるメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して外部サーバの秘密鍵を適用して生成された電子署名データを含むユニット対応トークンを、
前記情報記録媒体から取得し、取得データの正当性検証処理を実行し、正当性が確認されたことを条件として前記コンテンツ管理ユニットの再生処理を実行する構成であることを特徴とする情報処理装置。

【請求項１１】
利用管理対象コンテンツを格納した情報記録媒体であり、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記情報記録媒体の識別情報であるメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して外部サーバの秘密鍵を適用して生成された電子署名データを含むユニット対応トークンを記録データとして有し、情報処理装置における前記コンテンツ管理ユニットの再生条件として、前記ユニット対応コンテンツ証明書、前記ユニット対応使用許諾情報、および前記ユニット対応トークンの検証処理を実行させる構成としたことを特徴とする情報記録媒体。

【請求項１２】
情報記録媒体（メディア）に対する記録用データを出力するサーバにおける情報処理方法であり、
データ処理部が、記憶部から、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
を取得するデータ取得ステップと、
データ処理部が、前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を取得して、取得したメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して自装置対応の秘密鍵を適用して電子署名データを生成して、該電子署名データを含むユニット対応トークンを生成するトークン生成ステップと、
データ出力部が、
前記コンテンツ管理ユニットと、
前記ユニット対応コンテンツ証明書と、
前記ユニット対応使用許諾情報と、
前記ユニット対応トークンを含むデータを情報記録媒体に対する記録データとして出力するステップと、
を実行することを特徴とする情報処理方法。
【請求項１３】
情報記録媒体（メディア）間のコンテンツのコピー記録処理に対する管理処理を実行するサーバにおける情報処理方法であり、
入力部が、コピー記録対象となるコンテンツ管理ユニットのユニット識別情報を入力するとともに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を入力するデータ入力ステップと、
データ処理部が、前記メディア識別情報と前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書の識別情報とを含むデータに対して自装置対応の秘密鍵を適用して電子署名データを生成して、該電子署名データを含むコンテンツ管理ユニット対応のユニット対応トークンを生成するトークン生成ステップと、
出力部が、前記ユニット対応トークンを情報記録媒体記録データとして出力するデータ出力ステップと、
を有することを特徴とする情報処理方法。
【請求項１４】
情報処理装置において、情報記録媒体（メディア）に対するコンテンツ記録処理を実行する情報処理方法であり、
データ処理部が、情報記録媒体に対する記録データを取得または生成するデータ処理ステップを有し、
前記データ処理ステップは、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して外部サーバの秘密鍵を適用して生成された電子署名データを含むユニット対応トークンと、
を含むデータを情報記録媒体に対する記録データとして取得または生成するステップと、
前記コンテンツ管理ユニットの記録先である情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、新たに情報記録媒体に記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情

報を設定するステップと、
を含むことを特徴とする情報処理方法。
【請求項１５】
情報処理装置において、第１の情報記録媒体（メディア）の記録コンテンツを読み出し、第２の情報記録媒体（メディア）に対する記録データとして出力する処理を実行する情報処理方法であり、
データ処理部が、前記第１の情報記録媒体から読み取られたデータに基づいて、前記第２の情報記録媒体に記録するデータを生成するデータ処理ステップを有し、
前記データ処理ステップは、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを前記第１の情報記録媒体から読み出して出力するステップと、
前記第２の情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、該第２の情報記録媒体に新たに記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行するステップと、
前記第２の情報記録媒体のメディア識別情報と前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書の識別情報とを含むデータに対してサーバの秘密鍵を適用して生成された電子署名を含むコンテンツ管理ユニット対応のユニット対応トークンを前記第２の情報記録媒体への記録データとして出力するステップと、
を含むことを特徴とする情報処理方法。
【請求項１６】
情報処理装置において、情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理方法であり、
データ処理部が、前記情報記録媒体に記録され、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを取得して復号する処理を実行するデータ処理ステップ有し、
前記データ処理ステップは、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記情報記録媒体の識別情報であるメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して外部サーバの秘密鍵を適用して生成された電子署名データを含むユニット対応トークンを、
前記情報記録媒体から取得し、取得データの正当性検証処理を実行し、正当性が確認されたことを条件として前記コンテンツ管理ユニットの再生処理を実行するステップを含むことを特徴とする情報処理方法。
【請求項１７】
情報処理装置において、情報記録媒体（メディア）に対する記録用データを出力する処理を実行させるコンピュータ・プログラムであり、
データ処理部に、記憶部から、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
を取得させるデータ取得ステップと、
データ処理部に、前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を取得して、取得したメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して自装置対応の秘密鍵を適用して電子署名データを生成して、該電子署名データを含むユニット対応トークンを生成させるトークン生成ステップと、
データ出力部に、
前記コンテンツ管理ユニットと、

前記ユニット対応コンテンツ証明書と、
前記ユニット対応使用許諾情報と、
前記ユニット対応トークンを含むデータを情報記録媒体に対する記録データとして出力させるステップと、
を実行させることを特徴とするコンピュータ・プログラム。
【請求項１８】
情報処理装置において、情報記録媒体（メディア）間のコンテンツのコピー記録処理に対する管理処理を実行させるコンピュータ・プログラムであり、
入力部に、コピー記録対象となるコンテンツ管理ユニットのユニット識別情報を入力させるとともに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を入力させるデータ入力ステップと、
データ処理部に、前記メディア識別情報と前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書の識別情報とを含むデータに対して自装置対応の秘密鍵を適用して電子署名データを生成させて、該電子署名データを含むコンテンツ管理ユニット対応のユニット対応トークンを生成させるトークン生成ステップと、
出力部に、前記ユニット対応トークンを情報記録媒体記録データとして出力させるデータ出力ステップと、
を実行させることを特徴とするコンピュータ・プログラム。
【請求項１９】
情報処理装置において、情報記録媒体に記録されたコンテンツの再生処理を実行させるコンピュータ・プログラムであり、
データ処理部に、前記情報記録媒体に記録され、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを取得して復号する処理を実行させるデータ処理ステップ有し、
前記データ処理ステップは、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記情報記録媒体の識別情報であるメディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して外部サーバの秘密鍵を適用して生成された電子署名データを含むユニット対応トークンを、
前記情報記録媒体から取得し、取得データの正当性検証処理を実行し、正当性が確認されたことを条件として前記コンテンツ管理ユニットの再生処理を実行させるステップを含むことを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、利用制御の対象となるコンテンツを、例えばＲ型、ＲＥ型ディスクのような追加記録が可能なメディアに記録し、これらの記録コンテンツを適正な利用管理の下で利用する構成を実現する情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。
【背景技術】
【０００２】
音楽、映画等のコンテンツの記録媒体として、昨今は、ＤＶＤ(Digital Versatile Disc)、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などが利用されている。これらの情報記録媒体には、予めデータが記録され、新たなデータ書き込みを許容しない媒体（ＲＯＭ型）や、データ書き込み可能な媒体（Ｒ型、ＲＥ型など）がある。ユーザは、データ書き込み可能な情報記録媒体を利用することで、例えば、ネットワークや、公共の場所に設置された装置を介して様々なコンテンツを記録することが可能となる。
【０００３】

しかし、音楽データ、画像データ等、多くのコンテンツは、その作成者あるいは販売者に著作権、頒布権等が保有され、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

【０００４】

コンテンツ利用制限の１つの手法がコンテンツを暗号化して配付し、正当なコンテンツ利用権を持つユーザや機器のみが復号を可能としたシステムである。なお、コンテンツの暗号化を行なうことで、コンテンツの利用制御を行なう構成については、例えば特許文献１に記載されている。

【０００５】

コンテンツの暗号化に基づくコンテンツ利用形態を実現するコンテンツの著作権保護技術に関する規格としてＡＡＣＳ(Advanced Access Content System)がある。ＡＡＣＳの規格では、コンテンツをユニットとして区分し、各ユニットに対応するユニット鍵を適用した暗号化コンテンツをディスクに記録する構成としている。ユニット鍵を格納したユニット鍵ファイルは、暗号化したユニット鍵を記録したファイルとしてディスクに記録される。さらに、暗号鍵ブロックであるＭＫＢ（Media Key Block）もディスクに記録される。

【０００６】

ＭＫＢは、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックであり、有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみメディア鍵［Ｋｍ］の取得が可能となる。メディア鍵［Ｋｍ］を利用することで、ユニット鍵ファイルに含まれる暗号化ユニット鍵を復号してユニット鍵を取得して、ユニット鍵を用いて暗号化コンテンツの復号を行なうというシーケンスとなっている。

【０００７】

このように、コンテンツをユニット単位に区分して、各ユニット毎に異なる暗号鍵であるユニット鍵を割り当ててコンテンツを暗号化する構成により、ユニット単位のコンテンツの利用制御を実現している。

【０００８】

コンテンツを記録したメディア、例えばディスクが再生のみを共用するＲＯＭ型である場合は、ディスクに対する新たなコンテンツの追加記録や、編集は実行されないので、ディスクに記録されるコンテンツや鍵情報は固定のまま変更する必要がない。しかし、一方、データ書き込みが可能なＲ型、ＲＥ型などのメディアを利用した形態では、ディスクに記録されたコンテンツが固定でなく、新たな追加コンテンツの記録や記録コンテンツの削除、更新といった処理が実行され、これらのデータ更新に応じて、ユニット鍵の追加や削除といった処理も必要となる。

【０００９】

ディスクに新たなコンテンツを記録する場合の処理として、

（ａ）既にコンテンツの記録されたメディア（例えばＲＯＭディスク）からＲ型、ＲＥ型などのメディアにコンテンツをコピー記録する処理、

（ｂ）コンテンツサーバからコンテンツをダウンロードしてＲ型、ＲＥ型などのメディアにコンテンツを記録する処理、

（ｃ）は店頭や公共スペースに置かれた端末を利用して、Ｒ型、ＲＥ型などのメディアにコンテンツを記録する処理、

これらの様々な処理が想定される。

【００１０】

このように、メディアに対するコンテンツの新たな記録を行なってユーザがこのコンテンツを再生、利用する場合、個々の記録コンテンツに対応する利用制御が必要となる。すなわち、ＲＯＭ型ディスクであれば、メディアに記録された固定されたコンテンツに対応する固定的な利用制御構成を採用することが可能であるが、Ｒ型、ＲＥ型のような追加記録が可能なメディアに適宜、コンテンツを記録することを許容した場合、メディアに対し

て新規に記録したコンテンツ各々に対応する利用制御構成や、コンテンツ記録処理の効率化が問題となる。すなわち、媒体に対して1つの利用制御の構成しか考えられていないため、例えば小容量のデータを随時追加記録していくことができず、小容量のデータであっても追加して記録していくことができないという問題があった。

【特許文献１】特開２００３－１１６１００号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

本発明は、このような状況に鑑みてなされたものであり、データ書き込み可能なメディアに、新たに利用管理コンテンツを記録し、利用制御を行う構成において、コンテンツ記録処理の効率化、記録コンテンツ各々についての確実な利用制御を実現する情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【課題を解決するための手段】

【００１２】

本発明の第１の側面は、

情報記録媒体（メディア）に対する記録用データを出力するサーバとしての情報処理装置であり、

情報記録媒体に対する記録用データを記憶する記憶部と、

情報記録媒体に対する記録用データを生成するデータ処理部と、

前記記憶部の格納データおよび前記データ処理部の生成データを出力する出力部を有し、

前記記憶部は、

利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、

前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、

前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、

を含むデータを格納し、

前記データ処理部は、

前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を取得して、取得したメディア識別情報を含むデータに基づく電子署名データを生成して、該電子署名データを含むユニット対応トークンを生成し、

前記データ出力部は、

前記コンテンツ管理ユニットと、

前記ユニット対応コンテンツ証明書と、

前記ユニット対応使用許諾情報と、

前記ユニット対応トークンを含むデータを情報記録媒体に対する記録データとして出力する処理を実行する構成であることを特徴とする情報処理装置にある。

【００１３】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記メディア識別情報と前記ユニット対応コンテンツ証明書の識別情報とを含むデータに対して、自装置対応の秘密鍵を適用して生成した電子署名データを含むユニット対応トークンを生成する処理を実行する構成であることを特徴とする。

【００１４】

さらに、本発明の情報処理装置の一実施態様において、前記記憶部に格納されたユニット対応コンテンツ証明書は、正当なコンテンツ管理ユニットに対応するハッシュ値を照合用ハッシュ値として格納したコンテンツハッシュテーブルのダィジェスト値、および外部機関の電子署名が設定されたコンテンツ証明書であることを特徴とする。

【００１５】

さらに、本発明の情報処理装置の一実施態様において、前記記憶部に格納されたユニット対応コンテンツ証明書は、情報記録媒体（メディア）に対する記録用データを出力する

情報処理装置に対応する公開鍵情報を含む証明書であることを特徴とする。

【００１６】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記コンテンツ管理ユニットの記録先である情報記録媒体に、既にコンテンツ管理ユニットおよび該コンテンツ管理ユニット対応の鍵情報ファイルが記録されている場合、該記録済みの鍵情報ファイルの更新処理を実行する構成であることを特徴とする。

【００１７】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記コンテンツ管理ユニットの記録先である情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、新たに情報記録媒体に記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行する構成であることを特徴とする。

【００１８】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、新たに情報記録媒体に記録するコンテンツ管理ユニットに対応するコンテンツ証明書のファイル名を、前記固有のユニット識別情報を含むファイル名に設定することを特徴とする。

【００１９】

さらに、本発明の第２の側面は、

情報記録媒体（メディア）間のコンテンツのコピー記録処理に対する管理処理を実行するサーバとしての情報処理装置であり、

コピー記録対象となるコンテンツ管理ユニットのユニット識別情報を入力するとともに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を入力する入力部と、

前記メディア識別情報を含むデータに基づく電子署名データを生成して、該電子署名データを含むコンテンツ管理ユニット対応のユニット対応トークンを生成するデータ処理部と、

前記ユニット対応トークンを情報記録媒体記録データとして出力する出力部と、

を有することを特徴とする情報処理装置にある。

【００２４】

さらに、本発明の第３の側面は、

情報記録媒体（メディア）に対するコンテンツ記録処理を実行する情報処理装置であり、

情報記録媒体に対する記録データを取得または生成するデータ処理部を有し、

前記データ処理部は、

利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、

前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、

前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、

前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を含み、外部サーバの電子署名データを含むユニット対応トークンと、

を含むデータを情報記録媒体に対する記録データとして取得または生成する処理を実行し、

前記コンテンツ管理ユニットの記録先である情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、新たに情報記録媒体に記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行する構成であることを特徴とする情報処理装置にある。

【００２６】

さらに、本発明の第４の側面は、

第１の情報記録媒体（メディア）の記録コンテンツを読み出し、第２の情報記録媒体（メディア）に対する記録データとして出力する処理を実行する情報処理装置であり、

前記第１の情報記録媒体から読み取られたデータに基づいて、前記第２の情報記録媒体

に記録するデータを生成するデータ処理部を有し、
前記データ処理部は、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを前記第１の情報記録媒体から読み出して出力する構成であり、
前記第２の情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、該第２の情報記録媒体に新たに記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行する構成であることを特徴とする情報処理装置にある。
【００２８】
さらに、本発明の第５の側面は、
情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理装置であり、
前記情報記録媒体に記録され、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを取得して復号する処理を実行するデータ処理部を有し、
前記データ処理部は、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記情報記録媒体の識別情報であるメディア識別情報を含むデータに基づく電子署名データを含むユニット対応トークンを、
前記情報記録媒体から取得し、取得データの正当性検証処理を実行し、正当性が確認されたことを条件として前記コンテンツ管理ユニットの再生処理を実行する構成であることを特徴とする情報処理装置にある。
【００３２】
さらに、本発明の第６の側面は、
利用管理対象コンテンツを格納した情報記録媒体であり、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記情報記録媒体の識別情報であるメディア識別情報を含むデータに基づく電子署名データを含むユニット対応トークンを記録データとして有し、情報処理装置における前記コンテンツ管理ユニットの再生条件として、前記ユニット対応コンテンツ証明書、前記ユニット対応使用許諾情報、および前記ユニット対応トークンの検証処理を実行させる構成としたことを特徴とする情報記録媒体にある。
【００３４】
さらに、本発明の第８の側面は、
情報記録媒体（メディア）に対する記録用データを出力するサーバにおける情報処理方法であり、
データ処理部が、記憶部から、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
を取得するデータ取得ステップと、
データ処理部が、前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を取得して、取得したメディア識別情報を含むデータに基づく電子署名データを生成して、該電子署名データを含むユニット対応トークンを生成するトークン生成ステップと、
データ出力部が、
前記コンテンツ管理ユニットと、
前記ユニット対応コンテンツ証明書と、
前記ユニット対応使用許諾情報と、
前記ユニット対応トークンを含むデータを情報記録媒体に対する記録データとして出力

するステップと、
を実行することを特徴とする情報処理方法にある。
【００３９】
さらに、本発明の第９の側面は、
情報記録媒体（メディア）間のコンテンツのコピー記録処理に対する管理処理を実行するサーバにおける情報処理方法であり、
入力部が、コピー記録対象となるコンテンツ管理ユニットのユニット識別情報を入力するとともに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を入力するデータ入力ステップと、
データ処理部が、前記メディア識別情報を含むデータに基づく電子署名データを生成して、該電子署名データを含むコンテンツ管理ユニット対応のユニット対応トークンを生成するトークン生成ステップと、
出力部が、前記ユニット対応トークンを情報記録媒体記録データとして出力するデータ出力ステップと、
を有することを特徴とする情報処理方法にある。
【００４４】
さらに、本発明の第１０の側面は、
情報処理装置において、情報記録媒体（メディア）に対するコンテンツ記録処理を実行する情報処理方法であり、
データ処理部が、情報記録媒体に対する記録データを取得または生成するデータ処理ステップを有し、
前記データ処理ステップは、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を含み、外部サーバの電子署名データを含むユニット対応トークンと、
を含むデータを情報記録媒体に対する記録データとして取得または生成するステップと、
前記コンテンツ管理ユニットの記録先である情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、新たに情報記録媒体に記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定するステップと、
を含むことを特徴とする情報処理方法にある。
【００４６】
さらに、本発明の第１１の側面は、
情報処理装置において、第１の情報記録媒体（メディア）の記録コンテンツを読み出し、第２の情報記録媒体（メディア）に対する記録データとして出力する処理を実行する情報処理方法であり、
データ処理部が、前記第１の情報記録媒体から読み取られたデータに基づいて、前記第２の情報記録媒体に記録するデータを生成するデータ処理ステップを有し、
前記データ処理ステップは、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを前記第１の情報記録媒体から読み出して出力するステップと、
前記第２の情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、該第２の情報記録媒体に新たに記録するコンテンツ管理ユニットに対して、前記記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行するステップと、
を含むことを特徴とする情報処理方法にある。
【００４８】

さらに、本発明の第１２の側面は、
情報処理装置において、情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理方法であり、
データ処理部が、前記情報記録媒体に記録され、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを取得して復号する処理を実行するデータ処理ステップ有し、
前記データ処理ステップは、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記情報記録媒体の識別情報であるメディア識別情報を含むデータに基づく電子署名データを含むユニット対応トークンを、
前記情報記録媒体から取得し、取得データの正当性検証処理を実行し、正当性が確認されたことを条件として前記コンテンツ管理ユニットの再生処理を実行するステップを含むことを特徴とする情報処理方法にある。

【００５２】

さらに、本発明の第１３の側面は、
情報処理装置において、情報記録媒体（メディア）に対する記録用データを出力する処理を実行させるコンピュータ・プログラムであり、
データ処理部に、記憶部から、
利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
を取得させるデータ取得ステップと、
データ処理部に、前記コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を取得して、取得したメディア識別情報を含むデータに基づく電子署名データを生成して、該電子署名データを含むユニット対応トークンを生成させるトークン生成ステップと、
データ出力部に、
前記コンテンツ管理ユニットと、
前記ユニット対応コンテンツ証明書と、
前記ユニット対応使用許諾情報と、
前記ユニット対応トークンを含むデータを情報記録媒体に対する記録データとして出力させるステップと、
を実行させることを特徴とするコンピュータ・プログラムにある。

【００５３】

さらに、本発明の第１４の側面は、
情報処理装置において、情報記録媒体（メディア）間のコンテンツのコピー記録処理に対する管理処理を実行させるコンピュータ・プログラムであり、
入力部に、コピー記録対象となるコンテンツ管理ユニットのユニット識別情報を入力させるとともに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を入力させるデータ入力ステップと、
データ処理部に、前記メディア識別情報を含むデータに基づく電子署名データを生成させて、該電子署名データを含むコンテンツ管理ユニット対応のユニット対応トークンを生成させるトークン生成ステップと、
出力部に、前記ユニット対応トークンを情報記録媒体記録データとして出力させるデータ出力ステップと、
を実行させることを特徴とするコンピュータ・プログラムにある。

【００５４】

さらに、本発明の第１５の側面は、
情報処理装置において、情報記録媒体に記録されたコンテンツの再生処理を実行させる

コンピュータ・プログラムであり、
データ処理部に、前記情報記録媒体に記録され、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを取得して復号する処理を実行させるデータ処理ステップ有し、
前記データ処理ステップは、
前記コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、
前記コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、
前記情報記録媒体の識別情報であるメディア識別情報を含むデータに基づく電子署名データを含むユニット対応トークンを、
前記情報記録媒体から取得し、取得データの正当性検証処理を実行し、正当性が確認されたことを条件として前記コンテンツ管理ユニットの再生処理を実行させるステップを含むことを特徴とするコンピュータ・プログラムにある。
【００５５】
なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＤＶＤ、ＣＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。
【００５６】
本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【発明の効果】
【００５７】
本発明の一実施例の構成によれば、Ｒ／ＲＥ型ディスクなどのデータ記録可能なメディアに対して利用管理対象コンテンツを記録する構成において、ユニット単位で利用管理のなされるコンテンツ管理ユニット（ＣＰＳユニット）単位の各種管理データ、すなわち、ユニット対応コンテンツ証明書、ユニット対応使用許諾情報、さらに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を含むデータに基づく電子署名データを含むユニット対応トークンを生成して、これらの管理データをコンテンツ管理ユニットとともに、Ｒ／ＲＥ型ディスクなどのメディアに記録する構成とした。この構成によれば、管理データがコンテンツ管理ユニット単位で予め設定されているので、コンテンツの追記処理などに際して、ユニット対応の管理データの取得、生成、記録処理を迅速に行なうことが可能となり、メディアに随時記録されるコンテンツ管理ユニット対応の利用管理を確実に効率的に行なうことが可能となる。
【発明を実施するための最良の形態】
【００５８】
以下、図面を参照しながら本発明の情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は以下の項目に従って行なう。
１．コンテンツ記録処理を行なう複数の処理例について、
２．コンテンツ記録処理例および記録データの詳細について
（２－１）サーバからのコンテンツ記録処理（ＥＳＴ／Ｍｏｄサーバからのコンテンツ記録）
（２－２）メディア間のコピーによるコンテンツ記録処理（ＭＣ：Ｍａｎａｇｅｄ　Ｃｏｐｙ）
（２－３）ＣＰＳユニット対応の管理データを記録したディスクのディレクトリ例
３．コンテンツ再生処理例について

（３－１）ＳＫＢ（シーケンス鍵ブロック）を利用しない再生処理
（３－２）ＳＫＢ（シーケンス鍵ブロック）を利用した再生処理
４．情報処理装置の機能、構成について

【００５９】

［１．コンテンツ記録処理を行なう複数の処理例について］

まず、本発明の想定するコンテンツの記録、利用例について、図を参照して説明する。本発明は、例えば、データ書き込みが可能なＲ型、ＲＥ型などの情報記録媒体（メディア）に、ユーザが任意のタイミングでコンテンツを記録してコンテンツを利用する場合、記録コンテンツ各々の利用制御を実現するものである。

【００６０】

情報記録媒体（メディア）に新たなコンテンツを記録する処理例としては、
（ａ）既にコンテンツの記録されたメディア（例えばＲＯＭディスク）からＲ型、ＲＥ型などのメディアにコンテンツをコピー記録する処理、
（ｂ）コンテンツサーバからコンテンツをダウンロードしてＲ型、ＲＥ型などのメディアにコンテンツを記録する処理、
（ｃ）店頭や公共スペースに置かれた端末を利用して、Ｒ型、ＲＥ型などのメディアにコンテンツを記録する処理、
これらの処理が想定される。

【００６１】

（ａ）の処理は、例えば、図１（ａ）に示すように、ユーザ１が、既にコンテンツの記録されたメディアであるＲＯＭディスク２をデータ再生装置３にセットして、ＲＯＭディスク２から読み取られたコンテンツを例えばＲ型、ＲＥ型などのデータ書き込み可能なＲ／ＲＥディスク５、具体的には例えばＤＶＤ、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などのＲ／ＲＥディスク５をＰＣなどのデータ記録装置４にセットしてコピーを行なう処理である。なお、このようなコンテンツコピー処理を行なう場合、コンテンツが利用制御コンテンツである場合は、管理サーバ６とネットワーク７を介して接続して、コンテンツコピーの許可を得た上で、コピーが実行される。このような管理サーバの管理の下でのコンテンツコピー処理をＭＣ（Ｍａｎａｇｅｄ　Ｃｏｐｙ）と呼び、管理サーバ６はＭＣサーバと呼ばれる。

【００６２】

（ｂ）の処理は、図２（ｂ）に示すように、ユーザ１１の保持するＰＣなどの情報処理装置１３にユーザの保持するメディア、例えばデータ書き込み可能なメディアであるＲ型またはＲＥ型のディスク１２、具体的にはＤＶＤ、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などを装着し、ネットワーク１５を介してコンテンツサーバ１４からコンテンツを受信して記録する処理である。このコンテンツ提供処理は、ダウンロード型コンテンツ提供処理であり、ＥＳＴ（Ｅｌｅｃｔｒｉｃ　Ｓｅｌｌ　Ｔｈｒｏｕｇｈ）と呼ぶ。なお、コンテンツサーバ１４をＥＳＴサーバと呼ぶ。

【００６３】

（ｃ）の処理は、図２（ｃ）に示すように、ユーザ２１が、例えばコンビニや駅などの公共スペースに設置された端末としてのコンテンツサーバ２４を利用してコンテンツを記録購入する例であり、ユーザ２１の保持するデータ書き込み可能なメディアであるＲ型またはＲＥ型のディスク２２、例えばＤＶＤ、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）をコンビニ２３の端末としてのコンテンツサーバ２４にセットして、ユーザ２１のコンテンツ選択などの操作によって、所望のコンテンツをディスク２２に記録する処理である。このコンテンツ提供処理は、共用端末利用コンテンツ提供処理であり、ＭｏＤ（Ｍａｎｕｆａｃｔｕｒｉｎｇ　ｏｎＤｅｍａｎｄ）と呼ぶ。なお、コンテンツサーバ２４をＭｏＤサーバと呼ぶ。

【００６４】

このように、データ記録可能なＲ／ＲＥ型ディスクなどのメディアに、ユーザの意思に基づいてコンテンツ記録を行ないコンテンツを利用（再生など）する場合、コンテンツが

例えば著作権保護対象コンテンツなどである場合、無秩序な利用を防止するための利用制御が必要となる。前述したように、コンテンツの著作権保護技術に関する規格としてＡＡＣＳ(Advanced Access Content System)がある。ＡＡＣＳの規格では、コンテンツをユニットとして区分し、各ユニットに対応するユニット鍵を適用した暗号化コンテンツをディスクに記録する構成としている。

【００６５】

例えばディスクが再生のみを共用するＲＯＭ型である場合、ディスクに対する新たなコンテンツの追加記録や、編集は実行されないので、ディスクに記録されたコンテンツに対応するユニット鍵を格納したユニット鍵ファイルや、記録コンテンツに対応する使用許諾情報をディスクに記録した状態でユーザに提供することが可能となるが、データ書き込みが可能なＲ型、ＲＥ型などのメディアを利用したコンテンツ利用形態では、メディアの記録コンテンツが固定でなく、新たな追加コンテンツの記録や記録コンテンツの削除、更新といった処理が実行され、これらのデータ更新に応じて、ユニット鍵の追加や削除といった処理も必要となる。

【００６６】

すなわち、ユーザが新たに記録するコンテンツに対応するユニット鍵や、使用許諾情報など、個別のコンテンツ対応する利用制御を確実に行なうためのディスク記録情報の追加や更新が必要となる。

【００６７】

［２．コンテンツ記録処理例およびメディア記録データの詳細について］

次に、上述したようなデータ書き込みが可能なＲ型、ＲＥ型などのメディアに対して、コンテンツを記録する具体的処理シーケンスについて説明する。

上述したように、コンテンツの記録処理態様としては、以下の記録処理態様がある。

（ａ）ＭＣ（Ｍａｎａｇｅｄ　Ｃｏｐｙ）

既にコンテンツの記録されたメディア（例えばＲＯＭディスク）からＲ型、ＲＥ型などのメディアにコンテンツをコピー記録する処理、

（ｂ）ＥＳＴ（Ｅｌｅｃｔｒｉｃ　Ｓｅｌｌ　Ｔｈｒｏｕｇｈ）

コンテンツサーバからコンテンツをダウンロードしてＲ型、ＲＥ型などのメディアにコンテンツを記録する処理、

（ｃ）ＭｏＤ（Ｍａｎｕｆａｃｔｕｒｉｎｇ　ｏｎＤｅｍａｎｄ）

店頭や公共スペースに置かれた端末を利用して、Ｒ型、ＲＥ型などのメディアにコンテンツを記録する処理、

【００６８】

以下、下記の２つのコンテンツ記録処理例について、順次、説明する。

（２－１）サーバからのコンテンツ記録処理（ＥＳＴ／Ｍｏｄサーバからのコンテンツ記録）

（２－２）メディア間のコピーによるコンテンツ記録処理（ＭＣ（Ｍａｎａｇｅｄ　Ｃｏｐｙ））

【００６９】

（２－１）サーバからのコンテンツ記録処理（ＥＳＴ／Ｍｏｄサーバからのコンテンツ記録）

まず、サーバからのコンテンツ記録処理（ＥＳＴ／Ｍｏｄサーバからのコンテンツ記録）すなわち、図２（ｂ），（ｃ）に示すコンテンツサーバを適用したコンテンツ記録処理例について説明する。

【００７０】

図３は、右からコンテンツサーバ１１０、Ｒ型、ＲＥ型などのデータ書き込み可能なメディアに対してコンテンツの記録処理を実行する記録装置（Ｒｅｃｏｒｄｉｎｇ　Ｄｅｖｉｃｅ）１２０、Ｒ型、ＲＥ型などのデータ書き込み可能なメディアとしてのディスク１３０、ディスク１３０を装着して再生する再生装置１４０を示している。

【００７１】

なお、図２（ｂ）のようなダウンロード型コンテンツ提供処理構成（ＥＳＴ（Ｅｌｅｃｔｒｉｃ　Ｓｅｌｌ　Ｔｈｒｏｕｇｈ））では図３に示すコンテンツサーバ１１０が図２に示すコンテンツサーバ１４に相当し、図３に示す記録装置１２０、再生装置１４０は、図２（ｂ）に示すユーザの所有するＰＣなどの情報処理装置１３に相当する。

【００７２】

また、図２（ｃ）のような共用端末利用コンテンツ提供処理構成（Ｍｏｄ（Ｍａｎｕｆａｃｔｕｒｉｎｇ　ｏｎＤｅｍａｎｄ））の場合は、図３に示すコンテンツサーバ１１０と、記録装置１２０が、図２に示すコンテンツサーバ２４に相当する。図３に示す再生装置１４０は、図２（ｃ）には示されないユーザの所有する再生装置に相当する。

【００７３】

図３に示すコンテンツサーバ１１０は、例えばユーザの所有するデータ記録可能な情報記録媒体１３０に対して、新たなコンテンツを記録するとともに、この記録コンテンツに対応する利用制御を実現するための様々なデータ、例えばコンテンツの復号に適用するユニット鍵や、使用許諾情報などを記録する。

【００７４】

まず、コンテンツ提供サーバの実行する処理の説明の前に、情報記録媒体１３０に記録されるデータについて説明する。図３に示す情報記録媒体１３０は、データを書き込むことが可能なメディアであり、具体的には例えばＲ型、ＲＥ型のＢｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）、ＤＶＤディスクなどである。情報記録媒体１３０には、暗号化コンテンツ１３７の他、様々なデータが記録される。これらのデータは、コンテンツの利用制御のために必要となるデータであり、基本的に、ＡＡＣＳの規定に従ったコンテンツ利用制御を実現するために記録されるデータである。まず、これらのデータの概要について説明する。

【００７５】

情報記録媒体１３０に記録される暗号化コンテンツ１３７は、例えば高精細動画像データであるＨＤ（High Definition）ムービーコンテンツなどの動画コンテンツのＡＶ(Audio Visual)ストリーム、あるいは音楽データ、ゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるコンテンツである。

【００７６】

情報記録媒体に格納されるコンテンツは、ユニット単位の区分データ毎の異なる利用制御を実現するため、ユニット毎に異なる鍵（ＣＰＳユニット鍵またはユニット鍵（あるいはタイトル鍵と呼ぶ場合もある））が割り当てられ暗号化されて格納される。１つのユニット鍵が割り当てられるコンテンツ単位をコンテンツ管理ユニット（ＣＰＳユニット）と呼ぶ。

【００７７】

コンテンツ管理ユニット（ＣＰＳユニット）の設定態様について、図４を参照して説明する。図４に示すように、コンテンツは、（Ａ）タイトル２１０、（Ｂ）ムービーオブジェクト２２０、（Ｃ）プレイリスト２３０、（Ｄ）クリップ２４０の階層構成を有し、再生アプリケーションによってアクセスされるインデックスファイルとしてのタイトルが指定されると、タイトルに関連付けられた再生プログラムが指定され、指定された再生プログラムのプログラム情報に従ってコンテンツの再生順等を規定したプレイリストが選択され、プレイリストに規定されたクリップ情報によって、コンテンツ実データとしてのＡＶストリームあるいはコマンドが読み出されて、ＡＶストリームの再生、コマンドの実行処理が行われる。

【００７８】

図４には、２つのＣＰＳユニットを示している。これらは、情報記録媒体に格納されたコンテンツの一部を構成している。ＣＰＳユニット１，２７１、ＣＰＳユニット２，２７２の各々は、アプリケーションインデックスとしてのタイトルと、再生プログラムファイルとしてのムービーオブジェクトと、プレイリストと、コンテンツ実データとしてのＡＶストリームファイルを含むクリップを含むユニットとして設定されたＣＰＳユニットであ

る。
【００７９】
コンテンツ管理ユニット（ＣＰＳユニット）１，２７１には、タイトル１，２１１とタイトル２，２１２、再生プログラム２２１，２２２、プレイリスト２３１，２３２、クリップ２４１、クリップ２４２が含まれ、これらの２つのクリップ２４１，２４２に含まれるコンテンツの実データであるＡＶストリームデータファイル２６１，２６２がコンテンツ管理ユニット（ＣＰＳユニット）１，２７１に対応付けて設定される暗号鍵であるユニット鍵：Ｋｕ１を適用して暗号化される。
【００８０】
コンテンツ管理ユニット（ＣＰＳユニット）２，２７２には、タイトル３，２１３、再生プログラム２２４、プレイリスト２３３、クリップ２４３が含まれ、クリップ２４３に含まれるコンテンツの実データであるＡＶストリームデータファイル２６３がコンテンツ管理ユニット（ＣＰＳユニット）２，２７２に対応付けて設定される暗号鍵であるユニット鍵：Ｋｕ２を適用して暗号化される。
【００８１】
例えば、ユーザがコンテンツ管理ユニット１，２７１に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）１，２７１に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ１を取得して復号処理を実行することが必要であり、復号処理を実行後、アプリケーションプログラムを実行してコンテンツ再生を行なうことができる。コンテンツ管理ユニット２，２７２に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）２，２７２に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ１を取得して復号処理を実行することが必要となる。
【００８２】
コンテンツを再生する情報処理装置において実行される再生アプリケーションプログラムは、ユーザの再生指定コンテンツに対応したコンテンツ管理ユニット（ＣＰＳユニット）を識別し、識別したＣＰＳ管理ユニット情報に対応するＣＰＳ暗号鍵の取得処理を実行する。ＣＰＳ暗号鍵が取得できない場合には、再生不可能のメッセージ表示などを行なう。また、再生アプリケーションプログラムは、コンテンツ再生実行時におけるコンテンツ管理ユニット（ＣＰＳユニット）の切り替えの発生の検出を行ない、必要な鍵の取得、再生不可能のメッセージ表示などを行なう。
【００８３】
次に、暗号化コンテンツ１３７以外のデータについて説明する。
（１）ＭＫＢ
ＭＫＢ（Media Key Block）１３１は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。ＭＫＢ１３１は有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみ、コンテンツの復号に必要な鍵であるメディア鍵［Ｋｍ］の取得を可能とした鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式を適用したものであり、ユーザデバイス（情報処理装置）が有効なライセンスを持つ場合にのみ、メディア鍵［Ｋｍ］の取得を可能とし、無効化（リボーク処理）されたユーザデバイスにおいては、メディア鍵［Ｋｍ］の取得が不可能となる。
【００８４】
コンテンツ利用に関するライセンス管理者としての管理センタはＭＫＢに格納する鍵情報の暗号化に用いるデバイス鍵の変更により、特定のユーザデバイスに格納されたデバイス鍵では復号できない、すなわちコンテンツ復号に必要なメディア鍵を取得できない構成を持つＭＫＢを生成することができる。従って、任意タイミングで不正デバイスを排除（リボーク）して、有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。
【００８５】

（２）メディア識別子

メディア識別子（メディアＩＤ）１３２は、情報記録媒体としてのディスク固有の識別情報であり、例えばディスク個別に設定されたシリアルナンバーである。なお、メディア識別子は、データ記録領域とは異なる領域に記録されるのが一般的であり、書き換えを防止するため、例えば、ディスクの内周領域に物理的に書き込まれている。

メディア識別子のデータ構成例を、図５を参照して説明する。ディスクに記録されるメディア識別子情報には、例えば、以下の情報が含まれる。

コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）：シリアル番号の用途等を示す。このメディア識別子に記録されるコンテンツＩＤは、メディアに記録される記録コンテンツに対応する識別子とは異なる。

データ長（Ｌｅｎｇｔｈ）：メディア識別子としてのシリアル番号のバイト長を示す。この場合、例えば１６。

カテゴリ（Ｃａｔｅｇｏｒｙ）：例えば、メディア種別（ＢＤ－ＲＯＭ，　ＢＤ－ＲＥ　ｏｒ　ＢＤ－Ｒ）を示す。

製造者ＩＤ（Ｍａｎｕｆａｃｔｕｒｅｒ　ＩＤ）：シリアル番号を記録するディスク工場のＩＤ。

シリアルナンバー（Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ）：メディア識別子に相当する番号であり、製造者ＩＤ対応のＩＤ内で一意な番号。

【００８６】

（３）トークン

トークン（Ｔｏｋｅｎ）１３３は、Ｒ／ＲＥディスクなどのデータ記録可能なメディアに対するコンテンツ記録を行う際に、コンテンツとともに記録されるデータであり、コンテンツを提供した装置、すなわち、例えば図２（ｂ）に示すコンテンツサーバ１４や、図２（ｃ）に示す端末としてのコンテンツサーバ２４によって生成されて記録される。なお、図１に示すＲＯＭディスクからのコピー処理による記録に際しても、管理サーバ（ＭＣサーバ）において生成されたトークンが記録される。

【００８７】

本発明の構成では、各ＣＰＳユニットに対応して１つのトークンが設定される。トークンのデータ構成例について図６を参照して説明する、トークンは、図６に示すように、

例えばファイル名は［TokenXXXXX.inf"（XXXXX:CPSユニット番号）］として設定される。また、ファイル名に対応のＣＰＳユニット番号を記載することにより、複数のＴｏｋｅｎが一枚のディスクに記録されていても、再生装置が迅速に所定のＣＰＳユニットに対応するＴｏｋｅｎを把握することができる。また、Ｔｏｋｅｎは少なくとも以下の情報を含む。

＊サーバ公開鍵識別子（Ａｕｔｈｏｒｉｚｉｎｇ＿Ｓｅｒｖｅｒ＿ＩＤ）：トークンの検証に用いるサーバの公開鍵を決定するための識別情報（ＩＤ）。このＩＤに従って、コンテンツ証明書（ＣＣ）に記録された「ＭＣ／ＭｏＤ／ＥＳＴサーバの公開鍵リスト」からトークンの発行者であるサーバの公開鍵を選択する。若しくは、コンテンツ証明書（ＣＣ）に記録された公開鍵とは別に、トークンの「サーバによる電子署名」を検証する公開鍵自身が含まれていても良い。

＊サーバによる電子署名（Ｓｉｇｎａｔｕｒｅ　Ｄａｔａ）：トークンの発行者であるサーバの秘密鍵によって生成された電子署名であり、例えば、Ｒ／ＲＥディスクの識別子（シリアル番号）やコンテンツ（ＣＰＳユニット）に対応するコンテンツ証明書ＩＤに対する署名データである。なお、トークンに自体にＣＰＳユニット番号を含ませることもできる。

【００８８】

電子署名は、例えば、以下のデータによって構成される。

ＥＣＤＳＡ＿ＳＩＧＮ（ＡＳｐｕｂ，Ｃｏｎｔｅｎｔ＿Ｃｅｒｔｉｆｉｃａｔｅ＿ＩＤ｜｜Ｍｅｄｉａ＿ＩＤ）

上記データ構成において、

ＥＣＤＳＡ＿ＳＩＧＮは、楕円曲線暗号（ＥＳＤＳＡ）に従った署名アルゴリズムであることを示し、
その署名対象となるデータに、以下のデータが含まれることを意味している。
ＡＳｐｕｂ：トークン生成者であるサーバの公開鍵、
Ｃｏｎｔｅｎｔ＿Ｃｅｒｔｉｆｉｃａｔｅ＿ＩＤ：トークンに対応するコンテンツ（ＣＰＳユニット）の識別子、
Ｍｅｄｉａ＿ＩＤ：コンテンツを記録したＲ／ＲＥディスクの識別子、

【００８９】
トークンは、Ｒ／ＲＥディスクに記録されたコンテンツが、コンテンツ提供サーバまたは管理サーバによって正しくバインドされたものかどうかを検証するために用いられ、ファイルとしてＲ／ＲＥディスクに記録される。

【００９０】
図３に示す情報記録媒体１３０に記録されたトークン１３３は、再生装置１４０において、暗号化コンテンツ１３７を復号して再生しようとする場合、再生装置１４０において読み取られて、コンテンツサーバの公開鍵を適用した電子署名の検証を行い、トークンの正当性を確認する処理が実行される。この処理によって、暗号化コンテンツ１３７の供給元が正当な装置であることを確認した後、コンテンツの復号が許容される構成となっている。従って、トークンをコピーして不正利用したり、コンテンツを別ディスクに不正コピーしたりすることが防止される。

【００９１】
本発明の構成では、トークンは、各ＣＰＳユニット単位に設定される。従って、ＣＰＳユニット単位のデータ記録処理をＲ／ＲＥディスクに対して実行する場合、その記録対象となるＣＰＳユニットに対応するトークンをコンテンツに併せて記録することが可能となる。

【００９２】
（４）ＣＰＳユニット鍵ファイル
前述したようにコンテンツは、コンテンツの利用管理のため、各々、個別の暗号鍵（ＣＰＳユニット鍵）を適用した暗号化がなされて情報記録媒体１３０に格納される。すなわち、コンテンツを構成するＡＶ(Audio Visual)ストリームなどは、コンテンツ利用の管理単位としてのユニットに区分され、区分されたユニット毎に異なるユニット鍵による暗号化がなされている。

【００９３】
従って、再生装置１４０でコンテンツ再生を実行する場合は、各ＣＰＳユニット対応のＣＰＳユニット鍵を生成して、復号処理を行なうことが必要となる。このＣＰＳユニット鍵がＣＰＳユニット鍵ファイルに格納されている。なお、ＣＰＳユニット鍵はタイトル鍵とも呼ばれる。

【００９４】
ＣＰＳユニット鍵ファイル１３４は、暗号化したユニット鍵を記録したファイルであり、コンテンツ再生を実行する場合は、所定の予め定められたシーケンスでＣＰＳユニット鍵ファイルに含まれる暗号化されたユニット鍵を復号することが必要となる。

【００９５】
具体的には、ユーザデバイスとしての再生装置１４０が有効なライセンスを持つ場合にのみ上述のＭＫＢから取得可能となるメディア鍵［Ｋｍ］や、その他のデータを適用して復号が可能となる。

【００９６】
ＣＰＳユニット鍵ファイルのデータ構成例を図７に示す。ＣＰＳユニット鍵ファイルには以下のデータが含まれる。
クリップ数（Ｎｕｍ＿ｏｆ＿Ｃｌｉｐ（ｎｃ））：ＣＰＳユニット鍵ファイルに格納されたＣＰＳユニット鍵の適用されるコンテンツ（ＣＰＳユニット）に含まれるクリップ数。

タイトル対応ＣＰＳユニットナンバー（ＣＰＳ＿Ｕｎｉｔ＿ｎｕｍｂｅｒ　ｆｏｒ　Ｔｉｔｌｅ＃ｎ）：各タイトル対応のＣＰＳユニットナンバー。

ＣＰＳユニット数（Ｎｕｍ＿ｏｆ＿ＣＰＳ＿Ｕｎｉｔ（ｎｃｕ）：ＣＰＳユニット数。

暗号化ＣＰＳユニット鍵（Ｅｎｃｒｙｐｔｅｄ　Ｕｎｉｔ　Ｋｅｙ　ｆｏｒ　ＣＰＳ　Ｕｎｉｔ＃ｎ）：暗号化されたＣＰＳユニット鍵。

【００９７】

ＣＰＳユニット鍵ファイルに記録されるＣＰＳユニット鍵の暗号化に適用する鍵、すなわちユニット鍵暗号化鍵［Ｋｐａ］は、ＭＫＢから取得されるメディア鍵［Ｋｍ］と、乱数情報としてのバインディングナンス（Ｂｉｎｄｉｎｇ　Ｎｏｎｃｅ）を適用した暗号処理によって生成される。このバインディングナンス（Ｂｉｎｄｉｎｇ　Ｎｏｎｃｅ）についても、図３に示すように、コンテンツサーバ１１０から提供され、ＣＰＳユニット鍵ファイルに併せて情報記録媒体１３０に記録される。バインディングナンス（Ｂｉｎｄｉｎｇ　Ｎｏｎｃｅ）は単独の独立データ、あるいはＣＰＳユニット鍵ファイル内の構成データ、その他のデータファイルの構成データに含める設定など、各種の設定が適用可能である。

【００９８】

なお、図１、図２を参照して説明したようなＲ／ＲＥディスクなどのデータ記録可能なメディアに対してコンテンツを記録する毎にＣＰＳユニット鍵ファイルは更新される。また、コンテンツ再生処理に際して実行するコンテンツの正当性確認のためのコンテンツハッシュ検証に際しては、ＣＰＳユニット鍵ファイルを参照してクリップもしくはタイトルとＣＰＳユニットの対応を調べてハッシュ検証を実行する。コンテンツハッシュテーブル（ＣＨＴ）およびハッシュ検証処理については後述する。

【００９９】

（５）使用許諾情報

使用許諾情報１３５には、例えばコピー・再生制御情報（ＣＣＩ）が含まれる。すなわち、情報記録媒体１３０に格納される暗号化コンテンツ１３７に対応する利用制御のためのコピー制限情報や、再生制限情報である。このコピー・再生制御情報（ＣＣＩ）は、コンテンツ管理ユニットとして設定されるＣＰＳユニット個別の情報として設定される場合や、複数のＣＰＳユニットに対応して設定される場合など、様々な設定が可能である。

【０１００】

なお、この使用許諾情報ファイルのハッシュ値を「コンテンツ証明書に入れる」もしくは「ＣＰＳユニット鍵と排他的論理和をとった値をＣＰＳユニット鍵ファイルに記録しておく」ことによって、改竄を防止することが出来る。この使用許諾情報は、例えばファイル名は［ＣＰＳＵｎｉｔＸＸＸＸＸ．ｃｃｉ"（ＸＸＸＸＸ：ＣＰＳユニット番号）］とする。このように、使用許諾情報のファイル名に、対応のＣＰＳユニット番号を含ませることにより、複数の使用許諾情報が一枚のディスクに記録されていても、再生装置が迅速に所定のＣＰＳユニットに対応する使用許諾情報を把握することができる。また、使用許諾情報は、少なくとも以下の情報を含む。

ＥＰＮ：コピーフリーのコンテンツに対して暗号化記録及び伝送を必要とするかを示す情報。

ＣＣＩ：コピー制限を示す情報。例えば、「コピー禁止」、「コピーフリー」等。

Ｉｍａｇｅ＿Ｃｏｎｓｔｒａｉｎｔ＿Ｔｏｋｅｎ：解像度制限情報。

Ｄｉｇｉｔａｌ＿Ｏｎｌｙ＿Ｔｏｋｅｎ：アナログ／デジタル出力に関する情報。

ＡＰＳ：アナログ出力に対するコンテンツ保護情報。

【０１０１】

（６）証明書データ

証明書データ１３６は、具体的には、

（ａ）コンテンツ証明書（ＣＣ：Ｃｏｎｔｅｎｔ　Ｃｅｒｔ）、

（ｂ）コンテンツハッシュテーブル（ＣＨＴ：Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）、

（ｃ）コンテンツブラックリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）
等を含むデータである。

【０１０２】
（ａ）コンテンツ証明書（ＣＣ）、
（ｂ）コンテンツハッシュテーブル（ＣＨＴ）、
本発明の構成では、これらのデータは、各ＣＰＳユニットに対して個別に設定される。
（ｃ）コンテンツブラックリスト（ＣＲＬ）については、コンテンツ単位ではなく、１枚のディスクに１つ記録されればよい。

【０１０３】
コンテンツハッシュテーブル（ＣＨＴ）は、暗号化コンテンツ１３７の構成データから生成されるハッシュ値を格納したテーブルであり、
コンテンツ証明書（ＣＣ：Content Cert）は、情報記録媒体に格納されたコンテンツの正当性を示すための証明書であり、
コンテンツブラックリスト（ＣＲＬ）は、不正な記録や利用が発覚したコンテンツの識別子（ＩＤ）をリスト化したデータである。
再生装置においてコンテンツ再生を行なう際には、これらの証明書データの検証に基づいて記録コンテンツが正当なコンテンツであることを確認することが要求される。

【０１０４】
なお、現行のＡＡＣＳ規格では、コンテンツ証明書は、ディスクに対して１つのコンテンツ証明書の記録を行なう設定としており、ディスクに複数コンテンツが記録されている場合、すべての記録コンテンツに対応して１つのコンテンツ証明書を生成する設定としている。本発明では、コンテンツ証明書を各ＣＰＳユニットに対して個別に設定する。

【０１０５】
コンテンツ証明書のデータ構成例について、図８を参照して説明する。コンテンツ証明書のファイル名は、例えば、［ContentXXXXX.cer"（XXXXX:CPSユニット番号）］として設定される。このように、Ｔｏｋｅｎ、使用許諾情報のファイル名と同様に、コンテンツ証明書のファイル名に、コンテンツ証明書に対応するＣＰＳユニットのＣＰＳユニット番号を含ませることにより、複数のコンテンツ証明書が一枚のディスクに記録されていても、再生装置が迅速に所望のＣＰＳユニットに対応するコンテンツ証明書を把握することができる。

【０１０６】
コンテンツ証明書のファイル名は、サーバから記録データを受け取り、情報記録媒体に記録する処理を実行する記録装置がディスクに既に記録されているＣＰＳユニット番号とは重複しないように、受信したコンテンツに対するＣＰＳユニット番号を決定し、この決定されたＣＰＳユニット番号（ＸＸＸＸＸ）に対応して、コンテンツ証明書のファイル名を決定して記録する。かかる構成により、ディスクに記録されるＣＰＳユニット番号は、既に記録されているＣＰＳユニット番号と重複せずに設定ができると共に、またコンテンツ証明書自身にはＣＰＳユニット番号を含まずに設定できる。

【０１０７】
すなわち、コンテンツ証明書内に、ＣＰＳユニット番号を含ませると、下記署名（Signature data）がつけられているため、コンテンツ証明書の内容をユーザは変更ができない。したがって、受信・記録装置は、設定できるＣＰＳユニット番号に対応したコンテンツ証明書を取得する必要が出てくるため、サーバではＣＰＳユニット番号のみが異なる複数のコンテンツ証明書を準備しておく必要が出てくる。

【０１０８】
しかしながら、上記のように、記録装置がコンテンツ証明書のファイル名をＣＰＳユニット番号に対応させて設定することにより、コンテンツ証明書の署名は変更せずにすむ。この結果、サーバ側で複数のコンテンツ証明書を用意しておく必要はなくなるため、好適である。

【０１０９】
なお、情報記録媒体に記録するＣＰＳユニットのユニット識別子の決定処理や、コンテンツ証明書のファイル名の決定処理は、情報記録媒体に記録する処理を実行する記録装置が実行してもよいし、サーバ側が実行する構成としてもよい。サーバに対して、ディスクに既に記録されているＣＰＳユニット番号を送信して、そのＣＰＳユニット番号とは重複しないＣＰＳユニット番号をサーバ側で決定し、この決定されたＣＰＳユニット番号（ＸＸＸＸ）に対応して、コンテンツ証明書のファイル名をサーバ側で決定して記録処理を実行する記録装置に通知する構成としてもよい。
【０１１０】
なお、コンテンツ証明書は少なくとも以下の情報を含む。
証明書タイプ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｔｙｐｅ）：コンテンツ証明書である事を示すための情報。
ハッシュユニット総数（Ｔｏｔａｌ＿Ｎｕｍｂｅｒ＿ｏｆ＿ＨａｓｈＵｎｉｔｓ）：コンテンツハッシュテーブル（ＣＨＴ）に格納された照合用ハッシュユニットの総数を示す情報。コンテンツハッシュテーブル（ＣＨＴ）については後述する。
ダイジェスト数（Ｎｕｍｂｅｒ＿ｏｆ＿Ｄｉｇｅｓｔｓ）：コンテンツ証明書対応のＣＰＳユニットに含まれるクリップ（Ｃｌｉｐ）の総数。
コンテンツ証明書識別子（Ｃｏｎｔｅｎｔ　Ｃｅｒｔｉｆｉｃａｔｅ　ＩＤ）：コンテンツ証明書のＩＤ。
【０１１１】
コンテンツリボケーションリスト（ＣＲＬ）バーション最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）：コンテンツに付随しているＣＲＬのバージョン番号の最小値。ディスクに記録されているＣＲＬのバージョンが、この値よりも小さい場合、ディスク記録コンテンツは違反コンテンツとみなされる。
ＭＣマニフェストファイルハッシュ値（Ｈａｓｈ＿Ｖａｌｕｅ＿ｏｆ＿ＭＣ＿Ｍａｎｉｆｅｓｔ＿Ｆｉｌｅ）：先に図１を参照して説明したコンテンツコピー処理（Ｍａｎａｇｅｄ　Ｃｏｐｙ）に適用するためにＲＯＭディスクに記録されるＭＣマニフェストファイルの正当性検証のためのＭａｎｉｆｅｓｔ　Ｆｉｌｅのハッシュ値。なお、マニフェストファイルについては後述する。
【０１１２】
ＢＤＪルート証明書ハッシュ値（Ｈａｓｈ＿Ｖａｌｕｅ＿ｏｆ＿ＢＤＪ＿Ｒｏｏｔ＿Ｃｅｒｔ）：コンテンツ利用アプリケーションの正当性検証に利用されるハッシュ値。
ＣＰＳユニット使用許諾情報ハッシュ値（Ｈａｓｈ＿Ｖａｌｕｅ＿ｏｆ＿ＣＰＳ＿Ｕｎｉｔ＿Ｕｓａｇｅ＿Ｆｉｌｅ）：ＣＰＳユニット使用許諾情報の正当性検証に適用するハッシュ値。
【０１１３】
コンテンツハッシュテーブル（ＣＨＴ）ダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ：コンテンツハッシュテーブルの該当Ｃｌｉｐ部分のハッシュ値。
バインド処理実行サーバ公開鍵リスト（Ｐｕｂｌｉｃ　Ｋｅｙ　ｏｆ　Ａｕｔｈｏｒｉｚｉｎｇ　Ｓｅｒｖｅｒ）：コンテンツの提供サーバ、あるいはコンテンツコピー処理に際して、サーバＩＤとメディアＩＤとのバインド処理を実行してトークンを生成する可能性のあるサーバの公開鍵一覧。複数のサーバの公開鍵のリストとしてよい。なお、コンテンツのコピー処理は先に図１を参照して説明したマネージドコピー（ＭＣ）処理であり、この処理については、後段で説明する。
電子署名（Ｓｉｇｎａｔｕｒｅ　Ｄａｔａ）：ルート認証局による電子署名。
【０１１４】
これらの情報を記録したコンテンツ証明書が、各ＣＰＳユニット単位に設定される。従って、ＣＰＳユニット単位のデータ記録をＲ／ＲＥディスクに対して実行する場合、その記録対象となるＣＰＳユニットに対応するコンテンツ証明書をコンテンツに併せて記録す

ることが可能となる。なお、ルート認証局は、コンテンツの管理を行なう最上位の認証局に相当する。

【０１１５】

次にコンテンツハッシュテーブル（ＣＨＴ）について説明する。コンテンツハッシュテーブルは、ディスクに記録されたコンテンツの正当性を検証するために適用されるテーブルであり、予め正当なコンテンツの構成データ（ハッシュユニット）に基づいて生成されたハッシュ値を格納したテーブルである。

【０１１６】

本発明の構成においては、ＣＰＳユニット対応のコンテンツ証明書を設定する構成であり、コンテンツハッシュテーブルもＣＰＳユニット単位で設定される。図９にコンテンツハッシュテーブルのデータ構成例を示す。コンテンツハッシュテーブルのファイル名は、例えば、［ContentHashXXXXX.tbl"（XXXXX:CPSユニット番号）］とする。すなわち、コンテンツハッシュテーブルのファイル名も同様に、対応するＣＰＳユニット番号を含ませるものとする。

【０１１７】

コンテンツハッシュテーブル（ＣＨＴ）には、
全クリップ数（ＮＣ）
全ハッシュユニット数（ＮＨ）
の各データに続いて、各クリップ（ｉ）について、
クリップ（ｉ）の先頭のハッシュユニット番号、
クリップ（ｉ）のファイル名対応の番号
の各データが記録され、さらに、
各クリップ毎、ハッシュユニット毎のハッシュ値（照合用ハッシュ値）としての［Ｈａｓｈ　Ｖａｌｕｅ］が記録される。

【０１１８】

ハッシュユニット毎のハッシュ値（照合用ハッシュ値）としての［Ｈａｓｈ　Ｖａｌｕｅ］は、正当なコンテンツの記録処理を実行する例えばディスク工場によって記録される。

全ハッシュユニット数（ＮＨ）は、例えば情報処理装置（再生装置）において、ハッシュ値算出、照合処理によるコンテンツ検証を実行する場合に、ランダムにハッシュユニット番号を選択する際に、その選択範囲としての数を取得する際に使用される。

【０１１９】

全ハッシュ番号に対してハッシュユニットを選択することによって、改ざん検出精度を上げることができる。ハッシュユニット数を適用せず、全クリップ番号からランダムにクリップ番号を選択し、選ばれたクリップ内からランダムにハッシュユニットを選択するという方法にすると、例えば、「極端に小さいサイズの改ざんされていないクリップファイル９９９個」と「改ざんされている大きいサイズのクリップファイル１つ」をディスクに記録した場合、改ざんが検出される可能性が低くなるが、全ハッシュ番号に対してハッシュユニットを選択する構成により、改ざん検出の可能性を高めることができる。

【０１２０】

クリップ（ｉ）の先頭のハッシュユニット番号は、ディスク上のクリップファイル（例えば最大１０００個）に対して、それぞれ０～ＮＣまで番号を与える。そして、各クリップファイルに属するハッシュユニットの（論理的に）先頭のハッシュユニットの全体における番号を記述する。

【０１２１】

情報記録媒体からのコンテンツ再生を実行する情報処理装置（再生装置）は、情報記録媒体再生時に情報記録媒体上のコンテンツの任意のハッシュユニットから計算されたハッシュ値とコンテンツハッシュテーブルに記載された照合用ハッシュ値を比較してコンテンツの改ざんの検証を行なうことが出来る。

【０１２２】

コンテンツハッシュテーブル（ＣＨＴ）の具体的構成について、図１０を参照して説明する。図１０（Ａ）は２つの記録レイヤー（Ｌａｙｅｒ０，１）を持つ情報記録媒体（ディスク）のデータ記録構成を示し、図１０（Ｂ）は、この記録データに対応するコンテンツハッシュテーブルの構成を示している。

【０１２３】

図１０（Ａ）に示す例は、２つの記録レイヤー（Ｌａｙｅｒ０，１）を持つ情報記録媒体（ディスク）に４つのクリップ（Ｃｌｉｐ０～３）が記録された例である。ハッシュユニットの総数（ＮＨ）は６４個である。クリップ０は、１６個のハッシュユニットを有し、これらの全てがレイヤー０に記録されている。クリップ１は、８個のハッシュユニットがレイヤー０に記録され、レイヤー１に１２個のハッシュユニットが記録されている。クリップ２は、８個のハッシュユニットがレイヤー０に記録され、レイヤー１に４個のハッシュユニットが記録されている。クリップ３は、１６個のハッシュユニットがレイヤー１に記録されたクリップである。

レイヤー０のハッシュユニット総数（Ｌ０＿ＮＨ）＝３２、

レイヤー１のハッシュユニット総数（Ｌ１＿ＮＨ）＝３２、

である。

【０１２４】

この構成において、コンテンツハッシュテーブル（ＣＨＴ）はレイヤー単位で設定され、２つのコンテンツハッシュテーブルが記録される。図１０（Ｂ）に示すのはコンテンツハッシュテーブルのヘッダとボディの各データを示している。（Ｂ１）は、レイヤー０のコンテンツハッシュテーブルのヘッダーデータであり、レイヤー０に含まれる各クリップ（Ｃｌｉｐ０～２）について、

クリップ（ｉ）の先頭のハッシュユニット番号＝Ｓｔａｒｔ、

クリップ（ｉ）のファイル名対応の番号＝Ｃｌｉｐ＃

の各値を格納している。

【０１２５】

（Ｂ２）は、レイヤー０のコンテンツハッシュテーブルのボディデータであり、レイヤー０に含まれる各ハッシュユニット（ハッシュ番号０～３１）の照合用ハッシュ値を格納している。

【０１２６】

（Ｂ３）は、レイヤー１のコンテンツハッシュテーブルのヘッダーデータであり、レイヤー１に含まれる各クリップ（Ｃｌｉｐ１～３）について、

クリップ（ｉ）の先頭のハッシュユニット番号＝Ｓｔａｒｔ、

クリップ（ｉ）のファイル名対応の番号＝Ｃｌｉｐ＃

【０１２７】

（Ｂ４）は、レイヤー１のコンテンツハッシュテーブルのボディデータであり、レイヤー１に含まれる各ハッシュユニット（ハッシュ番号３２～６３）の照合用ハッシュ値を格納している。

【０１２８】

情報記録媒体からのコンテンツ再生を実行する情報処理装置（再生装置）は、情報記録媒体再生時に情報記録媒体上のコンテンツの任意のハッシュユニットから計算されたハッシュ値とコンテンツハッシュテーブルに記載された照合用ハッシュ値を比較してコンテンツの改ざんの検証を行なう。これらの処理については、後段で説明する。

【０１２９】

図１１にコンテンツ中のクリップに設定されるハッシュユニット（ＨＵ）と、コンテンツハッシュテーブルに格納される照合用ハッシュ値としての［Ｈａｓｈ　Ｖａｌｕｅ］と、コンテンツ証明書に格納されるコンテンツハッシュテーブルダイジェストとの対応関係を示す。

【０１３０】

図１１に示すように、コンテンツ中のクリップに複数のハッシュユニット［ＨＵ］（例

えば１９２ＫＢ）が設定され、これらのハッシュユニット各々に基づくハッシュ値が照合用ハッシュ値［Ｈａｓｈ　Ｖａｌｕｅ］としてコンテンツハッシュテーブルに格納され、さらに、コンテンツハッシュテーブルに格納された各クリップ単位の複数の照合用ハッシュ値［Ｈａｓｈ　Ｖａｌｕｅ］に基づく新たなハッシュ値が算出され、これがハッシュダイジェストとしてコンテンツ証明書に登録されることになる。すなわちハッシュダイジェストは、情報記録媒体に記録されるコンテンツ（ＣＰＳユニット）毎に設定されるハッシュ値となる。

【０１３１】

コンテンツハッシュテーブルは、例えばコンテンツ再生を実行する装置において、コンテンツの改ざん検証処理に適用される。例えば、再生対象コンテンツに設定されたハッシュユニットを選択して、予め定められたハッシュ値算出アルゴリズムに従ってハッシュ値を算出し、この算出ハッシュ値が、コンテンツハッシュテーブルに登録されたコンテンツハッシュと一致するか否かによって、コンテンツが改ざんされているか否かを判定する処理を行なう。

【０１３２】

次に、図３に戻り、コンテンツサーバ１１０の処理について説明する。上述した情報記録媒体１３０に記録された各種のデータ中、メディア識別子１３２は、情報記録媒体１３０の製造時に例えば物理的なカッティング処理などによって記録されているが、その他のデータは、コンテンツの記録時に、コンテンツサーバ１１０によって提供されて記録される。

【０１３３】

図３に示すように、コンテンツサーバ１１０は、ＭＫＢ１１１、トークン１１３、ＣＰＳユニット鍵ファイル１１４、使用許諾情報（ＣＣＩ）１１５、証明書データ（ＣＨＴ／ＣＣ／ＣＲＬ）１１６、暗号化コンテンツ１１７を保持、または逐次生成して、記録装置１２０を適用して情報記録媒体１３０に記録する処理を行なう。

【０１３４】

トークン１１３は、先に図６を参照して説明したように、情報記録媒体１３０に記録されたメディア識別子１３２等を含むデータに基づいて生成されたサーバの署名データ、すなわちバインド処理を実行するサーバの署名データを含むデータである。

【０１３５】

コンテンツサーバ１１０は、情報記録媒体１３０に記録されたメディア識別子１３２を取得し、その他のデータ、例えば、コンテンツ証明書（ＣＣ）等の証明書データＩＤ等を含めて、コンテンツサーバ１１０の保持するサーバ秘密鍵１１２を適用して、署名データを生成する。この処理が図３に示すコンテンツサーバ１１０の実行する処理ステップＳ１１のバインド処理である。

【０１３６】

ステップＳ１１のバインド処理によって生成されたトークン１１３と、その他のデータが記録装置１２０によって記録される。この結果として、情報記録媒体１３０には図に示すように、暗号化コンテンツ１３７の他の各データが記録されることになる。

【０１３７】

再生装置１４０は、コンテンツ再生に際して、図に示すステップＳ２１において、情報記録媒体１３０に記録された各データに基づく鍵生成処理、データ検証処理を実行し、暗号化コンテンツの復号に必要なＣＰＳユニット鍵を取得して、ステップＳ２２において、暗号化コンテンツの復号、再生を実行する。

【０１３８】

なお、ステップＳ２１の処理には、再生装置１４０の保持するデバイス鍵［Ｋｄ］１４１を利用してＭＫＢ１３１からメディア鍵［Ｋｍ］を取得する処理、ＣＰＳユニット鍵ファイル１３４に含まれる暗号化ユニット鍵の復号処理、証明書データ１３６に含まれるコンテンツ証明書（ＣＣ）の検証、コンテンツハッシュテーブル（ＣＨＴ）のハッシュ値を適用したコンテンツ検証処理、トークン１３３の検証処理等が含まれる。トークン１３３

の検証には、コンテンツサーバ１１０の公開鍵を適用した署名検証処理が含まれ、署名検証の成立が確認されることがコンテンツ再生の１つの条件となる。なお、Ｒ／ＲＥディスクとしての情報記録媒体１３０に記録されたコンテンツの再生シーケンスについては後段で説明する。

【０１３９】

図３を参照して説明したように、コンテンツサーバ１１０は、コンテンツの他、情報記録媒体１３０に記録するための様々な管理情報を提供し、記録装置１２０によって、これらの各種情報が情報記録媒体１３０に記録される。本発明の一実施例の構成では、

コンテンツ証明書、

トークン、

使用許諾情報、

これらのデータをＣＰＳユニット単位で設定することを特徴としている。

これらのデータをＣＰＳユニット単位で設定することで、Ｒ／ＲＥディスクなどのデータ追記可能なメディアに対するコンテンツの追記処理を効率的に行なうことが可能となる。

【０１４０】

すなわち、従来型のＡＡＣＳ規格では、コンテンツ証明書はディスク、あるいはディスクの１レイヤーに対して１つの設定となっていたため、新たなコンテンツをディスクに追記するためには、コンテンツ証明書の全体的な書き換えを行なうことが必要となる。コンテンツ証明書には、先に図８を参照して説明したように、コンテンツの管理を行なう最上位の認証局に相当するルート認証局の署名が設定されており、コンテンツ証明書のデータの更新を行なう場合には、更新データをルート認証局に送付して、新たなルート認証局の電子署名を設定してもらうという処理が必須となる。

【０１４１】

このような処理をコンテンツの追記毎に実行することは効率の低下を招く。すなわち、図１に示すようなＲＯＭディスクからのコンテンツコピーや、図２に示すコンテンツサーバからのコンテンツ追記毎にこのような処理を必須とした場合、データ記録処理以外の署名更新処理に要する時間が大きくなり、その間ユーザを待たせることになる。また、ルート認証局側の負荷も膨大になることが予測される。

【０１４２】

このような非効率性を排除するため、本発明の構成では、コンテンツ証明書をＣＰＳユニット単位で設定し、予めＣＰＳユニット単位のコンテンツ証明書をコンテンツ提供を実行するサーバが保持する設定としている。なお、後述するが、図１に示すＲＯＭディスクからＲ／ＲＥ型ディスクに対するコンテンツコピーに際しても、ＲＯＭディスクに記録されたコンテンツのＣＰＳユニット単位のコンテンツ証明書が記録されており、コンテンツコピー時には、コピー対象のコンテンツに含まれるＣＰＳユニットに対応するコンテンツ証明書をコンテンツに併せてコピーを行なうのみでよい構成としている。トークンや使用許諾情報についても同様であり、コンテンツを構成するＣＰＳユニット単位のトークン、および使用許諾情報を設定して、コンテンツ記録処理時におけるトークン、使用許諾情報の生成、記録処理を効率的に行なうことを可能としている。

【０１４３】

図３に示す構成では、Ｒ／ＲＥ型ディスクのようなデータ記録可能な情報記録媒体１３０に対して、サーバからコンテンツを記録する全体処理について説明した。次に、図１２を参照して、既に、何らかのコンテンツが記録され、記録コンテンツに対するＭＫＢや、管理情報が記録されているＲ／ＲＥディスクなどのメディアに対して、他のコンテンツを追記する場合の処理シーケンスについて、図１２を参照して説明する。

【０１４４】

図１２には、左から追記コンテンツを提供するコンテンツサーバ３３０、コンテンツサーバ３３０からのコンテンツ他の情報を受領して情報記録媒体３１０にデータ記録を実行する記録装置３４０と、情報記録媒体３１０を示している。情報記録媒体３１０は、例え

ばＲ／ＲＥディスクなどのデータ追記可能な記録メディアである。

【０１４５】

情報記録媒体３１０には、既にコンテンツが記録され、記録コンテンツに対応するＭＫＢ他の管理情報が記録済みである。なお、図に示す情報記録媒体３１０の記録データ中、新たに追記されるコンテンツは、ＣＰＳユニット＃２（暗号化コンテンツ）３２２である。すでに記録済みのコンテンツが、ＣＰＳユニット＃１（暗号化コンテンツ）３２１である。

【０１４６】

情報記録媒体３１０には、ＣＰＳユニット＃１（暗号化コンテンツ）３２１に対応する管理情報、ＭＫＢが既に記録されている。

ＣＰＳユニット＃１（暗号化コンテンツ）３２１に対応する管理データは、

コンテンツ証明書＃１，３１４、

使用許諾情報＃１，３１６、

トークン＃１，３１８、

である。

【０１４７】

新たに追記されるＣＰＳユニット＃２（暗号化コンテンツ）３２２に対応する管理データは、

コンテンツ証明書＃２，３１５、

使用許諾情報＃２，３１７、

トークン＃２，３１９、

であり、これらのデータは、サーバ３３０から新たに提供され情報記録媒体３１０に記録されることになる。

【０１４８】

なお、前述したように、コンテンツ管理ユニットの記録先である情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、新たに情報記録媒体に記録するコンテンツ管理ユニットのユニット識別子として、記録済みコンテンツ管理ユニットのユニット識別子と異なる固有のユニット識別子を設定する処理を実行し、コンテンツ証明書等のファイル名には、この固有のユニット識別情報を含むファイル名を設定する。なお、このユニット識別子の設定、ファイル名の設定は、記録装置、再生装置、またはサーバのいずれで実行してもよい。

【０１４９】

また、ＭＫＢ３１１は、逐次、更新されており、コンテンツの新たな追記の際には、更新された最新バージョンのＭＫＢがサーバから提供され、情報記録媒体３１０に記録済みの古いバージョンのＭＫＢと置き換えられる。

さらに、ＣＰＳユニット鍵ファイル３１３は、新たな記録コンテンツであるＣＰＳユニット＃２，３２２に対応するＣＰＳユニット鍵（タイトル鍵）を追加する更新処理がサーバ３３０において実行され、更新されたＣＰＳユニット鍵ファイル３１３が、情報記録媒体３１０に記録済みの古いＣＰＳユニット鍵ファイルに置きかえられて記録されることになる。

【０１５０】

図には、情報記録媒体３１０に新たに追記されるデータを太線枠で示し、更新のなされるデータを二重線で示している。その他のデータは、ＣＰＳユニット＃１，３２１の記録時から変更されないデータである。なお、メディア識別子３２０は固定データであり、変更されない。

【０１５１】

情報記録媒体３１０に、ＣＰＳユニット＃２（暗号化コンテンツ）３２２を新たに追記する場合に実行される処理について、以下説明する。

【０１５２】

（ＭＫＢの更新）

コンテンツサーバ３３０は、情報記録媒体３１０に記録済みのＭＫＢのバージョンを検証して、最新バージョンのＭＫＢでない場合は、最新バージョンの更新ＭＫＢ３３１を提供して、情報記録媒体に記録させる。

【０１５３】

（ＣＰＳユニット鍵ファイルの更新）

さらに、コンテンツサーバ３３０は、ＣＰＳユニット鍵ファイルに新たな記録コンテンツであるＣＰＳユニット＃２，３２２に対応するＣＰＳユニット鍵（タイトル鍵）を追加する処理を行なう。新たな追加鍵は、図に示すＣＰＳユニット鍵（タイトル鍵）３３３である。このＣＰＳユニット鍵を暗号化してＣＰＳユニット鍵ファイル中に追加して更新を行なう。

【０１５４】

なお、ＣＰＳユニット鍵ファイルの更新に際しては、ファイルに格納するＣＰＳユニット鍵を暗号化する処理が必要となる。コンテンツサーバ３３０は、この暗号化鍵（Ｋｐａ）の生成を行なう。この処理がステップＳ５１の処理である。ステップＳ５１において、メディア鍵３３２と、情報記録媒体３１０に記録済みのバインディングナンス３１２を適用した鍵生成処理（例えばＡＥＳアルゴリズムに従った鍵生成処理）を実行して、暗号化鍵［Ｋｐａ］を生成し、ステップＳ５２において、生成した暗号化鍵［Ｋｐａ］を適用して新たに追加するＣＰＳユニット鍵３３３の暗号化を実行して、ＣＰＳユニット鍵ファイルを更新して、記録装置３４０に出力して情報記録媒体３１０に書き込みを行なう。

【０１５５】

（コンテンツ証明書の追記）

コンテンツサーバ３３０は、情報記録媒体３１０に新たに追記するコンテンツであるＣＰＳユニット＃２に対応するコンテンツ証明書３３４を保持しており、このコンテンツ証明書３３４を記録装置３４０に出力して情報記録媒体３１０に書き込みを行なう。これが、情報記録媒体３１０の記録データとして示すコンテンツ証明書＃２，３１５である。

【０１５６】

コンテンツサーバ３３０は、各ＣＰＳユニットに対応するコンテンツ証明書を保持している。これらのコンテンツ証明書は、先に図８を参照して説明したデータ構成を有し、ＣＰＳユニットに含まれるハッシュユニット対応のハッシュ値を格納したハッシュテーブルのダイジェストを含み、ルート認証局の署名が付与された証明書である。コンテンツサーバ３３０は、新たに追記するコンテンツ（ＣＰＳユニット）に対応するコンテンツ証明書を選択して提供する。

【０１５７】

なお、図には示していないが、ＣＰＳユニット対応のコンテンツ証明書に併せてＣＰＳユニット対応のコンテンツハッシュテーブル（ＣＨＴ）もコンテンツサーバ３３０から記録装置３４０に出力されて情報記録媒体３１０に書き込まれる。

【０１５８】

（使用許諾情報の追記）

コンテンツサーバ３３０は、情報記録媒体３１０に新たに追記するコンテンツであるＣＰＳユニット＃２に対応する使用許諾情報３３５を保持している。コンテンツサーバ３３０は、ステップＳ５３において、使用許諾情報３３５に対して、サーバ秘密鍵３３６を適用した電子署名を実行して、記録装置３４０に出力して情報記録媒体３１０に書き込みを行なう。これが、情報記録媒体３１０の記録データとして示す使用許諾情報＃２，３１７である。

【０１５９】

コンテンツサーバ３３０は、各ＣＰＳユニットに対応する使用許諾情報を保持している。すなわち、各ＣＰＳユニット対応のコピー制限、利用制限を記述した情報である。コンテンツサーバ３３０は、新たに追記するコンテンツ（ＣＰＳユニット）に対応する使用許諾情報を選択して署名を付与して提供する。

【０１６０】

（トークンの追記）
コンテンツサーバ３３０は、情報記録媒体３１０に新たに追記するコンテンツであるＣＰＳユニット＃２に対応するトークンを生成して記録装置３４０に出力して情報記録媒体３１０に書き込みを行なう。トークンは、先に図６を参照して説明したように、メディア識別子やコンテンツ証明書のＩＤなどのデータに対応する署名データを含むデータである。

【０１６１】
コンテンツサーバ３３０は、ステップＳ５４において、情報記録媒体３１０に記録されているメディア識別子３２０を取得し、さらに、追記するＣＰＳユニットに対応するコンテンツ証明書３３４の識別子（ＩＤ）を入力してサーバ秘密鍵３３６を適用して電子署名データを生成し、この電子署名データを含むトークンを生成して、記録装置３４０に出力して情報記録媒体３１０に書き込みを行なう。これが、情報記録媒体３１０の記録データとして示すトークン＃２，３１９である。

【０１６２】
コンテンツサーバ３３０は、各ＣＰＳユニットに対応するトークンをＣＰＳユニットの追記毎に生成して追記ＣＰＳユニットに対応付けて情報記録媒体に記録させる処理を行なう。

【０１６３】
このように、コンテンツサーバ３３０は、情報記録媒体に対する新たなＣＰＳユニット（コンテンツ）の記録に際して、
（ａ）ＣＰＳユニット対応のコンテンツ証明書、
（ｂ）ＣＰＳユニット対応の使用許諾情報、
（ｃ）ＣＰＳユニット対応のトークン、
これら（ａ）～（ｃ）の管理情報の追記を実行し、
（ｄ）ＭＫＢ
（ｅ）ＣＰＳユニット鍵ファイル
これら（ｄ），（ｅ）の情報の更新処理を実行する。
これらの処理は、コンテンツサーバと記録装置間の処理として実行可能であり、ルート認証局の署名処理等、他のシステムやエンティティとの通信は不要であるので効率的で迅速な処理が可能となる。

【０１６４】
（２－２）メディア間のコピーによるコンテンツ記録処理（ＭＣ：Ｍａｎａｇｅｄ Ｃｏｐｙ）
次に、先に図１を参照して説明したメディア間のコピーによるコンテンツ記録処理（ＭＣ（Ｍａｎａｇｅｄ Ｃｏｐｙ））のシーケンスについて、図１３、図１４を参照して説明する。

【０１６５】
図１３には、左からコンテンツ記録済みのＲＯＭディスク４３０、ＲＯＭディスク４３０を再生する再生装置４４０、再生装置４４０の再生するコンテンツを入力して、データ記録可能なメディアであるＲ／ＲＥディスク４７０に記録する記録装置４６０、およびＲ／ＲＥディスク４７０、さらに、上部に、このコンテンツコピー処理の許可、管理データの提供処理を実行する管理サーバ（ＭＣサーバ）４５０を示している。

【０１６６】
このコンテンツコピー処理に際しても、前述のサーバを適用したコンテンツ記録処理と同様、コンテンツはＣＰＳユニット単位の利用制御がなされたコンテンツであり、
ＣＰＳユニット単位の
コンテンツ証明書、
トークン、
使用許諾情報、
が設定されている。ＲＯＭディスク４３０には、ＣＰＳユニット単位の利用制御がなさ

れたコンテンツが記録されており、記録されているＣＰＳユニットに対応するコンテンツ証明書、トークン、使用許諾情報も併せて記録されている。なお、これらのデータは、図に示す管理データ４３２に含まれる。

【０１６７】

ＲＯＭディスク４３０には、ＣＰＳユニット単位で利用管理のなされるコンテンツが暗号化コンテンツ４３３として記録されている。暗号化コンテンツはユニット単位の暗号化がなされている。ＲＯＭディスク４３０の記録情報として示す管理データ４３２は、ＡＡＣＳ(Advanced Access Content System)の規定する管理データであり、暗号化コンテンツ４３３の復号に適用する鍵（ユニット鍵）を格納したＣＰＳユニット鍵ファイル、使用許諾情報、コンテンツの正当性を示すコンテンツ証明書（ＣＣ：Ｃｏｎｔｅｎｔ　Ｃｅｒｔｉｆｉｃａｔｅ）、ＭＫＢ等を含むデータである。

【０１６８】

コピー処理管理ファイル（ＭＣＭＦ）４３１は、情報記録媒体に記録されたコンテンツのコピー処理を実行する際に適用するファイルであり、例えば、以下の情報を含むＸＭＬ記述データファイルである。

（ａ）コンテンツＩＤ：情報記録媒体（ＲＯＭディスク）に記録されたコンテンツを一意に示す識別子（ＩＤ）例えばコンテンツコード情報としてのＩＳＡＮナンバーが用いられる。

（ｂ）ＵＲＩ（ＵＲＬ）：コンテンツコピーを実行する際にコピーの許可、バインド処理よるトークンの生成などを実行する管理サーバ接続用の情報である。例えば図１に示す構成における管理サーバ６に対するアクセス情報であり、図１３に示す構成における管理サーバ４５０に対するアクセス情報である。

（ｃ）ディレクトリ名、ファイル名（Ｄｉｒｅｃｔｏｒｙ　Ｎａｍｅ／Ｆｉｌｅ　Ｎａｍｅ）コピー処理を許容するデータを記録したディレクトリ、ファイル名に関する情報である。

【０１６９】

ＲＯＭディスク４３０に記録されている暗号化コンテンツ４３３をＲ／ＲＥディスク４７０にコピーする場合、まず、再生装置４４０は、ＲＯＭディスク４３０に記録されているコピー処理管理ファイル（ＭＣＭＦ）４３１を適用して、管理サーバ４５０にアクセスを実行する。この際、コピー処理対象となるコンテンツに対応するコンテンツＩＤが管理サーバ４５０に送信される。

【０１７０】

管理サーバ４５０は、ステップＳ６１において、コンテンツＩＤに基づいて、処理許容リストを生成して、再生装置４４０に送信する。例えば、コンテンツコピーが許容されるか否か、コピー処理の料金などの情報からなるリストである。再生装置４４０は、許容処理リストをディスプレイに表示して、ステップＳ６２において、ユーザが実行する処理を選択すると、管理サーバ４５０との間で決済処理（ステップＳ６３）が実行され、ステップＳ６４で管理サーバが処理を許可して許可情報を再生装置４４０に送信する。

【０１７１】

再生装置４４０は、ステップＳ６５において、管理サーバ４５０から受信した許可情報４４２を適用して、ＲＯＭディスク４３０から読み込んだ管理データ４３２を、Ｒ／ＲＥディスク４７０に記録するコピーコンテンツ対応の管理データに変換する処理を実行する。例えば、コピーコンテンツ対応の暗号鍵（ユニット鍵）の追加や、使用許諾情報、コンテンツ証明書等をコピーコンテンツ対応のデータに変更する処理を行なう。これらのデータ変換に必要な情報は、許可情報に含まれる。変換された管理データは記録装置４６０に入力される。

【０１７２】

再生装置４４０は、さらに、ステップＳ６６において、ＲＯＭディスク４３０から暗号化コンテンツ４３３を読み取り、コピー情報を記録装置４６０に出力する。なお、必要に応じて、例えばフォーマット変換などのデータ変換を実行して出力する。

【０１７３】
次に、記録装置４６０の処理について説明する。記録装置４６０は、ステップＳ７１において、コンテンツのコピー先としてのＲ／ＲＥディスク４７０から、メディア識別子（シリアルナンバー）４７１を取得して管理サーバ４５０にアップロードする処理を実行する。
【０１７４】
管理サーバ４５０は、メディア識別子を受信して、ステップＳ７２のバインド処理を実行し、先に図６を参照して説明したトークンを生成する。すなわち、管理サーバ４５０の秘密鍵を適用して、メディア識別子等を含むデータに対する電子署名データを含むトークンを生成する。このトークンは、ＲＯＭディスク４３０からＲ／ＲＥディスク４７０にコピーされるＣＰＳユニット（コンテンツ）に対応するトークンとして設定されＲ／ＲＥディスク４７０に記録される。このように図１３に示す管理データ４５１にはトークンが含まれる。なお、管理データ４５１には、トークンの他、Ｒ／ＲＥディスク４７０に記録するコンテンツに対応する使用許諾情報、コンテンツ証明書や、ＭＫＢ、ＣＰＳユニット鍵ファイルを含めてもよい。
【０１７５】
ただし、使用許諾情報、コンテンツ証明書、ＭＫＢ、ＣＰＳユニット鍵ファイルについては、管理サーバ４５０から提供する管理データ４５１に含めてもよいし、ＲＯＭディスク４３０に記録されたＣＰＳユニット対応の使用許諾情報、コンテンツ証明書、ＭＫＢ、ＣＰＳユニット鍵ファイルを、適宜、変換してＲ／ＲＥディスク４７０に記録する構成としてもよい。記録装置４６０は、いずれかの態様で生成された管理データ４６１をＲ／ＲＥディスク４７０に記録する。
【０１７６】
結果として、Ｒ／ＲＥディスク４７０には、暗号化コンテンツ４７３と、この暗号化コンテンツ４７３に対応する管理情報４７２が記録される。メディア識別子４７１は、元々Ｒ／ＲＥディスク４７０に記録されているデータである。
【０１７７】
なお、管理データ４７２には、
ＭＫＢ、
ＣＰＳユニット鍵ファイル、
コンテンツ証明書（ＣＣ）、
コンテンツハッシュテーブル（ＣＨＴ）、
コンテンツリボケーションリスト（ＣＲＬ）、
トークン、
使用許諾情報、
これらのデータが含まれる。
【０１７８】
これらのデータ中、トークンは、コピー処理時に管理サーバ４５０の処理（ステップＳ７２）によって生成される。トークン以外のデータについては、管理サーバ４５０から提供するか、あるいはＲＯＭディスク４３０に記録されたデータを適宜、変換して記録するか、いずれかの態様において実行される。
【０１７９】
図１３に示す処理は、管理サーバ４５０におけるステップＳ７２のバインド処理（トークン生成）に適用するＲ／ＲＥディスク４７０のメディア識別子４７１を記録装置がＲ／ＲＥディスク４７０から読み取り、管理サーバ４５０に送信する処理例として説明したが、再生装置４４０側において、この処理を実行してもよい。この処理例を図１４に示す。
【０１８０】
図１４に示す処理例において、ステップＳ６１～Ｓ６６の処理は、図１３を参照して説明した処理と同様であり、説明を省略する。ステップＳ８１、ステップＳ８２の処理、すなわちＲ／ＲＥディスク４７０に記録されたメディア識別子４７１を読み取って管理サー

バ４５０に送信して、バインド処理、すなわち、トークンを生成する処理が、図１３を参照して説明した処理とは異なり、再生装置４４０側の処理として実行している。

【０１８１】

再生装置４４０は、ステップＳ８１において、コンテンツのコピー先としてのＲ／ＲＥディスク４７０から、メディア識別子（シリアルナンバー）４７１を取得して管理サーバ４５０にアップロードする処理を実行する。

【０１８２】

管理サーバ４５０は、再生装置４４０からメディア識別子を受信して、ステップＳ８２のバインド処理を実行し、先に図６を参照して説明したトークンを生成する。すなわち、管理サーバ４５０の秘密鍵を適用して、メディア識別子等を含むデータに対する電子署名データを含むトークンを生成する。このトークンは、ＲＯＭディスク４３０からＲ／ＲＥディスク４７０にコピーされるＣＰＳユニット（コンテンツ）に対応するトークンとして設定され、管理データ４５１に含められて、再生装置４４０において、ＲＯＭディスク４３０から読み取ったその他の管理データと併せた管理データ４４３として、記録装置４６０を介してＲ／ＲＥディスク４７０に記録される。

【０１８３】

このように図１４に示す処理例では、再生装置４４０と管理サーバ４５０間のデータ送受信等に基づいて管理データが生成されて記録装置４６０に供給され、Ｒ／Ｒｅディスク４７０に記録される。

【０１８４】

なお、この例においても、最終的にＲ／ＲＥディスク４７０に記録される管理データ４７２には、トークンの他、使用許諾情報、コンテンツ証明書、ＭＫＢ、ＣＰＳユニット鍵ファイル等が含まれる。

【０１８５】

本発明の構成では、前述したように、

コンテンツ証明書、

使用許諾情報、

トークン、

これらの管理データをＣＰＳユニット単位で設定した構成としている。従って、コンテンツのコピー処理に際しても、コピー対象のコンテンツ（ＣＰＳユニット）に対応する管理データを選択して、Ｒ／ＲＥディスクに記録することが可能となる。ＲＯＭディスクには、ＲＯＭディスクに記録されたコンテンツのＣＰＳユニット単位のコンテンツ証明書が記録されており、コンテンツコピー時には、コピー対象のコンテンツに含まれるＣＰＳユニットに対応するコンテンツ証明書をコンテンツに併せてコピーを行なうのみでよい。使用許諾情報についても同様である。なお、これらのデータについては、管理サーバ４５０が新たにＲ／ＲＥディスク４７０記録用のデータとしてトークンと併せて発行する構成としてもよい。

【０１８６】

ＲＯＭディスク４３０に記録されたＣＰＳユニット対応のコンテンツ証明書や、管理サーバ４５０が新たに発行するコンテンツ証明書には予めルート認証局の署名が付与されており、コピー処理時にルート認証局との通信を実行して署名を付与してもらうといった手続を行なう必要がなく、効率的に迅速なコピー処理が可能となる。

【０１８７】

このように、本発明の構成では、ＣＰＳユニット単位の各管理データ、すなわち、

コンテンツ証明書、

使用許諾情報、

トークン、

を設定した構成であり、ＣＰＳユニット単位の独立した処理が可能となる。

【０１８８】

次に、コンテツンコピー処理において、既にＲ／ＲＥディスクに記録されたコンテンツ

とその記録コンテンツに対応する管理データが記録されている場合に、さらに新たなコンテンツのコピー処理を行なう場合の処理例について、図１５を参照して説明する。

【０１８９】

図１５には、左からコピーコンテンツのソースとしてのＲＯＭディスク５５０、管理サーバ５３０、再生装置５６０、Ｒ／ＲＥディスク５１０にデータ記録を実行する記録装置５４０と、Ｒ／ＲＥディスク５１０を示している。

【０１９０】

Ｒ／ＲＥディスク５１０には、既にコンテンツが記録され、記録コンテンツに対応するＭＫＢ他の管理情報が記録済みである。なお、図に示すＲ／ＲＥディスク５１０の記録データ中、新たに追記されるコンテンツは、ＣＰＳユニット＃２（暗号化コンテンツ）５２２である。すでに記録済みのコンテンツが、ＣＰＳユニット＃１（暗号化コンテンツ）５２１である。

【０１９１】

Ｒ／ＲＥディスク５１０には、ＣＰＳユニット＃１（暗号化コンテンツ）５３２１に対応する管理情報、ＭＫＢが既に記録されている。

ＣＰＳユニット＃１（暗号化コンテンツ）５２１に対応する管理データは、

コンテンツ証明書＃１，５１４、

使用許諾情報＃１，５１６、

トークン＃１，５１８、

である。

【０１９２】

新たに追記されるＣＰＳユニット＃２（暗号化コンテンツ）５２２に対応する管理データは、

コンテンツ証明書＃２，５１５、

使用許諾情報＃２，５１７、

トークン＃２，５１９、

であり、これらのデータは、ＲＯＭディスク５５０、あるいは管理サーバ５３０から新たに提供されＲ／ＲＥディスク５１０に記録されることになる。

【０１９３】

なお、前述したように、コンテンツ管理ユニットの記録先である情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、新たに情報記録媒体に記録するコンテンツ管理ユニットのユニット識別子として、記録済みコンテンツ管理ユニットのユニット識別子と異なる固有のユニット識別子を設定する処理を実行し、コンテンツ証明書等のファイル名には、この固有のユニット識別情報を含むファイル名を設定する。なお、このユニット識別子の設定、ファイル名の設定は、再生装置、記録装置、またはサーバのいずれで実行してもよい。

【０１９４】

ＲＯＭディスク５５０に記録されたコンテンツ（ＣＰＳユニット）５５１～５５３中のＣＰＳユニット＃ｃ５５３がコピー対象のコンテンツであり、Ｒ／ＲＥディスク５１０のＣＰＳユニット＃２，５２２に対応する。ＲＯＭディスク５５０に記録されたＣＰＳユニット＃ｃ５５３と、管理データ５５４中のＣＰＳユニット＃ｃ５５３対応の係りデータが再生装置５６０によって読み取られて記録装置５４０を介してＲ／ＲＥディスク５１０に記録される手順は、先に図１４を参照して説明した処理と同様である。

【０１９５】

さらに、コンテンツの追加コピーの場合は、既にＲ／ＲＥディスク５１０に記録されている各種の各に情報の更新または追加記録処理が行われることになる。この処理は管理サーバ（ＭＣサーバ）５３０の処理として実行される。管理サーバ５３０との通信は、再生装置５６０、または記録装置５４０のいずれかにおいて実行する。

【０１９６】

Ｒ／ＲＥディスク５１０に、ＣＰＳユニット＃２（暗号化コンテンツ）５２２を、Ｒデ

ィスク５５０からコピーして新たに追記する場合に管理サーバ５３０の実行する処理について、以下説明する。

【０１９７】

（ＭＫＢの更新）

管理サーバ（ＭＣサーバ）５３０は、Ｒ／ＲＥディスク５１０に記録済みのＭＫＢのバージョンを検証して、最新バージョンのＭＫＢでない場合は、最新バージョンの更新ＭＫＢ５３１を提供して、情報記録媒体に記録させる。

【０１９８】

（ＣＰＳユニット鍵ファイルの更新）

さらに、管理サーバ（ＭＣサーバ）５３０は、ＣＰＳユニット鍵ファイルに新たな記録コンテンツであるＣＰＳユニット＃２，５２２に対応するＣＰＳユニット鍵（タイトル鍵）を追加する処理を行なう。新たな追加鍵は、図に示すＣＰＳユニット鍵（タイトル鍵）５３３である。このＣＰＳユニット鍵を暗号化してＣＰＳユニット鍵ファイル中に追加して更新を行なう。

【０１９９】

なお、ＣＰＳユニット鍵ファイルの更新に際しては、ファイルに格納するＣＰＳユニット鍵を暗号化する処理が必要となる。管理サーバ（ＭＣサーバ）５３０は、この暗号化鍵（Ｋｐａ）の生成を行なう。この処理がステップＳ９１の処理である。ステップＳ９１において、メディア鍵５３２と、Ｒ／ＲＥディスク５１０に記録済みのバインディングナンス５１２を適用した鍵生成処理（例えばＡＥＳアルゴリズムに従った鍵生成処理）を実行して、暗号化鍵［Ｋｐａ］を生成し、ステップＳ９２において、生成した暗号化鍵［Ｋｐａ］を適用して新たに追加するＣＰＳユニット鍵５３３の暗号化を実行して、ＣＰＳユニット鍵ファイルを更新して、記録装置５４０に出力してＲ／ＲＥディスク５１０に書き込みを行なう。

【０２００】

（コンテンツ証明書の追記）

管理サーバ（ＭＣサーバ）５３０は、Ｒ／ＲＥディスク５１０に新たに追記するコンテンツであるＣＰＳユニット＃２に対応するコンテンツ証明書５３４を保持しており、このコンテンツ証明書５３４を記録装置５４０に出力してＲ／ＲＥディスク５１０に書き込みを行なう。これが、Ｒ／ＲＥディスク５１０の記録データとして示すコンテンツ証明書＃２，５１５である。

【０２０１】

管理サーバ（ＭＣサーバ）５３０は、各ＣＰＳユニットに対応するコンテンツ証明書を保持している。これらのコンテンツ証明書は、先に図８を参照して説明したデータ構成を有し、ＣＰＳユニットに含まれるハッシュユニット対応のハッシュ値を格納したハッシュテーブルのダイジェストを含み、ルート認証局の署名が付与された証明書である。管理サーバ（ＭＣサーバ）５３０は、新たに追記するコンテンツ（ＣＰＳユニット）に対応するコンテンツ証明書を選択して提供する。

【０２０２】

なお、図には示していないが、ＣＰＳユニット対応のコンテンツ証明書に併せてＣＰＳユニット対応のコンテンツハッシュテーブル（ＣＨＴ）も管理サーバ（ＭＣサーバ）５３０から記録装置３４０に出力されてＲ／ＲＥディスク５１０に書き込まれる。

【０２０３】

（使用許諾情報の追記）

管理サーバ（ＭＣサーバ）５３０は、Ｒ／ＲＥディスク５１０に新たに追記するコンテンツであるＣＰＳユニット＃２に対応する使用許諾情報５３５を保持している。管理サーバ（ＭＣサーバ）５３０は、ステップＳ９３において、使用許諾情報３３５に対して、サーバ秘密鍵５３６を適用した電子署名を実行して、記録装置５４０に出力してＲ／ＲＥディスク５１０に書き込みを行なう。これが、Ｒ／ＲＥディスク５１０の記録データとして示す使用許諾情報＃２，５１７である。

【０２０４】
管理サーバ（ＭＣサーバ）５３０は、各ＣＰＳユニットに対応する使用許諾情報を保持している。すなわち、各ＣＰＳユニット対応のコピー制限、利用制限を記述した情報である。管理サーバ（ＭＣサーバ）５３０は、新たに追記するコンテンツ（ＣＰＳユニット）に対応する使用許諾情報を選択して署名を付与して提供する。
【０２０５】
（トークンの追記）
管理サーバ（ＭＣサーバ）５３０は、Ｒ／ＲＥディスク５１０に新たに追記するコンテンツであるＣＰＳユニット＃２に対応するトークンを生成して記録装置５４０に出力してＲ／ＲＥディスク５１０に書き込みを行なう。トークンは、先に図６を参照して説明したように、メディア識別子やコンテンツ証明書のＩＤなどのデータに対応する署名データを含むデータである。
【０２０６】
管理サーバ（ＭＣサーバ）５３０は、ステップＳ９４において、Ｒ／ＲＥディスク５１０に記録されているメディア識別子５２０を取得し、さらに、追記するＣＰＳユニットに対応するコンテンツ証明書５３４の識別子（ＩＤ）を入力してサーバ秘密鍵５３６を適用して電子署名データを生成し、この電子署名データを含むトークンを生成して、記録装置５４０に出力してＲ／ＲＥディスク５１０に書き込みを行なう。これが、Ｒ／ＲＥディスク５１０の記録データとして示すトークン＃２，５１９である。
【０２０７】
管理サーバ（ＭＣサーバ）５３０は、各ＣＰＳユニットに対応するトークンをＣＰＳユニットの追記毎に生成して追記ＣＰＳユニットに対応付けて情報記録媒体に記録させる処理を行なう。
【０２０８】
このように、管理サーバ（ＭＣサーバ）５３０は、情報記録媒体に対する新たなＣＰＳユニット（コンテンツ）の記録に際して、
（ａ）ＣＰＳユニット対応のコンテンツ証明書、
（ｂ）ＣＰＳユニット対応の使用許諾情報、
（ｃ）ＣＰＳユニット対応のトークン、
これら（ａ）～（ｃ）の管理情報の追記を実行し、
（ｄ）ＭＫＢ
（ｅ）ＣＰＳユニット鍵ファイル
これら（ｄ），（ｅ）の情報の更新処理を実行する。
これらの処理は、コンテンツサーバと記録装置間の処理として実行可能であり、ルート認証局の署名処理等、他のシステムやエンティティとの通信は不要であるので効率的で迅速な処理が可能となる。
【０２０９】
なお、Ｒディスク５５０に記録された管理情報５５４にもＣＰＳユニット単位の管理データとして、
（ａ）ＣＰＳユニット対応のコンテンツ証明書、
（ｂ）ＣＰＳユニット対応の使用許諾情報、
これらの情報が記録されているので、これらの情報をＲ／ＲＥディスク５１０に対する書き込み情報として利用する構成としてもよい。
【０２１０】
（２－３）ＣＰＳユニット対応の管理データを記録したディスクのディレクトリ例
上述したように、データの記録処理が可能なメディア、例えばＲ／ＲＥ型ディスクのようなメディアに対しては、任意のタイミングでＣＰＳユニット単位でコンテンツの追加記録が可能であり、ＣＰＳユニット単位でのコンテンツの追加記録に併せてＣＰＳユニット単位の管理データが記録され、また管理データの更新処理が実行されることになる。
【０２１１】

このような処理によって複数のＣＰＳユニット対応コンテンツと各ＣＰＳユニット対応の管理データが記録されたディスクの記録データに対応するディレクトリ構成例について、図１６を参照して説明する。

【０２１２】

図１６に示すディスクの記録データに対応するディレクトリは、大きく以下の２つのディレクトリに分割できる。

（Ａ）ＡＡＣＳディスレクトリ

（Ｂ）ＢＤＭＶディレクトリ

である。ＡＡＣＳディレクトリには、ＡＡＣＳ対応の各種の管理情報、鍵情報が記録され、ＢＤＭＶディレクトリには、コンテンツの実体情報が記録される。

【０２１３】

（Ｂ）ＢＤＭＶディレクトリには、先に、図４を参照して説明した階層構成に従った各ファイルが設定される。すなわち、

＊インデックスファイル［ｉｎｄｅｘ．ｂｄｍｖ］

＊ムービーオブジェクトファイル［ＭｏｖｉｅＯｂｊｅｃｔ．ｂｄｍｖ］

＊プレイリストファィル［ＰＬＡＹＬＩＳＴ］

＊クリップ情報ファイル［ＣＬＩＰＩＮＦ］

＊ＡＶストリームファィル［ＳＴＲＥＡＭ］

これらのデータファイルが設定される。

【０２１４】

一方、（Ａ）ＡＡＣＳディスレクトリには、ＡＡＣＳ対応の各種の管理情報、鍵情報が記録される。具体的には、

＊ＭＫＢファイル［ＭＫＢ＿ＲＯ．ｉｎｆ］

＊ＣＰＳユニット鍵ファイル［Ｕｎｉｙ＿Ｋｅｙ＿ＲＷ．ｉｎｆ］

＊ＣＰＳユニット対応使用許諾情報ファィル［ＣＰＳＵｎｉｔｎｎｎ．ｃｃｉ］

＊シーケンス鍵ブロックファイル［ＳＫＢｎ．ｉｎｆ］

＊セグメント鍵ファイル［Ｓｅｇｍｅｎｔ＿Ｋｅｙ．ｉｎｆ］

＊コピー処理管理ファイル［ＭＣＭＦ．ｘｍｌ］

＊コンテンツリボケーションリスト（ＣＲＬ）ファイル［ＣｏｎｔｅｎｔＲｅｖｏｃａｔｉｏｎ．ｌｓｔ］

＊コンテンツ証明書（ＣＣ）ファイル［Ｃｏｎｔｅｎｔｎｎｎ．ｃｅｒ］

＊コンテンツハッシュテーブル（ＣＨＴ）ファィル［ＣｏｎｔｅｎｔＨａｓｈｎｎｎ．ｔｂｌ］

＊トークンファイル［Ｔｏｋｅｎｎｎｎ．ｉｎｆ］

これらの管理情報ファィルおよび鍵ファィルが設定される。

【０２１５】

＊ＭＫＢファイル［ＭＫＢ＿ＲＯ．ｉｎｆ］

＊ＣＰＳユニット鍵ファイル［Ｕｎｉｙ＿Ｋｅｙ＿ＲＷ．ｉｎｆ］

これらの鍵ファイルは、１つのみ設定される。ただし、コンテンツの追加記録に際して、必要に応じてデータ更新がなされる。

【０２１６】

＊ＣＰＳユニット対応使用許諾情報ファイル［ＣＰＳＵｎｉｔｎｎｎ．ｃｃｉ］

このファイルは、情報記録媒体に記録されているＣＰＳユニットに対応して生成されるファイルである。

【０２１７】

＊シーケンス鍵ブロックファイル［ＳＫＢｎ．ｉｎｆ］

＊セグメント鍵ファイル［Ｓｅｇｍｅｎｔ＿Ｋｅｙ．ｉｎｆ］

これらのファイルは、特殊なコンテンツ暗号化を行っているコンテンツ（ＣＰＳユニット）を記録している場合に設定されるファイルであり、特殊なコンテンツの暗号化に適用する鍵情報を格納ファイルである。セグメント鍵ファイルは、情報記録媒体に格納された

コンテンツの一部を異なる暗号鍵で暗号化したセグメントデータの暗号鍵として適用されるセグメント鍵を記録したファイルである。
また、シーケンス鍵ブロックファイルは、セグメント鍵ファイルからセグメント鍵を取得するために必要とするシーケンス鍵情報を格納したファイルである。これらのファイルの格納情報についての詳細は後述する。

【０２１８】

＊コピー処理管理ファイル［ＭＣＭＦ．ｘｍｌ］
このファイルは、先に、図１３～図１５を参照して説明したＲＯＭディスクからのコンテンツコピーの際に適用するファルである。
＊コンテンツリボケーションリスト（ＣＲＬ）ファイル［ＣｏｎｔｅｎｔＲｅｖｏｃａｔｉｏｎ．ｌｓｔ］
このファイルは、無効コンテンツの識別子を設定したリストを格納したファイルである。

【０２１９】

＊コンテンツ証明書（ＣＣ）ファイル［Ｃｏｎｔｅｎｔｎｎｎ．ｃｅｒ］
＊コンテンツハッシュテーブル（ＣＨＴ）ファィル［ＣｏｎｔｅｎｔＨａｓｈｎｎｎ．ｔｂｌ］
＊トークンファイル［Ｔｏｋｅｎｎｎｎ．ｉｎｆ］
これらのファィルは、既に説明したように、
コンテンツ証明書はコンテンツの正当性を証明するためのファイル（図８参照）、
コンテンツハッシュテーブルは、コンテンツの正当性を確認するための照合用ハッシュ値を格納したファイル（図９～図１１参照）
トークンファイルは、メディアの識別子を含むデータに対するサーバ秘密鍵による署名データを含むファイル（図６参照）

【０２２０】

これらの情報中、
＊ＣＰＳユニット対応使用許諾情報ファィル［ＣＰＳＵｎｉｔｎｎｎ．ｃｃｉ］
＊コンテンツ証明書（ＣＣ）ファイル［Ｃｏｎｔｅｎｔｎｎｎ．ｃｅｒ］
＊コンテンツハッシュテーブル（ＣＨＴ）ファィル［ＣｏｎｔｅｎｔＨａｓｈｎｎｎ．ｔｂｌ］
＊トークンファイル［Ｔｏｋｅｎｎｎｎ．ｉｎｆ］
これらのファイルはＣＰＳユニット単位で個別に生成されるファイルである。

【０２２１】

次に、シーケンス鍵ブロックファイルに格納されるシーケンス鍵およびセグメント鍵ファイルに格納されるセグメント鍵について説明する。これらの鍵は、特殊なコンテンツ暗号化を行っているコンテンツ（ＣＰＳユニット）を記録している場合に設定されるファイルである。

【０２２２】

コンテンツは前述したようにＣＰＳユニット鍵によって暗号化されることが原則であるが、コンテンツをセグメント部と非セグメント部に区分して、非セグメント部をＣＰＳユニット鍵による暗号化データとし、セグメント部を複数の異なるバリエーションからなる構成として、各バリエーション毎に異なるセグメント鍵で暗号化した構成とする設定としたコンテンツがある。このようなコンテンツに利用される鍵がセグメント鍵、およびシーケンス鍵である。

【０２２３】

コンテンツ再生に際しては、複数のセグメント部から、特定のセグメントデータを選択して設定される特定のパス（シーケンス）に沿ったコンテンツ再生を行なうことになる。非セグメント部ではＣＰＳユニット鍵による復号処理を実行し、セグメント部は、セグメント鍵ファイルから取得可能なセグメント鍵によって復号処理を実行して、コンテンツ再生を行なう。

【０２２４】
コンテンツ再生処理を実行する情報処理装置は、非セグメント部対応のＣＰＳユニット鍵と、セグメント部に対応するセグメント鍵（Ｋｓｅｇ）を取得することが必要となる場合がある。セグメント鍵とシーケンス鍵の適用構成について、図１７以下を参照して説明する。

【０２２５】
図１７（ａ）は、情報記録媒体に格納されたコンテンツの構成を示している。時間軸ｔに沿ってコンテンツが再生されるものとする。コンテンツは、情報記録媒体に格納された複数（ｎ個）のシーケンス鍵ブロック（ＳＫＢ）から、各々求められる分類番号Ｘ１～Ｘｎによって、それぞれ選択されるｎ個のプレイリストＸ１～Ｘｎに対応するｎ個の再生区分に大きく分割されている。

【０２２６】
図に示す例では、ｎ＝６であり、６個のシーケンス鍵ブロック（ＳＫＢ）から、各々求められる分類番号Ｘ１～Ｘ６によって、それぞれ選択される６個のプレイリストＸ１～Ｘ６に対応する６個の再生区分に大きく分割されている。なお、ここでは、分類番号の識別情報Ｘ１～Ｘ６とプレイリストの識別情報Ｘ１～Ｘ６を同一の識別子Ｘ１～Ｘ６として示しているが、これは理解を容易にするための例であり、分類番号の識別情報Ｘ１～Ｘ６と、プレイリストの識別情報Ｘ１～Ｘ６は対応づけられていればよく、異なる識別情報を用いてもよい。

【０２２７】
各プレイリストは、再生パスを決定するプレイアイテムシーケンス列の設定情報であり、例えば図に示すプレイリストＸ１は、図に示すプレイリストＸ１対応のコンテンツ部分に示す矢印に従った再生パスからなるプレイリストである。プレイリストＸ２～Ｘ６についても、各対応コンテンツ部分における再生パスを規定する。コンテンツ再生を実行する情報処理装置は、情報記録媒体に格納された複数（ｎ個）のシーケンス鍵ブロック（ＳＫＢ）から、分類番号Ｘ１～Ｘｎを求め、求めた分類番号に従ってそれぞれ選択されるｎ個のプレイリストＸ１～Ｘｎを選択して、これらの複数のプレイリストＸ１～Ｘｎを順次、適用してコンテンツ再生を実行する。

【０２２８】
例えば、まず、プレイリストＸ１を適用したコンテンツ再生を実行する情報処理装置は、プレイリストＸ１に従って決定される再生パス、すなわち、図に示す矢印に従ったコンテンツ構成データ（プレイアイテム）を選択して再生を行なう。コンテンツは、図に示すようにセグメント部と非セグメント部に区分され、非セグメント部はＣＰＳユニット鍵によって暗号化され、セグメント部は複数のバリエーションからなり、それぞれが異なるセグメント鍵によって暗号化されたセグメントデータによって構成される。

【０２２９】
コンテンツ再生に際しては、非セグメント部ではＣＰＳユニット鍵による復号処理を実行し、セグメント部では、プレイリストによって規定される特定のセグメントデータを選択してセグメント鍵ファイルから取得されるセグメント鍵によって復号処理を実行して、コンテンツ再生を行なう。

【０２３０】
プレイリストＸ２～Ｘ６についても、同様、各プレイリストによって規定される再生パスに従った再生処理を実行する。

【０２３１】
図１８（ａ）は情報記録媒体に格納されたコンテンツの各プレイリスト対応の区分データ、例えば図１７に示すプレイリストＸ１に属するコンテンツの再生区分データ構成を示す図である。コンテンツ再生区分データ６００は、例えば、タイトル＝［○×物語］を構成する１つの映画コンテンツの一部、すなわち、１つのＳＫＢからも止められる分類番号によって、選択される１つのプレイリストに対応するコンテンツ再生区分データに相当する。

【０２３２】
このコンテンツ再生区分データ６００は、図に示すように、複数のセグメント部６０１と、複数の非セグメント部６０２によって構成される。図の左から右に再生データが再生時間に沿って格納されているものとする。コンテンツを再生する情報処理装置は、図に示すコンテンツ再生区分データ６００について、左から、非セグメント部とセグメント部を交互に再生することになる。非セグメント部６０２は、上述したＣＰＳユニット鍵（Ｋｕ）の取得処理によって再生可能なコンテンツ部分、すなわちすべての情報処理装置において共通するＣＰＳユニット鍵（Ｋｕ）が取得され、ＣＰＳユニット鍵（Ｋｕ）を適用した復号処理によって再生可能なコンテンツ部分である。
【０２３３】
一方、セグメント部６０１は、上述したＣＰＳユニット鍵（Ｋｕ）とは異なる鍵、すなわち、各セグメントの各バリエーションに応じたセグメント鍵（Ｋｓｅｇ）を取得して復号することが必要となる。１再生区分コンテンツデータあたりのセグメント数は、図に示すように、例えば０～１４の１５セグメントであり、これら複数のセグメント部６０１の各々は、０～１５の１６個のバリエーションを持つセグメントデータによって構成される。
【０２３４】
前述したように、コンテンツは複数（ｎ個）の再生区分データに分割されており、各再生区分データに１５セグメントが設定される場合、コンテンツ全体では、
ｎ×１５＝１５ｎ
のセグメントが設定される。
【０２３５】
各セグメント部６０１に含まれる１６個のセグメントデータは、いずれも同一のデータ（例えば映画の同一の数秒間の再生画像シーン）によって構成される。例えばセグメント０に含まれる１６個のバリエーションを持つセグメントデータは、セグメント０の前（図における左側）の非セグメント部６０２に続くシーンを格納している。
【０２３６】
セグメント０に含まれるバリエーション０～１５の１６個のセグメントデータはいずれも同一のシーンに対応するデータであるが、それぞれ異なるセグメント鍵［Ｋｓｅｇ（０，０）～Ｋｓｅｇ（０，１５）］を用いて暗号化されたデータである。
【０２３７】
なお、セグメント鍵Ｋｓｅｇ（ｘ，ｙ）として標記する場合、ｘ＝セグメント番号、ｙ＝バリエーション番号を示すものとする。すなわち、セグメント鍵Ｋｓｅｇ（ｘ，ｙ）は、セグメント番号＝ｘ、バリエーション番号ｙに対応するセグメント鍵である。図に示すセグメント０～１４に含まれる全てのセグメントデータ（１５×１６＝２４０個）は、各セグメントデータに対応して設定されたセグメント鍵［Ｋｓｅｇ（０，０）～Ｋｓ（１４，１５）］によって暗号化されたデータである。
【０２３８】
コンテンツ再生を行なう情報処理装置は、セグメント０に含まれるバリエーション０～１５の１６個のセグメントデータから選択される１つのセグメントデータのみを復号することができる。例えば、情報処理装置Ａは、セグメント鍵［Ｋｓｅｇ（０，０）～Ｋｓｅｇ（０，１５）］中の１つのセグメント鍵［Ｋｓｅｇ（０，０）］のみ取得可能であり、情報処理装置Ｂは、セグメント鍵［Ｋｓｅｇ（０，０）～Ｋｓｅｇ（０，１５）］中の１つのセグメント鍵［Ｋｓｅｇ（０，３）］のみ取得可能な設定となる。
【０２３９】
同様に、セグメント１に含まれるバリエーション０～１５の１６個のセグメントデータも共通シーンのデータを異なるセグメント鍵［Ｋｓｅｇ（１，０）～Ｋｓｅｇ（１，１５）］を用いて暗号化されたデータによって構成される。セグメント１に含まれるバリエーション０～１５の１６個のセグメントデータについても、情報処理装置は、セグメント１に含まれるバリエーション０～１５の１６個のセグメントデータから選択される１つのセ

グメントデータのみを復号することができる。例えば、情報処理装置Ａは、セグメント鍵［Ｋｓｅｇ（１，０）～Ｋｓｅｇ（１，１５）］中の１つのセグメント鍵［Ｋｓｅｇ（１，１）］のみ取得可能であり、情報処理装置Ｂは、セグメント鍵［Ｋｓｅｇ（１，０）～Ｋｓｅｇ（１，１５）］中の１つのセグメント鍵［Ｋｓｅｇ（１，３）］のみ取得可能となる。

【０２４０】

各情報処理装置は、コンテンツ再生処理に際して、情報記録媒体に格納されたシーケンス鍵ブロック（ＳＫＢ）から取得される分類番号に基づいて、プレイリストを選択して再生を実行する。

【０２４１】

各情報処理装置の再生可能なパスは、情報処理装置によって処理されるシーケンス鍵ブロック（ＳＫＢ）から取得される分類番号に基づいて選択されるプレイリストによって決定される。

【０２４２】

例えば、図１８（ａ）に矢印で示す再生パスは、それぞれプレイリスト０に対応する再生パス、プレイリスト１に対応する再生パスであり、これらは、情報処理装置によって処理されるシーケンス鍵ブロック（ＳＫＢ）から取得される分類番号に基づいて選択されるプレイリストによって規定されるプレイアイテムシーケンスに相当する。

【０２４３】

図に示す例では、プレイリスト０を選択した情報処理装置は、セグメント０ではバリエーション番号０のデータを選択し、セグメント１ではバリエーション番号１のデータを選択して、それぞれに対応するセグメント鍵を適用して復号を行なう。これは、図１８（ｂ）の（１）に示す再生シーケンスとなる。プレイリスト１を選択した情報処理装置は、セグメント０ではバリエーション番号３のデータを選択し、セグメント１ではバリエーション番号３のデータを選択して、それぞれに対応するセグメント鍵を適用して復号を行なう。これは、図１８（ｂ）の（２）に示す再生シーケンスとなる。非セグメント部は、すべての情報処理装置が共通の鍵（ＣＰＳユニット鍵（Ｋｕ））を取得して同一データの復号を行なう。

【０２４４】

セグメント数１５、バリエーション数１６の設定では、16^{15}の異なるパスの設定が可能となる。ＳＫＢ６個として、６個のプレイリストを組み合わせて再生を行なう１つのコンテンツでは、$16^{15\times 6}$の異なるパスの設定が可能となる。

【０２４５】

現実的には、１つのＳＫＢによって選択される１つのプレイリスト対応の再生区分において、16^{15}の異なるバージョン設定が可能となるが、以下では、１つのＳＫＢに対応して設定される１つの再生区分において、０～２５５の２５６種類のパス設定を行う例について説明する。

【０２４６】

図１８（ｂ）に示すように、あるコンテンツについて、バージョン０～バージョン２５５の２５６種類のバージョンを取得した情報処理装置は、それぞれ異なるパス０～パス２５５に従って再生を実行することになる。少なくともこれら２５６個のパスは異なる設定である。

【０２４７】

プレイリストの各々にどのようなパスを設定するかは、コンテンツの制作または編集サイドにおいて任意に設定可能であり、コンテンツに応じて、バージョン０～２５５の情報処理装置に適用するパスを任意に設定できる。

【０２４８】

１つの再生区分において２５６の再生パスを設定する場合、１つの再生区分において、２５６個のプレイリストを設定して、コンテンツデータにこれらのプレイリストを記録しておく。前述したように、１つのコンテンツには、各ＳＫＢが対応付けられた複数の再生

区分データが含まれる。ｎ個のＳＫＢ、すなわちＳＫＢ１～ＳＫＢｎがある場合、各ＳＫＢに対応して２５６個のプレイリストが設定されるので、１つのコンテンツに対応して準備されるプレイリストは、

ｎ×２５６＝２５６ｎ

の数のプレイリストとなる。

すなわち、１つのＳＫＢにより、再生装置を特定するための十分なプレイリストを用意しようとすると、バリエーション数のセグメント数乗個（上記の例では、２５６^{n}個）のプレイリストが必要となるが、複数のＳＫＢに分割することによって、より少ない数のプレイリストによって、多数の再生パスのバリエーションを設定することが可能となり、コンテンツの不正流出などに際して、不正流出コンテンツの再生パスを検証することで、コンテンツの不正流出元を特定することが可能となる。なお、コンテンツ再生を実行する情報処理装置は、再生区分データに対応するプレイリストを順次、選択するなどの処理を実行して、コンテンツ再生を行なう。これらのプレイリストの選択、コンテンツ再生処理例の詳細については、後述する。

【０２４９】

次に、情報記録媒体に格納されたシーケンス鍵ブロック（ＳＫＢ）の構成および処理について説明する。前述したように、情報記録媒体には、複数の異なるシーケンス鍵ブロック（ＳＫＢ）の集合としてのシーケンス鍵ブロック群（ＳＫＢ１～ＳＫＢｎ）が格納される。

【０２５０】

各シーケンス鍵ブロック（ＳＫＢ１～ＳＫＢｎ）は、再生パスを規定したプレイリストを選択するための分類番号（Ｖａｒｉａｎｔ　Ｎｏ．）や、セグメント鍵ファイルに暗号化されて格納されたセグメント鍵の復号取得に適用する情報（メディア鍵変数（Ｋｍｖ））などが格納され、コンテンツ再生処理を実行する情報処理装置は、各ＳＫＢから、これらの情報を取得する処理を実行する。

【０２５１】

図１９には、暗号鍵ブロックとしてのＭＫＢ（Media Key Block）６４１と、シーケンス鍵ブロック（ＳＫＢ）群６４２の格納された情報記録媒体６４０と、情報処理装置６５０の処理シーケンスを示している。情報記録媒体６４０には、暗号化コンテンツなど、先に図１を参照して説明した各種のデータが格納されているが、ここでは、ＭＫＢ、ＳＫＢの処理について説明するので、ＭＫＢ、ＳＫＢのみを示している。

【０２５２】

暗号鍵ブロックとしてのＭＫＢ（Media Key Block）６４１は、前述したように、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックとしてのＭＫＢ（Media Key Block）であり、情報処理装置６５０のメモリに格納されたデバイス鍵６５１を適用した処理によって、メディア鍵（Ｋｄ）を取り出すことができる。

【０２５３】

前述したように、情報処理装置が有効なライセンスを持つ場合にのみ、メディア鍵（Ｋｍ）の取得を可能とし、無効化（リボーク処理）されたユーザデバイスにおいては、メディア鍵（Ｋｍ）の取得が不可能となる。ライセンスエンティテイとしての管理センタはＭＫＢに格納する鍵情報の暗号化に用いるデバイス鍵の変更により、特定のユーザデバイスに格納されたデバイス鍵では復号できない、すなわちコンテンツ復号に必要なメディア鍵を取得できない構成を持つＭＫＢを生成することができる。従って、任意タイミングで不正デバイスを排除（リボーク）して、有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。

【０２５４】

シーケンス鍵ブロック（ＳＫＢ）群６４２は、複数のシーケンス鍵ブロック（ＳＫＢ１～ＳＫＢｎ）によって構成される。前述したように、各ＳＫＢは、それぞれコンテンツの区分データである各分割再生区間１～ｎに対応して設定され、ＳＫＢ１～ＳＫＢｎの処理

を実行して得られるプレイリスト指定情報としての分類番号などが取得可能なデータである。

【０２５５】

図に示す情報処理装置６５０の処理シーケンスについて説明する。まず、情報処理装置６５０は、自装置のメモリに格納されたデバイス鍵（Ｋｄ）を適用してステップＳ１０１においてＭＫＢ処理を実行してデバイス鍵（Ｋｄ）を取得する。情報処理装置６５０がリボークされた機器でない限り、ＭＫＢ処理に成功し、デバイス鍵（Ｋｄ）を取得することができる。情報処理装置６５０がリボークされた機器である場合、ＭＫＢ処理が失敗し、デバイス鍵（Ｋｄ）を取得することができない。この場合、その後の処理は実行できず、コンテンツ再生は不可能となる。

【０２５６】

情報処理装置６５０がリボークされた機器でなく、ＭＫＢ処理に成功してデバイス鍵（Ｋｄ）を取得すると、次に、ステップＳ１０２において、取得したデバイス鍵（Ｋｄ）と、情報処理装置に格納されたシーケンス鍵ファイルから取得したシーケンス鍵を適用してＳＫＢの処理を実行する。情報処理装置６５０は、デバイス鍵（Ｋｄ）とシーケンス鍵を適用したＳＫＢの処理によって、分類番号６６１と、メディア鍵変数（Ｋｍｖ）６６２を取得することができる。

【０２５７】

分類番号６６１は、前述したようにプレイリストの選択情報として利用される。メディア鍵変数（Ｋｍｖ）６６２は、選択したプレイリストによって規定される再生パスに含まれるセグメントの構成データの復号に適用するセグメント鍵を格納したセグメント鍵ファイルからのセグメント鍵取得に適用する情報として利用される。

【０２５８】

このように、シーケンス鍵、セグメント鍵は、コンテンツをセグメント部と非セグメント部に区分して、非セグメント部をＣＰＳユニット鍵による暗号化データとし、セグメント部を複数の異なるバリエーションからなる構成とした特殊な暗号化を行っているコンテンツに対応して設定される鍵である。

【０２５９】

なお、シーケンス鍵や、セグメント鍵を利用しないコンテンツもあり、このようなコンテンツについては、図１６に示す

＊シーケンス鍵ブロックファイル［ＳＫＢｎ．ｉｎｆ］

＊セグメント鍵ファイル［Ｓｅｇｍｅｎｔ＿Ｋｅｙ．ｉｎｆ］

これらの鍵ファイルは設定されない。

なお、コンテンツの一部、例えば映画コンテンツの一部データ領域にのみ、シーケンス鍵や、セグメント鍵を利用した設定としたコンテンツもあり、この場合には、これらの鍵ファイル、すなわち、

＊シーケンス鍵ブロックファイル［ＳＫＢｎ．ｉｎｆ］

＊セグメント鍵ファイル［Ｓｅｇｍｅｎｔ＿Ｋｅｙ．ｉｎｆ］

これらが設定される。

【０２６０】

［３．コンテンツ再生処理例について］

次に、Ｒ／ＲＥディスクなどの随時データ記録可能なメディアに対して記録したコンテンツを再生する再生装置における再生シーケンスについて説明する。再生シーケンスについて、以下の２つの再生例について順次説明する。

（３－１）ＳＫＢ（シーケンス鍵ブロック）を利用しない再生処理、

（３－２）ＳＫＢ（シーケンス鍵ブロック）を利用する再生処理、

【０２６１】

（３－１）ＳＫＢ（シーケンス鍵ブロック）を利用しない再生処理、

まず、ＳＫＢ（シーケンス鍵ブロック）を利用しない再生処理シーケンスについて、図２０を参照して説明する。

【０２６２】
まず、再生処理を実行する再生装置７２０は、メモリに格納しているデバイス鍵［Ｋｄ］７２１を読み出す。デバイス鍵７２１は、コンテンツ利用に関するライセンスを受けた情報処理装置に格納された秘密キーである。
【０２６３】
次に、情報処理装置７２０は、ステップＳ２０１において、デバイス鍵７２１を適用してＲ／ＲＥディスク等の情報記録媒体７１０に格納されたメディア鍵［Ｋｍ］を格納した暗号鍵ブロックであるＭＫＢ７１１の復号処理を実行して、メディア鍵［Ｋｍ］を取得する。ＭＫＢ（Media Key Block）７１１は、前述したようにブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。ＭＫＢ７１１は有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵［Ｋｍ］の取得を可能とした鍵情報ブロックである。ユーザデバイス（情報処理装置）が有効なライセンスを持つ場合にのみ、メディア鍵［Ｋｍ］の取得が可能であり、無効化（リボーク処理）されたユーザデバイスにおいては、メディア鍵［Ｋｍ］の取得が不可能となる。
【０２６４】
次に、ステップＳ２０２において、ステップＳ２０１におけるＭＫＢ処理で取得したメディア鍵Ｋｍと、情報記録媒体７１０から読み取ったバインディングナンス（Ｂｉｎｄｉｎｇ　Ｎｏｎｃｅ）７１２とに基づく暗号処理によって、ＣＰＳユニット鍵ファイルに格納されたユニット鍵（Ｋｔ）の暗号鍵［Ｋｐａ］を生成する。この鍵生成処理は、例えば、ＡＥＳ暗号アルゴリズムに従った処理として実行される。
【０２６５】
次に、ステップＳ２０３において、暗号鍵［Ｋｐａ］によって、情報記録媒体７１０から読み取ったＣＰＳユニット鍵ファイル７１３に格納された暗号化ユニット鍵の復号処理を行なう。ＣＰＳユニット鍵ファイル７１３は、各ＣＰＳユニットに対応して設定されるユニット鍵［Ｋｕｎ］を含むデータの暗号化データを格納したファイルである。
【０２６６】
ステップＳ２０３におけるＣＰＳユニット鍵ファイル７１３に格納された暗号化テデータの復号処理によって、
データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）
を取得する。データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）は、ユニット鍵［Ｋｕ＿ｎ］と使用許諾情報（ＣＣＩ）に基づいて生成されるデータであることを示す。
【０２６７】
ステップＳ２０４では、再生装置が保持するＡＡＣＳルート認証局公開鍵７２２を適用して、情報記録媒体７１０に記録されたコンテンツ証明書（ＣＣ）７１４の検証処理を実行する。ステップＳ２０４では、コンテンツ証明書（ＣＣ）の署名検証を実行してコンテンツ証明書７１４の正当性を確認し、正当性の確認されたコンテンツ証明書から、コンテンツ提供サーバ（Ｍｏｄ／ＥＳかサーバ）または管理サーバ（ＭＣサーバ）の公開鍵［ＡＳＰｕｂ］を取得する。
【０２６８】
なお、ステップＳ２０４では、正当性の確認されたコンテンツ証明書７１４に記録されたハッシュダイジェスト値に基づいてコンテンツハッシュテーブルの正当性を確認した後、コンテンツハッシュテーブルに格納されたハッシュ照合用データを適用して、コンテンツの正当性を確認する処理を実行する。コンテンツハッシュテーブル（ＣＨＴ）を適用したコンテンツの正当性確認処理については、後述する。
【０２６９】
さらに、ステップＳ２０５では、情報記録媒体７１０から読み取った使用許諾情報７１５に付与されている署名の検証を、ＡＡＣＳルート認証局公開鍵７２２を適用して実行し、使用許諾情報７１５の正当性を確認する。

【０２７０】
さらに、ステップＳ２０６では、ステップＳ２０４において正当性の確認されたコンテンツ証明書から取得した、コンテンツ提供サーバ（Ｍｏｄ／ＥＳかサーバ）または管理サーバ（ＭＣサーバ）の公開鍵［ＡＳＰｕｂ］を適用して、情報記録媒体７１０から読み取ったトークン７１６の署名の検証を実行し、トークンの正当性を確認し、トークンに格納されているメディア識別子と情報記録媒体７１０のメデイア識別子７１７の照合処理を実行して一致していることを確認する。
【０２７１】
その後、ステップＳ２０７において、ステップＳ２０３において生成したデータ、すなわち、
データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）、
に対して、情報記録媒体７１０から読み取った使用許諾情報（ＣＣＩ）７１５を適用した演算処理を実行して、ユニット鍵［Ｋｕ＿ｎ］を得る。
例えば、データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）が、ユニット鍵［Ｋｕ＿ｎ］と、使用許諾情報［ＣＣＩ］との排他論理和（ＸＯＲ）結果データである場合、再度、この演算結果に対して、情報記録媒体から読み取った使用許諾情報［ＣＣＩ］の排他論理和（ＸＯＲ）演算を実行することで、ユニット鍵［Ｋｕ＿ｎ］を取得することができる。
【０２７２】
次に、ステップＳ２０８において、情報記録媒体７１０から読み取った暗号化コンテンツとしてのＣＰＳユニット７１８に対して、ユニット鍵［Ｋｕ＿ｎ］を適用した復号処理（例えばＡＥＳ＿Ｄ）を実行し、さらに、例えばＭＰＥＧデコード、圧縮解除、スクランブル解除等、必要なデコード処理を実行して、コンテンツ７３１を取得する。
【０２７３】
この処理によって、情報記録媒体７１０に格納されたＣＰＳユニットとして管理される暗号化コンテンツが復号されて利用、すなわち再生することができる。
【０２７４】
なお、各検証処理ステップＳ２０４，Ｓ２０５、Ｓ２０６のいずれかにおいて、検証の不成立、すなわち情報記録媒体７１０に記録されたデータの正当性が確認されなかった場合は、処理は中止され、コンテンツの再生、利用は不可能となる。
【０２７５】
次に、ステップＳ２０４において実行するコンテンツハッシュテーブル（ＣＨＴ）を適用したコンテンツの正当性確認処理について、図２１、図２２を参照して説明する。なお、コンテンツハッシュテーブルを適用したコンテンツの正当性確認処理、すなわち、改竄検証処理の処理態様には２種類ある。
（ａ）ディスク上の全てのハッシュユニットから所定数のハッシュユニットをランダムに選択して照合を行なう方法
（ｂ）再生対象のＣＰＳュニットに含まれるハッシュユニットから所定数のハッシュユニットをランダムに選択して照合を行なう方法
これらの（ａ），（ｂ）の２種類の方法である。
【０２７６】
まず、（ａ）ディスク上の全てのハッシュユニットから所定数のハッシュユニットをランダムに選択して照合を行なう方法について、図２１を参照して説明する。再生装置７２０は、コンテンツを記録した情報記録媒体を装着し、コンテンツ再生に先立ち、再生予定のコンテンツに対応するハッシュユニットを選択して、ハッシュユニットに対して設定されたハッシュ値の照合を実行する。
【０２７７】
まず、ステップＳ３０１において、照合処理を実行するハッシュユニットを選択する。前述した説明から明らかなように、情報記録媒体の格納コンテンツは所定データ長（例えば１９２ＫＢ）のハッシュユニットに区分されている。再生装置７２０は、これらの多数のハッシュユニットから照合処理を実行するユニットの選択を実行する。照合処理の対象

として選択するハッシュユニットは、複数個（ｎ個）例えば３個のハッシュユニットをランダムに選択する。

【０２７８】

選択したハッシュユニットが、
ハッシュユニット＃１（ＣＰＳユニット＃１）
ハッシュユニット＃１２３４５（ＣＰＳユニット＃１）
ハッシュユニット＃２３４５（ＣＰＳユニット＃２）
であるとする。

【０２７９】

ステップＳ３０２では、選択されたハッシュユニットに対応するハッシュユニット対応データを情報記録媒体から読み取り、各選択ハッシュユニットのハッシュ値を算出する。算出ハッシュ値を、それぞれ、
ハッシュユニット＃１のハッシュ値＝ａａａ
ハッシュユニット＃１２３４５のハッシュ値＝ｂｂｂ
ハッシュユニット＃２３４５のハッシュ値＝ｃｃｃ
であるとする。

【０２８０】

一方、ステップＳ３０３、Ｓ３０４では、選択したハッシュユニットに対応するコンテンツハッシュテーブル上の照合用ハッシュ値を特定する処理を実行する。まず、ステップＳ３０３において選択ハッシュユニットに対応するクリップファイル番号に基づいてＣＰＳユニット番号を計算し、ステップＳ３０４において、ＣＰＳユニット番号に対応するコンテンツ証明書（ＣＣ）とコンテンツハッシュテーブル（ＣＨＴ）を特定する。ステップＳ３０５では特定したコンテンツハッシュテーブル（ＣＨＴ）からＳ３０１において選択した照合処理対象のコンテンツハッシュユニットの照合用ハッシュ値を読み取る。読み取った照合用ハッシュ値が、
ハッシュユニット＃１のハッシュ値＝ＡＡＡ
ハッシュユニット＃１２３４５のハッシュ値＝ＢＢＢ
ハッシュユニット＃２３４５のハッシュ値＝ＣＣＣ
であるとする。

【０２８１】

ステップＳ３０６では、ステップＳ３０２においてコンテンツのハッシュユニットに基づいて算出したハッシユ値と、コンテンツハッシュテーブル（ＣＨＴ）から読み取った照合用ハッシュ値との比較処理を実行する。すべての対応するハッシュユニットの算出ハッシュ値と照合用ハッシュ値とが一致した場合、すなわち、
ａａａ＝ＡＡＡ
ｂｂｂ＝ＢＢＢ
ｃｃｃ＝ＣＣＣ
が成立した場合は、コンテンツの改ざんが無いと判定し、コンテンツ再生が許容され、コンテンツの再生処理に移行する。

【０２８２】

一方、対応するハッシュユニットの算出ハッシュ値と照合用ハッシュ値とのいずれかの不一致が検出された場合、すなわち、
ａａａ≠ＡＡＡ
ｂｂｂ≠ＢＢＢ
ｃｃｃ≠ＣＣＣ
のいずれかが検出された場合は、コンテンツの改ざんが有ると判定し、コンテンツ再生を禁止し、その後のコンテンツ再生処理への移行を中止する。

【０２８３】

次に、（ｂ）再生対象のＣＰＳユニットに含まれるハッシュユニットから所定数のハッシュユニットをランダムに選択して照合を行なう方法について、図２２を参照して説明す

る。再生装置７２０は、コンテンツを記録した情報記録媒体を装着し、コンテンツ再生に先立ち、再生予定のコンテンツに対応するハッシュユニットを選択して、ハッシュユニットに対して設定されたハッシュ値の照合を実行する。

【０２８４】

まず、ステップＳ３２１において、再生するＣＰＳユニット番号（Ｘ）を決定し、ステップＳ３２２において、ＣＰＳユニット＃Ｘからハッシュユニットを選択する。ハッシュユニットは複数（ｍ個：例えば２個）をランダムに選択する。

【０２８５】

選択したハッシュユニットが、

ハッシュユニット＃１（ＣＰＳユニット＃Ｘ）

ハッシュユニット＃３４（ＣＰＳユニット＃Ｘ）

であるとする。

【０２８６】

ステップＳ３２３では、選択されたハッシュユニットに対応するハッシュユニット対応データを情報記録媒体から読み取り、各選択ハッシュユニットのハッシュ値を算出する。算出ハッシュ値を、それぞれ、

ハッシュユニット＃１のハッシュ値＝ａａａ

ハッシュユニット＃３４のハッシュ値＝ｂｂｂ

であるとする。

【０２８７】

一方、ステップＳ３２４では、選択したハッシュユニットに対応するコンテンツハッシュテーブル上の照合用ハッシュ値を特定する処理を実行する。すなわち、ＣＰＳユニット番号（Ｘ）に対応するコンテンツ証明書（ＣＣ）とコンテンツハッシュテーブル（ＣＨＴ）を特定する。ステップＳ３２５では特定したコンテンツハッシュテーブル（ＣＨＴ）からＳ３２２において選択した照合処理対象のコンテンツハッシュユニットの照合用ハッシュ値を読み取る。読み取った照合用ハッシュ値が、

ハッシュユニット＃１のハッシュ値＝ＡＡＡ

ハッシュユニット＃３４のハッシュ値＝ＢＢＢ

であるとする。

【０２８８】

ステップＳ３２６では、ステップＳ３２３においてコンテンツのハッシュユニットに基づいて算出したハッシユ値と、コンテンツハッシュテーブル（ＣＨＴ）から読み取った照合用ハッシュ値との比較処理を実行する。すべての対応するハッシュユニットの算出ハッシュ値と照合用ハッシュ値とが一致した場合、すなわち、

ａａａ＝ＡＡＡ

ｂｂｂ＝ＢＢＢ

が成立した場合は、コンテンツの改ざんが無いと判定し、コンテンツ再生が許容され、コンテンツの再生処理に移行する。

【０２８９】

一方、対応するハッシュユニットの算出ハッシュ値と照合用ハッシュ値とのいずれかの不一致が検出された場合、すなわち、

ａａａ≠ＡＡＡ

ｂｂｂ≠ＢＢＢ

のいずれかが検出された場合は、コンテンツの改ざんが有ると判定し、コンテンツ再生を禁止し、その後のコンテンツ再生処理への移行を中止する。

【０２９０】

このようにコンテンツの再生に際しては、コンテンツハッシュの検証を実行してコンテンツの改竄の有無に基づくコンテンツの正当性検証を行い、改ざんのない正当なコンテンツであることが確認されたことを条件としてコンンテンツ再生が許容される。

【０２９１】

（３－２）ＳＫＢ（シーケンス鍵ブロック）を利用した再生処理、

次に、先に説明したＳＫＢ（シーケンス鍵ブロック）を利用した再生処理シーケンスについて、図２３を参照して説明する。

【０２９２】

ＳＫＢ（シーケンス鍵ブロック）を利用した再生処理は、先に図１７～図１９を参照して説明したようにコンテンツをセグメント部と非セグメント部に分割して非セグメント部はＣＰＳユニット鍵を適用した暗号化データ、セグメント部は、複数の異なるバリエーションからなる構成として、各バリエーション毎に異なるセグメント鍵で暗号化した構成とする設定としたコンテンツを再生する処理である。コンテンツ再生に際しては、複数のセグメント部から、特定のセグメントデータを選択して設定される特定のパス（シーケンス）に沿ったコンテンツ再生を行なうことになる。すなわち、非セグメント部ではＣＰＳユニット鍵による復号処理を実行し、セグメント部は、セグメント鍵ファイルから取得可能なセグメント鍵によって復号処理を実行して、コンテンツ再生を行なう。

【０２９３】

図２３において、情報記録媒体７１０には、シーケンス鍵ブロック（ＳＫＢ）ファィル７４１、セグメント鍵ファイル７４２が記録されている。図２０と異なる処理は、ステップＳ２０１～Ｓ２０３において、ユニット鍵生成用データ［Ｋｔ］に加えてセグメント鍵［Ｋｓｅｇ］を算出する処理が行われる点である。

【０２９４】

ステップＳ２０１－２のＳＫＢ処理は、先に図１９を参照して説明した処理に相当する。ステップＳ２０１のＭＫＢ処理によって取得したデバイス鍵（Ｋｄ）と、情報処理装置に格納されたシーケンス鍵ファイル７２３から取得したシーケンス鍵を適用して情報記録媒体７１０に記録されたシーケンス鍵ブロック（ＳＫＢ）７４１の処理を実行してメディア鍵変数（Ｋｍｖ*）を取得する。再生装置７２０は、デバイス鍵（Ｋｄ）とシーケンス鍵を適用したＳＫＢの処理によって、分類番号と、メディア鍵変数（Ｋｍｖ）を取得することができる。

【０２９５】

分類番号は、前述したようにプレイリストの選択情報として利用される。メディア鍵変数（Ｋｍｖ*）は、選択したプレイリストによって規定される再生パスに含まれるセグメントの構成データの復号に適用するセグメント鍵を格納したセグメント鍵ファイルからのセグメント鍵取得に適用する情報として利用される。

【０２９６】

ステップＳ２０２～Ｓ２０３では、図２０の処理と同様、ＭＫＢから取得したメディア鍵［Ｋｍ］に基づいてユニット鍵生成用データ［Ｋｔ］の生成処理が実行され、これに併せて、ＳＫＢ処理において生成した分類番号と、メディア鍵変数（Ｋｍｖ）とに基づいて、セグメント鍵ファイル７４２からセグメント鍵［Ｋｓｅｇ］が取得される。

【０２９７】

ステップＳ２０８のコンテンツ復号処理に際しては、ＣＰＳユニット鍵とセグメント鍵を選択的に適用した復号処理が実行されてコンテンツ７３１を生成して出力する。

【０２９８】

［４．情報処理装置の機能、構成について］

次に、図２４～図２６を参照して、

（ａ）情報記録媒体（メディア）に対する記録コンテンツの出力を実行するサーバ（Ｍｏｄ／ＥＳＴサーバ）としての情報処理装置。

（ｂ）情報記録媒体（メディア）間のコンテンツコピーにおける管理処理を実行するサーバ（ＭＣサーバ）としての情報処理装置。

（ｃ）コンテンツ再生処理または記録処理の少なくともいずれかを実行する情報処理装置。

これらの各情報処理装置の機能、構成について説明する。

【０２９９】

（ａ）情報記録媒体（メディア）に対する記録コンテンツの出力を実行するサーバ（Ｍｏｄ／ＥＳＴサーバ）としての情報処理装置。

まず、情報記録媒体（メディア）に対する記録コンテンツの出力を実行するサーバ（Ｍｏｄ／ＥＳＴサーバ）としての情報処理装置の機能、構成について、図２４を参照して説明する。情報記録媒体（メディア）に対する記録コンテンツの出力を実行するサーバ（Ｍｏｄ／ＥＳＴサーバ）は、図２を参照して説明したサーバであり、具体的には、図３、図１２を参照して説明したシーケンスに従った処理を実行する。

【０３００】

すなわち、サーバ（Ｍｏｄ／ＥＳＴサーバ）は、情報記録媒体（メディア）に対する記録用データを出力する情報処理装置であり、図２４に示すように、

情報記録媒体に対する記録用データや鍵情報、処理プログラム等を格納した記憶部８０１と、情報記録媒体に対する記録用データを生成するデータ処理部８０２と、データ処理部の生成したデータを出力する出力部８０３を有する。記憶部８０１は、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、コンテンツ管理ユニットに対応するユニット対応使用許諾情報とを含むデータを格納している。

【０３０１】

記憶部８０１に格納されたコンテンツ証明書は、情報記録媒体（メディア）に対する記録用データを出力する情報処理装置に対応する公開鍵情報や、正当なコンテンツ管理ユニットに対応するハッシュ値を照合用ハッシュ値として格納したコンテンツハッシュテーブルのダイジェスト値を含み、外部機関の電子署名が設定されたコンテンツ証明書である。

【０３０２】

データ処理部８０２は、先に、図３、図１２を参照して説明した処理を実行する。すなわち、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報とユニット対応コンテンツ証明書の識別情報とを含むデータに対して、自装置対応の秘密鍵を適用して生成した電子署名データを含むユニット対応トークンを生成する。データ出力部８０３は、コンテンツ管理ユニットと、ユニット対応コンテンツ証明書と、ユニット対応使用許諾情報と、ユニット対応トークンを含むデータを情報記録媒体に対する記録データとして出力する処理を実行する。

【０３０３】

また、データ処理部８０２は、先に、図１２を参照して説明したように、コンテンツ管理ユニットの記録先である情報記録媒体に、既にコンテンツ管理ユニットおよび該コンテンツ管理ユニット対応の鍵情報ファイルが記録されている場合、該記録済みの鍵情報ファイルの更新処理を実行する。

【０３０４】

（ｂ）情報記録媒体（メディア）間のコンテンツコピーにおける管理処理を実行するサーバ（ＭＣサーバ）としての情報処理装置。

次に、図２５を参照して、情報記録媒体（メディア）間のコンテンツコピーにおける管理処理を実行するサーバ（ＭＣサーバ）としての情報処理装置の機能、構成について説明する。情報記録媒体（メディア）間のコンテンツコピーにおける管理処理を実行するサーバ（ＭＣサーバ）は、図１を参照して説明したサーバであり、具体的には、図１３～図１５を参照して説明したシーケンスに従った処理を実行する。

【０３０５】

すなわち、ＭＣサーバは、情報記録媒体（メディア）間のコンテンツのコピー記録処理に対する管理処理を実行する情報処理装置であり、図２５に示すように、コピー記録対象となるコンテンツ管理ユニットのユニット識別情報を入力するとともに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を入力する入力部８１１と、メディア識別情報を含むデータに基づく電子署名データを生成して、該電子署名データを含むコンテンツ管理ユニット対応のユニット対応トークンを生成するデータ処理部８１２と、ユニット対応トークンを情報記録媒体記録データとして出力する出力部

８１３と、鍵情報、処理プログラム等を格納した記憶部８１４を有する。

【０３０６】

データ処理部８１２は、メディア識別情報とコンテンツ管理ユニットに対応するユニット対応コンテンツ証明書の識別情報とを含むデータに対して、自装置対応の秘密鍵を適用して生成した電子署名データを含むユニット対応トークンを生成する処理を実行する。また、データ処理部８１２は、先に図１５を参照して説明したように、コンテンツ管理ユニットのコピー先である情報記録媒体に、既にコンテンツ管理ユニットおよび該コンテンツ管理ユニット対応の鍵情報ファイルが記録されている場合、記録済みの鍵情報ファイルの更新処理を実行する。

【０３０７】

（ｃ）コンテンツ再生処理または記録処理の少なくともいずれかを実行する情報処理装置。

次に、コンテンツの再生処理または記録処理の少なくともいずれかを実行する情報処理装置の機能、構成について、図２６を参照して説明する。この情報処理装置は、例えば、コンテンツのメデイア間コピー、サーバからの取得コンテンツの記録処理などを実行する。

【０３０８】

情報処理装置は、図２６に示すように、ユーザインタフェースおよびデータ出力部として機能するデータ入出力部８２１、データ処理部８２２、処理プログラム、鍵情報等を格納した記憶部８２３と、情報記録媒体８３０に対するデータ記録再生を実行する媒体ＩＦ８２４を有する。

【０３０９】

データ処理部８２２は、例えば、情報記録媒体８３０に対するコンテンツ記録処理を実行する場合、

利用管理単位として設定されたユニット単位のコンテンツ管理ユニットと、

コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、

コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、

コンテンツ管理ユニットの記録先である情報記録媒体８３０の識別情報であるメディア識別情報を含み、外部サーバの電子署名データを含むユニット対応トークンと、

を含むデータを情報記録媒体８３０に対する記録データとして取得または生成する処理を実行する。また、コンテンツ管理ユニットの記録先である情報記録媒体８３０に記録済みのコンテンツ管理ユニットがある場合には、新たに情報記録媒体８３０に記録するコンテンツ管理ユニットに対して、記録済みコンテンツ管理ユニットのユニット識別情報と異なる固有のユニット識別情報を設定する処理を実行する。さらに、新たに情報記録媒体８３０に記録するコンテンツ管理ユニットに対応するコンテンツ証明書のファイル名を、この固有のユニット識別情報を含むファイル名に設定する処理などを実行する。

【０３１０】

また、図２６に示す情報処理装置がコンテンツのコピー処理を実行する際の再生処理を実行する構成である場合、データ処理部８２２は、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを情報記録媒体８３０から読み出してデータ入出力部８２１を介して出力する構成であり、コンテンツコピー先である第２の情報記録媒体に記録済みのコンテンツ管理ユニットがある場合、該第２の情報記録媒体に新たに記録するコンテンツ管理ユニットに対して、該第２の情報記録媒体に記録済みのコンテンツ管理ユニットのユニット識別情報とは異なる新たな固有のユニット識別情報を設定する処理を実行する。さらに、データ処理部８２２は、情報記録媒体８３０から読み取られたコンテンツ管理ユニットに対応するユニット対応コンテンツ証明書を情報記録媒体８３０から取得して、データ入出力部８２１を介して記録データとして出力する。データ処理部８２２は、この出力するコンテンツ証明書のファイル名を、前述の新たな固有のユニット識別情報を含むファイル名に設定する。

【０３１１】

また、図２６に示す情報処理装置がコンテンツ再生を実行する装置である場合、データ処理部８２２は、利用管理単位として設定されたユニット単位のコンテンツ管理ユニットを取得して復号する処理を実行する。具体的には、先に図２０～図２３を参照して説明した処理を実行する。すなわち、コンテンツ管理ユニットに対応するユニット対応コンテンツ証明書と、コンテンツ管理ユニットに対応するユニット対応使用許諾情報と、情報記録媒体の識別情報であるメディア識別情報を含むデータに基づく電子署名データを含むユニット対応トークンを、情報記録媒体から取得し、取得データの正当性検証処理を実行し、正当性が確認されたことを条件としてコンテンツ管理ユニットの再生処理を実行する。すなわち、コンテンツ管理ユニットに対応する暗号鍵であるユニット鍵の生成処理を実行して、コンテンツ管理ユニットの復号処理を実行する。

【０３１２】

また、データ処理部８２２は、先に、図２１、図２２を参照して説明したように、コンテンツ証明書から、コンテンツに基づいて生成された照合用ハッシュ値を取得し、再生対象となるコンテンツ管理ユニットの構成データに基づいて生成したハッシュ値との照合処理を実行し、照合の成立を条件として、コンテンツ管理ユニットの再生処理を実行する。

【０３１３】

また、情報記録媒体に記録されたコンテンツが、同一再生データ部を異なるセグメント鍵で暗号化した複数のバリエーションデータからなるセグメント部を有するコンテンツである場合は、先に図２３を参照して説明したように、データ処理部８２２は、情報処理装置に応じて各セグメント部から選択されるバリエーションデータを含む再生許容パスに従ったデータを復号するセグメント鍵の生成を実行して、コンテンツ管理ユニットの復号処理を実行する。

【０３１４】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

【０３１５】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０３１６】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０３１７】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０３１８】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず

、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

【０３１９】

以上、説明したように、本発明の一実施例の構成によれば、Ｒ／ＲＥ型ディスクなどのデータ記録可能なメディアに対して利用管理対象コンテンツを記録する構成において、ユニット単位で利用管理のなされるコンテンツ管理ユニット（ＣＰＳユニット）単位の各種管理データ、すなわち、ユニット対応コンテンツ証明書、ユニット対応使用許諾情報、さらに、コンテンツ管理ユニットの記録先である情報記録媒体の識別情報であるメディア識別情報を含むデータに基づく電子署名データを含むユニット対応トークンを生成して、これらの管理データをコンテンツ管理ユニットとともに、Ｒ／ＲＥ型ディスクなどのメディアに記録する構成とした。この構成によれば、管理データがコンテンツ管理ユニット単位で予め設定されているので、コンテンツの追記処理などに際して、ユニット対応の管理データの取得、生成、記録処理を迅速に行なうことが可能となり、メディアに随時記録されるコンテンツ管理ユニット対応の利用管理を確実に効率的に行なうことが可能となる。

【図面の簡単な説明】

【０３２０】

【図１】本発明の適用可能なシステム例について説明する図である。

【図２】本発明の適用可能なシステム例について説明する図である。

【図３】コンテンツサーバの実行する処理、情報記録媒体の格納データの構成について説明する図である。

【図４】コンテンツのデータ構成例について説明する図である。

【図５】メディア固有データであるメディア識別子のデータ構成例について説明する図である。

【図６】メディア固有データであるトークンのデータ構成例について説明する図である。

【図７】ＣＰＳユニット鍵ファイルのデータ構成例について説明する図である。

【図８】コンテンツ証明書のデータ構成例について説明する図である。

【図９】コンテンツハッシュテーブルの構成について説明する図である。

【図１０】コンテンツハッシュテーブルの詳細構成について説明する図である。

【図１１】コンテンツ証明書およびコンテンツハッシュテーブルの構成について説明する図である。

【図１２】コンテンツサーバの処理例について説明する図である。

【図１３】コンテンツコピー処理を実行する際の処理、情報記録媒体の格納データの構成について説明する図である。

【図１４】コンテンツコピー処理を実行する際の処理、情報記録媒体の格納データの構成について説明する図である。

【図１５】コンテンツコピー処理を実行する際の処理、情報記録媒体の格納データの構成について説明する図である。

【図１６】コンテンツを格納した情報記録媒体の格納データの構成について説明する図である。

【図１７】情報記録媒体の格納データとしてのシーケンス鍵ブロック（ＳＫＢ）とプレイリストの対応、およびコンテンツに対するセグメント設定構成例について説明する図である。

【図１８】コンテンツに対するセグメント設定構成について説明する図である。

【図１９】シーケンス鍵ブロック（ＳＫＢ）のデータ構成、および情報処理装置におけるシーケンス鍵ブロック（ＳＫＢ）の処理について説明する図である。

【図２０】コンテンツ再生処理シーケンスについて説明する図である。

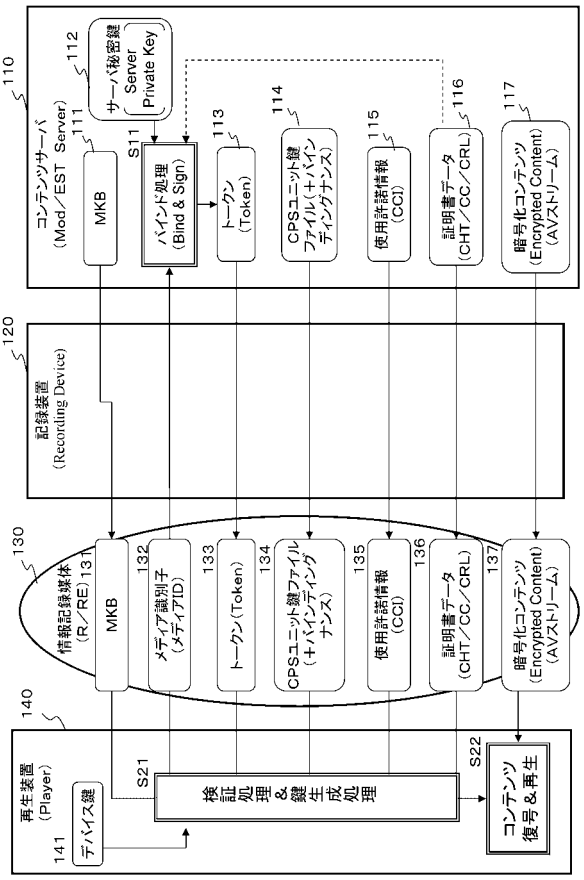
【図２１】コンテンツハッシュテーブルを適用したコンテンツ検証処理シーケンスについて説明する図である。

【図２２】コンテンツハッシュテーブルを適用したコンテンツ検証処理シーケンスについて説明する図である。
【図２３】コンテンツ再生処理シーケンスについて説明する図である。
【図２４】サーバの構成および機能について説明する図である。
【図２５】サーバの構成および機能について説明する図である。
【図２６】コンテンツ再生処理を実行する情報処理装置の構成および機能について説明する図である。
【符号の説明】
【０３２１】
１　ユーザ
２　ＲＯＭディスク
３　データ再生装置
４　データ記録装置
５　Ｒ／ＲＥディスク
６　管理サーバ
７　ネットワーク
１１　ユーザ
１２　情報記録媒体（メディア）
１３　情報処理装置
１４　コンテンツサーバ
１５　ネットワーク
２１　ユーザ
２２　情報記録媒体（メディア）
２３　コンビニ
２４　コンテンツサーバ
１１０　コンテンツサーバ
１１１　ＭＫＢ
１１２　サーバ秘密鍵
１１３　トークン
１１４　ＣＰＳユニット鍵ファイル
１１５　使用許諾情報
１１６　証明書データ
１１７　暗号化コンテンツ
１２０　記録装置
１３０　情報記録媒体
１３１　ＭＫＢ
１３２　メディア識別子
１３３　トークン
１３４　ＣＰＳユニット鍵ファイル
１３５　使用許諾情報
１３６　証明書データ
１３７　暗号化コンテンツ
１４０　再生装置
１４１　デバイス鍵
２１０　インデックス
２２０　ムービーオブジェクト
２３０　プレイリスト
２４０　クリップ
２６１，２６２，２６３　ＡＶストリーム
２７１，２７２　コンテンツ管理ユニット（ＣＰＳユニット）

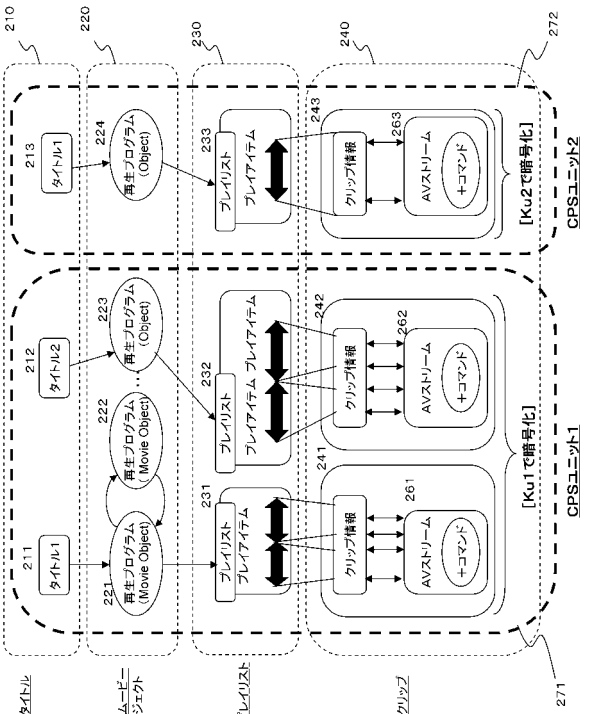
３１０　情報記録媒体
３１１　　ＭＫＢ
３１２　バインディングナンス
３１３　ＣＰＳユニット鍵ファイル
３１４，３１５　コンテンツ証明書
３１６，３１７　使用許諾情報
３１８，３１９　トークン
３２０　メディア識別子
３２１，３２２　ＣＰＳユニット
３３０　コンテンツサーバ
３３１　更新ＭＫＢ
３３２　メディア鍵
３３３　ＣＰＳユニット鍵
３３４　コンテンツ証明書
３３５　使用許諾情報
３３６　サーバ秘密鍵
３４０　記録装置
４３０　ＲＯＭディスク
４３１　コピー処理管理ファイル（ＭＣＭＦ）
４３２　管理データ
４３３　暗号化コンテンツ
４４０　再生装置
４４１　許容処理リスト
４４２　許可情報
４４３　管理データ
４５０　管理サーバ
４５１　管理データ
４６０　記録装置
４６１　管理データ
４６２　暗号化コンテンツ
４７０　Ｒ／ＲＥディスク
４７１　メディア識別子
４７２　管理データ
４７３　暗号化コンテンツ
５１０　情報記録媒体
５１１　ＭＫＢ
５１２　バインディングナンス
５１３　ＣＰＳユニット鍵ファイル
５１４，５１５　コンテンツ証明書
５１６，５１７　使用許諾情報
５１８，５１９　トークン
５２０　メディア識別子
５２１，５２２　ＣＰＳユニット
５３０　管理サーバ
５３１　更新ＭＫＢ
５３２　メディア鍵
５３３　ＣＰＳユニット鍵
５３４　コンテンツ証明書
５３５　使用許諾情報
５３６　サーバ秘密鍵

５４０　記録装置
５５０　ＲＯＭディスク
５５１～５５３　ＣＰＳユニット
５５４　管理データ
５５５　コピー処理管理ファィル（ＭＣＭＦ）
６００　コンテンツ再生区分データ
６０１　セグメント部
６０２　非セグメント部
６４０　情報記録媒体
６４１　ＭＫＢ（Media Key Block）
６４２　シーケンス鍵ブロック（ＳＫＢ）群
６５０　情報処理装置
６５１　デバイス鍵
６５２　シーケンス鍵ファイル
６６１　分類番号
６６２　メディア鍵変数
７１０　情報記録媒体
７１１　ＭＫＢ
７１２　バインディングナンス
７１３　ＣＰＳユニット鍵ファイル
７１４　コンテンツ証明書
７１５　使用許諾情報
７１６　トークン
７１７　メディア識別子
７１８　ＣＰＳユニット
７２０　再生装置
７２１　デバイス鍵
７２２　ＡＡＣＳルート認証局公開鍵
７３１　コンテンツ
７４１　ＳＫＢ
７４２　セグメント鍵ファイル
８０１　記憶部
８０２　データ処理部
８０３　データ入出力部
８１１　データ入力部
８１２　データ処理部
８１３　データ出力部
８１４　記憶部
８２１　データ入出力部
８２２　データ処理部
８２３　記憶部
８２４　媒体ＩＦ
８３０　情報記録媒体

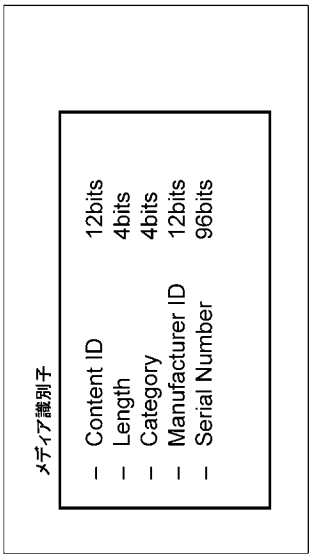
【図３】


110
コンテンツサーバ
(Mod／EST Server)
111
MKB
112
サーバ秘密鍵
Server Private Key
S11
バインド処理
(Bind & Sign)
113
トークン
(Token)
114
CPSユニット鍵
ファイル(+バインディングナンス)
115
使用許諾情報
(CCI)
116
証明書データ
(CHT／CC／CRL)
117
暗号化コンテンツ
(Encrypted Content)
(AVストリーム)
120
記録装置
(Recording Device)
130
情報記録媒体
(R／RE)131
MKB
132
メディア識別子
(メディアID)
133
トークン(Token)
134
CPSユニット鍵ファイル
(+バインディング
ナンス)
135
使用許諾情報
(CCI)
136
証明書データ
(CHT／CC／CRL)
137
暗号化コンテンツ
(Encrypted Content)
(AVストリーム)
140
再生装置
(Player)
141
デバイス鍵
S21
検証処理&鍵生成処理
S22
コンテンツ復号&再生

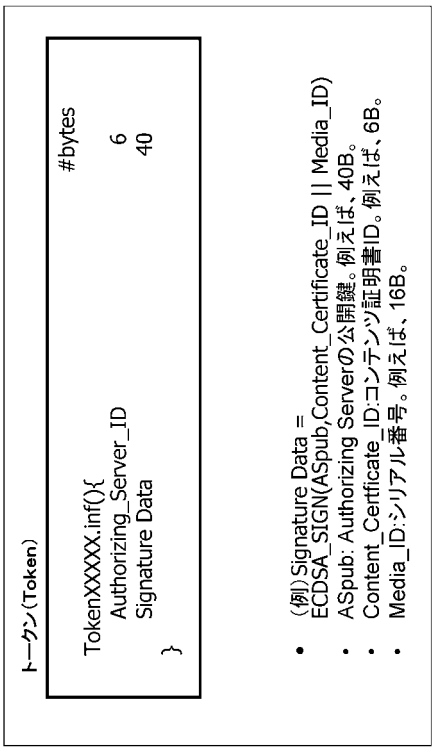
【図４】


210
220
230
240
272
213
タイトル1
224
再生プログラム
(Object)
233
プレイリスト
プレイアイテム
243
クリップ情報
263
AVストリーム
+コマンド
[Ku2で暗号化]
CPSユニット2
212
タイトル2
223
再生プログラム
(Object)
222
再生プログラム
(Movie Object)
232
プレイリスト
プレイアイテム プレイアイテム
242
クリップ情報
262
AVストリーム
+コマンド
211
タイトル1
221
再生プログラム
(Movie Object)
231
プレイリスト
プレイアイテム
241
クリップ情報
261
AVストリーム
+コマンド
[Ku1で暗号化]
CPSユニット1
271
(A)タイトル
(B)ムービーオブジェクト
(C)プレイリスト
(D)クリップ

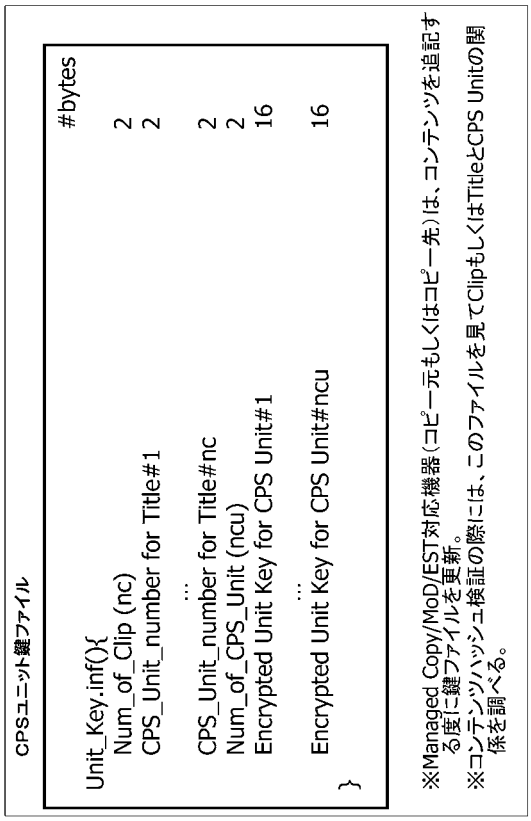
【図５】


メディア識別子
Content ID 12bits
Length 4bits
Category 4bits
Manufacturer ID 12bits
Serial Number 96bits

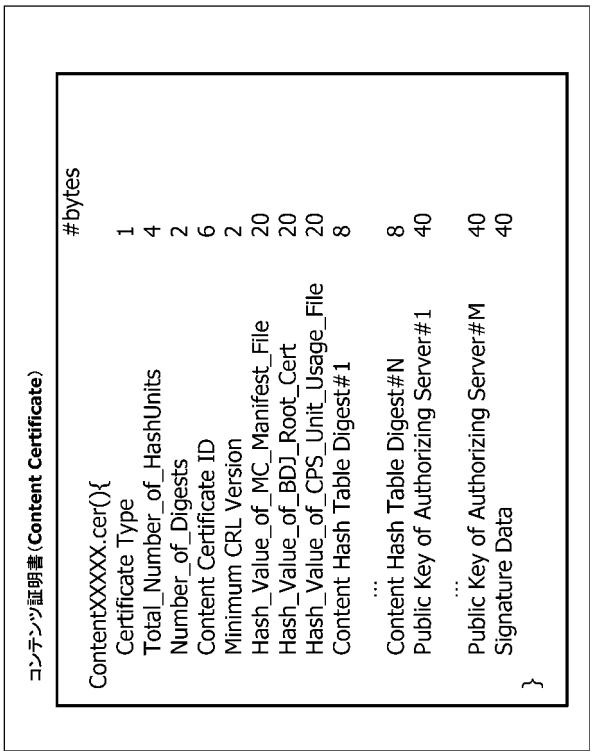
【図６】


トークン(Token)
TokenXXXXX.inf(){
Authorizing_Server_ID
Signature Data
}
#bytes
6
40
(例) Signature Data =
ECDSA_SIGN(ASpub,Content_Certificate_ID || Media_ID)
ASpub: Authorizing Serverの公開鍵。例えば、40B。
Content_Certificate_ID:コンテンツ証明書ID。例えば、6B。
Media_ID:シリアル番号。例えば、16B。

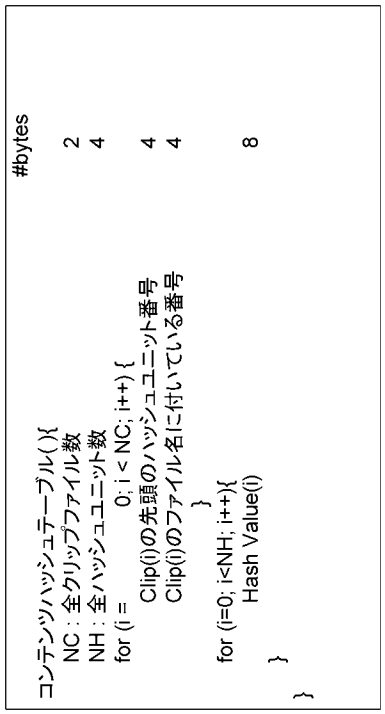
【図７】


CPSユニット鍵ファイル
#bytes
Unit_Key.inf(){
Num_of_Clip (nc) 2
CPS_Unit_number for Title#1 2
...
CPS_Unit_number for Title#nc 2
Num_of_CPS_Unit (ncu) 2
Encrypted Unit Key for CPS Unit#1 16
...
Encrypted Unit Key for CPS Unit#ncu 16
}
※Managed Copy/MoD/EST対応機器（コピー元もしくはコピー先）は、コンテンツを追記する度に鍵ファイルを更新。
※コンテンツハッシュ検証の際には、このファイルを見てClipもしくはTitleとCPS Unitの関係を調べる。

【図８】


コンテンツ証明書(Content Certificate)
#bytes
ContentXXXXX.cer(){
Certificate Type 1
Total_Number_of_HashUnits 4
Number_of_Digests 2
Content Certificate ID 6
Minimum CRL Version 2
Hash_Value_of_MC_Manifest_File 20
Hash_Value_of_BDJ_Root_Cert 20
Hash_Value_of_CPS_Unit_Usage_File 20
Content Hash Table Digest#1 8
...
Content Hash Table Digest#N 8
Public Key of Authorizing Server#1 40
...
Public Key of Authorizing Server#M 40
Signature Data 40
}

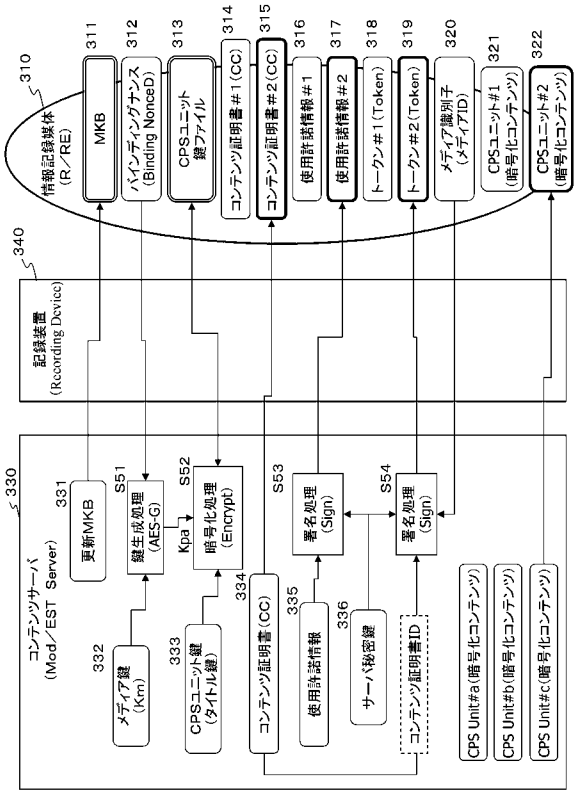
【図９】


#bytes
コンテンツハッシュテーブル(){
NC：全クリップファイル数 2
NH：全ハッシュユニット数 4
for (i = 0; i < NC; i++) {
Clip(i)の先頭のハッシュユニット番号 4
Clip(i)のファイル名に付いている番号 4
}
for (i=0; i<NH; i++){
Hash Value(i) 8
}
}

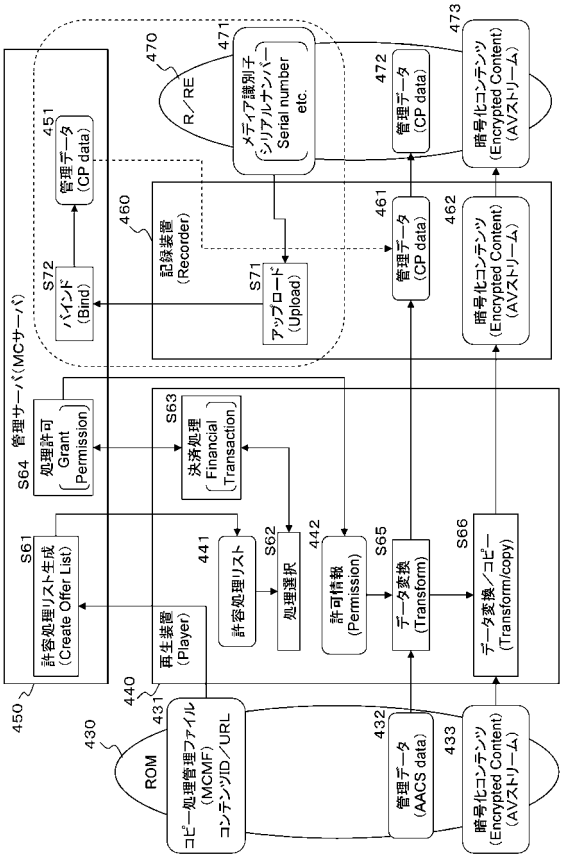
【図１１】

コンテンツ証明書
コンテンツハッシュテーブル
クリップファイル
Content001.cer
ContentHash001.tbl
Content Hash Table Digest #0
Content Hash Table Digest #2
Hash_Value #0
Hash_Value #1
Hash_Value #2
Hash_Value #3
Hash_Value #4
Hash_Value #5
Clip #0
HU#0
HU#1
Clip #1
HU#0
HU#1
HU#2
Clip #2
HU#0
Layer 0
Content002.cer
ContentHash002.tbl
Content Hash Table Digest #1
Content Hash Table Digest #3
Hash_Value #0
Hash_Value #1
Hash_Value #2
Hash_Value #3
Hash_Value #4
HU#2
HU#1
HU#2
Layer 1
Clip #3
HU#0
HU#1

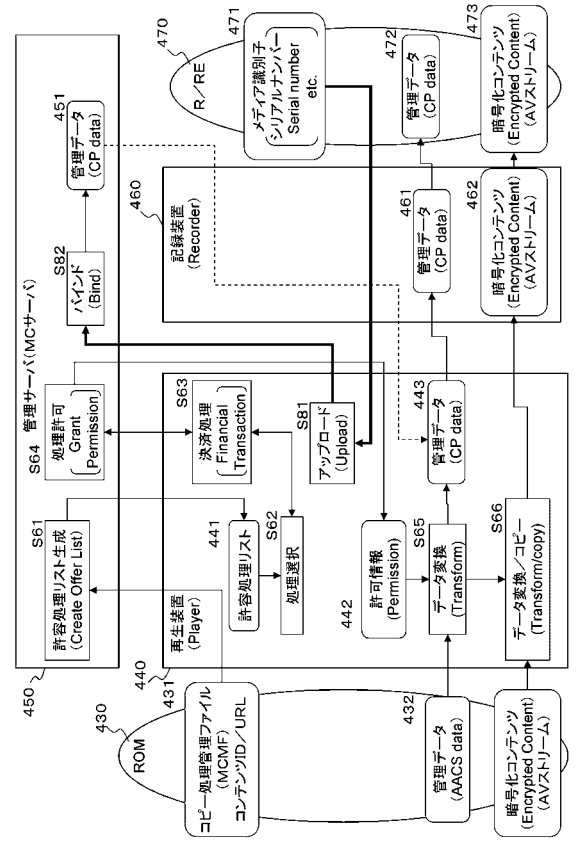
【図１２】



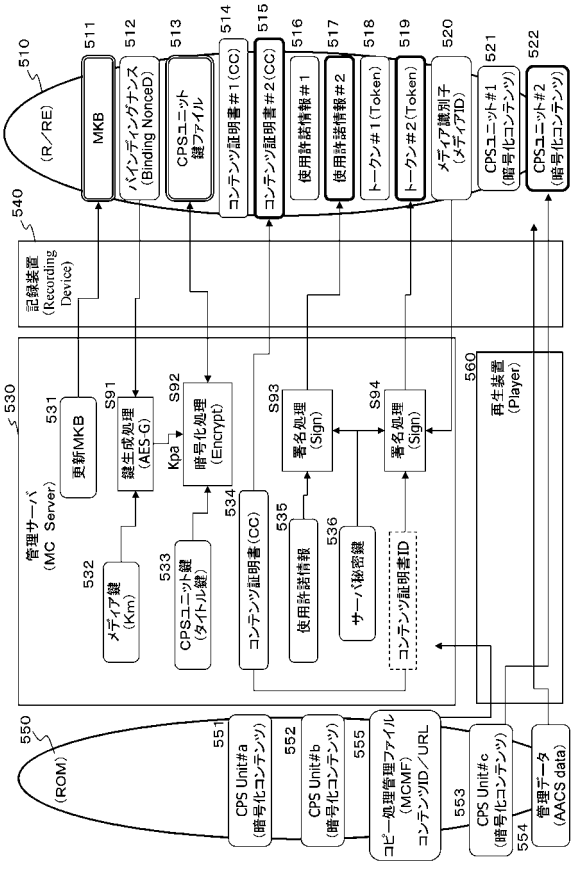
【図１３】



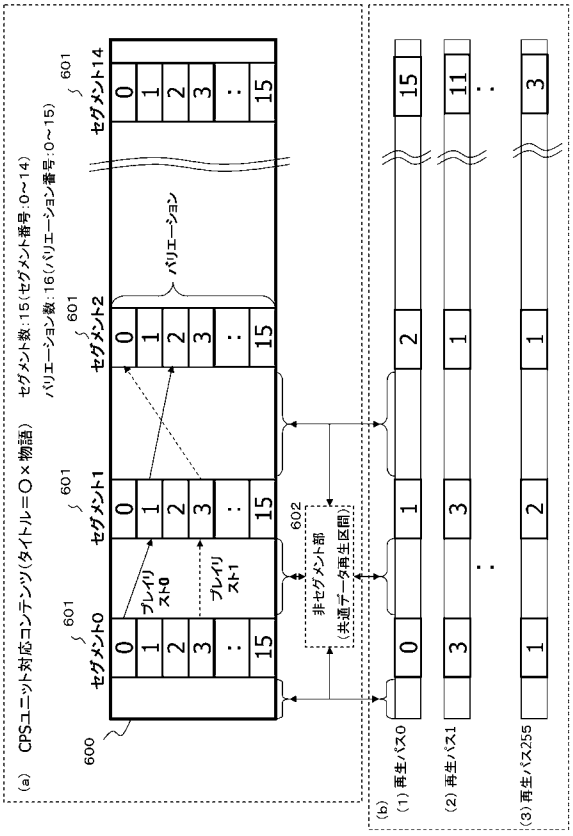
【図１４】



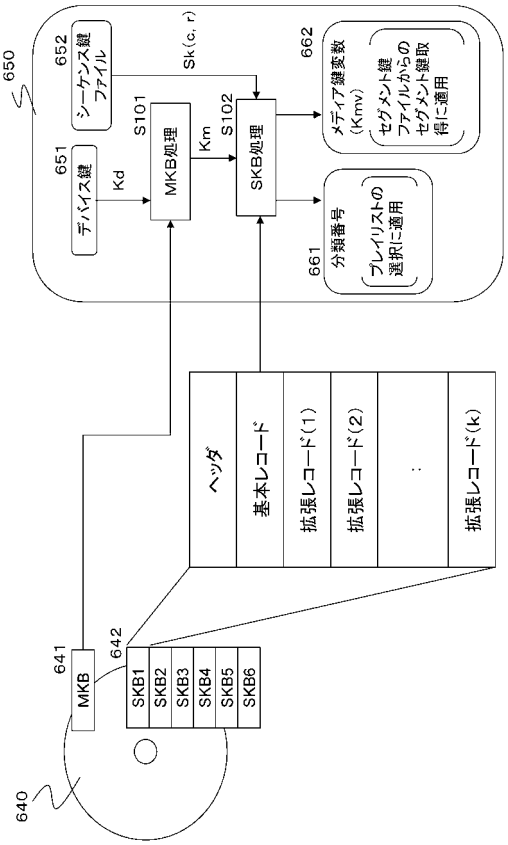
【図１５】



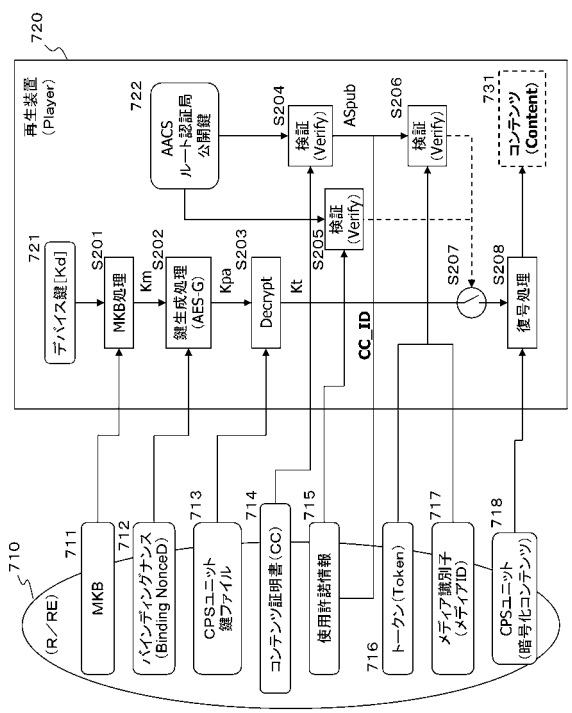
【図１８】



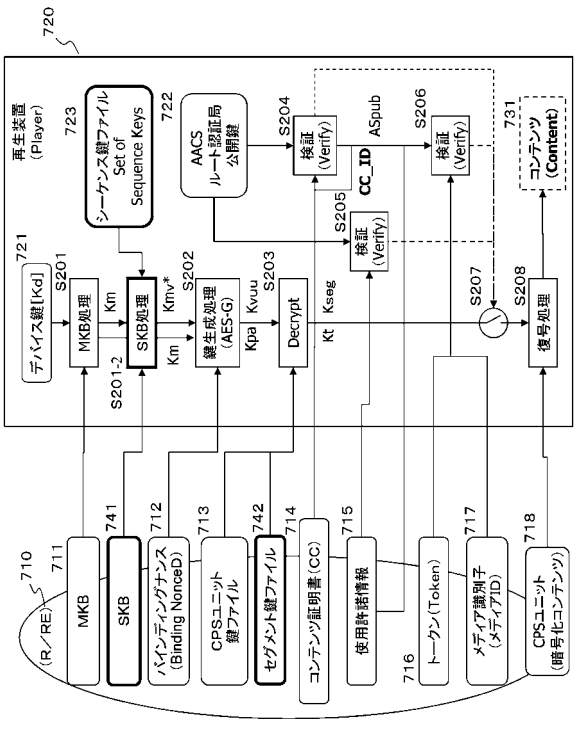
【図１９】



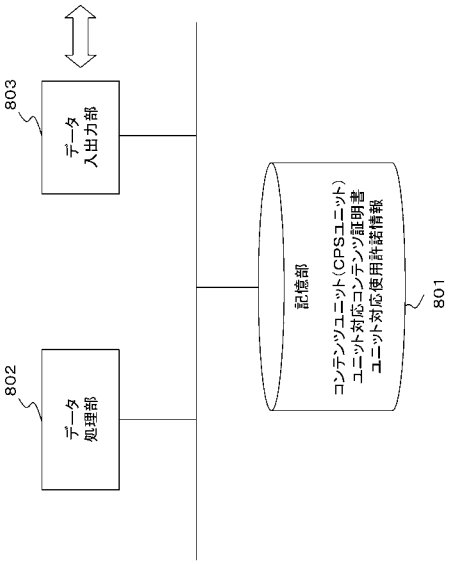
【図２０】



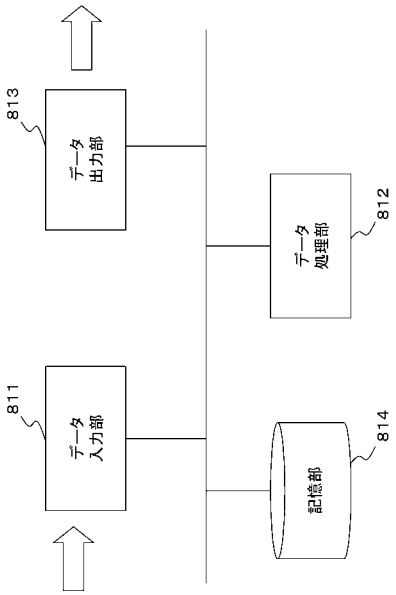
【図２３】



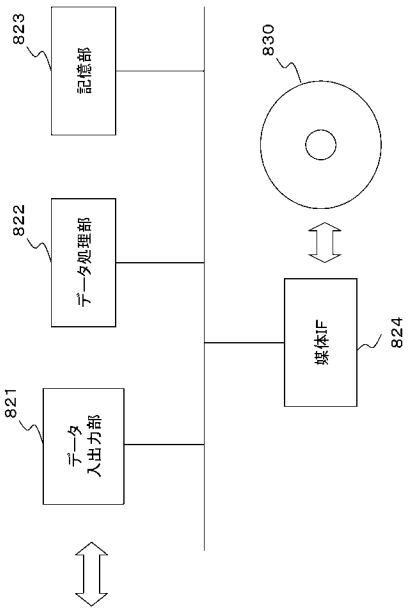
【図２４】


803
データ
入出力部
802
データ
処理部
記憶部
コンテンツユニット（CPSユニット）
ユニット対応コンテンツ証明書
ユニット対応使用許諾情報
801

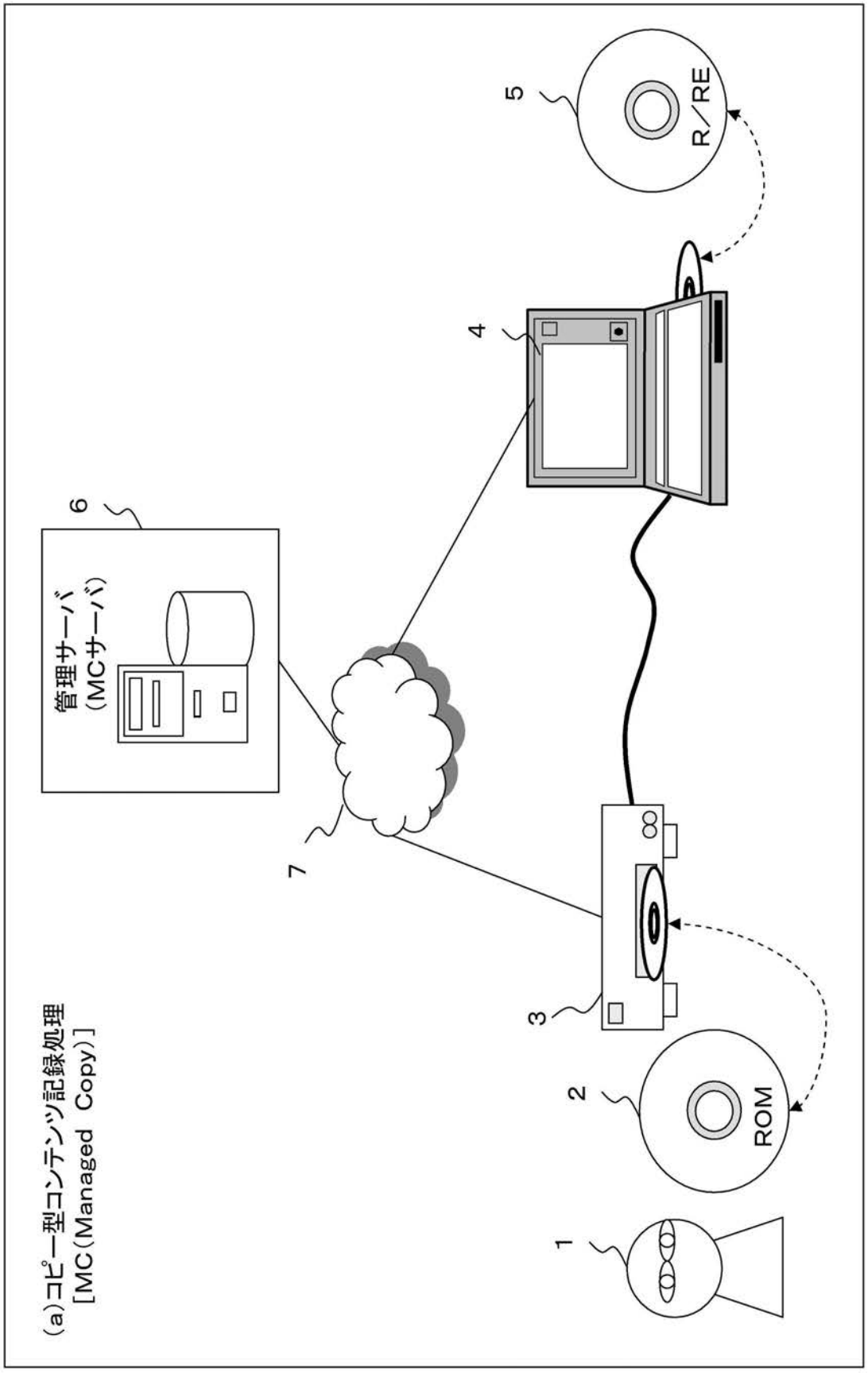
【図２５】


813
データ
出力部
811
データ
入力部
812
データ
処理部
814
記憶部

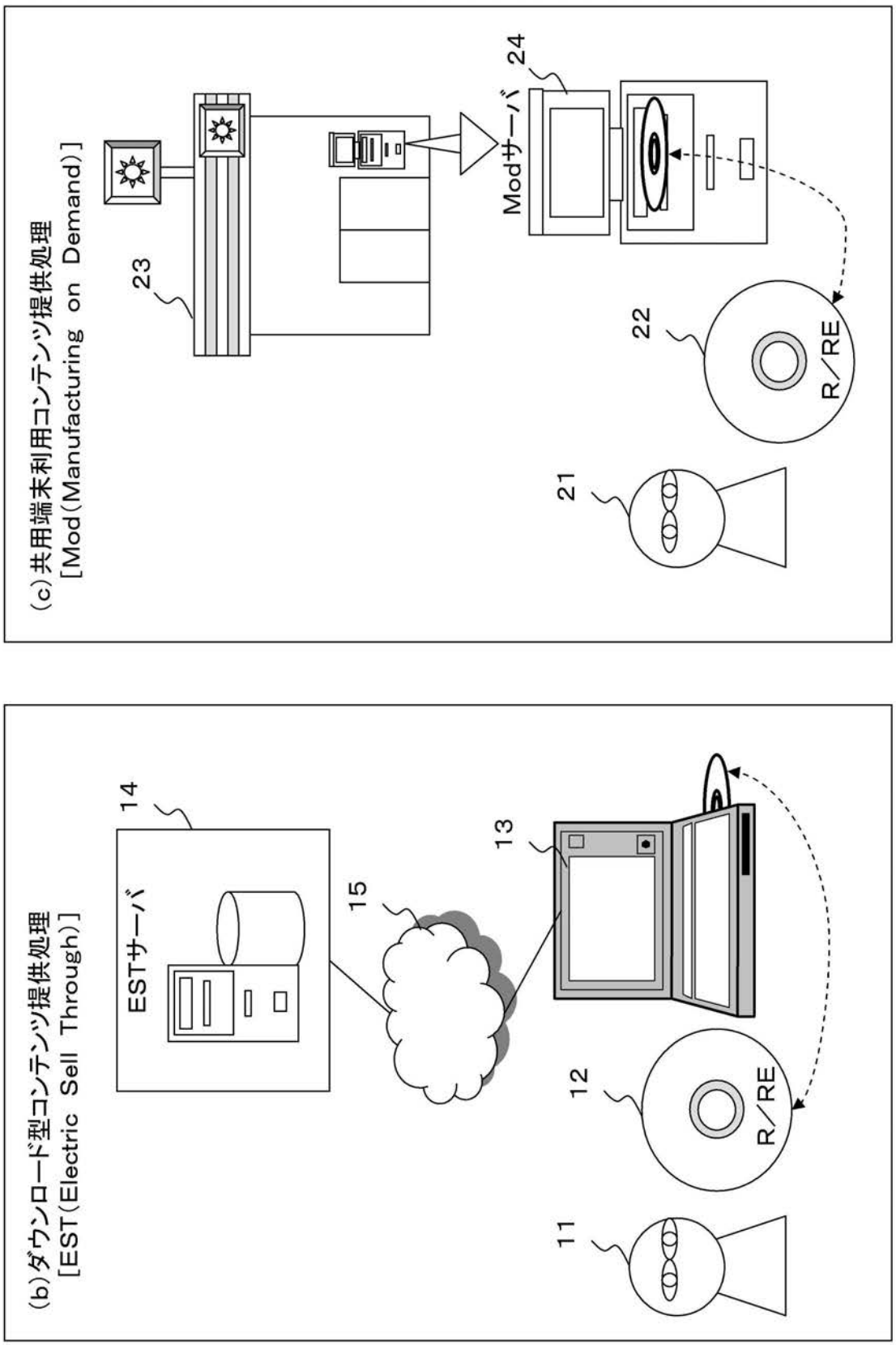
【図２６】


823
記憶部
822
データ処理部
821
データ
入出力部
830
媒体IF
824

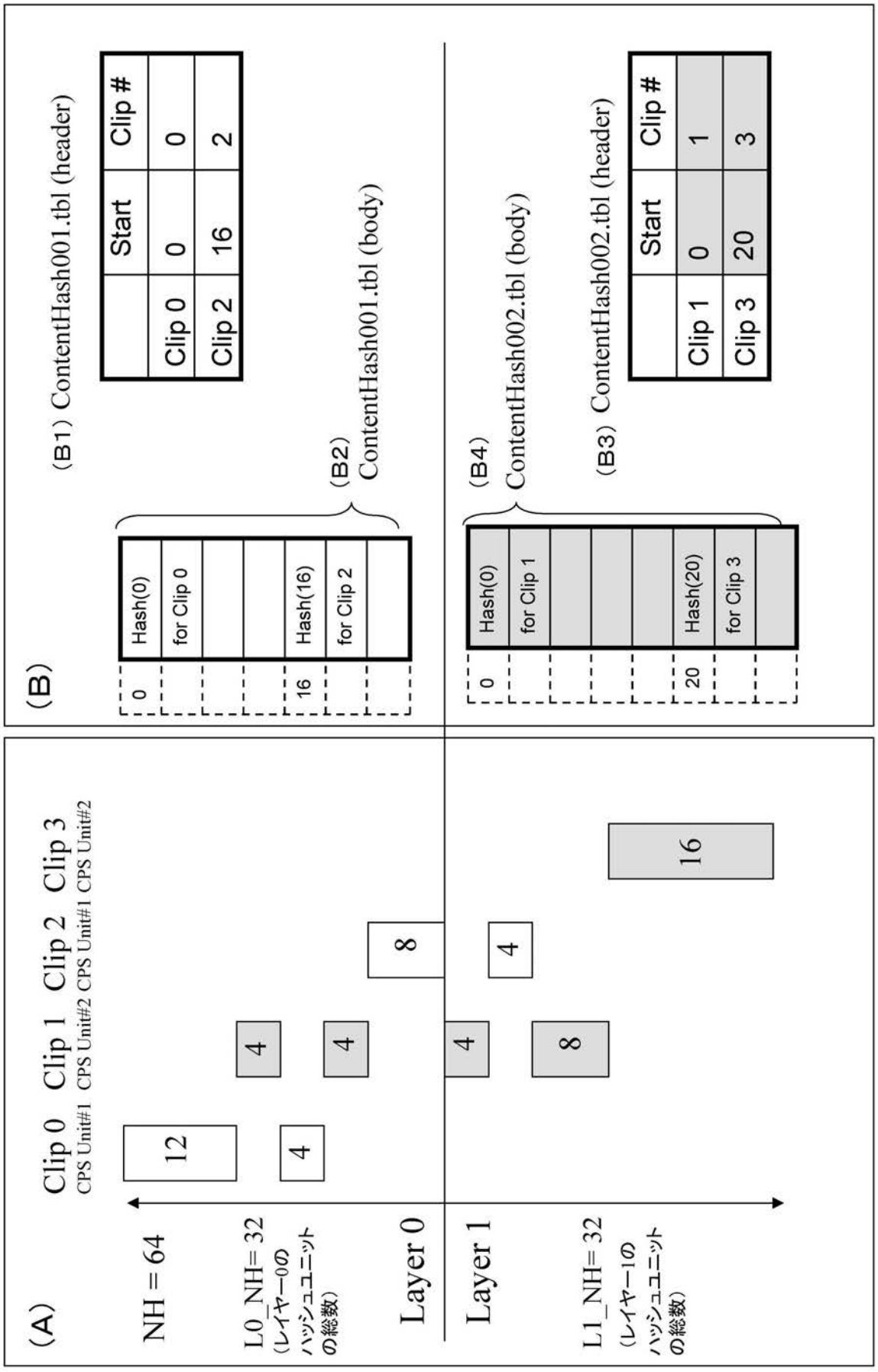
【図１】


(a)コピー型コンテンツ記録処理
[MC(Managed Copy)]
1
2
ROM
3
4
5
R/RE
6
管理サーバ
(MCサーバ)
7

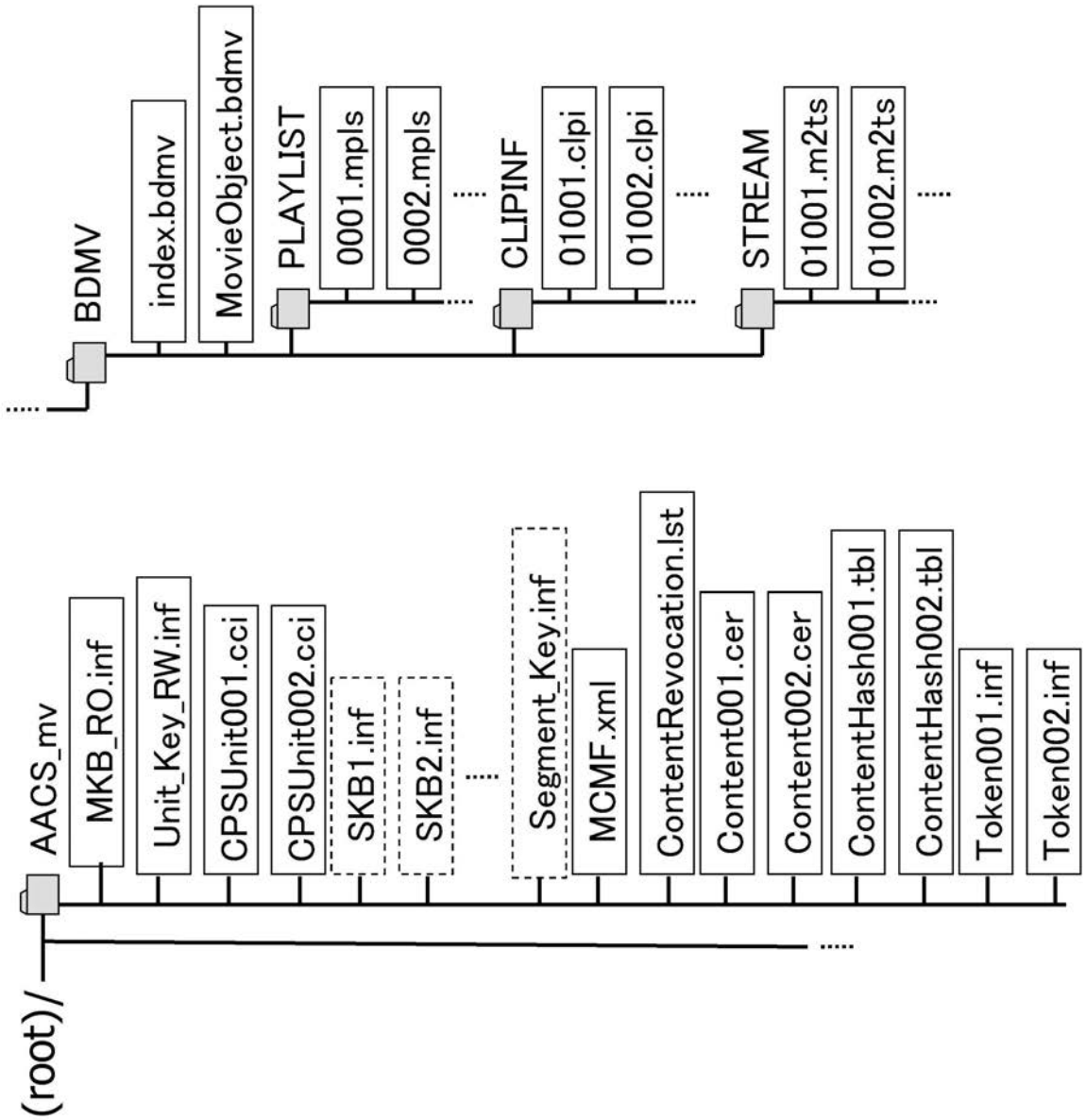
【図２】


(c)共用端末利用コンテンツ提供処理
[Mod(Manufacturing on Demand)]
23
Modサーバ
24
22
R/RE
21
(b)ダウンロード型コンテンツ提供処理
[EST(Electric Sell Through)]
14
ESTサーバ
15
13
12
R/RE
11

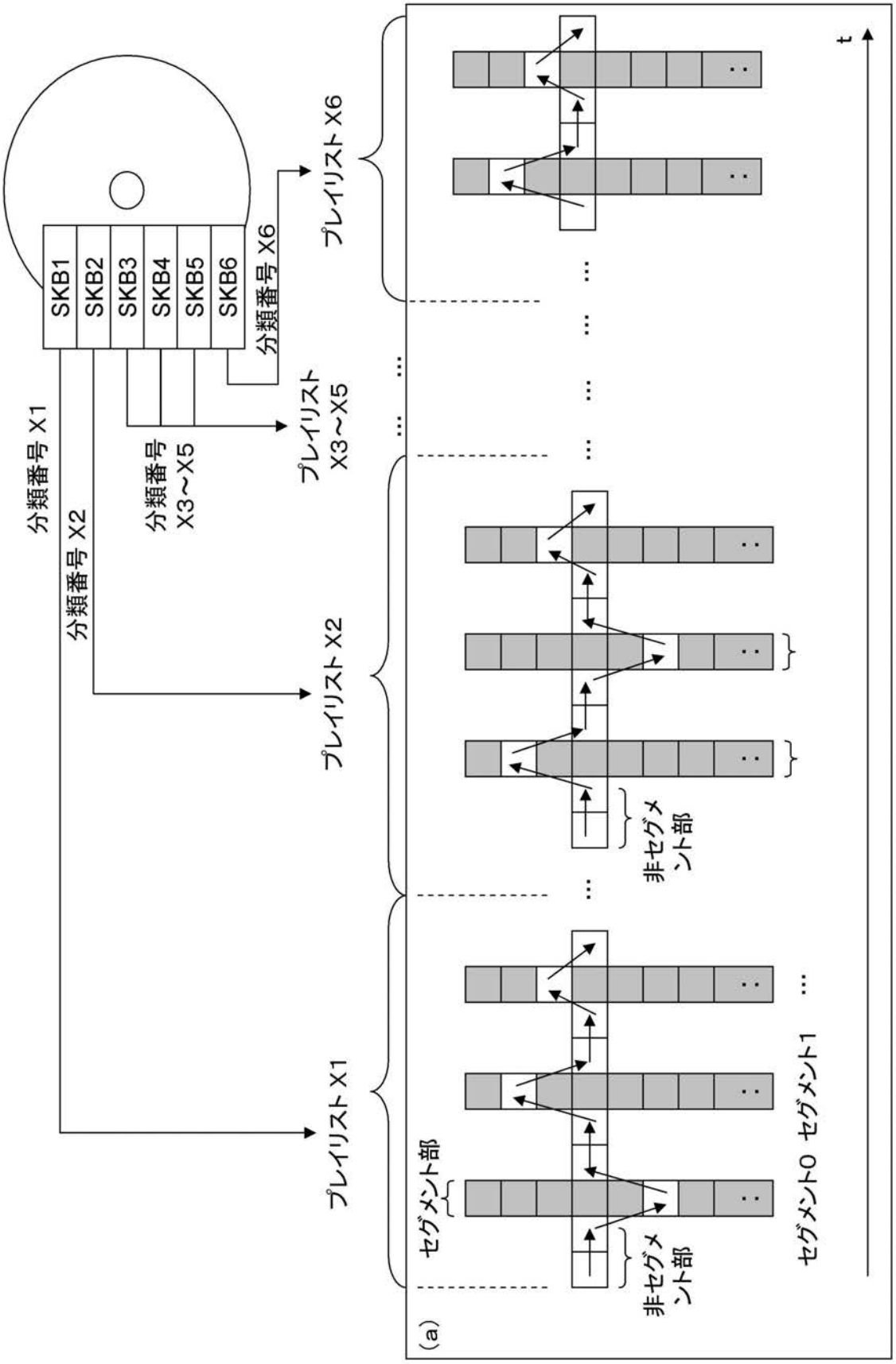
【図１０】


(A)
Clip 0 Clip 1 Clip 2 Clip 3
CPS Unit#1 CPS Unit#2 CPS Unit#1 CPS Unit#2
NH = 64
12
4
4
4
4
8
Layer 0
Layer 1
4
8
16
L0_NH= 32
(レイヤー0のハッシュユニットの総数)
L1_NH= 32
(レイヤー1のハッシュユニットの総数)
(B)
(B1) ContentHash001.tbl (header)
Start
Clip #
Clip 0
0
0
Clip 2
16
2
(B2)
ContentHash001.tbl (body)
0
Hash(0)
for Clip 0
16
Hash(16)
for Clip 2
(B4)
ContentHash002.tbl (body)
0
Hash(0)
for Clip 1
20
Hash(20)
for Clip 3
(B3) ContentHash002.tbl (header)
Start
Clip #
Clip 1
0
1
Clip 3
20
3

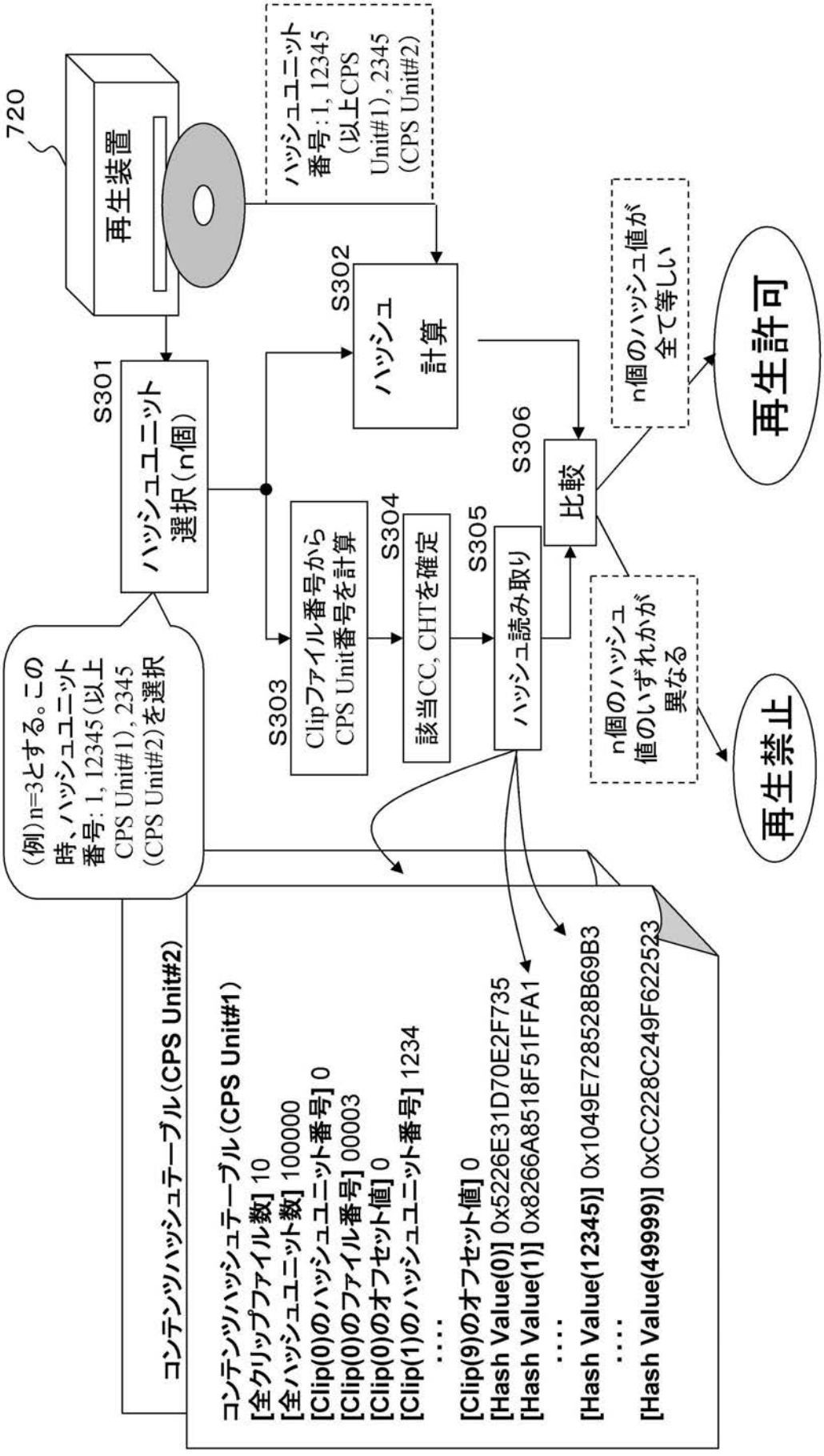
【図１６】


(root)/
AACS_mv
MKB_RO.inf
Unit_Key_RW.inf
CPSUnit001.cci
CPSUnit002.cci
SKB1.inf
SKB2.inf
Segment_Key.inf
MCMF.xml
ContentRevocation.lst
Content001.cer
Content002.cer
ContentHash001.tbl
ContentHash002.tbl
Token001.inf
Token002.inf
BDMV
index.bdmv
MovieObject.bdmv
PLAYLIST
0001.mpls
0002.mpls
CLIPINF
01001.clpi
01002.clpi
STREAM
01001.m2ts
01002.m2ts

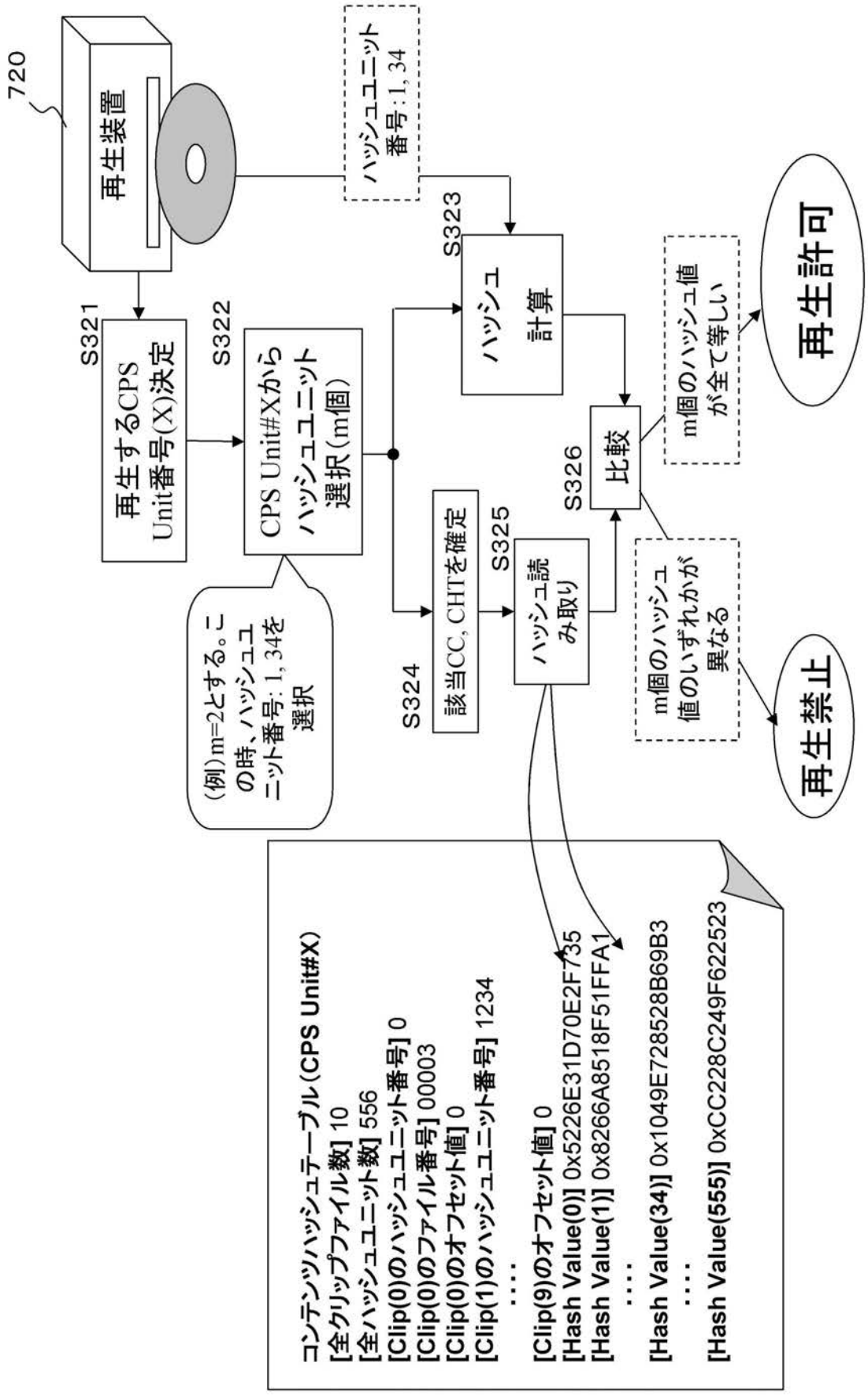
【図１７】


SKB1
SKB2
SKB3
SKB4
SKB5
SKB6
分類番号 X1
分類番号 X2
分類番号 X3～X5
分類番号 X6
プレイリスト X1
プレイリスト X2
プレイリスト X3～X5
プレイリスト X6
セグメント部
非セグメント部
セグメント0 セグメント1
t
(a)

【図２１】


720
再生装置
ハッシュユニット
番号: 1, 12345
(以上CPS
Unit#1), 2345
(CPS Unit#2)
S301
ハッシュユニット
選択(n個)
S302
ハッシュ
計算
S303
Clipファイル番号から
CPS Unit番号を計算
S304
該当CC, CHTを確定
S305
ハッシュ読み取り
S306
比較
n個のハッシュ値が
全て等しい
再生許可
n個のハッシュ
値のいずれかが
異なる
再生禁止
(例)n=3とする。この
時、ハッシュユニット
番号: 1, 12345(以上
CPS Unit#1), 2345
(CPS Unit#2)を選択
コンテンツハッシュテーブル(CPS Unit#2)
コンテンツハッシュテーブル(CPS Unit#1)
[全クリップファイル数] 10
[全ハッシュユニット数] 100000
[Clip(0)のハッシュユニット番号] 0
[Clip(0)のファイル番号] 00003
[Clip(0)のオフセット値] 0
[Clip(1)のハッシュユニット番号] 1234
....
[Clip(9)のオフセット値] 0
[Hash Value(0)] 0x5226E31D70E2F735
[Hash Value(1)] 0x8266A8518F51FFA1
....
[Hash Value(12345)] 0x1049E728528B69B3
....
[Hash Value(49999)] 0xCC228C249F622523

【図２２】


720
再生装置
ハッシュユニット番号:1, 34
S321
再生するCPS Unit番号(X)決定
S322
CPS Unit#Xからハッシュユニット選択(m個)
S323
ハッシュ計算
S324
該当CC, CHTを確定
S325
ハッシュ読み取り
S326
比較
m個のハッシュ値が全て等しい
再生許可
m個のハッシュ値のいずれかが異なる
再生禁止
(例)m=2とするとこの時、ハッシュユニット番号: 1, 34を選択
コンテンツハッシュテーブル(CPS Unit#X)
[全クリップファイル数] 10
[全ハッシュユニット数] 556
[Clip(0)のハッシュユニット番号] 0
[Clip(0)のファイル番号] 00003
[Clip(0)のオフセット値] 0
[Clip(1)のハッシュユニット番号] 1234
....
[Clip(9)のオフセット値] 0
[Hash Value(0)] 0x5226E31D70E2F735
[Hash Value(1)] 0x8266A8518F51FFA1
....
[Hash Value(34)] 0x1049E728528B69B3
....
[Hash Value(555)] 0xCC228C249F622523

フロントページの続き

(72)発明者　大石　丈於
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　村松　克美
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　加藤　元樹
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　高島　芳和
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　堀　洋介

(56)参考文献　特開２００６－０７４４２１（ＪＰ，Ａ）
特開２００４－３１１０００（ＪＰ，Ａ）
特開２００６－０３１８１８（ＪＰ，Ａ）
特開２００５－０２０７０３（ＪＰ，Ａ）
特開２００５－０９２８３０（ＪＰ，Ａ）
特開２００４－３４２２４６（ＪＰ，Ａ）
特開２００２－１３２４５７（ＪＰ，Ａ）
Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ　（ＡＡＣＳ）　Ｒｅｃｏｒｄａｂｌｅ　Ｖ，２００６年　２月１７日，Ｒｅｖｉｓｉｏｎ　０．９１，ｐ．５－１３，「平成２２年８月６日検索」、インターネット<URL:http://www.aacsla.com/specification/specs091/AACS_Spe

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ１１Ｂ　２０／１０
Ｇ０６Ｆ　２１／２４