(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4770650号
(P4770650)
(45)発行日　平成23年9月14日(2011.9.14)　(24)登録日　平成23年7月1日(2011.7.1)

(51)Int.Cl.　　F I
G11B 20/10 (2006.01)　　G11B 20/10　H
H04N 5/91 (2006.01)　　H04N 5/91　P

請求項の数 12　(全 58 頁)

(21)出願番号　特願2006-244908(P2006-244908)
(22)出願日　平成18年9月9日(2006.9.9)
(65)公開番号　特開2008-65946(P2008-65946A)
(43)公開日　平成20年3月21日(2008.3.21)
審査請求日　平成21年9月2日(2009.9.2)

(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　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

最終頁に続く

(54)【発明の名称】情報処理装置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、
情報記録媒体に記録されたデータの読み取りを実行する記録媒体制御部と、
コンテンツの利用制御単位として設定されるコンテンツ管理ユニットに対応するユニット鍵を、前記情報記録媒体に記録されたユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体に記録された暗号化コンテンツの復号処理を実行するデータ処理部とを有し、
前記データ処理部は、
情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号処理を実行する構成であり、
前記データ処理部は、
暗号化コンテンツのアプリケーションタイプが、
（ａ）リアルタイム記録コンテンツに対応するアプリケーションタイプであるか、
（ｂ）ダウンロードコンテンツに対応するアプリケーションタイプであるか、
上記（ａ），（ｂ）のいずれのアプリケーションタイプであるかを判別し、判別結果に応じて、ユニット鍵を適用した復号処理単位を決定し、決定した復号処理単位で個別のユニット鍵を適用した復号処理を実行する構成であり、
暗号化コンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応する

アプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対応するユニット鍵を、前記ユニット鍵ファイルから取得し、

暗号化コンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対応するユニット鍵を、前記ユニット鍵ファイルから取得する処理を行うとともに、

前記ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理によるユニット鍵の取得に際して、前記ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行してユニット鍵を取得することを特徴とする情報処理装置。

【請求項２】

前記データ処理部は、

情報記録媒体が、データ再書き込みの許容されないＲＯＭ型ディスクであるか否かを判別し、データ再書き込みの許容されたディスクである場合に、さらに、情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号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３】

前記データ処理部は、

情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプの判別情報に応じて、コンテンツに対応して設定されるコンテンツの正当性を示すコンテンツ証明書の検証を行なうか否かを決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４】

前記データ処理部は、

情報記録媒体から取得される鍵生成情報としてのシードを適用した暗号鍵生成処理を実行し、生成暗号鍵に基づく前記ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理によりユニット鍵の取得処理を実行する構成であることを特徴とする請求項１～３いずれかに記載の情報処理装置。

【請求項５】

前記データ処理部は、

情報処理装置に格納されたデバイス鍵を適用した暗号鍵ブロックの処理によって取得されるメディア鍵による前記シードの暗号処理によって生成する暗号鍵を適用して、前記ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理を実行する構成であることを特徴とする請求項４に記載の情報処理装置。

【請求項６】

情報記録媒体に対する情報記録処理を実行する情報処理装置であり、

情報記録媒体に記録するコンテンツに対して、コンテンツの利用制御単位であるコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化処理を実行して暗号化コンテンツを生成し、前記ユニット鍵の暗号化処理を実行して暗号化ユニット鍵ファイルの生成を行なうデータ処理部を有し、

前記データ処理部は、

情報記録媒体に記録するコンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の暗号化処理およびコンテンツ暗号化処理を実行する構成であり、

前記データ処理部は、

コンテンツのアプリケーションタイプが、

（ａ）リアルタイム記録コンテンツに対応するアプリケーションタイプであるか、

（ｂ）ダウンロードコンテンツに対応するアプリケーションタイプであるか、

上記（ａ），（ｂ）のいずれのアプリケーションタイプであるかに応じて、ユニット鍵を適用した暗号化処理単位を決定し、決定した暗号化処理単位で個別のユニット鍵を適用した暗号化処理を実行する構成であり、

情報記録媒体に記録予定のコンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行し、

情報記録媒体に記録予定のコンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行するとともに、

前記ユニット鍵ファイルに記録するユニット鍵の暗号化処理に際して、前記ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行することを特徴とする情報処理装置。

【請求項７】

前記データ処理部は、

鍵生成情報としてのシードを適用した暗号鍵生成処理を実行し、生成暗号鍵に基づく前記ユニット鍵ファイルに記録するユニット鍵の暗号化処理を実行する構成であることを特徴とする請求項６に記載の情報処理装置。

【請求項８】

前記データ処理部は、

情報処理装置に格納されたデバイス鍵を適用した暗号鍵ブロックの処理によって取得されるメディア鍵による前記シードの暗号処理によって生成する暗号鍵を適用して、前記ユニット鍵ファイルに記録するユニット鍵の暗号化処理を実行する構成であることを特徴とする請求項７に記載の情報処理装置。

【請求項９】

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、

記録媒体制御部において、情報記録媒体に記録されたデータの読み取りを実行する記録媒体制御ステップと、

データ処理部において、コンテンツの利用制御単位として設定されるコンテンツ管理ユニットに対応するユニット鍵を、前記情報記録媒体に記録されたユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体に記録された暗号化コンテンツの復号処理を実行するデータ処理ステップとを有し、

前記データ処理ステップは、

情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号処理を実行するステップであり、

前記データ処理ステップは、

暗号化コンテンツのアプリケーションタイプが、

（ａ）リアルタイム記録コンテンツに対応するアプリケーションタイプであるか、

（ｂ）ダウンロードコンテンツに対応するアプリケーションタイプであるか、

上記（ａ），（ｂ）のいずれのアプリケーションタイプであるかを判別し、判別結果に応じて、ユニット鍵を適用した復号処理単位を決定し、決定した復号処理単位で個別のユニット鍵を適用した復号処理を実行し、

暗号化コンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対応するユニット鍵を、前記ユニット鍵ファイルから取得し、

暗号化コンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対応するユニット鍵を、前記ユニット鍵ファイルから取得する処理を行うとともに、

前記ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理によるユニット鍵の取得に際して、前記ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行してユニット鍵を取得するステップであることを特徴とする情報処理方法。

【請求項１０】

情報処理装置において、情報記録媒体に対する情報記録処理を実行する情報処理方法であり、

データ処理部において、情報記録媒体に記録するコンテンツに対して、コンテンツの利用制御単位であるコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化処理を実行して暗号化コンテンツを生成し、前記ユニット鍵の暗号化処理を実行して暗号化ユニット鍵ファイルの生成を行なうデータ処理ステップを有し、

前記データ処理ステップは、

情報記録媒体に記録するコンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵ファイルに記録するユニット鍵の暗号化処理およびコンテンツ暗号化処理を実行するステップであり、

前記データ処理ステップは、

コンテンツのアプリケーションタイプが、

（ａ）リアルタイム記録コンテンツに対応するアプリケーションタイプであるか、

（ｂ）ダウンロードコンテンツに対応するアプリケーションタイプであるか、

上記（ａ），（ｂ）のいずれのアプリケーションタイプであるかに応じて、ユニット鍵を適用した暗号化処理単位を決定し、決定した暗号化処理単位で個別のユニット鍵を適用した暗号化処理を実行し、

情報記録媒体に記録予定のコンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行し、

情報記録媒体に記録予定のコンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行するとともに、

前記ユニット鍵ファイルに記録するユニット鍵の暗号化処理に際して、前記ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行するステップであることを特徴とする情報処理方法。

【請求項１１】

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、

記録媒体制御部において、情報記録媒体に記録されたデータの読み取りを実行させる記録媒体制御ステップと、

データ処理部において、コンテンツの利用制御単位として設定されるコンテンツ管理ユニットに対応するユニット鍵を、前記情報記録媒体に記録されたユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体に記録された暗号化コンテンツの復号処理を実行させるデータ処理ステップとを有し、

前記データ処理ステップは、

情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコン

テンツ復号処理を実行させるステップであり、
前記データ処理ステップは、
暗号化コンテンツのアプリケーションタイプが、
（ａ）リアルタイム記録コンテンツに対応するアプリケーションタイプであるか、
（ｂ）ダウンロードコンテンツに対応するアプリケーションタイプであるか、
上記（ａ），（ｂ）のいずれのアプリケーションタイプであるかを判別し、判別結果に応じて、ユニット鍵を適用した復号処理単位を決定し、決定した復号処理単位で個別のユニット鍵を適用した復号処理を実行し、
暗号化コンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対応するユニット鍵を、前記ユニット鍵ファイルから取得し、
暗号化コンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対応するユニット鍵を、前記ユニット鍵ファイルから取得する処理を行うとともに、
前記ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理によるユニット鍵の取得に際して、前記ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行してユニット鍵を取得するステップであることを特徴とするコンピュータ・プログラム。

【請求項１２】
情報処理装置において、情報記録媒体に対する情報記録処理を実行させるコンピュータ・プログラムであり、
データ処理部において、情報記録媒体に記録するコンテンツに対して、コンテンツの利用制御単位であるコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化処理を実行して暗号化コンテンツを生成し、前記ユニット鍵の暗号化処理を実行して暗号化ユニット鍵ファイルの生成を行なわせ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、
情報記録媒体に記録するコンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵ファイルに記録するユニット鍵の暗号化処理およびコンテンツ暗号化処理を実行させるステップであり、
前記データ処理ステップは、
コンテンツのアプリケーションタイプが、
（ａ）リアルタイム記録コンテンツに対応するアプリケーションタイプであるか、
（ｂ）ダウンロードコンテンツに対応するアプリケーションタイプであるか、
上記（ａ），（ｂ）のいずれのアプリケーションタイプであるかに応じて、ユニット鍵を適用した暗号化処理単位を決定し、決定した暗号化処理単位で個別のユニット鍵を適用した暗号化処理を実行し、
情報記録媒体に記録予定のコンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行し、
情報記録媒体に記録予定のコンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行するとともに、
前記ユニット鍵ファイルに記録するユニット鍵の暗号化処理に際して、前記ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行するステップであるこ

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、情報記録媒体の記録コンテンツの利用構成において、区分ユニット単位のコンテンツの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、ネットワークや放送を介して受信したコンテンツなどを記録することなどが可能となる。
【０００３】
しかし、放送コンテンツ、その他、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】
しかしながら、コンテンツを利用しようとする機器（情報処理装置）や、コンテンツを記録するメディア（情報記録媒体）には、様々な種類がある。例えばメディアの種類としては、
＊再生のみを共用するＲＯＭ型、＊新たなデータ書き込みが可能なＲ型、ＲＥ型などの様々なメディアの種類がある。一方、コンテンツを利用しようとする機器（情報処理装置

）にも、＊再生専用機器、＊記録処理が可能な機器など、様々な種類の機器が存在する。
【０００９】
このように様々なメディアおよび機器が存在する現状において、コンテンツの利用形態もメディアと機器に応じた様々な利用形態が想定される。例えばＲＯＭ型ディスクを利用したコンテンツ利用においては、ディスクに対する新たなコンテンツの記録や削除が行なわれることがないので、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。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。
【００１０】
また、ディスクに新たなコンテンツを記録する処理にも様々な態様がある。例えば、放送コンテンツなどをリアルタイム記録する処理や、コンテンツサーバからのコンテンツダウンロード処理などがある。このように、メディアや情報処理装置には様々な種類があり、コンテンツの利用形態にも様々な種類があり、様々な態様でのコンテンツ利用形態に応じた最適な利用制御構成を実現することが要請される。
【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、様々な種類のメディア（情報記録媒体）や機器（情報処理装置）に対応したコンテンツ利用形態に対応するコンテンツ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、
情報記録媒体に記録されたデータの読み取りを実行する記録媒体制御部と、
コンテンツの利用制御単位として設定されるコンテンツ管理ユニットに対応するユニット鍵を、前記情報記録媒体に記録されたユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体に記録された暗号化コンテンツの復号処理を実行するデータ処理部とを有し、
前記データ処理部は、
情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号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、情報記録媒体が、データ再書き込みの許容されないＲＯＭ型ディスクであるか否かを判別し、データ再書き込みの許容されたディスクである場合に、さらに、情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号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、前記データ処理部は、情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプの判別情報に応じて、コンテンツに対応して設定されるコンテンツの正当性を示すコンテンツ証明書の検証を行なうか否かを決定する処理を実行する構成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、前記データ処理部は、情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプであるか否かを判別し、リアルタイム記録コンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対応するユニット鍵を、前記ユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体に記録された暗号化コンテンツの復号処理を実行する構成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、情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプであるか否かを判別し、ダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対応するユニット鍵を、前記ユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体に記録された暗号化コンテンツの復号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、情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプであると判定した場合、前記ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理によるユニット鍵の取得に際して、前記ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行してユニット鍵を取得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、情報記録媒体から取得される鍵生成情報としてのシードを適用した暗号鍵生成処理を実行し、生成暗号鍵に基づく前記ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理によりユニット鍵の取得処理を実行する構成であることを特徴とする。

【００１９】

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、情報処理装置に格納されたデバイス鍵を適用した暗号鍵ブロックの処理によって取得されるメディア鍵による前記シードの暗号処理によって生成する暗号鍵を適用して、前記ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理を実行する構成であることを特徴とする。

【００２０】

さらに、本発明の第２の側面は、

情報記録媒体に対する情報記録処理を実行する情報処理装置であり、

情報記録媒体に記録するコンテンツに対して、コンテンツの利用制御単位であるコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化処理を実行して暗号化コンテンツを生成し、前記ユニット鍵の暗号化処理を実行して暗号化ユニット鍵ファイルの生成を行なうデータ処理部を有し、

前記データ処理部は、

情報記録媒体に記録するコンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵ファイルに記録するユニット鍵の暗号化処理およびコンテンツ暗号化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。

【００２１】

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、情報記録媒体に記録予定のコンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプであるか否かを判別し、リアルタイム記録コンテンツに

対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行する構成であることを特徴とする。

【００２２】

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、情報記録媒体に記録予定のコンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプであるか否かを判別し、ダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行する構成であることを特徴とする。

【００２３】

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、情報記録媒体に記録予定のコンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプである場合、前記ユニット鍵ファイルに記録するユニット鍵の暗号化処理に際して、前記ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行する構成であることを特徴とする。

【００２４】

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、鍵生成情報としてのシードを適用した暗号鍵生成処理を実行し、生成暗号鍵に基づく前記ユニット鍵ファイルに記録するユニット鍵の暗号化処理を実行する構成であることを特徴とする。

【００２５】

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、情報処理装置に格納されたデバイス鍵を適用した暗号鍵ブロックの処理によって取得されるメディア鍵による前記シードの暗号処理によって生成する暗号鍵を適用して、前記ユニット鍵ファイルに記録するユニット鍵の暗号化処理を実行する構成であることを特徴とする。

【００２６】

さらに、本発明の第３の側面は、

情報記録媒体であり、

コンテンツの利用制御単位として設定されるユニットに区分され、該ユニットに対応するユニット鍵を適用した暗号化データを構成データとして含むコンテンツ管理ユニットと、

前記ユニット鍵を格納した鍵ファイルであり、該鍵ファイルに含まれるユニット鍵の構成変更に従って値を更新するシードを適用して生成する暗号鍵に基づいて、前記ユニット鍵ファイルまたは該ファイル構成データの暗号化処理が施されたユニット鍵ファイルと、

前記シードと、

コンテンツの正当性を証明するコンテンツ証明書と、

コンテンツ提供サーバの識別情報を含むサーババインド処理情報と、

を格納した構成を有することを特徴とする情報記録媒体にある。

【００３０】

さらに、本発明の第４の側面は、

コンテンツの利用制御単位として設定されるユニットに区分され、該ユニットに対応するユニット鍵を適用した暗号化データを構成データとして含むコンテンツ管理ユニットと、

前記ユニット鍵を格納した鍵ファイルであり、該鍵ファイルに含まれるユニット鍵の構成変更に従って値を更新するシードを適用して生成する暗号鍵に基づいて、前記ユニット鍵ファイルまたは該ファイル構成データの暗号化処理が施されたユニット鍵ファイルと、

前記シードと、

コンテンツの正当性を証明するコンテンツ証明書と、

コンテンツ提供サーバの識別情報を含むサーババインド処理情報と、

を含むことを特徴とするデータ構造にある。

【００３１】

さらに、本発明の第５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、

記録媒体制御部において、情報記録媒体に記録されたデータの読み取りを実行する記録媒体制御ステップと、

データ処理部において、コンテンツの利用制御単位として設定されるコンテンツ管理ユニットに対応するユニット鍵を、前記情報記録媒体に記録されたユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体に記録された暗号化コンテンツの復号処理を実行するデータ処理ステップとを有し、

前記データ処理ステップは、

情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号処理を実行するステップであ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６の側面は、

情報処理装置において、情報記録媒体に対する情報記録処理を実行する情報処理方法であり、データ処理部において、情報記録媒体に記録するコンテンツに対して、コンテンツの利用制御単位であるコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化処理を実行して暗号化コンテンツを生成し、前記ユニット鍵の暗号化処理を実行して暗号化ユニット鍵ファイルの生成を行なうデータ処理ステップを有し、

前記データ処理ステップは、

情報記録媒体に記録するコンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵ファイルに記録するユニット鍵の暗号化処理およびコンテンツ暗号化処理を実行するステップであることを特徴とする情報処理方法にある。

【００４５】

さらに、本発明の第７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、

記録媒体制御部において、情報記録媒体に記録されたデータの読み取りを実行させる記録媒体制御ステップと、

データ処理部において、コンテンツの利用制御単位として設定されるコンテンツ管理ユニットに対応するユニット鍵を、前記情報記録媒体に記録されたユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体に記録された暗号化コンテンツの復号処理を実行させるデータ処理ステップとを有し、

前記データ処理ステップは、

情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号処理を実行させるステップであることを特徴とするコンピュータ・プログラムにある。

【００４６】

さらに、本発明の第８の側面は、

情報処理装置において、情報記録媒体に対する情報記録処理を実行させるコンピュータ・プログラムであり、

データ処理部において、情報記録媒体に記録するコンテンツに対して、コンテンツの利用制御単位であるコンテンツ管理ユニットに対応するユニット鍵を適用した暗号化処理を実行して暗号化コンテンツを生成し、前記ユニット鍵の暗号化処理を実行して暗号化ユニット鍵ファイルの生成を行なわせ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、
情報記録媒体に記録するコンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵ファイルに記録するユニット鍵の暗号化処理およびコンテンツ暗号化処理を実行させるステップであることを特徴とするコンピュータ・プログラムにある。

【００４７】

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。

【００４８】

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】

【００４９】

本発明の一実施例の構成によれば、コンテンツの利用制御単位として設定されるコンテンツ管理ユニット（ＣＰＳユニット）に基づくコンテンツの利用制御を行う構成において、コンテンツの記録、または再生処理に際して、記録コンテンツに対応するアプリケーションタイプの識別を行い、各アプリケーションタイプに応じた処理によるデータ記録または再生を実行する構成とした具体的には、例えばリアルタイム記録コンテンツに対応するアプリケーションタイプ、ダウンロードコンテンツに対応するアプリケーションタイプ等を設定し、それぞれのコンテンツに応じたユニット鍵の設定、コンテンツ管理ユニットの設定構成として、各コンテンツに応じた柔軟なコンテンツ利用制御を実現した。

【発明を実施するための最良の形態】

【００５０】

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．ディスク記録情報および再生シーケンス
（１－１）ディスク記録情報
（１－２）コンテンツ管理ユニット（ＣＰＳユニット）による管理構成
（１－３）コンテンツ利用シーケンス
２．コンテンツ利用形態に応じたデータ記録構成およびコンテンツ利用アプリケーション
（２－１）ＲＯＭ型ディスク対応のＢＤＭＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ１）
（２－２）ＲＥ型，Ｒ型ディスク対応のＢＤＡＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ２）
（２－３）ＲＯＭ型ディスク対応のＢＤＭＶ形式でのリアルタイム記録に適したデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ３）
（２－４）ＲＯＭ型ディスク対応のＢＤＭＶ形式でのダウンロード記録に適したデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ４）
３．コンテンツ再生処理
４．情報処理装置の構成例

【００５１】

［１．ディスク記録情報および再生シーケンス］

まず、ＡＡＣＳ(Advanced Access Content System)に従った情報記録媒体（ディスク）に対する記録データの種類、およびコンテンツの再生処理シーケンスについて説明する。

【００５２】

（１－１）ディスク記録情報

最初に、図１を参照して情報記録媒体１００の格納データについて説明する。情報記録媒体１００は、例えば、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）、ＤＶＤなどの情報記録媒体であり、著作権保護対象となるコンテンツを記録したディスクであり、ＡＡＣＳ(Advanced Access Content System)に従ったコンテンツ利用を可能とした各種のデータが記録されている。

【００５３】

図１に示すように、情報記録媒体１００には、暗号化処理および一部データの置き換え処理の施された暗号化コンテンツ１０１と、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）１０２、コンテンツ復号処理に適用するユニット鍵を暗号化したデータ（Encrypted CPS Unit Key）等から構成されるユニット鍵ファイル１０３、ユニット鍵ファイル１０３に含まれるユニット鍵の暗号化に適用される鍵の生成情報となるバインドシード（Ｂｉｎｄｉｎｇ　Ｎｏｎｃｅ）１０４、コンテンツのコピー・再生制御情報としてのＣＣＩ（Copy Control Information）等を含む利用制御情報１０５が格納される。

【００５４】

なお、図に示す情報記録媒体格納データ例は一例であり、格納データは、ディスクの種類などによって多少異なる。以下、これらの各種情報の概要について説明する。

【００５５】

（１）暗号化コンテンツ１０１

情報記録媒体１００には、様々なコンテンツが格納される。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)ストリームや特定の規格で規定された形式のゲームプログラム、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。これらのコンテンツは、特定のＡＶフォーマット規格データであり、特定のＡＶデータフォーマットに従って格納される。

【００５６】

情報記録媒体に格納されるコンテンツは、区分コンテンツ毎の異なる利用制御を実現するため、区分コンテンツ毎に異なる鍵（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つのユニット鍵を割り当てる単位をコンテンツ管理ユニット（ＣＰＳユニット）と呼ぶ。

【００５７】

（２）ＭＫＢ

ＭＫＢ（Media Key Block）１０２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。ＭＫＢ１０２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。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。

【００５８】

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。コンテンツの復号処理については後述する。

【００５９】

（３）ユニット鍵ファイル

前述したように各コンテンツまたは複数コンテンツの集合は、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１００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、音楽データ、動画、静止画等の画像データ、ゲームプログラム、ＷＥＢコンテンツなどは、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を生成して、復号処理を行なうことが必要となる。このユニット鍵を生成するための情報がＣＰＳユニット鍵であり、ＣＰＳユニット鍵を格納したファイルがユニット鍵ファイルである。ユニット鍵ファイルに記録されるユニット鍵は、暗号化されたデータとして記録される。

【００６０】

すなわち、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、上述のＭＫＢから取得可能なメディア鍵［Ｋｍ］や、図１に示すバインドシード（Ｂｉｎｄｉｎｇ　Ｎｏｎｃｅ）１０４を適用して復号が可能となる。復号シーケンスについては、後述する。

【００６１】

（４）バインドシード

バインドシードは、上述したように、ユニット鍵ファイルに記録されるユニット鍵の暗号化に適用される情報であり、バインドシードは、ユニット鍵ファイル内の暗号化ユニット鍵の復号に適用される。暗号化ユニット鍵の復号により、ユニット鍵が取得され、取得されたユニット鍵を適用してコンテンツの復号が実行される。なお、バインドシードは、Ｂｉｎｄｉｎｇ　Ｎｏｎｃｅとして配付して利用する構成と、ＣＰＳユニット鍵ファイルやその他のファイルに記録して配付して利用する構成など、様々な形態での配付および利用構成が可能である。

【００６２】

なお、バインドシードは固定データではなく、ユニット鍵ファイルに格納されるユニット鍵構成の変更に応じて、随時変更される。例えば、あるＣＰＳユニット＃１，の記録された情報記録媒体に対して、さらに、新たなコンテンツであるＣＰＳユニット＃２を記録するようなＣＰＳユニットの追加記録を行なう場合、ＣＰＳユニット鍵ファイルは、ＣＰＳユニット鍵＃１とＣＰＳユニット鍵＃２を含むファイルとして更新され、この更新処理に際して、バインドシードも更新する。

【００６３】

このように、ユニット鍵ファイルの構成に応じて、逐次バインドシードを変更することで、情報記録媒体に正規に格納されたＣＰＳユニットと適用可能なＣＰＳユニット鍵との対応を厳格に管理することが可能となる。

【００６４】

（５）利用制御情報

利用制御情報には、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１００に格納された暗号化コンテンツ１０１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。

【００６５】

（１－２）コンテンツ管理ユニット（ＣＰＳユニット）による管理構成

次に、コンテンツ管理ユニット（ＣＰＳユニット）の設定に基づくコンテンツ管理構成について、図２を参照して説明する。情報記録媒体に格納されるコンテンツは、ユニット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が割り当てられ暗号化処理が

なされて格納される。すなわち、コンテンツはコンテンツ管理ユニット（ＣＰＳユニット）に区分されて、個別の鍵（ユニット鍵（ＣＰＳユニット鍵））による暗号化処理がなされ、個別の利用管理がなされる。

【００６６】

コンテンツ利用に際しては、まず、各ユニットに割り当てられたＣＰＳユニット鍵を取得することが必要であり、さらに、その他の必要な鍵、鍵生成情報等を適用して予め定められた復号処理シーケンスに基づくデータ処理を実行して再生を行う。

【００６７】

コンテンツ管理ユニット（ＣＰＳユニット）の設定態様は、様々な設定が可能である。すなわち、

（ａ）ＲＯＭ型ディスク対応のＢＤＭＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ１）

（ｂ）ＲＥ型，Ｒ型ディスク対応のＢＤＡＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ２）

（ｃ）ＲＯＭ型ディスク対応のＢＤＭＶ形式でのリアルタイム記録に適したデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ３）

（ｄ）ＲＯＭ型ディスク対応のＢＤＭＶ形式でのダウンロード記録に適したデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ４）

これらの各種類に応じた設定が可能となる。

【００６８】

各アプリケーション対応のユニット設定構成については、後段で詳細に説明するが、ユニットの設定の概念を理解のために、図２を参照してコンテンツ管理ユニット（ＣＰＳユニット）の１つの設定例について説明する。

【００６９】

図２に示す例では、動画コンテンツや静止画コンテンツなどの様々なコンテンツに対応するタイトル、アプリケーションなどに対応してコンテンツ管理ユニット（ＣＰＳユニット）を設定した例である。各ＣＰＳユニット設定単位毎に、コンテンツ管理ユニット識別子（ＣＰＳユニットＩＤ）が設定され、各ＣＰＳユニット毎に異なる暗号鍵としてのユニット鍵（ＣＰＳユニット鍵）が割り当てられ、各ＣＰＳユニットは、対応するＣＰＳユニット鍵による暗号化がなされ、復号の際には、復号対象のコンテンツに対応するＣＰＳユニット鍵をＣＰＳユニット鍵ファイルから取得することが必要となる。

【００７０】

（１－３）コンテンツ再生シーケンス

次に、図３を参照して、情報記録媒体１００に記録された情報を適用したコンテンツの利用（再生）シーケンスについて説明する。

【００７１】

まず、情報処理装置１８０は、メモリに格納しているデバイス鍵［Ｋｄ］１８１を読み出す。デバイス鍵１８１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。

【００７２】

次に、情報処理装置１８０は、ステップＳ１１において、デバイス鍵１８１を適用して情報記録媒体１００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ＭＫＢ１０２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）１７１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。ＭＫＢ１０２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。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。

【００７３】

次に、ステップＳ１２において、ステップＳ１１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１００から読み取ったバインドシード（Ｂｉｎｄｉｎｇ Ｎｏｎｃｅ）１０４とに基づく暗号処理によって、暗号鍵としてのバインド鍵［Ｋｂ］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。

【００７４】

このように、ＣＰＳユニット鍵ファイルに含まれる暗号化ユニット鍵の暗号化に直接的に適用される暗号鍵はバインド鍵［Ｋｂ］であり、このバインド鍵［Ｋｂ］に適用する暗号鍵生成情報がバインドシードである。

【００７５】

次に、ステップＳ１３において、バインド鍵［Ｋｂ］によって、情報記録媒体１００から読み取ったＣＰＳユニット鍵ファイル１０３に含まれる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１０３は、各ＣＰＳユニットに対応して設定されるユニット鍵［Ｋｕｎ］の暗号化データを格納したファイルである。ユニット鍵ファイルの具体的構成については後述する。例えば、［Ｅｎｃ（Ｋｂ，ｆ（Ｋｕ＿ｎ，ＣＣＩ））］のような暗号化データとしてユニット鍵を格納している。Ｅｎｃ（ａ，ｂ）はデータｂの鍵ａによる暗号化データを示している。

【００７６】

ステップＳ１３におけるＣＰＳユニット鍵ファイル１０３に含まれる暗号化ユニット鍵の復号処理によって、

データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）

を取得し、ステップＳ１４において、

データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）、

に対して、情報記録媒体１００から読み取った利用制御情報（ＣＣＩ）１０５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、利用制御情報［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利用制御情報［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。

【００７７】

次に、ステップＳ１５において、情報記録媒体１００から読み取った暗号化コンテンツ１０１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、ステップＳ１６において、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１８２を取得する。

【００７８】

この処理によって、情報記録媒体１００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。

【００７９】

［２．コンテンツ利用形態に応じたデータ記録構成およびコンテンツ利用アプリケーション］

次に、コンテンツ利用形態に応じたデータ記録構成およびコンテンツ利用アプリケーションについて説明する。先に説明したように、コンテンツを利用しようとする機器（情報処理装置）や、コンテンツを記録するメディア（情報記録媒体）には、様々な種類がある。例えばメディアの種類としては、＊再生のみを共用するＲＯＭ型、＊新たなデータ書き込みが可能なＲ型、ＲＥ型などの様々なメディアの種類がある。一方、コンテンツを利用しようとする機器（情報処理装置）にも、＊再生専用機器、＊記録処理が可能な機器など、様々な種類の機器が存在する。さらに、ディスクに新たなコンテンツを記録する処理にも様々な態様がある。例えば、放送コンテンツなどをリアルタイム記録する処理や、コン

テンツサーバからのコンテンツダウンロード処理などがある。

【００８０】

このように、メディアや情報処理装置、コンテンツの利用形態には様々な種類があり、様々な態様でのコンテンツ利用形態に応じた最適な利用制御構成を実現することが要請される。以下では、これらの様々なコンテンツ利用形態に応じたコンテンツ利用制御を実現するためのユニット（ＣＰＳユニット）の設定構成、およびコンテンツ利用処理を実現するアプリケーションについて説明する。

【００８１】

なお、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）に対応するアプリケーション規格として、すでに以下の２つのアプリケーション規格が規定されている。

（２－１）ＲＯＭ型ディスク対応のＢＤＭＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ１）

（２－２）ＲＥ型，Ｒ型ディスク対応のＢＤＡＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ２）

【００８２】

本発明は、これらの２つの既存の規格に、さらに、以下の２つの新たな規格となり得る構成について提案するものである。

（２－３）ＲＯＭ型ディスク対応のＢＤＭＶ形式でのリアルタイム記録に適したデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ３）

（２－４）ＲＯＭ型ディスク対応のＢＤＭＶ形式でのダウンロード記録に適したデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ４）

【００８３】

以下においては、まず、既に存在する規格に従った構成である（２－１），（２－２）について、その概要を説明し、その後、本発明の提案する２つの構成（２－３），（２－４）について説明する。

【００８４】

（２－１）ＲＯＭ型ディスク対応のＢＤＭＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ１）

まず、既存の規格であるＲＯＭ型ディスク対応のＢＤＭＶ形式のデータ記録構成およびコンテンツ利用アプリケーションについて、アプリケーション１として説明する。

【００８５】

ＢＤＭＶは、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）における再生専用ディスクに対応するアプリケーション規格である。このＢＤＭＶ規格に従ったディスクにおけるデータ記録フォーマットについて、図４を参照して説明する。

【００８６】

情報記録媒体には、例えば、図４に示すように、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ストリームをメインコンテンツ２００として格納し、その他のデータ、プログラム、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどがサブコンテンツ３００として格納される。

【００８７】

少なくともメインコンテンツ２００は、特定のＡＶフォーマット、例えばＢｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）ＲＯＭ規格データとして、ＢＤＭＶ形式のフォーマットに従ったＢＤＭＶコンテンツとして格納される。図４に示すように、ＢＤＭＶコンテンツは、動画コンテンツ（ＡＶストリーム）を再生対象の実コンテンツとして格納しており、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）ＲＯＭ規格フォーマットに従った階層構成を持つ。すなわち、

（Ａ）アプリケーション２１０

（Ｂ）再生区間指定ファイル（プレイリスト）２３０

（Ｃ）クリップ（コンテンツデータファイル）２４０

である。

【００８８】

（Ｃ）クリップ（コンテンツデータファイル）２４０は、それぞれ区分されたコンテンツデータファイルであるクリップ２４１，２４２，２４３を有し、各クリップ２４１は、ＡＶ（Audio-Visual）ストリームファイル２６１とクリップ情報ファイル２５１を持つ。

【００８９】

クリップ情報ファイル２５１は、ＡＶ（Audio-Visual）ストリームファイル２６１に関する属性情報を格納したデータファイルである。ＡＶ（Audio-Visual）ストリームファイル２６１は例えばＭＰＥＧ－ＴＳ（Moving Picture Experts Group-Transport Stream）データであり、画像（Ｖｉｄｅｏ）、音声（Ａｕｄｉｏ）、字幕データ等の各情報を多重化したデータ構造となっている。また、再生時に再生装置の制御を行うためのコマンド情報も多重化されている場合がある。

【００９０】

（Ｂ）再生区間指定ファイル（プレイリスト）２３０は、複数の再生区間指定ファイル（プレイリスト）２３１，２３２，２３３を持つ。各再生区間指定ファイル（プレイリスト）２３１，２３２，２３３のそれぞれは、クリップ（コンテンツデータファイル）２４０に含まれる複数のＡＶストリームデータファイルのいずれかを選択し、また選択したＡＶストリームデータファイルの特定のデータ部分を、再生開始点と再生終了点として指定するプレイアイテムを１つ以上持つ構成となっており、１つの再生区間指定ファイル（プレイリスト）を選択することで、その再生区間指定ファイル（プレイリスト）の持つプレイアイテムに従って、再生シーケンスが決定されて再生が実行される。

【００９１】

例えば再生区間指定ファイル（プレイリスト）２３１を選択してコンテンツ再生を行うと、再生区間指定ファイル（プレイリスト）２３１に対応付けられたプレイアイテム２３４は、クリップ２４１に再生開始点ａと再生終了点ｂを持ち、また、プレイアイテム２３５は、クリップ２４１に再生開始点ｃと再生終了点ｄを持つので、再生区間指定ファイル（プレイリスト）２３１を選択してコンテンツ再生を行うと、クリップ２４１に含まれるコンテンツであるＡＶストリームファイル２６１の特定データ領域、ａ～ｂとｃ～ｄが再生されることになる。

【００９２】

（Ａ）アプリケーション２１０は、たとえばコンテンツ再生を実行するディスプレイに提示されるコンテンツタイトルを含むアプリケーションインデックスファイル２１１，２１２と再生プログラム２２１，２２２の組み合わせ、または、ゲームコンテンツ、ＷＥＢコンテンツなどのアプリケーション実行ファイル２１３，２１４と再生プログラム２２３，２２４の組み合わせを持つ層として設定される。ユーザは再生対象をアプリケーションインデックスファイル２１１，２１２に含まれるタイトルの選択によって決定することができる

【００９３】

各タイトルは、図に示すように、再生プログラム２２１～２２４の１つの再生プログラム（例えばムービーオブジェクト）に対応付けられており、ユーザが１つのタイトルを選択すると、その選択したタイトルに対応付けられた再生プログラムに基づく再生処理が開始することになる。なお、図に示すタイトル１、タイトル２として示されるアプリケーションインデックスファイル２１１，２１２は、情報記録媒体のセット、起動に際して、自動的に再生されるタイトル、メニューを表示するためのタイトル提示プログラムである「Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ」、「Ｔｏｐ　Ｍｅｎｕ」も含まれる。

【００９４】

アプリケーションインデックスファイル２１１，２１２や、アプリケーション実行ファイル２１３，２１４は、アプリケーション実行に使用されるアプリケーションリソースファイルを含む場合がある。また、情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイル、例えばＪＰＥＧ，ＰＮＧ，ＢＭＰなどの画像ファイル２

２５、ＰＣＭ、圧縮Ａｕｄｉｏなどの音声ファイル２２６、テキスト、データベースなどの各種データファイル２２７がアプリケーションリソースファイルとして適用される場合もある。

【００９５】

再生プログラム（例えばムービーオブジェクト）２２１～２２４は、再生する再生区間指定ファイル（プレイリスト）の指定のほか、ユーザから入力されるコンテンツ再生処理に関する操作情報に対する応答、タイトル間のジャンプ、再生シーケンスの分岐など、再生コンテンツ（ＨＤムービーコンテンツ）の提示に必要な機能をプログラマブルに提供するコンテンツ再生処理プログラムである。各再生プログラム２２１～２２４は、相互にジャンプ可能であり、ユーザの入力、あるいはあらかじめ設定されたプログラムに従って、実際に実行される再生プログラムが選択され、選択された再生プログラムの指定する再生区間指定ファイル（プレイリスト）２３０によって、再生コンテンツがクリップ２４０から選択され再生される。

【００９６】

このようにメインコンテンツ２００は、ＢＤＭＶフォーマットに従った階層構成で管理され、この階層構成の枠組みに対して、コンテンツ管理ユニット（ＣＰＳユニット）が設定され、コンテンツ管理ユニット（ＣＰＳユニット）単位でコンテンツの利用管理がなされる。なお、情報記録媒体には、メインコンテンツ２００の他にサブコンテンツ３００が併せて格納可能であり、サブコンテンツ３００は、特定のＡＶフォーマット、例えばＢｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）ＲＯＭ規格フォーマットに従わない任意のフォーマットで格納することが可能である。図４にはサブコンテンツとして、データグループ１，３１１～データグループＮ，３１２を示している。これらのデータグループも利用管理対象コンテンツとして設定可能であり、利用管理対象コンテンツとして設定した場合には、各データグループを単位としたコンテンツ管理ユニット（ＣＰＳユニット）が設定され、データグループ単位で利用管理がなされる。

【００９７】

次に、このアプリケーションタイプ１、すなわち、ＲＯＭ型ディスク対応のＢＤＭＶ形式のデータ記録構成に従って情報記録媒体に格納されたコンテンツについてのコンテンツ管理ユニット（ＣＰＳユニット）に基づく利用制御を実現するためのユニット設定構成について説明する。

【００９８】

先に図２を参照して説明したように、コンテンツ管理ユニット（ＣＰＳユニット）の各々に対して、異なる暗号鍵としてユニット鍵が割り当てられる。１つのユニット鍵を割り当てる単位がコンテンツ管理ユニット（ＣＰＳユニット）である。

【００９９】

それぞれのユニット鍵を適用して各ユニットに属するコンテンツを暗号化し、コンテンツ利用に際しては、各ユニットに割り当てられたユニット鍵を取得して再生を行う。各ユニット鍵は、個別に管理することが可能であり、例えばあるユニットＡに対して割り当てるユニット鍵は、情報記録媒体から取得可能な鍵として設定する。また、ユニットＢに対して割り当てるユニット鍵は、ネットワーク接続されるサーバにアクセスし、ユーザが所定の手続きを実行したことを条件として取得することができる鍵とするなど、各ユニット対応の鍵の取得、管理構成は、各ユニット鍵に独立した態様とすることが可能である。

【０１００】

アプリケーションタイプ１において規定するコンテンツ管理ユニット（ＣＰＳユニット）の設定構成例について、図５を参照して説明する。

【０１０１】

まず、メインコンテンツ２００側におけるコンテンツ管理ユニット（ＣＰＳユニット）の設定構成について説明する。メインコンテンツ２００側においては、（Ａ）アプリケーション２１０に含まれる１つ以上のタイトルを含むアプリケーションインデックスファイル２１１，２１２、またはアプリケーション実行ファイル２１３，２１４等を含むＣＰＳ

ユニットを設定する。
【０１０２】
図５に示すＣＰＳユニット１，４０１は、アプリケーションインデックスファイルと、再生プログラムファイルと、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群とを１つのユニットとして設定したユニットである。
【０１０３】
また、ＣＰＳユニット２，４０２は、アプリケーション実行ファイルと、再生プログラムファイルと、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群とを１つのユニットとして設定したユニットである。
【０１０４】
また、ＣＰＳユニット３，４０３は、アプリケーション実行ファイルと、再生プログラムファイルと、情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイルによって構成したユニットである。
【０１０５】
これらの各ユニットは、同一の鍵（ＣＰＳユニット鍵：図５中の鍵Ｋｕ１，Ｋｕ２，Ｋｕ３）でそれぞれ個別に暗号化して情報記録媒体に格納される。
【０１０６】
図５中、コンテンツ管理ユニット（ＣＰＳユニット）１，４０１、およびコンテンツ管理ユニット（ＣＰＳユニット）２，４０２は、上位層の（Ａ）アプリケーションと、下位層の（Ｂ）再生区間指定ファイル（プレイリスト）＋（Ｃ）クリップ（コンテンツデータファイル）によって構成されるユニットであり、コンテンツ管理ユニット（ＣＰＳユニット）３，４０３は、下位層の（Ｂ）再生区間指定ファイル（プレイリスト）＋（Ｃ）クリップ（コンテンツデータファイル）を含まず、上位層の（Ａ）アプリケーション層、および情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイルすなわち、画像ファイル２２５、音声ファイル２２６、データファイル２２７等によって構成されるユニットである。
【０１０７】
このように、アプリケーションタイプ１においては、クリップを構成用素とするコンテンツ管理ユニット（ＣＰＳユニット）を設定する場合、（Ａ）アプリケーション、（Ｂ）再生区間指定ファイル（プレイリスト）、（Ｃ）クリップ（コンテンツデータファイル）のすべてを含むユニットとして設定する。
【０１０８】
コンテンツ管理ユニット（ＣＰＳユニット）１，４０１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）１，４０１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。
【０１０９】
また、コンテンツ管理ユニット（ＣＰＳユニット）２，４０２には、ゲームコンテンツ、ＷＥＢコンテンツなどによって構成されるアプリケーションファイル２１３と、再生プログラム２２３、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）２，４０２に対応付けて設定される暗号鍵としてのユニット鍵：Ｋｕ２を適用して暗号化される。さらに、アプリケーションファイル２１３についても、ユニット鍵：Ｋｕ２を適用した暗号化ファイルとしてもよい。
【０１１０】
コンテンツ管理ユニット（ＣＰＳユニット）３，４０３は、上位層の（Ａ）アプリケーション層に含まれるアプリケーションファイル２１４，２１５と、再生プログラム２２４、さらに、再生プログラム２２４によって情報記録媒体、あるいはネットワーク接続サー

バから取得可能な様々なデータファイル、例えばＪＰＥＧ，ＰＮＧ，ＢＭＰなどの画像ファイル２２５、ＰＣＭ、圧縮Ａｕｄｉｏなどの音声ファイル２２６、テキスト、データベースなどの各種データファイル２２７が含まれるユニットとして設定される。

【０１１１】

コンテンツ管理ユニット（ＣＰＳユニット）３，４０３は、コンテンツ管理ユニット（ＣＰＳユニット）３，４０３に対応付けて設定される暗号鍵としてのユニット鍵：Ｋｕ３を適用して暗号化される。

【０１１２】

例えば、ユーザがコンテンツ管理ユニット１，４０１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）１，４０１に対応付けて設定された記録シードＶｕ１を適用した暗号処理により、ユニット鍵：Ｋｕ１を取得して、取得したユニット鍵Ｋｕ１を適用したコンテンツの復号処理シーケンス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。

【０１１３】

例えば、コンテンツ管理ユニット３，４０３に対応するアプリケーションファイルまたは、再生プログラム２２４に対応付けられた画像ファイル２２５、ＰＣＭ、圧縮Ａｕｄｉｏなどの音声ファイル２２６、テキスト、データベースなどの各種データファイル２２７の利用処理を行なう場合は、コンテンツ管理ユニット（ＣＰＳユニット）３，４０３に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ３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または各種ファイルを実行することになる。

【０１１４】

このように、ＲＯＭ型ディスク対応のＢＤＭＶ形式のデータ記録構成では、図５のメインコンテンツの構成から理解されるように、コンテンツ管理ユニット（ＣＰＳユニット）は、アプリケーション層からクリップまでの全ての階層を含む形で設定される。

【０１１５】

この形式に従ったユニット設定構成におけるユニット鍵の対応は、図６に示すようになる。図６に示すように、アプリケーション層において規定される「Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ」、「Ｔｏｐ　Ｍｅｎｕ」を含む各タイトル、アプリケーション、またはサブコンテンツのデータグループに対応付けてＣＰＳユニットが設定され、それぞれのユニット単位での暗号化処理が行なわれ利用制御が実行される。

【０１１６】

なお、暗号化の範囲は、クリップ内の実コンテンツデータのみとしてもよいが、このＢＤＭＶ形式のデータ記録構成を規定したアプリケーシ設定することが特徴となっている。ＲＯＭ型ディスクの場合、ディスクに記録されたコンテンツは不変であり、タイトルが増加することもなく、減少することもなく、データ更新を考慮する必要がないため、このようなユニット設定としている。

【０１１７】

（２－２）ＲＥ型，Ｒ型ディスク対応のＢＤＡＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ２）

次に、データの追記が可能なディスク、例えばＲ型、ＲＥ型ディスクの利用を想定したＲＥ型，Ｒ型ディスク対応のＢＤＡＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ２）について説明する。

【０１１８】

データの追記が可能なディスクを利用した場合、ディスクに格納されたコンテンツは追加、削除、編集などの更新がなされることを想定することが必要となる。ＢＤＡＶ形式のデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ２）では、このような処理に対応する構成を持つ。

【０１１９】

アプリケーションタイプ２において規定するコンテンツ管理ユニット（ＣＰＳユニット）の設定構成例について図７を参照して説明する。図７に示すように、アプリケーションタイプ２においては、コンテンツ管理ユニットは、クリップを単位として設定される。前述のアプリケーションタイプ１では、先に図５を参照して説明したようにアプリケーション層～クリップの全ての階層を含む形でコンテンツ管理ユニット（ＣＰＳユニット）の設定がなされていたが、アプリケーションタイプ２では、図７に示すように、コンテンツ管理ユニットは、クリップを単位として設定される。

【０１２０】

これは、ディスク記録コンテンツの追加、削除、編集などのデータ更新に対応するための構成である。ＲＥ型，Ｒ型ディスク対応のＢＤＡＶ形式のデータ記録構成に対応するアプリケーションタイプ２では、先に図４、図５を参照して説明した３つの層、すなわち、

（Ａ）アプリケーション層

（Ｂ）再生区間指定ファイル（プレイリスト）層

（Ｃ）クリップ（コンテンツデータファイル）層

これらの３層の関係についての規定がアプリケーションタイプ１に比較して緩やかとなっている。これは、コンテンツ編集を行なうと、タイトルやプレイリストの追加や削除などの処理を伴うことになり、タイトルやプレイリストとクリップの対応関係が変更されることが多いため、このような変更に対応した構成とするためである。

【０１２１】

アプリケーションタイプ２では、このようなデータ更新がなされることを想定し、実コンテンツを含むクリップのみを含むコンテンツ管理ユニット（ＣＰＳユニット）を設定し、タイトル等を含むアプリケーション層やプレイリストは、コンテンツ管理ユニットに含めない構成としたものである。このような構成により、コンテンツの追加、削除、編集等のデータ更新が容易になる。

【０１２２】

このアプリケーションタイプ２によるユニット鍵の設定構成について、図８を参照して説明する。このアプリケーションタイプ２では、図８に示すようにクリップに対応するＣＰＳユニットを設定し、各クリップ対応のユニット鍵が設定される。図８に示す例は、ＣＰＳユニット鍵ファイルの概念を説明する図である。実際のＣＰＳユニット鍵ファイルのデータ構成例について図９以下を参照して説明する。

【０１２３】

図９は、ＣＰＳユニット鍵ファイルの一構成例に対応するシンタックスを示す図である。図９に示すように、ＣＰＳユニット鍵ファイルには、ヘッダ情報を格納したユニット鍵ファイルヘッダ４２１と、ユニット鍵の暗号化データを格納したユニット鍵ブロック４２２が設定される。ユニット鍵ファイルヘッダ４２１の前には、ユニット鍵ブロックのスタートアドレス（Unit_Key_Block_start_address）が設定される。

【０１２４】

ユニット鍵ファイルヘッダ４２１の詳細、および、ユニット鍵ブロック４２２の詳細を図１０に示す。図１０（ａ）は、ユニット鍵ファイルヘッダの詳細であり、図１０（ｂ）は、ユニット鍵ブロックの詳細を示すシンタックスである。なお、図９、図１０に示すＣＰＳユニット鍵ファイルは、クリップ対応のＣＰＳユニットを設定した場合のＣＰＳユニット鍵ファイルの構成を示すものであり、先に図８を参照して説明したＣＰＳユニットの設定構成に対応するユニット鍵ファイルの設定例である。また、これは図９に示すユニット鍵ファイル構成に対応する。

【０１２５】

図１０（ａ）に示すように、ＣＰＳユニット鍵ファイルのヘッダ部には、以下のデータが含まれる。

（１）アプリケーションタイプ（Application_Type）：アプリケーションフォーマットの識別情報（例えば再生専用ディスク用フォーマット（BDMV）の場合１、記録再生ディスク用フォーマット（BDAV）の場合２）。なお、記録再生ディスクであっても、再生専用デ

ィスクフォーマットのフォーマットで記録ができるが、その場合には、アプリケーションタイプは再生専用ディスクフォーマット(BDMV)として記録する。
（２）ディレクトリ数（Num_of_BD_Directory）：ディレクトリ数（再生専用ディスク（BDMV）の場合は１のみ、記録再生ディスク（BDAV）の場合は１～５）
（３）メニューサムネイル＃１対応ＣＰＳユニット番号（CPS_Unit_number for Menu Thumbnail#I）：メニューサムネイル用のＣＰＳユニット番号
（４）マークサムネイル＃１対応ＣＰＳユニット番号（CPS_Unit_number for Mark Thumbnail#I）：マークサムネイル用のＣＰＳユニット番号
（５）ディレクトリＩのクリップ数（Num_of_Clip#I）：ディレクトリIの中に設定されたクリップ数
（６）ディレクトリＩに設定されたクリップのＩＤ＃Ｊ（Clip_ID#J in Directory #I）：クリップのＩＤ（ファイル名XXXXX.clpiのXXXXXに当たる10進5桁の数字）
ただし、このデータは、再生専用ディスク（BDMV）には設定しない構成としてもよい。
（７）ディレクトリ＃Ｉ、タイトル＃Ｊに対応するＣＰＳユニット番号（CPS_Unit_number for Title#J in Directory #I）：クリップのＩＤ（タイトル）に対応するＣＰＳユニット番号

【０１２６】

これらのデータがヘッダ情報として格納される。図９、図１０に示す構成を持つユニット鍵ファイルは、
各メニューサムネイル毎にＣＰＳユニット番号が対応付けられ、
各マークサムネイル毎にＣＰＳユニット番号が対応付けられ、
さらに、
各ディレクトリの各クリップ（＝タイトル）毎にＣＰＳユニット番号が対応付けられた構成である。

【０１２７】

図１０（ｂ）に示すＣＰＳユニット鍵ファイルのユニット鍵ブロックには、以下のデータが含まれる。
（１）ＣＰＳユニット数（Num_of_CPS_Unit）ディスク上のＣＰＳユニット数
（２）利用制御情報のＭＡＣ（MAC of Usage Rules#I）：ＣＰＳユニットに対応する利用制御情報（ＣＣＩ）ファイルデータの改竄検証用データとしてのＭＡＣ（Message Authentication Code）値
（３）メディアＩＤのＭＡＣ（MAC of Media ID#I）：メディアＩＤ［MediaID（記録型Discのシリアル番号）］の改竄検証用データとしてのＭＡＣ値
（４）各ＣＰＳユニット対応の暗号化ＣＰＳユニット鍵（Encrypted CPS Unit Key for CPS Unit#I）：ＣＰＳユニットごとに割り当てられるユニット鍵の暗号化データ

【０１２８】

なお、情報記録媒体が再生専用ディスク（BDMV）である場合のＢＤＭＶフォーマットと、記録再生ディスク（BDAV）である場合のＢＤＡＶフォーマットでは、データの記録処理あるいは再生処理を実行するアプリケーションが利用するディレクトリ構造が異なるが、図９および図１０に示すＣＰＳユニット鍵ファイルは、いずれのディスク、いずれのアプリケーションにも対応可能な構成となっている。なお、図９、図１０に示すＣＰＳユニット鍵ファイルのデータ構成は一例であり、必要に応じて、多少の構成データの変更は可能である。例えば、上述したように図１０（ａ）に示すユニット鍵ファイルヘッダ中、上述した（６）ディレクトリＩに設定されたクリップのＩＤ＃Ｊ（Clip_ID#J in Directory #I）：クリップのＩＤ（ファイル名XXXXX.clpiのXXXXXに当たる１０進５桁の数字）については、再生専用ディスク（BDMV）には設定しない構成としてもよい。

【０１２９】

情報記録媒体が記録再生ディスク（BDAV）である場合のＢＤＡＶフォーマットに対応するディレクトリ構造、すなわち情報記録媒体に記録されるデータに対応するディレクトリ構造を図１１に示す。データ部４３１は、各種の付加的な情報や制御情報の格納部であり

、前述した暗号鍵ブロックとしてのＭＫＢ（MKB.inf）と、上述したユニット鍵ファイル(Unit_Key.inf)と、さらに、各ＣＰＳユニットに対応するコンテンツの利用制御情報（ＣＣＩ：Copy Control Information）(CPSUnitxxxxxx.cci)が設定される。

【０１３０】

データ部４３２は、各種のＢＤＡＶフォーマットに従ったデータとしてのインデックス情報（info.bdav）、静止画コンテンツを構成するメニューサムネイル(Menu.tidx, Menu.tidx1)、マークサムネイル(Mark.tidx, Mark.tidx1)、さらに、動画コンテンツを構成するプレイリスト(PLAYLISTにある0001.mpls等)、クリップ(CLIPINFにある01001.clpi等)、ストリームデータファイル(STREAMにある01001.m2ts等)が設定される。

【０１３１】

（２－３）ＲＯＭ型ディスク対応のＢＤＭＶ形式でのリアルタイム記録に適したデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ３）

次に、ＲＯＭ型ディスク対応のＢＤＭＶ形式でのリアルタイム記録に適したデータ記録構成およびコンテンツ利用アプリケーションであるアプリケーションタイプ３について説明する。

【０１３２】

このアプリケーションタイプは、既存のタイプではなく、新規に提案する構成であり、たとえば放送コンテンツのリアルタイム記録などに適したデータ記録構成、コンテンツ管理ユニット（ＣＰＳユニット）設定構成を有する。このアプリケーションタイプ３に従ったコンテンツ管理ユニット（ＣＰＳユニット）の設定例について、図１２を参照して説明する。

【０１３３】

図１２に示すように、アプリケーションタイプ３は、ＢＤＭＶ形式に従ったデータ記録構成を有し、先に図４、図５を参照して説明したアプリケーションタイプ１と同様、

（Ａ）アプリケーション層

（Ｂ）再生区間指定ファイル（プレイリスト）層

（Ｃ）クリップ（コンテンツデータファイル）層

これらの３層の関係について明確に規定されている。この対応関係の規定は、アプリケーションタイプ１と同様であるが、図１２に示すように、アプリケーションタイプ３では、コンテンツ管理ユニット（ＣＰＳユニット）をクリップを単位として設定し、（Ａ）アプリケーション層、（Ｂ）再生区間指定ファイル（プレイリスト）層を含めない構成としている。このクリップを単位とする設定は、前述のＢＤＡＶ形式のアプリケーションタイプ２に類似するものである。すなわち、アプリケーションタイプ３は、ＢＤＭＶ形式において、ＢＤＡＶ形式型のコンテンツ管理ユニット（ＣＰＳユニット）設定構成を採用したものである。

【０１３４】

図１２に示す例では、３つのコンテンツ管理ユニット（ＣＰＳユニット）として、

ＣＰＳユニット１，５０１、

ＣＰＳユニット２，５０２、

ＣＰＳユニット３，５０３、

を設定した例を示している。これらのＣＰＳユニットは、クリップを単位として設定されたコンテンツ管理ユニット（ＣＰＳユニット）である。すなわち、クリップ情報ＡＶストリームを含むクリップを単位として設定されたＣＰＳユニットであり、アプリケーション層のタイトル情報や、プレイリストは、ユニットの構成要素から除外された構成となっている。

【０１３５】

例えば、放送コンテンツなどをディスクにリアルタイム記録する場合、タイトルやプレイリスト等は含まないコンテンツの実体データと、必要となる属性データのみが配信され、情報処理装置では、これらの受信データをディスクに記録することになる。このようなリアルタイム記録においては受信データに含まれるデータのみを暗号化して記録すること

で処理の効率化が実現されることになる。このアプリケーションタイプ３は、このようなリアルタイム記録に適する構成を実現する。

【０１３６】

さらに、アプリケーションタイプ３は、アプリケーションタイプ２と同様、コンテンツの編集にも適した構成である。アプリケーション３は、データの追記の可能なＲ型、ＲＥ型ディスクに対応するアプリケーションタイプであり、記録コンテンツの追加、削除、編集などの更新に対応したアプリケーションである。

【０１３７】

図１３に、異なる複数の異なるＣＰＳユニットにまたがるプレイリストを設定する編集処理を実行した場合の構成例を示す。例えば、図１３に示すＣＰＳユニット４，５０４が新たにディスクに追加記録したコンテンツを含むクリップである新たなＣＰＳユニット４，５０４であるとする。このＣＰＳユニット４，５０４に含まれるコンテンツをプレイリスト５１１によって再生指定可能とするデータ編集を行なう。この編集処理により、プレイリスト５１１には、ＣＰＳユニット４，５０４に含まれるコンテンツを再生区間指定情報が含まれる設定となる。すなわち、プレイリスト５１１は、図１３に示すＣＰＳユニット３，５０３とＣＰＳユニット４，５０４の２つのクリップを再生区間指定情報として含むプレイリストとして設定されることになる。

【０１３８】

このように、プレイリストやタイトルを含めず、クリップのみを構成要素とするコンテンツ管理ユニット（ＣＰＳユニット）の設定を可能としたアプリケーションタイプ３では、コンテンツの追加、削除、編集等のデータ更新に柔軟に対応することができる。

【０１３９】

このアプリケーションタイプ３に対応するユニット鍵の設定構成について、図１４を参照して説明する。このアプリケーションタイプ３では、図１４に示すようにクリップに対応するＣＰＳユニットを設定し、各クリップ対応のユニット鍵が設定される。図１４に示す例は、ＣＰＳユニット鍵ファイルの概念を説明する図である。実際のＣＰＳユニット鍵ファイルのデータ構成は、先に説明したアプリケーションタイプ２のＣＰＳユニット鍵ファイルのデータ構成と同様図９に示す構成を持つ。すなわち、図９を参照して説明したように、ヘッダ情報を格納したユニット鍵ファイルヘッダ４２１と、ユニット鍵の暗号化データを格納したユニット鍵ブロック４２２が設定される。ユニット鍵ファイルヘッダ４２１の前には、ユニット鍵ブロックのスタートアドレス（Unit_Key_Block_start_address）が設定される。

【０１４０】

アプリケーションタイプ３におけるユニット鍵ファイルヘッダ４２１の詳細、および、ユニット鍵ブロック４２２の詳細を図１５に示す。図１５（ａ）は、ユニット鍵ファイルヘッダの詳細であり、図１５（ｂ）は、ユニット鍵ブロックの詳細を示すシンタックスである。この構成も、先に図１０を参照して説明したアプリケーションタイプ２のＣＰＳユニット鍵ファイルのデータ構成とほぼ同様である。ただし、アプリケーションタイプ情報には、アプリケーションタイプ３であることを示す情報が記録される。アプリケーションタイプ３では、アプリケーションタイプ２と同様、クリップ単位でＣＰＳユニットが設定され、ＣＰＳユニット鍵が割り当てられる。

【０１４１】

このアプリケーションタイプ３に対応するＢＤＭＶフォーマットに対応するディレクトリ構造、すなわち、アプリケーションタイプ３に対応して情報記録媒体に記録されるデータに対応するディレクトリ構造を図１６に示す。データ部５３１は、各種の付加的な情報や制御情報の格納部であり、前述した暗号鍵ブロックとしてのＭＫＢ（MKB.inf）と、上述したユニット鍵ファイル(Unit_Key.inf)と、さらに、各ＣＰＳユニットに対応するコンテンツの利用制御情報（ＣＣＩ：Copy Control Information）(CPSUnitxxxxxx.cci)が設定される。データ部５３２は、各種のＢＤＭＶフォーマットに従ったデータとしてのインデックス情報（info.bdmv）、再生プログラムとしてのムービーオブジェクト（MovieObje

ct.bdmv）さらに、動画コンテンツを構成するプレイリスト(PLAYLISTにある0001.mpls等)、クリップ(CLIPINFにある01001.clpi等)、ストリームデータファイル(STREAMにある01001.m2ts等)が設定される。

【０１４２】

なお、前述したアプリケーションタイプ１、すなわちＲＯＭ型ディスクに対応するフォーマットに対応するアプリケーションタイプ１の場合、コンテンツの利用制御情報（ＣＣＩ：Copy Control Information）には、コンテンツの正当性を証明するデータとして特定の管理者の電子署名が付与されたコンテンツ証明書［ＣＣ：Ｃｏｎｔｎｔ　Ｃｅｒｔ］が格納されるが、このアプリケーションタイプ３では、記録コンテンツとして、例えば放送コンテンツ等、リアルタイム記録されたコンテンツ等を想定しており、コンテンツの利用制御情報（ＣＣＩ：Copy Control Information）には、コンテンツ証明書を含むことは必須としない。

【０１４３】

（２－４）ＲＯＭ型ディスク対応のＢＤＭＶ形式でのダウンロード記録に適したデータ記録構成およびコンテンツ利用アプリケーション（アプリケーションタイプ４）

次に、ＲＯＭ型ディスク対応のＢＤＭＶ形式でのダウンロード記録に適したデータ記録構成およびコンテンツ利用アプリケーションであるアプリケーションタイプ４について説明する。

【０１４４】

このアプリケーションタイプは、既存のタイプではなく、新規に提案する構成であり、たとえば放送コンテンツのリアルタイム記録などに適したデータ記録構成、コンテンツ管理ユニット（ＣＰＳユニット）設定構成を有する。このアプリケーションタイプ４に従ったコンテンツ管理ユニット（ＣＰＳユニット）の設定例について、図１７を参照して説明する。

【０１４５】

図１７に示すように、アプリケーションタイプ４は、ＢＤＭＶ形式に従ったデータ記録構成を有し、先に図４、図５を参照して説明したアプリケーションタイプ１と同様、

（Ａ）アプリケーション層

（Ｂ）再生区間指定ファイル（プレイリスト）層

（Ｃ）クリップ（コンテンツデータファイル）層

これらの３層の関係について明確に規定されている。この対応関係の規定は、アプリケーションタイプ１と同様である。また、図１７に示すように、アプリケーションタイプ４におけるコンテンツ管理ユニット（ＣＰＳユニット）の設定単位も、アプリケーションタイプ１と同様、クリップを構成用素とするコンテンツ管理ユニット（ＣＰＳユニット）を設定する場合、（Ａ）アプリケーション、（Ｂ）再生区間指定ファイル（プレイリスト）、（Ｃ）クリップ（コンテンツデータファイル）のすべてを含むユニットとして設定する。

【０１４６】

図１７に示す例では、クリップを構成用素とするコンテンツ管理ユニット（ＣＰＳユニット）は、ＣＰＳユニット６０１，６０２であり、これらは、いずれも、（Ａ）アプリケーション、（Ｂ）再生区間指定ファイル（プレイリスト）、（Ｃ）クリップ（コンテンツデータファイル）のすべてを含むユニットとして設定されている。

【０１４７】

このように、アプリケーションタイプ４のコンテンツ管理ユニット（ＣＰＳユニット）の設定単位は、アプリケーションタイプ１と同様のものとなる。ただし、アプリケーションタイプ４では、例えばコンテンツサーバからのダンンロードコンテンツの記録データを想定しており、正当なサーバからの提供コンテンツであることの確認が可能な情報が管理情報として設定される。この構成については後述する。

【０１４８】

このアプリケーションタイプ４に対応するユニット鍵の設定構成について、図１８を参

照して説明する。このアプリケーションタイプ４は、図１８に示すように、先に図６を参照して説明したアプリケーションタイプ１と同様のユニット鍵設定構成を持つ。すなわち、少なくともメインコンテンツについては、最上位層のアプリケーション層のインデックス情報などタイトル単位でのユニット設定がなされ、これらのユニットに対応してユニット鍵割り当てが実行される。

【０１４９】

ＣＰＳユニット鍵ファイルのデータ構成は、他のアプリケーションタイプ１～３のＣＰＳユニット鍵ファイルのデータ構成と同様である。例えば、図９に示す構成を持つ。すなわち、図９を参照して説明したように、ヘッダ情報を格納したユニット鍵ファイルヘッダ４２１と、ユニット鍵の暗号化データを格納したユニット鍵ブロック４２２が設定される。ユニット鍵ファイルヘッダ４２１の前には、ユニット鍵ブロックのスタートアドレス（Unit_Key_Block_start_address）が設定される。

【０１５０】

アプリケーションタイプ４におけるユニット鍵ファイルヘッダ４２１の詳細、および、ユニット鍵ブロック４２２の詳細を図１９に示す。図１９（ａ）は、ユニット鍵ファイルヘッダの詳細であり、図１９（ｂ）は、ユニット鍵ブロックの詳細を示すシンタックスである。アプリケーションタイプ４では、アプリケーションタイプ１と同様、アプリケーション層におけるタイトル単位でＣＰＳユニットが設定され、ＣＰＳユニット鍵が割り当てられる。

【０１５１】

このアプリケーションタイプ４に対応するＢＤＭＶフォーマットに従って情報記録媒体に記録されるデータに対応するディレクトリ構造例を図２０に示す。データ部６２１は、各種の付加的な情報や制御情報の格納部である。他のアプリケーションタイプと同様、前述した暗号鍵ブロックとしてのＭＫＢ（MKB.inf）と、上述したユニット鍵ファイル(Unit_Key.inf)と、さらに、各ＣＰＳユニットに対応するコンテンツの利用制御情報（ＣＣＩ：Copy Control Information）(CPSUnitxxxxxx.cci)が設定される。

【０１５２】

さらに、アプリケーションタイプ４では、これらの情報の他、コンテンツの正当性を証明するコンテンツ証明書（ＣＣ：Ｃｏｎｔｅｎｔ　Ｃｅｒｔ）６３１、コンテンツのハッシュ値を格納したコンテンツハッシュテーブル（ＣＨＴ：Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）６３２、コンテンツを利用しようとする情報処理装置のリボーク状況、すなわち、情報処理装置の保持する公開鍵証明書が無効化されているか否かを示す証明書リボケーションリスト（ＣＲＬ:Certificate Revocation list）６３３、さらに、コンテンツが正当な特定サーバから送信されたものであることを証明するサーババインド処理情報６３４が設定される。サーババインド処理情報６３４は、コンテンツ送信サーバのＩＤ情報を含み、コンテンツ管理者の電子署名が付加されたデータであり、コンテンツが正当な特定サーバから送信されたものであることを証明するデータである。これらの情報を適用した処理については、後述する。

【０１５３】

データ部６２２は、各種のＢＤＭＶフォーマットに従ったデータとしてのインデックス情報（info.bdmv）、再生プログラムとしてのムービーオブジェクト（MovieObject.bdmv）さらに、動画コンテンツを構成するプレイリスト(PLAYLISTにある0001.mpls等)、クリップ(CLIPINFにある01001.clpi等)、ストリームデータファイル(STREAMにある01001.m2ts等)が設定される。

【０１５４】

なお、記録可能なディスクであるＲ型、ＲＥ型の情報記録媒体を利用した場合、情報記録媒体に記録されるコンテンツは、ダウンロードコンテンツばかりではなく、前述したアプリケーションタイプ３に従ったリアルタイム記録コンテンツもあり、これらのコンテンツが混在する場合がある。これらのコンテンツを明確に区分可能とするため、ディレクトリをアプリケーションタイプ３に従ったリアルタイム記録コンテンツのディレクトリと、

アプリケーションタイプ４に従ったダウンロードコンテンツとに区分して設定する構成としてもよい。例えば、図２１に示すようなディレクトリ構造である。

【０１５５】

図２１に示すディレクトリ構造は、アプリケーションタイプ４に従ったダウンロードコンテンツ専用のディレクトリであり、ディレクトリＡＡＣＳ＿ｍｖ＿ｄｏｗｎｌｏａｄ６５１以下に、アプリケーションタイプ４に従ったダウンロードコンテンツに対応する管理情報およびコンテンツが設定される。ディレクトリＢＤＭＶ＿ＤＯＷＮＬＯＡＤ以下には、アプリケーションタイプ４に従ったダウンロードコンテンツ対応のデータとしてのインデックス情報（info.bdmv）、再生プログラムとしてのムービーオブジェクト（MovieObject.bdmv）さらに、動画コンテンツを構成するプレイリスト(PLAYLISTにある0001.mpls等)、クリップ(CLIPINFにある01001.clpi等)、ストリームデータファイル(STREAMにある01001.m2ts等)が設定される。

【０１５６】

なお、このディレクトリ設定構成の場合は、図には示していないが、アプリケーションタイプ３に従ったリアルタイム記録コンテンツ専用のディレクトリも設定されることになる。

【０１５７】

次に、図２２、図２３を参照して、アプリケーションタイプ４に従ってサーバから取得するダウンロードコンテンツのディスクに対する記録処理、および利用（再生など）処理のシーケンスについて説明する。

【０１５８】

図２２と、図２３の差異は、コンテンツの復号に適用するＣＰＳユニット鍵の導出手法が異なる。図２２に示す処理シーケンスは、先に説明したアプリケーションタイプ２、すなわちＢＤＡＶ形式に従ったフォーマットでのデータ記録、再生シーケンスと同様のシーケンスでのＣＰＳユニット鍵を導出可能とした設定である。

【０１５９】

なお、この設定では、ダウンロードコンテンツ（アプリケーションタイプ４）をアプリケーションタイプ２のコンテンツに置きかえることができると、コンテンツリボークのしくみを回避したコンテンツ再生ができてしまうが、コンテンツ再生の許容条件として、コンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）、証明書リボケーションリスト（ＣＲＬ）、サーババインド処理情報を検証して、検証の成立が確認されることを必須とすることで、アプリケーションタイプ４のコンテンツを、アプリケーションタイプ２のコンテンツと区別したコンテンツ利用制御を行うこととし、不正な利用を防止する構成としている。従って、例えば、ダウンロードコンテンツのＣＰＳ＿Ｕｎｉｔ鍵ファイルのヘッダを書き換えてＡｐｐｌｉｃａｔｉｏｎＴｙｐｅ＝２として再登録するような行為を行なっても、正規の再生機器（Ｐｌａｙｅｒ）では再生できないような設定とする。

【０１６０】

一方、図２３に示す処理シーケンスは、コンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）、サーババインド情報のどちらか一方、または両方をＣＰＳユニット鍵の導出に必要とする情報として設定した例である。これらの情報をＣＰＳユニット鍵の導出に使用することにより、ダウンロードコンテンツ（ＡｐｐｌｉｃａｔｉｏｎＴｙｐｅ＝４）に対してデータの変更を行なってＡｐｐｌｉｃａｔｉｏｎＴｙｐｅ＝２の状態に書き換えることが鍵生成の仕組み上不可能になる。ＰｌａｙｅｒはＡｐｐｌｉｃａｔｉｏｎＴｙｐｅをチェックして鍵生成方法を切り替えることになる。

【０１６１】

まず、図２２に示す処理例について説明する。図２２において、情報処理装置７１０は、ＣＰＳユニット対応コンテンツを情報記録媒体７５０に記録する処理、情報処理装置７２０は、情報記録媒体７５０に記録されたＣＰＳユニット対応コンテンツを読み取り復号、再生する処理を実行する装置として示している。なお、情報処理装置７１０，７２０は同一の装置であってもよい。

【０１６２】
まず、アプリケーションタイプ４のダウンロードコンテンツであるＣＰＳユニット対応コンテンツを情報記録媒体７５０に記録する処理について、情報処理装置７１０側のシーケンスに沿って説明する。ＣＰＳユニットを新たに情報記録媒体７５０に記録する際、まず、情報処理装置７５０は、ステップＳ３１において、自装置のメモリに格納されたデバイス鍵７１１を取得し、メディア鍵を格納した暗号鍵ブロックであるＭＫＢの処理によってメディア鍵を取得する。
【０１６３】
デバイス鍵７１１は、先に説明したように、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。ＭＫＢ（Media Key Block）７１２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、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。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。
【０１６４】
なお、ＭＫＢ７１２は、ダウンロードコンテンツとともに、サーバから受信するデータを利用可能であり、あるいは、情報記録媒体７５０に予め記録されたＭＫＢ７５１を読み取って利用することが可能である。あるいはその他の記録媒体等のメディア、あるいはネットワークを介してサーバから取得するなどの処理によって取得することも可能である。
【０１６５】
次に、ステップＳ３２において、バインドシード７１３を適用したバインドシード処理、すなわち、例えばメディア鍵［Ｋｍ］を適用したバインドシードのＡＥＳ暗号化処理によって、バインド鍵、すなわちＣＰＳユニット鍵を暗号化するための暗号鍵（バインド鍵）を生成する。バインドシード７１３は、例えば乱数生成処理によって生成される。なお、情報記録媒体７５０にはバインドシード７５２が記録される。
【０１６６】
さらに、図のステップとしては示していないが、コンテンツとともに、サーバからダウンロードされるコンテンツ対応の管理データ、すなわち、コンテンツの正当性を証明するコンテンツ証明書（ＣＣ：Ｃｏｎｔｅｎｔ　Ｃｅｒｔ）７５３、コンテンツのハッシュ値を格納したコンテンツハッシュテーブル（ＣＨＴ：Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）７５４、コンテンツを利用しようとする情報処理装置のリボーク状況、すなわち、情報処理装置の保持する公開鍵証明書が無効化されているか否かを示す証明書リボケーションリスト（ＣＲＬ:Certificate Revocation list）７５５、さらに、コンテンツが正当な特定サーバから送信されたものであることを証明するサーババインド処理情報７５６、これらの情報が、情報記録媒体７５０に記録する。
【０１６７】
ステップＳ３３は、ユニット鍵７１４の暗号化処理実行ステップである。ユニット鍵７１４は、記録対象とするコンテンツ７１６の属するＣＰＳユニットに対応するＣＰＳユニット鍵であり、例えば、コンテンツと共にサーバから受信する。あるいは、情報処理装置において乱数に基づいて生成する。ユニット鍵７１４は、ステップＳ３３においてバインドシードに基づいて生成した暗号鍵であるバインド鍵（Ｋｂ）と、ＣＰＳユニットに対応する利用制御情報（ＣＣＩ）７１５を利用して暗号化処理がなされ、ＣＰＳユニット鍵ファイル７５７として情報記録媒体７５０に記録する。
ステップＳ３３の処理は、例えば、
［Ｅｎｃ（Ｋｂ，ｆ（Ｋｕ＿ｎ，ＣＣＩ））］
上記式によって示される暗号化データとして暗号化ユニット鍵が生成される。ここで、

暗号鍵［Ｋｂ］は、バインドシードに基づいて生成した暗号鍵である。Ｅｎｃ（ａ，ｂ）はデータｂの鍵ａによる暗号化データを示している。また、ｆ（ａ，ｂ）はデータａとデータｂとに基づく演算結果データであり、例えばａとｂとの排他論理和演算結果である。

【０１６８】

なお、［Ｅｎｃ（Ｋｂ，ｆ（Ｋｕ＿ｎ，ＣＣＩ））］

は、例えばＣＰＳユニット＃ｎに対応するユニット鍵＃ｎと、ＣＰＳユニット＃ｎに対応する利用制御情報（ＣＣＩ＃ｎ）との排他論理和結果に対して、バインドシードに基づいて生成した暗号鍵［Ｋｂ］を適用して暗号化したデータを示している。このようにして生成した暗号化されたユニット鍵を格納したＣＰＳユニット鍵ファイル７５７を情報記録媒体７５０に記録する。なお、情報記録媒体には、利用制御情報（ＣＣＩ）７５８も記録される。

【０１６９】

なお、複数のユニット鍵を構成要素とするユニット鍵ファイルを設定する場合は、各ユニット鍵の連結データから構成される１つのユニット鍵ファイルに対してバインド鍵による暗号化する構成、あるいは各ＣＰＳユニット鍵と各ＣＰＳユニット対応の利用制御情報（ＣＣＩ）との連結データから構成される１つのユニット鍵ファイルに対してバインド鍵による暗号化を実行する構成としてもよい。

【０１７０】

情報処理装置７１０は、さらに、ステップＳ３４において、ユニット鍵７１４を適用して、コンテンツ７１６を暗号化する。コンテンツ７１６は、例えばダウンロードコンテンツとしてのＣＰＳユニットに含まれるＡＶストリームデータである。ステップＳ３４における暗号化結果としての暗号化コンテンツ７５９が情報記録媒体７５０に記録される。なお、情報記録媒体７５０の記録データとして示している暗号化コンテンツ７５９は、アプリケーションタイプ４に対応するダウンロードコンテンツとしてのＣＰＳユニットに相当する。

【０１７１】

次に、情報記録媒体７５０に格納されたコンテンツの再生処理について、情報処理装置７２０側のシーケンスに従って説明する。情報処理装置７２０は、まず、ステップＳ５０において、情報記録媒体７５０に格納されたコンテンツ正当性を証明するコンテンツ証明書（ＣＣ：Ｃｏｎｔｅｎｔ　Ｃｅｒｔ）７５３、コンテンツのハッシュ値を格納したコンテンツハッシュテーブル（ＣＨＴ：Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）７５４、コンテンツを利用しようとする情報処理装置のリボーク状況、すなわち、情報処理装置の保持する公開鍵証明書が無効化されているか否かを示す証明書リボケーションリスト（ＣＲＬ:Certificate Revocation list）７５５、さらに、コンテンツが正当な特定サーバから送信されたものであることを証明するサーババインド処理情報７５６を読み取り、これらの各証明書に基づく検証処理を実行する。

【０１７２】

すなわち、コンテンツ証明書７５３と、コンテンツハッシュテーブル７５４の検証に基づいてコンテンツの正当性を確認し、証明書リボケーションリスト（ＣＲＬ）７５５に基づいて情報処理装置がリボークされていないことを確認し、サーババインド処理情報７５６に基づいて、コンテンツが正当サーバから送信されたコンテンツであることを確認する。これらの確認がなされた場合に、ステップＳ５１に進む。これらの確認がなされなかった場合は、処理は中止される。ステップＳ５１においては、デバイス鍵７２１を適用して情報記録媒体７５０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ＭＫＢ７５１の復号処理を実行して、メディア鍵Ｋｍを取得する。

【０１７３】

次に、ステップＳ５２において、ステップＳ５１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７５０から読み取ったバインドシード７５２とに基づく暗号処理によって、暗号鍵（バインド鍵）Ｋｂ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。

【０１７４】
次に、ステップＳ５３において、バインド鍵Ｋｂによって、情報記録媒体７５０から読み取ったＣＰＳユニット鍵ファイル７５７に含まれる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７５７は、各ＣＰＳユニットに対応して設定されるユニット鍵［Ｋｕｎ］の暗号化データを格納したファイルである。ユニット鍵ファイルは、前述したように、例えば、［Ｅｎｃ（Ｋｂ，ｆ（Ｋｕ＿ｎ，ＣＣＩ））］の構成を持つ暗号化データとしてユニット鍵を格納している。この暗号化データに対して、バインド鍵Ｋｂによる復号、利用制御情報（ＣＣＩ）による演算、例えば排他論理和演算を実行して、ＣＰＳユニット鍵を取得する。

【０１７５】
すなわち、バインド鍵Ｋｂによる、下記の暗号化ユニット鍵、
［Ｅｎｃ（Ｋｂ，ｆ（Ｋｕ＿ｎ，ＣＣＩ））］
を復号して、データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）
を取得し、データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）に対して、情報記録媒体７５０から読み取った利用制御情報（ＣＣＩ）７５８を適用した演算処理を実行して、ユニット鍵［Ｋｕ＿ｎ］を得る。データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ）が、ユニット鍵［Ｋｕ＿ｎ］と、利用制御情報［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利用制御情報［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。

【０１７６】
次に、ステップＳ５４において、情報記録媒体７５０から読み取った暗号化コンテンツ７５９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、コンテンツ７２５を取得する。

【０１７７】
なお、図２２には、ＣＰＳユニット対応コンテンツの記録、再生処理のシーケンスを１つの情報処理装置の実行シーケンスとして示してあるが、例えば情報記録媒体に対するアクセスを行うドライブ装置を備えた、または接続したＰＣなどの情報処理装置によってコンテンツの記録や再生を行なう場合のＣＰＳユニット鍵ファイルの記録や、ＣＰＳユニット鍵ファイルからのＣＰＳユニット鍵の取得処理は、ＰＣ等の情報処理装置側のホストと、情報記録媒体に対するデータ記録読み取りを実行するドライブとの両者間のデータ送受信を介して行なわれる。

【０１７８】
次に、図２３に示す処理シーケンスについて説明する。この処理シーケンスは、コンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）、サーババインド情報のどちらか一方、または両方をＣＰＳユニット鍵の導出に必要とする情報として設定した例である。これらの情報をＣＰＳユニット鍵の導出に使用することにより、ダウンロードコンテンツ（ＡｐｐｌｉｃａｔｉｏｎＴｙｐｅ＝４）に対してデータの変更を行なってＡｐｐｌｉｃａｔｉｏｎＴｙｐｅ＝２の状態に書き換えることが鍵生成の仕組み上不可能になる。ＰｌａｙｅｒはＡｐｐｌｉｃａｔｉｏｎＴｙｐｅをチェックして鍵生成方法を切り替えることになる。

【０１７９】
基本的な処理の流れは、コンテンツ記録処理、コンテンツ利用（再生）処理とも、図２２を参照して説明した処理とほぼ同様であるので、図２２のシーケンスと異なる点について説明する。

【０１８０】
図２３に示すシーケンスにおいて、コンテンツを情報記録媒体７５０に記録する場合、情報処理装置７１０は、ステップＳ３３のユニット鍵暗号化処理において、コンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）７１７、サーババインド情報７１８のどちらか一方、または両方を適用した暗号化を実行する。これらのコンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）７１７、サーババインド情報７１８は、コンテンツを受信したサーバ

から受信したデータであり、情報記録媒体７５０に記録されるコンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）７５３、サーババインド情報７５６と同一データである。

【０１８１】

ステップＳ３３では、ユニット鍵７１４の暗号化処理を、バインドシードに基づいて生成した暗号鍵であるバインド鍵（Ｋｂ）と、ＣＰＳユニットに対応する利用制御情報（ＣＣＩ）７１５と、コンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）７１７、サーババインド情報７１８のどちらか一方、または両方を適用した暗号化処理として実行する。

ステップＳ３３の処理は、例えば、

［Ｅｎｃ（Ｋｂ，ｆ（Ｋｕ＿ｎ，ＣＣＩ，ＣＣ，サーババインド情報））］

上記式によって示される暗号化データとして暗号化ユニット鍵が生成される。ここで、暗号鍵［Ｋｂ］は、バインドシードに基づいて生成した暗号鍵である。Ｅｎｃ（ａ，ｂ）はデータｂの鍵ａによる暗号化データを示している。また、ｆ（ａ，ｂ，ｃ，ｄ）はデータａ，ｂ，ｃ，ｄとに基づく演算結果データであり、例えばａ，ｂ，ｃ，ｄとの排他論理和演算結果である。

【０１８２】

このようにして生成した暗号化されたユニット鍵を格納したＣＰＳユニット鍵ファイル７５７を情報記録媒体７５０に記録する。なお、情報記録媒体には、利用制御情報（ＣＣＩ）７５８も記録される。コンテンツ記録に関するその他の処理は、先に図２２を参照して説明した処理と同様である。

【０１８３】

コンテンツ利用（再生）を行なう情報処理装置７２０の処理において、先に説明した図２２に示すシーケンスと異なる点は、ステップＳ５３のユニット鍵データの復号処理である。図２２の処理シーケンスのステップＳ５３では、バインド鍵Ｋｂによって、情報記録媒体７５０から読み取ったＣＰＳユニット鍵ファイル７５７に含まれる暗号化ユニット鍵の復号処理を行なう構成であったが、図２３に示すシーケンスでは、バインド鍵の他、情報記録媒体７５０に記録されたコンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）７５３と、サーババインド情報７５６との少なくともいずれかと、利用制御情報（ＣＣＩ）７５８による演算処理によって、ＣＰＳユニット鍵ファイル７５７に含まれる暗号化ユニット鍵の復号処理を行なう。

【０１８４】

ユニット鍵ファイルは、前述したように、例えば、［Ｅｎｃ（Ｋｂ，ｆ（Ｋｕ＿ｎ，ＣＣＩ，ＣＣ，サーババインド情報））］の構成を持つ暗号化ユニット鍵を含むデータとして情報記録媒体７５０に記録されている。この暗号化データに対して、バインド鍵Ｋｂによる復号、利用制御情報（ＣＣＩ）７５８、コンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）７５３、サーババインド情報７５６による演算、例えば排他論理和演算を実行して、ＣＰＳユニット鍵を取得する。

【０１８５】

すなわち、バインド鍵Ｋｂによる、下記の暗号化ユニット鍵、

［Ｅｎｃ（Ｋｂ，ｆ（Ｋｕ＿ｎ，ＣＣＩ，ＣＣ，サーババインド情報））］

を復号して、データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ，ＣＣ，サーババインド情報）

を取得し、データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ，ＣＣ，サーババインド情報）に対して、情報記録媒体７５０から読み取った利用制御情報（ＣＣＩ）７５８、コンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）７５３、サーババインド情報７５６を適用した演算処理を実行して、ユニット鍵［Ｋｕ＿ｎ］を得る。

【０１８６】

例えば、データ［Ｋｔ］＝ｆ（Ｋｕ＿ｎ，ＣＣＩ，ＣＣ，サーババインド情報）が、ユニット鍵［Ｋｕ＿ｎ］と、利用制御情報［ＣＣＩ］と、コンテンツ証明書（ＣＣ）、サーババインド情報との排他論理和（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利用制御情報［ＣＣＩ］、コンテンツ証明書（ＣＣ）、サーババインド情報の排他論理和（ＸＯＲ）演算を実行することで、ユニット鍵［Ｋ

ｕ＿ｎ］を取得することができる。

【０１８７】

次に、ステップＳ５４において、情報記録媒体７５０から読み取った暗号化コンテンツ７５９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、コンテンツ７２５を取得する。

【０１８８】

このように、図２３に示すシーケンスでは、コンテンツの復号に適用するＣＰＳユニット鍵を取得するための処理として実行されるＣＰＳユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理において、コンテンツ証明書（ＣＣ：ＣｏｎｔｅｎｔＣｅｒｔ）７５３、サーババインド情報７５６の少なくともいずれかの情報を適用することが必要となり、前述のアプリケーションタイプ２とは異なる処理によってのみコンテンツ利用が可能となり、例えば、ダウンロードコンテンツ（ＡｐｐｌｉｃａｔｉｏｎＴｙｐｅ＝４）に対してデータの変更を行なってＡｐｐｌｉｃａｔｉｏｎＴｙｐｅ＝２の状態に書き換えることが鍵生成の仕組み上不可能になる。

【０１８９】

なお、アプリケーションタイプの異なるコンテンツが情報記録媒体に記録されている場合は、コンテンツの利用（再生）を行なう情報処理装置は、まず、利用コンテンツのアプリケーションタイプを判別して、判別したアプリケーションタイプに応じたコンテンツの復号、利用シーケンスを実行する。

【０１９０】

［３．コンテンツ再生処理］

次に、図２４に示すフローチャートを参照して、様々なアプリケーションタイプ、すなわち上述したアプリケーションタイプ１～４のいずれかに対応するコンテンツを格納した情報記録媒体からコンテンツを読み取り、再生する場合に情報処理装置が実行する処理について説明する。図２４に示すフローに従ったシーケンスは、ＡＡＣＳにおいて規定されるコンテンツの再生処理を行なうためのプログラムを情報処理装置の制御部において実行して行なわれる処理シーケンスであり、情報記録媒体の記録コンテンツのアプリケーションタイプを判別し、各タイプに従ったコンテンツ再生を実行する。

【０１９１】

まず、情報処理装置は、ステップＳ３０１において、情報処理装置に装着した情報記録媒体（ディスク）の判別処理を実行する。このディスク判別は、装着ディスクが再書き込みの許容されないＲＯＭディスクであるか、または再書き込みの許容されるＲディスクまたはＲＥディスクであるかを判別する処理である。このディスク判別は、ディスクに記録されたディスク情報（Ｄｉｓｃ　Ｉｎｆｏｒｍａｔｉｏｎ）の読み取りによる判別、または、ディスクの反射率、ウォブルの有無などの物理的なディスク判別処理のいずれかによって実行される。

【０１９２】

まず、ディスクがデータ再書き込みの許容されないＲＯＭディスクである場合の処理について説明する。この場合、ステップＳ３２１において、ディスクの記録データに対応するディレクトリにＡＡＣＳディレクトリが設定されているか否かを判定する。ＡＡＣＳディレクトリが設定されていない場合、ステップＳ３２２に進み、ＡＡＣＳ対応コンテンツを格納した正当なＲＯＭディスクではないと判定し、コンテンツの利用を行なうことなく、処理を中止する。

【０１９３】

ステップＳ３２１において、ディスクの記録データに対応するディレクトリにＡＡＣＳディレクトリが設定されていると判定した場合は、ステップＳ３２３に進み、コンテンツタイプがアプリケーションタイプ１であるか否かを判定する。この判定処理は、コンテンツに対応する属性データ、あるいはユニット鍵ファイルの格納データなどに基づいて判定することができる。格納コンテンツがアプリケーションタイプ１であることが確認されない場合は、ステップＳ３２４に進み、エラーと判定し、処理を中止する。格納コンテンツ

がアプリケーションタイプ１であることが確認された場合は、アプリケーションタイプ１に対応するコンテンツ再生シーケンスを実行する。具体的には、例えばコンテンツに対応するコンテンツ証明書の検証等の処理を実行し、タイトル単位のＣＰＳユニットの復号に基づくコンテンツ利用を実行する。

【０１９４】

次に、ステップＳ３０１において、ディスクがデータ再書き込みの許容されているＲまたはＲＥディスクである場合の処理について説明する。この場合、情報処理装置は、ステップＳ３０２において、記録フォーマットを確認する。すなわちＢＤＡＶフォーマットでの記録がなされているか。あるいはＢＤＭＶフォーマットでの記録がなされているかを判定する。前述したように、アプリケーションタイプ２は、ＢＤＡＶフォーマット、アプリケーションタイプ３，４は、ＢＤＭＶフォーマットに対応する。

【０１９５】

まず、ＢＤＡＶフォーマットであると判定された場合の処理について説明する。ＢＤＡＶフォーマットであると判定した場合は、ステップＳ３０３に進み、ディスクの記録データに対応するディレクトリにＡＡＣＳディレクトリが設定されているか否かを判定する。

【０１９６】

ディスクの記録データに対応するディレクトリにＡＡＣＳディレクトリが設定されていない場合、ステップＳ３０４に進み、ＣＰＳユニット鍵を適用した復号の必要のないコンテンツが記録されていると判定し、復号処理を行なわず再生処理を実行する。一方、ディスクの記録データに対応するディレクトリにＡＡＣＳディレクトリが設定されていると判定した場合は、ステップＳ３０５に進み、コンテンツタイプがアプリケーションタイプ２であるか否かを判定する。この判定処理は、コンテンツに対応する属性データ、あるいはユニット鍵ファイルの格納データなどに基づいて判定することができる。

【０１９７】

格納コンテンツがアプリケーションタイプ２であることが確認されない場合は、ステップＳ３０６に進み、エラーと判定し、処理を中止する。格納コンテンツがアプリケーションタイプ２であることが確認された場合は、アプリケーションタイプ２に対応するコンテンツ再生シーケンスを実行する。

【０１９８】

アプリケーションタイプ２に対応するコンテンツは、先に、図７を参照して説明したように、クリップ単位でのＣＰＳユニット設定がなされているのでＣクリップ単位のＣＰＳユニットの選択を行ってＣＰＳユニット鍵を取得して復号処理を実行する。なお、アプリケーションタイプ２では、コンテンツに対応するコンテンツ証明書の記録が必須要件とはなっていないので、コンテンツ証明書の検証は省略される。

【０１９９】

次に、ステップＳ３０２において、ディスク記録コンテンツがＢＤＭＶフォーマットであると判定された場合の処理について説明する。ＢＤＭＶフォーマットであると判定した場合は、ステップＳ３１１に進み、ディスクの記録データに対応するディレクトリにＡＡＣＳディレクトリが設定されているか否かを判定する。

【０２００】

ディスクの記録データに対応するディレクトリにＡＡＣＳディレクトリが設定されていない場合、ステップＳ３１２に進み、ＣＰＳユニット鍵を適用した復号の必要のないコンテンツが記録されていると判定し、復号処理を行なわず再生処理を実行する。一方、ディスクの記録データに対応するディレクトリにＡＡＣＳディレクトリが設定されていると判定した場合は、ステップＳ３１３に進み、コンテンツタイプがアプリケーションタイプ３であるか否かを判定する。この判定処理は、コンテンツに対応する属性データ、あるいはユニット鍵ファイルの格納データなどに基づいて判定することができる。

【０２０１】

格納コンテンツがアプリケーションタイプ３であることが確認された場合は、ステップＳ３１４に進み、プリケーションタイプ３に対応するコンテンツ再生シーケンスを実行す

る。アプリケーションタイプ３に対応するコンテンツは、先に、図１２、図１３を参照して説明したように、クリップ単位でのＣＰＳユニット設定がなされているのでクリップ単位のＣＰＳユニットの選択を行ってＣＰＳユニット鍵を取得して復号処理を実行する。なお、アプリケーションタイプ３では、コンテンツに対応するコンテンツ証明書の記録が必須要件とはなっていないので、コンテンツ証明書の検証は省略される。

【０２０２】

一方、ステップＳ３１３において、格納コンテンツがアプリケーションタイプ３であることが確認されない場合は、ステップＳ３１５に進み、コンテンツタイプがアプリケーションタイプ４であるか否かを判定する。この判定処理は、コンテンツに対応する属性データ、あるいはユニット鍵ファイルの格納データなどに基づいて判定することができる。コンテンツタイプがアプリケーションタイプ４であることが確認されない場合は、ステップＳ３１６に進み、エラーと判定し、処理を中止する。

【０２０３】

一方、格納コンテンツがアプリケーションタイプ４であることが確認された場合は、ステップＳ３１７に進み、アプリケーションタイプ４に対応するコンテンツ再生シーケンスを実行する。

【０２０４】

アプリケーションタイプ４に対応するコンテンツは、先に、図１７を参照して説明したように、タイトル単位でのＣＰＳユニット設定がなされているのでタイトル単位のＣＰＳユニットの選択を行ってＣＰＳユニット鍵を取得して復号処理を実行する。具体的なシーケンスは、先に図２２、図２３を参照して説明した処理となる。アプリケーションタイプ４では、コンテンツに対応するコンテンツ証明書の記録が必須要件とはなっており、コンテンツ証明書の検証が実行される。その他、サーババインド処理情報などの検証、さらに、ＣＰＳユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理もアプリケーションタイプ４に従った処理として、先に図２２、図２３を参照して説明した処理として実行される。

【０２０５】

［４．情報処理装置の構成例］

図２５にコンテンツ情報記録媒体に対する記録処理と、情報記録媒体に記録されたコンテンツの復号、再生、利用処理を実行する情報処理装置の機能を説明するブロック図を示す。

【０２０６】

情報処理装置は、コンテンツ暗号処理部８０１、ＣＰＳユニット鍵ファイル処理部８０２、管理情報制御部８０３を有するデータ処理部８００と、記録媒体制御部８０４、入力部８０５、出力部８０６を有する。

【０２０７】

コンテンツの情報記録媒体８１０に対する記録処理に際して、コンテンツ暗号処理部８０１は、コンテンツの利用制御単位として設定されるコンテンツ管理ユニット（ＣＰＳユニット）に対応するユニット鍵を適用した暗号化処理により、コンテンツ管理ユニット対応の暗号化データを生成する。

【０２０８】

ＣＰＳユニット鍵ファイル処理部８０２は、バインドシードに基づくバインド鍵の生成、バインド鍵、および各アプリケーションタイプに応じて必要となる各種の情報を適用したユニット鍵ファイルに記録されるユニット鍵の暗号化などの処理を実行する。すなわち、ユニット鍵ファイルに含まれるユニット鍵の構成変更に従って値を更新するシードを適用して生成する暗号鍵に基づいて、ユニット鍵ファイルまたはファイル構成データの暗号化処理を実行してユニット鍵ファイルの生成を行なう。

【０２０９】

管理情報制御部８０２は、コンテンツ管理ユニット、ユニット鍵ファイル、およびコンテンツ管理ユニットに対応する利用制御情報ファイルなどの対応判定、各種ファイルの生

成または更新必要性判断などの処理を実行する。記録媒体制御部８０４は、暗号化データ、ユニット鍵ファイル、および利用制御情報ファイルなどを予め設定された記録データフォーマットに従って情報記録媒体８１０に記録し、また読み取る処理を実行する。情報記録媒体８１０に対する記録データは、インデックス情報、プレイリスト、およびＡＶストリームを含むクリップを有する階層構成データによって構成される動画コンテンツを含む。

【０２１０】

ＣＰＳユニット鍵ファイル処理部８０２は、情報記録媒体８１０に記録済みの既存のユニット鍵ファイルに含まれるユニット鍵の増加または削除に応じて、新たな値を持つ新規バインドシードを設定し、新規バインドシードに基づく新規バインド鍵に基づく暗号化処理を施した更新ユニット鍵ファイルを生成する。

【０２１１】

すなわち、ＣＰＳユニット鍵ファイル処理部８０２は、情報記録媒体８１０に対する新たなコンテンツ管理ユニットの記録処理に応じて新たに設定された新規ユニット鍵をユニット鍵ファイルに格納するとともに、新規ユニット鍵の追加に応じて、新たな値を持つ新規バインドシードを設定し、新規バインドシードに基づく新規バインド鍵に基づく暗号化処理を施した更新ユニット鍵ファイルを生成する。また、情報記録媒体８１０からのコンテンツ管理ユニットの移動または削除処理に応じて、移動または削除対象のコンテンツ管理ユニット対応のユニット鍵をユニット鍵ファイルから削除するとともに、ユニット鍵の削除に応じて、新たな値を持つ新規バインドシードを設定し、該新規バインドシードによって生成する新規バインド鍵に基づく暗号化処理を施した更新ユニット鍵ファイルを生成する。

【０２１２】

なお、ＣＰＳユニット鍵ファイル処理部８０２は、情報処理装置に格納されたデバイス鍵を適用した暗号鍵ブロックの処理によって取得されるメディア鍵によるバインドシードの暗号処理によって生成する暗号鍵を適用して、ユニット鍵ファイルまたは該ファイル構成データの暗号化処理を実行する。

【０２１３】

なお、例えばアプリケーションタイプ４に対応するダウンロードコンテンツを情報記録媒体に記録する場合は、先に、図２３を参照して説明したように、コンテンツ証明書、サーババインド処理情報の少なくともいずれかの情報を適用した処理によって、ユニット鍵ファイルまたは該ファイル構成データの暗号化処理を実行する。

【０２１４】

記録媒体制御部８０４は、各種データの情報記録媒体８１０に対する記録や読み取りを実行する。また、情報記録媒体８１０に記録されたコンテンツの再生処理を実行する場合、コンテンツ暗号処理部８０１は、コンテンツの利用制御単位として設定されるコンテンツ管理ユニットに対応するユニット鍵に基づいて記録媒体制御部８０４が情報記録媒体８１０から読み取った暗号化コンテンツの復号処理を実行する。

【０２１５】

ＣＰＳユニット鍵ファイル処理部８０２は、コンテンツ管理ユニットに対応するユニット鍵を、情報記録媒体８１０に記録されたユニット鍵ファイルから取得する。この際、情報記録媒体から取得される鍵生成情報としてのシードを適用した暗号鍵生成処理を実行し、生成暗号鍵に基づいて、ユニット鍵ファイルまたはファイル構成データの復号処理を行なってユニット鍵の取得処理を実行する。

【０２１６】

ＣＰＳユニット鍵ファイル処理部８０２は、情報処理装置に格納されたデバイス鍵を適用した暗号鍵ブロックの処理によって取得されるメディア鍵によるバインドシードの暗号処理によって生成する暗号鍵を適用して、ユニット鍵ファイルまたは該ファイル構成データの復号処理を実行する。

【０２１７】

なお、例えばアプリケーションタイプ４に対応するダウンロードコンテンツを情報記録媒体に記録する場合は、先に、図２３を参照して説明したように、コンテンツ証明書、サーババインド処理情報の少なくともいずれかの情報を適用した処理によって、ユニット鍵ファイルまたは該ファイル構成データの復号処理を実行する。

【０２１８】

データ入力部８０５は、記録コンテンツの入力の他、ユーザからのコンテンツ指定情報や編集処理情報の入力に適用される。データ出力部８０６は、例えば再生コンテンツの出力に適用される。

【０２１９】

データ記録時およびデータ再生時にデータ処理部８００の実行する主な処理は、以下の通りである。

（データ記録時）

データ記録処理を実行する場合、データ処理部８００は、情報記録媒体８１０に記録する暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵ファイルまたはファイル構成データの暗号化処理およびコンテンツ暗号化処理を実行する。例えば、記録予定のコンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプであるか否かを判別し、リアルタイム記録コンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行する。

【０２２０】

また、データ処理部８００は、情報記録媒体８１０に記録予定のコンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプであるか否かを判別し、ダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対してユニット鍵に基づく暗号化処理を実行する。

【０２２１】

さらに、データ処理部８００は、情報記録媒体８１０に記録予定のコンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプである場合、先に図２３を参照して説明したように、ユニット鍵ファイルに含まれる暗号化ユニット鍵の暗号化処理に際して、ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行する。

【０２２２】

（データ再生時）

データ再生処理を実行する場合、データ処理部８００は、情報記録媒体８１０に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号処理を実行する。例えば、データ処理部８００は、情報記録媒体８１０が、データ再書き込みの許容されないＲＯＭ型ディスクであるか否かを判別し、データ再書き込みの許容されたディスクである場合に、さらに、情報記録媒体に記録された暗号化コンテンツのアプリケーションタイプを判別し、アプリケーションタイプに対応する処理シーケンスに従ったユニット鍵の取得処理およびコンテンツ復号処理を実行する。なお、データ処理部８００は、情報記録媒体８１０に記録された暗号化コンテンツのアプリケーションタイプの判別情報に応じて、コンテンツに対応して設定されるコンテンツの正当性を示すコンテンツ証明書の検証を行なうか否かを決定する処理を実行する。

【０２２３】

また、データ処理部８００は、情報記録媒体８１０に記録された暗号化コンテンツのアプリケーションタイプがリアルタイム記録コンテンツに対応するアプリケーションタイプ

であるか否かを判別し、リアルタイム記録コンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるコンテンツ格納ファイルとしてのクリップを単位としたコンテンツ管理ユニットに対応するユニット鍵を、ユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体８１０に記録された暗号化コンテンツの復号処理を実行する。

【０２２４】

さらに、データ処理部８００は、情報記録媒体８１０に記録された暗号化コンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプであるか否かを判別し、ダウンロードコンテンツに対応するアプリケーションタイプである場合には、コンテンツ記録フォーマットにおいて規定されるタイトルを単位としたコンテンツ管理ユニットに対応するユニット鍵を、ユニット鍵ファイルから取得し、取得したユニット鍵を適用して情報記録媒体８１０に記録された暗号化コンテンツの復号処理を実行する。

【０２２５】

さらに、データ処理部８００は、情報記録媒体８１０に記録された暗号化コンテンツのアプリケーションタイプがダウンロードコンテンツに対応するアプリケーションタイプであると判定した場合、ユニット鍵ファイルに含まれる暗号化ユニット鍵の復号処理によるユニット鍵の取得に際して、ダウンロードコンテンツに対応する情報として設定されたコンテンツ証明書またはサーババインド処理情報の少なくともいずれかのデータを適用したデータ処理を実行してユニット鍵を取得する。

【０２２６】

次に、図２６を参照して、上述のコンテンツの記録、再生処理を行う情報処理装置のハードウェア構成例について説明する。

【０２２７】

図２６に示す情報処理装置９００は、情報記録媒体９１０の駆動を行ない、データ記録再生信号の入手力を行なうドライブ９０９、各種プログラムに従ったデータ処理を実行する制御手段としてのＣＰＵ９０７、プログラム、パラメータ等の記憶領域としてのＲＯＭ９０６、メモリ９０８、デジタル信号を入出力する入出力Ｉ／Ｆ９０２、アナログ信号を入出力し、Ａ／Ｄ，Ｄ／Ａコンバータ９０４を持つ入出力Ｉ／Ｆ９０３、ＭＰＥＧデータのエンコード、デコード処理を実行するＭＰＥＧコーデック９２１、ＴＳ（Transport Stream）・ＰＳ(Program Stream)処理を実行するＴＳ・ＰＳ処理手段９２２、各種の暗号処理を実行する暗号処理手段９０５、各種のデータおよびデータ処理プログラムを格納するハードディスクなどローカルストレージとしての記憶手段９３０を有し、バス９０１に各ブロックが接続されている。

【０２２８】

情報処理装置９００において、情報記録媒体９１０に格納された例えばＭＰＥＧ－ＴＳデータからなるＡＶストリームデータの再生を行う場合、ドライブ９０９において情報記録媒体９１０から読み出されたデータは必要に応じて暗号処理手段９０５で暗号を解きＴＳ・ＰＳ処理手段９２２によって画像、音声などの各データに分けられる。

【０２２９】

さらに、ＭＰＥＧコーデック９２１において復号されたデジタルデータは入出力Ｉ／Ｆ９０３内のＤ／Ａコンバータ９０４によってアナログ信号に変換され出力される。またデジタル出力を行う場合、暗号処理手段９０５で復号されたＭＰＥＧ－ＴＳデータは入出力Ｉ／Ｆ９０２を通してデジタルデータとして出力される。この場合の出力は例えばＩＥＥＥ１３９４やイーサネット（登録商標）ケーブル、無線ＬＡＮなどのデジタルインターフェースに対して行われる。なお、ネットワーク接続機能に対応する場合入出力Ｉ／Ｆ９０２はネットワーク接続の機能を備える。

【０２３０】

また、情報処理装置９００内で出力先機器が受信可能な形式にデータ変換をして出力を行う場合、一旦ＴＳ処理手段９２２で分離した画像、音声などに対してＭＰＥＧコーデッ

ク９２１においてレート変換、コーデック変換処理を加え、ＴＳ・ＰＳ処理手段９２２で再度ＭＰＥＧ－ＴＳやＭＰＥＧ－ＰＳなどに多重化を行ったデータをデジタル用入出力Ｉ／Ｆ９０２から出力する。または、ＣＰＵ９０７の制御の下にＭＰＥＧ以外のコーデック、多重化ファイルに変換をしてデジタル用入出力Ｉ／Ｆ９０２から出力することも可能である。

【０２３１】

ＣＰＳユニットに対応する管理情報、例えば利用制御情報やＣＰＳユニット鍵ファイル等の管理データは、情報記録媒体９１０から読み出された後メモリ９０８に保管され、ＣＰＳユニット鍵ファイルについては、前述した処理によって、バインド鍵を生成した上で、各アプリケーションタイプに対応する必要情報を適用して復号が実行されてＣＰＳユニット鍵が取得される。

【０２３２】

次に、情報処理装置９００が、例えば放送信号受信などによって取得したデータを記録する際の動作について説明する。記録を行うデータとしてデジタル信号入力とアナログ信号入力の２つのケースが想定される。デジタル信号の場合、デジタル信号用入出力Ｉ／Ｆ９０２から入力され、必要に応じて暗号処理手段９０５によって適切な暗号化処理を施したデータを記録媒体９１０に保存する。

【０２３３】

入力されたデジタル信号のデータ形式を変換して保存する場合、ＭＰＥＧコーデック９２１およびＣＰＵ９０７、ＴＳ・ＰＳ処理手段９２２によって保存用のデータ形式に変換を行い、その後、暗号処理手段９０５で前述したＣＰＳユニット鍵を適用した暗号処理など、適切な暗号化処理を施して記録媒体９１０に保存する。アナログ信号の場合、入出力Ｉ／Ｆ９０３へ入力されたアナログ信号はＡ／Ｄコンバータ９０４によってデジタル信号に変換され、ＭＰＥＧコーデック９２１によって記録時に使用されるコーデックへと変換される。

【０２３４】

その後、ＴＳ・ＰＳ処理手段により、記録データの形式であるＡＶ多重化データへ変換され、必要に応じて暗号処理手段９０５によって適切な暗号化処理を施したデータが記録媒体９１０に保存される。

【０２３５】

情報処理装置９００において必用な情報を装置外部のネットワーク経由で取得する場合、取得したデータは情報処理装置９００内部のメモリ９０８に一時的に保存される。保存されるデータとしてはコンテンツ再生に必用な鍵情報、コンテンツ再生時に合わせて再生するための画像、音声などのデータ、さらに、コンテンツ利用制御情報（ＣＣＩ）などのコンテンツ管理情報などが存在する。

【０２３６】

なお、再生処理、記録処理を実行するプログラムはＲＯＭ９０６内に保管されており、プログラムの実行処理中は必要に応じて、パラメータ、データの保管、ワーク領域としてメモリ９０８を使用する。なお、図２６では、データ記録、再生の可能な装置構成を示して説明したが、再生機能のみの装置、記録機能のみを有する装置も構成可能であり、これらの装置においても本発明の適用が可能である。

【０２３７】

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。

【０２３８】

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。

【０２３９】

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。

【０２４０】

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。

【０２４１】

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】

【０２４２】

以上、説明したように、本発明の一実施例の構成によれば、コンテンツの利用制御単位として設定されるコンテンツ管理ユニット（ＣＰＳユニット）に基づくコンテンツの利用制御を行う構成において、コンテンツの記録、または再生処理に際して、記録コンテンツに対応するアプリケーションタイプの識別を行い、各アプリケーションタイプに応じた処理によるデータ記録または再生を実行する構成とした具体的には、例えばリアルタイム記録コンテンツに対応するアプリケーションタイプ、ダウンロードコンテンツに対応するアプリケーションタイプ等を設定し、それぞれのコンテンツに応じたユニット鍵の設定、コンテンツ管理ユニットの設定構成として、各コンテンツに応じた柔軟なコンテンツ利用制御を実現した。

【図面の簡単な説明】

【０２４３】

【図１】情報記録媒体の格納データについて説明する図である。

【図２】情報記録媒体の格納データのユニット設定構成およびユニット鍵の対応例について説明する図である。

【図３】情報記録媒体の記録コンテンツの再生シーケンスの一例を説明する図である。

【図４】アプリケーションタイプ１のコンテンツ構成について説明する図である。

【図５】アプリケーションタイプ１のコンテンツ管理ユニット（ＣＰＳユニット）設定構成について説明する図である。

【図６】アプリケーションタイプ１のコンテンツ管理ユニット（ＣＰＳユニット）の設定およびユニット鍵の設定例について説明する図である。

【図７】アプリケーションタイプ２のコンテンツ管理ユニット（ＣＰＳユニット）設定構成について説明する図である。

【図８】アプリケーションタイプ２のコンテンツ管理ユニット（ＣＰＳユニット）の設定およびユニット鍵の設定例について説明する図である。

【図９】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。

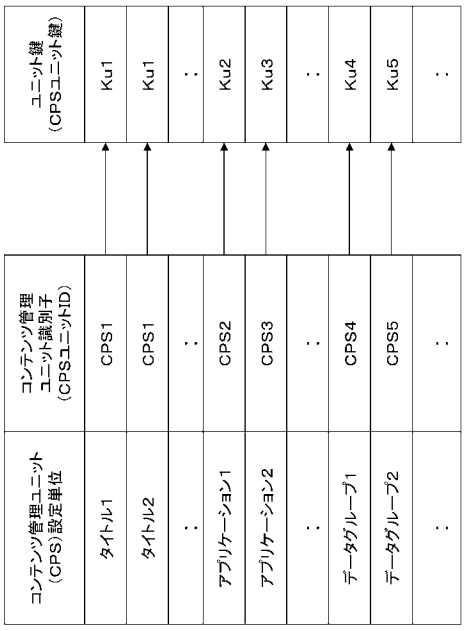
【図１０】アプリケーションタイプ２のユニット鍵ファイルのデータ構成例について説明

する図である。
【図１１】アプリケーションタイプ２のディレクトリ構造例について説明する図である。
【図１２】アプリケーションタイプ３のコンテンツ管理ユニット（ＣＰＳユニット）設定構成について説明する図である。
【図１３】アプリケーションタイプ３のコンテンツ管理ユニット（ＣＰＳユニット）設定構成および編集処理について説明する図である。
【図１４】アプリケーションタイプ３のコンテンツ管理ユニット（ＣＰＳユニット）の設定およびユニット鍵の設定例について説明する図である。
【図１５】アプリケーションタイプ３の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１６】アプリケーションタイプ２のディレクトリ構造例について説明する図である。
【図１７】アプリケーションタイプ３４コンテンツ管理ユニット（ＣＰＳユニット）設定構成について説明する図である。
【図１８】アプリケーションタイプ４のコンテンツ管理ユニット（ＣＰＳユニット）の設定およびユニット鍵の設定例について説明する図である。
【図１９】アプリケーションタイプ４の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２０】アプリケーションタイプ４のディレクトリ構造例について説明する図である。
【図２１】アプリケーションタイプ４のディレクトリ構造例について説明する図である。
【図２２】アプリケーションタイプ４のコンテンツの記録および再生シーケンス例について説明する図である。
【図２３】アプリケーションタイプ４のコンテンツの記録および再生シーケンス例について説明する図である。
【図２４】コンテンツの再生シーケンス例について説明するフローチャートを示す図である。
【図２５】コンテンツの情報記録媒体に対する記録処理と、情報記録媒体に記録されたコンテンツの復号、再生、利用処理を実行する情報処理装置の機能を説明するブロック図である。
【図２６】情報記録媒体を装着して再生処理または記録処理を実行する情報処理装置の構成例について説明する図である。
【符号の説明】
【０２４４】
１００　情報記録媒体
１０１　暗号化コンテンツ
１０２　ＭＫＢ
１０３　ユニット鍵ファィル
１０４　バインドシード
１０５　利用制御情報
１８１　デバイス鍵
１８２　コンテンツ
２００　メインコンテンツ
２１０　アプリケーション
２１１，２１２　アプリケーションインデックスファイル（タイトル）
２１３，２１４，２１５　アプリケーション実行ファイル
２２１～２２４　再生プログラム
２３０　再生区間指定ファイル（プレイリスト）
２３１～２３３　プレイリスト
２３４，２３５　プレイアイテム
２４０　クリップ（コンテンツデータファイル）
２４１～２４３　クリップ

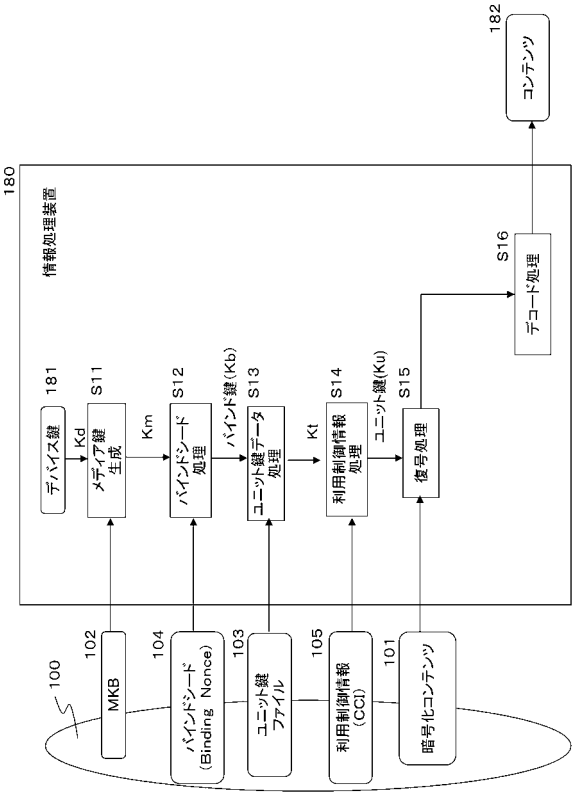
２５１　クリップ情報
２６１，２６２，２６３　ＡＶストリーム
３００　サブコンテンツ
３１１，３１２　データグループ
４０１～４０５　コンテンツ管理ユニット（ＣＰＳユニット）
５０１～５０４　コンテンツ管理ユニット（ＣＰＳユニット）
５１１　プレイリスト
６０１～６０２　コンテンツ管理ユニット（ＣＰＳユニット）
６３１　コンテンツ証明書
６３２　コンテンツハッシュテーブル
６３３　リボケーションリスト
６３４　サーババインド処理情報
７１０　情報処理装置
７１１　デバイス鍵
７１２　ＭＫＢ
７１３　バインドシード
７１４　ユニット鍵
７１５　利用制御情報
７１６　コンテンツ
７１７　コンテンツ証明書
７１８　サーババインド処理情報
７２０　情報処理装置
７２１　デバイス鍵
７２５　コンテンツ
７５０　情報記録媒体
７５１　ＭＫＢ
７５２　バインドシード
７５３　コンテンツ証明書
７５４　コンテンツハッシュテーブル
７５５　リボケーションリスト
７５６　サーババインド処理情報
７５７　ＣＰＳユニット鍵ファイル
７５８　利用制御情報
７５９　暗号化コンテンツ
８００　データ処理部
８０１　コンテンツ暗号処理部
８０２　ＣＰＳユニット鍵ファイル処理部
８０３　管理情報制御部
８０４　記録媒体制御部
８０５　入力部
８０６　出力部
８１０　情報記録媒体
９００　情報処理装置
９０１　バス
９０２　入出力Ｉ／Ｆ
９０３　入出力Ｉ／Ｆ
９０４　Ａ／Ｄ，Ｄ／Ａコンバータ
９０５　暗号処理手段
９０６　ＲＯＭ
９０７　ＣＰＵ

９０８　メモリ
９０９　ドライブ
９１０　情報記録媒体
９２１　ＭＰＥＧコーデック
９２２　ＴＳ・ＰＳ処理手段
９３０　記憶手段

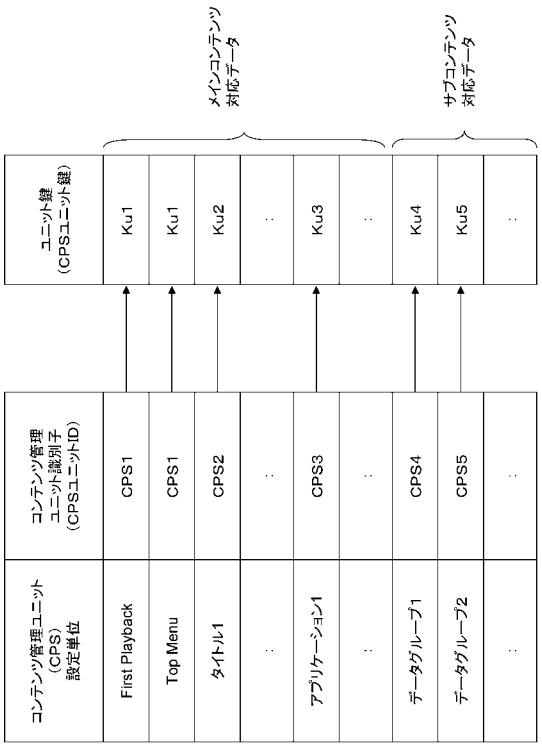
【図２】



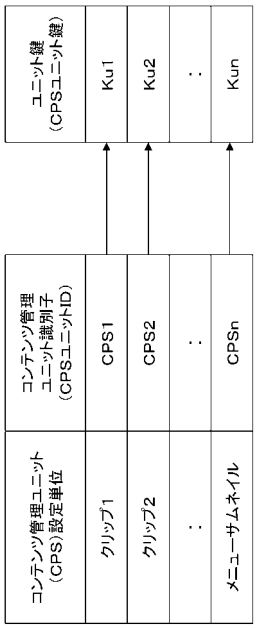
【図３】



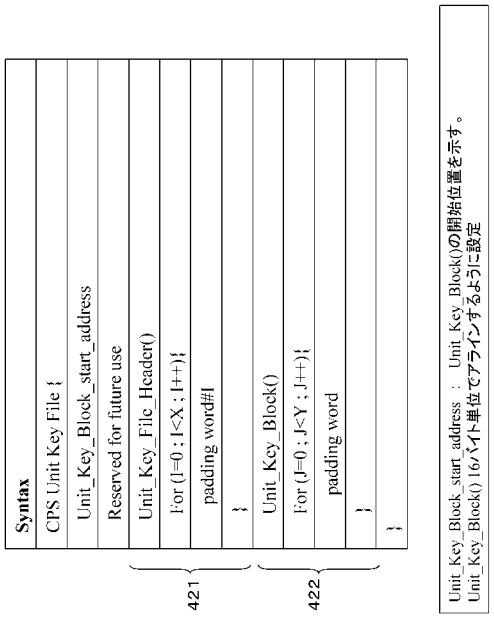
【図６】


コンテンツ管理ユニット (CPS) 設定単位
コンテンツ管理 ユニット識別子 (CPSユニットID)
ユニット鍵 (CPSユニット鍵)
メインコンテンツ対応データ
サブコンテンツ対応データ
First Playback
Top Menu
タイトル1
アプリケーション1
データグループ1
データグループ2
CPS1
CPS2
CPS3
CPS4
CPS5
Ku1
Ku2
Ku3
Ku4
Ku5

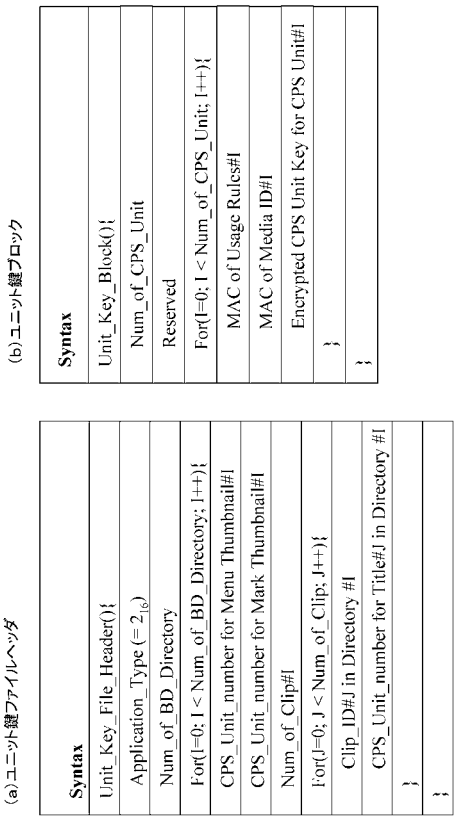
【図８】


コンテンツ管理ユニット (CPS) 設定単位
コンテンツ管理 ユニット識別子 (CPSユニットID)
ユニット鍵 (CPSユニット鍵)
クリップ1
クリップ2
メニューサムネイル
CPS1
CPS2
CPSn
Ku1
Ku2
Kun

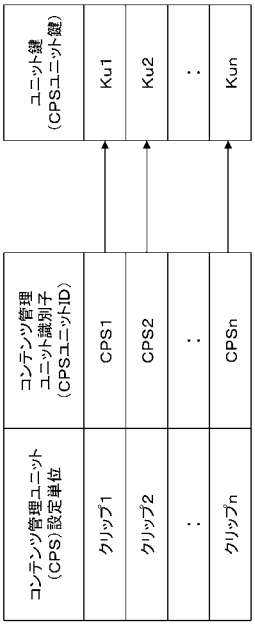
【図９】


Syntax
CPS Unit Key File {
Unit_Key_Block_start_address
Reserved for future use
Unit_Key_File_Header()
For (I=0 ; I<X ; I++){
padding word#I
}
Unit_Key_Block()
For (J=0 ; J<Y ; J++){
padding word
}
}
421
422
Unit_Key_Block_start_address : Unit_Key_Block()の開始位置を示す。
Unit_Key_Block() 16バイト単位でアラインするように設定

【図１０】


(a) ユニット鍵ファイルヘッダ
Syntax
Unit_Key_File_Header(){
Application_Type (= 2(6))
Num_of_BD_Directory
For(I=0; I < Num_of_BD_Directory; I++){
CPS_Unit_number for Menu Thumbnail#I
CPS_Unit_number for Mark Thumbnail#I
Num_of_Clip#I
For(J=0; J < Num_of_Clip; J++){
Clip_ID#J in Directory #I
CPS_Unit_number for Title#J in Directory #I
}
}
(b) ユニット鍵ブロック
Syntax
Unit_Key_Block(){
Num_of_CPS_Unit
Reserved
For(I=0; I < Num_of_CPS_Unit; I++){
MAC of Usage Rules#I
MAC of Media ID#I
Encrypted CPS Unit Key for CPS Unit#I
}
}

【図１４】



【図１５】

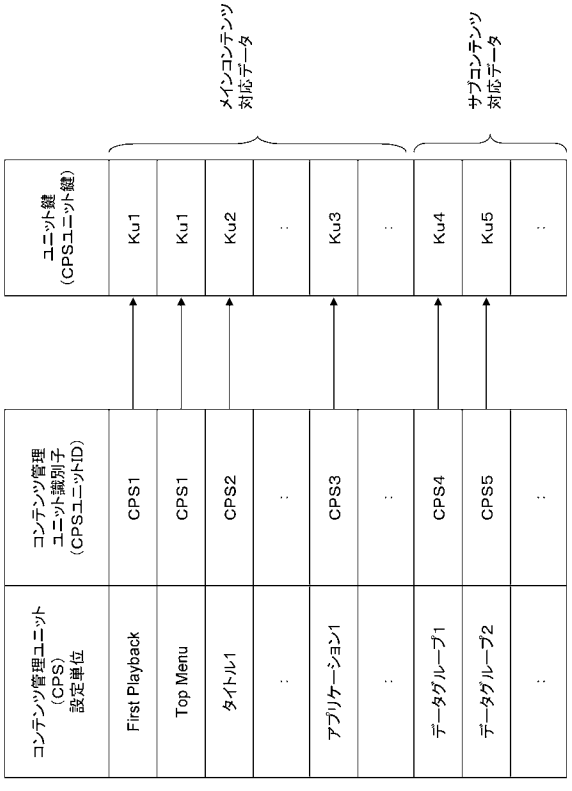
(a)ユニット鍵ファイルヘッダ

Syntax
Unit_Key_File_Header(){
Application_Type (= $3_{(h)}$)
Num_of_BD_Dirctory
For(I=0; I < Num_of_BD_Directory; I++){
CPS_Unit_number for Menu Thumbnail#I
CPS_Unit_number for Mark Thumbnail#I
Num_of_Clip#I
For(J=0; J < Num_of_Clip; J++){
Clip_ID#J in Directory #I
CPS_Unit_number for Title#J in Directory #I
}
}

(b)ユニット鍵ブロック

Syntax
Unit_Key_Block(){
Num_of_CPS_Unit
Reserved
For(I=0; I < Num_of_CPS_Unit; I++){
MAC of Usage Rules#I
MAC of Media ID#I
Encrypted CPS Unit Key for CPS Unit#I
}
}

【図１８】



【図１９】

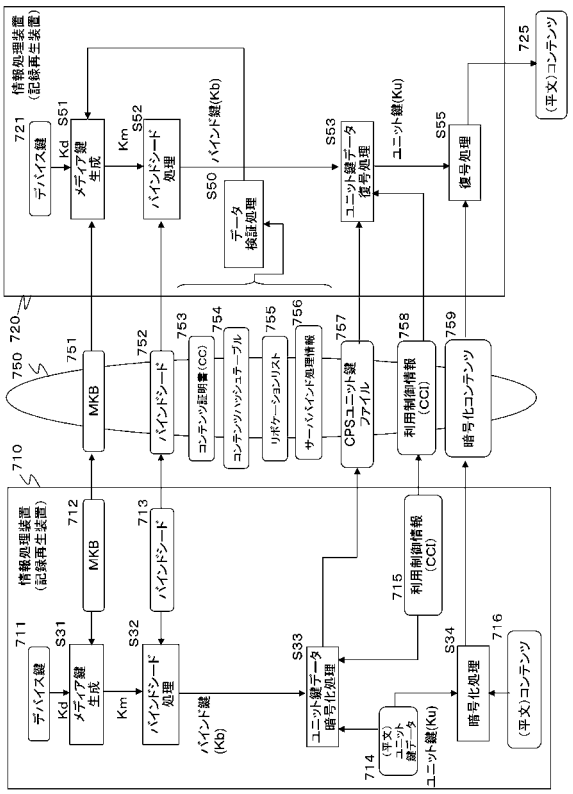
(a)ユニット鍵ファイルヘッダ

Syntax
Unit_Key_File_Header(){
Application_Type (= $4_{(h)}$)
Num_of_BD_Directory (=1)
For(I=0; I < Num_of_BD_Directory; I++){
CPS_Unit_number for_FirstPlay
CPS_Unit_number_for_TopMenu
Num_of_Title in Directory#I
For(J=0; J < Num_of_Title in Directory#I; J++){
Title_number#J in Directory #I
CPS_Unit_number for Title#J in Directory #I
}
}

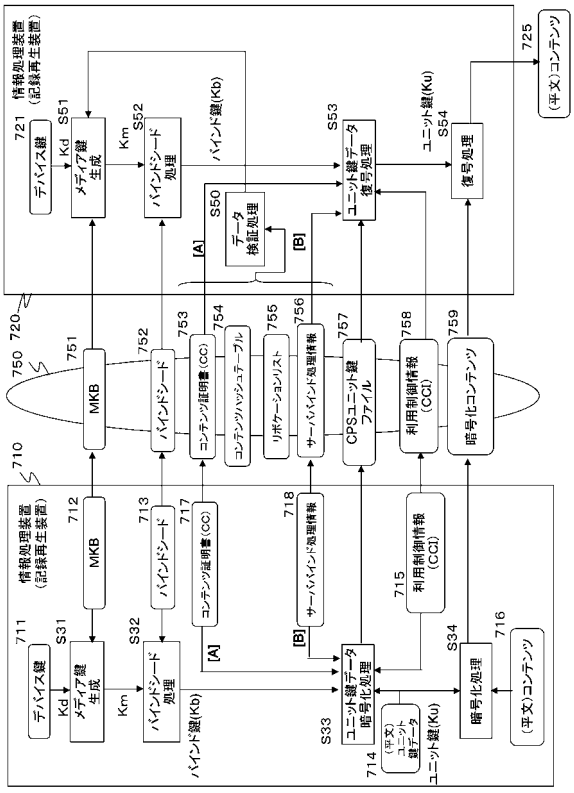
(b)ユニット鍵ブロック

Syntax
Unit_Key_Block(){
Num_of_CPS_Unit
Reserved
For(I=0; I < Num_of_CPS_Unit; I++){
MAC of Usage Rules#I
MAC of Media ID#I
Encrypted CPS Unit Key for CPS Unit#I
}
}

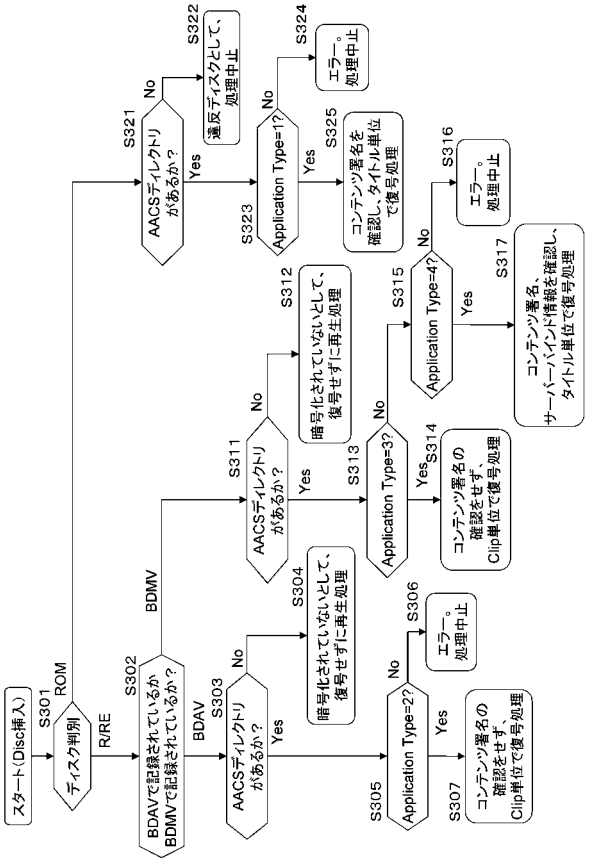
【図２２】



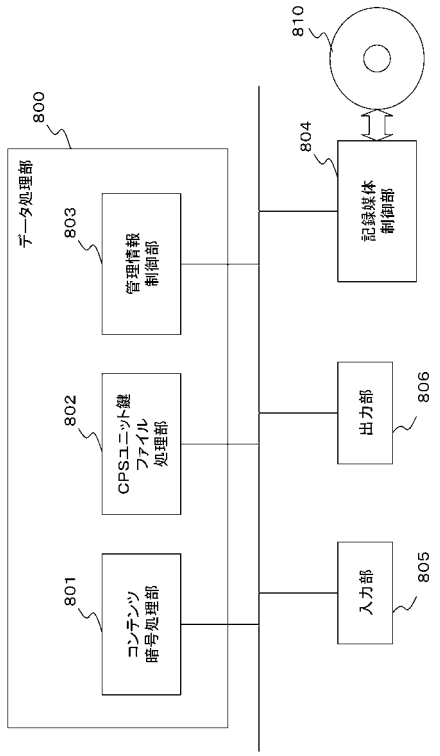
【図２３】



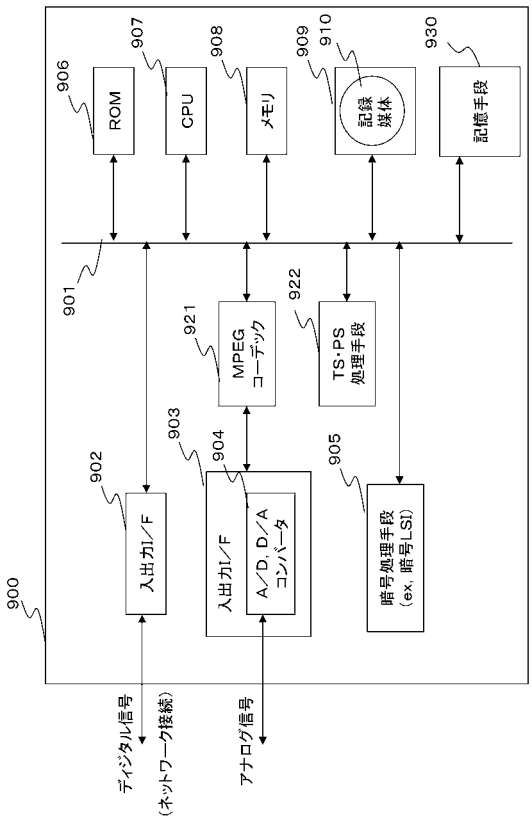
【図２４】



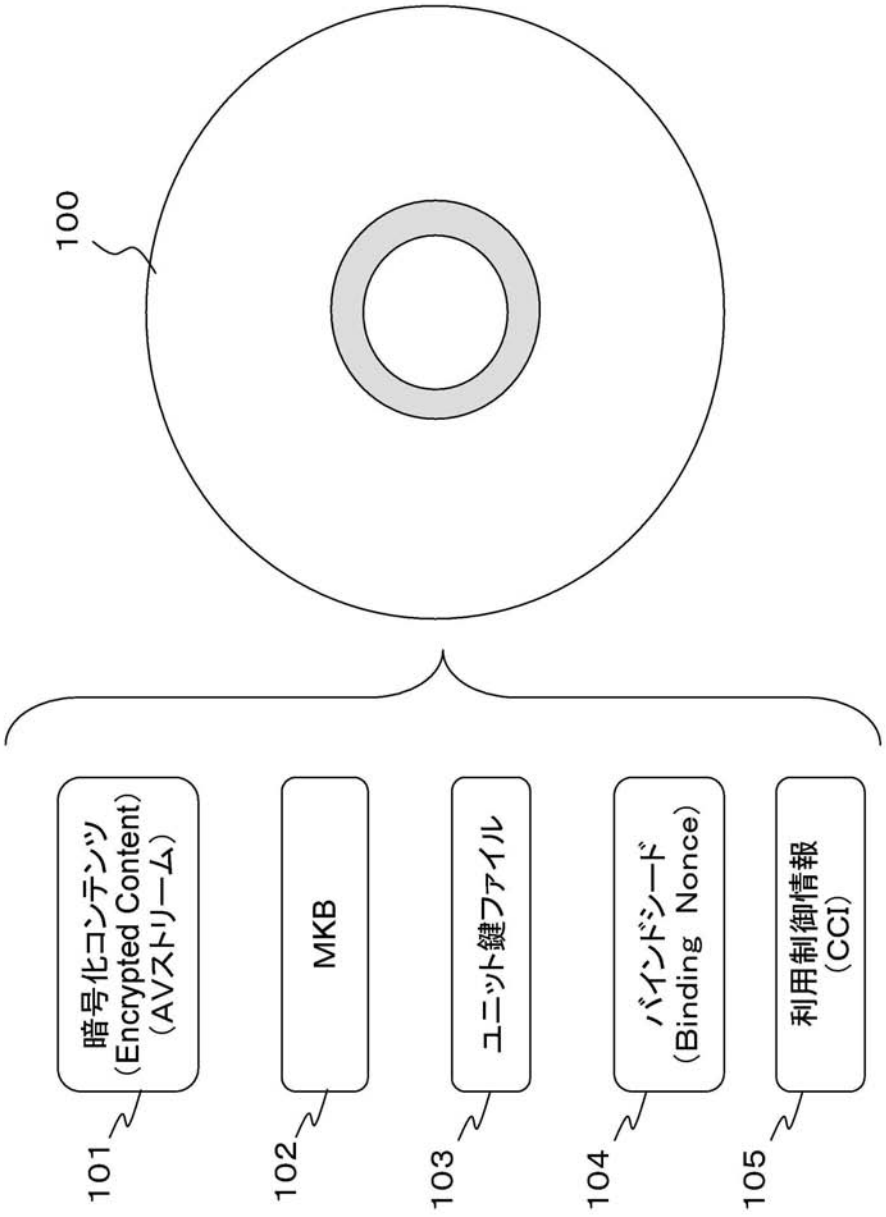
【図２５】



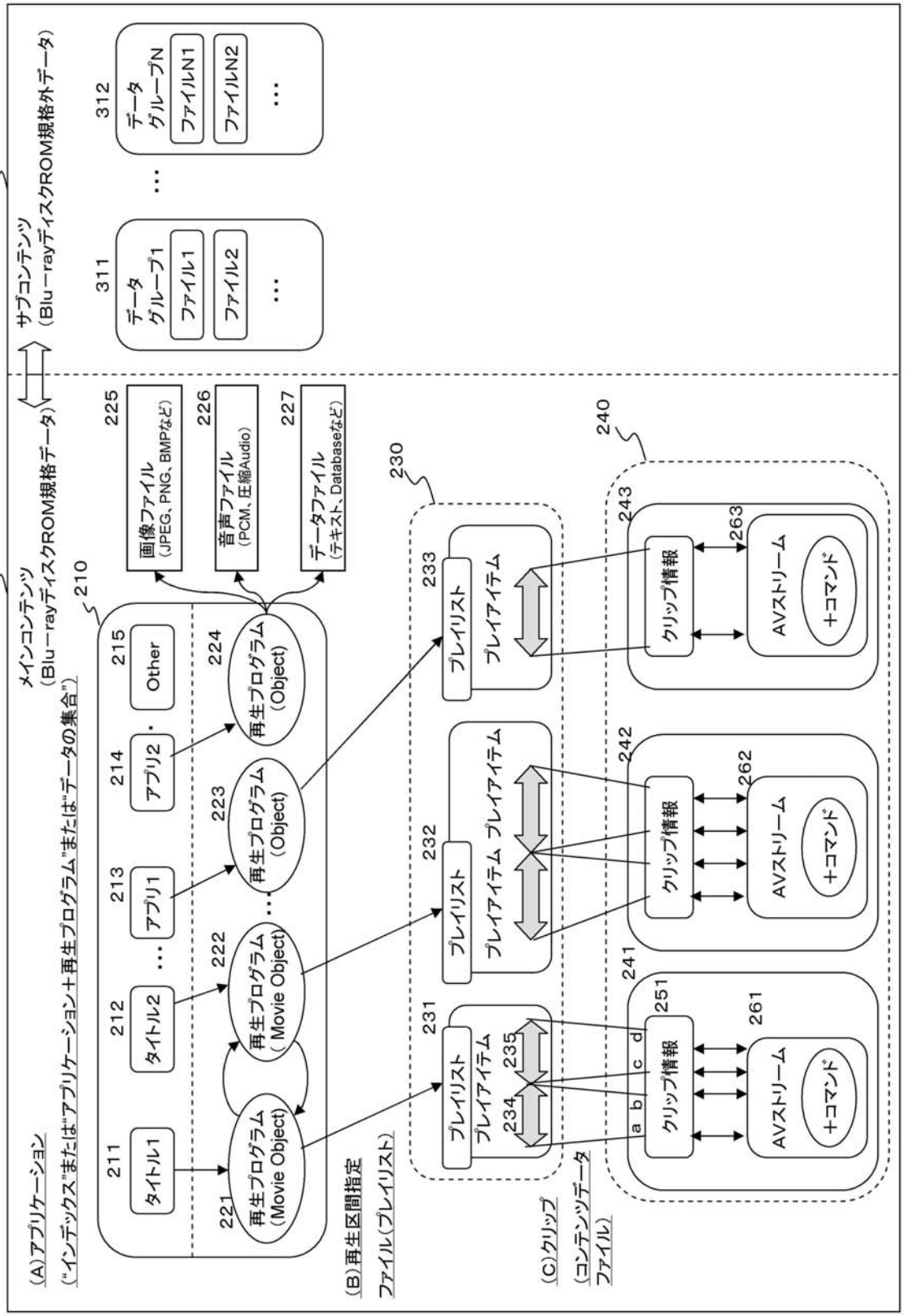
【図２６】


900
901
902
903
904
905
906
907
908
909
910
921
922
930
ROM
CPU
メモリ
記録媒体
記憶手段
MPEG コーデック
TS・PS 処理手段
入出力I／F
入出力I／F
A／D, D／A コンバータ
暗号処理手段 (ex. 暗号LSI)
ディジタル信号
(ネットワーク接続)
アナログ信号

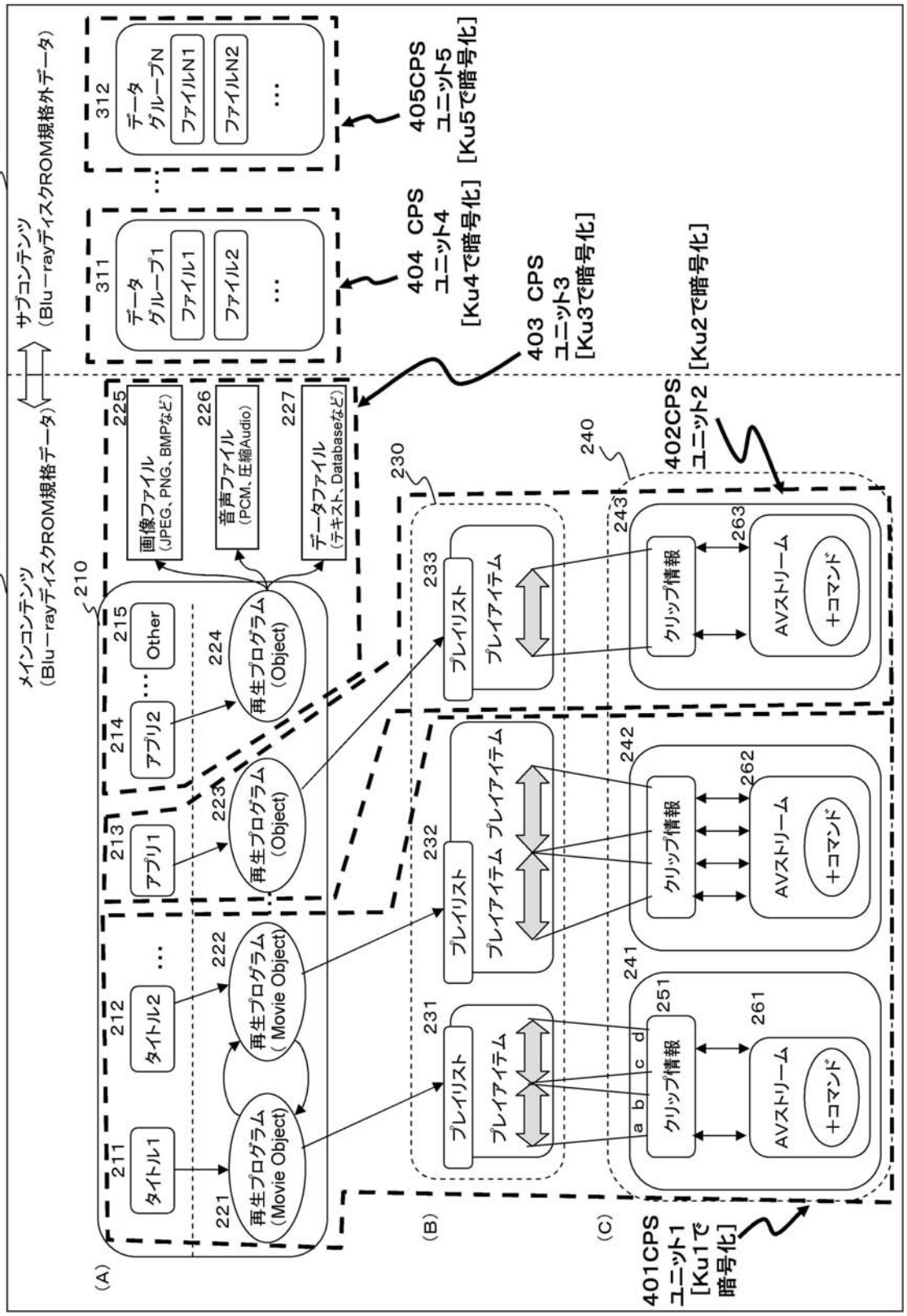
【図１】


100
暗号化コンテンツ
(Encrypted Content)
(AVストリーム)
MKB
ユニット鍵ファイル
バインドシード
(Binding Nonce)
利用制御情報
(CCI)
101
102
103
104
105

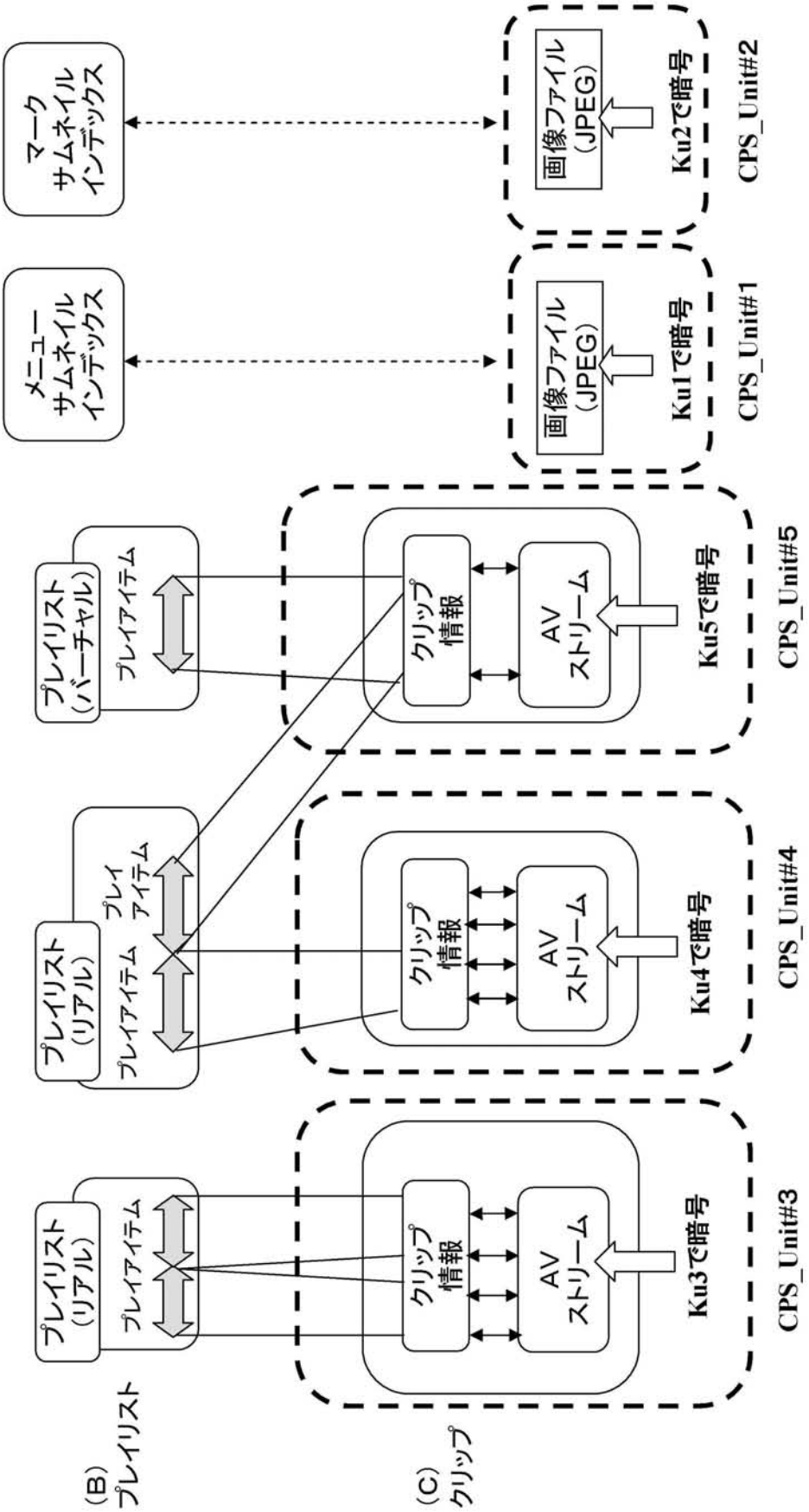
【図４】


300
サブコンテンツ
(Blu－rayディスクROM規格外データ)
311
データ
グループ1
ファイル1
ファイル2
312
データ
グループN
ファイルN1
ファイルN2
200
メインコンテンツ
(Blu－rayディスクROM規格データ)
210
225
画像ファイル
(JPEG、PNG、BMPなど)
226
音声ファイル
(PCM、圧縮Audio)
227
データファイル
(テキスト、Databaseなど)
230
240
(A)アプリケーション
("インデックス"または"アプリケーション＋再生プログラム"または"データの集合")
211
タイトル1
212
タイトル2
213
アプリ1
214
アプリ2
215
Other
221
再生プログラム
(Movie Object)
222
再生プログラム
(Movie Object)
223
再生プログラム
(Object)
224
再生プログラム
(Object)
(B)再生区間指定
ファイル(プレイリスト)
231
プレイリスト
プレイアイテム
234
235
232
プレイリスト
プレイアイテム
プレイアイテム
233
プレイリスト
プレイアイテム
(C)クリップ
(コンテンツデータ
ファイル)
241
242
243
a
b
c
d
251
クリップ情報
261
AVストリーム
＋コマンド
262
クリップ情報
AVストリーム
＋コマンド
263
クリップ情報
AVストリーム
＋コマンド

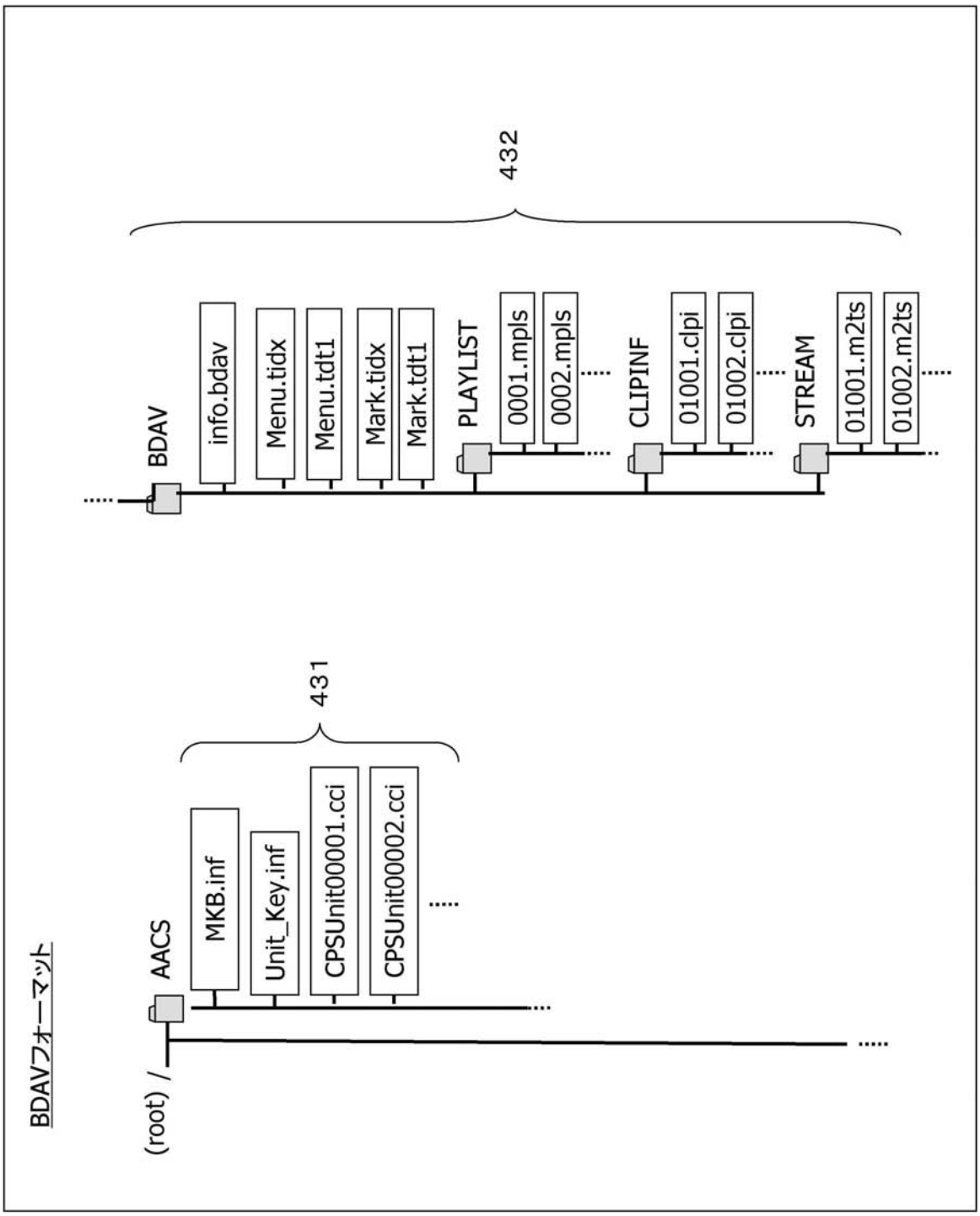
【図５】


300
サブコンテンツ
(Blu－rayディスクROM規格外データ)
200
メインコンテンツ
(Blu－rayディスクROM規格データ)
210
311
データ
グループ1
ファイル1
ファイル2
…
312
データ
グループN
ファイルN1
ファイルN2
…
404 CPS
ユニット4
[Ku4で暗号化]
405CPS
ユニット5
[Ku5で暗号化]
403 CPS
ユニット3
[Ku3で暗号化]
402CPS
ユニット2
[Ku2で暗号化]
401CPS
ユニット1
[Ku1で
暗号化]
225
画像ファイル
(JPEG、PNG、BMPなど)
226
音声ファイル
(PCM、圧縮Audio)
227
データファイル
(テキスト、Databaseなど)
211
タイトル1
212
タイトル2
213
アプリ1
214
アプリ2
215
Other
221
再生プログラム
(Movie Object)
222
再生プログラム
(Movie Object)
223
再生プログラム
(Object)
224
再生プログラム
(Object)
(A)
230
231
プレイリスト
プレイアイテム
232
プレイリスト
プレイアイテム プレイアイテム
233
プレイリスト
プレイアイテム
(B)
240
241
クリップ情報
a b c d
251
AVストリーム
261
+コマンド
242
クリップ情報
AVストリーム
262
+コマンド
243
クリップ情報
AVストリーム
263
+コマンド
(C)

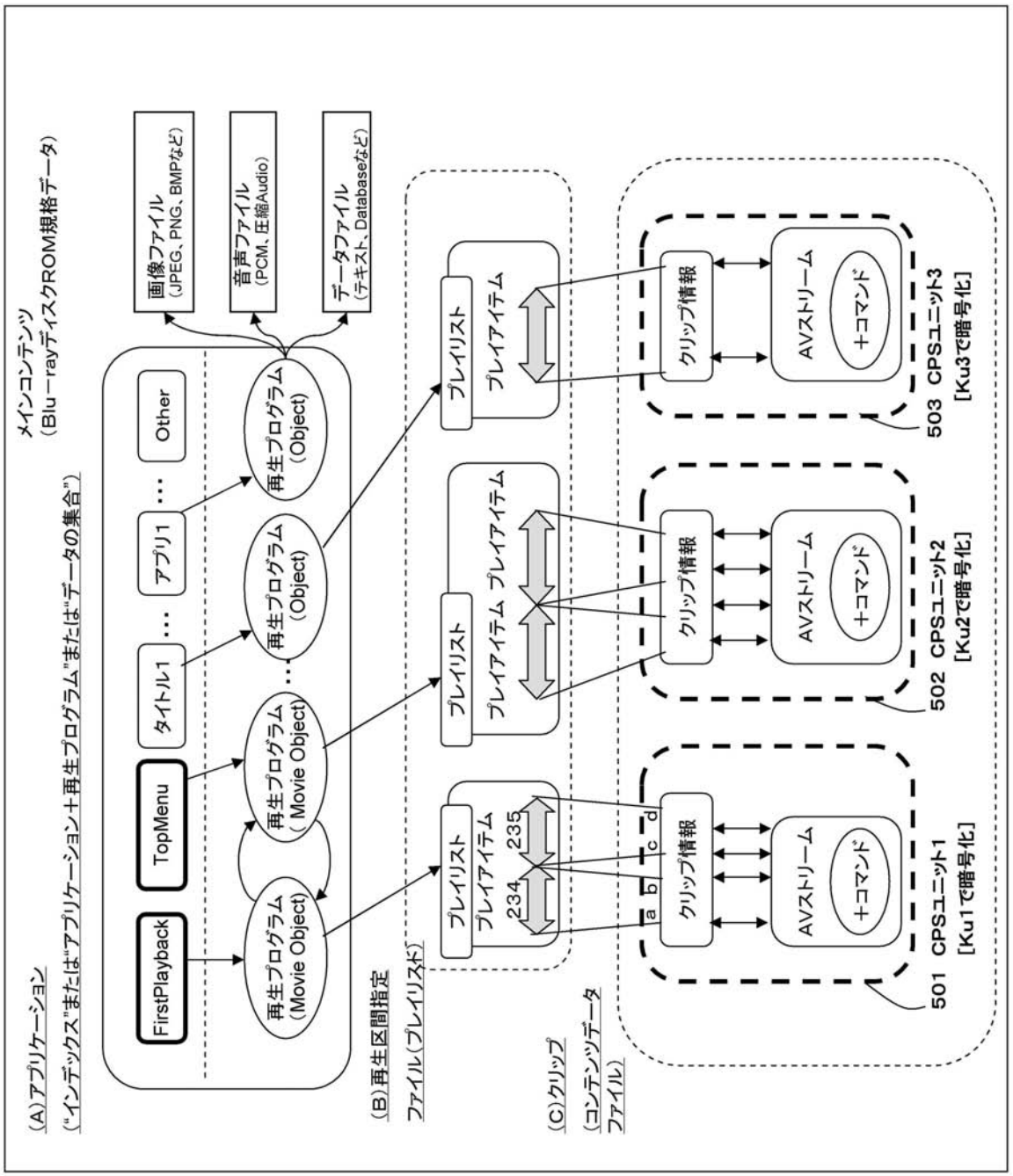
【図７】


マーク
サムネイル
インデックス
メニュー
サムネイル
インデックス
画像ファイル
(JPEG)
Ku2で暗号
CPS_Unit#2
画像ファイル
(JPEG)
Ku1で暗号
CPS_Unit#1
プレイリスト
(バーチャル)
プレイアイテム
クリップ
情報
AV
ストリーム
Ku5で暗号
CPS_Unit#5
プレイリスト
(リアル)
プレイアイテム
プレイアイテム
クリップ
情報
AV
ストリーム
Ku4で暗号
CPS_Unit#4
プレイリスト
(リアル)
プレイアイテム
クリップ
情報
AV
ストリーム
Ku3で暗号
CPS_Unit#3
(B)
プレイリスト
(C)
クリップ

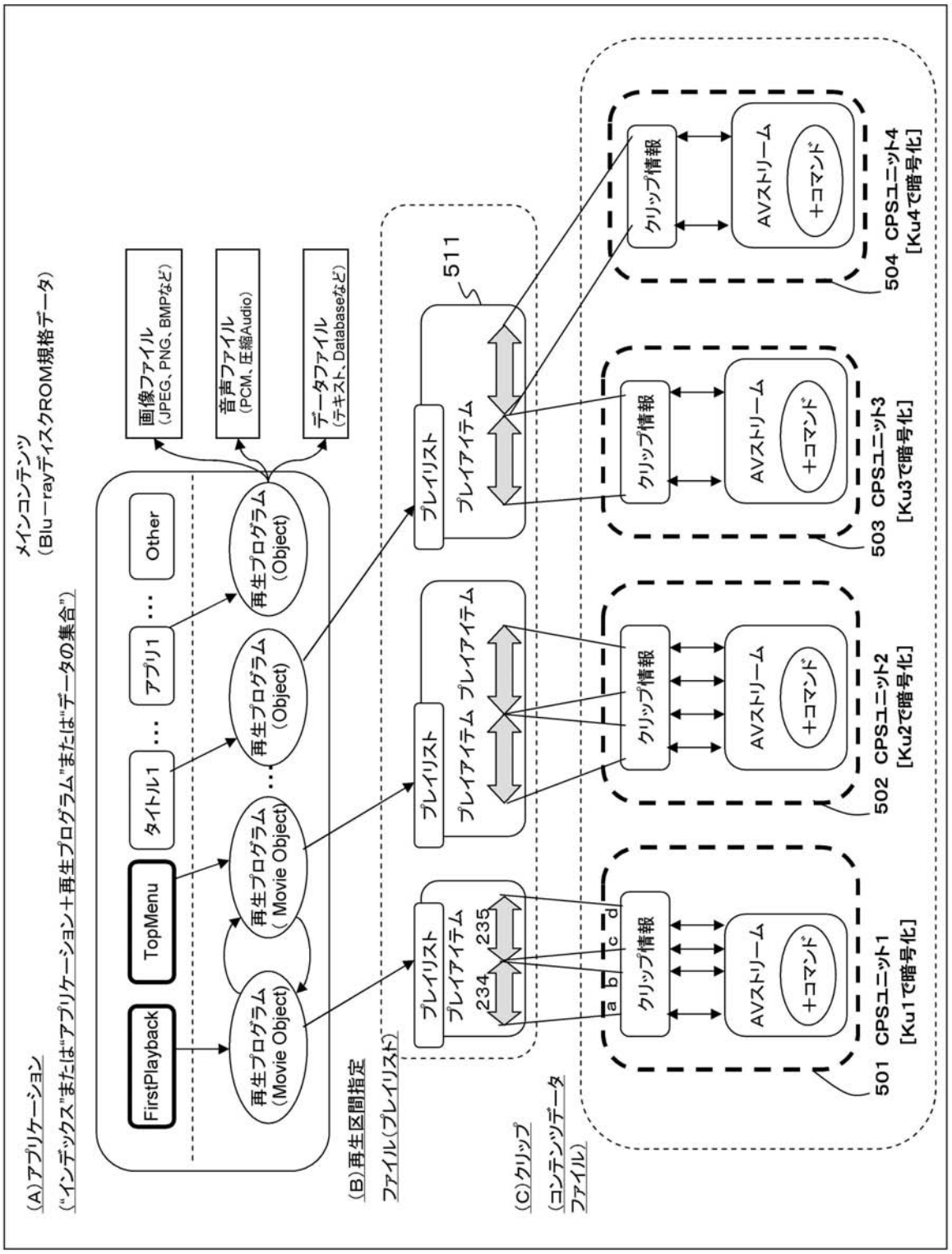
【図１１】


BDAVフォーマット
(root) /
AACS
MKB.inf
Unit_Key.inf
CPSUnit00001.cci
CPSUnit00002.cci
431
BDAV
info.bdav
Menu.tidx
Menu.tdt1
Mark.tidx
Mark.tdt1
PLAYLIST
0001.mpls
0002.mpls
CLIPINF
01001.clpi
01002.clpi
STREAM
01001.m2ts
01002.m2ts
432

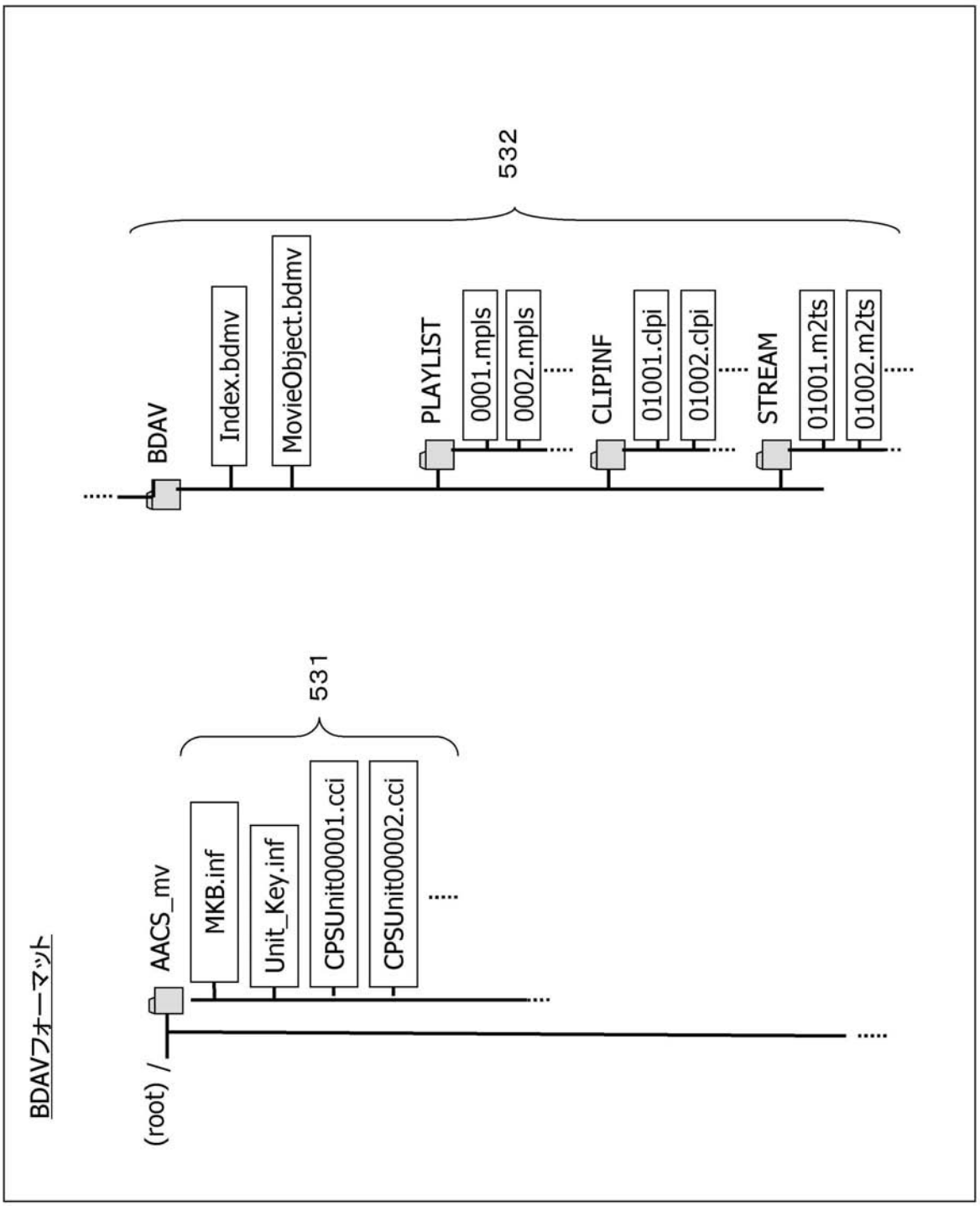
【図１２】


メインコンテンツ
(Blu-rayディスクROM規格データ)
(A)アプリケーション
("インデックス"または"アプリケーション+再生プログラム"または"データの集合")
FirstPlayback
TopMenu
タイトル1
アプリ1
Other
再生プログラム (Movie Object)
再生プログラム (Movie Object)
再生プログラム (Object)
再生プログラム (Object)
画像ファイル (JPEG、PNG、BMPなど)
音声ファイル (PCM、圧縮Audio)
データファイル (テキスト、Database など)
(B)再生区間指定 ファイル(プレイリスト)
プレイリスト
プレイアイテム
234
235
プレイリスト
プレイアイテム
プレイアイテム
プレイリスト
プレイアイテム
(C)クリップ (コンテンツデータ ファイル)
a
b
c
d
クリップ情報
AVストリーム
+コマンド
クリップ情報
AVストリーム
+コマンド
クリップ情報
AVストリーム
+コマンド
501 CPSユニット1 [Ku1で暗号化]
502 CPSユニット2 [Ku2で暗号化]
503 CPSユニット3 [Ku3で暗号化]

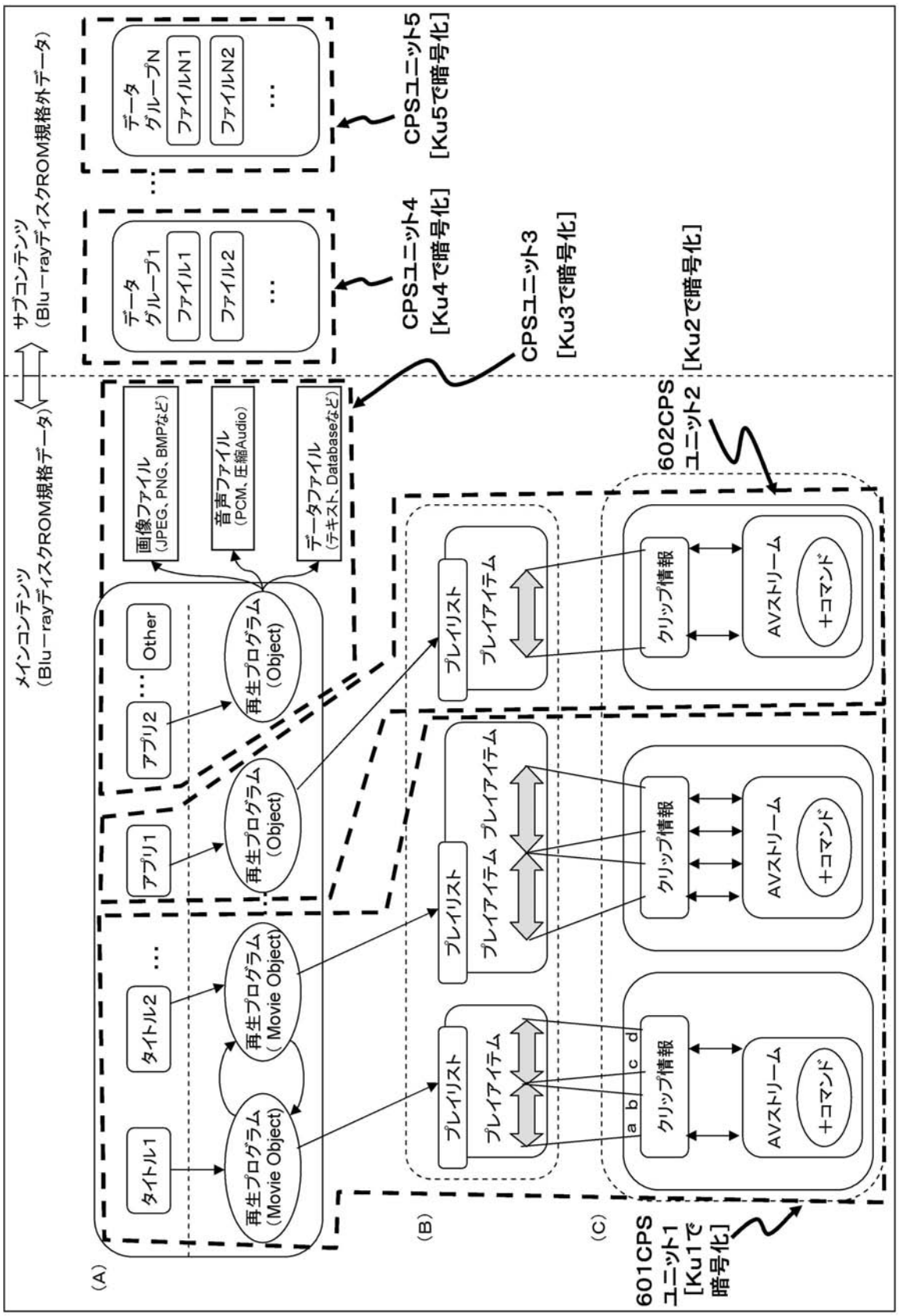
【図１３】


メインコンテンツ
(Blu－rayディスクROM規格データ)
(A)アプリケーション
("インデックス"または"アプリケーション＋再生プログラム"または"データの集合")
FirstPlayback
TopMenu
タイトル1
アプリ1
Other
再生プログラム
(Movie Object)
再生プログラム
(Movie Object)
再生プログラム
(Object)
再生プログラム
(Object)
画像ファイル
(JPEG、PNG、BMPなど)
音声ファイル
(PCM、圧縮Audio)
データファイル
(テキスト、Databaseなど)
(B)再生区間指定
ファイル(プレイリスト)
プレイリスト
プレイアイテム
234
235
プレイリスト
プレイアイテム
プレイアイテム
プレイリスト
プレイアイテム
511
(C)クリップ
(コンテンツデータ
ファイル)
a
b
c
d
クリップ情報
AVストリーム
＋コマンド
501 CPSユニット1
[Ku1で暗号化]
クリップ情報
AVストリーム
＋コマンド
502 CPSユニット2
[Ku2で暗号化]
クリップ情報
AVストリーム
＋コマンド
503 CPSユニット3
[Ku3で暗号化]
クリップ情報
AVストリーム
＋コマンド
504 CPSユニット4
[Ku4で暗号化]

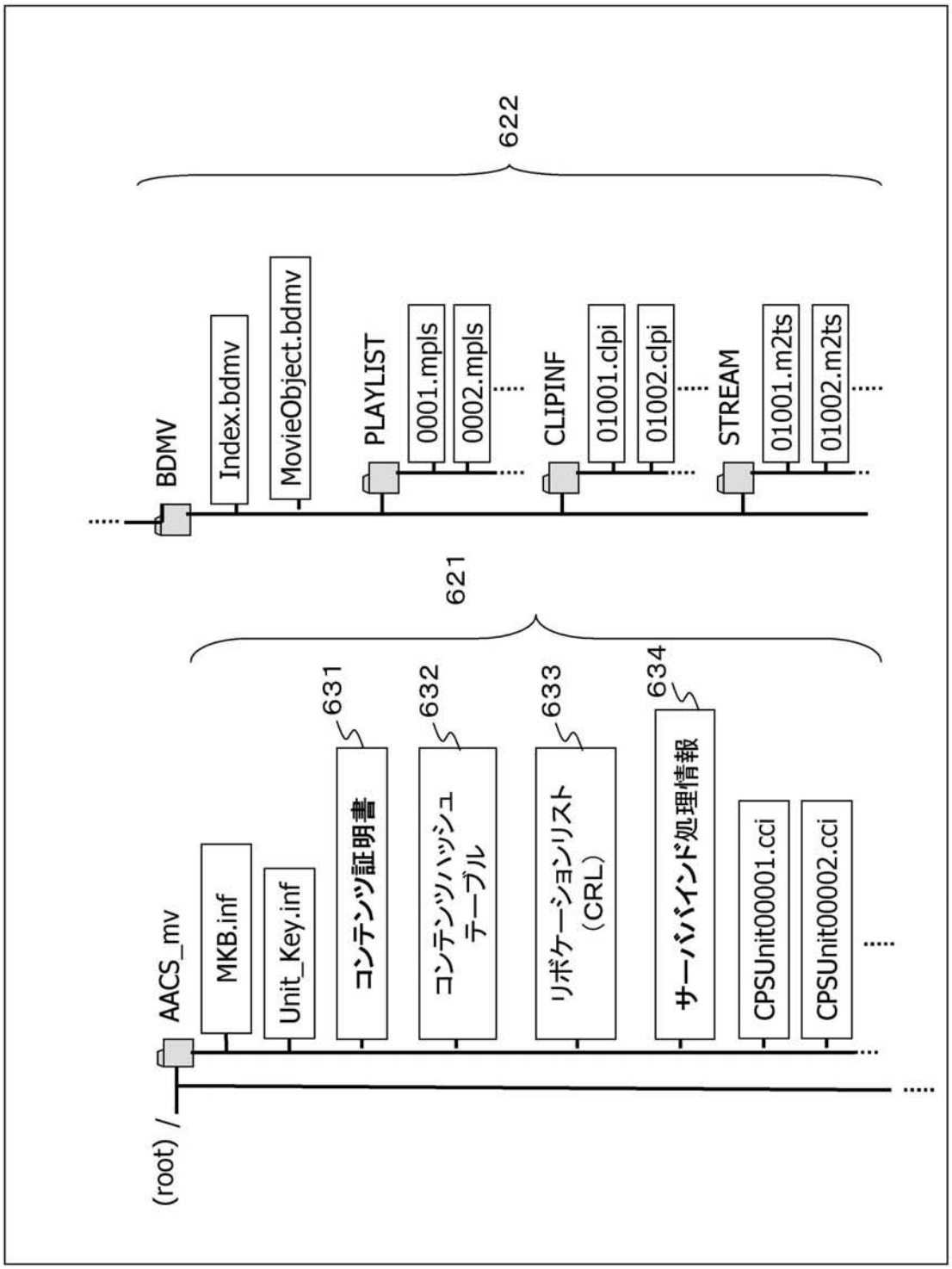
【図１６】


BDAVフォーマット
(root) /
AACS_mv
MKB.inf
Unit_Key.inf
CPSUnit00001.cci
CPSUnit00002.cci
531
BDAV
Index.bdmv
MovieObject.bdmv
PLAYLIST
0001.mpls
0002.mpls
CLIPINF
01001.clpi
01002.clpi
STREAM
01001.m2ts
01002.m2ts
532

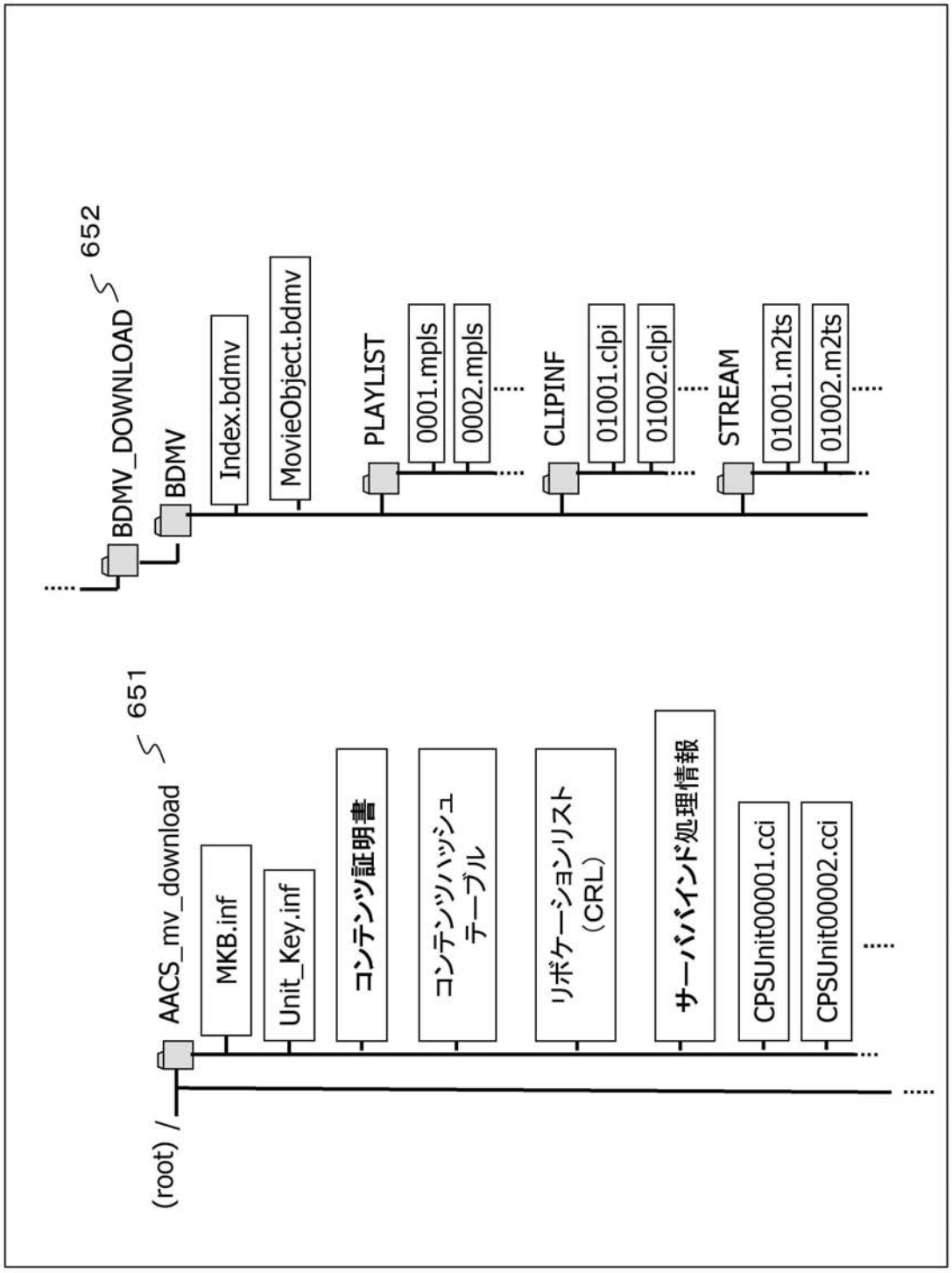
【図１７】


メインコンテンツ
(Blu－rayディスクROM規格データ)
サブコンテンツ
(Blu－rayディスクROM規格外データ)
タイトル1
タイトル2
…
アプリ1
アプリ2
…
Other
再生プログラム
(Movie Object)
再生プログラム
(Movie Object)
再生プログラム
(Object)
再生プログラム
(Object)
画像ファイル
(JPEG、PNG、BMPなど)
音声ファイル
(PCM、圧縮Audio)
データファイル
(テキスト、Databaseなど)
データ
グループ1
ファイル1
ファイル2
…
データ
グループN
ファイルN1
ファイルN2
…
CPSユニット4
[Ku4で暗号化]
CPSユニット5
[Ku5で暗号化]
CPSユニット3
[Ku3で暗号化]
602CPS
ユニット2
[Ku2で暗号化]
(A)
(B)
(C)
プレイリスト
プレイアイテム
プレイアイテム
プレイリスト
プレイアイテム
プレイアイテム
クリップ情報
AVストリーム
+コマンド
クリップ情報
AVストリーム
+コマンド
a b c d
クリップ情報
AVストリーム
+コマンド
601CPS
ユニット1
[Ku1で
暗号化]

【図２０】


(root) /
AACS_mv
MKB.inf
Unit_Key.inf
コンテンツ証明書
631
コンテンツハッシュテーブル
632
リボケーションリスト（CRL）
633
サーババインド処理情報
634
CPSUnit00001.cci
CPSUnit00002.cci
621
BDMV
Index.bdmv
MovieObject.bdmv
PLAYLIST
0001.mpls
0002.mpls
CLIPINF
01001.clpi
01002.clpi
STREAM
01001.m2ts
01002.m2ts
622

【図２１】


(root) /
AACS_mv_download
651
MKB.inf
Unit_Key.inf
コンテンツ証明書
コンテンツハッシュテーブル
リボケーションリスト（CRL）
サーババインド処理情報
CPSUnit00001.cci
CPSUnit00002.cci
BDMV_DOWNLOAD
652
BDMV
Index.bdmv
MovieObject.bdmv
PLAYLIST
0001.mpls
0002.mpls
CLIPINF
01001.clpi
01002.clpi
STREAM
01001.m2ts
01002.m2ts

フロントページの続き

(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

審査官　前田　祐希

(56)参考文献　特開２００５－０９２８３０（ＪＰ，Ａ）
特開２００６－０７２６８８（ＪＰ，Ａ）
特開２００２－２４６９９３（ＪＰ，Ａ）
特開２００６－０７４４２１（ＪＰ，Ａ）
特開２００５－１９１７０７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ１１Ｂ　２０／１０
Ｈ０４Ｎ　５／９１－５／９５