(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3946965号
(P3946965)

(45)発行日　平成19年7月18日(2007.7.18)　(24)登録日　平成19年4月20日(2007.4.20)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G11B 20/10 | (2006.01) | G11B | 20/10 | H |
| G06F 12/14 | (2006.01) | G06F | 12/14 | 320B |
| G06F 12/00 | (2006.01) | G06F | 12/00 | 511C |
| G11B 20/12 | (2006.01) | G06F | 12/00 | 537M |
| G11B 27/00 | (2006.01) | G11B | 20/12 | |

請求項の数 22　(全 24 頁)　最終頁に続く

(21)出願番号　特願2001-110541(P2001-110541)
(22)出願日　平成13年4月9日(2001.4.9)
(65)公開番号　特開2002-304805(P2002-304805A)
(43)公開日　平成14年10月18日(2002.10.18)
審査請求日　平成15年2月21日(2003.2.21)
審判番号　不服2006-15670(P2006-15670/J1)
審判請求日　平成18年7月20日(2006.7.20)

(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　100082762
弁理士　杉浦　正知
(72)発明者　石坂　敏弥
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　山田　誠
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　石黒　隆二
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】無体財産権を保護する情報を記録する記録装置、記録方法、記録媒体、およびプログラム

(57)【特許請求の範囲】

【請求項１】

暗号化されたデータを記録媒体に記録する記録装置において、

所定のファイル構造を持つように、前記データのデータ構造を変換する変換手段と、

前記ファイル構造に変換されたデータを前記記録媒体に記録する記録手段とを備え、

前記ファイル構造は、暗号化されたデータである実データ、当該実データを管理する管理データ、独立したファイルである前記実データの復号化に必要な暗号化鍵を導くための鍵を含む鍵暗号化鍵ファイルへの参照情報および前記暗号化鍵を導くための鍵で暗号化された前記暗号化鍵を有し、

前記実データは複数の第１データ単位により構成され、当該第１データ単位は前記実データが復号化可能な最小単位に対応づけられ、

前記管理データは１または複数の前記第１データ単位ごとに前記実データを管理するとともに、当該管理データが管理する１または複数の前記第１データ単位ごとに成立する無体財産権を保護するための保護情報を収容し、

前記保護情報は、前記１または複数の第１データ単位に関する使用条件を含む著作権保護のための情報が記録される領域および前記鍵暗号化鍵ファイルへの前記参照情報が格納される領域を含むことを特徴とする記録装置。

【請求項２】

前記記録媒体に記録された前記データを再生する再生手段を更に備え、

前記第１データ単位は、前記再生手段による前記実データの再生の最小単位であること

を特徴とする請求項１に記載の記録装置。
【請求項３】
前記所定のファイル構造は階層的なファイル構造であり、
前記管理データは、１または複数の前記第１データ単位に対応する、前記実データを伸張するために必要な情報および前記保護情報を同階層に収容することを特徴とする請求項２に記載の記録装置。
【請求項４】
前記ファイル構造は、前記管理データを前記実データと同一のファイル内に収容することを特徴とする請求項１に記載の記録装置。
【請求項５】
前記実データが復号化可能な最小単位は同一の鍵で暗号化されたデータの単位であることを特徴とする請求項１に記載の記録装置。
【請求項６】
前記使用条件は、前記実データに対し使用の開始の時を示す開始時および前記実データに対し使用の終了の時を示す終了時のうちの少なくとも１つを含むことを特徴とする請求項１に記載の記録装置。
【請求項７】
前記使用条件は、前記実データを再生することができ得る回数を制限する回数制限情報であることを特徴とする請求項１に記載の記録装置。
【請求項８】
前記使用条件は、前記実データを複製することができ得る回数を制限する複製制限情報であることを特徴とする請求項１に記載の記録装置。
【請求項９】
前記使用条件は、前記実データがオリジナルな実データであるか複製された実データであるかを識別する複製識別情報であることを特徴とする請求項１に記載の記録装置。
【請求項１０】
前記保護情報は、前記保護情報が改ざんされたか否かを識別する改ざん識別情報を収容することを特徴とする請求項１に記載の記録装置。
【請求項１１】
データを書き換え可能な記録媒体に記録する記録方法において、
所定のファイル構造を持つように、前記データのデータ構造を変換するステップと、
前記ファイル構造に変換されたデータを前記記録媒体に記録するステップとを備え、
前記ファイル構造は、暗号化されたデータである実データ、当該実データを管理する管理データ、独立したファイルである前記実データの復号化に必要な暗号化鍵を導くための鍵を含む鍵暗号化鍵ファイルへの参照情報および前記暗号化鍵を導くための鍵で暗号化された前記暗号化鍵を有し、
前記実データは複数の第１データ単位により構成され、当該第１データ単位は前記実データが復号化可能な最小単位に対応づけられ、
前記管理データは、１または複数の前記第１データ単位ごとに前記実データを管理するとともに、当該管理データが管理する１または複数の前記第１データ単位ごとに成立する無体財産権を保護するための保護情報を収容し、
前記保護情報は、前記１または複数の第１データ単位に関する使用条件を含む著作権保護のための情報が記録される領域および前記鍵暗号化鍵ファイルへの前記参照情報が格納される領域を含むことを特徴とする記録方法。
【請求項１２】
所定のファイル構造となるように変換された実データを記録する記録媒体であって、
前記ファイル構造は、暗号化されたデータである実データ、当該実データを管理する管理データ、独立したファイルである前記実データの復号化に必要な暗号化鍵を導くための鍵を含む鍵暗号化鍵ファイルへの参照情報および前記暗号化鍵を導くための鍵で暗号化された前記暗号化鍵を有し、

前記実データは複数の第１データ単位により構成され、当該第１データ単位は前記実データが復号化可能な最小単位に対応づけられ、
前記管理データは、１または複数の前記第１データ単位ごとに前記実データを管理するとともに、当該管理データが管理する１または複数の前記第１データ単位ごとに成立する無体財産権を保護するための保護情報を収容し、
前記保護情報は、前記１または複数の第１データ単位に関する使用条件を含む著作権保護のための情報が記録される領域および前記鍵暗号化鍵ファイルへの前記参照情報が格納される領域を含むことを特徴とする記録媒体。
【請求項１３】
前記第１データ単位は、前記実データの再生の最小単位であることを特徴とする請求項１１に記載の記録方法。
【請求項１４】
前記所定のファイル構造は階層的なファイル構造であり、
前記管理データは、１または複数の前記第１データ単位に対応する、前記実データを伸張するために必要な情報および前記保護情報を同階層に収容することを特徴とする請求項１３に記載の記録方法。
【請求項１５】
前記ファイル構造は、前記管理データを前記実データと同一のファイル内に収容することを特徴とする請求項１１に記載の記録方法。
【請求項１６】
前記実データが復号化可能な最小単位は同一の鍵で暗号化されたデータの単位であること
を特徴とする請求項１１に記載の記録方法。
【請求項１７】
前記使用条件は、前記実データに対し使用の開始の時を示す開始時および前記実データに対し使用の終了の時を示す終了時のうちの少なくとも１つを含むことを特徴とする請求項１１に記載の記録方法。
【請求項１８】
前記使用条件は、前記実データを再生することができ得る回数を制限する回数制限情報であることを特徴とする請求項１１に記載の記録方法。
【請求項１９】
前記使用条件は、前記実データを複製することができ得る回数を制限する複製制限情報であることを特徴とする請求項１１に記載の記録方法。
【請求項２０】
前記使用条件は、前記実データがオリジナルな実データであるか複製された実データであるかを識別する複製識別情報であることを特徴とする請求項１１に記載の記録方法。
【請求項２１】
前記保護情報は、前記保護情報が改ざんされたか否かを識別する改ざん識別情報を収容することを特徴とする請求項１１に記載の記録方法。
【請求項２２】
暗号化されたデータを記録媒体に記録するプログラムにおいて、
コンピュータに、
所定のファイル構造を持つように、前記データのデータ構造を変換するステップと、
前記ファイル構造に変換されたデータを前記記録媒体に記録するステップとを実行させ
、
前記ファイル構造は、暗号化されたデータである実データ、当該実データを管理する管理データ、独立したファイルである前記実データの復号化に必要な暗号化鍵を導くための鍵を含む鍵暗号化鍵ファイルへの参照情報および前記暗号化鍵を導くための鍵で暗号化された前記暗号化鍵を有し、
前記実データは複数の第１データ単位により構成され、当該第１データ単位は前記実デ

ータが復号化可能な最小単位に対応づけられ、
前記管理データは、１または複数の前記第１データ単位ごとに前記実データを管理するとともに、当該管理データが管理する１または複数の前記第１データ単位ごとに成立する無体財産権を保護するための保護情報を収容し、
前記保護情報は、前記１または複数の第１データ単位に関する使用条件を含む著作権保護のための情報が記録される領域および前記鍵暗号化鍵ファイルへの前記参照情報が格納される領域を含むことを特徴とするプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、記録媒体に映像データやオーディオデータなどを記録する記録装置において、特に、記録媒体に記録されているこれらデータに成立する無体財産権などの権利を保護する機能を備える記録装置に関する。そして、このような記録装置に用いられる記録方法、記録媒体、およびプログラムに関する。
【０００２】
【従来の技術】
映像データ、オーディオデータまたはコンピュータプログラムなどのデータは、記録媒体に製造工場で記録されて消費者に頒布されたり、通信回線を通じて記録媒体にダウンロードされて消費者に拡布されたりする。
【０００３】
記録媒体は、例えば、ＣＤ（compact disc）およびＤＶＤ（digital versataile discまたはdigital video disc）などの光ディスク、ＭＤなどの光磁気ディスクおよびメモリカードなどである。
【０００４】
【発明が解決しようとする課題】
ところで、データの頒布・拡布に際し、これらデータに成立する無体財産権、特に、著作権や特許権などを保護する必要がある。
【０００５】
そこで、本発明は、データに成立する無体財産権を保護する機能を備えた記録装置を提供することを目的とする。
【０００６】
さらに、本発明は、無体財産権を保護することができる記録方法、無体財産権を保護することができるようにデータが記録された記録媒体、および無体財産権を保護することができるプログラムを提供することを目的とする。
【０００７】
【課題を解決するための手段】
本発明は、暗号化されたデータを記録媒体に記録する記録装置において、
所定のファイル構造を持つように、データのデータ構造を変換する変換手段と、
ファイル構造に変換されたデータを記録媒体に記録する記録手段とを備え、
ファイル構造は、暗号化されたデータである実データ、当該実データを管理する管理データ、独立したファイルである実データの復号化に必要な暗号化鍵を導くための鍵を含む鍵暗号化鍵ファイルへの参照情報および暗号化鍵を導くための鍵で暗号化された暗号化鍵を有し、
実データは複数の第１データ単位により構成され、当該第１データ単位は実データが復号化可能な最小単位に対応づけられ、
管理データは１または複数の第１データ単位ごとに実データを管理するとともに、当該管理データが管理する１または複数の第１データ単位ごとに成立する無体財産権を保護するための保護情報を収容し、
保護情報は、１または複数の第１データ単位に関する使用条件を含む著作権保護のための情報が記録される領域および鍵暗号化鍵ファイルへの参照情報が格納される領域を含む

ことを特徴とする記録装置である。

【０００８】

本発明では、このような記録装置において、保護情報を独立なファイルに収容し、前記データ部分には前記ファイルを指定する指定情報を収容するようにしても良い。

【０００９】

本発明では、このような記録装置において、無体財産権を確実に保護する観点から、実データを所定の暗号方法で暗号化して、保護情報には、暗号化された実データを復号するために必要な鍵を含むようにすると好適であり、さらに、鍵自体を所定の暗号方法で暗号化し、データ部分に、暗号化された鍵を復号するために必要な鍵をさらに収容するようにすると好適である。

【００１０】

本発明では、このような記録装置において、無体財産権を確実に保護する観点から、データ部分に、保護情報が改ざんされたか否かを識別する改ざん識別情報をさらに収容するようにすると好適である。

【００１１】

本発明では、このような記録装置において、無体財産権を確実に保護する観点から、保護情報には、前記実データに対し使用の開始の時を示す開始時および前記実データに対し使用の終了の時を示す終了時のうちの少なくとも１つを含めたり、前記実データを再生することができ得る回数を制限する回数制限情報を含めたり、前記実データを複製することができ得る回数を制限する複製制限情報を含めたり、前記実データがオリジナルな実データであるか複製された実データであるかを識別する複製識別情報を含めたりすると好適である。

【００１２】

このように本発明は、無体財産権を保護するための保護情報を記録媒体に記録された実データと関連付けて記録するので、実データを権利侵害から確実に保護することができる。さらに、第１データ単位ごとに保護情報を付するので、記録媒体ごとではなく、個々の実データごとに権利侵害から確実に保護することができる。このため、第１データ単位ごとに様々なサービスを提供することができる。

【００１３】

【発明の実施の形態】

以下、本発明の実施形態について図面に基づいて説明する。なお、各図において、同一の符号は、同一の構成であることを示す。

【００１４】

図１は、ディジタル記録再生装置の一構成例を示すブロック図である。

【００１５】

図１において、ディジタル記録再生装置は、ビデオ符号器１１、オーディオ符号器１２、ビデオ復号器１３、オーディオ復号器１４、ファイル生成器１５、ファイル復号器１６、メモリ１７、２０、メモリコントローラ１８、システム制御マイコン１９、エラー訂正符号／復号器２１、ドライブ制御マイコン２２、データ変復調器２３、磁界変調ドライバ２４、操作部２６、サーボ回路３０、モータ３１、磁界ヘッド３２および光ピックアップ３３を備えて構成される。

【００１６】

ビデオ信号は、ビデオ入力端子からビデオ符号器１１に供給され、圧縮符号化される。オーディオ信号は、オーディオ入力端子からオーディオ符号器１２に供給され、圧縮符号化される。ビデオ符号器１１およびオーディオ符号器１２の各出力がエレメンタリストームと呼ばれる。

【００１７】

本実施形態では、ディジタル記録再生装置は、カメラ一体型ディジタル記録再生装置に備えられているものとする。ビデオ信号は、ビデオカメラで撮影された画像が供給され、ビデオカメラは、光学系によって被写体の撮像光がCCD(Charge Coupled Device)などの撮像

素子に供給されることによってビデオ信号を生成する。オーディオ信号は、マイクロフォンで集音された音声が供給される。

【００１８】

ビデオ符号器１１は、例えば、圧縮符号化がＭＰＥＧの場合には、アナログ／ディジタル変換器（Ａ／Ｄ変換器）、フォーマット変換部、画像並替部、減算器、ＤＣＴ部、量子化部、可変長符号化部、バッファメモリ、レート制御部、逆量子化部、逆ＤＣＴ部、加算部、フレームメモリ、動き補償予測部およびスイッチの各電子回路を備えて構成される。

【００１９】

ビデオ符号器１１に供給されたビデオ信号は、Ａ／Ｄ変換器でディジタル化された後に、フォーマット変換部で符号化で用いる空間解像度に変換され、画像並替部に出力される。画像並替部は、ピクチャの順序を符号化処理に適した順に並び替える。画面並替部の出力は、減算部を介してＤＣＴ部に入力され、ＤＣＴ符号化が行われる。ＤＣＴ部の出力は、量子化部に入力され、所定のビット数で量子化される。量子化部の出力は、可変長符号化部および逆量子化部に入力される。可変長符号化部は、ハフマン符号などの可変長符号で符号化され、符号化データは、メモリのバッファメモリに出力される。バッファメモリは、一定レートで符号化データをビデオ符号器の出力として出力する。また、レート制御部は、可変長符号化部で発生する符号量が可変であるため、バッファメモリを監視することによって所定のビットレートを保つように、量子化部の量子化動作を制御する。

【００２０】

一方、ＩピクチャおよびＰピクチャの場合は、動き補償予測部で参照画面として使用されるため、量子化部から逆量子化部に入力された信号は、逆量子化された後に逆ＤＣＴ部に入力され、逆ＤＣＴが行われる。逆ＤＣＴ部の出力は、加算部で動き補償予測部の出力と加算され、フレームメモリに入力される。フレームメモリの出力は、動き補償予測部に入力される。動き補償予測部は、前方向予測、後方向予測および両方向予測を行い、加算部および減算部に出力する。これら逆量子化部、逆ＤＣＴ部、加算部、フレームメモリおよび動き補償予測部は、ローカル復号部を構成し、ビデオ復号器と同一のビデオ信号が復元される。

【００２１】

減算部は、画像並替部の出力と動き補償予測部の出力との間で減算を行い、ビデオ信号とローカル復号部で復号された復号ビデオ信号との間の予測誤差を形成する。フレーム内符号化（Ｉピクチャ）の場合では、スイッチにより、減算部は、減算処理を行わず、単にデータが通過する。

【００２２】

図１に戻って、オーディオ符号器１２は、例えば、ＭＰＥＧ／Ａｕｄｉｏレイヤ１／レイヤ２の場合では、サブバンド符号化部および適応量子化ビット割り当て部などの各電子回路を備えて構成される。オーディオ信号は、サブバンド符号化部で３２帯域のサブバンド信号に分割され、適応量子化ビット割り当て部で心理聴覚重み付けに従って量子化され、ビットストリームに形成された後に出力される。なお、符号化品質を向上させるために、ＭＰＥＧ／Ａｕｄｉｏレイヤ３を適用しても良い。

【００２３】

ビデオ符号器１１の出力およびオーディオ符号器１２の出力がファイル生成器１５に供給される。ファイル生成器１５は、特定のハードウェア構成を使用することなく動画、音声およびテキストなどを同期して再生することができるコンピュータソフトウェアにより扱うことができるファイル構造を持つように、ビデオエレメンタリストリームおよびオーディオエレメンタリストームのデータ構造を変換する。このようなソフトウェアは、例えば、QuickTime（米Apple社が提供するクロスプラットホームマルチメディアフォーマットの代表、以下、「ＱＴ」と略記する。）が知られている。以下、ＱＴを使用する場合について説明する。ファイル生成器１５は、システム制御マイコン１９の制御下で符号化ビデオデータと符号化オーディオデータとを暗号化鍵で暗号化した後にこれらを多重化する。

【００２４】

暗号化アルゴリズムは、暗号化の単位を一定の単位長とする観点から、本実施形態では、ブロック暗号方式が好適であり、例えば、後述のＤＥＳ、ＦＥＡＬ、ＭＩＳＴＹ、ＭＵＬＴＩ、ＩＤＥＡ、ＲＣ５などがある。

【００２５】

ファイル生成器１５の出力であるQuickTimeムービーファイルは、メモリコントローラ１８を介してメモリ１７に順次に書き込まれる。メモリコントローラ１８は、システム制御マイコン１９から記録媒体４０へのデータ書き込みが要求されると、メモリ１７からQuickTimeムービーファイルを読み出す。また、システム制御マイコン１９は、プログラムを実行中に生じる各種データをメモリコントローラ１８を介してメモリ１７に格納する。

【００２６】

ここで、QuickTimeムービー符号化の転送レートは、記録媒体４０への書き込みデータの転送レートより低い転送レート、例えば、１／２に設定される。よって、QuickTimeムービーファイルが連続的にメモリ１７に書き込まれるのに対し、メモリ１７からのQuickTimeムービーファイルの読み出しは、メモリ１７がオーバーフローまたはアンダーフローしないように、システム制御マイコン１９によって監視されながら間欠的に行われる。

【００２７】

メモリ１７から読み出されたQuickTimeムービーファイルは、メモリコントローラ１８からエラー訂正符号／復号器２１に供給される。エラー訂正符号／復号器２１は、このQuickTimeムービーファイルを一旦メモリ２０に書き込み、インターリーブ（interleaved）およびエラー訂正符号の冗長データの生成を行う。エラー訂正符号／復号器２１は、冗長データが付加されたデータをメモリ２０から読み出し、これをデータ変復調器２３に供給する。

【００２８】

データ変復調器２３は、デジタルデータを記録媒体４０に記録する際に、再生時のクロック抽出を容易とし、符号間干渉などの問題が生じないように、データを変調する。例えば、（１，７）ＲＬＬ（run length limited）符号やトレリス符号などを利用することができる。

【００２９】

データ変復調器２３の出力は、磁界変調ドライバ２４および光ピックアップ３３に供給される。磁界変調ドライバ２４は、入力信号に応じて、磁界ヘッド３２を駆動して記録媒体４０に磁界を印加する。光ピックアップ３３は、入力信号に応じて記録用のレーザビームを記録媒体４０に照射する。このようにして、記録媒体４０にデータが記録される。

【００３０】

記録媒体４０は、ディスク状の記録媒体であり、例えば、光磁気ディスク（ＭＯ、magneto-optical disk）、相変化型ディスクなどの書き換え可能な光ディスクである。

【００３１】

本実施形態では、ＭＯ、例えば、直径約４ｃｍ、直径約５ｃｍ、直径約６．５ｃｍまたは直径約８ｃｍなどの比較的小径なディスクが使用される。記録媒体４０は、モータ３１によって、線速度一定（ＣＬＶ、constant linear velocity）、角速度一定（ＣＡＶ、constant angular velocity）またはゾーンＣＬＶ（ＺＣＬＶ、zone constant linear velocity）で回転される。

【００３２】

ドライブ制御マイコン２２は、システム制御マイコン１９の要求に応じて、サーボ回路３０に信号を出力する。サーボ回路３０は、この出力に応じて、モータ３１および光ピックアップ３３を制御することによって、ドライブ全体を制御する。例えば、サーボ回路３０は、光ピックアップ３３に対し、記録媒体４０の径方向の移動サーボ、トラッキングサーボおよびフォーカスサーボを行い、モータ３１に対し、回転数を制御する。

【００３３】

また、システム制御マイコン１９には、ユーザが所定の指示を入力する操作部２６が接続される。

【００３４】
再生の際には、光ピックアップ３３は、再生用の出力でレーザビームを記録媒体４０に照射し、その反射光を光ピックアップ３３内の光検出器で受光することによって、再生信号を得る。この場合において、ドライブ制御マイコン２２は、光ピックアップ３３内の光検出器の出力信号からトラッキングエラーおよびフォーカスエラーを検出し、読み取りのレーザビームがトラック上に位置し、トラック上に合焦するように、サーボ回路３０によって光ピックアップ３３を制御する。さらに、ドライブ制御マイコン２２は、記録媒体４０上における所望の位置のデータを再生するために、光ピックアップの径方向における移動も制御する。所望の位置は、記録時と同様にシステム制御マイコン１９によって、ドライブ制御マイコン２２に信号が与えられ、決定される。

【００３５】
光ピックアップ３３の再生信号は、データ変復調器２３に供給され、復調される。復調されたデータは、エラー訂正符号／復号器２１に供給され、再生データを一旦メモリ２０に格納し、デインターリーブ（deinterleaved）およびエラー訂正が行われる、エラー訂正後のQuickTimeムービーファイルは、メモリコントローラ１８を介してメモリ１７に格納される。

【００３６】
メモリ１７に格納されたQuickTimeムービーファイルは、システム制御マイコン１９の要求に応じて、ファイル復号器１６に出力される。システム制御マイコン１９は、ビデオ信号およびオーディオ信号を連続再生するために、記録媒体４０の再生信号がメモリ１７に格納されるデータ量と、メモリ１７から読み出されてファイル復号器１６に供給されるデータ量とを監視することによって、メモリ１７がオーバーフローまたはアンダーフローしないようにメモリコントローラ１８およびドライブ制御マイコン２２を制御する。こうして、システム制御マイコン１９は、記録媒体４０から間欠的にデータを読み出す。

【００３７】
ファイル復号器１６は、システム制御マイコン１９の制御下で、QuickTimeムービーファイルをビデオエレメンタリストリームとオーディオエレメンタリファイルとに分離する。ファイル復号器１６は、システム制御マイコン１９の制御下で後述の権利保護情報および暗号化鍵に基づいてデータを復号する。ここで、権利保護情報の内容がデータの使用を禁止する場合、または、暗号化鍵が適正ではない場合には、データは、復号されない。復号されたビデオエレメンタリストリームは、ビデオ復号器１３に供給され、圧縮符号化の復号が行われてビデオ出力となってビデオ出力端子から出力される。復号されたオーディオエレメンタリストリームは、オーディオ復号器１４に供給され、圧縮符号化の復号が行われてオーディオ出力となってオーディオ出力端子から出力される。ここで、ファイル復号器１６は、ビデオエレメンタリストリームとオーディオエレメンタリストリームとが同期するように出力する。

【００３８】
ビデオ復号器１３は、例えば、ＭＰＥＧの場合では、メモリのバッファメモリ、可変長符号復号部、逆量子化部、逆ＤＣＴ部、加算部、フレームメモリ、動き補償予測部、画面並替部およびディジタル／アナログ変換器（以下、「Ｄ／Ａ」と略記する。）の各電子回路を備えて構成される。ビデオエレメンタリストームは、一旦バッファメモリに蓄積され、可変長復号部に入力される。可変長復号部は、マクロブロック符号化情報が復号され、予測モード、動きベクトル、量子化情報および量子化ＤＣＴ係数が分離される。量子化ＤＣＴ係数は、逆量子化部でＤＣＴ係数に復元され、逆ＤＣＴ部で画素空間データに変換される。加算部は、逆量子化部の出力と動き補償予測部の出力とを加算するが、Ｉピクチャを復号する場合には、加算しない。画面内のすべてのマクロブロックが復号され、画面は、画面並替部で元の入力順序に並べ替えられて、Ｄ／Ａでアナログ信号に変換されて出力される。また、加算器の出力は、ＩピクチャおよびＰピクチャの場合には、その後の復号処理で参照画面として使用されるため、フレームメモリに蓄積され、動き補償予測部に出力される。

【００３９】
オーディオ復号器１４は、例えば、ＭＰＥＧ／Ａｕｄｉｏレイヤ１／レイヤ２の場合では、ビットストリーム分解部、逆量子化部およびサブバンド合成フィルタバンク部などの各電子回路を備えて構成される。入力されたオーディオエレメンタリストリームは、ビットストリーム分解部でヘッダと補助情報と量子化サブバンド信号とに分離され、量子化サブバンド信号は、逆量子化部で割り当てられたビット数で逆量子化され、サブバンド合成フィルタバンクで合成された後に、出力される。
【００４０】
このようなディジタル記録再生装置は、ビデオデータ、オーディオデータ、テキストデータおよびコンピュータプログラムなど、無体財産権（著作権や特許権など）が成立するデータを記録媒体４０に記録する際に、無体財産権を保護するためのデータ（以下、「権利保護データ」と呼称する。）も記録される。そして、権利保護データは、ディジタル記録再生装置がビデオデータなどの保護すべきデータと同様に扱えるように、保護すべきデータと同一のファイル形式で生成される。本実施形態では、保護すべきデータおよび権利保護データは、例えば、QuickTimeムービーファイルの形式で生成される。このため、記録再生装置は、すべてをＱＴで再生することができる。
【００４１】
ＱＴは、各種データを時間軸に沿って管理するソフトウェアであり、特殊なハードウェアを用いずに動画や音声やテキストなどを同期して再生するためのＯＳ拡張機能である。ＱＴは、例えば、「INSIDE MACINTOSH :QuickTime（日本語版）（アジソンウエスレス）」などに開示されている。以下、この文献に沿って、QuickTimeムービーファイルについて概説する。
【００４２】
ＱＴムービーリソースの基本的なデータユニットは、アトム（atom）と呼ばれ、各アトムは、そのデータとともに、サイズおよびタイプ情報を含んでいる。また、ＱＴでは、データの最小単位がサンプル（sample）として扱われ、サンプルの集合としてチャンク（chunk）が定義される。
【００４３】
図２は、QuickTimeムービーファイルの一構成例を示す図である。
【００４４】
図３は、ビデオメディア情報アトムの一構成例を示す図である。図３は、図２におけるビデオメディア情報アトムをより詳細に示した図となっており、トラックがビデオ情報の場合について示している。
【００４５】
図２および図３において、QuickTimeムービーファイルは、大きく２つの部分、ムービーアトム（movie atom）１０１およびムービー・データ・アトム（movie data atom）１０２から構成される。ムービーアトム１０１は、そのファイルを再生するために必要な情報や実データを参照するために必要な情報を格納する部分である。ムービー・データ・アトム１０２は、ビデオデータ、オーディオデータ、コンピュータプログラムおよびテキストデータなどの実データを格納する部分である。
【００４６】
ムービーアトム１０１は、ムービー全体に関する情報を収容するムービー・ヘッダ・アトム（movie header atom）１１１、クリッピング領域を指定するムービー・クリッピング・アトム（movie clipping atom）１１２、ユーザ定義データアトム１１３、および、１または複数のトラックアトム（track atom）１１４などを含む。
【００４７】
トラックアトム１１４は、ムービー内の１つのトラックごとに用意される。トラックアトム１１４は、トラック・ヘッダ・アトム（track header atom）１３１、トラック・クリッピング・アトム（track clipping atom）１３２、トラック・マット・アトム（track matte atom）１３３、エデットアトム（edit atom）１３４およびメディアアトム（media

atom）１３５に、ムービー・データ・アトム１０２の個々のデータに関する情報を記述する。図２では、１つのビデオムービーのトラックアトム１１４-1が示され、他のトラックアトムは、省略されている。

【００４８】

メディアアトム１３５は、メディア・ヘッダ・アトム（media header atom）１４４、メディア情報アトム（media information atom）（図２および図３では、ビデオメディア情報アトム１４５）、および、メディア・ハンドラ・リファレンス・アトム（media handler reference atom）１４６に、ムービートラックのデータやメディアデータを解釈するコンポーネントを規定する情報などを記述する。

【００４９】

メディア・ハンドラは、メディア情報アトムの情報を使用して、メディア時間からメディアデータへのマッピングを行う。

【００５０】

メディア情報アトム１４５は、データ・ハンドラ・リファレンス・アトム（data handler reference atom）１６１、メディア情報ヘッダ・アトム（media information header atom）１６２、データ情報アトム（data information atom）１６３およびサンプル・テーブル・アトム（sample table atom）１６４を含む。

【００５１】

メディア情報ヘッダ・アトム（図３では、ビデオ・メディア情報ヘッダ・アトム１６２）は、メディアにかかる情報が記述される。データ・ハンドラ・リファレンス・アトム１６１は、メディアデータの取り扱いにかかる情報が記述され、メディアデータへのアクセス手段を提供するデータ・ハンドラ・コンポーネントを指定するための情報が含まれる。データ情報アトム１６３は、データ・リファレンス・アトム（data reference atom）を含み、データについての情報が記述される。

【００５２】

サンプル・テーブル・アトム１６４は、メディア時間を、サンプル位置を指すサンプル番号に変換するために必要な情報を含む。サンプル・テーブル・アトム１６４は、サンプル・サイズ・アトム（sample size atom）１７２、時間サンプルアトム（time-to-sample atom）１７３、同期サンプルアトム（sync sample atom）１７４、サンプル・ディスクリプション・アトム（sample description atom）１７５、サンプル・チャンク・アトム（sample-to-chunk atom）１７６、チャンク・オフセット・アトム（chunk offset atom）１７７、および、シャドー同期アトム（shadow sync atom）１７８で構成される。

【００５３】

サンプル・サイズ・アトム１７２は、サンプルの大きさが記述される。時間サンプル・アトム１７３は、何秒分のデータが記録されているか？という、サンプルと時間軸との関係が記述される。同期サンプルアトム１７４は、同期にかかる情報が記述され、メディア内のキーフレームが指定される。キーフレームは、先行するフレームに依存しない自己内包型のフレームである。サンプル・ディスクリプション・アトム１７５は、メディア内のサンプルをデコード（decode）するために必要な情報が保存される。メディアは、当該メディア内で使用される圧縮タイプの種類に応じて、１つまたは複数のサンプル・ディスクリプション・アトムを持つことができる。サンプル・チャンク・アトム１７６は、サンプル・ディスクリプション・アトム１７５内のテーブルを参照することで、メディア内の各サンプルに対応するサンプル・ディスクリプションを識別する。サンプル・チャンク・アトム１７６は、サンプルとチャンクとの関係が記述され、先頭チャンク、チャンク当たりのサンプル数およびサンプル・ディスクリプションＩＤ（sample description-ID）の情報を基に、メディア内におけるサンプル位置が識別される。チャンク・オフセット・アトム１７７は、ムービーデータ内でのチャンクの開始ビット位置が記述され、データストリーム内の各チャンクの位置が規定される。

【００５４】

また、ムービー・データ・アトム１０２には、図２では、例えば、所定の圧縮符号化方式

によって符号化されたオーディオデータ、および、所定の圧縮符号化方式によって符号化された画像データがそれぞれ所定数のサンプルから成るチャンクを単位として格納される。なお、データは、必ずしも圧縮符号化する必要はなく、リニアデータを格納することもできる。そして、例えば、テキスト・データやＭＩＤＩなどを扱う場合には、ムービー・データ・アトム１０２にテキストやＭＩＤＩなどの実データが含くまれ、これに対応して、ムービーアトム１０１にテキストトラックやＭＩＤＩトラックなどが含まれる。

【００５５】

ムービーアトム１０１における各トラックアトム１１４と、ムービー・データ・アトム１０２に格納されているデータ（データストリーム）とは、唯一つに対応付けられている。このような特徴的な構造をもつことによって、データ実体そのものに手を加えずに再生同期のスケジューリングや編集(非破壊編集)、トラックの追加や削除が容易に実現することができる。

【００５６】

このような階層構造において、ＱＴは、ムービー・データ・アトム１０２内のデータを再生する場合に、ムービーアトム１０１から順次に階層を辿り、サンプル・テーブル・アトム１６４内の各アトム１７２～１７８を基に、サンプル・テーブルをメモリに展開して、各データにおけるデータの解釈方法・属性など、および、各データ間の関係（データの位置やデータのサイズなど）を識別する。そして、ＱＴは、各データ間の関係を基にデータを再生する。

【００５７】

本実施形態は、ＱＴの優れた特徴を生かしつつ、権利保護すべきデータを扱う際に必要となる機能やフォーマット上の構造を拡張することによって、データに成立する無体財産権を保護する。以下、無体財産権のうち、著作権について説明するが、他の無体財産権についても同様に扱うことができる。ＱＴ上の最少アクセス単位と言えるサンプルに、暗号化された実データの復号化可能な最少単位(データブロック)を対応させることにより、ＱＴの持つタイムベースでの管理能力を使って再生同期や編集などが行え、そして、鍵マネジメントとの組み合わせにおいては同一コンテンツ内においてもより細かく権利の付加や権利の利用条件の設定など、新たなコンテンツの運用を行うことができる。

【００５８】

より具体的には、本発明は、ＱＴで権利保護されたマルチメディアコンテンツを扱う際に、暗号化されたデータを解くための鍵情報とコンテンツの使用条件などの権利保護のための情報を、それぞれのデータストリームに対応した形で確保するために、各トラックアトム内のサンプルディスクリプションテーブルに権利保護データを格納する拡張フォーマットを備えて構成される。

【００５９】

図４は、本実施形態のQuickTimeムービーファイルの構成を示す図である。

【００６０】

図５は、本実施形態のサンプル・ディスクリプション・テーブルの構成を示す図である。

【００６１】

図４に示すように、権利保護情報ブロック（Security Information Block）１９１は、標準ＱＴのフィールドに続いて拡張されるフィールドであり、各トラックのサンプル・ディスクリプション・テーブル内に設けられる。そして、権利保護情報ブロック１９１は、図５に示すように、権利管理データ（Rights Management Data、以下、「ＲＭＤ」と略記する。)ユニット単独で、あるいはＲＭＤユニットとその他のユニット（other unit）との複数ユニットから構成される。なお、各ユニットの格納順は、任意である。

【００６２】

ユニット・サイズ（unit size）・フィールドは、それぞれのユニットに含まれ、そのユニットのバイト数を示す。ユニット・タイプ（unit type）・フィールドは、そのユニットのタイプを指定するタグであり、ここでは、例えば、ＲＭＤユニット場合 rigt と定義する。

【００６３】
バージョン（version）・フィールドは、それぞれのユニットのバージョンを表す値である。フラグ（Flag）・フィールドは、このユニットに付属するフラグ用として予約されている。
【００６４】
フラグ・フィールドに続いて、そのユニットのデータ実体（unit data）が格納される。ＲＭＤユニットでは、権利保護や暗号化鍵に関する情報をまとめたＲＭＤのデータ実体となる。
【００６５】
なお、この拡張に応じて、標準ＱＴのフィールド部分でこのテーブル内のデータタイプを指定しているデータ・フォーマット・フィールドが値として採るタグも、導入する権利保護システム、ファイルフォーマットなどに応じて新しく定義する必要があれば拡張して定義することができる。
【００６６】
標準ＱＴとは、本発明にかかる権利保護のために拡張したフィールドをサンプル・ディスクリプション・テーブルに備えないＱＴである。
【００６７】
図６は、権利管理データの構成を示す図である。
【００６８】
図６において、ＲＭＤユニットは、コンテンツの暗号化鍵（content key、以下、「ＣＫ」と略記する。）、Ｃ＿ＭＡＣ、ＲＭＦ、ＰＰＮ、プレイバック・カウンタ（playback counter）、使用開始日時（start time/date）、使用終了日時（end time/date）、ＣＣＦ、ＰＣＮ、複製カウンタ（copy counter）、予約領域（reserved）など、各種使用条件などの著作権保護のための情報がまとめて格納される。
【００６９】
ＣＫ・フィールドは、このトラックが対応するデータストリーム(詳細には、さらにトラックを細分化した各データブロック)を暗号化する際に使用されたコンテンツの暗号化鍵である。
【００７０】
Ｃ＿ＭＡＣ・フィールドは、ＲＭＤを対象とした改ざん防止コードが格納される。これは、例えばISO/IEC9797のＭＡＣ(message authentication code)演算手法によって、ＲＭＤの全フィールドの値を入力として得られた、一意に生成され非可逆の性質をもつ演算値である。
【００７１】
ＲＭＦ(rights management flag)・フィールドは、制限事項の有無と種類を示すフラグである。
【００７２】
ＰＰＮ(number of permitted playback)・フィールドは、再生可能回数の最大値である。
【００７３】
プレイバック・カウンタ・フィールドは、再生毎にデクリメントされる再生回数のカウンター値であり、初期値はＰＰＮ・フィールドと同値である。
【００７４】
使用開始日時・フィールドは、ＲＭＦ・フィールドによって再生期限による制限事項が設定されている場合にその開始日時を表す。
【００７５】
使用終了日時・フィールドは、ＲＭＦ・フィールドによって再生期限による制限事項が設定されている場合にその終了日時を表す。
【００７６】
ＣＣＦ(copy control flag)・フィールドは、複製制御用フラグであり、コピーが可能であるか／不可能であるかの別や、コピー可能な世代であるか、オリジナルであるか／複製

であるかなどの当該データの属性を指定する。
【００７７】
ＰＣＮ・フィールドは、例えば、ＬＣＭ(Licensed Compliant Module)などとメディア間で許される、コンテンツの移動／複製可能回数の最大値を表す。
【００７８】
複製カウンタ・フィールドは、コンテンツ移動／コピーごとにデクリメントされるカウンター値であり、初期値はＰＣＮ・フィールドと同値である。
【００７９】
これらＲＭＦ、ＰＰＮ、プレイバック・カウンタ、使用開始日時、使用終了日時、ＣＣＦ、ＰＣＮおよび複製カウンタは、そのコンテンツの利用条件を指定する。
【００８０】
次に、図７および図８に基づいて、ムービー・データ・アトムの構成および実データとメディア・アトムとの対応付けについて説明する。
【００８１】
図７は、ムービー・データ・アトムの構成を示す図である。
【００８２】
図８は、実データとメディア・アトムとの対応を示す図である。
【００８３】
図７において、ムービーデータは、アトム・サイズ（atom size）、タイプ（type)およびデータから構成されるアトムである。図７に示す、サイズとタイプに続くデータ部分が、コンテンツの実データ(データストリーム)である。
【００８４】
図７の権利保護データ（Secured Content Data）は、例えば、米国標準暗号方式であるＤＥＳ(Data Encryption Standard)のブロック暗号化アルゴリズムによって暗号化される。ブロック暗号化は、一般的にデータをある程度の塊(ブロック)ごとに暗号化するとともに、ある程度の時間ごとに暗号化鍵を変更する。同一鍵で暗号化された暗号化データを一塊とし、復号化するために必要な情報をヘッダ情報として付加してブロック化したものを、暗号化データブロック（Encrypted Data Block）と呼称することにする。すなわち、暗号化データブロックは、鍵があればそれ単独で復号化できる、復号化最少単位である。暗号化されたデータストリーム（Encrypted Data Block #1 ～ Encrypted Data Block #n）は、この暗号化データブロックが連続したものである。
【００８５】
以下、特に断りがない場合はブロックとは暗号化データブロックを指すものとする。暗号化データブロックは、ＢＫＬ ＩＤ、ＣＯＮＮＵＭ、ＢＬＫ Ｓｅｒｉａｌ Ｎｏ.、Ｂｌｏｃｋ ＳｅｅｄおよびＥｎｃｒｉｐｔｅｄ Ｄａｔａとを備えて構成される。
【００８６】
ＢＬＫ ＩＤ・フィールドは、ブロックの先頭を識別するコードを表す。
【００８７】
ＣＯＮＮＵＭ・フィールドは、コンテンツをユニークにする識別子ＩＤであり、あるコンテンツにおいて一定の値である。コンテンツが編集された場合でも、ＣＯＮＮＵＭ・フィールドの値は、変化させず、各ブロックがどのコンテンツを構成していたものであるかを特定する情報となる。
【００８８】
ＢＬＫ Ｓｅｒｉａｌ Ｎｏ.・フィールドは、あるコンテンツの先頭ブロックを０とし、続くブロックに連続して昇順につけられていくブロック番号である。
【００８９】
Ｂｌｏｃｋ Ｓｅｅｄ・フィールドは、該当ブロックを暗号化するための一種の鍵であり、ブロックごとに異なる。一般的に、コンテンツの暗号化鍵をコンテンツに対して唯一つにするため、実際にデータを暗号化する鍵は、コンテンツの暗号化鍵とこのＢｌｏｃｋ Ｓｅｅｄを組み合わせたものである。これによって、コンテンツの暗号化鍵が唯一つだと

しても、同一コンテンツ内で所定の時間ごとに暗号化鍵が変化していく。組み合わせ方や暗号化鍵を変化させる時間間隔などは、暗号化アルゴリズムやシステムに依存する。

【００９０】

続くＥｎｃｒｉｐｔｅｄ　Ｄａｔａは、暗号化されたデータの実体が格納される。1つのブロックは、例えば、動画であれば1フレーム、音声であれば1～数サウンドフレームなどのデータストリーム上の単位に相当させる。

【００９１】

図８において、ＱＴ上での最少アクセス単位であるサンプルを、一つの暗号化データブロックと対応させる。これによって、例えば、暗号化データブロックを動画の1フレームに相当させた場合に、ＱＴは、1フレーム単位でアクセス／再生したり、他のトラックと1フレーム精度で同期をとることができる。また、これによって、1フレーム精度での分割や結合、入れ替えなどの編集性も確保される。先に説明したサンプル・ディスクリプション・テーブルの構成から、1つのサンプル、もしくは複数のサンプルごとに使用条件やコンテンツの暗号化鍵などの著作権情報を設定することも可能となる。

【００９２】

データの保護は、データの暗号化、データの改ざん防止および暗号化鍵の管理の３段階で行われ、より多くの段階を用いることで保護が強化される。上述の実施形態は、データの暗号化にＤＥＳを適用し、改ざん防止にＣ＿ＭＡＣを適用している。そこで、データ保護の強化を図るため、上述の実施形態に更に暗号化鍵の管理を用いると好適である。以下、暗号化鍵の管理手法も用いる実施形態について説明する。

【００９３】

図９は、暗号化鍵の管理を用いた場合におけるサンプル・ディスクリプション・テーブルの構成を示す図である。

【００９４】

図９において、サンプル・ディスクリプション・テーブルは、標準ＱＴのフィールドに続いて拡張される権利保護情報ブロックとして、Enable Key Block(以下、「ＥＫＢ」と略記する。)・ユニットと、ＲＭＤ・ユニットとを拡張する。ＥＫＢ・ユニットには、ＥＫＢと呼ばれるコンテンツの暗号化鍵を導くために必要な鍵や鍵束、および付随する属性情報などが格納される。

【００９５】

ＥＫＢ・ユニットにおけるユニット・サイズ（unit size）・フィールドは、ＥＫＢ・ユニット全体のバイト数を示す。ユニット・タイプ（unit type）・フィールドは、ユニットのタイプを指定するタグで、ここでは、例えば ekbl と定義される。ＥＫＢ・ユニットにおけるバージョン（version）・フィールドは、それぞれのユニットのバージョンを表す値である。ＥＫＢ・ユニットにおけるフラグ（flag）・フィールドは、ユニットのデータ本体(ＥＫＢ)の有無と、参照方法を指定する。

【００９６】

ＥＫＢ・ユニットにおけるＥＫＢ・フィールドは、フラグの状態値によって、ＥＫＢデータの実体か、もしくはファイルＩＤやファイル名、ＵＲＬなどのリンク情報、またはデータ無し(ＥＫＢ・フィールドが存在しない)の各状態を取り得る。ＥＫＢは、データストリームと基本的に一対で、一つのコンテンツを形成する。ここで、ＥＫＢの実体は、必ずしもムービー・アトム（リソース）の中に保持する必要はなく、例えば、同一記録媒体上に独立したファイルとして保持し、ＥＫＢファイルへのリンク情報によって必要なときに参照するようにしてもよい。また、複数コンテンツが同じＥＫＢを使用すると場合のようにＥＫＢが重複している場合などは、積極的にこのような独立したファイルとすることで記録媒体の容量に関して利用効率を向上することができる。さらに、コンテンツ提供者の意図によっては、コンテンツの配信時にはＥＫＢと一対ではない状態でデータストリームのみを配信することもできる。このようにデータストリームのみを配信する場合に、例えば、ＥＫＢの取得先をインターネット上のＵＲＬによって指定することによって、後日に必要に応じてＥＫＢを取得するようなサービス形態を提供することもできる。

【００９７】
図１０は、ＥＫＢ・ユニットにおけるフラグの定義を示す図である。
【００９８】
図１０において、フラグ値０Ｘ００は、ＥＫＢデータが存在せず有効でないことを示す。フラグ値０Ｘ０１は、ＥＫＢデータが存在しＥＫＢユニット内に格納されていることを示す。フラグ値０Ｘ０２は、ＥＫＢデータがＥＫＢ・ユニット内に存在しないが、同一記録媒体上などに独立ファイルとして存在し、ファイルＩＤおよびファイル名などの参照先情報によって参照可能であることを示す。フラグ値０Ｘ０３は、ＥＫＢデータがＥＫＢ・ユニット内に存在しないが、インターネット上の取得先を指定するＵＲＬ情報によって、ＥＫＢを取得することが可能であることを示す。その他のフラグ値は予約されている。
【００９９】
また、ＥＫＢを外部参照する場合には、図11に示すように、ＥＫＢは、独立したファイルとして構成させ、ＥＫＢの実体とともにいくつのムービーからリンクされているかを示すリンク・カウンタ（Link Counter）や、バージョン、サイズなどの情報を付加させることで各コンテンツ(トラック)とＥＫＢとの相関関係を管理する。
【０１００】
また、この拡張に応じて、図９における標準ＱＴのフィールド部分でこのテーブル内のデータタイプを指定しているデータ・フォーマット（Data Format）・フィールドが値としてとるタグも、拡張の必要があれば、新たに拡張定義する。
【０１０１】
図１２は、ＥＫＢのデータ構造を示す図である。
【０１０２】
図１２は、上述のフラグ・フィールドにおいて、ＥＫＢが存在し実体がユニット内に格納されていると指定した場合に格納されるＥＫＢの実体の例である。
【０１０３】
図１２において、バージョン（version）・フィールドは、このＥＫＢのバージョンを表す値である。暗号化アルゴリズム（encryption algorithm）・フィールドは、ＥＫＢを構成する各々の暗号化鍵情報の暗号化に使用された暗号化アルゴリズムを指定する。Ａをｎという鍵で暗号化した結果のデータをＥｎ（Ａ）と表記する場合、Ｅｋｒｏｏｔ（ＫＥＫ）は、Ｋｒｏｏｔという鍵を使って暗号化された鍵暗号化鍵(ＫＥＫ＝Key Encryption Key)である。ＫＥＫは、データストリームの復号化に必要なコンテンツの暗号化鍵(KC)を導きだすのに必要な鍵である。つまり、本来、ＣＫ＝EKEK（コンテンツの暗号化鍵（ＫＣ））である。
【０１０４】
シグニチャ・パート（signature part）は、このＥＫＢに対する電子署名である。続くフィールドは、最も下位階層の鍵から順に、すぐ上位の鍵を下位の鍵によって暗号化した鍵情報が連続する。最も下位階層の鍵とは、リーフ鍵(例えば、Ｋｌｅａｆ などと表される)と呼ばれる、メディアや機器がユニークに保持する鍵であり、正規なメディアや機器であればＥＫＢを用いてＫＥＫが導き出せることになる。
【０１０５】
このようなファイルを対応アプリケーションＱＴによって再生する場合について以下に説明する。
【０１０６】
ムービーを表示しようとする際に、システム制御マイコン１９は、ファイル復号器１６を介して、特定の時間に対応するメディアデータにアクセスする。システム制御マイコン１９は、サンプル・テーブル・アトムの情報によって、要求されたサンプルに対応するデータストリームの位置を特定する。システム制御マイコン１９は、同様に、そのサンプルを解釈するためのサンプル・ディスクリプション・テーブルを参照し、拡張されたＥＫＢ・ユニットのフラグ・フィールドによってＥＫＢデータの属性を判断する。ＥＫＢデータが存在し実体が格納されている場合には、システム制御マイコン１９は、続くＥＫＢフィー

ルドをＥＫＢデータとして参照する。ＥＫＢデータが独立ファイルとして存在する場合は、システム制御マイコン１９は、ＥＫＢフィールドに示されたリンク情報により、該当するＥＫＢファイルを特定する。ＥＫＢフィールドがＵＲＬであった場合には、システム制御マイコン１９は、ＵＲＬで指定されたＨＰを参照し、そこから必要なＥＫＢデータをダウンロードする。一方、ＥＫＢが存在しないなど、このコンテンツに対して使用権利が与えられていない場合は、システム制御マイコン１９は、再生不可である旨や、ＥＫＢの取得を促すメッセージなど、必要に応じた処理をする。これによって得られたＥＫＢと、そのアプリケーションがユニークに持つリーフ鍵から、システム制御マイコン１９は、コンテンツの暗号化鍵を導くためのＫＥＫを得ることができる。そして、システム制御マイコン１９は、ＫＥＫとＲＭＤから復号化するためのコンテンツの暗号化鍵を導き、さらに各種使用条件などの情報を判断する。システム制御マイコン１９は、使用条件に応じた処理を行い、導かれたコンテンツの暗号化鍵と暗号化データブロック内のBlock Seedからこのブロックをファイル復号器１６を介して復号化する。復号化されたデータストリームは、対応するコーデックを用いて伸張され、ビデオ復号器表示される。

【０１０７】

次に、権利保護方法と提供されるサービスとの関係について説明する。

【０１０８】

図１３は、権利保護方法と提供されるサービスとの第１の関係を説明する図である。

【０１０９】

図１３において、複数トラックが用意され、各トラックにコンテンツの内容は、同一であるが品質（解像度、音質など）の異なるデータを収容し、それぞれのサンプル・ディスクリプション・テーブルに異なった著作権情報を付加する。そして、額の異なる利用料金を設定し、支払われた利用料金額に応じた著作権保護情報およびコンテンツの暗号化鍵をユーザに提供するようにする。このようにすることで、利用料金に応じた品質のコンテンツを提供するようにすることができる。

【０１１０】

例えば、トラック１は、第１の解像度のコンテンツを収容し、これに対応する著作権情報Ａおよびコンテンツの暗号化鍵Ａをサンプル・ディスクリプション・テーブルに収容する。そして、トラック２は、第１の解像度よりも高解像度でコンテンツを収容し、これに対応する著作権情報Ｂおよびコンテンツの暗号化鍵Ｂをサンプル・ディスクリプション・テーブルに収容する。このような場合に、初期料金が支払われた場合には、著作権情報ＡのＥＫＢおよびコンテンツの暗号化鍵Ａのうちユーザに提供していない一方または両方をユーザに提供してトラック１を再生することができるようにする。さらに、ユーザが初期料金に上乗せして支払う特別料金を支払った場合には、著作権情報ＢのＥＫＢおよびコンテンツの暗号化鍵Ｂのうちユーザに提供していない一方または両方をユーザに提供してトラック２を再生することができるようにする。

【０１１１】

あるいは、異なる額の利用料金を設定して購入時の金額に応じて、ユーザに、著作権情報ＡのＥＫＢおよびコンテンツの暗号化鍵Ａのうちユーザに提供していない一方または両方、あるいは、著作権情報ＢのＥＫＢおよびコンテンツの暗号化鍵Ｂのうちユーザに提供していない一方または両方を提供するようにする。これによって利用料金の額に応じた解像度のコンテンツを提供するようにすることができる。このように利用料金に応じてスケーラビリティを持つコンテンツを提供することができる。

【０１１２】

また、同様に、それぞれのトラックを異なるデータ、例えば、映像データおよび音楽データとすることで、例えば、音楽配信サービスにおいて購入した楽曲に対して特別料金を払うことでビデオクリップコンテンツになったり、カラオケコンテンツになったりなど、多様なサービスに対応できる。

【０１１３】

図１４は、権利保護方法と提供されるサービスとの第２の関係を説明する図である。

【０１１４】
図１４において、一個のトラックは、暗号化されたブロックと暗号化されないブロックとで構成される。暗号化されたブロックに対応するサンプル・ディスクリプション・テーブルには、その著作権情報を格納する。
【０１１５】
このような形態によって、例えば、音楽配信サービスにおいて、次のようなサービスを実現することができる。すなわち、ある楽曲の中でサビの一部分などコンテンツ提供者側が意図した部分のみを暗号化しないブロックとして構成することで、ユーザーは、無料でその楽曲の一部を試聴することができ、購入を希望する場合にはコンテンツ鍵を別途購入(そのコンテンツ鍵を導けるＥＫＢデータを購入)する。この購入によって、ユーザは、その時点で楽曲全てを楽しむことができるようになる。
【０１１６】
図１５は、権利保護方法と提供されるサービスとの第３の関係を説明する図である。
【０１１７】
図１５において、一個のトラックは、いくつかのブロックに分けられ、それぞれ異なるコンテンツの暗号化鍵で暗号化される。それぞれのブロックに対応するサンプル・ディスクリプション・テーブルには、それぞれの著作権情報を格納する。
【０１１８】
このような形態によって、例えば、動画配信サービスにおいて、次のようなサービスを実現することができる。すなわち、連続的なコンテンツを著作権者の意向に合わせて細かく切り売りすることができる。また、鍵は同じであっても再生期限などの使用条件を変えることで、連続ドラマのようなコンテンツを意図したタイミングで次々に公開(再生許可)することもできる。
【０１１９】
そして、これらの組み合わせによって、一つのコンテンツの中でより複雑な使用条件などを設定することができるので、より細かな、新しいコンテンツサービスを展開することができる。
【０１２０】
ここで、従来は、コンテンツとコンテンツを利用するための鍵とを一体に扱っていたので、ユーザには、ユーザの希望するコンテンツのみしか提供することができなかった。
【０１２１】
本発明を利用すれば、コンテンツとコンテンツを利用するために必要な著作権情報のＥＫＢおよびコンテンツの暗号化鍵とを別個に管理することができる。このため、ユーザに頒布する際には、複数のコンテンツを記録した記録媒体を予め頒布したり、複数のコンテンツを通信回線を通じて予め拡布することができる。すなわち、ユーザが初期に希望しないコンテンツも提供することができる。
【０１２２】
これによって、ユーザが初期に希望したコンテンツにさらに別のコンテンツを希望する場合には、ユーザが希望するコンテンツにおける著作権情報のＥＫＢおよびコンテンツの暗号化鍵のうちのユーザに提供していない一方または両方をユーザに提供するだけで、ユーザは、希望するコンテンツを利用することができる。
【０１２３】
したがって、著作権情報のＥＫＢやコンテンツの暗号化鍵と言った最小のデータのみをユーザに提供すればよい。このような最小のデータを通信回線を通じて提供する場合には、コンテンツとともに提供する従来の場合に較べ格段に短い通信時間で提供することができ、ユーザのダウンロードに伴うストレスや通信料金の高額化を避けることができる。
【０１２４】
なお、本発明に係るファイルを記録した記録媒体は、ＱＴを搭載したコンピュータによって読み取り可能である。また、コンテンツを復号するための暗号化鍵が記録媒体に記録されない場合であって、コンピュータにモデムなどの通信用インターフェースが搭載され通

信回線に接続可能である場合には、暗号化鍵は、通信回線を介して取得することが可能である。これによって、実データと実データを使用する権利とを別個に販売することが可能である。

【０１２５】

【発明の効果】

本発明によれば、特殊なハードウェアを用いずに動画等を同期して再生するためのコンピュータソフトウェアにより取り扱うことができるファイル構造を持つようにデータ構造が変換された実データに成立する無体財産権を確実に保護することができる。

【０１２６】

そして、本発明によれば、権利保護の単位を第１データ単位ごとに合わせたので、データ提供者が意図した単位で、ユーザにアクセス、再生、同期および編集などを行わせることができる。

【図面の簡単な説明】

【図１】ディジタル記録再生装置の一構成例を示すブロック図である。

【図２】　QuickTimeムービーファイルの一構成例を示す図である。

【図３】ビデオメディア情報アトムの一構成例を示す図である。

【図４】本実施形態のQuickTimeムービーファイルの構成を示す図である。

【図５】本実施形態のサンプル・ディスクリプション・テーブルの構成を示す図である。

【図６】権利管理データの構成を示す図である。

【図７】ムービー・データ・アトムの構成を示す図である。

【図８】実データとメディア・アトムとの対応を示す図である。

【図９】暗号化鍵の管理を用いた場合におけるサンプル・ディスクリプション・テーブルの構成を示す図である。

【図１０】ＥＫＢ・ユニットにおけるフラグの定義を示す図である。

【図１１】権利保護情報ブロックを独立ファイルとした場合を説明する図である。

【図１２】ＥＫＢのデータ構造を示す図である

【図１３】権利保護方法と提供されるサービスとの第１の関係を説明する図である。

【図１４】権利保護方法と提供されるサービスとの第２の関係を説明する図である。

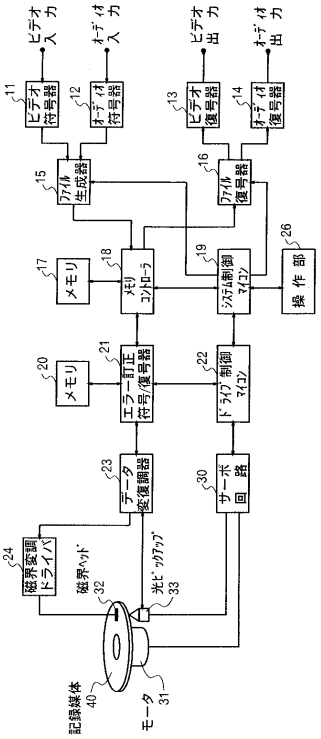
【図１５】権利保護方法と提供されるサービスとの第３の関係を説明する図である。

【符号の説明】

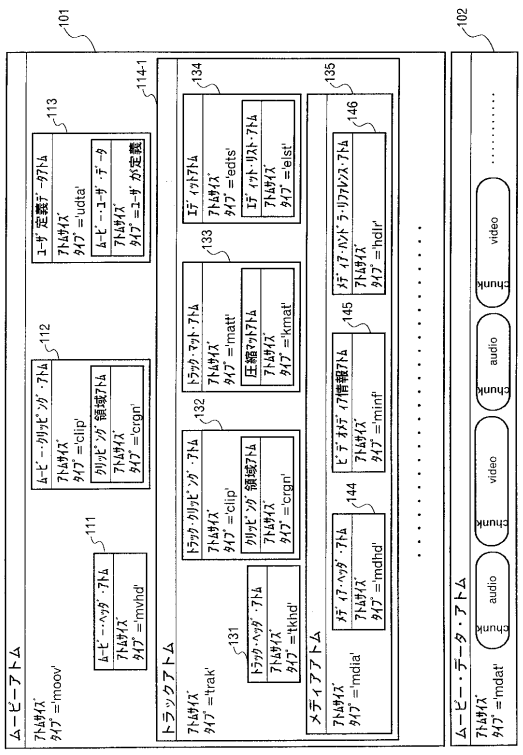
１１　ビデオ符号器
１２　オーディオ符号器
１３　ビデオ復号器
１４　オーディオ復号器
１５　ファイル生成器
１６　ファイル復号器
１７、２０　メモリ
１８　メモリコントローラ
１９　システム制御マイコン
２１　エラー訂正符号／復号器
２３　データ変復調器
２４　磁界変調ドライバ
２６　操作部
３０　サーボ回路
３１　モータ
３２　磁界ヘッド
３３　光ピックアップ
４０　記録媒体
１０３　ＥＫＢ・ファイル
１０４　リンク・カウンタ

１０５　ＥＫＢ・データ
１７５　サンプル・ディスクリプション・アトム
１８１、１８２　サンプル・ディスクリプション・テーブル
１９１　権利保護情報ブロック

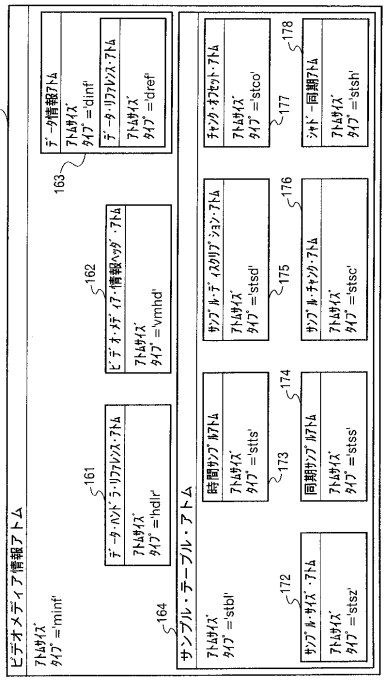
【図１】



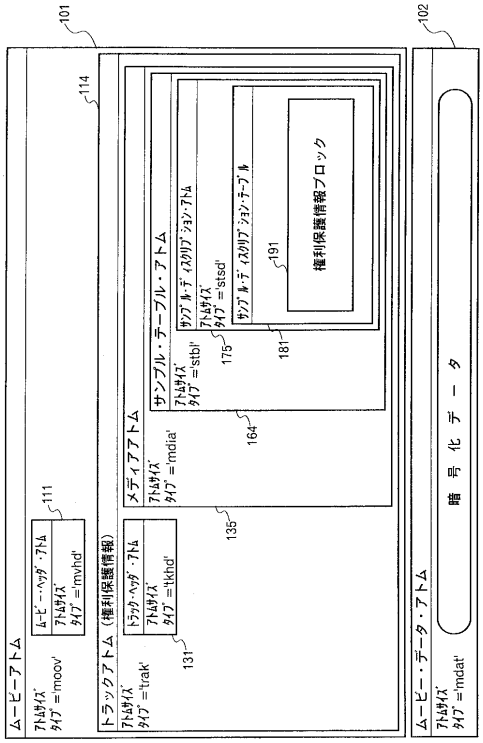

【図２】



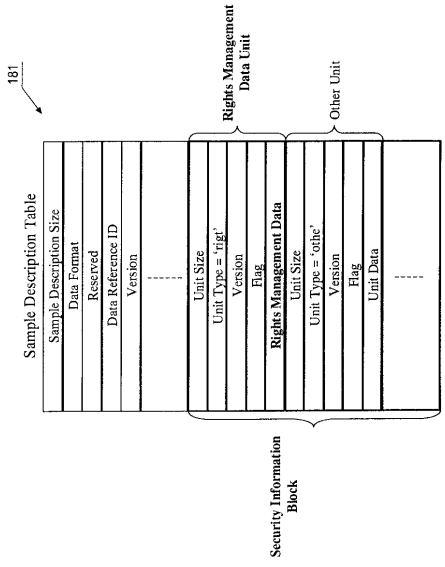
【図３】


145
ビデオメディア情報アトム
アトムサイズ
タイプ ='minf'
163
データ情報アトム
アトムサイズ
タイプ ='dinf'
161
データ・ハンドラ・リファレンス・アトム
アトムサイズ
タイプ ='hdlr'
162
ビデオ・メディア情報ヘッダ・アトム
アトムサイズ
タイプ ='vmhd'
データ・リファレンス・アトム
アトムサイズ
タイプ ='dref'
164
サンプル・テーブル・アトム
アトムサイズ
タイプ ='stbl'
時間サンプ ルアトム
アトムサイズ
タイプ ='stts'
173
サンプル・デ ィスクリプ ション・アトム
アトムサイズ
タイプ ='stsd'
175
チャンク・オフセット・アトム
アトムサイズ
タイプ ='stco'
177
176
174
172
サンプル・サイズ・アトム
アトムサイズ
タイプ ='stsz'
同期サンプ ルアトム
アトムサイズ
タイプ ='stss'
サンプル・チャンク・アトム
アトムサイズ
タイプ ='stsc'
シャド ー同期アトム
アトムサイズ
タイプ ='stsh'
178

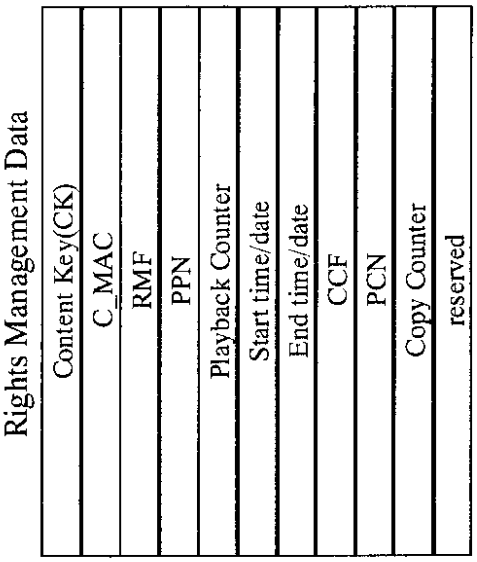
【図４】


101
ムービーアトム
アトムサイズ
タイプ ='moov'
ムービ ーヘッダ ・アトム
アトムサイズ
タイプ ='mvhd'
111
114
トラックアトム（権利保護情報）
アトムサイズ
タイプ ='trak'
トラック ヘッダ ・アトム
アトムサイズ
タイプ ='tkhd'
131
135
メディアアトム
アトムサイズ
タイプ ='mdia'
サンプル・テーブル・アトム
アトムサイズ
タイプ ='stbl'
175
サンプル・デ ィスクリプ ション・アトム
アトムサイズ
タイプ ='stsd'
191
サンプル・デ ィスクリプ ション・テーブル
181
権利保護情報ブロック
164
102
ムービー・データ・アトム
アトムサイズ
タイプ ='mdat'
暗 号 化 デ ー タ

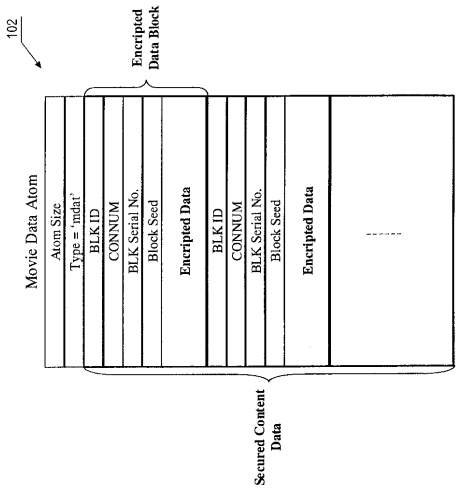
【図５】


181
Sample Description Table
Sample Description Size
Data Format
Reserved
Data Reference ID
Version
Unit Size
Unit Type = 'rigt'
Version
Flag
Rights Management Data
Unit Size
Unit Type = 'othe'
Version
Flag
Unit Data
Rights Management Data Unit
Other Unit
Security Information Block

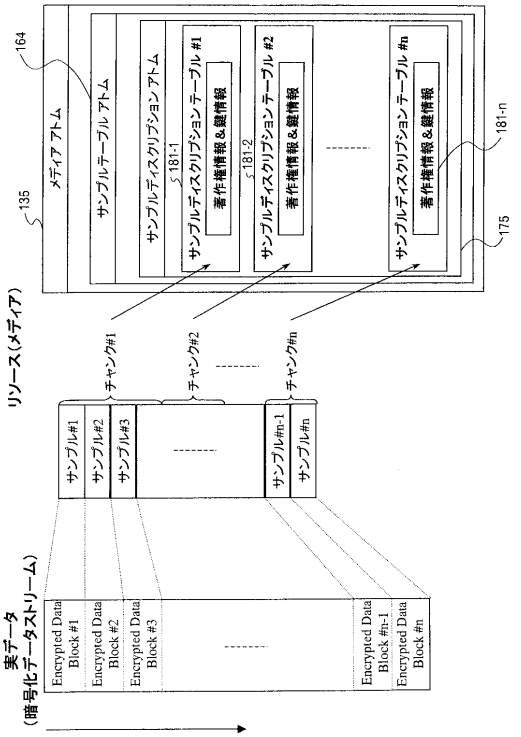
【図６】


Rights Management Data
Content Key(CK)
C_MAC
RMF
PPN
Playback Counter
Start time/date
End time/date
CCF
PCN
Copy Counter
reserved

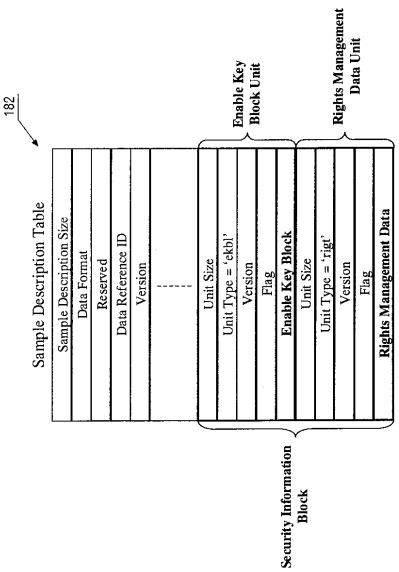
【図７】




【図８】



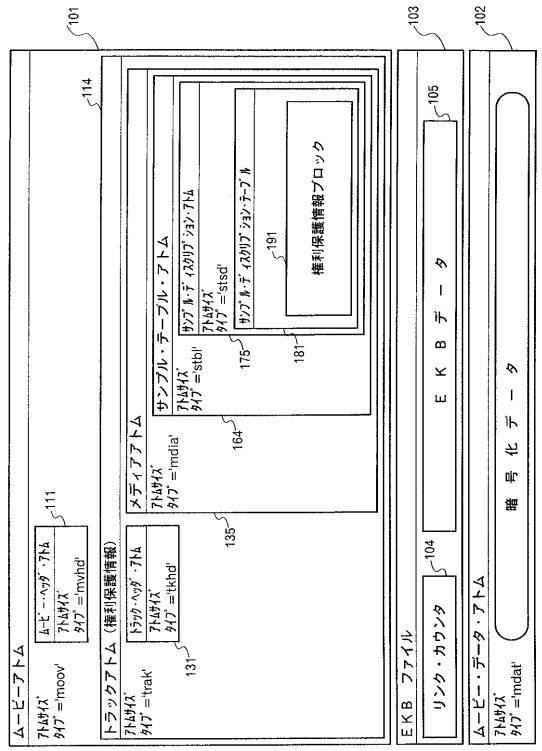

【図９】



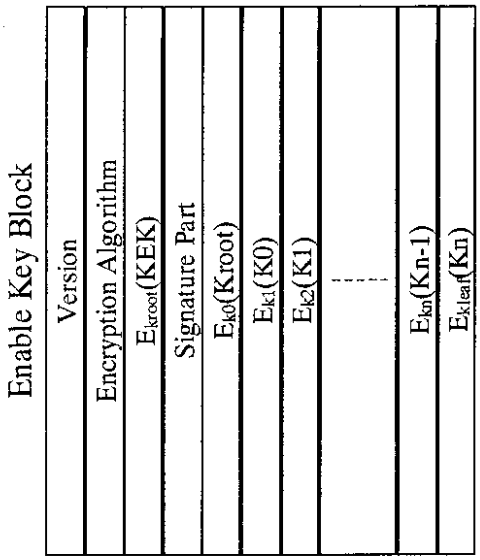

【図１０】

| Flag | Attribute | | EKB field |
|---|---|---|---|
| 0x00 | not-exist | non-valid | No data |
| 0x01 | exist | valid | EKB data |
| 0x02 | not-exist | valid as independent file | Link information (File ID, File name and etc.) |
| 0x03 | not-exist | valid on Internet | Link information (URL and etc.) |
| others | reserved | | |

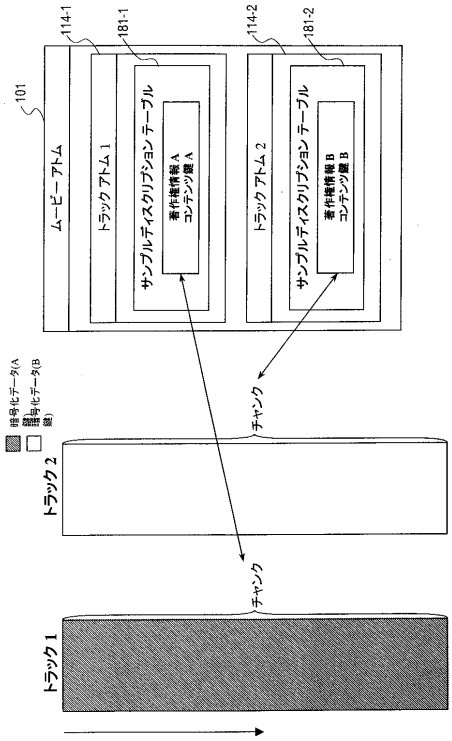
【図１１】



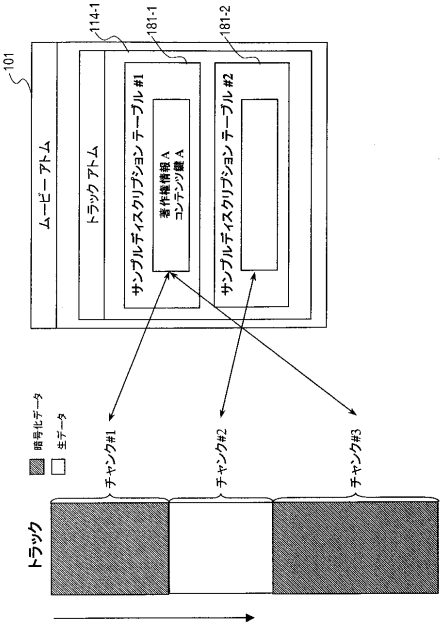

【図１２】



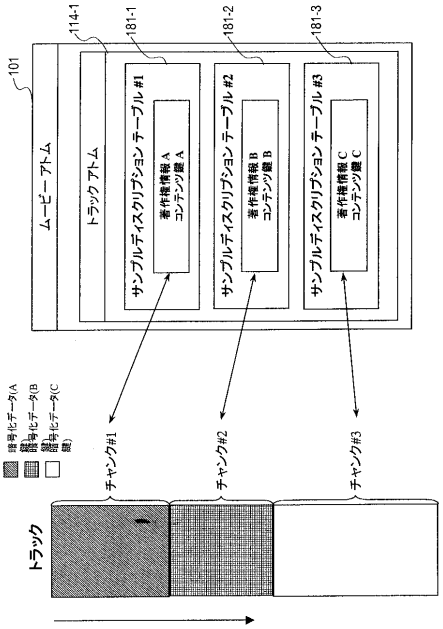

【図１３】




【図１４】



【図１５】


101
ムービーアトム
トラックアトム
サンプルディスクリプションテーブル #1
著作権情報 A
コンテンツ鍵 A
サンプルディスクリプションテーブル #2
著作権情報 B
コンテンツ鍵 B
サンプルディスクリプションテーブル #3
著作権情報 C
コンテンツ鍵 C
114-1
181-1
181-2
181-3
暗号化データ(A鍵)
暗号化データ(B鍵)
暗号化データ(C鍵)
チャンク#1
チャンク#2
チャンク#3
トラック

フロントページの続き

| (51)Int.Cl. | | | FI | | |
|---|---|---|---|---|---|
| ***H04N*** | ***5/91*** | ***(2006.01)*** | G11B | 20/12 | 103 |
| ***H04N*** | ***5/92*** | ***(2006.01)*** | G11B | 27/00 | D |
| | | | H04N | 5/91 | P |
| | | | H04N | 5/92 | H |

合議体
審判長　山田　洋一
審判官　小松　正
審判官　早川　卓哉

(56)参考文献　特開平９－４６６３０（ＪＰ，Ａ）
特開平１０－４０６４９（ＪＰ，Ａ）
特開平１０－２４１２８８（ＪＰ，Ａ）
特開２０００－３３９２０７（ＪＰ，Ａ）
特開２００１－７６４２５（ＪＰ，Ａ）
特開２００１－７６４６４（ＪＰ，Ａ）
特開２００１－９４５４９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G11B20/10,27/00,G06F12/00,12/14,H04N5/91,G10C1/00,H04L9/00