(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3689624号
(P3689624)
(45)発行日　平成17年8月31日(2005.8.31)　(24)登録日　平成17年6月17日(2005.6.17)

(51)Int.Cl.[7]　F I
G11B 20/10　G11B 20/10　H
H04L 9/08　H04L 9/00　601A

請求項の数 3　(全 22 頁)

(21)出願番号　特願2000-274803(P2000-274803)
(22)出願日　平成12年9月11日(2000.9.11)
(65)公開番号　特開2001-167518(P2001-167518A)
(43)公開日　平成13年6月22日(2001.6.22)
審査請求日　平成14年3月4日(2002.3.4)
(31)優先権主張番号　特願平11-280075
(32)優先日　平成11年9月30日(1999.9.30)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100062144
弁理士　青山　葆
(74)代理人　100086405
弁理士　河宮　治
(74)代理人　100098280
弁理士　石野　正弘
(72)発明者　弓場　隆司
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　石原　秀志
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
最終頁に続く

(54)【発明の名称】情報記録媒体、情報記録方法及び情報再生方法

(57)【特許請求の範囲】
【請求項１】
著作権を保護すべきコンテンツ情報と、暗号化鍵情報とが少なくとも記録された情報記録媒体であって、
上記コンテンツ情報の一部はスクランブルされて記録され、
上記スクランブルされて記録されたコンテンツ情報は、上記暗号化鍵情報をスクランブルされていないコンテンツ情報の一部を用いて変換することによって得られるスクランブル鍵情報を用いてスクランブルされ、
上記スクランブルされていないコンテンツ情報の一部は、少なくともコピー制御情報を含むことを特徴とする情報記録媒体。
【請求項２】
暗号化鍵情報を有する情報記録媒体にコンテンツ情報の一部をスクランブルして記録する情報記録方法であって、
上記暗号化鍵情報とスクランブルされないコンテンツ情報の一部とに基づいてスクランブル鍵情報を生成するステップと、
上記スクランブル鍵情報を用いて、コンテンツ情報の一部をスクランブルするステップと、
上記スクランブルされたコンテンツ情報と、スクランブルされていないコンテンツ情報とを情報記録媒体上に記録するステップとを含み、
上記スクランブルされないコンテンツ情報の一部は、少なくともコピー制御情報を含む

ことを特徴とする情報記録方法。
【請求項３】
暗号化鍵情報と、コンテンツ情報の一部がスクランブルされて記録されたコンテンツ情報とを有する情報記録媒体に記録された情報を再生する情報再生方法であって、
所定の鍵情報を用いて、上記情報記録媒体上に記録された暗号化鍵情報を、復号された鍵情報に復号するステップと、
上記復号化された鍵情報と、上記コンテンツ情報のうちスクランブルされていないコンテンツ情報とを用いてデスクランブル鍵情報を生成するステップと、
上記デスクランブル鍵情報を用いて、上記スクランブルされて記録されたコンテンツ情報をデスクランブルするステップとを含み、
上記スクランブルされないコンテンツ情報の一部は、少なくともコピー制御情報を含むことを特徴とする情報再生方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、映像情報や音声情報等を記録する情報記録媒体と、情報記録媒体に記録された情報を再生する情報再生方法と、情報記録媒体に記録された情報を再生する情報再生装置とに関し、特に、著作権を保護すべきコンテンツ情報が記録された情報記録媒体と、情報記録媒体に記録された著作権を保護すべきコンテンツ情報を再生する情報再生方法と、情報記録媒体に記録された著作権を保護すべきコンテンツ情報を再生する情報再生装置とに関する。
【０００２】
【従来の技術】
近年、音声情報の記録媒体として、コンパクトカセットテープやアナログレコードなどのアナログ信号で記録する記録媒体から、ＣＤ（Compact Disc）やＭＤ（Mini Disc）などのディジタル信号で記録する記録媒体が主流になってきている。また、映像信号を記録するための記録媒体として、ＭＰＥＧ１と呼ばれる圧縮方式で圧縮された映像信号をＣＤに記録するビデオＣＤ、さらには４．７ＧＢの大容量を有する光ディスクにＭＰＥＧ２と呼ばれる高品位な圧縮方式による圧縮映像信号を記録するＤＶＤ（Digital Video Disc）などのディジタル記録媒体が開発され、映像情報や音声情報を記録するための記録媒体として商品化されている。
【０００３】
図７は、第１の従来例の光ディスク再生装置４００の内部構成を示すブロック図であり、光ディスク再生装置４００は、光ディスク２０１から読み出した情報データに対して誤り訂正処理や伸長処理を施すことにより、所望の映像信号や音声信号を復号して出力する。
【０００４】
図７において、光ディスク再生装置４００には光ディスク２０１が搭載され、光ディスク再生装置４００は、スピンドルモータ２０２と、光学ヘッド２０３と、ヘッドアンプ２０４と、アナログ処理部２０５と、光ディスクコントローラ２０６と、誤り訂正用メモリ２０７と、オーディオ及びビデオデコーダ（以下、ＡＶデコーダという。）２０９と、オーディオ及びビデオ信号処理用メモリ（以下、ＡＶ信号処理用メモリという。）２１０と、サーボ制御部２１１と、ＣＰＵ２１２と、ＣＰＵバス２１３とを備えて構成される。
【０００５】
スピンドルモータ２０２は、サーボ制御部２１１からの制御信号に基づいて光ディスク２０１を回転させる。光学ヘッド２０３は、光ピックアップであり、レーザダイオードを駆動することにより発生されたレーザ光を光ディスク２０１に照射し、光ディスク２０１からの反射光を受光した後光電変換し、光電変換後の再生信号をヘッドアンプ２０４を介してアナログ処理部２０５に出力する。アナログ処理部２０５は、ＡＧＣと、イコライジングと、データスライスと、ＰＬＬとの機能を有し、入力される再生信号に対して所定のアナログ信号処理を実行した後、処理後の再生信号を光ディスクコントローラ２０６に出力

する。次いで、光ディスクコントローラ２０６は、入力される再生信号を再生ディジタルデータにＡ／Ｄ変換した後、再生データを復調し、誤り訂正用メモリ２０７をバッファメモリとして用いて、復調された再生データに対して誤り訂正処理などを行って、処理後の再生データをＡＶデコーダ２０９に出力する。さらに、ＡＶデコーダ２０９は、入力される再生データに基づいて、映像データ及び音声データに対する伸長処理に用いられる伸張用バッファメモリであるＡＶ信号処理用メモリ２１０を用いて、上記入力される再生データに圧縮されている映像データ及び音声データに対して伸長処理を含む復号処理を施し、処理後の映像信号及び音声信号を出力する。

【０００６】

サーボ制御部２１１は、アナログ処理部２０５、光ディスクコントローラ２０６及びＣＰＵ２１２からの信号に基づいて、スピンドルモータ２０２、光学ヘッド２０３及び光ディスクコントローラ２０６などを制御することにより、光ディスク２０１からのデータの読み出し等において光学ヘッド２０３のフォーカスやトラッキングなどのサーボ制御を行う。サーボ制御部２１１とアナログ処理部２０５と光ディスクコントローラ２０６とＡＶデコーダ２０９は、ＣＰＵバス２１３を介してＣＰＵ２１２に接続され、ＣＰＵ２１２は、ＣＰＵバス２１３を介してアナログ処理部２０５、光ディスクコントローラ２０６、ＡＶデコーダ２０９及びサーボ制御部２１１を制御することにより、光ディスク再生装置４００の全体の動作を制御する。

【０００７】

第１の従来例の光ディスク再生装置の動作について、図７を参照して簡単に説明する。ＣＰＵ２１２は所定のシーケンスに基づいて、光ディスク２０１から光学ヘッド２０３を用いてデータを読み出した後、再生データがヘッドアンプ２０４及びアナログ処理部２０５を介して光ディスクコントローラ２０６に出力され、次いでエラー訂正が施された再生データを誤り訂正用メモリ２０７に格納されるように制御する。このとき、ＣＰＵ２１２は誤り訂正用メモリ２０７に格納された再生データのうち、制御情報やデータの識別情報を読み出し、サーボ制御部２１１及びＡＶデコーダ２０９を制御することにより、映像データ及び音声データの再生を行っている。

【０００８】

一方、パーソナルコンピュータの高性能化やハードディスクの大容量化に伴い、パーソナルコンピュータのアプリケーションプログラムも大容量化が進んでいる。ＤＶＤは、その大容量の特徴を活かし、映像データや音声データを記録するための記録媒体としてだけでなく、パーソナルコンピュータのアプリケーションソフトウェア等の頒布媒体としても活用されており、パーソナルコンピュータの周辺装置としてのＤＶＤドライブ装置の普及が急激に進んでいる。さらに、パーソナルコンピュータ用としてＭＰＥＧの伸長処理機能を備えたＡＶデコーダカードや、パーソナルコンピュータのメインプロセッサのソフトウェア処理により、ＭＰＥＧ伸長処理機能を行うプログラムなども商品化されている。

【０００９】

しかしながら、ＤＶＤドライブ装置とＡＶデコーダカードを用いて、パーソナルコンピュータでＤＶＤの映像データや音声データを再生するシステムでは、これらの装置間は一般的なコンピュータバスの通信路により接続されていることから、当該通信路を介して伝送されるデータの不正コピーや、データを改ざんされて頒布されるなどの行為が行われ、著作権者の権利を保護することが極めて困難となるという問題点があった。

【００１０】

この問題点を解決するために、著作権を有するデータを暗号化して記録することが、例えば特開平７－２４９２６４号の公報（以下、第２の従来例という。）において提案されている。第２の従来例の図３に図示されたＣＤ－ＲＯＭでは、暗号化されたデータセクタとは異なるセクタのメインデータ領域に暗号鍵を記録する方式が提案されている。この第２の従来例では、記録時に暗号化されたデータとその暗号鍵をＣＤ－ＲＯＭに記録する一方、再生時にはパーソナルコンピュータから再生装置に対して暗号鍵の読み出し命令を行った後に暗号化データを読み出して、先に読み出した暗号鍵を用いて上記暗号化データを復

号することにより、データの再生を行う。
【００１１】
【発明が解決しようとする課題】
しかしながら、第２の従来例では、暗号鍵が一般的な読み出し命令（Readコマンド）によって読み出すことができるセクタのメインデータ領域に記録されているため、暗号鍵を一般のパーソナルコンピュータから容易に読み出すことができる。従って、暗号鍵と暗号化データをユーザが読み出すことができるために、暗号の解読を行われる危険性が高いという問題点があるとともに、暗号鍵と暗号化データを例えばハードディスクメモリにコピーされて不正な複製を作成することが可能となるという問題点があった。
【００１２】
また、セクタのメインデータ領域のすべてを暗号化して記録されているために、ＤＶＤプレイヤのように、セクタのメインデータ中に含まれる、コンテンツの識別情報やコンテンツのコピー制御情報等が含まれるコンテンツ制御情報を、ＤＶＤプレイヤの制御のためにＣＰＵにより光ディスクから読み出そうとすると、一度暗号化されたデータを復号してからでないと正しい情報を得ることはできない。
【００１３】
上述した問題点に対して、コンテンツ制御情報が含まれる領域を平文のまま記録してしまうと、コピー制御情報が不正に改ざんされた場合、不正な再生が行われることになる。
【００１４】
本発明の目的は以上の問題点を解決し、デスクランブル処理に用いる鍵情報を容易に読み出されないことを実現するためのデータ構造を有する情報記録媒体を提供することにある。
【００１５】
また、本発明の別の目的は以上の問題点を解決し、ＤＶＤプレイヤなどの情報再生装置において、情報再生装置を制御するＣＰＵが容易にコピー制御情報等を読み出し、情報再生装置の制御を容易に行うことができるとともに、情報記録媒体に記録されたコピー制御情報等が不正に改ざんされた場合にデータの再生を防止することができる情報記録媒体を提供することにある。
【００１６】
さらに、本発明のさらなる目的は以上の問題点を解決し、ＤＶＤプレイヤなどの情報再生装置において、情報再生装置を制御するＣＰＵが容易にコピー制御情報等を読み出し、情報再生装置の制御を容易に行うことができるとともに、情報記録媒体に記録されたコピー制御情報等が不正に改ざんされた場合にデータの再生を防止することができる情報再生方法及び情報再生装置を提供することにある。
【００１７】
【課題を解決するための手段】
本発明に係る情報記録媒体は、著作権を保護すべきコンテンツ情報と、暗号化鍵情報とが少なくとも記録された情報記録媒体であって、
上記コンテンツ情報の一部はスクランブルされて記録され、
上記スクランブルされて記録されたコンテンツ情報の一部は、上記暗号化鍵情報をスクランブルされていないコンテンツ情報の一部を用いて変換することによって得られるスクランブル鍵情報を用いてスクランブルされていることを特徴とする。
【００１８】
また、上記情報記録媒体において、上記スクランブル鍵情報を作成する際に用いられるスクランブルされていないコンテンツ情報の一部は、少なくともコピー制御情報を含むことを特徴とする。
【００１９】
さらに、上記情報記録媒体は複数のセクタに分割された記録領域を有し、上記コンテンツ情報は複数のデータに分割されて上記各セクタに記録され、上記スクランブル鍵情報を作成する際に用いられるスクランブルされていないコンテンツ情報の一部は、コピー制御情

報及びセクタ毎に変化するコンテンツ情報の一部を含むことを特徴とする。

【００２０】

本発明に係る情報再生方法は、暗号化鍵情報とコンテンツ情報とが少なくとも記録され、コンテンツ情報の一部がスクランブルされて記録されている情報記録媒体に記録された情報を再生する情報再生方法であって、

所定の鍵情報を用いて、上記情報記録媒体上に記録された暗号化鍵情報を、復号された鍵情報に復号するステップと、

上記コンテンツ情報のうちスクランブルされていないコンテンツ情報を用いて、上記復号された鍵情報を変換後の復号された鍵情報に変換するステップと、

上記変換後の復号された鍵情報を用いて、上記スクランブルされて記録されたコンテンツ情報をデスクランブルするステップとを含むことを特徴とする。

【００２１】

本発明に係る情報再生装置は、暗号化鍵情報とコンテンツ情報とが少なくとも記録され、上記コンテンツ情報の一部はスクランブルされて記録されている情報記録媒体に記録された情報を再生する情報再生装置であって、

所定の鍵情報を用いて、上記情報記録媒体に記録された暗号化鍵情報を、復号された鍵情報に復号する暗号化鍵情報復号手段と、

上記コンテンツ情報のうちスクランブルされていないコンテンツ情報を用いて、上記暗号化鍵情報復号手段から出力される復号された鍵情報を変換後の復号された鍵情報に変換する鍵情報変換手段と、

上記鍵情報変換手段から出力される変換後の復号された鍵情報を用いて、上記スクランブルされて記録されたコンテンツ情報をデスクランブルするデスクランブル手段とを備えたことを特徴とする。

【００２２】

本発明に係る情報記録媒体は、データ記録領域を少なくとも有し、著作権を保護すべきコンテンツ情報が記録された情報記録媒体であって、

上記データ記録領域には、暗号化鍵情報とコンテンツ情報とが少なくとも記録され、

上記データ記録領域に記録されるコンテンツ情報の一部はスクランブルされて記録され、

上記スクランブルされて記録されたコンテンツ情報の一部は、上記暗号化鍵情報をスクランブルされていないコンテンツ情報の一部を用いて変換することによって得られるスクランブル鍵情報を用いてスクランブルされていることを特徴とする。

【００２３】

本発明に係る情報記録媒体は、データ記録領域とリードイン領域とを少なくとも有し、著作権を保護すべきコンテンツ情報が記録された情報記録媒体であって、

上記データ記録領域には第１の暗号化鍵情報とコンテンツ情報とが少なくとも記録され、

上記リードイン領域には第２の暗号化鍵情報が記録され、

上記データ記録領域に記録されるコンテンツ情報の一部はスクランブルされて記録され、

上記スクランブルされて記録されたコンテンツ情報は、上記第２の暗号化鍵情報をスクランブルされていないコンテンツ情報の一部を用いて変換することによって得られるスクランブル鍵情報を用いてスクランブルされていることを特徴とする。

【００２４】

また、上記情報記録媒体において、上記スクランブル鍵情報を作成する際に用いられるスクランブルされていないコンテンツ情報の一部は、少なくともコピー制御情報を含むことを特徴とする。

【００２５】

さらに、上記情報記録媒体は複数のセクタに分割された記録領域を有し、上記コンテンツ情報は複数のデータに分割されて上記各セクタに記録され、上記スクランブル鍵情報を作成する際に用いられるスクランブルされていないコンテンツ情報の一部は、コピー制御情報及びセクタ毎に変化するコンテンツ情報の一部とを含むことを特徴とする。

【００２６】

本発明に係る情報再生方法は、データ記録領域とリードイン領域とを少なくとも有し、上記データ記録領域には第１の暗号化鍵情報とコンテンツ情報とが少なくとも記録され、上記リードイン領域には第２の暗号化鍵情報が記録され、データ記録領域に記録されるコンテンツ情報の一部はスクランブルされて記録されている情報記録媒体に記録された情報を再生する情報再生方法であって、
所定の鍵情報を用いて、上記データ記録領域に格納された第１の暗号化鍵情報を第１の鍵情報に復号するステップと、
上記第１の鍵情報を用いて、上記リードイン領域に格納された第２の暗号化鍵情報を第２の鍵情報に復号するステップと、
上記データ記録領域のスクランブルされていないコンテンツ情報を用いて、上記第２の鍵情報を変換後の第２の鍵情報に変換するステップと、
上記変換後の第２の鍵情報を用いて、上記スクランブルされて記録されたコンテンツ情報をデスクランブルするステップとを含むことを特徴とする。

【００２７】

本発明に係る情報再生装置は、データ記録領域とリードイン領域とを少なくとも有し、上記データ記録領域には第１の暗号化鍵情報とコンテンツ情報とが少なくとも記録され、上記リードイン領域には第２の暗号化鍵情報が記録され、上記データ記録領域に記録されるコンテンツ情報の一部はスクランブルされて記録されている情報記録媒体に記録された情報を再生する情報再生装置であって、
所定の鍵情報を用いて、上記データ記録領域に格納された第１の暗号化鍵情報を第１の鍵情報に復号する第１の鍵情報復号手段と、
上記第１の鍵情報復号手段から出力される第１の鍵情報を用いて、上記リードイン領域に格納された第２の暗号化鍵情報を第２の鍵情報に復号する第２の鍵情報復号手段と、
上記コンテンツ情報のうちスクランブルされていないコンテンツ情報を用いて、上記第２の鍵情報復号手段から出力される第２の鍵情報を変換後の第２の鍵情報に変換する鍵変換手段と、
上記鍵変換手段から出力される変換後の第２の鍵情報を用いて、上記スクランブルされて記録されたコンテンツ情報をデスクランブルするデスクランブル処理手段とを備えたことを特徴とする。

【００２８】

また、上記情報再生装置において、上記変換後の第２の鍵情報に変換する際に用いるスクランブルされていないコンテンツ情報は、少なくともコピー制御情報を含むことを特徴とする。

【００２９】

本発明に係る情報記録媒体は、リードイン領域とデータ記録領域とを少なくとも有し、著作権を保護すべきコンテンツ情報が記録された情報記録媒体であって、
上記リードイン領域には第１の暗号化鍵情報が記録され、
上記データ記録領域には第２の暗号化鍵情報とコンテンツ情報とが少なくとも記録され、
上記データ記録領域に記録されるコンテンツ情報の一部はスクランブルされて記録され、
上記スクランブルされて記録されたコンテンツ情報は、上記第２の暗号化鍵情報をスクランブルされていないコンテンツ情報の一部を用いて変換することによって得られるスクランブル鍵情報を用いてスクランブルされていることを特徴とする。

【００３０】

また、上記情報記録媒体において、上記データ記録領域は複数のセクタに分割され、上記各セクタはセクタを識別する情報を記録するセクタヘッダ領域とコンテンツ情報を記録するメインデータ領域とから構成され、
上記セクタヘッダ領域には第２の暗号化鍵情報が記録され、
上記メインデータ領域には上記コンテンツ情報の一部がスクランブルされて記録され、
上記スクランブルされて記録されたコンテンツ情報の一部は、上記第２の暗号化鍵情報をセクタ毎のスクランブルされていないコンテンツ情報の一部を用いて変換することによっ

て得られるスクランブル鍵情報を用いてスクランブルされていることを特徴とする。
【００３１】
さらに、上記情報記録媒体において、上記スクランブル鍵情報を作成する際に用いられるスクランブルされていないコンテンツ情報の一部は、少なくともコピー制御情報を含むことを特徴とする。
【００３２】
またさらに、上記情報記録媒体において、上記スクランブル鍵情報を作成する際に用いられるスクランブルされていないコンテンツ情報の一部は、コピー制御情報と、セクタ毎に変化するコンテンツ情報の一部とを少なくとも含むことを特徴とする。
【００３３】
またさらに、上記情報記録媒体において、上記セクタヘッダ領域に記録される第２の暗号化鍵情報は、上記リードイン領域に記録される第１の暗号化鍵情報を用いて、所定の第２の鍵情報を暗号化した情報であることを特徴とする。
【００３４】
本発明に係る情報再生方法は、リードイン領域とデータ記録領域とを少なくとも有し、上記リードイン領域には第１の暗号化鍵情報が記録され、上記データ記録領域には第２の暗号化鍵情報とコンテンツ情報とが少なくとも記録され、上記データ記録領域に記録されるコンテンツ情報の一部はスクランブルされて記録されている情報記録媒体に記録された情報を再生する情報再生方法であって、
所定の鍵情報を用いて、上記リードイン領域に格納された第１の暗号化鍵情報を第１の鍵情報に復号するステップと、
上記第１の鍵情報を用いて、上記データ記録領域に格納された第２の暗号化鍵情報を第２の鍵情報に復号するステップと、
上記データ記録領域のスクランブルされていないコンテンツ情報を用いて、上記第２の鍵情報を変換後の第２の鍵情報に変換するステップと、
上記変換後の第２の鍵情報を用いて、スクランブルされて記録されたコンテンツ情報をデスクランブルするステップとを含むことを特徴とする。
【００３５】
本発明に係る情報再生装置は、リードイン領域とデータ記録領域とを少なくとも有し、上記リードイン領域には第１の暗号化鍵情報が記録され、上記データ記録領域には第２の暗号化鍵情報とコンテンツ情報とが少なくとも記録され、上記データ記録領域に記録されるコンテンツ情報の一部はスクランブルされて記録されている情報記録媒体に記録された情報を再生する情報再生装置であって、
所定の鍵情報を用いて、上記リードイン領域に格納された第１の暗号化鍵情報を第１の鍵情報に復号する第１の鍵情報復号手段と、
上記第１の鍵情報復号手段から出力される第１の鍵情報を用いて、上記データ記録領域に格納された第２の暗号化鍵情報を第２の鍵情報に復号する第２の鍵情報復号手段と、
上記データ記録領域のスクランブルされていないコンテンツ情報を用いて、上記第２の鍵情報復号手段から出力される第２の鍵情報を変換後の第２の鍵情報に変換する鍵情報変換手段と、
上記鍵情報変換手段から出力される変換後の第２の鍵情報を用いて、上記スクランブルされて記録されたコンテンツ情報をデスクランブルするデスクランブル手段とを備えたことを特徴とする。
【００３６】
また、上記情報再生装置において、上記コンテンツ情報のうちスクランブルされていない部分は、少なくともコピー制御情報を含むことを特徴とする。
【００３７】
【発明の実施形態】
以下、図面を参照して本発明に係る実施形態である、光ディスク、光ディスクに記録された情報を再生する方法、及び光ディスクに記録された情報を再生する装置について説明す

る。ここで、光ディスクとは、ＣＤ、ビデオＣＤ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＭＤ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷなどの光ディスク又は光磁気ディスクを含む。

【００３８】

＜第１の実施形態＞

図１は、本発明に係る第１の実施形態である光ディスク２０１のデータ構造を示す階層図であり、図２は、図１の光ディスク２０１の各記録領域を示す平面図である。

【００３９】

図１において、１００Ａは光ディスク２０１全体の情報記録領域の構造を示しており、制御情報を記録するためのリードイン領域１００と、コンテンツ制御情報１３４とコンテンツデータ１３５からなるコンテンツ情報１３８を記録するためのデータ記録領域１０１と、リードアウト領域１０２とから構成されている。図２に示すように、光ディスク２０１は、その中央部に回転駆動孔２０１ｈを有し、その内側から順次、リードイン領域１００と、データ記録領域１０１と、リードアウト領域１０２とが配置されている。

【００４０】

図１において、リードイン領域１００は、図３の光ディスク再生装置２００が光ディスク２０１を再生するために必要とする情報が記録されるコントロールデータ領域１１０を含み、コントロールデータ領域１１０は１００Ｂで示すように物理情報セクタ１１１と、第２の暗号化鍵情報格納セクタ１５０等から構成される。ここで、物理情報セクタ１１１には、ディスク径、ディスク構造、記録密度などの光ディスク２０１の物理情報が記録されており、第２の暗号化鍵情報格納セクタ１５０には、所定の第２の鍵情報に対して暗号を施した第２の暗号化鍵情報が記録されている。

【００４１】

データ記録領域１０１には、第１の暗号化鍵情報を記録するためのスクランブル情報セクタ１５１と、圧縮された映画や音楽等のコンテンツ情報１３８がスクランブル処理された後スクランブルファイル１３０として記録されている。データ記録領域１０１において、図１の１００Ａに示すように、第１の暗号化鍵情報は、スクランブル情報ファイル１２０として記録され、著作権を保護すべきコンテンツ情報１３８の場合にはスクランブルされてスクランブルファイル１３０として記録され、著作権がフリーなコンテンツ情報１３８はスクランブルされずに、非スクランブルファイル１４０として記録されている。

【００４２】

データ記録領域１０１は、セクタと呼ばれる単位で区切られ、すなわち、複数のセクタに分割され、データ記録領域１０１に記録される各ファイルは、１００Ｃ、１００Ｄ及び１００Ｅで示すように、複数のスクランブル情報セクタ１５１と、複数のスクランブルセクタ１５２と、複数の非スクランブルセクタ１５３とで構成される。ここで、各スクランブルセクタ１５２と各非スクランブルセクタ１５３はそれぞれ、１００Ｆ及び１００Ｇに示すように、セクタを識別するためのアドレス情報１６１等を記録するための１２バイトのセクタヘッダ領域１３１，１４１と、コンテンツ情報１３８を記録するための２０４８バイトのメインデータ領域１３２，１４２とから構成される。また、１００Ｃで示されたスクランブル情報セクタ１５１も、これらの各スクランブルセクタ１５２と各非スクランブルセクタ１５３と同様に、セクタヘッダ領域と、メインデータ領域を有する。

【００４３】

さらに、各セクタのセクタヘッダ領域１３１，１４１には、上述のアドレス情報１６１に加え、スクランブルフラグ１６２が記録されている。セクタヘッダ領域１３１，１４１に記録されるスクランブルフラグ１６２は、そのセクタのメインデータ領域１３２，１４２の所定領域がスクランブルされているか否かを示すフラグであり、情報がスクランブルされているスクランブルセクタには“１”のスクランブルフラグ１６２が記録される一方、情報がスクランブルされていない非スクランブルセクタには“０”のスクランブルフラグ１６２が記録される。

【００４４】

さらに、リードイン領域１００に記録されている第２の暗号化鍵情報格納セクタ１５０内の第２の暗号化鍵情報は、データ記録領域１０１のスクランブル情報ファイル１２０に含まれる第１の暗号化鍵情報を所定の固定鍵情報を用いて復号した結果である第１の鍵情報を用いて第２の鍵情報に復号され、復号された第２の鍵情報は、コンテンツ情報１３８内のコピー制御情報１３６や参照データ１３７を用いて変換され、変換後の第２の鍵情報は、メインデータのデスクランブル処理に用いられるデスクランブル鍵情報となる。本実施形態においては、このデスクランブル鍵情報は、デスクランブル回路２０８に対応するスクランブル回路で暗号化するときに用いるスクランブル鍵情報と同一である。なお、参照データ１３７は、コンテンツデータ１３５の一部のデータである。

【００４５】

また、図１の１００Ｈに示すように、スクランブルセクタ１５２のメインデータ領域１３２は、メインデータ領域１３２のすべてをスクランブルして記録するものではなく、コンテンツ制御情報１３４が含まれる領域やコンテンツデータの一部を除いてスクランブルされている。コピー制御情報１３６は、コンテンツ情報１３８のコピー制限回数や再生時のダウンサンプリング制御等の情報を含んでいる。このスクランブルされたコンテンツデータは、復号された第２の鍵情報を、コンテンツ制御情報１３４に含まれるコピー制御情報１３６及び圧縮されたコンテンツデータ１３５の一部（例えば、図１の１００Ｈに示される参照データ１３７）を用いて変換して得られる、変換後の第２の鍵情報であるスクランブル鍵情報を用いて、所定の領域のコンテンツ情報１３８の一部がスクランブルされて記録されている。

【００４６】

図３は、図１及び図２の光ディスク２０１に記録された情報を再生するための光ディスク再生装置２００の内部構成を示すブロック図であり、図３を参照して、光ディスク再生装置２００について以下に説明する。

【００４７】

本実施形態の光ディスク再生装置２００は、光ディスク２０１から読み出した再生データをデスクランブル処理や伸長処理を施すことにより、所望の映像信号や音声信号を復号して出力する。図３において、図７と同様の構成を有するものは同一の符号を付しており、その詳細な説明は省略する。

【００４８】

図３において、光ディスク再生装置２００には光ディスク２０１が搭載され、光ディスク再生装置２００は、スピンドルモータ２０２と、光学ヘッド２０３と、ヘッドアンプ２０４と、アナログ処理部２０５と、光ディスクコントローラ２０６と、誤り訂正用メモリ２０７と、デスクランブル回路２０８と、ＡＶデコーダ２０９と、ＡＶ信号処理用メモリ２１０と、サーボ制御部２１１と、ＣＰＵ２１２と、ＣＰＵバス２１３とを備えて構成される。すなわち、図３の光ディスク再生装置２００は、図７の光ディスク再生装置４００と比較して、光ディスクコントローラ２０６とＡＶデコーダ２０９との間に、スクランブルされて記録されている情報にデスクランブル処理を施すデスクランブル回路２０８を挿入したことを特徴としている。

【００４９】

図３において、光ディスクコントローラ２０６は処理後の再生データをデスクランブル回路２０８に出力する。デスクランブル回路２０８は、入力される処理後の再生データに対してデスクランブル処理を施した後、処理後の再生データをＡＶデコーダ２０９に出力する。また、サーボ制御部２１１とアナログ処理部２０５と光ディスクコントローラ２０６とデスクランブル回路２０８とＡＶデコーダ２０９は、ＣＰＵバス２１３を介してＣＰＵ２１２に接続され、ＣＰＵ２１２は、ＣＰＵバス２１３を介してアナログ処理部２０５、光ディスクコントローラ２０６、デスクランブル回路２０８、ＡＶデコーダ２０９及びサーボ制御部２１１を制御することにより、光ディスク再生装置２００の全体の動作を制御する。

【００５０】

デスクランブル回路２０８には、データ記録領域１０１に記録されているスクランブル情報ファイル１２０の第１の暗号化鍵情報と、リードイン領域１００の第２の暗号化鍵情報格納セクタ１５０に含まれる第２の暗号化鍵情報と、コンテンツ情報１３８の一部であるコピー制御情報や参照データ１３７とが入力される。デスクランブル回路２０８は、所定の固定鍵情報を用いて、入力された第１の暗号化鍵情報を第１の鍵情報に復号した後、上記第１の鍵情報を用いて、入力された第２の暗号化鍵情報を第２の鍵情報に復号する。次いで、デスクランブル回路２０８は、入力されるコンテンツ情報１３８の一部を用いて、例えば２つの変数を有する高次式などの所定の変換式を利用して、上記第２の鍵情報を、変換後の第２の鍵情報であるデスクランブル鍵情報に変換する。さらに、デスクランブル回路２０８は、上記デスクランブル鍵情報を用いて、図１の１００Ｄで示された構造を有する複数のスクランブルセクタ１５２内のメインデータに対してデスクランブル処理を実行する。

【００５１】

図４は、図３のデスクランブル回路２０８の内部構成を示すブロック図であり、デスクランブル回路２０８の構成及び動作について以下に説明する。

【００５２】

図４において、デスクランブル回路２０８は、第１の信号選択部３０１と、固定鍵情報メモリ３０２と、第２の信号選択部３０３と、第１の鍵情報復号器３０４と、第２の鍵情報復号器３０５と、データデスクランブル処理器３０６と、第３の信号選択部３０７と、第１の鍵情報変換器３１１及び第２の鍵情報変換器３１２を備えてなる鍵変換部３１０とを備えて構成される。ここで、第１と第２と第３の信号選択部３０１，３０３，３０７はそれぞれ、例えばマルチプレクサ又はスイッチ回路で構成される。

【００５３】

図４において、第１の信号選択部３０１は、ＣＰＵバス２１３を介してＣＰＵ２１２から入力される復号モードの設定情報に応じて、光ディスクコントローラ２０６からデスクランブル回路２０８に入力される各データの内部での出力先を選択する。具体的には、第１の信号選択部３０１は、入力されるデータがリードイン領域１００に記録された第２の暗号化鍵情報であるときは、入力される第２の暗号化鍵情報を第２の鍵情報復号器３０５に出力する一方、入力されるデータがデータ記録領域１０１に記録された各セクタデータであるときは、入力される各セクタデータを第２の信号選択部３０３に出力する。固定鍵情報メモリ３０２は、第１の暗号化鍵情報の復号に用いる所定の固定鍵を記憶する。第２の信号選択部３０３は、第１の信号選択部３０１から出力されるセクタデータを入力して、セクタデータのセクタ内の位置に応じて、すなわちセクタデータのデータ数を計数した計数値に応じて、出力先を選択する。図１に示すように、セクタデータは、データ記録領域１０１において、その記録されるセクタデータの種類がセクタ内の位置に応じて決められているので、上記セクタデータのデータ数を計数した計数値に基づいて、第２の信号選択部３０３は、図４に示すように、

（ａ）入力されるセクタデータが第１の暗号化鍵情報であるときは、入力される第１の暗号化鍵情報を第１の鍵情報復号器３０４に出力し、

（ｂ）入力されるセクタデータがコピー制御データであるときは、入力されるコピー制御データを鍵変換部３１０内の第１の鍵情報変換器３１１に出力し、

（ｃ）入力されるセクタデータが参照データであるときは、入力される参照データを鍵変換部３１０内の第２の鍵情報変換器３１２に出力し、

（ｄ）入力されるセクタデータがスクランブルフラグであるときは、入力されるスクランブルフラグを第３の信号選択部３０７に出力し、

（ｅ）入力されるセクタデータがメインデータであるときは、入力されるメインデータをデータデスクランブル処理器３０６及び第３の信号選択部３０７に出力する。

【００５４】

また、第１の鍵情報復号器３０４は、固定鍵情報メモリ３０２から読み出される固定鍵情報を用いて、第２の信号選択部３０３から出力されるデータ記録領域１０１内のスクラン

ブル情報ファイル１２０に含まれる第１の暗号化鍵情報に対して、例えばＤＥＳ暗号方式、ＲＳＡ暗号方式などの公知の暗号方式の復号方法で復号処理を実行することにより、第１の暗号化鍵情報を第１の鍵情報に復号して第２の鍵情報復号器３０５に出力する。次いで、第２の鍵情報復号器３０５は、第１の鍵情報復号器３０４から出力される復号された第１の鍵情報を用いて、第１の信号選択部３０１から入力されるリードイン領域１１２内の第２の暗号化鍵情報格納セクタ１５０に格納された第２の暗号化鍵情報に対して、第１の鍵情報復号器３０４と同様に、例えばＤＥＳ暗号方式、ＲＳＡ暗号方式などの公知の暗号方式の復号方法で復号処理を実行することにより、第２の暗号化鍵情報を第２の鍵情報に復号して鍵変換部３１０内の第１の鍵情報変換器３１１に出力する。

【００５５】

さらに、鍵変換部３１０は、第１と第２の鍵情報変換器３１１，３１２を備えて構成され、第２の信号選択部３０３から出力されるコピー制御情報と参照データとを用いて、第２の鍵情報復号器３０５から出力される第２の鍵情報を、変換後の第２の鍵情報であるデスクランブル鍵情報に変換してデータデスクランブル処理器３０６に出力する。ここで、第１の鍵情報変換器３１１は、第２の信号選択部３０３から出力されるコピー制御情報を用いて、例えば、入力される２つのデータを２つの変数とする高次式に代入してその高次式の値を計算する方法など、所定の高次式などの所定の第１の変換式を利用して、第２の鍵情報復号器３０５から出力される第２の鍵情報を、第１の鍵情報変換後の第２の鍵情報に変換して第２の鍵情報変換器３１２に出力する。次いで、第２の鍵情報変換器３１２は、第２の信号選択部３０３から出力される参照データを用いて、第１の鍵情報変換器３１１と同様に、例えば、入力される２つのデータを２つの変数とする高次式に代入してその高次式の値を計算する方法など、所定の高次式などの所定の第２の変換式を利用して、第１の鍵情報変換器３１１から出力される第１の鍵情報変換後の第２の鍵情報を、第２の鍵情報変換後の第２の鍵情報である変換後の第２の鍵情報に変換してデータデスクランブル処理器３０６に出力する。

【００５６】

またさらに、データデスクランブル処理器３０６は、鍵変換部３１０内の第２の鍵情報変換器３１２から出力されるデスクランブル鍵情報を用いて、第２の信号選択部３０３から出力されるメインデータに対して、データのデスクランブル処理を実行することにより、デスクランブル処理後のメインデータを発生して第３の信号選択部３０７に出力する。ここで、データのデスクランブル処理は、例えばM系列信号などの所定長の擬似ランダムパターン信号を、送信機側と同様に、有限長のシフトレジスタと加算器とを用いて発生させた後、発生された擬似ランダムパターン信号と入力データとの排他的論理和を演算することにより実行される。

【００５７】

次いで、第３の信号選択部３０７は、第２の信号選択部３０３から出力されるスクランブルフラグと、内部で計数されるセクタデータのデータ数の計数値とに基づいて、第２の信号選択部３０３から出力されるデスクランブル処理が施されていないメインデータと、データデスクランブル処理器３０６から出力されるデスクランブル処理が施されたメインデータとのうちの１つを選択して、選択されたメインデータをＡＶデコーダ２０９に出力する。ここで、スクランブルフラグが“１”でありかつ非スクランブルデータ１６３の記憶領域でないとき、すなわち、メインデータがスクランブルされているときは、第３の信号選択部３０７は、データデスクランブル処理器３０６から出力されるデスクランブル処理が施されたメインデータを選択してＡＶデコーダ２０９に出力する。一方、スクランブルフラグが“１”でありかつ非スクランブルデータ１６３の記憶領域であるとき、もしくは、スクランブルフラグが“０”であるとき、すなわち、メインデータがスクランブルされていないときは、第３の信号選択部３０７は、第２の信号選択部３０３から出力されるデスクランブル処理が施されていないメインデータを選択してＡＶデコーダ２０９に出力する。

【００５８】

以上のように構成された、本実施形態に係る光ディスク再生装置２００の動作について、図３及び図４を用いて説明する。

【００５９】

光ディスク再生装置２００は、電源投入時に光ディスク２０１が挿入されている場合、もしくは新たに光ディスク２０１が挿入されたときには、ＣＰＵ２１２は、光学ヘッド２０３からリードイン領域１００のコントロールデータ領域１１０の第２の暗号化鍵情報格納セクタ１５０（図１参照。）に格納された情報データを光ディスク２０１から読み出すようにサーボ制御部２１１を制御する。読み出された情報データの電気信号は、ヘッドアンプ２０４、アナログ処理部２０５、光ディスクコントローラ２０６によりそれぞれ、増幅され、復調処理を施され、エラー訂正が施される。そして、ＣＰＵ２１２は、処理後の第２の暗号化鍵情報のデータを誤り訂正用メモリ２０７に記憶する。

【００６０】

次いで、ＣＰＵ２１２は、スクランブル情報ファイル（第１の暗号化鍵情報）１２０（図１参照。）が格納されたセクタを光ディスク２０１から読み出すように、サーボ制御部２１１を制御する。読み出された情報データの電気信号は、ヘッドアンプ２０４、アナログ処理部２０５、光ディスクコントローラ２０６によりそれぞれ、増幅され、復調処理を施され、エラー訂正が施される。このとき、デスクランブル回路２０８では、ＣＰＵ２１２からの復号モード設定情報により第１の暗号化鍵情報の復号モードが設定され、光ディスクコントローラ２０６から入力された第１の暗号化鍵情報は、第１の信号選択部３０１及び第２の信号選択部３０３により、第１の鍵情報復号器３０４に転送される。そして、転送された第１の暗号化鍵情報は、第１の鍵情報復号器３０４により、固定鍵情報メモリ３０２から読み出される固定鍵情報を用いて復号処理が実行され、復号された第１の鍵情報は第２の鍵情報復号器３０５に出力される。なお、この第１の鍵情報を復号する第１の暗号化鍵情報の復号モードでは、デスクランブル回路２０８からはデータは出力されない。

【００６１】

次いで、すでに誤り訂正用メモリ２０７に記憶されている第２の暗号化鍵情報が読み出され、デスクランブル回路２０８の第１の信号選択部３０１を介して第２の鍵情報復号器３０５に出力される。第２の鍵情報復号器３０５には、上述のように、すでに第１の鍵情報復号器３０４で復号された第１の鍵情報が入力されており、第２の鍵情報復号器３０５は、復号された第１の鍵情報を用いて、入力される第２の暗号化鍵情報に対して復号処理を実行することにより、第２の暗号化鍵情報を第２の鍵情報に復号して鍵変換部３１０の第１の鍵情報変換器３１１に出力する。

【００６２】

次いで、装置使用者の操作等に応じてファイルが選択され、映像信号や音声信号を再生する動作を説明する。

【００６３】

ＣＰＵ２１２は、サーボ制御部２１１、光学ヘッド２０３、アナログ処理部２０５、及び光ディスクコントローラ２０６を制御することにより、光ディスク２０１から所望の情報データを読み出し、エラー訂正後の情報データを誤り訂正用メモリ２０７に格納する。また、ＣＰＵ２１２はデスクランブル回路２０８に対してデータのデスクランブルモードを設定するとともに、ＡＶデコーダ２０９に必要な情報を設定した後に、エラー訂正後の情報データを誤り訂正用メモリ２０７からデスクランブル回路２０８に転送する。

【００６４】

デスクランブル回路２０８においては、復号モード設定情報としてデータのデスクランブルモードに設定されることから、入力されるセクタデータは、第１の信号選択部３０１により第２の信号選択部３０３に転送される。第２の信号選択部３０３は、入力されるセクタデータのデータ数を計数し、計数値に基づいて入力されるセクタデータを以下のように出力する。

（ａ）上記計数値がコピー制御情報が含まれるデータ位置の場合には、入力されるセクタデータを第１の鍵情報変換器３１１に出力する。

（ｂ）上記計数値が参照データが含まれるデータ位置の場合には、入力されるセクタデータを第２の鍵情報変換器３１２に出力する。
（ｃ）上記計数値がメインデータが含まれるデータ位置の場合には、入力されるセクタデータをデータデスクランブル処理器３０６及び第３の信号選択部３０７に出力する。
【００６５】
第２の鍵情報復号器３０５から出力される復号された第２の鍵情報は、メインデータに含まれるコピー制御情報を用いて、第１の鍵情報変換器３１１により第１の鍵情報変換後の第２の鍵情報に変換された後、第２の鍵情報変換器３１２に出力される。次いで、第１の鍵情報変換器３１１から出力される第１の鍵情報変換後の第２の鍵情報は、メインデータに含まれる参照データを用いて、第２の鍵情報変換器３１２により変換後の第２の鍵情報であるデスクランブル鍵情報に変換された後、データデスクランブル処理器３０６に出力される。さらに、データデスクランブル処理器３０６に入力されたメインデータは、鍵変換部３１０から出力されるデスクランブル鍵情報を用いて、デスクランブル処理を施され、デスクランブル処理後のメインデータが第３の信号選択部３０７に出力される。
【００６６】
第３の信号選択部３０７は、第２の信号選択部３０３により選択されたスクランブルフラグを受信するとともに、内部でセクタデータのデータ数を計数し、スクランブルフラグと計数値とに基づいて選択信号を発生し、当該発生した選択信号に基づいて、データデスクランブル処理器３０６からのメインデータと、第２の信号選択部３０３からのメインデータとのうちのいずれか１つを選択的に出力する。ここで、上記発生された選択信号により、スクランブルフラグが“１”でかつセクタデータのデータ数の計数値が非スクランブルデータ１６３の記録領域を示している場合は、第２の信号選択部３０３から出力されたデスクランブル処理が施されていないメインデータが第３の信号選択部３０７から出力される一方、スクランブルフラグが“１”でかつセクタデータのデータ数の計数値がスクランブルデータ１６４の記憶領域を示している場合、データデスクランブル処理器３０６から出力されたメインデータが第３の信号選択部３０７から出力される。さらに、上記発生された選択信号により、スクランブルフラグが“０”の場合には、セクタデータのデータ数の計数値に関わらず、第２の信号選択部３０３から出力されたデスクランブル処理を施されていないメインデータが第３の信号選択部３０７から出力される。
【００６７】
このように、スクランブルフラグ及びセクタデータのデータ数の計数値に応じてデスクランブル処理が施されたメインデータは、デスクランブル回路２０８からＡＶデコーダ２０９に出力される。ＡＶデコーダ２０９は、多重化されたオーディオとビデオの圧縮データを分離して、それぞれ伸長処理を施した後、伸張処理後の映像信号及び音声信号を出力する。
【００６８】
以上説明したように、本実施形態によれば、以下の特有の効果を有する。
【００６９】
まず、コピー回数の制限や再生時のダウンサンプリング制御情報などのコンテンツ制御情報１３４を、例えばＤＶＤプレイヤである光ディスク再生装置２００のシステムコントロール手段であるＣＰＵ２１２（図３参照。）が読み込んで、光ディスク再生装置２００の制御を行う際に、コンテンツ制御情報はスクランブルされずに記録されているので、容易に参照することができる。
【００７０】
また、コンテンツ制御情報１３４は、上記の観点からスクランブルされずに記録しているが、不正にコンテンツ制御情報１３４を改ざんした場合、鍵変換部３１０を備えており正しいデスクランブル鍵情報を生成することはできないので、不正な再生を防止することができる。
【００７１】
さらに、コンテンツ制御情報１３４を用いて、第２の暗号化鍵情報からスクランブル鍵情

報を得る際に、さらにセクタ単位で変化しやすいコンテンツデータを用いているので、コンテンツ制御情報１３４が図１に示すように上述のファイル単位に記録され、かつ第２の暗号化鍵情報がディスク単位で記録されたとしても、スクランブル鍵情報がセクタ毎に変化するので、スクランブルによるコンテンツの保護強度を高くすることができる。

【００７２】

＜第２の実施形態＞

図５は、本発明に係る第２の実施形態である光ディスク２０１のデータ構造を示す階層図であり、図６は、第２の実施形態で用いるデスクランブル回路２０８ａの内部構成を示すブロック図である。図５及び図６において、図１及び図４と同様のものについては同一の符号を付している。以下、第２の実施形態に係る光ディスク２０１のデータ構造及びデスクランブル回路２０８ａの構成及び動作について、特に、第１の実施形態と異なる部分を詳細に説明する。

【００７３】

第１の実施形態では、第１の暗号化鍵情報は、図１に示すように、スクランブル情報ファイル１２０としてデータ記録領域１０１に格納されていたが、本実施形態では、図５に示すように、リードイン領域１００のコントロールデータ領域１１０のスクランブル情報セクタ１１２に格納される。また、第１の実施形態では、第２の暗号化鍵情報は、図１に示すように、リードイン領域１００のコントロールデータ領域１１０の第２の暗号化鍵情報格納セクタ１５０に格納されていたが、本実施形態では、図５に示すように、データ記録領域１０１のスクランブルファイル１３０のスクランブルセクタ１５２のセクタヘッダ領域１３１にアドレス情報、スクランブルフラグと共に格納されている。

【００７４】

以上のように構成された光ディスク２０１に記録された情報を再生するための光ディスク再生装置２００について、図６を参照して説明する。本実施形態では、図４のデスクランブル回路２０８に代えて、図６のデスクランブル回路２０８ａを備えたことを特徴としている。具体的には、図６のデスクランブル回路２０８ａにおいて、図４のデスクランブル回路２０８に比較して以下の点が異なる。

【００７５】

（ａ）第１の信号選択部３０１に代えて、第１の信号選択部３０１ａを備えるとともに、第２の信号選択部３０３に代えて、第２の信号選択部３０３ａを備える。

（ｂ）図４のデスクランブル回路２０８では、第１の暗号化鍵情報は、第１と第２の信号選択部３０１，３０３により選択された後、第１の鍵情報復号器３０４に出力されているが、図６のデスクランブル回路２０８ａでは、第１の暗号化鍵情報は、第１の信号選択部３０１ａにより選択された後、第１の鍵情報復号器３０４に出力されている。

（ｃ）図４のデスクランブル回路２０８では、第２の暗号化鍵情報は、第１の信号選択部３０１により選択された後、第２の鍵情報復号器３０５に出力されているが、図６のデスクランブル回路２０８ａでは、第２の暗号化鍵情報は、第１と第２の信号選択部３０１ａ，３０３ａにより選択された後、第２の鍵情報復号器３０５に出力されている。

【００７６】

すなわち、図６のデスクランブル回路２０８ａは、光ディスクコントローラ２０６から入力される、リードイン領域１００のスクランブル情報セクタ１１２に記録されている第１の暗号化鍵情報を復号するとともに、図５の１１０Ｃで示したデータ構造を有するセクタデータに対して、第２の暗号化鍵情報の復号処理及びメインデータのデスクランブル処理を実行する。

【００７７】

次いで、デスクランブル回路２０８ａの動作において、図６を参照して第１の実施形態に係る図４のデスクランブル回路２０８との相違点について詳細に説明する。

【００７８】

第１の信号選択部３０１ａは、入力されるデータがリードイン領域１００のコントロールデータ領域１１０のスクランブル情報セクタ１１２に記録された第１の暗号化鍵情報であ

るときは、入力される第１の暗号化鍵情報を第１の鍵情報復号器３０４に出力する一方、入力されるデータがデータ記録領域１０１に記録された各セクタデータであるときは、入力される各セクタデータを第２の信号選択部３０３ａに出力する。次いで、第２の信号選択部３０３ａは、第１の信号選択部３０１ａから出力されるセクタデータを入力して、セクタデータのセクタ内の位置に応じて、すなわちセクタデータのデータ数を計数した計数値に応じて、出力先を選択する。図１に示すように、セクタデータは、データ記録領域１０１において、その記録されるセクタデータの種類がセクタ内の位置に応じて決められているので、上記セクタデータのデータ数を計数した計数値に基づいて、第２の信号選択部３０３ａは、図６に示すように、

（ａ）入力されるセクタデータが第２の暗号化鍵情報であるときは、入力される第２の暗号化鍵情報を第２の鍵情報復号器３０５に出力し、

（ｂ）入力されるセクタデータがコピー制御データであるときは、入力されるコピー制御データを鍵変換部３１０内の第１の鍵情報変換器３１１に出力し、

（ｃ）入力されるセクタデータが参照データであるときは、入力される参照データを鍵変換部３１０内の第２の鍵情報変換器３１２に出力し、

（ｄ）入力されるセクタデータがスクランブルフラグであるときは、入力されるスクランブルフラグを第３の信号選択部３０７に出力し、

（ｅ）入力されるセクタデータがメインデータであるときは、入力されるメインデータをデータデスクランブル処理器３０６及び第３の信号選択部３０７に出力する。

【００７９】

以上のように構成された本実施形態に係る光ディスク再生装置２００の動作について、図３及び図６を用いて説明する。なお、図３においては、デスクランブル回路２０８はデスクランブル回路２０８ａに置き換えられる。

【００８０】

光ディスク再生装置２００は電源投入時に光ディスク２０１が挿入されている場合、もしくは新たに光ディスク２０１が挿入された時には、リードイン領域１００のコントロールデータ領域１１０のスクランブル情報セクタ１１２に記録されている第１の暗号化鍵情報に対して復号処理を実行する。ＣＰＵ２１２はサーボ制御部２１１を制御して、光学ヘッド２０３を用いて光ディスク２０１からリードイン領域１００のコントロールデータ領域１１０のスクランブル情報セクタ１１２の情報データを読み出すよう制御する。読み出された情報データの電気信号は、ヘッドアンプ２０４、アナログ処理部２０５、光ディスクコントローラ２０６によりそれぞれ、増幅され、復調処理を施され、エラー訂正が施された後、エラー訂正処理後の情報データは誤り訂正用メモリ２０７に格納される。また、ＣＰＵ２１２は、デスクランブル回路２０８ａに対して復号モード設定情報として第１の暗号化鍵情報の復号モードを設定し、光ディスクコントローラ２０６からエラー訂正処理後のスクランブル情報セクタ１１２内の第１の暗号化鍵情報のデータをデスクランブル回路２０８ａに転送するよう制御する。

【００８１】

デスクランブル回路２０８ａでは、第１の暗号化鍵情報の復号モードが設定されることから、入力されたスクランブル情報セクタ１１２内の第１の暗号化鍵情報のデータは、第１の信号選択部３０１ａにより第１の鍵情報復号器３０４に転送され、転送された第１の暗号化鍵情報は、第１の鍵情報復号器３０４により、固定鍵情報メモリ３０２から読み出される固定鍵情報を用いて復号処理が施され、第１の暗号化鍵情報は第１の鍵情報に復号された後、第２の鍵情報復号器３０５に出力される。なお、この第１の暗号化鍵情報の復号モードでは、デスクランブル回路２０８ａからはデータは出力されない。

【００８２】

次いで、装置使用者の操作等に応じてファイルが選択され、映像信号や音声信号を再生する動作を説明する。

【００８３】

ＣＰＵ２１２は、サーボ制御部２１１、光学ヘッド２０３、アナログ処理部２０５及び光

ディスクコントローラ２０６を制御して、光ディスク２０１から所望の情報データを読み出した後、エラー訂正後の情報データを誤り訂正用メモリ２０７に格納する。また、ＣＰＵ２１２はデスクランブル回路２０８ａに対してデータのデスクランブルモードを設定するとともに、ＡＶデコーダ２０９に必要な情報データを設定した後に、エラー訂正後の情報データを誤り訂正用メモリ２０７からデスクランブル回路２０８ａに転送する。

【００８４】

デスクランブル回路２０８ａでは、復号モード設定情報としてデータのデスクランブルモードに設定されることから、第１の信号選択部３０１ａにより、入力されるセクタデータは、第２の信号選択部３０３ａに転送される。第２の信号選択部３０３ａは、入力されるセクタデータのデータ数を計数し、上記計数値に応じて入力されるセクタデータを以下のように選択的に出力する。

（ａ）上記計数値がセクタヘッダ領域１３１の第２の暗号化鍵情報１３３の場合に、セクタデータ内の第２の暗号化鍵情報１３３を第２の鍵情報復号器３０５に出力する。

（ｂ）上記計数値がコピー制御情報１３６が含まれるデータ位置の場合に、セクタデータ内のコピー制御情報１３６を第１の鍵情報変換器３１１に出力する。

（ｃ）上記計数値が参照データ１３７が含まれるデータ位置の場合に、セクタデータ内の参照データ１３７を第２の鍵情報変換器３１２に出力する。

（ｄ）上記計数値がメインデータが含まれるデータ位置の場合に、メインデータをデータデスクランブル処理器３０６及び第３の信号選択部３０７に出力する。

【００８５】

第２の鍵情報復号器３０５に入力された第２の暗号化鍵情報は、第１の鍵情報復号器３０４から出力される第１の鍵情報を鍵として用いて第２の鍵情報に復号され、復号された第２の鍵情報は、鍵変換部３１０内の第１の鍵情報変換器３１１に出力される。

【００８６】

次いで、復号された第２の鍵情報は、メインデータに含まれるコピー制御情報１３６を用いて、第１の鍵情報変換器３１１により第１の鍵情報変換後の第２の鍵情報に変換された後、第２の鍵情報変換器３１２に出力される。上記第１の鍵情報変換後の第２の鍵情報は、メインデータに含まれる参照データを用いて、第２の鍵情報変換器３１２により変換後の第２の鍵情報に変換され、変換された第２の鍵情報は、デスクランブル鍵情報としてデータデスクランブル処理器３０６に出力される。そして、データデスクランブル処理器３０６に入力されたメインデータは、鍵変換部３１０内の第２の鍵情報変換器３１２から出力されるデスクランブル鍵情報を用いて、デスクランブル処理が施され、デスクランブル処理後のメインデータは第３の信号選択部３０７に出力される。

【００８７】

次いで、第３の信号選択部３０７は、第２の信号選択部３０３ａから出力されるスクランブルフラグと、内部で計数されるセクタデータのデータ数の計数値とに基づいて、第２の信号選択部３０３ａから出力されるデスクランブル処理が施されていないメインデータと、データデスクランブル処理器３０６から出力されるデスクランブル処理が施されたメインデータとのうちの１つを選択して、選択されたメインデータをＡＶデコーダ２０９に出力する。ここで、スクランブルフラグが“１”でありかつ非スクランブルデータ１６３の記憶領域でないとき、すなわち、メインデータがスクランブルされているときは、第３の信号選択部３０７は、データデスクランブル処理器３０６から出力されるデスクランブル処理が施されたメインデータを選択してＡＶデコーダ２０９に出力する。一方、スクランブルフラグが“１”でありかつ非スクランブルデータ１６３の記憶領域であるとき、もしくは、スクランブルフラグが“０”であるとき、すなわち、メインデータがスクランブルされていないときは、第３の信号選択部３０７は、第２の信号選択部３０３ａから出力されるデスクランブル処理が施されていないメインデータを選択してＡＶデコーダ２０９に出力する。

【００８８】

なお、本実施形態においては、第２の暗号化鍵情報は、１つのスクランブルセクタ１５２

内に格納してもよいし、複数のデータに分割して複数のスクランブルセクタ１５２のスクランブルファイル１３０に格納してもよい。

【００８９】

以上説明したように、本実施形態によれば、第１の実施形態の効果に加えて、第２の暗号化鍵情報をセクタ単位又はファイル単位に記録することができるので、第２の暗号化鍵情報をセクタ単位又はファイル単位で変更することができ、スクランブルによる著作権保護の強度をさらに強めることができる。

【００９０】

＜変形例＞

以上の実施形態においては、光ディスク、光ディスクに記録された情報を再生する方法、及び光ディスクに記録された情報を再生する装置について説明しているが、本発明はこれに限らず、フロッピーディスクなどの磁気記録媒体と、フラッシュメモリ、ＥＰＲＯＭ、ＥＥＰＲＯＭなどのメモリとを含む情報記録媒体、当該情報記録媒体に記録された情報を再生する方法、及び当該情報記録媒体に記録された情報を再生する装置に適用することができる。

【００９１】

以上の実施形態においては、スクランブルされて記録されたコンテンツ情報１３８の一部は、第１と第２の暗号化鍵情報をスクランブルされていないコンテンツ情報１３８の一部を用いて変換することによって得られるスクランブル鍵情報を用いてスクランブルされているが、本発明はこれに限らず、スクランブルされて記録されたコンテンツ情報１３８の一部は、第１と第２の暗号化鍵情報のうちの少なくとも一方をスクランブルされていないコンテンツ情報１３８の一部を用いて変換することによって得られるスクランブル鍵情報を用いてスクランブルされてもよい。

【００９２】

以上の実施形態においては、第１と第２の鍵情報復号器３０４，３０５を備えているが、本発明はこれに限らず、第１と第２の鍵情報復号器３０４，３０５のうちの少なくとも一方を備えるようにしてもよい。ここで、第１の鍵情報復号器３０４のみを備えるときは、第１の鍵情報復号器３０４により復号された第１の鍵情報は鍵変換部３１０に出力される。また、第２の鍵情報復号器３０５のみを備えるときは、第２の鍵情報復号器３０５は、固定鍵情報メモリ３０２から読み出された固定鍵情報を用いて、第２の暗号化鍵情報を第２の鍵情報に復号して鍵変換部３１０に出力する。

【００９３】

以上の実施形態においては、鍵変換部３１０は、第１と第２の鍵情報変換器３１１，３１２を備えているが、本発明はこれに限らず、第１と第２の鍵情報変換器３１１，３１２のうちの少なくとも一方を備えてもよい。すなわち、第２の鍵情報復号器３０５から出力される復号された第２の鍵情報は、コンテンツ情報１３８の一部である、例えばコピー制御情報１３６と参照データ１３７のうちの少なくとも一方を用いて変換して、変換後の第２の鍵情報をデスクランブル鍵情報として用いてもよい。

【００９４】

以上の実施形態においては、鍵情報復号器３０４，３０５はそれぞれ、所定の鍵情報を用いて、所定の暗号化鍵情報を復号された鍵情報に復号しているが、本発明はこれに限らず、鍵情報復号器３０４，３０５はそれぞれ、所定の鍵情報を用いて、所定の変換式を利用して、所定の暗号化鍵情報を変換後の暗号化鍵情報に変換してもよい。

【００９５】

以上の実施形態においては、鍵情報変換器３１１，３１２はそれぞれ、所定の情報を用いて、所定の変換式を利用して、所定の暗号化鍵情報を変換後の暗号化鍵情報に変換しているが、本発明はこれに限らず、鍵情報変換器３１１，３１２はそれぞれ、所定の鍵情報を用いて、所定の暗号化鍵情報を復号された鍵情報に復号してもよい。

【００９６】

【発明の効果】

以上詳述したように本発明に係る情報記録媒体によれば、著作権を保護すべきコンテンツ情報と、暗号化鍵情報とが少なくとも記録された情報記録媒体であって、上記コンテンツ情報の一部はスクランブルされて記録され、上記スクランブルされて記録されたコンテンツ情報の一部は、上記暗号化鍵情報をスクランブルされていないコンテンツ情報の一部を用いて変換することによって得られるスクランブル鍵情報を用いてスクランブルされている。従って、本発明によれば、以下のような特有の効果を有する。

【００９７】

まず、コピー回数の制限や再生時のダウンサンプリング制御情報などのコンテンツ制御情報であるコンテンツ情報の一部を、例えばＤＶＤプレイヤである情報再生装置のシステムコントロール手段が読み込んで、情報再生装置の制御を行う際に、コンテンツ制御情報はスクランブルされずに記録されているので、容易に参照することができる。

【００９８】

また、コンテンツ制御情報などのコンテンツ情報の一部はスクランブルされずに記録しているが、不正にコンテンツ制御情報などのコンテンツ情報の一部を改ざんした場合、正しいデスクランブル鍵情報を生成することはできないので、不正な再生を防止することができる。

【００９９】

さらに、コンテンツ制御情報などのコンテンツ情報の一部を用いて、暗号化鍵情報からスクランブル鍵情報を得る際に、さらにセクタ単位で変化しやすいコンテンツデータを用いているので、コンテンツ制御情報などのコンテンツ情報の一部がファイル単位に記録され、かつ暗号化鍵情報がディスク単位で記録されたとしても、スクランブル鍵情報がセクタ毎に変化するので、スクランブルによるコンテンツの保護強度を高くすることができる。

【０１００】

さらに、スクランブルされないデータを参照データとしてスクランブル鍵情報の生成に用いているので、例えば暗号化鍵情報やコピー制御情報がファイル単位で設定されたとしてもスクランブル鍵情報はセクタ単位で変化するので、不正な攻撃に対しても強いという効果がある。

【０１０１】

またさらに、暗号化鍵情報をセクタ単位又はファイル単位に記録したとき、暗号化鍵情報をセクタ単位又はファイル単位で変更することができ、スクランブルによる著作権保護の強度をさらに強めることができる。

【図面の簡単な説明】

【図１】　本発明に係る第１の実施形態である光ディスク２０１のデータ構造を示す階層図である。

【図２】　図１の光ディスク２０１の各記録領域を示す平面図である。

【図３】　図１及び図２の光ディスク２０１に記録された情報を再生するための光ディスク再生装置２００の内部構成を示すブロック図である。

【図４】　図３のデスクランブル回路２０８の内部構成を示すブロック図である。

【図５】　本発明に係る第２の実施形態である光ディスク２０１のデータ構造を示す階層図である。

【図６】　第２の実施形態で用いるデスクランブル回路２０８ａの内部構成を示すブロック図である。

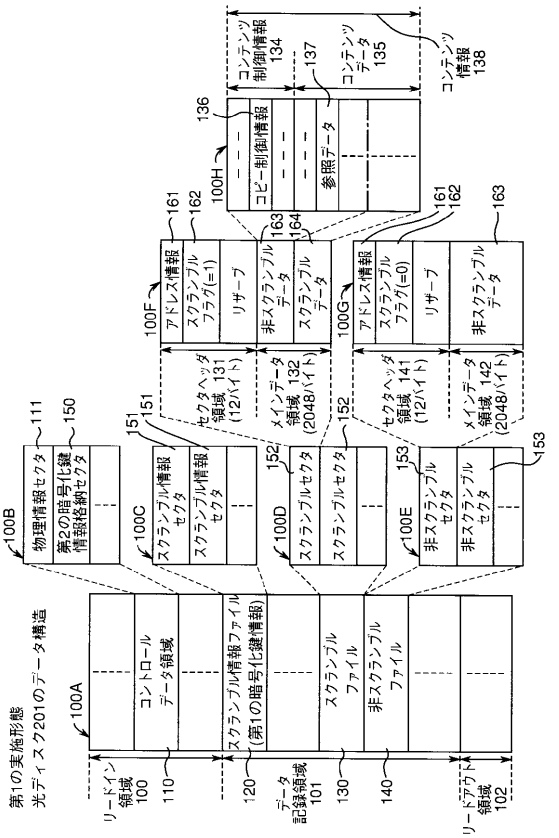
【図７】　第１の従来例の光ディスク再生装置４００の内部構成を示すブロック図である。

【符号の説明】

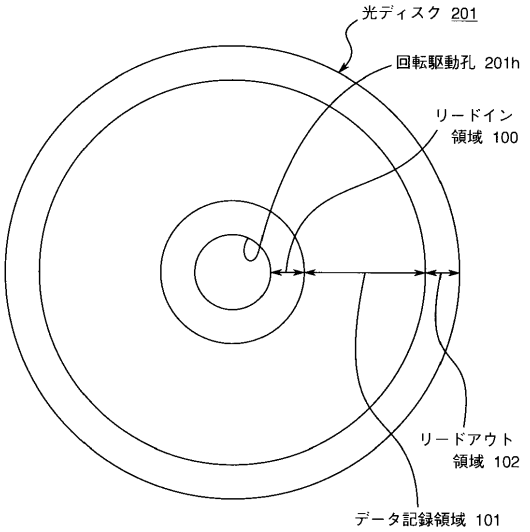
１００…リードイン領域、
１０１…データ記録領域、
１０２…リードアウト領域、
１１０…コントロールデータ領域、
１１１…物理情報セクタ、

１１２…スクランブル情報セクタ、
１２０…スクランブル情報ファイル、
１３０…スクランブルファイル、
１４０…非スクランブルファイル、
１３１、１４１…セクタヘッダ領域、
１３２、１４２…メインデータ領域、
１３３…第２の暗号化鍵情報、
１３４…コンテンツ制御情報、
１３５…コンテンツデータ、
１３６…コピー制御情報、
１３７…参照データ、
１３８…コンテンツ情報、
１５０…第２の暗号化鍵情報格納セクタ、
１５１…スクランブル情報セクタ、
１５２…スクランブルセクタ、
１５３…非スクランブルセクタ、
１６１…アドレス情報、
１６２…スクランブルフラグ、
１６３…非スクランブルデータ、
１６４…スクランブルデータ、
２００、４００…光ディスク再生装置、
２０１…光ディスク、
２０２…スピンドルモータ、
２０３…光学ヘッド、
２０４…ヘッドアンプ、
２０５…アナログ処理部、
２０６…光ディスクコントローラ、
２０７…誤り訂正用メモリ、
２０８，２０８ａ…デスクランブル回路、
２０９…ＡＶデコーダ、
２１０…ＡＶ信号処理用メモリ、
２１１…サーボ制御部、
２１２…ＣＰＵ、
２１３…ＣＰＵバス、
３０１，３０１ａ…第１の信号選択部、
３０２，３０２ａ…固定鍵情報メモリ、
３０３…第２の信号選択部、
３０４…第１の鍵情報復号器、
３０５…第２の鍵情報復号器、
３０６…データデスクランブル処理器、
３０７…第３の信号選択部、
３１０…鍵変換部、
３１１…第１の鍵情報変換器、
３１２…第２の鍵情報変換器。

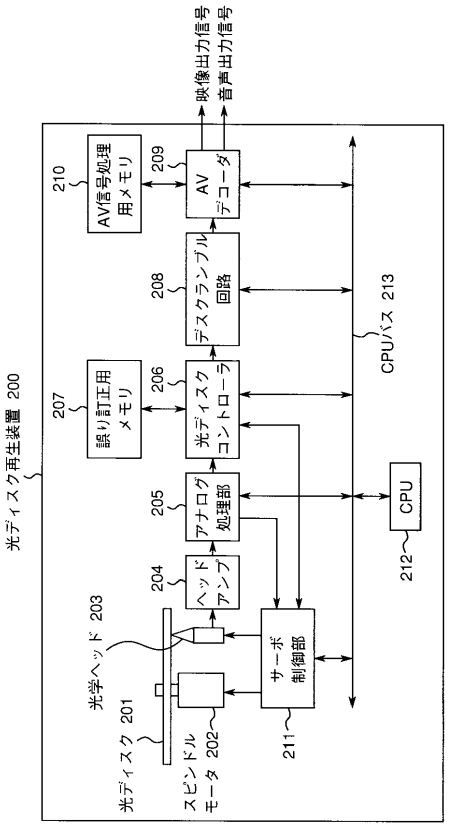
【図１】


第1の実施形態
光ディスク201のデータ構造
100A
コントロールデータ領域
スクランブル情報ファイル(第1の暗号化鍵情報)
スクランブルファイル
非スクランブルファイル
リードイン領域 100
110
120
データ記録領域 101
130
140
リードアウト領域 102
100B
物理情報セクタ
第2の暗号化鍵情報格納セクタ
111
150
100C
スクランブル情報セクタ
スクランブル情報セクタ
151
100D
スクランブルセクタ
スクランブルセクタ
152
100E
非スクランブルセクタ
非スクランブルセクタ
153
セクタヘッダ領域 131 (12バイト)
メインデータ領域 132 (2048バイト)
セクタヘッダ領域 141 (12バイト)
メインデータ領域 142 (2048バイト)
100F
アドレス情報
スクランブルフラグ(=1)
リザーブ
非スクランブルデータ
スクランブルデータ
161
162
163
164
100G
アドレス情報
スクランブルフラグ(=0)
リザーブ
非スクランブルデータ
100H
コピー制御情報
参照データ
136
137
コンテンツ制御情報 134
コンテンツデータ 135
コンテンツ情報 138

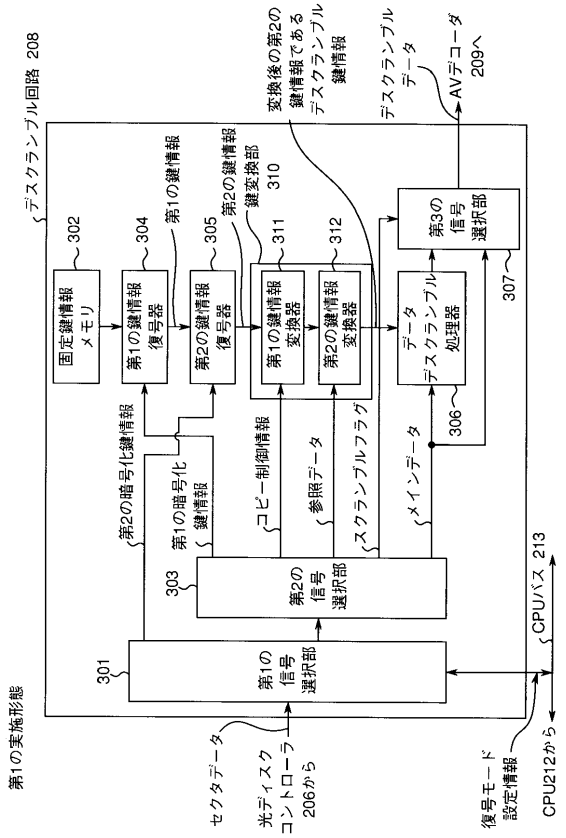
【図２】


光ディスク 201
回転駆動孔 201h
リードイン領域 100
リードアウト領域 102
データ記録領域 101

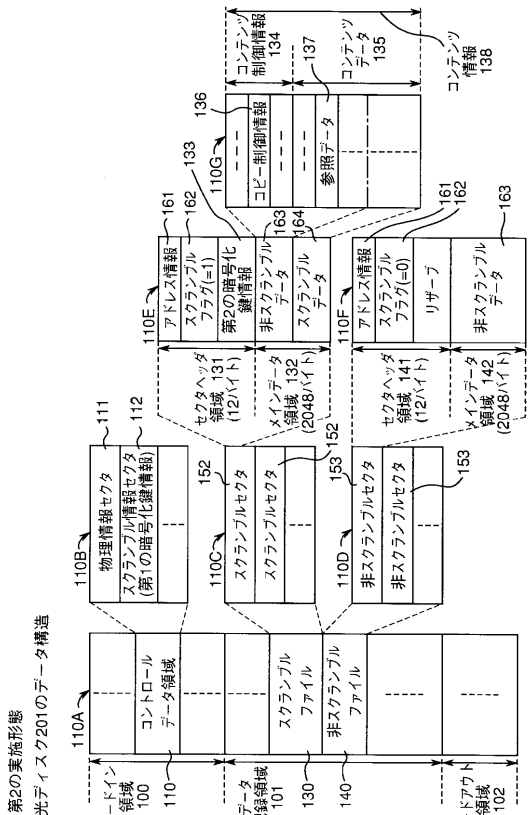
【図３】


光ディスク再生装置 200
光ディスク 201
光学ヘッド 203
スピンドルモータ 202
ヘッドアンプ 204
アナログ処理部 205
光ディスクコントローラ 206
誤り訂正用メモリ 207
デスクランブル回路 208
AV信号処理用メモリ 210
AVデコーダ 209
サーボ制御部 211
CPU 212
CPUバス 213
映像出力信号
音声出力信号

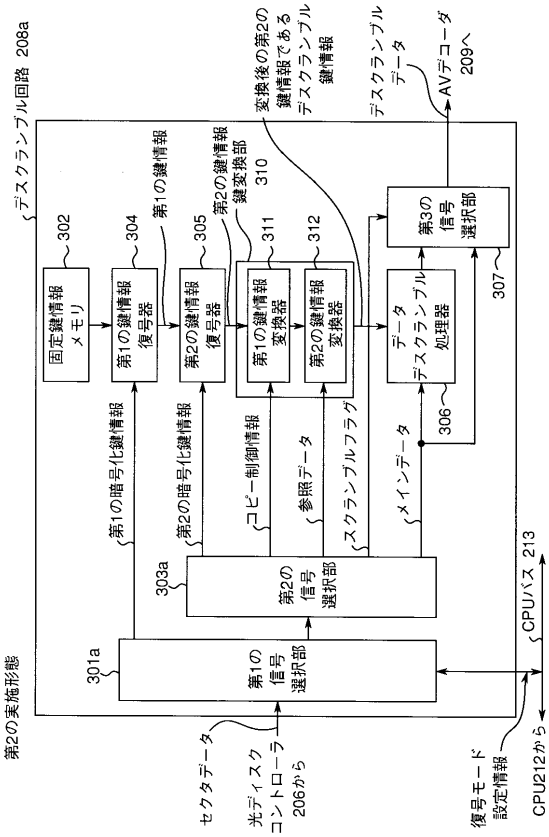
【図４】


第1の実施形態
デスクランブル回路 208
固定鍵情報メモリ 302
第1の鍵情報復号器 304
第2の鍵情報復号器 305
第1の鍵情報変換器 311
第2の鍵情報変換器 312
鍵変換部 310
第1の鍵情報
第2の鍵情報
変換後の第2の鍵情報であるデスクランブル鍵情報
デスクランブルデータ
AVデコーダ 209へ
第3の信号選択部 307
データデスクランブル処理器 306
第2の信号選択部 303
第1の信号選択部 301
第2の暗号化鍵情報
第1の暗号化鍵情報
鍵情報
コピー制御情報
参照データ
スクランブルフラグ
メインデータ
CPUバス 213
セクタデータ
光ディスクコントローラ 206から
復号モード設定情報
CPU212から

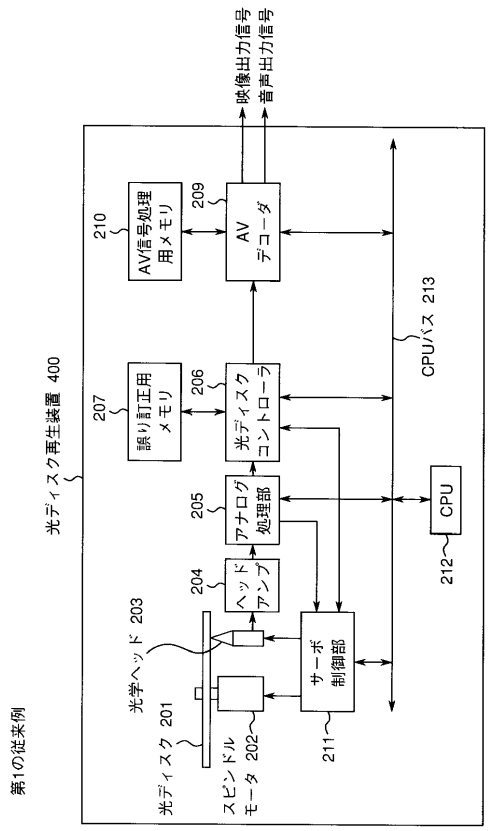
【図５】


第2の実施形態
光ディスク201のデータ構造
リードイン領域 100
コントロールデータ領域 110
データ記録領域 101
スクランブルファイル 130
非スクランブルファイル 140
リードアウト領域 102
110A
110B
物理情報セクタ
スクランブル情報セクタ（第1の暗号化鍵情報）
111
112
110C
スクランブルセクタ
152
110D
非スクランブルセクタ
153
セクタヘッダ領域 131（12バイト）
メインデータ領域 132（2048バイト）
セクタヘッダ領域 141（12バイト）
メインデータ領域 142（2048バイト）
110E
アドレス情報
スクランブルフラグ(=1)
第2の暗号化鍵情報
161
162
133
110G
非スクランブルデータ
163
スクランブルデータ
164
110F
アドレス情報
スクランブルフラグ(=0)
リザーブ
非スクランブルデータ
コピー制御情報
136
参照データ
137
コンテンツ制御情報 134
コンテンツデータ 135
コンテンツ情報 138

【図６】


第2の実施形態
デスクランブル回路 208a
固定鍵情報メモリ 302
第1の鍵情報復号器 304
第1の鍵情報
第2の鍵情報復号器 305
第2の鍵情報
第1の鍵情報変換器 311
第2の鍵情報変換器 312
第2の鍵情報変換部 310
変換後の第2の鍵情報であるデスクランブル鍵情報
デスクランブルデータ
AVデコーダ 209へ
データデスクランブル処理器 306
第3の信号選択部 307
第1の暗号化鍵情報
第2の暗号化鍵情報
コピー制御情報
参照データ
スクランブルフラグ
メインデータ
第2の信号選択部 303a
第1の信号選択部 301a
CPUバス 213
セクタデータ
光ディスクコントローラ 206から
復号モード設定情報
CPU212から

【図７】


第1の従来例
光ディスク再生装置 400
映像出力信号
音声出力信号
AV信号処理用メモリ 210
AVデコーダ 209
誤り訂正用メモリ 207
光ディスクコントローラ 206
CPUバス 213
アナログ処理部 205
CPU 212
ヘッドアンプ 204
光学ヘッド 203
サーボ制御部 211
光ディスク 201
スピンドルモータ 202

フロントページの続き

(72)発明者　福島　能久
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　横田　薫
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

審査官　鶴谷　裕二

(56)参考文献　特開平０９－３２６１６６（ＪＰ，Ａ）
特開平０７－２８８７９８（ＪＰ，Ａ）
特開平０６－０６２４０２（ＪＰ，Ａ）
国際公開第９７／０１４１４７（WO，Ａ１）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G11B 20/10
H04L 9/08