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

特許第4394250号
(P4394250)

(45)発行日　平成22年1月6日(2010.1.6)　(24)登録日　平成21年10月23日(2009.10.23)

(51)Int.Cl.		F I		
G11B 7/004	(2006.01)	G11B	7/004	C
G11B 7/24	(2006.01)	G11B	7/24	522Z
G11B 20/10	(2006.01)	G11B	7/24	538P
G11B 20/12	(2006.01)	G11B	7/24	538G
H04L 9/08	(2006.01)	G11B	7/24	571A

請求項の数 7　(全 65 頁)　最終頁に続く

(21)出願番号　特願2000-125933 (P2000-125933)
(22)出願日　平成12年4月26日 (2000.4.26)
(65)公開番号　特開2001-189015 (P2001-189015A)
(43)公開日　平成13年7月10日 (2001.7.10)
審査請求日　平成19年2月22日 (2007.2.22)
(31)優先権主張番号　特願平11-122104
(32)優先日　平成11年4月28日 (1999.4.28)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願平11-128197
(32)優先日　平成11年5月10日 (1999.5.10)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願平11-299635
(32)優先日　平成11年10月21日 (1999.10.21)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
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　100098280
弁理士　石野　正弘
(72)発明者　永井　隆弘
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】光ディスク、光ディスク記録装置及び光ディスク再生装置

(57)【特許請求の範囲】

【請求項１】

周方向にストライプ状に形成され、反射光量が低下した信号が断続的に得られる領域を備えた第１の領域と、

光ビームを第２の領域に照射することによりユーザがユーザデータを記録可能な第２の領域とを備えた光ディスクであって、

上記第１の領域は、上記第２の領域に対して径方向の所定間隔を有するように離れて形成され、

上記第１の領域に凹凸ピットの形式で記録されたデータと同じデータが、凹凸ピットの形式で上記第２の領域と上記第１の領域の間にも連続して繰り返し記録され、

前記周方向にストライプ状に形成され反射光量が低下した信号が断続的に得られる領域は、位相符号化変調されたデータが前記第１の領域の凹凸ピットに重ねて記録されたことにより形成されたことを特徴とする光ディスク。

【請求項２】

前記位相符号化変調されたデータには、同期コードとエラー検出コードとエラー訂正コードが付加されていることを特徴とする請求項１記載の光ディスク。

【請求項３】

上記第２の領域の内側に形成されたリードイン領域を備え、

上記リードイン領域は上記第１の領域の少なくとも一部を含むことを特徴とする請求項１又は２記載の光ディスク。

【請求項４】
上記第２の領域は書き換え可能な領域であることを特徴とする請求項１から３のいずれかに記載の光ディスク。
【請求項５】
上記第２の領域は追記可能な領域であることを特徴とする請求項１から３のいずれかに記載の光ディスク。
【請求項６】
請求項１～５のいずれか１項に記載された光ディスクに情報を記録することを特徴とする光ディスク記録装置。
【請求項７】
請求項１～５のいずれか１項に記載された光ディスクから情報を再生することを特徴とする光ディスク再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、著作権を有する映画の画像データや音楽の音声データを含むＡＶデータ（Audio and Visual Data）などのデータが記録されている光ディスクから、他の記録型光ディスクなどの記録媒体への不正なディジタルコピーを防止することができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法、及び情報処理システムに関する。
【０００２】
【従来の技術】
光ディスクは、従来のテープメディアに比べてランダムアクセス性に優れており、また、レーザ光を利用した非接触な記録及び再生が可能なため繰り返し利用による劣化が少ないという特徴を有している。さらに、光ディスクは、ディスク製造者によるマスタリングによって、安価に大量の複製が可能という特徴を有しており、高音質のディジタルオーディオとしてＣＤ（Compact Disk）が従来のアナログ記録のレコードにとって代わって一般的になっている。さらに、近年、高品質の画像データがディジタル記録されたＤＶＤ（Digital Video Disk、又はDigital Versatile Disk）が商品化されＡＶデータのディジタル記録媒体としての光ディスクが今後さらに発展していくことが予想される。
【０００３】
一方、音楽ＣＤ、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭのように、ディスク製造業者によってデータがプリピットの形式で予め記録されている再生専用の光ディスクだけでなく、近年、ユーザが家庭でＡＶデータを記録できる、例えば、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＭＯ、ＭＤやＤＶＤ－ＲＡＭなどの記録型の光ディスクが開発され、世に広がりつつある。
【０００４】
また、テレビ放送においても従来のアナログ方式から多チャンネル化や様々なサービスが可能なディジタル方式が導入されており、このような傾向は今後さらに広がっていく。特に、記録型光ディスクは、ディジタル化された放送や通信で配信されてくるコンテンツの記録媒体として、配信時に蓄積した後プログラム選択して視聴するタイムシフト利用を目的の中心としたＡＶデータの記録に利用されることが予想される。
【０００５】
従来、コンピュータを中心に利用されてきた記録型の光ディスクは、利用者自らが作成したデータの保存を目的として利用されており、記録型の光ディスク間でのコピーを制限する仕組みを有していなかった。記録型の光ディスクが広く利用されるようになると、記録された光ディスクのデータを、一般ユーザがそのまま他の記録型光ディスクに違法にコピーすることにより、本来そのＡＶデータの著作者に支払われるべき著作料を払うこと無しに、また、ディジタル記録が可能なことから音質や画質の劣化なしに不当な複製を入手することが可能になり、良質のコンテンツの広まりを阻害する要因にもなってきている。音

楽等をディジタル記録するＭＤでは、記録回数を制限する世代管理を行う仕組みが導入され、世代管理データとともに光ディスクに記録し、その世代管理データによりコピー回数の制限を行っている。

【０００６】

また、例えば、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭの不正なコピーを防止するために、光ディスクのピット部にバーコードを重ね書きするための追記領域であるバーストカッティング領域（Burst Cutting Area；以下、ＢＣＡという。）を設け、光ディスクの製造時にＢＣＡにディスク毎に異なるＩＤを記録しておく方法が、国際公開番号ＷＯ９７／１４１４４号の国際出願において提案されている。この方法によると、パスワードはディスクＩＤにより異なるので、１つのパスワードは１枚のディスクの暗号しか解読することができなくなり、コンテンツが不正にコピーされてもディスクＩＤの情報が欠落しているため、コンテンツは解読されなくなる。

【０００７】

図３９は、従来技術のＤＶＤ－ＲＯＭのユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。ＤＶＤ－ＲＯＭでは、図３９に示すように、ディスク上に記録するコンテンツのデータに対して暗号化を行っている。

【０００８】

図３９において、ＤＶＤ－ＲＯＭのユーザデータ領域は、セクタヘッダ領域３２０１と、メインデータ領域３２０２と、誤り検出コード３２０３とから構成される。ここで、セクタヘッダ領域３２０１には、セクタの位置を示すセクタアドレス３２０４と、メインデータ領域３２０２に記録されるデータに関する著作権制御情報（例えば、スクランブルフラグ、コピー制御情報など）が記録される著作権制御情報３２０５と、メインデータ領域３２０２のデータに暗号が施されている場合に復号するための復号鍵３２０６とが記録される。また、メインデータ領域３２０２には、主に著作権保護を必要とするＡＶデータなどが暗号化されて記録される。

【０００９】

このようなユーザデータ領域の再生時には、まず、セクタヘッダ領域３２０１から暗号化コンテンツの再生に必要な復号鍵３２０６を得る。取得した復号鍵３２０６は鍵復号器３２０７に入力され、鍵復号器３２０７は入力された復号鍵３２０６を所定のディスク鍵を用いてコンテンツ復号鍵を復号して、復号器３２０８に出力する。次いで、復号器３２０８は、メインデータ領域３２０２に対応するセクタヘッダ領域３２０１に格納された著作権制御情報３２０５に従って、メインデータ領域３２０２の暗号化コンテンツを上記復号されたコンテンツ復号鍵を用いて復号を行い、再生可能なデータである復号化コンテンツを得る。

【００１０】

図３９に示した構成による光ディスクでは、パーソナルコンピュータのドライブ装置などからメインデータ領域３２０２に対する読み出しが可能であるが、復号鍵３２０６を記録した領域を正規の認証機能を有する光ディスク再生装置しか読み出しできないように構成することにより、不正な複製や海賊版の作成を防止できるようにしている。

【００１１】

【発明が解決しようとする課題】

しかしながら、世代管理データを用いた不正コピー防止方法では、コピー時に世代管理データの変更（“１回コピー可能”から“コピー不可”への情報の変更“）が不可欠である。これに対して、光ディスク上のデータを世代管理データとともに変更を加えずコピーしたり、コンピュータ等で世代管理データを改ざんして記録したりすることにより、不正コピーを十分に防止できないという問題点を有していた。さらに、コンテンツとともに予め記録した世代管理データによりコピー回数の制限を行うため、たとえ正規の著作料を払ったとしても光ディスク上の“コピー不可”となったデータは他の光ディスクへのコピーが全く許されず、利用者はコンテンツ供給者から供給を待たなければならないという問題を

有していた。いずれもコンテンツ供給者が利用者の行う記録型光ディスクへのコピーを十分に管理できないことによるものである。

【００１２】

近年、パーソナルコンピュータが高性能化し、さらにそれらがネットワークに接続されることによって、高性能でかつ、複数台のパーソナルコンピュータによる高速な暗号の解読が行われている。このような解読に対して、より暗号の強度を高めるためには、暗号に使用する鍵の鍵長を拡張することが必要となる。しかしながら、従来から提案されているようなセクタヘッダに復号鍵を記録するような鍵管理方法では、予め決められた長さ（復号鍵領域のサイズ）以下の復号鍵しか記録することができず、将来に暗号の強度を高めるために鍵長を長くできないという問題点があった。

【００１３】

本発明の第１の目的は、以上の問題点を解決し、コンテンツ供給者が管理できない不正なディジタルコピーを防止できる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１４】

また、本発明の第２の目的は、以上の問題点を解決し、著作権保護を必要とするデータを復号化するために必要な復号鍵の信頼性をより高めることができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１５】

さらに、本発明の第３の目的は、以上の問題点を解決し、記録するコンテンツの著作権保護のレベルに応じて暗号強度の設定することができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１６】

【課題を解決するための手段】

本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、
データを記録して再生するデータ記録再生領域と、
上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域とを含むことを特徴とする。

【００１７】

上記光ディスクにおいて、上記ディスク識別情報は、好ましくは、上記光ディスク上の反射膜をストライプ状に除去することにより形成される。また、上記光ディスクにおいて、上記ディスク識別情報は、好ましくは、各光ディスク毎に固有なディスク識別子を含む。

【００１８】

また、上記光ディスクにおいて、上記データ記録再生領域は、好ましくは、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータを記録する領域を含む。上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、画像データと音楽データとのうちの少なくとも一方であるコンテンツのデータを含む。また、上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。さらに、上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含む。

【００１９】

本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、
上記光ディスクは、データを記録して再生するデータ記録再生領域を含み、

上記データ記録再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを記録する領域を含むことを特徴とする。

【００２０】

上記光ディスクにおいて、好ましくは、上記コンテンツのデータと、上記デスクランブルキーは、同一のセクタ内に記録され、もしくは、上記コンテンツのデータと、上記デスクランブルキーは異なるセクタに記録される。また、上記光ディスクにおいて、好ましくは、上記コンテンツが記録されたセクタに、上記デスクランブルキーが記録される領域を示すポインタを記録する。

【００２１】

本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、
上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域と、
暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータを記録して再生するデータ記録再生領域と、
上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとを記録するキー管理情報領域とを含むことを特徴とする。

【００２２】

本発明に係る光ディスク記録再生装置は、データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生装置であって、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域から上記ディスク識別情報を再生する再生手段と、
上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御する制御手段とを備えたことを特徴とする。

【００２３】

本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、
上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録する記録手段とを備えたことを特徴とする。

【００２４】

上記光ディスク記録装置において、上記暗号化されたデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。また、上記光ディスク記録装置において、上記暗号化されたデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含む。

【００２５】

本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、

少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化する復号化手段とを備えたことを特徴とする。

【００２６】

上記光ディスク再生装置において、上記復号化されるデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。また、光ディスク再生装置において、上記復号化されるデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含み、上記復号化手段は、上記デスクランブルキーに含まれる誤りを、上記誤り検出コードに基づいて検出する。

【００２７】

本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、

暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録する記録手段を備えたことを特徴とする。

【００２８】

上記光ディスク記録装置において、上記記録手段は、好ましくは、上記暗号化されたコンテンツのデータを所定の第１のセクタに記録し、上記デスクランブルキーを上記第１のセクタとは異なる第２のセクタに記録する。また、上記光ディスク記録装置において、上記記録手段は、好ましくは、上記暗号化されたコンテンツのデータが記録された第１のセクタに、上記デスクランブルキーが記録された第２のセクタ内の領域を示すポインタを記録する。

【００２９】

本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、

暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生する再生手段を備えたことを特徴とする。

【００３０】

上記光ディスク再生装置において、上記再生手段は、好ましくは、上記暗号化されたコンテンツを上記光ディスクの第１のセクタから再生し、上記デスクランブルキーを上記第１のセクタとは異なる第２のセクタから再生する。上記光ディスク再生装置において、上記再生手段は、好ましくは、上記暗号化されたコンテンツのデータが記録された第１のセクタから、上記デスクランブルキーが再生される第２のセクタ内の領域を示すポインタを再生する。

【００３１】

本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録装置であって、

記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得する取得手段と、

上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てる割当手段とを備えたことを特徴とする。

【００３２】

本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録装置であって、

コンテンツのデータを再生するために必要なデスクランブルキーを取得する取得手段と、

上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録する記録手段とを備えたことを特徴とする。

【００３３】

本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、

上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるか否かを判断する判断手段と、

上記コンテンツのデータを上記光ディスクに記録することができると判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てる割当手段と、

記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録する記録手段とを備えたことを特徴とする。

【００３４】

本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディスク再生装置であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記キー管理情報領域のデータを再生する第１の再生手段と、

上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているか否かを判断する判断手段と、

上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生する第２の再生手段と、

上記ディスク識別情報領域からディスク識別情報を再生する第３の再生手段と、

上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生する復号化手段とを備えたことを特徴とする。

【００３５】

上記光ディスク再生装置において、好ましくは、上記復号化されたデスクランブルキーに、誤り検出コードが付与され、上記復号化手段は、上記復号化されたデスクランブルキーに付与された誤り検出コードに基づいて、上記復号化されたデスクランブルキーにおける誤りの有無を判断し、上記判断結果に基づいて、上記復号化されたデスクランブルキーを再生するか否かを判断する。

【００３６】

本発明に係る光ディスク記録再生方法は、データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生方法であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域から上記ディスク識別情報を再生するステップと、

上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御するステップとを含むことを特徴とする。

【００３７】
本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域からディスク識別情報を再生するステップと、
上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録するステップとを含むことを特徴とする。
【００３８】
本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域からディスク識別情報を再生するステップと、
少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化するステップとを含むことを特徴とする。
【００３９】
本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、
暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録するステップを含むことを特徴とする。
【００４０】
本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、
暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生するステップを含むことを特徴とする。
【００４１】
本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録方法であって、
記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得するステップと、
上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てるステップとを含むことを特徴とする。
【００４２】
本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録方法であって、
コンテンツのデータを再生するために必要なデスクランブルキーを取得するステップと、
上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録するステップとを含むことを特徴とする。
【００４３】
本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生するステップと、
上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるか否かを判断するステップと、
上記コンテンツのデータを上記光ディスクに記録することができると判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てるステップと、
記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録するステップとを含むことを特徴とする。

【００４４】

本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディスク再生方法であって、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記キー管理情報領域のデータを再生するステップと、
上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているか否かを判断するステップと、
上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生するステップと、
上記ディスク識別情報領域からディスク識別情報を再生するステップと、
上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生するステップとを含むことを特徴とする。

【００４５】

本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、
第１のディスク情報を記録する第１の情報領域と、
各光ディスクを識別するための第２のディスク情報を記録する第２の情報領域と、
光ビームを当該領域に照射することにより情報データを記録するユーザデータ領域とを含むことを特徴とする。

【００４６】

上記光ディスクにおいて、上記第２のディスク情報は、好ましくは、上記第２の情報領域内の記録膜を、半径方向に長い形状でかつ複数個の領域において部分的に除去することにより記録される。また、上記光ディスクにおいて、好ましくは、上記第２の情報領域は、上記第１の情報領域内に配置され、又は、上記第１の情報領域の内周側に配置され、もしくは、上記第２の情報領域は、上記第１の情報領域内の一部の領域と、上記第１の情報領域よりも内周側に位置する別の領域とにわたって配置される。さらに、上記第１のディスク情報は、好ましくは、微少な凹凸ピットの形式で記録される。

【００４７】

本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、
上記光ディスクは、複数のセクタを備えたセクタ構造を有し、
上記各セクタは、セクタヘッダ領域と、暗号化されたデータを記録するメインデータ領域とを含み、
上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも１つの復号鍵を記録する復号鍵情報領域を含み、
上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする。

【００４８】

上記光ディスクにおいて、上記各復号鍵は、好ましくは、所定のサイズを有する複数の分割復号鍵に分割され、上記複数の分割復号鍵は、連続する複数のセクタの各復号鍵情報領域に記録される。ここで、上記復号鍵の分割数は、好ましくは、エラー訂正に必要な複数

のセクタである誤り訂正コード（ＥＣＣ）ブロックに含まれるセクタ数の約数である。また、上記光ディスクにおいて、上記各復号鍵は、好ましくは、複数の復号鍵を有する復号鍵テーブルに記録され、上記暗号化されたデータを復号化するために必要な復号鍵の、上記復号鍵テーブル内の記録位置を示すインデックスは、上記セクタの復号鍵情報領域に記録される。さらに、上記光ディスクにおいて、上記復号鍵テーブルの記録状態を表す情報として、好ましくは、上記復号鍵テーブルの各復号鍵領域に対する復号鍵状態を記録した復号鍵状態領域が記録される。またさらに、上記光ディスクにおいて、上記復号鍵テーブルは、好ましくは、異なる複数の誤り訂正コード（ＥＣＣ）ブロックにわたって記録される。また、上記光ディスクにおいて、上記各復号鍵は、好ましくは、ファイル管理領域で管理されるファイル単位と、光ディスク上で連続する複数のセクタからなるエクステント単位とのうちの少なくとも一方の単位で管理されて記録される。

【００４９】

本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、
上記光ディスクは、データを記録するメインデータ領域を含み、
上記メインデータ領域は、データを非暗号化状態で記録する非暗号化領域と、
データを暗号化状態で記録する暗号化領域とを含み、
上記非暗号化領域は、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含み、
上記暗号化領域のデータは、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする。

【００５０】

上記光ディスクにおいて、好ましくは、上記メインデータ領域は、データの再生制御のために用いられる制御情報を非暗号化状態で記録する制御情報記録セクタと、データを暗号化状態で記録するデータ記録セクタとを含み、
上記制御情報記録セクタは、上記復号鍵の変換のために用いられる復号鍵変換データを含み、
上記データ記録セクタのデータは上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化される。
また、上記光ディスクにおいて、好ましくは、上記データ記録セクタは、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、
上記非暗号化領域は別の復号鍵変換データを含み、
上記暗号化領域のＡＶデータは上記復号鍵変換データを用いて変換された復号鍵をさらに別の第２の復号鍵変換データを用いて変換された復号鍵を用いて暗号化される。
さらに、上記光ディスクにおいて、上記復号鍵変換データは、好ましくは、少なくともデータのコピー制御情報を含む。

【００５１】

本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクにデータを記録するための光ディスク記録方法において、
上記光ディスク上に記録された復号鍵ステータスを読み出し、上記読み出された復号鍵ステータスに基づいて復号鍵の空き領域があるか否かを判断するステップと、
上記復号鍵の空き領域があると判断されたときに、復号鍵領域を予約して復号鍵を記録するステップと、
ファイル単位とエクステント単位のうちの少なくとも一方の単位で著作権制御情報と復号鍵インデックスを設定するステップと、
上記復号鍵を用いてデータを暗号化して、暗号化されたデータを、ファイル単位とエクステント単位のうちの少なくとも一方の単位で上記光ディスクに記録するステップと、
上記光ディスクに記録されたデータを管理するためのファイル管理情報を上記光ディスクに記録するステップとを含むことを特徴とする。

【００５２】

本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクか

らデータを再生するための光ディスク再生方法において、
ファイル単位又はエクステント単位で記録された再生すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、
上記取得された復号鍵インデックスに対応する復号鍵を再生して取得するステップと、
上記復号鍵を用いて暗号化されたファイル単位又はエクステント単位のデータを再生するステップとを含むことを特徴とする。

【００５３】

本発明に係る光ディスク削除方法は、データを記録することができる記録型光ディスクからデータを削除するための光ディスク削除方法において、
ファイル単位又はエクステント単位で記録された削除すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、
上記取得された復号鍵インデックスに対応し、復号鍵の記録状態を示す復号鍵ステータスを更新して復号鍵を開放するステップと、
上記光ディスクに記録されたデータを管理するためのファイル管理情報から上記削除すべきデータに対応するファイルエントリを削除することにより上記ファイル管理情報を更新するステップとを含むことを特徴とする。

【００５４】

本発明に係る情報処理システムは、データを暗号鍵を用いて暗号化するデータ暗号化装置と、
上記データを復号化するために必要な復号鍵を記録型光ディスクに記録して再生する光ディスク記録再生装置と、
上記光ディスク記録再生装置及び上記データ暗号化装置に接続された制御装置とを備えた情報処理システムであって、
上記光ディスク記録再生装置は、
上記光ディスクに復号鍵テーブルを記録し、上記光ディスクから復号鍵テーブルを再生する第１の記録再生手段と、
上記復号鍵を暗号化して上記制御装置に送信し、上記制御装置から暗号化された復号鍵を受信して復号化する暗号化及び復号化手段と、
上記光ディスクに復号鍵の記録状態を示す復号鍵状態テーブルを記録し、上記光ディスクから復号鍵状態テーブルを再生する第２の記録再生手段とを備え、
上記データ暗号化装置は、
上記復号鍵を暗号化して上記制御装置に送信する暗号化手段を備え、
上記制御装置は、
上記データ暗号化装置の暗号化手段から暗号化された復号鍵を受信する受信手段と、
上記再生された復号鍵状態テーブルに基づいて復号鍵の空き領域を検索し、上記検索された空き領域に、上記受信された暗号化された復号鍵を割り当て、上記割り当てられた暗号化された復号鍵を上記光ディスク記録再生装置に送信する割当手段とを備え、
上記光ディスク記録再生装置の暗号化及び復号化手段は、上記制御装置の割当手段から上記割り当てられた暗号化された復号鍵を受信して復号化することを特徴とする。

【００５５】

本発明に係る情報処理システムは、データと、上記データを復号化するために必要な複数の復号鍵を備えた復号鍵テーブルを記録型光ディスクから再生する光ディスク再生装置と、
上記光ディスク再生装置に接続された制御装置と、
復号鍵を用いてデータを復号化するデータ復号化装置とを備えた情報処理システムであって、
上記光ディスク再生装置は、
上記光ディスクから復号鍵テーブルを再生する第１の再生手段と、
上記再生された復号鍵テーブルを暗号化して、暗号化された復号鍵テーブルを上記制御装置に送信する暗号化手段と、

上記光ディスクから複数の復号鍵の記録状態を示す復号鍵状態テーブルを再生する第２の再生手段とを備え、
上記制御装置は、
上記光ディスク再生装置から上記暗号化された復号鍵テーブルを受信する受信手段と、
上記再生された復号鍵状態テーブルに基づいて、上記受信された復号鍵テーブルから上記光ディスクに記録されたデータを復号化するために必要な暗号化された復号鍵を検索して上記データ復号化手段に送信する検索手段とを備え、
上記データ復号化装置は、
上記暗号化された復号鍵を復号化して復号鍵を生成する第１の復号化手段と、
光ディスク再生装置によって再生された暗号化されたデータを、上記復号化された復号鍵を用いて復号化する第２の復号化手段とを備えたことを特徴とする。

【００５６】

本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクにデータを記録する光ディスク記録装置において、
上記光ディスクは、非暗号化領域と、暗号化領域とを含み、
データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録する記録手段を備えたことを特徴とする。

【００５７】

上記光ディスク記録装置において、好ましくは、上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、
上記記録手段は、上記データの再生制御のために用いられる制御情報を上記制御情報記録セクタに非暗号化状態で記録し、上記制御情報に含まれる復号鍵変換データを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録する。
また、上記光ディスク記録装置において、上記記録手段は、好ましくは、別の復号鍵変換データを含むデータを非暗号化状態で上記データ記録セクタの非暗号化領域に記録し、上記制御情報に含まれる復号鍵変換データと、上記別の復号鍵変換データとを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録する。

【００５８】

本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからデータを再生する光ディスク再生装置において、
上記光ディスクは、非暗号化領域と、暗号化領域とを含み、
上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生する再生手段を備えたことを特徴とする。

【００５９】

上記光ディスク再生装置において、好ましくは、上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、
上記再生手段は、上記データの再生制御のために用いられる制御情報を制御情報記録セクタから再生し、上記制御情報に含まれる復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記データ記録セクタに記録されたデータを復号化して再生する。
また、上記光ディスク再生装置において、上記再生手段は、好ましくは、上記データ記録セクタの非暗号化領域に記録された別の復号鍵変換データを再生し、上記制御情報に含まれる復号鍵変換データと、上記再生された別の復号鍵変換データとを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記データ記録セクタに記録されたデータを復号化して再生する。

【００６０】
本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクにデータを記録する光ディスク記録方法において、
上記光ディスクは、非暗号化領域と、暗号化領域とを含み、
データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録するステップを含むことを特徴とする。
【００６１】
本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからデータを再生する光ディスク再生方法において、
上記光ディスクは、非暗号化領域と、暗号化領域とを含み、
上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生するステップを含むことを特徴とする。
【００６２】
本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、
データが記録されたデータ再生領域と、
上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域とを含み、
上記データ再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータが記録された領域を含むことを特徴とする。
【００６３】
本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、
上記光ディスクは、データが記録されたデータ再生領域を含み、
上記データ再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとが記録された領域を含むことを特徴とする。
【００６４】
本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、
上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域と、
暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータが記録されたデータ再生領域と、
上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとが記録されたキー管理情報領域とを含むことを特徴とする。
【００６５】
本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、
上記光ディスクは、複数のセクタを備えたセクタ構造を有し、
上記各セクタは、セクタヘッダ領域と、暗号化されたデータが記録されたメインデータ領域とを含み、
上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも１つの復号鍵が記録された復号鍵情報領域を含み、
上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする。
【００６６】

【発明の実施の形態】
以下、図面を参照して本発明に係る実施形態について説明する。
【００６７】
＜第１の実施形態＞
図１は、本発明に係る第１の実施形態である記録型光ディスク１００のデータ記録領域を示す平面図である。この記録型光ディスク１００は、ディジタルデータを記録することが可能な記録媒体であって、追記型光ディスクと、書き換え型光ディスクを含む。
【００６８】
図１において、１０１は光ディスク１００の管理情報が記録されたリードイン領域、１０２は映画などの画像データ（静止画及び動画を含む。）や音楽などの音声データの少なくとも一方を含むＡＶデータのコンテンツや、コンピュータのソフトウェアなどの、著作権保護が必要なディジタルデータが記録されるユーザデータ領域、１０３は欠陥管理情報等が記録されるリードアウト領域である。リードイン領域１０１は、プリピットの形で記録された再生専用領域１０４と、ガイド溝を有する書き換え可能領域である記録再生領域１０５により構成される。ここで、再生専用領域１０４には、光ディスク１００の物理特性を記述したコントロール領域などが製造業者によりプリピットの形式で記録される。リードアウト領域１０３や書き換え可能領域１０５には、光ディスク記録装置による書き込みテストのためのデータや光ディスク１００上の欠陥を管理するための管理情報などが光ディスク記録装置により記録される。さらに、リードイン領域１０１の再生専用領域１０４の内周側には、ディスク個別情報としてＢＣＡ１０６は、以下に示すように公知の方法で、コンテンツが記録された光ディスク１００が完成した後に、光ディスク１００に追記される。
【００６９】
図２（ａ）は図１の光ディスク１００のＢＣＡ１０６を形成するときの装置構成を示すブロック図及び縦断面図であり、図２（ｂ）は図１の光ディスク１００のＢＣＡ１０６を形成した後の光ディスク１００の縦断面図及びその水平方向に対する反射光の強度を示すグラフである。図２（ａ）及び図２（ｂ）では、両面記録型の光ディスク１００の例を示しており、光ディスク１００は、２つの基板２０１，２０７の間に、記録層２０２、反射層２０３、接着層２０４、反射層２０５及び記録層２０６が挿入されて構成される。
【００７０】
ＢＣＡを光ディスク１００に記録するときにおいては、図２（ａ）に示すように、高パワーレーザ光源２１１からのレーザ光をフォーカスレンズ２１２を介して、例えば光ディスク１００の反射層２０５にパルス状に照射して一部の反射層２０５を除去することにより、位相符号化変調（phase encoding modulation）したストライプ状のデータをピットに重ねて記録する。再生時には、図２（ｂ）に示すように、反射層２０５が除去されている部分で反射光量が低下した信号が断続的に再生され、再生された信号を２値化した後、位相符号化復調（phase encoding demodulation）することにより、ＢＣＡのデータを再生する。このような記録方式により作成されたＢＣＡは、各光ディスク１００毎に固有な情報であるディスク識別子を記録することができ、さらに改ざんすることが不可能であるなどの特徴を有する。
【００７１】
図３は、図１のＢＣＡ１０６の記録フォーマットを示す図である。図３に示すように、ＢＣＡ１０６には、同期コード３０１、エラー検出コード３０２、エラー訂正コード３０３などがＢＣＡデータ３０４の読み取り率を改善するために記録される。これらの複数のＢＣＡデータ３０４を連結することによって、ディスク識別情報３０５が構成される。ディスク識別情報３０５には、ユーザデータ領域へ記録可能なデータの種別の種別、ユーザデータ領域から再生可能なデータの種別が記録される。ＢＣＡ１０６のデータは改ざんが不可能であるため、光ディスク１００の製造時に記録されるディスク識別情報により利用者のディスク使用に一定の制限を与えることができる。
【００７２】

図４は、図１のユーザデータ領域１０２内のセクタデータ４０１のセクタ構造を示す図である。図４において、図１のユーザデータ領域１０２は、一定量の単位でアクセス可能なセクタ構造を有しており、そのセクタデータ４０１は、ヘッダ４０２、メインデータ４０３、エラー検出コード４０４により構成される。

【００７３】

ここで、メインデータ４０３は、ＡＶデータやコンピュータのデータなどが記録される領域である。また、ヘッダ４０２には、データＩＤ（Data Identifier）４０５、ＩＤエラー検出コード４０６、スクランブル制御情報４０７、キー情報４０８などが記録される。データＩＤ４０５には、セクタを識別するための論理アドレスなどが記録され、ＩＤエラー検出コード４０６はデータＩＤのエラー検出するためのコードである。また、スクランブル制御情報４０７は、メインデータにスクランブルが施されているか否かを示すフラグであり、キー情報４０８はメインデータをデスクランブルするためのキーに関する情報が記録される。キーに関する情報としては、デスクランブルキーそのもの（第１の実施形態の変形例）や、光ディスク１００上の別領域に記録したデスクランブルキーへのポインタであるキーインデックス（第１の実施形態）が記録される。図４の例では、光ディスク１００上の別領域である図１のキー管理情報領域１０７に記録したデスクランブルキーを参照するためのキーインデックスが記録されている場合を示している。

【００７４】

図５は、図１のキー管理情報領域１０７の構成を示す図である。図５において、キー管理情報領域１０７は、キー情報領域５０１と、コンテンツ情報領域５０２と、キーインデックスリスト領域５０３とから構成される。

【００７５】

キー情報領域５０１には、使用済みのデスクランブルキー領域の数５０４が記録されるとともに、キー情報領域５０１は、ＡＶデータ等に施されたスクランブルを解くためのデスクランブルキーを記録する領域であるデスクランブルキー領域５０５と、デスクランブルキー領域５０５に記録されるデスクランブルキーの記録状態（未使用、領域予約済、記録済などを示す。）を記録するキーステータス領域５０６とを含む。デスクランブルキー領域５０５には複数のデスクランブルキーが記録され、デスクランブルキー領域５０５中での格納位置を表すキーインデックスがキーインデックスリスト領域５０３に記録され、上記複数のデスクランブルキーは当該キーインデックスにより参照可能である。キーステータス領域５０６には、先のデスクランブルキーの記録状態を表すステータス情報がキーインデックスで参照可能な位置に格納される。

【００７６】

コンテンツ情報領域５０２には、光ディスク１００上に記録されるコンテンツの中で著作権保護が必要なものが登録され、それとともにコンテンツで使用されるキーに関する情報が登録される。コンテンツ情報領域５０２は、キーインデックスリスト領域５０３に登録されるコンテンツ数５０７と、コンテンツ数分のコンテンツ情報５０８が記録される。さらに、コンテンツ情報５０８には、コンテンツを識別するためのコンテンツＩＤと、そのコンテンツで使用されるデスクランブルキーの個数と、使用するキーを記録したキーインデックスリスト５０９へのポインタが記録される。キーインデックスリスト領域５０３は、コンテンツで使用するキーを参照するためのインデックスをコンテンツ単位でのリスト形式で記録する領域である。キーインデックスリスト領域５０３には、コンテンツで使用されている全デスクランブルキーの記録領域を参照するキーインデックスが記録される。

【００７７】

このように構成された記録型光ディスク１００では、書き換えが困難なディスク識別情報にディスクの使用条件を表すような情報として、地域識別子、データカテゴリ識別子、ディスク識別子などを製造時に記録することにより、光ディスク記録再生装置でこれらの情報を検出し、コンテンツが持つ著作権の保護レベルや利用レベルに応じて記録動作及び再生動作を制御することを可能とする。また、書き換えが困難な方法によって記録されており利用者の側での変更ができないため、別の光ディスクに著作権保護されたコンテンツを

コピーした場合でも、ユーザデータ領域はコピー可能であるが、ディスク識別情報はコピーすることはできない。従って、ディスク識別情報を用いてスクランブルしたデータを光ディスク上に記録しておくことで、異なるディスク識別情報を有する光ディスクではデスクランブルできないユーザデータ領域が存在し正しい再生ができない。

【００７８】

図１５（ａ）は第１の実施形態においてコンテンツの記録時に地域識別子を記録する場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図であり、図１５（ｂ）は第１の実施形態において地域識別子が光ディスクの出荷時に予め記録されている場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図である。

【００７９】

例えば、図１５（ａ）に示すように、光ディスクの出荷時に地域識別コードが記録されておらず、コンテンツの記録時にコンテンツが利用可能な地域を表す地域識別子を記録及び再生領域に記録した場合には、他の地域での利用は防止できる。しかしながら、他の地域で使用すべきディスク（図１５（ａ）中の地域ＲＣ２用）にもコンテンツの記録が可能であり、正しくコンテンツの再生が可能である。コンテンツのディジタルコピーが可能な記録媒体では、著作権者の利益を保護するために賦課金制度などが設けられ、光ディスクの販売時に料金に上乗せされて回収されている。しかしながら、上乗せされる賦課金は国毎に異なるため、他の国で使用されるべき記録媒体が不正に利用されると、本来、利益を得るべき著作権者に正しく配分されない可能性が有る。

【００８０】

また、図１５（ｂ）に示すように、地域識別子が光ディスクの出荷時に予め改ざんできない方法により記録しておくことで、他の地域で使用されるべき光ディスクへのコンテンツのコピーや再生を防止することができる。同様に、データカテゴリ識別子をディスク識別情報として記録した場合には、記録するデータが有するカテゴリ識別子と比較することで、データを記録及び再生可能なディスクへのコンテンツのコピーや再生を制限できる。光ディスク毎で固有なディスク識別子をディスク識別情報として記録した場合には、記録するデータをディスク識別子で暗号化するなどして、その光ディスクでのみ利用可能とすることができる。

【００８１】

本実施形態において、ディスク識別情報によってスクランブルされるデータは、著作権保護が必要なＡＶデータやコンピュータデータでもよいし、ＡＶデータやコンピュータデータに施されているスクランブルを解くためのデスクランブルキーでもよい。

【００８２】

図１３は、第１の実施形態の変形例に係る、暗号化デスクランブルキーから正規のデスクランブルキーであるか否かを判定するための方法を示すブロック図である。図１３に示すように、デスクランブルキーに、デスクランブルキーの誤りを検出するための誤り検出コードを付加したデータを、ディスク識別情報を用いてスクランブルすることにより計算した暗号化デスクランブルキーを光ディスクに記録してもよい。光ディスク再生装置では、暗号化デスクランブルキーをデスクランブルキーと誤り検出コードとに復号し、復号された誤り検出コードにおけるパリティチェックなどに基づいて誤り検出することにより復号されたデスクランブルキーが正規のものであるか否かを判定する。例えば、異なるディスク識別情報によってデスクランブルした場合、誤ったデスクランブルキーが生成され、誤り検出コードをチェックすることにより、正規のデスクランブルキーでないことを判定できるので、不正なコピーを検出することができる。

【００８３】

なお、ディスク識別情報を記録する別の方法として複数種類のディスク識別情報をプリピットで作成したスタンパを用意しそれぞれから光ディスクを作成することによって、異なるスタンパから作成される光ディスク毎で異なる利用制限を与えるようにしてもよい。さらに、ディスク識別情報を、秘密鍵を用いてスクランブルしてスクランブルされたディス

ク識別情報を光ディスクに記録しておくことによって、ディスク識別情報に記述される著作権の保護レベルを利用者にわからなくし、その結果、著作権保護がより強化される。

【００８４】

図４において説明したキーに関する情報としてデスクランブルキーそのものを記録した場合（第１の実施形態の変形例）と、ディスク上の別領域に記録したデスクランブルキーへのポインタであるキーインデックスを記録した場合（第１の実施形態）について、図６（ａ）及び図６（ｂ）を参照して説明する。ここで、図６（ａ）は第１の実施形態の変形例に係る、図１のセクタデータ４０１にデスクランブルキー及びＡＶデータを記録する記録方法を示すブロック図であり、図６（ｂ）は第１の実施形態に係る、図１のセクタデータ４０１にデスクランブルキーへのキーインデックス及びＡＶデータを記録する記録方法を示すブロック図である。

【００８５】

図６（ａ）の場合においては、同一のセクタデータ４０１に、メインデータ４０３と、メインデータ４０３をデスクランブルするために必要なキー情報４０８ａであるデスクランブルキーとを記録する。このため、ＡＶデータの記録時には、デスクランブルに必要なデスクランブルキーを取得しておく必要がある。つまり、ＡＶデータの記録時にキーそのものの入手や購入が不可欠である。

【００８６】

一方、図６（ｂ）の場合では、同一のセクタデータ４０１に、メインデータ４０３と、メインデータ４０３をデスクランブルするために必要な情報を記録するデスクランブルキー領域を参照するキー情報４０８であるキーインデックスとを記録し、キーインデックスにて指定される領域にデスクランブルキーを記録する。ＡＶデータの記録時には、記録するコンテンツで使用されるキーの中のどのキーでデータがデスクランブルできるのかを示すキーＩＤを取得し、コンテンツ情報に含まれるキーインデックスリストからキーＩＤに対応するキーインデックスであるキー情報４０８を取得し、メインデータ４０３とともに記録する。デスクランブルキーの記録はデスクランブルキーを入手した際に行われ、キーＩＤに対応するキーインデックスにより示されるデスクランブルキー領域に記録される。この結果、ＡＶデータとそれに対応するデスクランブルキーの記録は独立して行うことができる。つまり、ＡＶデータの記録とキーの入手又は購入は独立に行うことができ、ＡＶデータの記録時にキーの入手又は購入は必ずしも必要でなくなる。利用者はコンテンツを記録しておいて、実際に再生する際にキーを入手するという利用法が可能となる。

【００８７】

図１４は、第１の実施形態の変形例に係る、デスクランブル領域管理テーブルの構成を示す図である。以上の実施形態においては、暗号化されたコンテンツとその暗号を解くためのデスクランブルキーを関連付けるために、同一セクタデータ４０１にデスクランブルキーを参照するためのキーインデックスを記録する場合について説明したが、暗号化されたコンテンツが記録されるセクタのアドレス範囲とデスクランブルキーとの対応関係を管理する図１４のデスクランブル領域管理テーブルを用いてもよい。このデスクランブル領域管理テーブルでは、暗号化されたコンテンツが記録されるセクタのアドレス範囲が開始アドレスと終了アドレスで表され、それらのセクタのデータを再生する場合に、デスクランブルキーを参照し、暗号化されたコンテンツをデスクランブルする。

【００８８】

記録するコンテンツと、そこで使用されるデスクランブルキーを取得するために、コンテンツを識別可能とするコンテンツＩＤを利用する。図５に示したように光ディスク上に記録したコンテンツ情報領域５０２内のコンテンツ管理リストに記録されるコンテンツ情報中に、コンテンツＩＤとそのコンテンツで使用されるデスクランブルキーのリストとして記録される。１つのコンテンツに対して複数のデスクランブルキーを使用できるようなリスト構成を取ることによって、一部のコンテンツやソフトウェアの切り売りするようなサービスが可能となる。

【００８９】

また、図１３を参照して上述した変形例においては、チェックサムや巡回冗長検査符号などのエラー検出コードが付加されたデスクランブルキーをディスク識別情報でスクランブルしたデータを他のディスクへ不正にコピーした場合には、異なるディスク識別情報でデスクランブルを行うことによりエラーとして検出される。このような場合に、このデスクランブルキーを光ディスク上に記録されているディスク識別情報によってスクランブルされたデスクランブルキーを入手し、それに置きかえることによって正しく再生できるようなディスクを作成することもできる。

【００９０】

図１のキー管理情報領域１０７は書き換え可能なリードイン領域１０１に記録される。通常、ユーザデータ領域１０２はパーソナルコンピュータのドライブ装置からアクセス可能なユーザ領域と、光ディスク上の欠陥セクタに対するスペア領域とからなり、通常の読み出しコマンドや書き込みコマンドでは、ユーザ領域のみが論理的な連続領域としてアクセス可能である。キー管理情報をリードイン領域１０１に配置することにより、パーソナルコンピュータのドライブ装置などから直接アクセスされることを防止し、パーソナルコンピュータからＡＶデータ等に施されたスクランブルを解くためのキーの取得を不可能とすることができる。

【００９１】

＜第２の実施形態＞

図７は、本発明に係る第２の実施形態である光ディスク記録再生装置の構成を示すブロック図である。この光ディスク記録再生装置は、第１の実施形態に係る光ディスク１００に著作権保護を必要とする画像データや音楽データなどのＡＶデータのコンテンツを記録する装置である。

【００９２】

図７において、７０１は第１の実施形態の光ディスク、７０２は半導体レーザと光学素子から構成される光ピックアップである光ヘッド、７０３は半導体レーザの動作制御及び再生信号の２値化を行う記録再生制御回路、７０４は記録すべきディジタルデータをディジタル変調するとともに２値化された再生信号をディジタル復調する変復調回路、７０５は光ディスク７０１上の傷や埃等で生起したエラーの誤り検出及び訂正処理と、誤り検出及び訂正処理に必要な誤り訂正コードの生成処理を行う誤り検出及び訂正回路、７０６は誤り検出及び訂正回路７０５の作業用メモリ及びデータバッファメモリとして用いるＲＡＭであるバッファメモリ、７０７はスクランブルされて記録されているＡＶデータをデスクランブルするデスクランブル回路、７０８は圧縮されて記録された動画データ等を伸長するＭＰＥＧ復号回路、７０９は伸長された画像データをＤ／Ａ変換してビデオ信号及びオーディオ信号を生成して出力する出力回路、７１０は光ディスク記録再生装置全体の動作を制御する制御ＣＰＵ、７１１はコンテンツに施された暗号を解くデスクランブルキーを取得する通信回路、７１２はセットトップボックスなどの通信端末装置から画像データや音楽データなどの暗号化されたコンテンツのディジタルデータを受信するデータ受信回路である。

【００９３】

以上のように構成された、図７の光ディスク記録再生装置におけるデータ記録動作について説明する。セットトップボックスやＭＰＥＧエンコーダなどの通信端末装置から送信されてきた画像データや音楽データなどの暗号化されたコンテンツのディジタルデータはデータ受信回路７１２によって受信された後、バッファメモリ７０６に一時的に保存される。誤り検出及び訂正回路７０５は、保存されたコンテンツのディジタルデータに、光ディスク７０１の傷や埃等に起因する誤りの検出及び訂正処理に必要な誤り検出及び訂正コードを生成し、記録データを再構成する。誤り検出及び訂正コードには、例えば公知のリードソロモン符号などの符号が用いられる。ここで、再構成された記録データは、コンテンツのディジタルデータと、誤り検出及び訂正コードとを含む。変復調回路７０４は、記録の際に８／１６変調方式などの変調方式を用いて、記録データをディジタル変調する。そして、記録再生制御回路７０３は、ディジタル変調された記録データに従って、光ヘッド

７０２から出力されるレーザ光のパワーを強度変調して、当該レーザを光ディスク７０１に照射することにより、記録データを光ディスク７０１上に記録する。

【００９４】

図８は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるＡＶデータの記録処理を示すフローチャートである。

【００９５】

図８において、まず、ステップＳ８０１において、光ディスク７０１からのＡＶデータの記録に先立ち、リードイン領域１０１のディスク識別情報を再生し、次いで、ステップＳ８０２において、ディスク識別情報に記録されている、ユーザデータ領域１０２に記録可能なデータの種別から、現在記録しようとしているコンテンツのディジタルデータが記録可能であるか否かを判断する。ステップＳ８０２でＹＥＳのときはステップＳ８０３に進む一方、ＮＯであるときはステップＳ８１０で記録動作を中止して当該ＡＶデータの記録処理を終了する。

【００９６】

ステップＳ８０３では、リードイン領域１０１においてキー管理情報が記録されたセクタのデータを再生し、ステップＳ８０４では、再生したキー管理情報にコンテンツの記録に必要なキー情報に対する領域が割り当て済みであるか否かを判断する。ステップＳ８０４でＮＯであるときは、キー管理情報領域１０７にキー情報を記録するための領域を割り当てた後、ステップＳ８０６に進む。一方、ステップＳ８０４でＹＥＳのときはそのままステップＳ８０６に進む。

【００９７】

コンテンツの記録を行う場合には、光ディスク記録再生装置の制御ＣＰＵ７１０は、記録する暗号化されたコンテンツのデータと、暗号を解くためのデスクランブルキーに関する情報を、通信端末装置からデータ受信回路７１２を介して受信する。ここで、キーに関する情報とは、コンテンツで使用されるキーそのもの、もしくは、コンテンツ全体で使用するキーのうち何番目のキーに対応するのかを示すキーＩＤである。キーＩＤを受信した場合に、ステップＳ８０６では、受信されたキーＩＤを、キーＩＤに対応するデスクランブルキーが記録されている領域を示すポインタであるキーインデックスに変換し、変換されたデスクランブルキーを、そのデスクランブルキーで復号されるコンテンツのデータが記録されるセクタのヘッダ領域に配置される。そして、ステップＳ８０７では、制御ＣＰＵ７１０は、記録再生制御回路７０３と、変復調回路７０４と、誤り検出及び訂正回路７０５とを制御することにより、以下の記録データの処理を実行する。この処理では、記録したいセクタデータに対してエラー検出及び訂正用のコードを付加し、これらのコードが付加されたセクタデータを、公知の８／１６変調方式などの変調方式を用いてディジタル変調し、所定の記録位置に光ヘッド７０２を制御するとともに、ディジタル変調された記録データに従ってレーザ光を強度変調する。これによって、記録データを光ディスク７０１上に記録する。さらに、ステップＳ８０８では、コンテンツの記録の終了であるか否かを判断し、ＮＯであるときはステップＳ８０６に戻り、上記の処理を繰り返す。ステップＳ８０８でＹＥＳであれば、ステップＳ８０９で、更新されたキー管理情報を光ディスク７０１上のキー管理情報領域１０７に記録して当該ＡＶデータの記録処理を終了する。

【００９８】

図９は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるキー管理情報領域の割り当て処理を示すフローチャートである。この処理は、コンテンツのデータの記録に先立ち、デスクランブルキーを記録するための領域を割り当てる処理である。

【００９９】

図９において、まず、ステップＳ９０１において、例えば電子プログラムガイド等から記録するコンテンツのキーに関する情報（使用するデスクランブルキーの個数などを含む。）を取得し、次いで、ステップＳ９０２では、光ディスク７０１に記録されているキー管理情報領域１０７内のキー管理情報を再生し、ステップＳ９０３において、デスクランブルキー領域５０５の空き領域をキーステータス領域５０６から調べ、記録しようとしてい

るコンテンツで使用するデスクランブルキーを記録できるか否かを判定する。ステップＳ９０３でＮＯであるときは、ステップＳ９０７で記録動作を中止して当該割り当て処理を終了する。一方、ステップＳ９０３でＹＥＳであるときは、ステップＳ９０４で、記録するコンテンツをコンテンツ情報領域５０２内のコンテンツリストに登録し、ステップＳ９０５においてデスクランブルキー領域５０５に対して、デスクランブルキーの記録に必要な領域を予約するために、対応するキーステータス領域に領域予約済みフラグを設定することにより記録用領域を割り当てる。さらに、ステップＳ９０６で、デスクランブルキーを記録するために割り当てられた領域を示すキーインデックスをキーリストとして作成し、コンテンツ情報としてのポインタを割り当てた後、当該割り当て処理を終了する。

【０１００】

図１０は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるデスクランブルキーの記録処理を示すフローチャートである。この記録処理は、キー管理センターからデスクランブルキーを取得して光ディスク７０１に記録するための処理である。

【０１０１】

図１０において、まず、ステップＳ１００１において、光ディスク７０１のリードイン領域１０１のディスク識別情報を再生した後、ステップＳ１００２において、キー管理センターからデスクランブルキーを取得するために、ディスク識別情報と、所望のコンテンツのデスクランブルに必要なキーを識別するためのキーＩＤを通信回路７１１を介してキー管理センターに送信する。キー管理センターでは、与えられたキーＩＤからコンテンツのデスクランブルに必要なデスクランブル鍵を選択し、送られてきたディスク識別情報等の情報によって、デスクランブルキーを暗号化して返信する。

【０１０２】

ステップＳ１００３で、キー管理センターから通信回路７１１を介して、キーＩＤに対応するデスクランブルキーを取得した後、ステップＳ１００４で、キー管理情報領域１０７のデータを再生し、再生されたキー管理情報領域１０７内のデータのうちキーＩＤで示されるキーインデックスリストから、デスクランブルキーを記録する領域を示すキーインデックスを取得する。次いで、ステップＳ１００５において、キーインデックスにより示されたデスクランブルキー領域に上記取得したデスクランブルキーを配置し、対応するキーステータス領域５０６にキー取得済みを示す取得済みフラグを設定する。さらに、ステップＳ１００６で、すべてのキーの取得が終了したか否かが判断され、ＮＯであれば、ステップＳ１００３に戻り上記の処理を繰り返す。一方、ステップＳ１００６でＹＥＳであるときは、ステップＳ１００７において、更新されたキー管理情報をキー管理情報領域１０７に記録して当該デスクランブルキーの記録処理を終了する。

【０１０３】

次いで、本実施形態の光ディスク記録再生装置のデータ再生動作について図７を参照して説明する。光ディスク７０１に記録されたディジタルデータは、以下のようにして再生される。光ヘッド７０２の半導体レーザからのレーザ光は光ディスク７０１に照射され、そのときに光ディスク７０１で反射される反射光が光ヘッド７０２を介して記録再生制御回路７０３に入射する。記録再生制御回路７０３は、入射する反射光を光電変換した後、増幅及び２値化処理を実行することにより、ディジタル化された再生信号を生成して変復調回路７０４に出力する。変復調回路７０４は、記録の際に公知の８／１６変調方式などの変調方式を用いてディジタル変調された信号をディジタル信号にディジタル復調して、誤り検出及び訂正回路７０５に出力する。次いで、誤り検出及び訂正回路７０５は、バッファメモリ７０６を作業用メモリとして用いて、光ディスク７０１の傷や埃など起因する誤りの検出及び訂正処理を実行する。この誤り検出及び訂正処理は、例えば、既知のリードソロモン符号などの復号を行うことで実行される。

【０１０４】

誤り検出及び訂正処理された再生データは、デスクランブル処理を行うために、デスクランブル回路７０７に出力される。デスクランブル回路７０７は、予めデータの再生に先立って再生したキー管理情報領域１０７のデスクランブルキーを用いて再生データにデスク

ランブル処理を施した後、ＭＰＥＧ復号回路７０８に出力する。次いで、ＭＰＥＧ復号回路７０８は、圧縮された動画データや音楽データを伸長した後、伸長後のデータを出力回路７０９に出力する。さらに、出力回路７０９は、入力される伸長されたデータをビデオ信号及びオーディオ信号にＤ／Ａ変換して、テレビジョン装置やオーディオ機器などの上位の機器に出力する。

【０１０５】

図１１は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるＡＶデータの再生処理を示すフローチャートである。図１１において、まず、ステップＳ１１０１において、光ディスク７０１からのＡＶデータの記録に先立ち、リードイン領域１０１内のディスク識別情報を再生し、ステップＳ１１０２において、ディスク識別情報に記録されている再生可能なデータの種別から、現在再生しようとしているコンテンツが再生可能であるか否かを判断する。ステップＳ１１０２でＮＯであるときは、ステップＳ１１１２で再生動作を中止して当該ＡＶデータの再生処理を終了する。一方、ステップＳ１１０２でＹＥＳであるときは、ステップＳ１１０３で、リードイン領域１０１のキー管理情報領域１０７内でキー管理情報が記録されたセクタのデータを再生し、ステップＳ１１０４において再生したキー管理情報において、コンテンツの再生に必要なキー情報が記録済みであるか否かを判断する。ステップＳ１１０４でＹＥＳであるときはそのままステップＳ１１０６に進む一方、ＮＯであれば、ステップＳ１１０５において、キーを管理しているキー管理センターから通信回路７１１を介してデスクランブルキーを取得し、光ディスク７０１のキー管理情報領域１０７に記録してステップＳ１１０６に進む。

【０１０６】

次いで、ステップＳ１１０６では、制御ＣＰＵ７１０は、光ディスク７０１のユーザデータ領域に光ヘッド７０２を移動させ、記録再生制御回路７０３、変復調回路７０４、誤り検出及び訂正回路７０５を制御してＡＶデータを再生する。そして、ステップＳ１１０７では、再生されたセクタのヘッダに含まれるキーインデックスにより示されるデスクランブルキー領域５０５から、セクタデータのデスクランブルに必要なデスクランブルキーを取得し、ステップＳ１１０８では、デスクランブルキーに対して行われているスクランブルを、ディスク識別情報によってデスクランブルすることにより復号する。さらに、ステップＳ１１０８において、デスクランブルキーに付与されているエラー検出コードをチェックすることにより、デスクランブルキーに誤りがあるか否かを判断する。ステップＳ１１０８でＹＥＳであるときは、不正に入手したコンテンツ（又は不正にコピーしたコンテンツ）とみなし、ステップＳ１１１２で再生動作を中止して当該ＡＶデータの再生処理を終了する。

【０１０７】

一方、ステップＳ１１０８でＮＯであるときは、Ｓ１１０９において、デスクランブルキーによりコンテンツのデータをデスクランブルし、ステップＳ１１１０において、デスクランブルされたＡＶデータをＭＰＥＧ復号回路７０８に出力する。そして、制御ＣＰＵ７１０は、ＭＰＥＧ復号回路７０８及び出力回路７０９を制御することにより、デスクランブルされたＡＶデータをＭＰＥＧ伸長した後、ビデオ信号とオーディオ信号にＤ／Ａ変換してテレビジョン装置やオーディオ機器などの上位機器に出力する。次いで、ステップＳ１１１１では、コンテンツの再生の終了か否かが判断され、ＮＯであるときはステップＳ１１０６に戻り、上記の処理を繰り返す。一方、ステップＳ１１１１でＹＥＳのときは当該ＡＶデータの再生処理を終了する。

【０１０８】

なお、ステップＳ１１０９で誤りが検出された場合には、不正に入手したコンテンツとみなし、例えば、不正にコピーしたコンテンツとみなし、再生動作を中止したが、キーが記録されていない場合と同様に、ステップＳ１１０５の処理を実行することにより、通信回路７１１を介して、キーを管理しているキー管理センターからキー情報を取得し、光ディスク７０１のキー管理情報領域１０７に記録してもよい。これにより、コピーしたＡＶデータであっても、キーを正規に入手することによって再生可能にすることができる。

【０１０９】
図１２は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるデスクランブルキーの取得処理を示すフローチャートである。この処理は、再生されたキーインデックスからデスクランブルキーを再生する処理であり、図１１に図示されたＡＶデータの再生処理に先立って実行される。
【０１１０】
図１２において、まず、ステップＳ１２０１では、再生されたセクタ領域のデータがスクランブルされているか否かをスクランブル制御情報により判断し、ＮＯであるときはステップＳ１２０６に進む一方、ＹＥＳであるときは、ステップＳ１２０２において上記セクタ領域と同一のセクタ領域内に記録されているキー情報を再生することによりキーインデックスを取得し、次いで、ステップＳ１２０３においてデスクランブルキー領域５０５から上記キーインデックスによって示されるデスクランブルキーを取得した後、ステップＳ１２０４では、取得されたデスクランブルキーをディスク識別情報を用いてデスクランブルし、エラー検出コードを調べることによりデスクランブルキーが誤りがあるか否かを判断する。ステップＳ１２０４でＹＥＳのときは、ステップＳ１２０５で再生動作を中止して当該デスクランブルキーの取得処理を終了する。一方、ステップＳ１２０４でＮＯであるときは、ステップＳ１２０６に進む。再生されたセクタがスクランブルされていない場合やデスクランブルキーをディスク識別情報によってデスクランブルされた結果に誤りがない場合には、ステップＳ１２０６において再生動作の許可を行い、再生されたセクタのデータを出力して当該デスクランブルキーの取得処理を終了する。
【０１１１】
以上説明したように、本発明に係る実施形態の光ディスク及び光ディスク記録再生装置では、ディスク製造段階で作成された再生専用のディスク識別情報を用いて利用者による記録や再生動作を制御するできる。さらに、上記のディスク識別情報を用いてデータの一部をスクランブルすることにより、ユーザデータ領域の物理コピーが行われたディスクに対して正常に再生すること防止することができる。また、データのデスクランブルに必要なデスクランブルキーをデータとは別領域に配置することにより、コンテンツの記録とデスクランブルキーの記録を独立に行うことができる。このため、コンテンツを記録しておき、必要に応じて、例えばコンテンツのデータの再生時に、デスクランブルキーを取得することにより、コンテンツの再生可能な状態とすることができる。この際、デスクランブルキーをディスク識別情報によりスクランブルしておくことで、上述した場合と同様に、物理的なコピーによる不正な利用を防止できることは明らかである。それに加えて、不正にコピーしたディスクであっても、その光ディスクのディスク識別情報でスクランブルされたデスクランブルキーを正式にキー管理センターから取得し、光ディスクに記録することにより、正しく再生できる光ディスクにすることもできる。
【０１１２】
なお、光ディスク記録再生装置に入力されるコンテンツのデータについて既に暗号化されたものについて説明したが、光ディスク記録再生装置内にコンテンツを暗号化する回路を備えることで、入力されたコンテンツのデータを暗号化し、光ディスク上に記録することにより同様の効果が得られる。
【０１１３】
また、本実施形態では、暗号化されたコンテンツの解読に必要なデスクランブルキーのみをディスク識別情報を用いて暗号化することにより、異なるディスク識別情報を有するディスク間でのコピーの防止を行ったが、コンテンツ自身にディスク識別情報を用いた暗号化を施すことにより、同様にコピーの防止を行うことができる。さらに、ディスク識別情報にも秘密鍵を用いて暗号化を施すことにより、ディスク上に記録されたコンテンツの不正な解読をより困難にすることができる。
【０１１４】
＜第１及び第２の実施形態の効果＞
本発明に係る実施形態の光ディスクは、ユーザデータ領域への記録動作や再生動作を光デ

ィスク毎に行うディスク識別情報が書き換え不可能な再生専用領域に記録されることにより、利用者による光ディスク上へのコンテンツの記録動作や再生動作を光ディスクの製造時に記録する情報を用いて制御することができる。

【０１１５】

本発明に係る実施形態の光ディスクは、書き換えが不可能な再生専用のディスク識別情報を鍵として暗号化されたデータが光ディスク上のユーザデータ領域に記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とすることができる。

【０１１６】

本発明に係る実施形態の光ディスクは、暗号化されたデータと暗号を解くデスクランブルキーとが異なるセクタ領域に記録されることにより、映画や音楽などの著作権保護が必要なデータの取得と暗号を解くためのデスクランブルキーの取得を独立に行うことが可能となる。さらに、ディスク識別情報を鍵としてデスクランブルキーを暗号化して記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とし、コピー先の光ディスクのディスク識別情報を鍵として暗号化したデスクランブルキーを取得し記録することで、データの正しい復号並びに再生を可能とすることができる。

【０１１７】

＜第３の実施形態＞

次いで、本発明に係る第３の実施形態である暗号化コンテンツ記録及び再生方法について図面を参照しながら説明する。図１６は、本発明に係る第３の実施形態である光ディスク１１０１のデータ記録領域を示す平面図である。

【０１１８】

図１６において、１１０１はディジタルデータを記録することが可能な記録媒体であって、書き換え型又は追記型の光ディスクである記録型光ディスク、１１０２はディスク情報が微小な凹凸ピットの形式で記録されたコントロールユーザデータ領域、１１０３はレーザ光の光ビームを光ディスクに照射することによりユーザがデータを記録するユーザデータ領域、１１０４はディスクＩＤが記録されたＢＣＡである。ＢＣＡ１１０４において、コントロールユーザデータ領域１１０２の内周部分の微小な凹凸ピット上の記録膜は、半径方向に長い形状でかつ複数個のトリミング領域１１０５が形成されるように、その記録膜に対して部分的にＹＡＧレーザなどのパルスレーザのレーザ光を放射することによりトリミングされ、これによりデスクランブル識別情報であるディスクＩＤが記録される。

【０１１９】

図１７は、第３の実施形態に係るＢＣＡ再生回路１４０１における再生信号１２０１及び再生２値化信号１２０７の信号波形を示す波形図であり、図１８は、第３の実施形態に係るＢＣＡ再生回路１４０１の構成を示すブロック図である。図１７において、ＢＣＡ１１０４のデータを再生したときの再生信号１２０１を示している。図１８において、１３０１は光ピックアップ、１３０２はプリアンプ、１３０３は低域通過フィルタ（ＬＰＦ）、１３０４は２値化回路、１３０５は復調回路である。

【０１２０】

図１８において、光ピックアップ１３０１から出力されるレーザ光は光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光は光ピックアップ１３０１により光電変換された後、光電変換後の電気信号は、プリアンプ１３０２で増幅されて再生信号１２０１が得られる。ここで、図１７の再生信号１２０１はコントロールユーザデータ領域１１０２の凹凸ピットに応じたレベルを有する信号であり、この再生信号１２０１において、１２０２、１２０３、１２０４はパルスレーザによるトリミング処理により記録膜が取り除かれて、凹凸ピットによる信号が欠落しているトリミング部分である。このトリミング処理は、光ディスクの製造者によって行われる。

【０１２１】

図１８に戻り説明すると、再生信号１２０１は低域通過フィルタ１３０３に入力されて、凹凸ピットによる変調信号が除去された後に、２値化回路１３０４に入力される。２値化回路１３０４に入力された再生信号は、コントロールユーザデータ領域１１０２の信号を２値化する通常のスライスレベル１２０５ではなく、スライスレベル１２０５よりも十分に低いレベルであるスライスレベル１２０６を用いて２値化されて、再生２値化信号１２０７が得られる。２値化回路１３０４から出力される再生２値化信号１２０７は、復調回路１３０５で復調されてディスクＩＤ信号１３０６が得られる。

【０１２２】

以上説明したように、光ディスクを識別するディスク識別情報を付加することにより、光ディスクの管理を容易に実現することができる。また、ＢＣＡ１１０４が凹凸ピット上に記録されることにより、ＢＣＡ１１０４内の光ディスクを識別する情報が容易に改ざんされることを防止することができる。さらに、図１６のコントロールユーザデータ領域１１０２とＢＣＡ１１０４が隣接していることにより、コントロールユーザデータ領域１１０２のデータを再生する際に、ＢＣＡ１１０４のデータも続けて再生することができ、もしくはＢＣＡ１１０４のデータを再生する際に、コントロールユーザデータ領域１１０２のデータを続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかに光ディスクを識別するためのＢＣＡ１１０４の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【０１２３】

なお、本実施形態のＢＣＡ１１０４は、コントロールユーザデータ領域１１０２の内周部分の凹凸ピット上の記録膜をトリミングすることにより形成されているが、書き換え型又は追記型の光ディスクである記録形光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールユーザデータ領域１１０２の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミングの際に発生する熱からユーザデータ領域１１０３を保護することができる。また、コントロールユーザデータ領域１１０２の内周側にＢＣＡ１１０４を形成するのは、フォーカスサーボ回路の不安定性によりレーザ光のビームのスポットの径が変化する場合のマージンを考慮しているためである。

【０１２４】

なお、トリミング前のＢＣＡ１１０４に記録されているデータが、コントロールユーザデータ領域１１０２に記録されていてもよい。ＢＣＡ１１０４に記録されているデータが、コントロールユーザデータ領域１１０２にも記録されていることにより、トリミングを行ってもコントロールユーザデータ領域１１０２の上記データを保護することができる。さらに、ＢＣＡ１１０４に記録されているデータが、ＢＣＡ１１０４から、コントロールユーザデータ領域１１０２まで連続して繰り返し記録されている場合には、コントロールユーザデータ領域１１０２の上記データを見つけることによって、ＢＣＡ１１０４の位置を予想することができる。

【０１２５】

次いで、上記ＢＣＡ１１０４を有する光ディスク１１０１に、ネットワークを介して、ディスクＩＤで暗号化されたコンテンツを記録する手順を述べる。第３乃至第５の実施形態において、ネットワークとは、例えば、インターネット、公衆電話回線、又は専用線などの通信網をいう。図１９は、第３の実施形態に係る光ディスク記録再生システムの構成を示すブロック図であり、上記ＢＣＡ１１０４を有する書き換え型又は追記型の光ディスクである記録型光ディスク１１０１に暗号化コンテンツを記録する装置構成を示す。

【０１２６】

図１９において、光ディスク記録再生システムは、互いにインターネットなどのネットワーク１４０５を介して接続された、光ディスク記録再生装置１４１０と、暗号化部１４０６とを備えて構成される。光ディスク記録再生装置１４１０は、光ピックアップ１３０１と、ＢＣＡ再生回路１４０１と、インターネット４０３と、記録回路１４１１と、データ再生部１４１２と、暗号デコーダ１４１３とを備える。また、暗号化部１４０６は、イン

ターフェース１４０４と、コンテンツメモリ１４０７と、暗号化エンコーダ１４０８とを備える。

【０１２７】

まず、光ピックアップ１３０１から出力されるレーザ光は、例えばＲＡＭ型光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光は光ピックアップ１３０１によって光電変換された後、光電変換された再生信号がＢＣＡ再生回路１４０１に入力される。ＢＣＡ再生回路１４０１は入力された再生信号に基づいてＢＣＡ内のディスクＩＤ信号１４０２を再生して、再生されたディスクＩＤ信号１４０２を暗号デコーダ１４１３に出力するとともに、インターフェース１４０３及び１４０４とネットワーク１４０５を介して、暗号化部１４０６の暗号化エンコーダ１４０８に送られる。暗号化エンコーダ１４０８は、コンテンツメモリ１４０７内のコンテンツのデータが記録される光ディスク１１０１のディスクＩＤ信号１４０２が暗号を解く復号鍵となるように、当該コンテンツのデータを暗号化し、又は画像音声用のスクランブルを行う。

【０１２８】

なお、本実施形態では、暗号化処理について、コンテンツ１４０７を、ディスクＩＤ信号１４０２を暗号鍵として用いて暗号化すると表現しても同一の意味とする。また、本実施形態においては、暗号化や復号化を、錠と鍵の関係で考え、上記錠を上記鍵で閉めることを暗号化とし、上記錠を上記鍵で開けることを復号化とする。従って、暗号化と復号化で実際の演算は異なるが、暗号化するための鍵と復号化するための鍵は、同一であるとする。なお、コンテンツ１４０７をＣとし、ディスクＩＤ信号１４０２をＢＣＡＳとし、暗号化されたコンテンツ１４０９をＣ［ＢＣＡＳ］とし、暗号化処理の演算を＊で表し、次式のように表記する。

【０１２９】

【数１】

Ｃ＊ＢＣＡＳ＝Ｃ［ＢＣＡＳ］

【０１３０】

暗号化部１４０６によって暗号化されたコンテンツ１４０９は、インターフェース１４０３及び１４０４とネットワーク１４０５を介して記録再生装置１４１０の記録回路１４１１に送られる。記録回路１４１１は、入力されるコンテンツのデータを所定のディジタル変調し、ディジタル変調されたデータに応じて光ピックアップ１３０１からのレーザ光を強度変調して光ディスク１１０１に照射することにより、コンテンツのデータを光ディスク１１０１に記録する。

【０１３１】

次に、光ディスク１１０１に暗号化されて記録された上記コンテンツを再生する際は、光ピックアップ１３０１から出力されるレーザ光がユーザデータ領域１１０３の上記暗号化コンテンツが記録された領域を照射し、その反射光が光ピックアップ１３０１によって光電変換された後、光電変換された再生信号がデータ再生部１４１２に入力される。データ再生部１４１２は、入力された再生信号をディジタルデータにＡ／Ｄ変換して暗号デコーダ１４１３に出力する。一方、光ピックアップ１３０１からのレーザ光は光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光は光ピックアップ１３０１によって光電変換された後、光電変換された再生信号はＢＣＡ再生回路１４０１に入力される。ＢＣＡ再生回路１４０１は入力された再生信号をＡ／Ｄ変換してディスクＩＤ信号１４０２を発生して、当該ディスクＩＤ信号を暗号デコーダ１４１３に出力する。

【０１３２】

暗号デコーダ１４１３は、入力されたディスクＩＤ信号１４０２を鍵として用いて、暗号化されたコンテンツのデータを復号する。このとき、コンテンツが正規に光ディスク１１０１に記録されている場合は、光ディスク１１０１に記録されている暗号化コンテンツを復号するための鍵は、光ディスク１１０１のディスクＩＤ信号１４０２であり、再生時にＢＣＡ再生回路１４０１から出力されるディスクＩＤ信号１４０２も、光ディスク１１０１のディスクＩＤ信号（ＢＣＡＳ）である。従って、復号又はデスクランブルされたコン

テンツが暗号デコーダ１４１３から出力信号１４１４として出力される。なお、復号化処理の演算を＃とすると、次式のように表記される。

【０１３３】

【数２】

Ｃ［ＢＣＡＳ］＃ＢＣＡＳ＝Ｃ

【０１３４】

ここで、コンテンツのデータが画像データの場合は、例えばＭＰＥＧ信号のデータが伸長されて、画像信号のデータが得られる。

【０１３５】

以上説明したように、本実施形態における暗号化は、ディスクＩＤを鍵としており、ディスクＩＤは、１枚の光ディスクに対応して１個しか存在しないため、当該１枚の光ディスクにしか同一の暗号化コンテンツの記録をすることができないという効果がある。すなわち、上記コンテンツ１４０７を、例えばＩＤ１というディスクＩＤを持つ正規の光ディスクから、ＩＤ２という別のディスクＩＤを持つ別の光ディスクにコピーして再生しようとした場合、ＢＣＡ再生回路４０１からディスクＩＤ信号１４０２としてＩＤ２が出力される。しかしながら、暗号化コンテンツはＩＤ１というディスクＩＤ信号で暗号化されているので、暗号デコーダ１４１３で、暗号化コンテンツを復号することができない。

【０１３６】

なお、暗号化エンコーダ１４０８はコンテンツの供給元ではなく、ネットワークに対して記録再生装置側にあり、暗号化エンコーダを搭載したＩＣカードなどの形態であってもよい。また、上記光ディスク１１０１はディスクＩＤのみで暗号化されているので、ＢＣＡ再生回路１４０１と暗号デコーダ１４１３を有する任意の光ディスク記録再生装置で再生することが可能である。

【０１３７】

＜第４の実施形態＞

次いで、本発明に係る第４の実施形態である暗号化コンテンツ記録方法について図面を参照しながら説明する。図２０は、本発明に係る第４の実施形態である光ディスク記録再生システムの構成を示すブロック図であり、ＢＣＡを有する書き換え型又は追記型光ディスクである記録型光ディスクに、暗号化コンテンツを記録する装置構成を示す。なお、第４の実施形態の説明において、第３の実施形態と共通の部分はその説明を簡略化する。

【０１３８】

図２０において、第４の実施形態に係る光ディスク記録再生システムは、ＣＡＴＶ会社装置１５０１と、鍵発行センター装置１５０７と、ＣＡＴＶデコーダ１５０６と、光ディスク記録再生装置１５１４と、テレビジョン装置１５３０とを備えて構成される。ここで、ＣＡＴＶ会社装置１５０１は、映画ソフトウエアなどのコンテンツのデータを格納するコンテンツメモリ１５０２と、第１暗号鍵を格納する第１暗号鍵メモリ１５０３と、第１暗号化エンコーダ１５０４とを備える。また、鍵発行センター装置１５０７は、その装置１５０７の動作を制御する制御部１５０７ａと、時間制限情報を格納する時間制限情報メモリ１５１０と、記録許可コードを格納する記録許可コードメモリ１５１１とを備える。さらに、ＣＡＴＶデコーダ１５０６は、ＣＡＴＶデコーダ１５０６のシステムＩＤを格納するシステムＩＤメモリ１５０８と、第１暗号デコーダ１５１３と、第２暗号化エンコーダ１５１６と、ＩＣカード１５２２内の会社識別信号メモリ１５２３とを備える。またさらに、光ディスク記録再生装置１５１４は、記録回路１５１８と、データ再生部１５１９と、ＢＣＡ再生回路１５２１と、第２暗号デコーダ１５２０と、ＩＣカード１５２４内の会社識別信号メモリ１５２６とを備える。

【０１３９】

まず、ＣＡＴＶ会社装置１５０１の第１暗号化エンコーダ１５０４は、映画ソフトウエアなどのコンテンツメモリ１５０２内のコンテンツのデータを第１暗号鍵１５０３を用いて暗号化することにより、第１暗号化コンテンツ１５０５を生成し、生成された第１暗号化コンテンツ１５０５をネットワークを介して各ユーザのＣＡＴＶデコーダ１５０６の第１

暗号化デコーダ１５１３に送信する。ここで、コンテンツメモリ１５０２内のデータをＣとし、第１暗号鍵１５０３をＦＫとし、第１暗号化コンテンツ１５０５をＣ［ＦＫ］とすると、次式のように表記される。

【０１４０】

【数３】

Ｃ＊ＦＫ＝Ｃ［ＦＫ］

【０１４１】

ＣＡＴＶデコーダ１５０６は、システムＩＤメモリ１５０８内の当該ＣＡＴＶデコーダ１５０６のシステムＩＤと、視聴もしくはＲＡＭ型光ディスク１１０１への記録を行いたい上記コンテンツに予め付与され、例えば当該ＣＡＴＶデコーダ１５０６のキーボード（図示せず。）を用いて入力されたタイトルコード１５０９とを、ネットワークを介して鍵発行センター装置１５０７に送信する。ここで、タイトルコード１５０９はＴＶの画面に従って選択することにより入力してもよいし、直接にキーボードから入力してもよいし、リモートコントローラー等から入力してもよい。従って、タイトルコード１５０９は、ユーザが独自に入手していてもよいし、第１暗号化コンテンツ１５０５とともにＣＡＴＶデコーダ１５０６に送られてきてもよいし、番組案内などの形態で第１暗号化コンテンツ１５０５とは別の時刻に予め送られていてもよい。

【０１４２】

鍵発行センター装置１５０７の制御部１５０７ａは、ＣＡＴＶデコーダ１５０６のシステムＩＤと、上記コンテンツのタイトルコード１５０９とに基づいて、時間制限情報メモリ１５１０内の時間制限情報と、記録許可コードメモリ１５１１内の記録許可コードとを参照して、これらに対応する鍵（Ｋ）１５１２を記録許可コード及び時間制限コードとともにＣＡＴＶデコーダ１５０６の第１暗号デコーダ１５１３に対して、ネットワークを介して送信する。なお、時間制限情報により、同一のコンテンツを時刻を変えて複数回放送する場合を区別することができる。ここで、第１復号鍵をＦＫとし、ＣＡＴＶデコーダ１５０６のシステムＩＤをＤＩＤとし、時間制限情報をＴＩＭＥとし、記録許可コードをＣＯＰＹとし、コンテンツのタイトルコード１５０９をＴとするとき、鍵（Ｋ）は、次式の関係を満たしている。

【０１４３】

【数４】

ＦＫ＝Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ＊ＣＯＰＹ

【０１４４】

なお、記録許可コードメモリ１５１１内の記録許可コードは、例えばＣＡＴＶ会社装置１５０１が、放送するコンテンツが新作品か旧作品かを判断して、視聴のみ許可するのか、視聴、記録の両方を許可するのかを決定する。

【０１４５】

ＣＡＴＶデコーダ１５０６の第１暗号デコーダ１５１３は、第１復号鍵（ＦＫ）と、鍵（Ｋ）１５１２と、上記コンテンツのタイトルコード１５０９と、システムＩＤと、記録許可コードと、時間制限情報とが上述の関係を満たしており、かつクロック回路１５２７から出力される現在時刻情報が当該時間制限情報の条件を満たしていれば、第１暗号化コンテンツ１５０５を復号する。ここで、上記暗号化されたコンテンツが画像信号の場合は、デスクランブルされた画像信号が第１暗号化デコーダ１５１３からテレビジョン装置１５３０に出力されて視聴できる。ここで、第１暗号化デコーダ１５１３の復号化処理は次式で表される。

【０１４６】

【数５】

Ｃ［ＦＫ］＃（Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ＊ＣＯＰＹ）

＝Ｃ［ＦＫ］＃ＦＫ

＝Ｃ

【０１４７】

なお、記録許可コードが視聴のみ許可する場合は、光ディスク１１０１に記録できないが、視聴と記録の両方を許可する場合は記録することができるので、以下でこの方法について説明する。

【０１４８】

光ディスク記録再生装置１５１４のＢＣＡ再生回路１５２１は、光ディスク１１０１のＢＣＡ１１０４のデータを再生してディスクＩＤ信号１５１５を得て、当該ディスクＩＤ信号をＣＡＴＶデコーダ１５０６の第２暗号化エンコーダ１５１６に出力する。ＣＡＴＶデコーダ１５０６の第２暗号化エンコーダ１５１６は、ディスクＩＤ信号１５１５を第２暗号鍵として用いて、第１暗号デコーダ１５１３から出力されたコンテンツのデータを暗号化することにより、第２暗号化コンテンツ１５１７を生成して光ディスク記録再生装置１５１４の記録回路１５１８に送信する。なお、第２暗号デコーダ１５１６の上記暗号化は、第１暗号デコーダ１５１３から第１暗号化コンテンツが復号されて出力されている時間に限られる。ここで、第１暗号デコーダ１５１３の出力信号であるコンテンツをＣとし、第２暗号鍵であるディスクＩＤ信号１５１５をＢＣＡＳとし、第２暗号化コンテンツ１５１７をＣ［ＢＣＡＳ］とすると、次式のように表記される。

【０１４９】

【数６】

Ｃ＊ＢＣＡＳ＝Ｃ［ＢＣＡＳ］

【０１５０】

光ディスク記録再生装置１５１４の記録回路１５１８に送られた第２暗号化コンテンツ１５１７は、記録回路１５１８により、例えば公知の８／１６変調方式により変調されて、光ピックアップ（図示せず。）により光ディスク１１０１のユーザデータ領域１１０３に記録される。光ディスク１１０１に暗号化されて記録された上記コンテンツを再生する際は、光ピックアップから出力されるレーザ光が光ディスク１１０１の上記暗号化されたコンテンツが記録されている領域を照射し、その反射光が光ピックアップに入射する。上記光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をデータ再生部１５１９に出力し、データ再生部１５１９は、入力された再生信号をディジタル再生信号にＡ／Ｄ変換して第２暗号デコーダ１５２０に出力する。

【０１５１】

一方、光ピックアップから出力されるレーザ光は光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光が光ピックアップに入射する。上記光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をＢＣＡ再生回路１５２１に出力する。ＢＣＡ再生回路１５２１は入力された再生信号に基づいてディスクＩＤ信号１５１５を生成して第２暗号デコーダ１５２０に出力する。これに応答して、第２暗号デコーダ１５２０は、入力されたディスクＩＤ信号１５１５を鍵として用いて、データ再生部１５１９から出力される再生された暗号化コンテンツの復号を行う。このとき、コンテンツが正規に光ディスク１１０１に記録されている場合は、光ディスク１１０１に記録されている暗号化コンテンツを復号するための鍵は光ディスク１１０１のディスクＩＤであり、ＢＣＡ再生回路１５２１から出力されるディスクＩＤ信号も、光ディスク１１０１のディスクＩＤ信号（ＢＣＡＳ）であるので、第２暗号デコーダ１５２０は正常に復号処理を実行することができる。従って、復号又はデスクランブルされたコンテンツのデータは第２暗号デコーダ１５２０から出力信号１５２５として出力される。ここで、第２暗号デコーダ１５２０の復号化処理は次式で表記することができ、コンテンツが画像信号の場合は、第２暗号デコーダ１５２０は、例えばＭＰＥＧ信号を伸長して元の画像信号を再生して出力する。

【０１５２】

【数７】

Ｃ［ＢＣＡＳ］＃ＢＣＡＳ＝Ｃ

【０１５３】

また、上記光ディスク１１０１はディスクＩＤ信号（ＢＣＡＳ）１５１５のみで暗号化されているので、ＢＣＡ再生回路１５２１と第２暗号デコーダ１５２０を有する任意の光デ

ィスク記録再生装置で再生することが可能である。なお、暗号エンコーダ１５０４，１５１６で暗号化し、暗号デコーダ１５１３，１５２０で復号化することを説明したが、各装置１５０１，１５０６，１５１４内の制御部であるＣＰＵで実行されるプログラムに、暗号アルゴリズム及び復号アルゴリズムのプログラムを備えて暗号化や復号化を実行するように構成してもよい。

【０１５４】

なお、本実施形態において、ＣＡＴＶデコーダ１５０６の第２暗号化エンコーダ１５１６はディスクＩＤ信号１５１５を第２暗号鍵として用いてコンテンツを暗号化したが、以下のようにコンテンツを暗号化してもよい。例えば各ＣＡＴＶ会社装置１５０１毎に準備されたＩＣカード１５２２をＣＡＴＶデコーダ１５０６に装着して、ＩＣカード１５２２の会社識別信号メモリ１５２３内に記録されている会社識別信号と、ＢＣＡ再生回路１５２１により再生されたディスクＩＤ信号（ＢＣＡＳ）を組み合わせて第２暗号鍵として用いて、第２暗号化エンコーダ１５１６によりコンテンツを暗号化してもよい。ここで、第１暗号デコーダ１５１３の出力信号であるコンテンツをＣとし、第１の第２暗号鍵であるディスクＩＤ信号１５１５をＢＣＡＳとし、第２の第２暗号鍵である会社識別信号１５２３をＣＫとし、第２暗号化コンテンツ１５１７をＣ［ＢＣＡＳ，ＣＫ］とするとき、第２暗号化エンコーダ１５１６の暗号化処理を次式のように表記される。

【０１５５】

【数８】

Ｃ＊ＢＣＡＳ＊ＣＫ＝Ｃ［ＢＣＡＳ，ＣＫ］

【０１５６】

次に、光ディスク１１０１に暗号化して記録されたコンテンツを再生する際には、光ピックアップから出力されるレーザ光が光ディスク１１０１の上記暗号化されたコンテンツが記録されている領域を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射される反射光を再生信号に光電変換してデータ再生部１５１９に出力する。データ再生部１５１９は入力される再生信号をディジタル再生信号にＡ／Ｄ変換して第２暗号デコーダ１５２０に出力する。一方、光ピックアップから出力されるレーザ光は光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射される反射光を再生信号に光電変換してＢＣＡ再生回路１５２１に出力する。ＢＣＡ再生回路１５２１は入力される再生信号に基づいてディスクＩＤ信号１５１５を再生して、ディスクＩＤ信号１５１５を第２暗号化エンコーダ１５１６及び第２暗号デコーダ１５２０に出力する。

【０１５７】

さらに、光ディスク記録再生装置１５１４に装着されたＩＣカード１５２４の会社識別信号メモリ１５２６内の会社識別信号は、第２暗号デコーダ１５２０に入力される。なお、当該会社識別信号は、ＩＣカード１５２４の会社識別信号メモリ１５２６内に記録されていなくてもよく、例えば、光ディスク記録再生装置１５１４の記録プログラムのインストール時に、会社識別信号が、光ディスク記録再生装置１５１４の制御部であるＣＰＵに接続されたメモリ（図示せず。）に記録されていてもよい。とって代わって、会社識別信号を光ディスク記録再生装置１５１４のキーボード（図示せず。）を用いて入力してもよい。

【０１５８】

第２暗号デコーダ１５２０は、入力されたディスクＩＤ信号１５１５と、会社識別信号を復号鍵として用いて、暗号化されたコンテンツの復号を行う。このとき、ＣＡＴＶデコーダ１５０６のユーザがＣＡＴＶ会社装置１５０２を有する特定のＣＡＴＶ会社と正式に契約をし、コンテンツ１５０２が正規に光ディスク１１０１に記録されている場合は、光ディスク１１０１に暗号化されて記録されている暗号化コンテンツの第１の復号鍵は、まさに再生しようとする光ディスク１１０１のディスクＩＤ信号（ＢＣＡＳ）であり、第２の復号鍵は、契約したＣＡＴＶ会社から提供されたＩＣカード１５２４の会社識別信号メモリ１５２６内の会社識別信号（ＣＫ）である。従って、復号又はデスクランブルされたコ

ンテンツの出力信号１５２５が、第２暗号デコーダ１５２０から出力される。ここで、第２暗号デコーダ１５２０の復号化処理は次式のように表記され、コンテンツが画像信号の場合は、例えばＭＰＥＧ信号が第２暗号デコーダ１５２０により伸長されて、画像信号の出力信号１５２５が出力される。

【０１５９】

【数９】

Ｃ［ＢＣＡＳ，ＣＫ］＃（ＢＣＡＳ＊ＣＫ）＝Ｃ

【０１６０】

また、上記光ディスク１１０１のコンテンツは、ディスクＩＤ信号１５１５と会社識別信号で暗号化されているので、上記コンテンツの提供元のＣＡＴＶ会社と契約を結んでいれば、ＢＣＡ再生回路１５２１と、第２暗号デコーダ１５２０を有する任意の光ディスク記録再生装置で再生することが可能である。逆に、上記ＣＡＴＶ会社と契約していなければ、会社識別信号を入手できないので、コンテンツを再生することができず、契約済みのユーザとの差別化を可能にする。

【０１６１】

また、本実施形態では、各ユーザは自宅のＣＡＴＶデコーダ１５０６に光ディスク記録再生装置１５１４からディスクＩＤ信号を送り、画像データ等を暗号化するので、ＣＡＴＶ会社装置１５０１は各ユーザに配信する暗号化コンテンツを個別に変える必要がなく、放送時のシステムを簡単にでき、低コストで、大量の視聴者に同じコンテンツを提供することができる。さらに、本実施形態によれば、ＣＡＴＶデコーダ１５０６を有する各ユーザ毎にＲＡＭ型光ディスク１枚だけに記録を許可することができる。

【０１６２】

なお、本実施形態では、ケーブルテレビジョンのヘッドエンドからコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【０１６３】

＜第５の実施形態＞

さらに、本発明に係る第５の実施形態である暗号化コンテンツ記録及び再生方法について図面を参照しながら説明する。図２１は、本発明に係る第５の実施形態である光ディスク１６０１のデータ記録領域を示す平面図であり、図２２は、第５の実施形態に係る光ディスク記録再生システムの構成を示すブロック図である。なお、第５の実施形態において、第３及び第４の実施形態と共通の部分はその説明を簡略化する。

【０１６４】

図２１において、１６０１は書き換え型又は追記型光ディスクである記録型光ディスク、１６０２はディスク情報を凹凸ピットの形式で記録されたコントロールユーザデータ領域、１６０３はレーザ光の光ビームを光ディスクに照射することによりユーザがデータを記録するためのユーザデータ領域、１６０４はディスクＩＤが記録されたＢＣＡである。

【０１６５】

ＢＣＡ１６０４では、コントロールユーザデータ領域１６０２の内周部分の凹凸ピット上の記録膜が部分的にＹＡＧレーザなどのパルスレーザでトリミングされることにより、半径方向に長い形状でかつ複数個のトリミング領域１６０６が形成される。なお、トリミングはディスク製造者によって行われる。また、ＢＣＡ１６０４に記録されるデータにディスクＩＤを付加することにより、光ディスクの管理を容易に実現することができる。さらに、ＢＣＡ１６０４のデータが凹凸ピット上に記録されることにより、ＢＣＡ１６０４に記録された、光ディスクを識別する情報が容易に改ざんされることを防止することができる。

【０１６６】

さらに、コントロールユーザデータ領域１６０２とＢＣＡ１６０４が隣接していることにより、コントロールユーザデータ領域１６０２のデータを再生する際に、ＢＣＡ１６０４のデータも続けて再生することができ、もしくはＢＣＡ１６０４のデータを再生する際に、コントロールユーザデータ領域１６０２のデータを続けて再生することができるので、

例えば光ディスクを起動する際にＣＰＵが速やかにディスクを識別するためのＢＣＡ１６０４の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【０１６７】

なお、本実施形態のＢＣＡ１６０４を、コントロールユーザデータ領域１６０２の内周部分の凹凸ピット上の記録膜をトリミングすることにより形成しているが、書き換え型又は追記型光ディスクである記録型光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールユーザデータ領域６０２の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミングの際に発生する熱からユーザデータ領域１６０３の記録データを保護することができる。また、コントロールユーザデータ領域１６０２の内周側にＢＣＡ１６０４を形成するのは、フォーカスサーボ回路の不安定性によりレーザ光のビームのスポットの径が変化する場合のマージンを考慮しているためである。なお、トリミング前のＢＣＡ１６０４に記録されているデータが、コントロールユーザデータ領域１６０２に記録されていてもよい。ＢＣＡ１６０４に記録されているデータが、コントロールユーザデータ領域１６０２にも記録されていることにより、トリミングを行ってもコントロールユーザデータ領域１６０２の上記データを保護することができる。

【０１６８】

さらに、上記データが、ＢＣＡ１６０４から、コントロールユーザデータ領域１６０２まで連続して繰り返し記録されている場合には、コントロールユーザデータ領域１６０２の上記データを見つけることによって、ＢＣＡ１６０４の位置を予想することができる。また、鍵情報記録領域１６０５のデータは、ユーザデータ領域１６０３と同じく光ビームを照射することにより記録される。

【０１６９】

本実施形態のように、コントロールユーザデータ領域１６０２と鍵情報記録領域１６０５が隣接していることにより、コントロールユーザデータ領域１６０２のデータを再生する際に、鍵情報記録領域１６０５のデータも続けて再生することができ、もしくは鍵情報記録領域１６０５のデータを再生する際に、コントロールユーザデータ領域１６０２のデータを続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかにディスクを識別するためのＢＣＡ１６０４の情報を入手し、暗号化されたコンテンツを再生するための処理を早めることが可能になる。

【０１７０】

図２２において、第５の実施形態に係る光ディスク記録再生システムは、ＣＡＴＶ会社装置１７０１と、鍵発行センター装置１７０７と、ＣＡＴＶデコーダ１７０６と、光ディスク記録再生装置１７１４と、テレビジョン装置１７３０とを備えて構成される。ここで、ＣＡＴＶ会社装置１７０１は、映画ソフトウエアなどのコンテンツを格納するコンテンツメモリ１７０２と、第１暗号鍵を格納する第１暗号鍵メモリ１７０３と、第１暗号化エンコーダ１７０４とを備える。また、ＣＡＴＶデコーダ１７０６はシステムＩＤメモリ１７０８と、第１暗号デコーダ１７１３と、現在時刻情報を出力するクロック回路１７２５とを備える。さらに、鍵発行センター装置１７０７は、当該装置１７０７の動作を制御する制御部１７０７ａと、時間制限情報を格納する時間制限情報メモリ１７１０とを備える。またさらに、光ディスク記録再生装置１７１４は、記録回路１７１７と、鍵情報記録回路１７１９と、ＢＣＡ再生回路１７２０と、データ再生部１７２１と、第２暗号デコーダ１７２２と、鍵情報再生部１７２３とを備える。

【０１７１】

まず、ＣＡＴＶ会社装置１７０１の第１暗号化エンコーダ１７０４は、コンテンツメモリ１７０２内の映画ソフトウエアなどのコンテンツのデータを第１暗号鍵１７０３を用いて暗号化することにより、第１暗号化コンテンツ１７０５を生成し、ネットワークを介して各ユーザのＣＡＴＶデコーダ１７０６の第１暗号デコーダ１７１３に送信する。ここで、コンテンツメモリ１７０２内のコンテンツをＣとし、第１暗号鍵メモリ１７０３内の第１

暗号鍵をＦＫとし、第１暗号化コンテンツ１７０５をＣ［ＦＫ］とすると、次式のように表記される。

【０１７２】

【数１０】

Ｃ＊ＦＫ＝Ｃ［ＦＫ］

【０１７３】

ＣＡＴＶデコーダ１７０６は、ＣＡＴＶデコーダ１７０６のシステムＩＤメモリ１７０８内のシステムＩＤと、例えばキーボード（図示せず。）を用いて入力された、視聴したい上記コンテンツのタイトルコード１７０９を、ネットワークを介して鍵発行センター装置１７０７の制御部１７０７ａに送信する。なお、上記タイトルコードは、テレビジョン装置１７３０の画面に従って選択することにより入力してもよいし、直接キーボードから入力してもよいし、リモートコントローラー等から入力してもよい。従って、タイトルコードは、ユーザが独自に入手していてもよいし、第１暗号化コンテンツとともにＣＡＴＶデコーダ１７０６に送られてきてもよいし、番組案内などの形態で第１暗号化コンテンツとは別の時刻に予め送られていてもよい。

【０１７４】

鍵発行センター装置１７０７の制御部１７０７ａは、ＣＡＴＶデコーダ１７０６のシステムＩＤと、上記コンテンツのタイトルコードとに基づいて、時間制限情報メモリ１７１０内の対応する時間制限情報を参照して、対応する鍵（Ｋ）１７１２を生成して、ＣＡＴＶデコーダ１７０６の第１暗号デコーダ１７１３にネットワークを介して送信する。なお、時間制限情報により、同一のコンテンツを時刻を変えて複数回放送する場合を区別することができる。ここで、第１復号鍵をＦＫとし、ＣＡＴＶデコーダ１７０６のシステムＩＤをＤＩＤとし、時間制限情報をＴＩＭＥとし、コンテンツのタイトルコードをＴとするとき、鍵（Ｋ）１７１２は、次式の関係を満たしている。

【０１７５】

【数１１】

ＦＫ＝Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ

【０１７６】

第１暗号デコーダ１７１３は、第１復号鍵（ＦＫ）と、鍵発行センター装置１７０７から送信されてくる上記鍵（Ｋ）１７１２と、上記コンテンツのタイトルコードと、システムＩＤと、時間制限情報とが上述の関係を満たしており、かつ時間制限情報がクロック回路１７２５からの現在時刻情報の条件を満たしていれば、第１暗号化コンテンツ１７０５を復号することができる。ここで、第１暗号化コンテンツ１７０５が画像信号の場合は、デスクランブルされた画像信号が第１暗号化デコーダ１７１３からテレビジョン装置１７３０に出力され、ユーザはコンテンツをテレビジョン装置１７３０で視聴できる。ここで、第１暗号化デコーダ１７１３の復号化処理は次式のように表記される。

【０１７７】

【数１２】

Ｃ［ＦＫ］＃（Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ）

＝Ｃ［ＦＫ］＃ＦＫ

＝Ｃ

【０１７８】

次に、上記コンテンツを光ディスク１６０１に記録する方法を説明する。光ディスク１６０１にコンテンツを記録する際には、ＣＡＴＶデコーダ１７０６にて復号化されていない、第１暗号化コンテンツ１７０５が、ＣＡＴＶ会社装置１７０１の第１暗号化エンコーダ１７０４から光ディスク記録再生装置１７１４の記録回路１７１７に送信される。記録回路１７１７は、受信された第１暗号化コンテンツ１７０５のデータを、例えば公知の８／１６変調方式などの変調方式を用いてディジタル変調し、変調後のディジタルデータは、光ピックアップ（図示せず。）により光ディスク１６０１に記録される。従って、光ディスク１６０１に暗号化されて記録された上記コンテンツを再生するためには、第１暗号化

コンテンツ１７０５を復号する必要がある。
【０１７９】
光ディスク記録再生装置１７１４は、ＢＣＡ再生回路１７２０により再生された、光ディスク１６０１のディスクＩＤ信号１７１５と、例えばキーボード（図示せず。）を用いて入力された、再生したい上記コンテンツのタイトルコード１７１６とを、ネットワークを介して鍵発行センター装置１７０７の制御部１７０７ａに送信する。なお、ディスクＩＤを送るタイミングは、鍵発行センター装置１７０７とアクセスする際に送ってもよいし、もしくは、視聴の際に、タイトルコードと一緒に送ってもよい。
【０１８０】
また、ディスクＩＤの送信方法として、図２２に示すように光ディスク１６０１のＢＣＡ１６０４を再生して、ＢＣＡ再生回路１７２０の出力信号を直接鍵発行センター装置１７０７に送る方法を上記で開示しているが、本発明はこれに限らず、下記の方法を用いてもよい。例えばディスク起動時などの、鍵発行センター装置１７０７とのアクセス以前に、ＢＣＡ１６０４のデータを再生して、光ディスク記録再生装置１７１４又はＣＡＴＶデコーダ１７０６のメモリ（図示せず。）に保管しておき上記タイミングで鍵発行センター装置１７０７の制御部１７０７ａに送信してもよい。さらに、ディスクＩＤが、ラベルなどの形態で視覚的にも認識できる場合には、キーボードから入力してもよいし、ラベルがバーコードになっている場合にはバーコードリーダーから読みとってもよい。
【０１８１】
鍵発行センター装置１７０７の制御部１７０７ａは、光ディスク１６０１のディスクＩＤ信号１７１５及びコンテンツのタイトルコード１７１６に対応する鍵（ＤＫ）１７１８を生成して、光ディスク記録再生装置１７１４の鍵情報記録回路１７１９に送信する。ここで、第１復号鍵をＦＫとし、光ディスク１６０１のディスクＩＤ信号１７１５をＢＣＡＳとし、コンテンツのタイトルコード１７１６をＴとするとき、鍵（ＤＫ）は、次式の関係を満たしている。
【０１８２】
【数１３】
$$FK = DK * BCA * T$$
【０１８３】
光ディスク記録再生装置１７１４の鍵情報記録回路１７１９に入力された鍵（ＤＫ）は、例えば公知の８／１６変調方式などの変調方式を用いてディジタル変調され、変調後のディジタルデータが光ピックアップ（図示せず。）により光ディスク１６０１の鍵情報記録領域１６０５に記録される。なお、鍵（ＤＫ）は鍵情報記録領域１６０５に、同一の鍵が複数個記録されてもよい。同一の鍵が複数個記録されることにより、鍵情報記録領域１６０５の記録膜が劣化した場合や、光ディスク１６０１に傷がついた場合に鍵（ＤＫ）を保護することができ、いずれか１つの鍵（ＤＫ）のデータを再生することができれば、コンテンツを復号できる。
【０１８４】
また、本実施形態では、鍵情報記録領域１６０５はユーザデータ領域１６０３の内周側に設けられているが、ユーザデータ領域１６０３の外周側にあっても良く、内周側と外周側の両方に設けられていてもよい。外周側に設けられることにより、より多くの鍵（ＤＫ）を記録することが可能となる。また、鍵情報記録領域が複数個、分散して設けられることにより、１つの鍵情報記録領域が再生できなくなった場合でも、他の鍵情報記録領域により鍵（ＤＫ）を保護することができる。
【０１８５】
一方、光ピックアップから出力されるレーザ光が光ディスク１６０１の上記コンテンツが記録された領域を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をデータ再生部１７２１に出力する。これに応答して、データ再生部１７２１は、入力された再生信号を暗号化ディジタルデータにＡ／Ｄ変換して第２暗号デコーダ１７２２に出力する。さらに、光ピックアップか

ら出力されるレーザ光は光ディスク１６０１のＢＣＡ６０４を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をＢＣＡ再生回路１７２０に出力する。これに応答して、ＢＣＡ再生回路１７２０は、入力される再生信号に基づいてディスクＩＤ信号１７１５を再生して、暗号デコーダ１７２２に出力する。さらに、光ピックアップから出力されるレーザ光は光ディスク１６０１の鍵情報記録領域１６０５を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換して再生信号を鍵情報再生部１７２３に出力し、これに応答して、鍵情報再生部１７２３は、入力される再生信号に基づいて鍵（ＤＫ）のデータを生成して、第２暗号デコーダ１７２２に出力する。

【０１８６】

なお、鍵発行センター装置１７０７に対してアクセスしてすぐにコンテンツを再生する際は、鍵情報記録回路１７１９は、鍵（ＤＫ）を鍵情報記録領域１６０５に記録する前に、直接に第２暗号デコーダ１７２２に入力してもよい。このようにすることにより、再生を開始するまでの時間を短縮することができる。暗号デコーダ１７２２は、入力されたディスクＩＤ信号１７１５と、鍵（ＤＫ）と、上記コンテンツのタイトルコード１７１６とからなる復号鍵とを用いて、暗号化されたコンテンツの復号を行う。第２暗号デコーダ１７２２の復号化処理は次式で表される。コンテンツが画像信号の場合は、例えばＭＰＥＧ信号が伸長されて、画像信号の出力信号１７２４が第２暗号デコーダ１７２２から出力される。

【０１８７】

【数１４】

Ｃ［ＦＫ］＃（ＤＫ＊ＢＣＡ＊Ｔ）
＝Ｃ［ＦＫ］＃ＦＫ
＝Ｃ

【０１８８】

本実施形態において、鍵発行センター装置１７０７の制御部１７０７ａから鍵信号を受信するときに課金されるとすると、視聴するときと、光ディスク１６０１に記録したコンテンツを初めて再生するときに別々に課金され、光ディスク１６０１に記録しただけでは課金されない。従って、視聴と光ディスク１６０１への記録の両方に対してまとめて課金する場合に対して、視聴はしたいが光ディスク１６０１に記録する必要がないユーザや、光ディスク１６０１に記録したいが、放送されるときに視聴する必要がないユーザにとっては課金される金額を安くすることができる。また、光ディスク１６０１に記録しただけでは課金されないので、ユーザは視聴した後で、再度視聴するために光ディスク１６０１を再生するための鍵を受け取るかどうかを決定することができる。以上の実施形態においては、鍵（ＤＫ）は鍵発行センター装置１７０７の制御部１７０７ａからネットワークを介して受信する方法を用いているが、本発明はこれに限らず、コンテンツのタイトルとディスクＩＤ番号を電話等で口頭で伝えることにより、口頭で受け取ってキーボードから入力してもよい。

【０１８９】

次に、鍵情報記録領域１６０５に鍵（ＤＫ）が記録された光ディスク１６０１を鍵発行センター装置１７０７とのアクセス終了後に再生する場合について説明する。まず、光ピックアップから出力されるレーザ光が光ディスク１６０１の上記コンテンツが記録された領域を照射し、その反射光が光電変換を行う光ピックアップを介してデータ再生部１７２１に入力される。これに応答して、データ再生部１７２１は暗号化されたコンテンツのデータを第２暗号デコーダ１７２２に出力する。一方、光ピックアップから出力されるレーザ光は光ディスク１６０１のＢＣＡ１６０４を照射し、その反射光が光電変換を行う光ピックアップを介してＢＣＡ再生回路１７２０に入力される。これに応答して、ＢＣＡ再生回路１７２０は入力される再生信号に基づいてディスクＩＤ信号１７１５を生成して第２暗号デコーダ１７２２に出力する。

【０１９０】

さらに、光ピックアップから出力されるレーザ光は光ディスク１６０１の鍵情報記録領域１６０５を照射し、その反射光が光電変換を行う光ピックアップを介して鍵情報再生部１７２３に入力される。これに応答して、鍵情報再生部１７２３は入力される再生信号に基づいて鍵（ＤＫ）のデータを生成して第２暗号デコーダ１７２２に出力する。第２暗号デコーダ１７２２は、入力されたディスクＩＤ信号１７１５と、鍵（ＤＫ）と、上記コンテンツのタイトルコード１７１６からなる復号鍵を用いて、データ再生部１７２１から出力される、暗号化されたコンテンツの復号を行う。第２暗号デコーダ１７２２の復号化処理は次式で表される。コンテンツが画像信号の場合は、例えばＭＰＥＧ信号が伸長されて、画像信号が第２暗号デコーダ１７２２から出力される。

【０１９１】

【数１５】

Ｃ［ＦＫ］＃（ＤＫ＊ＢＣＡ＊Ｔ）
＝Ｃ［ＦＫ］＃ＦＫ
＝Ｃ

【０１９２】

鍵情報記録領域１６０５に鍵（ＤＫ）のデータが一度記録されることにより、鍵発行センター装置１７０７とのアクセスをすることなく、常に上記暗号化コンテンツを再生することができる。また、復号化処理に必要な復号鍵は全て光ディスク１６０１に記録されているので、上記光ディスク１６０１は、ＢＣＡ再生回路１７２０と、鍵情報再生部１７２３と、第２暗号デコーダ１７２２とを有する任意の光ディスク記録再生装置で再生することができる。

【０１９３】

さらに、上記暗号化コンテンツをディスクＩＤの異なる光ディスク１６０１にコピーして再生しようとした場合には、ＢＣＡ再生回路１７２０から上記光ディスク１６０１とは異なるディスクＩＤ信号が出力されるので、暗号化されたコンテンツを復号することができず、コンテンツはコピーされても再生されない。ただ、この場合にも、コンテンツのタイトルとディスクＩＤをネットワークもしくは口頭で鍵発行センターに伝えることにより、課金の後、復号鍵を受け取ってもよい。このように、暗号化されたコンテンツを別の光ディスク１６０１にコピーされても、不正に再生されることはなく、暗号化されたコンテンツをコピーした光ディスク１６０１を再生する際には必ず課金が伴うことから著作権を保護することができる。

【０１９４】

図２３は、第５の実施形態に係るＩＤ付与テーブルの構成を示す表であり、システムＩＤやディスクＩＤが異なる場合の第１暗号デコーダ１７１３に入力される鍵（Ｋ）と、鍵情報記録回路１７１９に入力される鍵（ＤＫ）とを整理して示したものである。図２３において、Ｔ１、Ｔ２、Ｔ３は異なるコンテンツのタイトルコードであり、ＦＫ１、ＦＫ２、ＦＫ３はそれぞれＴ１、Ｔ２、Ｔ３のタイトルコードを有する暗号化コンテンツを復号するための復号鍵である。また、ＤＩＤ１、ＤＩＤ２、ＤＩＤ３はそれぞれ異なるＣＡＴＶデコーダ１７０６のシステムＩＤであり、ＢＣＡＳ１、ＢＣＡＳ２、ＢＣＡＳ３はそれぞれ異なる光ディスク１６０１のディスクＩＤである。このとき、ＣＡＴＶデコーダ１７０６に入力される鍵（Ｋｍｎ）は、次式を満足するように決定される。

【０１９５】

【数１６】

ＦＫｎ＝Ｋｍｎ＊Ｔｎ＊ＤＩＤ＊ＴＩＭＥｎ

【０１９６】

また、光ディスク記録再生装置１７１４に入力される鍵（ＤＫｍｎ）は、次式を満足するように決定される。

【０１９７】

【数１７】

ＦＫｎ＝ＤＫｍｎ＊ＢＣＡｍ＊Ｔｎ

【０１９８】
図２３に示すように、コンテンツが異なるときはもちろんのこと、コンテンツが同じ場合でも、異なるＣＡＴＶデコーダ１７０６、異なる光ディスク、異なる放送時間毎に鍵発行センター装置１７０７から入手する鍵情報は異なることから細部にわたる著作権の保護が可能になる。同様に、コンテンツが同じでもシステムＩＤ、ディスクＩＤ、時間情報が異なれば鍵情報が異なることから、ＣＡＴＶ会社装置１７０１は、ユーザ毎に暗号化コンテンツを変える必要がなく、１つのコンテンツに対して１つの暗号化コンテンツを準備すればよい。これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。
【０１９９】
なお、本実施形態では、ケーブルテレビジョンのヘッドエンドからのコンテンツを放送する場合について説明したが、電波による放送でも同様である。
【０２００】
＜第３乃至第５の実施形態の効果＞
本実施形態に係る光ディスクは、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域を有する。従って、従来技術の光ディスクに、上記光ディスクを識別する情報を付加することにより、光ディスクの管理を容易に実現することができる。ここで、上記第２の情報領域は、好ましくは、上記第１の情報領域内に記録されているものであり、上記第１の情報領域を再生する光ピックアップによって再生することができる。また、上記第２の情報領域は、上記第１の情報領域内の記録膜を、半径方向に長い形状でかつ複数個のトリミング領域が形成されるように、部分的に除去することにより記録されているものであり、容易に上記第２のディスク情報が改ざんされることを防止することができる。
【０２０１】
また、本実施形態に係る暗号化コンテンツの記録方法によれば、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域を有する光ディスクの上記ユーザデータ領域にコンテンツのデータを記録する際に、少なくとも上記第２のディスク情報を用いた演算によりコンテンツのデータを復号して再生することができるように、コンテンツのデータを暗号化して記録する。従って、特定の１枚の光ディスクにしか存在しない光ディスクの識別情報を用いて、コンテンツを暗号化することにより、コンテンツの不正なコピーを防止することができ、著作権が保護できるという特有の効果がある。
【０２０２】
さらに、本実施形態に係る光ディスクは、ユーザデータ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する。従って、暗号化されて記録されたコンテンツを解読する際に鍵情報が必要なシステムにおいて、鍵情報記録領域に鍵情報が一度記録されることにより、再生する度に鍵情報を入力する必要がなくなるという特有の効果がある。
【０２０３】
またさらに、本実施形態に係る暗号化コンテンツの記録方法によれば、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域と、ユーザデータ領域内に、暗号化されて記録されたコンテンツのデータを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの上記ユーザデータ領域にコンテンツを記録する際に、少なくとも上記第２のディスク情報と、上記鍵情報を用いた演算によりコンテンツのデータを復号して再生することができるようにコンテンツのデータを暗号化して記録する。従って、暗号化されたコンテンツのデータを別の光ディスクにコピーされても、不正に再生されることはなく、暗号化されたコンテンツ

のデータをコピーした光ディスクを再生する際には必ず課金が伴うことから著作権を保護することができる。

【０２０４】

ここで、第１のディスク情報は、好ましくは、微少な凹凸ピットにより構成され、光ディスクを識別するための第２のディスク情報が、上記凹凸ピット上に記録される。従って、容易に第２のディスク情報が改ざんされることを防止することができる。さらに、好ましくは、上記第１のディスク情報と第２のディスク情報が隣接するように形成される。これにより、上記第１のディスク情報を再生する際に、第２のディスク情報も続けて再生することができ、もしくは第２のディスク情報を再生する際に、第１のディスク情報を続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかにディスクを識別するための第２のディスク情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【０２０５】

また、本実施形態に係る暗号化データの記録方法によれば、コンテンツが同じでもシステムＩＤ、ディスクＩＤ、時間情報が異なれば鍵情報が異なることから、ＣＡＴＶ会社装置７０１は、ユーザ毎に暗号化コンテンツを変える必要がなく、１つのコンテンツに対して１つの暗号化コンテンツを準備すればよく、これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【０２０６】

＜第３及び第５の実施形態の変形例＞

以上の第３と第５の実施形態においては、図１６及び図２１に示すように、トリミング領域１１０５，１６０６はそれぞれ、コントロールユーザデータ領域１１０２，１６０２内の内周部に位置するＢＣＡ１１０４，１６０４に形成しているが、本発明はこれに限らず、それぞれ第３と第５の実施形態の変形例に係る光ディスク１１０１ａ，１６０１ａのデータ記録領域を示す図２４及び図２５に示すように、コントロールユーザデータ領域１１０２，１６０２から光ディスクの内周側にはみ出るように記録膜をトリミングしてトリミング領域１１０５ａ，１６０６ａを形成してもよい。すなわち、ＢＣＡ１１０４ａ，１６０４ａはそれぞれ、コントロールユーザデータ領域１１０２，１６０２内に含まれず、コントロールユーザデータ領域１１０２，１６０２の内周部から、コントロールユーザデータ領域１１０２，１６０２の内側にはみ出るように配置されて形成される。この変形例において、ＢＣＡ１１０４ａ，１６０４ａをこのように形成するのは、フォーカスサーボ回路の不安定性によりレーザ光のビームのスポットの径が変化する場合のマージンを考慮しているためである。この変形例においても、コントローラユーザデータ領域１１０２，１６０２の外側にユーザデータ領域１１０３，１６０３が存在しているので、これらのユーザデータ領域１１０３，１６０２に記録されたデータを破壊しないように保護するために、トリミング領域１１０５ａ，１６０６ａが配置されて形成される。

【０２０７】

＜第６の実施形態＞

図２６は、本発明に係る第６の実施形態である光ディスク内のユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。本実施形態において、光ディスクは、例えば、ＤＶＤ－ＲＡＭなどの記録型光ディスクである。

【０２０８】

図２６に示すように、ユーザデータ領域２１５０は、セクタヘッダ領域２１０１と、メインデータ領域２１０２と、誤り検出コード２１０３とから構成される。セクタヘッダ領域２１０１には、セクタの位置を示すセクタアドレス２１０４と、メインデータ領域２１０２に記録されるデータに関する著作権制御情報（スクランブルフラグ、コピー制御情報などを含む。）が記録される著作権制御情報２１０５とが記録されるとともに、セクタヘッド領域２１０１は、メインデータ領域２１０２のデータに暗号が施されている場合に復号するための復号鍵領域２１０６を含む。また、メインデータ領域２１０２は、非暗号化コ

ンテンツ２１０７が記録される領域と、暗号化コンテンツ２１０８が記録される領域とに分割され、非暗号化コンテンツ２１０７は、ＭＰＥＧにおける同期パターンや、各種制御情報などの後続するデータの制御情報を含む。さらに、暗号化コンテンツ２１０８は、主に著作権保護を必要とするＡＶデータなどが暗号化されたコンテンツのデータを含む。

【０２０９】

復号鍵領域２１０６には、後続するメインデータ領域２１０２を再生するための復号鍵が所定のサイズを有する複数の分割された復号鍵（以下、分割復号鍵という。）に分割されて記録される。例えば、４バイトの１つの復号鍵領域に対して復号鍵が８バイトである場合、８バイトの復号鍵を各４バイトの分割復号鍵に分割し、論理的に連続する２つのセクタの復号鍵領域２１０６，２１０９にそれぞれ、分割された２つの分割復号鍵を記録する。このようなユーザデータ領域の再生時には、論理的に連続する（ただし、欠陥等により使用不可能なセクタはスキップする。）複数のセクタの復号鍵領域２１０６，２１０９から分割された複数の分割復号鍵を取得し、取得された必要数の分割復号鍵をデータ連結器２１１１にて連結し、再生に必要な暗号化復号鍵（８バイト）を得る。暗号化復号鍵（８バイト）を得ることのできたセクタのメインデータ領域２１０２に記録されたデータに対して、それぞれの著作権制御情報２１０５の内容に従って、復号器２１１４を用いて復号化処理を実行する。

【０２１０】

さらに、より暗号の強度を高めるために、復号鍵に対して暗号化を施すことも可能であるし、暗号の結果が一定とならないように、データ中の情報である復号鍵変換データを鍵に加えることにより、同一の暗号鍵であっても、異なる暗号結果を提供することも可能である。具体的には、図２６に示すように、データ連結器２１１１から出力される暗号化復号鍵が鍵復号器２１１２に入力され、鍵復号器２１１２は、入力された暗号化復号鍵を、所定のディスク鍵を用いて、ダミーデータであるパディングデータ（１バイト）と復号鍵（７バイト）に復号化して鍵変換器２１１３に出力する。ここで、ディスク鍵は、例えば、光ディスクに記録された暗号化ディスク鍵を、所定のマスター鍵である秘密鍵を用いて、ディスク鍵復号器（図示せず。）により復号することにより取得される。次いで、鍵変換器２１１３は、メインデータ領域２１０２から読み出した復号鍵変換データ２１１０を、上記鍵復号器２１１２から出力される復号鍵を用いて、例えば乗算や除算、所定の重み係数を用いた演算などの所定の変換演算によりデータ変換することによりコンテンツ復号鍵（７バイト）を生成して復号器２１１４に出力する。そして、復号器２１１４は、メインデータ領域２１０２から読み出したコンテンツのデータを、上記鍵変換器２１１３から出力されるコンテンツ復号鍵（７バイト）を用いて復号することにより、復号化されたコンテンツのデータを生成して出力する。なお、復号鍵変換データ２１１０としては、コピー世代管理情報や、アナログのマクロビジョン制御フラグなどの改ざんがされることによりデータの不正利用がすぐに検出可能であるようなデータを利用することが好ましい。

【０２１１】

図２７は、第６の実施形態に係る光ディスクにおいて、ユーザデータ領域への著作権制御情報と復号鍵の配置と、メインデータ領域への暗号化コンテンツの配置を示すブロック図である。図２７に図示されたユーザデータ領域２１５０の一例においては、復号鍵領域が、４バイトの分割復号鍵を有する第１の復号鍵領域２２０１と、４バイトの分割復号鍵を有する第２の復号鍵領域２２０２とに分割されて配置されている。このため、これらの２つのセクタに記録する暗号化コンテンツの大きさによらず、複数のセクタ（図２７では２つのセクタ）が使用されることとなる。この場合、未使用の領域には、ダミーデータが補完データとして記録される。図２７の例では、１セクタ分の暗号化コンテンツ２２０４しかない場合には、１セクタ分の補完データ２２０３が記録される。

【０２１２】

図２８は、第６の実施形態に係る光ディスクにおいて、エラー訂正の単位が複数のセクタにまたがる場合の配置を示すブロック図である。例えば、光ディスクがＤＶＤである場合、１６セクタのエラー訂正コードの単位ブロック（以下、ＥＣＣブロックという。）を用

いることにより、エラー訂正の能力を高めている。このため、データの記録や再生を行う際には、ＥＣＣブロック単位での記録が必要となる。復号鍵を任意の複数の分割復号鍵に分割して記録を行ったとすると、１つの復号鍵が複数のエラー訂正ブロックにまたがって記録される場合が発生する。再生の際には、分割された複数の分割復号鍵のすべてを再生する必要があるため、暗号化コンテンツのデータを記録したセクタ以外にも、復号鍵を記録した直前のＥＣＣブロックまでも再生する必要がある。図２８の例では、復号鍵を分割するときの分割数をＥＣＣブロックのセクタ数の約数に設定することを特徴としている。これにより、分割された複数の分割復号鍵がＥＣＣブロックにまたがって記録されることがなくなる。さらに、１つのＥＣＣブロック内で使用する復号鍵として、１種類の復号鍵のみを用い、記録するＡＶデータがＥＣＣブロックに満たない場合には、補完データ、並びに補完セクタを配置することによって、再生時に不要なセクタのデータを光ディスクから読み出すことを防止することができる。

【０２１３】

＜第７の実施形態＞

図２９は、本発明に係る第７の実施形態である光ディスク内のリードイン領域２４０１とユーザデータ領域２４０２の構成と、リードイン領域２４０１とユーザデータ領域２４０２のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。

【０２１４】

図２９において、図２６の第６の実施形態と同様に、リードイン領域２４０１とユーザデータ領域２４０２はそれぞれ、セクタヘッダ領域２１０１と、メインデータ領域２１０２と、誤り検出コード２１０３とを有するセクタから構成される。セクタヘッダ領域２１０１には、セクタの位置を示すセクタアドレス２１０４と、メインデータ領域２１０２に記録されるデータに関する著作権制御情報（スクランブルフラグ、コピー制御情報などを含む。）が記録される著作権制御情報２１０５とが記録されるとともに、セクタヘッダ領域２１０１は、メインデータ領域２１０２のデータに対して暗号が施されている場合に復号するための復号鍵を参照するための、復号鍵の記録位置（メインデータ領域２１０２内の復号鍵テーブル２４０４での記録位置又は格納位置をいう。）を示す鍵インデックスを記録する鍵インデックス領域２４０３を含む。ユーザデータ領域２４０２に記録された暗号化コンテンツを復号するための復号鍵は、テーブル形式で書き換え可能なリードイン領域２４０１に復号鍵テーブル２４０４の形式で記録される。鍵インデックス領域２４０３に記録される鍵インデックスによりリードイン領域２４０１に記録された復号鍵が参照される。図２６に図示された第６の実施形態と同様に、上記参照された復号鍵は、所定のディスク鍵を用いる鍵復号器２１１２によりパディングデータと復号鍵（又はタイトル鍵）とに復号された後、上記復号された復号鍵（又はタイトル鍵）は、復号鍵変換データを用いる鍵変換器２１１３によりコンテンツ復号鍵に変換されて復号器２１１４に出力される。復号器２１１４は、暗号化されたコンテンツのデータを、コンテンツ復号鍵を用いて復号することにより、復号化コンテンツのデータを生成して出力する。

【０２１５】

以上のように構成された第７の実施形態に係る光ディスクと光ディスク再生装置においては、セクタヘッダ領域２１０１内にある鍵インデックス領域２４０３に参照用の鍵インデックスを記録することにより、鍵インデックス領域２４０３のサイズとは独立に復号鍵テーブル２４０４の復号鍵サイズを割り当てることができる。また、復号鍵テーブル２４０４のサイズを割り当てた後も、鍵インデックス領域２４０３内の鍵インデックスで示される復号鍵テーブル２４０４から連続して複数の復号鍵を使用することにより、自由なサイズの復号鍵を利用することができる。

【０２１６】

図３０（ａ）は第７の実施形態に係る光ディスク内のリードイン領域２４０１のメインデータ領域２１０２において、復号鍵の初期値で未記録状態を表示する場合のデータ構成を示すブロック図である。図３０（ａ）において、光ディスクのフォーマット時などにおい

て記録される復号鍵の初期値として、鍵として使用しない既知の固定値（例えば、オール０などのデータ）である未記録状態データ２５０１を記録し、これにより、復号鍵の未記録状態を示す。

【０２１７】

図３０（ｂ）は第７の実施形態に係る光ディスク内のリードイン領域２４０１のメインデータ領域２１０２において、復号鍵状態テーブルで記録状態を表示する場合のデータ構成を示すブロック図である。図３０（ｂ）においては、図３０（ａ）に図示された復号鍵と同様に、インデックスにより参照可能なテーブル形式の復号鍵状態テーブル２５０２をリードイン領域２４０１に配置し、復号鍵の記録状態を記録状態データ２５０３として以下のように記載している。

（１）０ｘ００：未使用、
（２）０ｘ０１：領域予約、
（３）０ｘ０３：鍵記録済み、
（４）その他：予約済み。

ここで、０ｘは、それに続く文字について１６進数表示を示す。

【０２１８】

図３１は、第７の実施形態に係る光ディスクにおいて復号鍵の配置を示すブロック図である。図３１の例では、復号鍵の信頼性を高めるためにディスク上への復号鍵領域の配置を工夫している。通常、ユーザデータ領域２６０２においては欠陥管理が行われるため、書き込み不良が発生した場合には、代替領域等へ交代処理が行われる。しかしながら、リードイン領域２６０１では、上記のような欠陥管理は行われない。このため、書き込み不良や読み出し不良などの発生により、ＡＶデータの再生に必要な復号鍵が利用不能となり、さらには光ディスクそのものが利用不能となる場合がある。従って、異なる複数のＥＣＣブロックにわたって、合計複数の復号鍵を記録しておくことが望ましい。また、近接した領域に複数の復号鍵を記録した場合、傷や埃等により複数記録したものがすべて読めなくなる場合がある。このため、図３１に示すように、リードイン領域２６０１とリードアウト領域２６０３においてそれぞれ、光ディスクの内周側と外周側といったようなレイアウト上離れた位置に各復号鍵を記録しておくことがより好ましい。

【０２１９】

なお、図２９の実施形態においては、復号鍵領域をリードイン領域２４０１，２６０１に配置している。これは、ユーザデータ領域２６０２が通常のリードコマンドやライトコマンドでアクセス可能な領域であることを考慮し、パーソナルコンピュータのドライブ装置などからアクセスするときの安全性を高めるためである。従って、これらをユーザデータ領域２６０２に配置しても、同様の効果を得ることができる。

【０２２０】

＜第８の実施形態＞

図３２は、本発明に係る第８の実施形態である光ディスクのデータをファイル管理システムにより管理するときのデータ構成を示すブロック図である。図３２の例では、ファイルシステムの構造に基づいて、所望のファイルが格納されたセクタアドレスを管理している。

【０２２１】

国際標準化機構によりＩＳＯ１３３４６において規定されたファイルシステムの構造では、書き換え可能型光ディスクに対応するために、ファイルの記録位置はファイルエントリと呼ばれる情報を用いて管理される。図３２に示すように、例えば、ファイル（１）２７０３の記録位置のデータは、ファイル管理情報領域２７５１内のファイルエントリ（１）２７０１として格納され、ファイル（２）２７０４の記録位置のデータはファイルエントリ（２）２７０２として格納される。各ファイルは、光ディスク上で連続した複数のセクタの領域を管理するエクステント２７０５，２７０６で構成される。光ディスク上には、ファイルエントリが示すメインデータ領域２１０２において、第７の実施形態で示した暗号化コンテンツが記録され、また、復号鍵がリードイン領域２６０１内の復号鍵テーブル

２７０７に記録される。暗号化コンテンツが記録されたユーザデータ領域２６０２内のセクタヘッダ領域２１０１には、復号に必要な復号鍵を参照するための記録位置を示すポインタが、鍵インデックス領域２７０８において記録される。なお、本実施形態では、ファイル単位とエクステント単位で復号鍵を管理して記録しているが、本発明はこれに限らず、ファイル単位とエクステント単位とのうちの少なくとも一方で復号鍵を管理して記録してもよい。

【０２２２】

上記のようにファイルシステムにより管理される光ディスクにおいて、著作権保護を必要とするコンテンツの記録動作について図３３を用いて説明する。図３３は、第８の実施形態に係るファイル管理システムによって実行される、著作権保護を必要とするコンテンツの記録処理を示す。

【０２２３】

暗号化コンテンツの記録の際には、まず、ステップＳ２８０１において、図３０（ｂ）に図示された復号鍵状態テーブル２５０２を読み出して、復号鍵テーブル２７０７の空き領域を調べる。次いで、ステップＳ２８０２において、復号鍵テーブル２７０７の空き領域があるか否かが判断され、ＮＯのときは、暗号化コンテンツに対する復号鍵が記録できないために、ステップＳ２８０７において記録動作を中止して当該コンテンツの記録処理を終了する。一方、ステップＳ２８０２でＹＥＳであるときは、取得済みの復号鍵（又はタイトル鍵）を記録し、また、復号鍵を取得できていない場合には、復号鍵領域の予約を行う。次いで、ステップＳ２８０４では、記録するコンテンツの著作権制御情報（暗号化を行うか否かの情報と、暗号化の種類を示す種別の情報などを含む。）と、鍵インデックス領域２７０８に記録する鍵インデックスの設定を行った後、ステップＳ２８０５においてコンテンツを暗号化してエクステント単位でファイル形式で光ディスク上に記録する。このとき、ファイル単位で同一の著作権制御情報と鍵インデックスを使用してもよいし、エクステント単位でこれらを切り替えてもよい。すなわち、ステップＳ２８０４及びＳ２８０５において、処理する単位は、ファイル単位と、エクステント単位とのうちの少なくとも一方である。最後に、ステップＳ２８０６において、記録したコンテンツに関する情報に基づいて、上記記録されたデータを管理するためのファイル管理情報の更新を行った後、当該コンテンツの記録処理を終了する。

【０２２４】

図３４は、第８の実施形態に係るファイル管理システムによって実行される、コンテンツの再生処理を示すフローチャートである。図３４では、図３３に示した方法によりファイル形式で記録したコンテンツを光ディスクから再生する処理を示す。

【０２２５】

ファイルの再生動作を行う際には、再生するファイルが使用している復号鍵テーブルの領域を知るため、ファイル管理情報領域２７５１内のファイルエントリにより示される領域に対する鍵インデックスを取得する。具体的には、ステップＳ２９０１において、ファイル管理情報２７５１から再生するファイルのファイルエントリを読み出して再生することにより取得した後、ステップＳ２９０２において、ファイルエントリにより示される領域のセクタヘッダ領域２１０２から鍵インデックス領域の値を読み出して再生することにより取得する。エクステント単位で異なる暗号を行っている場合には、それぞれのエクステントにおいてセクタヘッダ中の鍵インデックス領域を読み出す。次いで、ステップＳ２９０３において、取得した鍵インデックスにより示される復号鍵テーブル２７０７の復号鍵領域から復号鍵を読み出して再生することにより取得する。さらに、ステップＳ２９０４において、ファイルエントリで示される領域からファイル内のコンテンツのデータを読み出して再生し、再生したコンテンツのデータを復号する。ここで、コンテンツのファイルの再生と復号が終了すれば、当該コンテンツの再生処理を終了する。

【０２２６】

図３５は、第８の実施形態に係るファイル管理システムによって実行される、コンテンツの削除処理を示すフローチャートであり、図３５では、図３３に示した方法により記録し

たファイル形式のコンテンツのデータを削除する動作について示す。

【０２２７】

ファイルの削除動作を行う際には、削除するファイルが使用している復号鍵テーブル２７０７の領域を知るため、ファイルエントリにより示される領域に対する鍵インデックスを取得する。具体的には、ステップＳ３００１において、ファイル管理情報領域２７５１内のファイル管理情報から削除するファイルのファイルエントリを取得した後、ステップＳ３００２においてファイルエントリにより示される領域のセクタヘッダから鍵インデックス領域の値を取得する。ここで、エクステント単位で異なる暗号を行っている場合には、それぞれのエクステントにおいてセクタヘッダ中の鍵インデックス領域を読み出す。次いで、ステップＳ３００３において、取得した鍵インデックスにより示される復号鍵テーブル２７０７の復号鍵領域から復号鍵を開放した（ここで、復号鍵の開放とは、当該復号鍵を当該テーブルから削除することをいう。）後、ステップＳ３００４において削除するファイルの書き込み位置を示すファイルエントリをファイル管理情報から削除して、当該コンテンツの削除処理を終了する。従来のファイルシステムでは、ファイルを削除する際にファイルエントリのみの削除を行っていたが、復号鍵と暗号化コンテンツの記録セクタが別の領域に記録されているために、別の領域に記録された復号鍵を削除できない。上述の実施形態においては、ファイルエントリの削除に先立って、セクタヘッダ領域中の鍵インデックスの示す復号鍵を復号鍵テーブル２７０７から削除することにより、光ディスク上での復号鍵の管理を行っている。

【０２２８】

＜第９の実施形態＞

図３６は、本発明に係る第９の実施形態である光ディスクシステムの構成を示すブロック図であり、この光ディスクシステムは、光ディスク３１００に著作権保護を必要とするコンテンツを記録及び再生する情報処理システムである。当該光ディスクシステムは、エンコード装置３１０１と、光ディスク装置３１０２と、デコード装置３１０３と、パーソナルコンピュータ３１０４とを備えて構成される。

【０２２９】

エンコード装置３１０１は、コンテンツのデータを格納するコンテンツメモリ３１３１と、上記コンテンツのデータをＭＰＥＧフォーマットの形式で符号化する符号化回路３１３２と、暗号鍵を格納する暗号鍵メモリ３１３３と、符号化されたコンテンツのデータを暗号鍵を用いて暗号化するとともに復号鍵を生成して復号鍵メモリ３１１１に格納する暗号回路３１３４と、復号鍵を格納する復号鍵メモリ３１１１と、復号鍵をバス暗号化するバス暗号回路３１１２と、パーソナルコンピュータ３１０４のインターフェース３１２２にＰＣＩバス３１５１を介して接続され暗号化されたコンテンツのデータや復号鍵を送信するインターフェース３１２４とを備える。また、光ディスク装置３１０２は、複数の復号鍵を格納する復号鍵テーブルメモリ３１１３と、バス暗号及び復号回路３１１４と、光ディスク３１００に対してデータを記録するとともに光ディスク３１００からデータを読み出して再生する記録再生回路３１１９と、パーソナルコンピュータ３１０４のインターフェース３１２１とＳＣＳＩバス３１５２を介して接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース３１２０とを備える。なお、ＳＣＳＩバス３１５２はＡＴＡＰＩバスであってもよい。ここで、バス暗号化及びバス復号化とはそれぞれ、ＰＣＩバス３１５１やＳＣＳＩバス３１５２上で暗号鍵や復号鍵を暗号化して送信し受信するために用いる暗号化処理、及び復号化処理をいう。

【０２３０】

さらに、パーソナルコンピュータ３１０４は、その動作を制御する制御部３１３０と、複数のバス暗号化復号鍵を格納するバス暗号化復号鍵テーブルメモリ３１１５と、上記複数のバス暗号化復号鍵に対応する複数の復号鍵ステータス（復号鍵の記録状態を示し、具体的には、未使用、領域予約、鍵記録済み、予約済みなどを示す。）のデータを格納する復号鍵状態テーブルメモリ３１１６と、光ディスク装置３１０２のインターフェース３１２０とＳＣＳＩバス３１５２を介して接続されデータや信号の送信及び受信並びに信号変換

、プロトコル変換などの処理を実行するインターフェース３１２１と、デコード装置３１０３のインターフェース３１２３及びエンコード装置３１０１のインターフェース３１２４とＰＣＩバス３１５１を介して接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース３１２２とを備える。またさらに、デコード装置３１０３は、パーソナルコンピュータ３１０４のインターフェース３１２２と接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース３１２３と、インターフェース３１２３によって受信された暗号化復号鍵をバス復号化するバス復号回路３１１７と、復号鍵を格納する復号鍵メモリ３１１８と、インターフェース３１２３によって受信された暗号化コンテンツのデータを復号鍵メモリ３１１８の復号鍵を用いて復号するとともに、ＭＰＥＧフォーマットの復号化処理を行って画像信号や音声信号を生成してディスプレイ装置３１０５に出力する復号化回路３１４１とを備える。

【０２３１】

この光ディスクシステムのエンコード装置３１０１においては、符号化回路３１３２は、コンテンツメモリ３１３１に格納され又は入力されるＡＶデータなどのコンテンツのデータをＭＰＥＧのフォーマットの形式で符号化し、暗号回路３１３４は、パーソナルコンピュータ３１０４上でのコンテンツの不正利用を避けるために生成された暗号鍵メモリ３１３３内の暗号鍵を用いて上記符号化されたコンテンツのデータを暗号化し、暗号化されたコンテンツのデータをインターフェース３１２４及びパーソナルコンピュータ３１０４を介して光ディスク装置３１０２に送信する。ここで、暗号化されたコンテンツのデータは、エンコード装置３１０１のインターフェース３１２４からＰＣＩバス３１５１と、パーソナルコンピュータ３１０４のインターフェース３１２２及びインターフェース３１２１と、光ディスク装置３１０２のインターフェース３１２０を介して記録再生回路３１１９に送信される。そして、暗号化されたコンテンツのデータは、光ディスク装置３１０２の記録再生回路３１１９により光ディスク３１００に記録される。また、光ディスク装置３１０２の記録再生回路３１１９は、光ディスク３１００に記録されている暗号化コンテンツのデータを再生して、再生された暗号化コンテンツのデータを、インターフェース３１２０と、パーソナルコンピュータ３１０４のインターフェース３１２１及びインターフェース３１２２と、デコード装置３１０３のインターフェース３１２３を介して復号化回路３１４１に送信する。デコード装置３１０３の復号化回路３１４１は、暗号化コンテンツのデータに対する暗号を復号化しかつＭＰＥＧフォーマットの復号化処理を行い、復号化されたコンテンツの画像信号や音声信号をそれぞれディスプレイ装置３１０５やスピーカ装置（図示せず。）に出力する。

【０２３２】

エンコード装置３１０１の暗号回路３１３４は、ＭＰＥＧフォーマットの形式で符号化されたコンテンツのデータに対して、暗号鍵メモリ３１３３内の暗号鍵を用いて暗号化を行うと同時に、再生時に必要な復号鍵を生成して復号鍵メモリ３１１１に格納する。光ディスク３１００には、符号化されたコンテンツのデータと復号鍵を記録する必要があるが、パーソナルコンピュータ３１０４上で復号鍵を平文のまま取り扱う場合には、復号鍵を光ディスク３１００から読み出すことにより、暗号化されたコンテンツのデータの解読が容易になってしまう可能性がある。これを避けるために、エンコード装置３１０１と光ディスク装置３１０２の間で、相互認証を行うとともに相互に共有したバス鍵を用いてバス暗号を行う。

【０２３３】

すなわち、具体的には、復号鍵メモリ３１１１内の復号鍵はエンコード装置３１０１のバス暗号回路３１１２によって暗号化が施された後、その暗号化復号鍵は、インターフェース３１２４、ＰＣＩバス３１５１及びインターフェース３１２２を介してパーソナルコンピュータ３１０４のバス暗号化復号鍵テーブルメモリ３１１５に格納される。一方、光ディスク装置３１０２のバス暗号及び復号回路３１１４においては、光ディスク３１００から記録再生回路３１１９により再生された、暗号化復号鍵の復号化が行われた後、復号化

された復号鍵は復号鍵テーブルメモリ３１１３に格納される。また、バス暗号及び復号回路３１１４は、例えば更新されたバス暗号化された復号鍵を、バス暗号化復号鍵テーブルメモリ３１１５からインターフェース３１２１、ＳＣＳＩバス３１５２及びインターフェース３１２０を介して受信してバス復号化して復号鍵テーブルメモリ３１１３に格納した後、記録再生回路３１１９を介して光ディスク３１００に記録する。

【０２３４】

また、復号鍵状態テーブルは記録再生回路３１１９により光ディスク３１００から再生された後、インターフェース３１２０、ＳＣＳＩバス３１５２及びインターフェース３１２１を介して復号鍵状態テーブルメモリ３１１６に転送されて格納される。さらに、パーソナルコンピュータ３１０４で更新された復号鍵状態テーブルは、復号鍵状態テーブルメモリ３１１６から読み出されて、インターフェース３１２１、ＳＣＳＩバス３１５２及びインターフェース３１２０を介して記録再生回路３１１９に転送された後、記録再生回路３１１９は受信した復号鍵状態テーブルを光ディスク３１００に記録する。従って、中間に位置するパーソナルコンピュータ３１０４上では、複数のバス暗号化復号鍵を格納するバス暗号化復号鍵テーブル３１１５と復号鍵状態テーブルメモリ３１１６とを用いて、暗号化された復号鍵のみが取り扱われることになり、一層の安全性が確保されることになる。

【０２３５】

光ディスク装置３１０２とデコード装置３１０３の間でも同様に復号鍵のバス暗号を行うことにより、一層の安全性が確保される。すなわち、デコード装置３１０３のバス復号回路３１１７は、パーソナルコンピュータ３１０４からインターフェース３１２３を介して受信した暗号化復号鍵を復号して復号鍵メモリ３１１８に格納する。復号化回路３１４１は、復号鍵メモリ３１１８内の復号鍵を用いて暗号化されたコンテンツのデータを復号する。

【０２３６】

上述の第７の実施形態に示したように、光ディスク３１００上に暗号化されたコンテンツのデータを復号するための復号鍵をテーブル形式で記録するような場合には、光ディスク装置３１０２上で再生した復号鍵テーブルをバス暗号及び復号回路３１１４によりバス暗号化した後、バス暗号化された復号鍵テーブルのデータをインターフェース３１２０を介してパーソナルコンピュータ３１０４のバス暗号化復号鍵テーブルメモリ３１１５に転送して格納する。コンテンツのデータを記録するときには、パーソナルコンピュータ３１０４が平文で光ディスク３１００に記録されている復号鍵状態テーブルから復号鍵テーブルの空き領域を検索することにより調べ、エンコード装置３１０１から転送されるバス暗号化された復号鍵を空き領域に割り当てる。このとき、バス暗号として復号鍵単位で完結するような暗号（例えば、復号鍵長単位でのブロック暗号）を用いれば、復号鍵ブロックへの割り当て時に、復号鍵の復号し再暗号する必要がない。

【０２３７】

なお、光ディスク装置３１００と、光ディスク装置３１０２と、パーソナルコンピュータ３１０４と間で転送されて格納される復号鍵テーブルや復号鍵状態テーブルはそれぞれ、１つのかたまりのブロックのデータであるので、ブロックデータということができる。

【０２３８】

コンテンツの再生時の場合も、光ディスク装置３１０２から再生された復号鍵ブロックから再生しようとしているコンテンツの復号化に必要な復号鍵のみを、バス暗号化復号鍵テーブルメモリ３１１５から検索して抜き出し、パーソナルコンピュータ３１０４及びデコード装置３１０３のバス復号回路３１１７を介して復号鍵メモリ３１１８に転送して格納する。そして、復号化回路３１４１は、光ディスク装置３１０２の記録再生回路３１１９によって光ディスク３１００から再生された暗号化されたＡＶデータを、パーソナルコンピュータ３１０４及びインターフェース３１２３を介して受信して、受信された暗号化されたＡＶデータを復号鍵メモリ３１１８内の復号鍵を用いて画像信号や音声信号に復号化して出力する。この場合も、上述のコンテンツの記録時と同様に、バス暗号として復号鍵単位で完結するような暗号（例えば、復号鍵長単位でのブロック暗号）を用いれば、復号

鍵ブロックからの復号鍵を抜き取る時に、復号鍵の復号し、再暗号する必要がない。さらに、復号鍵のサイズを大きくする場合には、光ディスク装置３１０２の構成を変更すること無く、複数の復号鍵を割り当てるなどの復号鍵領域の拡張がパーソナルコンピュータ３１０４上で容易かつ安全に行うことができる。

【０２３９】

＜第１０の実施形態＞

図３７は、本発明に係る第１０の実施形態である光ディスク内のユーザデータ領域の構成と、コンテンツを暗号してユーザデータ領域に記録する光ディスク記録装置の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。この第１０の実施形態は、第６の実施形態において光ディスク記録装置の構成を追加したことを特徴としており、この構成について詳細に説明する。

【０２４０】

光ディスク記録装置においては、暗号の結果が一定とならないように暗号の強度を高めるために、入力される暗号鍵を、コンテンツ中の情報である復号鍵変換データを用いて鍵変換器２１１９により、例えば乗算や除算、所定の重み係数を用いた演算などの所定の鍵変換の演算を行ってコンテンツ復号鍵を得た後、当該コンテンツ復号鍵を用いてコンテンツのデータを暗号化する。

【０２４１】

すなわち、コンテンツの記録時には、コンテンツのデータと、コンテンツのデータを暗号化するための暗号鍵が光ディスク記録装置に入力される。ここで、コンテンツのデータは鍵変換器２１１９と暗号器２１２０に入力され、暗号鍵は鍵暗号器２１１８と鍵変換器２１１９に入力される。鍵変換器２１１９は、上記入力された暗号鍵に対して、コンテンツ中の一部の情報である第１と第２の復号鍵変換データ２１１５，２１１６を用いて所定の鍵変換の演算を行うことにより、コンテンツ復号鍵を生成して暗号器２１２０に出力する。次いで、暗号器２１２０は、上記入力されるコンテンツのデータを、上記コンテンツ復号鍵を用いて暗号化して暗号化コンテンツを光ディスクのユーザデータ領域２１５０内のＡＶデータ記録セクタ２１５２に記録する。

【０２４２】

ここで、光ディスク再生装置において用いる復号鍵変換データとしては、セクタ単位でおおむね異なるようなＡＶデータ中の情報である第２の復号鍵変換データ２１１６や、制御情報が記録されたセクタ中に含まれるコピー世代管理情報やアナログのマクロビジョン制御フラグなどを含むコピー制御情報である第１の復号鍵変換データ２１１５を利用する。前者の第２の復号鍵変換データを利用することにより、コンテンツのデータを暗号化するためのコンテンツ復号鍵をセクタ毎で、第２の復号鍵変換データの内容に応じて鍵変換器２１１３により復元することが可能となる。また、後者の第１の復号鍵変換データは、その改ざん時にデータの不正利用を容易に検出できるデータであるので、当該第１の復号鍵変換データが改ざんされたときに、コンテンツのデータを復号することができなくすることが容易にできるという効果が得られる。具体的には、ＡＶデータの再生制御に用いられる再生制御情報が記録される再生制御記録セクタのデータを第１の復号鍵変換データとして用いて暗号鍵を所定の変換演算により復号鍵に変換し、これを暗号器２１２０においてコンテンツ復号鍵として用いる。さらには、再生制御記録セクタのデータである第１の復号鍵変換データと、暗号化されたコンテンツが記録されるセクタの非暗号化コンテンツの一部である第２の復号鍵変換データとを含む２つの復号鍵変換データを用いて、暗号鍵を所定の変換演算をすることにより、別のコンテンツ復号鍵を演算し、この別のコンテンツ復号鍵を暗号器２１２０においてコンテンツ復号鍵として用いてもよい。

【０２４３】

一方、鍵暗号器２１１８は、上記入力される暗号鍵を、光ディスク再生装置と同様に入力されるディスク鍵を用いて暗号化することにより、暗号化復号鍵を生成する。この暗号化復号鍵のサイズに比較して、セクタヘッダ領域中の復号鍵領域２１０６，２１０９が小さいため、データ分割器２１２１は暗号化復号鍵を複数の分割復号鍵に分割した後、各分割

復号鍵を異なる復号鍵領域２１０６，２１０９に記録する。図３７の例では、暗号化復号鍵は２つの暗号化分割復号鍵に分割され、それぞれ連続する２つのセクタの復号鍵領域２１０６，２１０９に記録される。ここでは、鍵暗号器２１１８により暗号鍵である復号鍵に対して暗号化を施しているので、暗号鍵に対する暗号の強度を高めることができる。

【０２４４】

コンテンツの再生時には、鍵変換器２１１３は、上述の第１の復号鍵変換データ２１１５と第２の復号鍵変換データ２１１６の情報を用いて、鍵復号器２１１２からの復号鍵を所定の鍵変換の演算を行うことにより、コンテンツ復号鍵を生成して復号器２１１４に出力する。次いで、復号器２１１４は、このコンテンツ復号鍵を用いて、暗号化コンテンツのデータを復号することにより、復号化コンテンツを得る。ここで、鍵変換器２１１３は、第１の復号鍵変換データ２１１５のみの情報を用いて、鍵復号器２１１２からの復号鍵を所定の鍵変換の演算を行ってもよい。

【０２４５】

＜第１１の実施形態＞

図３８は、本発明に係る第１１の実施形態である光ディスク内のユーザデータ領域の構成と、コンテンツを暗号してユーザデータ領域に記録する光ディスク記録装置の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。この第１１の実施形態は、第７の実施形態において光ディスク記録装置の構成を追加したことを特徴としており、この構成について詳細に説明する。

【０２４６】

図３８において、光ディスク記録装置は、図３７の第１０の実施形態と同様に、所定のディスク鍵を用いて暗号鍵の暗号化を行う鍵暗号器２１１８と、コンテンツ中の第１と第２の復号鍵変換データ２１１５，２１１６を用いて暗号鍵に対して所定の鍵変換の演算を行ってコンテンツ復号鍵を演算する鍵変換器２１１９と、上記コンテンツ復号鍵を用いてコンテンツを暗号化する暗号器２１２０を備えて構成される。ここで、鍵暗号器２１１８から出力される復号鍵はリードイン領域２４０１内のメインデータ領域２１０２に記録される。一方、光ディスク再生装置は、図２９の第７の実施形態と同様に、鍵復号器２１１２と、鍵変換器２１１３と、復号器２１１４とを備えて構成される。ここで、リードイン領域２４０１内のメインデータ領域２１０２に記録された復号鍵が読み出されて鍵復号器２１１２に入力され、鍵復号器２１１２は、所定のディスク鍵を用いて復号鍵を復号して鍵変換器２１１３に出力する。また、鍵変換器２１１３は、第１と第２の復号鍵変換データ２１１５，２１１６を用いて、鍵復号器２１１２からの復号鍵に対して所定の鍵変換の演算を行ってコンテンツ復号鍵を演算して復号器２１１４に出力する。

【０２４７】

＜第６乃至第９の実施形態の効果＞

以上詳述したように、本実施形態に係る記録型光ディスクは、復号鍵をセクタヘッダ領域に配置された所定サイズの復号鍵領域に分割して記録し、あるいは可変長の復号鍵をセクタヘッダ領域に配置された鍵インデックス領域で示された復号鍵領域に記録することによって、セクタヘッダ領域に予め規定されたサイズの復号鍵領域にとらわれることなく、自由な長さの復号鍵を利用できる記録型光ディスクを提供できる。これにより、記録するコンテンツに対する著作権保護レベルに応じて、任意の鍵長を用いた暗号を利用可能とすることができる。

【０２４８】

＜好ましい変形例＞

以上の実施形態において、上記ディスク識別情報は、好ましくは、書き換えることができないプリピットにより構成され、上記ディスク識別情報には、好ましくは、ディスクが使用される地域を表す地域識別子を有する。また、上記ディスク識別情報には、好ましくは、光ディスク上で記録及び再生可能なコンテンツの種類を示すデータカテゴリ識別子を有する。さらに、上記ディスク識別情報は、好ましくは、秘密鍵を用いて暗号化されてディスク識別情報領域に製造時に記録される。またさらに、上記ディスク識別情報は、好まし

くは、データ記録再生領域に記録可能なデータの種別、又はデータ記録再生領域から再生可能なデータの種別を表すデータを含む。

【０２４９】

以上の実施形態において、好ましくは、コンテンツのデータが記録されるセクタ領域と、デスクランブルキーとの対応関係を管理するデスクランブル領域管理テーブルを有する。また、キー管理情報領域は、好ましくは、ディスク識別情報を鍵として暗号化されたデスクランブルキーを記録するデスクランブルキー領域と、デスクランブルキーの記録状態を表すデスクランブルキーステータス領域を有するキー情報領域と、ディスク上に記録されたコンテンツ再生時に使用するキー情報を記録するコンテンツ情報領域と、コンテンツを再生するために必要なデスクランブルキーを参照するためのポインタを記録したキーインデックス領域とを含む。さらに、コンテンツのデータが記録されるセクタには、好ましくは、上記コンテンツのデータとともに、デスクランブルキーが記録される領域を示すポインタを記録する。

【０２５０】

以上の実施形態において、光ディスク記録再生装置のディスク識別情報の再生回路は、好ましくは、秘密鍵を用いて暗号化されたディスク識別情報を解読する回路を備える。また、光ディスク記録再生装置において、ディスク識別情報を鍵として暗号化されるデータは、好ましくは、画像データや音楽データなどのコンテンツのデータである。さらに、ディスク識別情報は、好ましくは、データ記録再生領域に記録可能なデータの種別を表し、ディスク識別情報の再生回路は、上記データの種別により記録可能なコンテンツのデータであるか否かを判断する。またさらに、ディスク識別情報を鍵として用いて復号されるデータは、好ましくは、画像データや音楽データなどのコンテンツのデータである。また、ディスク識別情報は、好ましくは、データ記録再生領域から再生可能なデータの種別を表し、ディスク識別情報の再生回路は、上記データの種別により再生可能なコンテンツのデータであるか否かを判断する。

【０２５１】

以上の実施形態において、コンテンツの記録回路は、好ましくは、暗号化された画像データや音楽データなどのコンテンツのデータと、上記コンテンツのデータに施された暗号を解くデスクランブルキーを同一のセクタに記録する。また、コンテンツの再生回路は、好ましくは、暗号化された画像データや音楽データなどのコンテンツのデータと、上記コンテンツのデータに施された暗号を解くデスクランブルキーを同一のセクタから再生する。

【０２５２】

以上の実施形態において、キー領域の割当回路又は方法は、好ましくは、デスクランブルキーの記録状態を表すデスクランブルキーステータス領域に領域予約済みフラグを配置し、コンテンツのデータの再生時に使用するキーに関する情報を記録し、コンテンツのデータに対して割り当てたデスクランブルキーの記録領域を表すキーインデックスを記録する。また、デスクランブルキーの配置回路又は方法は、好ましくは、コンテンツ情報領域からコンテンツで使用されるデスクランブルキー領域のインデックスを再生し、記録するデスクランブルキーに対応するキーインデックスに示されるデスクランブルキー領域にデスクランブルキーを配置し、記録するデスクランブルキーに対応するキーインデックスに示されるデスクランブルキーステータス領域に記録済みフラグを配置する。

【０２５３】

以上の実施形態において、光ディスク再生装置は、好ましくは、ディスク識別情報を再生し、コンテンツが再生可能であるか否かを調べ、キー管理情報を再生し、画像データや音楽データなどのコンテンツのデータが記録されたセクタを再生し、再生されたセクタからデスクランブルキーを取得する。さらに、好ましくは、再生したコンテンツのデータをデスクランブルキーによりデスクランブルし出力する。

【０２５４】

以上の実施形態において、コンテンツのデータを記録する方法は、好ましくは、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２の

ディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域とを有する光ディスクの上記ユーザデータ領域にコンテンツを記録する際に、少なくとも上記第２のディスク情報を用いた演算により復号して再生することができるように、暗号化して記録する。ここで、好ましくは、ユーザデータ領域内に、暗号化されて記録されたデータを解読するための鍵情報を記録する鍵情報記録領域を有する。

【０２５５】

以上の実施形態において、コンテンツのデータを記録する方法は、好ましくは、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域と、上記ユーザデータ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域とを有する光ディスクの、上記ユーザデータ領域にコンテンツを記録する際に、少なくとも上記第２のディスク情報と、上記鍵情報を用いた演算により復号して再生することができるように、暗号化して記録する。

【０２５６】

以上の実施形態において、連続する複数のセクタに、分割された複数の分割復号鍵を記録する復号鍵領域を有する光ディスクのセクタにおいて、好ましくは、ＡＶデータを含むデータのサイズが（メインデータサイズ）×（復号鍵の分割数）に満たないメインデータ領域に、ダミーデータを記録する。また、ＥＣＣブロックにおいて、好ましくは、連続する複数のセクタに分割された分割復号鍵を記録した復号鍵領域を有するセクタが、（ＥＣＣブロック単位）／（復号鍵の分割数）回だけ記録され、ＡＶデータを含むデータのサイズが（メインデータサイズ）×（ＥＣＣブロック単位）に満たないメインデータ領域に、ダミーデータを記録する。

【０２５７】

以上の実施形態において、ＡＶデータを含むデータに施された暗号を復号するための復号鍵は、好ましくは、所定のサイズを有する複数の分割復号鍵に分割され、分割された複数の分割復号鍵は、復号鍵テーブルの連続する複数の復号鍵領域に記録される。また、上記復号鍵テーブルは、好ましくは、書き換え可能なリードイン領域内のメインデータ領域に記録される。さらに、復号鍵テーブルの記録状態を表す情報は、好ましくは、復号鍵テーブルの各復号鍵領域に固定値として記録される。またさらに、復号鍵テーブルは、光ディスクの内周と外周に配置された異なる上記ＥＣＣブロックに複数回だけ記録される。

【０２５８】

以上の実施形態において、データ暗号化装置であるエンコード装置３１０１と、光ディスク記録再生装置である光ディスク装置３１０２は、好ましくは、相互認証方式によりバス鍵の共有を行う。また、データ復号化装置であるデコード装置３１０３と光ディスク記録再生装置である光ディスク装置３１０２は、好ましくは、相互認証方式によりバス鍵の共有を行う。

【０２５９】

以上の実施形態においては、ＲＡＭ型を含む書き換え型又は追記型の光ディスクであるデータを記録することができる記録型光ディスクについて説明しているが、本発明はこれに限らず、予め記録されたデータを読み出して再生することができるが新たに記録することができない再生専用型光ディスクに適用できる。再生専用型光ディスクの場合においては、データ記録再生領域をデータを読み出して再生するデータ再生領域と置き換え、コンテンツのデータやその他の種々の制御情報のデータは製造時に予め記録される。ここで、記録型光ディスクは、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＭＯ、ＭＤ、ＤＶＤ－ＲＡＭなどを含む。再生専用型光ディスクは、音楽ＣＤ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどを含む。

【０２６０】

【発明の効果】

以上詳述したように、本発明に係る光ディスクによれば、ユーザデータ領域への記録動作

や再生動作を光ディスク毎に行うディスク識別情報が書き換え不可能な再生専用領域に記録されることにより、利用者による光ディスク上へのコンテンツの記録動作や再生動作を光ディスクの製造時に記録する情報を用いて制御することができる。

【０２６１】

また、本発明に係る光ディスクによれば、書き換えが不可能な再生専用のディスク識別情報を鍵として暗号化されたデータが光ディスク上のユーザデータ領域に記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とすることができる。

【０２６２】

さらに、本発明に係る光ディスクによれば、暗号化されたデータと暗号を解くデスクランブルキーとが異なるセクタ領域に記録されることにより、映画や音楽などの著作権保護が必要なデータの取得と暗号を解くためのデスクランブルキーの取得を独立に行うことが可能となる。さらに、ディスク識別情報を鍵としてデスクランブルキーを暗号化して記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とし、コピー先の光ディスクのディスク識別情報を鍵として暗号化したデスクランブルキーを取得し記録することで、データの正しい復号並びに再生を可能とすることができる。

【０２６３】

また、本発明に係る光ディスクによれば、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域を有する。従って、従来技術の光ディスクに、上記光ディスクを識別する情報を付加することにより、光ディスクの管理を容易に実現することができる。ここで、上記第２の情報領域は、好ましくは、上記第１の情報領域内に記録されているものであり、上記第１の情報領域を再生する光ピックアップによって再生することができる。また、上記第２の情報領域は、上記第１の情報領域内の記録膜を、半径方向に長い形状でかつ複数個のトリミング領域が形成されるように、部分的に除去することにより記録されているものであり、容易に上記第２のディスク情報が改ざんされることを防止することができる。

【０２６４】

さらに、本発明に係る光ディスクによれば、復号鍵をセクタヘッダ領域に配置された所定サイズの復号鍵領域に分割して記録し、あるいは可変長の復号鍵をセクタヘッダ領域に配置された鍵インデックス領域で示された復号鍵領域に記録することによって、セクタヘッダ領域に予め規定されたサイズの復号鍵領域にとらわれることなく、自由な長さの復号鍵を利用できる記録型光ディスクを提供できる。これにより、記録するコンテンツに対する著作権保護レベルに応じて、任意の鍵長を用いた暗号を利用可能とすることができる。

【図面の簡単な説明】

【図１】　本発明に係る第１の実施形態である記録型光ディスク１００のデータ記録領域を示す平面図である。

【図２】　（ａ）は図１の光ディスク１００のＢＣＡ１０６を形成するときの装置構成を示すブロック図及び縦断面図であり、（ｂ）は図１の光ディスク１００のＢＣＡ１０６を形成した後の光ディスク１００の縦断面図及びその水平方向に対する反射光の強度を示すグラフである。

【図３】　図１のＢＣＡ１０６の記録フォーマットを示す図である。

【図４】　図１のユーザデータ領域１０２内のセクタデータ４０１のセクタ構造を示す図である。

【図５】　図１のキー管理情報領域１０７の構成を示す図である。

【図６】　（ａ）は第１の実施形態の変形例に係る、図１のセクタデータ４０１にデスクランブルキー及びＡＶデータを記録する記録方法を示すブロック図であり、（ｂ）は第１

の実施形態に係る、図１のセクタデータ４０１にデスクランブルキーへのキーインデックス及びＡＶデータを記録する記録方法を示すブロック図である。
【図７】　本発明に係る第２の実施形態である光ディスク記録再生装置の構成を示すブロック図である。
【図８】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるＡＶデータの記録処理を示すフローチャートである。
【図９】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるキー管理情報領域の割り当て処理を示すフローチャートである。
【図１０】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるデスクランブルキーの記録処理を示すフローチャートである。
【図１１】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるＡＶデータの再生処理を示すフローチャートである。
【図１２】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるデスクランブルキーの取得処理を示すフローチャートである。
【図１３】　第１の実施形態の変形例に係る、暗号化デスクランブルキーから正規のデスクランブルキーであるか否かを判定するための方法を示すブロック図である。
【図１４】　第１の実施形態の変形例に係る、デスクランブル領域管理テーブルの構成を示す図である。
【図１５】　（ａ）は第１の実施形態においてコンテンツの記録時に地域識別子を記録する場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図であり、（ｂ）は第１の実施形態において地域識別子が光ディスクの出荷時に予め記録されている場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図である。
【図１６】　本発明に係る第３の実施形態である光ディスク１１０１のデータ記録領域を示す平面図である。
【図１７】　第３の実施形態に係るＢＣＡ再生回路１４０１における再生信号１２０１及び再生２値化信号１２０７の信号波形を示す波形図である。
【図１８】　第３の実施形態に係るＢＣＡ再生回路１４０１の構成を示すブロック図である。
【図１９】　第３の実施形態に係る光ディスク記録再生システムの構成を示すブロック図である。
【図２０】　本発明に係る第４の実施形態である光ディスク記録再生システムの構成を示すブロック図である。
【図２１】　本発明に係る第５の実施形態である光ディスク１６０１のデータ記録領域を示す平面図である。
【図２２】　第５の実施形態に係る光ディスク記録再生システムの構成を示すブロック図である。
【図２３】　第５の実施形態に係るＩＤ付与テーブルの構成を示す表である。
【図２４】　第３の実施形態の変形例に係る光ディスク１１０１ａのデータ記録領域を示す平面図である。
【図２５】　第５の実施形態の変形例に係る光ディスク１６０１ａのデータ記録領域を示す平面図である。
【図２６】　本発明に係る第６の実施形態である光ディスク内のユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。
【図２７】　第６の実施形態に係る光ディスクにおいて、ユーザデータ領域への著作権制御情報と復号鍵の配置と、メインデータ領域への暗号化コンテンツの配置を示すブロック図である。
【図２８】　第６の実施形態に係る光ディスクにおいて、エラー訂正の単位が複数のセクタにまたがる場合の配置を示すブロック図である。

【図２９】　本発明に係る第７の実施形態である光ディスク内のリードイン領域２４０１とユーザデータ領域２４０２の構成と、リードイン領域２４０１とユーザデータ領域２４０２のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。
【図３０】　（ａ）は第７の実施形態に係る光ディスク内のリードイン領域のメインデータ領域において、復号鍵の初期値で未記録状態を表示する場合のデータ構成を示すブロック図であり、（ｂ）は第７の実施形態に係る光ディスク内のリードイン領域のメインデータ領域において、復号鍵状態テーブルで記録状態を表示する場合のデータ構成を示すブロック図である。
【図３１】　第７の実施形態に係る光ディスクにおいて復号鍵の配置を示すブロック図である。
【図３２】　本発明に係る第８の実施形態である光ディスクのデータをファイル管理システムにより管理するときのデータ構成を示すブロック図である。
【図３３】　第８の実施形態に係るファイル管理システムによって実行される、著作権保護を必要とするコンテンツの記録処理を示すフローチャートである。
【図３４】　第８の実施形態に係るファイル管理システムによって実行される、コンテンツの再生処理を示すフローチャートである。
【図３５】　第８の実施形態に係るファイル管理システムによって実行される、コンテンツの削除処理を示すフローチャートである。
【図３６】　本発明に係る第９の実施形態である光ディスクシステムの構成を示すブロック図である。
【図３７】　本発明に係る第１０の実施形態である光ディスク内のユーザデータ領域の構成と、コンテンツを暗号してユーザデータ領域に記録する光ディスク記録装置の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。
【図３８】　本発明に係る第１１の実施形態である光ディスク内のユーザデータ領域の構成と、コンテンツを暗号してユーザデータ領域に記録する光ディスク記録装置の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。
【図３９】　従来技術のＤＶＤ－ＲＯＭのユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。
【符号の説明】
１００…光ディスク、
１０１…リードイン領域、
１０２…ユーザデータ領域、
１０３…リードアウト領域、
１０４…再生専用領域、
１０５…記録再生領域、
１０６…バーストカッティング領域（ＢＣＡ）、
１０７…キー管理情報領域、
２０１…基板、
２０２…記録層、
２０３…反射層、
２０４…接着層、
２０５…反射層、
２０６…記録層、
２０７…基板、
２１１…高パワーレーザ光源、
２１２…フォーカスレンズ、

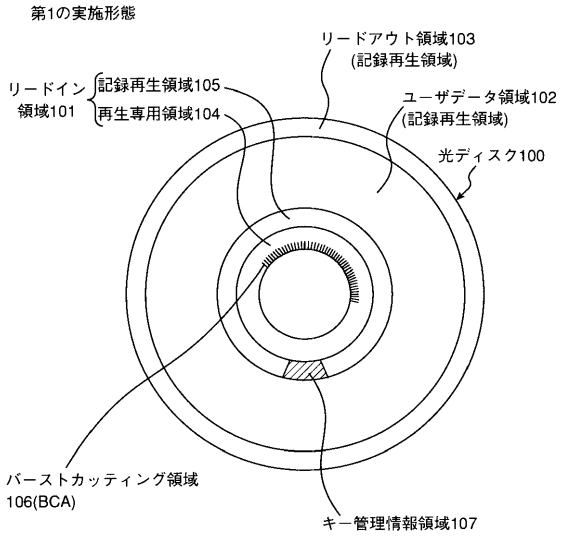
３０１…同期コード、
３０２…誤り検出コード、
３０３…誤り訂正コード、
３０４…ＢＣＡデータ、
３０５…ディスク識別情報、
４０１…セクタデータ、
４０２…ヘッダ、
４０３…メインデータ、
４０４…エラー検出コード、
４０５…データＩＤ、
４０６…ＩＤエラー検出コード、
４０７…スクランブル制御情報、
４０８，４０８ａ…キー情報、
５０１…キー情報領域、
５０２…コンテンツ情報領域、
５０３…キーインデックスリスト領域、
５０４…記録済みキー数、
５０５…デスクランブルキー領域、
５０６…キーステータス領域、
５０７…コンテンツ数、
５０８…コンテンツ情報、
５０９…キーインデックス、
７０１…記録型光ディスク、
７０２…光学ヘッド、
７０３…記録再生制御回路、
７０４…変復調回路、
７０５…誤り検出及び訂正回路、
７０６…バッファメモリ、
７０７…デスクランブル回路、
７０８…ＭＰＥＧ復号回路、
７０９…出力回路、
７１０…制御ＣＰＵ、
７１１…通信回路、
７１２…データ受信回路、
８０１…暗号化デスクランブルキー、
８０２…デスクランブルキー、
８０３…誤り検出コード、
１１０１，１１０１ａ…光ディスク、
１１０２…コントロールユーザデータ領域、
１１０３…ユーザデータ領域、
１１０４，１１０４ａ…ＢＣＡ、
１１０５，１１０５ａ…トリミング領域、
１２０１…再生信号、
１２０２乃至１２０４…トリミング部分、
１２０５，１２０６…スライスレベル、
１２０７…再生２値化信号、
１３０１…光ピックアップ、
１３０２…プリアンプ、
１３０３…低域通過フィルタ（ＬＰＦ）、
１３０４…２値化回路、

１３０５…復調回路、
１３０６…ディスクＩＤ信号、
１４０１…ＢＣＡ再生回路
１４０２…ディスクＩＤ信号、
１４０３，１４０４…インターフェース、
１４０５…ネットワーク、
１４０６…暗号化部、
１４０７…コンテンツメモリ、
１４０８…暗号化エンコーダ、
１４０９…暗号化コンテンツ、
１４１０…光ディスク記録再生装置、
１４１１…記録回路、
１４１２…データ再生部、
１４１３…暗号デコーダ、
１４１４…出力信号、
１５０１…ＣＡＴＶ会社装置、
１５０２…コンテンツメモリ、
１５０３…第１暗号鍵メモリ、
１５０４…第１暗号化エンコーダ、
１５０５…第１暗号化コンテンツ、
１５０６…ＣＡＴＶデコーダ、
１５０７…鍵発行センター装置、
１５０７ａ…制御部、
１５０８…システムＩＤメモリ、
１５０９…入力されたタイトルコード、
１５１０…時間制限情報メモリ、
１５１１…記録許可コードメモリ、
１５１２…鍵（Ｋ）、
１５１３…第１暗号デコーダ、
１５１４…光ディスク記録再生装置、
１５１５…ディスクＩＤ信号、
１５１６…第２暗号化エンコーダ、
１５１７…第２暗号化コンテンツ、
１５１８…記録回路、
１５１９…データ再生部、
１５２０…第２暗号デコーダ、
１５２１…ＢＣＡ再生回路、
１５２２…ＩＣカード、
１５２３…会社識別信号メモリ、
１５２４…ＩＣカード、
１５２５…出力信号、
１５２６…会社識別信号メモリ、
１５２７…クロック回路、
１５３０…テレビジョン装置、
１６０１，１６０１ａ…光ディスク、
１６０２…コントロールユーザデータ領域、
１６０３…ユーザデータ領域、
１６０４，１６０４ａ…ＢＣＡ、
１６０５…鍵情報記録領域、
１６０６，１６０６ａ…トリミング領域、

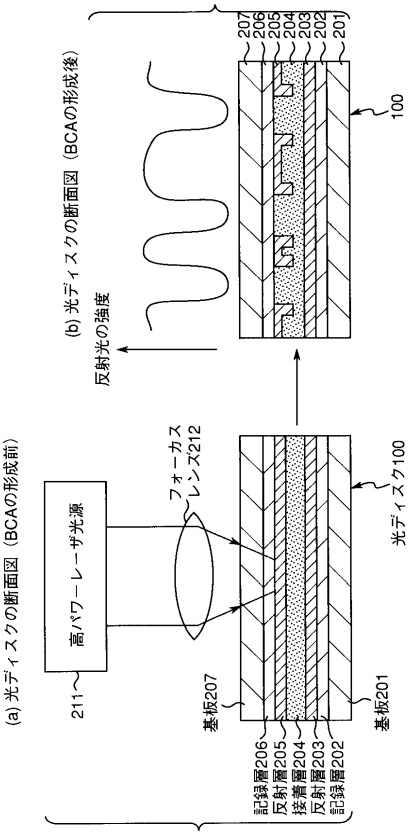
１７０１…ＣＡＴＶ会社装置、
１７０２…コンテンツメモリ、
１７０３…第１暗号鍵、
１７０４…第１暗号化エンコーダ、
１７０５…鍵（Ｋ）、
１７０６…ＣＡＴＶデコーダ、
１７０７…鍵発行センター装置、
１７０７ａ…制御部、
１７０８…システムＩＤメモリ、
１７０９…入力されたタイトルコード、
１７１０…時間制限情報メモリ、
１７１２…鍵（Ｋ）、
１７１３…第１暗号化デコーダ、
１７１４…光ディスク記録再生装置、
１７１５…ディスクＩＤ、
１７１６…入力されたタイトルコード、
１７１７…記録回路、
１７１８…鍵（ＤＫ）、
１７１９…鍵情報記録回路、
１７２０…ＢＣＡ再生回路、
１７２１…データ再生部、
１７２２…第２暗号デコーダ、
１７２３…鍵情報再生部、
１７２４…出力信号、
１７２５…クロック回路、
１７３０…テレビジョン装置、
２１０１…セクタヘッダ領域、
２１０２…メインデータ領域、
２１０３…誤り検出コード、
２１０４…セクタアドレス、
２１０５…著作権制御情報、
２１０６…復号鍵領域、
２１０７…非暗号化コンテンツ、
２１０８…暗号化コンテンツ、
２１０９…復号鍵領域、
２１１０…復号鍵変換データ、
２１１１…データ連結器、
２１１２…鍵復号器、
２１１３…鍵変換器、
２１１４…復号器、
２１１５…第１の復号鍵変換データ、
２１１６…第２の復号鍵変換データ、
２１１７…非暗号化制御情報、
２１１８…鍵暗号器、
２１１９…鍵変換器、
２１２０…暗号器、
２１２１…データ分割器、
２１５０…ユーザデータ領域、
２１５１…制御情報記録セクタ、
２１５２…ＡＶデータ記録セクタ、

２２０１…第１の復号鍵領域、
２２０２…第２の復号鍵領域、
２２０３…補完データ、
２２０４…暗号化コンテンツ、
２４０１…リードイン領域、
２４０２…ユーザデータ領域、
２４０３…鍵インデックス領域、
２４０４…復号鍵テーブル、
２４５１…制御情報記録セクタ、
２４５２…ＡＶデータ記録セクタ、
２５０１…未記録状態データ、
２５０２…復号鍵状態テーブル、
２５０３…記録状態データ、
２６０１…リードイン領域、
２６０２…ユーザデータ領域、
２６０３…リードアウト領域、
２７０１…ファイルエントリ（１）、
２７０２…ファイルエントリ（２）、
２７０３…ファイル（１）、
２７０４…ファイル（２）、
２７０５…ファイル（１）のエクステント（１）、
２７０６…ファイル（２）のエクステント（１）、
２７０７…復号鍵テーブル、
２７０８…鍵インデックス領域、
２７５１…ファイル管理情報領域、
３１０１…エンコード装置、
３１０２…光ディスク装置、
３１０３…デコード装置、
３１０４…パーソナルコンピュータ、
３１１１…復号鍵メモリ、
３１１２…バス暗号回路、
３１１３…復号鍵テーブルメモリ、
３１１４…バス暗号及び復号回路、
３１１５…バス暗号化復号鍵テーブルメモリ、
３１１６…復号鍵状態テーブルメモリ、
３１１７…バス復号回路、
３１１８…復号鍵メモリ、
３１１９…記録再生回路、
３１２０，３１２１，３１２３，３１２４…インターフェース、
３１３０…制御部、
３１３１…コンテンツメモリ、
３１３２…符号化回路、
３１３３…暗号鍵メモリ、
３１３４…暗号回路、
３１４１…復号化回路、
３１５１…ＰＣＩバス、
３１５２…ＳＣＳＩバス。

【図１】

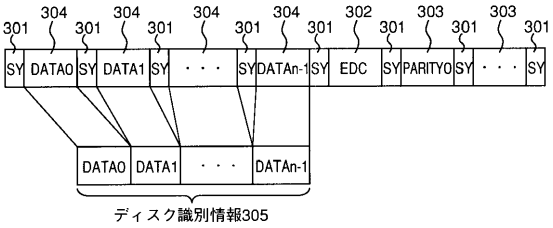


【図２】



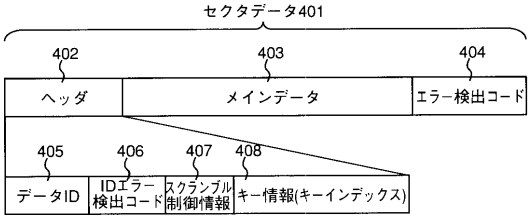
【図３】

BCA106の記録フォーマット

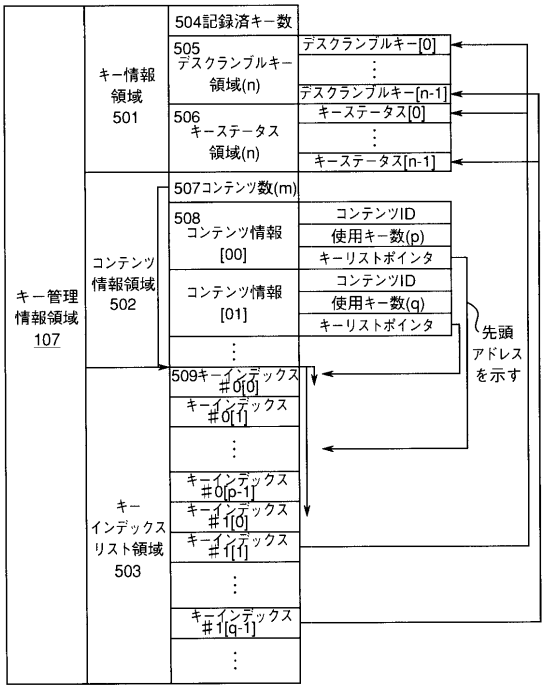


【図４】

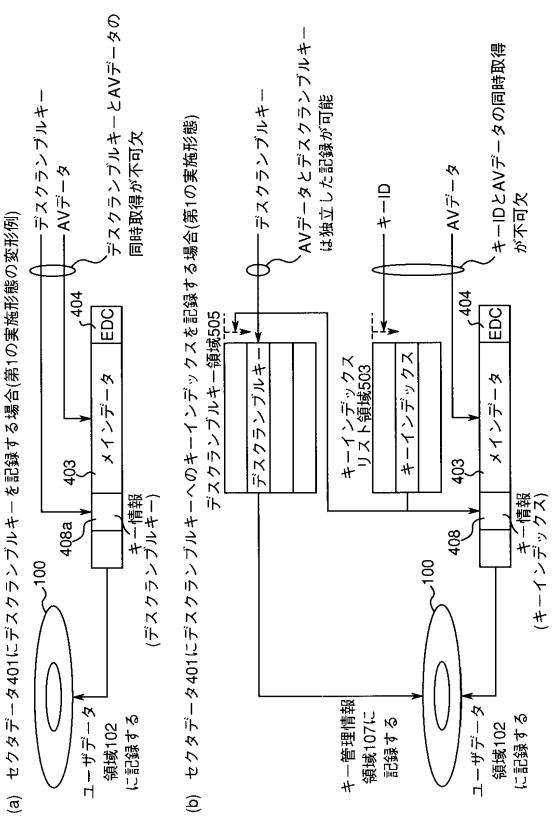
ユーザデータ領域102内のセクタデータ401のセクタ構造



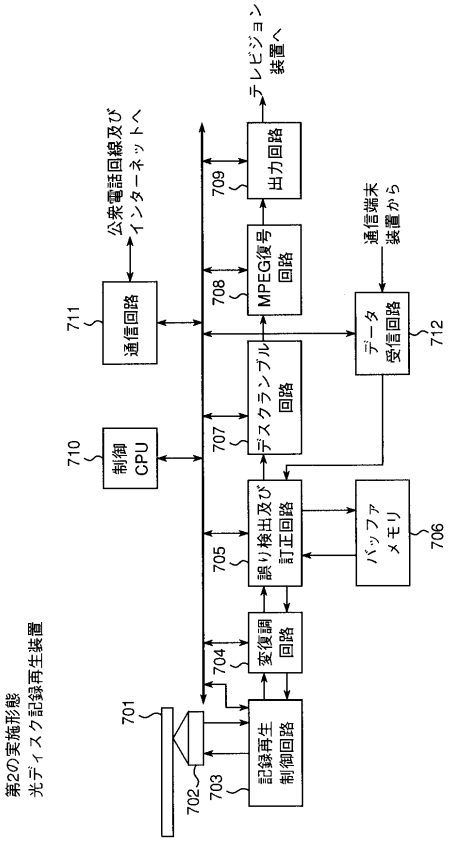
【図５】



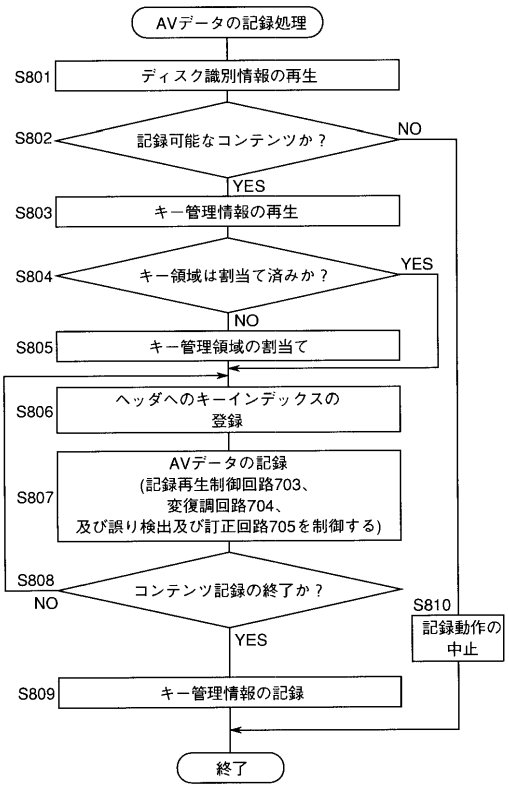
【図６】


(a) セクタデータ401にデスクランブルキーを記録する場合(第1の実施形態の変形例)
デスクランブルキー
AVデータ
デスクランブルキーとAVデータの同時取得が不可欠
EDC
404
メインデータ
403
408a
キー情報
(デスクランブルキー)
100
ユーザデータ領域102に記録する
(b) セクタデータ401にデスクランブルキーへのキーインデックスを記録する場合(第1の実施形態)
デスクランブルキー領域505
デスクランブルキー
AVデータとデスクランブルキーは独立した記録が可能
キーインデックスリスト領域503
キーインデックス
キーID
AVデータ
キーIDとAVデータの同時取得が不可欠
EDC
404
メインデータ
403
408
キー情報
(キーインデックス)
100
キー管理情報領域107に記録する
ユーザデータ領域102に記録する

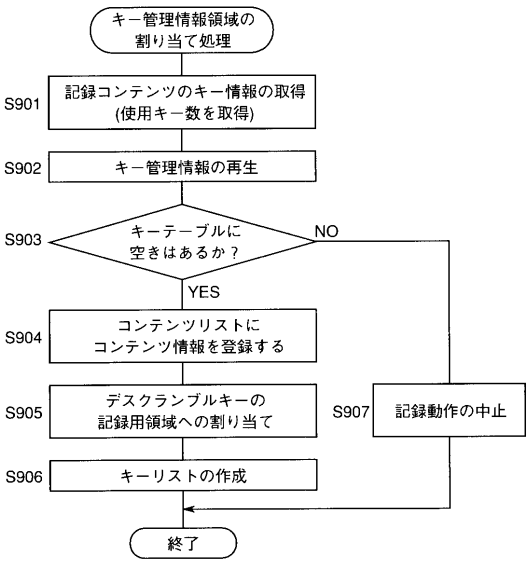
【図７】


第2の実施形態
光ディスク記録再生装置
テレビジョン装置へ
公衆電話回線及びインターネットへ
通信端末装置から
通信回路
711
制御CPU
710
出力回路
709
MPEG復号回路
708
デスクランブル回路
707
データ受信回路
712
誤り検出及び訂正回路
705
バッファメモリ
706
変復調回路
704
記録再生制御回路
703
701
702

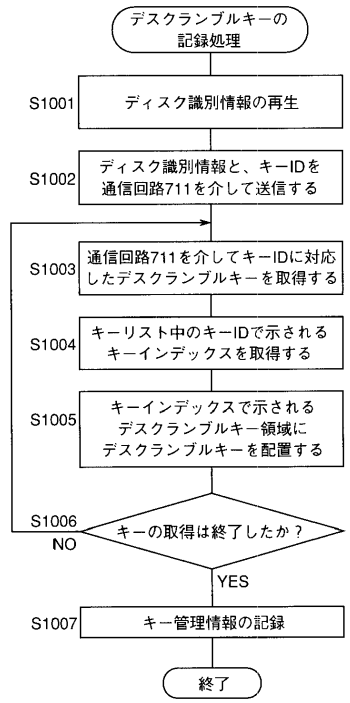
【図８】


AVデータの記録処理
S801
ディスク識別情報の再生
S802
記録可能なコンテンツか？
NO
YES
S803
キー管理情報の再生
S804
キー領域は割当て済みか？
YES
NO
S805
キー管理領域の割当て
S806
ヘッダへのキーインデックスの登録
S807
AVデータの記録
(記録再生制御回路703、
変復調回路704、
及び誤り検出及び訂正回路705を制御する)
S808
コンテンツ記録の終了か？
NO
YES
S810
記録動作の中止
S809
キー管理情報の記録
終了

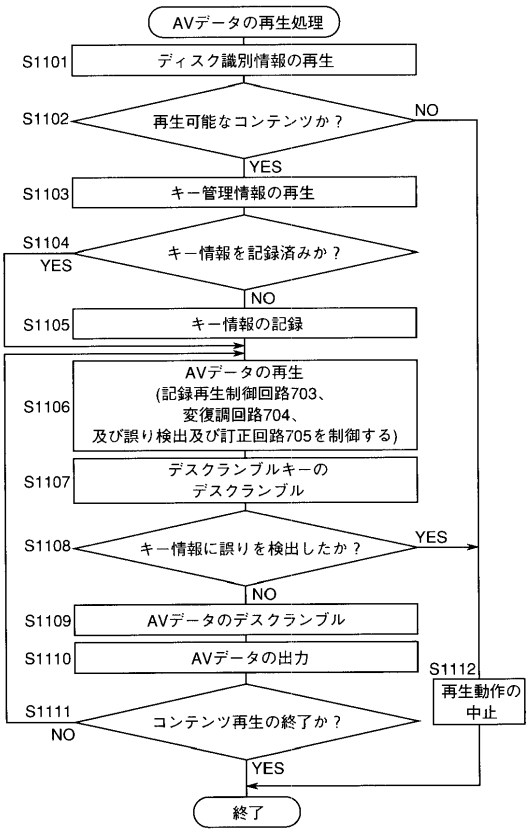
【図９】


キー管理情報領域の割り当て処理
S901
記録コンテンツのキー情報の取得
(使用キー数を取得)
S902
キー管理情報の再生
S903
キーテーブルに空きはあるか？
NO
YES
S904
コンテンツリストにコンテンツ情報を登録する
S905
デスクランブルキーの記録用領域への割り当て
S907
記録動作の中止
S906
キーリストの作成
終了

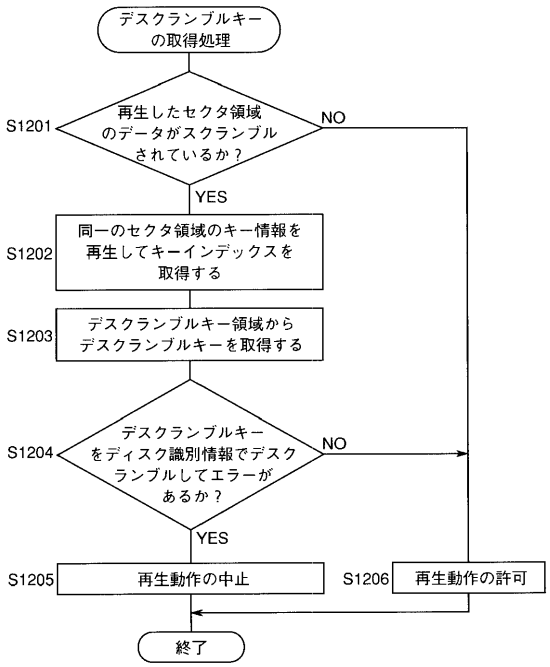
【図１０】



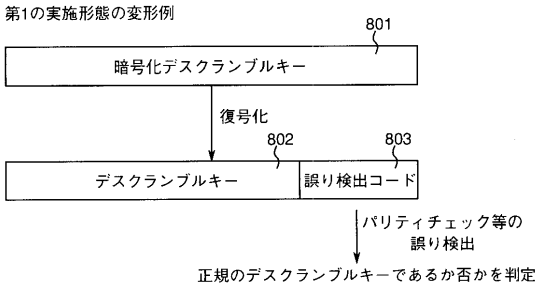
【図１１】



【図１２】



【図１３】



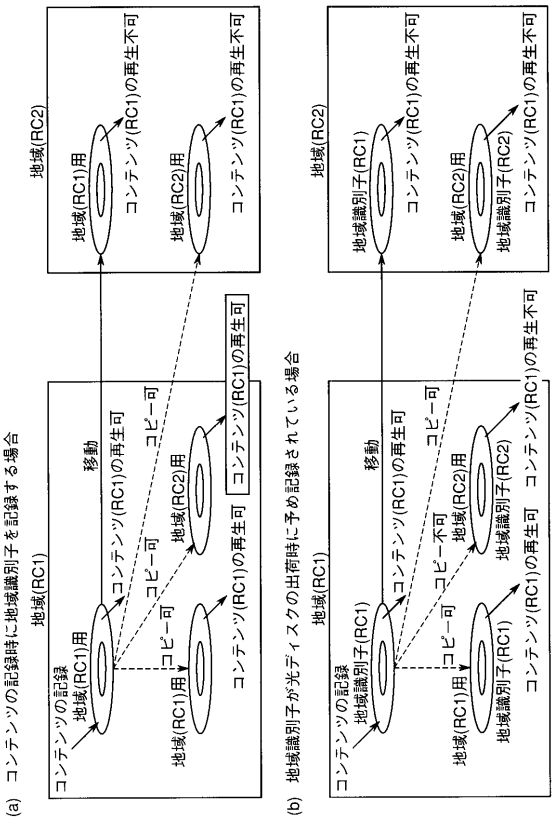
【図１４】

第1の実施形態の変形例

デスクランブル領域管理テーブル

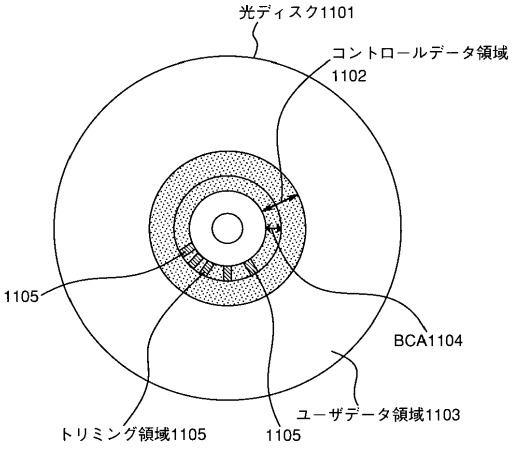
1	開始アドレス1	終了アドレス1	デスクランブルキー1
2	開始アドレス2	終了アドレス2	デスクランブルキー2
⋮	⋮	⋮	⋮
n	開始アドレスn	終了アドレスn	デスクランブルキーn

【図１５】

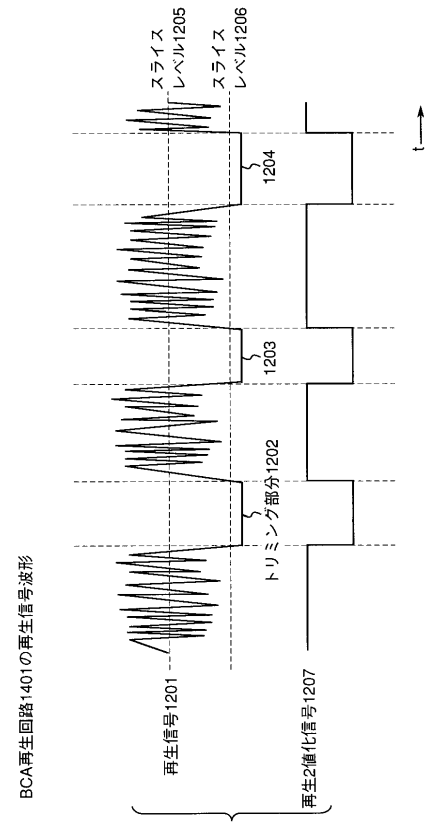


【図１６】

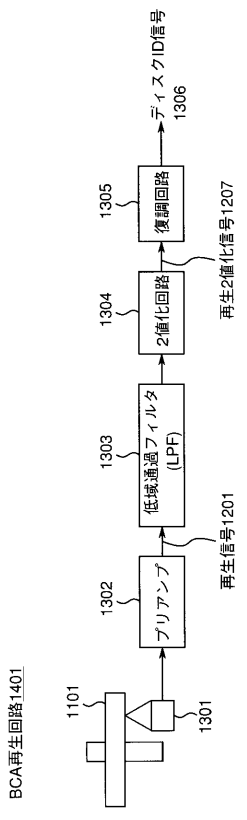
第3の実施形態



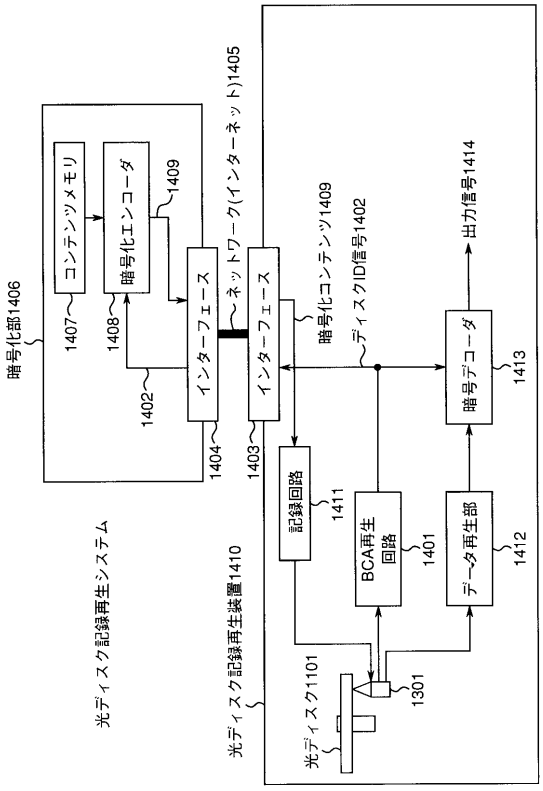
【図１７】



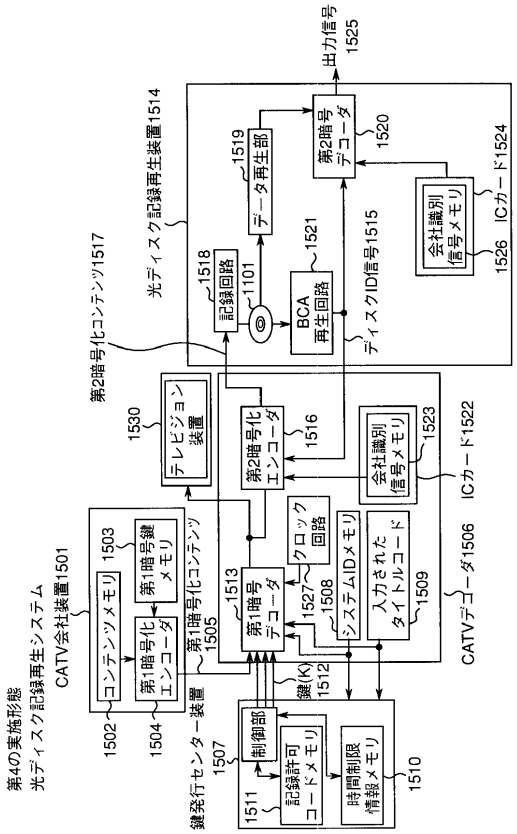
【図１８】



【図１９】

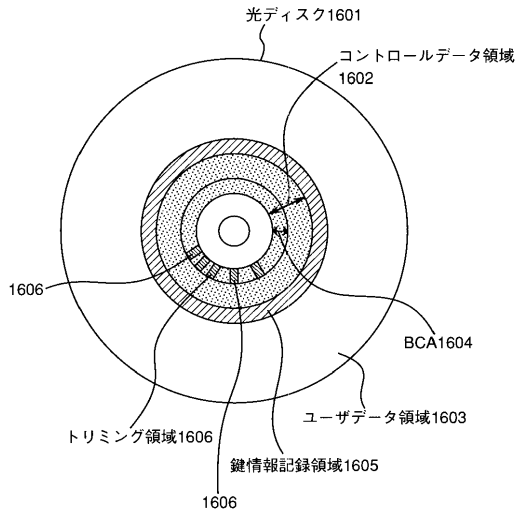


【図２０】

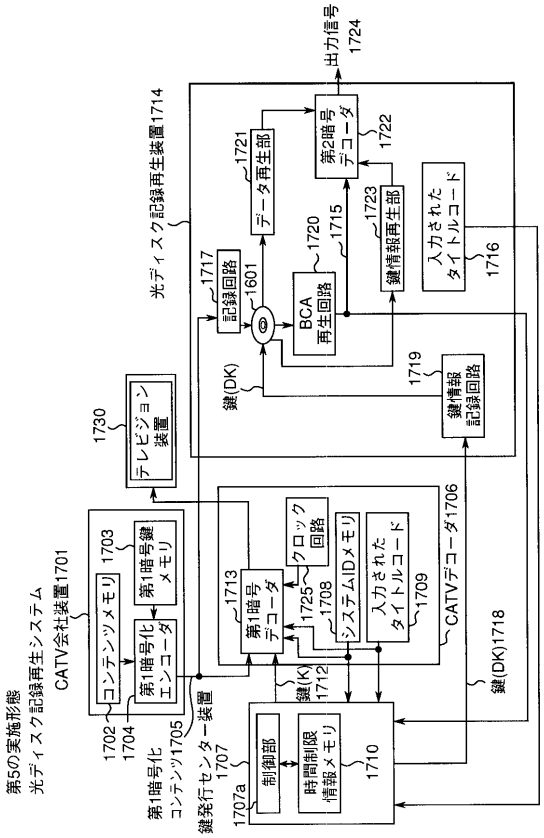


【図２１】

第5の実施形態



【図２２】



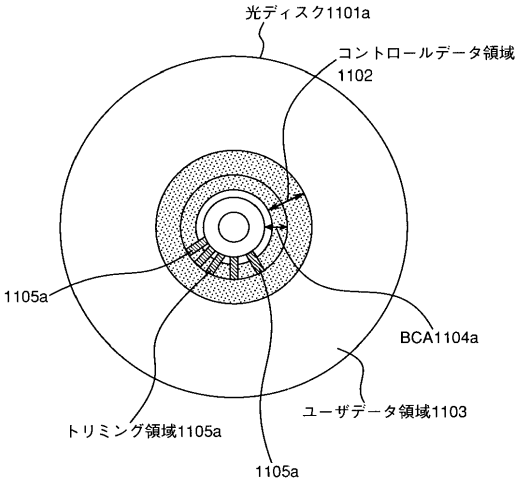
【図２３】

ID付きテーブル

タイトルコードT		T1	T2	T3
第1復号鍵FK		FK1	FK2	FK3
時間制限情報TIME		TIME1	TIME2	TIME3
システムID	DID1	K11	K12	K13
	DID2	K21	K22	K23
	DID3	K23	K32	K33
ディスクID	BCAS1	DK11	DK12	DK13
	BCAS2	DK21	DK22	DK23
	BCAS3	DK31	DK32	DK33

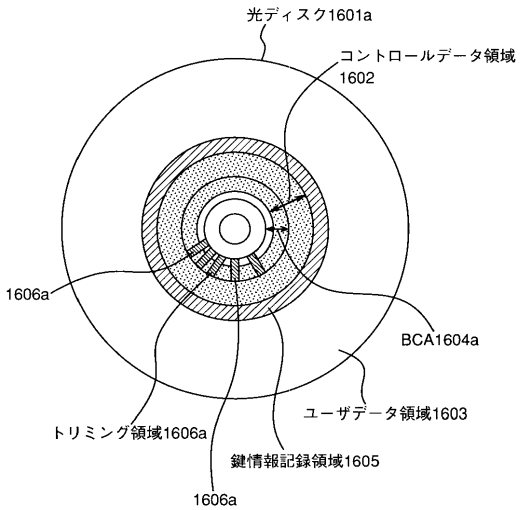
【図２４】

第3の実施形態の変形例

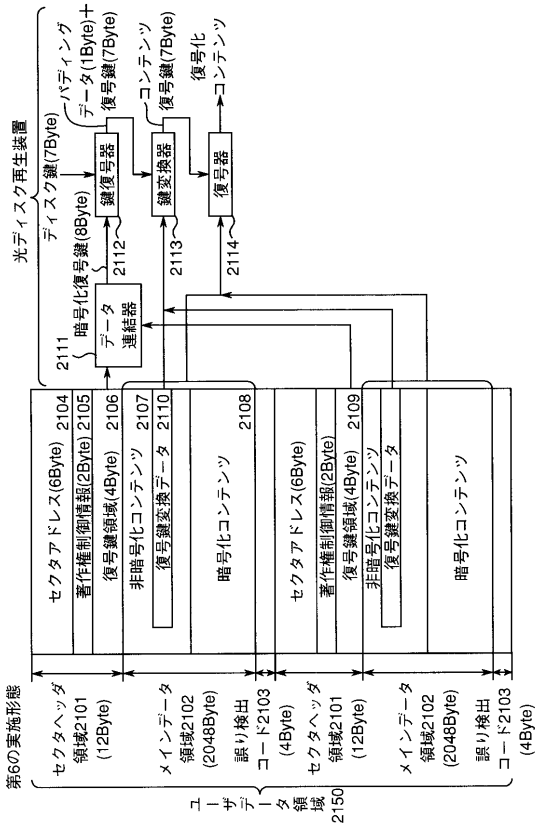


【図２５】

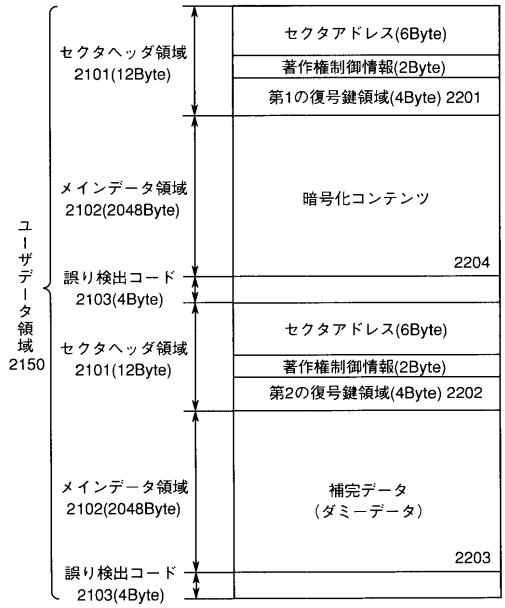
第5の実施形態の変形例



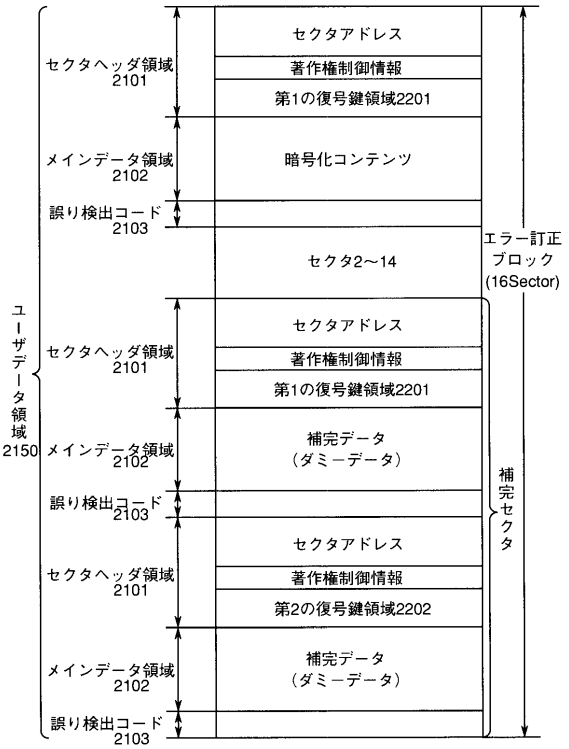
【図２６】



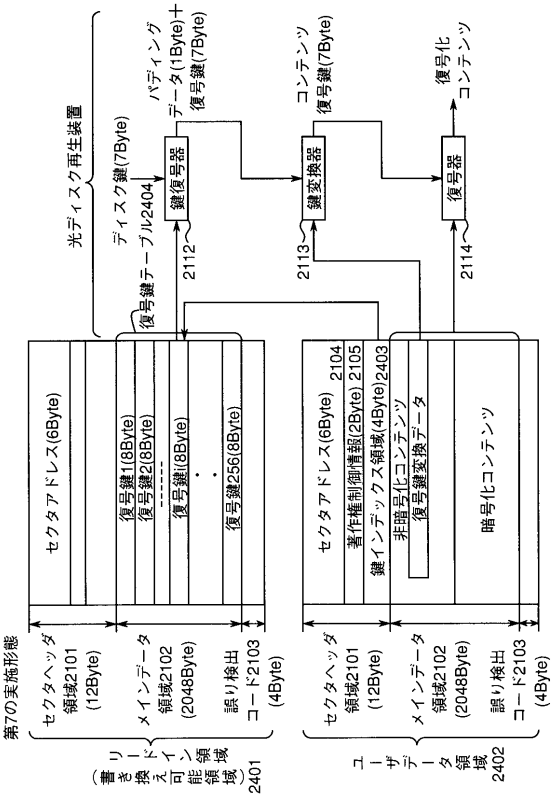
【図２７】



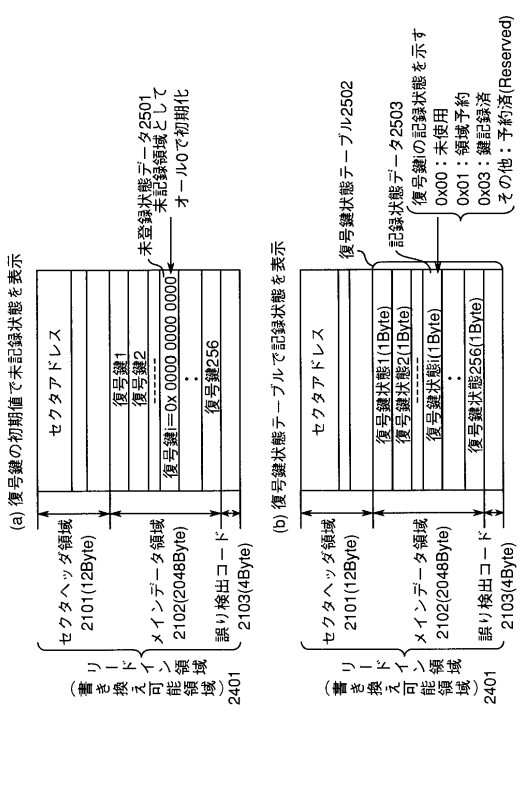
【図２８】



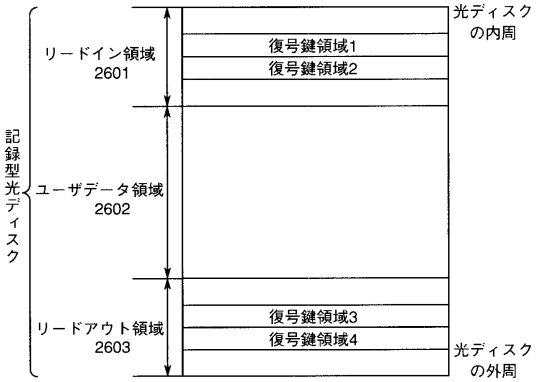
【図２９】



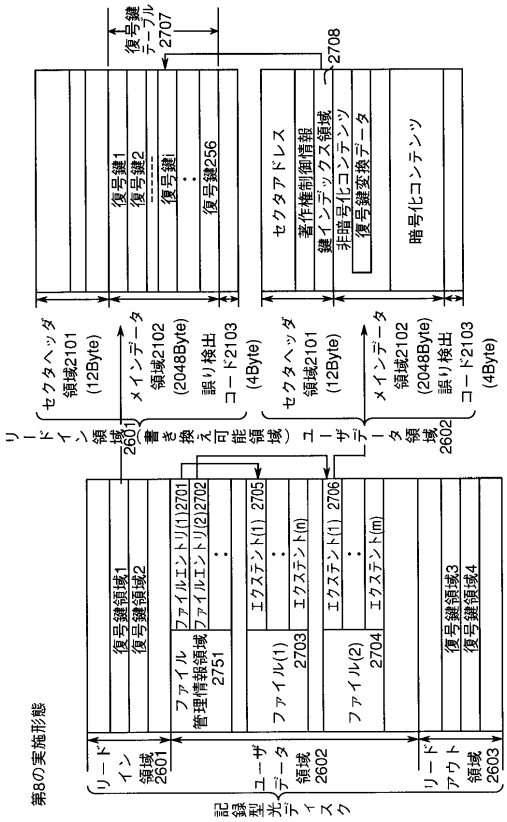
【図３０】



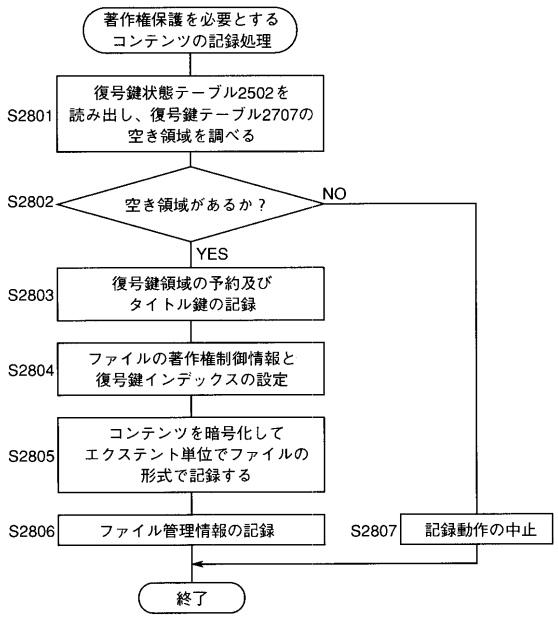
【図３１】



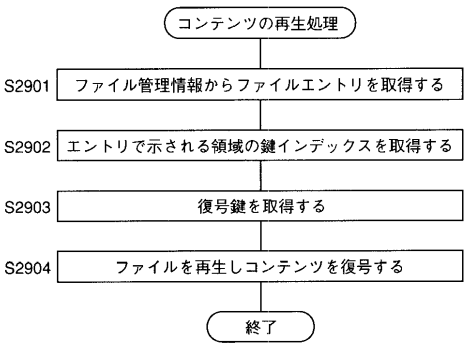
【図３２】



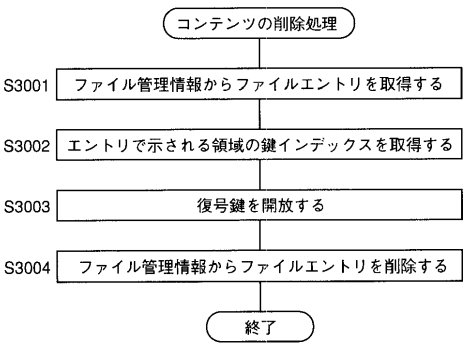
【図３３】



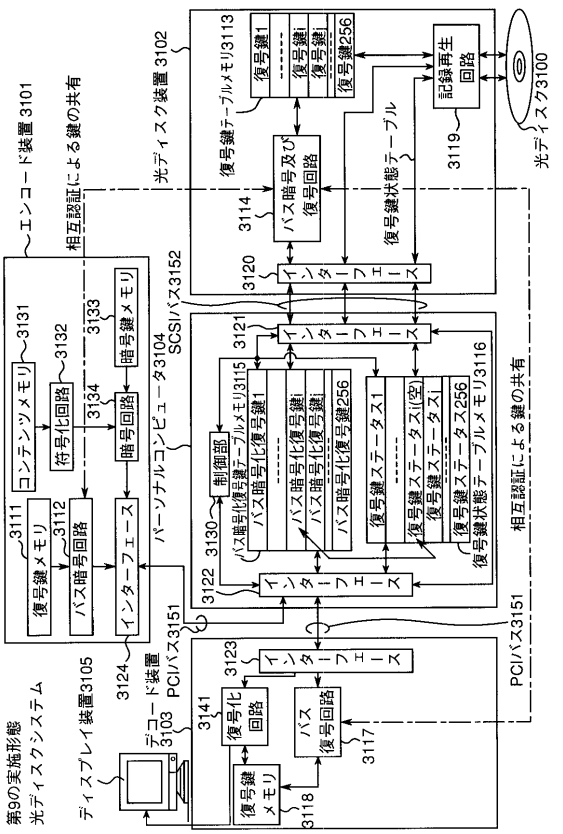
【図３４】



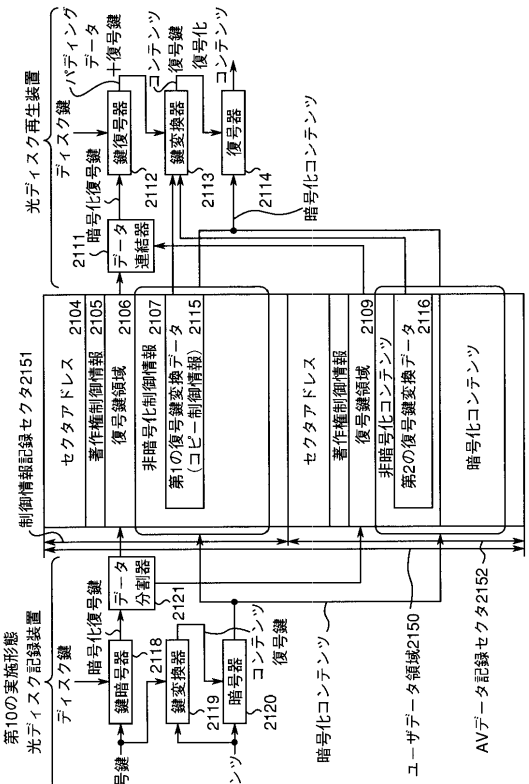
【図３５】



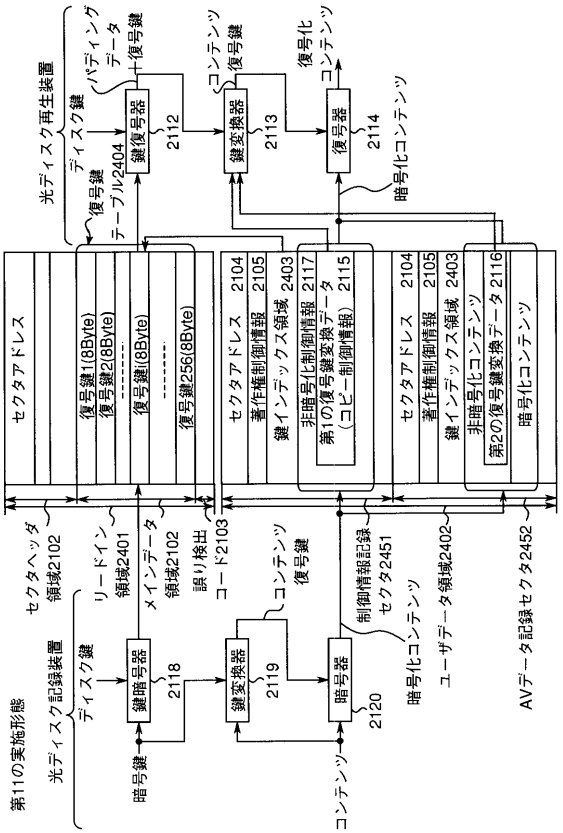
【図３６】



【図３７】



【図３８】



【図３９】

フロントページの続き

(51)Int.Cl.	FI	
	G11B 20/10	H
	G11B 20/12	
	H04L 9/00	601A
	H04L 9/00	601E

(72)発明者 高木 裕司
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 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 東海林 衛
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 大嶋 光昭
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 大原 俊次
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 伊藤 基志
大阪府門真市大字門真1006番地 松下電器産業株式会社内
(72)発明者 石田 隆
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 中村 敦史
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 謝花 正司
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 中田 浩平
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 山澤 宏

(56)参考文献 特開平11－073648（JP，A）
国際公開第97／014146（WO，A1）
特開昭58－083336（JP，A）

(58)調査した分野(Int.Cl.，DB名)
G11B 7/004
G11B 7/24
G11B 20/10
G11B 20/12
H04L 9/08