(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年2 月13 日 (13.02.2003)

PCT

(10) 国際公開番号
WO 03/012786 A1

(51) 国際特許分類[7]: G11B 20/10, H04L 9/14

(21) 国際出願番号: PCT/JP02/07164

(22) 国際出願日: 2002 年7 月15 日 (15.07.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-226242 2001 年7 月26 日 (26.07.2001) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 佐古 曜一郎 (SAKO,Yoichiro) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

猪口 達也 (INOKUCHI,Tatsuya) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 古川 俊介 (FURUKAWA,Shunsuke) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 杉浦 正知, 外(SUGIURA,Masatomo et al.); 〒171-0022 東京都 豊島区 南池袋 2丁目49番 7号 池袋パークビル７階 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

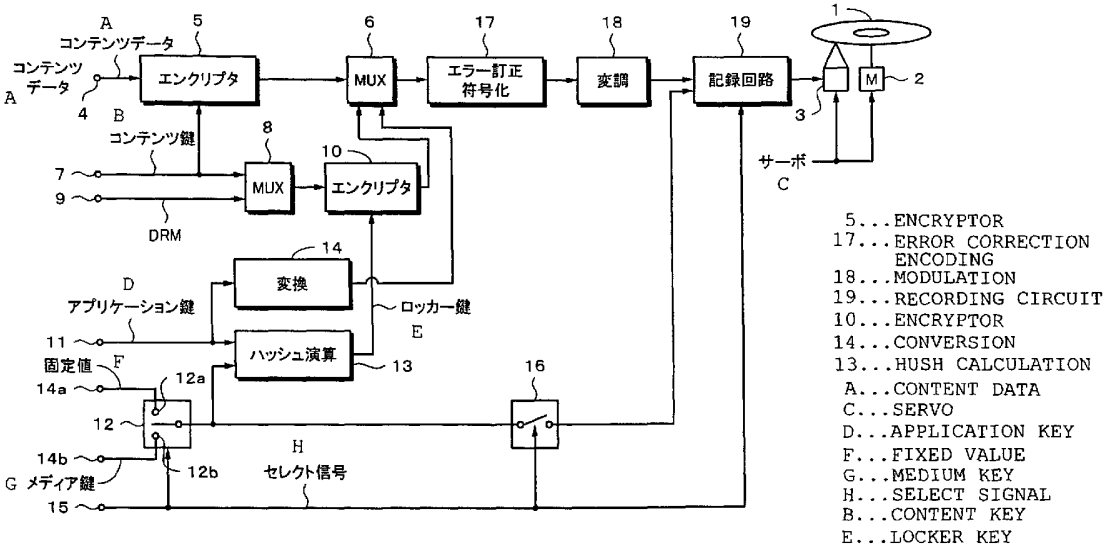
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) **Title:** DATA RECORDING APPARATUS AND METHOD, AND DATA REPRODUCTION APPARATUS AND METHOD

(54) 発明の名称: データ記録装置および方法、並びにデータ再生装置および方法



(57) **Abstract:** A recording medium recording method in which encryption is performed by using key data that can serve as key data dedicated for recording media when embedded in the input content data or fixed value data. When encoding the encrypted data, for the data encrypted by using the key data, the key data is embedded and the encoded data is recorded on a recording medium.

[続葉有]

WO 03/012786 A1

(57) 要約:

入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理し、暗号化処理されたデータにエンコード処理を施す際に、暗号化処理の際に記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込み、エンコード処理されたデータを記録媒体に記録する記録媒体の記録方法。

明　細　書

データ記録装置および方法、並びにデータ再生装置および方法

技術分野

この発明は、暗号化によってセキュリティを保つようにしたデータ記録装置および方法、並びにデータ再生装置および方法に関する。

背景技術

近年、音楽情報が記録された所謂ＣＤ(Compact Disc)のディジタルデータをＭＰ３（ＭＰＥＧ（Moving Picture Experts Group）－１Audio Layer Ⅲ）で圧縮したコンテンツがインターネットを介して配信されたり、ＣＤ－Ｒ(CD-Recordable)ディスクにＣＤから読み出されたデータがコピーされたり、米Napster社が提供するピア・ツー・ピア型の音楽ファイルの交換サービスが広まっており、著作権保護（以下、適宜セキュリティと称する）の問題が大きくクローズアップされている。このため、近年提案されている新規なメディア、例えば（ＳＡＣＤ(Super Audio CD)、ＤＶＤ(Digital Versatile Disc またはDigital Video Disc)オーディオ、メモリカード等の記録媒体では、コンテンツを暗号化することによって、セキュリティを保っている。例えばメモリカードは、フラッシュメモリを使用し、機器に着脱自在とされたもので、暗号化された音楽データをメモリカードに記録、記憶しようとするときには、機器の認証が行なわれ、認証が成立、即ち機器の認証が正しく行われて初めて暗号化データをメモリカードに記憶、記録することができる。

米DataPlay社の提案による小型光ディスク（直径３２ｍｍ）は、著作権保護技術が採用されている。この技術は、暗号化とコンテンツの再生条件を制御する技術で構成される。著作権保護システムのみがアクセ

スできるディスク内周部の専用領域にコンテンツに施されている暗号を解く「暗号化キー」とユーザによるアクセス条件を規定する「条件アクセスキー」が格納される。

コンテンツデータに施されている暗号化を解く為の鍵情報そのものではなく、鍵情報を生成するのに不可欠な情報を再生専用領域（ＲＯＭ部分）に記録することが考えられている。例えばＤＶＤの不正コピー防止技術として、書き換え可能なＤＶＤの最内周部の再生専用領域（ＲＯＭ部分）にメディアＩＤデータを記録し、メディアＩＤデータとＭＫＢ(Media Key Block) のハッシュ値を鍵データとして暗号化されたコンテンツをそのディスクに記録することが提案されている。メディアＩＤデータは、ディスク毎に異なる値であり、ユーザが書き換えることができない。その結果、たとえデータ部分を他の別のディスクに不正にコピーしても、メディアＩＤデータが複製元となったディスクのメディアＩＤデータとは異なるので、不正にコピーしたデータ部分を復号することが不可能である。

上述したような著作権保護対策がなされた新規メディアを利用するためには、新規なレコーダ／プレーヤを購入する必要がある。このことは、ユーザに新たな経済的な負担を生じさせるので、新規メディアが広く普及する妨げとなる。一方、既存のレコーダ／プレーヤに著作権保護対策を導入しようとしても、互換性の問題が生じたり、互換性をとるためにパーソナルコンピュータにインストールしたソフトウェアで暗号化を復号しようとすると、充分な著作権保護ができない問題があった。

したがって、この発明の目的は、メディアにバインドした鍵を使用して暗号化する本格的なセキュリティ機能の導入を容易とすることが可能なデータ記録装置および方法、並びにデータ再生装置および方法を提供することにある。

発明の開示

上述した課題を達成するために、請求の範囲第１項の発明は、入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理を施す暗号化処理部と、

暗号化処理部からの出力データにエンコード処理を施すとともに、暗号化処理部で記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込むエンコード処理部と、

エンコード処理部からの出力データを記録媒体に記録する記録部とを備えている記録媒体の記録装置である。

請求の範囲第９項の発明は、入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理し、

暗号化処理されたデータにエンコード処理を施す際に、暗号化処理の際に記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込み、

エンコード処理されたデータを記録媒体に記録する記録媒体の記録方法である。

請求の範囲第１７項の発明は、コンテンツデータが暗号化されて記録されている記録媒体からデータを読み出すヘッド部と、

ヘッド部からの信号にデコード処理を施すデコーダと、

記録媒体から読み出された記録媒体に記録されることによって記録媒体専用の鍵データとなる鍵データ又は固定値データのいずれかを用い

てデコーダからの出力データに施されている暗号を解く解読処理部とを備えている記録媒体の再生装置である。

請求の範囲第２３項の発明は、コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号されて記録されているとともに、コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録された記録媒体から識別データを読み出し、

読み出された識別データによってコンテンツデータが固定値データによって暗号化処理されていると判別されたときには、記録媒体から読み出されたデータを固定値データによって暗号の解読処理を行い、

読み出された識別データによってコンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データによって暗号化されていると判別されたときには、記録媒体から読み出されたコンテンツデータを記録媒体から読み出された記録されることによって記録媒体専用の鍵データとなる鍵データとを用いて暗号の解読処理を行う記録媒体の再生方法である。

請求の範囲第２５項の発明は、暗号化されたコンテンツデータが記録されるデータ領域と、

データ領域に先立って読み出される位置に設けられ、データ領域の管理データと、コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データとを含むデータが記録される管理データ領域とを備えている記録媒体である。

図面の簡単な説明

第１図は、この発明の一実施形態における記録装置の構成例を示すブロック図、第２図は、この発明の一実施形態における再生装置の構成例を示すブロック図、第３図は、この発明の一実施形態におけるタイプ識別動作の処理の流れを示すフローチャートである。

発明を実施するための最良の形態

以下、この発明の一実施形態について説明する。この一実施形態は、記録媒体として光ディスクに本発明を適用した例である。第１図を参照して、記録装置の一例について説明する。第１図において、参照符号１が光ディスク例えばＣＤ－ＲＷディスクまたはＣＤ－Ｒディスクと同様に記録可能な光ディスクを示す。この光ディスク１に対して記録されるコンテンツデータは、全て暗号化されるものと規定する。したがって、暗号化を行なわない既存の光ディスク記録及び／又は再生装置によって、光ディスク１を用いて記録又は再生を行うことができない。

第１図に示す記録装置および後述する再生装置（第２図）は、図示の如く専用のハードウエアである必要はなく、パーソナルコンピュータとソフトウェアによって実現することもできる。特に、この場合には、セキュリティに関連する暗号化および復号化の処理はソフトウェアによって実現される。

光ディスク１は、スピンドルモータ２によって、線速度一定または角速度一定で回転駆動される。第１図に示す記録装置では、光ディスク１にデータを記録し、光ディスク１に記録されたデータを読み出すために、光ピックアップ３が設けられている。光ピックアップ３が送りモータ（図示しない）によって光ディスク１の径方向に移動される。

この一実施形態の光ディスク１には、記録に必要とされる出力レベルのレーザ光を照射することによってデータの記録が可能で、光ディスク

１によって反射されたレーザ光の光量の変化を検出することによって再生可能な書き換え可能な光ディスクである相変化型ディスクである。相変化記録材料からなる記録膜が被着される基板は、例えばポリカーボネートを射出成形することによって形成される。基板の一方の面にはグルーブと呼ばれるトラック案内溝が予め形成されている。このディスク基板の一方の面に形成されるグルーブは、予め形成する意味でプリグルーブとも呼ばれ、グルーブの間は、ランドと呼ばれる。通常、読取レーザ光の入射側から見て手前側がランドであり、遠い側がグルーブであると定義される。グルーブは、内周から外周へスパイラル状に連続して形成されている。なお、本発明は、記録可能であれば、相変化型光ディスクに限らず、光磁気ディスク、有機色素を記録材料として使用する追記形ディスクに対しても適用できる。

グルーブは、光ディスク１の回転制御用と記録時の基準信号とするために光ディスクの径方向に蛇行（ウォブルと称する）している。データは、グルーブ内、またはグルーブおよびランドに記録される。さらに、グルーブのウォブル情報としてアドレス情報としての絶対時間情報を連続的に記録している。換言すると、グルーブはアドレス情報に基づいて光ディスク１の半径方向に蛇行、即ちウォブリングされている。ＣＤ－Ｒディスク、ＣＤ－ＲＷディスクでは、ウォブリングされているグルーブを検出することによって得られるアドレス情報としての絶対時間情報を参照して光ディスク１上の所望の書き込み位置を検索し、光ピックアップ３を光ディスク１の半径方向に移動させ、光ピックアップ３から光ディスク１に対してレーザ光を照射することによって、データをディスクに書き込むようにしている。

このようなウォブリングしたグルーブを有する光ディスクは、以下のようにして製造される。マスタリング装置は、ディスク状のガラス原盤

に塗布されたフォトレジスト膜にレーザ光を照射すると共に、レーザ光を径方向に偏向または径方向に振ることによって、アドレス情報、クロック情報等を有するウォブリンググルーブの潜像をフォトレジスト膜に形成する。レーザ光の照射によって露光されたフォトレジスト膜を現像することによってディスク原盤が作成され、ディスク原盤から電鋳処理によってスタンパが作成される。作成されたスタンパを用いて射出成形を行うことによって、上述したウォブリングされたグルーブを有するディスク基板が成形される。このディスク基板のグルーブが形成されている面に相変化型の記録材料等の光記録材料をスパッタリング等の手法を用いて被着することによって記録可能な光ディスクが作成される。

第１図に戻ると、記録すべきコンテンツデータ例えばオーディオおよび／またはビデオデータが入力端子４からエンクリプタ５に供給される。エンクリプタ５によって暗号化されたコンテンツデータがマルチプレクサ６に供給される。エンクリプタ５は、入力端子７からのコンテンツ鍵データを使用してコンテンツデータに暗号化する。入力端子７から入力されたコンテンツ鍵データは、マルチプレクサ８にも供給される。

マルチプレクサ８にどのようにコンテンツを扱うかを指示又は規定する管理情報（ＤＲＭ(Digital Rights Management)データと表記する）が入力端子９から供給される。例えばコピーの可否、コピー世代の管理の情報がＤＲＭに含まれている。マルチプレクサ８の出力データがエンクリプタ１０によって暗号化される。このエンクリプタ１０は、コンテンツ鍵データとＤＲＭデータとを暗号化するためのものである。エンクリプタ１０から出力される暗号化されたコンテンツ鍵データおよびＤＲＭデータがマルチプレクサ６に供給される。

エンクリプタ１０に対しては、ロッカー鍵データが供給され、ロッカー鍵データによってコンテンツ鍵データおよびＤＲＭデータが暗号化さ

れる。ハッシュ演算部１３において、入力端子１１からのアプリケーション鍵データとセレクタ１２で選択されたデータとのハッシュ値が演算される。このハッシュ値がロッカー鍵データである。アプリケーション鍵は、メディア、本発明では光ディスク１にバインドしていない鍵を意味し、ソフトウェアにより保持され、または、デバイスにより保持されている。アプリケーション鍵データは、変換部１４において例えばスクランブル処理のようなデータ変換処理を受け、マルチプレクサ６に供給される。

メディア、即ち光ディスク１にバインドしている鍵データとは、そのメディアに記録されることによって、そのメディアに専用の鍵データとなるものを意味する。メディアにバインドしている鍵データは、暗号化によるセキュリティ対策を行なわない既存の記録及び／又は再生装置によってメディアを再生した時には、読み取れないように、そのメディアに埋め込まれている。一方、セキュリティ対策を行う新規な記録及び／又は再生装置によって、メディアにバインドしている鍵データを読み取ることができる。具体的には、ピット自身の変形またはピットの変位（ウォブリング）により表される鍵データ、ＥＦＭ変調における結合ビット（３ビット）を使用して表現された鍵データ、ディスク最内周領域に記録されたディスク固有のＩＤデータ等がメディアにバインドしている鍵データである。新規な記録及び／又は再生装置は、メディアから読み出されたデータからメディアにバインドしている鍵データを抽出し、抽出された鍵データによって暗号化されているコンテンツデータを復号することができる。しかしながら、新規な記録及び／又は再生装置は、鍵データ自体を外部から知ることができないような対策がとられているのが普通であり、暗号化されたコンテンツデータと鍵データとを不正にコピーしたメディアを作成することができない。

セレクタ１２は、第１の入力端子１２ａ、第２の入力端子１２ｂおよび出力端子を有する。セレクタ１２の入力端子１２ａと接続された入力端子１４ａには、固定値データが供給され、セレクタ１２の入力端子１２ｂと接続された入力端子１４ｂには、メディア鍵データが供給される。セレクタ１２は、例えば第１図に示す記録装置全体の動作を制御するソフトウェアに基づいて形成され、入力端子１５に供給されるセレクト信号によって制御される。セレクタ１２が選択したメディア鍵データおよび固定値データの一方がハッシュ演算部１３およびゲート１６に供給される。

以下、セレクタ１２によって入力端子１４ａから入力される固定値が選択されてデータが記録される光ディスク、すなわち、メディアにバインドしない光ディスクをタイプＡのディスクと適宜呼び、セレクタ１２によって入力端子１２ｂから入力されるメディア鍵データが選択されてデータが記録される光ディスク、すなわち、メディアとしての光ディスクにバインドした光ディスクをタイプＢのディスクと適宜呼ぶことにする。タイプＡおよびタイプＢの何れのディスクも、暗号化されたコンテンツデータが記録されるものである。

第１図に示す記録装置全体の動作を制御するソフトウェアは、ＣＤ－ＲＯＭ等の記録媒体、またはインターネット等のネットワークを介して配布されたものである。例えばメディア鍵データが記録されたタイプＢのディスクを再生できる新規な記録及び／又は再生装置が未だ充分に普及していない段階では、固定値を選択するようにセレクタ１２を制御するセレクト信号をソフトウェアに基づいて、例えば図示しないコントローラが生成し、出力する。その後、新規な記録及び／又は再生装置が充分に普及した段階では、メディア鍵データを選択するようにセレクタ１２を制御するセレクト信号を発生するソフトウェアが配布される。なお、

ユーザが所有している記録及び／又は再生装置がタイプＡおよびタイプＢの何れのディスクに対応しているかに応じてセレクト信号を発生しても良い。この場合、例えば、本発明に係る第１図に示す記録装置では、図示しないコントローラが、記録装置自身がタイプＡ及びタイプＢの何れのディスクに対応しているのかに応じたセレクト信号を発生する。

固定値データを使用して暗号化されたタイプＡのディスクは、既存の記録再生装置又は再生装置で再生することができない。しかしながら、固定値データを使用して暗号化を復号するデクリプタを既存の装置に付加する変更を加えれば、タイプＡのディスクを再生することができる。メディア鍵データの読取、ロッカー鍵データおよびコンテンツ鍵データの生成等の処理に必要な構成を付加する必要がないので、比較的低コストな構成が可能である。さらに、コンテンツデータに施されている暗号の復号をソフトウェア処理を行う場合では、タイプＡのディスクを既存の再生装置又は記録再生装置で再生し、固定値を使用してタイプＡのディスクから読み出されたデータの暗号を解き復号することができる。この場合では、既存の再生装置、記録再生装置のハードウエアの変更を殆ど行なわずにタイプＡのディスクを再生することが可能となる。

メディア鍵データは、上述したメディア（ここでは光ディスク１）にバインドしている鍵データを意味する。一方、固定値データは、メディアにバインドしていない値である。例えば全て"1" のデータ、全て"0" のデータ、"101010・・・10"のような既知のパターンのデータが固定値データである。さらに、光ディスク１の最内周側のリードイン領域の特定のアドレスに記録されている特定のデータを固定値データとして使用しても良い。リードイン領域は暗号化されたコンテンツデータ等が記録されるデータ領域と、このデータ領域に記録されたデータの管理データとしてのＴＯＣデータが記録される管理データ領域として機能し、デー

タ領域に先立って読み出される。例えばＴＯＣ(Table Of Contents)データ中のプログラムスタート時間、曲数のデータ、そのディスクの総演奏時間のデータ等を使用できる。メディア鍵データは、光ディスク１に必ず記録されるが、再生装置又は記録再生装置にとって光ディスク１の再生にあたって既知の固定値データは光ディスク１に記録する必要がない。上述したＴＯＣデータ中の所定のデータを固定値データとする場合では、ＴＯＣデータ自身が例えば、第１図に示す記録装置によって記録されるので、殊更、固定値データを記録する必要はない。尚、ＴＯＣデータは光ディスク１がタイプＡのディスクであるのか、タイプＢのディスクであるのかを示すタイプＩＤデータを含んでいる。

メディア鍵データを光ディスク１に記録するときに、ゲート１６は、セレクタ１２がメディア鍵データを選択しているときにはオンするように、入力端子１５から供給されるセレクト信号によって制御される。セレクタ１２が固定値データを選択する時には、ゲート１６はセレクト信号によってオフとされる。メディア鍵データを記録するときは、ゲート１６を介してセレクタ１２から出力されたメディア鍵データが記録回路１９に供給される。

マルチプレクサ６は、暗号化されたコンテンツデータ、暗号化されたコンテンツ鍵データおよびＤＲＭデータ、並びに変換されたアプリケーション鍵データを所定のデータフォーマットに変換する。マルチプレクサ６の出力データがエラー訂正符号化器１７に供給される。マルチプレクサ６からの出力データは、エラー訂正符号化器１７によってエラー訂正符号化の処理がなされる。エラー訂正符号化器１７の出力データが変調部１８で変調される。例えば変調部１８によってＥＦＭ変調の処理がなされる。変調部１８の出力データが記録回路１９に供給される。

記録回路１９にゲート１６を介して出力されるメディア鍵データとセ

レクタ１２を制御するセレクト信号とが供給される。記録回路１９では、フレーム同期信号、アドレス情報等の付加の処理を行い、メディア鍵データおよびセレクト信号がそれぞれ記録データに変換される。例えばＥＦＭ変調における結合ビット（３ビット）を利用してメディア鍵データが光ディスク１に記録される。この場合では、メディア鍵データを変調部１８に供給するようにしても良い。リードインエリアのＴＯＣデータの一部のデータとしてセレクト信号に基づいて生成されたタイプ識別子が記録される。さらに、記録回路１９のレーザ駆動回路では、光ディスク１に記録データを記録するための所定のレベルを有するドライブ信号が生成される。レーザ駆動回路のドライブ信号が光ピックアップ３の半導体レーザに供給され、半導体レーザから供給されたドライブ信号に基づいて変調されたレーザ光が光ディスク１に照射され、データが記録される。

第２図は、この発明が適用され、第１図の記録系に対応する再生系の構成の一例を示す。光ディスク１に光ピックアップ３から再生に必要とされる出力レベルを有するレーザ光を照射し、光ピックアップ３に設けられた４分割フォトディテクタによって光ディスク１によって反射されたレーザ光を検出する。フォトディテクタからの出力信号としての検出された信号がＲＦ処理ブロック２１に供給される。ＲＦ処理ブロック２１では、マトリックスアンプがフォトディテクタの出力信号を演算することによって、再生（ＲＦ）信号、トラッキングエラー信号、フォーカスエラー信号を生成する。ウォブリンググルーブとしてクロック信号およびアドレス情報が記録されている場合では、リングされたグルーブを検出した信号がＲＦ処理ブロック２１から出力される。なお、記録系と同様に再生系も、第１図又は第２図に示すような装置、つまり専用のハードウエアに限らず、パーソナルコンピュータとソフトウェアによって

実現することが可能である。

ＲＦ信号が復調部２２に供給され、例えばＥＦＭ復調が行われる。復調部２２の出力データがエラー訂正回路２３に供給され、エラー検出及びエラー訂正処理が行われる。エラー訂正回路２３の出力信号がデマルチプレクサ２４およびタイプＩＤ（識別子）読取部２５に供給される。ＲＦ処理ブロック２１からは図示しないサーボ回路に、トラッキングエラー信号、フォーカスエラー信号が供給され、スピンドルモータ２の回転および光ピックアップ３のトラッキング制御およびフォーカス制御が行われる。サーボ回路は、光ピックアップ３に対するトラッキングサーボおよびフォーカスサーボと、スピンドルモータ２に対するスピンドルサーボと、光ピックアップ３の光ディスク１への移動を制御するスレッドサーボを行う。ウォブル信号を復調することによってアドレス情報が取り出される。このアドレス情報は、ＡＴＩＰ(Absolute Time In Pre-groove）と称され、時間情報によってディスク上の絶対アドレスを示すものである。アドレス情報は、第２図に示す再生装置のシステムコントローラ（図示しない）に供給され、光ディスク１上の所望のアドレスの情報を読み取る為に用いられる。

デマルチプレクサ２４は、暗号化されたコンテンツデータ、暗号化されたコンテンツ鍵データおよびＤＲＭデータ、並びに変換されたアプリケーション鍵データを分離して出力する。暗号化されたコンテンツデータが暗号化の復号を行うデクリプタ２６に供給される。デクリプタ２６によって暗号化されたコンテンツデータが復号され、出力端子２７には、光ディスク１から再生され、復号された、即ち暗号化が解かれたコンテンツデータが取り出される。

デマルチプレクサ２４で分離された暗号化されたコンテンツ鍵データおよびＤＲＭデータがデクリプタ２８に供給され、変換されたアプリケ

ーション鍵データが逆変換部２９に供給される。逆変換部２９は、記録系（第１図参照）の変換部１４でなされた変換処理と逆の処理を行なうものである。例えば記録系でアプリケーション鍵データに対してスクランブル処理が施される場合では、逆変換部２９では、アプリケーション鍵データにデスクランブル処理が行われる。逆変換部２９から出力されるアプリケーション鍵データがハッシュ演算部３０に供給される。

ハッシュ演算部３０には、セレクタ３１の出力データも供給されている。セレクタ３１の一方の入力端子３１ａには、デマルチプレクサ２４から出力される固定値データが供給され、その他方の入力端子３１ｂには、ＲＦ処理ブロック２１で分離されたメディア鍵データが供給される。固定値データは、例えばＴＯＣデータの一部に記録されている特定のデータである。デマルチプレクサ２４は、固定値データを分離して出力する。デマルチプレクサ２４が固定値データを発生し、発生した固定値データを出力するようにしても良い。

メディア鍵データは、光ディスク１（タイプＢ）にバインドしている鍵データであり、外部から知ることが殆ど不可能なように、秘密に光ディスク１に記録されている。光ディスク１がタイプＡのディスクであれば、メディア鍵データが記録されていない。セレクタ３１は、タイプＩＤ読取部２５から出力されるタイプＩＤデータによって制御される。

タイプＩＤデータは、例えば前述したように光ディスク１の最内周部のＴＯＣデータの一部のデータとして記録される。光ディスク１を第２図に示す再生装置に装着した場合、最初にＴＯＣデータが記録されている領域のデータ情報が読み出される。タイプＩＤデータがタイプＡのディスクを示している場合では、入力端子３１ａが選択され、デマルチプレクサ２４からの固定値データがハッシュ演算部３０に供給される。タイプＩＤデータがタイプＢのディスクを示している場合では、入力端子

３１ｂが選択され、ＲＦ処理ブロック２１からのメディア鍵データがハッシュ演算部３０に供給される。ハッシュ演算部３０によってセレクタ３１からの出力データとアプリケーション鍵データのハッシュ値が求められる。ハッシュ演算部３０によって求められたハッシュ値がロッカー鍵データである。

ハッシュ演算部３０からのロッカー鍵データがデクリプタ２８に供給される。デクリプタ２８によって、コンテンツ鍵データおよびＤＲＭデータに施されている暗号化が復号される。デクリプタ２８に接続されたデマルチプレクサ３２は、コンテンツ鍵データと、ＤＲＭデータとを分離して出力する。コンテンツ鍵データが上述したデクリプタ２６に供給され、暗号化されているコンテンツデータの暗号化が復号される。ＤＲＭデータが出力端子３３に取り出される。

第３図は、光ディスク１のタイプ判別とセレクタ３１の制御動作の流れを示すフローチャートである。最初のステップＳ１において、光ディスク１のタイプＩＤデータの読取がなされる。読み取られたタイプＩＤデータに基づいて、再生しようとする光ディスク１がタイプＡか否かがステップＳ２において判定される。ステップＳ２で装着された光ディク１がタイプＡのディスクであると判定されると、デマルチプレクサ２４からの固定値データをセレクタ３１が選択的に出力する（ステップＳ３）。第３図の例では、全て"1"の１２８ビットのデータを固定値データとして使用する例が示されている。

装着された光ディスク１がタイプＡのディスクでないと、ステップＳ２で判定された場合では、ステップＳ４において、装着された光ディスク１がタイプＢのディスクであるか否かが判定される。ステップＳ４で装着されたディスクがタイプＢのディスクであると判定されると、ステップＳ５に進みメディア鍵データが光ディスク１から読み出される。読

み出されたメディア鍵データがステップＳ６においてセレクタ３１から出力される。若し、ステップＳ４において、装着された光ディスク１がタイプＢのディスクでないと判定されると、装着された光ディスクはタイプＡおよびＢの何れのディスクでもないとの判定結果となる。この場合は、再生動作を停止又は中止し、エラー処理が行われる。例えば第２図に示す装置に設けられた図示しない表示部にエラー表示を行い、装着された光ディスクが装置から排出される（ステップＳ７）。

上述したこの発明の一実施形態において、メディアとしての光ディスクにバインドしていない固定値データを使用している場合では、全く同一のデータがコピーされたメディアの作成可能となるので、著作権保護が不十分となる。この影響を軽減するために、固定値データを使用したタイプＡのディスクの場合では、ディスクに記録されているデータ、即ちコンテンツデータの再生環境を制限することが好ましい。例えばタイプＡのディスクでは、ソフトウェアまたはハードウエアのＩＤ（識別子）データをディスクに記録し、そのＩＤデータを共有している装置のみが光ディスクから読み出されたコンテンツデータを再生できるようにする。極端な例は、記録を行なった装置またはソフトウェアのみがその光ディスクを再生することが可能なようにする。一方、メディア鍵データを使用している場合、即ちタイプＢのディスクではディスクから読み出されたコンテンツデータの再生環境を制限しない。

この発明は、上述したこの発明の一実施形態等に限定されるものでは無く、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えば使用する光ディスクとして、前述したタイプＡおよびＢのディスク以外の第３のタイプの光ディスクを使用しても良い。第３のタイプの光ディスクとは、読み出し専用エリアにその光ディスク固有の識別情報が記録されたものである。この識別情報を用いて求められたハッ

シュ値を鍵データとしてコンテンツデータの暗号化がなされる。この発明は、書き換え可能形光ディスク、追記形光ディスク以外に読み出し専用形光ディスクに対しても適用することができる。読み出し専用形の場合では、第１図に示す記録装置は、マスタリング装置に対して適用される。さらに、この発明は、光ディスクに限らず、他のデータ記録媒体例えば半導体メモリを用いるメモリカードに対しても適用することができる。

この発明では、メディアにバインドしているメディア鍵を使用した本格的なセキュリティ機能を実現する新規なドライブが普及していない段階では、本格的なセキュリティ機能との互換性を有する、固定値を使用したセキュリティ機能を実現することによって、新規なドライブをスムーズに導入することが可能となる。また、メディアにバインドしているか否かをタイプＩＤで識別することによって、メディア鍵を使用したセキュリティ機能と固定値を使用したセキュリティ機能とを同じセキュリティシステム上でハンドリングすることができ、互換性を容易にとることができる。さらに、メディアにバインドしていない固定値を使用した場合でも、再生環境を制限することによって、セキュリティを保持することができる。

請　求　の　範　囲

1．入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理を施す暗号化処理部と、

上記暗号化処理部からの出力データにエンコード処理を施すとともに、上記暗号化処理部で上記記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込むエンコード処理部と、

上記エンコード処理部からの出力データを記録媒体に記録する記録部とを備えている記録媒体の記録装置。

2．上記暗号化処理部は、上記入力されたコンテンツデータにコンテンツ鍵データを用いて暗号化処理を施すエンクリプタを備えている請求の範囲第1項記載の記録媒体の記録装置。

3．上記暗号化処理部は、更に上記コンテンツ鍵データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理を行う更なるエンクリプタを備えている請求の範囲第2項記載の記録媒体の記録装置。

4．上記更なるエンクリプタは、上記コンテンツ鍵データとともに上記コンテンツデータの著作権管理データを暗号化処理する請求の範囲第3項記載の記録媒体の記録装置。

5．上記暗号化処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データのいずれかのデータとアプリケーション鍵データとにより演算処理を行う演算処理部を備え、

上記演算処理部からの出力データを上記更なるエンクリプタに暗号化処理のための鍵データとして供給する請求の範囲第3項記載の記録媒体の記録装置。

6．上記エンクリプタからの出力データと上記アプリケーション鍵データと上記更なるエンクリプタからの出力データは、上記エンコード処理部に供給される請求の範囲第４項記載の記録媒体の記録装置。

7．上記暗号化処理部は、更に上記アプリケーション鍵データを変換する変換回路部を備え、上記変換回路部からの出力データが上記エンコーダに供給される請求の範囲第６項記載の記録媒体の記録装置。

8．上記装置は、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データを上記記録媒体に記録する請求の範囲第１項記載の記録媒体の記録装置。

9．入力されたコンテンツデータに記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれかを用いて暗号化処理し、

上記暗号化処理されたデータにエンコード処理を施す際に、上記暗号化処理の際に上記記録されることによって記録媒体専用の鍵データとなる鍵データを用いたときには記録されることによって記録媒体専用の鍵データとなる鍵データを埋め込み、

上記エンコード処理されたデータを記録媒体に記録する記録媒体の記録方法。

１０．上記方法は、上記入力されたコンテンツデータに先ずコンテンツ鍵データを用いて暗号化処理を施す請求の範囲第９項記載の記録媒体の記録方法。

１１．上記方法は、更に上記コンテンツ鍵データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理を行う請求の範囲第１０項記載の記録媒体の記録方法。

１２．上記方法は、上記コンテンツ鍵データとともに上記コンテンツデータの著作権管理データを上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データによって暗号化処理する請求の範囲第１１項記載の記録媒体の記録方法。

１３．上記方法は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データ又は上記固定値データのいずれかのデータとアプリケーション鍵データとにより演算処理を行い、上記演算処理の結果得られるデータを用いて上記コンテンツ鍵データを暗号化処理する請求の範囲第１１項記載の記録媒体の記録方法。

１４．上記方法は、上記暗号化されたコンテンツデータと上記アプリケーション鍵データと上記暗号化されたコンテンツ鍵データとがエンコード処理される請求の範囲第１３項記載の記録媒体の記録方法。

１５．上記方法は、上記アプリケーション鍵データは所定の変換処理が施されたあとにエンコード処理が施される請求の範囲第１４項記載の記録媒体の記録方法。

１６．上記方法は、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データを上記記録媒体に記録する請求の範囲第９項記載の記録媒体の記録方法。

１７．コンテンツデータが暗号化されて記録されている記録媒体からデータを読み出すヘッド部と、

上記ヘッド部からの信号にデコード処理を施すデコーダと、

上記記録媒体から読み出された上記記録媒体に記録されることによって記録媒体専用の鍵データとなる鍵データ又は固定値データのいずれかを用いて上記デコーダからの出力データに施されている暗号を解く解読処理部とを備えている記録媒体の再生装置。

１８．上記解読処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータと上記記録媒体から読み出されたアプリケーション鍵データとを用いて上記デコーダの出力データからコンテンツ鍵データを取り出すディクリプタとを備えている請求の範囲第１７項記載の記録媒体の再生装置。

１９．上記解読処理部は、更に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータと上記記録媒体から読み出されたアプリケーション鍵データとを用いて演算処理を行い、上記演算処理の結果得られるデータを上記ディクリプタに暗号解読の鍵データとして供給する演算処理部を備えている請求の範囲第１８項記載の記録媒体の再生装置。

２０．上記装置は、更に上記演算処理部に上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データとのいずれかのデータを選択的に供給する選択処理部を備えている請求の範囲第１９項記載の記録媒体の再生装置。

２１．上記記録媒体には、上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録されており、上記装置は更に上記デコーダの出力データから上記識別データを読み取る読み取り部を備え、上記読み取り部からの出力データにより上記選択処理部が制御される請求の範囲第２０項記載の記録媒体の再生装置。

２２．上記解読処理部は、更に上記デコーダの出力データに施されている暗号を上記コンテンツ鍵データを用いて解読する更なるディクリプタとを備えている請求の範囲第１８項記載の記録媒体の再生装置。

２３．コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号されて記

録されているとともに、上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データと上記固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データが記録された記録媒体から上記識別データを読み出し、

上記読み出された識別データによって上記コンテンツデータが上記固定値データによって暗号化処理されていると判別されたときには、上記記録媒体から読み出されたデータを上記固定値データによって暗号の解読処理を行い、

上記読み出された識別データによって上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データによって暗号化されていると判別されたときには、上記記録媒体から読み出されたコンテンツデータを上記記録媒体から読み出された上記記録されることによって記録媒体専用の鍵データとなる鍵データとを用いて暗号の解読処理を行う記録媒体の再生方法。

２４．上記方法は、上記記録媒体が上記コンテンツデータが上記記録されることによって記録媒体専用の鍵データとなる鍵データで暗号化されて記録された記録媒体か、上記固定値データを用いて上記コンテンツデータが暗号化されて記録された記録媒体のいずれでもない場合には再生処理を中止する請求の範囲第２３項記載の記録媒体の再生方法。

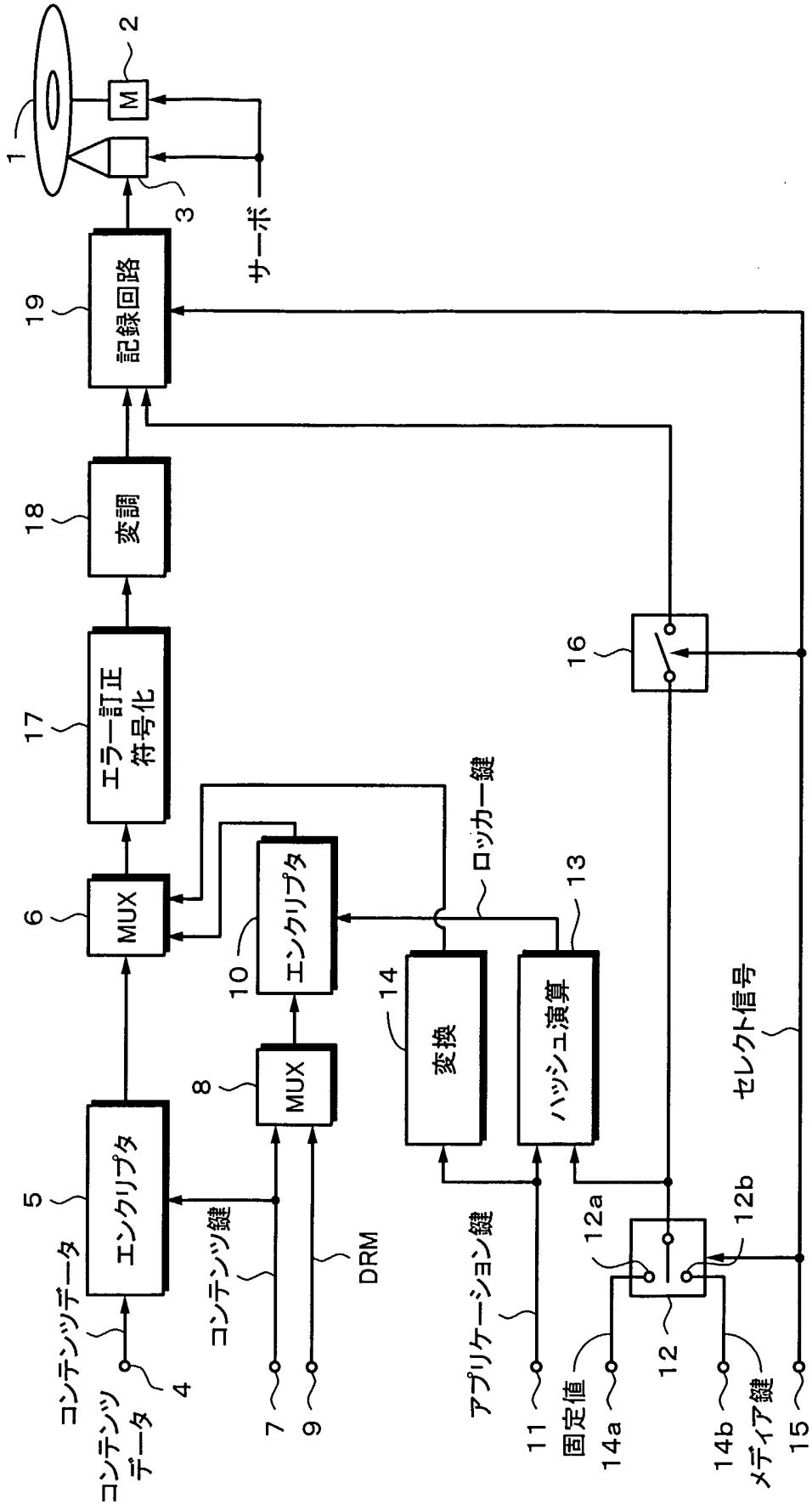
２５．暗号化されたコンテンツデータが記録されるデータ領域と、

上記データ領域に先立って読み出される位置に設けられ、上記データ領域の管理データと、上記コンテンツデータが記録されることによって記録媒体専用の鍵データとなる鍵データと固定値データのいずれが用いられて暗号化処理された記録媒体であるかを示す識別データとを含むデータが記録される管理データ領域とを備えている記録媒体。

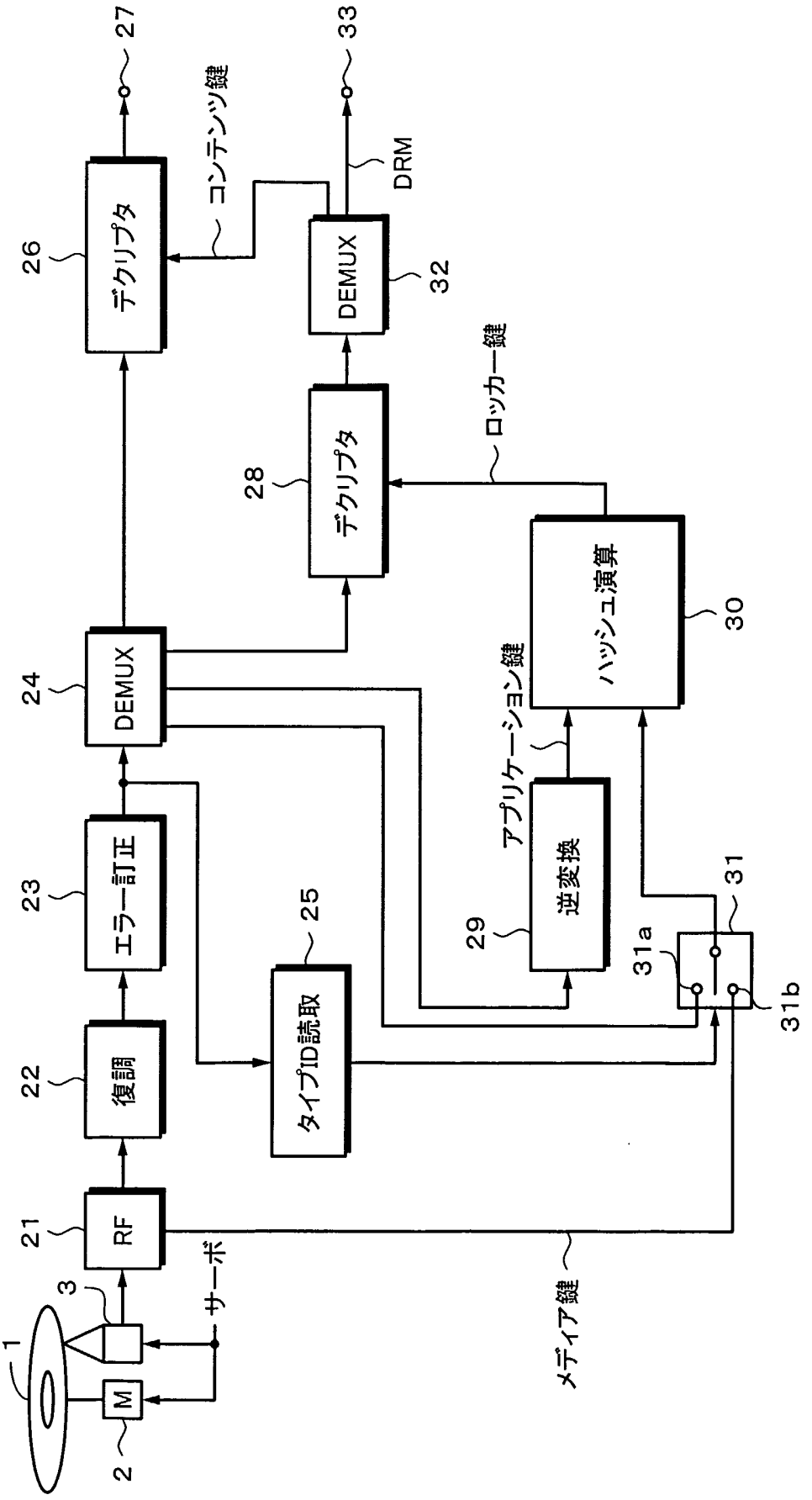
２６．上記管理データ領域には、上記固定値データが記録されている請

求の範囲第２５項記載の記録媒体。

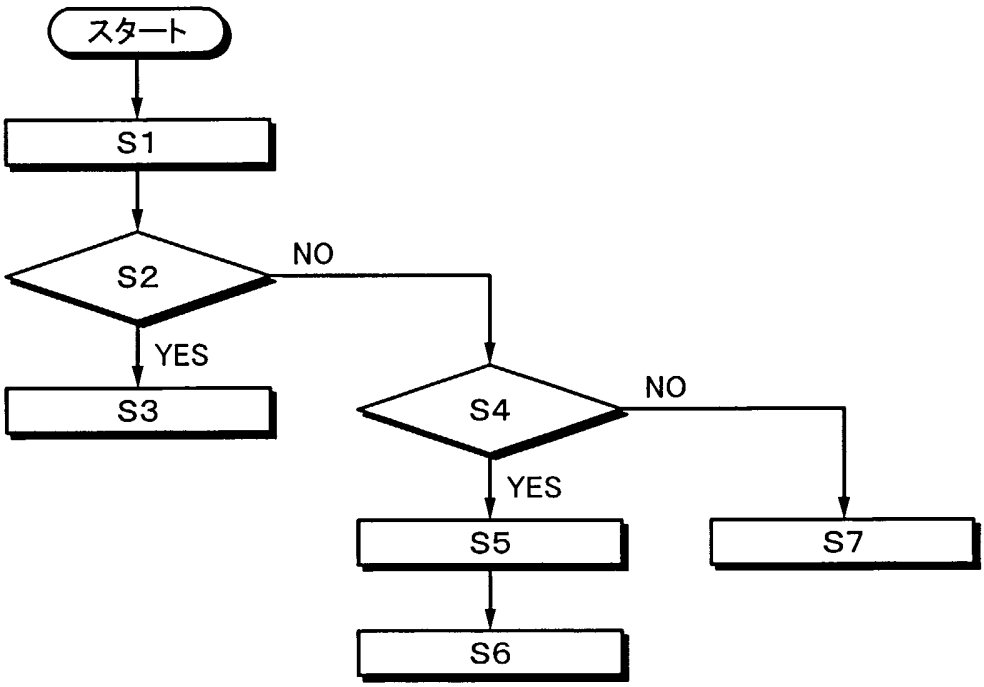
第１図


1
2
M
3
サーボ
19
記録回路
18
変調
17
エラー訂正
符号化
16
6
MUX
10
エンクリプタ
ロッカー鍵
13
14
変換
ハッシュ演算
セレクト信号
5
エンクリプタ
8
MUX
コンテンツデータ
4
コンテンツ
データ
コンテンツ鍵
7
9
DRM
アプリケーション鍵
11
固定値
14a
12a
12
12b
14b
メディア鍵
15

第２図


1
2
M
3
サーボ
21
RF
22
復調
23
エラー訂正
24
DEMUX
25
タイプID読取
26
デクリプタ
27
コンテンツ鍵
28
デクリプタ
29
逆変換
30
ハッシュ演算
31
31a
31b
32
DEMUX
33
DRM
アプリケーション鍵
ロッカー鍵
メディア鍵

第３図



符号の説明

１　光ディスク

３　光ピックアップ

５，１０　エンクリプタ

７　コンテンツ鍵の入力端子

１２　セレクタ

１３　ハッシュ演算部

１４ａ　固定値の入力端子

１４ｂ　メディア鍵の入力端子

１５　セレクト信号の入力端子

Ｓ１　タイプＩＤの読取

Ｓ２　タイプＡか

Ｓ３　固定値：１１・・・１（１２８ビット）出力

Ｓ４　タイプＢか

Ｓ５　メディア鍵読取

Ｓ６　メディア鍵（１２８ビット）出力

Ｓ７　エラー処理

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/07164

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B20/10, H04L9/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B20/10, G09C1/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2000-187935 A (Matsushita Electric Industrial Co., Ltd.), 04 July, 2000 (04.07.00), Full text; Figs. 1 to 25 (Family: none)	1,2,9,10,17, 18,23 3-8,11-16, 19-26
Y	JP 2001-77802 A (Sony Corp.), 23 March, 2001 (23.03.01), Full text; Figs. 1 to 21 (Family: none)	3-7,11-15, 19-22
Y	JP 7-288762 A (Asahi Optical Co., Ltd.), 31 October, 1995 (31.10.95), Full text; Figs. 1 to 17 (Family: none)	8,16,21, 23-26

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 October, 2002 (11.10.02)	29 October, 2002 (29.10.02)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/07164

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 10-283270 A (Fujitsu Ltd.), 23 October, 1998 (23.10.98), Column 16, line 29 to column 18, line 3; Figs. 1 to 3 (Family: none)	1-26
A	WO 00/22777 A (Mitsubishi Corp.), 20 April, 2000 (20.04.00), Full text; Figs. 1 to 14 & EP 1122910 A1	1-26

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０７１６４

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ１１Ｂ２０／１０，　Ｈ０４Ｌ９／１４

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ１１Ｂ２０／１０，　Ｇ０９Ｃ１／００，　Ｈ０４Ｌ９／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００２年
日本国登録実用新案公報	１９９４－２００２年
日本国実用新案登録公報	１９９６－２００２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	ＪＰ　２０００－１８７９３５　Ａ（松下電器産業株式会社） ２０００．０７．０４，全文，第１－２５図（ファミリーなし）	1, 2, 9, 10, 17, 18, 23
Y		3-8, 11-16, 19-26
Y	ＪＰ　２００１－７７８０２　Ａ（ソニー株式会社） ２００１．０３．２３，全文，第１－２１図（ファミリーなし）	3-7, 11-15, 19-22

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 １１．１０．０２	国際調査報告の発送日 29.10.02
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 早川　卓哉　　５Ｑ　９２９５ 電話番号　０３－３５８１－１１０１　内線　３５９０

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０７１６４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　７－２８８７６２　Ａ（旭光学工業株式会社） １９９５．１０．３１，全文，第１－１７図（ファミリーなし）	8, 16, 21, 23-26
Ａ	ＪＰ　１０－２８３２７０　Ａ（富士通株式会社） １９９８．１０．２３，第１６欄第２９行～第１８欄第３行，第１－３図（ファミリーなし）	1-26
Ａ	ＷＯ　００／２２７７７　Ａ（三菱商事株式会社） ２０００．０４．２０，全文，第１－１４図 ＆　ＥＰ　１１２２９１０　Ａ１	1-26