(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-200481
(P2007-200481A)
(43)公開日　平成19年8月9日(2007.8.9)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| G11B 20/10 | (2006.01) | G11B | 20/10 | H | 5B058 |
| G11B 23/30 | (2006.01) | G11B | 20/10 | F | 5D044 |
| G06K 17/00 | (2006.01) | G11B | 20/10 | 301Z | 5J104 |
| H04L 9/32 | (2006.01) | G11B | 23/30 | B | |
| H04L 9/08 | (2006.01) | G06K | 17/00 | F | |

審査請求 未請求　請求項の数 37　ＯＬ　（全 75 頁）　最終頁に続く

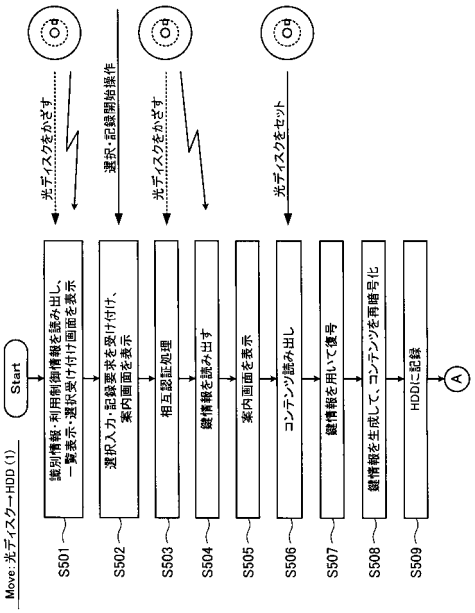
(21)出願番号　特願2006-19075(P2006-19075)
(22)出願日　平成18年1月27日(2006.1.27)

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100092152
弁理士　服部　毅巖
(72)発明者　千秋　進
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Ｆターム(参考)　5B058 CA17 KA31 YA13
5D044 AB05 AB07 BC01 BC02 CC05 CC06 DE49 DE50 DE57 EF05 FG18 GK17 HL08
5J104 EA16 EA20 KA02 NA36 NA38 PA14

(54)【発明の名称】情報記録装置および情報記録方法

(57)【要約】
【課題】ユーザの利便性を損なうことなく、かつ、コンテンツの利用権利情報を安全に管理しながら、光ディスク内のコンテンツを他の記録媒体にコピーできるようにする。
【解決手段】光ディスク内の各コンテンツの識別情報および利用制御情報を、その光ディスク上のＩＣチップから読み出し、それらのコンテンツ名と利用制御情報とを一覧表示させる（Ｓ５０１）。コンテンツの選択入力を受けると（Ｓ５０２）、ＩＣチップとの相互認証処理を実行し（Ｓ５０３）、正しく認証された場合に、選択されたコンテンツに対応する鍵情報をＩＣチップから読み出し（Ｓ５０４）、その鍵情報を用いて、光ディスクから読み出したコンテンツを復号し（Ｓ５０７）、復号されたコンテンツをＨＤＤに記録する（Ｓ５０９）。さらに、ＩＣチップとの相互認証処理を実行し、正しき認証された場合に、ＩＣチップ内の対応する利用制御情報を更新する。
【選択図】図１１



【特許請求の範囲】
【請求項１】
光ディスクドライブを備えた情報記録装置において、
前記光ディスクに設けられたＩＣチップとの間で非接触で情報の送受信を行う通信手段と、
前記通信手段を通じて、前記ＩＣチップの記録情報に対するアクセス許可を得るための前記ＩＣチップとの相互認証処理を実行する認証手段と、
前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上の前記ＩＣチップから前記通信手段を通じて読み込み、読み込んだ前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成手段と、
前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記通信手段を通じて読み込む鍵情報読み込み手段と、
前記鍵情報読み込み手段による前記鍵情報の読み込み後に、選択されたコンテンツに対応する前記暗号化データを前記光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録する記録処理手段と、
前記記録処理手段による前記他の記録媒体へのデータ記録後に、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、前記通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新手段と、
を有することを特徴とする情報記録装置。
【請求項２】
前記通信手段は、前記光ディスクドライブの外部に設けられていることを特徴とする請求項１記載の情報記録装置。
【請求項３】
前記一覧表示画面に従ってユーザに選択されたコンテンツに対応する前記ＩＣチップ内の前記利用制御情報が、ムーブのみ可能であることを示していた場合、前記利用制御情報更新手段は、当該利用制御情報を、利用不可を示すように更新することを特徴とする請求項１記載の情報記録装置。
【請求項４】
選択されたコンテンツに対応する前記鍵情報の読み込みが実行された後、当該コンテンツに対応する前記暗号化データを読み込む前に、前記光ディスクを前記光ディスクドライブにセットするようにユーザに案内するための案内画面を前記ディスプレイに表示させる案内画面生成手段をさらに有することを特徴とする請求項１記載の情報記録装置。
【請求項５】
前記記録処理手段による前記他の記録媒体へのデータ記録後に、前記光ディスクドライブから前記光ディスクを取り出して、前記通信手段の近傍にかざすようにユーザに案内するための案内画面を、前記ディスプレイに表示させる案内画面生成手段をさらに有することを特徴とする請求項１記載の情報記録装置。
【請求項６】
前記記録処理手段は、前記暗号化データを前記鍵情報を用いて復号した後、復号されたコンテンツのデータを他の鍵情報を用いて再び暗号化した後、前記他の記録媒体に記録することを特徴とする請求項１記載の情報記録装置。
【請求項７】
前記鍵情報読み込み手段が、前記選択入力により再生対象とするコンテンツの選択情報を受け付けた場合に、当該コンテンツに対応する前記暗号化データを前記光ディスクドラ

イブを通じて読み込み、前記鍵情報読み込み手段により読み込まれた前記鍵情報を用いて当該暗号化データを復号し、復号されたコンテンツのデータを再生出力する再生出力処理手段をさらに有することを特徴とする請求項１記載の情報記録装置。

【請求項８】

選択されたコンテンツに対応する前記ＩＣチップ内の前記利用制御情報が、再生回数を制限する制限情報を含む場合、前記再生出力処理手段は、当該コンテンツに対応する前記暗号化データの復号後に、当該コンテンツに対応する前記制限情報を更新することを特徴とする請求項７記載の情報記録装置。

【請求項９】

ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、前記認証手段に前記光ディスク上の前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、当該コンテンツのデータを暗号化して、前記光ディスクドライブを通じて当該光ディスクの前記データ領域に記録する光ディスク記録処理手段と、

前記光ディスク記録処理手段によるデータ記録が完了した後、前記認証手段に前記光ディスク上の前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、記録したコンテンツの前記識別情報と、当該コンテンツを復号するための前記鍵情報と、当該コンテンツの利用の可否を示す前記利用制御情報とを、前記通信手段を通じて当該ＩＣチップに記録するＩＣチップ記録処理手段と、

をさらに有することを特徴とする請求項１記載の情報記録装置。

【請求項１０】

前記光ディスク記録処理手段により記録されるコンテンツのデータが前記他の記録媒体に記録されていた場合に、当該コンテンツの利用の可否を示す前記利用制御情報を保持する利用制御情報保持手段をさらに有し、

前記ＩＣチップ記録処理手段は、前記光ディスク記録処理手段によるデータ記録の完了後に、前記利用制御情報保持手段が保持する前記利用制御情報に基づいて、前記ＩＣチップに記録する前記利用制御情報を生成するとともに、前記利用制御情報保持手段が保持する前記利用制御情報を更新する、

ことを特徴とする請求項９記載の情報記録装置。

【請求項１１】

前記光ディスク記録処理手段により記録されるコンテンツのデータが前記他の記録媒体に記録されていた場合に、前記光ディスク記録処理手段は、当該他の記録媒体に記録されたコンテンツを一覧表示した一覧表示画面を前記ディスプレイに表示させ、当該一覧表示画面に応じたユーザの選択操作により前記光ディスクに対するコンテンツの記録要求を受け付けることを特徴とする請求項９の情報記録装置。

【請求項１２】

前記光ディスク記録処理手段によるデータ記録が完了した後、前記光ディスクドライブから前記光ディスクを取り出して、前記通信手段の近傍にかざすようにユーザに案内するための案内画面を前記ディスプレイに表示させる案内画面生成手段をさらに有することを特徴とする請求項９記載の情報記録装置。

【請求項１３】

光ディスクドライブを備えた情報記録装置において、

前記光ディスクに設けられたＩＣチップとの間で非接触で情報の送受信を行う通信手段と、

前記通信手段を通じて、前記ＩＣチップの記録情報に対するアクセス許可を得るための前記ＩＣチップとの相互認証処理を実行する認証手段と、

前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上の前記ＩＣチップから前記通信手段を通じて読み込み、読み込んだ前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成手段と、

前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記通信手段を通じて読み込む鍵情報読み込み手段と、

前記鍵情報の読み込み後に、前記通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新手段と、

選択されたコンテンツに対応する前記暗号化データを前記光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録する記録処理手段と、

を有することを特徴とする情報記録装置。

【請求項１４】

ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、当該コンテンツのデータを暗号化して、前記光ディスクドライブを通じて当該光ディスクの前記データ領域に記録する光ディスク記録処理手段と、

前記光ディスク記録処理手段によるデータ記録が完了した後、前記認証手段に前記光ディスク上の前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、記録したコンテンツの前記識別情報と、当該コンテンツを復号するための前記鍵情報と、当該コンテンツの利用の可否を示す前記利用制御情報とを、前記通信手段を通じて当該ＩＣチップに記録するＩＣチップ記録処理手段と、

をさらに有することを特徴とする請求項１３記載の情報記録装置。

【請求項１５】

ユーザ操作に応じたコンテンツの選択入力および前記光ディスクに対するコンテンツの記録要求を受け付けると、前記認証手段に前記光ディスク上の前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、選択されたコンテンツの前記識別情報と、当該コンテンツを復号するための前記鍵情報と、当該コンテンツの利用の可否を示す前記利用制御情報とを、前記通信手段を通じて当該ＩＣチップに記録するＩＣチップ記録処理手段と、

当該コンテンツのデータを暗号化して、前記光ディスクドライブを通じて当該光ディスクの前記データ領域に記録する光ディスク記録処理手段と、

をさらに有することを特徴とする請求項１３記載の情報記録装置。

【請求項１６】

光ディスクドライブを備えた情報記録装置において、

光ディスクに設けられたＩＣチップとの間で非接触で情報の送受信を行う通信手段と、

前記通信手段を通じて、前記ＩＣチップの記録情報に対するアクセス許可を得るための前記ＩＣチップとの相互認証処理を実行する認証手段と、

前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上の前記ＩＣチップから前記通信手段を通じて読み込み、読み込んだ前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成手段と、

前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データとともに前記データ領域に暗号化されて記録された暗号化鍵情報を復号するための、前記光ディスクに固有な情報からなるディスク鍵を、前記通信手段を通じて読み込むディスク鍵読み込み手段と、

選択されたコンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップから読み込まれた前記ディスク鍵を用いて復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを他の記録媒体に記録する記録処理手段と、

前記他の記録媒体へのデータ記録後に、前記認証手段に前記ＩＣチップとの認証処理を

実行させ、正しく認証された場合に、前記通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新手段と、

を有することを特徴とする情報記録装置。

【請求項１７】

前記ディスク鍵読み込み手段が、前記選択入力により再生対象とするコンテンツの選択情報を受け付けた場合に、当該コンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み、前記ディスク鍵読み込み手段により読み込まれた前記ディスク鍵を用いて当該暗号化鍵情報を復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを再生出力する再生出力処理手段をさらに有することを特徴とする請求項１６記載の情報記録装置。

【請求項１８】

ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、前記通信手段を通じて当該ＩＣチップから前記ディスク鍵を読み込み、当該コンテンツのデータを暗号化して前記暗号化データを生成するとともに、前記暗号化データを復号するための前記鍵情報を前記ディスク鍵を用いて暗号化した前記暗号化鍵情報を生成して、当該暗号化データおよび当該暗号化鍵情報を前記光ディスクドライブを通じて当該光ディスクの前記データ領域に記録する光ディスク記録処理手段と、

前記光ディスク記録処理手段によるデータ記録が完了した後、前記認証手段に前記光ディスク上の前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、記録したコンテンツの前記識別情報と、当該コンテンツの利用の可否を示す前記利用制御情報とを、前記通信手段を通じて当該ＩＣチップに記録するＩＣチップ記録処理手段と、

をさらに有することを特徴とする請求項１６記載の情報記録装置。

【請求項１９】

新たな前記ディスク鍵を生成して前記鍵情報を暗号化し、前記光ディスクドライブを通じて前記光ディスクの前記データ領域に記録する鍵情報更新手段と、

生成された新たな前記ディスク鍵で、前記ＩＣチップ内の元の前記ディスク鍵を更新するディスク鍵更新手段と、

をさらに有し、

前記記録処理手段は、選択されたコンテンツに対応する前記暗号化データとともに、当該コンテンツを含む前記データ領域に記録されたすべてのコンテンツに対応する前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み、読み込んだすべての前記暗号化鍵情報を前記ディスク鍵を用いて復号した後、選択されたコンテンツに対応する復号された前記鍵情報を用いて前記暗号化データを復号し、復号されたコンテンツのデータを前記他の記録媒体に記録し、

前記鍵情報更新手段は、前記データ領域から読み込まれて復号された前記鍵情報のうち、前記他の記録媒体に記録されたコンテンツに対応するものを除くすべての前記鍵情報を、新たな前記ディスク鍵で暗号化して、生成した新たな前記暗号化鍵情報により、前記データ領域内のすべての前記暗号化鍵情報を更新し、

前記ディスク鍵更新手段は、前記利用制御情報更新手段による前記利用制御情報の更新の直前または直後に、前記認証手段により前記ＩＣチップとの間で正しく認証されている状態において、新たな前記ディスク鍵を前記ＩＣチップに上書き記録する、

ことを特徴とする請求項１６記載の情報記録装置。

【請求項２０】

ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、前記通信手段を通じて当該ＩＣチップから前記ディスク鍵を読み込み、当該コンテンツのデータを暗号化して前記暗号化データを生成するとともに、前記光ディスク内に記録されたコンテンツに対応するすべての前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み

、当該暗号化鍵情報を前記ＩＣチップからの前記ディスク鍵で復号した後、新たな前記ディスク鍵を生成して、復号された前記鍵情報と、生成した前記暗号化データを復号するための前記鍵情報とを、新たな前記ディスク鍵を用いて暗号化し、生成されたすべての前記暗号化鍵情報および前記暗号化データを前記光ディスクドライブを通じて当該光ディスクの前記データ領域に記録する光ディスク記録処理手段と、

前記光ディスク記録処理手段によるデータ記録が完了した後、前記認証手段に前記光ディスク上の前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、記録したコンテンツの前記識別情報と、当該コンテンツの利用の可否を示す前記利用制御情報と、新たな前記ディスク鍵とを、前記通信手段を通じて当該ＩＣチップに記録するＩＣチップ記録処理手段と、

をさらに有することを特徴とする請求項１９記載の情報記録装置。

【請求項２１】

光ディスクドライブを備えた情報記録装置において、

光ディスクに設けられたＩＣチップとの間で非接触で情報の送受信を行う通信手段と、

前記通信手段を通じて、前記ＩＣチップの記録情報に対するアクセス許可を得るための前記ＩＣチップとの相互認証処理を実行する認証手段と、

前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上の前記ＩＣチップから前記通信手段を通じて読み込み、読み込んだ前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成手段と、

前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データとともに前記データ領域に暗号化されて記録された暗号化鍵情報を復号するための、前記光ディスクに固有な情報からなるディスク鍵を、前記通信手段を通じて読み込むディスク鍵読み込み手段と、

前記ディスク鍵の読み込み後に、前記通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新手段と、

選択されたコンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップから読み込まれた前記ディスク鍵を用いて復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを他の記録媒体に記録する記録処理手段と、

を有することを特徴とする情報記録装置。

【請求項２２】

ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、前記通信手段を通じて、当該ＩＣチップからの前記ディスク鍵を読み込み、記録するコンテンツの前記識別情報と、当該コンテンツの利用の可否を示す前記利用制御情報とを前記ＩＣチップに記録するＩＣチップ記録処理手段と、

前記ＩＣチップ記録処理手段によるデータ記録が完了した後に、記録するコンテンツのデータを暗号化して前記暗号化データを生成するとともに、前記暗号化データを復号するための前記鍵情報を前記ディスク鍵を用いて暗号化した前記暗号化鍵情報を生成して、当該暗号化データおよび当該暗号化鍵情報を前記光ディスクドライブを通じて前記光ディスクの前記データ領域に記録する光ディスク記録処理手段と、

をさらに有することを特徴とする請求項２１記載の情報記録装置。

【請求項２３】

新たな前記ディスク鍵を生成して、前記ＩＣチップ内の元の前記ディスク鍵を更新するディスク鍵更新手段と、

生成された新たな前記ディスク鍵で前記鍵情報を暗号化し、前記光ディスクドライブを通じて前記光ディスクの前記データ領域に記録する鍵情報更新手段と、

をさらに有し、
前記ディスク鍵更新手段は、前記利用制御情報更新手段による前記利用制御情報の更新の直前または直後に、前記認証手段により前記ＩＣチップとの間で正しく認証されている状態において、新たな前記ディスク鍵を前記ＩＣチップに上書き記録し、
前記記録処理手段は、選択されたコンテンツに対応する前記暗号化データとともに、当該コンテンツを含む前記データ領域に記録されたすべてのコンテンツに対応する前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み、読み込んだすべての前記暗号化鍵情報を前記ディスク鍵を用いて復号した後、選択されたコンテンツに対応する復号された前記鍵情報を用いて前記暗号化データを復号し、復号されたコンテンツのデータを前記他の記録媒体に記録し、
前記鍵情報更新手段は、前記データ領域から読み込まれて復号された前記鍵情報のうち、前記他の記録媒体に記録されたコンテンツに対応するものを除くすべての前記鍵情報を、新たな前記ディスク鍵で暗号化して、生成した新たな前記暗号化鍵情報により、前記データ領域内のすべての前記暗号化鍵情報を更新する、
ことを特徴とする請求項２１記載の情報記録装置。
【請求項２４】
ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、前記通信手段を通じて当該ＩＣチップから前記ディスク鍵を読み込むとともに、新たな前記ディスク鍵を生成して、記録するコンテンツの前記識別情報と、当該コンテンツの利用の可否を示す前記利用制御情報と、新たな前記ディスク鍵とを前記ＩＣチップに記録するＩＣチップ記録処理手段と、
前記ＩＣチップ記録処理手段によるデータ記録が完了した後に、記録するコンテンツのデータを暗号化して前記暗号化データを生成するとともに、前記光ディスク内に記録されたコンテンツに対応するすべての前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップからの前記ディスク鍵で復号した後、復号された前記鍵情報と、生成した前記暗号化データを復号するための前記鍵情報とを、新たな前記ディスク鍵を用いて暗号化し、生成されたすべての前記暗号化鍵情報および前記暗号化データを、前記光ディスクドライブを通じて前記光ディスクの前記データ領域に記録する光ディスク記録処理手段と、
をさらに有することを特徴とする請求項２３記載の情報記録装置。
【請求項２５】
光ディスクに記録された情報を他の記録媒体に記録するための情報記録方法において、
情報読み込み手段が、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上のＩＣチップから非接触通信手段を通じて読み込む情報読み込みステップと、
一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
鍵情報読み込み手段が、認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記非接触通信手段を通じて読み込む鍵情報読み込みステップと、
前記鍵情報読み込み手段による前記鍵情報の読み込み後に、記録処理手段が、選択されたコンテンツに対応する前記暗号化データを光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを前記他の記録媒体に記録する記録処理ステップと、

前記記録処理手段による前記他の記録媒体へのデータ記録後に、利用制御情報更新手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、

を含むことを特徴とする情報記録方法。

【請求項２６】

光ディスクに記録された情報を他の記録媒体に記録するための情報記録方法において、

情報読み込み手段が、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上のＩＣチップから非接触通信手段を通じて読み込む情報読み込みステップと、

一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、

選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、

鍵情報読み込み手段が、認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記非接触通信手段を通じて読み込む鍵情報読み込みステップと、

前記鍵情報の読み込み後に、利用制御情報更新手段が、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、

記録処理手段が、選択されたコンテンツに対応する前記暗号化データを光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを前記他の記録媒体に記録する記録処理ステップと、

を含むことを特徴とする情報記録方法。

【請求項２７】

光ディスクに記録された情報を他の記録媒体に記録するための情報記録方法において、

情報読み込み手段が、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上のＩＣチップから非接触通信手段を通じて読み込む情報読み込みステップと、

一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、

選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、

ディスク鍵情報読み込み手段が、認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データとともに前記データ領域に暗号化されて記録された暗号化鍵情報を復号するための、前記光ディスクに固有な情報からなるディスク鍵を、前記非接触通信手段を通じて読み込むディスク鍵読み込みステップと、

記録処理手段が、選択されたコンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップから読み込まれた前記ディスク鍵を用いて復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを前記他の記録媒体に記録する記録処理ステップと、

前記記録処理手段による前記他の記録媒体へのデータ記録後に、利用制御情報更新手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、

を含むことを特徴とする情報記録方法。

【請求項２８】

光ディスクに記録された情報を他の記録媒体に記録するための情報記録方法において、

情報読み込み手段が、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上のＩＣチップから非接触通信手段を通じて読み込む情報読み込みステップと、

一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、

選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、

ディスク鍵情報読み込み手段が、認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データとともに前記データ領域に暗号化されて記録された暗号化鍵情報を復号するための、前記光ディスクに固有な情報からなるディスク鍵を、前記非接触通信手段を通じて読み込むディスク鍵読み込みステップと、

前記ディスク鍵の読み込み後に、利用制御情報更新手段が、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、

記録処理手段が、選択されたコンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップから読み込まれた前記ディスク鍵を用いて復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを前記他の記録媒体に記録する記録処理ステップと、

を含むことを特徴とする情報記録方法。

【請求項２９】

光ディスクを用いた情報記録方法において、

認証手段が、前記光ディスク上に設けられたＩＣチップとの間で非接触通信手段を通じて相互認証処理を実行する認証ステップと、

前記認証ステップで正しく認証された場合に、光ディスク記録処理手段が、記録対象のコンテンツのデータを暗号化して、光ディスクドライブを通じて当該光ディスクのデータ領域に記録する光ディスク記録処理ステップと、

前記光ディスク記録処理手段によるデータ記録が完了した後、ＩＣチップ記録処理手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、記録が完了したコンテンツを識別するための識別情報と、当該コンテンツを復号するための鍵情報と、当該コンテンツの利用の可否を示す利用制御情報とを、前記非接触通信手段を通じて前記ＩＣチップに記録するＩＣチップ記録処理ステップと、

情報読み込み手段が、前記データ領域に暗号化データとして記録された各コンテンツに対応する前記識別情報と、当該コンテンツのそれぞれに対応する前記利用制御情報とを、前記光ディスク上の前記ＩＣチップから前記非接触通信手段を通じて読み込む情報読み込みステップと、

一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディス

プレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
鍵情報読み込み手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記非接触通信手段を通じて読み込む鍵情報読み込みステップと、
前記鍵情報の読み込み後に、コピー処理手段が、選択されたコンテンツに対応する前記暗号化データを前記光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録するコピー処理ステップと、
前記コピー処理手段によるデータ記録後に、利用制御情報更新手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、
を含むことを特徴とする情報記録方法。
【請求項３０】
光ディスクを用いた情報記録方法において、
光ディスク記録処理手段が、ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、当該コンテンツのデータを暗号化して、光ディスクドライブを通じて当該光ディスクのデータ領域に記録する光ディスク記録処理ステップと、
前記光ディスク記録処理手段によるデータ記録が完了した後、ＩＣチップ記録処理手段が、認証手段に、前記光ディスク上に設けられたＩＣチップとの間で非接触通信手段を通じて相互認証処理を実行させ、正しく認証された場合に、記録が完了したコンテンツを識別するための識別情報と、当該コンテンツを復号するための鍵情報と、当該コンテンツの利用の可否を示す利用制御情報とを、前記非接触通信手段を通じて前記ＩＣチップに記録するＩＣチップ記録処理ステップと、
情報読み込み手段が、前記データ領域に暗号化データとして記録された各コンテンツに対応する前記識別情報と、当該コンテンツのそれぞれに対応する前記利用制御情報とを、前記光ディスク上の前記ＩＣチップから前記非接触通信手段を通じて読み込む情報読み込みステップと、
一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
鍵情報読み込み手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記非接触通信手段を通じて読み込む鍵情報読み込みステップと、
前記鍵情報の読み込み後に、利用制御情報更新手段が、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、
コピー処理手段が、選択されたコンテンツに対応する前記暗号化データを前記光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録するコピー処理ステップと、
を含むことを特徴とする情報記録方法。
【請求項３１】
光ディスクを用いた情報記録方法において、

ＩＣチップ記録処理手段が、ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、認証手段に、前記光ディスク上に設けられたＩＣチップとの間で非接触通信手段を通じて相互認証処理を実行させ、正しく認証された場合に、記録対象のコンテンツを識別するための識別情報と、当該コンテンツを復号するための鍵情報と、当該コンテンツの利用の可否を示す利用制御情報とを、前記非接触通信手段を通じて前記ＩＣチップに記録するＩＣチップ記録処理ステップと、

前記ＩＣチップ記録処理手段によるデータ記録が完了した後、光ディスク記録処理手段が、記録対象のコンテンツのデータを暗号化して、光ディスクドライブを通じて当該光ディスクのデータ領域に記録する光ディスク記録処理ステップと、

情報読み込み手段が、前記データ領域に暗号化データとして記録された各コンテンツに対応する前記識別情報と、当該コンテンツのそれぞれに対応する前記利用制御情報とを、前記光ディスク上の前記ＩＣチップから前記非接触通信手段を通じて読み込む情報読み込みステップと、

一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、

選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、

鍵情報読み込み手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記非接触通信手段を通じて読み込む鍵情報読み込みステップと、

前記鍵情報の読み込み後に、利用制御情報更新手段が、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、

コピー処理手段が、選択されたコンテンツに対応する前記暗号化データを前記光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録するコピー処理ステップと、

を含むことを特徴とする情報記録方法。

【請求項３２】

光ディスクを用いた情報記録方法において、

光ディスク記録処理手段が、ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、認証手段に、前記光ディスク上に設けられたＩＣチップとの間で非接触通信手段を通じて相互認証処理を実行させ、正しく認証された場合に、前記光ディスクに固有なディスク鍵を前記非接触通信手段を通じて前記ＩＣチップから読み込み、当該コンテンツのデータを暗号化して暗号化データを生成するとともに、当該暗号化データを復号するための鍵情報を前記ディスク鍵を用いて暗号化した暗号化鍵情報を生成して、当該暗号化データおよび当該暗号化鍵情報を光ディスクドライブを通じて当該光ディスクのデータ領域に記録する光ディスク記録処理ステップと、

ＩＣチップ記録処理手段が、前記光ディスク記録処理手段によるデータ記録が完了した後、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、記録が完了したコンテンツを識別するための識別情報と、当該コンテンツの利用の可否を示す利用制御情報とを、前記非接触通信手段を通じて前記ＩＣチップに記録するＩＣチップ記録処理ステップと、

情報読み込み手段が、前記データ領域に暗号化データとして記録された各コンテンツに対応する前記識別情報と、当該コンテンツのそれぞれに対応する前記利用制御情報とを、前記光ディスク上の前記ＩＣチップから前記非接触通信手段を通じて読み込む情報読み込みステップと、

一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対

応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
ディスク鍵情報読み込み手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データとともに前記データ領域に暗号化されて記録された暗号化鍵情報を復号するための前記ディスク鍵を、前記非接触通信手段を通じて読み込むディスク鍵読み込みステップと、
記録処理手段が、選択されたコンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップから読み込まれた前記ディスク鍵を用いて復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを他の記録媒体に記録する記録処理ステップと、
前記記録処理手段による前記他の記録媒体へのデータ記録後に、利用制御情報更新手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、
を含むことを特徴とする情報記録方法。

【請求項３３】
光ディスクを用いた情報記録方法において、
第１のディスク鍵読み込み手段が、ユーザ操作に応じた前記光ディスクに対するコンテンツの記録要求を受け付けると、認証手段に、前記光ディスク上に設けられたＩＣチップとの間で非接触通信手段を通じて相互認証処理を実行させ、正しく認証された場合に、前記光ディスクに固有なディスク鍵を前記非接触通信手段を通じて前記ＩＣチップから読み込む第１のディスク鍵読み込みステップと、
情報書き込み手段が、前記ディスク鍵の読み込み後に、記録対象のコンテンツを識別するための識別情報と、当該コンテンツの利用の可否を示す利用制御情報とを、前記非接触通信手段を通じて前記ＩＣチップに記録する情報書き込みステップと、
記録対象のコンテンツのデータを暗号化して暗号化データを生成するとともに、当該暗号化データを復号するための鍵情報を前記ディスク鍵を用いて暗号化した暗号化鍵情報を生成して、当該暗号化データおよび当該暗号化鍵情報を光ディスクドライブを通じて当該光ディスクのデータ領域に記録する光ディスク記録処理ステップと、
情報読み込み手段が、前記データ領域に暗号化データとして記録された各コンテンツに対応する前記識別情報と、当該コンテンツのそれぞれに対応する前記利用制御情報とを、前記光ディスク上の前記ＩＣチップから前記非接触通信手段を通じて読み込む情報読み込みステップと、
一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
第２のディスク鍵読み込み手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データとともに前記データ領域に暗号化されて記録された暗号化鍵情報を復号するための前記ディスク鍵を、前記非接触通信手段を通じて読み込む第２のディスク鍵読み込みステップと、
前記ディスク鍵の読み込み後に、利用制御情報更新手段が、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更

新する利用制御情報更新ステップと、
記録処理手段が、選択されたコンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を前記光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップから読み込まれた前記ディスク鍵を用いて復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを前記他の記録媒体に記録する記録処理ステップと、
を含むことを特徴とする情報記録方法。
【請求項３４】
光ディスクを用いた情報記録処理をコンピュータに実行させる情報記録プログラムにおいて、
情報読み込み手段が、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上のＩＣチップから非接触通信手段を通じて読み込む情報読み込みステップと、
一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
鍵情報読み込み手段が、認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記非接触通信手段を通じて読み込む鍵情報読み込みステップと、
前記鍵情報読み込み手段による前記鍵情報の読み込み後に、記録処理手段が、選択されたコンテンツに対応する前記暗号化データを光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録する記録処理ステップと、
前記記録処理手段による前記他の記録媒体へのデータ記録後に、利用制御情報更新手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、
を含む処理を前記コンピュータに実行させることを特徴とする情報記録プログラム。
【請求項３５】
光ディスクを用いた情報記録処理をコンピュータに実行させる情報記録プログラムにおいて、
情報読み込み手段が、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上のＩＣチップから非接触通信手段を通じて読み込む情報読み込みステップと、
一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
鍵情報読み込み手段が、認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記非接触通信手段を通じて読み込む鍵情報読み込みステップと、
前記鍵情報の読み込み後に、利用制御情報更新手段が、前記非接触通信手段を通じて前

記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、
記録処理手段が、選択されたコンテンツに対応する前記暗号化データを光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録する記録処理ステップと、
を含む処理を前記コンピュータに実行させることを特徴とする情報記録プログラム。
【請求項３６】
光ディスクを用いた情報記録処理をコンピュータに実行させる情報記録プログラムにおいて、
情報読み込み手段が、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上のＩＣチップから非接触通信手段を通じて読み込む情報読み込みステップと、
一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
ディスク鍵情報読み込み手段が、認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データとともに前記データ領域に暗号化されて記録された暗号化鍵情報を復号するための、前記光ディスクに固有な情報からなるディスク鍵を、前記非接触通信手段を通じて読み込むディスク鍵読み込みステップと、
記録処理手段が、選択されたコンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップから読み込まれた前記ディスク鍵を用いて復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを他の記録媒体に記録する記録処理ステップと、
前記記録処理手段による前記他の記録媒体へのデータ記録後に、利用制御情報更新手段が、前記認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、
を含む処理を前記コンピュータに実行させることを特徴とする情報記録プログラム。
【請求項３７】
光ディスクを用いた情報記録処理をコンピュータに実行させる情報記録プログラムにおいて、
情報読み込み手段が、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上のＩＣチップから非接触通信手段を通じて読み込む情報読み込みステップと、
一覧表示画面生成手段が、前記情報読み込みステップで読み込まれた前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成ステップと、
選択入力受け付け手段が、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付ける選択入力受け付けステップと、
ディスク鍵情報読み込み手段が、認証手段に前記非接触通信手段を通じて前記ＩＣチップとの相互認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データとともに前記データ領域に暗号化されて記録された暗号化鍵情報を

復号するための、前記光ディスクに固有な情報からなるディスク鍵を、前記非接触通信手段を通じて読み込むディスク鍵読み込みステップと、

前記ディスク鍵の読み込み後に、利用制御情報更新手段が、前記非接触通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新ステップと、

記録処理手段が、選択されたコンテンツに対応する前記暗号化データおよび前記暗号化鍵情報を光ディスクドライブを通じて読み込み、当該暗号化鍵情報を前記ＩＣチップから読み込まれた前記ディスク鍵を用いて復号し、復号された鍵情報を用いて前記暗号化データを復号して、復号されたコンテンツのデータを他の記録媒体に記録する記録処理ステップと、

を含む処理を前記コンピュータに実行させることを特徴とする情報記録プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、光ディスクを用いて情報を記録する情報記録装置、および情報記録方法に関し、特に、光ディスクに記録されたコンテンツの不正利用が防止された情報記録装置および情報記録方法に関する。

【背景技術】

【０００２】

近年、ＭＰＥＧ（Moving Picture Experts Group）などの信号圧縮技術や、高容量の光ディスクの製造および記録・再生技術などの発展に伴い、ビデオコンテンツをデジタルデータとして取り扱うことが家庭内においても一般的になっている。また、衛星放送に続いて地上波放送でもデジタル放送が開始され、その放送を受信可能なテレビジョン（ＴＶ）セットやレコーダの普及が加速している。特に、最近では、デジタル放送で伝送されたビデオコンテンツを、高解像度のままで長時間記録可能な光ディスクとして、ブルーレイディスク（Blu-ray Disc, ソニー株式会社の登録商標。以下、ＢＤと略称する。）が発売されている。

【０００３】

また、ビデオコンテンツを記録可能な記録媒体として、光ディスクに加えてＨＤＤ（Hard Disk Drive）を備えたビデオレコーダも普及が進んでいる。このようなビデオレコーダでは、例えば、一旦ＨＤＤに記録しておいたＴＶコンテンツのうち、ユーザが長期保存が必要と感じたものを光ディスクにダビングするといった使い方をすることができる。ここで、著作権保護されたビデオコンテンツでは、コピーの可否を示すコピー制御情報が付与されており、ビデオレコーダはこのコピー制御情報に基づき、コピーが可能なビデオコンテンツのみを記録媒体に記録するようになっている。

【０００４】

そして、このコピー制御情報が、１回のみのコピーが可能であることを示す“コピーワンス（Copy Once）”である場合には、ＨＤＤに記憶したビデオコンテンツを光ディスクに移動（ムーブと呼ばれる）することが可能となっている。このムーブという動作は、元の記録媒体から別の記録媒体にコンテンツのデータをコピーした後、元の記録媒体の中のコンテンツのデータを消去（無効化）するものであり、これにより、著作権保護されたコンテンツが不正に多数コピーされることが防止されている。

【０００５】

ところで、ＢＤなどの高容量の光ディスクでは、従来と比較して非常に高解像度のビデオコンテンツをデジタルデータとして取り扱うことが可能となっているため、著作権保護されたコンテンツの不正コピーをより確実に防止できるように、コンテンツの制作者や販売者から要求されている。特に、光ディスクに記録された情報が、ビット単位でそのまま別の記録媒体にコピー（ビットバイビット・コピー（bit by bit copy）と呼ばれる）された場合に、コピー先の記録媒体を再生不可能にするために、固有のＩＤを光ディスクごとに書き換え不可能な状態で記録し、かつ、そのＩＤを用いた鍵でコンテンツを暗号化し

て記録しておくことが現在行われている。

【０００６】

ＢＤを例に挙げると、書き換え可能な光ディスク（以下、ＲＷ（ReWritable）ディスクと呼称する）の場合、上記のＩＤは、ＢＣＡ（Burst Cutting Area）と言われる領域に記録される。また、読み出し専用の光ディスク（以下、ＲＯ（Read Only）ディスクと呼称する）の場合、上記のＩＤはいわゆるＲＯＭ（Read Only Memory）マークとして記録される。このように、上記のＩＤは、一般のユーザには簡単に読み取りや複製が不可能な状態で光ディスク上に記録されており、これにより、例えば、光ディスクの記録データがビット単位でそのまま別の記録媒体にコピー（ビットバイビット・コピー（bit by bit copy）と呼ばれる）された場合に、コピー先の記録媒体からは復号のための鍵を生成できないので、この記録媒体上のデータを利用不可能にすることができる。

【０００７】

しかし、このような対策が施されていた場合にも、不正コピーを完全に防止できるとは言えない。例えば、上記のＢＣＡやＲＯＭマークを信号レベルで読み取り可能な装置があれば、ＢＣＡやＲＯＭマークを複製するとともに、データ領域内の情報をビットバイビットでコピーすることで新たな光ディスクが作製されてしまい、この光ディスクに記録されたコンテンツのデータは再生可能となってしまう。また、光ディスク自体を複製できる装置があれば、新たな光ディスクが作製されてしまい、そのコンテンツが同様に再生可能となってしまう。

【０００８】

また、ＢＤの場合、データ領域内にＲＫＢ（Renewal Key Block）と呼ばれるデータを記録しておき、このＲＫＢと、レコーダやプレーヤごと、あるいはそのメーカごとに固有なデバイスＩＤとを用いて、プロセスＲＫＢと呼ばれる処理によりメディア鍵を生成し、このメディア鍵とディスクＩＤあるいはスタンパＩＤとを用いてブロック鍵を生成して、このブロック鍵を用いてコンテンツのデータを復号することも行われている。これにより、著作権保護技術のライセンスを正式に受けていない不正なデバイスを排除することが可能となる。しかし、この場合でも、ブロック鍵を用いた暗号化されたコンテンツのデータとＲＫＢとをビットバイビットでコピーし、ＢＣＡやＲＯＭマークを複製することにより新たな光ディスクが作製されると、あるいは光ディスク自体が複製されると、この光ディスク内のコンテンツは再生可能となってしまう。

【０００９】

このように、コンテンツのデータの暗号化に用いる情報を単に光ディスク内に記録した場合には、何らかの方法でこれらの情報が複製されると、不正にコピーされたコンテンツの利用を阻止することができなくなってしまうという問題があった。これに対して、複製が困難であり、かつ、再生機器側との相互認証機能により不正な読み出しが防止された非接触型のＩＣチップを光ディスク上に搭載し、このＩＣチップに復号鍵を記録しておくことで、不正な再生動作を防止することが考えられている（例えば、特許文献１参照）。

【特許文献１】特開２００５－１９０５１４号公報（段落番号〔００２４〕～〔００２８〕、図６）

【発明の開示】

【発明が解決しようとする課題】

【００１０】

ところで、光ディスクドライブやＨＤＤを備えたレコーダにおいては、現在、コピーワンスとされたコンテンツをデジタル放送からＨＤＤに録画した後、光ディスクをムーブすることが可能となっているが、光ディスクからＨＤＤに対して再びムーブすることは許されていない。これは、光ディスクからムーブする前に、光ディスクのデータをビットバイビットで他の記録媒体にバックアップしておき、ムーブを行った後、バックアップしてあったデータを元の光ディスクに戻すと、そのデータを再びムーブすることが可能となってしまい、何度でもムーブできてしまうためである。また、同じ理由で、光ディスクからＨＤＤ以外の他の記録媒体へのムーブも許されていない。

【００１１】
しかし、光ディスク上のコンテンツを作業のしやすいＨＤＤに戻して編集したいなど、光ディスクからＨＤＤに再ムーブしたいというユーザの要求は強い。また、近年では、ユーザのデジタルコンテンツの視聴環境は広がりを見せつつあり、例えば、半導体メモリや小型ＨＤＤなどを記録媒体として用いた携帯型プレーヤが実現され、光ディスクに記録したコンテンツであっても、必要に応じてこのような携帯型プレーヤなどに転送して視聴したいといった要求もある。
【００１２】
さらに、このような用途では、元のコンテンツのデータを低ビットレート化して転送する必要があるため、元の品質のデータを残しておきたいという要求もあり、その実現のためには、コンテンツの利用権利情報（例えばムーブ回数など）を安全な状態で管理できる必要もある。また、利用権利情報の安全性の確保とともに、ムーブ時などにおけるユーザの操作が容易であることも重要となる。
【００１３】
本発明はこのような点に鑑みてなされたものであり、ユーザの利便性を損なうことなく、かつ、コンテンツの利用権利情報を安全に管理しながら、光ディスク内のコンテンツを他の記録媒体にコピーできるようにした情報記録装置を提供することを目的とする。
【００１４】
また、本発明の他の目的は、ユーザの利便性を損なうことなく、かつ、コンテンツの利用権利情報を安全に管理しながら、光ディスク内のコンテンツを他の記録媒体にコピーできるようにした情報記録方法を提供することである。
【課題を解決するための手段】
【００１５】
本発明では上記課題を解決するために、光ディスクドライブを備えた情報記録装置において、前記光ディスクに設けられたＩＣチップとの間で非接触で情報の送受信を行う通信手段と、前記通信手段を通じて、前記ＩＣチップの記録情報に対するアクセス許可を得るための前記ＩＣチップとの相互認証処理を実行する認証手段と、前記光ディスクのデータ領域に暗号化データとして記録された１つ以上のコンテンツをそれぞれ識別するための識別情報と、当該コンテンツのそれぞれの利用の可否を示す利用制御情報とを、当該光ディスク上の前記ＩＣチップから前記通信手段を通じて読み込み、読み込んだ前記識別情報に対応するコンテンツ名と対応する前記利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる一覧表示画面生成手段と、前記一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付けると、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する前記暗号化データを復号するための鍵情報を、前記通信手段を通じて読み込む鍵情報読み込み手段と、前記鍵情報読み込み手段による前記鍵情報の読み込み後に、選択されたコンテンツに対応する前記暗号化データを前記光ディスクドライブを通じて読み込み、当該暗号化データを前記ＩＣチップから読み込まれた前記鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録する記録処理手段と、前記記録処理手段による前記他の記録媒体へのデータ記録後に、前記認証手段に前記ＩＣチップとの認証処理を実行させ、正しく認証された場合に、前記通信手段を通じて前記ＩＣチップにアクセスし、選択されたコンテンツに対応する前記利用制御情報を更新する利用制御情報更新手段とを有することを特徴とする情報記録装置が提供される。
【００１６】
このような情報記録装置では、非接触で情報の読み出しおよび書き込みが可能なＩＣチップが搭載された光ディスクから、ユーザに選択されたコンテンツのデータが他の記録媒体に転送され、記録される。光ディスクのデータ領域には、コンテンツのデータが暗号化データとして記録され、ＩＣチップには、各コンテンツを識別するための識別情報と、各コンテンツの利用の可否を示す利用制御情報と、各暗号化データを復号するための鍵情報とが記録されている。

【００１７】
一覧表示画面生成手段は、光ディスクのデータ領域に記録された各コンテンツの識別情報および利用制御情報を、この光ディスク上のＩＣチップから通信手段を通じて読み込み、読み込んだ識別情報に対応するコンテンツ名と対応する利用制御情報とを一覧表示した一覧表示画面をディスプレイに表示させる。鍵情報読み込み手段は、表示された一覧表示画面に応じたユーザからのコンテンツの選択入力を受け付けると、認証手段にＩＣチップとの認証処理を実行させ、正しく認証された場合に、選択されたコンテンツに対応する鍵情報を、ＩＣチップから通信手段を通じて読み込む。記録処理手段は、鍵情報が読み込まれた後、選択されたコンテンツに対応する暗号化データを光ディスクドライブを通じて読み込み、その暗号化データをＩＣチップから読み込まれた鍵情報を用いて復号し、復号されたコンテンツのデータを他の記録媒体に記録する。利用制御情報更新手段は、他の記録媒体へのコンテンツの記録後に、認証手段にＩＣチップとの認証処理を再び実行させ、正しく認証された場合に、通信手段を通じてＩＣチップにアクセスし、選択されたコンテンツに対応する利用制御情報を更新する。

【発明の効果】
【００１８】
本発明の情報記録装置によれば、光ディスクのデータ領域に記録されたコンテンツの暗号化データを復号するための鍵情報を、光ディスクに設けたＩＣチップに記録しておき、ＩＣチップとの間で正しく相互認証された場合のみ、鍵情報を読み出してコンテンツの他の記録媒体への記録処理に利用できるようにしたことで、そのコンテンツの不正利用を確実に防止できる。また、コンテンツの他の記録媒体への記録後、相互認証された状態で、選択されたコンテンツに対応する利用制御情報を更新するようにしたことで、そのコンテンツのユーザによる利用権利を安全に管理しながら、コンテンツのデータを他の記録媒体に記録することができる。例えば、光ディスク内のコンテンツの他の記録媒体への移動や、回数を制限したコピーなどの処理を確実に実行できるようになる。
【００１９】
さらに、ＩＣチップからコンテンツの識別情報と利用制御情報とを読み込み、それらの情報に基づいてコンテンツ名と利用制御情報とを一覧表示し、他の記録媒体に記録するコンテンツを一覧表示に基づいてユーザが選択できるようにしたことで、光ディスクのデータ領域からの情報の読み込みを行うことなく、他の記録媒体に記録可能なコンテンツをユーザが確認して、所望のコンテンツを確実に選択できる。従って、ユーザが余計な操作を行うことなく、所望のコンテンツを他の記録媒体に確実に記録させることができるようになり、ユーザの利便性が向上する。

【発明を実施するための最良の形態】
【００２０】
以下、本発明の実施の形態を図面を参照して詳細に説明する。はじめに、本発明を適用可能なシステム構成例について説明する。
図１は、本発明を適用可能な第１のシステム構成例を示す図である。
【００２１】
図１に示すビデオレコーダ１は、例としてデジタル放送を受信して記録することが可能な装置であり、後述するように、デジタル放送受信のためのチューナや、ＨＤＤ、光ディスク１０の記録再生用の光ディスクドライブなどを備えている。そして、デジタル放送から受信したコンテンツをＨＤＤおよび光ディスク１０に記録できるようになっている。また、このビデオレコーダ１には、ビデオコンテンツの再生画像を表示するためのディスプレイ２が接続されている。
【００２２】
さらに、このビデオレコーダ１には、ＩＣチップＲ／Ｗ（リーダ／ライタ）３が接続されている。ここでは例として、ＩＣチップＲ／Ｗ３は、図示しない通信Ｉ／Ｆを介してビデオレコーダ１の外部に設けられている。このＩＣチップＲ／Ｗ３は、アンテナ４を備えており、光ディスク１０に搭載されたＩＣチップ１１と間でデータを非接触で送受信する

。なお、ＩＣチップＲ／Ｗ３は、このような形態の他に、例えばビデオレコーダ１に搭載された光ディスクドライブのディスクトレイの前面に設けるなど、ビデオレコーダ１の外面にＲ／Ｗ部が露出する状態で、ビデオレコーダ１と一体に設けられてもよい。あるいは、光ディスク１０を内部に装填したまま通信できるように、光ディスクドライブの内部やディスクトレイ上に設けられてもよい。

【００２３】

一方、光ディスク１０には、ＩＣチップ１１およびアンテナ１２からなる、いわゆるＲＦＩＤ（Radio Frequency Identification）タグが搭載されている。これらのＩＣチップ１１およびアンテナ１２は、例えば光ディスク１０のデータ領域の内周側に設けられる。ＩＣチップ１１は、各種データを記憶するメモリや、その読み書き処理機能、外部との相互認証機能を担う処理回路などを備えている。また、このＩＣチップ１１は、内蔵電池を持たず、Ｒ／Ｗからの電波あるいは磁界をアンテナ１２で受信して起電力に変換し、アンテナ１２を通じてＲ／Ｗとのデータの受け渡しを非接触で行うことが可能となっている。

【００２４】

図２は、本発明を適用可能な第２のシステム構成例を示す図である。

図２のシステムでは、デジタル放送チューナが搭載されたセットトップボックス（ＳＴＢ）５を設け、ＳＴＢ５で受信したビデオコンテンツをビデオレコーダ１ａにおいて録画するようにしている。この場合、ＳＴＢ５とビデオレコーダ１ａとの間は、ＩＥＥＥ（Institute of Electrical and Electronic Engineers）１３９４などのデジタルＩ／Ｆ（インタフェース）を介して接続される。このデジタルＩ／Ｆでは、接続されたデバイス間の認証や伝送データの暗号化などが行われることが望ましい。

【００２５】

そして、図１の場合と同様に、ビデオレコーダ１ａは、ＳＴＢ５からのビデオコンテンツを、内部のＨＤＤおよび光ディスク１０に対して録画でき、ビデオレコーダ１ａには、光ディスク１０上のＩＣチップ１１との間で通信するＩＣチップＲ／Ｗ３が接続されている。また、ＳＴＢ５で受信したビデオコンテンツの画像や、ビデオレコーダ１ａでのＨＤＤあるいは光ディスク１０からのコンテンツの再生画像は、ディスプレイ２に表示できるようになっている。

【００２６】

その他のシステム構成としては、例えば、デジタル放送チューナを搭載したディスプレイを用い、このディスプレイにおいて受信したビデオコンテンツを、ビデオレコーダで録画できるようなシステムにも、本発明を適用することができる。また、ビデオレコーダにおいて、ネットワークを介して受信したビデオコンテンツを録画できるシステムにも、本発明を適用可能である。

【００２７】

ところで、上記のＩＣチップ１１には、後述するように、データ領域に記録されたコンテンツの識別情報、それらのコンテンツを利用するための鍵情報、コピー回数やムーブ回数などの利用権利を示す利用制御情報などが記憶される。また、外部機器との相互認証処理に必要な認証鍵なども記憶される。

【００２８】

このＩＣチップ１１は、複製が極めて困難であり、また相互認証機能により不正なデバイスによる記録情報の読み取りや書き換えを防止できるようになっている。以下の各実施の形態では、このようなＩＣチップ１１に対して上記のような情報を記録し、それらの情報を正規のデバイスから利用しないとコンテンツをコピーまたはムーブできないようにしておくことで、データ領域内のコンテンツの不正コピーを防止し、その利用権利を安全な状態で管理できるようにする。

【００２９】

しかし、このようなＩＣチップ１１を備えた光ディスク１０を利用した場合、上記効果が得られる反面、ユーザの利便性を損なう可能性が考えられた。例えば、ビデオレコーダ内の光ディスクドライブの内部にＩＣチップＲ／Ｗが設けられた場合、ユーザは、光ディ

スク１０を光ディスクドライブに装填した後、ＩＣチップ１１の読み取りが開始されるまで、その光ディスク１０内のコンテンツの再生やコピー・ムーブなどが許可されているか否かを知ることができない。

【００３０】

また、光ディスクドライブの内部には、例えば光ディスク１０のチャッキング用のマグネットなど、ＩＣチップ１１との通信状態を悪化させる要因が多い。このため、図１および図２のようにＩＣチップＲ／Ｗを光ディスクドライブの外部に接続して利用するシステム形態も想定しておく必要がある。しかし、この場合には当然、ＩＣチップ１１の記録情報の読み取りや書き換えのためには、光ディスク１０を光ディスクドライブから取り出す必要があるので、コンテンツのコピーやムーブの操作に混乱をきたす可能性がある。

【００３１】

そこで、以下の各実施の形態では、このようなＩＣチップＲ／Ｗを光ディスクドライブの外部に設けた場合を含む、様々なシステム構成において、ユーザの利便性をできるだけ損なうことなく、コンテンツの不正コピーを確実に防止し、かつその利用権利を安全に管理できるような記録・再生手順を提供する。

【００３２】

なお、以下の第１および第２の実施の形態では、例として上記の図１に示したシステム構成について説明し、その他のシステム構成を適用した場合の違いなどについては必要に応じて説明することにする。

【００３３】

《第１の実施の形態》

図３は、本発明の第１の実施の形態に係るビデオレコーダのハードウェア構成を示すブロック図である。

【００３４】

図３に示すビデオレコーダ１は、デジタルテレビジョン（ＴＶ）チューナ１０１、暗号処理回路１０２、ビデオデコーダ１０３、オーディオデコーダ１０４、画像合成処理回路１０５、ビデオＤＡＣ（Digital Analog Converter）１０６、オーディオＤＡＣ１０７、ＣＰＵ（Central Processing Unit）１０８、ＲＯＭ１０９、ＲＡＭ（Random Access Memory）１１０、ＥＥＰＲＯＭ（Electronically Erasable and Programmable Read Only Memory）１１１、ＨＤＤ１１２、光ディスクドライブ１１３、通信Ｉ／Ｆ１１４、および入力Ｉ／Ｆ１１５を具備する。このビデオレコーダ１は、ＣＰＵ１０８が内部バス１１６を介して装置内の各コンポーネントに接続して、これらに対する統括的な制御を実行する構成となっている。

【００３５】

デジタルＴＶチューナ１０１は、デジタルＴＶ放送を受信し、受信信号からビデオストリームやオーディオストリーム、データ放送用データなどを分離する。具体的には、外部のアンテナにより受信された放送電波の入力を受けて、ＣＰＵ１０８から指示された搬送周波数の信号を選択する。そして、選択した受信信号に対してＱＰＳＫ（Quadrature Phase Shift Keying）復調および誤り訂正処理を施して、トランスポートストリームを出力する。このとき、必要に応じてデスクランブル処理を行う。さらに、トランスポートストリームから、ＭＰＥＧ方式のビデオストリームおよびオーディオストリーム、ＥＰＧ（Electronic Program Guide）などのデータ放送用の付加情報、コピー制御情報などを分離する。

【００３６】

暗号処理回路１０２は、内部バス１１６を介して転送するコンテンツのデータの暗号化や、内部バス１１６を介して、あるいはデジタルＴＶチューナ１０１から受信したコンテンツのデータの復号化を行う。復号化したビデオデータはビデオデコーダ１０３へ、オーディオデータはオーディオデコーダ１０４に出力する。また、暗号処理回路１０２は、後述するように、暗号化のための鍵情報を生成する機能や、通信Ｉ／Ｆ１１４に接続されたＩＣチップＲ／Ｗ３を介して、光ディスク１０上のＩＣチップ１１と相互認証する機能な

ども備えている。なお、受信した放送コンテンツのデスクランブル処理機能を、デジタルＴＶチューナ１０１ではなく、暗号処理回路１０２に設けてもよい。

【００３７】

ビデオデコーダ１０３は、暗号処理回路１０２を通じて供給されたビデオデータをＭＰＥＧ－２方式に従って伸張復号処理し、処理後のビデオデータを画像合成処理回路１０５に出力する。また、オーディオデコーダ１０４は、暗号処理回路１０２を通じて供給されたオーディオデータを、ＭＰＥＧ－ＡＵＤＩＯ－Ｌａｙｅｒ２方式に従って伸張復号処理し、処理後のオーディオデータをオーディオＤＡＣ１０７に出力する。

【００３８】

画像合成処理回路１０５は、ビデオデコーダ１０３によりデコード処理されたビデオデータに、ＣＰＵ１０８の処理により生成されたＧＵＩ（Graphical User Interface）画像などのＯＳＤ（On Screen Display）画像データを必要に応じて合成し、ビデオＤＡＣ１０６に出力する。ビデオＤＡＣ１０６は、画像合成処理回路１０５によって生成されたビデオデータをアナログビデオ信号に変換し、外部のディスプレイ２などに出力する。オーディオＤＡＣ１０７は、オーディオデコーダ１０４によりデコード処理されたビデオデータをアナログオーディオ信号に変換し、外部のディスプレイ２のオーディオ入力端子などに出力する。

【００３９】

ＣＰＵ１０８は、ＲＯＭ１０９などに格納されたプログラムを実行することにより、ビデオレコーダ１内の各部を統括的に制御する。ＲＯＭ１０９には、ＯＳ（Operating System）やＢＩＯＳ（Basic Input／Output System）、アプリケーションプログラム、その他の各種データがあらかじめ格納される。ＲＡＭ１１０は、ＣＰＵ１０８に実行させるプログラムの少なくとも一部や、このプログラムによる処理に必要な各種データを一時的に記憶する。ＥＥＰＲＯＭ１１１は、ＣＰＵ１０８に実行させるプログラムや、処理に必要なデータがあらかじめ記録される。

【００４０】

光ディスクドライブ１１３は、光ディスク１０へのデータの書き込み、および光ディスク１０からのデータの読み取りを行う。通信Ｉ／Ｆ１１４は、例えばＵＳＢ（Universal Serial Bus）規格などに準じた、周辺機器とのデータ伝送を行うためのＩ／Ｆ回路であり、本実施の形態では、ＩＣチップＲ／Ｗ３がケーブルを介して接続されている。入力Ｉ／Ｆ１１５は、例えば、図示しないリモートコントローラからの赤外線信号を受信する受信回路や、ユーザが操作するための操作キーなどを具備し、ユーザの入力操作に応じた制御信号をＣＰＵ１０８に対して供給する。

【００４１】

このビデオレコーダ１において、ユーザがデジタル放送の放送コンテンツを視聴する際の基本的な動作は、以下のようになる。ＣＰＵ１０８は、入力Ｉ／Ｆ１１５からの制御信号に基づいて選局情報をデジタルＴＶチューナ１０１に出力する。デジタルＴＶチューナ１０１は、入力された選局情報に応じた搬送周波数の受信信号を選局し、その放送信号に対してＱＰＳＫ復調および誤り訂正処理を施した後、トランスポートストリームからビデオストリーム、オーディオストリーム、データ放送用の付加情報などを分離する。

【００４２】

分離されたビデオストリームおよびオーディオストリームは、暗号処理回路１０２を介してビデオデコーダ１０３およびオーディオデコーダ１０４に供給され、それぞれ伸張復号処理される。復号されたビデオデータは、画像合成処理回路１０５を介してビデオＤＡＣ１０６に供給され、復号されたオーディオデータはオーディオＤＡＣ１０７に供給される。これにより、選局された放送コンテンツが、外部のディスプレイ２などにおいて再生出力される。

【００４３】

なお、スクランブル処理された放送信号を受信する場合には、デジタルＴＶチューナ１０１において、選局された放送信号が復調された後に、デスクランブル処理が行われる。

このとき、例えば可搬型の半導体メモリである図示しないメモリカードに、番組の契約情報やデスクランブル処理のためのキー情報などが書き込まれており、ＣＰＵ１０８はこのメモリカードから契約情報を読み出すとともに、デジタルＴＶチューナ１０１は受信した放送信号中から契約情報を抽出して、ＣＰＵ１０８に供給する。ＣＰＵ１０８は、これらの契約情報を照合して、視聴可能と判断した場合にメモリカードからキー情報を読み取り、デジタルＴＶチューナ１０１に供給する。デジタルＴＶチューナ１０１は、供給されたキー情報を用いてデスクランブル処理を行う。

【００４４】

また、デジタルＴＶチューナ１０１において分離されたデータ放送用の付加情報は、入力Ｉ／Ｆ１１５を通じたユーザからの操作入力に応じて、ＣＰＵ１０８の処理により生成される所定のＯＳＤ画像データとともに画像合成処理回路１０５に供給され、動画像とともに表示される。

【００４５】

なお、ＳＴＢ５を用いた図２のようなシステム構成では、デジタルＴＶチューナ１０１の機能がＳＴＢ５に搭載され、放送により受信したコンテンツが暗号化された状態などとしてビデオレコーダ１に供給される。ビデオレコーダ１では、暗号処理回路１０２により受信したコンテンツを復号し、ビデオデコーダ１０３およびオーディオデコーダ１０４に供給することで、そのコンテンツを再生出力することができる。

【００４６】

次に、このビデオレコーダ１におけるコンテンツの記録・ムーブ動作、および記録媒体上のコンテンツの再生動作について、詳細に説明する。まず、図４は、ビデオレコーダが備えるコンテンツ記録・再生のための機能を示すブロック図である。

【００４７】

図４において、記録再生制御部８１は、例えばＣＰＵ１０８により実行される記録再生制御プログラムとして実現され、このビデオレコーダ１におけるコンテンツの記録（ムーブを含む）・再生動作を統括的に制御する。また、この記録再生制御部８１は、後述するコンテンツの一覧表示画面や案内画面などのＧＵＩ画像の信号を生成して画像合成処理回路１０５に供給し、ＧＵＩ画像をディスプレイ２に表示させる。そして、その表示画像に応じて入力Ｉ／Ｆ１１５を通じて入力された操作入力信号に応じて、記録・再生処理を実行する。

【００４８】

また、暗号処理回路１０２は、暗号処理部２１、鍵生成部２２、および認証処理部２３を備えている。暗号処理部２１は、各種記録媒体へのコンテンツのデータの記録や各コンテンツの再生の際に、鍵生成部２２により生成された、あるいは認証処理部２３を介して供給された鍵情報を用いて、コンテンツのデータを暗号化・復号処理を実行する。ここで、光ディスクドライブ１１３およびＨＤＤ１１２などに対して内部バス１１６を介して入出力されるコンテンツのデータは、必ず暗号処理部２１により暗号化されることで、内部バス１１６を通じたコンテンツの不正コピーが防止される。

【００４９】

鍵生成部２２は、例えば乱数発生機能などを備え、その暗号処理部２１での暗号化処理の際に、発生した乱数を基に暗号鍵を生成して、暗号処理部２１に供給する。また、暗号鍵は、認証処理部２３、通信Ｉ／Ｆ１１４、およびＩＣチップＲ／Ｗ３を介して、光ディスク１０上のＩＣチップ１１に出力することもある。

【００５０】

認証処理部２３は、記録再生制御部８１の要求により、光ディスク１０に搭載されたＩＣチップ１１との間でＩＣチップＲ／Ｗ３を介して通信を行う場合に、ＩＣチップ１１との間の相互認証処理を実行し、通信相手として正当なものであるか否かを判定する。そして、正当なものであると判定した場合に、ＩＣチップＲ／Ｗ３を通じたＩＣチップ１１へのアクセス（データの読み出しおよび書き込み）を許可する。

【００５１】

次に、ＩＣチップ１１とビデオレコーダ１との間の相互認証機能の例について説明する。図５は、相互認証機能を備えたＩＣチップの構成例を示すブロック図である。

図５に示すように、ＩＣチップ１１は、通信回路１３、不揮発性メモリ１４、暗号コア１５、シーケンサ１６、およびレジスタ・Ｉ／Ｆ１７を具備している。また、通信回路１３にはアンテナ１２が接続されている。

【００５２】

通信回路１３は、アンテナ１２を介してＩＣチップＲ／Ｗ３との間でデータを非接触で送受信するための回路であり、送受信データの変復調や通信プロトコルに従ったデータ処理などを行う。また、ＩＣチップＲ／Ｗ３からの電波を受けてアンテナ１２に発生する電力を回路内部に伝送する機能を具備してもよい。不揮発性メモリ１４には、認証用の鍵情報（認証鍵）や、後述するコンテンツの識別情報、コンテンツの記録・再生のための鍵情報、利用制御情報などが格納される。また、暗号コア１５による暗号化のための共通鍵や初期値、乱数発生のための一時的な値なども記憶される。なお、これらの情報のうち必要なものは、書き換えが不可能な状態で記憶されていてもよい。

【００５３】

暗号コア１５は、例えばＤＥＳ（Data Encryption Standard）、ＡＥＳ（Advanced Encryption Standard）といった暗号方式を用いた共通鍵による暗号処理を実行する。暗号コア１５は、不揮発性メモリ１４に記憶されたデータを用いて、トークン（token）と呼ばれる送信権を示すデータや乱数の生成、通信回路１３を介して外部と送受信するデータの暗号化・復号などを行う。シーケンサ１６は、ＩＣチップ１１内の各ブロックを統括的に制御する。また、認証処理時の乱数の一致判定なども行う。レジスタ・Ｉ／Ｆ１７は、暗号コア１５や通信回路１３に処理されるデータを一時的に保持する。

【００５４】

図６は、ＩＣチップとビデオレコーダとの間の相互認証処理シーケンスの例を示す図である。

〔ステップＳ１０１〕ビデオレコーダ１において、記録再生制御部８１から相互認証処理が要求されると、暗号処理回路１０２の認証処理部２３は、ＩＣチップ１１に対して、相互認証処理を開始するためのコマンド“Ｇｅｔ＿ｃｈａｌｌｅｎｇｅ”を送信する。

【００５５】

〔ステップＳ１０２〕コマンドを受信したＩＣチップ１１は、乱数（ここではＲａとする）を生成して、認証処理部２３に送信する。

〔ステップＳ１０３〕乱数Ｒａを受け取った認証処理部２３は、乱数（Ｒｂとする）を生成する。また、このとき一時的な数値として“ｔｅｘｔ１”も生成する。

【００５６】

〔ステップＳ１０４〕認証処理部２３は、生成した乱数Ｒｂおよび“ｔｅｘｔ１”と、ＩＣチップ１１からの乱数Ｒａを結合した値（Ｒｂ｜｜Ｒａ｜｜ｔｅｘｔ１とする）を生成し、この値を共通鍵である認証鍵Ｋｃで暗号化した値をトークン（ｔｏｋｅｎ１とする）として、ＩＣチップ１１に送信する。なお、認証鍵Ｋｃは、ビデオレコーダ１内の例えばＲＯＭ１０９あるいはＥＥＰＲＯＭ１１１などに、あらかじめ格納されている。

【００５７】

〔ステップＳ１０５〕ＩＣチップ１１は、認証処理部２３からの“ｔｏｋｅｎ１”を受け取り、認証鍵Ｋｃで復号して乱数Ｒａを取り出す。

〔ステップＳ１０６〕ＩＣチップ１１は、取り出した乱数と、ステップＳ１０２で生成した乱数とを比較する。

【００５８】

〔ステップＳ１０７〕ステップＳ１０６で、乱数が一致しなかった場合には、認証に失敗したものと判定して、処理を終了する。

〔ステップＳ１０８〕ステップＳ１０６で、乱数が一致した場合には、ＩＣチップ１１側が、認証処理部２３を正しく認証したと判定する。

【００５９】

〔ステップＳ１０９〕ＩＣチップ１１は、一時的な数値として“ｔｅｘｔ２”を生成し、この“ｔｅｘｔ２”と、“ｔｏｋｅｎ１”から取り出した乱数Ｒｂと、乱数Ｒａとを結合した値（Ｒａ｜｜Ｒｂ｜｜ｔｅｘｔ２）を生成し、この値を認証鍵Ｋｃで暗号化し、トークン（ｔｏｋｅｎ２とする）として認証処理部２３に送信する。なお、認証鍵Ｋｃは、ＩＣチップ１１内の不揮発性メモリ１４にあらかじめ格納されている。

【００６０】

〔ステップＳ１１０〕認証処理部２３は、ＩＣチップ１１からの“ｔｏｋｅｎ２”を受け取り、認証鍵Ｋｃで復号して乱数Ｒｂを取り出す。

〔ステップＳ１１１〕取り出した乱数と、ステップＳ１０３で生成した乱数とを比較する。

【００６１】

〔ステップＳ１１２〕ステップＳ１１１で、乱数が一致しなかった場合には、認証に失敗したものと判定して、処理を終了する。

〔ステップＳ１１３〕ステップＳ１１１で、乱数が一致した場合には、認証処理部２３側が、ＩＣチップ１１を正しく認証したと判定する。これにより、相互認証が正しく終了する。

【００６２】

なお、上記のステップＳ１０４では、ＩＣチップ１１に記録された情報を取得する際に、一時的な数値である上記の“ｔｅｘｔ１”“ｔｅｘｔ２”から一時的な共通鍵を生成し、この共通鍵を用いて情報を暗号化して転送してもよい。これにより、ＩＣチップ１１の記録情報をより安全に転送することができる。また、上記では共通鍵方式の認証処理を適用したが、これに限らず、例えば、ＩＣチップ１１内に認証局の公開鍵などを格納しておき、ビデオレコーダ１の認証処理部２３との間で公開鍵方式により相互認証を行うようにしてもよい。

【００６３】

次に、光ディスク１０に記録されるデータの具体例について説明する。図７は、光ディスク（ＲＷディスク）およびそのＩＣチップに記録される情報を示す図である。

図７のように、光ディスク１０のデータ領域に、１つ以上のコンテンツのデータファイル（コンテンツファイル）が記録された場合、この光ディスク１０のＩＣチップ１１には、データ領域に記録された各コンテンツファイルに対応する識別情報（例えばファイル名）と、それぞれに対応する鍵情報（復号鍵）および利用制御情報が記録される。さらに、相互認証処理に必要な情報として、認証鍵Ｋｃも記録される。

【００６４】

光ディスク１０のデータ領域には、コンテンツファイルが暗号化された状態で記録される。また、ＲＷディスクでは、データ領域上のコンテンツファイルが書き換え可能な状態であるため、対応するコンテンツファイルの識別情報も、ＩＣチップ１１内に書き換え可能な状態で記録される。ただし、識別情報の書き換えは、読み出しデバイスとの間で正しく相互認証処理された場合のみ可能で、実際の動作では、識別情報などの書き換えが可能になったとき、コンテンツファイルの書き換えも可能となる。

【００６５】

ＩＣチップ１１内の鍵情報は、不正なツールによりこの鍵情報が読み取られて対応するコンテンツが不正にコピーされることを防止するために、読み出しデバイスとの相互認証処理が正しく実行された場合にのみ、外部からの読み出しが可能となっている。また、データ領域内のコンテンツファイルとの対応づけが維持されている必要があるため、同様に正しく相互認証された場合のみ、書き換えが可能となっている。

【００６６】

利用制御情報は、対応するコンテンツファイルの利用権利を示す情報であり、本実施の形態では、例として利用の可否を示す情報としている。すなわち、利用“可”の状態では、対応するコンテンツの再生およびムーブが可能となり、このコンテンツが他の記録媒体にムーブされると、利用“不可”の状態となって対応するコンテンツの再生が不可能にな

る。なお、利用制御情報としては、再生の可否の他に、例えばコピー（ムーブ）の可否やその回数の制限情報なども記録しておき、再生の可否とは別にコピー（ムーブ）の権利を管理できるようにしてもよい。この利用制御情報は、不正なツールによりその内容が改ざんされ、対応するコンテンツが不正にコピーされることを防止するため、読み出しデバイスとの相互認証処理が正しく実行された場合にのみ、書き換え可能になっている。

【００６７】

なお、識別情報および利用制御情報は、ユーザが容易にその内容を確認できるように、相互認証処理なしで外部からの読み出しが可能となっている。ただし、これらの情報も、正しく相互認証された場合にのみ読み出し可能としてもよい。

【００６８】

認証鍵Ｋｃは、相互認証処理時においてＩＣチップ１１内でのみ利用されるので、外部からの読み出しも書き換えも不可能になっている。

なお、この図７ではＲＷディスクの場合について説明したが、本実施の形態では、ＲＯディスクで提供されたコンテンツについても、ムーブさせることが可能である。その場合、ＲＯディスク上のＩＣチップ１１には、上記と同様の識別情報、鍵情報、利用制御情報、および認証鍵情報が記録されるが、これらのうち、識別情報および鍵情報は書き換え不可能とされる。

【００６９】

次に、上記の各種情報を用いてコンテンツの記録・再生を行う場合の手順について、具体的に説明する。まず、図８は、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。なお、この図８では、参考のために、ユーザの操作手順についても併記している（図９以下に示すフローチャートでも同様）。

【００７０】

〔ステップＳ２０１〕ユーザからの記録処理の開始要求操作が行われる。ビデオレコーダ１では、記録再生制御部８１が、ユーザ操作に応じた記録要求を入力Ｉ／Ｆ１１５を通じて受け付け、記録処理を開始する。例えば、所定のキー操作により記録要求を受け付ける。あるいは、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざし、ビデオレコーダ１で認識されると、記録開始を含む処理の選択画面をディスプレイ２に表示し、ユーザからの選択操作を受けてもよい。その後、記録再生制御部８１は、光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する画面を生成し、ディスプレイ２に表示させる。または、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、以下の記録処理が自動的に開始されてもよい。

【００７１】

〔ステップＳ２０２〕ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。この相互認証処理は、例えば図６で説明した手順により実行される。なお、相互認証処理が正しく実行されなかった場合には、処理を終了する。

【００７２】

なお、ステップＳ２０１において、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざした後、ユーザからの記録開始要求操作を受け付けるようにした場合には、光ディスク１０がＩＣチップＲ／Ｗ３にかざされた時点で相互認証処理をし、正しく認証した場合に記録開始要求操作を受け付けて、次のステップＳ２０３に移行してもよい。

【００７３】

〔ステップＳ２０３〕ステップＳ２０２で相互認証処理が正しく実行された場合には、記録再生制御部８１は、光ディスク１０を光ディスクドライブ１１３にセットするように案内する案内画面を、ディスプレイ２に表示させる。

【００７４】

〔ステップＳ２０４〕ユーザは、光ディスクドライブ１１３に対して光ディスク１０をセットする。このとき、光ディスク１０上のＩＣチップ１１を認証したビデオレコーダ１

では、デジタルＴＶチューナ１０１で受信された放送コンテンツが、ビデオデコーダ１０３およびオーディオデコーダ１０４で伸張復号化され、映像および音声が再生出力される。なお、放送コンテンツは、例えばリモートコントローラなどを用いた局番号の選択操作や、放送信号に多重化されるなどして受信したＥＰＧ（Electronic Program Guide）の情報に基づく選択操作などにより選択される。

【００７５】

なお、ここでは、ＩＣチップ１１の認証後に、放送コンテンツを伸張復号化するようにして、例えば図２の構成のようにデジタルＴＶチューナが外部に接続されている場合などにも対応できる手順としている。具体的には、ＩＣチップ１１の認証後に、入力された暗号化されたコンテンツのデータを、暗号処理回路１０２で復号（またはデスクランブル）し、さらにビデオデコーダ１０３およびオーディオデコーダ１０４で伸張復号化することになる。

【００７６】

しかし、図３の例のように、デジタルＴＶチューナが記録装置と一体化していて、放送コンテンツの視聴権利を装置内で安全に管理できる場合（例えば、図３において、デジタルＴＶチューナ１０１で受信され、暗号処理回路１０２でデスクランブルされた放送コンテンツのデータを、再暗号化しない限り内部バス１１６に出力できないようにしておいた場合）は、例えば、ステップＳ２０１の時点で、放送コンテンツを選局して伸張復号化し、視聴できる状態としておいてもよい。

【００７７】

〔ステップＳ２０５〕ユーザによる記録開始操作が行われると、記録再生制御部８１は、入力Ｉ／Ｆ１１５を通じて記録開始要求を受け付け、暗号処理回路１０２に対して、記録するコンテンツの暗号化処理を開始させる。鍵生成部２２は、例えば乱数などを用いて鍵情報を生成し、暗号処理部２１は、生成された鍵情報を用いて、デジタルＴＶチューナ１０１からのコンテンツのデータを暗号化する。なお、生成した鍵情報は、ＲＡＭ１１０などに一時的に記録しておく。

【００７８】

〔ステップＳ２０６〕記録再生制御部８１は、暗号化されたコンテンツのデータ（コンテンツファイル）を光ディスクドライブ１１３に順次転送し、光ディスク１０に記録させる。

【００７９】

なお、ここではデジタルＴＶチューナ１０１により受信された放送コンテンツを記録しているが、例えば、所定のＩ／Ｆ回路を通じて外部から入力されたコンテンツ（例えばＳＴＢにおいて受信され、出力された放送コンテンツなど）を記録する場合でも、同様の手順で記録が行われる。すなわち、入力されたコンテンツのデータが暗号化され（ステップＳ２０５）、そのコンテンツファイルが光ディスク１０に順次記録される（ステップＳ２０６）。

【００８０】

〔ステップＳ２０７〕ユーザによる記録停止操作が行われると、記録再生制御部８１は、入力Ｉ／Ｆ１１５を通じて記録停止要求を受け付け、光ディスク１０への記録動作を停止させる。そして、光ディスクドライブ１１３に光ディスク１０を排出させるとともに、光ディスク１０をＩＣチップＲ／Ｗ３にかざすようにユーザに案内するための案内画面を生成し、ディスプレイ２に表示させる。

【００８１】

〔ステップＳ２０８〕ユーザが、光ディスクドライブ１１３から取り出した光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で、再び相互認証処理が実行される。なお、相互認証処理が正しく実行されなかった場合には、処理を終了する。

【００８２】

〔ステップＳ２０９〕ステップＳ２０８で相互認証処理が正しく実行された場合には、

記録再生制御部８１は、例えばＥＰＧを用いたコンテンツ選択操作に基づくコンテンツの情報などを基に、記録したコンテンツの識別情報（ファイル名など）を生成する。そして、その識別情報を、ＩＣチップＲ／Ｗ３を介して光ディスク１０上のＩＣチップ１１に送信し、書き込む。

【００８３】

〔ステップＳ２１０〕記録再生制御部８１は、ステップＳ２０５で生成した鍵情報を、上記の識別情報に対応付けてＩＣチップ１１に書き込む。

〔ステップＳ２１１〕記録再生制御部８１は、利用制御情報を生成して、上記の識別情報および鍵情報に対応付けてＩＣチップ１１に書き込む。この利用制御情報は、例えば放送波によりコンテンツとともに伝送されたコピー制御情報や、放送受信に際する条件や規約などに応じて生成される。例えば、記録されるコンテンツが１回のコピーのみ許可する“コピーワンス”とされている場合、利用制御情報として、再生動作と、１回のムーブとが可能であることを示す情報が書き込まれる。

【００８４】

なお、以上のステップＳ２０９～Ｓ２１１の処理は、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３に短時間かざしている間に済むように、一連の処理として実行される。

次に、放送コンテンツを一旦ＨＤＤ１１２に記録した後、光ディスク１０にムーブする場合について説明する。デジタルＴＶチューナ１０１により受信されたコンテンツをＨＤＤ１１２に記録する場合、記録再生制御部８１の制御により、デジタルＴＶチューナ１０１から出力されたコンテンツのデータが暗号処理部２１により暗号化された後、ＨＤＤ１１２に順次記録される。このとき鍵情報は、例えば乱数やＨＤＤ１１２のデバイスＩＤなどを用いて生成され、ＥＥＰＲＯＭ１１１などに記録される。コンテンツを記録したＨＤＤ１１２と別の記録媒体に鍵情報を記録しておくことで、ＨＤＤ１１２内のデータがビットバイビットでコピーされたり、あるいはＨＤＤ１１２が取り外された場合などでも、コンテンツの不正利用を防止できる。また、記録したコンテンツに対応する利用制御情報（ライセンス情報など）は、例えば、鍵情報とともにＥＥＰＲＯＭ１１１などに記録しておくか、あるいは、鍵情報により暗号化した状態でＨＤＤ１１２に記録しておく。

【００８５】

このようにＨＤＤ１１２に記録されたコンテンツは、以下の手順により光ディスク１０にムーブすることができる。図９は、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。

【００８６】

〔ステップＳ３０１〕ビデオレコーダ１では、記録再生制御部８１の制御により、ＨＤＤ１１２のディレクトリ情報などに基づいて、ＨＤＤ１１２内に記録されたコンテンツファイルのファイル名などを一覧表示した表示画面が生成され、この画面がディスプレイ２に表示される。ユーザは、上記の一覧表示画面から所望のコンテンツを選択し、光ディスク１０への記録（ムーブ）を開始させるための入力操作を行う。記録再生制御部８１は、ユーザ操作に応じた選択・記録要求を入力Ｉ／Ｆ１１５から受け付ける。そして、光ディスク１０をＩＣチップＲ／Ｗ３にかざすようにユーザに案内するための案内画面を、ディプレイ２に表示させる。

【００８７】

〔ステップＳ３０２〕ユーザが、光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。なお、正しく認証されなかった場合には、処理が終了される。

【００８８】

なお、図８のステップＳ２０１およびＳ２０２と同様に、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、ステップＳ３０２の相互認証処理に移行して、記録処理が自動的に開始されるようにしてもよい。また、光ディスク１０のＩＣチップ１１の認証処理が実行された後、記録開始の要求操作を行うようにしてもよい。

【００８９】

〔ステップＳ３０３〕ステップＳ３０２で正しく認証された場合には、記録再生制御部８１は、光ディスク１０を光ディスクドライブ１１３にセットするようにユーザに案内するための案内画面を、ディスプレイ２に表示させる。

【００９０】

〔ステップＳ３０４〕ユーザが、光ディスクドライブ１１３に対して光ディスク１０をセットすると、記録再生制御部８１は、ステップＳ３０１で選択されたコンテンツファイルをＨＤＤ１１２から読み出し、暗号処理部２１に復号させる。

【００９１】

〔ステップＳ３０５〕鍵生成部２２は、例えば乱数などを用いて新たな鍵情報を生成し、暗号処理部２１は、生成された鍵情報を用いて、ステップＳ３０４で復号されたコンテンツファイルを再び暗号化する。

【００９２】

〔ステップＳ３０６〕記録再生制御部８１は、暗号化されたコンテンツファイルを光ディスクドライブ１１３に順次転送し、光ディスク１０に記録させる。

〔ステップＳ３０７～Ｓ３１１〕これらのステップでは、図８のステップＳ２０７～Ｓ２１１と同様の処理が実行される。すなわち、光ディスク１０が排出されて、その光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面が表示され（ステップＳ３０７）、ユーザが、光ディスクドライブ１１３から取り出した光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される（ステップＳ３０８）。この相互認証処理が正しく実行された場合には、ＩＣチップ１１に対して、コンテンツの識別情報（ステップＳ３０９）、鍵情報（ステップＳ３１０）、および利用制御情報（ステップＳ３１１）が書き込まれる。

【００９３】

なお、ＩＣチップ１１に書き込む識別情報、鍵情報、利用制御情報は、例えばステップＳ３０１でムーブするコンテンツの選択を受けた時点で生成しておいてもよい。

〔ステップＳ３１２〕ＩＣチップ１１への情報記録が終了すると、記録再生制御部８１は、ＨＤＤ１１２内の元のコンテンツを無効化し、これにより光ディスク１０へのムーブが完了する。

【００９４】

この無効化処理では、例えば、このコンテンツが“コピーワンス”とされている場合には、このコンテンツファイルおよび対応する利用制御情報などの情報をすべて消去する。この場合には、ＨＤＤ１１２の空き容量を増やすことができる。また、コンテンツファイルを消去せず、例えば、ＥＥＰＲＯＭ１１１などに記録してあった対応する利用制御情報（ライセンス情報など）を、再生不可能を示すように書き換えてもよい。あるいは、利用制御情報を書き換えるとともに、鍵情報を消去してもよい。このように、ムーブしたコンテンツファイルを消去しないでおいた場合には、後に同じコンテンツを光ディスク１０からＨＤＤ１１２に再ムーブした場合に、コンテンツファイルを転送する必要がなくなり、短時間で処理できるようになる。

【００９５】

なお、ムーブするコンテンツについて複数回のコピーが許可されていて、例えば利用制御情報にムーブ回数の制限が記録されていた場合には、ムーブ可能な回数を１回分減算して更新する。

【００９６】

次に、上記の図８あるいは図９の手順により光ディスク１０に記録されたコンテンツを、ビデオレコーダ１において再生する場合の手順について説明する。図１０は、光ディスク内のコンテンツを再生する場合のビデオレコーダの処理手順を示すフローチャートである。

【００９７】

〔ステップＳ４０１〕まず、ユーザは、再生したいコンテンツが記録された光ディスク１０をＩＣチップＲ／Ｗ３にかざす。ビデオレコーダ１では、記録再生制御部８１の制御

により、ＩＣチップ１１に記録されたコンテンツファイルの識別情報と、対応する利用制御情報とが、ＩＣチップＲ／Ｗ３により読み出される。記録再生制御部８１は、読み出された情報を受け取ると、識別情報に基づき、光ディスク１０に記録されたコンテンツファイルのファイル名の一覧と、各ファイルに対応する利用制御情報の内容とを示す一覧表示・選択受け付け画面を、ディスプレイ２に表示させる。

【００９８】

〔ステップＳ４０２〕ユーザは、表示された一覧表示画面を参照して、所望のコンテンツが再生可能であるか否かを確認することができる。そして、所望のコンテンツが再生可能である場合に、それに対応するコンテンツファイルを選択する入力操作を行う。記録再生制御部８１は、選択入力を受け付けて、選択されたコンテンツファイルを認識した後、再び光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面を表示する。

【００９９】

〔ステップＳ４０３〕ユーザが、光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。

〔ステップＳ４０４〕ステップＳ４０３で相互認証処理が正しく実行された場合には、記録再生制御部８１は、ＩＣチップ１１から、選択されたコンテンツに対応する鍵情報を読み出し、ＲＡＭ１１０などに一時的に記録する。

【０１００】

〔ステップＳ４０５〕記録再生制御部８１は、光ディスク１０をセットするようにユーザを案内するための案内画面を、ディスプレイ２に表示させる。

〔ステップＳ４０６〕ユーザは、案内画面に従って、光ディスク１０を光ディスクドライブ１１３にセットし、ローディングさせる。記録再生制御部８１は、光ディスクドライブ１１３に対して、光ディスク１０のデータ領域から、選択されたコンテンツファイルの読み出しを実行させる。

【０１０１】

〔ステップＳ４０７〕記録再生制御部８１の制御の下で、暗号処理部２１は、ステップＳ４０４で読み出された鍵情報を用いて、光ディスク１０からのコンテンツファイルを復号する。復号後のコンテンツファイルは、暗号処理回路１０２からビデオデコーダ１０３およびオーディオデコーダ１０４に供給されて伸張復号化され、これによりコンテンツが再生出力される。なお、コンテンツの再生が終了すると、ビデオレコーダ１内の鍵情報は破棄される。

【０１０２】

〔ステップＳ４０８〕記録再生制御部８１は、光ディスクドライブ１１３に光ディスク１０を排出させる。

〔ステップＳ４０９〕ステップＳ４０１で読み出した利用制御情報に、再生したコンテンツに対応する再生回数の制限など、利用に関する制限情報が含まれていた場合には、記録再生制御部８１は、光ディスク１０を再びＩＣチップＲ／Ｗ３にかざすようにユーザに案内するための案内画面を、ディスプレイ２に表示させる。

【０１０３】

〔ステップＳ４１０〕ユーザが、光ディスク１０をＩＣチップＲ／Ｗ３に再びかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。

【０１０４】

〔ステップＳ４１１〕ステップＳ４１０で相互認証処理が正しく実行された場合には、記録再生制御部８１は、ＩＣチップ１１内の対応する利用制御情報を更新する。例えば、再生可能な回数を１だけ減算する。

【０１０５】

なお、実際には、例えば、ステップＳ４０３での相互認証処理後、ステップＳ４０４およびＳ４０５での一連の処理により、ＩＣチップ１１内の対応する利用制御情報を、一時的に再生不能になる、あるいは再生可能回数が減少されるように更新しておき、ステップ

Ｓ４１１で正しい手順が踏まれた場合に、利用制御情報を正しい情報に更新するようにしてもよい。

【０１０６】

なお、以上の図１０で適用した光ディスク１０は、図８あるいは図９の手順によりコンテンツが記録されたものとしたが、例えば他のビデオレコーダなどによりデータ領域にコンテンツが記録されるとともに、図７のような識別情報、鍵情報、利用制御情報などがＩＣチップ１１に記録された光ディスク１０であれば、ＲＷディスク・ＲＯディスクを問わず、同様の手順で再生することができる。

【０１０７】

次に、上記の図８あるいは図９の手順により光ディスク１０に記録されたコンテンツを、ビデオレコーダ１内のＨＤＤ１１２にムーブする場合の手順について説明する。図１１および図１２は、光ディスク内のコンテンツをＨＤＤにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。

【０１０８】

〔ステップＳ５０１〕ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、ビデオレコーダ１では、記録再生制御部８１の制御により、ＩＣチップ１１に記録されたコンテンツファイルの識別情報と、対応する利用制御情報とが、ＩＣチップＲ／Ｗ２により読み出される。記録再生制御部８１は、読み出された情報を受け取ると、識別情報に基づき、光ディスク１０に記録されたコンテンツファイルのファイル名の一覧と、各ファイルに対応する利用制御情報の内容とを示す一覧表示・選択受け付け画面を、ディスプレイ２に表示させる。

【０１０９】

〔ステップＳ５０２〕ユーザは、表示された一覧表示画面を参照して、所望のコンテンツがムーブ可能であるか否かを確認することができる。そして、所望のコンテンツがムーブ可能である場合に、それに対応するコンテンツファイルを選択し、ＨＤＤ１１２への記録（ムーブ）を開始させるための入力操作を行う。記録再生制御部８１は、選択入力・記録要求を受け付けて、選択されたコンテンツファイルを認識した後、再び光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面を表示する。

【０１１０】

〔ステップＳ５０３〕ユーザが、光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。

〔ステップＳ５０４〕ステップＳ５０３で相互認証処理が正しく実行された場合には、記録再生制御部８１は、ＩＣチップ１１から、選択されたコンテンツに対応する鍵情報を読み出し、ＲＡＭ１１０などに一時的に記録する。

【０１１１】

〔ステップＳ５０５〕記録再生制御部８１は、光ディスク１０をセットするようにユーザを案内するための案内画面を、ディスプレイ２に表示させる。

〔ステップＳ５０６〕ユーザは、案内画面に従って、光ディスク１０を光ディスクドライブ１１３にセットし、ローディングさせる。記録再生制御部８１は、光ディスクドライブ１１３に対して、光ディスク１０のデータ領域から、選択されたコンテンツファイルの読み出しを実行させる。

【０１１２】

〔ステップＳ５０７〕記録再生制御部８１の制御の下で、暗号処理部２１は、ステップＳ５０４で読み出された鍵情報を用いて、光ディスク１０からのコンテンツファイルを復号する。

【０１１３】

〔ステップＳ５０８〕鍵生成部２２は、例えば乱数やＨＤＤ１１２のデバイスＩＤなどを用いて新たな鍵情報を生成し、暗号処理部２１は、生成された鍵情報を用いて、ステップＳ５０７で復号されたコンテンツファイルを再び暗号化する。

【０１１４】

〔ステップＳ５０９〕暗号化されたコンテンツファイルは、暗号処理回路１０２からＨＤＤ１１２に対して順次転送され、記録される。

〔ステップＳ５１０〕記録再生制御部８１は、光ディスクドライブ１１３に光ディスク１０を排出させるとともに、光ディスク１０をＩＣチップＲ／Ｗ３に再びかざすようにユーザに案内するための案内画面を生成し、ディスプレイ２に表示させる。

【０１１５】

〔ステップＳ５１１〕ユーザが、光ディスク１０をＩＣチップＲ／Ｗ３に再びかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。

【０１１６】

〔ステップＳ５１２〕ステップＳ５１１で相互認証処理が正しく実行された場合には、記録再生制御部８１は、ＨＤＤ１１２に記録したコンテンツファイルを有効化する、すなわち利用（再生・コピーなど）可能にするための処理を実行する。例えば、記録したコンテンツに対応する、ステップＳ５０８で生成した鍵情報を、装置内部のＥＥＰＲＯＭ１１１などに記録する。また、これとともに、対応する利用制御情報を、暗号処理部２１により上記の鍵情報で暗号化させ、コンテンツファイルに対応付けてＨＤＤ１１２に記録しておく。

【０１１７】

〔ステップＳ５１３〕記録再生制御部８１は、ステップＳ５１１からの一連の処理で、ＩＣチップ１１内の対応する利用制御情報を、利用不可能である、すなわち再生およびコピーが不可能であることを示すように更新し、データ領域内の対応するコンテンツを無効化する。このとき、対応する鍵情報や識別情報を消去してもよい。

【０１１８】

なお、例えば、対応する利用制御情報にコピー回数の制限情報が記述されていた場合には、そのコピー許可回数を１回分減算して更新する。また、更新後のコピー許可回数が０回となったときには、対応するコンテンツが利用不可能（すなわち再生不可能）であることを示す情報を、利用制御情報として書き込むことが望ましい。

【０１１９】

なお、以上の図１１および図１２で適用した光ディスクは、図８あるいは図９の手順によりコンテンツが記録されたものとしたが、例えば他のビデオレコーダなどによりデータ領域にコンテンツが記録されるとともに、図７のような識別情報、鍵情報、利用制御情報などがＩＣチップ１１に記録された光ディスク１０であれば、同様の手順でＨＤＤ１１２にムーブすることが可能である。また、上記手順により、ＲＷディスクに限らず、ＲＯディスクに記録されたコンテンツをＨＤＤ１１２にムーブすることも可能である。

【０１２０】

また、光ディスク１０がＲＷディスクの場合は、コンテンツファイルのＨＤＤ１１２への記録完了後（または、ステップＳ５１３の無効化処理時）に、ムーブしたコンテンツファイルを光ディスク１０のデータ領域から消去してもよい。これにより、光ディスク１０の空き容量を増やし、例えば新たなコンテンツを記録できるようになる。ただし、ムーブしたコンテンツファイルをそのまま光ディスク１０内に残しておくことにより、同じコンテンツを光ディスク１０に再ムーブする際に、コンテンツファイルの転送を行う必要がなくなり、短時間で処理できるようにもなる。

【０１２１】

また、図１１および図１２では、光ディスク１０からＨＤＤ１１２へのムーブ手順について説明したが、例えば、ビデオレコーダ１に接続された携帯型プレーヤなどの他の機器に対して、光ディスク１０上のコンテンツファイルをムーブする場合にも、ほぼ同様の手順を適用できる。この場合、上記のステップＳ５１３の後、鍵生成部２２が例えば乱数やムーブ先機器のデバイスＩＤなどを用いて鍵情報を生成し、暗号処理部２１がその鍵情報を用いてコンテンツファイルを暗号化し、ムーブ先機器にムーブする。

【０１２２】

この場合、例えばムーブ先機器とビデオレコーダ１との間で相互認証できるなど、ムーブ先機器が正当な接続先であることを保証できることが望ましい。また、ムーブ先機器においても、ムーブしたコンテンツに対応する鍵情報が、不正なデバイスからの読み出しが不可能な状態で記録される必要があり、さらに、対応する利用制御情報も、不正なデバイスによる書き換えが不可能な状態で記録される必要がある。また、相互認証処理などによりムーブ先機器が正当な接続先として保証されている場合には、コンテンツファイルや利用制御情報をムーブ先機器において暗号化し、記録するようにしてもよい。

【０１２３】

ここで、図１３は、光ディスク内のコンテンツを選択するための一覧表示画面の表示例を示す図である。

図１３は、ＩＣチップ１１から読み出したコンテンツの識別情報および利用制御情報に基づく一覧表示画面の一例を示している。ここでは例として、コンテンツを選択して再生およびＨＤＤ１１２へのムーブのいずれかを実行できるようになっており、図１０のステップＳ４０１および図１１のステップＳ５０１の両方で共通に表示される画像となっている。

【０１２４】

この一覧表示画面では、光ディスク１０内に記録されたコンテンツファイルに対応するコンテンツ名を示すアイコン２０１～２０３と、各コンテンツに対応する利用制御情報に基づく再生・ムーブの可否を示す情報とが表示される。そして、ユーザの操作入力によりカーソル２０４を移動させることで、再生またはムーブを実行したいコンテンツを選択することができる。また、操作案内部２０５には、再生を行う場合には例えばリモートコントローラなどの再生ボタンを押下し、ＨＤＤ１１２へのムーブを行う場合には録画（ＲＥＣ）ボタンを押下するように案内する画像が示されており、これらのボタンをユーザが押下することで、選択されたコンテンツの再生またはムーブを開始させることが可能となっている。

【０１２５】

また、ユーザは、再生・ムーブの可否を示す情報の表示に基づき、所望のコンテンツの再生またはムーブが不可能である場合には、終了アイコン２０６を選択して処理を終了させることができる。従って、ユーザは、例えば所望のコンテンツの再生やムーブが不可能であるにもかかわらず、そのコンテンツのデータが記録された光ディスク１０をビデオレコーダ１にセットするといった無駄な操作を行うことがなくなる。また、データ領域の記録情報を読み取る前の時点で、単に光ディスク１０の内容を確認できるだけでなく、再生またはムーブを行うコンテンツを選択できるので、操作の混乱をきたすことなく所望のコンテンツの再生またはムーブを確実に実行できるようになり、ユーザの利便性が向上する。

【０１２６】

なお、この一覧表示画面では、再生またはムーブが可能なコンテンツのアイコンのみ表示してもよい。これにより、ユーザは再生またはムーブが可能なコンテンツのみを確実に選択できるようになる。逆に、図１３のように、再生またはムーブが不可能なコンテンツについても表示しておくことで、そのコンテンツを後にＨＤＤ１１２から光ディスク１０にムーブする場合に、コンテンツファイルを転送せず短時間でムーブを完了できることをユーザが認識できる。

【０１２７】

なお、識別情報や利用制御情報は、相互認証なしでＩＣチップ１１から読み出すことができるので、再生やムーブを行う機器（ビデオレコーダ１など）以外の、相互認証機能を持たないＩＣチップＲ／Ｗを備えた機器を用いて、上記各情報を読み取り、光ディスク１０内に記録されたコンテンツとその利用制御情報の内容を表示して、ユーザがその内容を確認することも可能である。

【０１２８】

図１４は、再生・ムーブの処理中における各種案内画面の表示例を示す図である。

図１４（Ａ）は、光ディスクドライブ１１３から排出された光ディスク１０を、ＩＣチップＲ／Ｗ３に対してかざすようにユーザに案内するための画面である。このような案内画面は、例えば、図８のステップＳ２０７、図９のステップＳ３０７において表示される。また、図１４（Ｂ）は、例として“コンテンツＡ”を読み込むために、光ディスク１０を光ディスクドライブ１１３にセットするようにユーザに案内するための画面である。この案内画面は、例えば、図１０のステップＳ４０５、図１１のステップＳ５０５において表示される。以上のような案内画面を表示することにより、ＩＣチップＲ／Ｗ３が光ディスクドライブ１１３の外部に設けられた場合でも、ユーザが混乱なく操作し、再生やムーブの処理を正しく完了させることができるようになる。

【０１２９】

以上説明したように、記録再生制御部８１の制御により、上記の図８～図１２の手順でコンテンツの記録、再生、ムーブを実行することにより、コンテンツの不正利用を確実に防止しながらも、光ディスク１０やＨＤＤ１１２へのコンテンツの記録、それらのコンテンツの再生に加えて、ＨＤＤ１１２と光ディスク１０との間の双方向のムーブや、光ディスク１０から他の機器へのムーブを実行できるようになり、さらに、それらの処理を、ユーザの混乱を招くことなく、簡単な操作で実行できるようになる。

【０１３０】

すなわち、光ディスク１０のデータ領域にコンテンツファイルを暗号化して記録しておくとともに、複製が非常に困難なＩＣチップ１１を光ディスク１０に搭載し、コンテンツファイルの復号に必要な鍵情報を、相互認証後にのみ読み出し可能な状態でＩＣチップ１１に記録しておくことにより、正当なデバイス（ビデオレコーダやビデオプレーヤ、光ディスクドライブなど）においてのみコンテンツの利用（再生およびムーブ）が可能となり、例えばデータ領域のデータをビットバイビットで他の記録媒体にコピーされた場合に、そのデータを不正に利用することができなくなる。また、相互認証後にのみ書き換え可能な利用制御情報をＩＣチップ１１に記録しておき、ムーブ後や再生後に利用制御情報を更新することで、コンテンツの利用権利を安全な状態で管理することができる。従って、特に光ディスク１０内のコンテンツのムーブを可能としながらも、それらのコンテンツの著作権を確実に保護し、またその利用権利を確実に管理することが可能になる。

【０１３１】

また、光ディスク１０へのコンテンツの記録の際には、光ディスク１０を光ディスクドライブ１１３にセットし、データの記録を実行した後に、排出された光ディスク１０のＩＣチップ１１に必要な情報を記録する手順とし、また、光ディスク１０内のコンテンツの利用（すなわち再生およびムーブ）の際には、ＩＣチップ１１への情報アクセスを行った後、光ディスク１０を光ディスクドライブ１１３にセットしてデータを読み出す手順として、いずれの場合にも、光ディスク１０の取り扱い手順に統一性を持たせ、単純にしている。さらに、光ディスク１０内のコンテンツの利用の際には、光ディスク１０の装填前に利用可能なコンテンツをユーザが選択可能としている。そして、ＩＣチップ１１への情報アクセスや、光ディスク１０のセットが必要な際に、そのための操作をユーザに案内する画面を順次表示している。これらの手順により、上記構成のようにＩＣチップＲ／Ｗ３が光ディスクドライブ１１３の外部に設けられた場合を含めた様々な構成のシステムにおいて、ユーザが混乱なく操作し、コンテンツの記録、再生、ムーブの処理を正しく完了させることができるようになる。

【０１３２】

また、光ディスク１０内のデータ領域には、暗号化されたコンテンツファイルのみが単に記録されるだけで、上記の手順を実現するためのプログラムなどは特に記録されず、ビデオレコーダ１側の機能だけで上記のようなユーザの利便性を高めたシステムを提供できる。このため、コンテンツ提供者側の開発費や製造コストなどの負担を小さくでき、またデータ領域への記録フォーマットなどを特に変えることなく、さらにデータ領域内の余分な記憶領域を使用することなく、上記のようにコンテンツの著作権保護とユーザの利便性向上とを両立することができる。

【０１３３】
次に、第２および第３の実施の形態として、上記の第１の実施の形態とは異なる手順により、コンテンツの記録や再生、ムーブなどが行われる場合について説明する。なお、以下の第２および第３の実施の形態で用いられる光ディスク１０には、第１の実施の形態と同様に、ともに図７に示すような情報が記録されるものとする。
【０１３４】
《第２の実施の形態》
図１５は、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。
【０１３５】
〔ステップＳ６０１〕ユーザは、光ディスクドライブ１１３に対して光ディスク１０をセットし、コンテンツの光ディスク１０に対する記録開始操作を行う。ビデオレコーダ１では、記録再生制御部８１が、ユーザ操作に応じた記録開始要求を入力Ｉ／Ｆ１１５から受け付ける。また、ビデオレコーダ１では、ユーザの選局に応じてデジタルＴＶチューナ１０１で受信された放送コンテンツが、ビデオデコーダ１０３およびオーディオデコーダ１０４で伸張復号化され、映像および音声が再生出力される。
【０１３６】
〔ステップＳ６０２～Ｓ６０８〕これらのステップは、図８に示したステップＳ２０５～Ｓ２１１にそれぞれ対応する。すなわち、ビデオレコーダ１では、鍵生成部２２が鍵情報を生成し、暗号処理部２１が、その鍵情報を用いて、デジタルＴＶチューナ１０１からのコンテンツのデータを暗号化する（ステップＳ６０２）。暗号化されたコンテンツのデータは、光ディスク１０に順次記録され（ステップＳ６０３）、記録が停止されると、光ディスク１０が排出されるとともに、その光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面が表示される（ステップＳ６０４）。
【０１３７】
ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、ＩＣチップ１１と認証処理部２３との間で相互認証処理が実行され（ステップＳ６０５）、正しく実行されると、記録再生制御部８１は、光ディスク１０に記録したコンテンツの識別情報を生成して、ＩＣチップ１１に書き込み（ステップＳ６０６）、さらに、そのコンテンツの鍵情報をＩＣチップ１１に書き込み（ステップＳ６０７）、さらに、そのコンテンツの利用制御情報を生成して、識別情報および鍵情報に対応付けてＩＣチップ１１に書き込む（ステップＳ６０８）。
【０１３８】
次に、図１６は、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。
〔ステップＳ７０１〕ビデオレコーダ１では、ＨＤＤ１１２内に記録されたコンテンツファイルのファイル名などを一覧表示した表示画面が、ディスプレイ２に表示され、ユーザは、光ディスク１０を光ディスクドライブ１１３に対してセットし、上記の一覧表示画面から所望のコンテンツを選択して、光ディスク１０への記録（ムーブ）を開始させるための入力操作を行う。記録再生制御部８１は、ユーザ操作に応じた選択・記録要求を入力Ｉ／Ｆ１１５から受け付ける。
【０１３９】
〔ステップＳ７０２～Ｓ７１０〕これらのステップは、図９に示したステップＳ３０４～Ｓ３１２にそれぞれ対応する。すなわち、ステップＳ７０１で選択されたコンテンツファイルがＨＤＤ１１２から読み出されて、暗号処理部２１に復号され（ステップＳ７０２）、鍵生成部２２で新たな鍵情報が生成されて、その鍵情報を用いてコンテンツファイルが再び暗号化されて（ステップＳ７０３）、光ディスク１０に記録される（ステップＳ７０４）。記録が終了すると、光ディスク１０が排出されて、その光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面が表示され（ステップＳ７０５）、ユーザが、光ディスクドライブ１１３から取り出した光ディスク１０をＩＣチップＲ／Ｗ３にか

ざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される（ステップＳ７０６）。この相互認証処理が正しく実行された場合には、ＩＣチップ１１に対して、コンテンツの識別情報（ステップＳ７０７）、鍵情報（ステップＳ７０８）、および利用制御情報（ステップＳ７０９）が書き込まれ、最後に、ＨＤＤ１１２内の元のコンテンツが無効化される（ステップＳ７１０）。

【０１４０】

次に、上記の図１５あるいは図１６の手順により光ディスク１０に記録されたコンテンツを、ビデオレコーダ１において再生する場合の手順について説明する。図１７は、光ディスク内のコンテンツを再生する場合のビデオレコーダの処理手順を示すフローチャートである。

【０１４１】

〔ステップＳ８０１〕ユーザが、再生したいコンテンツが記録された光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、ビデオレコーダ１では、記録再生制御部８１の制御により、ＩＣチップ１１に記録されたコンテンツファイルの識別情報と、対応する利用制御情報とが、ＩＣチップＲ／Ｗ３により読み出される。記録再生制御部８１は、読み出された識別情報に基づき、光ディスク１０に記録されたコンテンツファイルのファイル名の一覧と、各ファイルに対応する利用制御情報の内容とを示す一覧表示・選択受け付け画面を、ディスプレイ２に表示させる。

【０１４２】

〔ステップＳ８０２〕ユーザは、表示された一覧表示画面を参照して、所望のコンテンツが再生可能であるか否かを確認することができる。そして、所望のコンテンツが再生可能である場合に、それに対応するコンテンツファイルを選択する入力操作を行う。記録再生制御部８１は、選択入力を受け付けて、選択されたコンテンツファイルを認識した後、再び光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面を表示する。

【０１４３】

〔ステップＳ８０３〕ユーザが、光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。

〔ステップＳ８０４〕ステップＳ８０３で相互認証処理が正しく実行された場合には、記録再生制御部８１は、ＩＣチップ１１から、選択されたコンテンツに対応する鍵情報を読み出し、ＲＡＭ１１０などに一時的に記録する。

【０１４４】

〔ステップＳ８０５〕ＩＣチップ１１内の利用制御情報に、選択されたコンテンツに対応する再生回数の制限など、利用に関する制限情報が含まれている場合には、記録再生制御部８１は、ステップＳ８０４からの一連の処理により、その制限情報を更新する。

【０１４５】

〔ステップＳ８０６〕記録再生制御部８１は、光ディスク１０をセットするようにユーザを案内するための案内画面を、ディスプレイ２に表示させる。

〔ステップＳ８０７〕ユーザは、案内画面に従って、光ディスク１０を光ディスクドライブ１１３にセットし、ローディングさせる。記録再生制御部８１は、光ディスクドライブ１１３に対して、光ディスク１０のデータ領域から、選択されたコンテンツファイルの読み出しを実行させる。

【０１４６】

〔ステップＳ８０８〕記録再生制御部８１の制御の下で、暗号処理部２１は、ステップＳ８０４で読み出された鍵情報を用いて、光ディスク１０からのコンテンツファイルを復号する。復号後のコンテンツファイルは、暗号処理回路１０２からビデオデコーダ１０３およびオーディオデコーダ１０４に供給されて伸張復号化され、これによりコンテンツが再生出力される。なお、コンテンツの再生が終了すると、ビデオレコーダ１内の鍵情報は破棄される。

【０１４７】

次に、上記の図１５あるいは図１６の手順により光ディスク１０に記録されたコンテン

ツを、ビデオレコーダ１内のＨＤＤ１１２にムーブする場合の手順について説明する。図１８は、光ディスク内のコンテンツをＨＤＤにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。

【０１４８】

〔ステップＳ９０１～Ｓ９０４〕これらのステップは、図１１のステップＳ５０１～Ｓ５０４にそれぞれ対応する。すなわち、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、ＩＣチップ１１に記録されたコンテンツファイルの識別情報と、対応する利用制御情報とが、ビデオレコーダ１のＩＣチップＲ／Ｗ２により読み出され、それら情報を基に、光ディスク１０に記録されたコンテンツファイルのファイル名の一覧と、各ファイルに対応する利用制御情報の内容とを示す一覧表示・選択受け付け画面が、ディスプレイ２に表示される（ステップＳ９０１）。

【０１４９】

一覧表示画面を見たユーザが、ムーブ可能なコンテンツを選択し、記録（ムーブ）を開始させる操作を行うと、ディスプレイ２には、再び光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面が表示される（ステップＳ９０２）。ユーザが、光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行され（ステップＳ９０３）、相互認証処理が正しく実行された場合には、ＩＣチップ１１から、選択されたコンテンツに対応する鍵情報がビデオレコーダ１に読み出される（ステップＳ９０４）。

【０１５０】

〔ステップＳ９０５〕記録再生制御部８１は、ステップＳ９０３からの一連の処理として、さらに、ＩＣチップ１１内の対応する利用制御情報を、利用不可能である、すなわち再生およびコピーが不可能であることを示すように更新し、データ領域内の対応するコンテンツを無効化する。また、利用制御情報にコピー回数の制限情報が記述されていた場合には、そのコピー許可回数を１回分減算して更新する。

【０１５１】

〔ステップＳ９０６～Ｓ９１０〕これらのステップは、図１１のステップＳ５０５～Ｓ５０９にそれぞれ対応する。すなわち、光ディスク１０をセットするようにユーザを案内するための案内画面が、ディスプレイ２に表示され（ステップＳ９０６）、ユーザが光ディスク１０を光ディスクドライブ１１３にセットし、ローディングさせると、ビデオレコーダ１では、その光ディスク１０のデータ領域から、選択されたコンテンツファイルが読み出される（ステップＳ９０７）。

【０１５２】

読み出されたコンテンツファイルは、暗号処理部２１により、ステップＳ９０４で読み出された鍵情報を用いて復号され（ステップＳ９０８）、さらに、新たに生成された鍵情報を用いて、再び暗号化される（ステップＳ９０９）。そして、再暗号化されたコンテンツファイルがＨＤＤ１１２に順次記録される。これとともに、そのコンテンツに対応する鍵情報が、ビデオレコーダ１内のＥＥＰＲＯＭ１１１などに記録され、さらに、対応する利用制御情報が、暗号処理部２１により上記の鍵情報で暗号化された後、コンテンツファイルに対応付けてＨＤＤ１１２に記録されることで、ＨＤＤ１１２に記録されたコンテンツファイルが有効化される（ステップＳ９１０）。

【０１５３】

以上の図１５～図１８の手順により、コンテンツの記録、再生、ムーブが実行されることで、第１の実施の形態と同様に、コンテンツの不正利用を確実に防止しながらも、光ディスク１０やＨＤＤ１１２へのコンテンツの記録、それらのコンテンツの再生に加えて、ＨＤＤ１１２と光ディスク１０との間の双方向のムーブや、光ディスク１０から他の機器へのムーブを実行できるようになり、さらに、それらの処理を、ユーザの混乱を招くことなく、簡単な操作で実行できるようになる。

【０１５４】

特に、第２の実施の形態では、光ディスク１０への記録の際には、光ディスク１０を光

ディスクドライブ１１３にセットし、その後に光ディスク１０をＩＣチップＲ／Ｗ３にかざせばよく、その後に再び光ディスク１０をセットすることのないようにしている。また、光ディスク１０内のコンテンツの利用（再生およびムーブ）時には、光ディスク１０をＩＣチップＲ／Ｗ３にかざし、その後に光ディスク１０をセットすればよく、その後に再び光ディスク１０を取り出してＩＣチップＲ／Ｗ３にかざすことのないようにしている。これにより、第１の実施の形態の場合より、ユーザの操作がさらに簡略化される。

【０１５５】

また、第１の実施の形態と同様に、光ディスク１０内のコンテンツの利用の際には、光ディスク１０の装填前に利用可能なコンテンツをユーザが選択可能とし、ＩＣチップ１１への情報アクセスや、光ディスク１０のセットが必要な際には、そのための操作をユーザに案内する画面を順次表示しているため、ユーザが混乱なく、正しい操作をできるようになっている。

【０１５６】

《第３の実施の形態》

上記の第２の実施の形態では、コンテンツを光ディスク１０に記録する際に、光ディスク１０をビデオレコーダ１にセットした後、その光ディスク１０を取り出して、ＩＣチップＲ／Ｗ３にかざす手順としていた。これに対して、以下の第３の実施の形態では、光ディスク１０をＩＣチップＲ／Ｗ３にかざした後に、その光ディスク１０をビデオレコーダ１にセットする手順とし、その後に再び光ディスク１０をＩＣチップＲ／Ｗ３にかざすことのないようにして、ユーザの操作を簡略化する。

【０１５７】

図１９は、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。

〔ステップＳ１００１〕図８のステップＳ２０１と同様に、ユーザからの記録処理の開始要求操作が行われる。ビデオレコーダ１では、記録再生制御部８１が、ユーザ操作に応じた記録要求を入力Ｉ／Ｆ１１５を通じて受け付ける。また、光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面が、ディスプレイ２に表示される。

【０１５８】

〔ステップＳ１００２〕ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。なお、相互認証処理が正しく実行されなかった場合には、処理を終了する。

【０１５９】

〔ステップＳ１００３〕鍵生成部２２は、例えば乱数などを用いて鍵情報を生成する。

〔ステップＳ１００４～Ｓ１００６〕これらのステップでは、図８のステップＳ２０９～Ｓ２１１と同様の処理が実行される。すなわち、ＩＣチップ１１に対して、コンテンツの識別情報（ステップＳ１００４）、鍵情報（ステップＳ１００５）、および利用制御情報（ステップＳ１００６）が書き込まれる。なお、以上のステップＳ１００２～Ｓ１００６の処理は、光ディスク１０がＩＣチップＲ／Ｗ３にかざされている間に、一連の処理として実行される。

【０１６０】

〔ステップＳ１００７〕記録再生制御部８１は、光ディスク１０を光ディスクドライブ１１３にセットするように案内する案内画面を、ディスプレイ２に表示させる。ユーザは、この案内画面を確認して、光ディスクドライブ１１３に対して光ディスク１０をセットする。

【０１６１】

〔ステップＳ１００８〕ビデオレコーダ１では、デジタルＴＶチューナ１０１で受信された放送コンテンツが、ビデオデコーダ１０３およびオーディオデコーダ１０４で伸張復号化され、映像および音声が再生出力される。

【０１６２】

〔ステップＳ１００９〕記録再生制御部８１の要求に応じて、暗号処理回路１０２は、

ステップＳ１００３で生成した鍵情報を用いて、放送コンテンツを暗号化する。
〔ステップＳ１０１０〕記録再生制御部８１は、暗号化されたコンテンツファイルを光ディスクドライブ１１３に順次転送し、光ディスク１０に記録させる。
【０１６３】
図２０は、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。
〔ステップＳ１１０１〕図９のステップＳ３０１と同様に、ビデオレコーダ１では、ＨＤＤ１１２内に記録されたコンテンツファイルのファイル名などを一覧表示した表示画面が、ディスプレイ２に表示され、ユーザは、光ディスク１０を光ディスクドライブ１１３に対してセットし、上記の一覧表示画面から所望のコンテンツを選択して、光ディスク１０への記録（ムーブ）を開始させるための入力操作を行う。記録再生制御部８１は、ユーザ操作に応じた選択・記録要求を入力Ｉ／Ｆ１１５から受け付ける。また、光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面を、ディスプレイ２に表示させる。
【０１６４】
〔ステップＳ１１０２〕ユーザが、光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される。なお、正しく認証されなかった場合には、処理が終了される。
【０１６５】
〔ステップＳ１１０３〕鍵生成部２２は、例えば乱数などを用いて鍵情報を生成する。
〔ステップＳ１１０４～Ｓ１１０６〕これらのステップでは、図９のステップＳ３０９～Ｓ３１１と同様の処理が実行される。すなわち、ＩＣチップ１１に対して、コンテンツの識別情報（ステップＳ１１０４）、鍵情報（ステップＳ１１０５）、および利用制御情報（ステップＳ１１０６）が書き込まれる。なお、以上のステップＳ１１０２～Ｓ１１０６の処理は、光ディスク１０がＩＣチップＲ／Ｗ３にかざされている間に、一連の処理として実行される。
【０１６６】
〔ステップＳ１１０７〕記録再生制御部８１は、光ディスク１０を光ディスクドライブ１１３にセットするように案内する案内画面を、ディスプレイ２に表示させる。ユーザは、この案内画面を確認して、光ディスクドライブ１１３に対して光ディスク１０をセットする。
【０１６７】
〔ステップＳ１１０８〕記録再生制御部８１は、ステップＳ１１０１で選択されたコンテンツファイルをＨＤＤ１１２から読み出し、暗号処理部２１に復号させる。
〔ステップＳ１１０９〕暗号処理部２１は、ステップＳ１１０３で生成された鍵情報を用いて、ステップＳ１１０８で復号されたコンテンツファイルを再び暗号化する。
【０１６８】
〔ステップＳ１１１０〕記録再生制御部８１は、暗号化されたコンテンツファイルを光ディスクドライブ１１３に順次転送し、光ディスク１０に記録させる。
〔ステップＳ１１１１〕コンテンツファイルの記録が終了すると、記録再生制御部８１は、ＨＤＤ１１２内の元のコンテンツを無効化し、これにより光ディスク１０へのムーブが完了する。
【０１６９】
なお、以上の図１９および図２０の手順で光ディスク１０に記録されたコンテンツの再生は、上記の図１７の手順で行われればよく、そのコンテンツのＨＤＤ１１２へのムーブは、上記の図１８の手順で行われればよい。
【０１７０】
《第４の実施の形態》
図２１は、本発明の第４の実施の形態に用いられる光ディスクおよびそのＩＣチップに記録される情報を示す図である。なお、ここでは例として、ＲＷディスクの場合について

示しているが、記録される情報はＲＯディスクでも同じである。

【０１７１】

本実施の形態では、光ディスク１０のデータ領域に、暗号化したコンテンツファイルとともに、このコンテンツファイルを復号するのに必要な鍵情報を、ディスクごとに固有なディスク鍵Ｋｍにより暗号化した状態で記録しておく。また、ディスク鍵ＫｍをＩＣチップ１１内に記録しておき、コンテンツの利用時に、データ領域内の鍵情報を復号するために読み出して用いるようにする。ディスク鍵Ｋｍは、相互認証処理が正しく実行された場合にのみ読み出し可能で、書き換えは不可とされる。

【０１７２】

コンテンツを光ディスク１０に記録する際には、まず、ＩＣチップ１１との相互認証を行ってディスク鍵を読み出した後、光ディスク１０を光ディスクドライブ１１３にセットし、暗号化したコンテンツのデータとともに、その復号のための鍵情報をディスク鍵Ｋｍで暗号化した情報を、光ディスク１０のデータ領域に記録する。その後、光ディスク１０を排出して、対応する識別情報および利用制御情報をＩＣチップ１１に書き込む。

【０１７３】

この実施の形態では、上記の第１の実施の形態と比較すると、データ領域に複数のコンテンツファイルを記録した場合に、ファイルごとの鍵情報をＩＣチップ１１に記録しておく必要がなく、１つのディスク鍵Ｋｍのみ記録しておけばよくなる。このため、ＩＣチップ１１に必要な記憶容量を小さくし、その製造コストを低減することができる。あるいは、ＩＣチップ１１内に、コンテンツのメタデータなど、コンテンツに関する他の情報をさらに記録することが可能となり、コンテンツの再生やムーブの処理開始時にそれらの情報を表示することなどができるようになる。

【０１７４】

ただし、上述したように、コンテンツを光ディスク１０に記録する際には、光ディスク１０を光ディスクドライブ１１３にセットする前と後で、相互認証処理を伴うＩＣチップ１１へのアクセスが必要となる。従って、ＩＣチップ１１へのアクセスや光ディスク１０のセットが必要な際には、その都度、ユーザに対する案内画面をディスプレイ２に表示することで、ユーザが混乱することなく、コンテンツの記録を実行できるようになる。

【０１７５】

以下、図２１のような情報が記録された光ディスクを用いた場合のコンテンツの記録・再生などの処理手順を、具体的に説明する。まず、図２２は、第４の実施の形態に係るビデオレコーダにおいて、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。

【０１７６】

〔ステップＳ１２０１，Ｓ１２０２〕これらのステップでは、図８のステップＳ２０１およびＳ２０２と同様の処理が実行される。すなわち、ユーザからの記録処理の開始要求操作に応じて、記録処理が開始され（ステップＳ１２０１）、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される（ステップＳ１２０２）。なお、図８の場合と同様に、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、ステップＳ１２０２の相互認証処理に移行して、記録処理が自動的に開始されるようにしてもよい。また、光ディスク１０のＩＣチップ１１の認証処理が実行された後、記録開始の要求操作を行うようにしてもよい。

【０１７７】

〔ステップＳ１２０３〕相互認証処理が正しく実行された場合、記録再生制御部８１は、ＩＣチップＲ／Ｗ３を介して、ＩＣチップ１１からディスク鍵Ｋｍを読み出す。

〔ステップＳ１２０４～Ｓ１２０６〕これらのステップでは、図８のステップＳ２０３～Ｓ２０５と同様の処理が実行される。すなわち、光ディスク１０をセットするように案内する案内画面がディスプレイ２に表示され（ステップＳ１２０４）、ユーザにより光ディスク１０がビデオレコーダ１にセットされる。このとき、受信した放送コンテンツのデ

ータが伸張復号化されて出力されるとともに（ステップＳ１２０５）、生成された鍵情報によりコンテンツのデータが暗号化される（ステップＳ１２０６）。

【０１７８】

〔ステップＳ１２０７〕暗号処理回路１０２は、ステップＳ１２０６で生成された鍵情報を、ディスク鍵Ｋｍで暗号化する。

〔ステップＳ１２０８〕記録再生制御部８１は、ステップＳ１２０６で暗号化されたコンテンツファイルと、ステップＳ１２０７で暗号化された鍵情報とを、光ディスクドライブ１１３に順次転送し、光ディスク１０に記録させる。

【０１７９】

〔ステップＳ１２０９～Ｓ１２１２〕ステップＳ１２０９～Ｓ１２１１は、図８のステップＳ２０７～Ｓ２０９に対応し、ステップＳ１２１２は、図８のステップＳ２１１に対応する。すなわち、ビデオレコーダ１から光ディスク１０が排出されるとともに、その光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面がディスプレイ２に表示され（ステップＳ１２０９）、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、相互認証処理（ステップＳ１２１０）の後、記録されたコンテンツに対応する識別情報（ステップＳ１２１１）および利用制御情報（ステップＳ１２１２）が、ＩＣチップ１１に書き込まれる。

【０１８０】

図２３および図２４は、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。

〔ステップＳ１３０１，Ｓ１３０２〕これらのステップでは、図９のステップＳ３０１およびＳ３０２と同様の処理が実行され、ユーザによるコンテンツの選択入力および記録要求が行われた後（ステップＳ１３０１）、ＩＣチップ１１の認証処理が実行される（ステップＳ１３０２）。

【０１８１】

〔ステップＳ１３０３〕ステップＳ１３０２での相互認証処理が正しく実行された場合、記録再生制御部８１は、ＩＣチップＲ／Ｗ３を介して、ＩＣチップ１１からディスク鍵Ｋｍを読み出す。

【０１８２】

〔ステップＳ１３０４～Ｓ１３０６〕これらのステップでは、図９のステップＳ３０３～Ｓ３０５と同様の処理が実行される。すなわち、案内画面の表示（ステップＳ１３０４）に従って、ユーザにより光ディスク１０がビデオレコーダ１にセットされ、ＨＤＤ１１２のコンテンツファイルが復号されて（ステップＳ１３０５）、さらに鍵情報により再暗号化される（ステップＳ１３０６）。

【０１８３】

〔ステップＳ１３０７〕暗号処理回路１０２は、ステップＳ１３０６で生成された鍵情報を、ディスク鍵Ｋｍで暗号化する。

〔ステップＳ１３０８〕記録再生制御部８１は、ステップＳ１３０６で暗号化されたコンテンツファイルと、ステップＳ１３０７で暗号化された鍵情報とを、光ディスクドライブ１１３に順次転送し、光ディスク１０に記録させる。

【０１８４】

〔ステップＳ１３０９～Ｓ１３１３〕ステップＳ１３０９～Ｓ１３１１は、図９のステップＳ３０７～Ｓ３０９に対応し、ステップＳ１３１２およびＳ１３１３は、図９のステップＳ３１１およびＳ３１２に対応する。これらのステップにより、ＩＣチップ１１に対して、コンテンツに対応する識別情報と利用制御情報とが記録されるとともに、ＨＤＤ１１２内の元のコンテンツファイルが無効化される。

【０１８５】

図２５および図２６は、上記の手順により光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャートである。

〔ステップＳ１４０１～Ｓ１４０３〕これらのステップでは、図１１のステップＳ５０

１～Ｓ５０３と同様の処理が実行される。すなわち、ＩＣチップ１１内の識別情報および利用制御情報に基づくコンテンツの一覧表示（ステップＳ１４０１）に応じて、記録するコンテンツがユーザにより選択された後（ステップＳ１４０２）、再びＩＣチップ１１がＩＣチップＲ／Ｗ３に認識されて、相互認証処理が実行される（ステップＳ１４０３）。

【０１８６】

〔ステップＳ１４０４〕ステップＳ１４０３での相互認証処理が正しく実行された場合、記録再生制御部８１は、ＩＣチップＲ／Ｗ３を介して、ＩＣチップ１１からディスク鍵Ｋｍを読み出す。

【０１８７】

〔ステップＳ１４０５〕記録再生制御部８１は、光ディスク１０を光ディスクドライブ１１３にセットするように案内する案内画面を、ディスプレイ２に表示させる。

〔ステップＳ１４０６〕光ディスクドライブ１１３に対して光ディスク１０がセットされると、記録再生制御部８１は、ステップＳ１４０２で選択された暗号化されたコンテンツファイルと、これに対応する暗号化された鍵情報とを、光ディスクドライブ１１３を通じて光ディスク１０から読み出す。

【０１８８】

〔ステップＳ１４０７〕暗号処理部２１は、ステップＳ１４０６で読み出した鍵情報を、ステップＳ１４０４で読み出したディスク鍵Ｋｍで復号する。

〔ステップＳ１４０８〕暗号処理部２１は、ステップＳ１４０６で読み出したコンテンツファイルを、ステップＳ１４０７で復号した鍵情報で復号する。

【０１８９】

〔ステップＳ１４０９～Ｓ１４１４〕これらのステップでは、図１１のステップＳ５０８～Ｓ５１３と同様の処理が実行される。すなわち、コンテンツファイルが再暗号化されて（ステップＳ１４０９）ＨＤＤ１１２に記録された後（ステップＳ１４１０）、案内画面が表示される（ステップＳ１４１１）。そして、ＩＣチップ１１の相互認証処理の実行後に（ステップＳ１４１２）、ＨＤＤ１１２に記録されたコンテンツファイルの有効化（ステップＳ１４１３）と、光ディスク１０内の元のコンテンツファイルの無効化（ステップＳ１４１４）とが実行される。

【０１９０】

以上の手順により、上記各実施の形態と同様に、コンテンツの利用権利を安全に管理しながら、光ディスク１０内のコンテンツをＨＤＤ１１２などにムーブ（またはコピー）することが可能になる。なお、光ディスク１０内のコンテンツを再生する場合には、ＩＣチップ１１からディスク鍵Ｋｍを読み出した後（ステップＳ１４０４）、光ディスク１０のデータ領域から暗号化されたコンテンツファイルおよび鍵情報を読み出し（ステップＳ１４０６）、鍵情報をディスク鍵Ｋｍで復号した後（ステップＳ１４０７）、その鍵情報を用いてコンテンツファイルを復号し、再生すればよい。

【０１９１】

《第５の実施の形態》

以下の第５の実施の形態では、上記の図２１のような情報が記録された光ディスク１０を利用した場合の他の処理手順について説明する。この実施の形態では、光ディスク１０をＩＣチップＲ／Ｗ３にかざした後に、その光ディスク１０をビデオレコーダ１にセットする手順とし、その後に再び光ディスク１０をＩＣチップＲ／Ｗ３にかざすことのないようにして、第４の実施の形態と比較して、ユーザの操作をより簡略化する。

【０１９２】

図２７は、第５の実施の形態に係るビデオレコーダにおいて、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。

【０１９３】

〔ステップＳ１５０１～Ｓ１５０３〕これらのステップでは、図２２のステップＳ１２０１～Ｓ１２０３と同様の処理が実行される。すなわち、ユーザからの記録処理の開始要

求操作に応じて、記録処理が開始され（ステップＳ１５０１）、光ディスク１０上のＩＣチップ１１の相互認証処理が実行された後（ステップＳ１５０２）、ＩＣチップ１１からディスク鍵Ｋｍがビデオレコーダ１に読み出される（ステップＳ１５０３）。

【０１９４】

〔ステップＳ１５０４，Ｓ１５０５〕これらのステップは、図２２のステップＳ１２１１およびＳ１２１２に対応し、記録するコンテンツの識別情報と利用制御情報とが、ＩＣチップ１１に書き込まれる。なお、以上のステップＳ１５０３～Ｓ１５０５の処理は、光ディスク１０がＩＣチップＲ／Ｗ３にかざされている間に、一連の処理として実行される。

【０１９５】

〔ステップＳ１５０６～Ｓ１５１０〕これらのステップでは、図２２のステップ１２０４～Ｓ１２０８と同様の処理が実行される。これにより、鍵情報で暗号化されたコンテンツファイルと、ディスク鍵Ｋｍで暗号化された鍵情報とが、光ディスク１０のデータ領域に記録される。

【０１９６】

図２８は、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。

〔ステップＳ１６０１～Ｓ１６０３〕これらのステップでは、図２３のステップＳ１３０１～Ｓ１３０３に対応する処理が実行される。すなわち、ユーザによるコンテンツの選択入力および記録要求が行われた後（ステップＳ１６０１）、ＩＣチップ１１の認証処理が正しく実行されると（ステップＳ１６０２）、ＩＣチップ１１内のディスク鍵Ｋｍが、ビデオレコーダ１に読み出される（ステップＳ１６０３）。

【０１９７】

〔ステップＳ１６０４，Ｓ１６０５〕これらのステップは、図２４のステップＳ１３１１およびＳ１３１２に対応し、記録するコンテンツの識別情報と利用制御情報とが、ＩＣチップ１１に書き込まれる。なお、以上のステップＳ１６０３～Ｓ１６０５の処理は、光ディスク１０がＩＣチップＲ／Ｗ３にかざされている間に、一連の処理として実行される。

【０１９８】

〔ステップＳ１６０６～Ｓ１６１０〕これらのステップでは、図２３のステップＳ１３０４～Ｓ１３０８と同様の処理が実行され、これにより、鍵情報で暗号化されたコンテンツファイルと、ディスク鍵Ｋｍで暗号化された鍵情報とが、光ディスク１０のデータ領域に記録される。

【０１９９】

〔ステップＳ１６１１〕このステップは、図２４のステップＳ１３１３に対応し、ＨＤＤ１１２内のコンテンツが無効化されて、コンテンツのムーブが完了する。

図２９は、上記の手順により光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャートである。

【０２００】

〔ステップＳ１７０１～Ｓ１７０４〕これらのステップでは、図２５のステップＳ１４０１～Ｓ１４０４と同様の処理が実行される。すなわち、ＩＣチップ１１内の識別情報および利用制御情報に基づくコンテンツの一覧表示（ステップＳ１７０１）に応じて、記録するコンテンツがユーザにより選択された後（ステップＳ１７０２）、再びＩＣチップ１１がＩＣチップＲ／Ｗ３に認識されて、相互認証処理が実行される（ステップＳ１７０３）。そして、相互認証処理が正しく実行されると、ＩＣチップ１１内のディスク鍵Ｋｍが、ビデオレコーダ１に読み出される（ステップＳ１７０４）。

【０２０１】

〔ステップＳ１７０５〕さらに、記録再生制御部８１の制御により、ＩＣチップ１１内の対応する利用制御情報が更新され、ムーブ対象とするコンテンツファイルが無効化される。

【０２０２】
〔ステップＳ１７０６～Ｓ１７１１〕これらのステップは、図２５～図２６のステップＳ１４０５～Ｓ１４１０にそれぞれ対応する。すなわち、案内画面の表示（ステップＳ１７０６）に応じて、ユーザが光ディスク１０をビデオレコーダ１にセットすると、この光ディスク１０から暗号化されたコンテンツファイルおよび鍵情報がビデオレコーダ１に読み出される（ステップＳ１７０７）。鍵情報は、ディスク鍵Ｋｍで復号され（ステップＳ１７０８）、コンテンツファイルは、復号された鍵情報で復号されて（ステップＳ１７０９）、さらにコンテンツファイルは新たな鍵情報で再暗号化され（ステップＳ１７１０）、ＨＤＤ１１２に記録される（ステップＳ１７１１）。
【０２０３】
以上の手順により、上記各実施の形態と同様に、コンテンツの利用権利を安全に管理しながら、光ディスク１０内のコンテンツをＨＤＤ１１２などにムーブ（またはコピー）することが可能になる。なお、光ディスク１０内のコンテンツを再生する場合には、ＩＣチップ１１からディスク鍵Ｋｍを読み出した後（ステップＳ１７０４）、光ディスク１０のデータ領域から暗号化されたコンテンツファイルおよび鍵情報を読み出し（ステップＳ１７０７）、鍵情報をディスク鍵Ｋｍで復号した後（ステップＳ１７０８）、その鍵情報を用いてコンテンツファイルを復号し、再生すればよい。
【０２０４】
《既存システムに対する応用》
ここで、上記各実施の形態に係るビデオレコーダにおける、利用権利を確実に保護しながらコンテンツの記録・再生などを可能にする機能について説明する。
【０２０５】
まず、図３０は、第１～第３の実施の形態でのコンテンツ利用権利保護のための機能を示すブロック図である。
図３０では、光ディスク１０に対してコンテンツファイルなどを記録する装置と、この光ディスク１０のコンテンツファイルを再生する装置とを、それぞれ光ディスク記録装置３１０ａおよび光ディスク再生装置３２０ａとに分割して示している。なお、これらは同一の装置（例えば上記のビデオレコーダ１）とされてもよいし、個別の装置の場合でも、再生する光ディスク再生装置３２０ａ側に、光ディスク記録装置３１０ａ側と同様な記録機能が搭載されている、あるいは、光ディスク記録装置３１０ａに、光ディスク再生装置３２０ａ側と同様な再生機能が搭載されていてもよい。
【０２０６】
第１～第３の実施の形態では、図３０に示すように、光ディスク１０のデータ領域には、暗号化されたコンテンツファイルが記録される。これとともに、光ディスク１０には、相互認証機能を備えたＩＣチップ１１が設けられ、ＩＣチップ１１内に、コンテンツファイルを利用するための鍵情報が記録される。なお、ここではこの鍵情報をコンテンツ鍵（Ｃｏｎｔｅｎｔ　Ｋｅｙ）と呼ぶ。このコンテンツ鍵は、データ領域に記録されるコンテンツファイルごとに対応付けられて記録される。また、実際には、ＩＣチップ１１内には、上述したように、コンテンツファイルの識別情報と利用制御情報も記録されるが、図３０では省略している。
【０２０７】
コンテンツファイルを光ディスク１０に記録する場合、光ディスク記録装置３１０ａでは、暗号エンジン３１１によりコンテンツ鍵で暗号化されたコンテンツファイルが、光ディスク１０のデータ領域に記録される。これとともに、相互認証機能（図中“ＡＫＥ”と表記）３３１により、光ディスク１０のＩＣチップ１１との間で、認証鍵Ｋｃなどを用いた相互認証処理が実行された後、コンテンツ鍵がＩＣチップ１１に記録される。
【０２０８】
なお、実際の相互認証処理機能は、相互認証する装置のそれぞれに個別に設けられる。また、実際には、光ディスク記録装置３１０ａおよびＩＣチップ１１には、それぞれ暗号エンジン３１１および１１ａが設けられ、これらにより光ディスク記録装置３１０ａとＩ

Ｃチップ１１との間では、鍵情報Ｋｓなどを用いて暗号化された情報が送受信される。相互認証機能３３１、暗号エンジン３１１および３１２は、例えば図３の暗号処理回路１０２の機能に対応する。

【０２０９】

一方、光ディスク１０内のコンテンツファイルを再生する場合、光ディスク再生装置３２０ａでは、相互認証機能３３２により、光ディスク１０のＩＣチップ１１との間で、認証鍵Ｋｃなどを用いた相互認証処理が実行された後、ＩＣチップ１１内のコンテンツ鍵が読み出される。なお、実際には、光ディスク再生装置３２０ａおよびＩＣチップ１１には、セキュアな情報送受信を実現するために、暗号エンジン３２２および１１ｂがそれぞれ設けられている。

【０２１０】

また、光ディスク１０のデータ領域から読み出されたコンテンツファイルは、暗号エンジン３２１により、コンテンツ鍵で復号され、これにより再生可能となる。なお、このとき、必要に応じて、ＩＣチップ１１内の対応する利用制御情報の更新が行われる。また、コンテンツファイルのムーブの場合も同様に、コンテンツファイルは暗号エンジン３２１によって復号された後、別の記録媒体に記録できるようになり、このとき、ＩＣチップ１１内の対応する利用制御情報が更新される。

【０２１１】

なお、光ディスク記録装置３１０ａの場合と同様に、相互認証機能３３２、暗号エンジン３２１および３２２は、例えば図３の暗号処理回路１０２の機能に対応する。

以上の図３０のような構成のシステムにおいて、第１～第３の実施の形態で説明した手順で処理が実行されることで、コンテンツの利用権利を安全に管理しながら、そのコンテンツの再生やムーブ（あるいはコピー）を実行できるようになる。

【０２１２】

次に、図３１は、第４および第５の実施の形態でのコンテンツ利用権利保護のための機能を示すブロック図である。なお、図３１では、図３０に対応する機能については同じ符号を付して示し、その説明を省略する。

【０２１３】

図３０の場合と同様、図３１でも、光ディスク１０に対してコンテンツファイルなどを記録する光ディスク記録装置３１０ｂと、この光ディスク１０のコンテンツファイルを再生する光ディスク再生装置３２０ｂとを、それぞれ分割して示している。

【０２１４】

図３０との基本的な違いは、光ディスク１０のＩＣチップ１１に、コンテンツ鍵の代わりにディスク鍵（ｄｉｓｃ　Ｋｅｙ）が記録され、光ディスク１０のデータ領域には、コンテンツ鍵で暗号化されたコンテンツファイルとともに、ディスク鍵で暗号化されたコンテンツ鍵が記録される点である。ディスク鍵は、基本的に、ＩＣチップ１１内に書き換え不可能な状態で１つのみ記録される。また、コンテンツ鍵の暗号化・復号のために、光ディスク記録装置３１０ｂおよび光ディスク再生装置３２０ｂは、暗号エンジン３１３および３２３をそれぞれ備えている。なお、これらの暗号エンジン３１３および３２３も、例えば図３の暗号処理回路１０２の機能に対応する。

【０２１５】

コンテンツファイルを光ディスク１０に記録する場合、光ディスク記録装置３１０ｂでは、暗号エンジン３１１によりコンテンツ鍵で暗号化されたコンテンツファイルが、光ディスク１０のデータ領域に記録される。また、相互認証機能３３１により、光ディスク１０のＩＣチップ１１との間で相互認証処理が実行された後、ＩＣチップ１１からディスク鍵が読み出され、暗号エンジン３１３により、このディスク鍵でコンテンツ鍵が暗号化されて、光ディスク１０のデータ領域に記録される。

【０２１６】

光ディスク１０内のコンテンツファイルを再生する場合、光ディスク再生装置３２０ｂでは、まず、相互認証機能３３２により、光ディスク１０のＩＣチップ１１との間で相互

認証処理が実行された後、ＩＣチップ１１内のディスク鍵が読み出される。そして、光ディスク１０のデータ領域から読み出されたコンテンツ鍵が、暗号エンジン３２３によりディスク鍵で復号され、データ領域から読み出されたコンテンツファイルが、復号されたコンテンツ鍵で暗号エンジン３２１により復号されることで、このコンテンツファイルを再生できるようになる。なお、コンテンツファイルのムーブの場合も同様に、ディスク鍵で復号されたコンテンツ鍵を用いて、コンテンツファイルが復号されることで、このコンテンツファイルを別の記録媒体に記録できるようになり、このとき、ＩＣチップ１１内の対応する利用制御情報が更新される。

【０２１７】

以上の図３１のような構成のシステムにおいて、第４および第５の実施の形態で説明した手順で処理が実行されることで、コンテンツの利用権利を安全に管理しながら、そのコンテンツの再生やムーブ（あるいはコピー）を実行できるようになる。

【０２１８】

ここで、上記の図３１の構成と比較するために、記録型ＤＶＤ（ＤＶＤ Ｒｅｃｏｒｄａｂｌｅ，ＤＶＤ：Digital Versatile Disc）規格に採用されている著作権保護システムであるＣＰＲＭ（Content Protection for Recordable Media）を例に挙げ、このＣＰＲＭにおける鍵情報の受け渡しの構造について説明する。

【０２１９】

図３２は、記録型ＤＶＤに対するＣＰＲＭシステムでの、コンテンツの記録・再生時における鍵情報の受け渡し機能を概略的に示すブロック図である。

図３２に示すように、ＣＰＲＭでは、コンテンツのデータは、光ディスク記録装置３１０ｃの暗号エンジン３１１ｃにおいて、コンテンツごとのタイトル鍵ＫｔでＡＶパック（ＡＶ ｐａｃｋ）単位で暗号化され、光ディスク１０ｃのデータ領域に記録される。一方、光ディスク１０ｃの書き換え不可能な領域には、ＭＫＢ（Media Key Block）と、メディアごとに固有なメディアＩＤとが記録されており、光ディスク記録装置３１０ｃは、プロセスＭＫＢ３１４ｃにおいて、自身が保持するデバイス鍵Ｋｄ＿０～Ｋｄ＿ｎで、光ディスク１０ｃから読み取ったＭＫＢからディスク鍵Ｋｍ（ただし、規格上ではＭｅｄｉａ Ｋｅｙ）を取り出し、さらに、鍵生成部３１５ｃにおいて、光ディスク１０ｃから読み取ったメディアＩＤをディスク鍵Ｋｍに作用させて、メディアユニーク鍵Ｋｍｕを生成する。そして、暗号エンジン３１３ｃにおいて、光ディスク１０ｃに記録したコンテンツに対応するタイトル鍵Ｋｔを、メディアユニーク鍵Ｋｍｕで暗号化し、データ領域に記録する。

【０２２０】

また、光ディスク１０ｃ内のコンテンツを再生する場合には、光ディスク再生装置３２０ｃは、記録のときと同様に、プロセスＭＫＢ３２４ｃにおいて、自身が保持するデバイス鍵Ｋｄ＿０～Ｋｄ＿ｎで、光ディスク１０ｃから読み取ったＭＫＢからディスク鍵Ｋｍを取り出し、鍵生成部３２５ｃにおいて、光ディスク１０ｃから読み取ったメディアＩＤをディスク鍵Ｋｍに作用させて、メディアユニーク鍵Ｋｍｕを生成する。そして、光ディスク１０ｃのデータ領域から、暗号化されたタイトル鍵Ｋｔｅを読み取り、暗号エンジン３２３ｃにおいて、メディアユニーク鍵Ｋｍｕを用いて復号する。さらに、復号されたタイトル鍵Ｋｔを用いて、暗号エンジン３２１ｃにおいて、データ領域から読み出した暗号化されたコンテンツのデータ（ＡＶパック）を復号する。これにより、コンテンツのデータを再生できるようになる。なお、光ディスク１０ｃ内のコンテンツをムーブする場合にも、同様の手順でコンテンツのデータが復号され、他の記録媒体に記録される。

【０２２１】

以上の図３２のＣＰＲＭのシステムと、図３１に示したシステムとを比較すると、まず、図３２のＣＰＲＭのシステムでは、メディアユニーク鍵Ｋｍｕを生成するために、ＭＫＢおよびメディアＩＤを利用することで、コンテンツの不正コピー防止をより強固にしている。しかし、このような手順を、図３１でのＩＣチップ１１と各デバイスとの間の相互認証手順で置き換えても、同じコピー防止機能を、しかもより確実に実現できる。従って

、上記の不正防止機能を相互認証機能に置き換え、さらに、図３２のメディアＩＤをディスク鍵に置き換えると、図３２のシステムで実現されるコンテンツの利用権利保護の機能は、図３１の機能とほぼ同等と考えることができる。

【０２２２】

すなわち、図３１のシステムは、コンテンツの記録・再生のために利用されている情報や鍵情報の流れなどが、既存のＣＰＲＭのシステムに非常に近いため、既存のシステムから図３１のシステムに対して容易に移行させることができる。さらに、図３１のシステムは、ＩＣチップ１１を用いることで、コンテンツの不正なコピーに対する防止効果が、図３２のシステムと比較して、より高くなっている。

【０２２３】

また、他の例として、再生専用型のＢＤ規格に採用されている著作権保護システムであるＡＡＣＳ（ＡＡＣＳ　ｐｒｅ－ｒｅｃｏｒｄｅｄ規格，ＡＡＣＳ：Advanced Access Content System）における鍵情報の受け渡しの構造について説明する。

【０２２４】

図３３は、再生専用型ＢＤに対するＡＡＣＳシステムでの、コンテンツ再生時における鍵情報の受け渡し機能を概略的に示すブロック図である。

図３３のシステムでは、光ディスク１０ｄの書き換え不可能な領域に、ＭＫＢと、スタンパあるいはカッティングごとに固有なボリュームＩＤ（Ｖｏｌｕｍｅ　ＩＤ）とが記録されている。コンテンツ提供者側装置３４０ｄは、暗号エンジン３１１ｄにおいて、タイトル（ｔｉｔｌｅ：コンテンツに相当）をタイトル鍵（ｔｉｔｌｅ　Ｋｅｙ）で暗号化し、光ディスク１０ｄのデータ領域に記録する。これとともに、鍵生成部３１５ｄにおいて、光ディスク１０ｄのボリュームＩＤをメディア鍵（Ｍｅｄｉａ　Ｋｅｙ　Ｖａｒｉａｎｔ）Ｋｍｖに作用させて、ボリュームユニーク鍵（Ｖｏｌｕｍｅ　Ｖａｒｉａｎｔ　Ｕｎｉｑｕｅ　Ｋｅｙ）Ｋｖｖｕを生成し、タイトル鍵をこのボリュームユニーク鍵Ｋｖｖｕで暗号化して、光ディスク１０ｄのデータ領域に記録する。

【０２２５】

光ディスク１０ｄ内のタイトルを再生する場合には、光ディスク再生装置３２０ｄは、プロセスＭＫＢ３２４ｄにおいて、自身が保持するデバイス鍵Ｋｄ＿０～Ｋｄ＿ｎで、光ディスク１０ｄから読み取ったＭＫＢからメディア鍵Ｋｍｖを取り出し、鍵生成部３２５ｄにおいて、光ディスク１０ｄから読み取ったボリュームＩＤをメディア鍵Ｋｍｖに作用させて、ボリュームユニーク鍵Ｋｖｖｕを生成する。そして、光ディスク１０ｄのデータ領域から、暗号化されたタイトル鍵を読み取り、暗号エンジン３２３ｄにおいて、ボリュームユニーク鍵Ｋｖｖｕを用いて復号する。さらに、復号されたタイトル鍵Ｋｔを用いて、暗号エンジン３２１ｄにおいて、データ領域から読み出した暗号化されたタイトルのデータを復号する。これにより、コンテンツのデータを再生できるようになる。

【０２２６】

以上の図３３のＡＡＣＳのシステムと、図３１に示したシステムとを比較すると、図３３のシステムでは、タイトルの再生時にボリュームユニーク鍵Ｋｖｖｕを生成するために、ＭＫＢおよびボリュームＩＤを利用することで、タイトルの不正コピー防止効果をより強固にしているが、図３２の場合と同様に、このような手順は、図３１における相互認証手順に置き換えることができる。従って、このような不正コピー防止機能を相互認証機能に置き換え、さらに、図３３のボリュームＩＤをディスク鍵に置き換えると、図３３のシステムで実現されるコンテンツの利用権利保護の機能は、図３１の機能とほぼ同等と考えることができる。

【０２２７】

すなわち、図３１のシステムは、コンテンツの記録・再生のために利用されている情報や鍵情報の流れなどが、再生専用型ＢＤに採用されたＡＡＣＳのシステムにも非常に近いため、既存のシステムから図３１のシステムに対して容易に移行させることができる。また、光ディスクのＩＣチップ内に利用制御情報を記録することで、再生専用ＢＤ内のタイトルを他の記録媒体に安全にムーブすることも可能となる。

【０２２８】
なお、図３１のシステムに、図３２あるいは図３３のシステムと同様なデバイス鍵を用いたリボケーション（不正デバイス無効化）手法を導入することもできる。
以上のように、既存の光ディスクに利用されたメディアＩＤおよびボリューム鍵と同等な情報（ディスクＩＤ）を利用しながら、暗号化・復号の鍵情報の利用の流れや記憶場所などの運用手順を、新たなシステムにあわせて置き換えることで、図３２および図３３の既存のシステムを新たな図３１のシステムに容易に移行させることができる。このため、新たなシステムに対する記録装置・再生装置などの各種デバイスの対応が比較的容易になり、デバイスの新たな開発コストを抑制しながらも、より安全性の高いシステムを構築することができる。
【０２２９】
そして、このような図３１のシステムに対して、上記の第４および第５の実施の形態での処理手順を適用することで、コンテンツの利用権利を確実に保護しながらも、ユーザにとってわかりやすい操作で、光ディスクと他の記録媒体との間のムーブや、ムーブした光ディスク内のコンテンツの再生を実行できるようになる。
【０２３０】
《第６の実施の形態》
さらに、以下で説明するように、書き換え可能型ＢＤに採用されているＡＡＣＳ（ＡＡＣＳ　ｒｅｃｏｒｄａｂｌｅ）のシステムについても、上記の図３１の構成に近い、後述する第６および第７の実施の形態に係るシステムへ容易に移行させることができる。そこで、まず、このような既存のＡＡＣＳシステムについて説明する。
【０２３１】
図３４は、書き換え可能型ＢＤに対するＡＡＣＳシステムでの、コンテンツ再生時における鍵情報の受け渡し機能を概略的に示すブロック図である。
図３４のシステムでは、光ディスク１０ｅ内の所定の保護された領域（すなわち、一般のユーザには簡単に読み取りや複製が不可能な領域）に、ＭＫＢと、バインディングナンス（Ｂｉｎｄｉｎｇ　Ｎｏｎｃｅ）と言われる情報とが記録される。バインディングナンスは、後述するように、タイトルの新たな記録やムーブ（またはコピー）のたびに更新されるユニークな情報である。
【０２３２】
光ディスク１０ｅにタイトルが記録される場合、光ディスク記録装置３１０ｅでは、暗号エンジン３１１ｅによりタイトルがタイトル鍵で暗号化され、光ディスク１０ｅのデータ領域に記録される。一方、プロセスＭＫＢ３１４ｅは、自身が保持するデバイス鍵Ｋｄ＿０～Ｋｄ＿ｎで、光ディスク１０ｅから読み取ったＭＫＢからディスク鍵Ｋｍ（ただし、規格上ではＭｅｄｉａ　Ｋｅｙ）を取り出す。鍵生成部３１６ｅは、例えば乱数など、その都度ユニークな鍵情報を生成し、鍵生成部３１７ｅは、生成された鍵情報をディスク鍵Ｋｍに作用させて新たなバインディングナンスを生成し、光ディスク１０ｅに記録する。また、鍵生成部３１６ｅで生成された鍵情報は、暗号鍵Ｋｐａ（ｎ）として暗号エンジン３１３ｅに供給され、暗号エンジン３１３ｅは、この暗号鍵Ｋｐａ（ｎ）でタイトル鍵を暗号化し、暗号化されたタイトル鍵が光ディスク１０ｅのデータ領域に記録される。
【０２３３】
また、この光ディスク１０ｅに対して、光ディスク記録装置３１０ｅによりさらにタイトルが記録される場合には、まず、光ディスク１０ｅからＭＫＢおよびバインディングナンスが読み取られ、プロセスＭＫＢ３１４ｅによりディスク鍵Ｋｍが取り出された後、鍵生成部３１５ｅにより、バインディングナンスをディスク鍵Ｋｍに作用させることで、復号鍵Ｋｐａ（ｏ）が生成される。そして、光ディスク１０ｅのデータ領域に記録されたすべてのタイトル鍵が読み出され、これらのタイトル鍵が暗号エンジン３１８ｅにおいて復号鍵Ｋｐａ（ｏ）で復号される。
【０２３４】
その後、上記と同じ手順で、タイトルがタイトル鍵で暗号化され、光ディスク１０ｅの

データ領域に記録されるとともに、鍵生成部３１６ｅからの鍵情報およびディスク鍵Ｋｍによりバインディングナンスが更新される。さらに、新たに記録するタイトルのタイトル鍵と、暗号エンジン３１８ｅで復号された他のタイトル鍵とが、暗号エンジン３１３ｅにおいて新たな暗号鍵Ｋｐａ（ｎ）ですべて暗号化され、光ディスク１０ｅのデータ領域に記録される。

【０２３５】

このように、図３４のシステムでは、光ディスク１０ｅに新たなタイトルを記録する場合には、バインディングナンスが更新されるとともに、新たなタイトルのタイトル鍵に加えて、すでに光ディスク１０ｅに記録されている他のタイトルのタイトル鍵も、新たな暗号鍵Ｋｐａ（ｎ）で暗号化される。

【０２３６】

また、この光ディスク１０ｅ内のタイトルを再生する場合、光ディスク再生装置３２０ｅは、プロセスＭＫＢ３２４ｅにおいて、デバイス鍵Ｋｄ＿０～Ｋｄ＿ｎを利用して、光ディスク１０ｅから読み取ったＭＫＢからディスク鍵Ｋｍを取り出し、鍵生成部３２５ｅにおいて、光ディスク１０ｅから読み取ったバインディングナンスをディスク鍵Ｋｍに作用させて、タイトル鍵の復号鍵Ｋｐａを生成する。そして、光ディスク１０ｄのデータ領域から、再生するタイトルに対応するタイトル鍵を読み出し、暗号エンジン３２３ｅにおいて、そのタイトル鍵を復号鍵Ｋｐａで復号し、さらにデータ領域から読み出したタイトルを、暗号エンジン３２１ｅにおいて復号鍵Ｋｐａで復号する。これにより、タイトルを再生できるようになる。

【０２３７】

図３５は、書き換え可能型ＢＤに対するＡＡＣＳシステムでの、コンテンツのムーブ時における鍵情報の受け渡し機能を概略的に示すブロック図である。

図３５において、光ディスク記録装置３１０ｅは、図３４で示したものと同一である。また、図３５における光ディスク再生装置３２０ｅは、光ディスク記録装置３１０ｅにより光ディスク１０ｅに記録されたタイトルのデータを読み出し、他の記録媒体にムーブできる状態にして出力する。

【０２３８】

この光ディスク再生装置３２０ｅにおいて、光ディスク１０ｅ内のタイトルがムーブされる場合、まず、上記の再生時と同様の手順で、プロセスＭＫＢ３２４ｅにより、デバイス鍵Ｋｄ＿０～Ｋｄ＿ｎを利用して、光ディスク１０ｅから読み取られたＭＫＢからディスク鍵Ｋｍが取り出され、鍵生成部３２５ｅにより、光ディスク１０ｅから読み取られたバインディングナンスをディスク鍵Ｋｍに作用させて、タイトル鍵の復号鍵Ｋｐａ（ｏ）が生成される。

【０２３９】

また、光ディスク１０ｅのデータ領域からは、記録されたすべてのタイトル鍵が読み出され、暗号エンジン３２３ｅにおいて、復号鍵Ｋｐａ（ｏ）でそれらが復号される。そして、復号されたタイトル鍵のうち、ムーブ対象のタイトルに対応するものだけが暗号エンジン３２１ｅに供給され、光ディスク１０ｅのデータ領域から読み出されたタイトルが、暗号エンジン３２１ｅにおいて復号されて、他の記録媒体にムーブできるようになる。

【０２４０】

さらに、鍵生成部３２６ｅは、乱数などの新たな鍵情報を生成し、この鍵情報をディスク鍵Ｋｍに作用させて、新たなバインディングナンスを生成し、光ディスク１０ｅ内の情報を更新する。また、鍵生成部３２６ｅからの鍵情報は、新たな暗号鍵Ｋｐａ（ｎ）として暗号エンジン３２８ｅに供給され、暗号エンジン３２８ｅは、この暗号鍵Ｋｐａ（ｎ）で、ムーブに利用された以外の残りのタイトル鍵を暗号化する。このように暗号化されたタイトル鍵が、光ディスク１０ｅのデータ領域に再び記録される。

【０２４１】

以上の図３４および図３５のようなシステムは、次の図３６および図３７に示すシステムに置き換えることができる。すなわち、上述した図３２および図３３のシステムと図３

１のシステムとの関係のように、図３４および図３５に示すコンテンツの利用権利保護の機能とほぼ同等の機能を、図３６および図３７に示すシステムにおいても実現でき、デバイスの開発コストなどを抑制しながら容易にシステムの移行を行うことができる。

【０２４２】

図３６は、本発明の第６の実施の形態に係るコンテンツ記録システムでの、コンテンツ再生時における鍵情報の受け渡し機能を概略的に示すブロック図である。

図３６のシステムでは、図３１のシステムと同様に、光ディスク１０は、相互認証機能付きのＩＣチップ１１を備え、その中のメモリには、相互認証のための認証鍵Ｋｃと、ディスク鍵Ｋｍとが記録される。ただし、ディスク鍵Ｋｍは、上記のバインディングナンスに対応するユニークな情報であり、光ディスク１０への新たなコンテンツファイルの記録や、他の記録媒体へのムーブ（あるいはコピー）などに応じて更新される点が異なる。

【０２４３】

コンテンツファイルを光ディスク１０に記録する場合、光ディスク記録装置３１０ｆでは、暗号エンジン３１１ｆによりコンテンツ鍵で暗号化されたコンテンツファイルが、光ディスク１０のデータ領域に記録される。また、相互認証機能３３１により、光ディスク１０のＩＣチップ１１との間で相互認証処理が実行された後、ＩＣチップ１１からディスク鍵が読み出される。なお、暗号エンジン３１２ｆおよび１１ａは、ＩＣチップ１１に送受信されるデータの暗号化および復号を行うブロックである。

【０２４４】

ここで、光ディスク１０にすでにコンテンツファイルが記録されている場合、各コンテンツファイルに対応するすべての暗号化されたコンテンツ鍵が、光ディスク１０のデータ領域から読み出される。また、ＩＣチップ１１から読み出されたディスク鍵は、復号鍵Ｋｗ（ｏ）として暗号エンジン３１８ｆに供給され、暗号エンジン３１８ｆは、データ領域から読み出されたすべてのコンテンツ鍵を、復号鍵Ｋｗ（ｏ）で復号する。

【０２４５】

一方、鍵生成部３１６ｆは、乱数などにより新たな暗号鍵Ｋｗ（ｎ）を生成し、暗号エンジン３１３ｆは、復号したコンテンツ鍵と、新たなコンテンツ鍵とを、すべて暗号鍵Ｋｗ（ｎ）で暗号化する。暗号化されたすべてのコンテンツ鍵は、光ディスク１０のデータ領域に記録される。さらに、暗号鍵Ｋｗ（ｎ）は、新たなディスク鍵としてＩＣチップ１１に上書き記録される。なお、ディスク鍵の記録の際には、ＩＣチップ１１と光ディスク記録装置３１０ｆとの間で相互認証されている必要がある。

【０２４６】

次に、このような光ディスク１０内のコンテンツが再生される場合、光ディスク再生装置３２０ｆでは、相互認証機能３３２により、光ディスク１０のＩＣチップ１１との間で相互認証処理が実行された後、ＩＣチップ１１からディスク鍵が読み出される。なお、暗号エンジン３２２ｆおよび１１ｂは、ＩＣチップ１１に送受信されるデータの暗号化および復号を行うブロックである。

【０２４７】

光ディスク１０のデータ領域からは、まず、再生するコンテンツに対応する暗号化されたコンテンツ鍵が読み出される。暗号エンジン３２３ｆは、ディスク鍵を復号鍵Ｋｗとして用いて、読み出されたコンテンツ鍵を復号し、暗号エンジン３２１ｆは、光ディスク１０のデータ領域から読み出された暗号化されたコンテンツファイルを、復号されたコンテンツ鍵で復号する。これにより、復号されたコンテンツファイルを再生できるようになる。

【０２４８】

図３７は、本発明の第６の実施の形態に係るコンテンツ記録システムでの、コンテンツのムーブ時における鍵情報の受け渡し機能を概略的に示すブロック図である。

光ディスク１０内のコンテンツがムーブされる場合、光ディスク再生装置３２０ｆでは、まず、相互認証機能３３２により、光ディスク１０のＩＣチップ１１との間で相互認証処理が実行された後、ＩＣチップ１１からディスク鍵が読み出される。また、光ディスク

１０のデータ領域からは、記録されたすべてのコンテンツに対応するコンテンツ鍵が読み出され、暗号エンジン３２３ｆは、ディスク鍵を復号鍵Ｋｗ（ｏ）として利用して、すべてのコンテンツ鍵を復号する。さらに、暗号エンジン３２１ｆは、光ディスク１０のデータ領域から読み出されたムーブ対象のコンテンツファイルを、対応するコンテンツ鍵で復号する。これにより、復号されたコンテンツファイルを他の記録媒体にムーブ（またはコピー）できるようになる。

【０２４９】

さらに、鍵生成部３２６ｆは、乱数などにより新たな暗号鍵Ｋｗ（ｎ）を生成し、暗号エンジン３２８ｆは、ムーブに利用された以外の残りのコンテンツ鍵を、新たな暗号鍵Ｋｗ（ｎ）で暗号化する。暗号化されたコンテンツ鍵は、光ディスク１０のデータ領域に上書き記録される。また、新たな暗号鍵Ｋｗ（ｎ）は、ＩＣチップ１１との相互認証が行われた状態で、新たなディスク鍵としてＩＣチップ１１に上書き記録される。

【０２５０】

以上のように、図３６および図３７のシステムでは、光ディスク１０に新たなコンテンツを記録する場合、および光ディスク１０内のコンテンツを他の記録媒体にムーブ（あるいはコピー）する場合に、ＩＣチップ１１内のディスク鍵が更新されるとともに、その新たなディスク鍵で、光ディスク１０内のすべてのコンテンツ鍵が再暗号化される。

【０２５１】

なお、光ディスク１０内のコンテンツを、利用権利を安全に保護しながらムーブまたはコピーするためには、実際には、後述するように、ムーブやコピーの可不可を示す利用制御情報が、安全な状態で光ディスク１０内（あるいはＩＣチップ１１内）において更新される必要がある。また、光ディスク１０内のコンテンツを再生する場合に、そのコンテンツに再生回数などの制限がある場合には、図３７のムーブ時の手順と同様に、コンテンツを再生するたびに、ＩＣチップ１１内のディスク鍵を更新するとともに、光ディスク１０内のすべてのコンテンツ鍵を再暗号化する必要がある。

【０２５２】

ここで、図３６および図３７のシステムと、上述した図３４および図３５のシステムとを比較すると、図３４および図３５のシステムでは、タイトルの記録やムーブ時に、ＭＫＢから得られたディスク鍵Ｋｍにバインディングナンスを作用させて、復号鍵Ｋｐａ（ｏ）を生成するとともに、そのディスク鍵Ｋｍを用いて新たなバインディングナンスを生成することで、タイトルの不正コピー効果をより強固にしている。しかし、このような手順は、図３６および図３７における相互認証手順に置き換えることができる。従って、このような不正コピー防止機能を相互認証機能に置き換え、さらに、図３４および図３５のバインディングナンスをディスク鍵に置き換えると、図３４および図３５のシステムで実現されるコンテンツの利用権利保護の機能は、図３６および図３７の機能とほぼ同等と考えることができる。

【０２５３】

すなわち、図３６および図３７のシステムは、コンテンツの記録・再生・ムーブ・コピーなどのために利用されている情報や鍵情報の流れが、図３４および図３５に示した既存のＡＡＣＳのシステムに非常に近いため、このような既存のシステムから図３６および図３７のシステムに対して容易に移行できる。

【０２５４】

なお、図３６および図３７のシステムに、図３４および図３５のシステムと同様なデバイス鍵を用いたリボケーション（不正デバイス無効化）手法を導入することもできる。

次に、上記の図３６および図３７のシステムを利用して、光ディスク１０内のコンテンツの再生・ムーブ・コピーを、ユーザの操作をわかりやすくしつつ、コンテンツの利用権利を安全に保護しながら実行するための処理手順について説明する。本実施の形態では、上述した第４の実施の形態での処理手順を応用して、上記の図３６および図３７のシステムに適用した場合の処理手順について説明する。

【０２５５】

まず、図３８は、第６の実施の形態に用いられる光ディスクおよびそのＩＣチップに記録される情報を示す図である。

本実施の形態では、光ディスク１０のデータ領域に、暗号化したコンテンツファイルとともに、これらの各コンテンツファイルを復号するのに必要な鍵情報（コンテンツ鍵）を、ディスク鍵Ｋｍにより暗号化した状態で記録しておく。また、ディスク鍵ＫｍをＩＣチップ１１内に記録しておき、コンテンツの利用時に、データ領域内の鍵情報を復号するために読み出して用いるようにする。ディスク鍵Ｋｍは、相互認証処理が正しく実行された場合にのみ、読み出しおよび書き換えが可能となっている。

【０２５６】

以下、図３８のような情報が記録された光ディスクを用いた場合のコンテンツの記録・再生などの処理手順を、具体的に説明する。なお、以下では、図３６および図３７における光ディスク記録装置３１０ｆおよび光ディスク再生装置３２０ｆの双方の機能を、図３に示したビデオレコーダ１が備えているものとして、このようなビデオレコーダ１におけるコンテンツの記録・再生などの処理手順について説明する。

【０２５７】

まず、図３９および図４０は、第６の実施の形態に係るビデオレコーダにおいて、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。

【０２５８】

〔ステップＳ１８０１～Ｓ１８０６〕これらのステップでは、図２２のステップＳ１２０１～Ｓ１２０６と同様の処理が実行される。すなわち、ユーザからの記録処理の開始要求操作に応じて、記録処理が開始され（ステップＳ１８０１）、ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３と光ディスク１０上のＩＣチップ１１との間で相互認証処理が実行される（ステップＳ１８０２）。

【０２５９】

相互認証処理が正しく実行された場合、ＩＣチップ１１からディスク鍵Ｋｍがビデオレコーダ１に読み出され（ステップＳ１８０３）、光ディスク１０をセットするように案内する案内画面がディスプレイ２に表示されて（ステップＳ１８０４）、ユーザにより光ディスク１０がビデオレコーダ１にセットされる。このとき、受信した放送コンテンツのデータが伸張復号化されて出力されるとともに（ステップＳ１８０５）、生成された鍵情報によりコンテンツのデータが暗号化される（ステップＳ１８０６）。

【０２６０】

〔ステップＳ１８０７〕記録再生制御部８１は、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に記録されたすべての全コンテンツファイルに対応する、暗号化された鍵情報を読み出す。

【０２６１】

〔ステップＳ１８０８〕暗号処理回路１０２は、ステップＳ１８０７で読み出されたすべての鍵情報を、ステップＳ１８０３で読み出されたディスク鍵Ｋｍで復号する。

〔ステップＳ１８０９〕鍵生成部２２は、例えば乱数を発生するなどして、新たなディスク鍵Ｋｍを生成する。

【０２６２】

〔ステップＳ１８１０〕暗号処理回路１０２は、ステップＳ１８０６で生成された、新たなコンテンツの鍵情報と、ステップＳ１８０８で復号されたすべての鍵情報とを、新たなディスク鍵Ｋｍで暗号化する。

【０２６３】

〔ステップＳ１８１１〕記録再生制御部８１は、ステップＳ１８０６で暗号化されたコンテンツファイルと、ステップＳ１８１０で暗号化された鍵情報とを、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に記録する。

【０２６４】

〔ステップＳ１８１２〕コンテンツファイルおよび鍵情報の記録が完了すると、記録再

生制御部８１は、光ディスクドライブ１１３に光ディスク１０を排出させるとともに、その光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面をディスプレイ２に表示させる。

【０２６５】

〔ステップＳ１８１３〕ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３とＩＣチップ１１との間で相互認証処理が実行される。

〔ステップＳ１８１４～Ｓ１８１６〕認証処理が正しく実行された場合、記録再生制御部８１の制御の下で、新たなディスク鍵（ステップＳ１８１４）と、記録したコンテンツの識別情報（ステップＳ１８１５）および利用制御情報（ステップＳ１８１６）が、一連の処理によりＩＣチップ１１に書き込まれる。

【０２６６】

図４１および図４２は、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。

〔ステップＳ１９０１～Ｓ１９０６〕これらのステップでは、図２３のステップＳ１３０１～Ｓ１３０６と同様の処理が実行される。すなわち、ユーザによるコンテンツの選択入力および記録要求が行われた後（ステップＳ１９０１）、ＩＣチップ１１の認証処理が実行される（ステップＳ１９０２）。

【０２６７】

相互認証処理が正しく実行された場合、ＩＣチップ１１からディスク鍵Ｋｍを読み出され（ステップＳ１９０３）、案内画面の表示（ステップＳ１９０４）に応じて、ユーザにより光ディスク１０がビデオレコーダ１にセットされると、ＨＤＤ１１２のコンテンツファイルが復号されて（ステップＳ１９０５）、さらに鍵情報により再暗号化される（ステップＳ１９０６）。

【０２６８】

〔ステップＳ１９０７〕記録再生制御部８１は、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に記録されたすべての全コンテンツファイルに対応する、暗号化された鍵情報を読み出す。

【０２６９】

〔ステップＳ１９０８〕暗号処理回路１０２は、ステップＳ１９０７で読み出されたすべての鍵情報を、ステップＳ１９０３で読み出されたディスク鍵Ｋｍで復号する。

〔ステップＳ１９０９〕鍵生成部２２は、例えば乱数を発生するなどして、新たなディスク鍵Ｋｍを生成する。

【０２７０】

〔ステップＳ１９１０〕暗号処理回路１０２は、ステップＳ１９０６で生成された新たなコンテンツの鍵情報と、ステップＳ１９０８で復号されたすべての鍵情報とを、新たなディスク鍵Ｋｍで暗号化する。

【０２７１】

〔ステップＳ１９１１〕記録再生制御部８１は、ステップＳ１９０６で暗号化されたコンテンツファイルと、ステップＳ１９１０で暗号化された鍵情報とを、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に記録する。

【０２７２】

〔ステップＳ１９１２〕コンテンツファイルおよび鍵情報の記録が完了すると、記録再生制御部８１は、光ディスクドライブ１１３に光ディスク１０を排出させるとともに、その光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面をディスプレイ２に表示させる。

【０２７３】

〔ステップＳ１９１３〕ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３とＩＣチップ１１との間で相互認証処理が実行される。

〔ステップＳ１９１４～Ｓ１９１６〕認証処理が正しく実行された場合、記録再生制御部８１の制御の下で、新たなディスク鍵（ステップＳ１９１４）と、記録したコンテンツ

の識別情報（ステップＳ１９１５）および利用制御情報（ステップＳ１９１６）が、一連の処理によりＩＣチップ１１に書き込まれる。なお、当然、各情報はどのような順番で書き込まれてもよい。

【０２７４】

〔ステップＳ１９１７〕ＩＣチップ１１への情報記録が終了すると、記録再生制御部８１は、ＨＤＤ１１２内の元のコンテンツを無効化し、これにより光ディスク１０へのムーブが完了する。

【０２７５】

図４３および図４４は、上記の手順により光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャートである。

〔ステップＳ２００１～Ｓ２００５〕これらのステップでは、図２５のステップＳ１４０１～Ｓ１４０５と同様の処理が実行される。すなわち、ＩＣチップ１１内の識別情報および利用制御情報に基づくコンテンツの一覧表示（ステップＳ２００１）に応じて、記録するコンテンツがユーザにより選択された後（ステップＳ２００２）、再びＩＣチップ１１がＩＣチップＲ／Ｗ３に認識されて、相互認証処理が実行される（ステップＳ２００３）。

【０２７６】

相互認証処理が正しく実行された場合、ＩＣチップ１１からディスク鍵Ｋｍがビデオレコーダ１に読み出され（ステップＳ２００４）、その後、光ディスク１０を光ディスクドライブ１１３にセットするように案内する案内画面が、ディスプレイ２に表示される（ステップＳ２００５）。

【０２７７】

〔ステップＳ２００６〕　記録再生制御部８１は、光ディスク１０のデータ領域から、ステップＳ２００２で選択されたコンテンツの暗号化されたコンテンツファイルと、このデータ領域に記録されたすべての全コンテンツファイルに対応する暗号化された鍵情報とを、光ディスクドライブ１１３を通じて読み出す。

【０２７８】

〔ステップＳ２００７〕暗号処理回路１０２は、ステップＳ２００６で読み出されたすべての鍵情報を、ステップＳ２００４で読み出されたディスク鍵Ｋｍで復号する。

〔ステップＳ２００８〕暗号処理回路１０２は、ステップＳ２００６で読み出されたコンテンツファイルを、ステップＳ２００７で復号された鍵情報のうち、対応する鍵情報を用いて復号する。

【０２７９】

〔ステップＳ２００９〕鍵生成部２２は、例えば乱数やＨＤＤ１１２のデバイスＩＤなどを用いて新たな鍵情報を生成し、暗号処理部２１は、生成された鍵情報を用いて、ステップＳ２００８で復号されたコンテンツファイルを再暗号化する。

【０２８０】

〔ステップＳ２０１０〕暗号化されたコンテンツファイルは、暗号処理回路１０２からＨＤＤ１１２に対して順次転送され、記録される。

〔ステップＳ２０１１〕コンテンツファイルの記録が完了すると、鍵生成部２２は、例えば乱数を発生するなどして、新たなディスク鍵Ｋｍを生成する。

【０２８１】

〔ステップＳ２０１２〕暗号処理回路１０２は、ステップＳ２００７で復号された鍵情報のうち、ムーブ対象のコンテンツ以外の鍵情報を、新たなディスク鍵Ｋｍで暗号化する。

【０２８２】

〔ステップＳ２０１３〕記録再生制御部８１は、ステップＳ２０１２で暗号化された鍵情報を、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に上書き記録する。

【０２８３】

〔ステップＳ２０１４〕鍵情報の記録が完了すると、記録再生制御部８１は、光ディスクドライブ１１３に光ディスク１０を排出させるとともに、その光ディスク１０をＩＣチップＲ／Ｗ３にかざすように案内する案内画面をディスプレイ２に表示させる。

【０２８４】

〔ステップＳ２０１５〕ユーザが光ディスク１０をＩＣチップＲ／Ｗ３にかざすと、認証処理部２３とＩＣチップ１１との間で相互認証処理が実行される。

〔ステップＳ２０１６〕認証処理が正しく実行された場合、記録再生制御部８１は、まず、ステップＳ２０１０でＨＤＤ１１２に記録されたコンテンツファイルを有効化する。

【０２８５】

〔ステップＳ２０１７〕記録再生制御部８１は、ＩＣチップＲ／Ｗ３を通じて、新たなディスク鍵ＫｍをＩＣチップ１１に書き込む。

〔ステップＳ２０１８〕記録再生制御部８１は、ムーブしたコンテンツに対応するＩＣチップ１１内の利用制御情報を更新し、そのコンテンツファイルを無効化する。

【０２８６】

以上の手順により、上記の第４の実施の形態などと同様に、ユーザの操作がわかりやすく、かつ、コンテンツの利用権利を安全に管理しながら、光ディスク１０内のコンテンツをＨＤＤ１１２などにムーブすることが可能になる。

【０２８７】

また、コピー回数などの制限のあるコンテンツについても、ステップＳ２０１８で利用制御情報中のコピー可能回数を更新するなどの処理を行うようにすることで、上記と同様の手順で利用権利を安全に管理しながらコピーを実行することができる。

【０２８８】

さらに、再生回数などの制限のあるコンテンツを再生する場合には、上記のステップＳ２００１～Ｓ２００８の手順で、コンテンツファイルを光ディスク１０から読み出して復号し、再生する。これとともに、そのコンテンツを含むすべてのコンテンツの鍵情報を新たなディスク鍵で暗号化して、光ディスク１０のデータ領域に上書き記録し、さらに、相互認証された状態のＩＣチップ１１に対して、新たなディスク鍵Ｋｍを書き込むとともに、再生したコンテンツの利用制御情報を更新する。

【０２８９】

《第７の実施の形態》

次に、上記の図３６および図３７のシステムを利用して、光ディスク１０内のコンテンツの再生・ムーブ・コピーを実行するための別の処理手順を、第７の実施の形態として説明する。

【０２９０】

図４５および図４６は、第７の実施の形態に係るビデオレコーダにおいて、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。

【０２９１】

〔ステップＳ２１０１～Ｓ２１０３〕これらのステップでは、図２７のステップＳ１５０１～Ｓ１５０３と同様の処理が実行される。すなわち、ユーザからの記録処理の開始要求操作に応じて、記録処理が開始され（ステップＳ２１０１）、光ディスク１０上のＩＣチップ１１の相互認証処理が実行された後（ステップＳ２１０２）、ＩＣチップ１１からディスク鍵Ｋｍがビデオレコーダ１に読み出される（ステップＳ２１０３）。

【０２９２】

〔ステップＳ２１０４〕鍵生成部２２は、例えば乱数を発生するなどして、新たなディスク鍵Ｋｍを生成する。

〔ステップＳ２１０５～Ｓ２１０７〕ＩＣチップ１１との相互認証が保たれた状態で、新たなディスク鍵（ステップＳ２１０５）と、記録するコンテンツの識別情報（ステップＳ２１０６）および利用制御情報（ステップＳ２１０７）が、ＩＣチップ１１に書き込まれる。

【０２９３】
〔ステップＳ２１０８～Ｓ２１１０〕これらのステップでは、図２７のステップＳ１５０６～Ｓ１５０８と同様の処理が実行される。すなわち、光ディスク１０をセットするように案内する案内画面がディスプレイ２に表示されて（ステップＳ２１０８）、ユーザにより光ディスク１０がビデオレコーダ１にセットされる。このとき、受信した放送コンテンツのデータが伸張復号化されて出力されるとともに（ステップＳ２１０９）、生成された鍵情報によりコンテンツのデータが暗号化される（ステップＳ２１１０）。
【０２９４】
〔ステップＳ２１１１〕記録再生制御部８１は、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に記録されたすべての全コンテンツファイルに対応する、暗号化された鍵情報を読み出す。
【０２９５】
〔ステップＳ２１１２〕暗号処理回路１０２は、ステップＳ２１１１で読み出されたすべての鍵情報を、ステップＳ２１０３で読み出されたディスク鍵Ｋｍで復号する。
〔ステップＳ２１１３〕暗号処理回路１０２は、ステップＳ２１１０で生成された、新たなコンテンツの鍵情報と、ステップＳ２１１２で復号されたすべての鍵情報とを、新たなディスク鍵Ｋｍで暗号化する。
【０２９６】
〔ステップＳ２１１４〕記録再生制御部８１は、ステップＳ２１１０で暗号化されたコンテンツファイルと、ステップＳ２１１３で暗号化された鍵情報とを、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に記録する。
【０２９７】
図４７および図４８は、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。
〔ステップＳ２２０１～Ｓ２２０３〕これらのステップでは、図２８のステップＳ１６０１～Ｓ１６０３に対応する処理が実行され、ユーザによるコンテンツの選択入力および記録要求が行われた後（ステップＳ２２０１）、ＩＣチップ１１の認証処理が正しく実行されると（ステップＳ２２０２）、ＩＣチップ１１内のディスク鍵Ｋｍが、ビデオレコーダ１に読み出される（ステップＳ２２０３）。
【０２９８】
〔ステップＳ２２０４〕鍵生成部２２は、例えば乱数を発生するなどして、新たなディスク鍵Ｋｍを生成する。
〔ステップＳ２２０５～Ｓ２２０７〕ＩＣチップ１１との相互認証が保たれた状態で、新たなディスク鍵（ステップＳ２２０５）と、記録するコンテンツの識別情報（ステップＳ２２０６）および利用制御情報（ステップＳ２２０７）が、ＩＣチップ１１に書き込まれる。なお、当然、各情報はどのような順番で書き込まれてもよい。
【０２９９】
〔ステップＳ２２０８～Ｓ２２１０〕これらのステップでは、図２８のステップＳ１６０６～Ｓ１６０８と同様の処理が実行され、案内画面の表示（ステップＳ２２０８）に応じて、ユーザにより光ディスク１０がビデオレコーダ１にセットされると、ＨＤＤ１１２のコンテンツファイルが復号されて（ステップＳ２２０９）、さらに鍵情報により再暗号化される（ステップＳ２２１０）。
【０３００】
〔ステップＳ２２１１〕記録再生制御部８１は、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に記録されたすべての全コンテンツファイルに対応する、暗号化された鍵情報を読み出す。
【０３０１】
〔ステップＳ２２１２〕暗号処理回路１０２は、ステップＳ２２１１で読み出されたすべての鍵情報を、ステップＳ２２０３で読み出されたディスク鍵Ｋｍで復号する。
〔ステップＳ２２１３〕鍵生成部２２は、例えば乱数を発生するなどして、新たなディ

スク鍵Ｋｍを生成する。
【０３０２】
〔ステップＳ２２１４〕暗号処理回路１０２は、ステップＳ２２１０で生成された新たなコンテンツの鍵情報と、ステップＳ２２１２で復号されたすべての鍵情報とを、新たなディスク鍵Ｋｍで暗号化する。
【０３０３】
〔ステップＳ２２１５〕記録再生制御部８１は、ステップＳ２２１０で暗号化されたコンテンツファイルと、ステップＳ２２１４で暗号化された鍵情報とを、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に記録する。
【０３０４】
〔ステップＳ２２１６〕コンテンツファイルおよび鍵情報の記録が完了すると、記録再生制御部８１は、ＨＤＤ１１２内の元のコンテンツを無効化し、これにより光ディスク１０へのムーブが完了する。
【０３０５】
図４９および図５０は、上記の手順により光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャートである。
〔ステップＳ２３０１～Ｓ２３０４〕これらのステップでは、図２９のステップＳ１７０１～Ｓ１７０４と同様の処理が実行される。すなわち、ＩＣチップ１１内の識別情報および利用制御情報に基づくコンテンツの一覧表示（ステップＳ２３０１）に応じて、記録するコンテンツがユーザにより選択された後（ステップＳ２３０２）、再びＩＣチップ１１がＩＣチップＲ／Ｗ３に認識されて、相互認証処理が実行される（ステップＳ２３０３）。そして、相互認証処理が正しく実行されると、ＩＣチップ１１内のディスク鍵Ｋｍが、ビデオレコーダ１に読み出される（ステップＳ２３０４）。
【０３０６】
〔ステップＳ２３０５〕鍵生成部２２は、例えば乱数を発生するなどして、新たなディスク鍵Ｋｍを生成する。
〔ステップＳ２３０６〕記録再生制御部８１は、ＩＣチップＲ／Ｗ３を通じて、新たなディスク鍵ＫｍをＩＣチップ１１に書き込む。
【０３０７】
〔ステップＳ２３０７〕記録再生制御部８１は、ムーブ対象のコンテンツに対応するＩＣチップ１１内の利用制御情報を更新し、そのコンテンツファイルを無効化する。
なお、ステップＳ２３０６およびＳ２３０７は、ＩＣチップ１１との相互認証処理後に一連の処理として実行される。
【０３０８】
〔ステップＳ２３０８〕記録再生制御部８１は、光ディスク１０を光ディスクドライブ１１３にセットするように案内する案内画面を、ディスプレイ２に表示させる。
〔ステップＳ２３０９〕記録再生制御部８１は、光ディスク１０のデータ領域から、ステップＳ２３０２で選択されたムーブ対象のコンテンツの、暗号化されたコンテンツファイルと、このデータ領域に記録されたすべての全コンテンツファイルに対応する暗号化された鍵情報とを、光ディスクドライブ１１３を通じて読み出す。
【０３０９】
〔ステップＳ２３１０〕暗号処理回路１０２は、ステップＳ２３０９で読み出されたすべての鍵情報を、ステップＳ２３０４で読み出されたディスク鍵Ｋｍで復号する。
〔ステップＳ２３１１〕暗号処理回路１０２は、ステップＳ２３０９で読み出されたコンテンツファイルを、ステップＳ２３１０で復号された鍵情報のうち、対応する鍵情報を用いて復号する。
【０３１０】
〔ステップＳ２３１２〕鍵生成部２２は、例えば乱数やＨＤＤ１１２のデバイスＩＤなどを用いて新たな鍵情報を生成し、暗号処理部２１は、生成された鍵情報を用いて、ステップＳ２３１１で復号されたコンテンツファイルを再暗号化する。

【０３１１】
〔ステップＳ２３１３〕暗号化されたコンテンツファイルは、暗号処理回路１０２からＨＤＤ１１２に対して順次転送され、記録される。
〔ステップ２３１４〕暗号処理回路１０２は、ステップＳ２３１１で復号された鍵情報のうち、ムーブ対象のコンテンツ以外の鍵情報を、新たなディスク鍵Ｋｍで暗号化する。
【０３１２】
〔ステップＳ２３１５〕記録再生制御部８１は、ステップＳ２３１４で暗号化された鍵情報を、光ディスクドライブ１１３を通じて、光ディスク１０のデータ領域に上書き記録する。なお、実際には、これらの処理の後、ＨＤＤ１１２に記録されたコンテンツファイルを有効化することで、ムーブ処理が終了する。
【０３１３】
以上の手順により、上記の第５の実施の形態などと同様に、ユーザの操作がわかりやすく、かつ、コンテンツの利用権利を安全に管理しながら、光ディスク１０内のコンテンツをＨＤＤ１１２などにムーブすることが可能になる。
【０３１４】
また、コピー回数などの制限のあるコンテンツについても、ステップＳ２３０７で利用制御情報中のコピー可能回数を更新するなどの処理を行うようにすることで、上記と同様の手順で利用権利を安全に管理しながらコピーを実行することができる。
【０３１５】
さらに、再生回数などの制限のあるコンテンツを再生する場合には、上記の図４９および図５０の手順で、再生するコンテンツの利用制御情報を更新し（ステップＳ２３０７に対応）、ステップＳ２３１３およびＳ２３１４の代わりに、復号されたコンテンツファイルを再生出力すればよい。
【０３１６】
《第８の実施の形態》
上記の第１～第７の実施の形態で実現される光ディスク１０内のコンテンツの再生やムーブ・コピーの手順は、ビデオレコーダのみならず、例えばＰＣ（パーソナルコンピュータ）などの情報処理装置（コンピュータ装置）においても実現可能である。その場合、上記の記録再生制御部８１や暗号処理回路１０２（暗号処理部２１、鍵生成部２２、認証処理部２３）の機能は、これらの機能の処理内容を記述したプログラムが情報処理装置のＣＰＵによって実行されることで実現される。
【０３１７】
しかし、一般にコンピュータ装置はオープンな仕様であり、上記機能がオープンな仕様上でのプログラムの実行により実現されるため、例えば解析ソフトウェアを用いることなどにより、鍵情報などの秘匿情報の出力が可能になるなど、完全な安全性を確保することは困難であると言える。そこで、以下の第８の実施の形態では、このような不正なプログラムの実行などによる攻撃に対する防御機能が強化された構成の情報処理装置に、本発明を適用した場合の構成例を示す。
【０３１８】
図５１は、本発明の第８の実施の形態に係る情報処理装置の構成を示すブロック図である。
図５１に示す情報処理装置４００では、ＴＣＰ（Trusted Computing Platform）準拠のＣＰＵ（ＴＣＰ－ＣＰＵ）４０８（またはＴＣＰ準拠のＣＰＵチップセット）が用いられ、汎用の内部バス４１６から隔離された領域にＲＯＭ４０９、ＲＡＭ４１０、ＥＥＰＲＯＭ４１１、ＨＤＤ４１２などを設けている。そして、上述した記録再生制御部８１および暗号処理回路１０２によるコンテンツの記録・再生・ムーブの手順を実現するプログラムをこれらの領域に記憶し、このプログラムをＴＣＰ－ＣＰＵ４０８が実行することにより、プログラムが安全に実行されるようになっている。また、これらの領域に記憶されるデータは、ＴＣＰ－ＣＰＵ４０８の相互認証・鍵交換（暗号化・復号）機能（図中“ＡＫＥ”と表記）により暗号化されるようになっており、これにより認証や暗号化・復号のため

の鍵情報などが漏洩した場合にも、情報の安全性を確保できるようになっている。

【０３１９】

さらに、内部バス４１６には、この内部バス４１６との入出力段に相互認証・鍵交換機能（ＡＫＥ）を備えたデバイスとして、デジタルＴＶチューナ４０１、グラフィックＩ／Ｆ４０６、入力Ｉ／Ｆ４１５が接続され、ＴＣＰ－ＣＰＵ４０８との間でデバイスの相互認証を行い、暗号化したデータを送受信するようになっている。なお、デジタルＴＶチューナ４０１および入力Ｉ／Ｆ４１５の機能は、図３のデジタルＴＶチューナ１０１および入力Ｉ／Ｆ１１５にそれぞれ対応し、グラフィックＩ／Ｆ４０６の機能は、図３の画像合成処理回路１０５およびビデオＤＡＣ１０６の機能に対応する。

【０３２０】

また、光ディスク１０内のコンテンツの記録・再生・ムーブ処理では、上記の相互認証・鍵交換機能（ＡＫＥ）を光ディスク１０上のＩＣチップ１１が担っており、上述した相互認証処理と、暗号化したデータの送受信により、ＩＣチップ１１とＴＣＰ－ＣＰＵ４０８との間で通信Ｉ／Ｆ４１４を介して安全な情報交換を行うことが可能となる。

【０３２１】

従って、以上の構成の情報処理装置４００により、第１～第７の実施の形態のビデオレコーダと同様に、コンテンツの不正利用を確実に防止しながらも、光ディスク１０やＨＤＤ４１２へのコンテンツの記録、それらのコンテンツの再生、ＨＤＤ４１２と光ディスク１０との間の双方向のムーブ、および、光ディスク１０から他の機器へのムーブを実行できるようになり、さらに、それらの処理を、ユーザの混乱を招くことなく、簡単な操作で実行できるようになる。

【０３２２】

なお、上述したように、上記各実施の形態で説明した処理機能は、コンピュータによって実現することができる。その場合、上記のビデオレコーダや情報処理装置が有すべき機能（記録再生制御部、暗号処理部、鍵生成部、認証処理部など）の処理内容を記述したプログラムが提供される。そして、そのプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置、光ディスク、光磁気ディスク、半導体メモリなどがある。

【０３２３】

プログラムを流通させる場合には、例えば、そのプログラムが記録された光ディスクや半導体メモリなどの可搬型記録媒体が販売される。また、プログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することもできる。

【０３２４】

プログラムを実行するコンピュータは、例えば、可搬型記録媒体に記録されたプログラムまたはサーバコンピュータから転送されたプログラムを、自己の記憶装置に格納する。そして、コンピュータは、自己の記憶装置からプログラムを読み取り、プログラムに従った処理を実行する。なお、コンピュータは、可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することもできる。また、コンピュータは、サーバコンピュータからプログラムが転送されるごとに、逐次、受け取ったプログラムに従った処理を実行することもできる。

【図面の簡単な説明】

【０３２５】

【図１】本発明を適用可能な第１のシステム構成例を示す図である。

【図２】本発明を適用可能な第２のシステム構成例を示す図である。

【図３】本発明の第１の実施の形態に係るビデオレコーダのハードウェア構成を示すブロック図である。

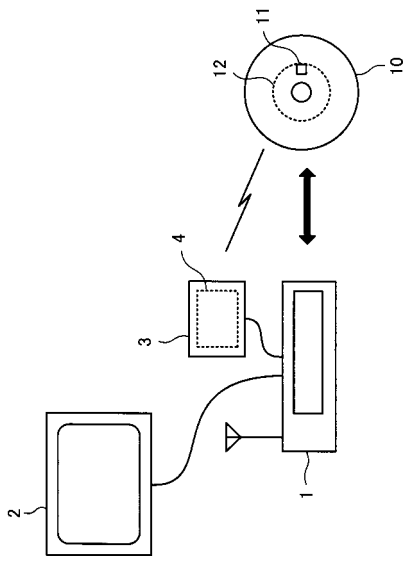
【図４】ビデオレコーダが備えるコンテンツ記録・再生のための機能を示すブロック図で

ある。
【図５】相互認証機能を備えたＩＣチップの構成例を示すブロック図である。
【図６】ＩＣチップとビデオレコーダとの間の相互認証処理シーケンスの例を示す図である。
【図７】第１の実施の形態に用いられる光ディスク（ＲＷディスク）およびそのＩＣチップに記録される情報を示す図である。
【図８】第１の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。
【図９】第１の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。
【図１０】第１の実施の形態において、光ディスク内のコンテンツを再生する場合のビデオレコーダの処理手順を示すフローチャートである。
【図１１】第１の実施の形態において、光ディスク内のコンテンツをＨＤＤにムーブする場合のビデオレコーダの処理手順を示すフローチャート（その１）である。
【図１２】第１の実施の形態において、光ディスク内のコンテンツをＨＤＤにムーブする場合のビデオレコーダの処理手順を示すフローチャート（その２）である。
【図１３】光ディスク内のコンテンツを選択するための一覧表示画面の表示例を示す図である。
【図１４】再生・ムーブの処理中における各種案内画面の表示例を示す図である。
【図１５】第２の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。
【図１６】第２の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。
【図１７】第２の実施の形態において、光ディスク内のコンテンツを再生する場合のビデオレコーダの処理手順を示すフローチャートである。
【図１８】第２の実施の形態において、光ディスク内のコンテンツをＨＤＤにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。
【図１９】第３の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。
【図２０】第３の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。
【図２１】第４の実施の形態に用いられる光ディスクおよびそのＩＣチップに記録される情報を示す図である。
【図２２】第４の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。
【図２３】第４の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャート（その１）である。
【図２４】第４の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャート（その２）である。
【図２５】第４の実施の形態において、光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャート（その１）である。
【図２６】第４の実施の形態において、光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャート（その２）である。
【図２７】第５の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャートである。
【図２８】第５の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャートである。
【図２９】第５の実施の形態において、光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャートである。
【図３０】第１～第３の実施の形態でのコンテンツ利用権利保護のための機能を示すブロ

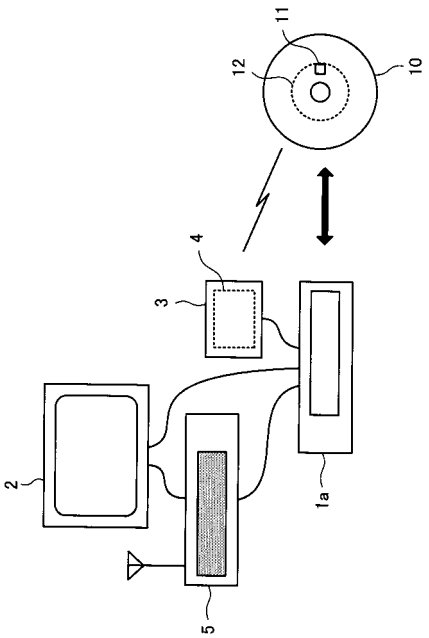
ック図である。
【図３１】第４および第５の実施の形態でのコンテンツ利用権利保護のための機能を示すブロック図である。
【図３２】記録型ＤＶＤに対するＣＰＲＭシステムでの、コンテンツの記録・再生時における鍵情報の受け渡し機能を概略的に示すブロック図である。
【図３３】再生専用型ＢＤに対するＡＡＣＳシステムでの、コンテンツ再生時における鍵情報の受け渡し機能を概略的に示すブロック図である。
【図３４】書き換え可能型ＢＤに対するＡＡＣＳシステムでの、コンテンツ再生時における鍵情報の受け渡し機能を概略的に示すブロック図である。
【図３５】書き換え可能型ＢＤに対するＡＡＣＳシステムでの、コンテンツのムーブ時における鍵情報の受け渡し機能を概略的に示すブロック図である。
【図３６】第６の実施の形態に係るコンテンツ記録システムでの、コンテンツ再生時における鍵情報の受け渡し機能を概略的に示すブロック図である。
【図３７】第６の実施の形態に係るコンテンツ記録システムでの、コンテンツのムーブ時における鍵情報の受け渡し機能を概略的に示すブロック図である。
【図３８】第６の実施の形態に用いられる光ディスクおよびそのＩＣチップに記録される情報を示す図である。
【図３９】第６の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャート（その１）である。
【図４０】第６の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャート（その２）である。
【図４１】第６の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャート（その１）である。
【図４２】第６の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャート（その２）である。
【図４３】第６の実施の形態において、光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャート（その１）である。
【図４４】第６の実施の形態において、光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャート（その２）である。
【図４５】第７の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャート（その１）である。
【図４６】第７の実施の形態において、放送により受信したコンテンツなどを光ディスクに記録する場合のビデオレコーダの処理手順を示すフローチャート（その２）である。
【図４７】第７の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャート（その１）である。
【図４８】第７の実施の形態において、ＨＤＤ内のコンテンツを光ディスクにムーブする場合のビデオレコーダの処理手順を示すフローチャート（その２）である。
【図４９】第７の実施の形態において、光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャート（その１）である。
【図５０】第７の実施の形態において、光ディスクに記録されたコンテンツをＨＤＤにムーブする場合の処理手順を示すフローチャート（その２）である。
【図５１】第８の実施の形態に係る情報処理装置の構成を示すブロック図である。
【符号の説明】
【０３２６】
１，１ａ……ビデオレコーダ、２……ディスプレイ、３……ＩＣチップＲ／Ｗ、４……アンテナ、５……ＳＴＢ、１０……光ディスク、１１……ＩＣチップ、１２……アンテナ、１３……通信回路、１４……不揮発性メモリ、１５……暗号コア、１６……シーケンサ、１７……レジスタ・Ｉ／Ｆ、２１……暗号処理部、２２……鍵生成部、２３……認証処理部、８１……記録再生制御部、１０１……デジタルＴＶチューナ、１０２……暗号処理回路、１０３……ビデオデコーダ、１０４……オーディオデコーダ、１０５……画像合成

処理回路、１０６……ビデオＤＡＣ、１０７……オーディオＤＡＣ、１０８……ＣＰＵ、１０９……ＲＯＭ、１１０……ＲＡＭ、１１１……ＥＥＰＲＯＭ、１１２……ＨＤＤ、１１３……光ディスクドライブ、１１４……通信Ｉ／Ｆ、１１５……入力Ｉ／Ｆ、１１６……内部バス

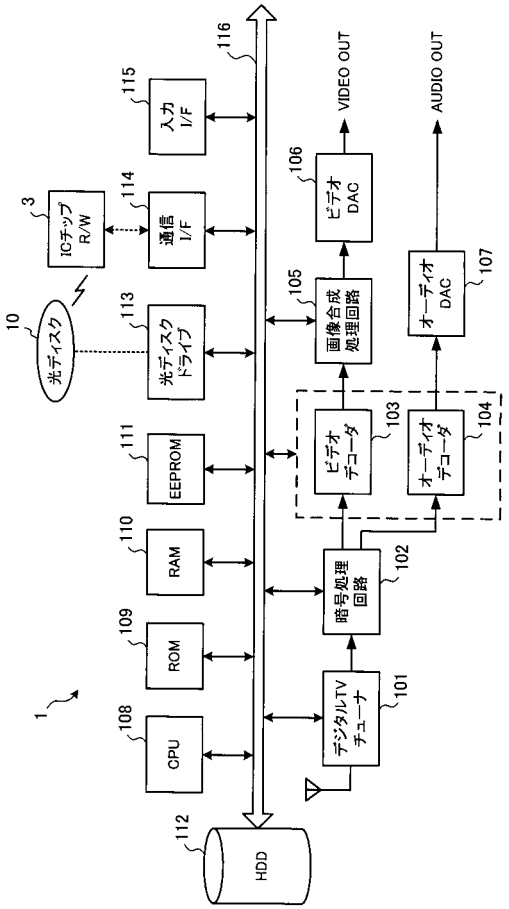
【図１】



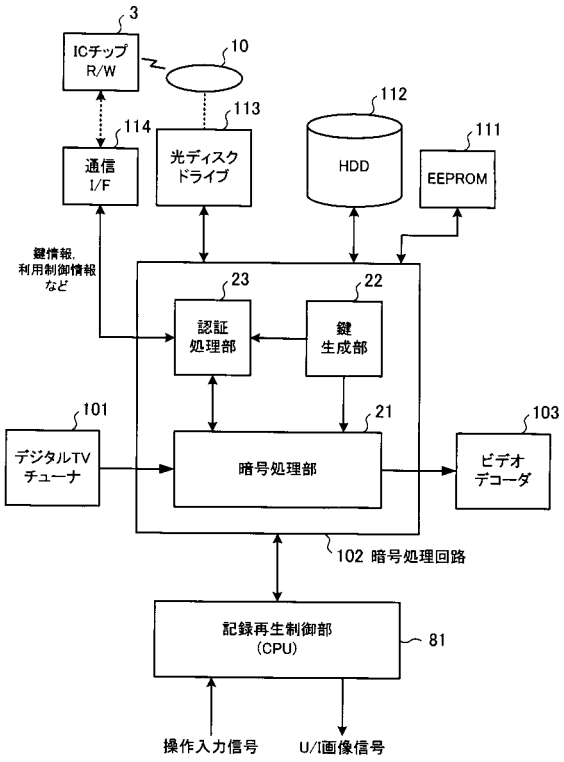

【図２】



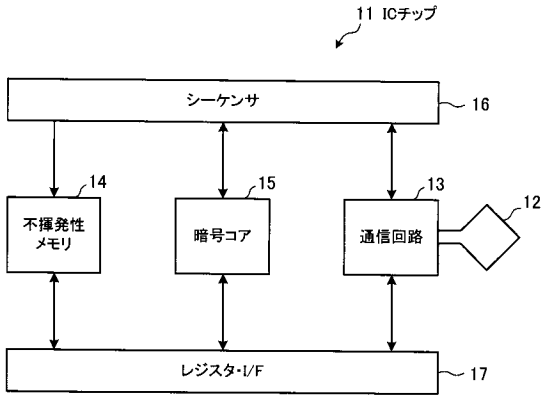
【図３】


116
115
入力 I/F
VIDEO OUT
AUDIO OUT
106
ビデオ DAC
3
ICチップ R/W
114
通信 I/F
107
オーディオ DAC
105
画像合成処理回路
10
光ディスク
113
光ディスクドライブ
103
ビデオデコーダ
104
オーディオデコーダ
111
EEPROM
110
RAM
102
暗号処理回路
109
ROM
101
デジタルTVチューナ
1
108
CPU
112
HDD

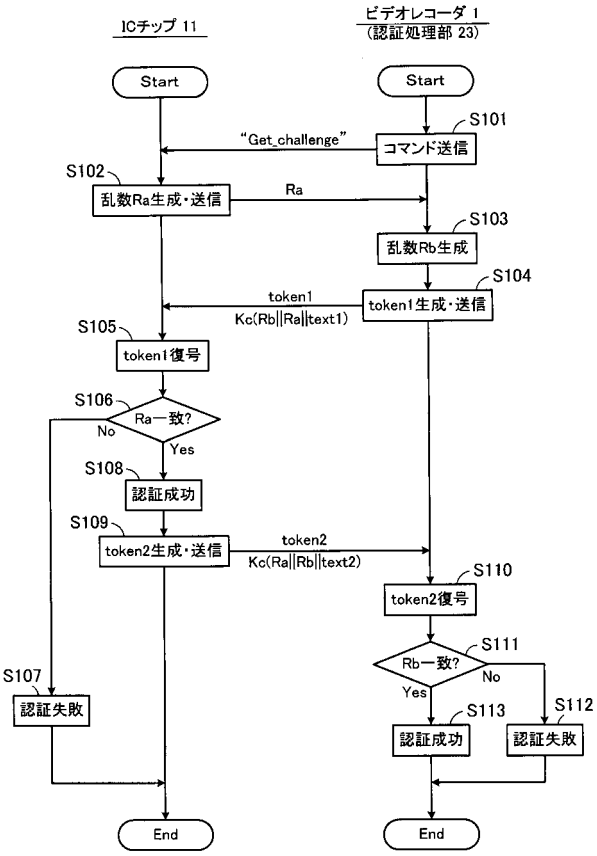
【図４】


3
ICチップ R/W
10
112
HDD
114
通信 I/F
113
光ディスクドライブ
111
EEPROM
鍵情報、利用制御情報など
23
認証処理部
22
鍵生成部
101
デジタルTVチューナ
21
暗号処理部
103
ビデオデコーダ
102 暗号処理回路
記録再生制御部 (CPU)
81
操作入力信号
U/I画像信号

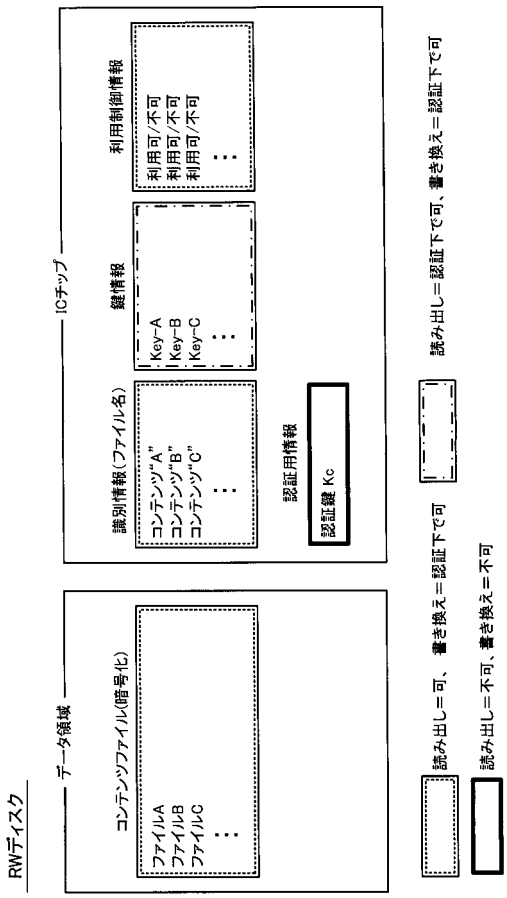
【図５】


11 ICチップ
シーケンサ
16
14
不揮発性メモリ
15
暗号コア
13
通信回路
12
レジスタ・I/F
17

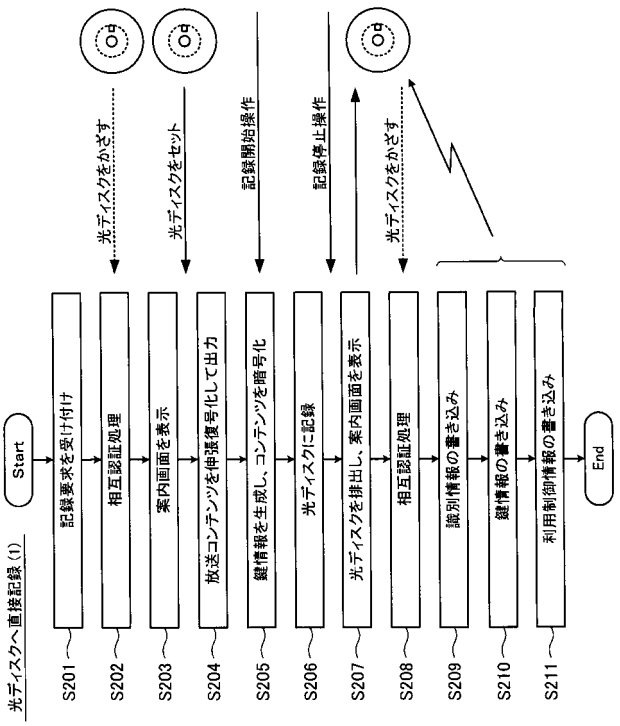
【図６】


ICチップ 11
ビデオレコーダ 1 (認証処理部 23)
Start
Start
S101
"Get_challenge"
コマンド送信
S102
乱数Ra生成・送信
Ra
S103
乱数Rb生成
S104
token1
Kc(Rb||Ra||text1)
token1生成・送信
S105
token1復号
S106
Ra一致?
No
Yes
S108
認証成功
S109
token2生成・送信
token2
Kc(Ra||Rb||text2)
S110
token2復号
S111
Rb一致?
No
Yes
S112
S113
認証成功
認証失敗
S107
認証失敗
End
End

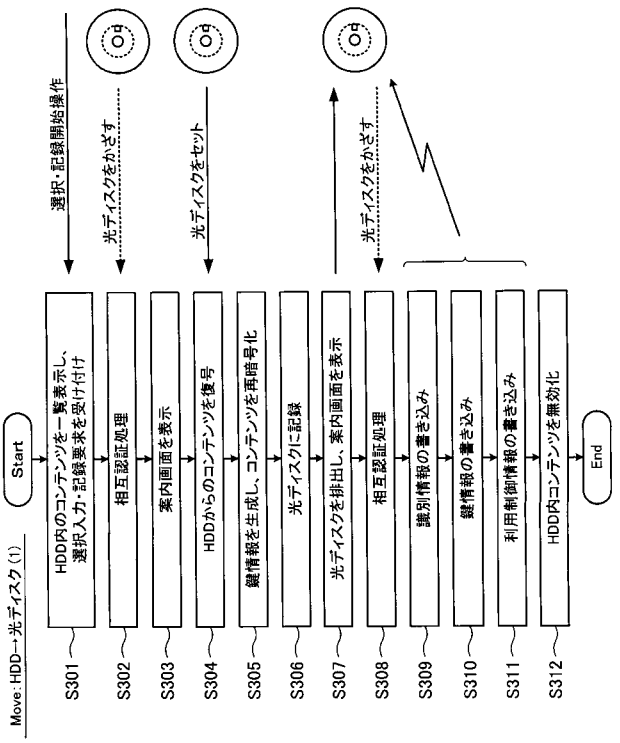
【図７】


RWディスク
データ領域
コンテンツファイル(暗号化)
ファイルA
ファイルB
ファイルC
ICチップ
識別情報(ファイル名)
コンテンツ"A"
コンテンツ"B"
コンテンツ"C"
鍵情報
Key-A
Key-B
Key-C
利用制御情報
利用可/不可
利用可/不可
利用可/不可
認証用情報
認証鍵 Kc
読み出し＝可、 書き換え＝認証下で可
読み出し＝認証下で可、書き換え＝認証下で可
読み出し＝不可、書き換え＝不可

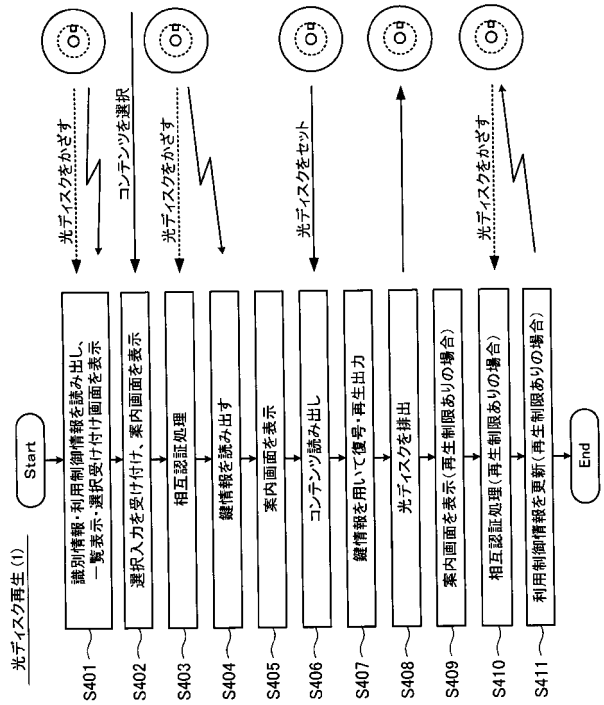
【図８】


光ディスクへ直接記録(1)
Start
記録要求を受け付け
相互認証処理
案内画面を表示
放送コンテンツを伸張復号化して出力
鍵情報を生成し、コンテンツを暗号化
光ディスクに記録
光ディスクを排出し、案内画面を表示
相互認証処理
識別情報の書き込み
鍵情報の書き込み
利用制御情報の書き込み
End
光ディスクをかざす
光ディスクをセット
記録開始操作
記録停止操作
光ディスクをかざす
S201
S202
S203
S204
S205
S206
S207
S208
S209
S210
S211

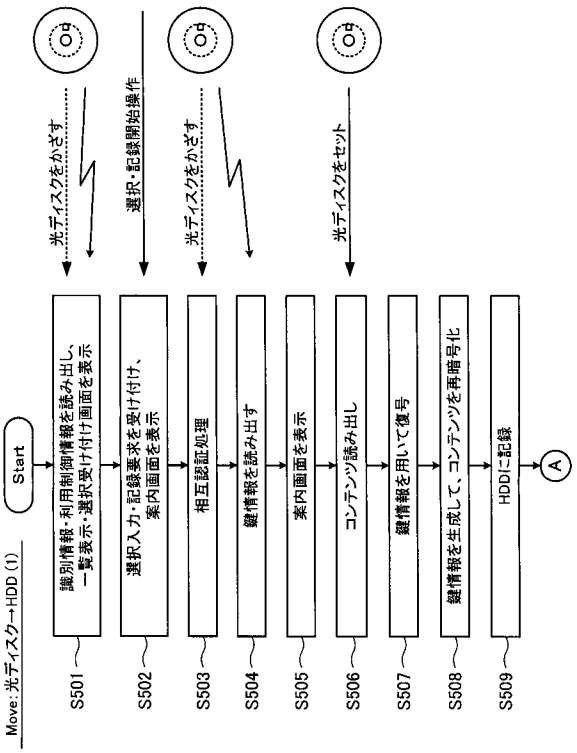
【図９】


Move:HDD→光ディスク(1)
Start
HDD内のコンテンツを一覧表示し、選択入力・記録要求を受け付け
選択・記録開始操作
相互認証処理
光ディスクをかざす
案内画面を表示
光ディスクをセット
HDDからのコンテンツを復号
鍵情報を生成し、コンテンツを再暗号化
光ディスクに記録
光ディスクを排出し、案内画面を表示
光ディスクをかざす
相互認証処理
識別情報の書き込み
鍵情報の書き込み
利用制御情報の書き込み
HDD内コンテンツを無効化
End
S301
S302
S303
S304
S305
S306
S307
S308
S309
S310
S311
S312

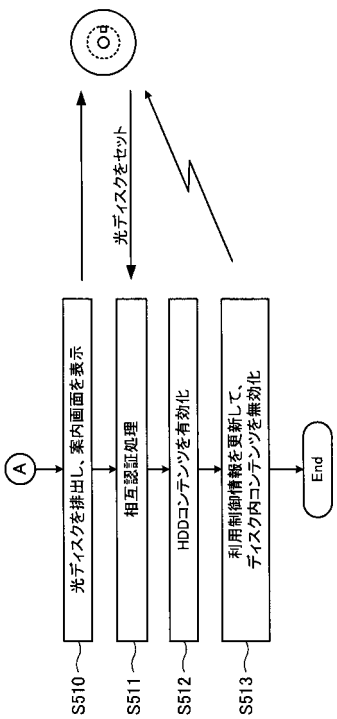
【図１０】


光ディスク再生(1)
Start
識別情報・利用制御情報を読み出し、一覧表示・選択受け付け画面を表示
光ディスクをかざす
選択入力を受け付け、案内画面を表示
コンテンツを選択
相互認証処理
光ディスクをかざす
鍵情報を読み出す
案内画面を表示
光ディスクをセット
コンテンツ読み出し
鍵情報を用いて復号・再生出力
光ディスクを排出
案内画面を表示(再生制限ありの場合)
光ディスクをかざす
相互認証処理(再生制限ありの場合)
利用制御情報を更新(再生制限ありの場合)
End
S401
S402
S403
S404
S405
S406
S407
S408
S409
S410
S411

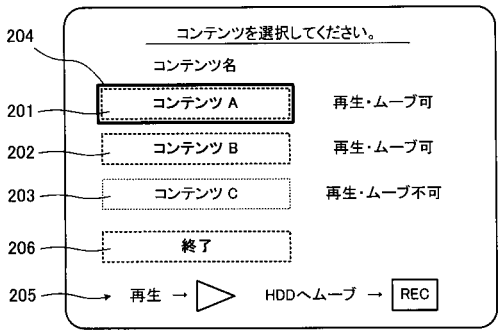
【図１１】



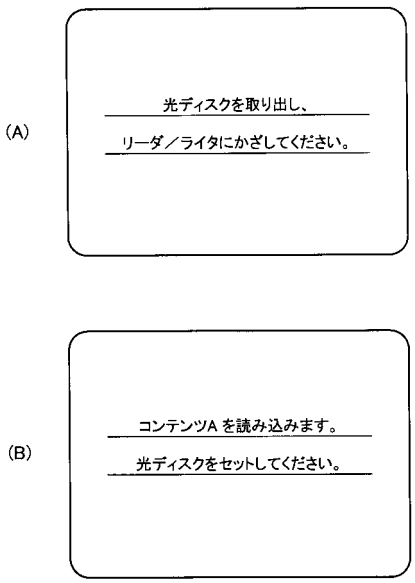

【図１２】



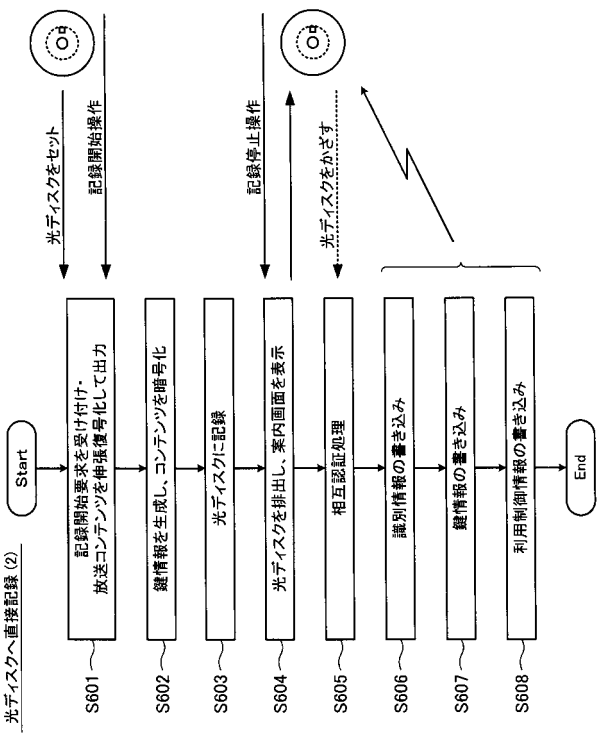

【図１３】



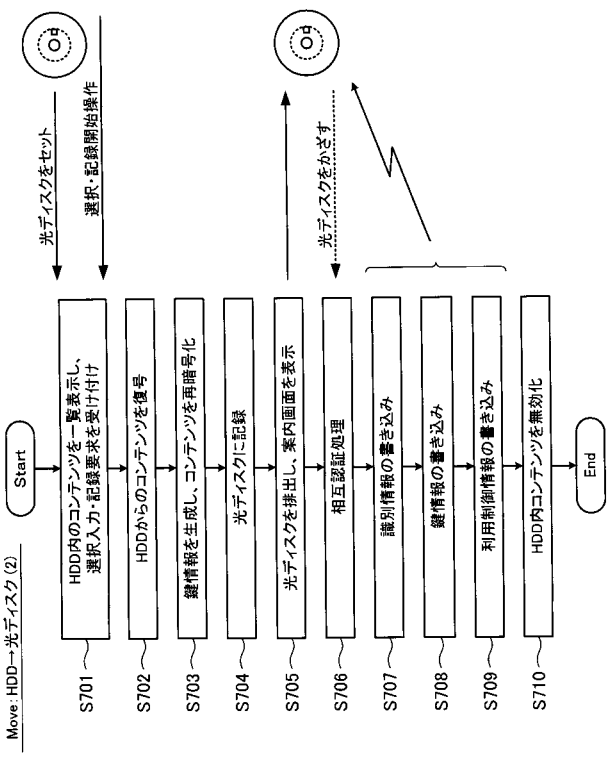

【図１４】



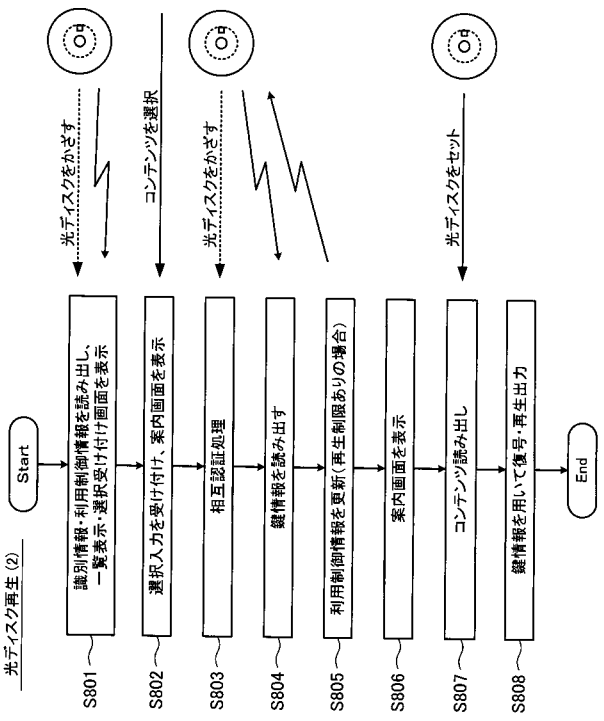
【図１５】



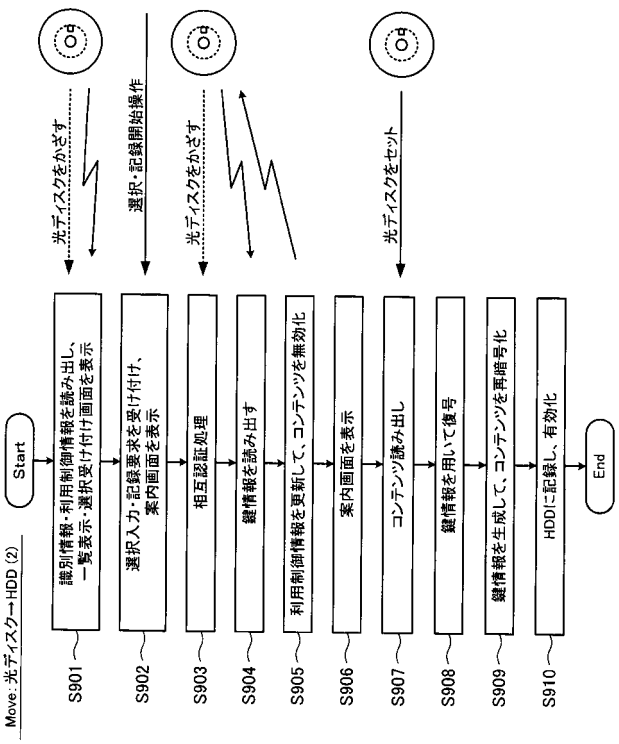

【図１６】



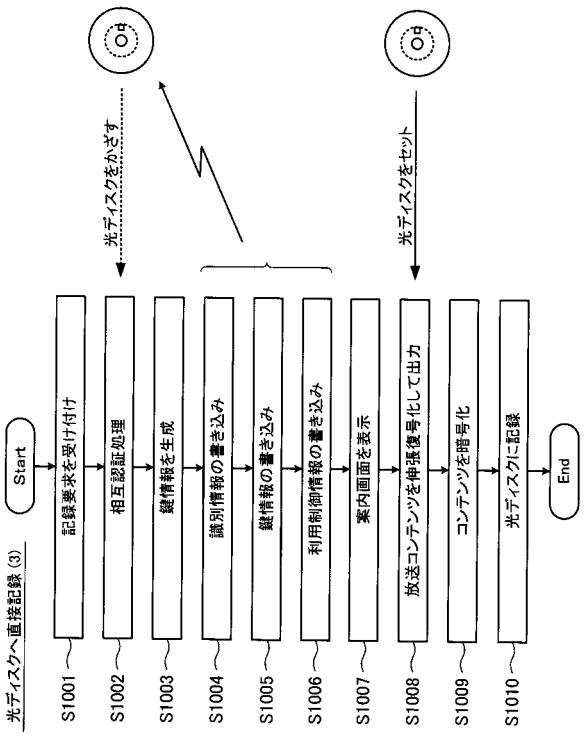

【図１７】



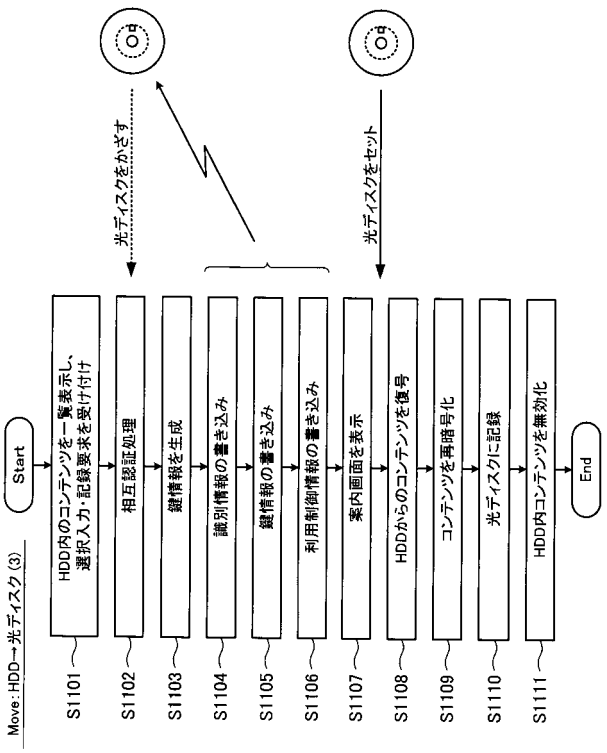

【図１８】



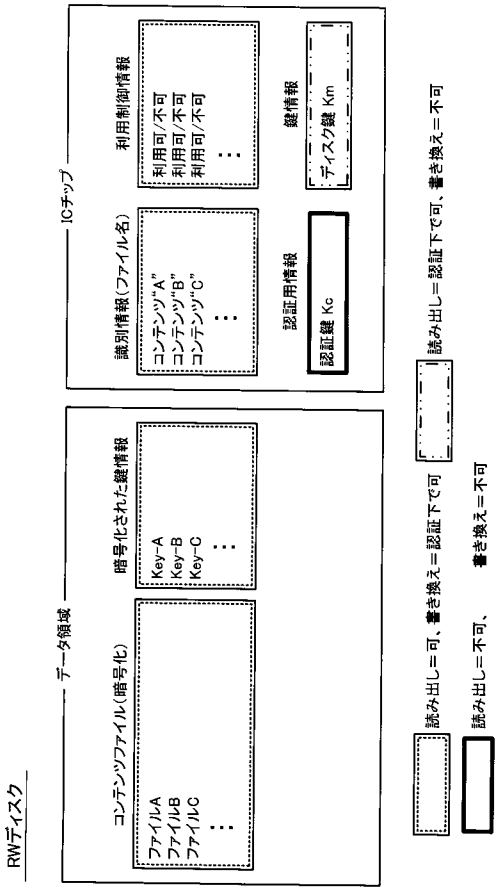
【図１９】



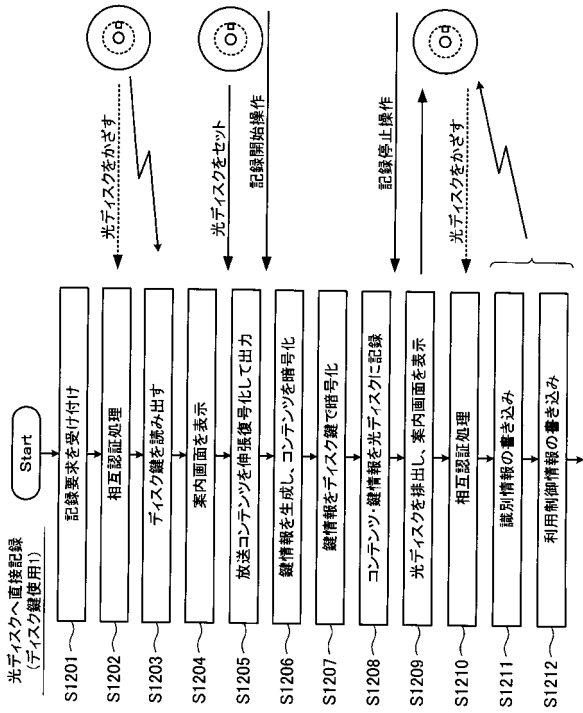

【図２０】



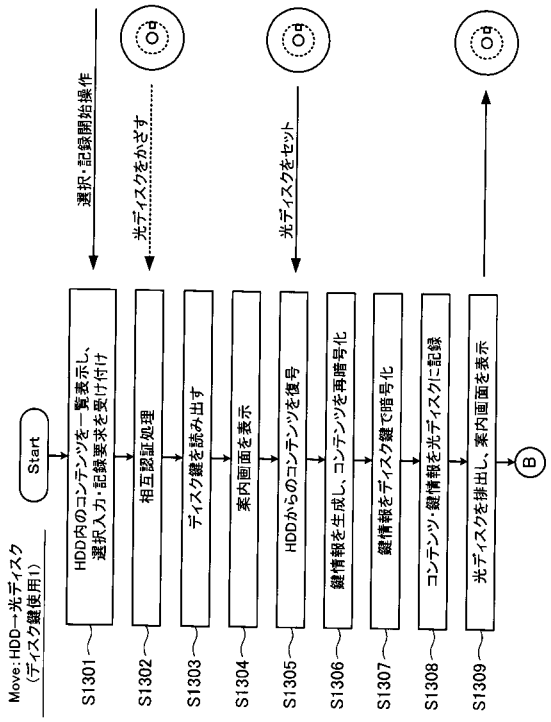

【図２１】



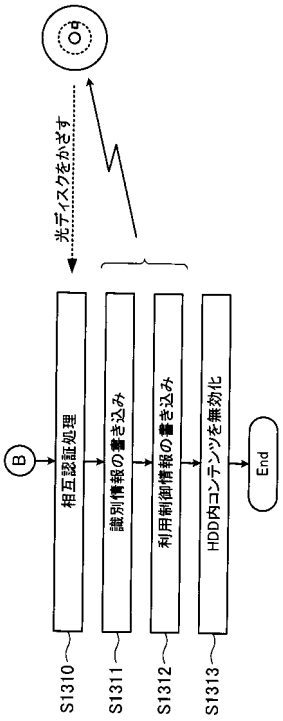

【図２２】



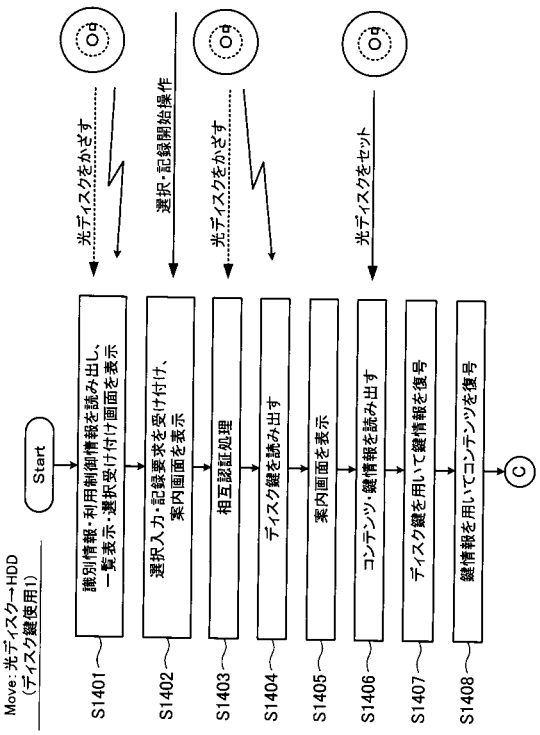
【図２３】



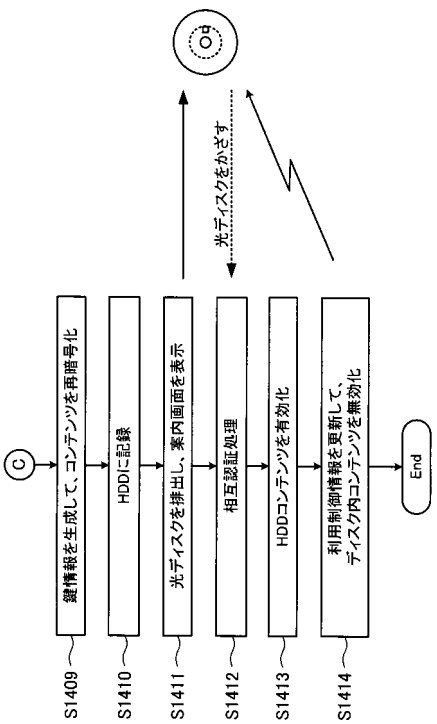

【図２４】



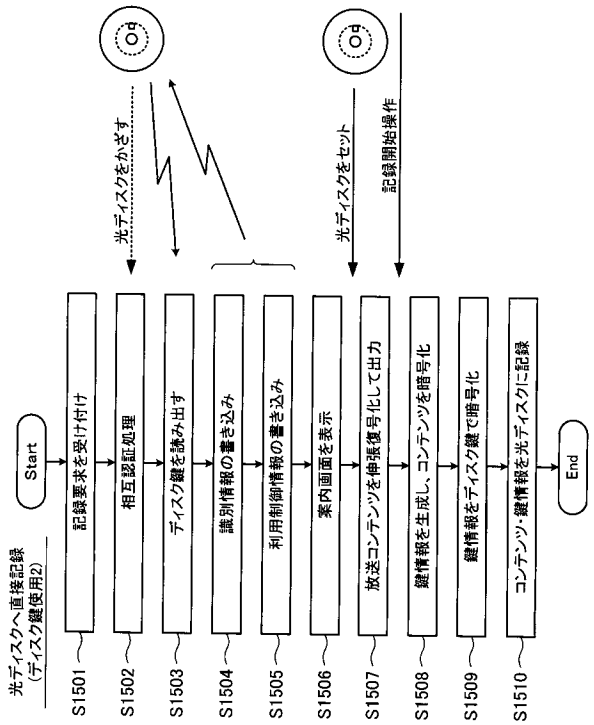

【図２５】



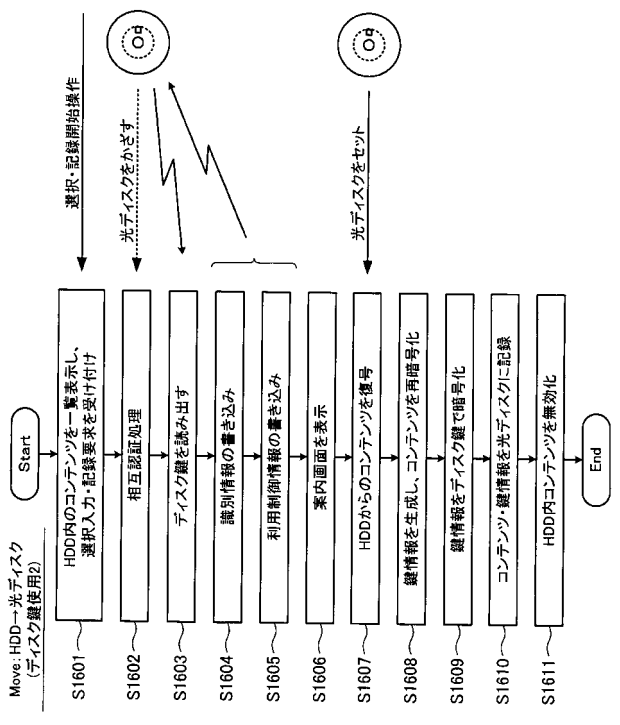

【図２６】



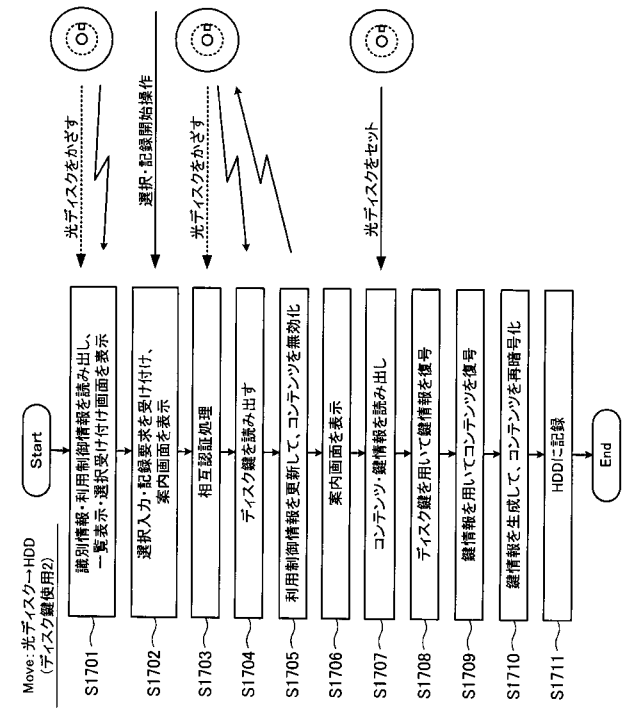
【図２７】



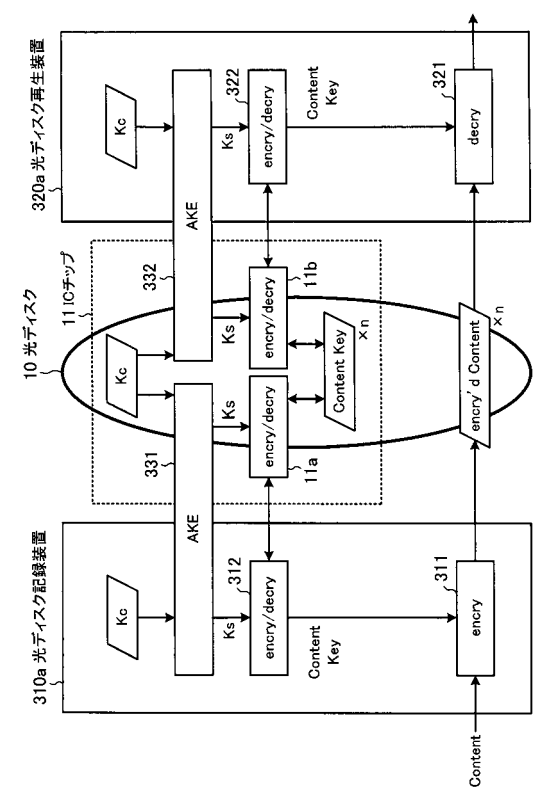

【図２８】



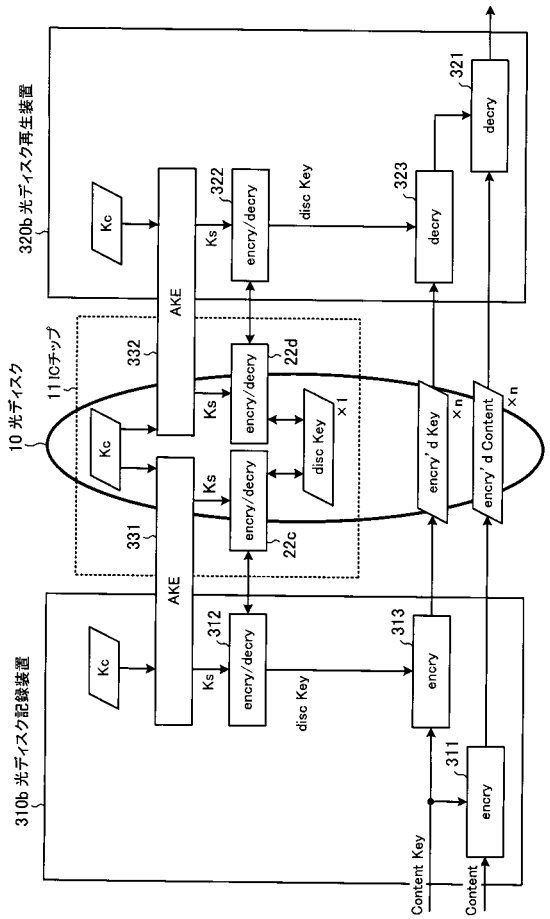

【図２９】



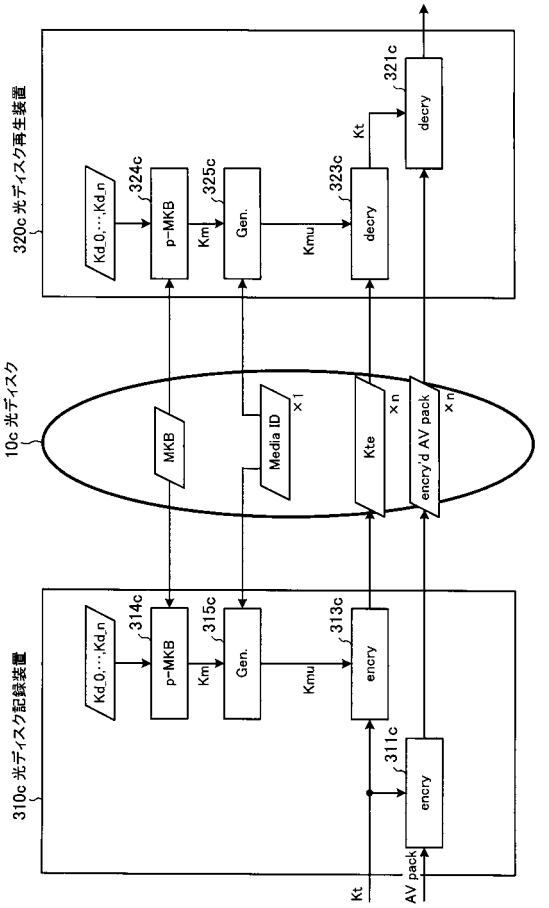

【図３０】



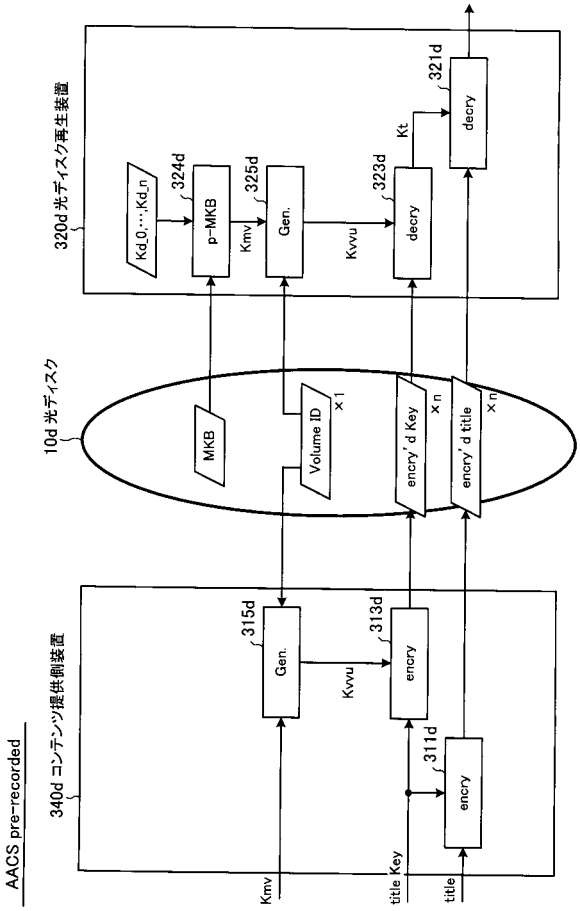
【図３１】



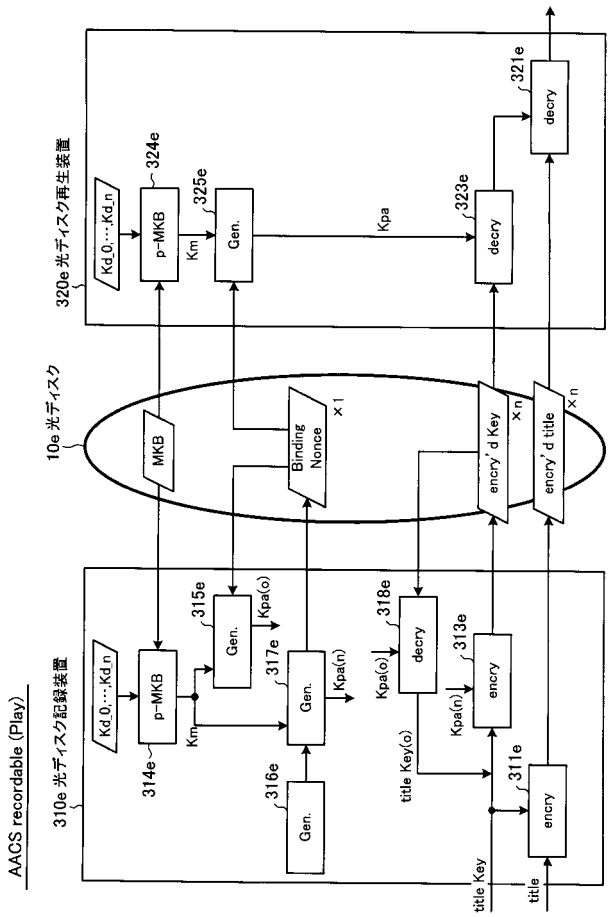

【図３２】



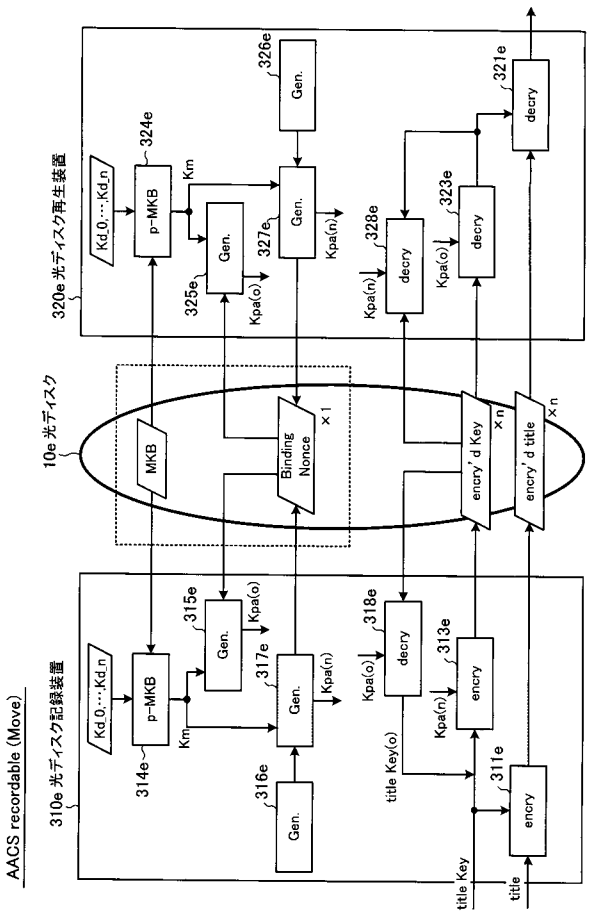

【図３３】



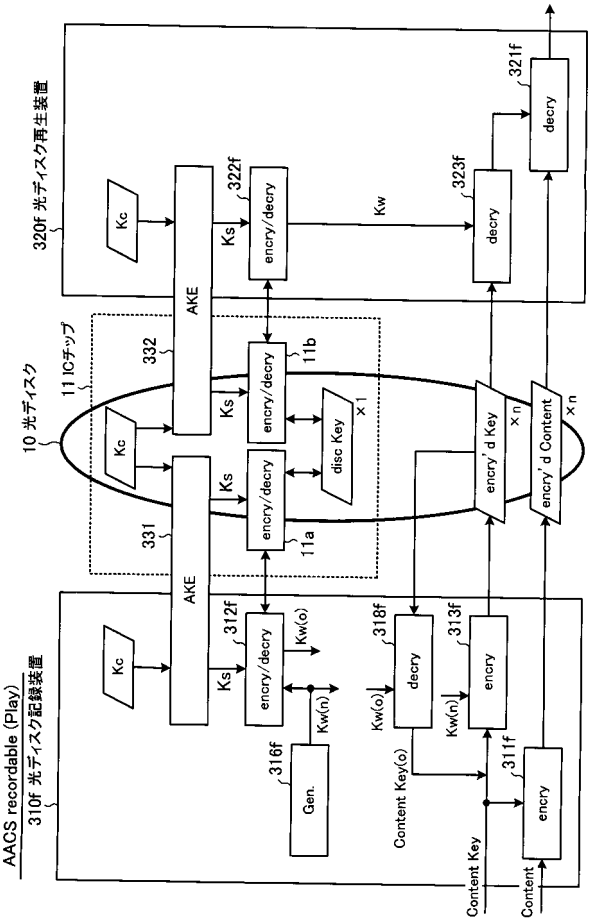

【図３４】



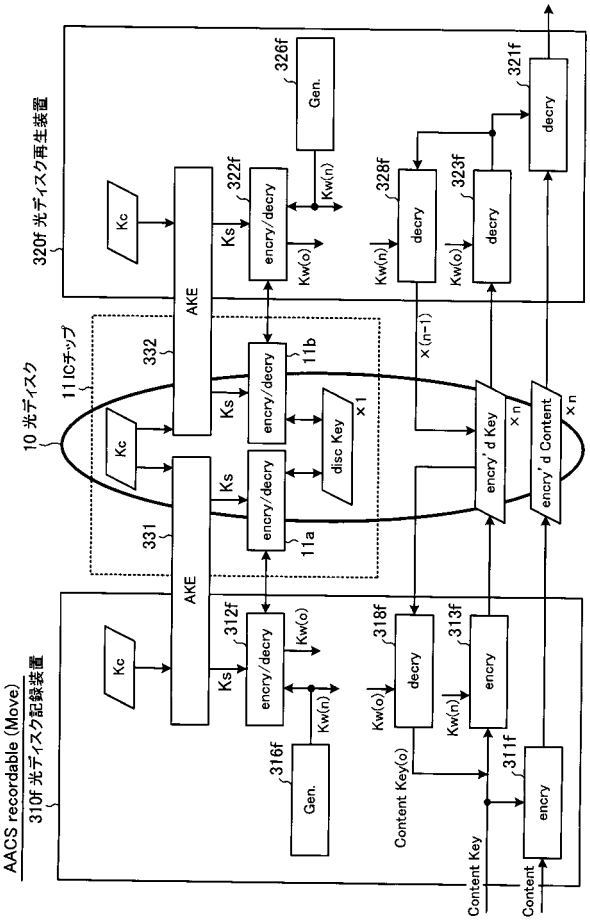
【図３５】



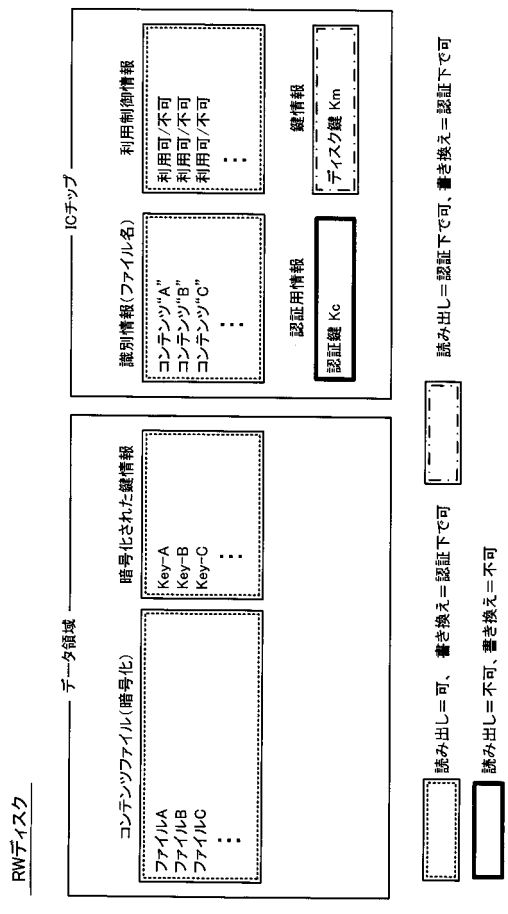

【図３６】



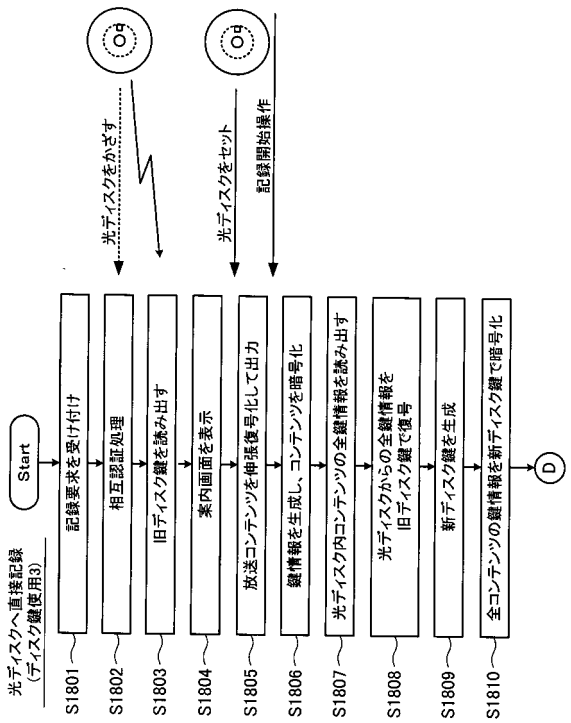

【図３７】



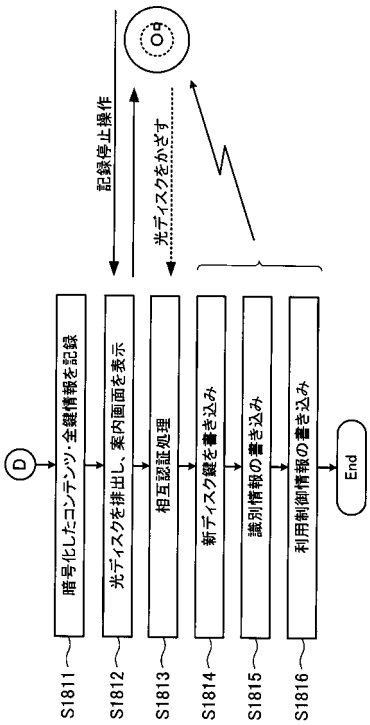

【図３８】



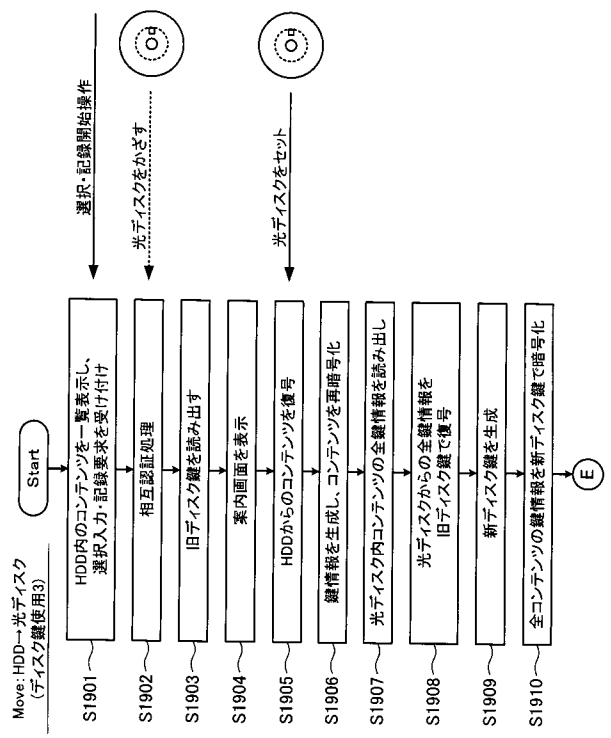
【図３９】



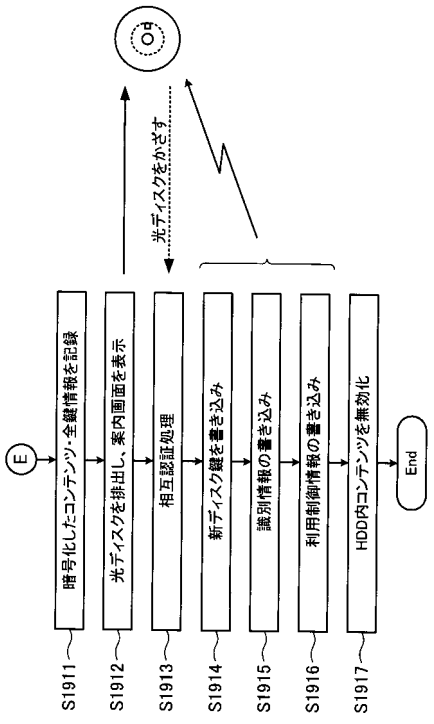

【図４０】



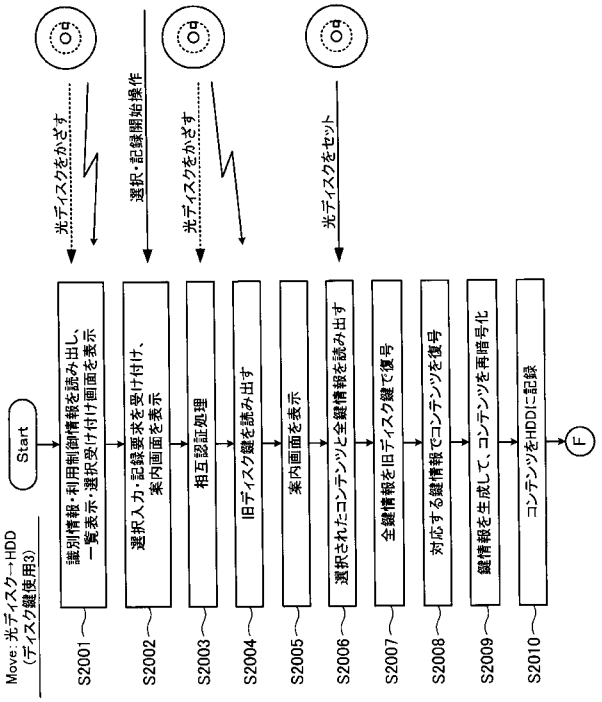

【図４１】



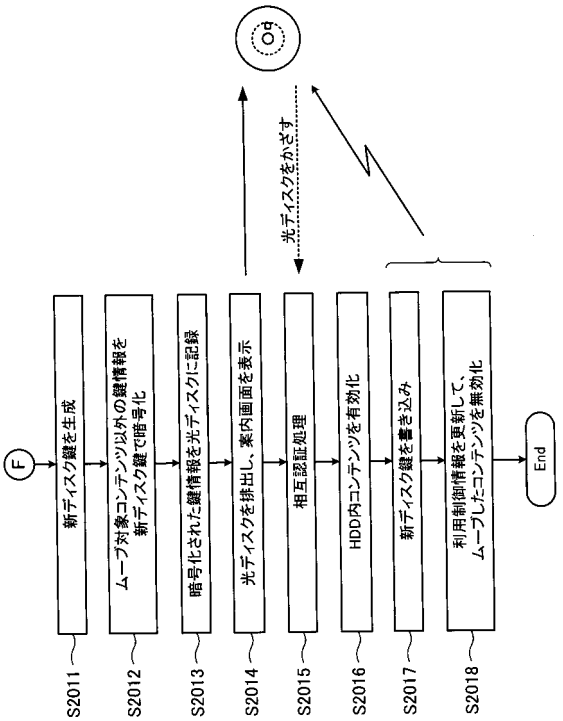

【図４２】



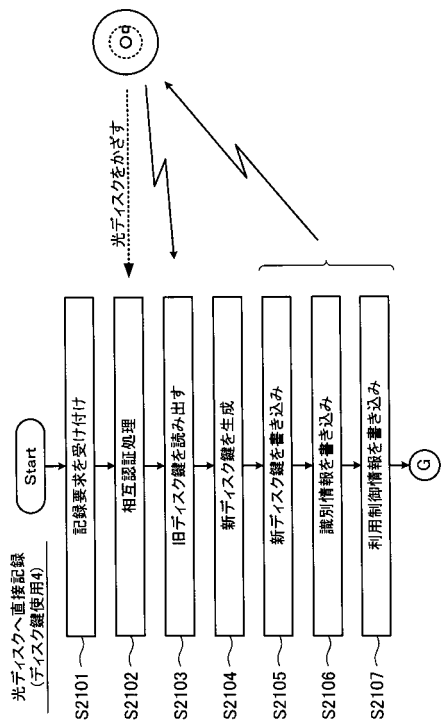
【図４３】



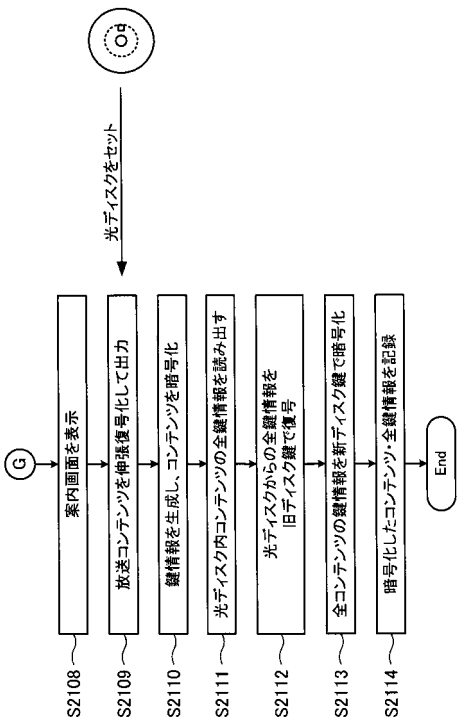

【図４４】



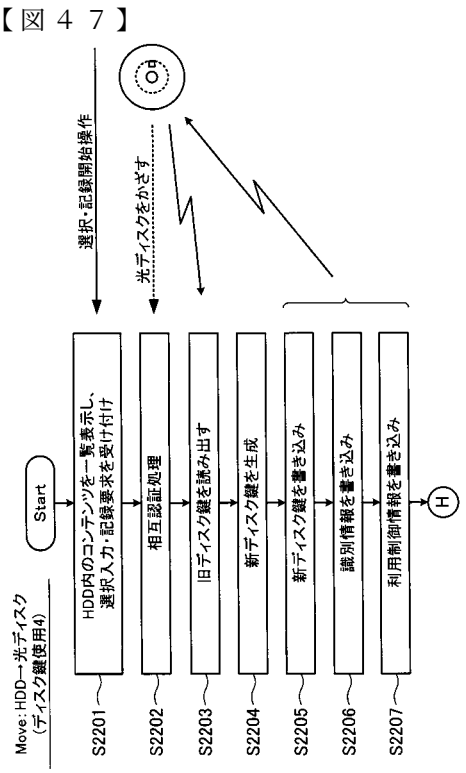

【図４５】



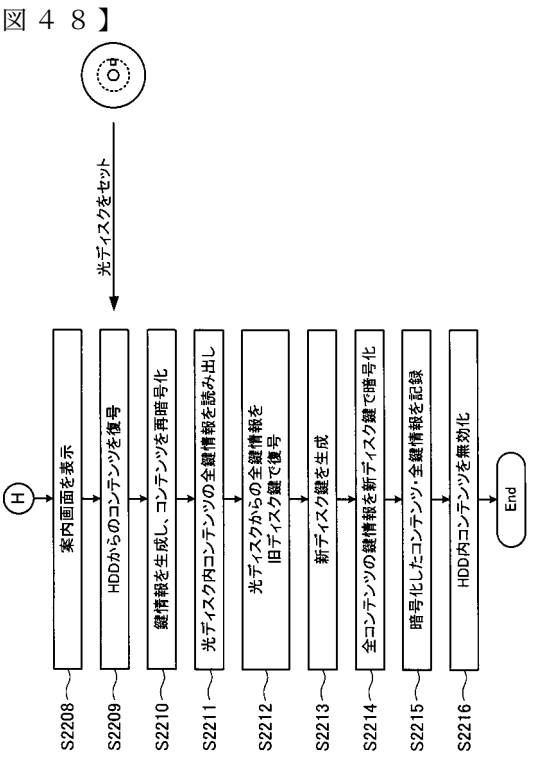

【図４６】



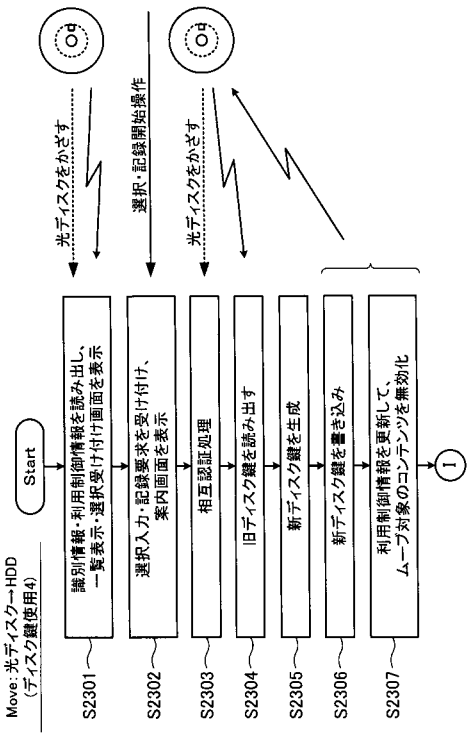
【図４７】



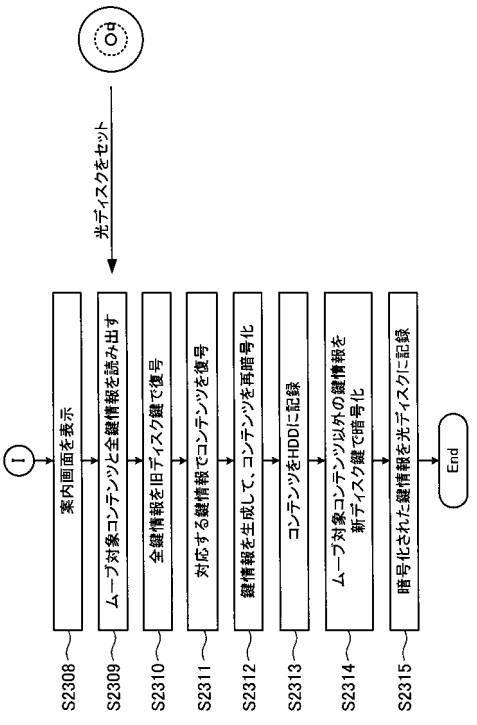

【図４８】



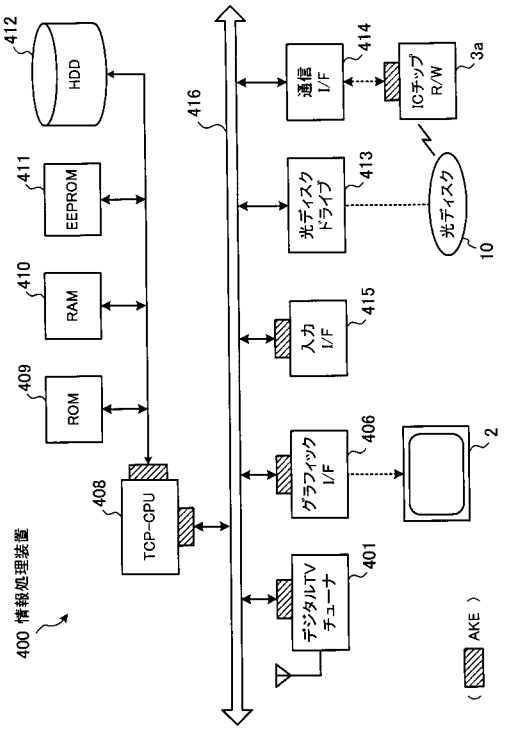

【図４９】




【図５０】



【図５１】


400 情報処理装置
412
HDD
411
EEPROM
410
RAM
409
ROM
408
TCP-CPU
416
通信 I/F
414
ICチップ R/W
3a
光ディスク ドライブ
413
光ディスク
10
入力 I/F
415
グラフィック I/F
406
2
デジタルTV チューナ
401
AKE

フロントページの続き

| (51)Int.Cl. | FI | | テーマコード（参考） |
|---|---|---|---|
| | Ｇ０６Ｋ 17/00 | Ｌ | |
| | Ｇ０６Ｋ 17/00 | Ｓ | |
| | Ｈ０４Ｌ 9/00 | ６７３Ｅ | |
| | Ｈ０４Ｌ 9/00 | ６０１Ｂ | |
| | Ｈ０４Ｌ 9/00 | ６０１Ｅ | |