(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2005-242972
(P2005-242972A)
(43)公開日　平成17年9月8日(2005.9.8)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	540C	5B017
G06F 12/00	G06F 12/14	530E	5B082
G11B 20/10	G06F 12/14	560C	5C053
G11B 20/12	G06F 12/00	537H	5D044
G11B 27/00	G11B 20/10	H	5D110

審査請求 未請求　請求項の数 65　ＯＬ　（全 75 頁）　最終頁に続く

(21)出願番号　特願2004-123100 (P2004-123100)
(22)出願日　平成16年4月19日 (2004.4.19)
(31)優先権主張番号　特願2003-376789 (P2003-376789)
(32)優先日　平成15年11月6日 (2003.11.6)
(33)優先権主張国　日本国 (JP)
(31)優先権主張番号　特願2004-22638 (P2004-22638)
(32)優先日　平成16年1月30日 (2004.1.30)
(33)優先権主張国　日本国 (JP)

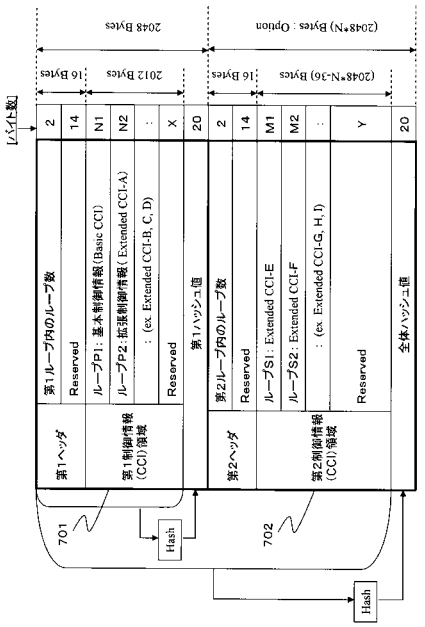
（特許庁注：以下のものは登録商標）
１．ＪＡＶＡ
２．イーサネット

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　高島　芳和
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)　5B017 AA03　AA08　BA07　CA09　CA16
5B082 EA11
5C053 FA13　FA23　GB06　JA30
最終頁に続く

(54)【発明の名称】情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】　ユニット単位に区分したコンテンツ毎の利用管理およびコンテンツ利用制御情報の格納、利用をセキュアにかつ効率的に実行可能とした構成を提供する。
【解決手段】　コンテンツ管理ユニットに区分されたコンテンツに対応するコンテンツ利用制御情報を、ユニットに対応するユニット鍵による暗号化データとするとともに、コンテンツ利用制御情報を含むデータに対応する改ざん検証用データを設定して記録する構成とした。本構成により、コンテンツ利用制御情報の漏洩や改ざんを防止することができ、よりセキュリティレベルの高いコンテンツ利用管理が実現される。
【選択図】　図２７



【特許請求の範囲】
【請求項１】
利用管理対象コンテンツを記録した情報記録媒体であり、
特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツと、前記ＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツを記録データとして格納するとともに、
前記メインコンテンツおよび前記サブコンテンツの構成データをコンテンツ管理ユニットとして設定し、
該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納した構成を有することを特徴とする情報記録媒体。
【請求項２】
前記ＡＶフォーマットは、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットであり、
前記メインコンテンツはＢｌｕ－ｒａｙディスクＲＯＭフォーマットに従った階層データ構成を持つ記録データであることを特徴とする請求項１に記載の情報記録媒体。
【請求項３】
前記サブコンテンツは、１以上のデータファイルを含むデータグループの集合であり、前記コンテンツ管理ユニットは、前記データグループを単位として設定され、
前記情報記録媒体は、
コンテンツ管理ユニットに対応するデータグループの構成ファイルのパス識別情報をデータグループ管理情報として格納した構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項４】
前記サブコンテンツは、１以上のデータファイルを含むデータグループの集合であり、前記コンテンツ管理ユニットは、前記データグループを単位として設定され、
前記情報記録媒体は、
前記データグループを個別フォルダとして設定したディレクトリ構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項５】
前記情報記録媒体は、
コンテンツ管理ユニットに対応するデータグループの個別フォルダの識別情報をデータグループ管理情報として格納した構成を有することを特徴とする請求項４に記載の情報記録媒体。
【請求項６】
前記情報記録媒体は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報を各コンテンツ管理ユニットに対応するユニット鍵によって暗号化したデータとして格納した構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項７】
前記情報記録媒体は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報を、改ざん防止処理構成を持つデータ構成として格納した構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項８】
前記情報記録媒体は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報と、該コンテンツ利用制御情報に基づくハッシュ値とを対応付けたデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して格納した構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項９】

前記情報記録媒体は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報の繰り返しデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して格納した構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項１０】
前記情報記録媒体は、
情報記録媒体のドライブ装着に基づいて再生されるコンテンツとしてのファーストプレイバック・コンテンツを格納し、該ファーストプレイバック・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納した構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項１１】
前記情報記録媒体は、
メニュー表示機能実行に基づいて再生されるコンテンツとしてのトップメニュー・コンテンツを格納し、該トップメニュー・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納した構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項１２】
前記情報記録媒体は、さらに、
コンテンツ管理ユニットと各インデックスとの対応情報、およびユニット鍵の生成に用いる乱数情報を定義したデータファイルを格納した構成を有することを特徴とする請求項１に記載の情報記録媒体。
【請求項１３】
利用管理対象コンテンツを記録する情報処理装置であり、
特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツ、および前記ＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツの構成データをコンテンツ管理ユニットとして設定し、
該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして情報記録媒体に格納する処理を実行する構成を有することを特徴とする情報処理装置。
【請求項１４】
前記ＡＶフォーマットは、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットであり、
前記情報処理装置は、
前記メインコンテンツを、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットに従った階層データ構成を持つ記録データとして情報記録媒体に格納する処理を実行する構成であることを特徴とする請求項１３に記載の情報処理装置。
【請求項１５】
前記情報処理装置は、
前記コンテンツ管理ユニットを、前記サブコンテンツに含まれる１以上のデータファイルを含むデータグループの集合に対応付けて設定し、
コンテンツ管理ユニットに対応するデータグループの構成ファイルのパス識別情報をデータグループ管理情報として情報記録媒体に格納する処理を実行する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項１６】
前記情報処理装置は、
前記コンテンツ管理ユニットを、前記サブコンテンツに含まれる１以上のデータファイルを含むデータグループの集合に対応付けて設定し、
前記データグループを個別フォルダとして設定したディレクトリ構成に基づいて、前記サブコンテンツに含まれる１以上のデータファイルを情報記録媒体に格納する処理を実行

する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項１７】
前記情報処理装置は、
コンテンツ管理ユニットに対応するデータグループの個別フォルダの識別情報をデータグループ管理情報として情報記録媒体に格納する処理を実行する構成を有することを特徴とする請求項１６に記載の情報処理装置。
【請求項１８】
前記情報処理装置は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報を各コンテンツ管理ユニットに対応するユニット鍵によって暗号化したデータとして情報記録媒体に格納する処理を実行する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項１９】
前記情報処理装置は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報を、改ざん防止処理構成を持つデータ構成として情報記録媒体に格納する処理を実行する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項２０】
前記情報処理装置は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報と、該コンテンツ利用制御情報に基づくハッシュ値とを対応付けたデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して情報記録媒体に格納する処理を実行する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項２１】
前記情報処理装置は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報の繰り返しデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して情報記録媒体に格納する処理を実行する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項２２】
前記情報処理装置は、
情報記録媒体のドライブ装着に基づいて再生されるコンテンツとしてのファーストプレイバック・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納する処理を実行する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項２３】
前記情報処理装置は、
メニュー表示機能実行に基づいて再生されるコンテンツとしてのトップメニュー・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納する処理を実行する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項２４】
前記情報処理装置は、さらに、
コンテンツ管理ユニットと各インデックスとの対応情報、およびユニット鍵の生成に用いる乱数情報を定義したデータファイルを格納する処理を実行する構成を有することを特徴とする請求項１３に記載の情報処理装置。
【請求項２５】
利用管理対象コンテンツの再生処理を実行する情報処理装置であり、
情報記録媒体に格納されたコンテンツ管理ユニットに対応する暗号化コンテンツ利用制御情報を取得し、

コンテンツ管理ユニットに対応して設定されたユニット鍵を適用した復号処理、および改ざん検証処理を実行し、改ざんの無いことの確認を条件として、該コンテンツ利用制御情報に基づくコンテンツ利用処理を実行する構成を有することを特徴とする情報処理装置。

【請求項２６】

利用管理対象コンテンツを記録する情報処理方法であり、

特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツ、および前記ＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツの構成データをコンテンツ管理ユニットとして設定するコンテンツ管理ユニット設定ステップと、

コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして情報記録媒体に格納するデータ格納ステップと、

を有することを特徴とする情報処理方法。

【請求項２７】

前記ＡＶフォーマットは、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットであり、

前記データ格納ステップは、

前記メインコンテンツを、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットに従った階層データ構成を持つ記録データとして情報記録媒体に格納するステップであることを特徴とする請求項２６に記載の情報処理方法。

【請求項２８】

前記情報処理方法は、さらに、

前記コンテンツ管理ユニットを、前記サブコンテンツに含まれる１以上のデータファイルを含むデータグループの集合に対応付けて設定するステップと、

コンテンツ管理ユニットに対応するデータグループの構成ファイルのパス識別情報をデータグループ管理情報として情報記録媒体に格納するステップと、

を有することを特徴とする請求項２６に記載の情報処理方法。

【請求項２９】

前記情報処理方法は、さらに、

前記コンテンツ管理ユニットを、前記サブコンテンツに含まれる１以上のデータファイルを含むデータグループの集合に対応付けて設定するステップと、

前記データグループを個別フォルダとして設定したディレクトリ構成に基づいて、前記サブコンテンツに含まれる１以上のデータファイルを情報記録媒体に格納するステップと、

を有することを特徴とする請求項２６に記載の情報処理方法。

【請求項３０】

前記情報処理方法は、さらに、

コンテンツ管理ユニットに対応するデータグループの個別フォルダの識別情報をデータグループ管理情報として情報記録媒体に格納する処理を実行するステップ、

を有することを特徴とする請求項２９に記載の情報処理方法。

【請求項３１】

前記情報処理方法は、さらに、

コンテンツ管理ユニットに対応するコンテンツ利用制御情報を各コンテンツ管理ユニットに対応するユニット鍵によって暗号化したデータとして情報記録媒体に格納するステップ、

を有することを特徴とする請求項２６に記載の情報処理方法。

【請求項３２】

前記情報処理方法は、さらに、

コンテンツ管理ユニットに対応するコンテンツ利用制御情報を、改ざん防止処理構成を持つデータ構成として情報記録媒体に格納する処理を実行するステップ、

を有することを特徴とする請求項２６に記載の情報処理方法。
【請求項３３】
前記情報処理方法は、さらに、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報と、該コンテンツ利用制御情報に基づくハッシュ値とを対応付けたデータを、各コンテンツ管理ユニット、
を有することを特徴とする請求項２６に記載の情報処理方法。
【請求項３４】
前記情報処理方法は、
コンテンツ管理ユニットに対応するコンテンツ利用制御情報の繰り返しデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して情報記録媒体に格納する処理を実行するステップ、
を有することを特徴とする請求項２６に記載の情報処理方法。
【請求項３５】
前記情報処理方法は、
情報記録媒体のドライブ装着に基づいて再生されるコンテンツとしてのファーストプレイバック・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納する処理を実行することを特徴とする請求項２６に記載の情報処理方法。
【請求項３６】
前記情報処理方法は、
メニュー表示機能実行に基づいて再生されるコンテンツとしてのトップメニュー・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納する処理を実行することを特徴とする請求項２６に記載の情報処理方法。
【請求項３７】
前記情報処理方法は、さらに、
コンテンツ管理ユニットと各インデックスとの対応情報、およびユニット鍵の生成に用いる乱数情報を定義したデータファイルを格納する処理を実行することを特徴とする請求項２６に記載の情報処理方法。
【請求項３８】
利用管理対象コンテンツの再生処理を実行する情報処理方法であり、
情報記録媒体に格納されたコンテンツ管理ユニットに対応する暗号化コンテンツ利用制御情報を取得するステップと、
コンテンツ管理ユニットに対応して設定されたユニット鍵を適用した復号処理、および改ざん検証処理を実行するステップと、
改ざんの無いことの確認を条件として、該コンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップと、
を有することを特徴とする情報処理方法。
【請求項３９】
利用管理対象コンテンツを記録するコンピュータ・プログラムであり、
特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツ、および前記ＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツの構成データをコンテンツ管理ユニットとして設定するコンテンツ管理ユニット設定ステップと、
コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして情報記録媒体に格納するデータ格納ステップと、
を有することを特徴とするコンピュータ・プログラム。

【請求項４０】
利用管理対象コンテンツの再生処理を実行するコンピュータ・プログラムであり、
情報記録媒体に格納されたコンテンツ管理ユニットに対応する暗号化コンテンツ利用制御情報を取得するステップと、
コンテンツ管理ユニットに対応して設定されたユニット鍵を適用した復号処理、および改ざん検証処理を実行するステップと、
改ざんの無いことの確認を条件として、該コンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップと、
を有することを特徴とするコンピュータ・プログラム。
【請求項４１】
情報記録媒体であり、
コンテンツ管理ユニット単位に区分され、各コンテンツ管理ユニットに対応して設定されたユニット鍵による暗号化データを含む１以上のコンテンツと、
前記コンテンツ管理ユニット各々に対応して設定されたコンテンツ利用制御情報とを格納し、
前記コンテンツ利用制御情報は、
前記コンテンツ管理ユニット各々に対応して設定されたユニット鍵を適用した暗号処理が実行された暗号化データとして格納されているとともに、改ざん検証用データを付加した構成であることを特徴とする情報記録媒体。
【請求項４２】
前記コンテンツ利用制御情報は、
所定データ量からなるブロック単位での暗号化のなされた構成であり、
各ブロックの構成データであるブロックシードと、前記ユニット鍵を適用した暗号処理により生成されるブロック鍵に基づいて暗号化のなされた暗号化ブロックデータとして格納した構成であることを特徴とする請求項４１に記載の情報記録媒体。
【請求項４３】
前記ブロックシードは、コンテンツ利用制御情報を構成しないブロック構成データであることを特徴とする請求項４２に記載の情報記録媒体。
【請求項４４】
前記コンテンツ利用制御情報は、基本制御情報と拡張制御情報の異なるカテゴリの制御情報を含むデータであり、
前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する改ざん検証用データを同一ブロック内に格納した構成を有することを特徴とする請求項４２に記載の情報記録媒体。
【請求項４５】
前記コンテンツ利用制御情報は、基本制御情報と拡張制御情報の異なるカテゴリの制御情報を含むデータであり、
前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する第１の改ざん検証用データを同一ブロック内に格納し、
前記基本制御情報および前記拡張制御情報の全データを含むデータに対する第２の改ざん検証用データを格納した構成を有することを特徴とする請求項４２に記載の情報記録媒体。
【請求項４６】
利用管理対象コンテンツの再生処理を実行する情報処理装置であり、
情報記録媒体に格納されたコンテンツ管理ユニットに対応するコンテンツ利用制御情報を取得し、
コンテンツ管理ユニットに対応して設定されたユニット鍵を適用して、前記コンテンツ利用制御情報を構成する所定データ量単位のブロックデータのブロック単位の復号処理と、ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理とを実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテン

ツ利用処理を実行する構成を有することを特徴とする情報処理装置。
【請求項４７】
前記情報処理装置は、
前記コンテンツ利用制御情報を構成する各ブロックからブロックシードを取得し、該ブロックシードと前記ユニット鍵を適用した暗号処理により生成されるブロック鍵に基づいて、ブロック単位の復号処理を実行する構成であることを特徴とする請求項４６に記載の情報処理装置。
【請求項４８】
前記情報処理装置は、
前記コンテンツ利用制御情報を構成する複数のブロックデータから基本制御情報を含む１つのブロックデータのみを選択し、該選択した基本制御情報格納ブロックについての復号処理と、ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理とを実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行する構成を有することを特徴とする請求項４６に記載の情報処理装置。
【請求項４９】
前記情報処理装置は、
前記コンテンツ利用制御情報を構成する複数のブロックデータから基本制御情報および拡張制御情報を含む複数のブロックデータを選択し、該選択した複数ブロックについてのブロック単位の復号処理を実行し、複数のブロックデータに含まれるデータに対する検証用データに基づく改ざん検証処理を実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行する構成を有することを特徴とする請求項４６に記載の情報処理装置。
【請求項５０】
情報記録媒体に対するデータ記録処理を実行する情報処理装置であり、
個別の利用管理制御を行うために設定されたコンテンツ管理ユニット各々に対応するコンテンツ利用制御情報に対する改ざん検証用データを生成し、前記コンテンツ管理ユニット各々に対応して設定されたユニット鍵を適用した暗号化処理を実行して暗号化データを生成し、前記改ざん検証用データを含む暗号化コンテンツ利用制御情報の生成および記録処理を実行する構成を有することを特徴とする情報処理装置。
【請求項５１】
前記情報処理装置は、
前記コンテンツ利用制御情報を、所定データ量からなるブロック単位に区分し、各ブロックの構成データから抽出したブロックシードと、前記ユニット鍵を適用した暗号処理によりブロック鍵を生成し、該ブロック鍵によるブロック暗号化データを生成して情報記録媒体に記録する処理を実行する構成であることを特徴とする請求項５０に記載の情報処理装置。
【請求項５２】
前記情報処理装置は、
前記ブロックシードを、コンテンツ利用制御情報を構成しないブロック構成データから抽出する構成であることを特徴とする請求項５１に記載の情報処理装置。
【請求項５３】
前記情報処理装置は、
前記コンテンツ利用制御情報を、基本制御情報と拡張制御情報の異なるカテゴリに区分し、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する改ざん検証用データを生成し、同一ブロック内に格納して記録する処理を実行する構成であることを特徴とする請求項５１に記載の情報処理装置。
【請求項５４】
前記情報処理装置は、
前記コンテンツ利用制御情報を、基本制御情報と拡張制御情報の異なるカテゴリに区分

し、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する第１の改ざん検証用データを生成し、同一ブロック内に格納して記録し、
前記基本制御情報および前記拡張制御情報の全データを含むデータに対する第２の改ざん検証用データを生成し、記録する構成であること特徴とする請求項５１に記載の情報処理装置。
【請求項５５】
利用管理対象コンテンツの再生処理を実行する情報処理方法であり、
情報記録媒体に格納されたコンテンツ管理ユニットに対応するコンテンツ利用制御情報を取得するステップと、
コンテンツ管理ユニットに対応して設定されたユニット鍵を適用して、前記コンテンツ利用制御情報を構成する所定データ量単位のブロックデータのブロック単位の復号処理を実行する復号ステップと、
ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理を実行するステップと、
改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップと、
を有することを特徴とする情報処理方法。
【請求項５６】
前記復号ステップは、
前記コンテンツ利用制御情報を構成する各ブロックからブロックシードを取得し、該ブロックシードと前記ユニット鍵を適用した暗号処理により生成されるブロック鍵に基づいて、ブロック単位の復号処理を実行するステップであることを特徴とする請求項５５に記載の情報処理方法。
【請求項５７】
前記情報処理方法は、さらに、
前記コンテンツ利用制御情報を構成する複数のブロックデータから基本制御情報を含む１つのブロックデータのみを選択するステップを有し、
選択した基本制御情報格納ブロックについての復号処理と、ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理とを実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップを含むことを特徴とする請求項５５に記載の情報処理方法。
【請求項５８】
前記情報処理方法は、さらに、
前記コンテンツ利用制御情報を構成する複数のブロックデータから基本制御情報および拡張制御情報を含む複数のブロックデータを選択するステップを有し、
選択した複数ブロックについてのブロック単位の復号処理を実行し、複数のブロックデータに含まれるデータに対する検証用データに基づく改ざん検証処理を実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップを含むことを特徴とする請求項５５に記載の情報処理方法。
【請求項５９】
情報記録媒体に対するデータ記録処理を実行する情報処理方法であり、
個別の利用管理制御を行うために設定されたコンテンツ管理ユニット各々に対応するコンテンツ利用制御情報に対する改ざん検証用データを生成するステップと、
前記コンテンツ管理ユニット各々に対応して設定されたユニット鍵を適用した暗号化処理を実行して暗号化データを生成する暗号化処理ステップと、
前記改ざん検証用データを含む暗号化コンテンツ利用制御情報の生成および記録処理を実行するステップと、
を有することを特徴とする情報処理方法。
【請求項６０】
前記情報処理方法は、さらに、

前記コンテンツ利用制御情報を、所定データ量からなるブロック単位に区分し、各ブロックの構成データから抽出したブロックシードと、前記ユニット鍵を適用した暗号処理によりブロック鍵を生成し、該ブロック鍵によるブロック暗号化データを生成して情報記録媒体に記録する処理を実行するステップを含むことを特徴とする請求項５９に記載の情報処理方法。

【請求項６１】

前記情報処理方法において、

前記ブロックシードを、コンテンツ利用制御情報を構成しないブロック構成データから抽出することを特徴とする請求項６０に記載の情報処理方法。

【請求項６２】

前記情報処理方法は、さらに、

前記コンテンツ利用制御情報を、基本制御情報と拡張制御情報の異なるカテゴリに区分し、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する改ざん検証用データを生成し、同一ブロック内に格納して記録する処理を実行するステップを含むことを特徴とする請求項６０に記載の情報処理方法。

【請求項６３】

前記情報処理方法は、さらに、

前記コンテンツ利用制御情報を、基本制御情報と拡張制御情報の異なるカテゴリに区分し、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する第１の改ざん検証用データを生成し、同一ブロック内に格納して記録し、

前記基本制御情報および前記拡張制御情報の全データを含むデータに対する第２の改ざん検証用データを生成し、記録するステップを含むこと特徴とする請求項６０に記載の情報処理方法。

【請求項６４】

利用管理対象コンテンツの再生処理を実行するコンピュータ・プログラムであり、

情報記録媒体に格納されたコンテンツ管理ユニットに対応するコンテンツ利用制御情報を取得するステップと、

コンテンツ管理ユニットに対応して設定されたユニット鍵を適用して、前記コンテンツ利用制御情報を構成する所定データ量単位のブロックデータのブロック単位の復号処理を実行する復号ステップと、

ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理を実行するステップと、

改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップと、

を有することを特徴とするコンピュータ・プログラム。

【請求項６５】

情報記録媒体に対するデータ記録処理を実行するコンピュータ・プログラムであり、

個別の利用管理制御を行うために設定されたコンテンツ管理ユニット各々に対応するコンテンツ利用制御情報に対する改ざん検証用データを生成するステップと、

前記コンテンツ管理ユニット各々に対応して設定されたユニット鍵を適用した暗号化処理を実行して暗号化データを生成する暗号化処理ステップと、

前記改ざん検証用データを含む暗号化コンテンツ利用制御情報の生成および記録処理を実行するステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、コンテンツ利用管理の要求される様々なコンテンツの格納、および細分化されたデータユニット毎の利用管理を実現する情報処理装置、

情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。
【背景技術】
【０００２】
音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）は、記録メディア、例えば、青色レーザを適用したＢｌｕ－ｒａｙディスク、あるいはＤＶＤ(Digital Versatile Disc)、ＭＤ(Mini Disc)、ＣＤ(Compact Disc)にデジタルデータとして格納することができる。特に、青色レーザを利用したＢｌｕ－ｒａｙディスクは、高密度記録可能なディスクであり大容量の映像コンテンツなどを高画質データとして記録することができる。
【０００３】
これら様々な情報記録媒体（記録メディア）にデジタルコンテンツが格納され、ユーザに提供される。ユーザは、所有するＰＣ（Personal Computer）、ディスクプレーヤ等の再生装置においてコンテンツの再生、利用を行う。
【０００４】
音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。
【０００５】
デジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをＣＤ－Ｒ等にコピーした、いわゆる海賊版ディスクの流通や、ＰＣ等のハードディスクに格納したコピーコンテンツの利用が蔓延しているといった問題が発生している。
【０００６】
ＤＶＤ、あるいは近年開発が進んでいる青色レーザを利用した記録媒体等の大容量型記録媒体は、１枚の媒体に例えば映画１本～数本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。
【０００７】
例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステム（Ｃｏｎｔｅｎｔ Ｓｃｒａｍｂｌｅ Ｓｙｓｔｅｍ）が採用されている。コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いる鍵が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。
【０００８】
一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するための鍵を有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、デジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。
【０００９】
一方、昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコン

ピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

【００１０】

このようなネットワーク化が進むことにより、情報記録媒体の格納コンテンツは、ホームネットワークにネットワーク接続された機器からアクセスして利用することが多くなる。上述した、従来の不正コピー防止システムは、例えばライセンスされた１つの再生機においてのみコンテンツ再生を許容する考え方を基本とするものである。従って、ネットワーク接続された機器において、記録媒体を装着した機器、例えばホームサーバあるいはプレーヤに他のネットワーク接続機器、例えばＰＣ、ＴＶなどからアクセスを行い、ネットワークを介してコンテンツを再生する処理についての対応については、十分な考慮がなされてはいなかった。

【００１１】

従来は、記録媒体上に格納された１つのコンテンツの利用を１つの再生装置で実行するといった利用形態が主流であったため、コンテンツあるいは再生装置に対してライセンス等のコンテンツ利用権を設定してコンテンツの利用管理を行うことで、十分であったが、情報記録媒体の大容量化、および家庭内の機器のデジタル化・ネットワーク化が進む現代では、過去の構成とは異なるコンテンツの利用管理構成が必要となってきている。具体的に、以下のような要求が発生している。

【００１２】

（１）記録媒体上に複数のコンテンツを記録し、各コンテンツ毎に異なる利用管理を可能とする構成の実現。

（２）家庭内ネットワーク等、特定のネットワーク内でのコンテンツの利用、すなわちネットワーク接続機器によるコンテンツ再生、あるいはホームサーバに対するコンテンツコピーなどに付いて許容するコンテンツ利用管理構成の実現。

（３）ネットワーク経由でコンテンツ再生に必要な情報、例えばコンテンツの復号に適用する鍵などを安全に、特定ユーザに配布する構成の実現。

上記、（１）～（３）の構成を実現することが求められている。

【発明の開示】

【発明が解決しようとする課題】

【００１３】

本発明は、このような状況に鑑みてなされたものであり、著作権管理など利用管理の要求される様々なコンテンツが格納された情報記録媒体のコンテンツ利用において、記録媒体に格納されたコンテンツの細分化されたデータ毎の著作権管理および利用管理を実現する情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

【００１４】

さらに、コンテンツ管理ユニットに区分されたコンテンツに対応するコンテンツ利用制御情報を、ユニットに対応するユニット鍵による暗号化データとするとともに、コンテンツ利用制御情報を含むデータに対応する改ざん検証用データを設定して記録する構成とすることにより、よりセキュリティレベルの高いコンテンツ利用管理を実現する情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

【課題を解決するための手段】

【００１５】

本発明の第１の側面は、

利用管理対象コンテンツを記録した情報記録媒体であり、

特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコ

ンテンツと、前記ＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツを記録データとして格納するとともに、
前記メインコンテンツおよび前記サブコンテンツの構成データをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納した構成を有することを特徴とする情報記録媒体にある。
【００１６】
さらに、本発明の情報記録媒体の一実施態様において、前記ＡＶフォーマットは、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットであり、前記メインコンテンツはＢｌｕ－ｒａｙディスクＲＯＭフォーマットに従った階層データ構成を持つ記録データであることを特徴とする。
【００１７】
さらに、本発明の情報記録媒体の一実施態様において、前記サブコンテンツは、１以上のデータファイルを含むデータグループの集合であり、前記コンテンツ管理ユニットは、前記データグループを単位として設定され、前記情報記録媒体は、コンテンツ管理ユニットに対応するデータグループの構成ファイルのパス識別情報をデータグループ管理情報として格納した構成を有することを特徴とする。
【００１８】
さらに、本発明の情報記録媒体の一実施態様において、前記サブコンテンツは、１以上のデータファイルを含むデータグループの集合であり、前記コンテンツ管理ユニットは、前記データグループを単位として設定され、前記情報記録媒体は、前記データグループを個別フォルダとして設定したディレクトリ構成を有することを特徴とする。
【００１９】
さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、コンテンツ管理ユニットに対応するデータグループの個別フォルダの識別情報をデータグループ管理情報として格納した構成を有することを特徴とする。
【００２０】
さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報を各コンテンツ管理ユニットに対応するユニット鍵によって暗号化したデータとして格納した構成を有することを特徴とする。
【００２１】
さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報を、改ざん防止処理構成を持つデータ構成として格納した構成を有することを特徴とする。
【００２２】
さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報と、該コンテンツ利用制御情報に基づくハッシュ値とを対応付けたデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して格納した構成を有することを特徴とする。
【００２３】
さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報の繰り返しデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して格納した構成を有することを特徴とする。
【００２４】
さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、情報記録媒体のドライブ装着に基づいて再生されるコンテンツとしてのファーストプレイバック・コンテンツを格納し、該ファーストプレイバック・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納した構成を有す

ることを特徴とする。

【００２５】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、メニュー表示機能実行に基づいて再生されるコンテンツとしてのトップメニュー・コンテンツを格納し、該トップメニュー・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納した構成を有することを特徴とする。

【００２６】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、さらに、コンテンツ管理ユニットと各インデックスとの対応情報、およびユニット鍵の生成に用いる乱数情報を定義したデータファイルを格納した構成を有することを特徴とする。

【００２７】

さらに、本発明の第２の側面は、

利用管理対象コンテンツを記録する情報処理装置であり、

特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツ、および前記ＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツの構成データをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして情報記録媒体に格納する処理を実行する構成を有することを特徴とする情報処理装置にある。

【００２８】

さらに、本発明の情報処理装置の一実施態様において、前記ＡＶフォーマットは、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットであり、前記情報処理装置は、前記メインコンテンツを、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットに従った階層データ構成を持つ記録データとして情報記録媒体に格納する処理を実行する構成であることを特徴とする。

【００２９】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記コンテンツ管理ユニットを、前記サブコンテンツに含まれる１以上のデータファイルを含むデータグループの集合に対応付けて設定し、コンテンツ管理ユニットに対応するデータグループの構成ファイルのパス識別情報をデータグループ管理情報として情報記録媒体に格納する処理を実行する構成を有することを特徴とする。

【００３０】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記コンテンツ管理ユニットを、前記サブコンテンツに含まれる１以上のデータファイルを含むデータグループの集合に対応付けて設定し、前記データグループを個別フォルダとして設定したディレクトリ構成に基づいて、前記サブコンテンツに含まれる１以上のデータファイルを情報記録媒体に格納する処理を実行する構成を有することを特徴とする。

【００３１】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、コンテンツ管理ユニットに対応するデータグループの個別フォルダの識別情報をデータグループ管理情報として情報記録媒体に格納する処理を実行する構成を有することを特徴とする。

【００３２】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報を各コンテンツ管理ユニットに対応するユニット鍵によって暗号化したデータとして情報記録媒体に格納する処理を実行する構成を有することを特徴とする。

【００３３】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報を、改ざん防止処理構成を持つデータ構成として情報記録媒体に格納する処理を実行する構成を有することを特徴とする。

【００３４】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報と、該コンテンツ利用制御情報に基づくハッシュ値とを対応付けたデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して情報記録媒体に格納する処理を実行する構成を有することを特徴とする。
【００３５】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報の繰り返しデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して情報記録媒体に格納する処理を実行する構成を有することを特徴とする。
【００３６】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、情報記録媒体のドライブ装着に基づいて再生されるコンテンツとしてのファーストプレイバック・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納する処理を実行する構成を有することを特徴とする。
【００３７】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、メニュー表示機能実行に基づいて再生されるコンテンツとしてのトップメニュー・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納する処理を実行する構成を有することを特徴とする。
【００３８】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、コンテンツ管理ユニットと各インデックスとの対応情報、およびユニット鍵の生成に用いる乱数情報を定義したデータファイルを格納する処理を実行する構成を有することを特徴とする。
【００３９】
さらに、本発明の第３の側面は、
利用管理対象コンテンツの再生処理を実行する情報処理装置であり、
情報記録媒体に格納されたコンテンツ管理ユニットに対応する暗号化コンテンツ利用制御情報を取得し、コンテンツ管理ユニットに対応して設定されたユニット鍵を適用した復号処理、および改ざん検証処理を実行し、改ざんの無いことの確認を条件として、該コンテンツ利用制御情報に基づくコンテンツ利用処理を実行する構成を有することを特徴とする情報処理装置にある。
【００４０】
さらに、本発明の第４の側面は、
利用管理対象コンテンツを記録する情報処理方法であり、
特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツ、および前記ＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツの構成データをコンテンツ管理ユニットとして設定するコンテンツ管理ユニット設定ステップと、
コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして情報記録媒体に格納するデータ格納ステップと、
を有することを特徴とする情報処理方法にある。
【００４１】
さらに、本発明の情報処理方法の一実施態様において、前記ＡＶフォーマットは、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットであり、前記データ格納ステップは、前記メイン

コンテンツを、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットに従った階層データ構成を持つ記録データとして情報記録媒体に格納するステップであることを特徴とする。

【００４２】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツ管理ユニットを、前記サブコンテンツに含まれる１以上のデータファイルを含むデータグループの集合に対応付けて設定するステップと、コンテンツ管理ユニットに対応するデータグループの構成ファイルのパス識別情報をデータグループ管理情報として情報記録媒体に格納するステップと、を有することを特徴とする。

【００４３】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツ管理ユニットを、前記サブコンテンツに含まれる１以上のデータファイルを含むデータグループの集合に対応付けて設定するステップと、前記データグループを個別フォルダとして設定したディレクトリ構成に基づいて、前記サブコンテンツに含まれる１以上のデータファイルを情報記録媒体に格納するステップと、を有することを特徴とする。

【００４４】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、コンテンツ管理ユニットに対応するデータグループの個別フォルダの識別情報をデータグループ管理情報として情報記録媒体に格納する処理を実行するステップを有することを特徴とする。

【００４５】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、コンテンツ管理ユニットに対応するコンテンツ利用制御情報を各コンテンツ管理ユニットに対応するユニット鍵によって暗号化したデータとして情報記録媒体に格納するステップを有することを特徴とする。

【００４６】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、コンテンツ管理ユニットに対応するコンテンツ利用制御情報を、改ざん防止処理構成を持つデータ構成として情報記録媒体に格納する処理を実行するステップを有することを特徴とする。

【００４７】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、コンテンツ管理ユニットに対応するコンテンツ利用制御情報と、該コンテンツ利用制御情報に基づくハッシュ値とを対応付けたデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して情報記録媒体に格納する処理を実行するステップを有することを特徴とする。

【００４８】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、コンテンツ管理ユニットに対応するコンテンツ利用制御情報の繰り返しデータを、各コンテンツ管理ユニットに対応するユニット鍵によって暗号化して情報記録媒体に格納する処理を実行するステップを有することを特徴とする。

【００４９】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、情報記録媒体のドライブ装着に基づいて再生されるコンテンツとしてのファーストプレイバック・コンテンツをコンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納する処理を実行することを特徴とする。

【００５０】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、メニュー表示機能実行に基づいて再生されるコンテンツとしてのトップメニュー・コンテンツをコ

ンテンツ管理ユニットとして設定し、該コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして格納する処理を実行することを特徴とする。

【００５１】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、コンテンツ管理ユニットと各インデックスとの対応情報、およびユニット鍵の生成に用いる乱数情報を定義したデータファイルを格納する処理を実行することを特徴とする。

【００５２】

さらに、本発明の第５の側面は、

利用管理対象コンテンツの再生処理を実行する情報処理方法であり、

情報記録媒体に格納されたコンテンツ管理ユニットに対応する暗号化コンテンツ利用制御情報を取得するステップと、

コンテンツ管理ユニットに対応して設定されたユニット鍵を適用した復号処理、および改ざん検証処理を実行するステップと、

改ざんの無いことの確認を条件として、該コンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップと、

を有することを特徴とする情報処理方法にある。

【００５３】

さらに、本発明の第６の側面は、

利用管理対象コンテンツを記録するコンピュータ・プログラムであり、

特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツ、および前記ＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツの構成データをコンテンツ管理ユニットとして設定するコンテンツ管理ユニット設定ステップと、

コンテンツ管理ユニットに含まれるデータを前記コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして情報記録媒体に格納するデータ格納ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００５４】

さらに、本発明の第７の側面は、

利用管理対象コンテンツの再生処理を実行するコンピュータ・プログラムであり、

情報記録媒体に格納されたコンテンツ管理ユニットに対応する暗号化コンテンツ利用制御情報を取得するステップと、

コンテンツ管理ユニットに対応して設定されたユニット鍵を適用した復号処理、および改ざん検証処理を実行するステップと、

改ざんの無いことの確認を条件として、該コンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００５５】

さらに、本発明の第８の側面は、

情報記録媒体であり、

コンテンツ管理ユニット単位に区分され、各コンテンツ管理ユニットに対応して設定されたユニット鍵による暗号化データを含む１以上のコンテンツと、

前記コンテンツ管理ユニット各々に対応して設定されたコンテンツ利用制御情報とを格納し、

前記コンテンツ利用制御情報は、

前記コンテンツ管理ユニット各々に対応して設定されたユニット鍵を適用した暗号処理が実行された暗号化データとして格納されているとともに、改ざん検証用データを付加した構成であることを特徴とする情報記録媒体にある。

【００５６】

さらに、本発明の情報記録媒体の一実施態様において、前記コンテンツ利用制御情報は、所定データ量からなるブロック単位での暗号化のなされた構成であり、各ブロックの構成データであるブロックシードと、前記ユニット鍵を適用した暗号処理により生成されるブロック鍵に基づいて暗号化のなされた暗号化ブロックデータとして格納した構成であることを特徴とする。

【００５７】

さらに、本発明の情報記録媒体の一実施態様において、前記ブロックシードは、コンテンツ利用制御情報を構成しないブロック構成データであることを特徴とする。

【００５８】

さらに、本発明の情報記録媒体の一実施態様において、前記コンテンツ利用制御情報は、基本制御情報と拡張制御情報の異なるカテゴリの制御情報を含むデータであり、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する改ざん検証用データを同一ブロック内に格納した構成を有することを特徴とする。

【００５９】

さらに、本発明の情報記録媒体の一実施態様において、前記コンテンツ利用制御情報は、基本制御情報と拡張制御情報の異なるカテゴリの制御情報を含むデータであり、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する第１の改ざん検証用データを同一ブロック内に格納し、前記基本制御情報および前記拡張制御情報の全データを含むデータに対する第２の改ざん検証用データを格納した構成を有することを特徴とする。

【００６０】

さらに、本発明の第９の側面は、

利用管理対象コンテンツの再生処理を実行する情報処理装置であり、

情報記録媒体に格納されたコンテンツ管理ユニットに対応するコンテンツ利用制御情報を取得し、

コンテンツ管理ユニットに対応して設定されたユニット鍵を適用して、前記コンテンツ利用制御情報を構成する所定データ量単位のブロックデータのブロック単位の復号処理と、ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理とを実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行する構成を有することを特徴とする情報処理装置にある。

【００６１】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記コンテンツ利用制御情報を構成する各ブロックからブロックシードを取得し、該ブロックシードと前記ユニット鍵を適用した暗号処理により生成されるブロック鍵に基づいて、ブロック単位の復号処理を実行する構成であることを特徴とする。

【００６２】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記コンテンツ利用制御情報を構成する複数のブロックデータから基本制御情報を含む１つのブロックデータのみを選択し、該選択した基本制御情報格納ブロックについての復号処理と、ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理とを実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行する構成を有することを特徴とする。

【００６３】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記コンテンツ利用制御情報を構成する複数のブロックデータから基本制御情報および拡張制御情報を含む複数のブロックデータを選択し、該選択した複数ブロックについてのブロック単位の復号処理を実行し、複数のブロックデータに含まれるデータに対する検証用データに基づく改ざん検証処理を実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行する構成を有することを特徴とする。

【００６４】
さらに、本発明の第１０の側面は、
情報記録媒体に対するデータ記録処理を実行する情報処理装置であり、
個別の利用管理制御を行うために設定されたコンテンツ管理ユニット各々に対応するコンテンツ利用制御情報に対する改ざん検証用データを生成し、前記コンテンツ管理ユニット各々に対応して設定されたユニット鍵を適用した暗号化処理を実行して暗号化データを生成し、前記改ざん検証用データを含む暗号化コンテンツ利用制御情報の生成および記録処理を実行する構成を有することを特徴とする情報処理装置にある。
【００６５】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記コンテンツ利用制御情報を、所定データ量からなるブロック単位に区分し、各ブロックの構成データから抽出したブロックシードと、前記ユニット鍵を適用した暗号処理によりブロック鍵を生成し、該ブロック鍵によるブロック暗号化データを生成して情報記録媒体に記録する処理を実行する構成であることを特徴とする。
【００６６】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記ブロックシードを、コンテンツ利用制御情報を構成しないブロック構成データから抽出する構成であることを特徴とする。
【００６７】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記コンテンツ利用制御情報を、基本制御情報と拡張制御情報の異なるカテゴリに区分し、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する改ざん検証用データを生成し、同一ブロック内に格納して記録する処理を実行する構成であることを特徴とする。
【００６８】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記コンテンツ利用制御情報を、基本制御情報と拡張制御情報の異なるカテゴリに区分し、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する第１の改ざん検証用データを生成し、同一ブロック内に格納して記録し、前記基本制御情報および前記拡張制御情報の全データを含むデータに対する第２の改ざん検証用データを生成し、記録する構成であること特徴とする。
【００６９】
さらに、本発明の第１１の側面は、
利用管理対象コンテンツの再生処理を実行する情報処理方法であり、
情報記録媒体に格納されたコンテンツ管理ユニットに対応するコンテンツ利用制御情報を取得するステップと、
コンテンツ管理ユニットに対応して設定されたユニット鍵を適用して、前記コンテンツ利用制御情報を構成する所定データ量単位のブロックデータのブロック単位の復号処理を実行する復号ステップと、
ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理を実行するステップと、
改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップと、
を有することを特徴とする情報処理方法にある。
【００７０】
さらに、本発明の情報処理方法の一実施態様において、前記復号ステップは、前記コンテンツ利用制御情報を構成する各ブロックからブロックシードを取得し、該ブロックシードと前記ユニット鍵を適用した暗号処理により生成されるブロック鍵に基づいて、ブロック単位の復号処理を実行するステップであることを特徴とする。
【００７１】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツ利用制御情報を構成する複数のブロックデータから基本制御情報を含む１つのブロックデータのみを選択するステップを有し、選択した基本制御情報格納ブロックについての復号処理と、ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理とを実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップを含むことを特徴とする。

【００７２】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツ利用制御情報を構成する複数のブロックデータから基本制御情報および拡張制御情報を含む複数のブロックデータを選択するステップを有し、選択した複数ブロックについてのブロック単位の復号処理を実行し、複数のブロックデータに含まれるデータに対する検証用データに基づく改ざん検証処理を実行し、改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップを含むことを特徴とする。

【００７３】

さらに、本発明の第１２の側面は、

情報記録媒体に対するデータ記録処理を実行する情報処理方法であり、

個別の利用管理制御を行うために設定されたコンテンツ管理ユニット各々に対応するコンテンツ利用制御情報に対する改ざん検証用データを生成するステップと、

前記コンテンツ管理ユニット各々に対応して設定されたユニット鍵を適用した暗号化処理を実行して暗号化データを生成する暗号化処理ステップと、

前記改ざん検証用データを含む暗号化コンテンツ利用制御情報の生成および記録処理を実行するステップと、

を有することを特徴とする情報処理方法にある。

【００７４】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツ利用制御情報を、所定データ量からなるブロック単位に区分し、各ブロックの構成データから抽出したブロックシードと、前記ユニット鍵を適用した暗号処理によりブロック鍵を生成し、該ブロック鍵によるブロック暗号化データを生成して情報記録媒体に記録する処理を実行するステップを含むことを特徴とする。

【００７５】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法において、前記ブロックシードを、コンテンツ利用制御情報を構成しないブロック構成データから抽出することを特徴とする。

【００７６】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツ利用制御情報を、基本制御情報と拡張制御情報の異なるカテゴリに区分し、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する改ざん検証用データを生成し、同一ブロック内に格納して記録する処理を実行するステップを含むことを特徴とする。

【００７７】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツ利用制御情報を、基本制御情報と拡張制御情報の異なるカテゴリに区分し、前記基本制御情報を１つのブロックに格納し、該基本制御情報格納ブロックのデータに対する第１の改ざん検証用データを生成し、同一ブロック内に格納して記録し、前記基本制御情報および前記拡張制御情報の全データを含むデータに対する第２の改ざん検証用データを生成し、記録するステップを含むこと特徴とする。

【００７８】

さらに、本発明の第１３の側面は、

利用管理対象コンテンツの再生処理を実行するコンピュータ・プログラムであり、

情報記録媒体に格納されたコンテンツ管理ユニットに対応するコンテンツ利用制御情報を取得するステップと、
コンテンツ管理ユニットに対応して設定されたユニット鍵を適用して、前記コンテンツ利用制御情報を構成する所定データ量単位のブロックデータのブロック単位の復号処理を実行する復号ステップと、
ブロックデータに含まれる改ざん検証用データに基づく改ざん検証処理を実行するステップと、
改ざんの無いことの確認を条件として、復号したコンテンツ利用制御情報に基づくコンテンツ利用処理を実行するステップと、
を有することを特徴とするコンピュータ・プログラムにある。

【００７９】
さらに、本発明の第１４の側面は、
情報記録媒体に対するデータ記録処理を実行するコンピュータ・プログラムであり、
個別の利用管理制御を行うために設定されたコンテンツ管理ユニット各々に対応するコンテンツ利用制御情報に対する改ざん検証用データを生成するステップと、
前記コンテンツ管理ユニット各々に対応して設定されたユニット鍵を適用した暗号化処理を実行して暗号化データを生成する暗号化処理ステップと、
前記改ざん検証用データを含む暗号化コンテンツ利用制御情報の生成および記録処理を実行するステップと、
を有することを特徴とするコンピュータ・プログラムにある。

【００８０】
なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００８１】
本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００８２】
本発明の構成によれば、例えば、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットなどの特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツと、そのＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツの構成データをコンテンツ管理ユニットとして設定し、コンテンツ管理ユニットに含まれるデータを、コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして情報記録媒体に格納する構成としたので、ＡＶ（Audio Visual）フォーマットに従ったデータのみならず、ＡＶ（Audio Visual）フォーマットに従わない任意のフォーマットのデータについても、様々な態様での利用制御を行うことが可能となる。

【００８３】
本発明の構成によれば、メインコンテンツ、サブコンテンツの構成データをユニットに区分し、各ユニット毎のコンテンツの利用管理、具体的には、再生制御、コピー制御など、各種のコンテンツ利用制御を行うことが可能となる。このように、コンテンツ利用制御を個々のコンテンツ管理ユニットを単位として行うことができるので、多くのコンテンツを格納した情報記録媒体において、細分化したコンテンツ毎の管理が可能となる。

【００８４】
本発明の構成によれば、メインコンテンツ、サブコンテンツの構成データをユニットに

区分し、各ユニット毎のコンテンツの利用制御情報を改ざん防止データとして設定し暗号化して提供する構成としたので、利用制御情報の不正取得、改ざんによるコンテンツの不正利用が防止される。

【００８５】

さらに、本発明の構成によれば、コンテンツ管理ユニット（ＣＰＳユニット）に区分されたコンテンツに対応するコンテンツ利用制御情報を、コンテンツ管理ユニットに対応するユニット鍵による暗号化データとするとともに、コンテンツ利用制御情報を含むデータに対応する改ざん検証用データを設定して記録する構成としたので、コンテンツ利用制御情報の漏洩や改ざんを防止することができ、よりセキュリティレベルの高いコンテンツ利用管理が実現される。

【００８６】

さらに、本発明の構成によれば、コンテンツ管理ユニット（ＣＰＳユニット）に区分されたコンテンツに対応するコンテンツ利用制御情報を、基本制御情報と、拡張制御情報に区分し、基本制御情報を含む特定のブロックデータを設定する構成とし、ブロック単位の暗号化を行ない、またその基本制御情報を含む特定のブロックデータに対応する改ざん検証用データを設定したので、基本制御情報のみに従ったコンテンツ利用を行なう装置は、拡張制御情報を格納したデータブロックの復号や、改ざん検証処理を実行する必要がなく、効率的な処理が可能となる。

【発明を実施するための最良の形態】

【００８７】

以下、図面を参照しながら本発明の情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の記載項目に従って行う。

１．情報記録媒体の格納データ構成
２．格納コンテンツ構成例
３．格納コンテンツの暗号化、利用管理構成
４．ファーストプレイバックおよびメニュー表示処理構成
５．ネットワーク独立、接続状態に基づくコンテンツ利用管理
６．ネットワークでのコンテンツコピー管理
７．コンテンツ管理ユニット対応の管理情報
８．メインコンテンツ、サブコンテンツ、およびコンテンツ管理情報の格納構成
９．コンテンツ利用制御情報の暗号化および改ざん防止処理構成
（９－１）コンテンツ利用制御情報の暗号化および改ざん防止処理構成の概要
（９－２）コンテンツ利用制御情報の暗号化および改ざん防止処理の具体的構成例
１０．情報処理装置の構成例

【００８８】

［１．情報記録媒体の格納データ構成］

まず、情報記録媒体の格納データ構成について説明する。図１に、本発明の処理の適用可能なコンテンツの格納された情報記録媒体の一例を示す。ここでは、コンテンツ格納済みディスクとしてのＲＯＭディスクの情報格納例を示す。

【００８９】

このＲＯＭディスクは、正当なコンテンツ著作権、あるいは頒布権を持ついわゆるコンテンツ権利者の許可の下にディスク製造工場において製造された正当なコンテンツを格納した情報記録媒体である。なお、以下の実施例では、情報記録媒体の例としてディスク型の媒体を例として説明するが、本発明は様々な態様の情報記録媒体を用いた構成において適用可能である。

【００９０】

図１に示すように、情報記録媒体１００には、様々なコンテンツが格納される。コンテンツは、大きく２つのカテゴリに分類される。１つは、例えば高精細動画像データであるＨＤ（High Definition）ムービーコンテンツなどの動画コンテンツのＡＶ(Audio Visual

)ストリームや特定の規格で規定された形式のゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるメインコンテンツ１０１である。メインコンテンツ１０１は、特定のＡＶフォーマット規格データであり、特定のＡＶデータフォーマットに従って格納される。具体的には、例えばＢｌｕ－ｒａｙディスクＲＯＭ規格データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従って格納される。

【００９１】

さらに、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどがサブコンテンツ１０２として格納される。サブコンテンツ１０２は、特定のＡＶデータフォーマットに従わないデータフォーマットを持つデータである。すなわち、Ｂｌｕ－ｒａｙディスクＲＯＭ規格外データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従わない任意のフォーマットで格納される。

【００９２】

メインコンテンツ１０１、サブコンテンツ１０２とともに、コンテンツの種類としては、音楽データ、動画、静止画等の画像データ、ゲームプログラム、ＷＥＢコンテンツなど、様々なコンテンツが含まれ、これらのコンテンツには、情報記録媒体１００からのデータのみによって利用可能なコンテンツ情報と、情報記録媒体１００からのデータと、ネットワーク接続されたサーバから提供されるデータとを併せて利用可能となるコンテンツ情報など、様々な態様の情報が含まれる。

【００９３】

メインコンテンツ１０１、サブコンテンツ１０２に含まれる各コンテンツまたは複数コンテンツの集合は、コンテンツの利用管理のため、各々、個別の暗号鍵（ユニット鍵）を適用した暗号化がなされて情報記録媒体１００に格納される。情報記録媒体１００には、さらに、情報記録媒体１００の識別情報としてのディスクＩＤ１０３を格納している。

【００９４】

［２．格納コンテンツ構成例］

図２を参照して、本発明の情報記録媒体に格納されるコンテンツの格納フォーマットについて説明する。

【００９５】

情報記録媒体には、図２に示すように、例えば高精細動画像データであるＨＤ（High Definition）ムービーコンテンツなどの動画コンテンツのＡＶストリームをメインコンテンツ２００として格納し、その他のデータ、プログラム、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどがサブコンテンツ３００として格納されている。

【００９６】

メインコンテンツ２００は、特定のＡＶフォーマット、例えばＢｌｕ－ｒａｙディスクＲＯＭ規格データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従って格納され、サブコンテンツ３００は、Ｂｌｕ－ｒａｙディスクＲＯＭ規格外データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従わない任意のフォーマットで格納される。

【００９７】

図２に示すように、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従って格納されるメインコンテンツ２００は、動画コンテンツ（ＡＶストリーム）を再生対象の実コンテンツとして格納しており、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従った階層構成を持つ。すなわち、

（Ａ）アプリケーション２１０

（Ｂ）再生区間指定ファイル（プレイリスト）２３０

（Ｃ）クリップ（コンテンツデータファイル）２４０

である。

【００９８】

（Ｃ）クリップ（コンテンツデータファイル）２４０は、それぞれ区分されたコンテン

ツデータファイルであるクリップ２４１，２４２，２４３を有し、各クリップ２４１は、ＡＶ（Audio-Visual）ストリームファイル２６１とクリップ情報ファイル２５１を持つ。

【００９９】

クリップ情報ファイル２５１は、ＡＶ（Audio-Visual）ストリームファイル２６１に関する属性情報を格納したデータファイルである。ＡＶ（Audio-Visual）ストリームファイル２６１は例えばＭＰＥＧ－ＴＳ（Moving Picture Experts Group-Transport Stream）データであり、画像（Ｖｉｄｅｏ）、音声（Ａｕｄｉｏ）、字幕データ等の各情報を多重化したデータ構造となっている。また、再生時に再生装置の制御を行うためのコマンド情報も多重化されている場合がある。

【０１００】

（Ｂ）再生区間指定ファイル（プレイリスト）２３０は、複数の再生区間指定ファイル（プレイリスト）２３１，２３２，２３３を持つ。各再生区間指定ファイル（プレイリスト）２３１，２３２，２３３のそれぞれは、クリップ（コンテンツデータファイル）２４０に含まれる複数のＡＶストリームデータファイルのいずれかを選択し、また選択したＡＶストリームデータファイルの特定のデータ部分を、再生開始点と再生終了点として指定するプレイアイテムを１つ以上持つ構成となっており、１つの再生区間指定ファイル（プレイリスト）を選択することで、その再生区間指定ファイル（プレイリスト）の持つプレイアイテムに従って、再生シーケンスが決定されて再生が実行される。

【０１０１】

例えば再生区間指定ファイル（プレイリスト）２３１を選択してコンテンツ再生を行うと、再生区間指定ファイル（プレイリスト）２３１に対応付けられたプレイアイテム２３４は、クリップ２４１に再生開始点ａと再生終了点ｂを持ち、また、プレイアイテム２３５は、クリップ２４１に再生開始点ｃと再生終了点ｄを持つので、再生区間指定ファイル（プレイリスト）２３１を選択してコンテンツ再生を行うと、クリップ２４１に含まれるコンテンツであるＡＶストリームファイル２６１の特定データ領域、ａ～ｂとｃ～ｄが再生されることになる。

【０１０２】

（Ａ）アプリケーション２１０は、たとえばコンテンツ再生を実行するディスプレイに提示されるコンテンツタイトルを含むアプリケーションインデックスファイル２１１，２１２と再生プログラム２２１，２２２の組み合わせ、または、ゲームコンテンツ、ＷＥＢコンテンツなどのアプリケーション実行ファイル２１３，２１４と再生プログラム２２３，２２４の組み合わせを持つ層として設定される。ユーザは再生対象をアプリケーションインデックスファイル２１１，２１２に含まれるタイトルの選択によって決定することができる

【０１０３】

各タイトルは、図に示すように、再生プログラム２２１～２２４の１つの再生プログラム（ムービーオブジェクト）に対応付けられており、ユーザが１つのタイトルを選択すると、その選択したタイトルに対応付けられた再生プログラムに基づく再生処理が開始することになる。なお、図に示すタイトル１、タイトル２として示されるアプリケーションインデックスファイル２１１，２１２は、情報記録媒体のセット、起動に際して、自動的に再生されるタイトル、メニューを表示するためのタイトル提示プログラムも含まれる。

【０１０４】

アプリケーションインデックスファイル２１１，２１２や、アプリケーション実行ファイル２１３，２１４は、アプリケーション実行に使用されるアプリケーションリソースファイルを含む場合がある。また、情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイル、例えばＪＰＥＧ，ＰＮＧ，ＢＭＰなどの画像ファイル２２５、ＰＣＭ、圧縮Ａｕｄｉｏなどの音声ファイル２２６、テキスト、データベースなどの各種データファイル２２７がアプリケーションリソースファイルとして適用される場合もある。

【０１０５】

再生プログラム（ムービーオブジェクト）２２１～２２４は、再生する再生区間指定ファイル（プレイリスト）の指定のほか、ユーザから入力されるコンテンツ再生処理に関する操作情報に対する応答、タイトル間のジャンプ、再生シーケンスの分岐など、再生コンテンツ（ＨＤムービーコンテンツ）の提示に必要な機能をプログラマブルに提供するコンテンツ再生処理プログラムである。各再生プログラム２２１～２２４は、相互にジャンプ可能であり、ユーザの入力、あるいはあらかじめ設定されたプログラムに従って、実際に実行される再生プログラムが選択され、選択された再生プログラムの指定する再生区間指定ファイル（プレイリスト）２３０によって、再生コンテンツがクリップ２４０から選択され再生される。

【０１０６】

メインコンテンツ２００は、図に示すように、例えばＢｌｕ－ｒａｙディスクＲＯＭ規格データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従った階層構成で管理され、この階層構成の枠組みに対して、コンテンツ管理ユニット（ＣＰＳユニット）が設定され、コンテンツ管理ユニット（ＣＰＳユニット）単位でコンテンツの利用管理がなされる。コンテンツ管理ユニット（ＣＰＳユニット）についての詳細は後述する。

【０１０７】

情報記録媒体には、メインコンテンツ２００の他にサブコンテンツ３００が併せて格納される。サブコンテンツ３００は、特定のＡＶフォーマット、例えばＢｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従わない任意のフォーマットで格納されるコンテンツである。

【０１０８】

サブコンテンツ３００は、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどであり、複数のデータファイルからなる集合がデータグループとして設定される。

【０１０９】

図２にはデータグループ１，３１１～データグループＮ，３１２を示している。これらのデータグループも利用管理対象コンテンツとして設定可能であり、利用管理対象コンテンツとして設定した場合には、各データグループを単位としたコンテンツ管理ユニット（ＣＰＳユニット）が設定され、データグループ単位で利用管理がなされる。

【０１１０】

［３．格納コンテンツの暗号化、利用管理構成］

次に、図３以下を参照して、情報記録媒体に格納されたコンテンツを区分して、区分コンテンツ毎に異なる利用制御を実現するコンテンツ管理構成について説明する。

【０１１１】

本発明においては、区分コンテンツ毎の異なる利用制御を実現する基本構成として、区分コンテンツ毎に異なる鍵（ユニット鍵）を割り当てる。１つのユニット鍵を割り当てる単位をコンテンツ管理ユニット（ＣＰＳユニット）と呼ぶ。

【０１１２】

それぞれのユニット鍵を適用して各ユニットに属するコンテンツを暗号化し、コンテンツ利用に際しては、各ユニットに割り当てられた鍵（ユニット鍵）を取得して再生を行う。各ユニット鍵は、個別に管理することが可能であり、例えばあるユニットＡに対して割り当てるユニット鍵は、情報記録媒体から取得可能な鍵として設定する。また、ユニットＢに対して割り当てるユニット鍵は、ネットワーク接続されるサーバにアクセスし、ユーザが所定の手続きを実行したことを条件として取得することができる鍵とするなど、各ユニット対応の鍵の取得、管理構成は、各ユニット鍵に独立した態様とすることが可能である。

【０１１３】

１つの鍵を割り当てる単位、すなわち、コンテンツ管理ユニット（ＣＰＳユニット）の設定態様について、図３を参照して説明する。

【０１１４】

まず、メインコンテンツ２００側におけるコンテンツ管理ユニット（ＣＰＳユニット）の設定構成について説明する。

【０１１５】

メインコンテンツ２００側においては、（Ａ）アプリケーション２１０に含まれる１つ以上のタイトルを含むアプリケーションインデックスファイル２１１，２１２、またはアプリケーション実行ファイル２１３，２１４等を含むＣＰＳユニットを設定する。

【０１１６】

図３に示すＣＰＳユニット１，４０１は、アプリケーションインデックスファイルと、再生プログラムファイルと、プレイリストと、コンテンツ実データとしてのＡＶストリームファイル群とを１つのユニットとして設定したユニットである。

【０１１７】

また、ＣＰＳユニット２，４０２は、アプリケーション実行ファイルと、再生プログラムファイルと、プレイリストと、コンテンツ実データとしてのＡＶストリームファイル群とを１つのユニットとして設定したユニットである。

【０１１８】

また、ＣＰＳユニット３，４０３は、アプリケーション実行ファイルと、再生プログラムファイルと、情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイルによって構成したユニットである。

【０１１９】

これらの各ユニットは、同一の鍵（ＣＰＳユニット鍵：図３中の鍵Ｋｕ１，Ｋｕ２，Ｋｕ３）でそれぞれ個別に暗号化して情報記録媒体に格納される。

【０１２０】

図３中、コンテンツ管理ユニット（ＣＰＳユニット）１，４０１、およびコンテンツ管理ユニット（ＣＰＳユニット）２，４０２は、上位層の（Ａ）アプリケーションと、下位層の（Ｂ）再生区間指定ファイル（プレイリスト）＋（Ｃ）クリップ（コンテンツデータファィル）によって構成されるユニットであり、コンテンツ管理ユニット（ＣＰＳユニット）３，４０３は、下位層の（Ｂ）再生区間指定ファイル（プレイリスト）＋（Ｃ）クリップ（コンテンツデータファィル）を含まず、上位層の（Ａ）アプリケーション層、および情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイルすなわち、画像ファイル２２５、音声ファイル２２６、データファイル２２７等によって構成されるユニットである。

【０１２１】

コンテンツ管理ユニット（ＣＰＳユニット）１，４０１には、タイトル１，２１１とタイトル２，２１２、再生プログラム２２１，２２２、プレイリスト２３１，２３２、クリップ２４１、クリップ２４２が含まれ、これらの２つのクリップ２４１，２４２に含まれるコンテンツの実データであるＡＶストリームデータファイル２６１，２６２がコンテンツ管理ユニット（ＣＰＳユニット）１，４０１に対応付けて設定される暗号鍵であるユニット鍵：Ｋｕ１を適用して暗号化される。

【０１２２】

また、コンテンツ管理ユニット（ＣＰＳユニット）２，４０２には、ゲームコンテンツ、ＷＥＢコンテンツなどによって構成されるアプリケーションファイル２１３と、再生プログラム２２３、プレイリスト２３３、クリップ２４３が含まれ、クリップ２４３に含まれるコンテンツの実データであるＡＶストリームデータファイル２６３がコンテンツ管理ユニット（ＣＰＳユニット）２，４０２に対応付けて設定される暗号鍵としてのユニット鍵：Ｋｕ２を適用して暗号化される。さらに、アプリケーションファイル２１３についても、ユニット鍵：Ｋｕ２を適用した暗号化ファイルとしてもよい。

【０１２３】

コンテンツ管理ユニット（ＣＰＳユニット）３，４０３は、上位層の（Ａ）アプリケーション層に含まれるアプリケーションファイル２１４，２１５と、再生プログラム２２４、さらに、再生プログラム２２４によって情報記録媒体、あるいはネットワーク接続サー

バから取得可能な様々なデータファイル、例えばＪＰＥＧ，ＰＮＧ，ＢＭＰなどの画像ファイル２２５、ＰＣＭ、圧縮Ａｕｄｉｏなどの音声ファイル２２６、テキスト、データベースなどの各種データファイル２２７が含まれるユニットとして設定される。

【０１２４】

コンテンツ管理ユニット（ＣＰＳユニット）３，４０３は、コンテンツ管理ユニット（ＣＰＳユニット）３，４０３に対応付けて設定される暗号鍵としてのユニット鍵：Ｋｕ３を適用して暗号化される。

【０１２５】

例えば、ユーザがコンテンツ管理ユニット１，４０１に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）１，４０１に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ１を取得して復号処理を実行することが必要であり、復号処理を実行後、アプリケーションプログラムを実行してコンテンツ再生を行なうことができる。

【０１２６】

例えば、コンテンツ管理ユニット３，４０３に対応するアプリケーションファイルまたは、再生プログラム２２４に対応付けられた画像ファイル２２５、ＰＣＭ、圧縮Ａｕｄｉｏなどの音声ファイル２２６、テキスト、データベースなどの各種データファイル２２７の利用処理を行なう場合は、コンテンツ管理ユニット（ＣＰＳユニット）３，４０３に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ３を取得して、復号処理を実行することが必要であり、復号処理を実行後、アプリケーションプログラムを実行または各種ファイルを実行することになる。

【０１２７】

この方法を適用した処理の実行における制限事項としては、ある特定のタイトル再生中はそのタイトルが属するＣＰＳユニットに含まれないＡＶストリームファイルを再生することはできない。つまり、タイトル再生中に実行されるムービーオブジェクトはそのタイトルが属するＣＰＳユニットに含まれないＡＶストリームファイルを再生するコマンドを含んではならない。なお、ムービーオブジェクトはタイトル切り替えを実行するコマンドを持つことができ、タイトルジャンプコマンドなどでタイトル切り替えが発生した時点で再生装置は再生中のタイトルが変化したと判断する。つまり、図３においてタイトル１，２１１の再生中にタイトル２，２１２へジャンプするコマンドを実行することは可能である。この場合ジャンプ後はタイトル２，２１２が再生されている状態となる。

【０１２８】

プレイリストは複数のクリップを参照することができるが、参照するクリップは１つのＣＰＳユニットに含まれるクリップに限られる。

【０１２９】

これらの制限を設定することにより、１つのＣＰＳユニットに属するタイトルを再生している間はユニット鍵の変更は起こらない。その結果タイトル内でＡＶストリームを連続に再生する際シームレスな接続が容易となる。

【０１３０】

なお、タイトルはユーザに見える情報であるため、ＣＰＳユニット単位で鍵の配信、コンテンツ管理などを行う場合に、ユーザへの説明やコンテンツ管理がしやすいという利点がある。

【０１３１】

アプリケーション実行中にプレイリストを参照する場合もタイトルを再生する場合と同様に１つのＣＰＳユニットに属するＡＶストリームを再生する間はシームレスな接続が容易となる。１つのアプリケーションを実行中に使用するリソースファイルが同一の鍵で暗号化されていることにより、アプリケーション実行中の暗号鍵（ＣＰＳユニット鍵）の変更がなく、復号処理をスムーズに行うことができる。

【０１３２】

情報記録媒体には、前述したように、メインコンテンツ２００の他にサブコンテンツ３

００が併せて格納される。サブコンテンツ３００は、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどであり、複数のデータファイルからなる集合がデータグループとして設定される。サブコンテンツ３００は、Ｂｌｕ－ｒａｙディスクＲＯＭ規格外データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従わない任意のフォーマットで格納される。

【０１３３】

サブコンテンツ３００内のデータグループも利用管理対象コンテンツとして設定可能であり、利用管理対象コンテンツとして設定した場合には、データグループが、コンテンツ管理ユニット（ＣＰＳユニット）として設定され、データグループ単位で利用管理がなされる。

【０１３４】

図３に示す例では、サブコンテンツ３００内のデータグループ１，３１１が、コンテンツ管理ユニット（ＣＰＳユニット）４，４０４として設定され、データグループＮ，３１２が、コンテンツ管理ユニット（ＣＰＳユニット）５，４０５として設定されている。

【０１３５】

コンテンツ管理ユニット（ＣＰＳユニット）４，４０４に含まれる各ファイルは、コンテンツ管理ユニット（ＣＰＳユニット）４，４０４に対応付けて設定される暗号鍵としてのユニット鍵：Ｋｕ４を適用して暗号化される。

【０１３６】

例えば、ユーザがコンテンツ管理ユニット４，４０４に対応するファイルに含まれるプログラムやデータの利用処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）４，４０４に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ４を取得し、復号処理を実行することが必要となる。

【０１３７】

また、コンテンツ管理ユニット（ＣＰＳユニット）５，４０５に含まれる各ファイルは、コンテンツ管理ユニット（ＣＰＳユニット）５，４０５に対応付けて設定される暗号鍵としてのユニット鍵：Ｋｕ５を適用して暗号化される。

【０１３８】

ユーザがコンテンツ管理ユニット５，４０５に対応するファイルに含まれるプログラムやデータの利用処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）５，４０５に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ５を取得し、復号処理を実行することが必要となる。

【０１３９】

なお、図には示していないが、コンテンツ再生処理を統括的に制御する統括再生制御プログラムが存在し、統括再生制御プログラムがコンテンツ再生の統括的制御を行う。

【０１４０】

統括再生制御プログラムは、ユーザの再生指定コンテンツに対応したコンテンツ管理ユニット（ＣＰＳユニット）を識別し、識別したＣＰＳ管理ユニット情報に対応するＣＰＳ暗号鍵の取得処理を実行する。ＣＰＳ暗号鍵が取得できない場合には、再生不可能のメッセージ表示などを行なう。また、統括再生制御プログラムは、コンテンツ再生実行時におけるコンテンツ管理ユニット（ＣＰＳユニット）の切り替えの発生の検出を行ない、必要な鍵の取得、再生不可能のメッセージ表示などを行なう。

【０１４１】

統括再生制御プログラムは、図４に示すようなユニット構成およびユニット鍵管理テーブルに基づく再生管理を実行する。

【０１４２】

ユニット構成およびユニット鍵管理テーブルは、図４に示すように、アプリケーション層のインデックスまたはアプリケーションファイル、またはデータグループに対応するコンテンツ管理ユニット（ＣＰＳユニット）と、ユニット鍵情報を対応付けたテーブルである。統括再生制御プログラムは、この管理テーブルに基づく管理を行う。

【０１４３】
なお、図に示す管理テーブルは、特定のＡＶフォーマット（例えばＢｌｕ－ｒａｙディスクＲＯＭ規格フォーマット）に従って格納されたメインコンテンツに対応する管理データと、特定のＡＶフォーマットと異なる格納コンテンツとしてのサブコンテンツに対応する管理データとを１つの管理テーブルとして設定した例を示しているが、これらの管理データは、メインコンテンツ対応の管理データと、サブコンテンツ対応の管理データとに分離して管理する構成としてもよい。具体的な管理データのファイル構成（ディレクトリ構成）については、後段で説明する。
【０１４４】
統括再生制御プログラムは、例えば、アプリケーションインデックスの切り替えによって、コンテンツ管理ユニット（ＣＰＳユニット）の切り替えが発生したことを検知すると、コンテンツ管理ユニット（ＣＰＳユニット）の切り替えによって適用する鍵の切り替えを行う。あるいはユニット鍵の取得が必要であることのメッセージ表示などの処理を実行する。
【０１４５】
例えばコンテンツ再生処理を実行している再生装置に、コンテンツ管理ユニット（ＣＰＳユニット）１，４０１のユニット鍵Ｋｕ１が格納されており、コンテンツ管理ユニット（ＣＰＳユニット）２，４０２のユニット鍵Ｋｕ２も格納されている場合、コンテンツ再生処理を統括的に制御する統括再生制御プログラムは、アプリケーションのユニット間の切り替えやコンテンツの切り替えがあったことを検知すると、コンテンツ管理ユニット（ＣＰＳユニット）の切り替えに対応したユニット鍵の切り替え、すなわちＫｕ１→Ｋｕ２の切り替えを行う。
【０１４６】
また、コンテンツ再生処理を実行している再生装置に、コンテンツ管理ユニット（ＣＰＳユニット）１，４０１のユニット鍵Ｋｕ１が格納されており、コンテンツ管理ユニット（ＣＰＳユニット）２，４０２のユニット鍵Ｋｕ２が格納されていない場合は、コンテンツ再生処理を統括的に制御する統括再生制御プログラムは、アプリケーションのユニット間の切り替えやコンテンツの切り替えがあったことを検知すると、ユニット鍵の取得が必要であることのメッセージ表示などの処理を実行する。
【０１４７】
これらの処理は、メインコンテンツ間のユニット切り替え、サブコンテンツ間のユニット切り替え、さらに、メインコンテンツのユニットとサブコンテンツのユニット間の切り替えにおいても同様に実行され、各ユニットの切り替えの検出に応じて、ユニット鍵Ｋｕ１～Ｋｕｎの切り替え、あるいは鍵取得メッセージの提示が実行されることになる。
【０１４８】
［４．ファーストプレイバックおよびメニュー表示処理構成］
図２～図４を参照して情報記録媒体に格納されるコンテンツの格納フォーマットおよびコンテンツ管理ユニット（ＣＰＳユニット）に基づくコンテンツの暗号化および管理構成について説明した。以下、図５～図７を参照して情報記録媒体（ディスク）のドライブへの装着時に起動する再生コンテンツとしてのファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）と、メニュー表示機能の起動時に再生するコンテンツとしてのトップメニュー（Ｔｏｐ　Ｍｅｎｕ）を有する構成について説明する。
【０１４９】
図５に、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）とトップメニュー（Ｔｏｐ　Ｍｅｎｕ）を有する構成におけるコンテンツ格納フォーマットを示し、図６に、図５に示すコンテンツ格納構成における暗号化およびコンテンツ管理ユニット（ＣＰＳユニット）の設定例を示す。
【０１５０】
図５に示すコンテンツ格納フォーマットは、先に説明した図２と同様、例えば高精細動画像データであるＨＤ（High Definition）ムービーコンテンツなどの動画コンテンツの

ＡＶストリームをメインコンテンツ２００として格納し、その他のデータ、プログラム、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどがサブコンテンツ３００として格納した構成である。なお、図５において、図２と同一の構成には同一の参照符号を付与している。

【０１５１】

図５に示す構成において、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従って格納されるメインコンテンツ２００は、動画コンテンツ（ＡＶストリーム）を再生対象の実コンテンツとして格納しており、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従った階層構成を持つ。すなわち、

（Ａ）アプリケーション２１０

（Ｂ）再生区間指定ファイル（プレイリスト）２３０

（Ｃ）クリップ（コンテンツデータファイル）２４０

である。

【０１５２】

（Ｃ）クリップ（コンテンツデータファイル）２４０、（Ｂ）再生区間指定ファイル（プレイリスト）２３０については、図２を参照して説明した構成と同様である。

【０１５３】

図５に示す構成では、（Ａ）アプリケーション２１０に、情報記録媒体（ディスク）のドライブへの装着時に起動する再生コンテンツのインデックス情報としてのファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）２８１と、メニュー表示機能の起動時に再生するコンテンツのインデックス情報としてのトップメニュー（Ｔｏｐ　Ｍｅｎｕ）２８２を有する。ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）は、ＢＤ－ＲＯＭＡＶアプリケーション規格によって規定され、タイトルと同様の構造をもつ再生対象（コンテンツ）である。

【０１５４】

ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）２８１は、情報記録媒体（ディスク）のドライブへの装着時に起動し再生されるコンテンツを指定するインデックスであり、たとえば著作権情報の表示などが含まれ、コンテンツ編集を行なうスタジオやオーサリング会社の会社ロゴの表示など、スタジオやオーサリング会社に固有の再生シーケンスに従って再生されるコンテンツである。また、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）２８２は、再生装置においてメニュー表示機能が動作した際に表示されるべきコンテンツを指定するインデックスである。

【０１５５】

これらのインデックスに基づいて、インデックス特定の対応の再生プログラムが起動し、再生プログラムによって指定されるプレイリストに従って特定されるコンテンツデータファイル（ＡＶストリーム）の再生が実行される。再生手順は、図２を参照して説明したタイトルなどのインデックスに基づく再生処理と同様である。

【０１５６】

図６を参照して、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）対応コンテンツと、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）対応コンテンツを有する構成におけるコンテンツ管理構成例について説明する。

【０１５７】

先に説明したように、本発明においては、区分コンテンツ毎の異なる利用制御を実現する基本構成として、区分コンテンツ毎に異なる鍵（ユニット鍵）を割り当てる。１つのユニット鍵を割り当てる単位がコンテンツ管理ユニット（ＣＰＳユニット）である。ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）対応コンテンツと、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）対応コンテンツを有する構成においても、これらのコンテンツに対してコンテンツ管理ユニット（ＣＰＳユニット）が対応付けられて、ユニット管理がなされる。

【０１５８】

ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）対応コンテンツ、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）対応コンテンツについても、それぞれのユニット鍵を適用してコンテンツが暗号化され、コンテンツ利用に際しては、各ユニットに割り当てられた鍵（ユニット鍵）を取得して再生を行う。

【０１５９】

図６に示す例では、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）対応コンテンツと、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）対応コンテンツを含む１つのユニットを設定した例を示している。すなわち、図６において、ＣＰＳユニット１，４２１が、これらのコンテンツを含むコンテンツ管理ユニットである。

【０１６０】

なお、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）対応コンテンツのみを含むＣＰＳユニットと、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）対応コンテンツを含むＣＰＳユニットを個別に設定した構成としてもよい。

【０１６１】

図６に示すＣＰＳユニット１，４２１は、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）インデックス２８１と、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）インデックス２８２を含むアプリケーションインデックスファイルと、再生プログラムファイルと、プレイリストと、コンテンツ実データとしてのＡＶストリームファイル群とを１つのユニットとして設定したユニットである。

【０１６２】

また、ＣＰＳユニット２，４２２は、アプリケーション実行ファイルと、再生プログラムファイルと、プレイリストと、コンテンツ実データとしてのＡＶストリームファイル群とを１つのユニットとして設定したユニットである。

【０１６３】

また、ＣＰＳユニット３，４２３は、アプリケーション実行ファイルと、再生プログラムファイルと、情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイルによって構成したユニットである。

【０１６４】

これらの各ユニットは、同一の鍵（ＣＰＳユニット鍵：図３中の鍵Ｋｕ１，Ｋｕ２，Ｋｕ３）でそれぞれ個別に暗号化して情報記録媒体に格納される。

【０１６５】

コンテンツ管理ユニット（ＣＰＳユニット）１，４２１には、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）インデックス２８１と、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）インデックス２８２と、再生プログラム２２１，２２２、プレイリスト２３１，２３２、クリップ２４１、クリップ２４２が含まれ、これらの２つのクリップ２４１，２４２に含まれるコンテンツの実データであるＡＶストリームデータファイル２６１，２６２がコンテンツ管理ユニット（ＣＰＳユニット）１，４２１に対応付けて設定される暗号鍵であるユニット鍵：Ｋｕ１を適用して暗号化される。

【０１６６】

また、コンテンツ管理ユニット（ＣＰＳユニット）２，４２２には、タイトル１，２８３、再生プログラム２２３、プレイリスト２３３、クリップ２４３が含まれ、このクリップ２４３に含まれるコンテンツの実データであるＡＶストリームデータファイル２６３がコンテンツ管理ユニット（ＣＰＳユニット）２，４２２に対応付けて設定される暗号鍵であるユニット鍵：Ｋｕ２を適用して暗号化される。

【０１６７】

コンテンツ管理ユニット（ＣＰＳユニット）３，４２３は、上位層の（Ａ）アプリケーション層に含まれるアプリケーションファイル２１４，２１５と、再生プログラム２２４、さらに、再生プログラム２２４によって情報記録媒体、あるいはネットワーク接続サーバから取得可能な様々なデータファイル、例えばＪＰＥＧ，ＰＮＧ，ＢＭＰなどの画像ファイル２２５、ＰＣＭ、圧縮Ａｕｄｉｏなどの音声ファイル２２６、テキスト、データベ

ースなどの各種データファイル２２７が含まれるユニットとして設定される。

【０１６８】

コンテンツ管理ユニット（ＣＰＳユニット）３，４２３は、コンテンツ管理ユニット（ＣＰＳユニット）３，４２３に対応付けて設定される暗号鍵としてのユニット鍵：Ｋｕ３を適用して暗号化される。

【０１６９】

例えば、ユーザがコンテンツ管理ユニット１，４２１に対応するコンテンツ、すなわち、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）インデックス２８１と、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）インデックス２８２に対応付けられたコンテンツの再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）１，４２１に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ１を取得して復号処理を実行することが必要であり、復号処理を実行後プログラムを実行してコンテンツ再生を行なうことができる。

【０１７０】

前述したように、統括再生制御プログラムは、再生コンテンツに対応したコンテンツ管理ユニット（ＣＰＳユニット）を識別し、識別したＣＰＳ管理ユニット情報に対応するＣＰＳ暗号鍵の取得処理を実行する。ＣＰＳ暗号鍵が取得できない場合には、再生不可能のメッセージ表示などを行なう。また、統括再生制御プログラムは、コンテンツ再生実行時におけるコンテンツ管理ユニット（ＣＰＳユニット）の切り替えの発生の検出を行ない、必要な鍵の取得、再生不可能のメッセージ表示などを行なう。

【０１７１】

情報記録媒体（ディスク）のドライブへの装着時に起動する再生コンテンツとしてのファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）と、メニュー表示機能の起動時に再生するコンテンツとしてのトップメニュー（Ｔｏｐ　Ｍｅｎｕ）とに対応するコンテンツが１つのコンテンツ管理ユニットとして設定された構成におけるユニット鍵管理テーブルの構成例を図７に示す。

【０１７２】

ユニット構成およびユニット鍵管理テーブルは、図７に示すように、アプリケーション層のインデックスまたはアプリケーションファイル、またはデータグループに対応するコンテンツ管理ユニット（ＣＰＳユニット）と、ユニット鍵情報を対応付けたテーブルである。統括再生制御プログラムは、この管理テーブルに基づく管理を行う。

【０１７３】

図７のテーブル構成は、図６に示すＣＰＳ設定に対応しており、コンテンツ管理ユニット（ＣＰＳユニット）１は、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）と、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）とに対応するコンテンツを含むユニットであり、ユニット鍵Ｋｕ１が対応付けられている。以下、各ＣＰＳユニット（ＣＰＳ２～）毎に異なるユニット鍵（Ｋｕ２～）が対応付けられ、各ユニットのコンテンツ再生時には対応するユニット鍵を適用した復号処理を行なうことが必要となる。

【０１７４】

前述したように、統括再生制御プログラムは、例えば、アプリケーションインデックスの切り替えによって、コンテンツ管理ユニット（ＣＰＳユニット）の切り替えが発生したことを検知すると、コンテンツ管理ユニット（ＣＰＳユニット）の切り替えによって適用する鍵の切り替えを行う。あるいはユニット鍵の取得が必要であることのメッセージ表示などの処理を実行する。

【０１７５】

［５．ネットワーク独立、接続状態に基づくコンテンツ利用管理］

次に、ホームネットワークなどのネットワーク接続機器としての再生装置に、上述したコンテンツ管理ユニットに区分され、ユニット単位の暗号鍵としてのユニット鍵を適用して暗号化されたコンテンツを格納した情報記録媒体を装着してコンテンツの再生、利用を行う場合、各コンテンツがネットワーク独立状態にあるか、ネットワーク接続状態にある

かに基づいてコンテンツ利用管理を行う構成について説明する。なお、以下で説明するコンテンツは、メインコンテンツ、サブコンテンツの両者を含むものである。

【０１７６】

図８（Ａ）に示すように、記録媒体上のコンテンツ管理ユニット（ＣＰＳユニット）の状態として、ネットワークから独立した状態（ネットワーク独立状態＝Ｄｉｓｃｒｅｔｅ状態）、ネットワークに関連付けられた状態（ネットワーク関連状態＝Ｂｏｕｎｄ状態）の２つを定義する。

【０１７７】

記録媒体上に複数のコンテンツ（コンテンツ管理ユニット）がある場合、コンテンツ管理ユニット（ＣＰＳユニット）ごとに、各コンテンツ管理ユニット（ＣＰＳユニット）がいずれの状態であるかが管理される。このコンテンツ管理ユニット（ＣＰＳユニット）ごとのＤｉｓｃｒｅｔｅ／Ｂｏｕｎｄ状態の管理情報は、情報記録媒体、あるいは情報記録媒体を装着したプレーヤ（情報再生装置）、情報管理処理を実行するホームネットワーク上の管理サーバに記録される。

【０１７８】

図８に示すコンテンツ１～コンテンツ６は、それぞれコンテンツ管理ユニット（ＣＰＳユニット）に対応し、メインコンテンツまたはサブコンテンツに属するコンテンツである。

【０１７９】

コンテンツの再生方法について説明する。

情報記録媒体に格納されたコンテンツ管理ユニット（ＣＰＳユニット）に区分された各コンテンツは、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツと、再生できないコンテンツがある。

【０１８０】

図８中のコンテンツ１～４はネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）で再生可能なコンテンツであり、コンテンツ５～６はネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）で再生できないコンテンツである。

【０１８１】

ユーザ操作、再生装置の処理などにより、記録媒体上の各コンテンツ（コンテンツ管理ユニット）は、ネットワーク関連状態（Ｂｏｕｎｄ状態）になることができる。なお、図８（ａ）に示すコンテンツ１のようにネットワーク関連状態（Ｂｏｕｎｄ状態）になることを禁止されたコンテンツも存在する。

【０１８２】

これらの情報は、情報記録媒体に格納された各コンテンツ（コンテンツ管理ユニット）の属性として決定されており、各コンテンツ管理ユニットに対応する属性情報として情報記録媒体に格納されている。

【０１８３】

各コンテンツ（コンテンツ管理ユニット）は、

（１）ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）で実行可能な処理と、

（２）ネットワーク関連状態（Ｂｏｕｎｄ状態）で実行可能な処理

上記２つの状態における実行可能な処理態様があらかじめ決定され、これらの情報が、各コンテンツ（コンテンツ管理ユニット）の対応属性情報として情報記録媒体に記録、あるいは、管理情報を保有する管理サーバに記録されている。

【０１８４】

その例として、たとえば図８（ａ）～（ｆ）に示すコンテンツ（コンテンツ管理ユニット）がある。

（ａ）コンテンツ１は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）に移行できないコンテンツ（コンテンツ管理ユニット）である。

【０１８５】

（ｂ）コンテンツ２は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）ではネットワーク接続を使用したストリーミング再生が可能なコンテンツ（コンテンツ管理ユニット）である。ストリーミング再生とは記録媒体上のデータまたは記録媒体上のデータを変換したものをデジタルデータとしてネットワーク経由で送信し、受信側の機器によってデコード・表示を行うコンテンツ再生処理である。

【０１８６】

（ｃ）コンテンツ３は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）ではネットワーク接続を使用した遠隔再生が可能なコンテンツ（コンテンツ管理ユニット）である。遠隔再生とは、ＤＶＤ－Ｖｉｄｅｏのインタラクティブコンテンツにあるようなユーザ操作への応答を含めた処理を送信側の装置が行い、画面に表示されるべき映像と再生されるべき音声のみを受信装置が表示可能なデータ形式で送信するコンテンツ再生処理である。遠隔再生においてはユーザの操作コマンドは受信側の装置が受け取り、送信を行っている再生装置にネットワーク経由で届ける必要がある。

【０１８７】

（ｄ）コンテンツ４は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）では、記録媒体上のコンテンツとネットワーク経由でダウンロードしたデータを合わせて再生するコンテンツ再生を実現するコンテンツ（コンテンツ管理ユニット）である。

【０１８８】

ダウンロードするデータとしては記録媒体に保存されていない言語の字幕、音声データ、メニュー画面データのほか、コンテンツ再生時に使用するデータの最新版などが想定される。コンテンツ４は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）でも再生可能なコンテンツが、ネットワーク関連状態（Ｂｏｕｎｄ状態）ではダウンロードしたデータと合わせて再生されるコンテンツの例である。

【０１８９】

（ｅ）コンテンツ５は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生不可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）でのみ、再生可能となるコンテンツ（コンテンツ管理ユニット）である。

【０１９０】

ネットワーク経由で再生に必要な鍵、すなわち、コンテンツ５として定義されるコンテンツ管理ユニットに対応するユニット鍵を取得し再生が可能になる。このようなユニット鍵の取得を条件とした再生許容構成とすることで、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）で再生できないコンテンツを配布・販売し、再生を行う際に課金して鍵情報を販売する形態のサービスも可能になる。

【０１９１】

（ｆ）コンテンツ６は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生不可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）でのみ、再生可能となるコンテンツ（コンテンツ管理ユニット）であり、さらに、記録媒体上のコンテンツとネットワーク経由でダウンロードしたデータを合わせて再生するコンテンツ再生を実現するコンテンツ（コンテンツ管理ユニット）である。

【０１９２】

なお、（ｄ）コンテンツ４～（ｆ）コンテンツ６は、ネットワーク接続を行い、ダウンロードデータ、またはユニット鍵の取得処理を行うことになるが、これらのデータ取得の前提条件として、正当な機器、またはユーザによるデータ要求であることの確認として、認証処理を実行し、認証の成立を条件として、サーバからダウンロードデータ、ユニット鍵の提供が実行されることになる。なお、ネットワーク経由の転送データは、暗号化されてユーザ機器に提供される。これらの処理については、後段で説明する。

【０１９３】

［６．ネットワークでのコンテンツコピー管理］

次に、ホームネットワークなどのネットワーク接続機器としての再生装置に、上述したコンテンツ管理ユニットに区分され、ユニット単位の暗号鍵としてのユニット鍵を適用して暗号化されたコンテンツを格納した情報記録媒体を装着してコンテンツの再生、利用を行う場合、各コンテンツがネットワーク独立状態にあるか、ネットワーク接続状態にあるかに基づいてコンテンツコピー管理を行う構成について説明する。なお、以下で説明するコンテンツは、メインコンテンツ、サブコンテンツの両者を含むものである。

【０１９４】

図９（Ａ）に示すように、記録媒体上のコンテンツ管理ユニット（ＣＰＳユニット）の状態として、ネットワークから独立した状態（ネットワーク独立状態＝Ｄｉｓｃｒｅｔｅ状態）、ネットワークに関連付けられた状態（ネットワーク関連状態＝Ｂｏｕｎｄ状態）の２つを定義する。

【０１９５】

記録媒体上に複数のコンテンツ（コンテンツ管理ユニット）がある場合、コンテンツ管理ユニット（ＣＰＳユニット）ごとに、各コンテンツ管理ユニット（ＣＰＳユニット）がいずれの状態であるかが管理される。このコンテンツ管理ユニット（ＣＰＳユニット）ごとのＤｉｓｃｒｅｔｅ／Ｂｏｕｎｄ状態の管理情報は、情報記録媒体、あるいは情報記録媒体を装着したプレーヤ（情報再生装置）、情報管理処理を実行するホームネットワーク上の管理サーバに記録される。

【０１９６】

図９に示すコンテンツ１～コンテンツ６は、それぞれコンテンツ管理ユニット（ＣＰＳユニット）に対応する。ユーザ操作、再生装置の処理などにより、記録媒体上の各コンテンツ（コンテンツ管理ユニット）は、ネットワーク関連状態（Ｂｏｕｎｄ状態）になることができる。なお、図９（ａ）に示すコンテンツ１のようにネットワーク関連状態（Ｂｏｕｎｄ状態）になることを禁止されたコンテンツも存在する。

【０１９７】

これらの情報は、情報記録媒体に格納された各コンテンツ（コンテンツ管理ユニット）の属性として決定されており、各コンテンツ管理ユニットに対応する属性情報として情報記録媒体、あるいは管理情報を格納した管理サーバに格納されている。

【０１９８】

各コンテンツ（コンテンツ管理ユニット）は、

（１）ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）で実行可能な処理と、

（２）ネットワーク関連状態（Ｂｏｕｎｄ状態）で実行可能な処理

上記２つの状態における実行可能なコピー処理態様があらかじめ決定され、これらの情報が、各コンテンツ（コンテンツ管理ユニット）の対応属性情報として情報記録媒体に記録、あるいは、管理情報を保有する管理サーバに記録されている。

【０１９９】

その例として、たとえば図９（ａ）～（ｆ）に示すコンテンツ（コンテンツ管理ユニット）がある。

（ａ）コンテンツ１は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）に移行できないコンテンツ（コンテンツ管理ユニット）である。

【０２００】

（ｂ）コンテンツ２は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）でも再生可能であるが、コピーは許容されないコンテンツ（コンテンツ管理ユニット）である。

【０２０１】

（ｃ）コンテンツ３は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）でも再生可能である。さらに、ネットワーク関連状態（Ｂｏｕｎｄ状態）でのみ、コピー元と同種の記録媒体

へのコンテンツコピーが許容されたコンテンツ（コンテンツ管理ユニット）である。
【０２０２】
コピー先区分として、
コピー元と同種の記録媒体、
異なる記録媒体（ネットワーク内）、
携帯機器
の３つが想定される。コンテンツ３のケースは同種の記録媒体へコピーすることのみが許容されたコンテンツであり、コピー先がコピー元と同種の記録媒体であることが確認された場にのみ、コピー元は記録媒体上のデータをそのままコピー先へ送ることができる。
【０２０３】
（ｄ）コンテンツ４は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）でも再生可能である。さらに、ネットワーク関連状態（Ｂｏｕｎｄ状態）でのみ、コピー元と異なる種類の記録媒体へのコンテンツコピーが許容されたコンテンツ（コンテンツ管理ユニット）である。
【０２０４】
コンテンツ４のケースは異なる記録媒体へのコピーが許容され、必要に応じてコピー元またはコピー先の機器がデータの変換を行い、コピーデータを記録することが必要となる。
【０２０５】
（ｅ）コンテンツ５は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生不可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）でも再生可能である。さらに、ネットワーク関連状態（Ｂｏｕｎｄ状態）でのみ、携帯機器へのコピーが許容されたコンテンツ（コンテンツ管理ユニット）である。携帯機器は家庭内ネットワークの外部へ機器を持ち出すことがあり、外部への持ち出しを考慮してコピー管理を行う必要がある。
【０２０６】
コピーに関する制限として、コピー回数、有効期限、オリジナルの記録媒体がネットワーク関連状態（Ｂｏｕｎｄ状態）でなくなった場合の処理などを規定する必要がある。これらの情報は上記３つのコピー形態のそれぞれについて別個に規定できることが望ましい。なおオリジナルの記録媒体がネットワーク関連状態（Ｂｏｕｎｄ状態）でなくなった場合の処理としては、コピーデータについて無効、一定期間後に無効、消去などが想定される。消去されないデータは再び記録媒体がネットワーク関連状態（Ｂｏｕｎｄ状態）になった際に、そのまま使用可能である。これにより、記録媒体を友人に貸し出す場合なども、コピーデータが一時的に使用できなくなるだけで、媒体の返却とともにコピーデータの使用も元通り可能になる。
【０２０７】
（ｆ）コンテンツ６は、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）において再生不可能なコンテンツであり、ネットワーク関連状態（Ｂｏｕｎｄ状態）でのみ、再生可能となるコンテンツ（コンテンツ管理ユニット）であり、さらに、あらかじめ記録媒体上に家庭内ネットワークでのコピーを前提にしたコピー用のデータを保存してあるコンテンツ（コンテンツ管理ユニット）とした例である。
【０２０８】
このコピー用データは例えばコピー元の装置で再生できない形式でも良く、他の機器へコピーした結果、再生が可能とした構成としてもよい。例えば図２、図３を参照して説明した複数階層フォーマットのデータが保存された記録媒体に、一般的なネットワーク接続機器で再生可能なデータ形式（例えばパーソナルコンピュータで再生可能なＡＶＩ等のファイル形式やＭＰＥＧ－ＰＳ形式）で同じ内容のコピー用データを保存しておき、ネットワーク経由のコピーではコピー用のデータを送出し、これらの機器での再生を可能とする構成が適用できる。

【０２０９】
なお、コンテンツのコピーを行う前にネットワーク経由での認証や鍵取得を行わせる構成とすることが好ましい。また、例えばコピーするごとに課金を行う、コピーに鍵を必要とするシステムにおいては、鍵の配信回数でコピー回数を制限するなどのコンテンツ管理処理構成とすることが好ましい。
【０２１０】
［７．コンテンツ管理ユニット対応の管理情報］
次に、上述したコンテンツ管理ユニットに区分され、ユニット単位の暗号鍵としてのユニット鍵を適用して暗号化されたコンテンツを格納した情報記録媒体におけるコンテンツ管理ユニット対応の管理情報について説明する。なお、以下で説明するコンテンツは、メインコンテンツ、サブコンテンツの両者を含むものである。
【０２１１】
前述したように、コンテンツ管理ユニット（ＣＰＳユニット）には、１つのユニット鍵が対応付けて設定され、コンテンツ管理ユニット（ＣＰＳユニット）構成および鍵管理テーブルについては、図４に示すようなユニット鍵情報の管理テーブル［ユニット構成およびユニット鍵管理テーブル］として設定される。
【０２１２】
さらに、コンテンツ管理ユニット（ＣＰＳユニット）に対応する属性情報として、上述したように、各コンテンツ管理ユニット（ＣＰＳユニット）が、
ａ．ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）
ｂ．ネットワーク関連状態（Ｂｏｕｎｄ状態）
のいずれの状態であるかの状態情報がある。ただし、データ書き込みが不可能な情報記録媒体については、これらの状態情報は初期状態のみが記述されることになる。
【０２１３】
データ書き込みが可能な情報記録媒体については、初期状態と現在の状態の２つの情報が記録される。現在の状態情報の記録媒体に対する書き込み処理は、情報記録媒体を装着した再生装置としての情報処理装置、あるいはネットワーク接続された管理サーバによって行われる。
【０２１４】
図１０に、データ書き込みが可能な情報記録媒体において初期状態と現在の状態が記録された「状態管理テーブル」の構成例を示す。コンテンツ管理ユニット（ＣＰＳユニット）に対応する初期状態と現在の状態が、ａ．ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）ｂ．ネットワーク関連状態（Ｂｏｕｎｄ状態）のいずれの状態であるかが記述される。
【０２１５】
なお、図１０に示す状態管理テーブルは、情報記録媒体に記録されるとともに、かつ、情報記録媒体を装着した再生装置としての情報処理装置、あるいはネットワーク接続された管理サーバ等の外部装置にも記録される。
【０２１６】
データ書き込みのできない記録媒体の場合は、初期状態データのみが情報記録媒体に記録され、情報記録媒体を装着した再生装置としての情報処理装置、あるいはネットワーク接続された管理サーバ等の外部装置には、初期状態と現在の状態を記録した状態管理テーブルを持つことになる。
【０２１７】
状態管理テーブルに設定される初期状態としては、以下の４つの状態のいずれかが設定される。
ａ．Ｄｉｓｃｒｅｔｅ　ｏｎｌｙ
ｂ．Ｄｉｓｃｒｅｔｅ　ｉｎｉｔｉａｌｌｙ
ｃ．Ｂｏｕｎｄ　ｏｎｌｙ
ｄ．Ｂｏｕｎｄ　ｉｎｉｔｉａｌｌｙ

【０２１８】
ａ．Ｄｉｓｃｒｅｔｅ　ｏｎｌｙは、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）のみが許容状態であり、ネットワーク関連状態（Ｂｏｕｎｄ状態）への遷移が許容されないコンテンツ（コンテンツ管理ユニット）である。
【０２１９】
ｂ．Ｄｉｓｃｒｅｔｅ　ｉｎｉｔｉａｌｌｙは、初期的にネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）であるが、ネットワーク関連状態（Ｂｏｕｎｄ状態）への遷移が許容されるコンテンツ（コンテンツ管理ヨニット）である。
【０２２０】
ｃ．Ｂｏｕｎｄ　ｏｎｌｙは、ネットワーク関連状態（Ｂｏｕｎｄ状態）のみが許容状態であり、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）への遷移が許容されないコンテンツ（コンテンツ管理ヨニット）である。
【０２２１】
ｂ．Ｂｏｕｎｄ　ｉｎｉｔｉａｌｌｙは、初期的にネットワーク関連状態（Ｂｏｕｎｄ状態）であるが、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）への遷移が許容されるコンテンツ（コンテンツ管理ユニット）である。
【０２２２】
初期状態でネットワーク関連状態（Ｂｏｕｎｄ状態）というのは、あらかじめコンテンツがネットワーク上の情報と関連付けられて配布されるケースを想定している。例えばネットワーク上の情報とあわせて再生することを前提にしたコンテンツなどである。
【０２２３】
現在の状態としては、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）、または、ネットワーク関連状態（Ｂｏｕｎｄ状態）のいずれかが設定される。
【０２２４】
コンテンツ管理ユニット毎に、現状態の設定は可能であるが、コンテンツの利用管理を行う態様として、２つの状態管理方法が考えられる。第一の方法は記録媒体を家庭内ネットワークの外に出す場合は必ず初期状態に戻す構成とするものである。
【０２２５】
たとえばコンテンツ格納記録媒体として、再生装置に対して着脱可能なリムーバブルメディアを用いた場合、リムーバブルメディアを再生装置から取り出した時点で、各コンテンツの状態を初期状態に戻す。この場合、記録媒体外部に保存された状態管理テーブルも初期化する。
【０２２６】
第二の方法は記録媒体の状態を外部の管理サーバなどに登録しておく方法である。この場合、リムーバブルメディアを取り出しただけでは記録媒体外部の状態管理テーブルを初期化する必要はない。
【０２２７】
ホームネットワーク（Ａ）の再生機器において、ネットワーク関連状態（Ｂｏｕｎｄ状態）に設定したコンテンツを格納したリムーバブルメディアを、例えば別の家庭に構築されたホームネットワーク（Ｂ）に接続された再生装置に装着し、ネットワーク関連状態（Ｂｏｕｎｄ状態）に設定しようとすると、管理サーバは、状態管理テーブルに基づいて、ホームネットワーク（Ａ）においてネットワーク関連状態（Ｂｏｕｎｄ状態）であるコンテンツが、重複して異なるホームネットワーク（Ｂ）でネットワーク関連状態（Ｂｏｕｎｄ状態）に設定されようとしていることを検出し、ホームネットワーク（Ｂ）でのネットワーク関連状態（Ｂｏｕｎｄ状態）への設定を許容しないとするものである。
【０２２８】
このような管理を行うことで、同一コンテンツが複数、並列して利用されることを防止することができる。
【０２２９】
なお、管理サーバ等に、図１０に示すような状態管理テーブルを保持する構成とするこ

とにより、リムーバブルメディアを再生装置から取り出しても現在の状態が参照でき、その状態に基づくコンテンツの利用管理が可能となる。

【０２３０】

なお、情報記録媒体が記録可能な媒体であり、現在の状態が記録される構成とした場合は、記録媒体上に現在の状態が記録されているため、サーバ経由で、ネットワーク関連状態（Ｂｏｕｎｄ状態）にあるか否かを確認することなく、直接、記録媒体上から現在の状態を読み取り、読み取り情報に基づいて、コンテンツの利用管理を行うことが可能である。

【０２３１】

なお、通常のデータ領域に対する追記書き込みの許容されないＲＯＭメディアの場合に、上述のような状態管理情報を書き込むための構成としては、ＲＯＭメディアに部分的に書き込み可能な領域を形成し、このような構成を持つＲＯＭメディアを使用する構成とすることが望ましい、

【０２３２】

あるいは、追記書き込み可能な光ディスク媒体、ＩＣメモリなどを持ったカートリッジ入りメディアなどの使用を行う構成とすることが好ましい。

【０２３３】

なお、図１０に示す状態管理テーブルは、図４に示すようなコンテンツ管理ユニット（ＣＰＳユニット）構成およびユニット鍵を管理したテーブル［ユニット構成およびユニット鍵管理テーブル］と一体化した情報テーブルとしても、あるいはそれぞれ独立した管理テーブルとして構成してもよい。

【０２３４】

コンテンツ管理ユニットに対応する管理情報としては、さらに、コンテンツがネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）にある場合のコンテンツの再生、利用制限情報、また、ネットワーク関連状態（Ｂｏｕｎｄ状態）にある場合のコンテンツの再生、利用制限情報がある。

【０２３５】

これらのコンテンツ管理情報は、情報記録媒体にコンテンツに対応する属性情報として記述するか、あるいは、コンテンツ管理処理を行う管理サーバにおいて記録される。なお、ネットワーク関連状態（Ｂｏｕｎｄ状態）でのみコンテンツ利用を許容したコンテンツについては、管理サーバにおいて記録されるコンテンツ管理情報のみに基づいてコンテンツの利用管理構成をとることが可能である。

【０２３６】

コンテンツ管理情報のデータ例について、図１１を参照して説明する。図１１は、固定長データで記録したコンテンツ利用制御情報、すなわち、コンテンツ再生およびコピー制御情報管理テーブルの構成例である。コンテンツ再生およびコピー制御情報管理テーブルは、各ＣＰＳユニット単位のデータとして、あるいは全てのＣＰＳユニットについてまとめた情報テーブルとして設定される。

【０２３７】

図１１に示すコンテンツ再生およびコピー制御情報管理テーブルには、例えば、コンテンツの状態、すなわち、コンテンツがネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）にあるか、ネットワーク関連状態（Ｂｏｕｎｄ状態）にあるかに応じたコンテンツ管理情報など、コンテンツの利用、コピーに関する制御情報が固定長データで記録されている。

【０２３８】

家庭内ネットワークでのコンテンツ利用を考慮すると、図１１に示すような固定長のコンテンツ管理情報の設定が好ましい。ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）の管理情報としては、例えば、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）での再生の可否が記述される。ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）で再生できないコンテンツについてはコンテンツを再生するための方法が記述される。例えば鍵配信サーバへの接続、別メディア（メモリーカードなど）で配布される鍵データの取得が必要であるこ

と、サーバを特定するためのＵＲＬ、電話番号などの情報またはそれらの情報が保存されたリストへのインデックス値が記述される。

【０２３９】

また、ネットワーク関連状態（Ｂｏｕｎｄ状態）の管理情報としては、ネットワーク内のコピー、ストリーミング、遠隔再生に関する可否、および対象となる機器の分類ごとにコピー回数、有効期限、コピー・ストリーミング用データの有無、データ変換方式、コンテンツがネットワーク関連状態（Ｂｏｕｎｄ状態）でなくなった場合のコピーデータの扱いなどを記述する。

【０２４０】

なお、図１１はこれらの情報の一部または全てを固定長のフィールドに保存することを想定しているため、ＵＲＬやデータの位置（パス情報）など文字数の多いデータは別ファイルに保存し、固定長フィールドへは別ファイルに保存されたリストへのインデックスを保存することになる。

【０２４１】

また、記録媒体上の再生制御情報を使用せず、サーバから再生時の動作制御情報を取得し、それに従って動作することを可能にするため、図１１に示すコンテンツ管理情報構成データ５０１に示すように、サーバから情報を取得することを示すフラグ、およびサーバへのアクセス方法を示す情報を保存する構成としてもよい。

【０２４２】

このような情報をコンテンツ管理情報として設定することにより、固定長データでは表現できない複雑な制御や記録媒体を販売した後での制御方法の変更などが可能になる。

【０２４３】

図１２は、各ＣＰＳユニット毎に設定されるコンテンツ利用制御情報、すなわち、コンテンツ再生およびコピー制御情報を可変長データで記録したコンテンツ再生およびコピー制御情報管理テーブルの構成例である。

【０２４４】

設定する情報の内容は図１１と同じである。可変長の情報を入れることができるため、ＵＲＬやデータの位置（パス情報）など文字数の多いデータもコンテンツ管理情報の中に直接記述することができる。また、ループ構造をとり、コンテンツ管理情報の種類ごとにタイプ（図中のＣＣＩ＿ａｎｄ＿ｏｔｈｅｒ＿ｉｎｆｏ＿ｔｙｐｅ）を定義しているため、後から新たなコピー制御方法が追加された場合にもタイプとそれに付随する情報（図中のＣＣＩ＿ａｎｄ＿ｏｔｈｅｒ＿ｉｎｆｏ＿ｖａｌｕｅ および Ａｄｄｉｔｉｏｎａｌ＿ｉｎｆｏ）を定義することにより、対応が容易である。この場合、過去に発売された機器は未知のタイプについては処理を行わないでよい。

【０２４５】

なお、図１２（Ａ）のように、ネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）、ネットワーク関連状態（Ｂｏｕｎｄ状態）に関するコンテンツ管理情報を分けない構造と、図１２（Ｂ）のように２つの状態それぞれにコンテンツ管理情報のループをもつ構造の２つの設定が可能である。

【０２４６】

なお、記録媒体上の再生制御情報を使用せず、サーバから再生時の動作制御情報を取得し、それに従って動作することを可能にするため、図１２に示すコンテンツ管理情報構成データ５０２に示すように、サーバから情報を取得することを示すフラグ、およびサーバへのアクセス方法を示す情報を保存する構成としてもよい。

【０２４７】

このような情報をコンテンツ管理情報として設定することにより、固定長データでは表現できない複雑な制御や記録媒体を販売した後での制御方法の変更などが可能になる。

【０２４８】

さらに、図１２に示すようにコンテンツ再生およびコピー制御情報管理テーブル中にユーザ定義情報５０３を設定し、ここにユーザ定義可能な制御情報のタイプなどを設定する

構成とすることにより、個々のユーザに対応するコンテンツ再生制御、例えば特定の会員ユーザと非会員ユーザとを区別して、会員ユーザにのみ許容する再生処理を可能とする、あるいは、記録媒体規格に依存しないコピー制御情報（ＣＣＩ情報）の定義を設定するなど、記録媒体に属する規格の範囲を超える制御方法、コンテンツ配布者が自由に定義できる制御方法を実現することができる。

【０２４９】

ユーザ定義に基づくコピー制御情報（ＣＣＩ情報）の使用例としては、例えば、記録媒体規格に依存しないコピー制御情報（ＣＣＩ情報）の定義を設定する使用例がある。

【０２５０】

コピー制御情報（ＣＣＩ情報）のパラメータなどは、特定の記録システム（ＤＶＤ規格など）ごとに規格で定められており、一旦それに対応した再生装置が普及した後で、コピー制御情報（ＣＣＩ情報）を拡張することは困難である。

【０２５１】

そこで、記録システムによって決められたコピー制御情報（ＣＣＩ情報）にない任意の制御情報をユーザ定義情報として設定し、コンテンツ所有者や管理者が独自のコピー制御情報（ＣＣＩ情報）を設定する。

【０２５２】

コンテンツ所有者や管理者が独自に設定したコピー制御情報（ＣＣＩ情報）の解釈は、規格準拠の再生装置だけでは不可能なため、コピー制御情報（ＣＣＩ情報）の解釈を行うアプリケーション（例えばＪａｖａ）を記録媒体上、またはサーバ等、外部から取得可能とし、取得したアプリケーションの実行により、独自定義のコピー制御情報（ＣＣＩ情報）の解釈、ＣＣＩ情報に従った動作制御を再生装置において実行させることが可能となる。

【０２５３】

［８．メインコンテンツ、サブコンテンツ、およびコンテンツ管理情報の格納構成］

次に、メインコンテンツ、サブコンテンツ、およびコンテンツ管理情報の格納構成について説明する。

【０２５４】

上述した各種のコンテンツ管理ユニット（ＣＰＳユニット）、およびユニットに対応する各種の管理情報を格納するディレクトリ構成、および管理情報の格納部の設定例について、図１３を参照して説明する。ＢＤＭＶディレクトリはＢｌｕ－ｒａｙ　Ｄｉｓｃ　ＲＯＭフォーマットにおいてアプリケーション用ファイルを保管するディレクトリである。

【０２５５】

図１３に示すディレクトリ構成において、メインコンテンツデータ部５１１は、先に、図２、図３を参照して説明した特定のＡＶフォーマットに従った複数階層構成からなるメインコンテンツのデータファイル、すなわち、アプリケーション、プレイリスト、クリップ等の階層構成を持つ特定のＡＶフォーマット（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ　ＲＯＭフォーマット）に従ったコンテンツおよびプログラム等を格納したディレクトリである。

【０２５６】

これらのデータファイルは情報記録媒体のユーザデータ領域に格納される。なお、クリップに含まれるＡＶストリームは、コンテンツ管理ユニット（ＣＰＳユニット）ごとに設定されるユニット鍵によって暗号化されたデータファイルである。

【０２５７】

メインコンテンツ管理データ部５１２には、メインコンテンツに対応する管理ファイルが格納される。前述した図４に示すようなコンテンツ管理ユニット（ＣＰＳユニット）構成およびユニット鍵を管理したテーブル、すなわち［ユニット構成および鍵管理テーブル］と、図１０を参照して説明した各コンテンツ管理ユニット毎のネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）、ネットワーク関連状態（Ｂｏｕｎｄ状態）の状態を管理する［状態管理テーブル］、図１１、図１２を参照して説明した各状態におけるコンテンツの利用、コピー制御情報を格納した［コンテンツ再生およびコピー制御情報管理テーブル］の

各テーブルのデータファイルが格納される。これらの各テーブルは個別のデータファイル、あるいは複数のテーブルを組み合わせたテーブルを含むデータファイルのいずれかの態様で格納される。

【０２５８】

サブコンテンツデータ部５１３は、メインコンテンツに属さないコンテンツ、すなわち特定のＡＶフォーマット（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ　ＲＯＭフォーマット）に従わないコンテンツ、すなわち、図２、図３に示すデータグループに属するコンテンツを格納したディレクトリである。これらのデータファイルも、情報記録媒体のユーザデータ領域に格納される。なお、このサブコンテンツデータ部５１３に属するコンテンツは、コンテンツ管理ユニット（ＣＰＳユニット）として設定されるコンテンツと設定されないコンテンツが並存可能である。コンテンツ管理ユニット（ＣＰＳユニット）として設定されるコンテンツは、ユニット鍵によって暗号化されたデータファイルとなる。

【０２５９】

サブコンテンツ管理データ部５１４には、サブコンテンツに対応する管理ファイルが格納される。前述した図４に示すようなコンテンツ管理ユニット（ＣＰＳユニット）構成およびユニット鍵を管理したテーブル、すなわち［ユニット構成および鍵管理テーブル］と、図１０を参照して説明した各コンテンツ管理ユニット毎のネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）、ネットワーク関連状態（Ｂｏｕｎｄ状態）の状態を管理する［状態管理テーブル］、図１１、図１２を参照して説明した各状態におけるコンテンツの利用、コピー制御情報を格納した［コンテンツ再生およびコピー制御情報管理テーブル］の各テーブルのデータファイルが格納される。

【０２６０】

データグループ情報５１５は、サブコンテンツのデータグループ情報を格納したファイルであり、図に示すように、各データグループ１～Ｎ毎に、各グループに属するデータファイルのパスが登録されている。サブコンテンツをオープンする際は、データグループ情報５１５を、まずオープンし、所望のコンテンツの属するグループの情報を取得して、取得した情報に基づいてデータファイルを特定することができる。

【０２６１】

なお、コンテンツ管理ユニット（ＣＰＳユニット）として設定されたグループである場合は、各データグループ毎に対応付けられたユニット鍵で暗号化されており、コンテンツ管理ユニット（ＣＰＳユニット）として設定されたグループに属するデータファイルを利用する場合には、ユニット鍵を取得して復号処理を行なうことが必要となる。これらの情報は、サブコンテンツ管理データ部５１４の管理ファイルから取得可能である。

【０２６２】

図１３に示すサブコンテンツデータ部５１３は、すべてのデータグループに属するファイルを混在して設定した構成であるが、例えば図１４に示すサブコンテンツデータ部５２１のように、各データグループ毎のフォルダを設定し、それぞれのデータグループに属するデータ等のファイルをグループ毎にまとめた構成としてもよい。

【０２６３】

図１４に示す構成とした場合には、データグループ情報５２２は、図に示すように、各データグループに対応するディレクトリ名（フォルダ名）を設定したデータとして構成される。サブコンテンツをオープンする際は、データグループ情報５２２を、まずオープンし、所望のコンテンツの属するグループの情報としてのディレクトリ名を取得して、取得した情報に基づいてデータファイルを取得する。

【０２６４】

図１３、図１４に示すデータ格納構成においては、メインコンテンツに対応する管理情報と、サブコンテンツに対応する管理情報とをそれぞれ別々に設定した例を示したが、例えば、図１５に示すように、これらの管理情報をルートに直結するファイルとして設定し、メインコンテンツおよびサブコンテンツに対応するすべての管理情報をまとめて管理する構成としてもよい。

【０２６５】
図１５に示すディレクトリ構成は、メインコンテンツデータ部５５１、サブコンテンツデータ部５５２と、メインコンテンツとサブコンテンツに対応するコンテンツ管理データ部５５３を設定した構成である。
【０２６６】
コンテンツ管理データ部５５３には、メインコンテンツとサブコンテンツの両コンテンツに対応する管理ファイルが格納される。前述した図４に示すようなコンテンツ管理ユニット（ＣＰＳユニット）構成およびユニット鍵を管理したテーブル、すなわち［ユニット構成および鍵管理テーブル］と、図１０を参照して説明した各コンテンツ管理ユニット毎のネットワーク独立状態（Ｄｉｓｃｒｅｔｅ状態）、ネットワーク関連状態（Ｂｏｕｎｄ状態）の状態を管理する［状態管理テーブル］、図１１、図１２を参照して説明した各状態におけるコンテンツの利用、コピー制御情報を格納した［コンテンツ再生およびコピー制御情報管理テーブル］の各テーブルのデータファイルが格納される。
【０２６７】
メインコンテンツ管理データ、サブコンテンツ管理データ、あるいは両者を含むコンテンツ管理データの格納態様には、様々な態様がある。
【０２６８】
図１６にこれらの管理データの格納構成例を示す。管理データは、例えば、下記の態様で格納される。
（Ａ）記録媒体のユーザデータ領域に専用ファイルとして保存
（Ｂ）記録媒体上のユーザデータ領域にあるＡＶフォーマット用ファイルに挿入する。例えばタイトル、インデークスデータファイルや、プレイリスト等のＡＶフォーマット用ファイルに管理テーブルデータを挿入して格納する。
（Ｃ）記録媒体の物理領域、すなわち、ユーザが直接アクセスできない領域に格納する。
（Ｄ）外部のサーバに保存する。
上記（Ａ）～（Ｄ）のいずれかの態様で管理データの格納がなされる。
【０２６９】
なお、管理データの具体例として、［ユニット構成および鍵管理テーブル］、［状態管理テーブル］、［コンテンツ再生およびコピー制御情報管理テーブル］の各テーブルを挙げたが、これらの全てを１つの態様で格納する必要はなく、それぞれのテーブルごとに異なる態様を用いて格納することも可能である。
【０２７０】
記録媒体上のリードイン領域など、物理領域（ユーザが直接アクセスできない領域）に上記３つの情報を保存する場合の例が（Ｃ）である。記録媒体上ではなく、外部のサーバなどに上記３つの情報を保存する場合の例が（Ｄ）である。この場合再生装置は記録媒体の再生開始前に必ず外部のサーバから３つのテーブルに該当する情報を取得しなければならない。
【０２７１】
［９．コンテンツ利用制御情報の暗号化および改ざん防止処理構成］
次に、コンテンツ利用制御情報の暗号化処理と改ざん防止処理構成について説明する。
以下では、
（９－１）において、複数の構成例についての概要について説明し、
（９－２）において、１つの具体的処理構成の詳細について説明する。
【０２７２】
（９－１）コンテンツ利用制御情報の暗号化および改ざん防止処理構成の概要
まず、コンテンツ利用制御情報の暗号化および改ざん防止処理構成の概要について説明する。先に、図１１、図１２を参照して説明した各ＣＰＳユニットに対応するコンテンツに対応するコンテンツ利用制御情報、すなわち、コンテンツ利用、コピー制御情報を格納した［コンテンツ再生およびコピー制御情報管理テーブル］は、不正な改ざんや読み取り

を防止するために、改ざん防止処理を施すとともに、暗号化して格納することが好ましい。

【０２７３】

図１７以下を参照して再生／コピー制御情報の改ざん防止処理、暗号化処理構成について説明する。

【０２７４】

各ＣＰＳユニット毎に設定される再生／コピー制御情報は、図１７に示すように、それぞれ改ざん検証用のデータが付加され、さらに暗号化して格納される。

【０２７５】

例えばＣＰＳユニット１に対応する再生／コピー制御情報１，５７１には、改ざん検証用データ１，５７２が設定される。改ざん検証用データとしては、再生／コピー制御情報に基づく、例えばＳＨＡ－１等のハッシュデータ、あるいは、再生／コピー制御情報に基づくＭＡＣ(Message Authentication code)を設定した構成などが適用される。

【０２７６】

この改ざん検証用データ１，５７２を付加した再生／コピー制御情報１，５７１は、各ＣＰＳユニットに対応して設定されたユニット鍵に基づいて暗号化されて格納される。

【０２７７】

再生／コピー制御情報の格納態様は、図１７（Ａ－１）に示すように、各ＣＰＳユニット毎の再生／コピー制御情報ファイルを設定する態様、図１７（Ａ－２）に示すように、全ＣＰＳユニットの制御情報を、先に図１１を参照して説明した固定長データからなる１つのデータファイルとしてまとめて格納する態様、図１７（Ａ－３）に示すように、全ＣＰＳユニットの制御情報を、先に図１２を参照して説明した可変長データからなる１つのデータファイルとしてまとめて格納する態様がある。

【０２７８】

図１８を参照して、改ざん検証用データとしてハッシュ関数を適用した処理を実行する場合のシーケンスを説明する。

【０２７９】

各ＣＰＳユニットに対応する再生／コピー制御情報データ５８１，５８２は、例えばＳＨＡ－１等のハッシュ生成関数５８３によって、各コピー制御情報データ５８１，５８２に基づくハッシュ値が生成される。

【０２８０】

このハッシュ値を各ＣＰＳユニットに対応する再生／コピー制御情報データ５８１，５８２に対応する改ざん検証用データ５８４，５８５として設定し、再生／コピー制御情報と改ざん検証用データの連結データ５８６，５８７に対して、それぞれのＣＰＳユニットに対応するユニット鍵Ｋｕ１，Ｋｕ２を適用して暗号化を行い格納ファイルとする。

【０２８１】

さらに、ハッシュ関数を適用しない改ざん防止構成について、図１９を参照して説明する。図１９に示す処理は、各ＣＰＳユニットに対応する再生／コピー制御情報データ５９１，５９は、再生／コピー制御情報データを複数回繰り返して連結した連結データ５９３，５９４として設定し、この連結データ５９３，５９４に対して、それぞれのＣＰＳユニットに対応するユニット鍵Ｋｕ１，Ｋｕ２を適用して暗号化を行い格納ファイルとする。

【０２８２】

このような同一データの連結データの暗号化データを格納ファイルとして設定し、ユニット鍵Ｋｕ１，Ｋｕ２を適用して復号した際に、同一データの繰り返しパターンが検出されたか否かに基づいて改ざんの検証を行なうことができる。

【０２８３】

コンテンツの再生処理を実行する情報処理装置は、情報記録媒体に格納されたコンテンツ管理ユニット（ＣＰＳユニット）に対応する暗号化されたコンテンツ利用制御情報、すなわち、再生／コピー制御情報データを取得し、コンテンツ管理ユニットに対応して設定されたユニット鍵を適用した復号処理、および改ざん検証処理を実行し、改ざんの無いこ

との確認を条件として、該コンテンツ利用制御情報に基づくコンテンツ利用処理を実行する。

【０２８４】

（９－２）コンテンツ利用制御情報の暗号化および改ざん防止処理の具体的構成例

次に、コンテンツ利用制御情報の暗号化および改ざん防止処理の具体的構成例について説明する。

【０２８５】

ここで説明する具体例において、コンテンツ利用制御情報としての再生／コピー制御情報は、図１７（Ａ－１）に示す態様、すなわち、各ＣＰＳユニット毎の再生／コピー制御情報に対応する個別ファイルを設定して格納している。

【０２８６】

図２０以下を参照して、コンテンツ利用制御情報としての再生／コピー制御情報の暗号化構成について説明する。

【０２８７】

図２０は、情報記録媒体に格納されるコンテンツ利用制御情報のデータ構成、すなわち、各ＣＰＳユニット毎の再生／コピー制御情報に対応する個別ファイルを構成するデータの記録構成を示す図である。

【０２８８】

図２０（ａ）は、ＣＰＳユニット００１のコンテンツ利用制御情報の情報記録媒体に対する記録データ構成を示している。記録データは、図に示すように、

１８バイトのユーザ制御データ（ＵＣＤ：User Control Data）６０１、

コンテンツ利用制御情報と、改ざん検証用データとしてのハッシュデータを含む２０４８バイトのユーザデータ(User Data)６０２

とから構成されるデータブロックを複数ブロック備えた構成を持つ。コンテンツ利用制御情報のデータ長に応じて利用されるデータブロック数は異なってくる。

【０２８９】

図２０（ａ）に示すＣＰＳユニットａのコンテンツ利用制御情報は、情報記録媒体に格納される複数のＣＰＳユニット中の１つのＣＰＳユニットに対応するコンテンツ利用制御情報である。例えば図２１に示す情報記録媒体に記録される全体データ構成を示すディレクトリ中の、ＣＰＳユニット００１のコンテンツ利用制御情報［ＣＰＳＵｎｉｔ００１．ｃｃｉ］６１０に対応する。

【０２９０】

図２１に示すディレクトリ構成は、コンテンツデータ部６１２と、コンテンツに対応するコンテンツ管理データ部６１１を設定した構成である。コンテンツデータ部６１２に示すＢＤＭＶディレクトリは Ｂｌｕ－ｒａｙ Ｄｉｓｃ ＲＯＭフォーマットに従ったコンテンツ、アプリケーションを保管するディレクトリとして設定されている。

【０２９１】

Ｂｌｕ－ｒａｙ Ｄｉｓｃ ＲＯＭフォーマットに従ったコンテンツは、先に図２、図３を参照して説明したように、タイトル、オブジェクト、プレイリスト、クリップ情報、ＡＶストリーム等の階層構成を持ち、これらを構成するデータファイルがＢＤＭＶディレクトリに設定される。

【０２９２】

管理データ部６１１には、コンテンツに対応する管理ファイルが格納される。例えば、前述した図４に示したコンテンツ管理ユニット（ＣＰＳユニット）毎のＣＰＳユニット鍵を管理したテーブルに対応する情報としてのユニット鍵生成値情報（Ｕｎｉｔ＿Ｋｅｙ＿Ｇｅｎ＿Ｖａｌｕｅ．ｉｎｆ）、さらに、各ユニットに対応して設定されるコンテンツの再生／コピー制御情報としてのコンテンツ利用制御情報（ＣＰＳＵｎｉｔ０ｎｎ．ｃｃｉ）が各ＣＰＳユニット毎に格納される。

【０２９３】

ユニット鍵生成値情報（Ｕｎｉｔ＿Ｋｅｙ＿Ｇｅｎ＿Ｖａｌｕｅ．ｉｎｆ）６０９のデ

ータ構成について、図２２を参照して説明する。図２２は、ユニット鍵生成値情報（Ｕｎｉｔ＿Ｋｅｙ＿Ｇｅｎ＿Ｖａｌｕｅ．ｉｎｆ）ファイルのＳｙｎｔａｘ例である。ユニット鍵生成値情報ファイルは、コンテンツ管理ユニットと各インデックスとの対応情報、およびユニット鍵の生成に用いる乱数情報を定義したデータファイルである。

【０２９４】

すなわち、ユニット鍵生成値情報（Ｕｎｉｔ＿Ｋｅｙ＿Ｇｅｎ＿Ｖａｌｕｅ．ｉｎｆ）ファイルは、先に、図５～図７を参照して説明した情報記録媒体（ディスク）のドライブへの装着時に起動する再生コンテンツとしてのファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）と、メニュー表示機能の起動時に再生するコンテンツとしてのトップメニュー（Ｔｏｐ　Ｍｅｎｕ）の各インデックスと、その他のインデックスとしてのタイトルなどをＣＰＳユニットに対応付けた情報と、ＣＰＳユニットごとに割り当てられた鍵生成用の乱数（Ｖｕ）情報を定義したファイルである。

【０２９５】

ユニット鍵生成値情報（Ｕｎｉｔ＿Ｋｅｙ＿Ｇｅｎ＿Ｖａｌｕｅ．ｉｎｆ）には以下のデータが含まれる。

（ａ）ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）に対応するＣＰＳユニットＮｏ．の指定情報としての［CPS_Unit_number_for_FirstPlayback］

（ｂ）トップメニュー（Ｔｏｐ　Ｍｅｎｕ）に対応するＣＰＳユニットＮｏ．の指定情報としての［CPS_Unit_number for Title］

（ｃ）タイトル番号情報としての［Number of Titles］

（ｄ）各タイトルに対応するＣＰＳユニットＮｏ．の指定情報としての［CPS_Unit_number for Title］

（ｅ）ＣＰＳユニット番号情報としての［Number of CPS_Units］

（ｆ）各ＣＰＳユニットに対応する鍵生成用の乱数（Ｖｕ）情報としての［Unit Key Generation Value for CPS_Unit］

の各情報である。

【０２９６】

なお、ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）対応コンテンツが格納されていない場合は、［CPS_Unit_number_for_FirstPlayback=0］を設定し、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）対応コンテンツが格納されていない場合は、［CPS_Unit_number_for_TopMenu=0］を設定する。また、各タイトル番号（Title#1～Title#）に各ＣＰＳユニット番号が対応付けられて設定される。

【０２９７】

コンテンツの再生／コピー制御情報は、各ＣＰＳユニット毎に個別の情報として設定される。具体的には、

［ＣＰＳユニット１］

記録媒体に対するコピー許容回数：ａ回、再生許容回数：ｂ回、遠隔再生可否：可・・

［ＣＰＳユニット２］

記録媒体に対するコピー許容回数：０回、再生許容回数：ｃ回、遠隔再生可否：否・・

などのように、情報記録媒体に格納された各ＣＰＳユニット毎に個別のコンテンツ利用制御情報が設定されている。

【０２９８】

図２１に示すコンテンツ利用制御情報［ＣＰＳＵｎｉｔ００１．ｃｃｉ］６１０は、ＣＰＳユニット００１に対応するコンテンツ利用制御情報であり、コンテンツ利用制御情報［ＣＰＳＵｎｉｔ００２．ｃｃｉ］は、ＣＰＳユニット００２に対応するコンテンツ利用制御情報である。

【０２９９】

これらは、各ＣＰＳユニットに格納されたコンテンツ、具体的には例えば、図２１に示すディレクトリにおけるクリップＡＶストリームデータ６１３，６１４，６１５の利用制御情報に対応する。

【０３００】
図２３にこれらのＡＶストリームと、ＣＰＳユニットの対応を示すＢｌｕ－ｒａｙ Ｄｉｓｃ ＲＯＭフォーマットに従ったコンテンツ構成図を示す。図２１に示すクリップＡＶストリームデータ６１３，６１４，６１５は、図２３に示すＡＶストリームデータ６１３，６１４，６１５に対応する。
【０３０１】
すなわち、クリップＡＶストリームデータ６１３，６１４は、ＣＰＳユニット＃１に属するデータであり、クリップＡＶストリームデータ６１５は、ＣＰＳユニット＃２に属するデータである。
【０３０２】
従って、クリップＡＶストリームデータ６１３，６１４のコンテンツ再生制御情報は、ＣＰＳユニット００１に対応して設定されたコンテンツ再生制御情報ファイル、例えば、図２１に示すコンテンツ利用制御情報［ＣＰＳＵｎｉｔ００１．ｃｃｉ］６１０であり、クリップＡＶストリームデータ６１５のコンテンツ再生制御情報は、ＣＰＳユニット００２に対応して設定されたコンテンツ再生制御情報ファイル、例えば、図２１に示すコンテンツ利用制御情報［ＣＰＳＵｎｉｔ００２．ｃｃｉ］である。
【０３０３】
情報処理装置において、いずれかのＣＰＳユニットに含まれるコンテンツの利用を行なう際には、そのＣＰＳユニットに対応するコンテンツ利用制御情報を読み取って、読み取った制御情報に従った利用処理を実行する。
【０３０４】
図２０に戻り、コンテンツ利用制御情報の記録構成についての説明を続ける。図２０（ａ）に示す記録データ中の１８バイトの制御データ（ＵＣＤ：User Control Data）６０１は、２０４８バイトのユーザデータ(User Data)６０２ごとに設定される制御データであり、再生制御情報などの制御データによって構成される。ＣＰＳユニット毎の再生／コピー制御情報と、その改ざん検証用データとしてのハッシュ値は、ユーザデータ６０２に格納される。
【０３０５】
各データブロックは、ブロック内に設定されたブロックシード６０３と、各コンテンツ管理ユニット（ＣＰＳユニット）対応のユニット鍵Ｋｕによって生成されるブロック鍵Ｋｂを適用したブロック暗号化が行なわれる。
【０３０６】
ブロック鍵Ｋｂによるブロック暗号化処理について、図２４を参照して説明する。図２４に示すユーザデータ６２１は、１つのデータブロック中のユーザデータ（２０４８バイト）を示している。このユーザデータは、ＣＰＳユニット毎の再生／コピー制御情報を含むデータである。
【０３０７】
ブロック暗号化処理においては、この１つのブロック中のユーザデータ（２０４８バイト）から所定長のブロックシードを抽出し、ブロックシードとユニット鍵Ｋｕに基づく暗号化処理によりブロック鍵Ｋｂを生成してブロックシードを除くデータ部の暗号化処理を行なう。
【０３０８】
図に示す例では、１６バイトのデータをユーザデータの先頭部から抽出し、抽出した１６バイトデータをブロックシード６２２として適用した例を示している。
【０３０９】
図に示すように、ユーザデータから先頭１６バイトのブロックシード６２２は、ステップＳ１１において、ＣＰＳユニット鍵Ｋｕ－ａ６２３による暗号処理、具体的には例えばＡＥＳ暗号処理が実行されて、ブロック鍵Ｋｂ６２４が生成される。
【０３１０】
ここで適用されるＣＰＳユニット鍵Ｋｕ－ａ６２３は、ブロック暗号化の対象データで

あるコンテンツ利用制御情報に対応するユニットのユニット鍵であり、ブロック暗号化の対象データであるコンテンツ利用制御情報がＣＰＳユニットａに対応する制御データである場合、ＣＰＳユニットａに対応するユニット鍵Ｋｕ－ａが適用されることになる。このように、ＣＰＳユニット毎に設定された異なるユニット鍵が適用されてブロック鍵の生成が実行される。

【０３１１】

ステップＳ１１において、ブロック鍵Ｋｂ６２４が生成されると、ステップＳ１２において、ユーザデータ６２１のブロックシード６２２の１６バイトを除くデータ部分、すなわち、２０３２バイトデータ領域を対象としたブロック鍵Ｋｂ６２４を適用した暗号化処理が実行される。例えばＡＥＳ暗号化処理が実行される。

【０３１２】

このブロック暗号化によって、ブロックデータを構成する２０４８バイトのユーザデータは、暗号化のなされていない１６バイトのブロックシード６２２と、ブロック鍵Ｋｂ６２４による暗号化のなされた２０３２バイトの暗号化データとして設定される。このデータが情報記録媒体に記録されることになる。

【０３１３】

ブロックシードは、ユーザデータからの抽出データであり、各ブロック毎に異なるデータとして設定される。従って、共通のＣＰＳユニット鍵Ｋｕを適用した場合であっても、ブロック鍵Ｋｂは、ブロック毎に異なるものとなり、よりセキュリティの高い暗号化処理が行なわれることになる。

【０３１４】

次に、図２５を参照して、ブロック暗号化処理のなされたデータの復号処理シーケンスについて説明する。図２５に示す２０４８バイトのユーザデータ６３１は、図２４を参照して説明したブロック暗号化を施したデータであり、暗号化処理のなされていない１６バイトのブロックシード６２２と、ブロック鍵Ｋｂによる暗号化のなされた２０３２バイトの暗号化データ６３３とによって構成されるデータである。

【０３１５】

図に示すように、ユーザデータから先頭１６バイトのブロックシード６３２は、ステップＳ２１において、ＣＰＳユニット鍵Ｋｕ－ａ６３４による暗号処理、具体的には例えばＡＥＳ暗号処理が実行されて、ブロック鍵Ｋｂ６３５が生成される。

【０３１６】

ここで適用されるＣＰＳユニット鍵Ｋｕ－ａ６３４は、ブロック暗号化の対象データであるコンテンツ利用制御情報に対応するユニットのユニット鍵であり、ブロック暗号化の対象データであるコンテンツ利用制御情報がＣＰＳユニットａに対応する制御データである場合、ＣＰＳユニットａに対応するユニット鍵Ｋｕ－ａが適用されることになる。

【０３１７】

ステップＳ２１において、ブロック鍵Ｋｂ６３５が生成されると、ステップＳ２２において、ユーザデータ６３１のブロックシード６３２の１６バイトを除くデータ部分、すなわち、２０３２バイトの暗号化データ６３３を対象としたブロック鍵Ｋｂ６３５を適用した復号処理が実行される。例えばＡＥＳ復号処理が実行される。

【０３１８】

この復号処理によって、ブロックデータを構成する２０４８バイトのユーザデータは、暗号化のなされていない１６バイトのブロックシード６２２と、ブロック鍵Ｋｂ６３５による復号のなされた２０３２バイトの復号データ６３６となる。このデータは、特定のＣＰＳユニットに対応するコンテンツ利用制御情報であり、コンテンツの再生、利用を行なう情報処理装置は、この制御情報に従ったコンテンツ利用を行なうこととなる。

【０３１９】

なお、図２４、図２５では、１つのブロックに対応する暗号化および復号処理について説明したが、先に図２０を参照して説明したように、ＣＰＳ対応のコンテンツ利用制御情報は、そのデータ長に応じた複数のブロックを使用して記録される。従って、ＣＰＳ対応

のコンテンツ利用制御情報の記録および再生の処理においては、図２４、図２５を参照して説明したブロック単位の処理を複数ブロックに対して実行することになる。

【０３２０】

図２６に、ある１つのＣＰＳユニットａに対応するコンテンツ利用制御情報の記録データの全体構成例を示す。コンテンツ利用制御情報は、複数のブロックデータのユーザデータ領域に分割して格納される。図に示す例は、第１～ｎのｎ個のブロックのユーザデータを使用した例を示している。

【０３２１】

各ブロックから、それぞれユーザデータの先頭１６バイトがシードとして抽出され、ユニット対応のユニット鍵Ｋｕａ６５１を適用した暗号処理による鍵生成が実行される。

【０３２２】

第１ブロックについては、シード１とユニット鍵Ｋｕａ６５１を適用した暗号処理による鍵生成が実行されて、ブロック鍵Ｋｂ１を生成し、ブロック鍵Ｋｂ１を適用して、ユーザデータのシード部を除くデータ領域が暗号化される。同様に、第２ブロックについては、シード２とユニット鍵Ｋｕａ６５１を適用した暗号処理による鍵生成が実行されて、ブロック鍵Ｋｂ２を生成し、ブロック鍵Ｋｂ２を適用して、ユーザデータのシード部を除くデータ領域が暗号化される。以下、すべてのブロックに対して同様の処理が実行されて記録データが生成されることになる。

【０３２３】

次に図２７を参照して、１つのコンテンツ管理ユニット（ＣＰＳユニット）対応のコンテンツ利用制御情報ファイルの記録例、および改ざん検証用データとしてのハッシュ値設定例について説明する。

【０３２４】

図２０～図２６を参照して説明したように、各ＣＰＳユニットの再生／コピー制御情報としてのコンテンツ利用制御情報は、ブロックデータを構成する２０４８バイトのユーザデータ領域に分割されて格納される。

【０３２５】

図２７には、コンテンツ利用制御情報を格納したブロックデータを構成する２０４８バイトのユーザデータ領域としての第１ブロック７０１と、後続ブロック７０２を示している。後続ブロック７０２は、１以上のブロックによって構成される。後続ブロック７０２は、Ｎ個のブロックのユーザデータであり、２０４８×Ｎバイトのデータとする。

【０３２６】

第１ブロック７０１はユーザデータの総バイト数：２０４８バイトであり、

ａ．第１ヘッダ部：１６バイト

ｂ．第１制御情報（ＣＣＩ）領域：２０１２バイト

ｃ．第１ハッシュ値：２０バイト

の各データが格納される。

【０３２７】

ａ．第１ヘッダ部（１６バイト）には、第１制御情報（ＣＣＩ）領域に含まれるコンテンツ利用制御情報（再生／コピー制御情報）のループ数についての情報およびリザーブ領域が設定される。この第１ヘッダ部（１６バイト）のデータがこのブロックに対応するブロック鍵生成のためのシード情報として利用される。

【０３２８】

図２０～図２６を参照して説明したようにシード情報は、ブロック暗号化対象領域とはならないため、平文データのまま情報記録媒体に格納されることになる。従って、シード情報として利用されるブロックデータのユーザデータ領域の先頭１６バイトデータに、各ＣＰＳユニットの再生／コピー制御情報としてのコンテンツ利用制御情報を含めると、制御情報の具体的な内容が漏洩してしまう可能性がある。そこでこの先頭１６バイト領域をヘッダ情報領域として設定し、秘密性の低いデータを格納する構成としている。

【０３２９】

ヘッダ部に続くｂ．第１制御情報（ＣＣＩ）領域（２０１２バイト）には、各ＣＰＳユニット対応のコンテンツ利用制御情報（再生／コピー制御情報）が格納される。

【０３３０】

図２７には、第１ブロック７０１のコンテンツ利用制御情報（再生／コピー制御情報）として、

基本制御情報（Ｂａｓｉｃ　ＣＣＩ）と、

拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）

これら２つの種類の制御情報を含めた例を示している。図に示す例では、１つの基本制御情報（Ｂａｓｉｃ　ＣＣＩ）と、４つの拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）Ａ～Ｄの合計５つの情報ブロックが格納された例を示している。

【０３３１】

基本制御情報（Ｂａｓｉｃ　ＣＣＩ）は、ベーシックな最低限のコンテンツ利用制御情報（再生／コピー制御情報）によって構成されたデータであり、所定のコンテンツ再生処理プログラムに従ってコンテンツ再生処理を実行するほぼすべての情報処理装置において読み取られ、制御情報に従った処理を実行することが要請される情報である。一方、拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）は、高度なコンテンツ利用処理、例えば、ネットワーク転送や、データのストリーミング送受信などの処理機能を持つ情報処理装置に適用するための拡張的なコンテンツ利用制御情報（再生／コピー制御情報）によって構成されたデータである。

【０３３２】

基本制御情報（Ｂａｓｉｃ　ＣＣＩ）については再生／コピー制御情報格納ファイルから迅速に取り出すことが要求される。また、拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）は、将来の拡張のためにサイズなどの制限が少ない格納方法が採用されている。基本制御情報（Ｂａｓｉｃ　ＣＣＩ）と、拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）の具体例を図２８に示す。

【０３３３】

図２８に示すように、基本制御情報(Ｂａｓｉｃ　ＣＣＩ）には、例えば以下の制御情報が含まれる。

コピー可/不可情報：コピー可／不可／１世代のみ可

映像出力解像度制限情報：出力制限有り／無し

アナログコピー制御情報：可／不可（使用するアナログコピー防止技術を指定）

暗号化の有無を示す情報：暗号化有り／無し

権利主張の有無を示す情報：権利主張有り／無し

【０３３４】

また、拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）には、例えば以下の制御情報が含まれる。

情報記録媒体（Ｄｉｓｃ）単体での再生可否情報：情報記録媒体（Ｄｉｓｃ）上の情報だけでコンテンツ再生が可能かどうかを示す

情報記録媒体（Ｄｉｓｃ）単体では再生できないコンテンツの再生方法：「鍵配信サーバへ接続」、「鍵の入ったメモリカード挿入」など

サーバの指定：サーバリストへのインデックス値

コピー・ストリーミング互換性情報：コンテンツをネットワーク内の他の機器で再生するための互換性情報

コピー・ストリーミング時のデータ変換方式：コンテンツを他の機器用に変換する際に使用できる方式

【０３３５】

さらに、

ネットワーク内の同種記録媒体へのコピー可否他コピー制限情報、

携帯機器へのコピー可否他コピー制限情報

ストリーミング、遠隔再生の可否等の情報

ダウンロード処理に対する制御情報、
サーバから動作制御情報を取得するための情報
などによって構成される。
なお、拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）は、任意の制御情報が設定可能である。

【０３３６】
図２７に戻り、コンテンツ利用制御情報を格納したブロックデータを構成する２０４８バイトのユーザデータ領域としての第１ブロック７０１の構成データについて説明を続ける。

【０３３７】
第１ブロック７０１には、上述した
ａ．第１ヘッダ部：１６バイト
ｂ．第１制御情報（ＣＣＩ）領域：２０１２バイト
の各データに基づいて生成された第１ハッシュ値（２０バイト）が格納される。このハッシュ値は、第１ヘッダ部のデータと、第１制御情報（ＣＣＩ）領域の各データに対して、例えばＳＨＡ－１等のハッシュ関数を適用して生成したデータであり、第１ヘッダ部のデータと、第１制御情報（ＣＣＩ）領域の各データの改ざん検証用データとして設定される。

【０３３８】
なお、ハッシュ値のサイズは使用するハッシュ関数によって異なり、図２７ではＳＨＡ－１を使用した例として１６０ビット（２０バイト）のハッシュ値を使用した例を示しているが、異なるハッシュ関数・ハッシュ値長を用いることも可能である。第１ハッシュ値はファイルの先頭からハッシュ値を記録する領域の直前まで（ＳＨＡ－１を使用する場合は先頭から２０２８バイトの領域）をハッシュ関数に入力して得られた値を使用する。

【０３３９】
コンテンツ利用制御情報を読み取り、利用制御情報に従ったコンテンツ利用を実行する情報処理装置は、第１ヘッダ部のデータと、第１制御情報（ＣＣＩ）領域の各データに基づくハッシュ値を算出し、算出ハッシュ値と、ブロックデータのユーザデータ領域に格納されたハッシュ値との比較を実行し、一致する場合はデータ改ざんなしと判定し、処理を続行する。一致しない場合は、データ改ざんありと判定し、コンテンツ利用制御情報に従ったコンテンツ再生、利用処理を中止する。

【０３４０】
図２７に示す後続ブロック７０２は、Ｎ個のブロックのユーザデータであり、２０４８×Ｎバイトのデータによって構成される。
後続ブロック７０２のユーザデータには、以下のデータが格納される。
ａ．第２ヘッダ部：１６バイト
ｂ．第２制御情報（ＣＣＩ）領域：任意バイト
ｃ．全体ハッシュ値：２０バイト
の各データが格納される。

【０３４１】
ａ．第２ヘッダ部：１６バイトは、第１ブロック７０１に続く第２ブロックのユーザデータの先頭１６バイトであり、この領域には、第２制御情報（ＣＣＩ）領域に含まれるコンテンツ利用制御情報（再生／コピー制御情報）のループ数についての情報およびリザーブ領域が設定される。この第２ヘッダ部（１６バイト）のデータは、第２ブロックの先頭２０４８バイトに対応するブロック鍵生成のためのシード情報として利用される。

【０３４２】
ｂ．第２制御情報（ＣＣＩ）領域：任意バイトは、後続ブロック７０２のデータサイズ（２０４８×Ｎ）バイトからヘッダ部と全体ハッシュのデータ部分を除いた（２０４８×Ｎ－（１６＋２０））バイトを超えない範囲で複数のコンテンツ利用制御情報（再生／コピー制御情報）を格納する領域として設定される。図２７に示す例では拡張制御情報（Ｅ

ｘｔｅｎｄｅｄ　ＣＣＩ）Ｅ～Ｉの合計５つの情報ブロックが格納された例を示している。

【０３４３】

なお、後続ブロック７０２が複数ブロックを使用する場合は、各ブロックのユーザデータの先頭１６バイトデータは、それぞれのブロックのブロック鍵生成情報としてのシード領域とされる。このシード領域には、コンテンツ利用制御情報（再生／コピー制御情報）の構成データを格納するか、または第２ヘッダと同様の情報を格納するか、またはダミーデータを格納する構成とする。

【０３４４】

全体ハッシュ値：２０バイトは、
第１ブロック７０１の全体データと、
後続ブロック７０２の
第２ヘッダ部：１６バイト
第２制御情報（ＣＣＩ）領域：任意バイト

の全データに基づいて生成された全体ハッシュ値（２０バイト）が格納される。この全体ハッシュ値は、第１ブロック７０１の全体データと、後続ブロック７０２の第２ヘッダと、第２制御情報（ＣＣＩ）の全体データに対して、例えばＳＨＡ－１等のハッシュ関数を適用して生成したデータであり、第１ブロック７０１の全体データと、後続ブロック７０２の第２ヘッダと、第２制御情報（ＣＣＩ）の全体データの改ざん検証用データとして設定される。

【０３４５】

なお、ハッシュ値のサイズは使用するハッシュ関数によって異なり、図２７ではＳＨＡ－１を使用した例として１６０ビット（２０バイト）のハッシュ値を使用した例を示しているが、異なるハッシュ関数・ハッシュ値長を用いることも可能である。全体ハッシュ値はファイルの先頭からハッシュ値を記録する領域の直前まで（ＳＨＡ－１を使用する場合は先頭から［ファイルサイズ－２０］バイトの領域）をハッシュ関数に入力して得られた値を使用する。

【０３４６】

コンテンツ利用制御情報を読み取り、利用制御情報に従ったコンテンツ利用を実行する情報処理装置において、拡張制御情報に従った高度なコンテンツ利用処理を実行する装置は、第１ブロックのハッシュ値検証を行なわず、全体ハッシュ値に基づくデータ改ざん検証を実行する。

【０３４７】

すなわち、コンテンツ利用を実行する情報処理装置は、第１ブロック７０１の全データと、後続ブロック７０２の第２ヘッダと、第２制御情報（ＣＣＩ）に基づくハッシュ値を算出し、算出ハッシュ値と、後続ブロック７０２のユーザデータ領域に格納された全体ハッシュ値との比較を実行し、一致する場合はデータ改ざんなしと判定し、処理を続行する。一致しない場合は、データ改ざんありと判定し、コンテンツ利用制御情報に従ったコンテンツ再生、利用処理を中止する。

【０３４８】

このように、高度なコンテンツ利用を行い、拡張制御情報に従った高度なコンテンツ利用処理を実行する装置は、第１ブロックのみならず、第２ブロック以降の後続ブロックに含まれるデータに基づくハッシュ値を算出し、これを全体ハッシュ値と比較照合する処理を実行し、一方、高度なコンテンツ利用を行わず、基本制御情報のみに従ったコンテンツ利用処理を実行する装置は、第１ブロック７０１に設定された情報に基づくハッシュ値算出を実行して、第１ブロック７０１に設定された第１ハッシュ値との比較照合を実行すればよい。

【０３４９】

図２７に示すコンテンツ利用制御情報の格納構成、ハッシュ値設定構成には、以下の３つの利点を有する。

（１）先頭２０４８バイト（第１ブロック）のブロック鍵の生成、復号処理と、ハッシュ値照合による改ざん検証によって基本制御情報の取得、検証が可能となる。
（２）拡張制御情報のサイズが小さい場合は拡張制御情報も併せて先頭２０４８バイト（第１ブロック）中に格納することで、先頭２０４８バイト（第１ブロック）のブロック鍵の生成、復号処理と、ハッシュ値照合による改ざん検証によって基本制御情報および拡張制御情報の取得、検証が可能となる。
（３）拡張制御情報のサイズが大きい場合は、第２ブロック以下の後続ブロックを使用してコンテンツ利用制御情報を格納することが可能となる。

【０３５０】

図２９は、図２７に示すコンテンツ利用制御情報の格納例に対応するシンタックス図である。

【０３５１】

先頭２０４８バイトからなる第１ブロック領域データ７２１と、それ以降に配置され２０４８バイトの整数倍のサイズを持つ後続ブロック領域データ７２２が存在する。

【０３５２】

第１ブロック領域データ７２１は、ヘッダ部情報として、
第１ブロック領域内に記述されるコンテンツ利用制御情報（再生/コピー制御情報）を構成する情報ブロック（ループ）の数を示す情報としての［Number_of_Primary_CCI_loop］：１６ビット
リザーブ［reserved］領域：１１２ビット
が設定される。上記データがヘッダ部の１６バイトデータである。

【０３５３】

さらに、第１制御情報（ＣＣＩ）領域情報として、
コンテンツ利用制御情報（再生/コピー制御情報）のデータタイプ情報としての［CCI_and_other_info_type］：１６ビット、
コンテンツ利用制御情報（再生/コピー制御情報）のデータ長情報としての［CCI_and_other_info_data_length］：１６ビット、
コンテンツ利用制御情報（再生/コピー制御情報）のデータ値情報としての［CCI_and_other_info_data］：（CCI_and_other_info_data_length×８）ビット、
リザーブ［reserved］領域：Ｘビット、
が設定される。

【０３５４】

さらに、上述の第１ブロック構成データに基づいて算出されたハッシュ値としての［Hash_value_for_Primary_CCI］：１６０ビット
が設定される。

【０３５５】

後続ブロック領域データ７２２も、データ構成は、第１ブロック領域とほぼ同様であり、ループ数を示す情報とリザーブ領域によって構成されるヘッダと、データタイプ、データ長、データ値を含むコンテンツ利用制御情報（再生/コピー制御情報）部と、リザーブ領域、および全体ハッシュ値［Hash_value_for_All_CCI］：１６０ビットが設定される。

【０３５６】

全体ハッシュ値［Hash_value_for_All_CCI］：１６０ビットは、第１ブロック領域データ７２１の全体データと、後続ブロック領域データ７２２の全体ハッシュ値を除くデータに基づいて生成されたハッシュ値である。

【０３５７】

次に図３０を参照して、図２７の態様とは異なるコンテンツ利用制御情報ファイルの記録例、および改ざん検証用データとしてのハッシュ値設定例について説明する。

【０３５８】

図２７のコンテンツ利用制御情報ファイルの記録例では、第１ブロック領域に基本制御情報と、拡張制御情報の双方を格納する構成として説明したが、図３０に示す例は、第１

ブロックは、基本制御情報のみを格納する領域とし、拡張制御情報についてはすべて第２ブロック以下の後続ブロックに格納する構成である。

【０３５９】

図３０を参照して、本実施例におけるコンテンツ利用制御情報ファイルの記録構成を説明する。

【０３６０】

図３０には、コンテンツ利用制御情報を格納したブロックデータを構成する２０４８バイトのユーザデータ領域としての第１ブロック７５１と、後続ブロック７５２を示している。後続ブロック７５２は、１以上のブロックによって構成される。後続ブロック７０２は、Ｎ個のブロックのユーザデータであり、２０４８×Ｎバイトのデータとする。

【０３６１】

第１ブロック７５１はユーザデータの総バイト数：２０４８バイトであり、

ａ．基本ヘッダ部：１６バイト

ｂ．基本制御情報（ＣＣＩ）領域：２０１２バイト

ｃ．基本ハッシュ値：２０バイト

の各データが格納される。

【０３６２】

ａ．基本ヘッダ部（１６バイト）には、第１ブロック７５１の基本制御情報（ＣＣＩ）領域に含まれるコンテンツ利用制御情報（再生／コピー制御情報）のループ数についての情報およびリザーブ領域が設定される。この基本ヘッダ部（１６バイト）のデータがこのブロックに対応するブロック鍵生成のためのシード情報として利用される。

【０３６３】

ヘッダ部に続くｂ．基本制御情報（ＣＣＩ）領域（２０１２バイト）には、各ＣＰＳユニット対応のコンテンツ利用制御情報（再生／コピー制御情報）の中の基本制御情報（Ｂａｓｉｃ　ＣＣＩ）のみが格納される。拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）は、第１ブロック７５１には格納されず、すべて後続ブロック７５２に格納される。図に示す例では、第１ブロック７５１に５つの基本制御情報（Ｂａｓｉｃ　ＣＣＩ）Ａ～Ｅの合計５つの情報ブロックが格納された例を示している。

【０３６４】

前述したように、基本制御情報（Ｂａｓｉｃ　ＣＣＩ）は、ベーシックな最低限のコンテンツ利用制御情報（再生／コピー制御情報）によって構成されたデータであり、所定のコンテンツ再生処理プログラムに従ってコンテンツ再生処理を実行するほぼすべての情報処理装置において読み取られ、制御情報に従った処理を実行することが要請される情報である。

【０３６５】

第１ブロック７５１には、さらに、基本ヘッダ：１６バイトと、基本制御情報（ＣＣＩ）領域：２０１２バイトの各データに基づいて生成された基本ハッシュ値（２０バイト）が格納される。このハッシュ値は、基本ヘッダと、基本制御情報（ＣＣＩ）データに対して、例えばＳＨＡ－１等のハッシュ関数を適用して生成したデータであり、これらのデータの改ざん検証用データとして設定される。なお、ハッシュ値のサイズは使用するハッシュ関数によって異なり、図３０ではＳＨＡ－１を使用した例として１６０ビット（２０バイト）のハッシュ値を使用した例を示しているが、異なるハッシュ関数・ハッシュ値長を用いることも可能である。第１ハッシュ値はファイルの先頭からハッシュ値を記録する領域の直前まで（ＳＨＡ－１を使用する場合は先頭から２０２８バイトの領域）をハッシュ関数に入力して得られた値を使用する。

【０３６６】

基本制御情報のみの制御に従ったコンテンツ利用を実行する情報処理装置は、基本ヘッダ部のデータと、基本制御情報（ＣＣＩ）領域の各データに基づくハッシュ値を算出し、算出ハッシュ値と、ブロックデータのユーザデータ領域に格納されたハッシュ値との比較を実行し、一致する場合はデータ改ざんなしと判定し、処理を続行する。一致しない場合

は、データ改ざんありと判定し、コンテンツ利用制御情報に従ったコンテンツ再生、利用処理を中止する。

【０３６７】

基本制御情報のみの制御に従ったコンテンツ利用を実行する情報処理装置は、第２ブロック以下の情報読み取りおよびハッシュ算出等の処理を実行する卒用がなく、効率的な処理が可能となる。

【０３６８】

図３０に示す後続ブロック７５２は、Ｎ個のブロックのユーザデータであり、２０４８×Ｎバイトのデータによって構成される。

後続ブロック７５２のユーザデータには、以下のデータが格納される。

ａ．拡張ヘッダ部：１６バイト

ｂ．拡張制御情報（ＣＣＩ）領域：任意バイト

ｃ．全体ハッシュ値：２０バイト

の各データが格納される。

【０３６９】

ａ．拡張ヘッダ部：１６バイトは、第１ブロック７５１に続く第２ブロックのユーザデータの先頭１６バイトであり、この領域には、拡張制御情報（ＣＣＩ）領域に含まれるコンテンツ利用制御情報（再生／コピー制御情報）のループ数についての情報およびリザーブ領域が設定される。この拡張ヘッダ部（１６バイト）のデータは、第２ブロックに対応するブロック鍵生成のためのシード情報として利用される。

【０３７０】

ｂ．拡張制御情報（ＣＣＩ）領域：任意バイトは、後続ブロック７５２のデータサイズ（２０４８×Ｎ）バイトからヘッダ部と全体ハッシュのデータ部分を除いた（２０４８×Ｎ－（１６＋２０））バイトを超えない範囲で複数のコンテンツ利用制御情報（再生／コピー制御情報）を格納する領域として設定される。この後続ブロック７５２には、第１ブロック７５１に格納された基本制御情報を除く拡張制御情報のみが格納される。図３０に示す例では拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）Ａ～Ｅの合計５つの情報ブロックが格納された例を示している。

【０３７１】

なお、後続ブロック７５２が複数ブロックを使用して拡張制御情報を格納している場合は、各ブロックのユーザデータの先頭１６バイトデータは、それぞれのブロックのブロック鍵生成情報としてのシード領域とされる。このシード領域には、コンテンツ利用制御情報（再生／コピー制御情報）の構成データを格納するか、または第２ブロックの先頭の拡張ヘッダと同様の情報を格納するか、またはダミーデータを格納する構成とする。

【０３７２】

全体ハッシュ値：２０バイトは、

第１ブロック７５１の全体データと、

後続ブロック７５２の

拡張ヘッダ部：１６バイト

拡張制御情報（ＣＣＩ）領域：任意バイト

の全データに基づいて生成された全体ハッシュ値（２０バイト）が格納される。この全体ハッシュ値は、第１ブロック７５１の全体データと、後続ブロック７５２の拡張ヘッダと、拡張制御情報（ＣＣＩ）の全体データに対して、例えばＳＨＡ－１等のハッシュ関数を適用して生成したデータであり、これらの全データの改ざん検証用データとして設定される。ハッシュ値のサイズは使用するハッシュ関数によって異なり、図３０ではＳＨＡ－１を使用した例として１６０ビット（２０バイト）のハッシュ値を使用した例を示しているが、異なるハッシュ関数・ハッシュ値長を用いることも可能である。

【０３７３】

コンテンツ利用制御情報を読み取り、利用制御情報に従ったコンテンツ利用を実行する情報処理装置中、拡張制御情報に従った高度なコンテンツ利用処理を実行する装置は、第

１ブロックのハッシュ値検証を行なわず、全体ハッシュ値に基づくデータ改ざん検証を実行し、データ改ざんなしとの判定があった場合にのみ処理を続行しコンテンツの利用を行なう。データ改ざんありの判定がなされた場合は、コンテンツ利用制御情報に従ったコンテンツ再生、利用処理を中止する。

【０３７４】

このように、本実施例の構成では、基本制御情報によってコンテンツの利用を行なう情報処理装置は、第１ブロック７５１のデータのみの復号、ハッシュ検証を実行すればよく、後続ブロック７５２に対する復号処理や、ハッシュ算出、検証を省略可能となり効率的な処理が可能となる。

【０３７５】

図３１は、図３０に示すコンテンツ利用制御情報の格納例に対応するシンタックス図である。

【０３７６】

先頭２０４８バイトからなる第１ブロック領域データ７７１と、それ以降に配置され２０４８バイトの整数倍のサイズを持つ後続ブロック領域データ７７２が存在する。

【０３７７】

第１ブロック領域データ７７１は、ヘッダ部情報として、

基本制御情報（ＣＣＩ）領域内に記述されるコンテンツ利用制御情報（再生/コピー制御情報）を構成する情報ブロック（ループ）の数を示す情報としての［Number_of_Basic_CCI_loop］：１６ビット

リザーブ［reserved］領域：１１２ビット

が設定される。上記データがヘッダ部の１６バイトデータである。

【０３７８】

さらに、基本制御情報（ＣＣＩ）領域情報として、

コンテンツ利用制御情報（再生/コピー制御情報）のデータタイプ情報としての［CCI_and_other_info_type］：１６ビット、

コンテンツ利用制御情報（再生/コピー制御情報）のデータ長情報としての［CCI_and_other_info_data_length］：１６ビット、

コンテンツ利用制御情報（再生/コピー制御情報）のデータ値情報としての［CCI_and_other_info_data］：（CCI_and_other_info_data_length×８）ビット、

リザーブ［reserved］領域：Ｘビット、

が設定される。

【０３７９】

さらに、上述の第１ブロック構成データに基づいて算出されたハッシュ値としての［Hash_value_for_Basic_CCI］：１６０ビット

が設定される。

【０３８０】

後続ブロック領域データ７７２も、データ構成は、第１ブロック領域とほぼ同様であり、ループ数を示す情報とリザーブ領域によって構成されるヘッダと、データタイプ、データ長、データ値を含むコンテンツ利用制御情報（再生/コピー制御情報）部と、リザーブ領域、および全体ハッシュ値［Hash_value_for_All_CCI］：１６０ビットが設定される。

【０３８１】

全体ハッシュ値［Hash_value_for_All_CCI］：１６０ビットは、第１ブロック領域データ７７１の全体データと、後続ブロック領域データ７７２の全体ハッシュ値を除くデータに基づいて生成されたハッシュ値である。

【０３８２】

上述したように、コンテンツ利用制御情報（再生/コピー制御情報）には、基本制御情報（Ｂａｓｉｃ　ＣＣＩ）と、拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）があり、基本制御情報（Ｂａｓｉｃ　ＣＣＩ）は、ベーシックな最低限のコンテンツ利用制御情報（再生／コピー制御情報）によって構成されたデータであり、所定のコンテンツ再生処理プロ

グラムに従ってコンテンツ再生処理を実行するほぼすべての情報処理装置において読み取られ、制御情報に従った処理を実行することが要請される情報である。一方、拡張制御情報（Ｅｘｔｅｎｄｅｄ　ＣＣＩ）は、高度なコンテンツ利用処理、例えば、ネットワーク転送や、データのストリーミング送受信などの処理機能を持つ情報処理装置に適用するための拡張的なコンテンツ利用制御情報（再生／コピー制御情報）によって構成されたデータである。

【０３８３】

このような異なるカテゴリのコンテンツ利用制御情報（再生/コピー制御情報）を情報記録媒体から読み取って、各制御情報に従った処理を実行する情報処理装置における処理シーケンスについて、図３２、図３３を参照して説明する。

【０３８４】

図３２は、基本制御情報のみを読み取り、基本制御情報に従ったコンテンツ利用を実行する情報処理装置の処理シーケンスである。

【０３８５】

ステップＳ１０１において、情報処理装置は、ある特定のＣＰＳユニットに対応するコンテンツ制御情報ファイル（ＣＣＩファイル）を選択し、そのファイルの第１ブロックに相当するデータ領域である先頭２０４８バイトを読み出す。

【０３８６】

ステップＳ１０２において、読み出した第１ブロックの２０４８バイトデータの先頭１６バイトを取得し、これをシードとして、ＣＰＳユニット鍵による暗号化、例えばＡＥＳ暗号処理を適用した鍵生成処理を実行して、ブロック鍵Ｋｂを生成する。ここで適用するＣＰＳユニット鍵は、読み出しを実行したコンテンツ制御情報ファイル（ＣＣＩファイル）に対応付けられたコンテンツ管理ユニット（ＣＰＳユニット）に対応するＣＰＳユニット鍵である。

【０３８７】

ステップＳ１０３において、生成したブロック鍵Ｋｂを適用して、ステップＳ１０１において読み出した第１ブロックの２０４８バイトデータの先頭１６バイトを除くブロック暗号化データ領域の復号処理を実行する。例えばＡＥＳ暗号アルゴリズムに基づく復号処理を実行する。

【０３８８】

ステップＳ１０４において、復号結果として得られたブロックデータのハッシュ部データ２０バイトを除く２０２８バイトのデータに基づいてハッシュ値Ｘを算出する。ハッシュ値算出アルゴリズムは例えばＳＨＡ－１が適用される。

【０３８９】

ステップＳ１０５において、算出ハッシュ値と、ブロックデータに書き込まれたハッシュ値（ブロックデータの第２０２８～２０４７バイトの２０バイトデータ）との比較照合処理を実行する。

【０３９０】

算出ハッシュ値と読み取られたハッシュ値が一致していない場合は、ステップＳ１０７に進み、データ改ざんありと判定し、コンテンツ制御情報に従ったコンテンツ利用を中止する。

【０３９１】

算出ハッシュ値と読み取られたハッシュ値が一致している場合は、ステップＳ１０６に進み、データ改ざんなしと判定し、コンテンツ制御情報を取得して、取得したコンテンツ制御情報に従ったコンテンツ利用を実行する。この場合の制御情報は、基本制御情報であり、情報処理装置は、基本制御情報に従ったコンテンツ利用処理を実行する。

【０３９２】

次に、図３３を参照して、基本制御情報と拡張制御情報の双方を読み取り、基本制御情報および拡張制御情報に従ったコンテンツ利用を実行する情報処理装置の処理シーケンスについて説明する。

【０３９３】
ステップＳ２０１において、情報処理装置は、ある特定のＣＰＳユニットに対応するコンテンツ制御情報ファイル（ＣＣＩファイル）を選択し、そのファイルの第１ブロックに相当するデータ領域である先頭２０４８バイトを読み出す。
【０３９４】
ステップＳ２０２において、読み出した第１ブロックの２０４８バイトデータの先頭１６バイトを取得し、これをシードとして、ＣＰＳユニット鍵による暗号化、例えばＡＥＳ暗号処理を適用した鍵生成処理を実行して、ブロック鍵Ｋｂを生成する。ここで適用するＣＰＳユニット鍵は、読み出しを実行したコンテンツ制御情報ファイル（ＣＣＩファイル）に対応付けられたコンテンツ管理ユニット（ＣＰＳユニット）に対応するＣＰＳユニット鍵である。
【０３９５】
ステップＳ２０３において、生成したブロック鍵Ｋｂを適用して、ステップＳ２０１において読み出した第１ブロックの２０４８バイトデータの先頭１６バイトを除くブロック暗号化データ領域の復号処理を実行する。例えばＡＥＳ暗号アルゴリズムに基づく復号処理を実行する。
【０３９６】
ステップＳ２０４では、コンテンツ制御情報ファイル（ＣＣＩファイル）を構成する全ブロックデータの読み出し、復号が終了したか否かを判定し、終了していない場合は、ステップＳ２０１に戻り、後続ブロックについて同様の処理、すなわち、シード取得、ブロック鍵Ｋｂ生成、復号処理を繰り返し実行する。
【０３９７】
コンテンツ制御情報ファイル（ＣＣＩファイル）を構成する全ブロックデータの読み出し、復号が終了したと判定すると、ステップＳ２０５に進む。
【０３９８】
ステップＳ２０５では、復号結果として得られたコンテンツ制御情報ファイル（ＣＣＩファイル）を構成する全ブロックデータ中、全体ハッシュ部データ２０バイトを除く全データに基づいてハッシュ値Ｘを算出する。ハッシュ値算出アルゴリズムは例えばＳＨＡ－１が適用される。
【０３９９】
ステップＳ２０６において、算出ハッシュ値と、コンテンツ制御情報ファイル（ＣＣＩファイル）から読み取った全体ハッシュ値との比較照合処理を実行する。
【０４００】
算出ハッシュ値と読み取られたハッシュ値が一致していない場合は、ステップＳ２０８に進み、データ改ざんありと判定し、コンテンツ制御情報に従ったコンテンツ利用を中止する。
【０４０１】
算出ハッシュ値と読み取られたハッシュ値が一致している場合は、ステップＳ２０７に進み、データ改ざんなしと判定し、コンテンツ制御情報を取得して、取得したコンテンツ制御情報に従ったコンテンツ利用を実行する。この場合の制御情報は、基本制御情報および拡張制御情報であり、情報処理装置は、これらの制御情報に従ったコンテンツ利用処理を実行する。
【０４０２】
［１０．情報処理装置の構成例］
次に、図３４を参照して、上述のコンテンツ管理ユニット（ＣＰＳユニット）構成を持つメインコンテンツ、サブコンテンツの記録処理または再生処理を行う情報処理装置の構成例について説明する。
【０４０３】
情報処理装置８００は、情報記録媒体８９１の駆動を行ない、データ記録再生信号の入手力を行なうドライブ８９０、各種プログラムに従ったデータ処理を実行するＣＰＵ８７

０、プログラム、パラメータ等の記憶領域としてのＲＯＭ８６０、メモリ８８０、デジタル信号を入出力する入出力Ｉ／Ｆ８１０、アナログ信号を入出力し、Ａ／Ｄ，Ｄ／Ａコンバータ８４１を持つ入出力Ｉ／Ｆ８４０、ＭＰＥＧデータのエンコード、デコード処理を実行するＭＰＥＧコーデック８３０、ＴＳ（Transport Stream）・ＰＳ(Program Stream)処理を実行するＴＳ・ＰＳ処理手段８２０、各種の暗号処理を実行する暗号処理手段８５０を有し、バス８０１に各ブロックが接続されている。

【０４０４】

まず、データ記録時の動作について説明する。記録を行うデータとしてデジタル信号入力とアナログ信号入力の２つのケースが想定される。

【０４０５】

デジタル信号の場合、デジタル信号用入出力Ｉ／Ｆ８１０から入力され、必要に応じて暗号化処理手段８５０によって適切な暗号化処理を施したデータを情報記録媒体８９１に保存する。また、入力されたデジタル信号のデータ形式を変換して保存する場合、ＭＰＥＧコーデック８３０およびＣＰＵ８７０、ＴＳ・ＰＳ処理手段８２０によって保存用のデータ形式に変換を行い、その後暗号化処理手段８５０で適切な暗号化処理を施して情報記録媒体８９１に保存する。

【０４０６】

アナログ信号の場合、入出力Ｉ／Ｆ８４０へ入力されたアナログ信号はＡ／Ｄコンバータ８４１によってデジタル信号となり、ＭＰＥＧコーデック８３０によって記録時に使用されるコーデックへと変換される。その後、ＴＳ・ＰＳ処理手段８２０により、記録データの形式であるＡＶ多重化データへ変換され、必要に応じて暗号化処理手段８５０によって適切な暗号化処理を施したデータが記録媒体８９１に保存される。

【０４０７】

例えば、ＭＰＥＧ－ＴＳデータによって構成されるＡＶストリームデータからなるメインコンテンツの記録を行なう場合、メインコンテンツは、コンテンツ管理ユニット（ＣＰＳユニット）に区分された後、ユニット鍵による暗号化処理が暗号処理手段８５０によって暗号化され、ドライブ８９０を介して記録媒体８９１に記録される。

【０４０８】

サブコンテンツについても、各データグループ対応のコンテンツ管理ユニット（ＣＰＳユニット）に区分された後、ユニット鍵による暗号化処理が暗号処理手段８５０によって暗号化され、ドライブ８９０を介して記録媒体８９１に記録される。

【０４０９】

なお、前述した各管理情報、すなわち、

［ユニット構成および鍵管理テーブル］

［状態管理テーブル］

［コンテンツ再生およびコピー制御情報管理テーブル］

についても、適宜、作成または更新し、必要に応じて改ざん検証用データとして、また暗号化データとして記録媒体８９１上に保存する。

【０４１０】

次に、情報記録媒体からのデータ再生を行なう場合の処理について説明する。例えばメインコンテンツとしてのＭＰＥＧ－ＴＳデータからなるＡＶストリームデータの再生を行う場合、ドライブ８９０において情報記録媒体８９１から読み出されたデータはコンテンツ管理ユニットとして識別されると、コンテンツ管理ユニットに対応するユニット鍵の取得処理が実行され、取得されたユニット鍵に基づいて、暗号化処理手段８５０で暗号を解きＴＳ（Transport Stream）・ＰＳ(Program Stream)処理手段８２０によってＶｉｄｅｏ、Ａｕｄｉｏ、字幕などの各データに分けられる。

【０４１１】

ＭＰＥＧコーデック８３０において復号されたデジタルデータは入出力Ｉ／Ｆ８４０内のＤ／Ａコンバータ８４１によってアナログ信号に変換され出力される。またデジタル出力を行う場合、暗号化処理手段８５０で復号されたＭＰＥＧ－ＴＳデータは入出力ＩＦ８

１０を通してデジタルデータとして出力される。この場合の出力は例えばＩＥＥＥ１３９４やイーサネットケーブル、無線ＬＡＮなどのデジタルインターフェースに対して行われる。なお、ネットワーク接続機能に対応する場合入出力ＩＦ８１０はネットワーク接続の機能を備える。また、再生装置内で出力先機器が受信可能な形式にデータ変換をして出力を行う場合、一旦、ＴＳ・ＰＳ処理手段８２０で分離したＶｉｄｅｏ、Ａｕｄｉｏ、字幕などに対してＭＰＥＧコーデック８３０においてレート変換、コーデック変換処理を加え、ＴＳ・ＰＳ処理手段８２０で再度ＭＰＥＧ－ＴＳやＭＰＥＧ－ＰＳなどに多重化を行ったデータをデジタル用入出力Ｉ／Ｆ８１０から出力する。または、ＣＰＵ８７０を使用してＭＰＥＧ以外のコーデック、多重化ファイルに変換をしてデジタル用入出力Ｉ／Ｆ８１０から出力することも可能である。

【０４１２】

サブコンテンツの場合も、コンテンツ管理ユニットとして識別されると、コンテンツ管理ユニットに対応するユニット鍵の取得処理が実行され、取得されたユニット鍵に基づいて、暗号化処理手段８５０で暗号を解き、再生処理が実行される。

【０４１３】

なお、上述した各管理情報、すなわち、

［ユニット構成および鍵管理テーブル］

［状態管理テーブル］

［コンテンツ再生およびコピー制御情報管理テーブル］

は、情報記録媒体８９１に格納されている場合は、情報記録媒体８９１から読み出された後メモリ８８０に保管される。再生を行う際に必要なコンテンツ管理ユニット（ＣＰＳユニット）ごとの鍵情報は、メモリ８８０上に保管されたデータから取得することができる。なお、各管理テーブル、ユニット鍵は情報記録媒体に格納されていない場合は、ネットワーク接続サーバから所定の手続きを行うことで取得可能である。

【０４１４】

前述したように、コンテンツ管理ユニット（ＣＰＳユニット）は、メインコンテンツ、サブコンテンツのそれぞれの構成データに対応付けられて設定され、１つのコンテンツ管理ユニット（ＣＰＳユニット）に１つのユニット鍵が対応付けられている。コンテンツ再生の再生制御を統括的に実行する統括再生制御プログラムが、コンテンツ管理ユニット（ＣＰＳユニット）の切り替えの発生を検出し、切り替えに応じて適用する鍵の切り替えを実行する。鍵が取得されていない場合は、鍵取得を促すメッセージを提示する処理を実行する。

【０４１５】

なお、コンテンツ利用制御情報、すなわち、コンテンツ再生およびコピー制御情報が暗号化され、改ざん検証用データとして設定されている場合は、コンテンツ利用に際し、情報記録媒体に格納されたコンテンツ管理ユニットに対応する暗号化されたコンテンツ利用制御情報を取得し、コンテンツ管理ユニットに対応して設定されたユニット鍵を適用した復号処理、および改ざん検証処理を実行して、改ざんの無いことの確認を条件として、コンテンツ利用制御情報に基づくコンテンツ利用処理を実行する。

【０４１６】

記録再生装置において必要な情報を装置外部のネットワーク経由で取得する場合、取得したデータは記録再生装置内部のメモリ８８０に保存される。保存されるデータとしてはコンテンツ再生に必要な鍵情報、コンテンツ再生時に合わせて再生するための字幕、音声（Ａｕｄｉｏ）情報、静止画などのデータ、コンテンツ管理情報、およびコンテンツ管理情報に対応した再生装置の動作ルール（Ｕｓａｇｅ　Ｒｕｌｅ）などが存在する。

【０４１７】

なお、再生処理、記録処理を実行するプログラムはＲＯＭ８６０内に保管されており、プログラムの実行処理中は必要に応じて、パラメータ、データの保管、ワーク領域としてメモリ８８０を使用する。なお、図３４では、データ記録、再生の可能な装置構成を示して説明したが、再生機能のみの装置、記録機能のみを有する装置も構成可能であり、これ

らの装置においても本発明の適用が可能である。

【０４１８】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０４１９】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０４２０】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０４２１】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０４２２】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

【０４２３】

以上、説明したように、本発明の構成によれば、例えば、Ｂｌｕ－ｒａｙディスクＲＯＭフォーマットなどの特定のＡＶ（Audio Visual）フォーマットに従ったデータフォーマットを持つメインコンテンツと、そのＡＶフォーマットに従わないデータフォーマットを持つサブコンテンツの構成データをコンテンツ管理ユニットとして設定し、コンテンツ管理ユニットに含まれるデータを、コンテンツ管理ユニット毎に対応付けられた個別のユニット鍵に基づく暗号化データとして情報記録媒体に格納する構成としたので、ＡＶ（Audio Visual）フォーマットに従ったデータのみならず、ＡＶ（Audio Visual）フォーマットに従わない任意のフォーマットのデータについても、様々な態様での利用制御を行うことが可能となるので、本発明の構成は、例えば、複数のコンテンツを情報記録媒体に格納し、各コンテンツ毎の利用制御を実行することが要請されるシステムにおいて適用する情報記録媒体、情報処理装置などにおいて有効に適用可能である。

【０４２４】

さらに、本発明の構成によれば、メインコンテンツ、サブコンテンツの構成データをユニットに区分し、各ユニット毎のコンテンツの利用管理、具体的には、再生制御、コピー制御など、各種のコンテンツ利用制御を行うことが可能となる。このように、コンテンツ利用制御を個々のコンテンツ管理ユニットを単位として行うことができるので、多くのコ

ンテンツを格納した情報記録媒体において、細分化したコンテンツ毎の管理が可能となるので、本発明の構成は、例えば、複数のコンテンツを情報記録媒体に格納し、各コンテンツ毎の利用制御を実行することが要請されるシステムにおいて適用する情報記録媒体、情報処理装置などにおいて有効に適用可能である。

【０４２５】

さらに、本発明の構成によれば、メインコンテンツ、サブコンテンツの構成データをユニットに区分し、各ユニット毎のコンテンツの利用制御情報を改ざん検証用データとして設定し暗号化して提供する構成としたので、利用制御情報の不正取得、改ざんによるコンテンツの不正利用が防止されるので、厳格なコンテンツの利用制御を要請されるシステムにおいて適用する情報記録媒体、情報処理装置などにおいて有効に適用可能である。

【０４２６】

さらに、本発明の構成によれば、コンテンツ管理ユニット（ＣＰＳユニット）に区分されたコンテンツに対応するコンテンツ利用制御情報を、コンテンツ管理ユニットに対応するユニット鍵による暗号化データとするとともに、コンテンツ利用制御情報を含むデータに対応する改ざん検証用データを設定して記録する構成としたので、コンテンツ利用制御情報の漏洩や改ざんを防止することができ、よりセキュリティレベルの高いコンテンツ利用管理が実現される。

【０４２７】

さらに、本発明の構成によれば、コンテンツ管理ユニット（ＣＰＳユニット）に区分されたコンテンツに対応するコンテンツ利用制御情報を、基本制御情報と、拡張制御情報に区分し、基本制御情報を含む特定のブロックデータを設定する構成とし、ブロック単位の暗号化を行ない、またその基本制御情報を含む特定のブロックデータに対応する改ざん検証用データを設定したので、基本制御情報のみに従ったコンテンツ利用を行なう装置は、拡張制御情報を格納したデータブロックの復号や、改ざん検証処理を実行する必要がなく、効率的な処理が可能となる。

【図面の簡単な説明】

【０４２８】

【図１】情報記録媒体の格納データ構成について説明する図である。

【図２】情報記録媒体の格納コンテンツのフォーマット例について説明する図である。

【図３】情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットの設定例について説明する図である。

【図４】コンテンツ管理ユニット構成およびユニット鍵管理テーブルの例を示す図である。

【図５】ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）と、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）を含む格納コンテンツのフォーマット例について説明する図である。

【図６】ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）と、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）を含むコンテンツ構成に対して設定するコンテンツ管理ユニットの設定例について説明する図である。

【図７】ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）と、トップメニュー（Ｔｏｐ　Ｍｅｎｕ）を含む構成におけるコンテンツ管理ユニット構成およびユニット鍵管理テーブルの例を示す図である。

【図８】コンテンツのネットワーク独立、ネットワーク関連状態におけるコンテンツ利用態様、利用制限について説明する図である。

【図９】コンテンツのネットワーク独立、ネットワーク関連状態におけるコンテンツコピー制限について説明する図である。

【図１０】コンテンツの状態管理テーブルのデータ例について説明する図である。

【図１１】コンテンツのコンテンツ再生およびコピー制御情報管理テーブルのデータ例について説明する図である。

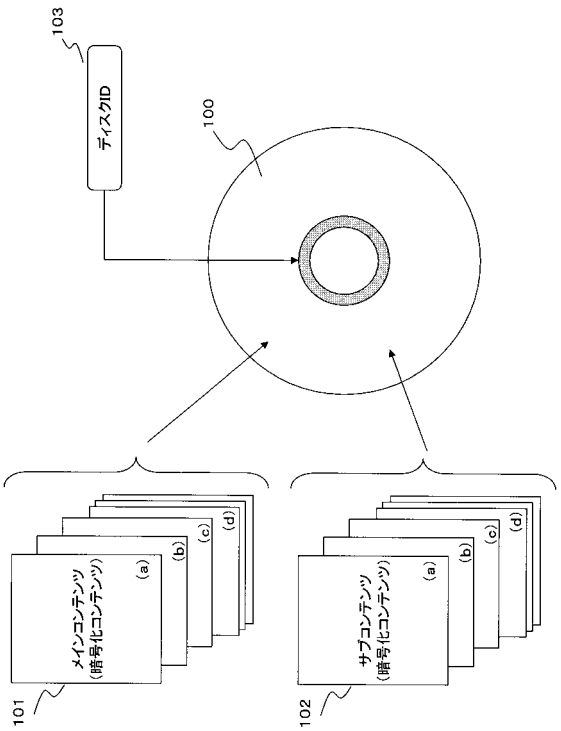
【図１２】コンテンツの状態に応じたコンテンツ管理情報を可変長データで記録したコン

テンツ再生およびコピー制御情報管理テーブルの例について説明する図である。
【図１３】情報記録媒体におけるデータ格納ディレリクトリの構成例（例１）について説明する図である。
【図１４】情報記録媒体におけるデータ格納ディレリクトリの構成例（例２）について説明する図である。
【図１５】情報記録媒体におけるデータ格納ディレリクトリの構成例（例３）について説明する図である。
【図１６】管理情報の格納態様について説明する図である。
【図１７】再生／コピー制御情報の改ざん防止および暗号処理構成について説明する図である。
【図１８】再生／コピー制御情報に対するハッシュ関数を適用した改ざん防止および暗号処理構成について説明する図である。
【図１９】再生／コピー制御情報の繰り返しデータを適用した改ざん防止および暗号処理構成について説明する図である。
【図２０】情報記録媒体に格納されるコンテンツ利用制御情報のデータ構成、すなわち、各ＣＰＳユニット毎の再生／コピー制御情報に対応する個別ファイルを構成するデータの記録構成を示す図である。
【図２１】情報記録媒体に記録される全体データ構成を示すディレクトリ図である。
【図２２】ユニット鍵生成値情報（Ｕｎｉｔ＿Ｋｅｙ＿Ｇｅｎ＿Ｖａｌｕｅ．ｉｎｆ）のデータ構成について説明する図である。
【図２３】ＡＶストリームと、ＣＰＳユニットの対応を示すＢｌｕ－ｒａｙ　Ｄｉｓｃ ＲＯＭフォーマットに従ったコンテンツ構成図である。
【図２４】ブロック鍵Ｋｂによるブロック暗号化処理について説明する図である。
【図２５】ブロック鍵Ｋｂによる復号処理について説明する図である。
【図２６】ある１つのＣＰＳユニットに対応するコンテンツ利用制御情報の記録データの全体構成例を示す図である。
【図２７】１つのコンテンツ管理ユニット（ＣＰＳユニット）対応のコンテンツ利用制御情報ファイルの記録例、および改ざん検証用データとしてのハッシュ値設定例について説明する図である。
【図２８】基本制御情報（Ｂａｓｉｃ　ＣＣＩ）と、拡張制御情報（Ｅｘｔｅｎｄｅｄ ＣＣＩ）の具体例を示す図である。
【図２９】図２７に示すコンテンツ利用制御情報の格納例に対応するシンタックス図である。
【図３０】コンテンツ利用制御情報ファイルの記録例、および改ざん検証用データとしてのハッシュ値設定例について説明する図である。
【図３１】図３０に示すコンテンツ利用制御情報の格納例に対応するシンタックス図である。
【図３２】基本制御情報のみを読み取り、基本制御情報に従ったコンテンツ利用を実行する情報処理装置の処理シーケンスを説明するフロー図である。
【図３３】基本制御情報と拡張制御情報の双方を読み取り、基本制御情報および拡張制御情報に従ったコンテンツ利用を実行する情報処理装置の処理シーケンスを説明するフロー図である。
【図３４】情報記録媒体を装着して再生する情報処理装置の構成例について説明する図である。
【符号の説明】
【０４２９】
１００　情報記録媒体
１０１　メインコンテンツ
１０２　サブコンテンツ
１０３　ディスクＩＤ

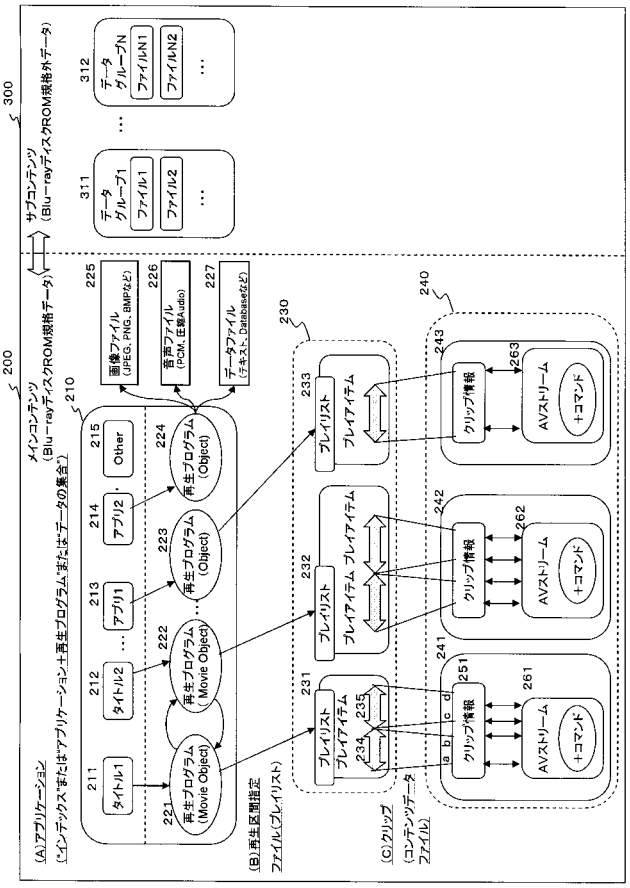
２００　メインコンテンツ
２１０　アプリケーション
２１１，２１２　アプリケーションインデックスファイル（タイトル）
２１３，２１４，２１５　アプリケーション実行ファイル
２２１～２２４　再生プログラム
２３０　再生区間指定ファイル（プレイリスト）
２３１～２３３　プレイリスト
２３４，２３５　プレイアイテム
２４０～２４４　クリップ
２５１　クリップ情報
２６１，２６２，２６３　ＡＶストリーム
２８１　ファーストプレイバック（Ｆｉｒｓｔ　Ｐｌａｙｂａｃｋ）インデックス
２８２　トップメニュー（Ｔｏｐ　Ｍｅｎｕ）インデックス
２８３　アプリケーションインデックスファイル（タイトル）
３００　サブコンテンツ
３１１，３１２　データグループ
４０１～４０５　コンテンツ管理ユニット（ＣＰＳユニット）
４２１～４２３　コンテンツ管理ユニット（ＣＰＳユニット）
５０１　コンテンツ管理情報構成データ
５０２　コンテンツ管理情報構成データ
５０３　ユーザ定義情報（コンテンツ管理情報構成データ）
５１１　メインコンテンツデータ部
５１２　管理データ部
５１３　サブコンテンツデータ部
５１４　管理データ部
５１５　データグループ情報
５２１　サブコンテンツデータ部
５２２　データグループ情報
５５１　メインコンテンツデータ部
５５２　サブコンテンツデータ部
５５３　管理データ部
５７１　再生／コピー制御情報
５７２　改ざん防止用データ
５８１，５８２　再生／コピー制御情報
５８３　ハッシュ生成関数
５８４，５８５　改ざん防止用データ
５８６，５８７　連結データ
５９１，５９２　再生／コピー制御情報
５９３，５９４　連結データ
６０１　ユーザ制御データ（ＵＣＤ：User Control Data）
６０２　ユーザデータ(User Data)
６０３　ブロックシード
６０９　ユニット鍵生成値情報ファイル
６１０　コンテンツ利用制御情報
６１１　コンテンツ管理データ部
６１２　コンテンツデータ部
６１３，６１４，６１５　クリップＡＶストリームデータ
６２１　ユーザデータ
６２２　ブロックシード
６２３　ユニット鍵

６２４　ブロック鍵
６２５　暗号化データ
６３１　ユーザデータ
６３２　ブロックシード
６３３　暗号化データ
６３４　ユニット鍵
６３５　ブロック鍵
６３６　復号データ
７０１　第１ブロック
７０２　後続ブロック
７２１　第１ブロック領域データ
７２２　後続ブロック領域データ
７５１　第１ブロック
７５２　後続ブロック
７７１　第１ブロック領域データ
７７２　後続ブロック領域データ
８００　情報処理装置
８０１　バス
８１０　入出力Ｉ／Ｆ
８２０　ＴＳ・ＰＳ処理手段
８３０　ＭＰＥＧコーデック
８４０　入出力Ｉ／Ｆ
８４１　Ａ／Ｄ，Ｄ／Ａコンバータ
８５０　暗号処理手段
８６０　ＲＯＭ
８７０　ＣＰＵ
８８０　メモリ
８９０　ドライブ
８９１　情報記録媒体

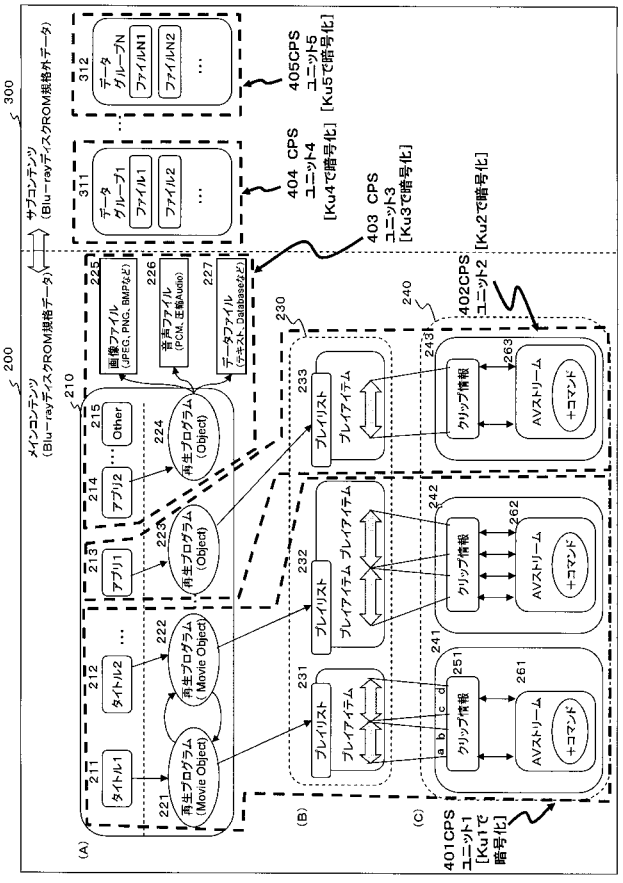
【図１】



【図２】



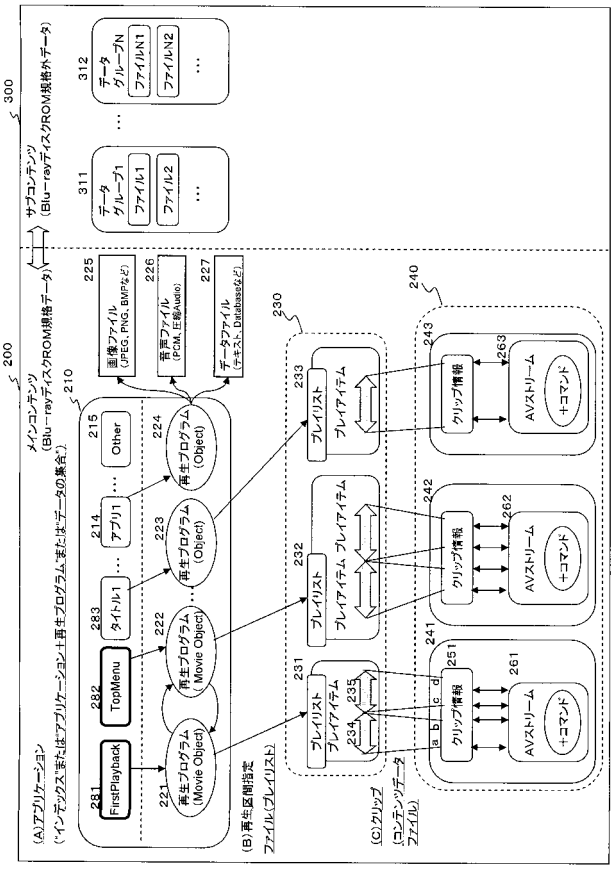
【図３】



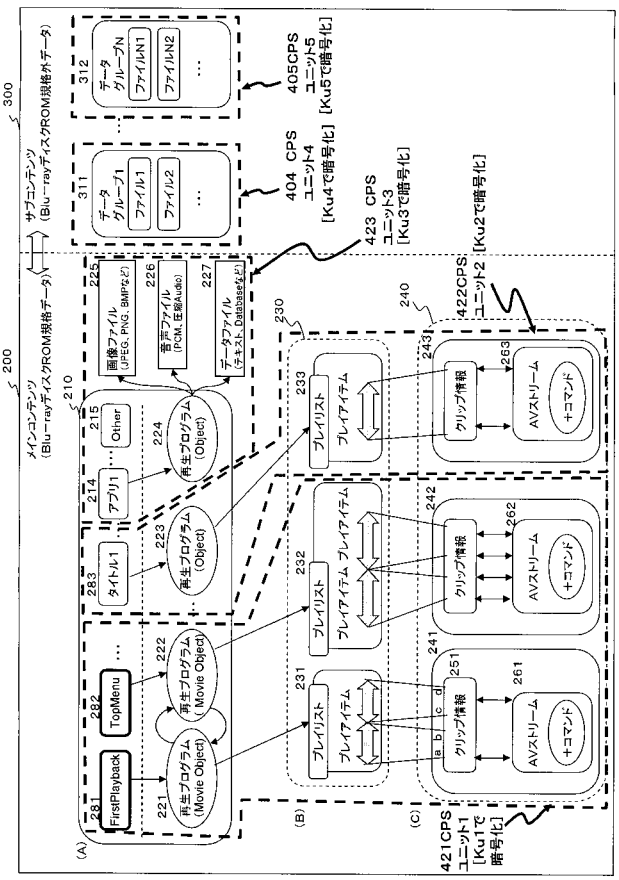
【図４】

アプリケーション層における インデックスまたは アプリケーションファイル またはデータグループ	コンテンツ管理ユニット (CPS)	ユニット鍵 (CPS)	
タイトル1	CPS1	Ku1	メインコンテンツ対応データ
タイトル2	CPS1	Ku1	
アプリケーション1	CPS2	Ku2	
アプリケーション2	CPS3	Ku3	
：	：	：	
データグループ1	CPS4	Ku4	サブコンテンツ対応データ
データグループ2	CPS5	Ku5	
：	：	：	

【図５】



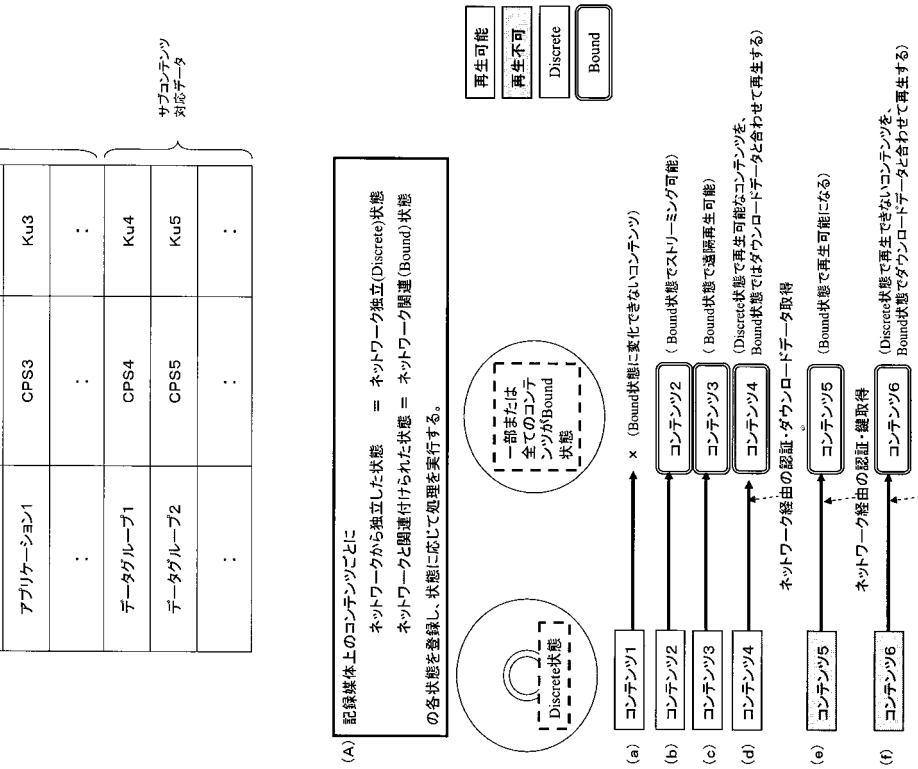
【図６】



【図７】

アプリケーション層における インデックスまたは アプリケーションファイル またはデータグループ	コンテンツ管理ユニット (CPS)	ユニット鍵 (CPS)	
First Playback	CPS1	Ku1	メインコンテンツ対応データ
Top Menu	CPS1	Ku1	
タイトル1	CPS2	Ku2	
:	:	:	
アプリケーション1	CPS3	Ku3	
:	:	:	
データグループ1	CPS4	Ku4	サブコンテンツ対応データ
データグループ2	CPS5	Ku5	
:	:	:	

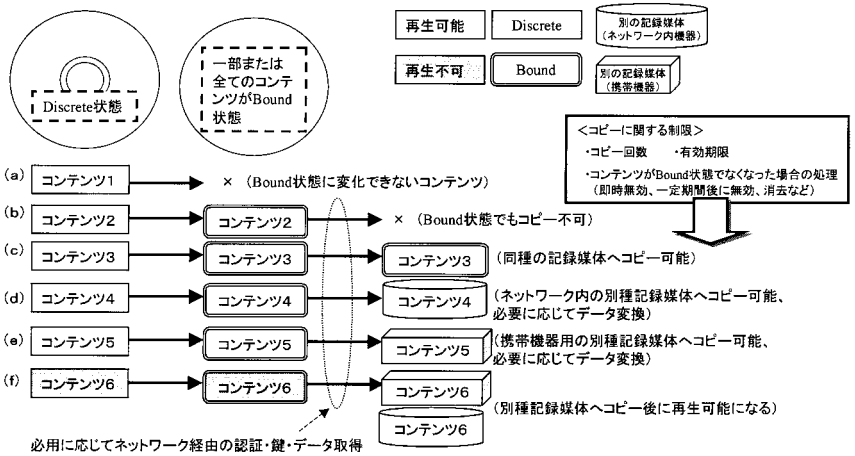
【図８】



【図９】

（A）

記録媒体上のコンテンツごとに
ネットワークから独立した状態　＝　ネットワーク独立(Discrete)状態
ネットワークと関連付けられた状態 ＝　ネットワーク関連(Bound)状態
の各状態を登録し、状態に応じて処理を実行する。



【図１０】

コンテンツ管理ユニット（CPS）	初期状態	現状態
CPS1	Discrete only	Discrete
CPS2	Discrete initially	Bound
CPS3	Bound only	Bound
CPS4	Bound initially	Discrete
:	:	:
CPSm	Discrete only	Discrete

【図１１】

field名	num_of_bits
Num_of_Content	16
for(I=0; I<Num_of_Content; I++){	
CCI_and_other_info_for_Content [I]	128
}	

CCI_and_other_info_for_Content [I]の中身：　以下の情報の一部または全てをフラグ、値によって保持する。(値が使用するbit数は任意)

	(フラグ/値)	(内容)
<Discrete状態での動作>		
再生	フラグ	OK/NG
Discrete状態で再生できないコンテンツの再生方法	値	「鍵配信サーバーへ接続」、「鍵の入ったメモリカード挿入」 など
サーバーの指定	値	サーバーリストへのインデックス値
<Bound状態での動作>		
コピー・ストリーミング互換性情報	値	コンテンツをネットワーク内の他の機器で再生するための互換性情報
コピー・ストリーミング時のデータ変換方式	値	コンテンツを他の機器用に変換する際に使用できる方式
ネットワーク内の同種記録媒体へのコピー可否	フラグ	OK/NG
ネットワーク内の同種記録媒体へのコピー回数	値	回数
ネットワーク内の同種記録媒体へのコピー有効期限	値	有効期限
ネットワーク内の他種記録媒体へのコピー可否	フラグ	OK/NG
ネットワーク内の他種記録媒体へのコピー回数	値	回数
ネットワーク内の他種記録媒体へのコピー有効期限	値	有効期限
ネットワーク内の他種記録媒体へのコピー用データの有無	フラグ	OK/NG
ネットワーク内の他種記録媒体へのコピー用データの指定	値	コピー用のデータを指定するインデックス値
携帯機器へのコピー可否	フラグ	OK/NG
携帯機器へのコピー回数	値	回数
携帯機器へのコピー有効期限	値	有効期限
携帯機器へのコピー用データの有無	フラグ	OK/NG
携帯機器へのコピー用データの指定	値	コピー用のデータを指定するインデックス値
ストリーミングの可否	フラグ	OK/NG
ストリーミング受信対象指定	値	対象機器を限定
遠隔再生の可否	フラグ	OK/NG
遠隔再生受信対象指定	値	対象機器を限定
コンテンツがBound状態でなくなった場合の処理	値	コピーを即時無効化、一定期間後に無効化、消去など
ダウンロードデータ種別	値	ダウンロードデータの種別（字幕、Audio、静止画など）
ダウンロードデータの取得方法	値	「ダウンロードサーバーへ接続」、「データの入ったメモリカード挿入」 など
501 ダウンロードサーバーの指定	値	ダウンロードサーバーリストへのインデックス値
サーバーから動作制御情報を取得する	フラグ	サーバーから取得した動作制御情報に従う
動作制御情報取得用サーバーの指定	値	動作制御情報取得用サーバーを示すサーバーリストへのインデックス値

【図１２】

（A） 全情報を1つのループに入れる場合

field名	num_of_bits
Num_of_Content	16
for(I=0; I<Num_of_Content; I++){	
Num_of_function[I]	16
for(J=0; J<Num_of_function; J++){	
CCI_and_other_info_length	16
CCI_and_other_info_type	8
CCI_and_other_info_value	8
Additional_info	N
}	
}	

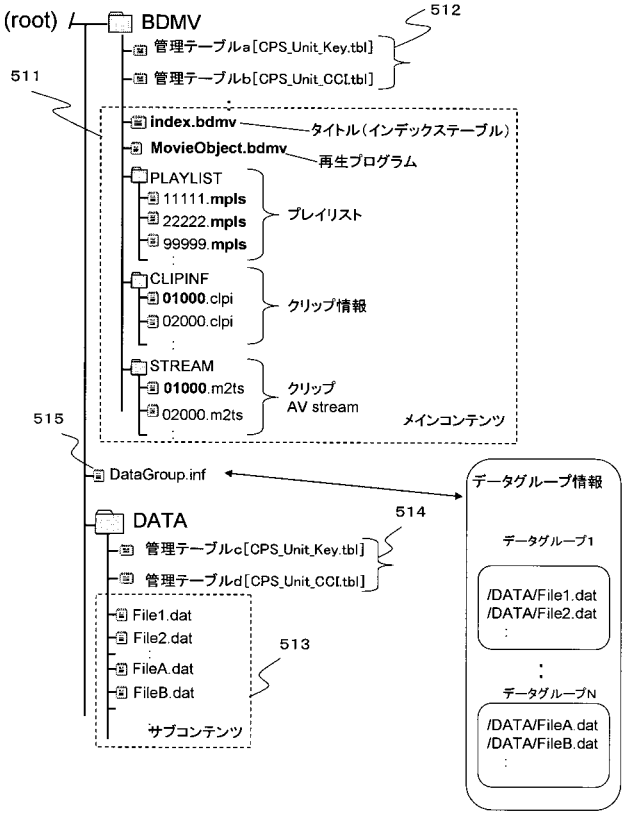
（B） 状態ごとにループを分ける場合

field名	num_of_bits
Num_of_Content	16
for(I=0; I<Num_of_Content; I++){	
Num_of_Discrete_function[I]	16
for(J=0; J<Num_of_function; J++){	
CCI_and_other_info_length	16
CCI_and_other_info_type	8
CCI_and_other_info_value	8
Additional_info	N
}	
Num_of_Bound_function[I]	16
for(J=0; J<Num_of_function; J++){	
CCI_and_other_info_length	16
CCI_and_other_info_type	8
CCI_and_other_info_value	8
Additional_info	N
}	
}	

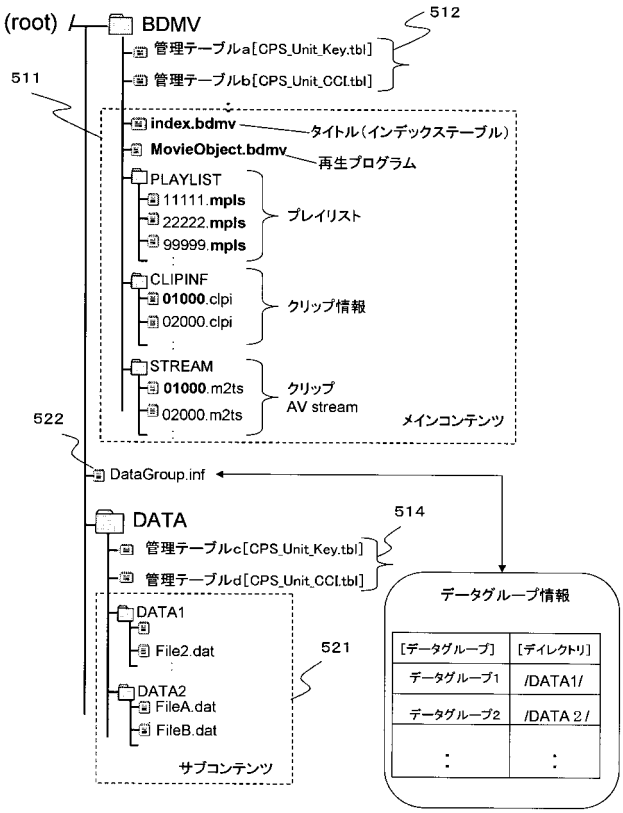
CCI_and_other_info_type一覧 および 対応するCCI_and_other_info_value、Additional_infoの内容

"CCI_and_other_info_type"	"CCI_and_other_info_value"	"Additional_info"
Discrete状態での再生	OK/NG	Discrete状態で再生できないコンテンツの再生方法 サーバーの指定
ネットワーク内の同種記録媒体へのコピー	OK/NG	コピー回数、有効期限
ネットワーク内の他種記録媒体へのコピー	OK/NG	コピー回数、有効期限、コピー用データの有無、コピー用データ指定 コピー時にデータ変換を行う場合の方式指定
携帯機器へのコピー	OK/NG	コピー回数、有効期限、コピー用データの有無、コピー用データ指定 コピー時にデータ変換を行う場合の方式指定
ネットワーク内のストリーミング	OK/NG	ストリーミング対象機器指定 ストリーミング用データの有無、ストリーミング用データ指定 ストリーミング時にデータ変換を行う場合の方式指定
502 ネットワーク内の遠隔再生	OK/NG	遠隔再生の対象機器指定
Bound状態でなくなった場合の処理	値	コピーを即時無効化、一定期間後に無効化、消去など
503 ダウンロードデータの再生	値(データ種別)	ダウンロードデータの取得方法、ダウンロードサーバーの指定
サーバーからの動作制御情報取得用情報	値	サーバーの指定
ユーザー定義情報	コンテンツ所有者が独自に定義	コンテンツ所有者が独自に定義

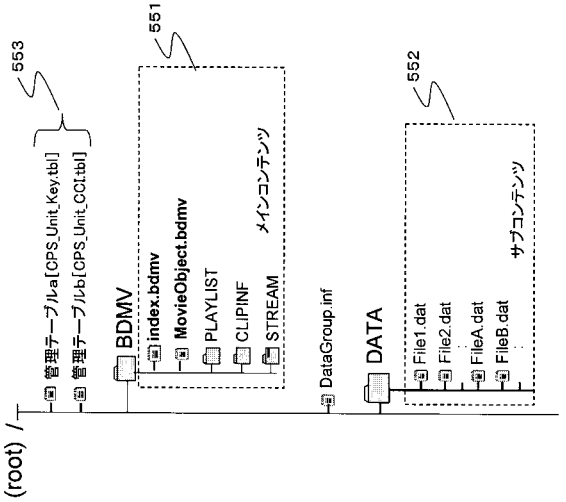
【図１３】



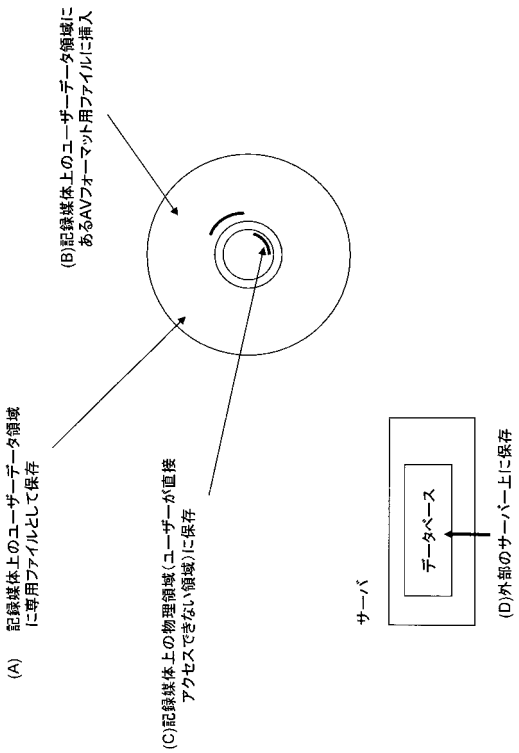
【図１４】



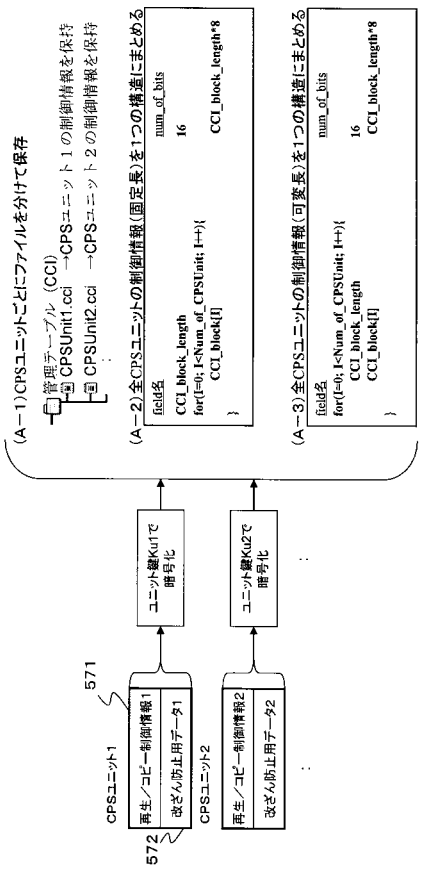
【図１５】



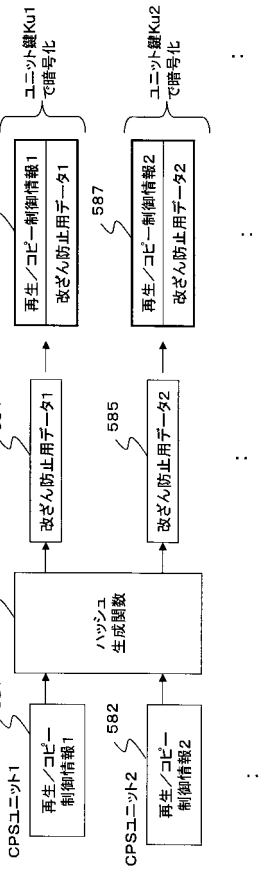
【図１６】



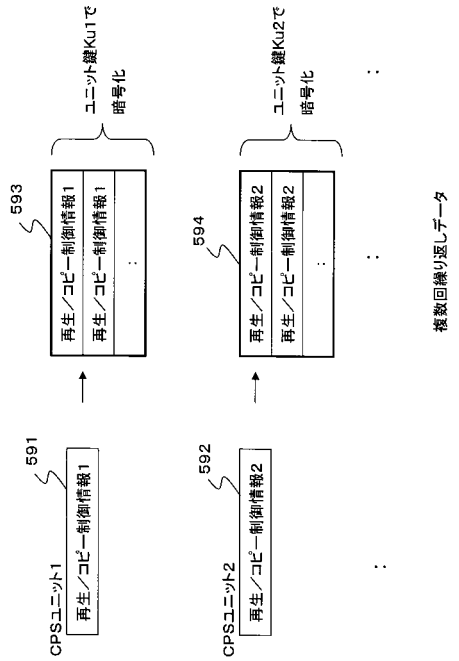
【図１７】



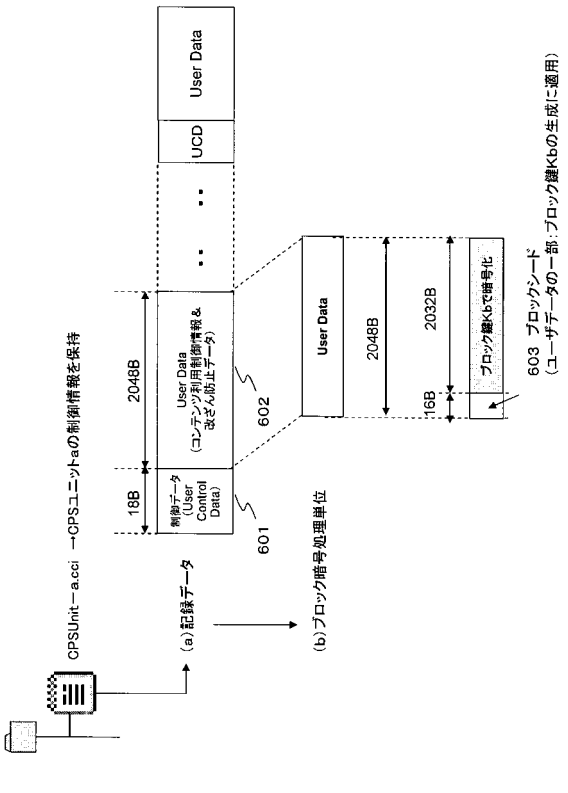
【図１８】



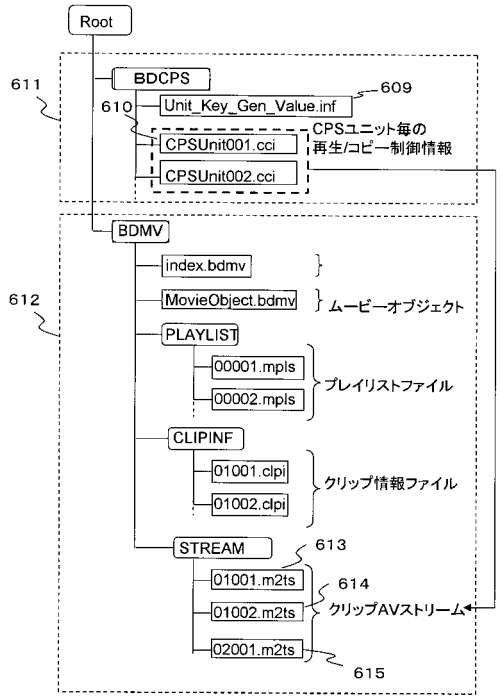
【図１９】



【図２０】



【図２１】



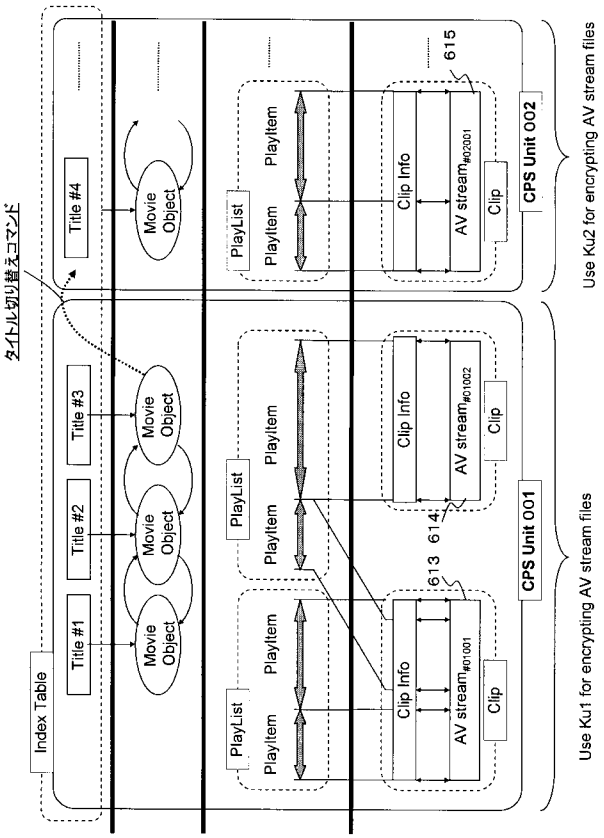
【図２２】

Unit_Key_Generation_Value.infファイルの構造例:シンタックス図

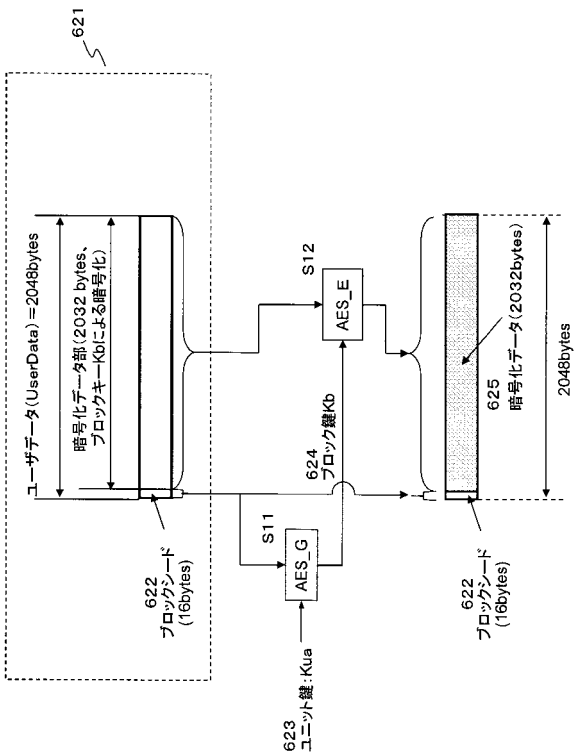
[field名]	[num_of_bits]
Unit_Key_Generation_Value.inf { CPS_Unit_number_for_FirstPlayback	16
CPS_Unit_number_for_TopMenu	16
Number of Titles	16
for(i=1; i< Number_of_Titles+1; i++){ CPS_Unit_number for Title #i	16
}	
Number of CPS_Units	16
for(i=1; i< Number_of_CPS_Unit+1; i++){ Unit Key Generation Value for CPS_Unit #i	128
} }	

・First PlaybackがAVコンテンツ内に存在しない場合CPS_Unit_number_for_FirstPlayback=0とする
・TopMenuがAVコンテンツ内に存在しない場合CPS Unit number for TopMenu=0とする
・Title#1～Title#[Number_of_Titles] は上記Syntaxで対応するCPS_Unit番号を定義する

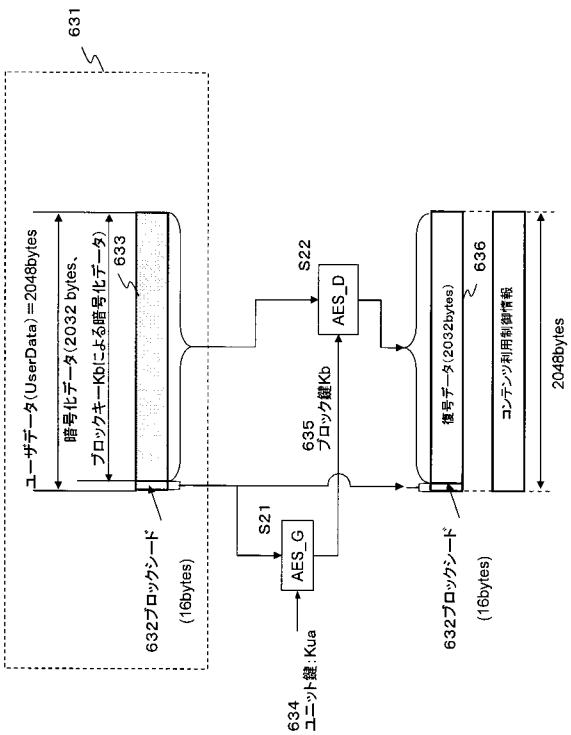
【図２３】



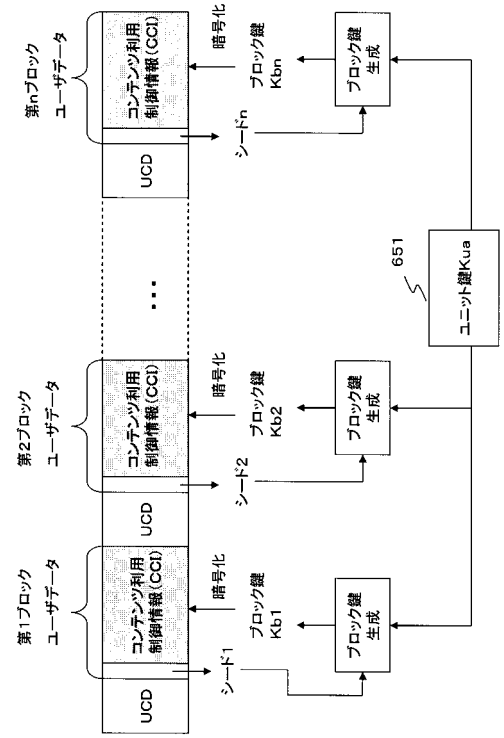
【図２４】



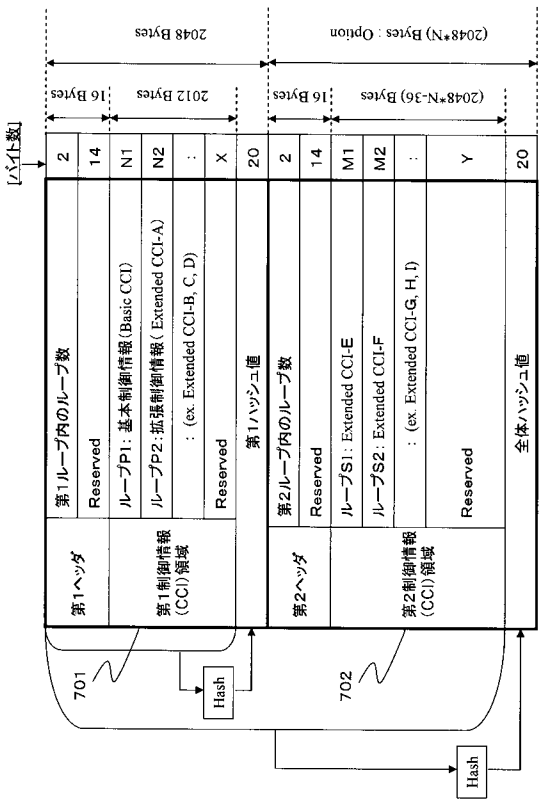
【図２５】



【図２６】



【図２７】



【図２８】

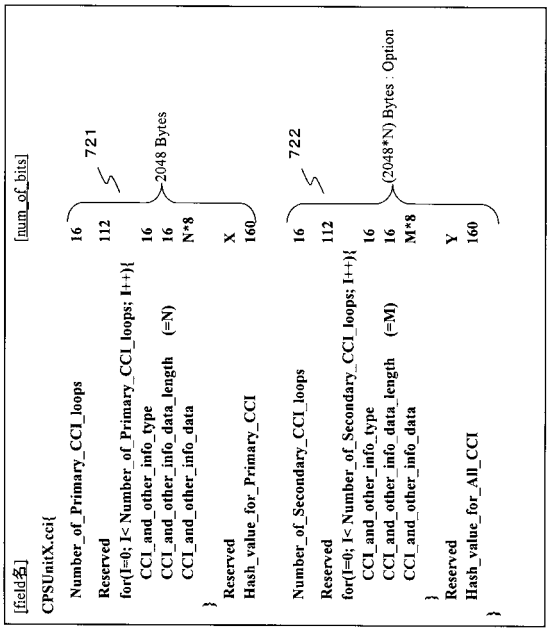
CCI_and_other_info()：基本情報の例

（名称）	（内容）
コピー可/不可情報	コピー可／不可／1世代のみ可
映像出力保護制御情報	出力制限有り／無し
アナログコピー制御情報	可／不可(使用するアナログコピー防止技術を指定)
暗号化の有無を示す情報	暗号化有り／無し
権利主張の有無を示す情報	権利主張有り／無し

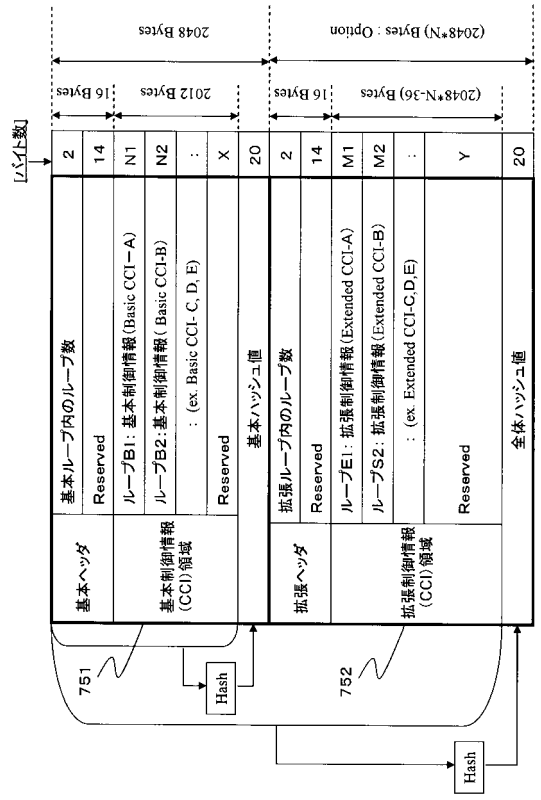
CCI_and_other_info()：拡張情報の例

（名称）	（内容）
Disc単体での再生可否情報	Disc上の情報だけでコンテンツ再生が可能かどうかを示す
Disc単体では再生できないコンテンツの再生方法	「配信サーバーへ接続」、「鍵の入ったメモリカード挿入」など
サーバーの指定	サーバーリストへのインデックス値
コピーストリーミング互換性情報	コンテンツをネットワーク内の他の機器で再生するための互換性情報
コピーストリーミング時のデータ変換方式	コンテンツを他の機器用に変換する際に使用できる方式
ネットワーク内の用補記録媒体へのコピー可否	OK/NG
ネットワーク内の用補記録媒体へのコピー回数	回数
ネットワーク内の同時記録媒体へのコピー有効期限	有効期限
ネットワーク内の伸張記録媒体へのコピー可否	OK/NG
ネットワーク内の他機記録媒体へのコピー回数	回数
ネットワーク内の他機記録媒体へのコピー有効期限	有効期限
ネットワーク内の他機記録媒体へのコピー用データの有無	OK/NG
ネットワーク内の他機記録媒体へのコピー用データの指定	コピー用のデータを指定するインデックス値
携帯機器へのコピー可否	OK/NG
携帯機器へのコピー回数	回数
携帯機器へのコピー有効期限	有効期限
携帯機器へのコピー用データの有無	OK/NG
携帯機器へのコピー用データの指定	コピー用のデータを指定するインデックス値
ストリーミングの可否	OK/NG
ストリーミング配信対象指定	対象機器を限定
遠隔再生の可否	OK/NG
遠隔再生受信対象指定	対象機器を限定
コンテンツのネットワーク内利用を終了する場合の処理	コピーを即時無効化、一定期間後に無効化、消去など
ダウンロードデータ種別	ダウンロードデータの種別(字幕、Audio、静止画など)
ダウンロードデータの取得方法	「ダウンロードサーバーへ接続」、「データの入ったメモリカード挿入」など
ダウンロードサーバーの指定	ダウンロードサーバーリストへのインデックス値
サーバーから動作制御情報を取得する	サーバーから取得した動作制御情報に従う
動作制御情報取得用サーバーの指定	動作制御情報取得用サーバーを示すサーバーリストへのインデックス値

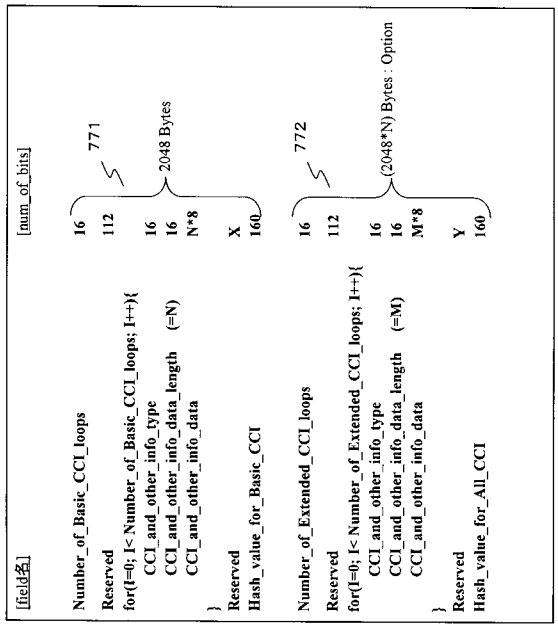
【図２９】



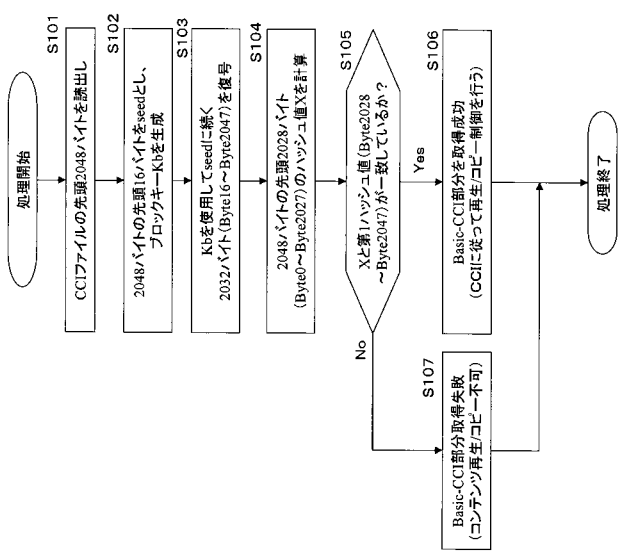
【図３０】



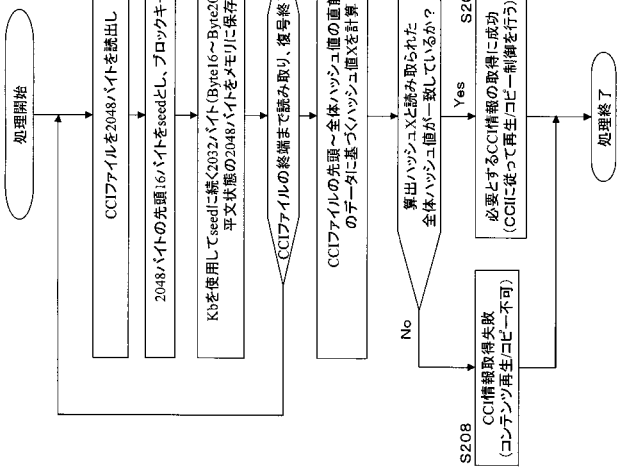
【図３１】



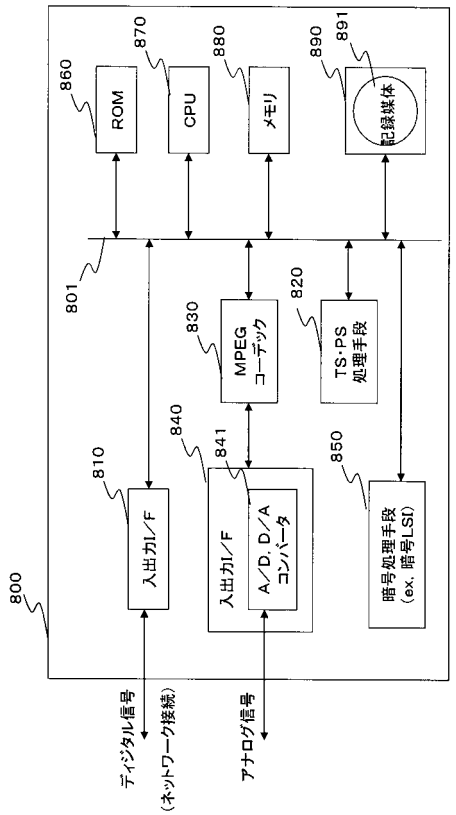
【図３２】



【図３３】


処理開始
S201
CCIファイルを2048バイトを読出し
S202
2048バイトの先頭16バイトをseedとし、ブロックキーKbを生成
S203
Kbを使用してseedに続く2032バイト(Byte16～Byte2047)を復号し、平文状態の2048バイトをメモリに保存
S204
CCIファイルの終端まで読み取り、復号終了？
S205
CCIファイルの先頭～全体ハッシュ値の直前までのデータに基づくハッシュ値Xを計算
S206
算出ハッシュXと読み取られた全体ハッシュ値が一致しているか？
Yes
S207
必要とするCCI情報の取得に成功（CCIに従って再生/コピー制御を行う）
No
S208
CCI情報取得失敗（コンテンツ再生/コピー不可）
処理終了

【図３４】


800
801
ROM
860
CPU
870
メモリ
880
記録媒体
890
891
入出力I／F
810
入出力I／F
840
A／D. D／A コンバータ
841
MPEG コーデック
830
TS・PS 処理手段
820
暗号処理手段 (ex. 暗号LSI)
850
ディジタル信号 (ネットワーク接続)
アナログ信号

フロントページの続き

(51)Int.Cl.[7]	FI			テーマコード（参考）
Ｈ０４Ｌ 9/14	Ｇ１１Ｂ 20/12			５Ｊ１０４
Ｈ０４Ｎ 5/91	Ｇ１１Ｂ 20/12	１０３		
	Ｇ１１Ｂ 27/00		Ｄ	
	Ｈ０４Ｌ 9/00	６４１		
	Ｈ０４Ｎ 5/91		Ｐ	

Ｆターム(参考) 5D044 AB05 AB07 BC02 CC06 DE50 DE57 GK08 GK12 GK17 HL02
5D110 AA14 AA27 AA29 DA03 DA04 DA11 DB03 DC05 DE01
5J104 AA12 PA14