(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4936652号
(P4936652)
(45)発行日　平成24年5月23日(2012.5.23)　(24)登録日　平成24年3月2日(2012.3.2)

(51)Int.Cl.　　F I
G11B 20/10 (2006.01)　　G11B 20/10 H
HO4L 9/08 (2006.01)　　HO4L 9/00 601B
HO4L 9/00 601E

請求項の数 7　(全 42 頁)

(21)出願番号　特願2004-246640 (P2004-246640)
(22)出願日　平成16年8月26日 (2004.8.26)
(65)公開番号　特開2006-67184 (P2006-67184A)
(43)公開日　平成18年3月9日 (2006.3.9)
審査請求日　平成19年5月30日 (2007.5.30)
審判番号　不服2011-1023 (P2011-1023/J1)
審判請求日　平成23年1月17日 (2011.1.17)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(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
(72)発明者　上田　健二朗
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

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)【特許請求の範囲】
【請求項１】
情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、
情報記録媒体に記録された暗号化コンテンツの復号処理を実行する暗号処理手段を有し、
前記暗号処理手段は、
前記情報記録媒体に格納されたコンテンツ管理ユニット各々に対応するユニット鍵を生成し、該ユニット鍵を適用したデータ処理により前記情報記録媒体に格納されたコンテンツの復号を実行する構成であり、
前記ユニット鍵の生成において、前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行し、該データ処理によって生成した鍵を適用して、前記ユニット鍵の暗号化データである暗号化ユニット鍵の復号処理を実行してユニット鍵を生成する構成であり、
前記コピー・再生制御情報は、前記コンテンツ管理ユニット対応の（ａ）コピー可／不可情報、（ｂ）映像出力解像度制限情報、（ｃ）アナログコピー制御情報、（ｄ）暗号化有無情報、（ｅ）権利主張有無情報からなる上記（ａ）～（ｅ）の各情報中、少なくとも複数の情報を含む情報であることを特徴とする情報処理装置。
【請求項２】
前記暗号処理手段は、
前記ユニット鍵の生成において、前記コンテンツ管理ユニットの構成データに基づくハ

ッシュ値であるコンテンツハッシュを適用したデータ処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記暗号処理手段は、

前記ユニット鍵の生成において、前記コンテンツ管理ユニットに対応する記録シードを適用したデータ処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項４】

前記暗号処理手段は、

前記ユニット鍵の生成処理において、情報記録媒体からの読み出しデータを適用したＡＥＳ暗号処理、またはハッシュ関数に基づくデータ処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項５】

前記暗号処理手段は、

前記ユニット鍵の生成処理において、

情報記録媒体からの読み出しデータである暗号鍵ブロックに対して、情報処理装置に格納したデバイスキーを適用した復号処理を実行して取得した鍵データを適用した処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項６】

情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、

前記情報記録媒体に格納されたコンテンツ管理ユニット各々に対応するユニット鍵を生成するユニット鍵生成ステップと、

該ユニット鍵を適用したデータ処理により前記情報記録媒体に格納されたコンテンツの復号を実行する復号ステップとを含み、

前記ユニット鍵生成ステップは、

前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行し、該データ処理によって生成した鍵を適用して、前記ユニット鍵の暗号化データである暗号化ユニット鍵の復号処理を実行してユニット鍵を生成するステップを含み、

前記コピー・再生制御情報は、前記コンテンツ管理ユニット対応の（ａ）コピー可／不可情報、（ｂ）映像出力解像度制限情報、（ｃ）アナログコピー制御情報、（ｄ）暗号化有無情報、（ｅ）権利主張有無情報からなる上記（ａ）～（ｅ）の各情報中、少なくとも複数の情報を含む情報であることを特徴とする情報処理方法。

【請求項７】

情報記録媒体からのコンテンツ再生処理をコンピュータにおいて実行させるコンピュータ・プログラムであり、

前記情報記録媒体に格納されたコンテンツ管理ユニット各々に対応するユニット鍵を生成するユニット鍵生成ステップと、

該ユニット鍵を適用したデータ処理により前記情報記録媒体に格納されたコンテンツの復号を実行する復号ステップとを含み、

前記ユニット鍵生成ステップは、

前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行し、該データ処理によって生成した鍵を適用して、前記ユニット鍵の暗号化データである暗号化ユニット鍵の復号処理を実行してユニット鍵を生成するステップを含み、

前記コピー・再生制御情報は、前記コンテンツ管理ユニット対応の（ａ）コピー可／不可情報、（ｂ）映像出力解像度制限情報、（ｃ）アナログコピー制御情報、（ｄ）暗号化有無情報、（ｅ）権利主張有無情報からなる上記（ａ）～（ｅ）の各情報中、少なくとも複数の情報を含む情報であ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ピー・再生制御情報、あるいはコンテンツのハッシュ値などをコンテンツ管理ユニットに対応する暗号鍵であるユニット鍵の生成情報として設定することにより、コンテンツおよびコピー・再生制御情報の改竄を防止し不正なコンテンツ利用を排除し、厳格でかつ効率的な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、
情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、
情報記録媒体に記録された暗号化コンテンツの復号処理を実行する暗号処理手段を有し、
前記暗号処理手段は、
前記情報記録媒体に格納されたコンテンツ管理ユニット各々に対応するユニット鍵を生成し、該ユニット鍵を適用したデータ処理により前記情報記録媒体に格納されたコンテンツの復号を実行する構成であり、
前記ユニット鍵の生成において、前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行する構成であることを特徴とする情報処理装置にある。
【００１６】
さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記ユニット鍵の生成において、前記コンテンツ管理ユニットの構成データに基づくハッシュ値であるコンテンツハッシュを適用したデータ処理を実行する構成であることを特徴とする。
【００１７】
さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記ユニット鍵の生成において、前記コンテンツ管理ユニットに対応する記録シードを適用したデータ処理を実行する構成であることを特徴とする。
【００１８】
さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記ユニット鍵の生成処理において、情報記録媒体からの読み出しデータを適用したＡＥＳ暗号処理、またはハッシュ関数に基づくデータ処理を実行する構成であることを特徴とする。
【００１９】
さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記ユニット鍵の生成処理において、情報記録媒体からの読み出しデータである暗号鍵ブロックに対して、情報処理装置に格納したデバイスキーを適用した復号処理を実行して取得した鍵データを適用した処理を実行する構成であることを特徴とする。
【００２０】
さらに、本発明の第２の側面は、
コンテンツ管理システムであり、
コンテンツ利用管理のための管理情報の提供を行なう管理センタと、コンテンツ編集処理を行なうコンテンツ編集エンティテイと、前記コンテンツ編集エンティテイから、編集コンテンツを受領して、情報記録媒体に対するコンテンツ記録を行なう情報記録媒体製造エンティテイを有し、
前記管理センタは、前記管理情報として、コンテンツ復号に適用するメディアキーを暗号化データとして格納した暗号鍵ブロックデータを前記コンテンツ編集エンティテイ、または情報記録媒体製造エンティテイのいずれかに提供する構成であり、
前記コンテンツ編集エンティテイ、または情報記録媒体製造エンティテイのいずれかは、
前記情報記録媒体に格納するコンテンツ管理ユニット各々に対応するユニット鍵を生成し、該ユニット鍵を適用したコンテンツ管理ユニットの構成データの暗号化を実行する構成であり、
前記ユニット鍵の生成において、前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行する構成であることを特徴とするコンテンツ管理システムにある。
【００２１】
さらに、本発明のコンテンツ管理システムの一実施態様において、前記コンテンツ編集

エンティティ、または情報記録媒体製造エンティティのいずれかは、前記ユニット鍵の生成において、前記コンテンツ管理ユニットの構成データに基づくハッシュ値であるコンテンツハッシュを適用したデータ処理を実行する構成であることを特徴とする。

【００２２】

さらに、本発明のコンテンツ管理システムの一実施態様において、前記コンテンツ編集エンティティ、または情報記録媒体製造エンティティのいずれかは、前記ユニット鍵の生成において、前記コンテンツ管理ユニットに対応する記録シードを適用したデータ処理を実行する構成であることを特徴とする。

【００２３】

さらに、本発明の第３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、

記録データとして、少なくとも１以上のコンテンツ管理ユニットを含み、

前記コンテンツ管理ユニットに含まれるデータは、前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理によって生成されるユニット鍵を適用した暗号化データとして格納されていることを特徴とする情報記録媒体にある。

【００２４】

さらに、本発明の情報記録媒体の一実施態様において、前記ユニット鍵は、前記コンテンツ管理ユニットの構成データに基づくハッシュ値であるコンテンツハッシュを適用したデータ処理により生成される鍵であ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、前記ユニット鍵は、前記コンテンツ管理ユニットに対応する記録シードを適用したデータ処理により生成される鍵であることを特徴とする。

【００２６】

さらに、本発明の第４の側面は、

情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、

前記情報記録媒体に格納されたコンテンツ管理ユニット各々に対応するユニット鍵を生成するユニット鍵生成ステップと、

該ユニット鍵を適用したデータ処理により前記情報記録媒体に格納されたコンテンツの復号を実行する復号ステップとを含み、

前記ユニット鍵生成ステップは、

前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行するステップを含むことを特徴とする情報処理方法にある。

【００２７】

さらに、本発明の情報処理方法の一実施態様において、前記ユニット鍵生成ステップは、前記コンテンツ管理ユニットの構成データに基づくハッシュ値であるコンテンツハッシュを適用したデータ処理を実行するステップを含むことを特徴とする。

【００２８】

さらに、本発明の情報処理方法の一実施態様において、前記ユニット鍵生成ステップは、前記コンテンツ管理ユニットに対応する記録シードを適用したデータ処理を実行するステップを含むことを特徴とする。

【００２９】

さらに、本発明の情報処理方法の一実施態様において、前記ユニット鍵生成ステップは、情報記録媒体からの読み出しデータを適用したＡＥＳ暗号処理、またはハッシュ関数に基づくデータ処理を実行するステップを含むことを特徴とする。

【００３０】

さらに、本発明の情報処理方法の一実施態様において、前記ユニット鍵生成ステップは、情報記録媒体からの読み出しデータである暗号鍵ブロックに対して、情報処理装置に格納したデバイスキーを適用した復号処理を実行して取得した鍵データを適用した処理を実

行するステップを含むことを特徴とする。

【００３１】

さらに、本発明の第５の側面は、

情報記録媒体に対する記録コンテンツを生成する情報処理方法であり、

前記情報記録媒体に格納するコンテンツ管理ユニット各々に対応するユニット鍵を生成するユニット鍵生成ステップと、

該ユニット鍵を適用したデータ処理により前記情報記録媒体に格納するコンテンツの暗号化を実行する暗号化ステップとを含み、

前記ユニット鍵生成ステップは、

前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行するステップを含むことを特徴とする情報処理方法にある。

【００３２】

さらに、本発明の情報処理方法の一実施態様において、前記ユニット鍵生成ステップは、前記コンテンツ管理ユニットの構成データに基づくハッシュ値であるコンテンツハッシュを適用したデータ処理を実行するステップを含むことを特徴とする。

【００３３】

さらに、本発明の情報処理方法の一実施態様において、前記ユニット鍵生成ステップは、前記コンテンツ管理ユニットに対応する記録シードを適用したデータ処理を実行するステップを含むことを特徴とする。

【００３４】

さらに、本発明の第６の側面は、

情報記録媒体からのコンテンツ再生処理をコンピュータにおいて実行させるコンピュータ・プログラムであり、

前記情報記録媒体に格納されたコンテンツ管理ユニット各々に対応するユニット鍵を生成するユニット鍵生成ステップと、

該ユニット鍵を適用したデータ処理により前記情報記録媒体に格納されたコンテンツの復号を実行する復号ステップとを含み、

前記ユニット鍵生成ステップは、

前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行するステップを含むことを特徴とするコンピュータ・プログラムにある。

【００３５】

さらに、本発明の第７の側面は、

情報記録媒体に対する記録コンテンツの生成処理をコンピュータにおいて実行させるコンピュータ・プログラムであり、

前記情報記録媒体に格納するコンテンツ管理ユニット各々に対応するユニット鍵を生成するユニット鍵生成ステップと、

該ユニット鍵を適用したデータ処理により前記情報記録媒体に格納するコンテンツの暗号化を実行する暗号化ステップとを含み、

前記ユニット鍵生成ステップは、

前記コンテンツ管理ユニットに対応して設定されたコピー・再生制御情報の構成データを適用したデータ処理を実行するステップを含むことを特徴とするコンピュータ・プログラムにある。

【００３６】

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。

【００３７】
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】
【００３８】
本発明の構成によれば、情報記録媒体の格納コンテンツをユニットに区分したコンテンツ管理ユニット（ＣＰＳユニット）を設定するとともに、各コンテンツ管理ユニット（ＣＰＳユニット）個別にユニット鍵を対応付け、各ユニットの構成データを暗号化して記録する構成とし、再生時にはユニット鍵を生成し、ユニット鍵を適用したデータ処理を行なうことを必須とした。さらに、ユニット鍵の生成情報として、コンテンツ管理ユニット（ＣＰＳユニット）に対応して設定されるコピー・再生制御情報（ＣＣＩ）、コンテンツ管理ユニット（ＣＰＳユニット）の構成データに基づくハッシュ値であるコンテンツハッシュを適用する構成としたので、コピー・再生制御情報（ＣＣＩ）やコンテンツデータの改竄が行われた場合、正しいユニット鍵の生成が不可能となり、コピー・再生制御情報（ＣＣＩ）やコンテンツデータの改竄を防止でき、不正なコンテンツ利用を排除することができ、正当なコンテンツ利用構成が実現される。さらに、再生装置において、データ改竄の有無の検証処理を行なう必要がなくなり、効率的なデータ再生が可能となる。
【発明を実施するための最良の形態】
【００３９】
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．格納コンテンツの暗号化、利用管理構成
３．情報記録媒体の製造、データ格納処理の詳細
４．情報処理装置におけるコンテンツ再生処理
５．情報記録媒体における記録データ、およびコンテンツ暗号化、復号処理の詳細
６．コピー・再生制御情報（ＣＣＩ）の詳細構成
７．情報処理装置の構成例
【００４０】
［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。
【００４１】
このＲＯＭディスクは、例えば、Ｂｌｕ－ｒａｙディスク、ＤＶＤなどの情報記録媒体であり、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。
【００４２】
図１に示すように、情報記録媒体１００は、コンテンツ等のデータを格納するデータ格納領域１０１と、ディスクおよび格納コンテンツに対応する付帯情報、コンテンツの復号処理に適用する鍵情報などを格納するリードイン領域１０２を持つ。
【００４３】
データ格納領域１０１には、暗号化コンテンツ１１１と、暗号化コンテンツの復号処理に適用する鍵の生成に必要となる情報としての記録シード（ＲＥＣ　ＳＥＥＤ）１１２と、コンテンツのコピー・再生制御情報としてのＣＣＩ（Copy Control Information）１１

３、およびコンテンツのハッシュ値としてのコンテンツハッシュ１１４が格納される。なお、記録シード（ＲＥＣ　ＳＥＥＤ）１１２、ＣＣＩ（Copy Control Information）１１３、およびコンテンツハッシュ１１４は、コンテンツの暗号化、復号に適用する暗号鍵（ユニット鍵）の生成情報として利用される。詳細構成については、後述する。

【００４４】

リードイン領域１０２には、暗号化コンテンツ１１１の復号処理に適用する鍵の生成に必要となる暗号鍵情報１２０が格納される。暗号鍵情報１２０には、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックとしてのＥＫＢ（Enabling Key Block）１２１が含まれる。さらに、情報記録媒体１００は、物理インデックス（Ｐｈｙｓｉｃａｌ　Ｉｎｄｅｘ）１３１が記録される。以下、これらの各種情報の概要について説明する。

【００４５】

（１）暗号化コンテンツ１１１

情報記録媒体１００には、様々なコンテンツが格納される。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である。これらのコンテンツは、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。

【００４６】

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として格納される場合もある。サブコンテンツは、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可能である。

【００４７】

メインコンテンツ、サブコンテンツとともに、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。

【００４８】

（２）記録シード１１２

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。すなわち、コンテンツを構成するＡＶ(Audio Visual)ストリーム、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コンテンツなどは、コンテンツ利用の管理単位としてのユニットに区分され、区分されたユニット毎に異なる記録シード：Ｖｕ１１２が割り当てられている。

【００４９】

コンテンツ利用に際しては、記録シード：Ｖｕ１１２、暗号鍵情報１２０を適用した所定の暗号鍵生成シーケンスに従って、各ユニット対応の暗号鍵（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。すなわち、暗号化コンテンツ１１１は、ＣＰＳユニット単位に区分され、各ＣＰＳユニットに対応するユニット鍵で暗号化されて情報記録媒体１００に格納されている。

【００５０】

（３）コピー・再生制御情報（ＣＣＩ）１１３

コピー・再生制御情報（ＣＣＩ）１１３は、情報記録媒体１００に格納された暗号化コ

ンテンツ１１１に対応する利用制御のためのコピー制限情報や、再生制限情報である。このコピー・再生制御情報（ＣＣＩ）１１３は、ＣＰＳユニット個別の情報として設定される場合や、複数のＣＰＳユニットに対応して設定される場合など、様々な設定が可能である。この情報の詳細については後段で説明する。

【００５１】

（４）コンテンツハッシュ１１４

コンテンツハッシュ１１４は、情報記録媒体１００に格納されたコンテンツあるいは暗号化コンテンツの構成データに基づくハッシュ値であり、コンテンツの暗号処理、復号処理に適用する暗号鍵の生成情報として利用されるデータである。コンテンツハッシュ１１４の生成、利用態様については後段で説明する。

【００５２】

（５）物理インデックス１３１

物理インデックス１３１には、情報記録媒体のカテゴリ情報、例えばディスクの種別などのディスク付帯情報や、データ領域１０１に格納されたコンテンツに対応するコンテンツの付帯情報などが記録される。さらに、記録シード１１２と同様、情報記録媒体のデータ格納領域１０１に格納された暗号化コンテンツの復号処理に適用する鍵を生成するための鍵情報（鍵生成情報）が記録される場合もある。なお、物理インデックス１１３は、リードイン領域１０２に記録する構成としてもよい。

【００５３】

（６）暗号鍵情報１２０

暗号鍵情報１２０は、前述の記録シード１１２と同様、情報記録媒体のデータ格納領域１０１に格納された暗号化コンテンツの復号処理に適用する鍵を生成するための鍵情報（鍵生成情報）を取得するための暗号鍵ブロック、すなわち、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックとしてのＥＫＢ（Enabling Key Block）１２１を含む。

【００５４】

ＥＫＢ１２１は有効なライセンスを持つユーザの情報処理装置に格納されたデバイスキーに基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディアキー（Ｋｍ）を取得することを可能とした鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式によって、ユーザデバイス（情報処理装置）が有効なライセンスを持つ場合にのみ、鍵取得を可能としたものであり、無効化（リボーク処理）されたユーザデバイスの鍵（メディアキー）取得を阻止可能としたものである。管理センタはＥＫＢに格納する鍵情報の変更により、特定のユーザデバイスに格納されたデバイスキーでは復号できない、すなわちコンテンツ復号に必要なメディアキーを取得できない構成を持つＥＫＢを生成することができる。従って、任意タイミングで不正デバイスを排除（リボーク）して、有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。

【００５５】

［２．格納コンテンツの暗号化、利用管理構成］

次に、図２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。

【００５６】

前述したように、情報記録媒体に格納されるコンテンツは、区分コンテンツ毎の異なる利用制御を実現するため、区分コンテンツ毎に異なる鍵（ユニット鍵）が割り当てられ暗号化されて格納される。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。

【００５７】

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。

【００５８】

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２を参照して説明する。

【００５９】

図２に示すように、コンテンツは、（Ａ）タイトル２１０、（Ｂ）ムービーオブジェクト２２０、（Ｃ）プレイリスト２３０、（Ｄ）クリップ２４０の階層構成を有し、再生アプリケーションによってアクセスされるインデックスファイルとしてのタイトルが指定されると、タイトルに関連付けられた再生プログラムが指定され、指定された再生プログラムのプログラム情報に従ってコンテンツの再生順等を規定したプレイリストが選択され、プレイリストに規定されたクリップ情報によって、コンテンツ実データとしてのＡＶストリームあるいはコマンドが読み出されて、ＡＶストリームの再生、コマンドの実行処理が行われる。

【００６０】

図２には、２つのＣＰＳユニットを示している。これらは、情報記録媒体に格納されたコンテンツの一部を構成している。ＣＰＳユニット１，３０１、ＣＰＳユニット２，３０２の各々は、アプリケーションインデックスとしてのタイトルと、再生プログラムファイルとしてのムービーオブジェクトと、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を含むクリップを含むユニットとして設定されたＣＰＳユニットである。

【００６１】

コンテンツ管理ユニット（ＣＰＳユニット）１，３０１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）１，３０１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。

【００６２】

コンテンツ管理ユニット（ＣＰＳユニット）２，３０２には、タイトル３，２１３、再生プログラム２２４、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）２，３０２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。

【００６３】

例えば、ユーザがコンテンツ管理ユニット１，３０１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）１，３０１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。コンテンツ管理ユニット２，３０２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）２，３０２に対応付けて設定された暗号鍵としてのユニット鍵：Ｋｕ２を取得して復号処理を実行することが必要となる。

【００６４】

コンテンツを再生する情報処理装置において実行される再生アプリケーションプログラムは、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、再生アプリケーションプログラムは、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。

【００６５】

再生アプリケーションプログラムは、図３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。ユニット構成およびユニット鍵管理テーブルは、図３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。再生アプリケーションプログラムは、この管理テーブルに基づく管理を行う。

【００６６】

再生アプリケーションプログラムは、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。

【００６７】

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）１，３０１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）２，３０２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再生アプリケーションプログラムは、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。

【００６８】

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）１，３０１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）２，３０２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再生アプリケーションプログラムは、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。

【００６９】

［３．情報記録媒体の製造、データ格納処理の詳細］

上述したように、情報記録媒体１００には、暗号化コンテンツ１１１とともに、暗号化コンテンツ１１１の復号、再生に必要な様々な鍵情報、すなわち、ユニット鍵の生成に必要となる鍵生成情報が含まれる。図４を参照して、情報記録媒体の製造ルートについて説明する。

【００７０】

図４に示すように、情報記録媒体に格納するコンテンツは、コンテンツ編集エンティテイ（ＡＳ：Authoring Studio）３３０において編集され、その後、情報記録媒体製造エンティテイ（ＤＭ：Disc Manufacturer)３５０において、例えば、ＣＤ、ＤＶＤ、Ｂｌｕ－ｒａｙディスク等が大量に複製（レプリカ）されて、情報記録媒体１００が製造され、ユーザに提供される。情報記録媒体１００はユーザのデバイス（情報処理装置）４００において再生される。

【００７１】

このディスク製造、販売、使用処理全体についての管理を実行するのが管理センタ（ＴＣ：Trusted Center）３１０である。管理センタ（ＴＣ：Trusted Center）３１０は、情報記録媒体製造エンティテイ（ＤＭ：Disc Manufacturer)３５０に対して様々な管理情報、例えばメディア（情報記録媒体）に対応して設定されたメディアキーＫｍや、メディア

キーＫｍを暗号化データとして格納した暗号化キーブロックとしてのＥＫＢを提供し、情報記録媒体製造エンティテイ（ＤＭ：Disc Manufacturer)３５０は、管理センタ（ＴＣ：Trusted Center）３１０から受領した管理情報に基づいて、コンテンツ編集エンティテイ（ＡＳ：Authoring Studio）３３０から受領したコンテンツの編集、暗号化、鍵情報の、生成、格納処理などを行う。また、管理センタ（ＴＣ：Trusted Center）３１０は、ユーザの情報処理装置４００に格納するデバイスキーの管理、提供も行う。

【００７２】

管理センタ３１０、コンテンツ編集エンティテイ３３０、および情報記録媒体製造エンティテイ３５０の実行する２つの処理例について、図５、図６を参照して説明する。

【００７３】

図５は、管理センタ３１０、コンテンツ編集エンティテイ３３０、および情報記録媒体製造エンティテイ３５０の実行する１つの処理例を示した図である。

【００７４】

編集前コンテンツ３０３はコンテンツ編集エンティテイ３３０へ持ち込まれ、エンコーダによるＭＰＥＧデータ等へのエンコード処理（ステップＳ１２）、オーサリングシステムによる編集処理（ステップＳ１３）がなされた後、編集済コンテンツ３３１となる。

【００７５】

このオーサリングシステムによる編集処理（ステップＳ１３）の際、コンテンツに対応するコピー制限情報や、再生制限情報であるＣＣＩ情報（コピー・再生制御情報）３３２、およびコンテンツ暗号化に使用する記録シードＶｕ３３３も生成される。記録シード３３３は、前述したように、ＣＰＳユニットごとに設定することが可能であり、編集済コンテンツ３３１が複数のコンテンツ管理単位（ＣＰＳユニット）を持つ場合、記録シードＶｕ３３３もＣＰＳユニットの数だけ生成される。なお、記録シードＶｕ３３３の値は例えば１２８ビットの長さを持つ乱数である。ＣＣＩ情報３３２については、ＣＰＳユニット個別の情報として設定される場合や、複数のＣＰＳユニットに対応して設定される場合など、様々な設定が可能である。なお、図に示す編集済コンテンツ３３１にはＣＣＩ情報、記録シードＶｕが含まれ、編集済コンテンツ３３１は情報記録媒体製造エンティテイ３５０へ送られる。

【００７６】

情報記録媒体製造エンティテイ３５０はコンテンツ暗号化に必要な情報（管理情報）を管理センタ３１０から取得する。

【００７７】

管理センタ３１０ではメディアキーＫｍ３１１を生成し、さらに、メディアキーＫｍ３１１を暗号化データとして暗号化キーブロックとしてのＥＫＢに格納するＥＫＢ生成処理（ステップＳ１１）を実行し、ＥＫＢ３１２を生成する。

【００７８】

ＥＫＢ３１２は、前述したように、正当なコンテンツ利用権としてのライセンスを保持する再生装置に格納されたデバイスキーを適用した復号処理によってのみ復号することを可能とした暗号化データを格納しており、正当なコンテンツ利用権としてのライセンスを保持する再生装置のみがメディアキーＫｍを取得できる。

【００７９】

管理センタ３１０は、メディアキーＫｍを格納したＥＫＢ３１２と、メディアキーＫｍ３１１を含む管理情報を情報記録媒体製造エンティテイ３５０へ送る。

【００８０】

これらの情報を受け取った情報記録媒体製造エンティテイ３５０は以下の手順でコンテンツの暗号化を行う。

【００８１】

まず、ステップＳ１４において、ＣＰＳユニットに対応するユニット鍵の生成元となる鍵であるユニット鍵生成キーＫｅ（Embedded Key）を生成する。ユニット鍵生成キーＫｅ（Embedded Key）は、管理センタ３１０から取得したメディアキーＫｍと情報記録媒体製

造エンティテイ３５０内でセキュアに生成される物理インデックスＶｅ３５１を用いた暗号処理（例えばＡＥＳ暗号処理）によって生成される。

【００８２】

さらに、ステップＳ１５において、コンテンツ編集エンティテイ３３０から取得した編集済みコンテンツに対するハッシュ値（コンテンツハッシュ）を生成する。生成されるハッシュ値は、ＣＰＳユニットの構成データ、あるいはその一部データに基づいて生成されるハッシュ値である。ハッシュ生成処理は、例えばＡＥＳベースのハッシュ関数を適用したハッシュ値生成処理がなされる。

【００８３】

ステップＳ１６において、コンテンツハッシュと、ユニット鍵生成キーＫｅ（Embedded Key）と、コンテンツ編集エンティテイ３３０から取得したＣＣＩ情報と記録シードＶｕ、を利用して、コンテンツの暗号化に使用するユニット鍵Ｋｕを生成する。このユニット鍵Ｋｕ生成処理も例えばＡＥＳ暗号処理によって実行される。

【００８４】

前述したように、情報記録媒体に格納されるコンテンツは、コンテンツ管理ユニット（ＣＰＳユニット）に区分され、ＣＰＳユニット毎に記録シードＶｕが設定される。例えば、情報記録媒体に格納されるコンテンツに対応してｎ個のＣＰＳユニット１～ｎが設定されている場合、記録シードもＶｕ１～Ｖｕｎ生成されて、コンテンツ編集エンティテイ３３０から情報記録媒体製造エンティテイ３５０に提供される。

【００８５】

情報記録媒体製造エンティテイ３５０は、ユニット鍵生成キーＫｅ（Embedded Key）と、コンテンツ編集エンティテイ３３０から取得した編集済みコンテンツに基づいて生成したコンテンツハッシュと、ＣＣＩ情報、ｎ個の記録シードＶｕ１～Ｖｕｎを個別に、順次適用してｎ個のユニット鍵Ｋｕ１～Ｋｕｎを生成する。記録シードＶｕ１～Ｖｕｎはコンテンツ（ＣＰＳユニット）に応じた異なる値を有しており、生成されるユニット鍵Ｋｕ１～Ｋｕｎもそれぞれ異なる鍵データとなる。

【００８６】

次に、情報記録媒体製造エンティテイ３５０は、ステップＳ１７において、コンテンツ編集エンティテイ３３０から情報記録媒体製造エンティテイ３５０に提供される編集済みコンテンツの暗号化を実行する。すなわちＣＰＳユニット毎に、対応するユニット鍵Ｋｕ１～Ｋｕｎを適用した暗号化を実行し、暗号化コンテンツを生成する。なお、ユニット鍵を直接適用してコンテンツの暗号化を実行してもよいが、さらに、コンテンツをブロック単位に分割して、ブロック単位のブロックキーを生成してコンテンツの暗号化を行って記録する構成が好ましい。このブロックキーを適用した暗号化構成例については、後述する。

【００８７】

さらに、情報記録媒体製造エンティテイ３５０は、ステップＳ１８において、物理インデックス情報３５１、およびリードイン領域に記録する情報、ＥＫＢなどの各データ各々を予め定められた記録フォーマットとするフォーマット処理を実行し、最終的に図１で記載した情報の全てを情報記録媒体１００上に記録する。記録データには、ユニット鍵を適用して暗号化された暗号化コンテンツ、およびコンテンツハッシュが含まれる。なお、暗号化コンテンツには、ＣＣＩ情報、記録シードが含まれ、その一部は非暗号化データとされる場合もある。具体的なコンテンツ構成については後述する。また、情報記録媒体製造エンティテイ３５０の実行する各種の鍵生成処理の具体例としてのＡＥＳ暗号を適用した処理例については、後段で詳細に説明する。

【００８８】

次に、図６を参照して、コンテンツハッシュをユニット鍵Ｋｕ１～Ｋｕｎの生成に適用しない処理例について説明する。管理センタ３１０、コンテンツ編集エンティテイ３３０の処理は、図５を参照して説明した処理と同一であるので説明を省略する。情報記録媒体製造エンティテイ３５０は、以下の手順でコンテンツの暗号化を行う。

【００８９】
まず、ステップＳ２１において、ＣＰＳユニットに対応するユニット鍵の生成元となる鍵であるユニット鍵生成キーＫｅ（Embedded Key）を生成する。ユニット鍵生成キーＫｅ（Embedded Key）は、管理センタ３１０から取得したメディアキーＫｍと情報記録媒体製造エンティテイ３５０内でセキュアに生成される物理インデックスＶｅ３５１を用いた暗号処理（例えばＡＥＳ暗号処理）によって生成される。
【００９０】
さらに、ステップＳ２２において、ユニット鍵生成キーＫｅ（Embedded Key）と、コンテンツ編集エンティテイ３３０から取得したＣＣＩ情報と記録シードＶｕを利用して、コンテンツの暗号化に使用するユニット鍵Ｋｕを生成する。このユニット鍵Ｋｕ生成処理も例えばＡＥＳ暗号処理によって実行される。この例では、コンテンツハッシュはユニット鍵生成情報として適用されない。
【００９１】
情報記録媒体製造エンティテイ３５０は、ユニット鍵生成キーＫｅ（Embedded Key）と、コンテンツ編集エンティテイ３３０から取得したＣＣＩ情報、ｎ個の記録シードＶｕ１～Ｖｕｎを個別に、順次適用してｎ個のユニット鍵Ｋｕ１～Ｋｕｎを生成する。記録シードＶｕ１～Ｖｕｎはコンテンツ（ＣＰＳユニット）に応じた異なる値を有しており、生成されるユニット鍵Ｋｕ１～Ｋｕｎもそれぞれ異なる鍵データとなる。
【００９２】
ステップＳ２３において、コンテンツ編集エンティテイ３３０から情報記録媒体製造エンティテイ３５０に提供される編集済みコンテンツの暗号化を実行する。すなわちＣＰＳユニット毎に、対応するユニット鍵Ｋｕ１～Ｋｕｎを適用した暗号化を実行し、暗号化コンテンツを生成する。
【００９３】
さらに、ステップＳ２４において、暗号化済みのコンテンツに基づいてハッシュ値（コンテンツハッシュ）を生成する。生成されるコンテンツハッシュは、図５を参照して説明した先の例と異なり、暗号化されたコンテンツに基づいて生成される。ハッシュ生成処理は、例えばＡＥＳベースのハッシュ関数が適用される。
【００９４】
次に、情報記録媒体製造エンティテイ３５０は、ステップＳ２５において、物理インデックス情報３５１、およびリードイン領域に記録する情報、ＥＫＢなどの各データ各々を予め定められた記録フォーマットとするフォーマット処理を実行し、最終的に図１で記載した情報の全てを情報記録媒体１００上に記録する。記録データには、ユニット鍵を適用して暗号化された暗号化コンテンツ、およびコンテンツハッシュが含まれる。なお、暗号化コンテンツには、ＣＣＩ情報、記録シードが含まれ、その一部は非暗号化データとされる場合もある。
【００９５】
図４～図６を参照して説明した処理例は、管理センタからの管理情報、すなわち、メディアキーＫｍやＥＫＢを情報記録媒体製造エンティテイに提供する処理例であった。次に、図７～図９を参照して、管理センタからの管理情報、すなわち、メディアキーＫｍやＥＫＢをコンテンツ編集エンティテイに提供する処理例について説明する。
【００９６】
図７は、管理センタからの管理情報、すなわち、メディアキーＫｍやＥＫＢをコンテンツ編集エンティテイに提供する処理例における情報の流れを示している。情報記録媒体に格納するコンテンツは、コンテンツ編集エンティテイ（ＡＳ：Authoring Studio）３３０において編集され、その後、情報記録媒体製造エンティテイ（ＤＭ：Disc Manufacturer）３５０において、例えば、ＣＤ、ＤＶＤ、Ｂｌｕ－ｒａｙディスク等が大量に複製（レプリカ）されて、情報記録媒体１００が製造され、ユーザに提供される。情報記録媒体１００はユーザのデバイス（情報処理装置）４００において再生される。
【００９７】

このディスク製造、販売、使用処理全体についての管理を実行するのが管理センタ（ＴＣ：Trusted Center）３１０である。本実施例において、管理センタ（ＴＣ：Trusted Center）３１０は、コンテンツ編集エンティテイ（ＡＳ：Authoring Studio）３３０に対して様々な管理情報、例えばメディア（情報記録媒体）に対応して設定されたメディアキーＫｍや、メディアキーＫｍを暗号化データとして格納した暗号化キーブロックとしてのＥＫＢを提供し、コンテンツ編集エンティテイ（ＡＳ：Authoring Studio）３３０は、管理センタ（ＴＣ：Trusted Center）３１０から受領した管理情報に基づいてコンテンツの編集処理を実行し、情報記録媒体製造エンティテイ（ＤＭ：Disc Manufacturer)３５０に提供する。情報記録媒体製造エンティテイ（ＤＭ：Disc Manufacturer)３５０は、コンテンツ編集エンティテイ（ＡＳ：Authoring Studio）３３０から受領したコンテンツの暗号化、鍵情報の、生成、格納処理などを行う。また、管理センタ（ＴＣ：Trusted Center）３１０は、ユーザの情報処理装置４００に格納するデバイスキーの管理、提供も行う。

【００９８】

管理センタ３１０、コンテンツ編集エンティテイ３３０、および情報記録媒体製造エンティテイ３５０の実行する２つの処理例について、図８、図９を参照して説明する。

【００９９】

図８は、管理センタ３１０、コンテンツ編集エンティテイ３３０、および情報記録媒体製造エンティテイ３５０の実行する１つの処理例であり、コンテンツ編集エンティテイ３３０においてコンテンツの暗号化およびコンテンツハッシュ生成処理を実行する例を示した図である。

【０１００】

編集前コンテンツ３０３はコンテンツ編集エンティテイ３３０へ持ち込まれ、エンコーダによるＭＰＥＧデータ等へのエンコード処理（ステップＳ３２）、オーサリングシステムによる編集処理（ステップＳ３３）がなされた後、編集済コンテンツ３３１となる。

【０１０１】

このオーサリングシステムによる編集処理（ステップＳ３３）の際、コンテンツに対応するコピー制限情報や、再生制限情報であるＣＣＩ情報（コピー・再生制御情報）３３２、およびコンテンツ暗号化に使用する記録シードＶｕ３３３も生成される。記録シード３３３は、前述したように、ＣＰＳユニットごとに設定することが可能であり、編集済コンテンツ３３１が複数のコンテンツ管理単位（ＣＰＳユニット）を持つ場合、記録シードＶｕ３３３もＣＰＳユニットの数だけ生成される。なお、記録シードＶｕ３３３の値は例えば１２８ビットの長さを持つ乱数である。ＣＣＩ情報３３２については、ＣＰＳユニット個別の情報として設定される場合や、複数のＣＰＳユニットに対応して設定される場合など、様々な設定が可能である。

【０１０２】

本例においては、コンテンツ編集エンティテイ３３０において、コンテンツの暗号化が実行される。コンテンツ編集エンティテイ３３０は、コンテンツ暗号化に必要な情報（管理情報）を管理センタ３１０から取得する。

【０１０３】

管理センタ３１０ではメディアキーＫｍ３１１を生成し、さらに、メディアキーＫｍ３１１を暗号化データとして暗号化キーブロックとしてのＥＫＢに格納するＥＫＢ生成処理（ステップＳ１１）を実行し、ＥＫＢ３１２を生成する。ＥＫＢ３１２は、前述したように、正当なコンテンツ利用権としてのライセンスを保持する再生装置に格納されたデバイスキーを適用した復号処理によってのみ復号することを可能とした暗号化データを格納しており、正当なコンテンツ利用権としてのライセンスを保持する再生装置のみがメディアキーＫｍを取得できる。管理センタ３１０は、メディアキーＫｍを格納したＥＫＢ３１２と、メディアキーＫｍ３１１を含む管理情報をコンテンツ編集エンティテイ３３０へ送る。

【０１０４】

これらの情報を受け取ったコンテンツ編集エンティテイ３３０は以下の手順でコンテン

ツの暗号化を行う。

【０１０５】

まず、ステップＳ３４において、ＣＰＳユニットに対応するユニット鍵の生成元となる鍵であるユニット鍵生成キーＫｅ（Embedded Key）を生成する。ユニット鍵生成キーＫｅ（Embedded Key）は、管理センタ３１０から取得したメディアキーＫｍとコンテンツ編集エンティテイ３３０内でセキュアに生成される物理インデックスＶｅ３５１を用いた暗号処理（例えばＡＥＳ暗号処理）によって生成される。

【０１０６】

さらに、ステップＳ３５において、ユニット鍵生成キーＫｅ（Embedded Key）と、ＣＣＩ情報と記録シードＶｕを利用して、コンテンツの暗号化に使用するユニット鍵Ｋｕを例えばＡＥＳ暗号処理によって生成する。

【０１０７】

コンテンツ編集エンティテイ３３０は、ユニット鍵生成キーＫｅ（Embedded Key）と、ＣＣＩ情報、ｎ個の記録シードＶｕ１～Ｖｕｎを個別に、順次適用してｎ個のユニット鍵Ｋｕ１～Ｋｕｎを生成する。

【０１０８】

次に、ステップＳ３６において、編集済みコンテンツの暗号化を実行する。すなわちＣＰＳユニット毎に、対応するユニット鍵Ｋｕ１～Ｋｕｎを適用した暗号化を実行し、暗号化コンテンツを生成する。さらに、ステップＳ３７において、暗号化済みのコンテンツに基づいてハッシュ値（コンテンツハッシュ）を生成する。生成されるコンテンツハッシュは暗号化されたコンテンツに基づいて生成される。ハッシュ生成処理は、例えばＡＥＳベースのハッシュ関数が適用される。

【０１０９】

次に、コンテンツ編集エンティテイ３３０は、暗号化コンテンツ、コンテンツハッシュ、物理インデックス、および管理センタ３１０から受領したＥＫＢを情報記録媒体製造エンティテイ３５０に提供する。情報記録媒体製造エンティテイ３５０は、ステップＳ３８において、コンテンツ編集エンティテイ３３０から受領した各種情報のフォーマット処理を実行して、情報記録媒体１００上に記録する。ＥＫＢはリードイン領域に記録され、暗号化コンテンツ、コンテンツハッシュは、ユーザデータ領域に記録される。なお、暗号化コンテンツには、ＣＣＩ情報、記録シードが含まれ、その一部は非暗号化データとされる場合もある。

【０１１０】

図９は、コンテンツ編集エンティテイ３３０においてコンテンツの暗号化を行い、暗号化コンテンツに基づくコンテンツハッシュの生成処理を情報記録媒体製造エンティテイ３５０において実行する処理例を示した図である。

【０１１１】

図９に示すステップＳ３１～Ｓ３６の処理は、図８を参照して説明した処理と同様の処理であり、説明を省略する。コンテンツ編集エンティテイ３３０は、ユニット鍵生成キーＫｅ（Embedded Key）と、ＣＣＩ情報、ｎ個の記録シードＶｕ１～Ｖｕｎを個別に、順次適用してｎ個のユニット鍵Ｋｕ１～Ｋｕｎを生成し、ステップＳ３６において、ユニット鍵Ｋｕ１～Ｋｕｎを適用して編集済みコンテンツの暗号化を実行すると、暗号化コンテンツ、物理インデックス、および管理センタ３１０から受領したＥＫＢを情報記録媒体製造エンティテイ３５０に提供する。

【０１１２】

情報記録媒体製造エンティテイ３５０は、ステップＳ３７において、コンテンツ編集エンティテイ３３０から受領した暗号化コンテンツに基づいて、ハッシュ値（コンテンツハッシュ）を生成する。ハッシュ生成処理は、例えばＡＥＳベースのハッシュ関数が適用される。

【０１１３】

次に、情報記録媒体製造エンティテイ３５０は、ステップＳ３８において、コンテンツ

編集エンティティ３３０から受領した各種情報、および生成したコンテンツハッシュのフォーマット処理を実行して、情報記録媒体１００上に記録する。ＥＫＢはリードイン領域に記録され、暗号化コンテンツ、コンテンツハッシュは、ユーザデータ領域に記録される。なお、暗号化コンテンツには、ＣＣＩ情報、記録シードが含まれ、その一部は非暗号化データとされる場合もある。

【０１１４】

［４．情報処理装置におけるコンテンツ再生処理］

次に、上述したＣＰＳユニット単位の暗号化がなされた暗号化コンテンツおよび各種の鍵情報を格納した情報記録媒体の再生処理を実行する情報処理装置におけるコンテンツ再生処理の詳細について説明する。

【０１１５】

図１０に示すように、情報処理装置４００におけるコンテンツ再生は、暗号処理手段４１０における暗号化コンテンツの復号処理と、再生制御手段４２０における再生制御処理の２つのステップを含む。

【０１１６】

情報記録媒体１００から各種の情報が読み取られ、暗号処理手段４１０における暗号化コンテンツの復号処理が実行され、復号コンテンツが再生制御手段４２０に渡され、再生条件判定処理が実行され、再生条件を満足する場合にのみコンテンツ再生が継続して実行され、再生条件を満足しない場合には、コンテンツ再生が停止される。

【０１１７】

まず、暗号処理手段４１０における暗号化コンテンツの復号処理の詳細について、図１１を参照して説明する。

【０１１８】

コンテンツ復号プロセスでは、まず、暗号処理手段４１０は、メモリに格納しているデバイスキー４１１を読み出す。デバイスキー４１１は、コンテンツ利用に関するライセンスを受けた情報処理装置に格納された秘密キーである。

【０１１９】

次に、暗号処理手段４１０は、ステップＳ４１において、デバイスキー４１１を適用して情報記録媒体１００に格納されたメディアキーＫｍを格納した暗号鍵ブロックであるＥＫＢ４０１の復号処理を実行して、メディアキーＫｍを取得する。

【０１２０】

次に、ステップＳ４２において、ステップＳ４１におけるＥＫＢ処理で取得したメディアキーＫｍと、情報記録媒体１００から読み取った物理インデックス４０２とに基づく暗号処理（ＡＥＳ＿Ｈ）によって、ユニット鍵生成キーＫｅ（embedded Key）生成する。この鍵生成処理は、例えばＡＥＳ暗号アルゴリズムに従った処理として実行される。なお、図１１においてＡＥＳ＿Ｄは、ＡＥＳ暗号処理を適用したデータ復号（Decryption）処理、ＡＥＳ＿Ｈは、例えばＡＥＳベースのハッシュ関数であり、その具体構成は、図１５に示すように、ＡＥＳ暗号処理を適用したデータ復号処理を伴う鍵生成（Key Generation）処理実行部（ＡＥＳ＿ＧＤ）と排他的論理和部との組み合わせによって構成される。ＡＥＳ＿ＧＤ部は、図１５に示すようにＡＥＳ復号部と排他的論理和部との組みによって構成される。なお、先に図５、図６、図８、図９を参照して説明した情報記録媒体に記録するコンテンツハッシュの生成も、図１５に示すと同様のハッシュ演算部４３４の適用によって生成することができる。なお、図１５においてX、hで示している入力はAES_Hに対する２つの入力値のどちらを割り当ててもよく、例えば図１２の(b)の場合においてはXがKeでhがCCIとなる場合と、XがCCIでhがKeとなる場合の両方がありえ、実際の記録再生装置においてはどのように割り当てるかを選択して処理を実行することになる。また、ＡＥＳ＿ＧＥは、ＡＥＳ暗号処理を適用したデータ暗号処理を伴う鍵生成（Key Generation）処理を示している。

【０１２１】

次に、ステップＳ４３において、ユニット鍵生成キーＫｅ（embedded Key）と、情報記

録媒体１００から読み取ったコピー・再生制御情報（ＣＣＩ）４０３とに基づく暗号処理（ＡＥＳ＿Ｈ）によって、コントロールキーＫｃを生成し、ステップＳ４４において、コントロールキーＫｃと情報記録媒体１００から読み取ったコンテンツハッシュ４０４とに基づく暗号処理（ＡＥＳ＿Ｈ）によって、コンテンツハッシュキーＫｈを生成する。

【０１２２】

次に、ステップＳ４５において、情報記録媒体１００から読み取った暗号化ユニット鍵Ｅｎｃ（Ｋｕ）４０５に対して、コンテンツハッシュキーＫｈを適用して復号（ＡＥＳ＿Ｄ）し、ユニット鍵Ｋｕを取得する。なお、本例において、情報記録媒体１００に格納されるユニット鍵は、図１１のステップＳ４１～Ｓ４４と同様のプロセスによって生成されたコンテンツハッシュキーＫｈによる暗号化データとして格納されている。

【０１２３】

なお、情報記録媒体１００に記録されている暗号化ユニット鍵Ｅｎｃ（Ｋｕ）４０５はＣＰＳユニットごとに定義されており、Ｓ４５において生成されるユニット鍵Ｋｕも同様にＣＰＳユニットごとに定義される。生成するＣＰＳユニット鍵のＫｕ（ｉ）は、再生対象のコンテンツに対応するＣＰＳユニット、すなわち情報記録媒体１００に格納されたＣＰＳユニット１～ｎから選択されたＣＰＳユニット（ｉ）に対応して設定されているＣＰＳユニット鍵Ｋｕ（ｉ）である。

【０１２４】

暗号化コンテンツの復号を行う際、まずＳ４６において、情報記録媒体１００から読み出した暗号化コンテンツ４０６からのブロックシードの取り出し、復号処理の必要な復号処理部（暗号化データ）、復号処理の不要な非復号処理部（平文データ）のデータ選択が行われる。

【０１２５】

なお、ブロックシードは、暗号化処理単位としてのブロックに対応して設定される暗号鍵生成情報である。ＣＰＳユニットとしてのコンテンツデータは、所定データ長のブロック単位で異なるブロックキーＫｂが適用された暗号化がなされ、復号に際しては、各ブロック毎の復号処理鍵としてのブロックキーＫｂを、各ブロックデータに対応して設定されているブロックシードとＣＰＳユニット鍵Ｋｕに基づく暗号処理（Ｓ４７：ＡＥＳ＿ＧＥ）によって生成して、生成したブロックキーＫｂで復号処理（Ｓ４８）を行なう。

【０１２６】

ブロックキーＫｂは特定サイズの暗号処理単位において暗号化コンテンツの復号に使用される鍵である。暗号化処理単位のサイズとしては、例えば６１４４バイトのＵｓｅｒ Ｄａｔａを含むものや２０４８バイトのＵｓｅｒ Ｄａｔａを含むものが想定される。ブロックキーＫｂの生成およびブロックキーＫｂに基づく復号処理の詳細については、後段で説明する。

【０１２７】

ステップＳ４９は、暗号化コンテンツに含まれる例えばブロックシード部分などの非暗号化データと、ステップＳ４８において復号したデータを結合する処理であり、この結果、復号コンテンツ（ＣＰＳユニット）４１２が暗号処理手段４１０から再生制御手段４２０に出力される。

【０１２８】

なお、本例においては、コンテンツハッシュを暗号鍵生成に用いる構成であり、この場合、コンテンツハッシュは平文のコンテンツデータから生成されたものを適用する。具体的には、例えば先に図５を参照して説明したプロセスで製造されたデータ記録のなされた情報記録媒体１００に対する処理として実行される。

【０１２９】

ステップＳ４２～Ｓ４５、Ｓ４７において実行する暗号処理の具体例を図１２を参照して説明する。図１２において、ＡＥＳ復号部（ＡＥＳ＿Ｄ）４３１は、例えば１２８ビットの鍵長を持つＡＥＳ、ＥＣＢモードによる復号化処理部であり、ＡＥＳ暗号化部（ＡＥＳ＿Ｅ）４３３は、例えば１２８ビットの鍵長を持つＡＥＳ、ＥＣＢモードによる暗号化

処理部である。排他的論理和部４３２は、同じ長さを持つ２つのビット列間で排他的論理和（ＸＯＲ）処理を行う演算部を表している。

【０１３０】

図１１のステップＳ４２におけるユニット鍵生成キーＫｅの生成処理（ＡＥＳ＿Ｈ）は、具体的には、図１２（ａ）に示すように、情報記録媒体１００に格納された物理インデックスと、ＥＫＢから取得したメディアキーＫｍをＡＥＳ＿Ｈ処理に入力し、ＡＥＳ＿Ｈ処理を実行した結果値をユニット鍵生成キーＫｅとする処理として実行される。

【０１３１】

図１１のステップＳ４３におけるコントロールキーＫｃの生成、ステップＳ４４におけるコンテンツハッシュキーの生成も、図１２（ｂ），（ｃ）に示すようにＡＥＳ＿Ｈ処理によって行われる。ユニット鍵Ｋｕの生成は、図１２（ｄ）に示すように、情報記録媒体１００から取得した暗号化ユニット鍵ｅＫｈ（Ｋｕ）をコンテンツハッシュキーＫｈを適用してＡＥＳ復号部４３１において復号する処理として実行される。図１１のステップＳ４７のブロックキーＫｂの生成は、図１２（ｅ）に示すようにＡＥＳ復号部４３１と排他的論理和部４３２による演算によって行われる。

【０１３２】

なお、本実施例では、ＡＥＳ暗号アルゴリズムを適用し、１２８ビットの鍵長を持つ鍵データの生成例を示しているが、アルゴリズムや鍵長は、これらの例に限定されるものではなく、他のアルゴリズム、鍵長を適用することも可能である。

【０１３３】

次に、図１３を参照して、コンテンツ再生処理の他の処理例について説明する。図１３に示す例は、ステップＳ４２におけるユニット鍵生成キーＫｅ（embedded Key）の生成処理と、ステップＳ４３におけるコントロールキーＫｃの生成処理と、ステップＳ４４におけるコンテンツハッシュキーＫｈの生成処理を、ＡＥＳ暗号処理ではなく、ハッシュ関数（ＨＡＳＨ）を適用して実行する処理例である。

【０１３４】

これらの処理の具体的構成について、図１４を参照して説明する。図１４において、ハッシュ演算部（ＨＡＳＨ）４４１は、ハッシュ関数を用いた処理を実行して、２つの入力データに基づくハッシュ値を算出する。ハッシュ演算部（ＨＡＳＨ）４４１の出力は一意性の高い固定長のデータとなる。

【０１３５】

ハッシュ演算部（ＨＡＳＨ）４４１は、例えばＳＨＡ１などのハッシュ関数である。２つの値をハッシュ関数に入力し、１つの出力を得る場合、入力となる２つの値を連続してハッシュ関数に入力することによって１つの出力を得ることができる。例えば図１４(a)の場合、MediaKey(Km)と物理インデックスを連続してハッシュ関数へ入力することにより、EmbeddedKey(Ke)を得ることができる。この際、２つの入力のどちらを先に入力するかについては、Km→物理インデックスの順番と物理インデックス→Kmの順番の２通りがありえる。ハッシュ関数の説明、用法については図１４(b)、(c)についても同様である。

【０１３６】

図１４に戻り、コンテンツ再生処理における各種の鍵データの生成処理についての説明を続ける。図１３のステップＳ４２におけるユニット鍵生成キーＫｅ（embedded Key）の生成処理と、ステップＳ４３におけるコントロールキーＫｃの生成処理と、ステップＳ４４におけるコンテンツハッシュキーＫｈの生成処理は、図１４（ａ）～（ｃ）に示すように、ハッシュ演算部（ＨＡＳＨ）４４１の適用によって実行され、ハッシュ演算によって出力された結果が鍵データとなる。ステップＳ４５のユニット鍵生成、ステップＳ４７のブロックキーの生成は、図１４（ｄ）～（ｅ）に示すように、先の図１１、図１２を参照して説明した処理と同様の処理である。

【０１３７】

次に、図１６を参照して、コンテンツ再生処理の他の処理例について説明する。図１６に示す例は、コンテンツハッシュを鍵生成に適用しない処理例を示している。図１６のス

テップＳ５１～Ｓ５３は、図１１におけるステップＳ４１～Ｓ４３と同様の処理である。本例では、図１１におけるステップＳ４４の処理が省略される。すなわち、ステップＳ５３において生成したコントロールキーＫｃに基づいて、コンテンツハッシュキーを生成することなく、ステップＳ５４において、コントロールキーＫｃに基づいて情報記録媒体１００から読み取った暗号化ユニット鍵Ｅｎｃ（Ｋｕ）を復号（ＡＥＳ＿Ｄ）し、ユニット鍵Ｋｕを取得する。なお、本例において、情報記録媒体１００に格納されるユニット鍵は、図１６のステップＳ５１～Ｓ５３と同様のプロセスによって生成されたコントロールキーＫｃによる暗号化データとして格納されている。

【０１３８】

なお、情報記録媒体１００に記録されている暗号化ユニット鍵Ｅｎｃ（Ｋｕ）４０５はＣＰＳユニットごとに定義されており、Ｓ５４において生成されるユニット鍵Ｋｕも同様にＣＰＳユニットごとに定義される。生成するＣＰＳユニット鍵のＫｕ（ｉ）は、再生対象のコンテンツに対応するＣＰＳユニット、すなわち情報記録媒体１００に格納されたＣＰＳユニット１～ｎから選択されたＣＰＳユニット（ｉ）に対応して設定されているＣＰＳユニット鍵Ｋｕ（ｉ）である。ステップＳ５５～Ｓ５８の処理は、図１１におけるステップＳ４６～Ｓ４９の処理と同様の処理として実行される。本実施例では、コンテンツハッシュキーの生成プロセスが省略され、鍵生成処理が簡略化される。

【０１３９】

図１６のステップＳ５１，Ｓ５２，Ｓ５３，Ｓ５６の鍵生成プロセスの詳細について、図１７を参照して説明する。図１７の（ａ），（ｂ）は、図１２の（ａ），（ｂ）に対応し、図１７の（ｃ），（ｄ）は、図１２の（ｄ），（ｅ）に対応する。図１７に示す鍵生成処理では、図１７（ｃ）のユニット鍵生成プロセスにおいて、コントロールキーＫｃによる暗号化ユニット鍵のＡＥＳ復号処理が行われる点が、図１１、図１２を参照して説明したプロセスと異なる点である。

【０１４０】

図１８は、図１６と同様、コンテンツハッシュを鍵生成に適用しない処理例であり、ステップＳ５２におけるユニット鍵生成キーＫｅ（embedded Key）の生成処理と、ステップＳ５３におけるコントロールキーＫｃの生成処理を、図１５に示すＡＥＳ暗号を用いた処理ではなく、ハッシュ関数（ＨＡＳＨ）を適用して実行する処理例である。

【０１４１】

これらの処理の具体的構成について、図１９を参照して説明する。図１９において、ハッシュ演算部（ＨＡＳＨ）４４１は、ハッシュ関数を用いた処理を実行して、２つの入力データに基づくハッシュ値を算出する。前述したように、ハッシュ演算部（ＨＡＳＨ）４４１の出力は一意性の高い固定長のデータとなる。ハッシュ演算部（ＨＡＳＨ）４４１は、例えばＳＨＡ１などのハッシュ関数である。

【０１４２】

図１９の（ａ），（ｂ）は、先に説明した図１４の（ａ），（ｂ）に対応し、図１９の（ｃ），（ｄ）は、図１４の（ｄ），（ｅ）に対応する。図１９に示す鍵生成処理では、図１９（ｃ）のユニット鍵生成プロセスにおいて、コントロールキーＫｃによる暗号化ユニット鍵のＡＥＳ復号処理が行われる点が、図１３、図１４を参照して説明したプロセスと異なる点である。

【０１４３】

さらに、他のコンテンツ再生処理例について、図２０、図２１を参照して説明する。図２０は、先に図１１を参照して説明した処理では、ステップＳ４３においてコントロールキーＫｃ生成処理を実行し、ステップＳ４４において、コントロールキーＫｃに基づいて、コンテンツハッシュキーＫｈの生成処理を実行していたが、図２０に示す例では、この順番が変更され、ステップＳ６３において、情報記録媒体１００からコンテンツハッシュ４０４を読み取り、ステップＳ６２において生成したユニット鍵生成キーＫｅ（embedded Key）とコンテンツハッシュ４０４とに基づくＡＥＳ暗号アルゴリズムに従った処理によって、コンテンツハッシュキーＫｈを生成し、その後、ステップＳ６４において、情報記

録媒体１００からコピー・再生制御情報（ＣＣＩ）４０３を読み取って、コンテンツハッシュキーＫｈとコピー・再生制御情報（ＣＣＩ）４０３とに基づくＡＥＳ暗号アルゴリズムに従った処理によって、コントロールキーＫｃを生成する構成とした処理例である。その他のステップＳ６１～Ｓ６２，Ｓ６５～Ｓ６９の処理は、図１１を参照して説明した処理ステップＳ４１～Ｓ４２，Ｓ４５～Ｓ４９の処理と同様の処理である。

【０１４４】

本構成によれば、コンテンツハッシュキーＫｈは、コピー・再生制御情報（ＣＣＩ）４０３と無関係に生成可能となる。従って、コンテンツ編集エンティテイから管理センタに対してＣＣＩファイルを提出し、管理センタにおいて、ＣＣＩファイルに基づいてコンテンツハッシュキーＫｈを生成し、コンテンツ編集エンティテイに提供するという処理を行なう必要がなくなる。管理センタは、コンテンツ編集エンティテイに対してＥＫＢ、および記録シードＶｅ、さらに、ＣＣＩファイルに依存しない任意のコンテンツハッシュキーＫｈを発行するのみでよく、処理が簡略化される。

【０１４５】

図２１に示す処理例は、図２０に示す処理と同様、ＣＣＩファイルに依存しない任意のコンテンツハッシュキーＫｈを適用可能な例であるが、さらに、コンテンツハッシュキーＫｈの生成ステップを遅らせ、ステップＳ７４において生成したユニット鍵Ｋｕを適用して、ステップＳ７５において、コンテンツハッシュ４０５とのＡＥＳ暗号アルゴリズムに従った処理によって、コンテンツハッシュキーＫｈを生成する構成としたものである。

【０１４６】

なお、前述したように、情報記録媒体１００に記録されている暗号化ユニット鍵Ｅｎｃ（Ｋｕ）４０５はＣＰＳユニットごとに定義されており、Ｓ７４において生成されるユニット鍵Ｋｕも同様にＣＰＳユニットごとに定義される。生成するＣＰＳユニット鍵のＫｕ（ｉ）は、再生対象のコンテンツに対応するＣＰＳユニット、すなわち情報記録媒体１００に格納されたＣＰＳユニット１～ｎから選択されたＣＰＳユニット（ｉ）に対応して設定されているＣＰＳユニット鍵Ｋｕ（ｉ）である。

【０１４７】

従って、ステップＳ７５において生成するコンテンツハッシュキーＫｈも、ＣＰＳユニット（ｉ）に対応して設定されるコンテンツハッシュキーＫｈ（ｉ）となる。ステップＳ７７では、コンテンツハッシュキーＫｈ（ｉ）を適用してブロックキーＫｂが生成される。その他の処理は、図１１を参照して説明し他処理と同様である。

【０１４８】

本構成例では、コンテンツハッシュキーＫｈ（ｉ）の生成に適用するコンテンツハッシュも、各ＣＰＳユニット単位のコンテンツハッシュとなる。従って、より細かな単位でのコンテンツハッシュを取得することが必要となる。結果として、コンテンツ改竄を防止効果がより高まることになる。

【０１４９】

［５．情報記録媒体における記録データ、およびコンテンツ暗号化、復号処理の詳細］

次に、情報記録媒体における記録データ、およびコンテンツの暗号化、復号処理の詳細について説明する。まず、図２２を参照して、情報記録媒体に格納されるデータ記録構成および、記録データの復号処理の概要を説明する。情報記録媒体に格納されるデータは、前述したようにＣＰＳユニット単位のユニット鍵Ｋｕに基づいて生成されるブロック鍵Ｋｂでブロック単位の暗号化が施された暗号化データである。

【０１５０】

再生を行う場合には、先に、説明したように情報記録媒体に格納された各種の鍵生成情報に基づいて、ＣＰＳユニット鍵Ｋｕを生成し、さらに、ブロックデータ単位に設定されるブロックシードと、ＣＰＳユニット鍵Ｋｕに基づいてブロック鍵Ｋｂを生成し、ブロック鍵Ｋｂに基づくブロック単位の復号処理を行なう必要がある。

【０１５１】

図２２（ａ）は、情報記録媒体に格納されるデータ記録構成例を示している。１８バイトの制御データ（ＵＣＤ：User Control Data）と、実際のＡＶコンテンツデータを含む２０４８バイトのユーザデータ(User Data)が１つのセクタデータとして構成され、例えば3セクタ分６１４４バイトのデータが１つの暗号処理単位、すなわちブロックとして設定される。なお、ブロックの設定単位は、3セクタ分６１４４バイトのデータとする方式に限らず、１セクタ分２０４８バイトのデータを１つの暗号処理単位、すなわちブロックとして設定する方式など、様々な設定が可能である。これらの具体例については後述する。

【０１５２】

図２２（ｂ）は、3セクタ分６１４４バイトのデータを１つのブロックとして設定した場合の暗号処理単位としての１ユニット（１ＡＵ：Aligned Unit）の構成である。１８バイトの制御データ（User Control Data）は暗号化対象から除去され、実際のＡＶコンテンツデータであるユーザデータのみが、暗号処理単位として設定される。情報記録媒体に格納された暗号化データの再生を実行する情報処理装置は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Aligned Unit）を判別して抽出する。

【０１５３】

従って3セクタ分６１４４バイトのデータを１つのブロックとして設定した場合には、暗号化データの再生を実行する情報処理装置は、制御データ内のフラグに基づいて、暗号処理単位である６１４４バイトのデータを１ＡＵとして判別して６１４４バイト単位でブロック鍵Ｋｂを生成して復号処理を実行する。また、１セクタ分２０４８バイトのデータを１つのブロックとして設定した場合には、暗号化データの再生を実行する情報処理装置は、制御データ内のフラグに基づいて、暗号処理単位である２０４８バイト単位でブロック鍵Ｋｂを生成して復号処理を実行する。

【０１５４】

３セクタ分６１４４バイトのデータを１つのブロックとして設定した場合、暗号処理単位である1ユニット（１ＡＵ）には、図２２（ｃ）暗号化構成例に示すように、ブロック鍵Ｋｂによって暗号化された領域が含まれる。ブロック鍵を生成するためには、前述したようにブロックシードが必要となる。ブロックシードは、ＣＰＳユニット鍵Ｋｕとともに、ブロック鍵Ｋｂを生成するために必要となるブロック単位の鍵生成情報である。

【０１５５】

ブロック暗号化の対象となるユーザデータの詳細構成を図２３に示す。図２３（ａ）は、3セクタをブロックデータ（暗号化処理単位（６１４４バイト＝３２ソースパケット））とした場合のデータ構造である。

【０１５６】

ＡＶストリームはＢｌｕ－ｒａｙ　Ｄｉｓｃ　Ｒｅｗｒｉｔａｂｌｅフォーマットや Ｂｌｕ－ｒａｙ　Ｄｉｓｃ　ＲＯＭフォーマットにおいて規定されるデータ構造を持ち、3セクタ分６１４４バイトのデータを１つのブロックとして設定した場合、図２３(ａ)に示すように、６１４４バイトの暗号化処理単位（ブロック）が連続して、１つのＣＰＳユニットが設定される。６１４４バイトのデータは１９２バイトの長さを持つソースパケット３２個分のデータから構成される。

【０１５７】

各ソースパケットは、図２３（ｂ）に示すように、ヘッダ部４バイトとＴＳパケット部１８４バイトで構成されている。情報記録媒体に格納される暗号化コンテンツは、例えばＭＰＥＧ－２システムで規定（ISO/IEC１３８１８－１）されている符号化データとしてのトランスポートストリーム（ＴＳ）として構成される。トランスポートストリームは、１本のストリームの中に複数のプログラムを構成することができ、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されている。

【０１５８】

図２３（ｃ）は、ソースパケットのヘッダ部４バイトの詳細構成である。ヘッダ部４バ

イト中、先頭２ビットがコピー・再生制御情報ＣＣＩ（Copy Control Information）であり、その後に各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されている。タイムスタンプは、ＭＰＥＧ－２システムで規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport Stream System Target Decoder)を破綻させないように符号化時に決定され、ストリームの再生時に、各トランスポートパケットに付加されたＡＴＳによって出現タイミングを制御して、復号、再生を行う。

【０１５９】

例えば、トランスポートストリームパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

【０１６０】

以下、ブロック鍵Ｋｂを適用したブロックデータ単位の暗号化および復号処理の２つの具体例について説明する。

（１）処理例１

図２４に示す暗号化処理単位（ブロック）５００は、情報記録媒体に格納された暗号化コンテンツ（ＣＰＳユニット）を構成する１つの暗号化処理単位（ブロック）の構成である。

【０１６１】

暗号化処理単位５００は、３セクタ（６１４４バイト）分のユーザデータと、ユーザデータの先頭セクタに対応する１８バイトのユーザ制御データ（ＵＣＤ）５０１によって構成される。３セクタ（６１４４バイト）分のユーザデータの先頭１６バイト（１２８ビット）にブロックシード５１１が設定され、ブロック鍵Ｋｂによって暗号化されたデータ部が図に示す復号処理部５０２である。

【０１６２】

コンテンツ再生を実行する情報処理装置は、暗号化処理単位を順次取得し、例えば、図１１を参照して説明したセレクタ処理実行ステップＳ４６において、ブロックシード（１６バイト）５１１と、その他の復号処理部５０２を分離する処理を実行する。

【０１６３】

図２４のステップＳ８１の処理は、ブロック鍵Ｋｂ生成処理である。ステップＳ８１では、ブロックシード５１１に対して、ユニット鍵Ｋｕを適用したＡＥＳ暗号処理あるいはハッシュ処理を実行し、ブロック鍵Ｋｂを生成する。

【０１６４】

図２４のステップＳ８２の処理は、例えば図１１におけるステップＳ４８の復号処理に相当する処理である。ステップＳ８２では、復号処理部５０２を入力し、ステップＳ８１において生成したブロック鍵Ｋｂを適用したＡＥＳ復号処理を実行する。

【０１６５】

ステップＳ８２の復号処理の結果、復号されたユーザデータ５０３が生成され、このデータが、図１０に示す再生制御処理手段４２０に出力される。

【０１６６】

（２）処理例２

処理例２は、

暗号化処理単位（ブロック）：１セクタ（２０４８バイト）分のユーザデータ

暗号化対象データ：１セクタ（２０４８バイト）分のユーザデータの先頭１６バイト（１２８ビット）を除く部分（２０３２バイト）

ブロックシード：１セクタ（２０４８バイト）のユーザデータの先頭１６バイト（１２８ビット）

とした例である。

処理例２における記録データ構成例を図２５に示し、復号処理例を図２６に示す。

【０１６７】
まず、処理例２における記録データ構成について図２５を参照して説明する。図２５（ａ）には、１セクタ（２０４８バイト）のユーザデータとセクタ対応のユーザ制御データ１８バイトを示している。
【０１６８】
図２５（ｂ）に示すように、１セクタ（２０４８バイト）のユーザデータを１つの暗号処理単位（ブロック）として設定する。
【０１６９】
図２５（ｃ）暗号化構成に示すように、ブロックシードは、１セクタ（２０４８バイト）のユーザデータの先頭１６バイト（１２８ビット）とする。
【０１７０】
なお、暗号化されるコンテンツデータの内容は任意であり、ブロックシードに該当する部分のデータも任意のバイト列になる可能性がある。コンテンツデータの内容によっては、ブロックシード部分に特定のパターンのバイト列が配置されている可能性もあり、ブロックシードを使用して生成されるブロック鍵Ｋｂの値が暗号化処理単位ごとに異なる値となることは保証されない。
【０１７１】
この方法を利用する場合の利点として、1セクタ分（２０４８バイト）のデータを取得すれば、ブロックシードの取得、ブロック鍵の生成、コンテンツデータの復号化が可能であり、ＰＣに接続されるドライブなど、２０４８バイト単位のデータを汎用的な処理単位として使用するシステムに対する親和性が高いという利点がある。
【０１７２】
次に、図２６を参照して、本処理例における記録データの復号処理シーケンスについて説明する。図２６に示す暗号化処理単位（ブロック）５２０は、情報記録媒体に格納された暗号化コンテンツ（ＣＰＳユニット）を構成する１つの暗号化処理単位（ブロック）の構成である。
【０１７３】
暗号化処理単位５２０は、１セクタ（２０４８バイト）分のユーザデータ５２２と、ユーザデータの先頭セクタに対応する１８バイトのユーザ制御データ（ＵＣＤ）５２１によって構成される。本例において、ブロックシード５２３は、１セクタ（２０４８バイト）分のユーザデータ５２２の先頭１６バイト（１２８ビット）として設定されている。
【０１７４】
コンテンツ再生を実行する情報処理装置は、暗号化処理単位を順次取得し、例えば図１１を参照して説明したセレクタ処理実行ステップＳ４６において、ブロックシード（１６バイト）５２３と、その他の暗号化データ部（２０３２バイト）を分離する処理を実行する。なお、ユーザ制御データ（ＵＣＤ）５２１は非暗号化データとして分離される。
【０１７５】
図２６のステップＳ９１の処理は、ブロック鍵Ｋｂ生成処理である。ステップＳ９１では、１セクタ（２０４８バイト）のユーザデータの先頭１６バイト（１２８ビット）によって構成されるブロックシード５２３に対して、ユニット鍵Ｋｕを適用したＡＥＳ鍵生成処理アルゴリズムあるいはハッシュ処理を実行し、ブロック鍵Ｋｂを生成する。
【０１７６】
図２６のステップＳ９２の処理は、例えば図１１におけるステップＳ４８の復号処理に相当する処理である。ステップＳ９２では、１セクタ（２０４８バイト）のユーザデータの先頭１６バイト（１２８ビット）を除いた暗号化データ（２０３２バイト）のユーザデータを入力し、ステップＳ９１において生成したブロック鍵Ｋｂを適用したＡＥＳ復号処理を実行する。
【０１７７】
さらに、例えば図１１に示すセレクタステップＳ４９において、２０４８バイトのユーザデータの先頭１６バイト（１２８ビット）のブロックシード５２３を除く暗号化データ

部の復号結果と、ブロックシード５２３が結合されたデータとして復号データ５３１が生成され、その結果が、図１０に示す再生制御処理手段４２０に出力される。

【０１７８】

［６．コピー・再生制御情報（ＣＣＩ）の詳細構成］

次に、コピー・再生制御情報（ＣＣＩ）の詳細構成について説明する。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）対応のコピー・再生制御情報（ＣＣＩ）ファイルの構成例について説明する。

【０１７９】

各ＣＰＳユニットに対応するコピー・再生制御情報（ＣＣＩ）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。図２７には、コピー・再生制御情報（ＣＣＩ）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。

【０１８０】

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：２０３２バイト

の各データが格納される。

【０１８１】

ａ．第１ヘッダ部（１６バイト）には、第１制御情報（ＣＣＩ）領域に含まれるコピー・再生制御情報（ＣＣＩ）（再生／コピー制御情報）のループ数についての情報および追加制御情報領域が設定される。

【０１８２】

第１ヘッダ部に設定される追加情報領域とは、例えば基本制御情報のみに対応した再生装置に対して、基本制御情報のみによる再生を禁止するためのフラグを配置するなど、コピー・再生制御情報の追加・拡張のために使用する領域である。

【０１８３】

ヘッダ部に続くｂ．第１制御情報（ＣＣＩ）領域（２０３２バイト）には、各ＣＰＳユニット対応のコピー・再生制御情報（ＣＣＩ）（再生／コピー制御情報）が格納される。

【０１８４】

図２７には、第１ブロック７０１のコピー・再生制御情報（ＣＣＩ）（再生／コピー制御情報）として、

基本制御情報１（Ｂａｓｉｃ　ＣＣＩ-１）と、

拡張制御情報２（Ｂａｓｉｃ　ＣＣＩ-２）

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、５つの基本制御情報（Ｂａｓｉｃ　ＣＣＩ－１～５）ブロックが格納された例を示している。

【０１８５】

基本制御情報（Ｂａｓｉｃ　ＣＣＩ）は、ベーシックな最低限のコピー・再生制御情報（ＣＣＩ）（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ピー・再生制御情報（ＣＣＩ）（再生／コピー制御情報）によって構成されたデータである。

【０１８６】

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。

【０１８７】

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

【０１８８】

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

【０１８９】

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。

【０１９０】

図２７に戻り、コピー・再生制御情報（ＣＣＩ）を格納したブロックデータについて説明を続ける。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

の各データが格納される。

【０１９１】

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）領域に含まれるコピー・再生制御情報（ＣＣＩ）（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。

【０１９２】

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を除いた（２０４８×Ｎ－１６）バイトを超えない

範囲で複数のコピー・再生制御情報（ＣＣＩ）（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（Ｅｘｔｅｎｄｅｄ　ＣＣＩ－１～４）の合計４つの情報ブロックが格納された例を示している。

【０１９３】

以上の構成により、基本制御情報のみを使用する再生装置はＣＣＩファイルの先頭2048バイトを読み出すことにより、基本制御情報を取り出して再生やコピー動作の制御をおこなうことができる。

【０１９４】

図２９は、図２７に示すコピー・再生制御情報（ＣＣＩ）の格納例に対応するシンタックス図である。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。

【０１９５】

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ピー・再生制御情報（ＣＣＩ）（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

制御情報[Used for control info］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。

【０１９６】

さらに、第１制御情報（ＣＣＩ）領域情報として、

コピー・再生制御情報（ＣＣＩ）（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、

コピー・再生制御情報（ＣＣＩ）（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、

コピー・再生制御情報（ＣＣＩ）（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。

【０１９７】

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制御情報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、データ値を含むコピー・再生制御情報（ＣＣＩ）（再生/コピー制御情報）部が設定される。

【０１９８】

［７．情報処理装置の構成例］

次に、図３０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。

【０１９９】

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ＣＰＵ８７０、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。

【０２００】

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。

【０２０１】

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。

【０２０２】

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。

【０２０３】

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。

【０２０４】

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。

【０２０５】

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。

【０２０６】

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ＩＦ８１０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。

【０２０７】

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。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、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。

【０２０８】

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再生アプリケーションプログラムが、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。

【０２０９】

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。

【０２１０】

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３０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。

【０２１１】

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、特許請求の範囲の欄を参酌すべきである。

【０２１２】

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。

【０２１３】

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。

【０２１４】

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。

【０２１５】

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】

【０２１６】

以上、説明したように、本発明の構成によれば、情報記録媒体の格納コンテンツをユニットに区分したコンテンツ管理ユニット（ＣＰＳユニット）を設定するとともに、各コンテンツ管理ユニット（ＣＰＳユニット）個別にユニット鍵を対応付け、各ユニットの構成データを暗号化して記録する構成とし、再生時にはユニット鍵を生成し、ユニット鍵を適用したデータ処理を行なうことを必須とした。さらに、ユニット鍵の生成情報として、コンテンツ管理ユニット（ＣＰＳユニット）に対応して設定されるコピー・再生制御情報（ＣＣＩ）、コンテンツ管理ユニット（ＣＰＳユニット）の構成データに基づくハッシュ値であるコンテンツハッシュを適用する構成としたので、コピー・再生制御情報（ＣＣＩ）やコンテンツデータの改竄が行われた場合、正しいユニット鍵の生成が不可能となり、コピー・再生制御情報（ＣＣＩ）やコンテンツデータの改竄を防止でき、不正なコンテンツ利用を排除することができ、正当なコンテンツ利用構成が実現される。さらに、再生装置において、データ改竄の有無の検証処理を行なう必要がなくなり、効率的なデータ再生が可能となる。

【図面の簡単な説明】

【０２１７】

【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３】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４】情報記録媒体の製造工程における処理および情報管理構成例について説明する図である。

【図５】管理センタ、コンテンツ編集エンティテイ、および情報記録媒体製造エンティテイの実行する処理例について説明する図である。

【図６】管理センタ、コンテンツ編集エンティテイ、および情報記録媒体製造エンティテイの実行する処理例について説明する図である。

【図７】情報記録媒体の製造工程における処理および情報管理構成例について説明する図である。

【図８】管理センタ、コンテンツ編集エンティテイ、および情報記録媒体製造エンティテイの実行する処理例について説明する図である。

【図９】管理センタ、コンテンツ編集エンティテイ、および情報記録媒体製造エンティテイの実行する処理例について説明する図である。

【図１０】情報処理装置におけるコンテンツ再生の概要について説明する図である。

【図１１】情報処理装置におけるコンテンツ再生の一態様の詳細例について説明する図である。

【図１２】情報処理装置におけるコンテンツ再生に適用する鍵生成などの暗号処理の詳細について説明する図である。

【図１３】情報処理装置におけるコンテンツ再生の一態様の詳細例について説明する図である。

【図１４】情報処理装置におけるコンテンツ再生に適用する鍵生成などの暗号処理の詳細について説明する図である。

【図１５】情報処理装置におけるコンテンツ再生時に適用するハッシュ関数について説明する図である。

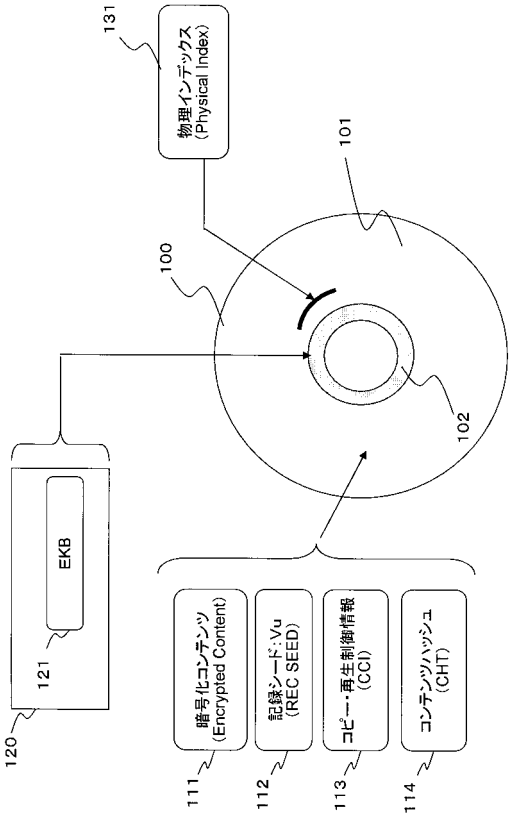
【図１６】情報処理装置におけるコンテンツ再生の一態様の詳細例について説明する図である。

【図１７】情報処理装置におけるコンテンツ再生に適用する鍵生成などの暗号処理の詳細について説明する図である。

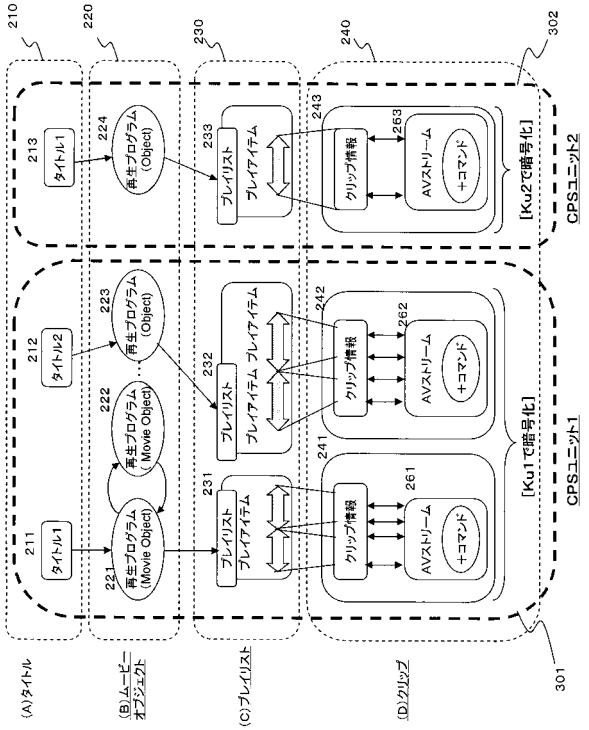
【図１８】情報処理装置におけるコンテンツ再生の一態様の詳細例について説明する図である。
【図１９】情報処理装置におけるコンテンツ再生に適用する鍵生成などの暗号処理の詳細について説明する図である。
【図２０】情報処理装置におけるコンテンツ再生の一態様の詳細例について説明する図である。
【図２１】情報処理装置におけるコンテンツ再生の一態様の詳細例について説明する図である。
【図２２】情報記録媒体に格納されるデータ記録構成および、記録データの復号処理の概要を説明する図である。
【図２３】ブロック暗号化の対象となるユーザデータの詳細構成について説明する図である。
【図２４】暗号化コンテンツの復号、再生処理例を説明する図である。
【図２５】暗号化コンテンツの記録データ構成例を説明する図である。
【図２６】暗号化コンテンツの復号、再生処理例を説明する図である。
【図２７】コンテンツ管理ユニット（ＣＰＳユニット）対応のコピー・再生制御情報（ＣＣＩ）ファイル構成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に示すコピー・再生制御情報（ＣＣＩ）の格納例に対応するシンタックス図である。
【図３０】情報記録媒体を装着して情報の記録再生を実行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】
【０２１８】
１００　情報記録媒体
１０１　ユーザデータ領域
１０２　リードイン領域
１１１　暗号化コンテンツ
１１２　記録シード
１１３　コピー・再生制御情報
１１４　コンテンツハッシュ
１２０　暗号鍵情報
１２１　ＥＫＢ（Enabling Key Block）
１３１　物理インデックス
２１０　タイトル
２２０　ムービーオブジェクト
２３０　プレイリスト
２４０　クリップ
２６１，２６２，２６３　ＡＶストリーム
３０１，３０２　コンテンツ管理ユニット（ＣＰＳユニット）
３１０　管理センタ
３１１　メディアキー
３１２　ＥＫＢ
３３０　コンテンツ編集エンティテイ
３３１　編集済コンテンツ
３３２　ＣＣＩ情報
３３３　記録シードＶｕ
３５０　情報記録媒体製造エンティテイ
３５１　物理インデックス

４００　情報処理装置
４０１　ＥＫＢ
４０２　物理インデックス
４０３　コピー・再生制御情報
４０４　コンテンツハッシュ
４０５　暗号化ユニット鍵
４０６　暗号化コンテンツ
４１０　暗号処理手段
４２０　再生制御処理手段
４３１　ＡＥＳ復号部
４３２　排他的論理和部
４３３　ＡＥＳ暗号化部
４４１　ハッシュ演算部
５００　暗号化処理単位（ブロック）
５０１　ユーザ制御データ（ＵＣＤ）
５０２　復号処理部
５０３　ユーザデータ
５１１　制御データ
５２０　暗号化処理単位（ブロック）
５２１　制御データ
５２２　ユーザデータ
５２３　ブロックシード
５３１　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
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】



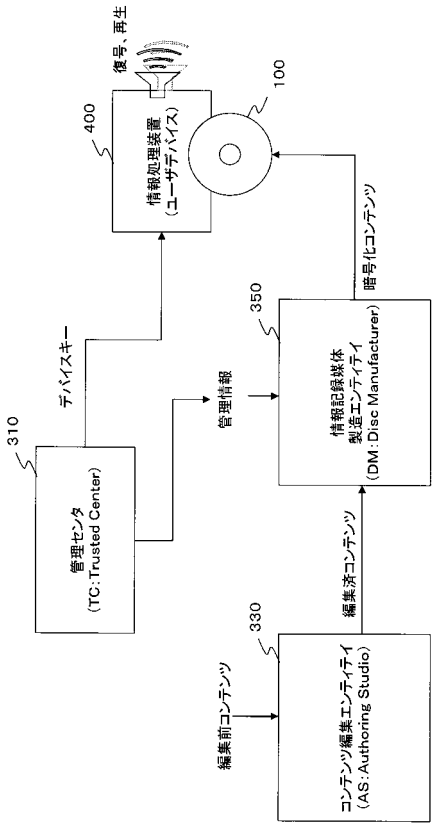
【図２】



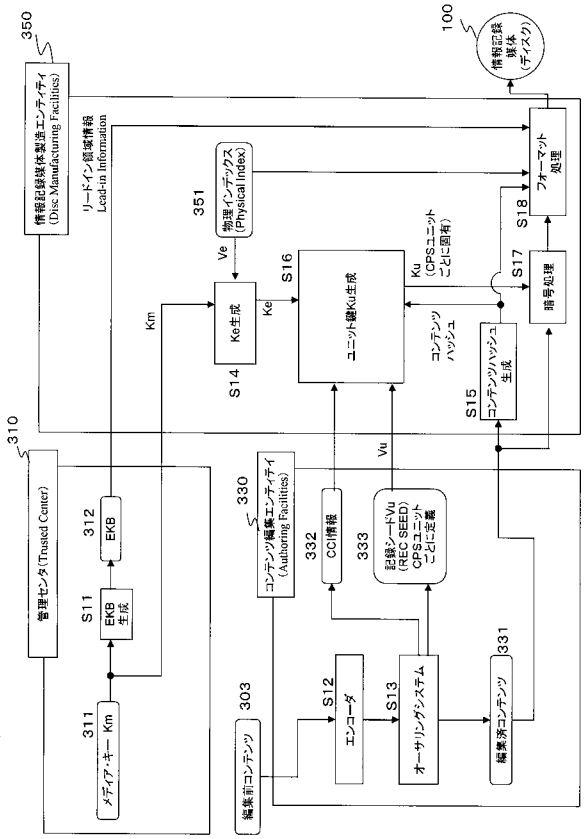
【図３】

タイトル等、アプリケーション層において区別可能なインデックス	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
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
データグループ2	CPS5	Ku5
：	：	：

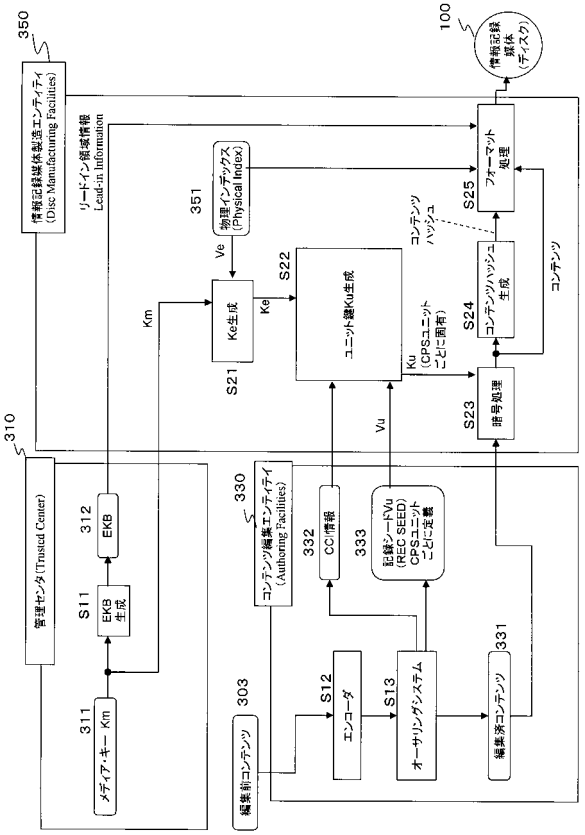
【図４】



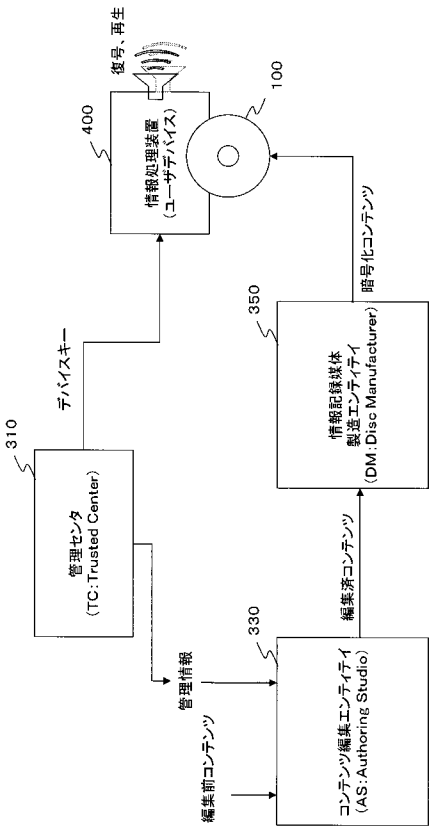
【図５】


情報記録媒体製造エンティティ (Disc Manufacturing Facilities)
リードイン領域情報 Lead-in Information
物理インデックス (Physical Index)
Ke生成
ユニット鍵Ku生成
コンテンツハッシュ生成
暗号処理
フォーマット処理
情報記録媒体 (ディスク)
管理センタ (Trusted Center)
メディア・キー Km
EKB生成
EKB
コンテンツ編集エンティティ (Authoring Facilities)
CCI情報
記録シードVu (REC SEED) CPSユニットごとに定義
編集前コンテンツ
エンコーダ
オーサリングシステム
編集済コンテンツ
Km
Ve
Ke
Ku (CPSユニットごとに固有)
Vu
コンテンツハッシュ
S11
S12
S13
S14
S15
S16
S17
S18
310
311
312
330
331
332
333
350
351

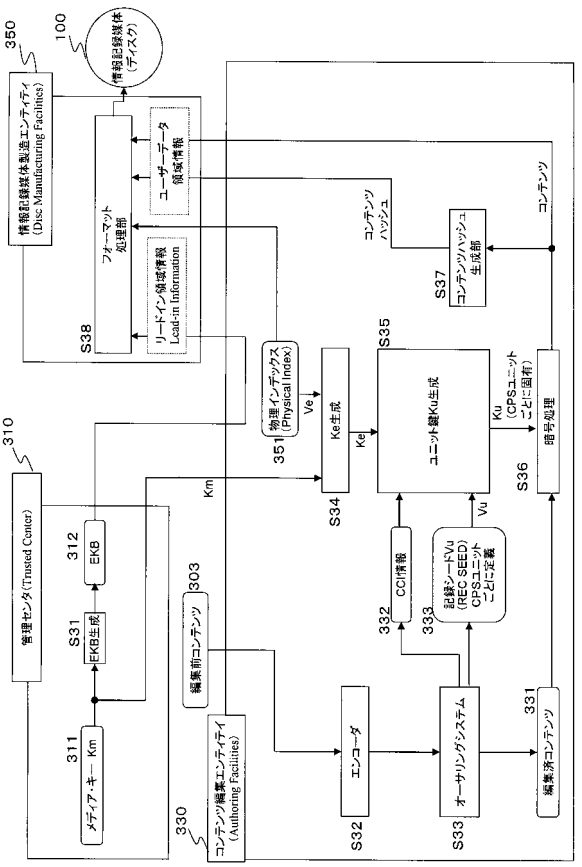
【図６】


情報記録媒体製造エンティティ (Disc Manufacturing Facilities)
リードイン領域情報 Lead-in Information
物理インデックス (Physical Index)
Ke生成
ユニット鍵Ku生成
コンテンツハッシュ生成
暗号処理
フォーマット処理
情報記録媒体 (ディスク)
管理センタ (Trusted Center)
メディア・キー Km
EKB生成
EKB
コンテンツ編集エンティティ (Authoring Facilities)
CCI情報
記録シードVu (REC SEED) CPSユニットごとに定義
編集前コンテンツ
エンコーダ
オーサリングシステム
編集済コンテンツ
Km
Ve
Ke
Ku (CPSユニットごとに固有)
Vu
コンテンツハッシュ
コンテンツ
S21
S22
S23
S24
S25
310
311
312
330
331
332
333
350
351

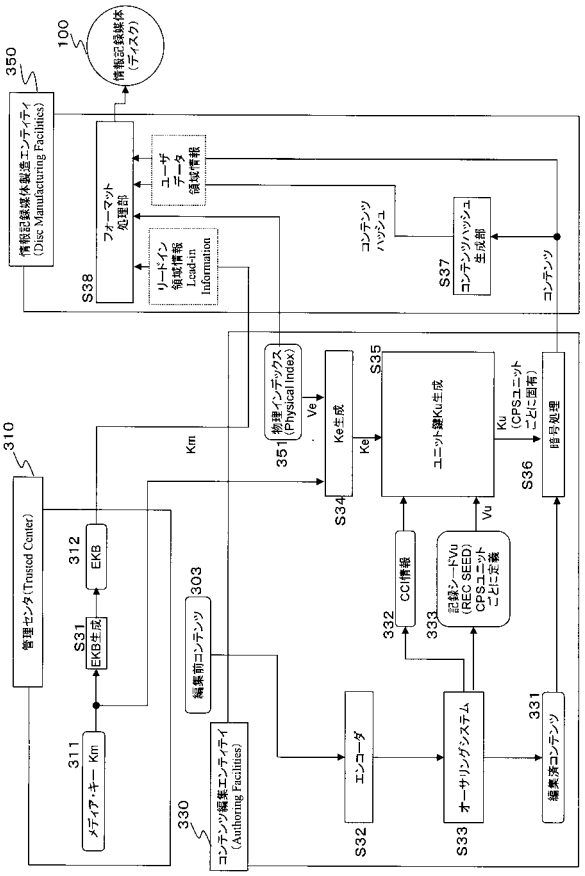
【図７】


復号、再生
情報処理装置 (ユーザデバイス)
デバイスキー
管理センタ (TC:Trusted Center)
管理情報
編集前コンテンツ
コンテンツ編集エンティティ (AS:Authoring Studio)
編集済コンテンツ
情報記録媒体 製造エンティティ (DM:Disc Manufacturer)
暗号化コンテンツ
100
310
330
350
400

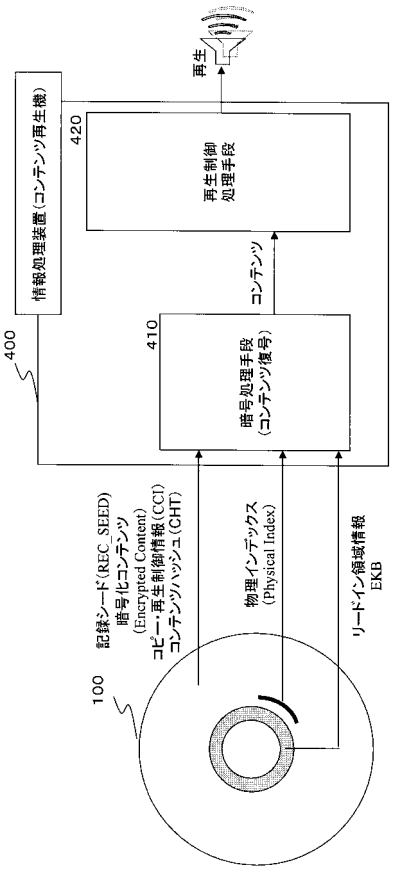
【図８】


情報記録媒体製造エンティティ (Disc Manufacturing Facilities)
情報記録媒体 (ディスク)
フォーマット処理部
ユーザーデータ領域情報
リードイン領域情報 Lead-in Information
物理インデックス (Physical Index)
Ke生成
ユニット鍵Ku生成
コンテンツハッシュ生成部
暗号処理
管理センタ (Trusted Center)
メディア・キー Km
EKB生成
EKB
コンテンツ編集エンティティ (Authoring Facilities)
CCI情報
記録シードVu (REC SEED) CPSユニットごとに定義
編集前コンテンツ
エンコーダ
オーサリングシステム
編集済コンテンツ
Km
Ve
Ke
Ku (CPSユニットごとに固有)
Vu
コンテンツハッシュ
コンテンツ
S31
S32
S33
S34
S35
S36
S37
S38
310
311
312
330
331
332
333
350
351

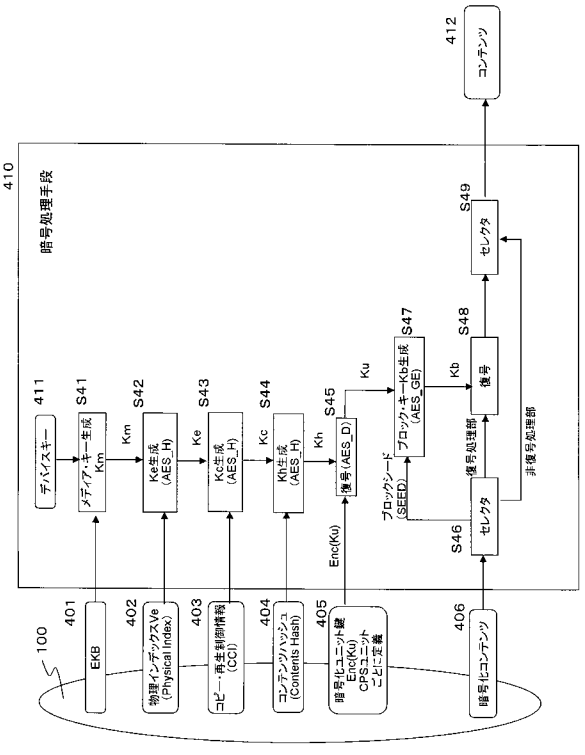
【図９】



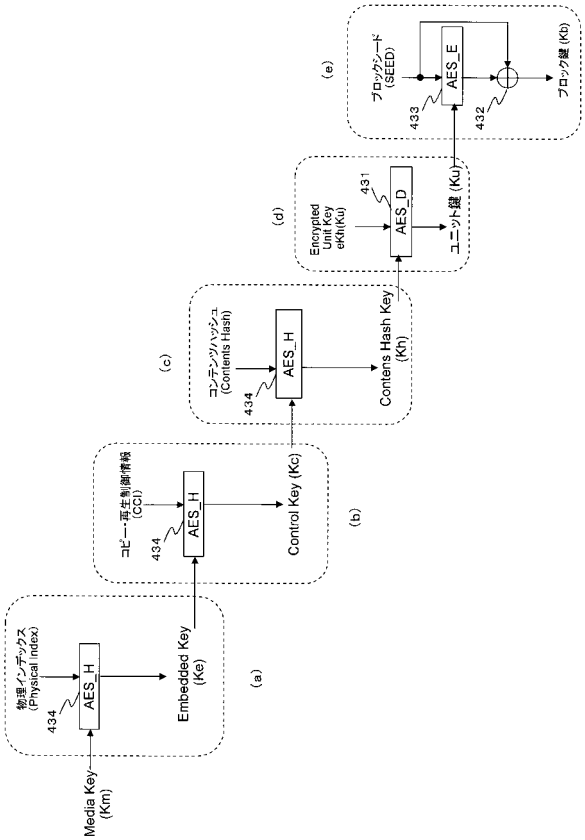
【図１０】



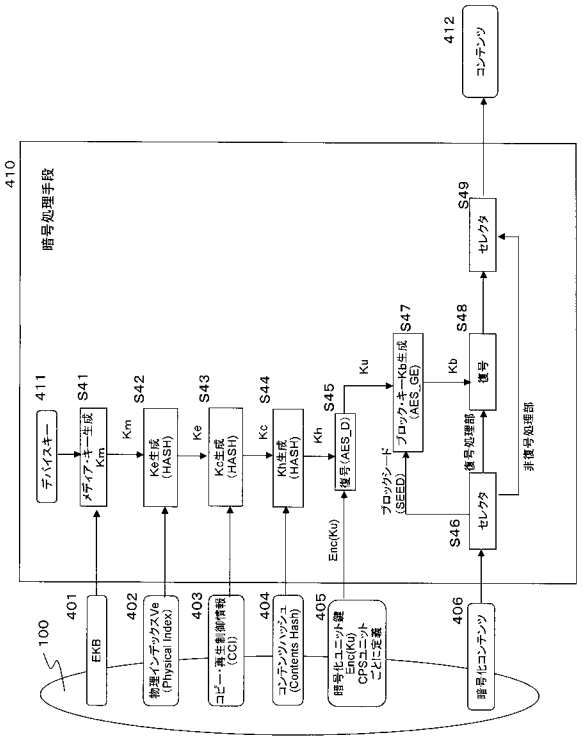
【図１１】



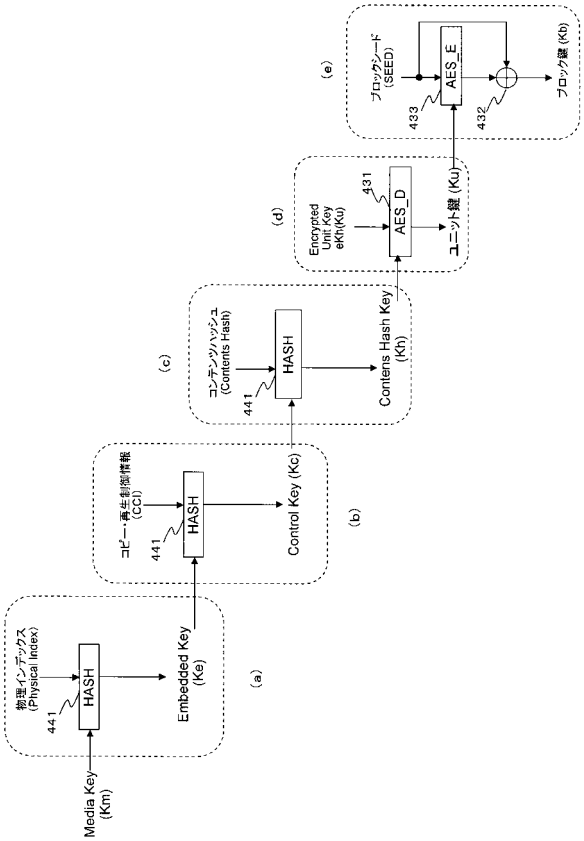
【図１２】



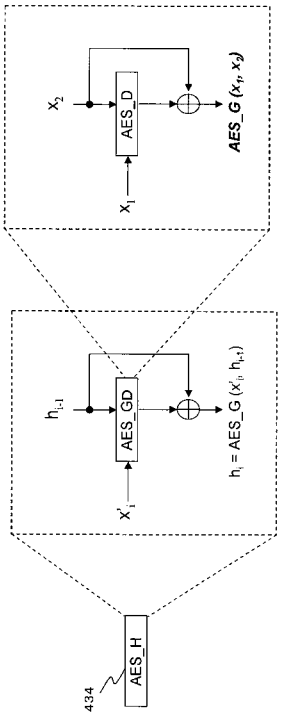
【図１３】



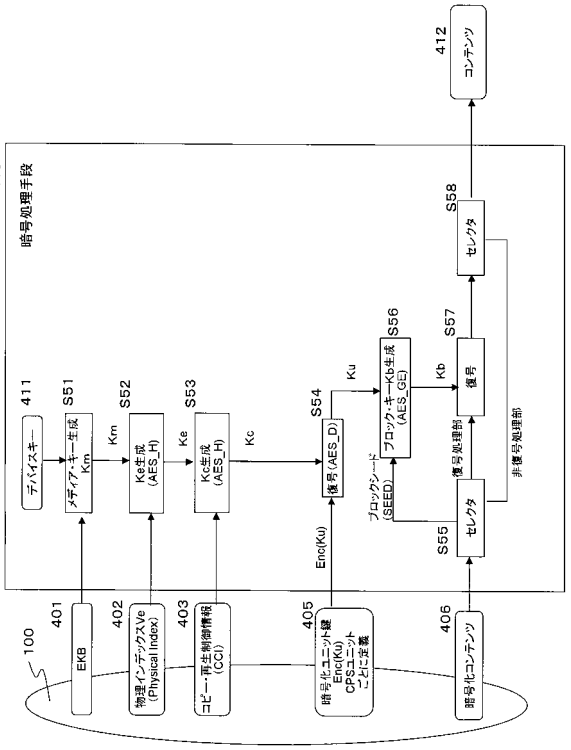
【図１４】



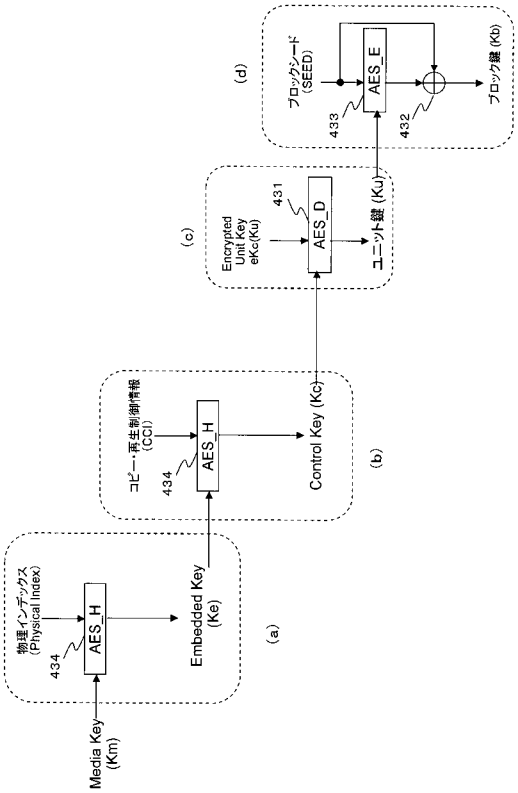
【図１５】



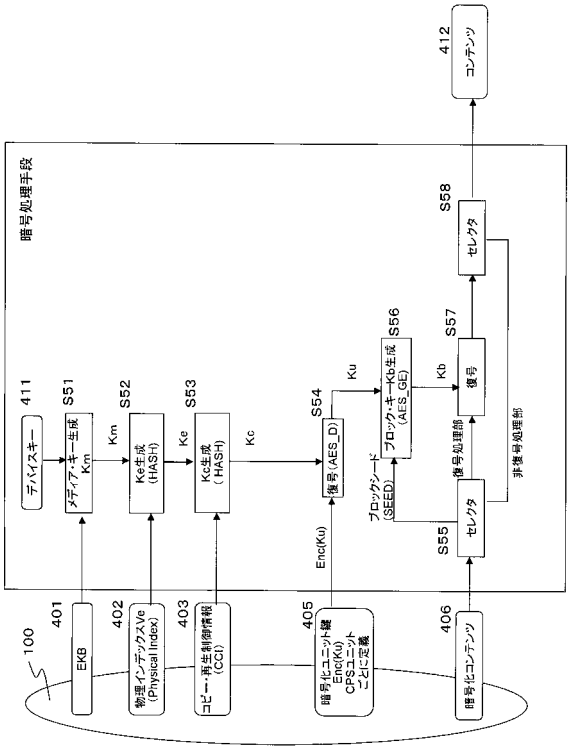
【図１６】



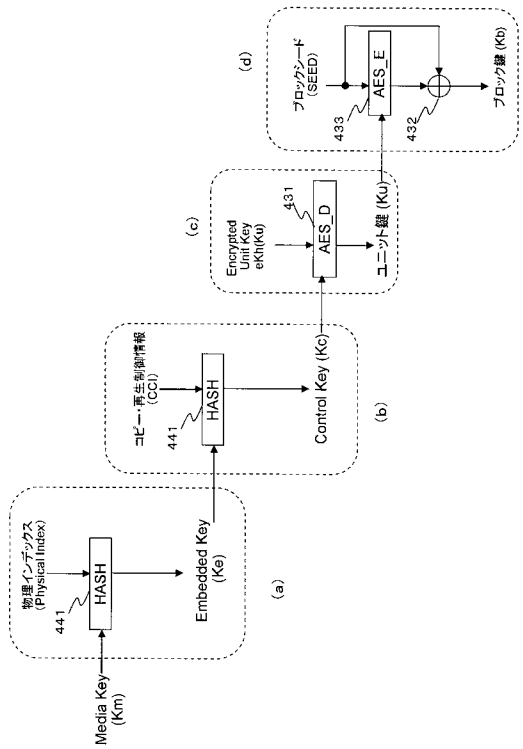
【図１７】



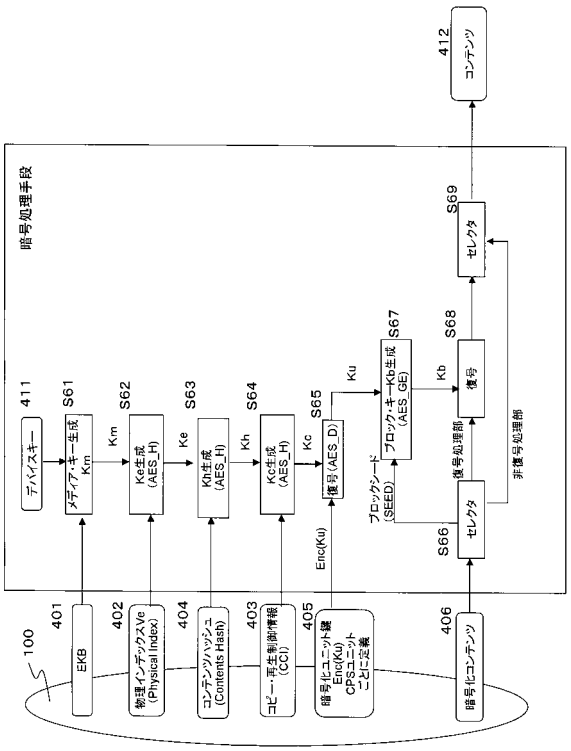
【図１８】



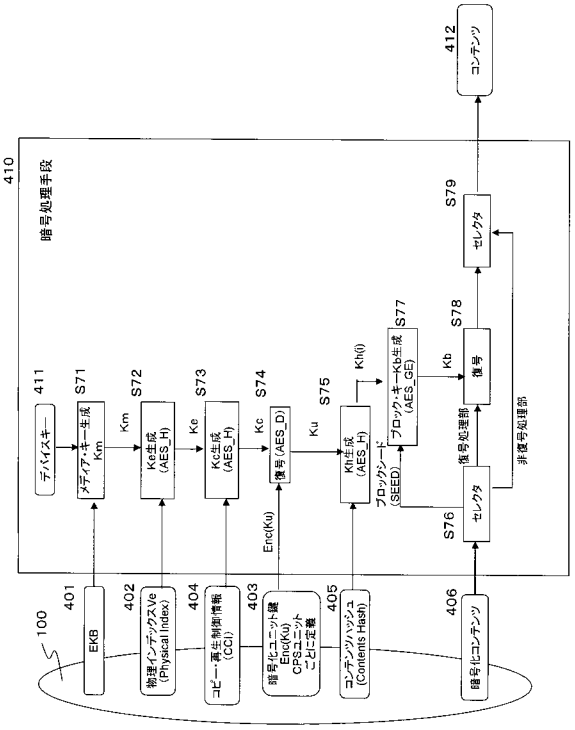
【図１９】



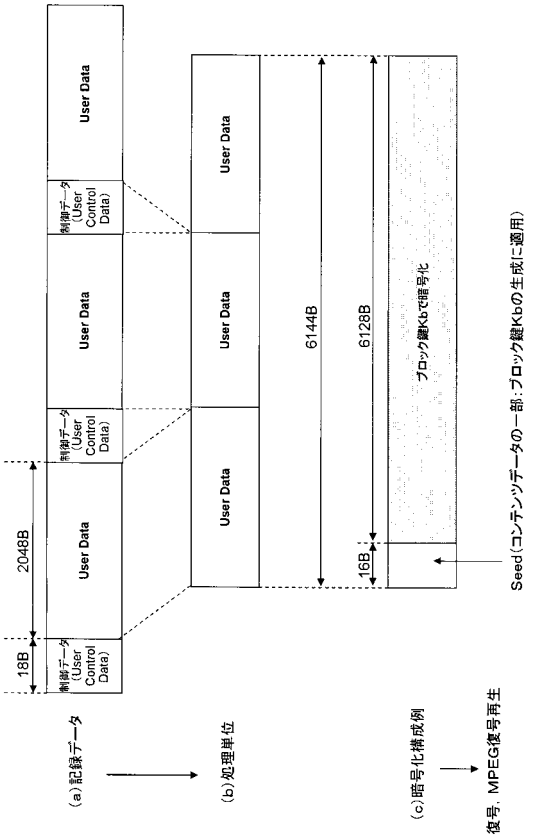
【図２０】



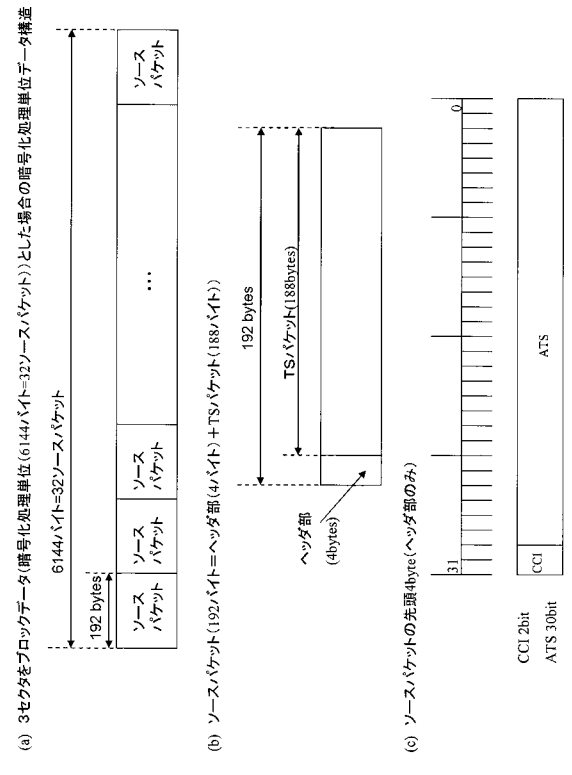
【図２１】



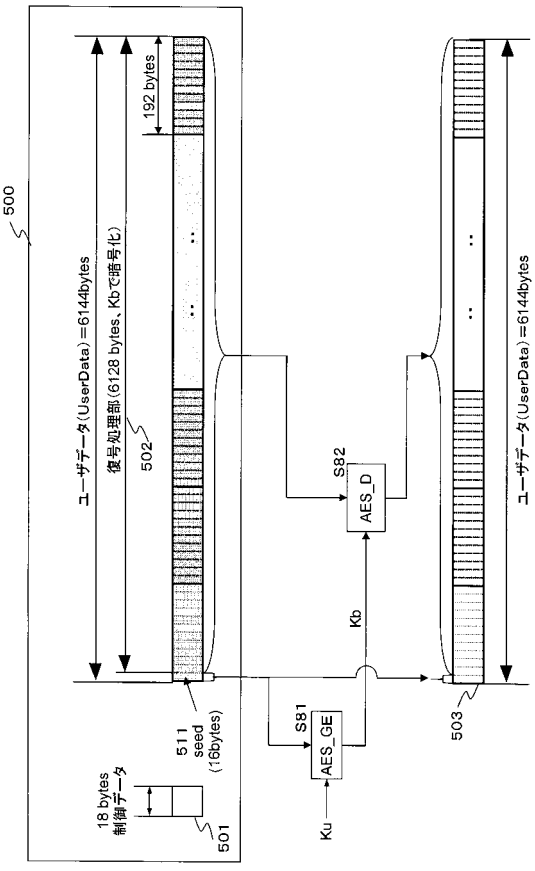
【図２２】



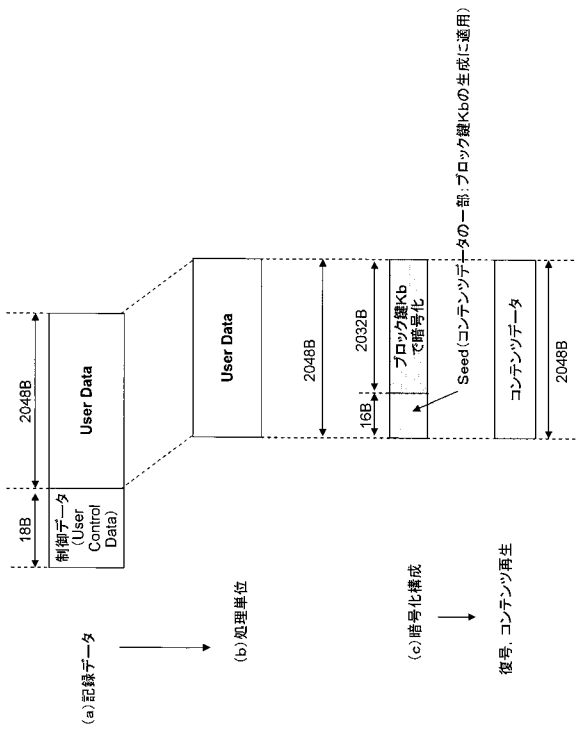
【図２３】



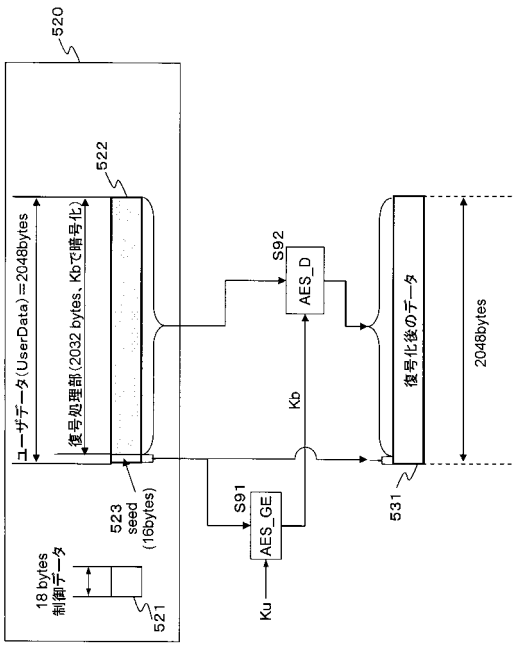
【図２４】



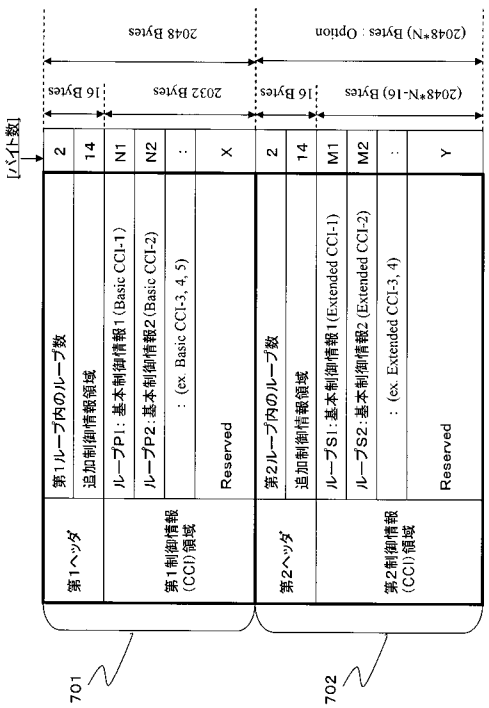
【図２５】



【図２６】



【図２７】



【図２８】

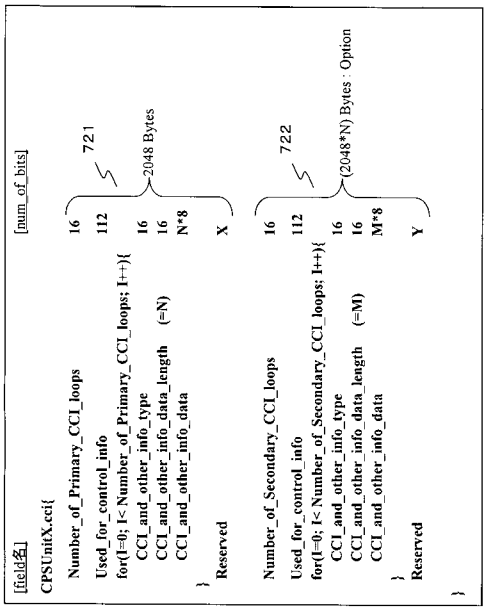
CCI_and_other_info() 基本情報の例

(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

CCI_and_other_info() 拡張情報の例

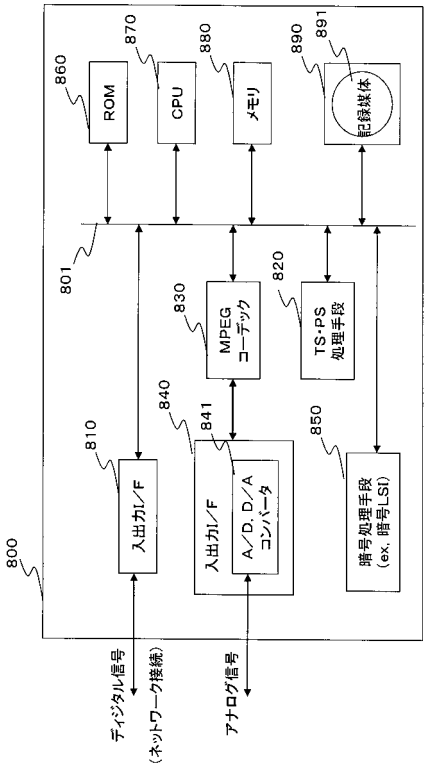
(名称)	(内容)
Disc単体での再生可否情報	Disc上の情報だけでコンテンツ再生が可能かどうかを示す
Disc単体では再生できないコンテンツの再生方法	「鍵配信サーバーへ接続」,「鍵の入ったメモリカードを挿入」 など
サーバーの指定	サーバーリストへのインデックス値
コピーストリーミング互換性情報	コンテンツをネットワーク内の他の機器で再生するための互換性情報
コピーストリーミング時のデータ変換方式	コンテンツを他の機器用に変換する際に使用できる方式
ネットワーク内の同種記録媒体へのコピー可否	OK/NG
ネットワーク内の同種記録媒体へのコピー回数	回数
ネットワーク内の同種記録媒体へのコピー有効期限	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	OK/NG
ネットワーク内の他種記録媒体へのコピー回数	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	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処の有無	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	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
ストリーミング可否	OK/NG
ストリーミング受信対象指定	対象機器を限定
連続再生の可否	OK/NG
連続再生要求対象指定	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	コピー自由無効化, 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を挿入」 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】



[field名]	[num_of_bits]	
CPSUnitX.cci{		
Number_of_Primary_CCI_loops	16	721
Used_for_control_info	112	
for(I=0; I< Number_of_Primary_CCI_loops; I++){		2048 Bytes
CCI_and_other_info_type	16	
CCI_and_other_info_data_length (=N)	16	
CCI_and_other_info_data	N*8	
}		
Reserved	X	
Number_of_Secondary_CCI_loops	16	722
Used_for_control_info	112	
for(I=0; I< Number_of_Secondary_CCI_loops; I++){		(2048*N) Bytes : Option
CCI_and_other_info_type	16	
CCI_and_other_info_data_length (=M)	16	
CCI_and_other_info_data	M*8	
}		
Reserved	Y	
}		

【図３０】



フロントページの続き

合議体
審判長　酒井　伸芳
審判官　石井　茂和
審判官　清木　泰

(56)参考文献　特開２００１－１６７５１８（ＪＰ，Ａ）
特開２００３－５０７４５（ＪＰ，Ａ）
特開平１０－２０８３８６（ＪＰ，Ａ）
特開平１０－３２０７７９（ＪＰ，Ａ）
特開２００１－２１６７２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08
G09C 1/00
G06F 21/24
G11B 20/10