(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4679093号
(P4679093)
(45)発行日　平成23年4月27日(2011.4.27)　(24)登録日　平成23年2月10日(2011.2.10)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
G06F 21/24 (2006.01)　H04L 9/00 601E
G09C 1/00 (2006.01)　G06F 12/14 530E
G06F 12/14 540B
G06F 12/14 540C
請求項の数 19　外国語出願　(全 35 頁)　最終頁に続く

(21)出願番号　特願2004-226124 (P2004-226124)
(22)出願日　平成16年8月2日 (2004.8.2)
(65)公開番号　特開2005-124149 (P2005-124149A)
(43)公開日　平成17年5月12日 (2005.5.12)
審査請求日　平成19年6月14日 (2007.6.14)
(31)優先権主張番号　0317967.8
(32)優先日　平成15年7月31日 (2003.7.31)
(33)優先権主張国　英国(GB)

(73)特許権者　593081408
ソニー　ヨーロッパ　リミテッド
イギリス国　サリー，ウェーブリッジ，ブルックランズ，ザ　ハイツ（番地なし）
(74)代理人　100104215
弁理士　大森　純一
(74)代理人　100117330
弁理士　折居　章
(72)発明者　ペリー　ジェイソン　チャールズ
イギリス国　ＫＴ１３　ＯＸＷ、　ウエィブリッジ、　ブルックランズ、　ザ　ハイツ　（番地無し）　ソニー　ユナイテッド　キングダム　リミテッド内

最終頁に続く

(54)【発明の名称】デジタルコンテンツのためのアクセス制御

(57)【特許請求の範囲】
【請求項１】
１つ以上のコンテンツ鍵の組を用いて、アクセス制御処理を入力データコンテンツに適用し、アクセス制御されたデータコンテンツをコンテンツストレージ媒体に記録する記録システムにおいて、
上記コンテンツ鍵の組に基づいて上記入力データコンテンツの一部を暗号化し、暗号化された入力データコンテンツを生成する暗号化ロジックを有する暗号化装置と、
データコンテンツを記録したユーザ又はユーザグループに関連する秘密鍵／公開鍵の対の秘密鍵を導出可能な情報を安全に保存するアクセス制御メモリ装置とを備え、
上記暗号化装置及びアクセス制御メモリ装置は、協働して、コンテンツアクセス制御データを生成するコンテンツアクセス制御データ生成器を提供し、上記コンテンツアクセス制御データは、上記コンテンツ鍵の組のそれぞれのサブセットの少なくとも１つの暗号化されたバージョンを含み、上記コンテンツアクセス制御データは、コンテンツ記録アクセス制御データとデフォルトアクセス制御データを含み、上記コンテンツ記録アクセス制御データは、上記アクセス制御メモリ装置に保存された情報から導出可能な秘密鍵に対応する公開鍵に基づいて生成され、上記デフォルトコンテンツアクセス制御データは、上記装置又は上記アクセス制御メモリ装置によってデフォルト公開鍵として定義された、それぞれのデフォルト公開鍵／デフォルト秘密鍵の対の１つ以上の公開鍵に基づいて生成され、上 記デフォルトコンテンツアクセス制御データは、上記デフォルト秘密鍵の１つを介して、上記入力データコンテンツに対し、上記データコンテンツを記録するユーザ又はユー

ザグループのアクセスレベルと同じアクセスレベルを提供し、
上記暗号化装置は、上記暗号化された入力データコンテンツを、上記コンテンツ記録アクセス制御データと上記デフォルトコンテンツアクセス制御データと共に上記コンテンツストレージ媒体に記録することを特徴とする記録システム。
【請求項２】
上記暗号化ロジックは、１つ以上のコンテンツ鍵の組を用いて、上記データコンテンツの一部に対称的な暗号化を適用することを特徴とする請求項１記載の記録システム。
【請求項３】
上記コンテンツアクセス制御データ生成器は、コンテンツセッション鍵を用いて、１つ以上のコンテンツ鍵の組の上記少なくとも１つのサブセットを対称的に暗号化し、それぞれの公開鍵／秘密鍵の対の公開鍵を用いて、上記コンテンツセッション鍵を非対称的に暗号化することを特徴とする請求項１記載の記録システム。
【請求項４】
上記コンテンツアクセス制御データ生成器は、それぞれの公開鍵／秘密鍵の対の公開鍵を用いて、上記１つ以上のコンテンツ鍵の組の上記少なくとも１つのサブセットを非対称的に暗号化することを特徴とする請求項１記載の記録システム。
【請求項５】
上記暗号化装置は、上記１つ以上のコンテンツ鍵の組を生成するためのロジックを有することを特徴とする請求項１記載の記録システム。
【請求項６】
上記アクセス制御メモリ装置と上記暗号化装置の少なくとも一方は、複数のアクセス制御メモリ装置のそれぞれに関連する公開鍵を保存するためのメモリを有することを特徴とする請求項１記載の記録システム。
【請求項７】
上記アクセス制御メモリ装置は、他のアクセス制御メモリ装置に保存されている秘密鍵に関連する公開鍵を格納することを特徴とする請求項１記載の記録システム。
【請求項８】
上記アクセス制御メモリ装置は、リムーバブルメモリ装置であり、上記暗号化装置は、上記暗号化装置と上記リムーバブルメモリ装置の間の安全なデータ接続を提供するインタフェースを備えることを特徴とする請求項１記載の記録システム。
【請求項９】
上記暗号化装置は、上記複数のリムーバブルメモリ装置のそれぞれに関連する上記複数の公開鍵を保存するためのメモリを含み、上記リムーバブルメモリ装置 は、該リムーバブルメモリ装置をそれぞれの公開鍵に関連させる識別データを保存することを特徴とする請求項８記載の記録システム。
【請求項１０】
上記リムーバブルメモリ装置は、上記情報コンテンツの暗号化を実行し、及び／又は上記コンテンツアクセス制御データを生成するデータ処理モジュールを備えることを特徴とする請求項８記載の記録システム。
【請求項１１】
上記リムーバブルメモリ装置は、スマートカードであることを特徴とする請求項８記載の記録システム。
【請求項１２】
上記リムーバブルメモリ装置は、マジックゲート（商標）メモリースティック（商標）装置であることを特徴とする請求項８記載の記録システム。
【請求項１３】
上記リムーバブルメモリ装置は、セキュアデジタルカードであることを特徴とする請求項８記載の記録システム。
【請求項１４】
上記暗号化装置は、オーディオ及び／又はビデオ捕捉又は処理装置を備えることを特徴

とする請求項１記載の記録システム。
【請求項１５】
上記入力データコンテンツは、ビデオ画像を含み、上記暗号化ロジックは、上記ビデオ画像に対し、対称暗号化、非対称暗号化及び可視ウォータマークの付与のうちの少なくとも１つを適用することを特徴とする請求項１記載の記録システム。
【請求項１６】
１つ以上のコンテンツ鍵の組を用いて、入力データコンテンツにアクセス制御処理を適用し、コンテンツストレージ媒体にアクセス制御されたデータコンテンツを記録する記録システムにおいて、
上記コンテンツ鍵の組に基づいて上記入力データコンテンツの一部を暗号化し、暗号化された入力データコンテンツを生成する暗号化ロジックと、
上記暗号化ロジックと、データコンテンツを記録したユーザ又はユーザグループに関連する秘密鍵／公開鍵の対の秘密鍵を導出可能な情報を安全に保存するアクセス制御メモリ装置との間の安全なデータ接続を提供するインタフェースと、
上記コンテンツ鍵の組のそれぞれのサブセットの少なくとも１つの暗号化されたバージョンと、上記アクセス制御メモリ装置に保存された情報から導出可能な秘密鍵に対応する公開鍵に基づいて生成されるコンテンツ記録アクセス制御データと、上記暗号化ロジック装置又は上記アクセス制御メモリ装置によってデフォルト公開鍵として定義されるそれぞれのデフォルト公開鍵／デフォルト秘密鍵組の１つ以上の公開鍵に基づいて生成され、上記デフォルト秘密鍵の１つを介して、上記入力データコンテンツに対し上記データコンテンツを記録したユーザ又はユーザグループに対するアクセスレベルと同じアクセスレベルを提供するデフォルトコンテンツアクセス制御データとを含むコンテンツアクセス制御データを生成するコンテンツアクセス制御データ生成器とを備え、
上記暗号化ロジックは、上記コンテンツストレージ媒体に上記コンテンツ記録アクセス制御データ及び上記デフォルトコンテンツアクセス制御データと共に上記暗号化された入力データコンテンツを記録することを特徴とする記録システム。
【請求項１７】
暗号化装置とアクセス制御メモリ装置とを備える記録システムにより、１つ以上のコンテンツ鍵の組を用いて、アクセス制御処理を入力データコンテンツに適用し、アクセス制御されたデータコンテンツをコンテンツストレージ媒体に記録する記録方法において、
上記暗号化装置により、上記コンテンツ鍵の組に基づいて上記入力データコンテンツの一部を暗号化し、暗号化された入力データコンテンツを生成するステップと、
上記アクセス制御メモリ装置により、データコンテンツを記録したユーザ又はユーザグループに関連する秘密鍵／公開鍵の対の秘密鍵を導出可能な情報を安全に保存するステップと、
上記暗号化装置及び上記アクセス制御メモリ装置の協働により、上記コンテンツ鍵の組のそれぞれのサブセットの少なくとも１つの暗号化されたバージョンと、上記アクセス制御メモリ装置に保存された情報から導出可能な秘密鍵に対応する公開鍵に基づいて生成されるコンテンツ記録アクセス制御データと、上記暗号化装置又は上記アクセス制御メモリ装置によってデフォルト公開鍵として定義されるそれぞれのデフォルト公開鍵／デフォルト秘密鍵組の１つ以上の公開鍵に基づいて生成され、上記デフォルト秘密鍵の１つを介して、上記入力データコンテンツに対し上記データコンテンツを記録したユーザ又はユーザグループに対するアクセスレベルと同じアクセスレベルを提供するデフォルトコンテンツアクセス制御データとを含むコンテンツアクセス制御データを生成するステップと、
上記暗号化装置により、上記暗号化された入力データコンテンツを、上記コンテンツ記録アクセス制御データと上記デフォルトコンテンツアクセス制御データと共に上記コンテンツストレージ媒体に記録するステップとを有する記録方法。
【請求項１８】
コンピュータに、請求項１７記載の記録方法における各ステップを実行させるプログラム。

【請求項１９】
請求項１８記載のプログラムを記録した記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタルコンテンツのためのアクセス制御に関する。このようなコンテンツとしては、例えばオーディオビジュアルコンテンツ等、ビデオコンテンツ、オーディオコンテンツ、メタデータコンテンツ、テキストコンテンツ、画像コンテンツの１つ以上が含まれる。
【背景技術】
【０００２】
プロセッサパワーの強化と相まって、デジタル機器及び高速ネットワークを始めとする新たなデジタルインフラストラクチャの成長により、コンテンツの作成、処理及び配布が簡単で高速に行えるようになった。このことは、コンテンツの合法的な使用を大いに促進するが、このようなコンテンツ（特に、著作権コンテンツ）の権限なき不正使用、例えば権限のない再生又は配布もより容易に行うことができるようになり、コンテンツの所有者の被害も大きくなっている。
【０００３】
ユーザがコンテンツを使用する権利を所有者から購入する前に、商業的理由から、コンテンツの所有者が潜在的ユーザにコンテンツの視聴又は使用を試させる場合があり、このことが状況をより複雑にしている。
【０００４】
これらの問題を解決するために、所謂デジタル著作権管理（digital rights management：以下、ＤＲＭという。）システムが提案されている。周知のＤＲＭシステムは、通常、コンテンツを配信するために、データ暗号化技術を用いてコンテンツを暗号化する。認証された受信者（recipient）は、復号鍵を受け取り、受信者は、暗号化されたコンテンツを復号することができる。これは、コンテンツへのアクセス制御を実現する極めて基本的な手法であるが、この手法は煩雑であり、柔軟性に欠ける。アクセスを提供するために用いられる全てのデータ（この場合、復号鍵及び関連するアクセス許可データを含む）は、それが関係する記録された情報コンテンツとは別に保存されている。この手法では、コンテンツと関連するアクセスデータとの関係を把握するためのある種のデータベースを維持しなくてはならないという問題が生じる。これらの短所の全ては、職場の生産性を低下することになる。
【発明の開示】
【課題を解決するための手段】
【０００５】
本発明に係る記録システムは、１つ以上のコンテンツ鍵の組を用いて、アクセス制御処理を入力データコンテンツに適用し、アクセス制御されたデータコンテンツをコンテンツストレージ媒体に記録する記録システムにおいて、コンテンツ鍵の組に基づいて入力データコンテンツの一部を暗号化し、暗号化された入力データコンテンツを生成する暗号化ロジックを有する暗号化装置と、データコンテンツを記録したユーザ又はユーザグループに関連する秘密鍵／公開鍵の対の秘密鍵を導出可能な情報を安全に保存するアクセス制御メモリ装置とを備え、暗号化装置及びアクセス制御メモリ装置は、協働して、コンテンツアクセス制御データを生成するコンテンツアクセス制御データ生成器を提供し、コンテンツアクセス制御データは、コンテンツ鍵の組のそれぞれのサブセットの少なくとも１つの暗号化されたバージョンを含み、コンテンツアクセス制御データは、コンテンツ記録アクセス制御データとデフォルトアクセス制御データを含み、コンテンツ記録アクセス制御データは、アクセス制御メモリ装置に保存された情報から導出可能な秘密鍵に対応する公開鍵に基づいて生成され、デフォルトコンテンツアクセス制御データは、装置又はアクセス制御メモリ装置によってデフォルト公開鍵として定義された、それぞれのデフォルト公開鍵

／デフォルト秘密鍵の対の１つ以上の公開鍵に基づいて生成され、デフォルトコンテンツアクセス制御データは、デフォルト秘密鍵の１つを介して、入力データコンテンツに対し、データコンテンツを記録するユーザ又はユーザグループのアクセスレベルと同じアクセスレベルを提供し、暗号化装置は、暗号化された入力データコンテンツを、コンテンツ記録アクセス制御データとデフォルトコンテンツアクセス制御データと共にコンテンツストレージ媒体に記録する。

【０００６】

本発明は、コンテンツに対する選択的且つ個別のアクセスの必要性を見出し、これを実現する。更に、本発明は、コンテンツに対する単独のアクセス権を個々のユーザに与えるだけでは不十分であるという問題を見出し、これを解決する。

【０００７】

例えば、映画制作スタジオ等のプロフェッショナルの環境では、その制作の様々な段階において、制作に関わる多くの異なった個人について、コンテンツへの限定的なアクセスを実現することが必要となる。ここで、コンテンツの全体的な安全性を確保するためには、コンテンツ全体へのアクセス権は、制作チームのうちの僅かな主要メンバ（senior members）だけに与えることが望ましい。本発明の実施例は、例えば、個々のユーザに対し、記録／再生装置に保存された全体のコンテンツのうちのサブセットの復号を可能にする１つ以上の秘密鍵が格納されたリムーバブルメモリ装置（removable memory device：ＲＭＤ）（例えば、所謂スマートカード、ソニー（商標）マジックゲート（商標）セキュリティ技術を用いることができるソニー（商標）メモリースティック（商標）ストレージ装置、セキュアデジタルカード等）を与えることによって上述の問題を解決する。デフォルト公開鍵は、制作チームのシニアメンバの要求に応えるために用いられる。制作チームの個人のメンバがチームを去っても、又はそのメンバがリムーバブルメモリ装置を紛失しても、デフォルト公開鍵に関連付けられたユーザは、コンテンツにアクセスすることができる。

【０００８】

別の例示的な状況として、コンテンツは、例えば、コンパクトディスク、ＤＶＤディスク、又は所謂ブルーレイ（商標）ディスク等の高密度ストレージデバイスを介して配付してもよい。本発明に基づく手法では、生産を容易にするために、異なるディスクを生成してこの在庫を保有する必要がないよう、単一のディスクに全体のコンテンツを保存する。なお、各ユーザに許可されるアクセスの程度は、それぞれのＲＭＤに保存された秘密鍵によって制限される。有効なＲＭＤを保有しているユーザには、そのユーザのＲＭＤに保存されている秘密鍵に基づいて、コンテンツの選択された部分へのアクセスが許可される。所定のユーザのアクセス権は、その所定のユーザより広範囲なアクセス権を有している他のユーザ又は実際のコンテンツ作成者によって拡張することもできる。アクセス権の変更は、コンテンツストレージ媒体に保存されたコンテンツアクセス制御データを変更することによって実現できる。コンテンツアクセスデータは、所定のユーザの公開鍵を用いて暗号化された追加的な鍵を提供することによって変更でき、その追加的な鍵は、追加的なコンテンツデータへのアクセスを提供する。これに代えて、電子メールによって、新しいコンテンツアクセス制御データをユーザに送付し、これを記録媒体に記録されている既存のコンテンツアクセスデータに併合し又は付加してもよい。これらに加えて、秘密鍵／公開鍵の対によってデフォルトユーザのレベルが与えられたユーザは、コンテンツの作成者と同等のアクセスレベルを有している。

【０００９】

本発明の更なる側面及び特徴は、添付の請求の範囲において定義されている。

【発明を実施するための最良の形態】

【００１０】

図１は、本発明に基づくデジタルデータコンテンツのためのアクセス制御システムを図式的に示している。このアクセス制御システムは、画像を撮像し、ディスクやビデオテープ等の記録媒体にデジタル画像データを記録するカメラ１１０と、記録された画像データ

を再生する再生装置１２０と、デジタル的に記録された画像データをコピーすることによって、複製及び再生を可能にする記録装置１２４と、アクセス制御メモリ装置（この実施例ではリムーバブルメモリ装置）１３０と、ディスク状記録媒体１４０とを備える。カメラ１１０及び再生装置１２０は、いずれもリムーバブルメモリ装置１３０に接続するためのインタフェースを有する。カメラ１１０は、静止画及び／又は動画を撮影することができる。このアクセス制御システムは、ディスク状記録媒体１４０に記録された暗号化されたコンテンツへの選択的なアクセスを提供し、復号された情報コンテンツの異なる部分へのアクセスを異なるユーザ及び／又はユーザグループに選択的に許可することができる。

【００１１】

情報コンテンツを暗号化／復号するための暗号方式には、対称鍵暗号（symmetric key cryptography）と非対称鍵暗号（asymmetric key cryptography）といった２つの主要な暗号方式がある。対称鍵暗号では、情報を復号するために用いられる鍵は、情報を暗号化するために用いられる鍵と同じ（又は容易に導出可能）である。一方、非対象鍵暗号では、復号に用いられる鍵は、暗号化に用いられる鍵とは異なり、ある鍵から他の鍵を演算によって推定することが不可能である必要がある。非対称鍵暗号では、一対の公開鍵／秘密鍵が生成され、情報の暗号化には、公開鍵（秘密にされる必要はない。）が使用され、情報の復号には、秘密鍵（秘密にする必要がある。）が使用される。使用できる非対称鍵暗号アルゴリズムの具体例としては、ＲＳＡアルゴリズムがある。ＲＳＡアルゴリズムは、一方向性関数に基づいている。公開鍵Ｘは、共に秘密鍵を構成する２つの大きな素数ｐとｑの積である。公開鍵Ｘは、暗号化処理において、一方向性関数に挿入され、これにより、受信者の公開鍵に適合する特定の一方向性関数が得られる。特定の一方向性関数は、メッセージを暗号化するために使用される。受信者は秘密鍵（ｐとｑ）のみに関する知識に基づいて、特定の一方向性関数の逆関数を求めることができる。なお、公開鍵Ｘに関する知識のみからは、ｐとｑを推定することが不可能となるように、公開鍵Ｘは、十分大きくなければならない。

【００１２】

ＲＳＡの代替となる非対称暗号方式としては、楕円曲線暗号（elliptical curve cryptography：以下、ＥＣＣという。）がある。ＲＳＡの場合のように、非常に大きい素数の積として鍵を生成するのではなく、ＥＣＣでは、楕円曲線方程式の性質によって鍵を生成する。ＥＣＣは、鍵をＲＳＡよりも高速に生成でき、したがって、本発明に基づく構成においては、より好ましい非対称暗号技術である。ディスク状記録媒体１４０に記録された情報コンテンツは、１つ以上のコンテンツ暗号化鍵（content encryption key：以下、ＣＥＫという。）を用いて対称的に暗号化され、ＣＥＫは、公開鍵／秘密鍵の対を用いて非対称的に暗号化される。本発明の他の実施例では、情報コンテンツを非対称的に暗号化してもよい。ＣＥＫは、図８を用いて以下に詳細に説明するように、バイナリツリー暗号化方式（binary tree encryption）に基づいて生成され、暗号化された情報コンテンツの異なった部分がＣＥＫの異なるサブセットに対応するように、例えば１０秒毎等、定期的に更新される。これにより、復号された情報コンテンツへの選択的なアクセスが実現する。対称暗号方式は、演算負荷が小さく、したがって非対称暗号方式より高速に実行できるため、ここでは、情報コンテンツの暗号化には対称暗号方式を使用する。

【００１３】

この実施例では、各ユーザ及び／又はユーザグループに対し、複数のユーザのそれぞれと、ＣＥＫのサブセットを暗号化するために用いることができる公開鍵とのリストであるユーザディレクトリを保存する安全なリムーバブルメモリ装置１３０を提供する。他の実施例では、公開鍵及び／又は秘密鍵が保存されるメモリ装置は、リムーバブルではなく、固定メモリ（例えば、カメラ内に設けられる）であってもよい。これにより、ユーザは、ＣＥＫのサブセットに対応する情報コンテンツの一部にアクセスすることができる。また、リムーバブルメモリ装置（removable memory device：以下、ＲＭＤとも呼ぶ。）は、そのＲＭＤを所有するユーザ又はユーザグループに対する秘密鍵も保存する。

【００１４】

記録情報コンテンツへのアクセス許可は、必要に応じて新しいユーザにＲＭＤを発行し、及び既存のユーザから認証を奪う権限が与えられた管理者（administrator）が集中的に管理することができる。それぞれの新しい認可されたユーザに対して、公開鍵／秘密鍵の対を生成する必要があり、そのユーザのための秘密鍵は、そのユーザに対応するＲＭＤに保存される。また、新しいユーザは、そのユーザのＲＭＤに保存されているユーザディレクトリにも追加される。ユーザディレクトリには、バージョン番号を示すタグがあり、新しいユーザが追加され又は削除される毎にバージョン番号を増やすことができる。

【００１５】

ＲＭＤに保存されている情報に対する権限のないコピーを防ぐために、ＲＭＤには、情報を安全に格納する必要がある。秘密鍵に対する権限のないアクセスを防止することは特に重要である。この装置に適切に用いられる安全なメモリ装置の具体例としては、スマートカード、ソニー株式会社（商標）のマジックゲートメモリースティック（Magic Gate Memory Stick、商標）記憶装置、セキュアデジタルカード（Secure Digital Card：ＳＤカード）等があり、この場合、インタフェースは、ＲＭＤが挿入される、ＲＭＤの形状に対応するスロットであることが望ましい。マジックゲートシステムの動作については、図１８～図２０を用いて後に詳細に説明する。

【００１６】

ＲＭＤは、ユーザディレクトリとＲＭＤ所有者データとを含むデータの保存のみに使用してもよい。なお、他の実施例として、ＲＭＤは、暗号化及び／又は復号の処理を実行可能なオンボードデータ処理モジュールを有していてもよい。この場合、データコンテンツの暗号化及び／又はコンテンツアクセス制御データを生成するための暗号化処理の少なくとも一部は、ＲＭＤ上のデータ処理モジュールによって実行することができる。同様に、データコンテンツ又はコンテンツアクセス制御データの復号の少なくとも一部をＲＭＤのデータ処理モジュールによって実行することもできる。更に、リムーバブルメモリ装置と機器との間の接続は、物理接続で行ってもよく無線インタフェースを介して行ってもよい。リムーバブルメモリ装置は、入力データコンテンツを暗号化し、コンテンツアクセス制御データを生成するデータ処理モジュールを備えていてもよい。

【００１７】

ディスク状記録媒体１４０には、対称的に暗号化された情報コンテンツと非対称的に暗号化されたＣＥＫが記録される。この実施例では、ディスク状記録媒体１４０は、コンパクトディスク（ＣＤ）、デジタルバーサタイルディスク（ＤＶＤ）、光ディスク、又はブルーレイ技術を用いた高密度ディスク等のディスク状記録媒体である。なお、これに代えて、テープ状記録媒体等の他の種類の記録媒体を用いてもよい。情報コンテンツの復号された部分へのアクセスは、それらの部分に関連しているＣＥＫを復号する能力に依存するので、異なる権限を有するユーザは、情報コンテンツのそれぞれ異なる復号された部分へのアクセス権を有していることとなる。

【００１８】

カメラ１１０によって情報コンテンツを撮影する場合、カメラ操作者は、ＲＭＤ１３０をカメラＲＭＤインタフェース１１２に挿入する。撮影された画像データの対照的な暗号化に用いるＣＥＫは、その画像データへのアクセス権を与えられた認証されたユーザの個々の公開鍵を用いて、非対称的にエンコードされる。公開鍵は、カメラの撮影者のメモリーカードに登録されたユーザディレクトリから入手される。この実施例では、メモリーカード内に公開鍵自体を保存しているが、これに代えて、公開鍵は、例えばハッシュ値（このハッシュ値を逆にすることによって鍵が復元される）として保存してもよく、又はルックアップテーブルとして保存してもよい。データセットのハッシュは、データから擬似ランダム的に得られる固定長ビット列である。また、秘密鍵も、そのままルックアップテーブル内に又はハッシュ値として保存してもよい。再生時には、認証されたユーザのＲＭＤ１３０は、再生装置１２０のＲＭＤインタフェース１２２に挿入され、ディスク状記録媒体１４０にそのユーザに対応する公開鍵を用いて格納されたユーザの秘密鍵を用いてＣＥＫが復号される。適切なＣＥＫが復号されると、それらのＣＥＫを用いて、対応する情報

コンテンツを復号することができるようになる。記録装置１２４を用いて、再生装置１２０内のディスク状記録媒体１４０をコピーする操作が行われることがある。記録装置１２４と再生装置１２０は、共通のＲＭＤインタフェース１２２を有する。ＲＭＤは、記録媒体上のコンテンツに関するアクセスを制御するが、記録装置（実際には如何なる記録装置でもよい）を用いて、復号された情報コンテンツをコピーすることができる。これは、復号された情報コンテンツが安全な環境で操作されることを仮定している。これにより、アクセス制御システムがビデオ編集者による仕事の流れの障害となることを比較的少なくすることができる。例えば、新たにコピーされたバージョンは、そのバージョンをコピーしたユーザのみがアクセスできるようにしてもよい。これに代えて、新たにコピーされたバージョンには、（このバージョンとともに保存された、暗号化されたＣＥＫの異なるバージョンによって）、アクセス権限を記録してもよく、これにより、元のコピーへアクセス権を有する全てのユーザが、このコピーされた新たなバージョンにもアクセスできるようにしてもよい。

【００１９】

図２は、本発明に基づくカメラ１１０内における録画処理を説明するための図である。この構成のカメラ１１０では、捕捉されたオーディオビジュアル（audio-visual：以下、ＡＶという。）情報は、圧縮エンジン２１０によって圧縮され、圧縮されたＡＶデータは、暗号化エンジン２２０に供給され、暗号化エンジン２２０は、次世代暗号化規格（Advanced Encryption Standard：以下、ＡＥＳという。）アルゴリズムを用いて、圧縮されたＡＶデータを暗号化する。暗号化エンジン２２０は、一般的な圧縮データレート（例えば、ＤＶＣａｍ圧縮のための２５Ｍｂｐｓ又はＩＭＸ圧縮のための５０Ｍｂｐｓ）を容易に取り扱うことができる。また、圧縮データには、可視ウォータマーク法として知られる暗号化の手法も適用でき、この処理は、ＡＥＳ対称暗号化に加えて行ってもよく、ＡＥＳ対称暗号化に代えて行ってもよい。

【００２０】

可視ウォータマーク法とは、可逆的なアルゴリズムを用いて画像マテリアルに目に見える変更を施し、これによって画像マテリアルの品質を低減する処理である。目に見える変更は、画像／ビデオデータの選択された部分に適用され、例えば、コンテンツにおいて「ロゴ」が見えるようにする。変更される画像の部分は、ビットマップ又は変更テンプレートによって定義される。この変更処理は、変換画像の離散コサイン変換（Discrete Cosine Transform：以下、ＤＣＴという。）係数の一部を変更する処理を含んでいてもよい。この可視ウォータマークにより、安全な形式で（すなわち、品質が損なわれていないコンテンツへの直接のアクセスを許可することなく）ユーザにコンテンツをプレビューさせることができる。画像の変更は、暗号的に安全な手法（cryptographically secure manner）で完全に可逆的に行われ、元のコンテンツは、「ウォッシング鍵（washing key）」として知られている復号鍵にアクセスすることにより、ビット毎に復元することができる。可視のウォータマーク付与と、対称／非対称の暗号化の両方を画像に適用することができる。アクセス許可の第１のレベルではユーザに画像の復号を許可するが、ウォータマークの除去（wash）は許可せず、更なる第２のレベルでは、ユーザにウォッシング鍵を提供し、これにより画像から可視ウォータマークを取り除くことを許可する。このウォッシング鍵は、例えば、ユーザによる料金の支払いに応じて提供してもよい。

【００２１】

暗号化エンジン２２０は、バイナリツリー暗号化方式により、ＣＥＫを生成する。対称ＣＥＫは、認証された複数のユーザのそれぞれの公開鍵によって非対称的に暗号化される。公開鍵は、カメラ１１０に現在接続されているＲＭＤ１３０に保存されている公開鍵のユーザディレクトリから得られる。暗号化されたＡＶデータの異なる部分に対応するＣＥＫの異なるサブセットは、認証された各ユーザに対し、それぞれのアクセス許可に応じて、非対称的に暗号化することができる。複数のユーザのそれぞれに対する非対称的に暗号化されたＣＥＫは、対称的に暗号化されたＡＶ情報コンテンツの単一のコピーとともにディスク状記録媒体１４０に記録される。非対称の暗号化は、ＲＭＤ１３０自体の回路（例

えば、スマートカードプロセッサ）で行ってもよく、カメラ１１０自体の暗号化エンジン２２０で行ってもよい。

【００２２】

図３は、本発明に基づく再生装置１２０において行われる再生処理を説明するための図である。圧縮され、対称的に暗号化された情報コンテンツと、非対称的に暗号化されたＣＥＫは、ディスク状記録媒体１４０から読み出され、復号エンジン３１０に供給される。認証されたユーザは、再生装置１２０のＲＭＤインタフェース１２２にＲＭＤ１３０を挿入し、復号エンジン３１０は、ＲＭＤインタフェース１２２に保存されている秘密鍵にアクセスし、ＡＶコンテンツの少なくとも一部を復号する。認証されたユーザがアクセス可能なＡＶコンテンツの一部（例えば、フレーム、ショット又はシーンのあるサブセット）は、ユーザの公開鍵を用いて暗号化され、ディスク状記録媒体１４０に記録されているＣＥＫに依存する。ユーザが再生装置１２０を用いて保護されたコンテンツを復号すると、ユーザは、「保護が解除された（de-protected）」情報コンテンツをディスク状記録媒体１４０に戻すか、或いは新たなディスク記録媒体に記録するかを選択することができる。この実施例では、再生装置１２０は、記録処理も行うことができると仮定している。データパッケージ３２８は、復号された情報コンテンツとともに、ディスク状記録媒体１４０に記録される。データパッケージ３２８は、ソースデータパッケージ内に、ユーザの保有するアクセス権の詳細を示している。復号されたコンテンツをディスク状記録媒体１４０に記録したユーザ、又はこれ以外のユーザが、ディスク状記録媒体１４０に記録されている情報コンテンツにアクセスしようとする場合、そのユーザは、保護が解除され、その保護が解除されたフォーマットで記録されたコンテンツの少なくとも一部にアクセスすることが許可される場合がある。ここで、再生装置１２０が、単に、ユーザが視聴することを選択した（ユーザがアクセス権を有するフレームのサブセットから選択された）フレームを復号するのであれば、その選択されたフレームの組が既に保護が解除され、記録された所定のフレームを含んでいる場合、これらの所定のフレームは、スクランブされている情報コンテンツを残して、再び復号することができてしまう。このような問題は、データパッケージ３２８に、保護が解除されたフォーマットで記録された個々のフレーム又はフレームの範囲の詳細を示す保護解除情報リスト（de-protection information list）を含めることによって回避することができる。保護解除情報リストを用いることにより、認証されたユーザから所定のフレームの視聴が要求された際に、第２の復号は実行されないことを確実にすることができる。保護解除情報リストは、ユーザが保護が解除されたフレームをディスク状記録媒体１４０に記録する毎に更新される。

【００２３】

図４は、ＲＭＤ１３０に保存されている代表的な情報の組を示している。情報は、１つ以上のＸＭＬファイルとして、ＲＭＤ１３０に保存される。ＭＸＬは、マークアップ言語である。広く知られているマークアップ言語であるハイパーテキストマークアップ言語（Hypertext Markup Language：以下、ＨＴＭＬという。）は、ヘッディング及びタイトルによりドキュメント構造を定義し、及び例えばキャプション及びフォントによってその表現を定義することによってウェブページテキスト及び画像をどのように表示するかに関する指示をウェブブラウザに提供する。一方、ＸＭＬは、共通の情報フォーマットを定義する手法並びにこれらのフォーマット及び関連するデータをウェブ及びイントラネット上で共有する手法を提供する。ＨＴＭＬの用途は、テキストと情報とをどのように表示し、インタラクトさせるかを定義することに制限されるが、ＸＭＬでは、アプリケーション開発者は、特定のデータカテゴリに属するように文書内のセクション又は単語をマークするカスタムタグを定義することができ、これにより、ドキュメントのコンテンツに関するコンテキスト情報を与えることができる。例えば、ＲＭＤ１３０上のユーザディレクトリについて、タグ＜ＮＡＭＥ＞及び＜ＰＵＢＬＩＣ　ＫＥＹ＞を定義することができる。カスタムタグを利用して、情報を特定し及び選択的に抽出することによって、データ処理タスクをＸＭＬドキュメント上で実行することができる。

【００２４】

図４に示すように、ＲＭＤ１３０に保存された情報は、パスワードデータ、ＲＭＤ所有者データ４１０、ユーザディレクトリ４２０及び一組のデフォルトユーザデータ４３０を含んでいる。ＲＭＤ所有者データ４１０は、認証されたユーザの氏名、そのユーザが所属する会社名、ユーザが任命されたプロジェクト名及び秘密鍵／公開鍵の対を含む。なお、ここでは、例えば認証されたユーザの氏名と、非対称鍵とを最低限保存する必要があり、会社名やプロジェクト名等の他のデータは任意の項目である。ユーザディレクトリ４２０は、Ｎ人のユーザのそれぞれについて、一組のデータを含んでいる。ユーザに割り当てられたアクセス権に応じて、ユーザディレクトリ内の１つ以上のユーザリストに復号された情報へのアクセスに関する情報を含めてもよい。この場合、ユーザディレクトリ内の各エントリには、認証されたユーザの氏名、会社名及びプロジェクト名とともに、そのユーザの公開鍵の値が含まれる。公開鍵は、そのユーザがアクセスすることを許可された情報コンテンツを復号するために必要であるＣＥＫを暗号化するために用いられる。ユーザディレクトリは、認証されたユーザが追加及び／又は削除される毎に定期的に更新されるので、ユーザディレクトリの比較と更新を容易にするために、ユーザディレクトリバージョンＩＤタグも保存される。この更新は、カメラ１１０及び／又は再生装置１２０に保存されているユーザディレクトリのローカルなコピーと、ＲＭＤ１３０に保存されているユーザディレクトリの外部のコピーとを比較し、ローカルの又は外部のユーザディレクトリが最近更新されているか否かを判定し、一方が更新されている場合、最近更新されていない方のユーザディレクトリのユーザ識別情報、公開鍵、バージョンＩＤタグを更新することによって実行される。

【００２５】

デフォルトユーザデータ４３０の組は、Ｄ人のデフォルトユーザそれぞれの氏名と関連する公開鍵とを含む。特定のＲＭＤ１３０の所有者については、デフォルトユーザは何人いてもよく、又はデフォルトユーザが一人もいなくてもよい。デフォルトユーザは、所定の組の情報コンテンツの全てに対するアクセス権を有している（図１１Ｂを用いて後に説明する）。如何なるユーザをデフォルトユーザとして選択してもよい。デフォルトユーザデータ４３０の組は、ＲＭＤ所有者に固有のデフォルトユーザのリストを含んでおり、例えば、ＲＭＤ所有者のマネージャ又はスーパーバイザをＲＭＤ所有者のデフォルトユーザとしてリストに登録してもよい。管理者は、どのユーザをデフォルトユーザ状態に割り当てるかを決定する権限を有している。情報コンテンツが作成されると、その情報コンテンツに関連する全てのＣＥＫの組は、常にデフォルトのユーザの公開鍵を用いて暗号化され、記録媒体に記録され、これにより、デフォルトユーザによる全てのコンテンツへのアクセスが保証される。復号された情報コンテンツへのアクセスがデフォルトユーザに保証されるので、デフォルトユーザは、ＲＭＤの不注意による紛失に対するセーフガードを提供する。

【００２６】

ＲＭＤ所有者には、パスワードデータが関連付けられ、パスワードデータは、ＣＥＫの符号化における安全性の追加的なレベルとして用いてもよく、例えば、ＣＥＫを非対称的に暗号化する前にパスワードに結合してもよい。この特定の実施例では、ユーザは、それらのＲＭＤ１３０上のパスワードデータに保存されているパスワードに対応するパスワードを用いてシステムにログインしなければならない。図４の実施例では、ユーザディレクトリはＲＭＤ１３０に保存されるが、他の実施例では、カメラ１１０又は再生装置１２０が備える固定メモリ（すなわち、リムーバブルではないメモリ）にユーザディレクトリ全体又は少なくともユーザディレクトリの公開鍵のリストを保存する。ユーザディレクトリの公開鍵がカメラ１１０又は再生装置１２０の固定メモリに保存される場合、ユーザ又はユーザグループの秘密鍵を保存するＲＭＤは、そのＲＭＤと、カメラ１１０又は再生装置１２０に保存されている各公開鍵とを関連付ける識別データを保存できる。更なる他の実施例として、記録／再生装置とＲＭＤの両方にユーザディレクトリのコピーを保存してもよい。

【００２７】

ここでＲＭＤを用いず、秘密鍵が機器内のメモリに保存される実施例について説明する。この実施例では、５個のリモートカメラと、制作設備（production facility）とを用いるとする。この場合、制作設備機器の全てが共通の公開鍵／秘密鍵の対を共有し、共通の秘密鍵は、制作設備機器のそれぞれが備える固定メモリ内に保存されている。５個のカメラのそれぞれは、それぞれの公開鍵／秘密鍵の組（各カメラには、異なる鍵の組が関連付けられている。）を保存する固定アクセス制御メモリ装置を備える。この実施例では、各カメラが「ユーザ」であるとみなされる。撮影されたデータコンテンツは、共通の公開鍵と、データコンテンツを撮影するために用いられているカメラの公開鍵の両方に基づいて暗号化される。これにより、「フィールド」すなわち撮影が行われる場所では、撮影されたデータコンテンツにアクセスすることができるが、制作設備にコンテンツを送信する際には、認証されていないアクセスからコンテンツを保護することができる。制作設備においては、共通の秘密鍵を用いて、データコンテンツにアクセスすることができ、これを編集することができる。

【００２８】

図５は、本発明に基づく第１の暗号化方式を図式的に示している。この方式では、情報コンテンツは、ステージ５１０において、１つ以上のコンテンツ暗号化鍵５２０を用いて対称的に暗号化される。対称的に暗号化された情報コンテンツは、ディスク状記録媒体１４０に記録される。ステージ５３０では、コンテンツ暗号化鍵５２０は、複数のユーザのそれぞれに対応する複数の公開鍵５４０のそれぞれを用いて非対称的に暗号化される。公開鍵５４０は、ＲＭＤ１３０のユーザディレクトリ４２０から読み出される。非対称暗号化ステージ５３０の出力は、一組の暗号化されたコンテンツ暗号化鍵５５０である。各ユーザは、ユーザディレクトリ４２０からのそれぞれの公開鍵５４０に関連付けられているので、各ユーザについて、暗号化されたコンテンツ暗号化鍵５５０のバージョンがそれぞれ１つある。暗号化されたコンテンツ暗号化鍵５５０は、対称的に暗号化された情報とともに、ディスク状記録媒体１４０に記録される。

【００２９】

図６は、図５に示す暗号化方式に対応する第１の復号方式を図式的に示している。復号の最初のステージでは、ディスク状記録媒体１４０から暗号化されたコンテンツ暗号化鍵５５０（図５参照）を読み出す。ＲＭＤ１３０の所有者に関連する秘密鍵６２０は、ＲＭＤ所有者データ４１０から読み出され、ステージ６１０において、使用可能な秘密鍵に対応する公開鍵を用いて暗号化された暗号化されたコンテンツ暗号化鍵５５０のバージョンが非対称的に復号される。非対称復号ステージ６１０の出力は、ＲＭＤ所有者のアクセス許可に適するコンテンツ暗号化／復号鍵６３０の組である。これらのコンテンツ暗号化鍵６３０は、ディスク状記録媒体１４０から読み出された暗号化されたコンテンツの少なくとも一部に対する対称復号のために用いられる。

【００３０】

図７Ａ～図７Ｄは、３人の異なるユーザに対する選択的なアクセス許可の具体例を示している。図７Ａは、ディスク状記録媒体１４０に保存された情報コンテンツを表す８個の画像フレームを表している。８個の画像フレームのそれぞれは、暗号化されて、可視ウォータマークが付されている（ここでは、影付きのフレームで示している）。図７Ｂは、コンテンツ所有者のアクセス許可を示しており、ここでは、全てのフレームが影付きではなく、これは、所有者が、全ての画像フレームの復号されたコンテンツを見ることが許可されていることを示している。図７Ｃは、コンテンツ保有者が個人Ｂに与えた許可を表している。「W」のマークが付されたフレーム（フレーム４、５）は、復号されているがウォータマークは付されたままであるフレームを示し、影付きではないフレーム１、２、３、６は、復号され、ウォータマークも除去されたフレームを示している。図７Ｄは、個人Ｂが個人Ｃに与えた許可のサブセットを示している。個人Ｂは、自らが許可されていないフレーム７、８については、許可を与えることができないことは明らかである。個人Ｃには、フレーム２、３に対するフルアクセスと、復号されているがウォータマークが付されたままであるフレーム４、５に対するアクセスが許可されている。但し、個人Ｂは、個人Ｃ

に対し、フレーム１、６へのアクセスを許可していない。アクセス許可は、ユーザがそのユーザの公開鍵を用いてアクセスすることができるコンテンツ暗号鍵のサブセットによって決定されるため、アクセス許可は、事実上、ディスク状記録媒体１４０に保存されていると言える。また、個人のユーザではなく、カメラマンのチーム又は編集者のグループ等のようなユーザグループに対してアクセス許可を割り当ててもよい。所定のフレームのサブセットへのアクセスは、暗号化技術によって実現することができ、この構成では、階層的バイナリツリー暗号化法（hierarchical binary tree cryptography scheme）を用いる。

【００３１】

図８は、復号された情報コンテンツの一部に選択的にアクセスするための本発明に基づく階層的暗号化法を説明する図である。図８に示すように、暗号化方式は、複数のＬ個の階層レベルを有するバイナリツリーとして表すことができる。この具体例では、４つの階層レベルＬ０、Ｌ１、Ｌ２、Ｌ３を示している。レベルＬ３における８つのノードは、図７Ｄに示す８個のピクチャフレームに対応している。ルートノードであるＬ０を除くレベルＬｊ（ｊ＝１，２，３）の各ノードは、上位の階層レベルＬ（ｊ－１）のノードへの単一のブランチと、下位の階層レベル（Ｌ＋１）の各ノードへの２つのブランチとを有し、各階層レベルは、２ｊ個のノードを含んでいる。

【００３２】

図８に示すバイナリツリーの各ノードには、親へのブランチに基づくラベルが付され、すなわち、左側のブランチには０が、右側のブランチには１が付されている。各ノードは、ルートからそのノードまでを辿るブランチラベルのシーケンスによって定義された２ｊビットのコードによって識別される。カメラ１１０内の暗号化エンジン２２０は、レベルＬ０から暗号化処理を開始する。レベルＬ０では、周知の手法により、鍵及び初期化ベクトルを含む暗号化コードが生成される。２つのＬ１暗号化コードは、Ｌ０暗号化コードに基づいて生成され、それぞれが個々の鍵及び初期化ベクトルを含む。レベルＬ２における暗号化コード００及び暗号化コード０１は、レベルＬ１の親ノード０に基づいて生成される。同様に、レベルＬ２における暗号化コード１０及び暗号化コード１１は、レベルＬ１の親ノード１に基づいて生成される。このように、暗号化コードは、階層的な依存性を有している。

【００３３】

ここで、階層レベルＬ３において、（図７Ｄにおける個人Ｃのみに対する）フレーム２～５のみの選択的なアクセス許可をどのようにして実現するかを説明する。バイナリツリー技術では、暗号コードの全てをディスク状記録媒体に記録するのではなく、許可されたデータの一部の復号を行うために十分な復号データを提供しながら、ユーザに提供すべき復号コードの数を削減できる。この実施例では、フレーム１～８のうち、フレーム２～５のみが復号される。フレーム２を復号し、フレーム１を復号しなくてもよい場合は、ノード００１のコードＫ１が必要である。フレーム３及びフレーム４を復号するためには、ノード０１のコードＫ２が必要である。また、フレーム５を復号し、フレーム６を復号しなくてもよい場合は、ノード１００のコード３が必要である。したがって、フレーム２～５を選択的に復号するためには、３つのノード００１、１００、０１に対応する鍵及び初期化ベクトルが必要となる。包括的に言えば、ビデオシーケンスの特定の部分（フレーム／フィールドのサブセット）の復号に必要なコードの最小の組は、復号すべきビデオシーケンスの部分のみに接続されている（Ｌ０を最高のレベルとして）最低の階層レベルにおけるノードを判定することによって導出される。他のコードは、復号を実行するために必要ではない。このように、コンテンツ暗号化鍵の所定の組は、復号すべき情報シーケンスの各部分に関連付けられる。

【００３４】

図７に示す異なるユーザに対するコンテンツのアクセス許可の階層について、図８に示すバイナリツリー暗号化方式とともに説明する。上述のように、コンテンツへの選択的なアクセスは、ユーザによってアクセスできるコンテンツ暗号鍵の適切なサブセットを作成

することによって実現できる。ユーザがアクセス権を有するフレームに適切なコンテンツ暗号化鍵の所定の組は、暗号化された形式で、データアクセスパッケージ内の記録媒体に保存される。この暗号化は、ユーザの公開鍵を用いて行われる。各ユーザについて保存された、暗号化されたコンテンツ暗号化鍵のサブセットがあり、各ユーザは、そのユーザのコンテンツ暗号化鍵のサブセットを暗号化した各公開鍵を有している。但し、あるユーザに対して、重複する範囲のフレームに対してアクセスが許可される場合、又はユーザが隣り合うフレームの範囲についてアクセス権を有している場合、バイナリ鍵暗号化法から導出されるコンテンツ暗号化鍵間の関係を利用して、データパッケージ内に保存すべきデータの量を削減することができる。例えば、第１の具体例では、アクセス許可が重複しており、詳しくは、ユーザＡがフレーム０～２００へのアクセス権を有し、ユーザＢがフレーム１００～４００へのアクセス権を有し、ユーザＣは、ユーザＡからフレーム１５０～１９０へのアクセス権を与えられ及びユーザＢからフレーム１８０～３００へのアクセス権を与えられているとする。更に、第２の具体例では、許可されたフレームが隣接しており、詳しくは、ユーザＣは、ユーザＡからフレーム１９０～２００へのアクセス権を与えられ及びユーザＢからフレーム２０１～２１０へのアクセス権を与えられているとする。これらの第１及び第２の具体例において、ユーザＣの公開鍵によってそれぞれ暗号化されたコンテンツ暗号化鍵の２つの個々の組（ユーザＡからユーザＣに与えられたアクセス権に関するフレーム範囲に対応し、他方がユーザＢからユーザＣに与えられたアクセス権に関するフレーム範囲に対応する。）を保存するのではなく、２つの個々の鍵の組を結合することによって形成された、単一の暗号化されたコンテンツの暗号化鍵を保存する。結合された鍵の組は、２つの個々の組ではなく、結果的にアクセス可能なフレームの範囲を考慮して、基準ノード（principle node）のみを含んでいる。２組の鍵を結合することが自明である（trivial）場合もあるが、幾つかの場合、２つの兄弟ノード（sibling nodes）をその親ノードに置き換えることが適切な場合もある。この兄弟ノードを置き換える処理は、基準ノードの核となる組（core set of principal nodes）を導出するために、複数回行う必要がある場合もある。図８に示すようなバイナリツリーの構成では、兄弟の鍵を排他的論理和演算することによって親の鍵を導出することができる。２つの鍵の組を併合することにより、データパッケージのサイズを削減でき、更に、再生ステージにおいて、ユーザの秘密鍵を用いて、コンテンツ暗号化鍵を復元（復号）する際に必要とされる演算量を低減できる。

【００３５】

図９は、本発明に基づく第２の暗号化方式を説明する図である。この場合、暗号化処理において、ディスク状記録媒体１４０から読み出されるユニークな又は準ユニークな読出専用ディスク識別子（ＩＤ）を利用する。これにより、認証されていないディスク状記録媒体のコピーに由来するデータの復号を効果的に阻止することができる。ここでは、図５に示す構成と同様、例えば、図８に示すバイナリツリー暗号化方式に基づいて一組のコンテンツ暗号化鍵が生成される。アクセスバンドル９１０として示すコンテンツ暗号化鍵の組は、ステージ９２０において、情報コンテンツの暗号化及び／又は可視ウォータマーク付与に用いられ、暗号化された情報コンテンツは、ディスク状記録媒体１４０に記録される。なお、ここでは、記号Ｅ（暗号化すべきデータ，鍵）は、図９～図１３及び図１５に示す暗号化処理を表し、記号Ｄ（復号しべきデータ，鍵）は、復号処理を表すものとする。ステージ９３０では、アクセスバンドル９１０が、ランダムに生成されるセッション鍵k_aを用いて、対称的に暗号化され、ステージ９３０の出力は、データ１としてディスク状記録媒体１４０に記録される。また、ランダムに生成されたセッション鍵k_aは、結合器９４０にも供給され、結合器９４０は、２を法とする加算（すなわち、ＸＯＲ論理ゲート）によってセッション鍵k_aをディスクＩＤに結合し、セッション鍵及びディスクＩＤの組合せ（session key/ disc ID combination）Ｃを生成する。他の実施例として、２を法とする加算以外の演算によってセッション鍵とディスクＩＤを結合してもよい。ステージ９５０では、ｎ人の予定される受信者の各公開鍵k_{w1}、k_{w2}、k_{w3}・・・k_{wn}を用いて、組合せＣが非対称的にエンコードされる。公開鍵k_{w1}、k_{w2}、k_{w3}・・

・k_{wn}は、ＲＭＤ１３０のユーザディレクトリ４２０から得られる。非対称的に暗号化された組合せＣの複数のバージョンは、データ２として、対称的に暗号化されたコンテンツ暗号化鍵のバンドルと共にディスク状記録媒体１４０に記録される。

【００３６】

図１０は、図９に示す第２の暗号化法によって暗号化された情報を復元するための復号処理を説明する図である。復号処理の第１のステージ１０１０では、ディスク状記録媒体１４０からデータ２が読み出され、再生装置にインストールされているＲＭＤに対応する受信者の秘密鍵を用いて、エンコードされた組合せＣが非対称的に復号される。これにより、組合せＣが復元される。次に、ステージ１０２０において、ディスク状記録媒体１４０から固有のディスクＩＤが読み出され、これを用いて、ディスクＩＤ及びセッション鍵の組合せのときと逆の処理を行い、セッション鍵k_aが得られる。ステージ１０３０において、セッション鍵k_aを用いてＲＭＤ所有者のアクセス許可に適切なコンテンツ暗号化鍵を含むアクセスバンドルが復号される。そして、ステージ１０４０において、アクセスバンドル鍵を用いて、ユーザに対してアクセスが許可された情報コンテンツの部分が復号される。

【００３７】

図１１Ａは、図９に示すディスクＩＤを含む他の暗号化処理を説明する図である。ここでは、図９に示す処理と同様、情報コンテンツは、コンテンツ暗号化鍵のアクセスバンドルを用いて対称的に暗号化され、アクセスバンドルは、ランダムに生成されたセッション鍵k_aを用いて対称的に暗号化され、データ１としてディスク状記録媒体に記録される。但し、この実施例では、セッション鍵k_aをディスクＩＤに結合するのではなく、ディスクＩＤは、ステージ１１１０において、更なるセッション鍵k_dを用いて対称的に暗号化され、「実効ディスクＩＤ（effective disc ID）」として示されるディスクＩＤに基づく暗号化鍵（対称鍵）が生成される。セッション鍵k_aは、ステージ１１２０において、予定される受信者の各公開鍵k_{w1}、k_{w2}、k_{w3}・・・k_{wn}を用いて非対称的に暗号化され、この非対称暗号化の結果は、ステージ１１３０において、実効ディスクＩＤを用いて対称的に暗号化され、データ２としてディスク状記録媒体に記録される。また、更なるセッション鍵k_dは、ステージ１１４０において、予定される受信者の各公開鍵k_{w1}、k_{w2}、k_{w3}・・・k_{wn}を用いて非対称的に暗号化され、この暗号化の結果は、データ３としてディスク状記録媒体に記録される。したがって、この場合、ディスク状記録媒体に記録されたアクセスデータパッケージは、ＣＥＫの対称的に暗号化されたバンドルと、受信者の公開鍵を用いて非対称的に暗号化された後、実行ディスクＩＤを用いて対称的に暗号化されたセッション鍵k_aと、受信者の公開鍵を用いて非対称的に暗号化された第２のセッション鍵k_dとを含む。

【００３８】

図１１Ｂは、ディスク状記録媒体に記録されているコンテンツアクセス制御データの組に含まれるデータアクセスパッケージ１１５０の具体例を示している。ディスク状記録媒体には、２つ以上のデータアクセスパッケージ１１５０を記録することができる。各データアクセスパッケージ１１５０は、データコンテンツの単一の断片（single piece）（例えば与えられたカメラのオペレータによって撮影された一連のビデオ画像）に関連しており、そのデータコンテンツの断片へのアクセスに関する何らかのレベルが与えられた、認証された全てのユーザ又はユーザグループによって要求される全ての情報をリストアップしている。認証された各ユーザ又はユーザグループは、それぞれの秘密鍵によって利用可能なアクセスレベルに基づいて、コンテンツアクセス制御データと共に記録媒体に記録された、暗号化された情報コンテンツの部分にアクセスすることができる。また、データアクセスパッケージ１１５０は、データコンテンツの対応する断片について、バイナリツリー（図８参照）のレベルの数をリストアップしている（すなわち、最小数のレベルを用いて、コンテンツの特定の断片の全体のフレーム範囲がカバーされる）。データアクセスパッケージ１１５０は、保護が解除されたセクション１１５２と、媒体識別子鍵セクション１１５４と、プライマリアクセスセクション１１５６と、第１のアクセスセクション１１

６０と、第２のアクセスセクション１１７０とを含む。データアクセスパッケージ１１５０は、複数のアクセスセクションを含んでいてもよい、各アクセスセクション１１６０、１１７０は、ユーザセクション１１６２と、可視ウォータマーク（visible watermarking：以下、ＶＷＭという。）ウォッシュバンドルセクション１１６４と、復号バンドルセクション１１６６とを含む。

【００３９】

保護が解除されたセクション１１５２は、復号され及び可視ウォータマークが除去された画像フレームの範囲のリストを示す。これにより、復号処理が同じフレームに２回適用されないことが確実にされる。既に復号したフレームを再び復号すると、画像が歪む。媒体識別子鍵セクション１１５４は、データアクセスパッケージ１１５０によって何らかのアクセスが許可される全てのユーザのリストを示す。このリストでは、各ユーザについて、暗号化された媒体識別子セッション鍵k_dがリストアップされている。媒体識別子セッション鍵k_dの値は、特定のデータアクセスパッケージに固有である（一方、コンテンツアクセスセッション鍵k_aは、各アクセスセクション１１６０、１１７０毎に異なっている）。各ユーザは、それぞれ自らの秘密鍵を用いて、k_dを復号することができる。アクセスセクション１１６０、１１７０は、それぞれ情報コンテンツの断片のある一定のセクションへのアクセスを許可する情報を提供する。データアクセスパッケージ１１５０に更なるアクセスセクションを追加することにより、コンテンツの他の部分へのアクセス許可を追加することができる。第１のアクセスセクション１１６０は、情報コンテンツの全体へのアクセスを特定のユーザグループに提供する「プライマリアクセスセクション」である。このデータアクセスパッケージ１１５０は、コンテンツがディスク状記録媒体に記録された際に（通常、コンテンツが作成された際に）記録される。プライマリアクセスセクションは、通常、コンテンツの記録／作成時においては、唯一のアクセスセクションである。プライマリアクセスセクションに示される各ユーザは、「デフォルトユーザ」と呼ばれる。デフォルトユーザには、暗号化されたデータコンテンツを記録した（及び作成した場合もある）個人として、データアクセスパッケージ１１５０が関連する情報コンテンツの断片への同じアクセスレベルが与えられ、すなわち、データパッケージの全体のコンテンツへのアクセス権が与えられる。後に、更なるアクセスセクションをディスク状記録媒体に加えることができ、これにより、データアクセスパッケージ１１５０にリストとして登録された他の認証されたユーザに対して、コンテンツの全て又は一部へのアクセス権を与えることができる。

【００４０】

図１１に示す実施例において、対応するアクセスセクションが媒体識別子に関連付けられているか否かを示すフラグを設けてもよい。コンテンツセッション鍵k_aは、媒体識別子に関連付けるのではなく、そのアクセスセクションにリストとして示されたユーザの公開鍵を用いて単に非対称的に暗号化してもよい。コンテンツセッション鍵k_aの非対称的に暗号化されたバージョンは、記録媒体に記録される。この場合、媒体識別子セッション鍵k_dは、復号に必要でなくなる。この暗号化方式は、図１３に関して以下に説明するように、「マスタユーザ（master user）」に対して適用される。なお、マスタユーザに対しては、コンテンツの全てへのアクセスを提供する。これは、媒体識別子に関連付けられていないアクセスセクションに関連しているユーザグループの場合には不要である。

【００４１】

各アクセスセクションは、ユーザセクション１１６２、ＶＷＭウォッシュバンドルセクション１１６４及び復号バンドルセクション１１６６を含む。ユーザセクション１１６２は、アクセスセクションに関連するコンテンツの断片へのアクセス権を有する各ユーザ又はユーザグループのリストを示す。各ユーザ対して、暗号化されたアクセスセッション鍵k_aが関連付けられている。ユーザは、（アクセスセクションが媒体識別子に関連付けられていない場合）ユーザの秘密鍵のみを用いて、又は（アクセスセクションが媒体識別子に関連付けられている場合）ユーザの秘密鍵と媒体識別子セッション鍵k_dの両方を用いて、アクセスセッション鍵k_aを復号することができる。各アクセスセクションについて

、異なるコンテンツアクセスセッション鍵k_aが用いられる。ＶＷＭウォッシュバンドルセクション１１６４は、１つ以上のサブセクションを有する。各サブセクションは、サブセクションヘッダの特定のフレーム範囲に関連し、それらのフレームから可視ウォータマークを除去するために必要な（バイナリツリー暗号化方式からの）鍵の暗号化されたバージョンを保存する。アクセスセクション１１６０のユーザセクション１１６２のリストに示されるユーザのみがそれらを復号することができるように、ＶＷＭ鍵は、コンテンツアクセスセッション鍵k_aを用いて全て暗号化されている。また、復号バンドルセクション１１６６は、それぞれがサブセクションヘッダに示されたフレーム範囲をカバーする１つ以上のサブセクションを有し、これらのフレームを復号するために必要な（バイナリツリー暗号化方式からの）鍵のリストを含んでいる。この場合、暗号化方式は、可視ウォータマークではなく、対称又は非対称の暗号化である。ここでも、全ての鍵は、コンテンツアクセスセッション鍵k_aを用いて暗号化され、したがって、これらは、アクセスセクション１１６０のユーザセクション１１６２のリストに示されているユーザによってのみ復号される。

【００４２】

図１２は、図１１Ａに示す暗号方式に基づいて暗号化されたデータを復元するための復号処理を示している。まず、ステージ１２１０において、受信者の秘密鍵k_{si}を用いて、（データ３として）ディスクに記録されている非対称的に暗号化されたバージョンから、更なるセッション鍵k_dが復号される。次に、ステージ１２２０において、ステージ１２１０で復元された更なるセッション鍵k_dを用いて、ディスクＩＤから実効ディスクＩＤが再生される。対称鍵である実効ディスクＩＤは、非対称的に暗号化された第１のセッション鍵Ｅ（k_a，k_{wi}）を復元するために、ディスク状記録媒体からの数量データ（quantity Data）２を復号する第１のステージに用いられる。次に、受信者の秘密鍵k_{si}を用いて、次の復号のステージ１２４０が実行され、ここでは、非対称の暗号化の逆の処理を行うことにより、セッション鍵k_aが復元される。次に、ステージ１２５０において、セッション鍵k_aを用いて、アクセスバンドルＣＥＫが復号される。そして、ステージ１２６０において、アクセスバンドルＣＥＫを用いて、ディスク状記録媒体に記録されている、対称的に暗号化された及び／又は可視ウォータマークが付された情報コンテンツが復号される。

【００４３】

図１３は、情報コンテンツの全てに関するアクセスを「マスタユーザ」に許可するための暗号化方式を図式的に説明する図である。マスタユーザとは、媒体識別子にかかわらずデータアクセスパッケージ１１５０（図１１Ｂ参照）が関連付けられているコンテンツ全体へのアクセス権を有するユーザ又はユーザグループと定義される。したがって、媒体識別子セッション鍵k_dは、コンテンツの復号には不要である。また、データアクセスパッケージ１１５０のプライマリアクセスセクション１１６０にリストとして示されたデフォルトユーザは、全体のコンテンツへのアクセス権を有しているが、デフォルトユーザは、媒体識別子に関連付けてもよく、関連付けなくてもよい。データアクセスパッケージ１１５０内のデフォルトユーザのマスタユーザのグループには、何人のユーザ又はユーザグループを追加してもよい。この暗号化方式は、図１１Ａに示す暗号化方式に類似しているが、更なるステージ１３１０が追加されている点が異なり、このステージ１３１０においては、セッション鍵k_aは、マスタ公開鍵k_{w_master}を用いて非対称的に暗号化され、ディスク状記録媒体１４０に保存される。マスタ公開鍵k_{w_master}は、全てのユーザのＲＭＤに保存され、マスタユーザには、記録媒体に記録された情報コンテンツの全体に対するアクセスが許可される。各マスタユーザのそれぞれについて、異なるマスタ公開鍵を設けてもよい。マスタユーザの対応する秘密鍵は、マスタＲＭＤに安全に保存される。マスタＲＭＤを用いることにより、マスタではないＲＭＤが不注意に紛失されても、暗号化されたデータへのアクセス権が失われないようにすることができる。図１４のステージ１４１０に示すように、マスタユーザは、ディスクＩＤにアクセスすることなく、マスタ秘密鍵k_{s_master}を含む単一の復号ステップによって、セッション鍵k

$_a$を復元できる。マスタユーザが、ディスクＩＤにかかわらず、データアクセスパッケージに関連する全体のコンテンツにアクセスするのを可能にするために、プライマリアクセスセクションのＶＷＭウォッシュバンドルセクション１１６４及び復号バンドルセクション１１６６（図１１Ｂ参照）の両方において、暗号化された鍵へのアクセス権をそれぞれのマスタユーザに与えなくてはならない。マスタユーザの公開鍵を用いてプライマリアクセスセクションのコンテンツアクセス鍵k_aを直接暗号化し、データアクセスパッケージ内のどこかにこの暗号化されたk_aを保存することによって、それぞれのマスタユーザにこのようなアクセスを提供することができる。

【００４４】

図１３の実施例では、セッション鍵k_aの暗号化においてマスタユーザのディスクＩＤを用いない。なお、他の構成では、マスタユーザをディスクＩＤに関連付けてもよい。同様に、ある受信者の組をディスクＩＤに関連付け、他の受信者の組に対しては、図１３におけるマスタユーザの場合と同様に、そのユーザの公開鍵でセッション鍵k_aを直接暗号化することによって、より自由なアクセス許可を与えてもよい。

【００４５】

図１５は、図１１及び図１３に対応する暗号化シーケンスのフローチャートである。ステージ１５１０において、ＣＥＫのアクセスバンドルを用いて、情報コンテンツを暗号化し及び／又はウォータマークを付与し、暗号化したコンテンツを記録媒体に保存する。この処理に続くステージには、暗号化コンテンツとともにディスクに記録するためのアクセスデータパッケージの作成が含まれる。ランダムに生成された第１のセッション鍵k_aを用いて、ステージ１５２０では、アクセスバンドルのＣＥＫを対称的に暗号化し、次に、ステージ１５３０において、アクセスデータパッケージの一部として、暗号化されたアクセスバンドルを記録媒体に記録する。ステージ１５４０において、ディスクＩＤを入手し、ステージ１５５０において、第２のセッション鍵k_dを生成し、これを用いて、ディスクＩＤを対称的に暗号化する。この暗号化の結果は後に、「実効ディスクＩＤ」と呼ばれる暗号化鍵として用いられる。暗号化処理は１５６０に進み、ｎ人の各受信者（すなわち、予定される認証ユーザ）ｗ１，ｗ２・・・ｗｎに対して暗号化シーケンスを実行する。詳しくは、ステージ１５７０において、ユーザの公開鍵を用いて第２のセッション鍵k_dを暗号化し、この結果を記録媒体に保存する。ステージ１５８０では、各受信者について、まず、受信者の公開鍵を用いて、第１のセッション鍵k_aを非対称的に暗号化し、次に、実効ディスクＩＤを用いて、非対称の暗号化の出力を対称的に暗号化して記録媒体に保存するといった、２段階の暗号化処理を実行する。図１３に示す暗号化方式の場合、フローチャートには、マスタユーザの公開鍵を用いて第１のセッション鍵k_aを暗号化し、結果をディスクに保存するための更なるステージ１５９０が追加される。

【００４６】

図１６は、図１２及び１４に対応する復号シーケンスのフローチャートである。復号は個々の受信者毎に行われ、各受信者は、そのユーザのＲＭＤ１３０に保存された秘密鍵を用いて、そのユーザがアクセスを許可された情報コンテンツの部分を復号する。復号処理はステージ１６１０において開始され、ここで、ユーザの秘密鍵k_sを用いて、第２のセッション鍵k_dを復号する。次に、ステージ１６２０において、第２のセッション鍵k_dを用いて、（受信者が利用可能であると仮定される）ディスクＩＤを暗号化することによって実効ディスクＩＤを生成する。次に、ステージ１６３０において、実効ディスクＩＤとユーザの秘密鍵の両方を用いて、第１のセッション鍵k_aを復号する。ステージ１６４０においては、第１のセッション鍵k_aを用いて、ＣＥＫのアクセスバンドルを復号するこれにより、ステージ１６５０において、復号及び／又は可視ウォータマークの除去が可能になる。図１４の復号構成の場合、フローチャートには、マスタユーザの秘密鍵を用いて、第１のセッション鍵k_aを復号するステージ１６６０、第１のセッション鍵k_aを用いることでアクセスバンドルを復号するステージ１６７０、復号されたアクセスバンドルを用いて、情報コンテンツを復号する及び／又は可視ウォータマークを除去するステージ１６８０といった更なるステージが追加される。

【００４７】
図１７は、ディスクがコピーされる際に行われるアクセス許可を図式的に説明する図である。コピーに対して付与されるアクセス許可は、用いられている特定の暗号化方式に依存する。ここで、元のディスク１７１０がディスクＩＤ「Ａ」を有しているとする。この元のディスクの直接的なバイナリコピー（すなわち、ビット毎のコピー）が作成された場合、ディスクＩＤを用いた暗号化処理を行ったとすると、ディスクＩＤ「Ｂ」を有する不正コピー１７２０のコンテンツには、如何なるユーザもアクセスすることができない。暗号化処理において、マスタユーザをディスクＩＤに関連付けなかったと仮定すると（すなわち、第１のセッション鍵k_aがマスタ受信者の公開鍵だけを用いて暗号化されたと仮定すると）、この場合、マスタユーザは、コンテンツにアクセスすることができる。

【００４８】
ディスクＩＤ「Ｃ」を有するディスク１７３０は、ディスクＡに保存されたアクセスデータパッケージにおいて、第１のセッション鍵k_aをディスクＩＤに結合し、この結果を受信者の公開鍵を用いて非対称的に暗号化することによって、暗号化とディスクＩＤとが結びつけられている場合における、ディスクＡの正当なコピーを表している。これは、図９に示す暗号化処理に対応している。この場合、ＩＤ「Ｃ」を有するディスク１７３０を用いてユーザによって作成された正当なコピーは、コピーを作成した認証されたユーザだけがアクセス可能な情報コンテンツを含む。但し、この情報コンテンツには、元のディスク１７１０に記録された情報コンテンツに対するアクセス権を有する認証されたユーザは、クセスできない。コピーの作成者は、元のアクセスデータパッケージで指定されている情報コンテンツの部分のみに対するアクセス権を有する。また、この場合も、暗号化処理においてマスタユーザとディスクＩＤとを関連付けていない場合、マスタユーザは、正当なコピー１７３０上の情報コンテンツへのアクセス権のみを有する。

【００４９】
ディスクＩＤ「Ｄ」を有するディスク１７４０は、ディスクＡに保存されたアクセスデータパッケージにおいて、第１のセッション鍵k_aを非対称的に暗号化し、次に、実効ディスクＩＤによって第１のセッション鍵を対照的に暗号化することにより、暗号化とディスクＩＤとが結びつけられている場合におけるディスクＡの正当なコピーを表している。これは、図１１及び図１３に示す暗号化処理に対応している。この暗号化方式は、正当なコピーが認証されたユーザによって作成された場合、元のユーザアクセス許可の組が引き継がれるという点で図９に示す暗号化方式より優れている。したがって、元のディスクＡについて、情報コンテンツへのアクセス権を有する全てのユーザは、正当なコピーであるディスクＤに記録された情報に対して同じアクセスレベルを有する。また、マスタユーザは、マスタユーザがディスクＩＤに関連付けられているか否かにかかわらず正当なコピー１７４０における情報コンテンツへのアクセス権を有している。

【００５０】
更に、データをディスクＥに保存する前に、ディスクＩＤへの依存性を取り除いて、元のディスク１７１０の正当なコピーを作成したとする。この場合、元のディスク１７１０のアクセス許可は、正当なコピー１７５０及びその正当なコピー１７５０の不正なバイナリコピー１７６０の両方に引き継がれる。また、この場合も、マスタユーザは、正当なコピー１７５０及び不正なバイナリコピー１７６０の両方に対してアクセス権を有する。

【００５１】
図１１及び図１３に示す暗号化方式には、元のディスクの正当なコピーが作成された場合、アクセス許可をコピーにも引き継ぎ、元のディスクの不正なバイナリコピーにおいては、情報コンテンツへのアクセスを拒否することができるといった、明らかな利点がある。

【００５２】
図１８は、マジックゲートメモリースティック及びマジックゲートメモリースティック装置を図式的に示している。マジックゲートメモリースティックは、本発明に基づくユーザディレクトリと秘密鍵の安全なストレージに用いることができるＲＭＤの１つの具体例

である。マジックゲートシステムは、マジックゲート装置１８１０とマジックゲートメモリースティック１８６０とを備える。マジックゲート装置は、データ処理を実行する中央演算処理装置（central processing unit：以下、ＣＰＵという。）１８３０と、暗号化回路１８４２を含むマジックゲートモジュール１８４０と、メモリースティック１８６０とマジックゲート装置１８５０との接続を確立するためのインタフェース（ＩＦ）１８５０とを備える。メモリースティック１８６０は、データを保存するためのフラッシュメモリモジュール１８８０と、オフボード暗号化回路１８７２を含むマジックゲート（ＭＧ）モジュール１８７０とを備える。機器の暗号化回路１８４２は、ＭＧセッション鍵$ＳｅＫ_{ＭＧ}$及び$ＭＧコンテンツ鍵ＣＫ_{ＭＧ}$といった２つの関連する暗号鍵を有する。一方、メモリースティックのオフボード暗号化回路１８７０は、$ＭＧセッション鍵ＳｅＫ_{ＭＧ}$と$ＭＧストレージ鍵ＫＳＴ_{ＭＧ}$を使用する。

【００５３】

マジックゲート装置１８１０は、$ＭＧコンテンツ鍵ＣＫ_{ＭＧ}$を用いて情報コンテンツを暗号化／復号する。$ＭＧセッション鍵ＳｅＫ_{ＭＧ}$は、マジックゲート装置１８１０とメモリースティック１８６０の両方によって用いられる。$ＭＧセッション鍵ＳｅＫ_{ＭＧ}$は、各認証レベルにおいて生成され、一時的なデータの交換に利用される。メモリースティックは、$ＭＧストレージ鍵ＫＳＴ_{ＭＧ}$を用いて、$ＭＧコンテンツ鍵ＣＫ_{ＭＧ}$を暗号化／復号する。

【００５４】

マジックゲートシステムは、メモリースティック１８６０とマジックゲート装置１８１０の間で、メモリースティック１８６０及びマジックゲート装置１８１０の双方がコピー保護をサポートし、暗号化／復号が認証されたメモリスティック１８６０を用いてマジックゲート装置１８１０において実行されることを確実にする。マジックゲートシステムは、情報コンテンツのためだけではなく、認証処理においても暗号化／復号（及び関連付けられた鍵）を用いる。メモリースティック１８６０がインタフェースを介してマジックゲート装置１８１０との接続を確立し、この後に記録を行い、コンテンツの再生を可能とする処理のそれぞれにおいて、毎回、最初のステップとして認証を行う必要がある。

【００５５】

図１９は、マジックゲートシステムにおける記録処理を説明するフローチャートである。記録処理はステージ１９１０において開始され、ここで、ＭＧ装置に供給された情報コンテンツは、暗号化回路１８４２において、$ＭＧコンテンツ鍵ＣＫ_{ＭＧ}$を用いて暗号化される。次に、ステージ１９２０において、$ＭＧセッション鍵ＳｅＫ_{ＭＧ}$を用いて$ＭＧコンテンツ鍵ＣＫ_{ＭＧ}$を暗号化し、インタフェース１８５０を介して、メモリースティック１８６０に供給する。$セッション鍵ＳｅＫ_{ＭＧ}$を用いる暗号化により、メモリースティック１８６０とマジックゲート装置１８１０の間で安全なリンクが実現する。ステージ１９３０において、メモリースティック１８６０は、確立された$ＭＧセッション鍵ＳｅＫ_{ＭＧ}$を用いて$ＭＧコンテンツ鍵ＣＫ_{ＭＧ}$を復号し、次に、ステージ１９４０において、メモリスティック１８６０は、$ＭＧストレージ鍵ＫＳＴ_{ＭＧ}$を用いて$ＣＫ_{ＭＧ}$を暗号化した後、暗号化されたコンテンツ鍵をマジックゲート装置１８１０に渡す。そして、ステージ１９５０において、マジックゲート装置１８１０は、メモリースティック１８６０のフラッシュメモリ１８８０に暗号化されたコンテンツと暗号化されたコンテンツ鍵を書き込む。

【００５６】

図２０は、マジックゲートシステムにおける再生処理を説明するである。再生処理は、ステージ２０１０から開始され、ここで、ＭＧマジックゲート装置１８１０は、メモリスティック１８６０から暗号化された情報コンテンツと暗号化されたコンテンツ鍵とを読み出し、データが不正コピーされているものではないことを確認する。次に、ステージ２０２０において、ＭＧデバイス１８６０は、暗号化されたコンテンツ鍵をメモリースティック１８６０に供給する。次に、再生処理は、ステージ２０３０に進み、ここで、メモリースティックは、$ＭＧストレージ鍵ＫＳＴ_{ＭＧ}$を用いてコンテンツ鍵$ＣＫ_{ＭＧ}$を復号する。ステージ２０４０において、メモリースティック１８６０は、$ＭＧセッション鍵ＳｅＫ_{Ｍ}$

$_{G}$を用いてコンテンツ鍵ＣＫ$_{ＭＧ}$を暗号化し、この結果をＭＧマジックゲート装置１８１０に供給する。そして、ステージ２０５０において、ＭＧマジックゲート装置１８１０は、ＭＧセッション鍵ＳｅＫ$_{ＭＧ}$を用いてＭＧコンテンツ鍵ＣＫ$_{ＭＧ}$を復号し、続いてコンテンツを復号する。

【００５７】

図２１は、本発明に基づき、新たに認証されたユーザをどのようにシステムに追加し、及び、認証の期限が切れたユーザをどのようにシステムから削除するかを説明するフローチャートである。処理の最初のステージ２１１０は、管理用のステージであり、ここでは、認証された新たなユーザに対し、その認証されたユーザに固有の公開鍵／秘密鍵の対が保存された個人用のＲＭＤが供給される。また、新たに割り当てられたＲＭＤは、そこに保存されたユーザディレクトリの新たに更新されたバージョンを含んでいる。更新されたユーザディレクトリは、この新たに認証されたユーザの公開鍵を含んでいる。また、この実施例では、認証の期限が切れたユーザは、最も最近に更新されるユーザディレクトリから削除される。次に、ステージ２１２０において、新しいユーザは、新しいユーザは、そのユーザに新たに割り当てられたＲＭＤを互換性がある記録装置に挿入し、ここで、ＲＭＤ及び記録装置が互いに認証を確認する。

【００５８】

次に、ステージ２１３０において、記録装置のメモリにローカルに保存されているユーザディレクトリのコピーと、ＲＭＤに保存されているユーザディレクトリの外部のバージョンとを比較する。各ユーザディレクトリは、バージョン識別タグを有し、これにより、ユーザディレクトリのローカルのバージョンと、外部のバージョンとのどちらかがより最近に更新されているかを判定することができる。この実施例では、簡単なタイムスタンプタグを使用している。このステージでは、認証された新たなユーザがシステムに追加され、期限切れのユーザがシステムから削除されているため、ＲＭＤユーザディレクトリは、ローカルのユーザディレクトリより最近に更新されている。これに応じて、ステージ２１４０では、認証された新たなユーザの公開鍵を加え、期限切れのユーザに関連している公開鍵を除去するように、記録装置のローカルのユーザディレクトリを更新する。更に、ユーザディレクトリを更新するステージにおいて、デフォルトユーザの組４３０を検証し、これらのデフォルトユーザが新たなユーザディレクトリにおいて、有効なデフォルトユーザとしてリストに残っているかを確かめる必要がある。次に、ステージ２１５０において、記録装置において記録処理を実行する。例えば、記録装置がカメラである場合、そのＲＭＤがカメラにインストールされている新たに認証されたユーザによって新しい場面が撮影される。コンテンツ鍵を暗号化するためのユーザの公開鍵の入手には、ユーザディレクトリの外部のバージョンとローカルのバージョンのどちらを用いてもよい。この時点では、更新処理が完了しているので、ユーザディレクトリの２つのバージョンは、現在、同一のものである。ステージ２１５０における記録処理の間に、記録媒体に保存されたアクセスデータパッケージは、新たに認証されたユーザの公開鍵を用いて暗号化を行い、これにより、新たに認証されたユーザは、記録された情報コンテンツの少なくとも一部へのアクセスが許可される。通常、カメラマンは、新たに撮影した情報コンテンツの全体に対するアクセス権を有する。新たなマテリアルが撮影されると、コンテンツアクセス許可の詳細を示す新たなアクセスデータパッケージが記録媒体に記録される。既存のユーザが、新たなユーザに対して、既存の情報コンテンツに関するアクセス許可を与える場合、その既存の情報コンテンツに関連するアクセスデータパッケージにその新たなユーザを加えることができる。これは、新しいユーザの公開鍵を用いて、新たなユーザにアクセス権が与えられる既存のコンテンツに関連するＣＥＫのサブセットを暗号化し、これらの暗号化されたＣＥＫを既存のアクセスデータパッケージに追加することによって実現される。ステージ２１６０において、新たに認証されたユーザは、記録セッションを終了させ、記録装置から自らのＲＭＤを取り出す。

【００５９】

次に、ステージ２１７０では、既存のユーザが、新たな記録操作を開始するために自ら

のＲＭＤを記録装置に挿入する。ステージ２１８０においては、ユーザディレクトリのローカル及び外部のバージョンが比較され、一方のバージョンがより最近に更新されているか否かが判定される。この時点では、ステージ２１４０において、新たに認証されたユーザが追加され、及び期限切れのユーザが削除されているユーザディレクトリのローカルのバージョンが、外部の、すなわち既存のユーザのＲＭＤに記録されているユーザディレクトリより最近に更新されている。ここでも、デフォルトユーザの組４３０の検証が行われる。そして、ステージ２１９０において、既存のユーザのＲＭＤのユーザディレクトリが更新され、新たに認証されたユーザが追加され、期限切れのユーザが削除される。このように、ユーザディレクトリに関する変更は、接続が確立される毎に、ＲＭＤ及び互換機器のユーザディレクトリのバージョンを比較することによって伝播する。上述の実施例では、この比較は、機器にＲＭＤを挿入した際、最初に実行されるが、この比較は、ＲＭＤと機器の間の通信シーケンスの他の段階で行ってもよい。

【００６０】

なお、更新されたユーザディレクトリの伝播には、いくらかの時間がかかる場合がある。ここで、コンテンツの作成時に、新しいユーザがユーザディレクトリに追加されていない場合その新しいユーザに対し、記録ステージ後において、その記録されたデータに対するフルアクセスを許可してもよい。同様に、ユーザディレクトリの更新によって期限切れのユーザのアクセス権を取り消すには、一定の時間がかかるが、期限切れのユーザに対し、認証が取り消された時点で（例えば、退職時に）そのＲＭＤを返却することを要求してもよい。

【００６１】

更新処理におけるユーザディレクトリに対する不正行為を防ぐために、ユーザディレクトリの与えられたバージョンの真正性を確かめることができることは重要である。この目的で、デジタル署名を用いることができる。一実施例においては、デジタル署名は、バージョン識別タグを含むユーザディレクトリの全体のコンテンツに基づいていてもよい。これは、例えば、バージョン識別に用いられる日付タグの変更等、ユーザディレクトリに対する如何なる無許可の改竄はそのユーザディレクトリのデジタル署名によって検証されないので、ユーザディレクトリを平文で保存できることを意味する。

【００６２】

図２２は、デジタル署名に関連するメッセージ署名及び検証手続を図式的に説明する図である。デジタル署名を含むユーザディレクトリの署名は、ステージ２２１０において、ユーザディレクトリの平文バージョンＰから開始される。次に、ステージ２２２０において、平文Ｐのハッシュが生成される。ハッシュは、平文データから一義的に導出される短い固定長ビット列である。次に、ステージ２２３０において、デジタル署名の作成者が自らの秘密鍵を用いて、ハッシュ化された平文を暗号化し、ハッシュ化され、暗号化された平文、すなわち署名Ｑを生成する。そして、ステージ２２４０において、平文自体に、ハッシュ化され、暗号化された平文、すなわち署名Ｑを添付することによって、デジタル署名の処理が終了する。署名検証処理は、ステージ２２５０において開始され、ここでは、例えば、記録装置に平文Ｐと署名Ｑとが供給される。ステージ２２６０では、受信者は、署名の作成者の公開鍵を用いて、署名Ｑを復号し、数値ｈ２（quantity h2）を生成する。ここでは、ユーザディレクトリが完全且つ正しいことのみではなく、ユーザディレクトリのソースが、そのユーザディレクトリの更新を許可されていることを確かめる必要がある。具体的には、ユーザディレクトリに添付されたデジタル署名が、信頼できるパーティから発行されたものであることを確かめる必要がある。このため、ユーザディレクトリを検証する公開鍵（図２２に示す発行者の公開鍵に対応する）を各機器に保存する。ユーザディレクトリは、検証を通過するために、対応する秘密鍵を用いて署名されている必要がある。ステージ２２７０では、平文のハッシュが生成され、出力値ｈ１が出力される。そして、ステージ２２８０では、ｈ１＝ｈ２であることを確認することによって、デジタル署名が検証される。比較されているバージョンより最近のものであると判定されたユーザディレクトリのデジタル署名が検証を通過しなかった場合、図２１のフローチャートに示

す更新のステージ２１４０は実行されない。本発明に基づく手法では、認証されたユーザに対し、ストレージ媒体内の情報コンテンツへのアクセスを選択的に許可することができ、例えば、ユーザには、ビデオシーケンス内のフレームのあるサブセットのみに関するアクセス権を与えることができる。選択的なアクセスは、認証されたユーザにコンテンツ暗号化鍵のサブセットのみの復号を許可し、これにより、復号されたコンテンツ鍵を用いて復号できる画像フレームのみへのアクセスを可能とすることによって実現される。これを実現するバイナリツリー暗号化方式については、図８を用いて上述した通りである。既知の暗号化方式では、情報コンテンツは、全体として暗号化又は復号され、したがって、復号されたデータストリームの処理は、単純である。一方、本発明に基づく選択的なアクセス方式では、再生されたデータストリームは、暗号化されたままのビデオフレーム及び復号された又は部分的に復号された（例えば、可視ウォータマークが付された）フレームの両方を含んでいることが多い。そこで、再生装置は、連続したビデオフレームにおいて、そのビデオフレームが暗号化されたまま（所定のユーザによってはアクセス不可能）であるか、アクセスバンドルの利用可能な鍵を用いて復号されているかを区別できることが望ましい。更に、フレーム境界が暗号化されたデータストリームにおいて、認識可能であるならば、個別の配信のために、暗号化されたデータの個々のサブセットを分離することが可能となる。暗号化されたコンテンツは、特定のデータ形式に従っていることが多い。ここでは、フレーム境界を特定するのに役立つデータの部分をデータの「フォーマット識別部分（format identifying portion）」と呼び、残りのデータを「ペイロードデータ部分（payload data portion）」と呼ぶ。例えば、ＭＰＥＧ－２フォーマットのビデオストリームデータについて検討する。ＭＰＥＧ－２では、ビデオストリームは、ヘッダと、画像要素（画素）を復号して表示するために必要な情報を提供するデータとの階層的構造として組織化される。ビデオデータは、グループオブピクチャ（groups of pictures：ＧＯＰ）を構成する所定の異なる種類のフレーム（Ｉフレーム、Ｐフレーム、Ｂフレーム）を有するフレームを含む。各ヘッダは、３バイトの開始コード接頭辞プレフィックスと、これに続く１バイトの開始コードＩＤからなる４バイトのコードを含む。開始コードプレフィックスは、２３個の（又はこれ以上の）バイナリ値０と、これに続く１つのバイナリ値１を含む。開始コードＩＤは、下記の表１に示すように、後に続くデータの種類を示す。ビデオストリームの様々な箇所において、幾つかの「拡張」を行うことも認められている。拡張は、拡張開始コードと、これに続く、所定の拡張ＩＤの１つによって表される。下記の表２は、所定の拡張ＩＤのリストを示している。

【００６３】

【表１】

開始コードタイプ	開始コードＩＤ（８ビット）
Picture_start_code	00
Slice_start_code	01 to AF
User_data_start_code	B2
Sequence_header_cod	B3
Sequence_error_code	B4
Extension_start_code	B5
Sequence_end_code	B7
Group_start_code	B8
予備	B0, B1, B6

【００６４】

【表２】

Extension_ID（４ビット）	名称
1	シーケンス拡張 Sequence extension
2	シーケンス表示拡張 Sequence display extension
3	Quant Matrix Extension
4	著作権拡張 Copyright Extension
5	シーケンススケーラブル拡張 Sequence Scalable Extension
7	ピクチャ表示拡張 Picture Display Extension
8	ピクチャ符号化拡張 Picture Coding Extension
9	ピクチャ空間スケーラブル拡張 Picture Spatial Scalable Extension
A	ピクチャ時間スケーラブル拡張 Picture Temporal Scalable Extensio
0, 6, B to F	予備

【００６５】

ＭＰＥＧ－２ビデオストリームにおいて、フレーム境界を特定するために、暗号化されたデータストリームにおいて、フレーム境界が識別されるように、データを選択的に暗号化する。図２３は、ビデオストリームの所定の部分に対する選択的な暗号化を説明する図である。データストリームは、「開始コード」２３１０、２３１２、２３１６、２３１８と、これに続く、関連する可変長のヘッダとからなる複数の４バイトのヘッダＩＤを含む。この実施例における４バイトの開始コードは１６進ストリングであるが、これは、１０進ストリング又は８進ストリングであってもよい。ＭＰＥＧでは、開始コードストリング長は、４バイト（すなわち、バイト整列された３２バイト）でなくてはならない。

【００６６】

ヘッダＩＤ内の１バイトの開始コードＩＤは、表１に示すように、ヘッダの種類を特定する。ピクチャペイロードデータ部分２３６０、２３６２は、それぞれスライスヘッダ２３５０、２３５２の直後に続いている。各画像フレームは、複数のスライスを含む。ピクチャヘッダ２３２０とピクチャ拡張２３３０は、フレーム境界に関する情報を提供する。したがって、暗号化するべきビデオストリームの部分にはピクチャヘッダ２３２０とピクチャ拡張２３３０とは含まれないが、残りのヘッダ及びピクチャデータは、暗号化に割り当てられる。暗号化エンジンは、ピクチャヘッダ２３２０に先行するヘッダＩＤ２３１０を検出し、ヘッダＩＤに続く所定数のデータビットを暗号化しない。すなわち、この特定の実施例では、ヘッダに続く所定数のデータビットを識別し、これらの識別されたデータビットに対しては暗号化を行わない。なお、他の実施例では、処理の時点で、例えば、ヘッダを解析してそのヘッダの正確な長さを判定することにより、ヘッダに続くデータビットの数を判定する。同様に、ピクチャ拡張２３３０に先行するヘッダＩＤ２３１２が暗号化エンジンによって検出された場合、暗号化処理では、そのヘッダに続く所定数のバイトを暗号化しない。ピクチャヘッダ２３２０とピクチャ拡張２３３０とは、可変長であり、所定数のビットはスキップされる（暗号化されない）ので、データストリームの暗号化されていない部分は、例えば、ピクチャデータの最初のスライス等、ピクチャデータ内に拡張することが可能である。データの部分を特定するフォーマット（この具体例では、フレーム境界データ）は、暗号化されていないピクチャヘッダ及びピクチャ拡張から導出されるため、ストリームにおける残りのデータ、すなわち、ヘッダ２３４０、スライスヘッダ２３５０、２３５２及びピクチャペイロードデータ部２３６０、２３６２は、暗号化してもよい。フレーム境界データ以外のデータは、ペイロードデータとして分類できる。但し、関連するヘッダＩＤ２３１４、２３１６、２３１８は、いずれも暗号化されない。所定のヘッダＩＤの１つに対応するビットシーケンスが誤って生成されないことを確実にするように行われる。このような誤生成は、フレーム境界の識別に悪影響を与え、すなわち、

デコーダにおいて、誤った境界が認識される虞があるため、避けなくてはならない。ヘッダＩＤシーケンスの生成を回避する暗号化ストリームは英国特許出願番号０１２８８８７．７号（公開番号ＧＢ２３８２７５３号）「全ての暗号化されたデータ値が正当な範囲となることを確実にするビデオデータ暗号化方法（Encrypting video data ensuring that all encrypted data values lie in a legal range）」に開示されている。データストリームの選択的な暗号化により、ＭＰＥＧ－２ビデオデコーダ／プレーヤーは、フレーム境界エラーを生じさせることなく、データストリームの暗号化され及び復号されたサブセクションの両方を再生することができる。

【００６７】

選択的に暗号化されたデータストリームは、入力データのフォーマット識別部分（例えば、フレーム境界データ）と、暗号化されたペイロード部分とを弁別する弁別器（discriminator）を備える復号装置を用いて復号される。復号装置は、弁別器の出力に応じて、入力データを処理し、フォーマット識別部分は復号せず、暗号化されたペイロード部分の少なくとも一部を復号する。

【００６８】

以上、主にデータ暗号化及び可視ウォータマーク法と関連して、本発明に基づくデジタル権利管理システムについて説明したが、本発明は、脆弱ウォータマーク法（fragile watermarking）、ユニークマテリアルＩＤ（Unique Material ID：ＵＭＩＤ）ウォータマーク法及びフィンガプリント法等のこの他の画像処理形式にも同様に適用できる。

【００６９】

上述の手法は、少なくとも部分的に、記録／再生装置内の又はＲＭＤ内のデータプロセッサ上で実行されるコンピュータプログラムによって実現でき、例えば、暗号化及び復号処理は、コンピュータプログラムによって実現してもよい。このソフトウェアは、ＣＤ－ＲＯＭ又はフロッピディスク等のストレージ媒体によって提供してもよい。これに代えて、コンピュータネットワークを介して装置にソフトウェアを供給してもよい（例えば、インターネットからダウンロードしてもよい。

【００７０】

図２４は、記録／再生装置の概略を示している。この記録／再生装置は、記録のための信号を受け取り、この信号を処理し、記録に適するフォーマットにフォーマット化する記録ロジック２５１０と、ロータリヘッド（ヘリカルスキャン方式）構成体等の記録ヘッド構成体２５２０と、磁気テープ媒体等の線形アクセス記録媒体２５３０と、ヘッド構成体２５２０から信号を受け取り、この信号を処理し、出力信号にフォーマット化する再生ロジック２５４０とを備える。

【００７１】

以下、この記録／再生装置を用いて、暗号化されたコンテンツを処理する手法について説明する。

【００７２】

上述したアクセス制御装置では、圧縮されたオーディオ／映像信号は、コンテンツ鍵を用いて暗号化される。暗号化は、ＭＰＥＧデータストリーム内の現在のヘッダ情報が無くならないような手法で行われる。これにより、暗号化されたデータストリームにおいて、データの各フレームを特定できる。この具体例では、この記録／再生装置において、同様の構成を用いているが、もちろん、これに代えて他の構成を用いてもよい。

【００７３】

ここで、上述の構成においては、（例えば）暗号化されたコンテンツ鍵を含む「アクセスパッケージ」がセットアップされる。このアクセスパッケージは、ユーザが記録媒体からの再生時にビデオコンテンツの復号を望む場合に必要となる。

【００７４】

暗号化されたビデオコンテンツとアクセスパッケージは、例えばディスク等のランダムアクセスストレージ媒体に記録するのではなく、図２４に示すような線形アクセス記録媒体２５３０にこれらのアイテムを記録してもよい。以下では、これを実現するための様々

な手法について説明する。

【００７５】

図２５、図２６及び図２７は、それぞれ線形アクセス記録媒体２５３０に記録された一連のビデオフレームを図式的に示している。

【００７６】

図２５に示す実施例では、暗号化されたコンテンツ鍵（及び他の情報）を含むアクセスパッケージは、「ダミー」フレーム２６１０として記録されている。このダミーフレームは、図２５では、影付きの領域として示している。アクセスパッケージは先に記録され、次に、ビデオデータの連続したフレーム２６２０が記録される。少なくとも幾つかのフレーム２６２０は、フレームのシーケンスにおけるアクセスパッケージ２６１０の位置を示すポインタ２６３０を含んでいる。図２５に示す構成では、ポインタ２６３０は相対的位置を、ポインタ２６３０を含むフレームとアクセスパッケージとの間のフレームの数として表現している。この相対的なアドレス指示法には、アドレスをシーケンスが記録されているテープ上の位置から独立して取り扱えるという利点がある。

【００７７】

各フレーム又はビデオデータに、アクセスパッケージを示す関連するポインタを設けてもよく、或いは、これに代えて、フレームの１つ以上のサブセットにこのようなポインタを設けてもよい。もちろん、例えば、フレーム単位の分解能を有するタイムコード（frame-resolution time code）によって、テープが「予め区分されている（pre-striped）」場合、絶対アドレスを用いてもよい。ユニークな又は準ユニークであるＳＭＰＴＥ　ＵＭＩＤ等の物理的な識別子（ウォータマークとして、コンテンツに任意に組み込まれる）を用いて適切な絶対アドレスを提供してもよい。

【００７８】

先に（暗号化されたコンテンツデータより先に）アクセスパッケージを記録する構成は、例えば、カメラ－レコーダ（カムコーダ）等のオーディオ／ビデオデータが事実上リアルタイムに捕捉され、記録される記録構成において特に有益である。カムコーダを用いる場合、記録処理の特定のいずれの時刻においても、記録処理がいつ終了するかは未知である。したがって、シーケンスの始めに記録されたアクセスパッケージを含んでいるダミーのフレームを遡って示すポインタを用いることが好適であり、シーケンスの途中のフレーム又はシーケンスの最後に設けられたダミーフレームを指示する順方向ポインタ（forward pointer）を実現することは、困難であり、これを実現するには、記録処理後に記録されたフレームを変更する必要がある。

【００７９】

一方、編集装置又はマスタリング装置等の他の記録構成では、現在の記録シーケンスの長さを事前に知ることができる場合がある。このような場合、アクセスパッケージは、シーケンスの途中又はシーケンスの最後に設けてもよく、ポインタは、各フレームにおいて、後ろにあるアクセスパッケージを指示することもできる。図２６は、記録されたフレームのシーケンス２７２０の最後に設けられたアクセスパッケージ２７１０を示している。少なくとも幾つか（全てでもよい）の記録フレームに添付されたポインタ２７３０は、順方向にあるアクセスパッケージ２７１０の位置を示している。

【００８０】

図２７は、記録されたフレームのシーケンス２８２０の最初に「メイン」アクセスパッケージ２８１０を記録した更なる構成を図式的に示している。ポインタ２８３０は、逆方向にあるメインアクセスパッケージ２８１０を指示している。シーケンスの最後には、「予備」アクセスパッケージ２８４０を設けている。この予備アクセスパッケージ２８４０を設けることにより、メインアクセスパッケージ２８１０が記録されたテープ位置が破損した場合であっても、記録されたマテリアルにアクセスすることができる。

【００８１】

また、図２７は、各フレームが先行するフレームを指示し、メインアクセスパッケージ２８１０に戻る連鎖的アドレスリンク（address chain of links）２８３０を形成する相

対アドレスの更なる可能性も示している。

【００８２】

図２８は、アクセス記録媒体２５３０に記録されたビデオフレームを図式的に示している。多くのビデオテープ記録フォーマットは、各フレームに、ユーザデータを記録するために、メタデータ「ユーザビット」を含んでいる。ポインタ２６３０、２７３０、２８３０は、これらのユーザビットに設けることが理想的である。そこで、図２８に示す実施例では、ビデオデータとオプションのオーディオデータは、テープ上のフレームのペイロードセクション２９１０に記録され、ポインタは、フレームのユーザビットセクション２９２０に格納されている。

【００８３】

図２９及び図３０は、データアクセスパッケージのフォーマットを図式的に示している。データアクセスパッケージは、１個以上の「ダミー」フレームに保存され、すなわち、ビデオフレームの１つと同じ総合的なデータフォーマットで保存され、暗号化されたコンテンツ鍵は、ビデオフレームのペイロードセクション内に保存される。これにより、ビデオフレームに適用される記録処理と同じ記録処理をアクセスパッケージにも適用できるため、この手法は特に有益である。換言すれば、これにより、ビデオテープ記録／再生装置において必要となる変更を減らすことができる。また、図２７に示す構成において、そのシーケンスに関するアクセスパッケージが「メイン」アクセスパッケージであるか否かを示すフラグをユーザビット３０２０に格納してもよい。

【００８４】

図３１は、ダミーのビデオフレーム３２１０を図式的に示している。

【００８５】

この実施例におけるビデオフレームは、一連の画像領域３２２０として画像の空間周波数成分に関連する圧縮映像データを保存する。この領域は、所謂マクロブロックであってもよく、所謂スライスであってもよく、他の領域であってもよい。このような領域のそれぞれにおいて、圧縮データの最も低い空間周波数（所謂「ＤＣ」）部分に格納される。この実施例では、この領域に暗号化されたコンテンツ鍵及びアクセスパッケージの他の部分を保存する。この手法の有益な点は、ＤＣデータは、従来のビデオ画像の再生をうまく行うために重要な部分であるので、多くのテープフォーマットにおいて、ＤＣデータに対してはより慎重な処理が行われるという点である。より慎重な処理とは、より高度なエラー検出及びエラー訂正処理及び／又は例えば、テープの中央領域等、エラーが生じにくい領域へのＤＣデータの保存を含む。

【００８６】

アクセスパッケージは、単一のフレームのためのＤＣ係数によって提供されるストレージ容量より大きいストレージ容量を必要とする場合がある。したがって、データアクセスパッケージは、複数のダミーフレームに亘って格納してもよい。このような場合、ポインタにより、例えば、アクセスパッケージを表す最初のダミーフレームのアドレスを指示してもよい。

【００８７】

添付の図面を参照して本発明を詳細に説明したが、本発明は上述の実施の形態の詳細に限定されるものではなく、当業者は、添付の請求の範囲に定義された本発明の思想及び範囲から逸脱することなく、上述の実施の形態を様々に変更及び修正することができる。

【図面の簡単な説明】

【００８８】

【図１】本発明に基づくデジタルコンテンツのためのアクセス制御システムの構成を示す図である。

【図２】図１に示すカメラの記録処理を説明する図である。

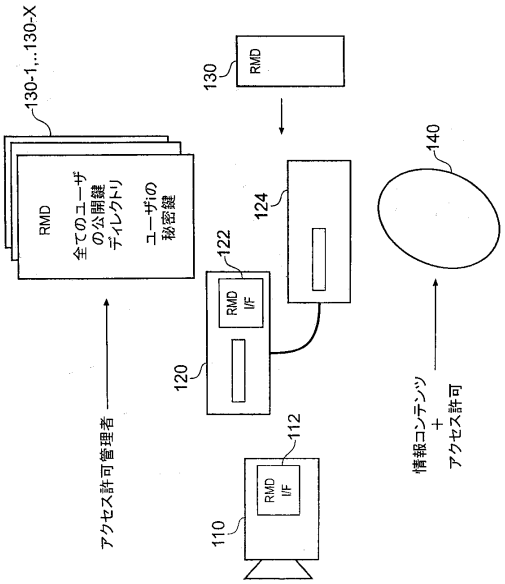
【図３】図１に示す再生装置における再生処理を説明する図である。

【図４】図１に示すリムーバブルメモリ装置に保存される情報の組を示す図である。

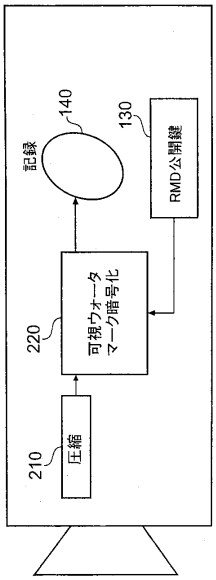
【図５】本発明に基づく第１の暗号化方式を説明する図である。

【図６】図５に示す暗号化方式に対応する復号方式を説明する図である。
【図７】３人の異なるユーザに対する選択的なアクセス許可の一例を説明する図である。
【図８】異なる鍵が異なる情報部分に関連付けられたバイナリツリー暗号方式を説明する図である。
【図９】ディスクＩＤを暗号化処理に用いる暗号化方式を説明する図である。
【図１０】図９に示す暗号化方式に対応する復号方式を説明する図である。
【図１１Ａ】ディスクＩＤを含む代替的な暗号化方式を説明する図である。
【図１１Ｂ】記録媒体に保存されるコンテンツアクセス制御データを示す図である。
【図１２】図１１Ａに示す暗号化方式に対応する復号方式を説明する図である。
【図１３】マスタユーザに対するデータの暗号化を含む暗号化方式を説明する図である。
【図１４】図１３に示す暗号化方式に対応する復号方式を説明する図である。
【図１５】図１１及び図１３の暗号化方式で実行される処理シーケンスのフローチャートである。
【図１６】図１２及び図１４の復号方式で実行される処理シーケンスのフローチャートである。
【図１７】ディスクがコピーされたときに実行されるアクセス許可を説明する図である。
【図１８】マジックゲート（商標）装置とメモリースティックからなるシステムを示す図である。
【図１９】マジックゲート（商標）システムにおける記録処理のフローチャートである。
【図２０】マジックゲート（商標）システムにおける再生処理のフローチャートである。
【図２１】ユーザディレクトリの更新によって、どのようにユーザがシステムに追加され、及びシステムから削除されるかを説明する図である。
【図２２】デジタル署名に関連するメッセージ署名及び検証手続を説明する図である。
【図２３】ビデオストリームの所定の部分の選択的な暗号化を説明する図である。
【図２４】テープ記録／再生装置を示す図である。
【図２５】テープに記録される一連のビデオフレームを示す図である。
【図２６】テープに記録される一連のビデオフレームを示す図である。
【図２７】テープに記録される一連のビデオフレームを示す図である。
【図２８】ビデオフレームを示す図である。
【図２９】データアクセスパッケージのフォーマットを示す図である。
【図３０】データアクセスパッケージのフォーマットを示す図である。
【図３１】ダミービデオフレームを示す図である。

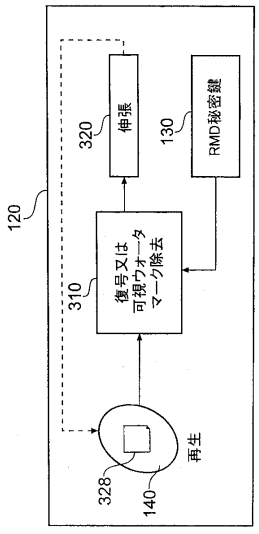
【図１】


130-1,...130-X
RMD
全てのユーザの公開鍵ディレクトリ
ユーザiの秘密鍵
130
RMD
124
122
RMD I/F
120
112
RMD I/F
110
140
アクセス許可管理者
情報コンテンツ
＋
アクセス許可

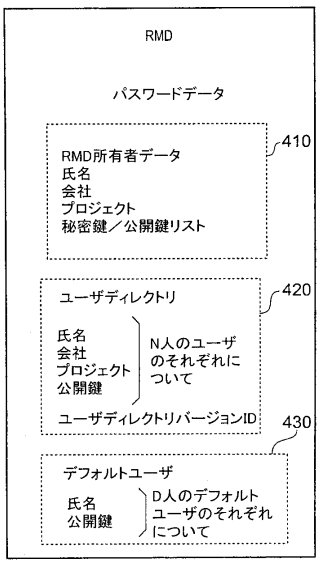
【図２】


記録
140
130
RMD公開鍵
220
可視ウォータマーク暗号化
210
圧縮

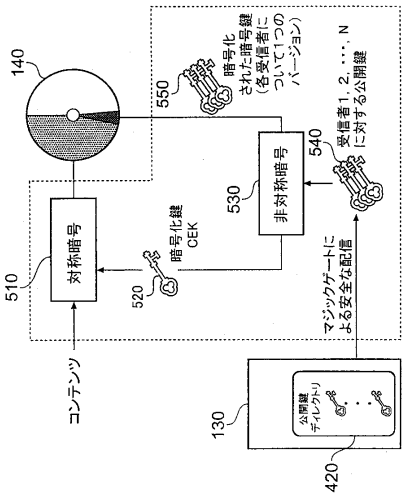
【図３】


120
320
伸張
130
RMD秘密鍵
310
復号又は可視ウォータマーク除去
再生
328
140

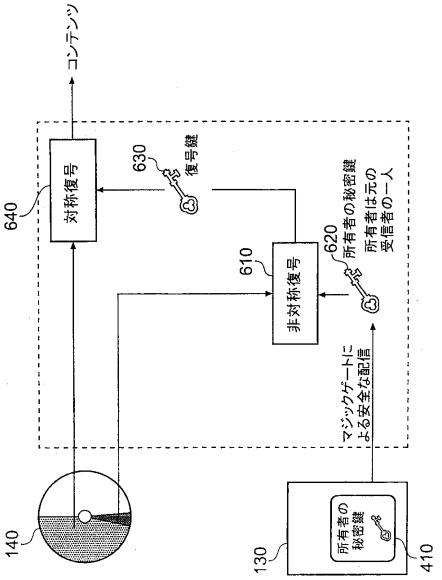
【図４】


RMD
パスワードデータ
RMD所有者データ
氏名
会社
プロジェクト
秘密鍵／公開鍵リスト
410
ユーザディレクトリ
氏名
会社
プロジェクト
公開鍵
N人のユーザのそれぞれについて
ユーザディレクトリバージョンID
420
430
デフォルトユーザ
氏名
公開鍵
D人のデフォルトユーザのそれぞれについて

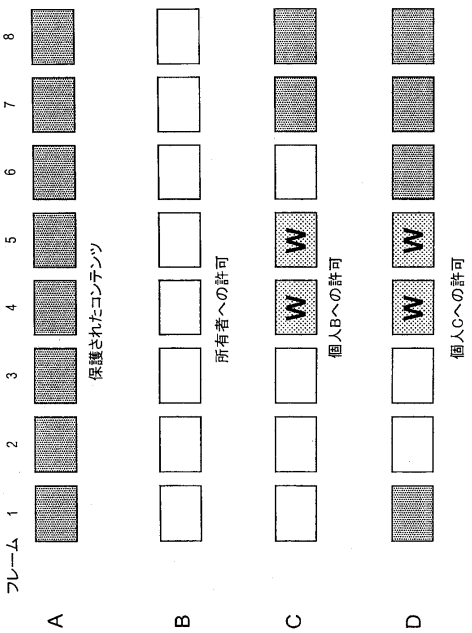
【図５】


140
550
暗号化された暗号鍵（各受信者についてｌつのバージョン）
530
非対称暗号
540
受信者1，2，…，Nに対する公開鍵
510
対称暗号
520
暗号化鍵CEK
マジックゲートによる安全な配信
コンテンツ
130
公開鍵ディレクトリ
420

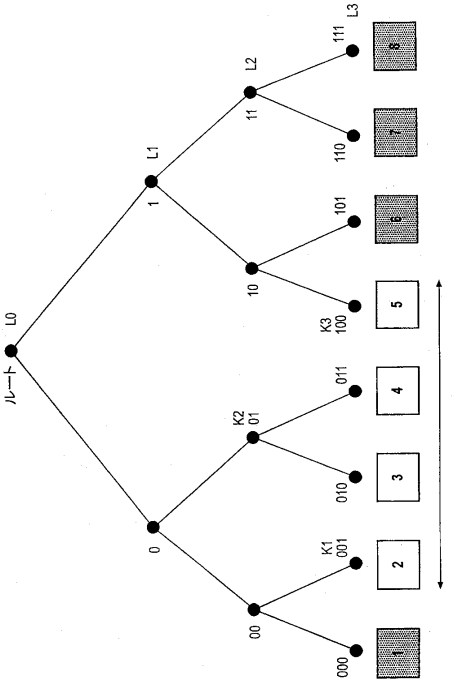
【図６】


コンテンツ
640
対称復号
630
復号鍵
610
非対称復号
620
所有者の秘密鍵
所有者は元の受信者の一人
マジックゲートによる安全な配信
140
130
所有者の秘密鍵
410

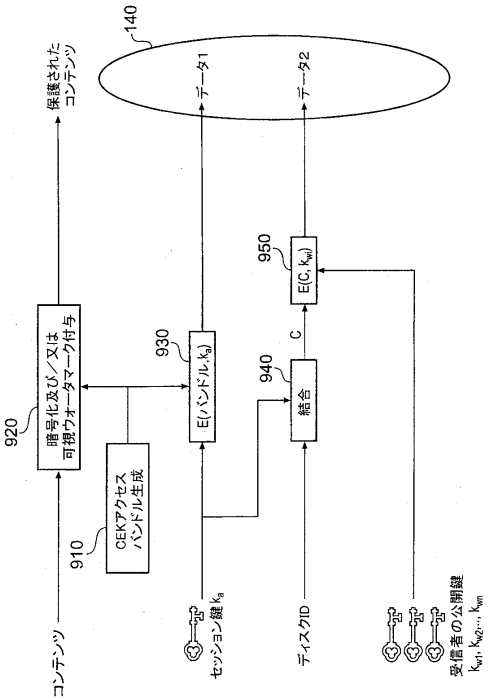
【図７】


フレーム 1 2 3 4 5 6 7 8
保護されたコンテンツ
A
所有者への許可
B
個人Bへの許可
C
個人Cへの許可
D
W

【図８】


ルート L0
L1
L2
L3
K1 001
K2 01
K3 100
000
001
010
011
100
101
110
111
1
2
3
4
5
6
7
8

【図９】



【図１０】

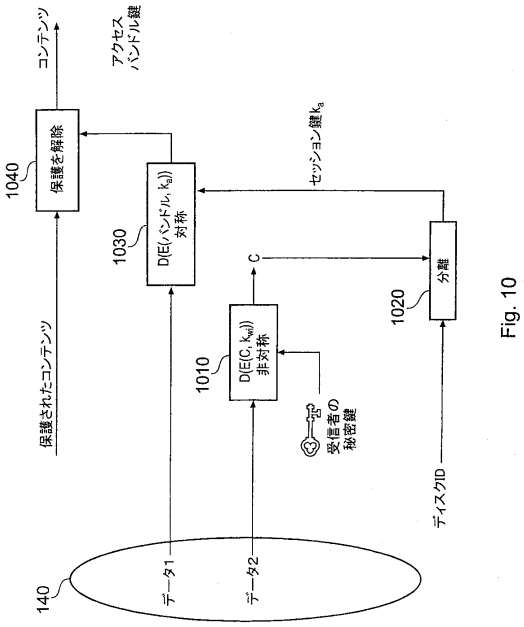
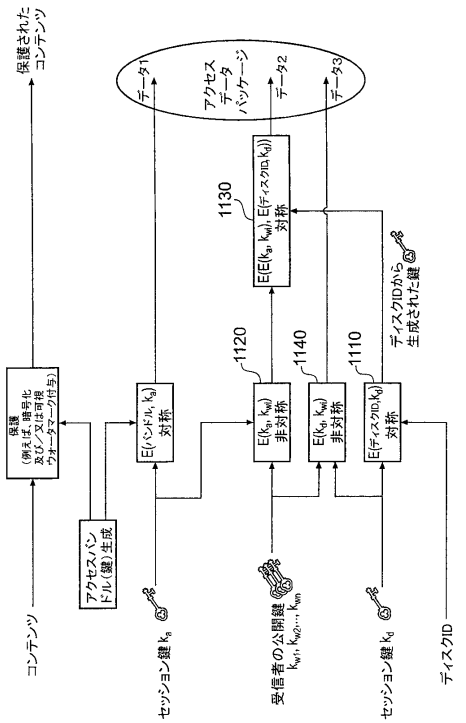
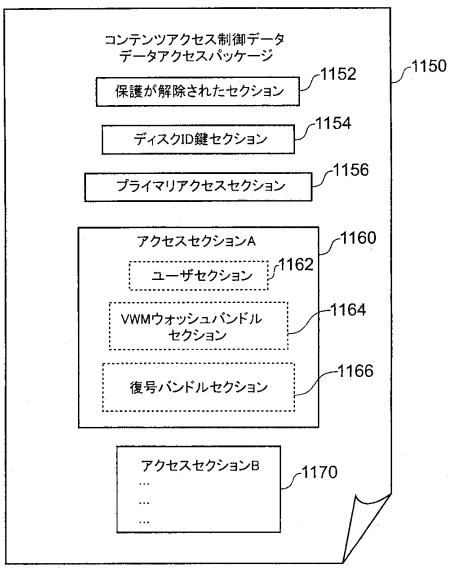


Fig. 10

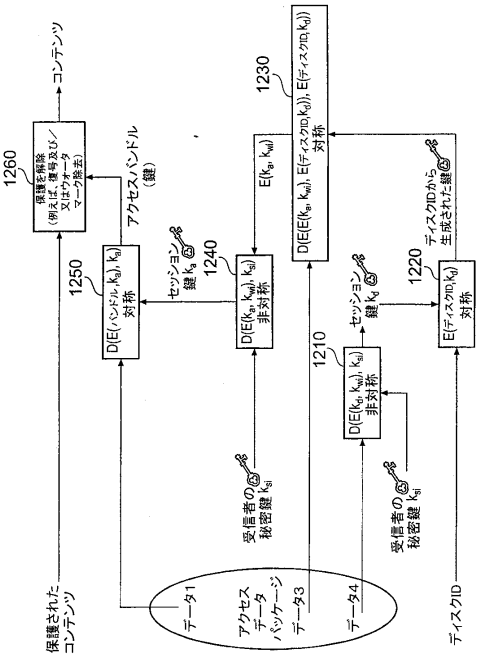
【図１１Ａ】



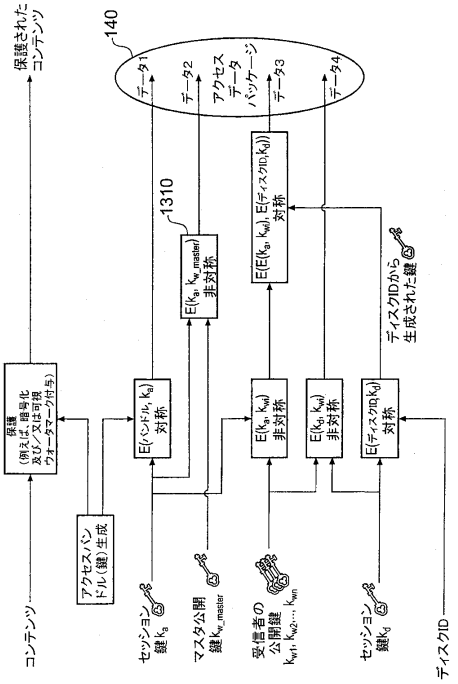
【図１１Ｂ】



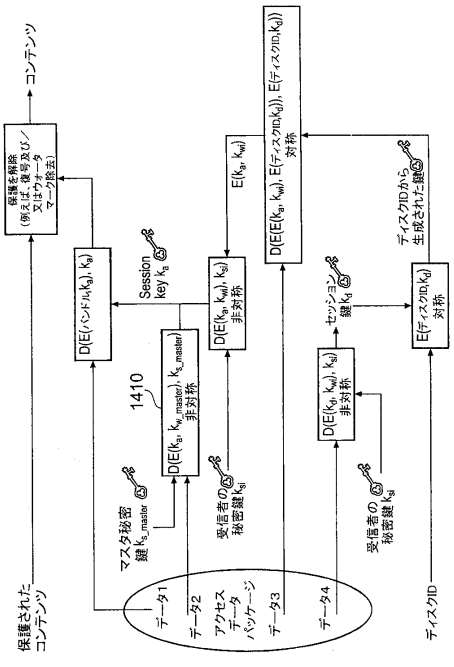
【図１２】



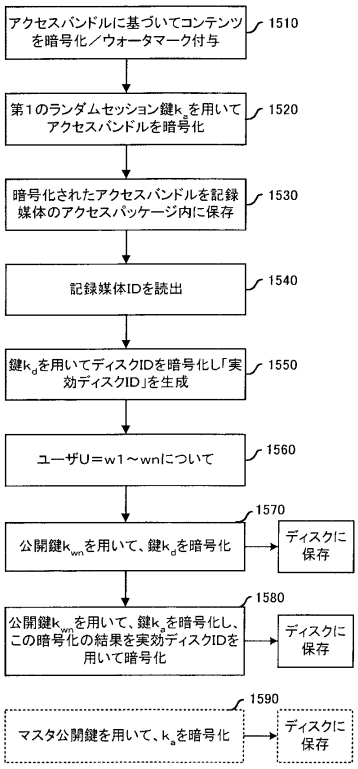
【図１３】



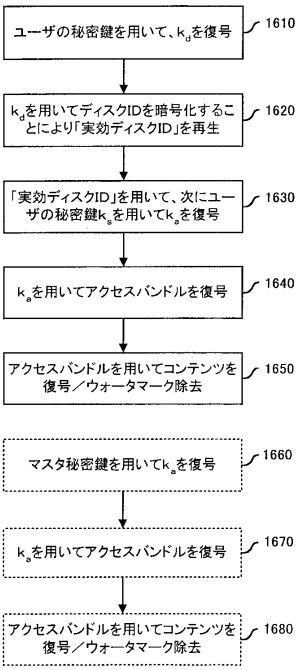
【図１４】



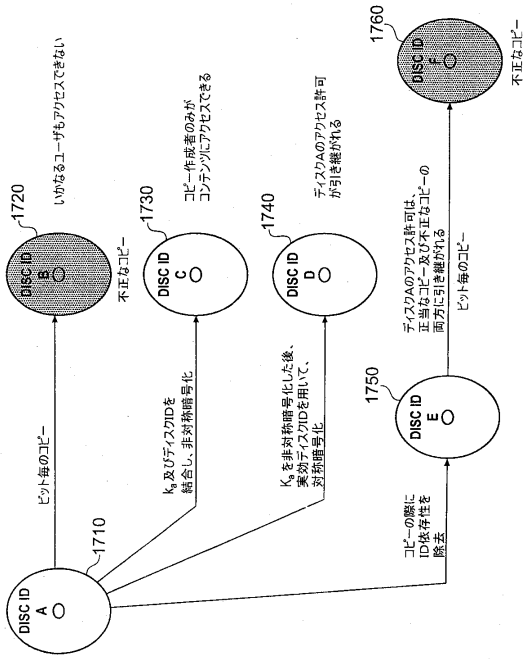
【図１５】



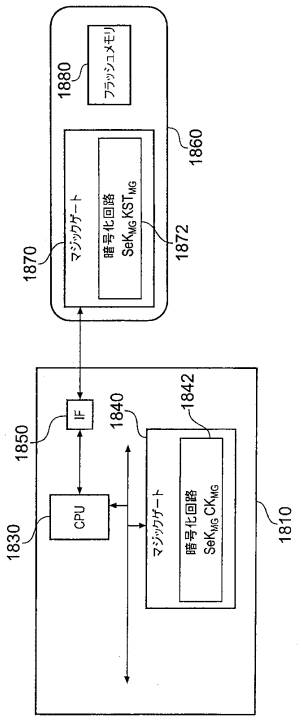
【図１６】



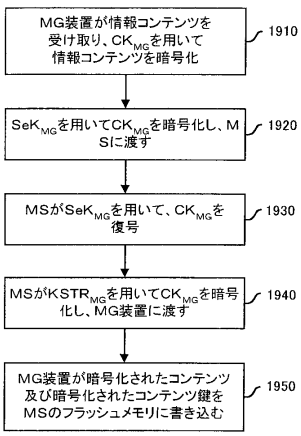
【図１７】



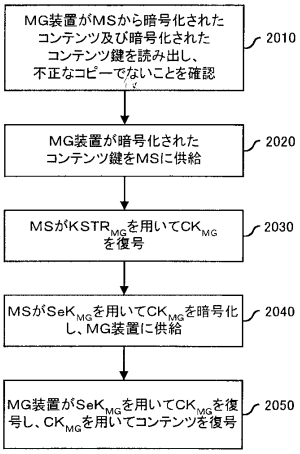
【図１８】



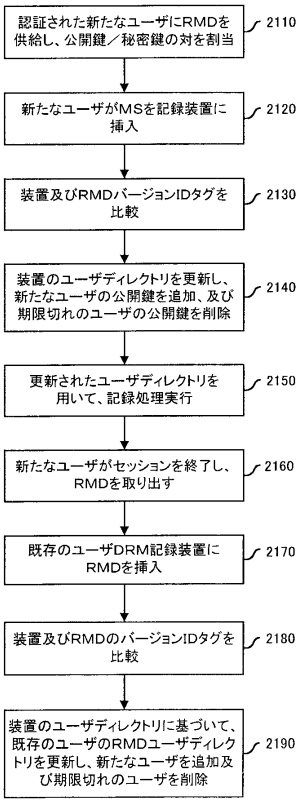
【図１９】



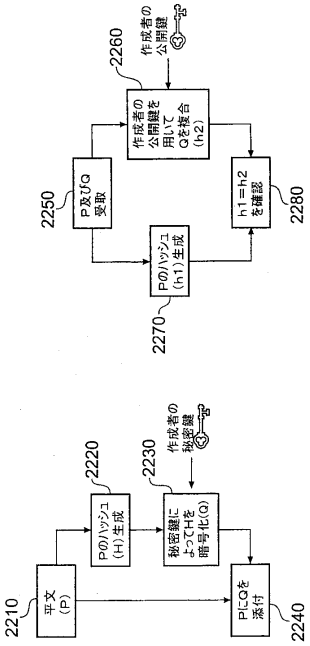
【図２０】



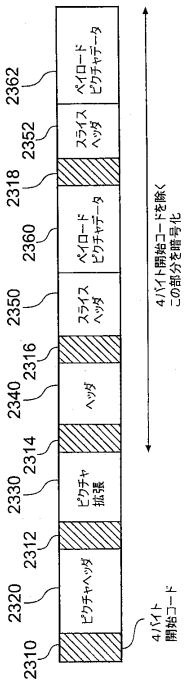
【図２１】



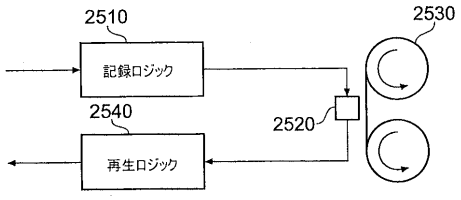
【図２２】



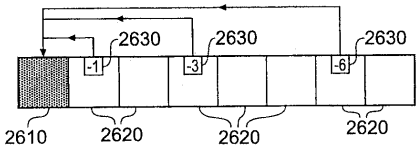
【図２３】



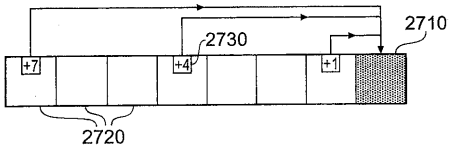
【図２４】



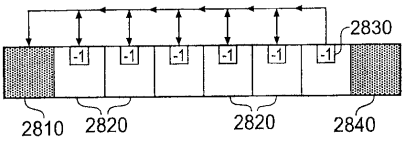
【図２５】



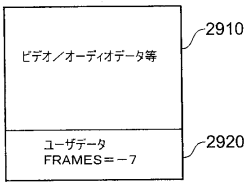
【図２６】



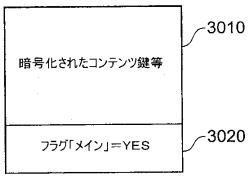
【図２７】



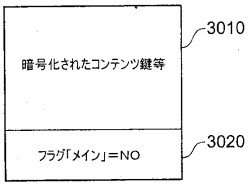
【図２８】



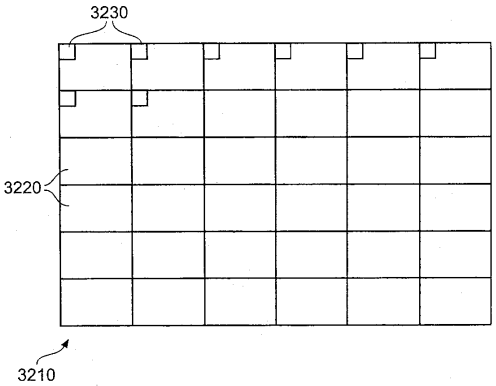
【図２９】



【図３０】



【図３１】



フロントページの続き

(51)Int.Cl. FI
G06F 12/14 540P
G09C 1/00 660D

(72)発明者 テイラー、 アンドリュー ロバート
イギリス国 KT13 OXW、 ウエィブリッジ、 ブルックランズ、 ザ ハイツ （番地無し） ソニー ユナイテッド キングダム リミテッド内
(72)発明者 タプソン、 ダニエル ワレン
イギリス国 KT13 OXW、 ウエィブリッジ、 ブルックランズ、 ザ ハイツ （番地無し） ソニー ユナイテッド キングダム リミテッド内
(72)発明者 フーパー、 ダニエル ルーク
イギリス国 KT13 OXW、 ウエィブリッジ、 ブルックランズ、 ザ ハイツ （番地無し） ソニー ユナイテッド キングダム リミテッド内
(72)発明者 エマニマル、 アルベスーモーリア
イギリス国 KT13 OXW、 ウエィブリッジ、 ブルックランズ、 ザ ハイツ （番地無し） ソニー ユナイテッド キングダム リミテッド内

審査官 青木 重徳

(56)参考文献 特開２００３－１５８５１４（ＪＰ，Ａ）
特開２００３－１０１５２６（ＪＰ，Ａ）
特開２００２－００９７６３（ＪＰ，Ａ）
特開２０００－０２２６８０（ＪＰ，Ａ）
国際公開第２００３／０２８２８１（WO，Ａ１）
芳尾太郎，“ディジタル著作権：小型メモリ・カードで音楽著作権を守る”，日経エレクトロニクス，日本，日経ＢＰ社，１９９９年 3月２２日，第７３９号，ｐ．４９－５３
“デジタルコンテンツのキーテクノロジー メモリースティック著作権保護技術 MagicGate”，ＣＸ－ＰＡＬ，日本，[online]，２０００年 4月，４４号，[検索日：平成２２年8月２７日]，インターネット，ＵＲＬ，http://www.sony.co.jp/Products/SC-HP/cx_pal/vol44/index.html

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