(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4621314号
(P4621314)
(45)発行日　平成23年1月26日(2011.1.26)　(24)登録日　平成22年11月5日(2010.11.5)

(51)Int.Cl.　F I
*G06F 21/24 (2006.01)*　G06F 12/14　５３０Ｐ

請求項の数 3　(全 11 頁)

(21)出願番号　特願平11-169980
(22)出願日　平成11年6月16日(1999.6.16)
(65)公開番号　特開2000-357126(P2000-357126A)
(43)公開日　平成12年12月26日(2000.12.26)
審査請求日　平成16年10月19日(2004.10.19)
審判番号　不服2008-24070(P2008-24070/J1)
審判請求日　平成20年9月18日(2008.9.18)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100084618
弁理士　村松　貞男
(72)発明者　上林　達
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
最終頁に続く

(54)【発明の名称】記憶媒体

(57)【特許請求の範囲】
【請求項１】
デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、
コントローラと、
読み出し専用であり、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された公開ＲＯＭ領域と、
デジタルコンテンツがコンテンツ鍵を用いて暗号化された暗号化コンテンツと、前記コンテンツ鍵が前記電子機器との間でデジタルコンテンツの交換に用いる前記記憶媒体に固有の予め記憶されたメディア鍵を用いて暗号化された暗号化コンテンツ鍵との記録に用いられる書き換え可能な公開Ｒ／Ｗ領域とを具備し、
前記コントローラは、前記記憶媒体が任意の電子機器に装着されて使用される場合に、前記公開ＲＯＭ領域に登録された前記リボケーション情報と当該電子機器から受け取った情報とに従って当該電子機器による前記記憶媒体の利用を無効化すべきか否かを判定し、無効化すべきでないと判定した場合、前記記憶媒体に固有の前記メディア鍵を当該電子機器に送信する
ことを特徴とする記憶媒体。
【請求項２】
前記コントローラは、前記電子機器による前記記憶媒体の利用を無効化すべきと判定した場合に、以降の処理を停止する

ことを特徴とする請求項１記載の記憶媒体。
【請求項３】
前記コントローラが電子機器から受け取った情報は暗号化された情報であり、
前記コントローラは、前記電子機器との間で認証処理を行うことにより前記暗号化された情報を受け取り、当該暗号化された情報を前記認証処理に基づいて復号化することにより当該電子機器の識別情報を取得し、当該取得された識別情報に一致する情報が前記公開ＲＯＭ領域に登録された前記リボケーション情報に含まれているならば、当該電子機器による前記記憶媒体の利用を無効化する
ことを特徴とする請求項１記載の記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、画像データや音楽データに代表される種々のデジタルコンテンツを記録再生するのに用いられる記憶媒体に係り、特に不当な電子機器によるコンテンツの記録再生を抑止するのに好適な記憶媒体及び同媒体を使用したコンテンツ保護方法に関する。
【０００２】
【従来の技術】
近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メディアに格納された画像データや音楽データなど様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。
【０００３】
これらのデジタルコンテンツは、例えばＭＰＥＧ２、ＭＰ３といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。
【０００４】
【発明が解決しようとする課題】
しかし、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器で用いられる記憶媒体は、別の機器に移動しても記録／再生できるリムーバブルなものが多く、その仕様は基本的にはオープンである。このためコンテンツの移動／コピーを自由に行うことができるので、記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護することは実際上困難である。
【０００５】
そこで、メモリカードのように記憶メディア部とコントローラとが一体化された記憶媒体については、秘匿された特定手続にてのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことにより、コンテンツの保護を図ることが考えられる。
【０００６】
この場合、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際には、それぞれが、著作権保護（コンテンツ保護）に関する所定の仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互に認証し、正しいと認証できた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを暗号化するキー）の暗号化（ライセンス暗号化）／復号化またはコンテンツの暗号化／復号化に用いることも考えられる。
【０００７】
ところが、上記相互認証に必要な情報は、機器の出荷段階で予め設定されていることから

、機器の購入後に当該機器（上で動作するプログラム）が改変されるといった攻撃により、例えばコンテンツ保護の仕組みが無用なものになった場合等においては、上記相互認証だけでは、この種の、問題のある機器を検出できないことになる。

【０００８】

本発明は上記事情を考慮してなされたものでその目的は、特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された構成とすることで、当該リボケーション情報で表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることが可能な記憶媒体及び同媒体を使用したコンテンツ保護方法を提供することにある。

【０００９】

【課題を解決するための手段】

本発明の記憶媒体は、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能であって、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された特定記憶領域を備えることで、自身が任意の電子機器に装着されて使用される場合に、当該電子機器の無効化を上記リボケーション情報に従って制御可能としたことを特徴とする。

【００１０】

このように本発明の記憶媒体においては、その特定記憶領域にリボケーション情報が予め登録された構成とすることで、当該リボケーション情報で表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることが可能となる。

【００１１】

ここで、記憶媒体を、メモリカードのように、記憶メディア部とコントローラとが一体化された構成とし、当該記憶媒体が任意の電子機器に装着されて使用される場合に、上記コントローラが当該電子機器から当該電子機器を表す情報を受け取って、その情報によりリボケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御するならば、記憶媒体側で不当な電子機器によるコンテンツの記録または再生を抑止することが可能となる。

【００１２】

また、上記特定記憶領域を、読み出し専用の不揮発性メモリ上に確保するか、或いは秘匿された特定手続以外ではアクセスできない書き換え可能な不揮発性メモリ上に確保するならば、リボケーション情報の改ざんにも対処可能となる。

【００１３】

なお本発明は、上記構成の記憶媒体を使用したコンテンツ保護方法としても成立する。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態につき図面を参照して説明する。

【００１５】

図１は本発明の一実施形態に係るコンテンツ利用管理システム１の構成例を示す。なお、ここでは、コンテンツ（デジタルコンテンツ）として音楽データを一例として用いているが、この場合に限らす、映画や、ゲームソフト等のデータであってもよい。

【００１６】

ＥＭＤ（Electronic Music Distributor）は、音楽配信サーバまたは音楽配信放送局である。

【００１７】

コンテンツ利用管理システム（以下、ＬＣＭ（Licence (SDMI-)Compliant Module）と称する）１は、例えば、パーソナルコンピュータ（ＰＣ）を用いて実現される。このＬＣＭ１におけるコンテンツ保護の方法は、コンテンツを記録すべき記憶メディア（記憶媒体）１３毎に、その記憶メディアの識別情報（メディアＩＤ）を用いてコンテンツの暗号化／復号化を管理することを前提としている。

【００１８】
ＬＣＭ１は、複数のＥＭＤ（ここでは、ＥＭＤ＃１～＃３）に対応した受信部＃１～＃３を有しており、当該受信部＃１～＃３を通してＥＭＤが配信する暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツ復号キー）などを受信する。受信部＃１～＃３は、再生機能や課金機能を有していても良い。また、課金機能を利用して、気に入ったコンテンツを購入することが可能である。
【００１９】
ＬＣＭ１は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Server：ＳＭＳであり、以下ＳＭＳと称する）２を有する。このＳＭＳ２は、利用者が購入した暗号化コンテンツをＥＭＤＩ／Ｆ（インタフェース）部３を経由して受け取る。暗号化コンテンツ（ここでは音楽コンテンツ）は、必要に応じてＥＭＤＩ／Ｆ部３で復号され、形式変換や再暗号化が施される。ＳＭＳ２は暗号化コンテンツを受け取ると、それを音楽データ格納部１０に格納し、音楽データ復号鍵（コンテンツ復号キー）をライセンス格納部９に格納する。ここでＳＭＳ２は、配信された音楽コンテンツを利用者が試聴するために再生機能を有していても良く、この場合、ＳＭＳ２が管理する音楽コンテンツをＰＣ上で再生することができる。
【００２０】
ＳＭＳ２はまた、メディアＩ／Ｆ部６に装着可能なメモリカード等の記憶メディア（以下、ＰＭ（Portable Memory）と称する）１３に対してコンテンツデータ（デジタルコンテンツ）を当該Ｉ／Ｆ部６経由で出力する機能を有している。このＰＭ１３は、図２に示す構成の専用の記録再生装置（以下、簡単にＰＤ（Portable Device）と称する）１２にセットして用いることで、当該ＰＭ１３に記録されたコンテンツをＰＤ１２上で再生することができる。
【００２１】
ＳＭＳ２からＰＭ１３へのコンテンツの記録は、メディアＩ／Ｆ部６を通じて直接行われるか、またはＰＤ１２を経由して行うことができる。
【００２２】
ここで、ＬＣＭ１によるチェックイン／チェックアウト機能について簡単に説明する。チェックアウトとは、ＬＭＳ１が「親」としてのコンテンツを格納しており、ＰＭ１３に、その複製を「子」コンテンツとしてコピーすることをいう。「子」コンテンツは基本的にはＰＤ１２で自由に再生することが可能であるが、「子」から「孫」コンテンツを作成することは許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、ＰＭ１３をＬＣＭ１のメディアＩ／Ｆ部６に装着し、ＬＣＭ１が「子」コンテンツを消去（または利用不能）することで、ＬＣＭ１内の「親」コンテンツは「子」を１つ作る権利を回復することをいう。これを「親」にチェックインするともいう。
【００２３】
ＰＭ１３は、図３に示すように、コントローラ１３０と、公開領域１３１及び秘匿領域１３４からなる記憶メディア部とから構成される。秘匿領域１３４は、コントローラ１３０を通して非公開の手順（つまり秘匿された特定手続）でしかアクセスできない記憶領域であり、コンテンツ復号に必要な情報を記憶するのに用いられる。秘匿領域１３４は、対応するＰＭ１３に固有のメディア識別情報（以下、メディアキーと称する）$K_M$等の定数が記憶される秘匿ＲＯＭ領域と、ライセンスする側から提供される（メディアマークと呼ばれる）秘密データであるライセンス復号キー等の変数が記憶される秘匿Ｒ／Ｗ（リード／ライト）領域からなる。メディアキー$K_M$は、各ＰＭ１３に固有であればよく、シリアル番号や製造番号（ＰＭ１３個々の製造番号、または製造ロット番号）、他の様々な識別情報を用いることができる。なお、メディアキー$K_M$を、各ＰＭ１３に固有な識別情報とライセンス復号キーから生成するようにしても構わない。秘匿ＲＯＭ領域は例えばＲＯＭ（読み出し専用の不揮発性メモリ）上に確保され、秘匿Ｒ／Ｗ領域は例えばフラッシュメモリ（書き換え可能な不揮発性メモリ）の特定領域に確保される。

【００２４】
公開領域１３１は、秘匿領域以外の、通常の手順にてアクセス可能な領域であり、読み出し専用の公開領域（以下、公開ＲＯＭ領域と称する）１３２と、書き換え可能な公開領域（以下、公開Ｒ／Ｗ領域と称する）１３３からなる。公開ＲＯＭ領域は例えばＲＯＭ上に確保され、公開Ｒ／Ｗ領域は例えばフラッシュメモリ上に確保される。この公開ＲＯＭ領域、公開Ｒ／Ｗ領域は、先の秘匿ＲＯＭ領域が確保されるＲＯＭ、秘匿Ｒ／Ｗ領域が確保されるフラッシュメモリ上に、それぞれ確保されるようにしても構わない。
【００２５】
公開ＲＯＭ領域１３２には、本発明に直接関係するリボケーション情報が対応するＰＭ１３の出荷段階で予め登録されている。このリボケーション情報は、コンテンツの保護のためにＰＭ１３の利用を無効化すべき機器（ＬＣＭ，ＰＤ）、更に具体的に述べるならばＰＭ１３（内の公開Ｒ／Ｗ領域１３３）を対象とするデジタルコンテンツの記録または再生のためのアクセス要求を無効化すべき機器（ＬＣＭ、ＰＤ）が判別可能な情報である。本実施形態において、リボケーション情報は無効化すべき機器の識別情報（デバイスＩＤ）のリストである。そこで、以下の説明では、「リボケーション情報」に代えて「リボケーションリストＲＬ」なる用語を用いる。つまり、公開ＲＯＭ領域１３２には、リボケーションリストＲＬが予め登録されている。
【００２６】
公開Ｒ／Ｗ領域１３３には、暗号化されたコンテンツキー（コンテンツ復号キー）、暗号化されたコンテンツ等が適宜記憶される。暗号化されたコンテンツキーは、コンテンツＣを復号するための（当該コンテンツＣに固有の）コンテンツキー$K_C$を、ＰＭ１３に依存するメディアキー$K_M$で暗号化することで取得されるものである。また、暗号化されたコンテンツ（ここでは２重に暗号化されたコンテンツ）は、$K_C$で暗号化されたコンテンツ（$K_C$［Ｃ］）をＰＭ１３に依存するメディアキー$K_M$で暗号化する（$K_M$［$K_C$［Ｃ］］）ことで取得されるものである。
【００２７】
ＬＣＭ１、ＰＤ１２もまた、図４に示すようにＰＭ１３と同様の記憶領域を有している。即ちＬＣＭ１は、公開ＲＯＭ領域１１２及び公開Ｒ／Ｗ領域１１３からなる公開領域１１１と、非公開の手順でしかアクセスできない秘匿領域１１４との各記憶領域を有している。公開Ｒ／Ｗ領域１１３には、図１に示す音楽データ格納部１０が確保されている。秘匿領域１１４には、ＬＣＭ１の識別情報（デバイスＩＤ）$ID_{LCM}$が予め記憶されている。秘匿領域１１４にはまた、各コンテンツ毎のコンテンツキー$K_C$が適宜記憶される。秘匿領域１１４には更に、図１に示す宿帳格納部８が確保されている。ＳＭＳ２の管理下にある音楽データ格納部１０（公開Ｒ／Ｗ領域１１３）にて保持される全ての音楽コンテンツは、その識別情報であるコンテンツＩＤ（ＴＩＤ）と予め定められた複製可能コンテンツ数、即ち子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼び、（秘匿領域１１４内の）宿帳格納部８に格納される。ＬＣＭ１は、ＳＭＳ２にてこの宿帳格納部８にアクセスするための秘匿された特定の手続が行われた後、宿帳格納部８（を提供する秘匿領域１１４）からデータを読み取るための秘匿領域ドライバ７を有している。なお、この宿帳は本発明に直接関係しないため、その利用方法の詳細については説明を省略する。
【００２８】
一方、ＰＤ１２は、公開ＲＯＭ領域１２２及び公開Ｒ／Ｗ領域１２３からなる公開領域１２１と、非公開の手順でしかアクセスできない秘匿領域１２４との各記憶領域を有している。秘匿領域１２４には、ＰＤ１２の識別情報$ID_{PD}$が予め固定記憶されている。秘匿領域１２４にはまた、各コンテンツ毎のコンテンツキー$K_C$が適宜記憶される。
【００２９】
図２は、ＰＤ１２の構成例を示す。
ＰＭ１３は、ＰＤ１２のメディアＩ／Ｆ部１２ｆに装着して利用される。ＬＣＭ１がＰＤ１２を介してＰＭ１３に読み書きする場合は、ＬＣＭ１内のＰＤＩ／Ｆ部５、ＰＤ１２内

のＬＣＭＩ／Ｆ部１２ｅ、メディアＩ／Ｆ部１２ｆを経由して当該ＰＭ１３の秘匿領域１３４（図３参照）にアクセスする。メディアＩ／Ｆ部１２ｆは、ＰＭ１３の秘匿領域１３４にアクセスするための秘匿領域アクセス部（図示せず）を有している。ＰＤ１２内の公開Ｒ／Ｗ領域１２３及び秘匿領域１２４（図４参照）は、例えばフラッシュメモリ１２ｄ上に確保されている。また公開ＲＯＭ領域１２２（図４参照）は、ＲＯＭ１２ｃ上に確保されている。このＲＯＭ１２ｃには、ＰＭ１３との間で相互認証を行うためのプログラムが書き込まれている。ＰＤ１２では、ＣＰＵ１２ａの制御のもと、このプログラムに従ってＰＭ１３との間の相互認証等の処理が実行される。

【００３０】

次に、本実施形態の動作について、ＥＭＤから配信された暗号化された音楽コンテンツをＬＣＭ１のＥＭＤＩ／Ｆ部３で受信して、ＳＭＳ２により音楽データ格納部１０に一時格納した後、その「複製」を「子」コンテンツとして、例えばメディアＩ／Ｆ部６に装着されたＰＭ１３に記録（コピー）するチェックアウト時の動作を例に、図５の流れ図を参照して説明する。

【００３１】

この場合、チェックアウトの指示が例えばＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介してなされ、且つＰＭ１３がＬＣＭ１のメディアＩ／Ｆ部６に装着された段階で、ＬＣＭ１のメディアＩ／Ｆ部６とＰＭ１３のコントローラ１３０との間で周知の相互認証が行われる（ステップＳ１０１）。この相互認証は、ＬＣＭ１を機器Ａ、ＰＭ１３を機器Ｂとすると、次のように行われるのが一般的である。

【００３２】

まず、機器Ａから機器Ｂを認証するものとする。ここで機器Ａは、公開鍵ｋｐを保持しており、機器Ｂは、機器Ａとの間で所定のコンテンツ保護機能を共有しているならば、公開鍵ｋｐに対応する秘密鍵ｋｓを保持している。機器Ａは乱数Ｒを発生して機器Ｂに送る。機器Ｂは、機器Ａで発生された乱数Ｒを受け取ると、それを秘密鍵ｋｓで暗号化して、その暗号化された乱数（ｋｓ［Ｒ］と表す）を機器Ａに返す。機器Ａでは、公開鍵ｋｐを用いて、ｋｓ［Ｒ］を復号し、復号結果が先に発生した乱数Ｒに等しければ、機器Ｂは正しい相手であると判定する。

【００３３】

その後、上記と同じことを機器Ｂから機器Ａに対して行うことで、相互認証を行うことができる。この場合、機器Ｂは公開鍵を保持し、機器Ａは秘密鍵を保持し、機器Ａが機器Ｂにて発生した乱数を秘密鍵で暗号化してそれを機器Ｂで公開鍵を用いて復号し、先に発生した乱数に等しいかを確認する。

【００３４】

以上の相互認証（Ｓ１０１）により、ＬＣＭ１及びＰＭ１３の双方にて正当な相手であることが確認されたとき、ＬＣＭ１のメディアＩ／Ｆ部６とＰＭ１３のコントローラ１３０との間でキー交換が行われ、同一の認証鍵（$K_{X1}$）が共有される。このキー交換は、例えばＤＶＤ－ＲＯＭのコンテンツ暗号化アルゴリズムとして使用されているＣＳＳ（Content Scrambling System）に代表されるランダムチャレンジ・レスポンスを用いた方法により行われる。認証鍵（$K_{X1}$）は毎回代わる時変キーである。

【００３５】

ＬＣＭ１のメディアＩ／Ｆ部６は、秘匿領域１１４に秘匿（記憶）されている自身の識別情報$ID_{LCM}$を読み出して当該$ID_{LCM}$を認証鍵（$K_{X1}$）で暗号化し、その暗号化された$ID_{LCM}$（＝$K_{X1}$［$ID_{LCM}$］）をメディアＩ／Ｆ部６からＰＭ１３に送る（ステップＳ１０２）。

【００３６】

ＰＭ１３のコントローラ１３０は、ＬＣＭ１側からの$K_{X1}$［$ID_{LCM}$］を、先のキー交換で取得した認証鍵（$K_{X1}$）で復号し、$ID_{LCM}$を得る（ステップＳ１０３）。

次にＰＭ１３のコントローラ１３０は、復号したＬＣＭ１の識別情報$ID_{LCM}$により公開ＲＯＭ領域１３２内のリボケーションリストＲＬを参照し、当該$ID_{LCM}$に一致する識別

情報が登録されているか否かにより、ＬＣＭ１によるＰＭ１３の利用を無効化するか否かを判定する（ステップＳ１０４）。

【００３７】

もし、$ＩＤ_{LCM}$に一致する識別情報がリボケーションリストＲＬに登録されている場合には、コントローラ１３０は該当するＬＣＭ１によるＰＭ１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【００３８】

これに対し、$ＩＤ_{LCM}$に一致する識別情報がリボケーションリストＲＬに登録されていない場合は、コントローラ１３０は該当するＬＣＭ１によるＰＭ１３の利用が許可されているものと判定し、秘匿領域１３４に秘匿されているメディアキー$K_M$を読み出し出力する（ステップＳ１０５）。そしてコントローラ１３０は、ＬＣＭ１のメディアＩ／Ｆ部６との間で（当該ＬＣＭ１のメディアＩ／Ｆ部６を介して）キー交換を行い、同一の認証鍵（$K_{X2}$）を共有した上で、上記読み出したメディアキー$K_M$を認証鍵（$K_{X2}$）で暗号化し、その暗号化された$K_M$（＝$K_{X2}$［$K_M$］）をＬＣＭ１に送る（ステップＳ１０６）。

【００３９】

ＬＣＭ１のメディアＩ／Ｆ部６は、ＰＭ１３側からの$K_{X2}$［$K_M$］を、先のキー交換で取得した認証鍵（$K_{X2}$）で復号し、メディアキー$K_M$を得る（ステップＳ１０７）。

次にＬＣＭ１のメディアＩ／Ｆ部６は、秘匿領域１１４に秘匿されているコンテンツキー$K_C$を取得したメディアキー$K_M$により暗号化し、その暗号化された$K_C$（＝$K_M$［$K_C$］）をＰＭ１３の公開Ｒ／Ｗ領域１３３に書き込む（ステップＳ１０８）。

【００４０】

このように本実施形態では、リボケーションリストＲＬに従って無効化（リボケート）されたならばＰＭ１３から渡されることのない（暗号化された）メディアキー$K_M$を、当該ＰＭ１３からＬＣＭ１が受け取って、そのＬＣＭ１の秘匿領域１１４に秘匿されているコンテンツキー$K_C$を当該メディアキー$K_M$により暗号化して、ＰＭ１３の公開Ｒ／Ｗ領域１３３に書き込むようにしている。このため、ＬＣＭ１とＰＭ１３との間で認証鍵の交換を行い、その認識鍵を用いてコンテンツキーの暗号化／復号化を行う方法に比べて、リボケーションリストＲＬで指定される無効化対象ＬＣＭ（ＰＭ１３を利用しようとする電子機器）を確実に無効化（排除）できる。なお、ＬＣＭ１の公開Ｒ／Ｗ領域１１３に確保された音楽データ格納部１０に蓄積されている暗号化コンテンツ（$K_C$［Ｃ］）をＰＭ１３に送る際に、上記取得した$K_M$で更に暗号化するようにしても構わない。

【００４１】

次に、ＰＭ１３に格納された暗号化コンテンツをＰＤ１２上で復号して再生する場合の動作について、図６の流れ図を参照して説明する。

まず、再生の指示が例えばＰＤ１２に対してなされ、且つＰＭ１３がＰＤ１２のメディアＩ／Ｆ部１２ｆに装着された段階で、ＰＤ１２のＣＰＵ１２ａとＰＭ１３のコントローラ１３０との間で（前記ステップＳ１０１と同様の）相互認証が行われる（ステップＳ２０１）。そして、この相互認証（Ｓ２０１）により、ＰＤ１２及びＰＭ１３の双方にて正当な相手であることが確認されたとき、ＰＤ１２のＣＰＵ１２ａとＰＭ１３のコントローラ１３０との間でキー交換が行われ、同一の認証鍵（$K_{X3}$）が共有される。

【００４２】

ＰＤ１２のＣＰＵ１２ａは、秘匿領域１２４に秘匿されている自身の識別情報$ＩＤ_{PD}$を読み出して当該$ＩＤ_{PD}$を認証鍵（$K_{X3}$）で暗号化し、その暗号化された$ＩＤ_{PD}$（＝$K_{X3}$［$ＩＤ_{PD}$］）をメディアＩ／Ｆ部１２ｆからＰＭ１３に送る（ステップＳ２０２）。

【００４３】

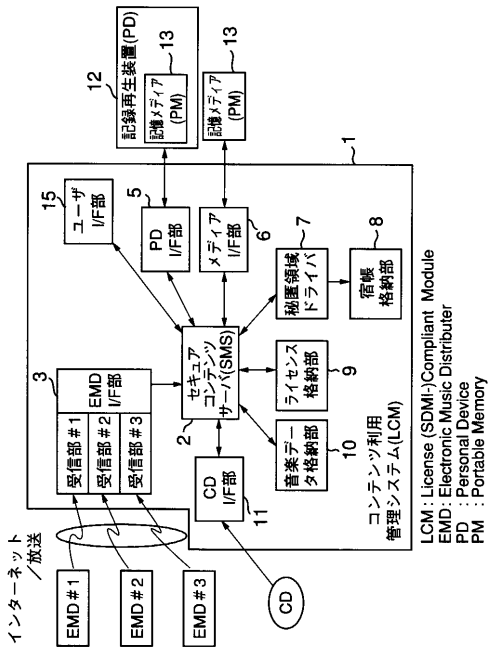
ＰＭ１３のコントローラ１３０は、ＰＤ１２側からの$K_{X3}$［$ＩＤ_{PD}$］を、先のキー交換で取得した認証鍵（$K_{X3}$）で復号し、$ＩＤ_{PD}$を得る（ステップＳ２０３）。

次にＰＭ１３のコントローラ１３０は、復号したＰＤ１２の識別情報$ＩＤ_{PD}$により公開ＲＯＭ領域１３２内のリボケーションリストＲＬを参照し、当該$ＩＤ_{PD}$に一致する識別情報が登録されているか否かにより、ＰＤ１２によるＰＭ１３の利用を無効化するか否かを判

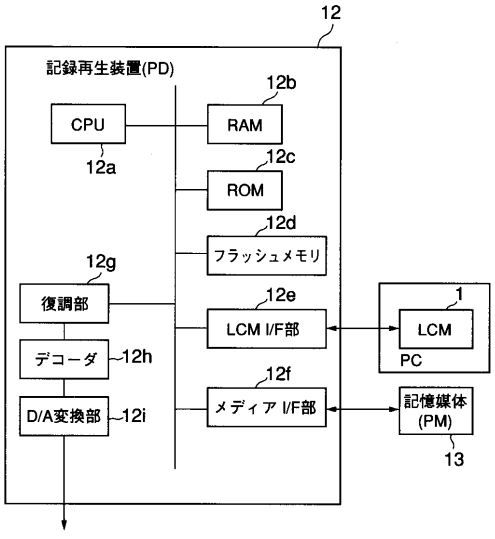
定する（ステップＳ２０４）。
【００４４】
もし、$ＩＤ_{PD}$に一致する識別情報がリボケーションリストＲＬに登録されている場合には、コントローラ１３０は該当するＰＤ１２によるＰＭ１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。
【００４５】
これに対し、$ＩＤ_{PD}$に一致する識別情報がリボケーションリストＲＬに登録されてない場合は、コントローラ１３０は該当するＰＤ１２によるＰＭ１３の利用が許可されているものと判定し、秘匿領域１３４に秘匿されているメディアキー$K_{M}$を読み出し出力する（ステップＳ２０５）。そしてコントローラ１３０は、ＰＤ１２のＣＰＵ１２ａとの間で（当該ＰＤ１２のメディアＩ／Ｆ部１２ｆを介して）キー交換を行い、同一の認証鍵（$K_{X4}$）を共有した上で、上記読み出したメディアキー$K_{M}$を認証鍵（$K_{X4}$）で暗号化し、その暗号化された$K_{M}$（＝$K_{X4}$［$K_{M}$］）をＰＤ１２に送る（ステップＳ２０６）。
【００４６】
ＰＤ１２のＣＰＵ１２ａは、ＰＭ１３側からの$K_{X4}$［$K_{M}$］を、先のキー交換で取得した認証鍵（$K_{X4}$）で復号し、メディアキー$K_{M}$を得る（ステップＳ２０７）。
次にＰＤ１２のＣＰＵ１２ａは、ＰＭ１３の公開Ｒ／Ｗ領域１３３に記憶されている暗号化されたコンテンツキー$K_{C}$（＝$K_{M}$［$K_{C}$］）を読み込んで、ステップＳ２０７で取得したメディアキー$K_{M}$により復号し、その復号されたコンテンツキー$K_{C}$を秘匿領域１２４に書き込んで秘匿化する（ステップＳ２０８）。したがってＰＤ１２では、この復号されたコンテンツキー$K_{C}$（と、必要ならば先に復号化したメディアキー$K_{M}$と）を利用して、ＰＭ１３の公開Ｒ／Ｗ領域１３３に記憶されている暗号化コンテンツを復号して再生することが可能となる。
【００４７】
このように本実施形態では、リボケーションリストＲＬに従って無効化（リボケート）されたならばＰＭ１３から渡されることのない（暗号化された）メディアキー$K_{M}$を、当該ＰＭ１３からＰＤ１２が受け取って、当該ＰＭ１３の秘匿領域１３４に秘匿されている暗号化コンテンツキー（$K_{M}$［$K_{C}$］）を、そのメディアキー$K_{M}$により復号化して、ＰＤ１２の秘匿領域１２４に書き込むようにしている。このため、ＰＤ１２とＰＭ１３との間で認証鍵の交換を行い、その認識鍵を用いて暗号化コンテンツキーの復号化を行うのに比べて、リボケーションリストＲＬで指定される無効化対象ＰＤ（ＰＭ１３を利用しようとする電子機器）を確実に無効化できる。
【００４８】
なお、以上の実施形態では、ＬＣＭ１とＰＭ１３の間、ＰＤ１２とＰＭ１３の間で、秘匿領域に秘匿されている情報、または秘匿領域に秘匿すべき情報の授受を行う際に、当該情報を認証鍵（$K_{Xi}$）により暗号化するものとしたが、認証鍵による暗号化は必ずしも必要ではない。但し、コンテンツ保護をより確実なものとするには、認証鍵による暗号化を行うことが好ましい。
【００４９】
また、以上の実施形態では、リボケーションリストＲＬが公開ＲＯＭ領域１３２に登録されているものとして説明したが、リボケーションリストＲＬが改ざんされない領域であれば良く、例えば秘匿された特定手続でしかアクセスできない秘匿領域１３４に登録されるようにしても良い。
【００５０】
【発明の効果】
以上詳述したように本発明によれば、記憶媒体の特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された構成としたので、当該記憶媒体が上記リストで表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることができる。
【図面の簡単な説明】

【図１】本発明の一実施形態に係るコンテンツ利用管理システムのブロック構成図。
【図２】図１中のＰＤ（記録再生装置）１２のブロック構成図。
【図３】図１中のＰＭ（記憶メディア）１３のブロック構成図。
【図４】ＬＣＭ１、ＰＤ１２の記憶領域構成例を示す図。
【図５】ＬＣＭ１からＰＭ１３へのコンテンツ記録時の動作手順を説明するための図。
【図６】ＰＭ１３に格納された暗号化コンテンツをＰＤ１２上で復号して再生する場合の動作手順を説明するための図。
【符号の説明】
１…ＬＣＭ（コンテンツ利用管理システム）
２…ＳＭＳ（セキュア・コンテンツ・サーバ）
５…ＰＤＩ／Ｆ部
６…メディアＩ／Ｆ部
７…秘匿領域ドライバ
８…宿帳格納部
９…ライセンス格納部
１０…音楽データ格納部
１１…ＣＤＩ／Ｆ部
１２…ＰＤ（記録再生装置）
１３…ＰＭ（記憶媒体、記憶メディア）
１１２，１２２，１３２…公開ＲＯＭ領域
１１３，１２３，１３３…公開Ｒ／Ｗ領域
１１４，１２４，１３４…秘匿領域
１３０…コントローラ

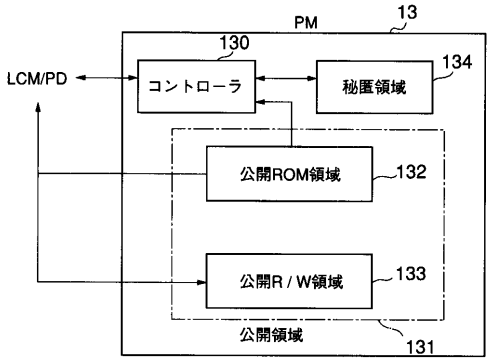
【図１】



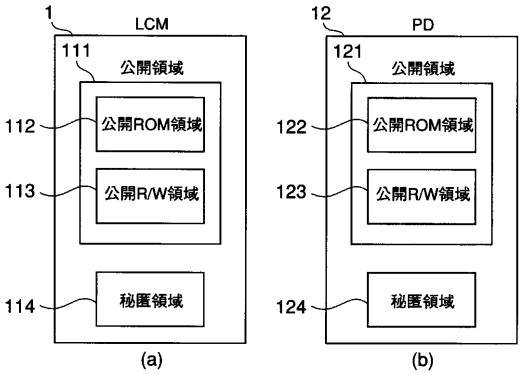

【図２】



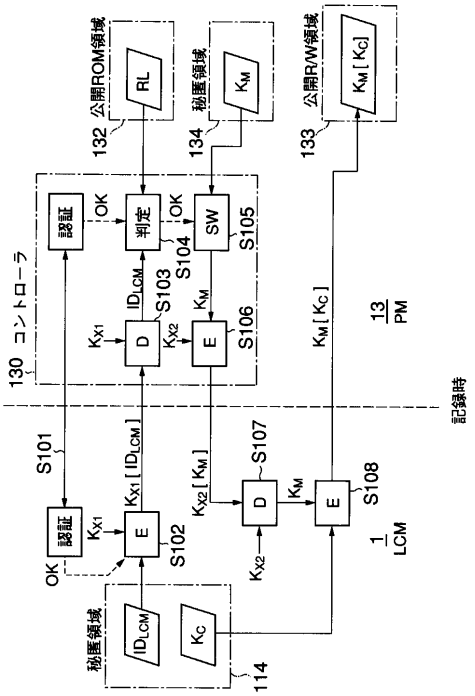
【図３】


PM
13
130
LCM/PD
コントローラ
秘匿領域
134
公開ROM領域
132
公開R / W領域
133
公開領域
131

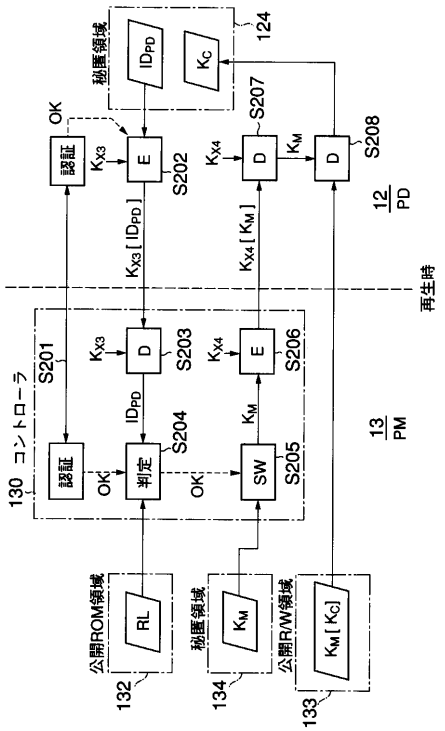
【図４】


1
LCM
111
公開領域
112
公開ROM領域
113
公開R/W領域
114
秘匿領域
(a)
12
PD
121
公開領域
122
公開ROM領域
123
公開R/W領域
124
秘匿領域
(b)

【図５】


公開ROM領域
RL
132
秘匿領域
134
公開R/W領域
133
130 コントローラ
認証
判定
SW
S101
S102
S103
S104
S105
S106
S107
S108
記録時
13/PM
1/LCM
114

【図６】


秘匿領域
124
S207
S208
12/PD
再生時
130 コントローラ
S201
S202
S203
S204
S205
S206
13/PM
公開ROM領域
132
秘匿領域
134
公開R/W領域
133

フロントページの続き

(72)発明者 山田 尚志
東京都港区芝浦一丁目１番１号 株式会社東芝本社事務所内
(72)発明者 岩崎 博
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝マイクロエレクトロニクスセンター内
(72)発明者 田村 正文
東京都港区芝浦一丁目１番１号 株式会社東芝本社事務所内
(72)発明者 石橋 泰博
東京都青梅市末広町２丁目９番地 株式会社東芝青梅工場内
(72)発明者 加藤 拓
東京都府中市東芝町１番地 株式会社東芝府中工場内
(72)発明者 館林 誠
大阪府門真市大字門真１００６番地 松下電器産業株式会社内
(72)発明者 原田 俊治
大阪府門真市大字門真１００６番地 松下電器産業株式会社内
(72)発明者 勝田 昇
大阪府門真市大字門真１００６番地 松下電器産業株式会社内

合議体
審判長 山崎 達也
審判官 宮司 卓佳
審判官 石井 茂和

(56)参考文献 Ｈｉｔａｃｈｉ, Ｌｔｄ., Ｉｎｔｅｌ Ｃｏｒｐｏｒａｔｉｏｎ, Ｍａｔｓｈｓｈｉｔａ Ｅｌｅｃｔｒｉｃ Ｉｎｄｕｓｔｒｉａｌ, Ｃｏ., Ｌｔｄ., Ｓｏｎｙ Ｃｏｒｐｏｒａｔｉｏｎ, Ｔｏｓｈｉｂａ Ｃｏｒｐｏｒａｔｉｏｎ, 5Ｃ Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ Ｗｈｉｔｅ Ｐａｐｅｒ, １９９８年 7月１４日
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 第７３９号, 日経ＢＰ社, １９９９年3月２２日, ｐ. ４９－ｐ. ５３

(58)調査した分野(Int.Cl., ＤＢ名)
G06F21/24