(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4660123号
(P4660123)

(45)発行日　平成23年3月30日(2011.3.30)　(24)登録日　平成23年1月7日(2011.1.7)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601B
H04L	9/10	(2006.01)	H04L	9/00	601E
H04L	9/32	(2006.01)	H04L	9/00	621A
			H04L	9/00	675D

請求項の数 11　(全 15 頁)

(21)出願番号　特願2004-178432(P2004-178432)
(22)出願日　平成16年6月16日(2004.6.16)
(65)公開番号　特開2006-5557(P2006-5557A)
(43)公開日　平成18年1月5日(2006.1.5)
審査請求日　平成19年4月2日(2007.4.2)

(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
(74)代理人　100092820
弁理士　伊丹　勝
(72)発明者　笠原　章裕
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　三浦　顕彰
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　嵩　比呂志
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

最終頁に続く

(54)【発明の名称】記憶媒体処理方法、データ処理装置及び記憶媒体処理プログラム

(57)【特許請求の範囲】
【請求項１】
媒体識別子データと、この媒体識別子データに基づいて生成可能な媒体固有鍵データと、この媒体固有鍵データによりユーザ鍵データが復号可能に暗号化されてなる暗号化ユーザ鍵データと、前記ユーザ鍵データによりコンテンツ鍵データが復号可能に暗号化されてなる暗号化コンテンツ鍵データとが記憶された記憶媒体と、
前記コンテンツ鍵データによりコンテンツデータが復号可能に暗号化されてなる暗号化コンテンツデータを保持したユーザ端末と
を用い、
前記記憶媒体が接続されたユーザ端末が適宜ライセンスセンタにアクセスして各種データを取得することを可能にされた記憶媒体処理方法において、
前記ユーザ端末が前記媒体識別子データを提示して前記記憶媒体の前記ユーザ鍵データの更新を前記ライセンスセンタに対し要求する更新要求ステップと、
前記ライセンスセンタが、前記更新要求ステップにおいて提示された前記媒体識別子データに係る前記ユーザ鍵データの更新履歴を参照する更新履歴参照ステップと、
提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていないと判定される場合、前記ライセンスセンタが、前記ユーザ端末の更新の要求に基づき前記ユーザ鍵データの更新を実行する更新実行ステップと、
提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていると判定される場合、前記ライセンスセンタが、前記ユーザ端末の更新の要求を

拒否する更新拒否ステップと
を備えたことを特徴とする記憶媒体処理方法。
【請求項２】
前記更新拒否ステップによる前記拒否の後、前記記憶媒体の送付を要求するメッセージを表示させるステップを実行する請求項１記載の記憶媒体処理方法。
【請求項３】
前記更新実行ステップは、更新された前記ユーザ鍵データにより、前記記憶媒体が保持するコンテンツ鍵データを暗号化した新規の暗号化コンテンツ鍵データを生成するステップを含むことを特徴とする請求項１の記憶媒体処理方法。
【請求項４】
前記ユーザ鍵データは、鍵本体のデータと、その鍵を管理する管理メタデータとを含み、
前記更新実行ステップは、前記鍵本体のデータはそのままとし、前記管理メタデータのみを更新するステップを含むことを特徴とする請求項１記載の記憶媒体処理方法。
【請求項５】
媒体識別子データと、この媒体識別子データに基づいて生成可能な媒体固有鍵データと、この媒体固有鍵データによりユーザ鍵データが復号可能に暗号化されてなる暗号化ユーザ鍵データと、前記ユーザ鍵データによりコンテンツ鍵データが復号可能に暗号化されてなる暗号化コンテンツ鍵データとが記憶された記憶媒体と接続され、前記コンテンツ鍵データによりコンテンツデータが復号可能に暗号化されてなる暗号化コンテンツデータを保持したユーザ端末を介して前記記憶媒体のデータ処理を行なうデータ処理装置において、
前記媒体識別子データの提示を伴う前記ユーザ鍵データの更新要求を前記ユーザ端末から受信し、更新要求が適正と判定される場合に新しいユーザ鍵データを発行して前記ユーザ端末に送信する鍵配信サーバと、
前記ユーザ鍵データの更新の履歴を、前記媒体識別子データ毎に保持する更新履歴データベースと
を備え、
前記鍵配信サーバは、前記更新履歴データベースを参照して、
提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていないと判定される場合、前記ユーザ端末の更新の要求に基づき前記ユーザ鍵データの更新を実行し、
提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていると判定される場合、前記ユーザ端末の更新の要求を拒否する
ように構成されたことを特徴とするデータ処理装置。
【請求項６】
前記鍵配信サーバは、前記拒否の後、前記記憶媒体の送付を要求するよう構成された請求項５記載のデータ処理装置。
【請求項７】
前記ユーザ鍵データを保持するユーザ鍵データベースを更に備え、
前記鍵配信サーバは、前記ユーザ鍵データの更新を実行する場合、このユーザ鍵データベースに保持されるユーザ鍵データを書き換える請求項５記載のデータ処理装置。
【請求項８】
前記鍵配信サーバは、前記ユーザ鍵データの更新を実行する場合、その更新されたユーザ鍵データにより、前記記憶媒体が保持するコンテンツ鍵データを暗号化した新規の暗号化コンテンツ鍵データを生成することを特徴とする請求項５のデータ処理装置。
【請求項９】
前記ユーザ鍵データは、鍵本体のデータと、その鍵を管理する管理メタデータとを含み、
前記鍵配信サーバは、前記ユーザ鍵の更新を実行する場合、前記鍵本体のデータはそのままとし、前記管理メタデータのみを更新することを特徴とする請求項５記載のデータ処

理装置。
【請求項１０】
媒体識別子データと、この媒体識別子データに基づいて生成可能な媒体固有鍵データと、この媒体固有鍵データによりユーザ鍵データが復号可能に暗号化されてなる暗号化ユーザ鍵データと、前記ユーザ鍵データによりコンテンツ鍵データが復号可能に暗号化されてなる暗号化コンテンツ鍵データとが記憶された記憶媒体と接続され且つ前記コンテンツ鍵データによりコンテンツデータが復号可能に暗号化されてなる暗号化コンテンツデータを保持したユーザ端末からライセンスセンタへのアクセスに応じて、前記ライセンスセンタが前記ユーザ端末に対し各種データを与える記憶媒体処理方法に用いられる記憶媒体処理プログラムであって、
前記ユーザ端末からライセンスセンタに対し、前記媒体識別子データを提示して前記記憶媒体の前記ユーザ鍵データの更新を要求する更新要求がされた場合、前記ライセンスセンタが、前記媒体識別子データに係る前記ユーザ鍵データの更新履歴を参照する更新履歴参照ステップと、
提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていないと判定される場合、前記ライセンスセンタが、前記ユーザ端末の更新の要求に基づき前記ユーザ鍵データの更新を実行する更新実行ステップと、
提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていると判定される場合、前記ライセンスセンタが、前記ユーザ端末の更新の要求を拒否する更新拒否ステップと、
を実行するように構成されたことを特徴とする記憶媒体処理プログラム。
【請求項１１】
前記更新拒否ステップは、前記拒否の後、前記記憶媒体の送付を要求するメッセージを表示させるステップを実行する請求項１０記載の記憶媒体処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化二重鍵方式に対応する記憶媒体を、ユーザ端末を介してライセンスセンタ装置とオンライン接続することにより、ユーザ端末がライセンスセンタ装置からコンテンツ等を取得することができるようにした記憶媒体処理方法、システム及びプログラムに関するものである。
【背景技術】
【０００２】
近年、情報化社会の発展に伴い、本、新聞、音楽又は動画などを電子化したコンテンツをユーザ端末に配信し、コンテンツを閲覧可能とするコンテンツ流通システムが広く用いられてきている。
但し、電子化したコンテンツ（以下、単にコンテンツという）は、容易に複製可能なため、著作権を無視する違法行為が生じ易い。このような違法行為からコンテンツを保護する観点から、コンテンツは、通常、暗号化鍵により、暗号化されて記録され、再生時に復号される。この種のコンテンツ保護技術には、ＣＰＲＭ（Content Protection for Prerecorded Media）があり、例えばＳＤオーディオ(SD-Audio)、ＳＤビデオ(SD-video)、ＳＤイー・パブリッシュ(SD-ePublish：ＳＤ電子出版)のように規格化された暗号化鍵方式を用いている（例えば、非特許文献１参照）。この非特許文献１で採用されている暗号化鍵方式は、タイトル鍵をメディア固有鍵で一重に暗号化する暗号化一重鍵方式である。一方、以下のようにコンテンツ鍵がユーザ鍵及びメディア固有鍵で二重に暗号化された暗号化二重鍵方式が考えられている（例えば、非特許文献２参照）。この種の暗号化二重鍵方式は、例えばＭＱｂｉｃ（登録商標）に用いられている。
【０００３】
図１０は係るＭＱｂｉｃにおいて採用されている暗号化二重鍵方式に対応したＳＤカード及びユーザ端末の構成を示す模式図である。ここで、ＳＤカードＳＤｑは、データをセ

キュアに記憶したセキュア記憶媒体の一例であり、システム領域(System Area)１、秘匿領域(Hidden Area)２、保護領域(Protected Area)３、ユーザデータ領域(User Data Area)４及び暗復号部５を備えており、各領域１～４にデータが記憶されている。

このようなＳＤカードＳＤｑは、具体的には、システム領域１には鍵管理情報ＭＫＢ(Media Key Block)及びメディア識別子ＩＤｍが記憶され、秘匿領域２にはメディア固有鍵Ｋｍｕが記憶され、保護領域３には暗号化ユーザ鍵Ｅｎｃ（Ｋｍｕ、Ｋｕ）が記憶され、ユーザデータ領域４には暗号化コンテンツ鍵Ｅｎｃ（Ｋｔ、Ｋｃ）が記憶されている。なお、Ｅｎｃ（Ａ、Ｂ）の表記は、本明細書中ではデータＡにより暗号化されたデータＢを意味する。ここで、ユーザ鍵Ｋｕは、コンテンツ鍵Ｋｃに対する暗号化／復号鍵であり、同一のＳＤカードＳＤｑでは複数個の暗号化コンテンツ鍵Ｅｎｃ（Ｋｕ、Ｋｃ１）、Ｅｎｃ（Ｋｕ、Ｋｃ２）、…に対しても、共通に使用される。また、ＳＤカードＳＤｑの添字ｑは、ＭＱｂｉｃ（登録商標）に対応する旨を表す。

【０００４】

ここで、システム領域１は、読取専用でＳＤカード外部からアクセス可能な領域である。秘匿領域２は、読取専用でＳＤカード自身が参照する領域であり、外部からのアクセスが一切不可となっている。保護領域３は、認証に成功した場合にＳＤカード外部から読出／書込可能な領域である。ユーザデータ領域４は、ＳＤカード外部から自由に読出／書込可能な領域である。暗復号部５は、保護領域３とＳＤカード外部との間で、認証、鍵交換及び暗号通信を行なうものであり、暗号化／復号機能をもっている。

【０００５】

このようなＳＤカードＳＤｑに対し、再生用のユーザ端末１０ｑは以下のように論理的に動作する。すなわち、ユーザ端末１０ｑでは、ＳＤカードＳＤｑのシステム領域１から読み出した鍵管理情報ＭＫＢを、予め設定されたデバイス鍵ＫｄによりＭＫＢ処理し（ＳＴ１）、メディア鍵Ｋｍを得る。次に、ユーザ端末１０ｑは、このメディア鍵Ｋｍと、ＳＤカードＳＤｑのシステム領域１から読み出したメディア識別子ＩＤｍとを共にハッシュ処理し（ＳＴ２）、メディア固有鍵Ｋｍｕを得る。

【０００６】

しかる後、ユーザ端末１０ｑは、このメディア固有鍵Ｋｍｕに基づいて、ＳＤカードＳＤｑの暗復号部５との間で認証及び鍵交換（ＡＫＥ： Authentication Key Exchange）処理を実行し（ＳＴ３）、ＳＤカードＳＤｑとの間でセッション鍵Ｋｓを共有する。なお、ステップＳＴ３の認証及び鍵交換処理は、暗復号部５に参照される秘匿領域２内のメディア固有鍵Ｋｍｕと、ユーザ端末１０ａに生成されたメディア固有鍵Ｋｍｕとが一致するときに成功し、セッション鍵Ｋｓが共有される。

続いて、ユーザ端末１０ｑは、セッション鍵Ｋｓを用いた暗号通信を介して保護領域３から暗号化ユーザ鍵Ｅｎｃ（Ｋｍｕ、Ｋｕ）を読み出すと（ＳＴ４）、この暗号化ユーザ鍵Ｅｎｃ（Ｋｍｕ、Ｋｕ）をメディア固有鍵Ｋｍｕにより復号処理し（ＳＴ５）、ユーザ鍵Ｋｕを得る。

【０００７】

最後に、ユーザ端末１０ｑは、ＳＤカードＳＤｑのユーザデータ領域４から暗号化コンテンツ鍵Ｅｎｃ（Ｋｔ、Ｋｃ）を読出すと、この暗号化コンテンツ鍵Ｅｎｃ（Ｋｕ、Ｋｃ）をユーザ鍵Ｋｕにより復号処理し（ＳＴ５ｑ）、コンテンツ鍵Ｋｃを得る。最後に、ユーザ端末１０ａは、メモリ１１ｑから暗号化コンテンツＥｎｃ（Ｋｃ、Ｃ）を読出すと、この暗号化コンテンツＥｎｃ（Ｋｃ、Ｃ）をコンテンツ鍵Ｋｃにより復号処理し（ＳＴ６）、得られたコンテンツＣを再生する。なお、上記の例では、暗号化コンテンツは、ユーザ端末１０ｑ内のメモリ１１ｑに記憶されるとしたが、外部の記憶媒体に記憶されていてもよい。

【０００８】

以上のような暗号化二重鍵方式は、保護領域３よりも記憶容量が大きいユーザデータ領域４に暗号化コンテンツ鍵を保持するので、暗号化一重鍵方式よりも大量の暗号化コンテンツ鍵を保存できる利点がある。また、暗号化二重鍵方式は、暗号化コンテンツをＳＤカ

ード外部に保持できることから、暗号化コンテンツの流通を促すことが期待されている。
さらに、暗号化二重鍵方式では、各ＳＤカードには識別子としてのメディアＩＤが付与されており、メディアＩＤごとに固有のユーザ鍵が発行される。このユーザ鍵も暗号化されて、ＳＤカードの保護領域（プロテクトエリア）に格納される。ユーザ鍵の暗号化はメディアＩＤに依存しており、また正当なプレイヤーでしか復号できない。このため、侵害者がコンテンツ鍵のみをユーザデータ領域から不正にコピーしたとしても、コンテンツを取得することはできないようになっている。

【０００９】

【非特許文献１】４Ｃ　エンティティ、ＬＬＣ、［online］、インターネット＜ＵＲＬ：http://www.4Centity.com/、平成１６年６月１４日検索＞

【非特許文献２】ＩＴ情報サイト・ＩＴｍｅｄｉａニュース［online］、インターネット＜ＵＲＬ：http://www.itmedia.co.jp/news/0307/18/njbt_02.html、平成１６年６月１４日検索＞

【発明の開示】

【発明が解決しようとする課題】

【００１０】

ＳＤカードにおいては、偽造ＳＤカード（偽造記憶媒体）の存在が確認されており、その蔓延を防止することが喫緊の課題となっている。偽造ＳＤカードが存在する主な理由は、ＳＤカードのライセンスを受けた製造メーカが、裏で不正を働いたこと等による場合が多い。同一メディア識別子を有する偽造ＳＤカードが、数百枚も流通することも十分に起こり得る。偽造ＳＤカードの保持者は、悪意の場合もあれば、善意（偽造と知らずに、購入し使用している）の場合もあり得る。偽造カードは、メディア識別子だけが同じであれば、同一のメディア識別子を有する正規のカードの保持者に、別のメディア識別子を付与されたカードを再発行すれば済む。しかし、偽造カードが蔓延し、ユーザ鍵等までコピーされたクローンＳＤカード（ＭＫＢ（Media key block）、メディアＩＤ、メディア固有鍵、暗号化ユーザ鍵、暗号化コンテンツ鍵等が、正当なＳＤカードと全て同一であるＳＤカード）が出回る事態に発展すると問題が生じる。すなわち、クローンＳＤカードの保持者がライセンスセンタにアクセスし、コンテンツを取得した場合、その課金が同一ＩＤ等を有する正規のＳＤカードにチャージされてしまうなどの問題が生じる可能性がある。従って、偽造ＳＤカードの使用を可能な限り排除することが、システムの正常な運用のために不可欠である。

【課題を解決するための手段】

【００１１】

この発明に係る記憶媒体処理方法は、予め媒体識別子データと、この媒体識別子データに基づいて生成可能な媒体固有鍵データと、この媒体固有鍵データによりユーザ鍵データが復号可能に暗号化されてなる暗号化ユーザ鍵データと、前記ユーザ鍵データによりコンテンツ鍵データが復号可能に暗号化されてなる暗号化コンテンツ鍵データとが記憶された記憶媒体と、前記コンテンツ鍵データによりコンテンツデータが復号可能に暗号化されてなる暗号化コンテンツデータを保持したユーザ端末とを用い、前記記憶媒体が接続されたユーザ端末が適宜ライセンスセンタにアクセスして各種データを取得することを可能にされた記憶媒体処理方法において、前記ユーザ端末が、前記媒体識別子データを提示して前記記憶媒体の前記ユーザ鍵データの更新をライセンスセンタに対し要求する更新要求ステップと、前記ライセンスセンタが、前記更新要求ステップにおいて提示された前記媒体識別子データに係る前記ユーザ鍵データの更新履歴を参照する更新履歴参照ステップと、提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていないと判定される場合、前記ライセンスセンタが、前記ユーザ端末の更新の要求に基づき前記ユーザ鍵データの更新を実行する更新実行ステップと、提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていると判定される場合、前記ライセンスセンタが、前記ユーザ端末の更新の要求を拒否する更新拒否ステップとを備えたことを特徴とする。

【００１２】
この発明に係るデータ処理装置は、媒体識別子データと、この媒体識別子データに基づいて生成可能な媒体固有鍵データと、この媒体固有鍵データによりユーザ鍵データが復号可能に暗号化されてなる暗号化ユーザ鍵データと、前記ユーザ鍵データによりコンテンツ鍵データが復号可能に暗号化されてなる暗号化コンテンツ鍵データとが記憶された記憶媒体と接続され、前記コンテンツ鍵データによりコンテンツデータが復号可能に暗号化されてなる暗号化コンテンツデータを保持したユーザ端末を介して前記記憶媒体のデータ処理を行なうデータ処理装置において、前記媒体識別子データの提示を伴う前記ユーザ鍵データの更新要求を前記ユーザ端末から受信し、更新要求が適正と判定される場合に新しいユーザ鍵データを発行して前記ユーザ端末に送信する鍵配信サーバと、前記ユーザ鍵データの更新の履歴を、前記媒体識別子データ毎に保持する更新履歴データベースとを備え、前記鍵配信サーバは、前記更新履歴データベースを参照して、提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていないと判定される場合、前記ユーザ端末の更新の要求に基づき前記ユーザ鍵データの更新を実行し、提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていると判定される場合、前記ユーザ端末の更新の要求を拒否するように構成されたことを特徴とする。
【００１３】
この発明に係る記憶媒体処理プログラムは、媒体識別子データと、この媒体識別子データに基づいて生成可能な媒体固有鍵データと、この媒体固有鍵データによりユーザ鍵データが復号可能に暗号化されてなる暗号化ユーザ鍵データと、前記ユーザ鍵データによりコンテンツ鍵データが復号可能に暗号化されてなる暗号化コンテンツ鍵データとが記憶された記憶媒体と接続され且つ前記コンテンツ鍵データによりコンテンツデータが復号可能に暗号化されてなる暗号化コンテンツデータを保持したユーザ端末からライセンスセンタへのアクセスに応じて、前記ライセンスセンタが前記ユーザ端末に対し各種データを与える記憶媒体処理方法に用いられる記憶媒体処理プログラムであって、前記ユーザ端末からライセンスセンタに対し、前記媒体識別子データを提示して前記記憶媒体の前記ユーザ鍵データの更新を要求する更新要求がされた場合、前記ライセンスセンタが、前記媒体識別子データに係る前記ユーザ鍵データの更新履歴を参照する更新履歴参照ステップと、提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていないと判定される場合、前記ライセンスセンタが、前記ユーザ端末の更新の要求に基づき前記ユーザ鍵データの更新を実行する更新実行ステップと、提示された前記媒体識別子データに係る前記ユーザ鍵データの更新が所定期間内に行なわれていると判定される場合、前記ライセンスセンタが、前記ユーザ端末の更新の要求を拒否する更新拒否ステップとを実行するように構成されたことを特徴とする。
【発明の効果】
【００１４】
この発明によれば、記憶媒体を継続使用するため、記憶媒体の保持者がユーザ鍵データの更新要求をライセンスセンタに送信する場合、ユーザ端末からは媒体識別子データが提示される。ライセンスセンタは、提示された媒体識別子データに係るユーザ鍵データの更新履歴を参照する。提示された媒体識別子データに係るユーザ鍵データの更新が所定期間内に行なわれていないと判定される場合、ユーザ鍵データの更新が実行される。一方、提示された媒体識別子データに係るユーザ鍵データの更新が所定期間内に行なわれていると判定される場合、更新の要求は拒否される。これにより、例えば偽造記憶媒体の保持者が、正規の記憶媒体の保持者に遅れてユーザ鍵データの更新を要求した場合には、更新の要求は拒否され、その偽造記憶媒体は、有効期限切れにより記憶媒体の継続使用が不可能となる。一方、正規の記憶媒体の保持者は、偽造記憶媒体の保持者よりもユーザ鍵の更新要求が遅れたとしても、その後ユーザ登録データの確認を受けて、別の媒体識別子データを割り振られた記憶媒体の提供を受ける等により、保護を受けることができる。従って、本発明によれば、正規の記憶媒体の保持者の被害及び手数を最小限に抑えつつ、偽造記憶媒

体の蔓延を防止することができる。
【発明を実施するための最良の形態】
【００１５】
以下、本発明の各実施形態について図面を参照しながら説明する。
図１は本発明の実施形態に係る記憶媒体処理システムの構成を示す模式図である。図１０と同種の部分には同一符号を付してその詳しい説明を省略し、ここでは異なる部分について主に述べる。
【００１６】
具体的には本実施形態のシステムは、ＳＤカードＳＤｑを着脱自在に保持するユーザ端末２０がネットワーク３０を介してライセンスセンタ装置４０に通信可能となっている。
ユーザ端末２０は、メモリ２１、ダウンロード部２２、ＳＤカード処理部２３、及び制御部２５を備えており、例えばパーソナルコンピュータ、携帯電話又は携帯情報端末（ＰＤＡ）などのように、ＳＤカードＳＤｑを着脱自在に保持する電子機器であれば任意なデバイスが使用可能となっている。
ここで、メモリ２１は、他の各部２２～２５から読出／書込な記憶領域であり、例えば暗号化コンテンツＥｎｃ（Ｋｃ、Ｃ）が記憶される。
【００１７】
ダウンロード部２２は、制御部２５により制御され、ライセンスセンタ装置４０から暗号化コンテンツ鍵Ｅｎｃ（Ｋｕ、Ｋｃ）や新しいユーザ鍵Ｋｕｎをダウンロードする機能を有しており、例えばブラウザ等が使用可能となっている。　ＳＤカード処理部２３は、制御部２５により制御され、ＳＤカードＳＤｑとの間の認証機能、暗号通信機能及び各領域１、３、４の記憶内容を読出／書込する機能をもっている。　制御部２５は、通常のコンピュータ機能と、ユーザの操作に応じて他の各部２１～２４を制御する機能とを有している。
【００１８】
ライセンスセンタ装置４０は、鍵配信サーバ４１、メディア識別子データベース４２、ユーザ鍵データベース４３、有効期限データベース４４、更新履歴データベース４５、コンテンツ鍵データベース４６、権利発行済みコンテンツＩＤデータベース４７、及びユーザ登録データベース４８を備えている。
鍵配信サーバ４１は、ユーザ端末２０からネットワーク３０を介してコンテンツ鍵送信要求を受けた場合、所定の認証プロセスを経た後、要求に係る新しいコンテンツ鍵データをネットワーク３０を介してユーザ端末２０に返信する機能を有する。また、鍵配信サーバ４１は、ユーザ端末２０からネットワーク３０を介してユーザ鍵更新要求を受けた場合、各種データベース４２、４４、４５等にアクセスし、要求の適否を判定すると共に、要求が適正と判定される場合、新しいユーザ鍵データを生成すると共に、その新しいユーザ鍵データ等をネットワーク３０を介してユーザ端末２０に返信する機能を有する。
【００１９】
メディア鍵データベース４２は、各ＳＤカードが有するメディア識別子ＩＤｍのデータを保持するものである。ユーザ鍵データベース４３は、各ＳＤカードが有するユーザ鍵、及び鍵配信サーバ４１がユーザ鍵更新要求に対応して新たに生成したユーザ鍵を保存するためのものである。有効期限データベース４４は、各ＳＤカードが保有するユーザ鍵Ｋｕの有効期限に関するデータを保持するものである。
更新履歴データベース４５は、ＳＤカードＳＤｑのユーザ鍵Ｋｕの更新の履歴のデータを、各ＳＤカードＳＤｑが有するメディア識別子ＩＤｍと対応付けて保持するものである。
コンテンツ鍵データベース４６は、各種コンテンツ鍵を保持するものである。権利発行済みコンテンツＩＤデータベース４７は、ＳＤカード保持者の要求に応じて発行したコンテンツ鍵のデータを、当該ＳＤカードのメディア識別子ＩＤｍと対応付けて保持するものである。ユーザ登録データベース４８は、ＳＤカード保持者が、自身の個人データ等（住所、氏名、電話番号等）を示して行なったユーザ登録のデータを保持するものである。ユ

ーザ登録を行なうことにより、正規のＳＤカードの保持者は、偽造ＳＤカードの保持者が先んじてユーザ鍵の更新等を行なったとしても、後述するように、別の媒体識別子データを割り振られた新しい記憶媒体の提供を受ける等の保護を受けることができる。

【００２０】

セキュリティモジュール５１は、ユーザ鍵Ｋｕ及びコンテンツ鍵Ｋｃの暗復号処理を実行する装置であり、管理用鍵取得部５２及び鍵暗号化管理部５３を備えている。

管理用鍵取得機能５２は、鍵配信サーバ４１から読出可能に管理用鍵を保持するものである。

鍵暗号化管理部５３は、鍵配信サーバ４１から管理用鍵が設定される機能と、この管理用鍵に基づいて、鍵配信サーバ４１から受けた管理用の暗号化ユーザ鍵及び管理用の暗号化コンテンツ鍵をそれぞれ復号し、ユーザ鍵及びコンテンツ鍵を得る機能と、コンテンツ鍵と基本メタデータとをユーザ鍵で暗号化し、得られた暗号化コンテンツ鍵（基本メタデータを含む）と購入日等の（付加的な）メタデータとを鍵配信サーバ４１に送信する機能とを持っている。

【００２１】

次に、以上のように構成された記憶媒体処理システムによる記憶媒体処理方法を図２乃至図９を用いて説明する。まずコンテンツ鍵の取得処理を述べ、その後、ユーザ鍵の更新処理を説明する。

【００２２】

（コンテンツ鍵の取得処理）

ＳＤカードＳＤｑがユーザ端末２０を介してコンテンツ鍵を取得する手順について、図２を参照して説明する。ユーザ端末２０においては、ユーザの操作により、制御部２５がダウンロード部２２を起動し、図２に示すように、ダウンロード部２２が予めコンテンツ鍵を購入又は課金済みである旨を確認する（ＳＴ１１）。未購入の場合、ユーザ端末２０は、コンテンツ鍵の購入及び決済処理をライセンスセンタ装置４０との間で実行し、コンテンツ鍵を購入又は課金済の状態にしておく。

続いて、ダウンロード部２２は、取得したい暗号化コンテンツ鍵及びメタデータの送信要求を鍵配信サーバ４１に送信する（ＳＴ１２）。なお、この送信要求は、少なくとも暗号化コンテンツ鍵に対応するコンテンツＩＤと、ＳＤカードＳＤｑのメディア識別子ＩＤｍとを含む。

【００２３】

鍵配信サーバ４１は、この送信要求を受けると、予めメディア識別子ＩＤｍ毎に記憶された管理用の暗号化ユーザ鍵をユーザ鍵データベース４３から読み込むと共に（ＳＴ１３）、予めコンテンツＩＤ毎に記憶された管理用の暗号化コンテンツ鍵及び基本メタデータ（コンテンツＩＤ、タイトル、製作者、その他）をコンテンツ鍵データベース４６から読み込む（ＳＴ１４）。しかる後、鍵配信サーバ４１は、管理用鍵取得部５２から管理用鍵を読み込むと（ＳＴ１５）、この管理用鍵を鍵暗号化管理部５３に設定し（ＳＴ１６）、コンテンツ鍵の暗号化要求を鍵暗号化管理部５３に送信する（ＳＴ１７）。なお、この暗号化要求は、管理用の暗号化ユーザ鍵、管理用の暗号化コンテンツ鍵及び基本メタデータを含んでいる。

【００２４】

鍵暗号化管理部５３は、管理用鍵に基づいて、管理用の暗号化ユーザ鍵及び管理用の暗号化コンテンツ鍵をそれぞれ復号し、ユーザ鍵及びコンテンツ鍵を得る。しかる後、鍵暗号化管理部５３は、コンテンツ鍵と基本メタデータとをユーザ鍵で暗号化し、得られた暗号化コンテンツ鍵（基本メタデータを含む）と購入日等の（付加的な）メタデータとを鍵配信サーバ４１に送信する（ＳＴ１８）。

鍵配信サーバ４１は、付加メタデータを読み込むと（ＳＴ１９）、暗号化コンテンツ鍵及びメタデータを含む例えばＳＯＡＰ(Simple Object Access Protocol)メッセージを生成し（ＳＴ２０）、ＳＯＡＰメッセージにより暗号化コンテンツ鍵及びメタデータをユーザ端末２０に送信する（ＳＴ２１）。なお、ＳＯＡＰメッセージは、メッセージ方式の一

例であり、他の方式に変更してもよいことは言うまでもない。

【００２５】

ユーザ端末２０においては、ＳＯＡＰメッセージを受けたダウンロード部２２が、暗号化コンテンツ鍵の保存要求をＳＤカード処理部２３に送出する。なお、暗号化コンテンツ鍵の保存要求は、暗号化コンテンツ鍵及びメタデータのうち、暗号化コンテンツ鍵のみを含んでいる。ＳＤカード処理部２３は、この暗号化コンテンツ鍵をＳＤカードＳＤｑのユーザデータ領域４に書込む。

また、ダウンロード部２２は、ＳＤカード処理部２３に送出しなかったメタデータを保存する（ＳＴ２３）。これにより、コンテンツ鍵の取得処理を終了する。

【００２６】

（ユーザ鍵の更新処理）

次に、ユーザ鍵の更新の手順を、図３に基づいて説明する。

ユーザ端末２０においては、ユーザの操作により、制御部２５がＳＤカード処理部２３及びダウンロード部２２を起動する。ＳＤカード処理部２３は、ユーザ鍵の更新要求のため、ＳＤカードＳＤｑのメディア識別子ＩＤｍをシステム領域１から読み出すと共に（ＳＴ３０）、乱数Ｒ１を生成する（ＳＴ３１）。この乱数Ｒ１は、ユーザ端末２０とライセンスセンタ装置４０との間のセキュアな通信を行なうため、共通鍵暗号化方式を用いたチャレンジ・レスポンスによる認証とセッション鍵の生成のために発生されるものである。

続いて、ダウンロード部２２は、ユーザ鍵Ｋｕの更新要求を鍵配信サーバ４１に送信する（ＳＴ３２）。この更新要求は、ＳＤカードＳＤｑのメディア識別子ＩＤｍと、更新対象である古いユーザ鍵データＫｕｏと、生成した乱数Ｒ１とを含む。

【００２７】

鍵配信サーバ４１は、この送信要求を受けると、後述するように、そのメディア識別子ＩＤｍによる更新の履歴を、更新履歴データベース４５を参照し(ＳＴ３３)、所定期間内に更新がなければ、次のステップＳＴ３４へ移行する。所定期間内に更新があった場合については、後述する。

ＳＴ３４では、管理用の暗号化ユーザ鍵Ｋｕｏをユーザ鍵データベース４３から読み込み、このユーザ鍵データＫｕｏに基づいて、有効期限が更新された新規のユーザ鍵データＫｕｎを生成する。なお、この明細書では、ユーザ鍵Ｋｕのうち、更新前の古いユーザ鍵データＫｕにはＫｕｏの符号を付し、更新後の新しいユーザ鍵データＫｕには、Ｋｕｎを付すものとする。また、更新後の有効期限の長さは、状況により様々に変更することができる。通常は、更新前の有効期限の長さと同一でよいが、例えば、ライセンスセンタの業務が諸事情により終了する場合など特定の場合には、有効期間を十分長い期間にしたり、或いは有効期限自体を取り外すようにしてもよい。

そして、このメディア識別子ＩＤｍと、新しいユーザ鍵データＫｕｎをユーザ鍵データベース４３に保存する（ＳＴ３５）。

【００２８】

続いて、鍵配信サーバ４１は、乱数Ｒ２を生成し（ＳＴ３６）、続いて、ＳＤカード処理部２３から受信した乱数Ｒ１と、この乱数Ｒ２と、共通暗号化鍵としての秘密情報Ｋ１、Ｋ２とを用いて、セッション鍵Ｋｓを生成する（ＳＴ３７）。鍵配信サーバ４１は、この生成されたセッション鍵Ｋｓで、新しいユーザ鍵Ｋｕｎを暗号化し（ＳＴ３８）、ＳＯＡＰメッセージにより暗号化されたユーザ鍵データＫｕｎを乱数Ｒ２と共にダウンロード部２５を介してＳＤカード処理部２３に送信する（ＳＴ３９）。ＳＤカード処理部２３は、乱数Ｒ１、Ｒ２及び秘密情報Ｋ１、Ｋ２からセッション鍵Ｋｓを生成すると共に（ＳＴ４０）、暗号化されたユーザ鍵Ｋｕｎをセッション鍵Ｋｓで復号する（ＳＴ４１）。この復号化されたユーザ鍵Ｋｕｎは、再びＳＤカード処理部２３によりメディア固有鍵Ｋｍｕを用いて暗号化されて、ＳＤカードＳＤｑの保護領域４に書き込まれる（ＳＴ４２）。これにより、ユーザ鍵Ｋｕの更新処理を終了する。

【００２９】

図４により、前述のＳＴ３３の詳細を、更新履歴データベース４５の参照の結果、所定

期間内に同一のメディア識別子ＩＤｍによる更新がなされていると判定される場合を含めて説明する。鍵配信サーバ４１が、メディア識別子ＩＤｍと及び古いユーザ鍵Ｋｕｏと共に更新要求を受け取ると（ＳＴ５１）、メディア識別子ＩＤｍを提示を伴うユーザ鍵Ｋｕの更新の履歴を、更新履歴データベース４５で参照する（ＳＴ５２）。なお、ユーザ鍵Ｋｕの更新要求がされるのは、ユーザ自らが更新手続を自発的に実行する場合の他、ライセンスセンタ等が有効期限を検知して、プログラムにより更新手続が自動的に実行される場合を含む。

参照の結果、所定期間内に更新がされていないと判定される場合には（ＳＴ５３のＮＯ）、新しいユーザ鍵Ｋｕｎを再発行（生成）し、最終的にＳＤカードＳＤｑの保護領域３に暗号化して書き込む（ＳＴ５４）。そして、図２では説明していないが、権利発行済みコンテンツＩＤデータベース４７において古いユーザ鍵Ｋｕｏにより暗号化され保存されているコンテンツ鍵Ｅｎｃ（Ｋｕｏ、Ｋｃｓｅｌｌｉ）に代えて、新しいユーザ鍵Ｋｕｎにより暗号化したコンテンツ鍵Ｅｎｃ（Ｋｕｎ、Ｋｃｓｅｌｌｉ）を生成する（ＳＴ５５、図５参照）。この暗号化したコンテンツ鍵Ｅｎｃ（Ｋｕｎ、Ｋｃｓｅｌｌｉ）は、例えば図２のＳＴ３９において、暗号化された新しいユーザ鍵Ｋｕｎ等と共にユーザ端末２０のＳＤカード処理部２３に送信される。

【００３０】

一方、ＳＴ５３において、所定期間内に更新がされていると判定される場合には、鍵配信サーバ４１は、既に同一のメディア識別子ＩＤｍによるユーザ鍵Ｋｕの更新がされているため、直ちにはユーザ鍵Ｋｕの更新は受付けられないという問題がある旨報告すると共に、ユーザ登録をしているユーザ（登録ユーザ）には、手持ちのＳＤカードを郵送するよう依頼する（ＳＴ５６）。郵送されたＳＤカードの処理については後述する。

【００３１】

上記の更新履歴データベース４５の参照ステップＳＴ３３について、図４とは別の詳細な手順を図６を参照して説明する。

ＳＴ５１′～ＳＴ５３′、ＳＴ５６′は、図４のＳＴ５１′～ＳＴ５３′、ＳＴ５６′と同様である。この図６の例では、ＳＴ５４′において、新しいユーザ鍵データＫｕｎを再発行するが、このとき、ユーザ鍵データＫｕ全体を書き換えるのではなく、鍵本体データＫｕｍは不変とし、その管理メタデータ（有効期限等のデータを含んでいる）のみを書き換える（図７、図８参照）。これにより、図４の手順の場合のように、古いユーザ鍵Ｋｕｏにより暗号化され保存されているコンテンツ鍵Ｅｎｃ（Ｋｕｏ、Ｋｃｓｅｌｌｉ）に代えて、新しいユーザ鍵Ｋｕｎにより暗号化したコンテンツ鍵Ｅｎｃ（Ｋｕｎ、Ｋｃｓｅｌｌｉ）を生成するという手順（ＳＴ５５）が不要となり、システムの負荷が軽減される。

【００３２】

（郵送されてきたＳＤカードに対する処理）

郵送されてきた登録ユーザのＳＤカードが偽造でなく正規のＳＤカードである場合には、別のメディア識別子を有する正規のＳＤカードを返送する。このように、ユーザ登録をしておくことにより、正規のＳＤカードの保持者は、偽造ＳＤカード保持者の存在に拘わらず、保護を受けることができる。

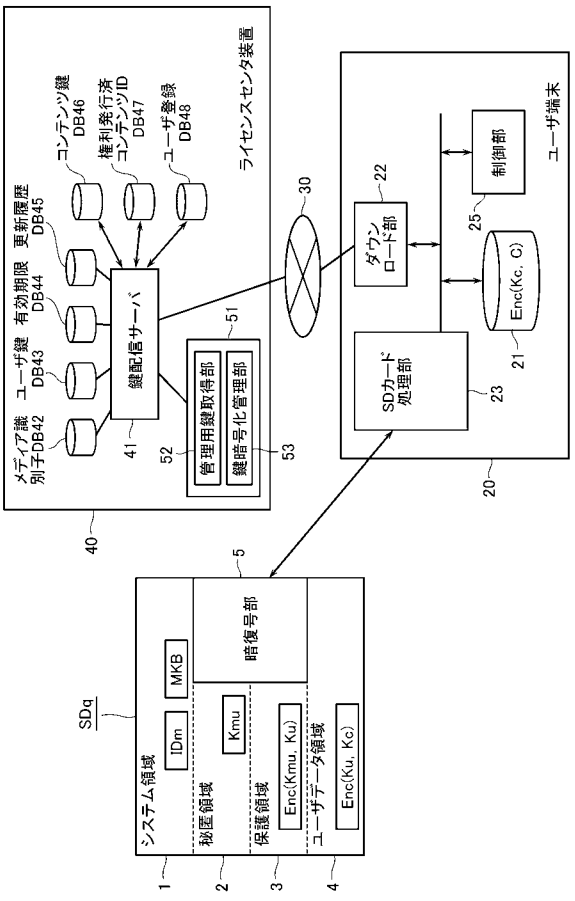
郵送されてきた登録ユーザのＳＤカードが偽造ＳＤカードである場合の処理について、図９のフローチャートを参照して説明する。

ランセンスセンタが、郵送されてきた偽造ＳＤカードを、その入手経路及び時期などの情報提供と共に受領した場合（ＳＴ６１）、ライセンスセンタは、その偽造ＳＤカードのユーザ鍵及びコンテンツ鍵を削除し（ＳＴ６２）、ユーザの実費負担において、正規ＳＤユーザカードを、新規ユーザ鍵、コンテンツ鍵を書き込んだ状態で新たに発行する（ＳＴ６３）。その新しい正規のＳＤカードのメディア識別子、ユーザ鍵、コンテンツ鍵は、データベース４２、４３及び４６に保存される（ＳＴ６４）。そして、この新しい正規ＳＤカードと、偽造ＳＤカードをユーザに返送する（ＳＴ６５）。偽造ＳＤカードは、各種鍵を削除されコンテンツ配信サービス（ＭＱｂｉｃサービス）を受けられなくなっている旨、ユーザに報告する。

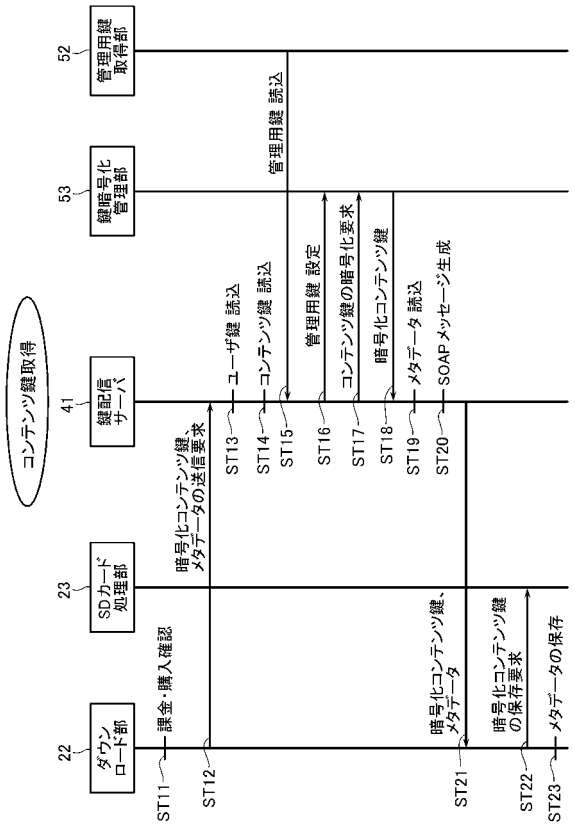
【００３３】
なお、上記各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。
また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。
また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。
【００３４】
さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。
また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。
尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。
また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。
【００３５】
また、上記の実施の形態では、ユーザ鍵の更新手順の際、更新要求において示されたメディア識別子による更新履歴を参照していたが、これに加えて、示されたメディア識別子をユーザ登録データベース４８で参照し、一致するユーザ登録が存在しないときはユーザ鍵の更新を拒否するようにしてもよい。
なお、本願発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。
【図面の簡単な説明】
【００３６】
【図１】本発明の実施形態に係る記憶媒体処理システムの構成を示す模式図である。
【図２】ＳＤカードＳＤｑがユーザ端末２０を介してコンテンツ鍵を取得する手順を説明している。
【図３】ユーザ鍵の更新の手順を説明している。
【図４】図３のＳＴ３３の詳細を、所定期間内に同一のメディア識別子ＩＤｍによる更新がなされていると判定される場合を含めて説明する。
【図５】図４に示す手順によりユーザ鍵の更新を行なった場合における更新前後のＳＤカードＳＤｑの保持データの変化の様子を示す。
【図６】図３のＳＴ３３の詳細の別の例を、所定期間内に同一のメディア識別子ＩＤｍによる更新がなされていると判定される場合を含めて説明する。
【図７】図６に示す手順によりユーザ鍵の更新を行なった場合における更新前後のＳＤカードＳＤｑの保持データの変化の様子を示す。
【図８】図６に示す手順によりユーザ鍵の更新を行なった場合における更新前後のユーザ鍵データＫｕの内容の変化を示す。
【図９】郵送されてきた登録ユーザのＳＤカードが偽造ＳＤカードである場合の処理を説

明するフローチャートである。
【図１０】ＭＱｂｉｃにおいて従来採用されている暗号化二重鍵方式に対応したＳＤカード及びユーザ端末の構成を示す模式図である。
【符号の説明】
【００３７】
ＳＤｑ・・・ＳＤカード、１・・・システム領域、　２・・・秘匿領域、　３・・・保護領域、　４・・・ユーザデータ領域、　５・・・暗復号部、　２０・・・ユーザ端末、　２１・・・メモリ、　２２・・・ダウンロード部、　２３・・・ＳＤカード処理部、　２５・・・制御部、　４０・・・ライセンスセンタ装置、　４１・・・鍵配信サーバ、　４２・・・メディア鍵データベース、　４３・・・ユーザ鍵データベース、　４４・・・有効期限データベース、　４５・・・更新履歴データベース、　４６・・・コンテンツ鍵データベース、　４７・・・権利発行済みコンテンツＩＤデータベース、　５１・・・セキュリティモジュール５１、　５２・・・管理用鍵取得部、５３・・・鍵暗号化管理部。

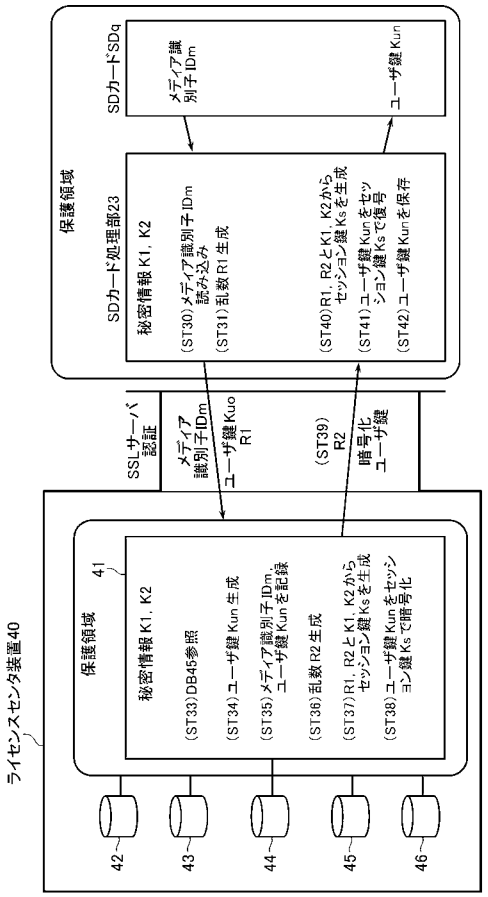
【図１】



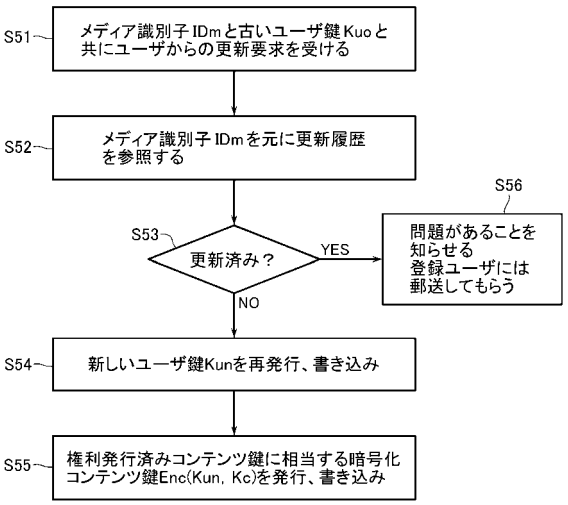
【図２】



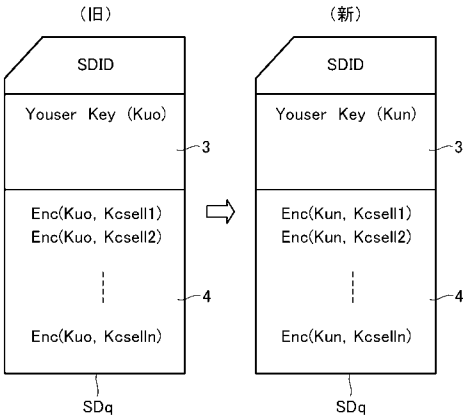
【図３】


SDカードSDq
メディア識別子IDm
ユーザ鍵Kun
保護領域
SDカード処理部23
秘密情報K1, K2
(ST30)メディア識別子IDm読み込み
(ST31)乱数R1生成
(ST40)R1, R2とK1, K2からセッション鍵Ksを生成
(ST41)ユーザ鍵Kunをセッション鍵Ksで復号
(ST42)ユーザ鍵Kunを保存
SSLサーバ認証
メディア識別子IDm
ユーザ鍵Kuo
R1
(ST39)
R2
暗号化ユーザ鍵
ライセンスセンタ装置40
保護領域
41
秘密情報K1, K2
(ST33)DB45参照
(ST34)ユーザ鍵Kun生成
(ST35)メディア識別子IDmとユーザ鍵Kunを記録
(ST36)乱数R2生成
(ST37)R1, R2とK1, K2からセッション鍵Ksを生成
(ST38)ユーザ鍵Kunをセッション鍵Ksで暗号化
42
43
44
45
46

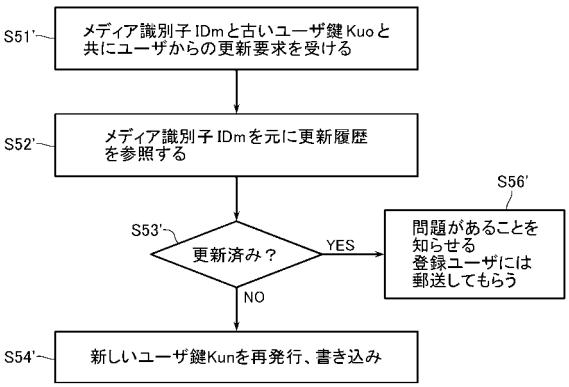
【図４】


S51
メディア識別子IDmと古いユーザ鍵Kuoと共にユーザからの更新要求を受ける
S52
メディア識別子IDmを元に更新履歴を参照する
S53
更新済み？
YES
NO
S56
問題があることを知らせる
登録ユーザには郵送してもらう
S54
新しいユーザ鍵Kunを再発行、書き込み
S55
権利発行済みコンテンツ鍵に相当する暗号化コンテンツ鍵Enc(Kun, Kc)を発行、書き込み

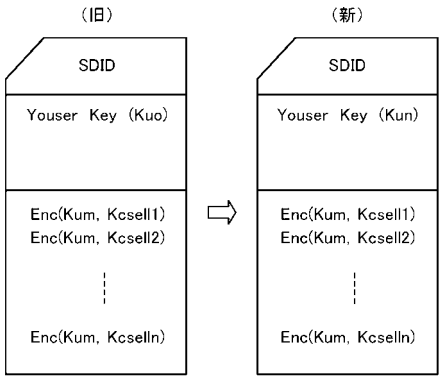
【図５】


(旧)
(新)
SDID
Youser Key (Kuo)
Youser Key (Kun)
3
Enc(Kuo, Kcsel1)
Enc(Kuo, Kcsel2)
Enc(Kuo, Kcseln)
4
Enc(Kun, Kcsel1)
Enc(Kun, Kcsel2)
Enc(Kun, Kcseln)
SDq

【図６】


S51'
メディア識別子IDmと古いユーザ鍵Kuoと共にユーザからの更新要求を受ける
S52'
メディア識別子IDmを元に更新履歴を参照する
S53'
更新済み？
YES
NO
S56'
問題があることを知らせる
登録ユーザには郵送してもらう
S54'
新しいユーザ鍵Kunを再発行、書き込み

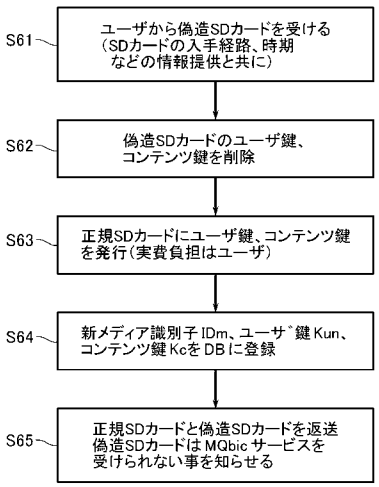
【図７】


(旧)
(新)
SDID
Youser Key (Kuo)
Youser Key (Kun)
Enc(Kum, Kcsel1)
Enc(Kum, Kcsel2)
Enc(Kum, Kcseln)

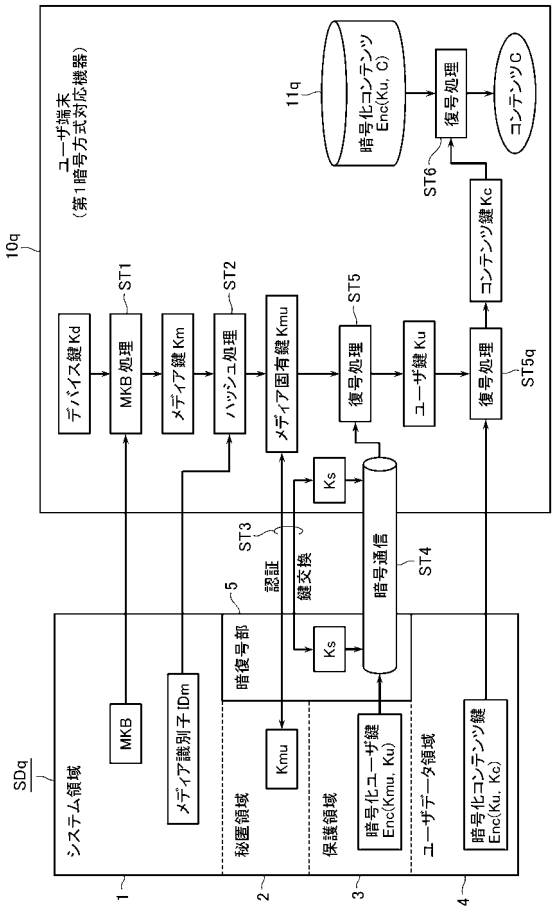
【図８】


Kun：新ユーザ鍵
鍵本体：Kum
新管理メタデータ（新有効期限）
Kuo：旧ユーザ鍵
鍵本体：Kum
旧管理メタデータ（旧有効期限）

【図９】


S61
ユーザから偽造SDカードを受ける
（SDカードの入手経路、時期
などの情報提供と共に）
S62
偽造SDカードのユーザ鍵、
コンテンツ鍵を削除
S63
正規SDカードにユーザ鍵、コンテンツ鍵
を発行（実費負担はユーザ）
S64
新メディア識別子IDm、ユーザ゛鍵Kun、
コンテンツ鍵KcをDBに登録
S65
正規SDカードと偽造SDカードを返送
偽造SDカードはMQbicサービスを
受けられない事を知らせる

【図１０】


10q
ユーザ端末
（第1暗号方式対応機器）
11q
暗号化コンテンツ
Enc(Ku, C)
復号処理
コンテンツC
ST6
コンテンツ鍵Kc
デバイス鍵Kd
MKB処理
ST1
メディア鍵Km
ハッシュ処理
ST2
メディア固有鍵Kmu
復号処理
ST5
ユーザ鍵Ku
復号処理
ST5q
Ks
ST3
認証
鍵交換
暗号通信
ST4
5
暗復号部
Ks
SDq
システム領域
MKB
メディア識別子IDm
秘匿領域
Kmu
保護領域
暗号化ユーザ鍵
Enc(Kmu, Ku)
ユーザデータ領域
暗号化コンテンツ鍵
Enc(Ku, Kc)
1
2
3
4

フロントページの続き

審査官　青木　重徳

(56)参考文献　特開２００２－２４５０１３（ＪＰ，Ａ）
特開２００３－０６９５５１（ＪＰ，Ａ）
特開２００３－２１６５００（ＪＰ，Ａ）
特開２００４－０３８２４７（ＪＰ，Ａ）
特開２０００－２９３４３９（ＪＰ，Ａ）
特開平１１－２２４４６１（ＪＰ，Ａ）
特開平１１－０９６６７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／１０
Ｈ０４Ｌ　　９／３２