(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-14035
(P2006-14035A)
(43)公開日　平成18年1月12日(2006.1.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/10	(2006.01)	H04L	9/00	621A	5B017
G06F 21/24	(2006.01)	G06F	12/14	520D	5B035
G06F 21/00	(2006.01)	G06F	12/14	540C	5B058
G06Q 50/00	(2006.01)	G06F	15/00	330Z	5B085
G06Q 30/00	(2006.01)	G06F	17/60	142	5J104

審査請求 未請求　請求項の数 11　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願2004-189839 (P2004-189839)
(22)出願日　平成16年6月28日 (2004.6.28)

(71)出願人　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

Ｆターム(参考)　5B017 AA07　BA07　CA14

最終頁に続く

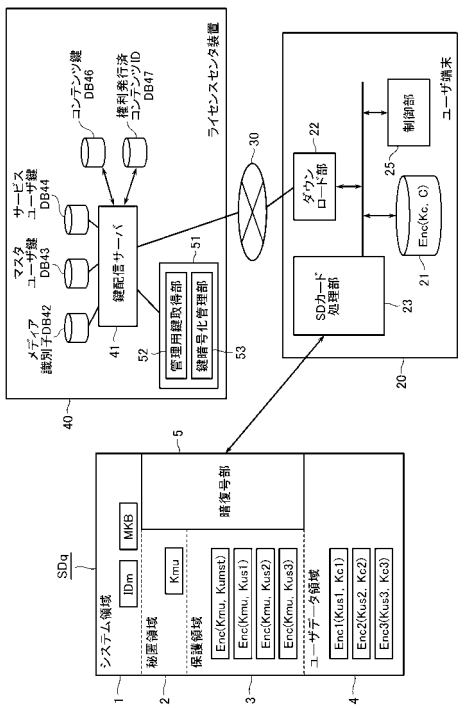
(54)【発明の名称】記憶媒体処理方法、記憶媒体処理装置及びプログラム

(57)【要約】

【課題】　ユーザ鍵により、サービスの種別ごとにきめ細かく異なるユーザの管理が可能になる。

【解決手段】　ＳＤカードＳＤｑは、サービスの種類によって異なるサービスユーザ鍵Ｋｕｓを、複数種類格納し得る。サービスユーザ鍵Ｋｕｓは、メディア固有鍵Ｋｍｕにより暗号化され、保護領域３に格納されている。保護領域３には、このサービスユーザ鍵Ｋｕｓ以外に、マスタユーザ鍵Ｋｕｍｓｔが、メディア固有鍵Ｋｍｕにより暗号化されて格納されている。マスタユーザ鍵Ｋｕｍｓｔは、サービスユーザ鍵Ｋｕｓを取得する場合に、サービスユーザ鍵Ｋｕｓを暗号化するために用いられる鍵である。

【選択図】　図１



【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ユーザ鍵データの発行を要求するステップと、
前記ライセンスセンタが、前記ユーザ端末の要求に応じて、前記ユーザ端末が提供を希望するサービスの種別及び前記媒体識別子データにより異なるユーザ鍵データを生成し前記ユーザ端末に配信するステップと、
前記ユーザ鍵データを前記ライセンスセンタにおいてデータベースに記録するステップと、
前記ユーザ端末において、配信された前記ユーザ鍵データを、前記媒体固有鍵データで暗号化して前記記憶媒体に記憶させるステップと
を備えたことを特徴とする記憶媒体処理方法。
【請求項２】
前記ユーザ鍵データを前記ユーザ端末に配信するステップは、配信済みの特定のユーザ鍵データにより生成したユーザ鍵データを暗号化し配信するものである請求項１記載の記憶媒体処理方法。
【請求項３】
前記特定のユーザ鍵データは、他のユーザ鍵データを暗号化するのに用いられると共に、特定のサービスに関するコンテンツ鍵データの暗号化のためにも使用される請求項２記載の記憶媒体処理方法。
【請求項４】
前記特定のユーザ鍵データは、他のユーザ鍵データを暗号化するためだけに用いられる請求項２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記憶媒体処理装置において、
前記媒体識別子データの提示を伴う前記ユーザ端末からの要求に応じて、前記ユーザ端末が提供を希望するサービスの種類毎に異なるユーザ鍵データを生成して前記ユーザ端末に配信する鍵配信サーバと、
前記鍵配信サーバで生成された前記ユーザ鍵データを格納するユーザ鍵データベースと
を備えたことを特徴とする記憶媒体処理装置。
【請求項６】
前記鍵配信サーバは、共通鍵暗号方式に用いる秘密鍵データを前記ユーザ端末と共有しており、前記ユーザ鍵データのうち特定のユーザ鍵データは、前記秘密鍵データにより暗号化される一方、
その他の前記ユーザ鍵データは、この特定のユーザ鍵データにより暗号化され、前記ユ

ーザ端末に配信される
ことを特徴とする、請求項５記載の記憶媒体処理装置。
【請求項７】
前記特定のユーザ鍵データは、その他の前記ユーザ鍵データを暗号化するために用いられると共に、特定のサービスに関するコンテンツ鍵データの暗号化のためにも使用される請求項６記載の記憶媒体処理装置。
【請求項８】
前記特定のユーザ鍵データは、他のユーザ鍵データを暗号化するためだけに用いられる請求項６記載の記憶媒体処理装置。
【請求項９】
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す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、
前記ユーザ端末が、前記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ユーザ鍵データの発行を要求するステップと、
前記ライセンスセンタが、前記ユーザ端末の要求に応じて、前記ユーザ端末が提供を希望するサービスの種別及び前記媒体識別子データにより異なるユーザ鍵データを生成し前記ユーザ端末に配信するステップと、
前記ユーザ鍵データを前記ライセンスセンタにおいてデータベースに記録するステップと、
前記ユーザ端末において、配信された前記ユーザ鍵データを、前記媒体固有鍵データで暗号化して前記記憶媒体に記憶させるステップと
を実行可能なように構成された記憶媒体処理プログラム。
【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に接続可能とされ、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において、
希望するサービスの種別に関するデータ及び前記媒体識別子データをライセンスセンタに提示してユーザ鍵データの発行要求を送信すると共に前記サービスの種別及び前記媒体識別子データにより異なるユーザ鍵データを受信する送受信部と、
受信した前記ユーザ鍵データを、前記媒体固有鍵データで暗号化して前記記憶媒体に記憶させる記憶媒体処理部と
を備えたことを特徴とするユーザ端末。
【請求項１１】
共通鍵暗号方式に用いる秘密鍵データを前記ライセンスセンタと共有しており、
前記送受信部は、前記ユーザ鍵データのうち特定のユーザ鍵データを、この秘密鍵データで暗号化した形式で受信し、前記秘密鍵データによりこれを復号化する一方、その他の前記ユーザ鍵データを、前記特定のユーザ鍵データで暗号化した形式で受信し、前記特定のユーザ鍵データによりこれを復号化する
ように構成されたことを特徴とする、請求項１０記載のユーザ端末。

【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９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。
【０００４】
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。
【０００５】
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。
【０００６】
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（Ｓ

１）、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（Ｓ２）、メディア固有鍵Ｋｍｕを得る。

【０００７】

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（Ｓ３）、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Ｓ３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（Ｓ４）、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（Ｓ５）、ユーザ鍵Ｋｕを得る。

【０００８】

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（Ｓ５ｑ）、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（Ｓ６）、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。

【０００９】

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。

【００１０】

【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】

【００１１】

上述のように、ユーザ鍵Ｋｕは、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。

ところで、このようなコンテンツ流通システムが普及し、サービスを提供する企業の数が増加し、サービスの種類及び形式等も豊富になった場合、このような単一のユーザ鍵では、十分な対応が難しくなることが予想される。例えば、コンテンツのレンタルを行なおうと考えた場合、コンテンツの貸出し期限や貸出し本数等を管理する必要がある他、ユー

ザの会員資格も管理する必要がある。また、このような管理手法は、サービスを提供する企業毎に異なることが予想される。

しかし、従来のシステムは、ユーザ鍵が１つしかなく、この１つのユーザ鍵では、こうしたサービスの多様化に対応したユーザの適切な管理が難しくなることが予想される。

【課題を解決するための手段】

【００１２】

この発明に係る記憶媒体処理方法は、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、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ユーザ鍵データの発行を要求するステップと、前記ライセンスセンタが、前記ユーザ端末の要求に応じて、前記ユーザ端末が提供を希望するサービスの種別及び前記媒体識別子データにより異なるユーザ鍵データを生成し前記ユーザ端末に配信するステップと、前記ユーザ鍵データを前記ライセンスセンタにおいてデータベースに記録するステップと、前記ユーザ端末において、配信された前記ユーザ鍵データを、前記媒体固有鍵データで暗号化して前記記憶媒体に記憶させるステップとを備えたことを特徴とする。

【００１３】

この発明に係る記憶媒体処理装置は、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記憶媒体処理装置において、前記媒体識別子データの提示を伴う前記ユーザ端末からの要求に応じて、前記ユーザ端末が提供を希望するサービスの種類毎に異なるユーザ鍵データを生成して前記ユーザ端末に配信する鍵配信サーバと、前記鍵配信サーバで生成された前記ユーザ鍵データを格納するユーザ鍵データベースとを備えたことを特徴とする。

【００１４】

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、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す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、前記ユーザ端末が、前記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ユーザ鍵データの発行を要求するステップと、前記ライセンスセンタが、前記ユーザ端末の要求に応じて、前記ユーザ端末が提供を希望するサービスの種別及び前記媒体識別子データにより異なるユーザ鍵データを生成し前記ユーザ端末に配信するステップと、前記ユーザ鍵データを前記ライセンスセンタにおいてデータベースに記録するステップと、前記ユーザ端末において、配信された前記ユーザ鍵データを、前記媒体固有鍵データで暗号化して前記記憶媒体に記憶させるステップとを実行可能なように構成されたことを特徴とする。

また、この発明に係るユーザ端末は、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に接続可能とされ、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において、希望するサービスの種別に関するデータ及び前記媒体識別子データをライセンスセンタに提示してユーザ鍵データの発行要求を送信すると共に前記サービスの種別及び前記媒体識別子データにより異なるユーザ鍵データを受信する送受信部と、受信した前記ユーザ鍵データを、前記媒体固有鍵データで暗号化して前記記憶媒体に記憶させる記憶媒体処理部とを備えたことを特徴とする。

【発明の効果】

【００１５】

この発明によれば、ユーザ端末の要求に応じて、ユーザ端末が提供を希望するサービスの種別及び前記媒体識別子データにより異なるユーザ鍵データが生成され、ユーザ端末に配信される。生成されたユーザ鍵データは、データベースに記録される。また、ユーザ端末において、配信されたユーザ鍵データを、媒体固有鍵データで暗号化して前記記憶媒体に記憶させる。すなわち、この発明によれば、サービスの種別ごとに異なるユーザ鍵データが生成されるので、ユーザ鍵データにより、サービスの種別ごとにきめ細かく異なるユーザの管理が可能になる。ここで、「サービスの種別」とは、サービスの主体（業者等）、対象（コンテンツの内容等）又は手続その他の諸性質等が何らかの意味で異なっているという程度の意味に使用される。

【発明を実施するための最良の形態】

【００１６】

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９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。

【００１７】

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。

このＳＤカードＳＤｑでは、サービスの種類によって異なるユーザ鍵（以下では、サービスユーザ鍵という）Ｋｕｓが、複数種類格納され得る。この例では、３種類のサービスユーザ鍵Ｋｕｓ１、Ｋｕｓ２、Ｋｕｓ３により、それぞれコンテンツ鍵Ｋｃ１、Ｋｃ２、Ｋｃ３が暗号化されているものとする。各サービスユーザ鍵Ｋｕｓは、それぞれメタデータを保持しており、メタデータに、例えば鍵の有効期限等のデータを含ませることができる。

【００１８】

また、この複数種類のサービスユーザ鍵Ｋｕｓは、メディア固有鍵Ｋｍｕにより暗号化され、保護領域３に格納されている。保護領域３には、このサービスユーザ鍵Ｋｕｓ以外に、別のユーザ鍵Ｋｕｍｓｔが、メディア固有鍵Ｋｍｕにより暗号化されて格納されている。このユーザ鍵Ｋｕｍｓｔ（以下、「マスタユーザ鍵」と称する）は、サービスユーザ鍵Ｋｕｓをライセンスセンタ装置４０から取得する場合に、サービスユーザ鍵Ｋｕｓを暗号化するために用いられる鍵である。このマスタユーザ鍵Ｋｕｍｓｔは、サービスユーザ鍵Ｋｕｓを暗号化する機能のみを与えられていてもよいし、また、この機能に加え、サービスユーザ鍵Ｋｕｓと同様、コンテンツ鍵を暗号化するユーザ鍵としての一般的な機能を兼用するものであってもよい。

【００１９】

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）等のように、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のデバ

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／書込可能な記憶領域であり、例えば暗号化コンテンツＥｎｃ（Ｋｃ、Ｃ）が記憶される。
【００２０】
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）やユーザ鍵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。
【００２１】
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、マスタユーザ鍵データベース４３、サービスユーザ鍵データベース４４、コンテンツ鍵データベース４６、及び権利発行済みコンテンツＩＤデータベース４７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を介してユーザ鍵配信要求を受けた場合、データベース４２等にアクセスし、要求に係るユーザ鍵データを生成すると共に、その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。
【００２２】
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。マスタユーザ鍵データベース４３は、各ＳＤカードが有するマスタユーザ鍵Ｋｕｍｓｔのデータを保存するためのものである。
サービスユーザ鍵データベース４４は、ＳＤカードが有するサービスユーザ鍵Ｋｕｓのデータを保存するためのものである。
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。
【００２３】
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。管理用鍵取得部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。
【００２４】
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４を用いて説明する。上記のように、各ＳＤカードＳＤｑが、マスタユーザ鍵Ｋｕｍｓｔと、サービスの種別ごとに異なるサービスユーザ鍵Ｋｕｓを備えたシステムにおいては、各ＳＤカードＳＤｑは、まずマスタユーザ鍵Ｋｕｍｓｔを取得し、次いで所望のサービスに対応するサービスユーザ鍵Ｋｕｓを取得し、その後このサービスユーザ鍵Ｋｕｓを利用して、コンテンツ鍵Ｋｃを取得する。
【００２５】
（マスタユーザ鍵Ｋｕｍｓｔの取得）
まず、ＳＤカードＳＤｑがユーザ端末２０を介してライセンスセンタ装置４０にアクセ

スしてマスタユーザ鍵Ｋｕｍｓｔ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、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（Ｓ１１）、乱数Ｒ１を生成する（Ｓ１２）。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Ｋｓの生成のために発生されるものである。

【００２６】

続いて、ダウンロード部２２は、マスタユーザ鍵Ｋｕｍｓｔの取得要求を鍵配信サーバ４１に送信する（Ｓ１３）。この取得要求は、ＳＤカードＳＤｑのメディア識別子ＩＤｍと、生成した乱数Ｒ１とを含む。

【００２７】

鍵配信サーバ４１は、この取得要求を受けて、所定の認証手順等を経た後、マスタユーザ鍵Ｋｕｍｓｔを生成する（Ｓ１４）。そして、このマスタユーザ鍵Ｋｕｍｓｔのデータを、メディア識別子ＩＤｍと対応付けてマスタユーザ鍵データベース４３に格納する（Ｓ１５）。続いて、鍵配信サーバ４１は、乱数Ｒ２を発生させる（Ｓ１６）。この乱数Ｒ２は、乱数Ｒ１と同様、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Ｋｓの生成のために発生されるものである。

【００２８】

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（Ｓ１７）。鍵配信サーバ４１は、セキュリティモジュール５１を用いて、この生成されたセッション鍵Ｋｓで、生成したマスタユーザ鍵Ｋｕｍｓｔを暗号化し（Ｓ１８）、ＳＯＡＰメッセージにより暗号化されたマスタユーザ鍵Ｋｕｍｓｔのデータを乱数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（Ｓ１９）。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（Ｓ２０）、暗号化されたマスタユーザ鍵Ｋｕｍｓｔをセッション鍵Ｋｓで復号する（Ｓ２１）。この復号化されたユーザ鍵Ｋｕｍｓｔ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３に書き込まれる（Ｓ２２）。これにより、マスタユーザ鍵Ｋｕｍｓｔの取得処理を終了する。

【００２９】

（サービスユーザ鍵Ｋｕｓの取得処理）

次に、ＳＤカードＳＤｑがユーザ端末２０を介してライセンスセンタ装置４０にアクセスしてサービスユーザ鍵Ｋｕｓを取得する手順について、図３を参照して説明する。ユーザ端末２０におけるユーザの操作により、制御部２５がダウンロード部２２を起動すると、ダウンロード部２２は、メディア識別子ＩＤｍをＳＤカードＳＤｑのシステム領域１から読み込んで（Ｓ３０）、その後、このメディア識別子ＩＤｍ及び取得したいサービスユーザ鍵Ｋｕｓに対応するサービスＩＤを含んだサービスユーザ鍵取得要求を鍵配信サーバ４１に送信する（Ｓ３１）。

【００３０】

鍵配信サーバ４１は、この取得要求を受けると、予めメディア識別子ＩＤｍ毎に記憶された管理用のマスタユーザ鍵Ｋｕｍｓｔ（要求元のＳＤカードＳＤｑにおいて取得済みのマスタユーザ鍵Ｋｕｍｓｔ）をマスタユーザ鍵データベース４３から読み込むと共に（Ｓ３２）、予めサービスＩＤ毎に記憶された管理用の暗号化サービスユーザ鍵Ｋｕｓをサービスユーザ鍵データベース４４から読み込んで取得する（Ｓ３３）。なお、要求元のＳＤカードＳＤｑにおいてマスタユーザ鍵Ｋｕｍｓｔの取得処理が済んでおらず、マスタユーザ鍵データベース４３に、そのカードＳＤｑが有するメディア識別子ＩＤｍに対応するマスタユーザ鍵Ｋｕｍｓｔがマスタユーザ鍵データベース４３に格納されていない場合には、その旨のメッセージを返信して、サービスユーザ鍵Ｋｕｓの取得の前にマスタユーザ鍵

Ｋｕｍｓｔの取得を行なうことを促す。

【００３１】

鍵配信サーバ４１は、このサービスユーザ鍵Ｋｕｓをメディア識別子ＩＤｍと対応付けてサービスユーザ鍵データベース４４に格納すると共に、マスタユーザ鍵Ｋｕｍｓｔで暗号化し（Ｓ３４）、ＳＯＡＰ(Simple Object Access Protocol)メッセージによりユーザ端末２０に送信する（Ｓ３５）。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。

【００３２】

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、暗号化されたサービスユーザ鍵ＫｕｓをＳＤカード処理部２３に送出する。ＳＤカード処理部２３は、この暗号化されたサービスユーザ鍵Ｋｕｓを、保護領域３に格納されたマスタユーザ鍵Ｋｕｍｓｔで復号する（Ｓ３６）。そして、この復号されたサービスユーザ鍵Ｋｕｓを、再びＳＤカードＳＤｑが有するメディア固有鍵Ｋｍｕにより暗号化して、保護領域３に格納する（Ｓ３７）。これにより、サービスユーザ鍵Ｋｕｓの取得処理が完了する。前述のようにこのサービスユーザ鍵Ｋｕｓは、サービスの種類ごとに用意されるものである。例えばサービスユーザ鍵Ｋｕｓ１はコンテンツ販売（売り切り）用のものであり、サービスユーザ鍵Ｋｕｓ２はコンテンツのレンタル用のものである場合には、両者にはそれぞれ別のサービスＩＤが与えられている。従って、それぞれのサービスユーザ鍵Ｋｕｓ１、Ｋｕｓ２を取得するには、それぞれのサービスＩＤを提示して上記の手順を実行する必要がある。

【００３３】

また、本実施の形態では、共通鍵暗号化方式を用いたチャレンジ・レスポンス（乱数Ｒ１、Ｒ２及び秘密情報Ｋ１、Ｋ２を用いている）による鍵の送信は、マスタユーザ鍵Ｋｕｍｓｔの送信の際の１回だけに限られ、サービスユーザ鍵Ｋｕｓの送信の際には、チャレンジ・レスポンスは実行されない。これにより、通信のセキュリティレベルを高く保ったまま、通信の速度を向上させることができる。

【００３４】

（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Ｋｃを取得する手順について、図４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、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（Ｓ４１）。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、暗号化コンテンツ鍵Ｋｃのデータの取得要求を鍵配信サーバ４１に送信する（Ｓ４２）。この例では、取得要求には、メディア識別子ＩＤｍのデータ、希望するサービスを示すサービスＩＤ、及び取得を要求するコンテンツ鍵Ｋｃのコンテンツ ＩＤが含まれるものとする。

【００３５】

鍵配信サーバ４１は、この取得要求を受けると、予めメディア識別子ＩＤｍ毎に記憶された管理用の暗号化マスタユーザ鍵及び暗号化サービスユーザ鍵を、それぞれマスタユーザ鍵データベース４３及びサービスユーザ鍵データベース４４から読み込む（Ｓ４３）。そして、指定されたコンテンツＩＤに係る管理用の暗号化コンテンツ鍵Ｋｃ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（Ｓ４４）。

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（Ｓ４５）、この管理用鍵を鍵暗号化管理部５３に設定し（Ｓ４６）、コンテンツ鍵Ｋｃの暗号化要求を鍵暗号化管理部５３に送信する（Ｓ４７）。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。

【００３６】

鍵暗号化管理部５３は、管理用鍵に基づいて、管理用の暗号化コンテンツ鍵を復号し、コンテンツ鍵Ｋｃを得る（Ｓ４８）。しかる後、鍵暗号化管理部５３は、コンテンツ鍵Ｋｃと基本メタデータとをサービスユーザ鍵Ｋｕｓで暗号化し、得られた暗号化コンテンツ鍵Ｋｃ（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（Ｓ４８）。

鍵配信サーバ４１は、付加メタデータを読み込むと（Ｓ４９）、暗号化コンテンツ鍵Ｋｃ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（Ｓ５０）、ＳＯＡＰメッセージにより暗号化コンテンツ鍵Ｋｃ及びメタデータをユーザ端末２０に送信する（Ｓ５１）。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。

【００３７】

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Ｋｃの保存要求をＳＤカード処理部２３に送出する（Ｓ５２）。なお、暗号化コンテンツ鍵Ｋｃの保存要求は、暗号化コンテンツ鍵Ｋｃ及びメタデータのうち、暗号化コンテンツ鍵Ｋｃ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ＫｃをＳＤカードＳＤｑのユーザデータ領域４に書き込む。

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（Ｓ５３）。これにより、コンテンツ鍵Ｋｃの取得処理を終了する。このコンテンツ鍵Ｋｃは、取得要求時に提示したサービスユーザ鍵Ｋｕｓによってのみ復号化することができる。

【００３８】

上記のように、本実施の形態は、一枚のＳＤカードＳＤｑが、サービスの種別等によって異なる複数のサービスユーザ鍵Ｋｕｓを保有可能にしたものである。その形態の例を以下に図５～図８を参照して説明する。

図５の例は、１枚のＳＤカードＳＤｑが、提供されるコンテンツの種類毎に異なるサービスユーザ鍵Ｋｕｓ１～Ｋｕｓ４を保有するようにしたものである。いずれのサービスユーザ鍵Ｋｕｓも、その取得の際にはマスタユーザ鍵Ｋｕｍｓｔにより暗号化されてライセンスセンタ装置４０からユーザ端末２０へ送信される。

【００３９】

図６の例は、１枚のＳＤカードＳＤｑが、コンテンツ配信業者（業者Ａ，Ｂ）、及びその配信形態（販売、レンタル）の違いごとに、異なる複数のサービスユーザ鍵Ｋｕｓ１～Ｋｕｓ４を保有するようにしたものである。業者毎にサービスユーザ鍵を異ならせることにより、各業者がサービスユーザ鍵ベースで、ユーザの会員資格等の管理を独自に行なうことができる。例えば、業者Ａと業者Ｂとで会員条件が異なる場合、各業者はこれを独自にそれぞれのサービスユーザ鍵のメタデータに含ませることができる。

また、販売用とレンタル用とで別個にサービスユーザ鍵を準備することにより、コンテンツの貸出し期限、有効期限等をサービスユーザ鍵Ｋｕｓ１～Ｋｕｓ４毎に独自に設定することができる。例えば、販売用のサービスユーザ鍵とレンタル用のサービスユーザ鍵とで、有効期限を異ならせることにより、レンタル会員資格の見直し期間を、サービスユーザ鍵ベースで適正に設定することができる。

図７は、配信業者、配信形態の違いに加え、さらにコンテンツの種類の組合せの違い毎に異なるサービスユーザ鍵を発行するようにした例を示している。

【００４０】

図８は、ファミリーカード登録された複数のＳＤカードＳＤｑ（１～４）の所有者のうちのいずれか一人がコンテンツ鍵Ｋｃ取得した場合、他のファミリーカードの所有者がこれを共有することができるシステムを示している。ここで、ファミリカードとは、家族等特定の関係にある複数人がそれぞれカードを所有することにより、割引等の恩恵を受けることができるようにしたシステムを意味する。

【００４１】

例えば、図８に示すように、ＳＤカードＳＤｑ１の所有者が、サービスユーザ鍵Ｋｕｓ

１－１に基づいてコンテンツ鍵Ｋｃ１を取得したとする。この場合、そのコンテンツ鍵Ｋｃ１は、他のファミリーカードＳＤｑ２～４の所有者が共有することができる（図８）。各ファミリーカードＳＤｑ１～４は、同一のサービスについて、それぞれ異なるサービスユーザ鍵Ｋｕｓ－１～４を有している。しかし、それぞれのサービスユーザ鍵Ｋｕｓ－１～４は、ファミリーカードであることを示すため、同一のファミリーカードＩＤを備えている。このファミリカードＩＤを備えていることにより、ファミリカードＳＤｑ２～４の所有者がそのコンテンツ鍵Ｋｃ１に係るコンテンツＩＤと、そのファミリカードＩＤとを提示してコンテンツ鍵Ｋｃ１の取得要求をライセンスセンタ装置４０に送信した場合、課金無しでそのコンテンツ鍵Ｋｃ１を受信することができる。

【００４２】

このようにファミリカードとして登録された複数のＳＤカード間において、ＳＤカードが挿入されているユーザ端末２０の種類に応じて、コンテンツ鍵が共有されるＳＤカードの範囲を決定するようにしてもよい。例えば、図８に示すように、ＳＤカードＳＤｑ１がデスクトップパソコンに、ＳＤカードＳＤｑ２がノートパソコンに、ＳＤカードＳＤｑ３がＤＶＤレコーダに、ＳＤカードＳＤ４がポータブルオーディオプレイヤにそれぞれ挿入されている場合を考える。この場合、音楽のコンテンツ鍵（Ｋｃ１）は全てのＳＤカードに共有されるようにすることができる。一方、映像のコンテンツ鍵（Ｋｃ２）はオーディオ専用機であるポータブルオーディオプレイヤに挿入されたＳＤカードＳＤｑ４以外のＳＤカード間で共有されるようにすることができる。また、ゲームのコンテンツ鍵（Ｋｃ３）はコンピュータ機器に挿入されたＳＤカードＳＤｑ１、ＳＤｑ２のみにより共有されるようにすることができる。このような処理は、例えば鍵配信サーバ４１側でファミリカードＩＤやマスタユーザ鍵Ｋｕｍｓｔ等をチェックすることにより行なうことができる。ユーザ端末２０側において、そのユーザ端末の特性に応じたコンテンツ鍵のみがダウンロードできるように、ＳＤカード処理部２３等が設定されているようにすることでも対応可能である。

【００４３】

また、コンテンツのジャンルにより、コンテンツ鍵が共有されるＳＤカードの範囲が決定されるようにしてもよい。例えば、映画のコンテンツ鍵において、その映画が特定のジャンル（バイオレンス系、Ｒ指定等）に属する場合、そのコンテンツ鍵は、特定のＳＤカード（例えば、子供が持つＳＤカード）では共有されないようにすることができる。このような処理も、鍵配信サーバ４１側でファミリカードＩＤやマスタユーザ鍵Ｋｕｍｓｔ等をチェックすることにより行なうことができる。又は、ＳＤカード処理部２３自体が、そのようなコンテンツ鍵をダウンロードできないように設定されていてもよい。

【００４４】

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。

【００４５】

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。

【００４６】

また、上記の実施の形態では、各ＳＤカードＳＤｑがマスタユーザ鍵Ｋｕｍｓｔをチャレンジ・レスポンスを用いた共通鍵暗号化方式により取得し、その後このマスタユーザ鍵Ｋｕｍｓｔを用いた暗号化により、サービスユーザ鍵Ｋｕｓを取得するようにしていた。しかし、本発明はこれに限らず、例えばメディア識別子ＩＤｍ等から直接サービスユーザ鍵Ｋｕｓを取得し、サービスユーザ鍵Ｋｕｓの送信には、逐一チャレンジ・レスポンスによる共通暗号化方式を使用する必要があるが、マスタユーザ鍵を発行する手順を省略することができる。サービスユーザ鍵の種類が少ない場合や、サービスユーザ鍵の有効期限が長いような場合には、この方式が有効である。

【００４７】

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】

【００４８】

【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】マスタユーザ鍵Ｋｕｍｓｔの取得手順を説明する。

【図３】サービスユーザ鍵Ｋｕｓの取得手順を説明する。

【図４】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５】一枚のＳＤカードＳＤｑが、複数のサービスユーザ鍵Ｋｕｓを保有可能にした形態の一例を説明する。

【図６】一枚のＳＤカードＳＤｑが、複数のサービスユーザ鍵Ｋｕｓを保有可能にした形態の一例を説明する。

【図７】一枚のＳＤカードＳＤｑが、複数のサービスユーザ鍵Ｋｕｓを保有可能にした形態の一例を説明する。

【図８】一枚のＳＤカードＳＤｑが、複数のサービスユーザ鍵Ｋｕｓを保有可能にした形態の一例を説明する。

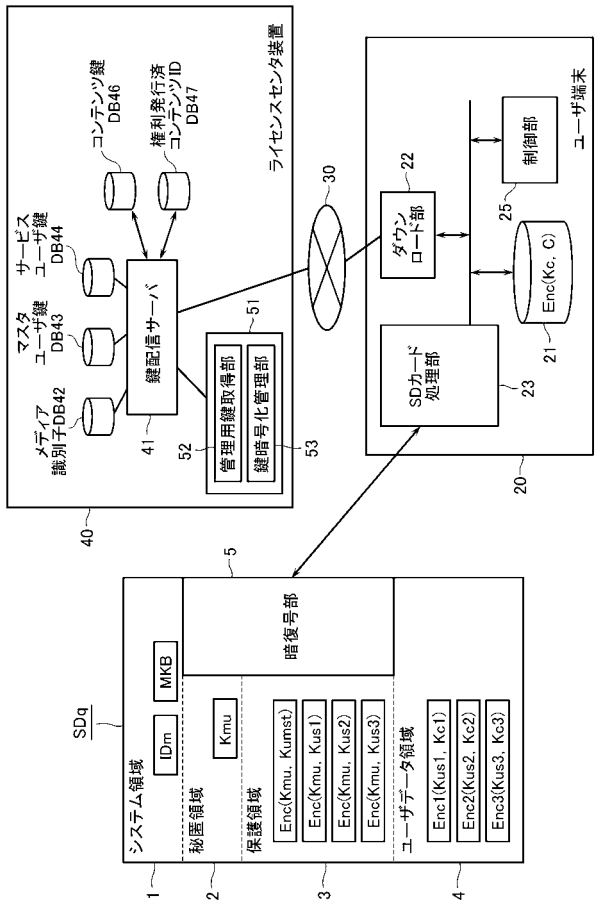
【図９】ＭＱｂｉｃにおいて従来採用されている暗号化二重鍵方式に対応したＳＤカード及びユーザ端末の構成を示す模式図である。

【符号の説明】

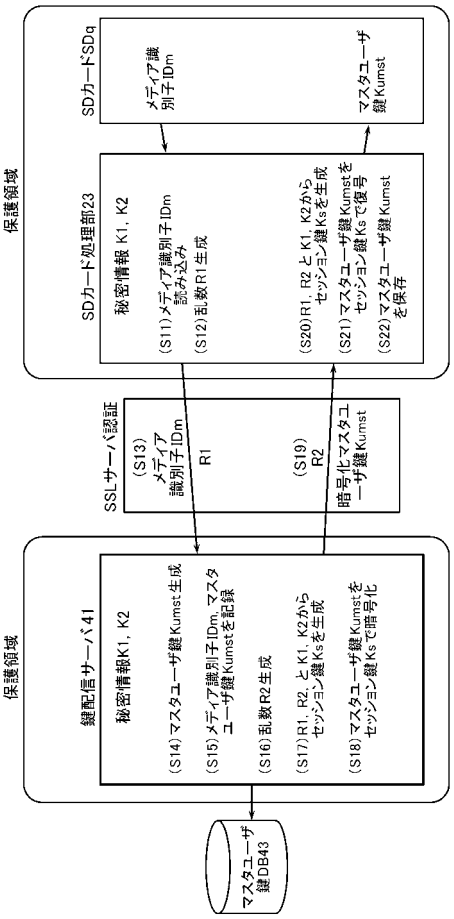
【００４９】

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・・・マスタユーザ鍵データベース、４４・・・サービスユーザ鍵データベース、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。

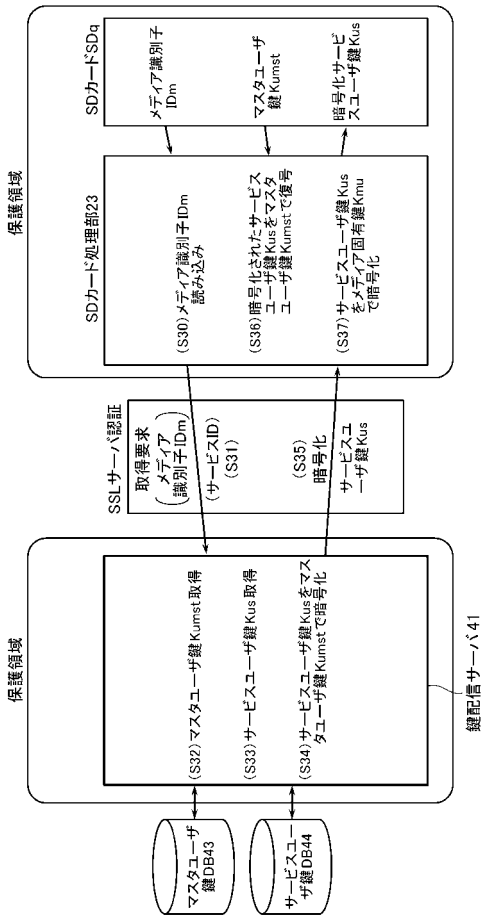
【図１】


ライセンスセンタ装置
ユーザ端末
メディア識別子DB42
マスタユーザ鍵DB43
サービスユーザ鍵DB44
コンテンツ鍵DB46
権利発行済コンテンツID DB47
鍵配信サーバ
管理用鍵取得部
鍵暗号化管理部
ダウンロード部
SDカード処理部
制御部
Enc(Kc, C)
SDq
システム領域
IDm
MKB
秘匿領域
Kmu
保護領域
Enc(Kmu, Kumst)
Enc(Kmu, Kus1)
Enc(Kmu, Kus2)
Enc(Kmu, Kus3)
暗復号部
ユーザデータ領域
Enc1(Kus1, Kc1)
Enc2(Kus2, Kc2)
Enc3(Kus3, Kc3)

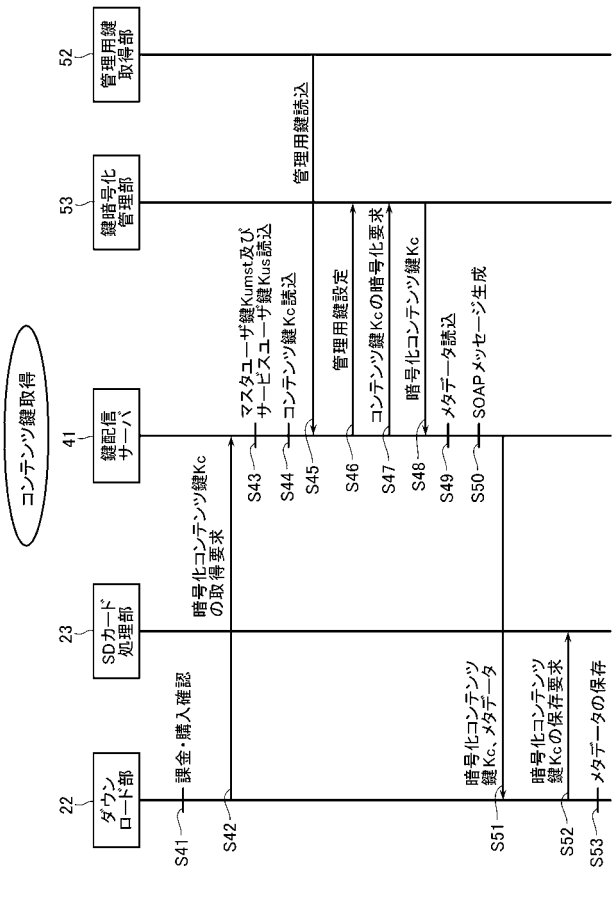
【図２】


保護領域
SDカードSDq
メディア識別子IDm
マスタユーザ鍵Kumst
SDカード処理部23
秘密情報 K1, K2
(S11)メディア識別子IDm読み込み
(S12)乱数R1生成
(S20)R1, R2とK1, K2からセッション鍵Ksを生成
(S21)マスタユーザ鍵Kumstをセッション鍵Ksで復号
(S22)マスタユーザ鍵Kumstを保存
SSLサーバ認証
(S13)メディア識別子IDm
R1
(S19)R2
暗号化マスタユーザ鍵Kumst
鍵配信サーバ41
秘密情報K1, K2
(S14)マスタユーザ鍵Kumst生成
(S15)メディア識別子IDm, マスタユーザ鍵Kumstを記録
(S16)乱数R2生成
(S17)R1, R2, とK1, K2からセッション鍵Ksを生成
(S18)マスタユーザ鍵Kumstをセッション鍵Ksで暗号化
マスタユーザ鍵DB43

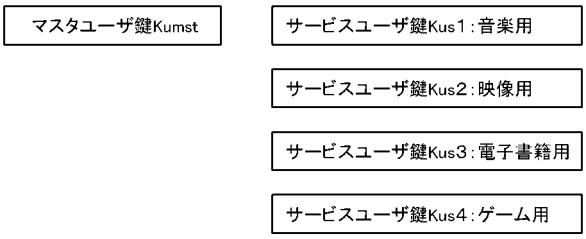
【図３】


保護領域
SDカードSDq
メディア識別子IDm
マスタユーザ鍵Kumst
暗号化サービスユーザ鍵Kus
SDカード処理部23
(S30)メディア識別子IDm読み込み
(S36)暗号化されたサービスユーザ鍵Kusをマスタユーザ鍵Kumstで復号
(S37)サービスユーザ鍵Kusをメディア固有鍵Kmuで暗号化
SSLサーバ認証
取得要求
メディア識別子(IDm)
(サービスID)
(S31)
(S35)
暗号化
サービスユーザ鍵Kus
保護領域
(S32)マスタユーザ鍵Kumst取得
(S33)サービスユーザ鍵Kus取得
(S34)サービスユーザ鍵Kusをマスタユーザ鍵Kumstで暗号化
鍵配信サーバ41
マスタユーザ鍵DB43
サービスユーザ鍵DB44

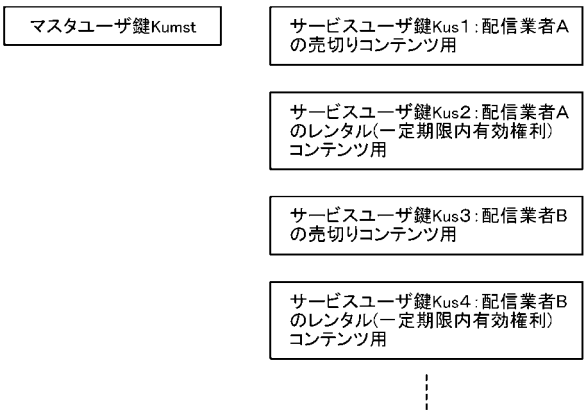
【図４】


コンテンツ鍵取得
ダウンロード部
SDカード処理部
鍵配信サーバ
鍵暗号化管理部
管理用鍵取得部
課金・購入確認
暗号化コンテンツ鍵Kcの取得要求
マスタユーザ鍵Kumst及びサービスユーザ鍵Kus読込
コンテンツ鍵Kc読込
管理用鍵読込
管理用鍵設定
コンテンツ鍵Kcの暗号化要求
暗号化コンテンツ鍵Kc
メタデータ読込
SOAPメッセージ生成
暗号化コンテンツ鍵Kc, メタデータ
暗号化コンテンツ鍵Kcの保存要求
メタデータの保存
S41
S42
S43
S44
S45
S46
S47
S48
S49
S50
S51
S52
S53

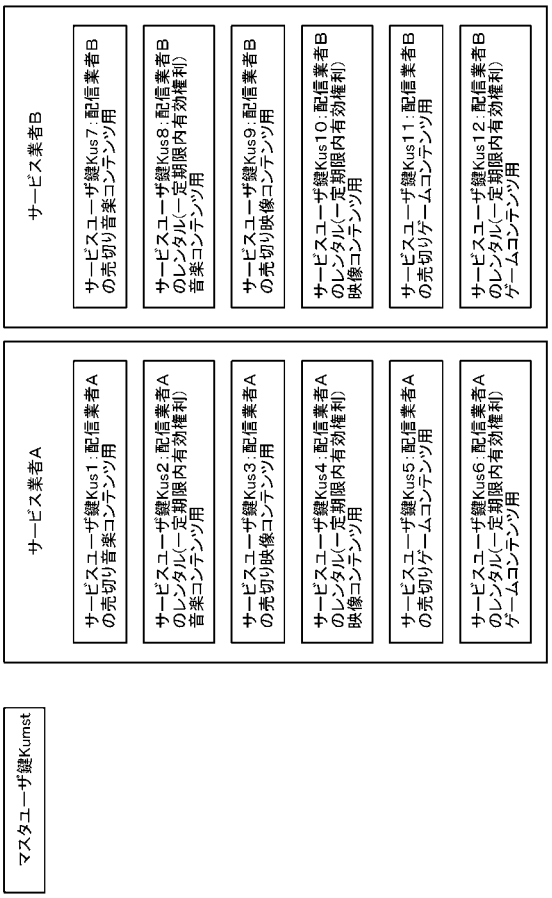
【図５】


マスタユーザ鍵Kumst
サービスユーザ鍵Kus1：音楽用
サービスユーザ鍵Kus2：映像用
サービスユーザ鍵Kus3：電子書籍用
サービスユーザ鍵Kus4：ゲーム用

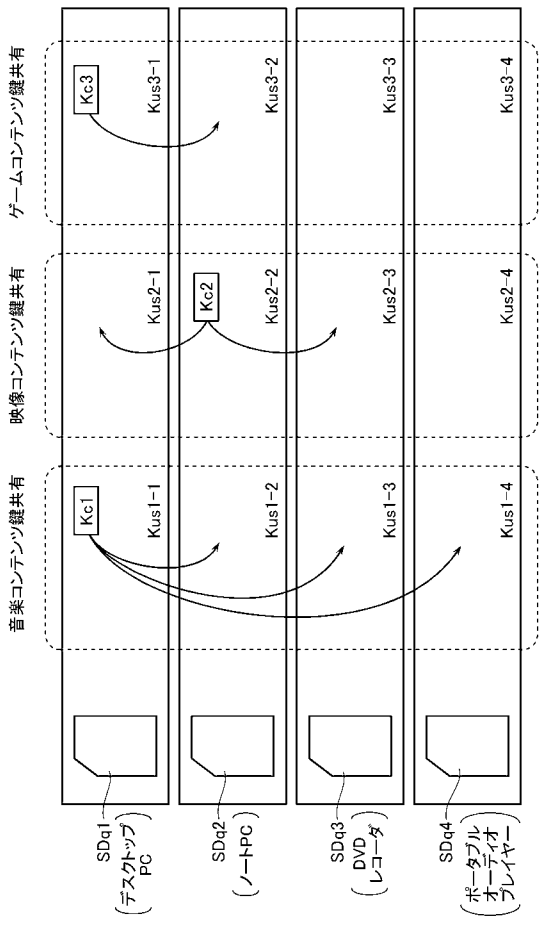
【図６】


マスタユーザ鍵Kumst
サービスユーザ鍵Kus1：配信業者Aの売切りコンテンツ用
サービスユーザ鍵Kus2：配信業者Aのレンタル(一定期限内有効権利)コンテンツ用
サービスユーザ鍵Kus3：配信業者Bの売切りコンテンツ用
サービスユーザ鍵Kus4：配信業者Bのレンタル(一定期限内有効権利)コンテンツ用

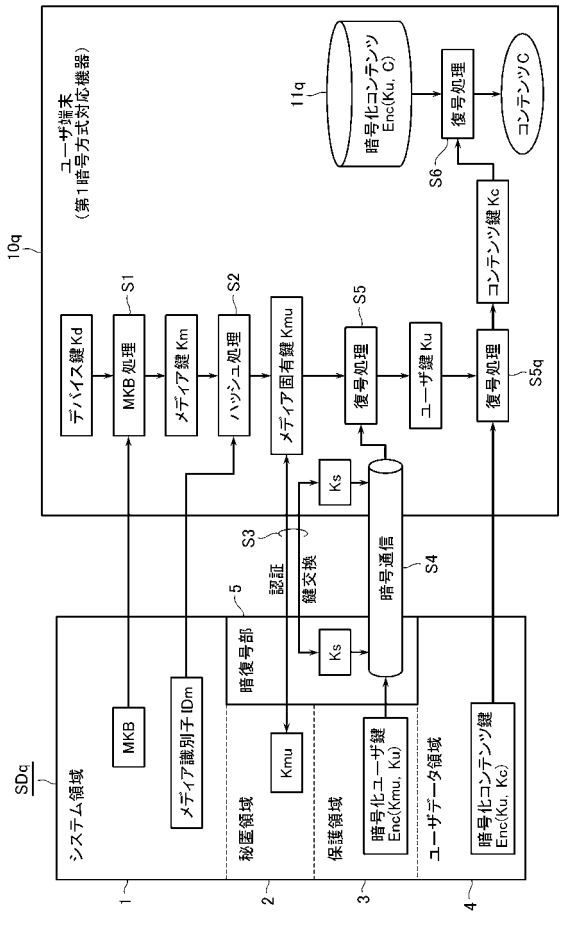
【図７】


サービス業者B
サービスユーザ鍵Kus7：配信業者Bの売切り音楽コンテンツ用
サービスユーザ鍵Kus8：配信業者Bのレンタル(一定期限内有効権利)音楽コンテンツ用
サービスユーザ鍵Kus9：配信業者Bの売切り映像コンテンツ用
サービスユーザ鍵Kus10：配信業者Bのレンタル(一定期限内有効権利)映像コンテンツ用
サービスユーザ鍵Kus11：配信業者Bの売切りゲームコンテンツ用
サービスユーザ鍵Kus12：配信業者Bのレンタル(一定期限内有効権利)ゲームコンテンツ用
サービス業者A
サービスユーザ鍵Kus1：配信業者Aの売切り音楽コンテンツ用
サービスユーザ鍵Kus2：配信業者Aのレンタル(一定期限内有効権利)音楽コンテンツ用
サービスユーザ鍵Kus3：配信業者Aの売切り映像コンテンツ用
サービスユーザ鍵Kus4：配信業者Aのレンタル(一定期限内有効権利)映像コンテンツ用
サービスユーザ鍵Kus5：配信業者Aの売切りゲームコンテンツ用
サービスユーザ鍵Kus6：配信業者Aのレンタル(一定期限内有効権利)ゲームコンテンツ用
マスタユーザ鍵Kumst

【図８】


音楽コンテンツ鍵共有
映像コンテンツ鍵共有
ゲームコンテンツ鍵共有
Kc1
Kc2
Kc3
Kus1-1
Kus1-2
Kus1-3
Kus1-4
Kus2-1
Kus2-2
Kus2-3
Kus2-4
Kus3-1
Kus3-2
Kus3-3
Kus3-4
SDq1 (デスクトップPC)
SDq2 (ノートPC)
SDq3 (DVDレコーダ)
SDq4 (ポータブルオーディオプレイヤー)

【図９】


SDq
システム領域
秘匿領域
保護領域
ユーザデータ領域
MKB
メディア識別子 IDm
Kmu
暗号化ユーザ鍵 Enc(Kmu, Ku)
暗号化コンテンツ鍵 Enc(Ku, Kc)
5
認証
鍵交換
Ks
暗号通信
S3
S4
ユーザ端末 (第1暗号方式対応機器)
10q
デバイス鍵Kd
MKB処理
S1
メディア鍵Km
ハッシュ処理
S2
メディア固有鍵Kmu
S5
復号処理
ユーザ鍵Ku
復号処理
S5q
コンテンツ鍵Kc
11q
暗号化コンテンツ Enc(Ku, C)
復号処理
S6
コンテンツC

フロントページの続き

(51)Int.Cl.		FI		テーマコード（参考）
G06K 17/00	***(2006.01)***	G06F 17/60	302E	
G06K 19/10	***(2006.01)***	G06K 17/00	T	
		G06K 19/00	R	

Fターム(参考) 5B035 AA13 BB09 CA11 CA29
5B058 CA01 KA04 KA35
5B085 AE00 AE29
5J104 AA16 EA22 NA37 PA07