(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2007-60066
(P2007-60066A)
(43)公開日　平成19年3月8日(2007.3.8)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601D	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 7　OL　（全 14 頁）

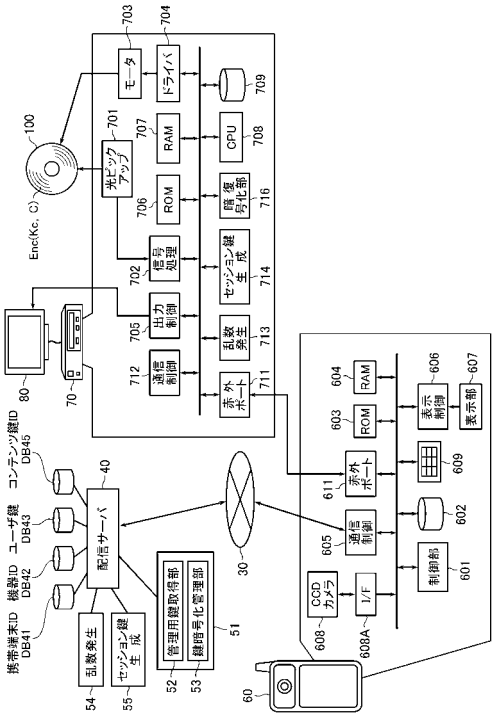
(21)出願番号　特願2005-240616 (P2005-240616)
(22)出願日　平成17年8月23日 (2005.8.23)

(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
(74)代理人　100106389
弁理士　田村　和彦
(72)発明者　笠原　章裕
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
(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

最終頁に続く

(54)【発明の名称】コンテンツデータ配信方法、並びにコンテンツデータ配信システム及びこれに用いられる携帯端末。

(57)【要約】
【課題】通信機能を有さない再生機器にコンテンツ鍵データ等を転送する場合において、ユーザに手間を取らせることなく使い勝手の良いコンテンツデータ配信システム及び方法を提供する。
【解決手段】ユーザがＤＶＤプレーヤ７０が有する暗号化されたコンテンツデータＣの再生を希望する場合には、ユーザが配信サーバ４０に対し携帯端末６０を用いてコンテンツ鍵データＫｃの配信要求を送信する。携帯端末６０により受信されたコンテンツ鍵データＫｃは、赤外通信機能を用いてＤＶＤプレーヤ７０に転送され保存される。初期登録動作において、ＤＶＤプレーヤ７０を識別するための機器ＩＤ、及びコンテンツ鍵データＫｃを暗号化するためのユーザ鍵データＫｕが、配信サーバ４０から携帯端末６０を介してＤＶＤプレーヤ７０に送信される。
【選択図】図１



【特許請求の範囲】
【請求項１】
コンテンツ鍵データにより暗号化されたコンテンツデータを復号して再生可能に構成されると共に自身を識別するための機器ＩＤを保持する再生機器と、
この再生機器とデータ通信可能に構成されると共に自身を識別するための携帯端末ＩＤを保持する携帯端末と、
前記携帯端末を介して前記再生機器に前記コンテンツ鍵データを配信するサーバと
を要素とするコンテンツデータ配信システムにおいてコンテンツデータを配信するコンテンツデータ配信方法であって、
前記サーバが第１乱数を発生させると共にこれを前記携帯端末を介して前記再生機器に送信するステップと、
前記再生機器が第２乱数を発生させるステップと、
前記携帯端末から前記サーバに対し、前記機器ＩＤと前記携帯端末ＩＤと前記第２乱数を送信して前記コンテンツ鍵データの配信を要求するステップと、
前記サーバ及び前記再生機器が、前記第１乱数及び第２乱数に基づいてセッション鍵を生成するステップと、
前記サーバが、前記セッション鍵により、前記コンテンツ鍵データを暗号化して前記携帯端末を介して前記再生機器に送信するステップと
を備えたことを特徴とするコンテンツデータ配信方法。
【請求項２】
前記第２乱数は、異なる前記コンテンツデータの配信要求がされる毎に異なる乱数とされることを特徴とする請求項１記載のコンテンツデータ配信方法。
【請求項３】
前記第１乱数は、前記コンテンツデータの配信に先立って行われる初期登録において発行されるものである請求項２記載のコンテンツデータ配信方法。
【請求項４】
コンテンツ鍵データにより暗号化されたコンテンツデータを保持し適宜前記コンテンツ鍵データを取得して前記コンテンツデータを復号して再生可能に構成されると共に自身を識別するための機器ＩＤを保持する再生機器と、
この再生機器とデータ通信可能に構成されると共に自身を識別するための携帯端末ＩＤを保持する携帯端末と、
前記携帯端末を介して前記再生機器に前記コンテンツ鍵データを配信するサーバと
を備え、
前記サーバは、
前記携帯端末からの要求に応じて、前記再生機器を識別するための機器ＩＤを、前記携帯端末を介して前記再生機器に送信する機器ＩＤ送信手段と、
前記再生機器に付与された機器ＩＤと前記携帯端末を識別するための携帯端末ＩＤとを関連付けて格納するデータベースと、
前記携帯端末からの前記機器ＩＤ及び前記携帯端末ＩＤの提示を伴うコンテンツ鍵データの配信要求に応じて、前記携帯端末に前記コンテンツ鍵データを送信する送信手段と、
第１の乱数を発生させる乱数発生部と、
を備え、
前記再生機器は、
第２の乱数を発生させる乱数発生部を備え、
前記サーバ及び前記再生機器は、前記第１及び第２の乱数を送受信して前記機器ＩＤ及び前記コンテンツ鍵データの送受信に用いるセッション鍵を生成するように構成された
ことを特徴とするコンテンツデータ配信システム。
【請求項５】
前記第２乱数は、異なる前記コンテンツデータの配信要求がされる毎に異なる乱数とされることを特徴とする請求項４記載のコンテンツデータ配信システム。

【請求項６】
前記第１乱数は、前記コンテンツデータの配信に先立って行われる初期登録において発行されるものである請求項５記載のコンテンツデータ配信システム。
【請求項７】
コンテンツ鍵データにより暗号化されたコンテンツデータを復号して再生可能に構成されると共に自身を識別するための機器ＩＤを保持する再生機器と、この再生機器とデータ通信可能に構成されると共に自身を識別するための携帯端末ＩＤを保持する携帯端末と、前記携帯端末を介して前記再生機器に前記コンテンツ鍵データを配信するサーバとで構成されるコンテンツデータ配信システムにおいて用いられる携帯端末であって、
前記サーバから第１乱数を受信して、前記再生機器に送信する手段と、
前記再生機器から第２乱数を受信する手段と、
前記サーバに対し、前記機器ＩＤと前記携帯端末ＩＤと前記第２乱数を送信して前記コンテンツ鍵データの配信を要求する手段と、
前記サーバが前記第１乱数及び第２乱数に基づいて生成したセッション鍵により暗号化したコンテンツ鍵データを受信して前記再生機器に転送する手段と
を備えたことを特徴とする携帯端末。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツデータ配信方法、並びにコンテンツデータ配信システム及びこれに用いられる携帯端末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配信システムが広く用いられてきている。
【０００３】
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、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。
【０００４】
このような暗号化方式を用いたコンテンツ配信システムは、携帯電話端末やパソコンなどデータを配信するサーバに直接アクセス可能な機器だけでなく、ＤＶＤプレーヤなど、そうした通信機能を有さない再生機器でも有効に用いられ得る。こうした再生機器にコンテンツ配信システムからコンテンツデータを送り込むには、通信機能を有する携帯電話端末やパソコン等を介してコンテンツデータを転送する必要がある。この転送時における各種操作が簡略化されれば、ユーザにとって使い勝手の良いシステムとなる。
【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】
【０００５】
この発明は、こうした通信機能を有さない再生機器にコンテンツ鍵データ等を転送する場合において、ユーザに手間を取らせることなく使い勝手の良いコンテンツデータ配信サーバ及び方法、並びに携帯端末を提供することを目的とする。
【課題を解決するための手段】
【０００６】
この発明の一態様に係るコンテンツデータ配信方法は、コンテンツ鍵データにより暗号化されたコンテンツデータを復号して再生可能に構成されると共に自身を識別するための機器ＩＤを保持する再生機器と、この再生機器とデータ通信可能に構成されると共に自身を識別するための携帯端末ＩＤを保持する携帯端末と、
前記携帯端末を介して前記再生機器に前記コンテンツ鍵データを配信するサーバとを要素とするコンテンツデータ配信システムにおいてコンテンツデータを配信するコンテンツデータ配信方法であって、前記サーバが第１乱数を発生させると共にこれを前記携帯端末を介して前記再生機器に送信するステップと、前記再生機器が第２乱数を発生させるステップと、前記携帯端末から前記サーバに対し、前記機器ＩＤと前記携帯端末ＩＤと前記第２乱数を送信して前記コンテンツ鍵データの配信を要求するステップと、前記サーバ及び前記再生機器が、前記第１乱数及び第２乱数に基づいてセッション鍵を生成するステップと、前記サーバが、前記セッション鍵により、前記コンテンツ鍵データを暗号化して前記携帯端末を介して前記再生機器に送信するステップとを備えたことを特徴とする。
【０００７】
この発明の一態様に係るコンテンツデータ配信サーバは、コンテンツ鍵データにより暗号化されたコンテンツデータを保持し適宜前記コンテンツ鍵データを取得して前記コンテンツデータを復号して再生可能に構成されると共に自身を識別するための機器ＩＤを保持する再生機器と、この再生機器とデータ通信可能に構成されると共に自身を識別するための携帯端末ＩＤを保持する携帯端末と、前記携帯端末を介して前記再生機器に前記コンテンツ鍵データを配信するサーバとを備え、前記サーバは、前記携帯端末からの要求に応じて、前記再生機器を識別するための機器ＩＤを、前記携帯端末を介して前記再生機器に送信する機器ＩＤ送信手段と、前記再生機器に付与された機器ＩＤと前記携帯端末を識別するための携帯端末ＩＤとを関連付けて格納するデータベースと、前記携帯端末からの前記機器ＩＤ及び前記携帯端末ＩＤの提示を伴うコンテンツ鍵データの配信要求に応じて、前記携帯端末に前記コンテンツ鍵データを送信する送信手段と第１の乱数を発生させる乱数発生部とを備え、前記再生機器は、第２の乱数を発生させる乱数発生部を備え、前記サーバ及び前記再生機器は、前記第１及び第２の乱数を送受信して前記機器ＩＤ及び前記コンテンツ鍵データの送受信に用いるセッション鍵を生成するように構成されたことを特徴とする。
【０００８】
この発明の一態様に係る携帯端末は、コンテンツ鍵データにより暗号化されたコンテンツデータを復号して再生可能に構成されると共に自身を識別するための機器ＩＤを保持する再生機器と、この再生機器とデータ通信可能に構成されると共に自身を識別するための携帯端末ＩＤを保持する携帯端末と、前記携帯端末を介して前記再生機器に前記コンテンツ鍵データを配信するサーバとで構成されるコンテンツデータ配信システムにおいて用いられる携帯端末であって、前記サーバから第１乱数を受信して、前記再生機器に送信する手段と、前記再生機器から第２乱数を受信する手段と、前記サーバに対し、前記機器ＩＤと前記携帯端末ＩＤと前記第２乱数を送信して前記コンテンツ鍵データの配信を要求する手段と、前記サーバが前記第１乱数及び第２乱数に基づいて生成したセッション鍵により暗号化したコンテンツ鍵データを受信して前記再生機器に転送する手段とを備えたことを特徴とする。
【発明の効果】

【０００９】
この発明によれば、通信機能を有さない再生機器にコンテンツ鍵データ等を転送する場合において、ユーザに手間を取らせることなく使い勝手の良いコンテンツデータ配信システム及び方法、並びに携帯端末を提供することができる。
【発明を実施するための最良の形態】
【００１０】
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。
【００１１】
図１は本発明の第１の実施形態に係るコンテンツデータ配信システムの構成を示す模式図である。
【００１２】
この実施の形態のコンテンツデータ配信システムは、携帯電話網やインターネット、及びこれらの組み合わせからなるネットワーク３０を介して、コンテンツ鍵データＫｃ等を配信する配信サーバ４０と、携帯端末６０とを通信可能に構成したものである。また、携帯端末６０は、例えば赤外線通信等により、携帯端末６０のユーザが所有するＤＶＤプレーヤ７０と通信可能に構成されている。ＤＶＤプレーヤ７０は、ＤＶＤディスク１００を再生するためのものであり、再生データである音声等をＴＶ受像機８０において出力可能に構成されている。ＤＶＤディスク１００には、コンテンツ鍵データＫｃにより暗号化されたコンテンツデータＥｎｃ（Ｋｃ：Ｃ）のみが記録され、コンテンツデータＣの再生のためには、コンテンツ鍵データＫｃの配信サーバ４０からの購入が必要とされている。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。
【００１３】
ユーザがＤＶＤプレーヤ７０が有する暗号化コンテンツデータＥｎｃ（Ｋｃ：Ｃ）の再生を希望する場合には、ユーザが配信サーバ４０に対し携帯端末６０を用いてコンテンツ鍵データＫｃの配信要求を送信する。これにより、コンテンツ鍵データＫｃが配信サーバ４０から携帯端末６０に送信される。携帯端末６０により受信されたコンテンツ鍵データＫｃは、赤外通信機能を用いてＤＶＤプレーヤ７０に転送され保存される。なお、この実施の形態においては、コンテンツ鍵データＫｃの配信要求に先立ち実行される初期登録動作において、ＤＶＤプレーヤ７０を識別するための機器ＩＤ、及びコンテンツ鍵データＫｃを暗号化するためのユーザ鍵データＫｕが、配信サーバ４０から携帯端末６０を介してＤＶＤプレーヤ７０に与えられる。ただし、ユーザ鍵データＫｕ及び機器ＩＤは、オンライン送信でなくとも、製造時や販売時等に予め付与されるようにすることもできる。
【００１４】
配信サーバ４０は、携帯端末６０からのコンテンツ鍵データＫｃ等の配信要求を受信して、要求に係るコンテンツ鍵データＫｃ等を、ネットワーク３０を介して携帯端末６０に配信する機能を有する。
【００１５】
配信サーバ４０は、携帯端末ＩＤデータベース４１と、機器ＩＤデータベース４２と、ユーザ鍵データベース４３と、コンテンツ鍵データベース４５と、セキュリティモジュール５１と、乱数発生部５４と、セッション鍵生成部５５とを備えている。
【００１６】
携帯端末ＩＤデータベース４１は、携帯端末６０が有する携帯端末ＩＤ（ＩＤ６０）のデータを、初期登録動作等によりその携帯端末６０と関連づけられたＤＶＤプレーヤ７０の機器ＩＤ及びユーザ鍵データＫｃと関連付けて保持するものである。
【００１７】
機器ＩＤデータベース４２は、発行済みの機器ＩＤ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、ＤＶＤプレーヤ７０が有するユーザ鍵データＫｕ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４５は、ＤＶＤプレーヤ７０が有するコンテンツ鍵データＫｃを保持するものである。

【００１８】
セキュリティモジュール５１は、ユーザ鍵データＫｕ及びコンテンツ鍵データ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、配信サーバ４０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、配信サーバ４０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、配信サーバ４０から受けた管理用の暗号化ユーザ鍵データ及び管理用の暗号化コンテンツ鍵データをそれぞれ復号し、ユーザ鍵データＫｕ及びコンテンツ鍵データＫｃを得る機能と、コンテンツ鍵データＫｃをユーザ鍵データＫｕで暗号化し、得られた暗号化コンテンツ鍵データＥｎｃ（Ｋｕ：ｋｃ）を配信サーバ４０に送信する機能とを持っている。

【００１９】
乱数発生部５４は、携帯端末６０を介してＤＶＤプレーヤ７０にコンテンツ鍵データ等を送信する場合に、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の乱数Ｒ１を発生させる機能を有する。セッション鍵生成部５５は、この乱数Ｒ１と、後述する乱数発生部７１３で生成される乱数Ｒ２、Ｒ３とを用いてセッション鍵を生成する機能を有する。

【００２０】
携帯端末６０は、制御部６０１、メモリ６０２、ＲＯＭ６０３、ＲＡＭ６０４、通信制御部６０５、表示制御部６０６、表示部６０７、ＣＣＤカメラ６０８、インタフェース６０８Ａ、キーボード６０９、赤外線ポート６１１等を含んでいる。制御部６０１は、携帯端末６０全体の制御を司り、またメモリ６０２は、通信用アプリケーションプログラムの他、初期設定動作等により得られた各種データ（機器ＩＤ等）を保存するためのものである。ＲＯＭ６０３は電源投入時に起動されるブートプログラム等を格納するものであり、ＲＡＭ６０４は例えばプログラム実行時の各種データを一時保存するものである。

【００２１】
通信制御部６０５は、例えば配信サーバ４０及びＤＶＤプレーヤ７０へのデータ送受信等を制御するためのものである。表示制御部６０６は、通信用アプリケーションの実行画面その他の出力画面を表示部６０７において制御するためのものである。赤外線ポート６１１は、通信制御部６０５において赤外線パルス信号に変換された各種データを赤外線として外部例えばＤＶＤプレーヤ７０に向けて出力するためのものである。

【００２２】
ＤＶＤプレーヤ７０は、ＤＶＤディスク１００の信号を読み取る光ピックアップ７０１、光ピックアップ７０１の出力信号を処理する信号処理部７０２、ＤＶＤディスクを回転させるスピンドルモータ７０３、スピンドルモータ７０３を駆動するドライバ７０４、出力制御部７０５、ＲＯＭ７０６、ＲＡＭ７０７、及びＣＰＵ７０８等を備えている。これらはＤＶＤプレーヤ７０の通常の構成であるので、詳細な説明は省略する。またＤＶＤプレーヤ７０は、前述の機器ＩＤ（Ｉ７０）、ユーザ鍵データＫｃ、コンテンツ鍵データＫｃ等を保存するためのメモリ７０９を備えている。なお、この実施の形態では、メモリ７０９内に鍵管理用のソフトウエアを備える。

【００２３】
またＤＶＤプレーヤ７０は、携帯端末６０との間の赤外線通信を行うため赤外線ポート７１１を備えている。通信制御部７１２は、この赤外線ポート７１１で受信された赤外線パルス信号を解析し所定の制御を行うためのものである。

【００２４】
また、ＤＶＤプレーヤ７０は、外部への信号出力のための手段として、乱数発生部７１３、セッション鍵生成部７１４、及び暗復号化部７１６とを備えている。乱数発生部７１３は、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の乱数Ｒ２、Ｒ３を発生させるものである。また、セッション鍵生成部７１４は、前述の乱数Ｒ１とこの乱数Ｒ２、Ｒ３とを用いてセッション鍵を生成する機能を有する。これにより、携帯端末６０を介したＤＶＤプレーヤ７０と配信サーバ４０との間のセキ

ュアな通信が可能となる。暗復号化部７１６は、乱数Ｒ２、Ｒ３その他の情報を所定のプロトコルに従って暗号化すると共に、携帯端末６０から送られた暗号化データを復号する機能を有する。

【００２５】

次に、このコンテンツデータ配信システムの動作手順を、図２乃至図７を用いて説明する。このコンテンツデータ配信システムにおいては、ＤＶＤプレーヤ７０の機器データ及びユーザ鍵データＫｕの配信を配信サーバ４０から受ける初期登録動作が最初に行われる。この初期登録動作に続いて、コンテンツ鍵データＫｃを配信サーバ４０から購入してＤＶＤプレーヤ７０に格納する鍵購入動作が実行される。

【００２６】

まず、初期登録動作の動作手順の例を、図２を参照して説明する。初期登録動作を開始する場合、ユーザは携帯端末６０の通信用アプリケーションを起動させる（Ｓ１）。続いて、このアプリケーションのメニューにおいて、初期登録動作の申請を選択する（Ｓ２）。次にユーザは、携帯端末ＩＤ（Ｉ６０）を提示して、自身が有するＤＶＤプレーヤ７０に対する機器ＩＤの付与を要求する（Ｓ３）。

配信サーバ４０は、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乱数Ｒ１を発生させ、これをＭＡＣ鍵で暗号化したデータＥｎｃ（ＭＡＣ：Ｒ１）を携帯端末６０に送信する（Ｓ４）。

【００２７】

携帯端末６０はこのデータＥｎｃ（ＭＡＣ：Ｒ１）を赤外線ポート６１１によりＤＶＤプレーヤ７０に転送する（Ｓ５）。ＤＶＤプレーヤ７０は、ＭＡＣ鍵を用いてこの乱数Ｒ１を復号しメモリ７０９に保存した後、乱数Ｒ１とは別の乱数Ｒ２を乱数発生部７１３において発生させる（Ｓ６）。そして、この乱数Ｒ２をＭＡＣ鍵で暗号化したデータＥｎｃ（ＭＡＣ：Ｒ２）を、所定のプロトコルに基づいて４桁×４組＝１６字の数字列に変換して、図３に示すように、ＴＶ受像機８０に表示する（Ｓ７）。なお、数字列の代わりに、平仮名、片仮名、漢字、アルファベット等の数が多い文字を表示させるようにすれば、より少ない文字数で乱数Ｒ２を表現することができる。携帯電話等においては平仮名入力が基本とされているため、平仮名の文字列とすれば、入力モードの変換作業が不要となり、しかも入力文字数が少なくて済み、ユーザにとって便利になる。

【００２８】

ユーザは、このＴＶ受像機８０の表示を見て、図３に示すようにこの表示された４桁×４組の数字列を携帯端末６０のキーボード６０９を用いて入力し、「送信」ボタンを押すことによりこれを配信サーバ４０に送信する（Ｓ８）。配信サーバ４０は、受信された４桁×４組の数字列を前述のプロトコルに基づいて逆変換し、暗号化データＥｎｃ（ＭＡＣ：Ｒ２）を得る。この暗号化データを更にＭＡＣ鍵を用いて復号して乱数Ｒ２を得る（Ｓ９）。配信サーバ４０、及びＤＶＤレコーダ７０は、このようにして両者が得た乱数Ｒ１、Ｒ２並びに共通鍵暗号方式の秘密情報Ｋ１、Ｋ２を用いてセッション鍵Ｋｓを生成する（Ｓ１０、Ｓ１１）。続いて配信サーバ４０は、機器ＩＤ（Ｉ７０）のデータ、並びにセッション鍵Ｋｓを用いてユーザ鍵Ｋｕ及び機器ＩＤ（Ｉ７０）を暗号化したデータＥｎｃ（Ｋｓ：（Ｋｕ、Ｉ７０））を携帯端末６０に送信する（Ｓ１２）。携帯端末６０は、機器ＩＤ（Ｉ７０）を自身が有するメモリ６０２に保存すると共に（Ｓ１３）、暗号化データＥｎｃ（Ｋｓ：（Ｋｕ、Ｉ７０））はＤＶＤ７０に赤外線ポート６１１から転送する（Ｓ１４）。ＤＶＤプレーヤ７０は、ＭＡＣ鍵を用いて機器ＩＤ（Ｉ７０）のデータ及びユーザ鍵データＫｕを復号し、メモリ７０９に保存する（Ｓ１５）。これにより、初期登録動作が終了する。初期登録動作が終了したことはＴＶ受像機８０に表示され（Ｓ１６）、ユーザはこれを確認する（Ｓ１７）。これにより、初期登録動作の終了を確認することができる。

【００２９】

続いて、ユーザ鍵データＫｕ及び機器ＩＤ（Ｉ７０）取得後においてコンテンツ鍵データＫｃを購入する場合の動作手順の例を、図４を参照して説明する。ユーザは携帯端末６

０の通信用アプリケーションを起動した後（Ｓ２１）、このアプリケーションを用いて、ＤＶＤプレーヤ７０に対し、ＤＶＤディスク１００に格納されている暗号化されたコンテンツデータＣのリスト表示を要求する（Ｓ２２）。この要求は赤外線ポート６１１を用いて送信する。この要求を受けたＤＶＤプレーヤ７０は、ＤＶＤディスク１００を読んで、図５に示すように、格納されているコンテンツータＣのコンテンツ番号(４桁程度の番号列)やコンテンツデータＣのタイトル等のリストを、「通信番号」として表示される乱数Ｒ３（図５では、Ｒ３＝１２３４の例が示されている）と共にＴＶ受像機８０において表示する（Ｓ２３）。この乱数Ｒ３は、乱数発生部７１３において、携帯端末６０からコンテンツデータＣのリスト表示の要求がされる毎に発生させられる、乱数Ｒ２とは別の乱数である。

【００３０】

ユーザは、このリストを見て、再生させたいコンテンツデータＣの４桁のコンテンツ番号と、通信番号としての乱数Ｒ３をキーボード６０９から入力し、画面上で正しく入力されたことを確認後、「送信」ボタンを押して送信を行う（Ｓ２４）。コンテンツ番号は、機器ＩＤ（Ｉ７０）のデータと共に携帯端末６０からＤＶＤプレーヤ７０に赤外線ポート６１１を介して送信される（Ｓ２５）。ＤＶＤプレーヤ７０は、コンテンツ番号を確認すると共に、送られてきた機器ＩＤのデータが、自己の保持している機器ＩＤ（Ｉ７０）と一致しているか否かを確認する。一致している場合、初期登録が配信サーバ４０において完了していることを確認し（Ｓ２６）、続いて選択されたコンテンツ番号に係るコンテンツデータＣをＴＶ受像機８０に表示すると共に、購入意思の確認をユーザに対し要求する（Ｓ２７）。ユーザが携帯端末６０のキーボード６０９を操作して、購入意思を示す信号をＤＶＤプレーヤ７０及び配信サーバ４０に向けて送信すると、ＴＶ受像機８０には購入済であることを示すメッセージが表示される（Ｓ２９）。配信サーバ４０に送信される購入意思を示す信号には、コンテンツ番号、機器ＩＤ（Ｉ７０）、携帯端末ＩＤ（Ｉ６０）に加え、通信番号として表示された乱数Ｒ３（ＭＡＣ鍵で暗号化されている）が含まれる（Ｓ３０）。乱数Ｒ３を受信すると、配信サーバ４０は、初期登録動作の際用いた乱数Ｒ１とこの乱数Ｒ３とを用いてセッション鍵Ｋｓを生成する（Ｓ３１）。ＤＶＤプレーヤ７０も、同様に乱数Ｒ１とＲ３のデータを有しているので、同様にセッションＫｓを生成する。

【００３１】

配信サーバ４０は、送信された機器ＩＤ（Ｉ７０）及び携帯端末ＩＤ（Ｉ６０）の組み合わせのデータが携帯端末ＩＤデータベース４１に存在するか否かを確認し、確認されたら、携帯端末ＩＤ（Ｉ６０）に基づいて、コンテンツ番号に対応する金額の課金決済を行う（Ｓ３２）。その後、コンテンツ番号に対応するコンテンツＩＤ、選択されたコンテンツデータに対応するコンテンツ鍵データＫｃをユーザ鍵Ｋｕで暗号化し、これを更にセッション鍵Ｋｓで二重に暗号化したデータＥｎｃ（Ｋｓ：Ｅｎｃ（Ｋｕ：Ｋｃ））を、配信サーバ４０から携帯端末６０に送信する。送信中は、図６に示すように、携帯端末６０の画面に「サーバと通信中」との表示がされ、受信が完了すると、図６右に示すように、携帯電話の先端即ち赤外ポート６１１をＤＶＤプレーヤ７０の赤外ポート７１１に向けて送信ボタンを押すことを要求するメッセージが表示される。送信ボタンが押されると、このＥｎｃ（Ｋｓ：Ｅｎｃ（Ｋｕ：Ｋｃ））がＤＶＤプレーヤ７０に向けて送信される。ＤＶＤプレーヤ７０は、これを受信した後、生成したセッション鍵Ｋｓで復号化して暗号化データＥｎｃ（Ｋｕ：Ｋｃ）をメモリ７０９に保存する。これにより、コンテンツ鍵データＫｃの購入手順が完了する。図７に示すように、ＴＶ受像機８０及び携帯端末６０の画面には再生が可能となった旨が表示される。ユーザ鍵データＫｕでメモリ７０９内の暗号化データＥｎｃ（Ｋｕ：Ｋｃ）を復号してコンテンツ鍵データＫｃを得て、このコンテンツ鍵データＫｃによりＤＶＤディスク１００に格納されたコンテンツデータＣを復号してコンテンツデータＣを再生することができる。

【００３２】

この実施の形態では、コンテンツ鍵データＫｃの購入手順において、コンテンツ鍵デー

タＫｃを、ユーザ鍵Ｋｕを用いて暗号化してＥｎｃ（Ｋｕ：Ｋｃ）とし、このＥｎｃ（Ｋｕ：Ｋｃ）を、更に購入手順において新たに生成した乱数Ｒ３を用いて生成したセッション鍵Ｋｓにより暗号化し、Ｅｎｃ（Ｋｓ：Ｅｎｃ（Ｋｕ：Ｋｃ））としてＤＶＤプレーヤ７０に送信している。乱数Ｒ３をコンテンツ鍵データＫｃの配信要求毎に変化させて異なるセッション鍵Ｋｓとするのは、例えばコンテンツ鍵データＫｃが有効期限付きのレンタル用である場合に、次のような不正を防止するためである。すなわち、セッション鍵Ｋｓが毎回同じであると、ユーザが、赤外線通信信号に含まれるデータＥｎｃ（Ｋｓ：Ｅｎｃ（Ｋｕ：Ｋｃ））を例えば所謂学習リモコン等にコピーし、有効期限（レンタル期限）経過後もその学習リモコン等を利用して不正にコンテンツデータを利用することが可能となってしまう。そこで、レンタル業務の適正な運営を可能にするため、上記のように毎回新しい乱数Ｒ３による新しいセッション鍵の生成をすることが有効となる。

【００３３】

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。

【００３４】

例えば、上記の実施の形態では、ＤＶＤプレーヤ７０を再生機器の例として例示したが、暗号化されたコンテンツデータを復号して再生する機能を有するものであればよく、例えばハードディスク型の記録再生機器、パソコン等にも本発明は適用可能である。また、上記実施の形態では、ＤＶＤプレーヤ７０と携帯端末６０との間の通信は赤外線ポート６１１，７１１を用いて赤外線通信より行うものとして説明したが、その他のインタフェース、例えばＵＳＢ、ＩＥＥＥ１３９４等によるデータ通信とすることも可能である。

【００３５】

また例えば、上記の実施の形態において、ＭＱｂｉｃ（登録商標）において採用されている暗号化二重化方式を適用することもでき、また、ＭＱｂｉｃに対応したＳＤカードに上記のユーザ鍵データＫｕ、コンテンツ鍵データＫｃを格納させることも可能である。図８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。

【００３６】

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（Ｋｕ：Ｋｃ）が記憶されている。ここで、ユーザ鍵Ｋｕ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、共通に使用され得る。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。

【００３７】

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。

【００３８】

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。

【００３９】

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。

【００４０】

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。

【００４１】

最後に、ユーザ端末２０ｑ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（Ｋｕ：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（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２０ｑ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。

【００４２】

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。

【００４３】

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識別子が付与されており、メディア識別子ごとに固有のユーザ鍵（メディア固有鍵）が発行される。このメディア固有鍵によりユーザ鍵が暗号化されて、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識別子に依存しており、また正当なプレーヤ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。このようなユーザ端末を再生機器とし、携帯端末によりコンテンツ鍵データ等をこうしたユーザ端末に供給する場合にも、本発明が適用可能である。

【図面の簡単な説明】

【００４４】

【図１】本発明の第１の実施形態に係るコンテンツデータ配信システムの構成を示す模式図である。

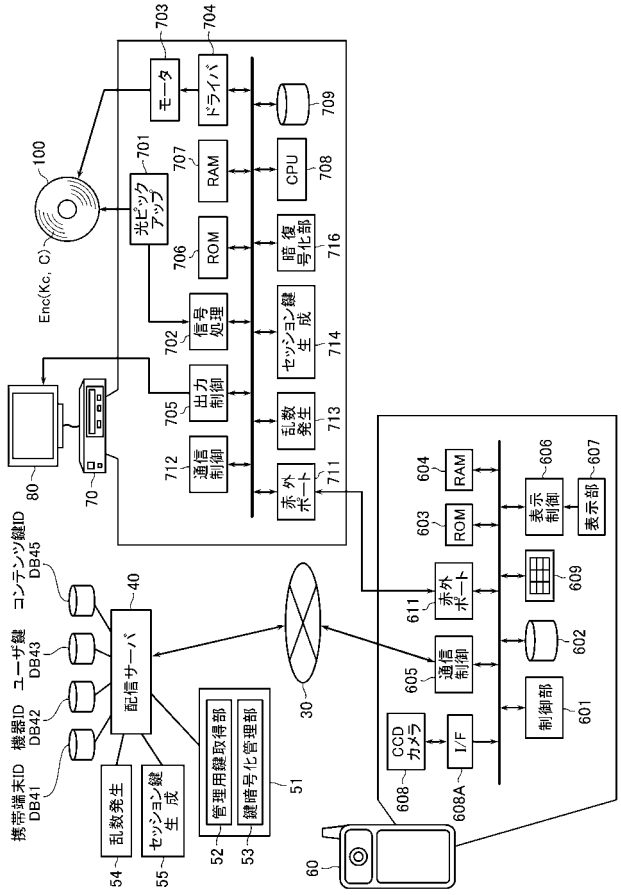
【図２】図１のシステムにおいて、ＤＶＤプレーヤ７０に対する初期登録動作の動作手順の例を示す流れ図である。

【図３】図２の初期登録動作におけるＴＶ受像機８０及び携帯端末６０における画面表示例である。

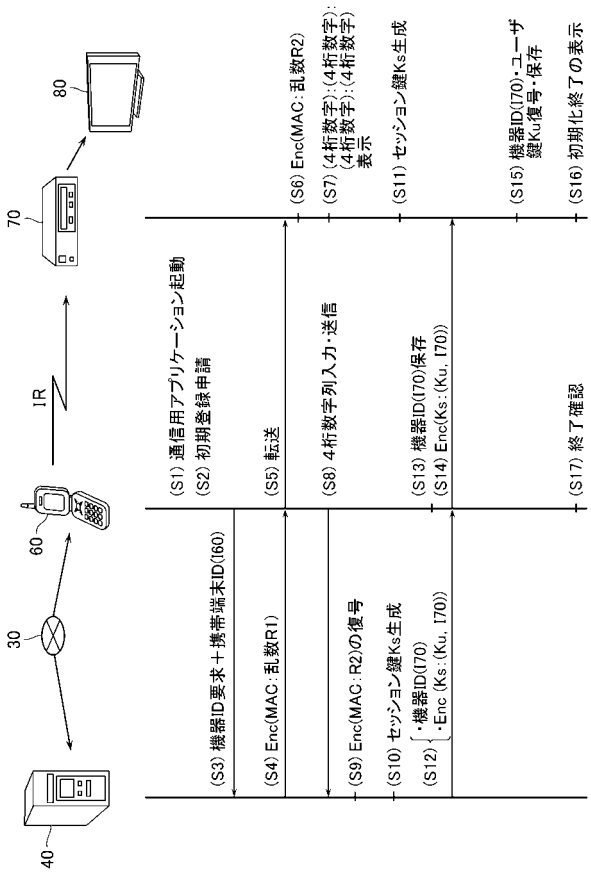
【図４】ユーザ鍵データＫｕ及び機器ＩＤ取得後においてコンテンツ鍵データＫｃを購入する場合の動作手順の例を説明する流れ図である。

【図５】図５の購入手順におけるＴＶ受像機８０及び携帯端末６０の画面表示例である。
【図６】図５の購入手順における携帯端末６０の画面表示例である。
【図７】図５の購入手順におけるＴＶ受像機８０及び携帯端末６０の画面表示例である。
【図８】ＭＱｂｉｃ（登録商標）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。
【符号の説明】
【００４５】
３０・・・ネットワーク、　４０・・・配信サーバ、　４１・・・携帯端末ＩＤデータベース、　４２・・・機器ＩＤデータベース、　４３・・・ユーザ鍵データベース、　４５・・・コンテンツ鍵データベース、　５１・・・セキュリティモジュール、　５２・・・管理用鍵取得部、　５３・・・鍵暗号化管理部、　６０・・・携帯端末、　７０・・・ＤＶＤプレーヤ、　６０１・・・制御部、　６０２・・・メモリ、　６０３・・・ＲＯＭ、　６０４・・・ＲＡＭ、　６０５・・・通信制御部、　６０６・・・表示制御部、　６０７・・・表示部、　６０８・・・ＣＣＤカメラ、　６０９・・・キーボード、　６１１・・・赤外線ポート、　７０１・・・光ピックアップ、　７０２・・・信号処理部、　７０３・・・スピンドルモータ、　７０４・・・ドライバ、　７０５・・・出力制御部、　７０６・・・ＲＯＭ、　７０７・・・ＲＡＭ、　７００・・・ＣＰＵ、　７０９・・・メモリ、　７１１・・・赤外線ポート、　７１２・・・通信制御部、　７１３・・・乱数発生部、　７１４・・・セッション鍵生成部、　７１６・・・暗復号化部。

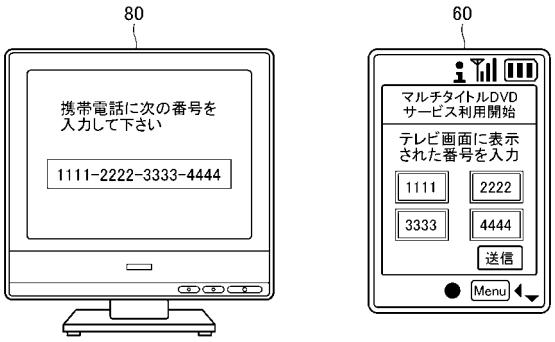
【図１】



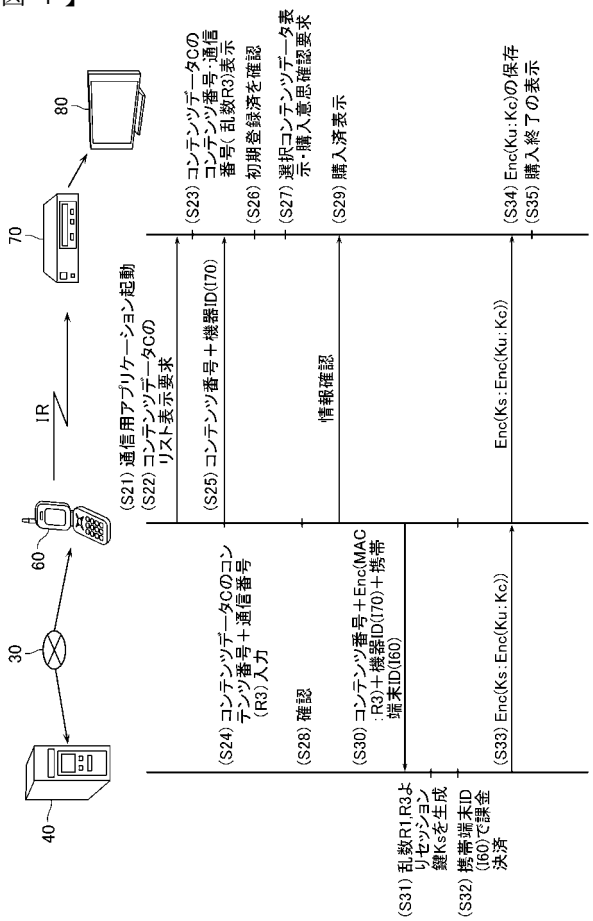
【図２】



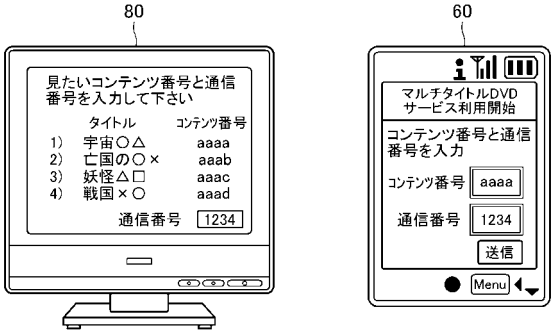
【図３】


80
携帯電話に次の番号を
入力して下さい
1111-2222-3333-4444
60
マルチタイトルDVD
サービス利用開始
テレビ画面に表示
された番号を入力
1111
2222
3333
4444
送信
Menu

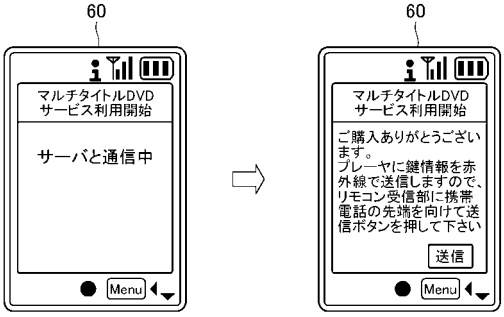
【図４】


80
70
IR
60
30
40
(S21) 通信用アプリケーション起動
(S22) コンテンツデータCのリスト表示要求
(S23) コンテンツデータCのコンテンツ番号・通信番号(乱数R3)表示
(S25) コンテンツ番号＋機器ID(I70)
(S26) 初期登録済を確認
(S27) 選択コンテンツデータ表示・購入意思確認要求
(S29) 購入済表示
情報確認
(S34) Enc(Ku:Kc)の保存
(S35) 購入終了の表示
Enc(Ks:Enc(Ku:Kc))
(S24) コンテンツデータCのコンテンツ番号＋通信番号(R3)入力
(S28) 確認
(S30) コンテンツ番号＋Enc(MAC:R3)＋機器ID(I70)＋携帯端末ID(I60)
(S33) Enc(Ks:Enc(Ku:Kc))
(S31) 乱数R1,R3よりセッション鍵Ksを生成
(S32) 携帯端末ID(I60)で課金決済

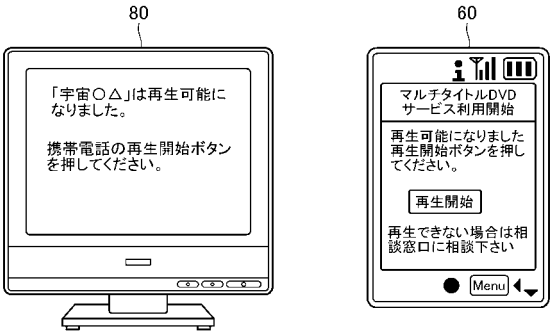
【図５】


80
見たいコンテンツ番号と通信
番号を入力して下さい
タイトル
コンテンツ番号
1) 宇宙○△ aaaa
2) 亡国の○× aaab
3) 妖怪△□ aaac
4) 戦国×○ aaad
通信番号 1234
60
マルチタイトルDVD
サービス利用開始
コンテンツ番号と通信
番号を入力
コンテンツ番号 aaaa
通信番号 1234
送信
Menu

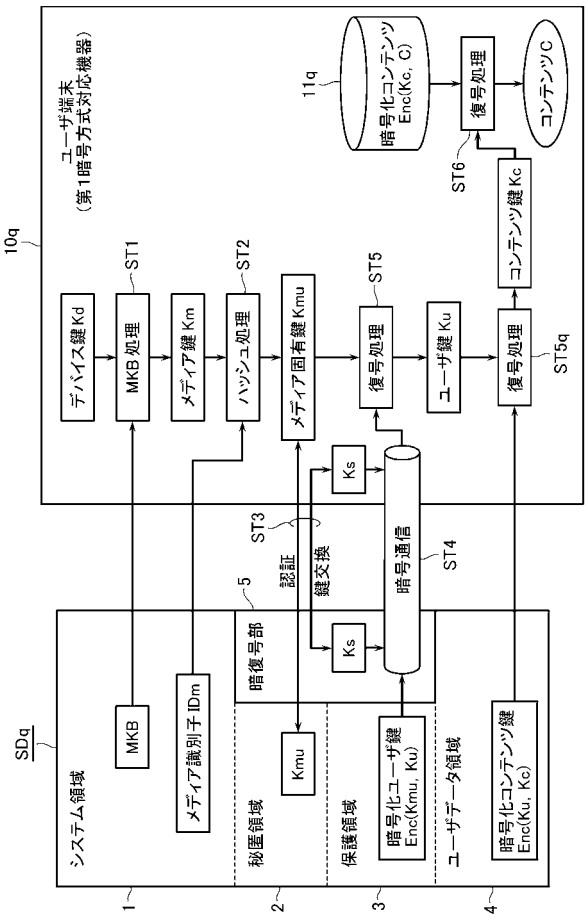
【図６】


60
マルチタイトルDVD
サービス利用開始
サーバと通信中
Menu
60
マルチタイトルDVD
サービス利用開始
ご購入ありがとうございます。
プレーヤに鍵情報を赤外線で送信しますので、リモコン受信部に携帯電話の先端を向けて送信ボタンを押して下さい
送信
Menu

【図７】


80
「宇宙○△」は再生可能になりました。
携帯電話の再生開始ボタンを押してください。
60
マルチタイトルDVD
サービス利用開始
再生可能になりました
再生開始ボタンを押してください。
再生開始
再生できない場合は相談窓口に相談下さい
Menu

【図８】


10q
ユーザ端末
（第1暗号方式対応機器）
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
ST5
復号処理
ユーザ鍵Ku
復号処理
ST5q
11q
暗号化コンテンツ
Enc(Kc, C)
復号処理
ST6
コンテンツC
コンテンツ鍵Kc
Ks
Ks
ST3
認証
鍵交換
暗号通信
ST4
5
暗復号部
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

(72)発明者　嵩　比呂志
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

Ｆターム(参考) 5J104 EA23　PA01　PA07