(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3925095号
(P3925095)
(45)発行日　平成19年6月6日(2007.6.6)　(24)登録日　平成19年3月9日(2007.3.9)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601A
H04L	9/14	(2006.01)	H04L	9/00	601E
H04N	7/16	(2006.01)	H04L	9/00	641
			H04N	7/16	A

請求項の数 6　(全 16 頁)

(21)出願番号　特願2001-91685(P2001-91685)
(22)出願日　平成13年3月28日(2001.3.28)
(65)公開番号　特開2002-305512(P2002-305512A)
(43)公開日　平成14年10月18日(2002.10.18)
審査請求日　平成16年9月29日(2004.9.29)
(31)優先権主張番号　特願2001-25011(P2001-25011)
(32)優先日　平成13年2月1日(2001.2.1)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　森野　東海
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内
(72)発明者　岡山　祐孝
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】データ受信装置

(57)【特許請求の範囲】
【請求項１】
暗号化されたデータを受信するデータ受信装置であって、
データ鍵により暗号化された前記データを受信する受信器、
暗号化された前記データ鍵を復号化するデータ鍵復号器と接続され、受信された前記データを復号化された前記データ鍵により復号化する復号器、
復号化された前記データを、再暗号鍵により再暗号化する暗号器、
前記暗号器と接続され、再暗号化された前記データを、外部の記憶装置に記憶するよう、外部へ送信する送信部、および
複数の再暗号鍵と各再暗号鍵に対応するインデックスとを記憶する記憶媒体と、暗号通信により通信する通信制御部を有し、
前記通信制御部は、前記通信制御部の認証データを前記記憶媒体へ送信して前記記憶媒体で前記通信制御部が認証された場合に、前記記憶媒体で生成されたセッション鍵及び前記通信制御部で生成された乱数を公開鍵方式により前記記憶媒体と共有し、前記記憶媒体とやり取りする情報を前記セッション鍵又は前記乱数により暗号化・復号化して、前記記憶媒体との前記暗号通信を実現し、
前記暗号器は、乱数を用いて前記記憶媒体にある前記複数の再暗号鍵のどれを使用するかを決めるインデックスを生成し、前記インデックスを前記暗号通信により前記記憶媒体に送信し、前記記憶媒体から前記暗号通信により前記インデックスに対応する再暗号鍵を取得し、

前記送信部は、前記再暗号化されたデータを前記再暗号鍵の取得に用いた前記インデックスと共に外部へ送信することを特徴とするデータ受信装置。
【請求項２】
請求項１に記載のデータ受信装置であって、
前記外部と接続するための第１のインターフェースユニット、および
前記記憶媒体と接続するための第２のインターフェースユニットを有することを特徴とするデータ受信装置。
【請求項３】
請求項１に記載のデータ受信装置であって、
前記送信部は、前記再暗号鍵の取得に用いた前記インデックスに乱数を付加し、乱数が付加された前記インデックスを暗号化し、暗号化された前記インデックスを前記再暗号化されたデータと共に外部へ送信することを特徴とするデータ受信装置。
【請求項４】
請求項１に記載のデータ受信装置であって、
当該データ受信装置は、前記記憶媒体をさらに有することを特徴とするデータ受信装置。
【請求項５】
請求項１に記載のデータ受信装置であって、
当該データ受信装置は、バスを介して前記記憶媒体と接続することを特徴とするデータ受信装置。
【請求項６】
請求項１に記載のデータ受信装置であって、
さらに、当該データ受信装置の利用者からの入力に応じて、前記再暗号鍵を用いて前記外部の記憶装置に記憶された前記データを復号化する再復号器、および
前記再復号器と接続され、復号化された前記データを出力する出力器を有することを特徴とするデータ受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、暗号化されたコンテンツを受信するデータ受信装置及びそのデータ受信装置を有する情報処理装置に係わる。そのなかでも特にデジタル放送データやネットワークを介して伝送されたデータを受信するデータ受信装置及びそのデータ受信装置を有する情報処理装置に関する。なお、データ受信装置には、テレビ受像機（チューナ）、ビデオレコーダ、セットトップボックス等が含まれる。また、情報処理装置には、パーソナルコンピュータ、ワークステーション、携帯電話が含まれる。
【０００２】
【従来の技術】
近年、衛星放送等を用いた電子配信により、暗号化された映像や音声コンテンツをユーザに提供するデータ配信が行われている。「ＢＳデジタル放送限定受信方式」ＡＲＩＢ・ＳＴＤ－Ｂ２５では、ＢＳデジタル放送における限定受信の方法が記述されている。図２に、この記述内容であるＢＳデジタル放送での暗号化されたデータを受信する限定受信方式を示す。
【０００３】
この図２を用いてデータの流れを説明する。まず、映像や音声等のコンテンツはコンテンツ暗号器１０１でスクランブル鍵Ｋｓ１０２を用いて暗号化される。また、スクランブル鍵Ｋｓ１０２は暗号器１０６でワーク鍵１０３を用いて暗号化され、ワーク鍵Ｋｗ１０３と契約情報１０４は暗号器１０７でマスター鍵Ｋｍ１０５を用いて暗号化される。これら、暗号化されたコンテンツ、スクランブル鍵Ｋｓ及びワーク鍵Ｋｓと契約情報は多重器１０８で多重化され受信機に配信される。また、受信機１２０では分離器１１８を用いて暗号化されたコンテンツ、スクランブル鍵Ｋｓ及びワーク鍵Ｋｗと契約情報に分離される。

暗号化されたワーク鍵Ｋｗと契約情報は復号器１１７でマスター鍵１１５を用いて復号されワーク鍵Ｋｗと契約情報１１４を得て保存する。暗号化されたスクランブル鍵は復号器１１６でワーク鍵Ｋｗを用いて復号されスクランブル鍵Ｋｓを得る。また、暗号化されたコンテンツは、契約情報１１９を用いて視聴判定器１１９で視聴可能かどうかを判定し可能であればコンテンツ復号器１１１でスクランブル鍵Ｋｓを用いて復号化される。ここでスクランブル鍵Ｋｓは暗号化され全ての受信機で受信されるが、ワーク鍵Ｋｗと契約情報は受信機毎のデータであり受信機毎にユニークなマスター鍵Ｋｍで暗号化され他の受信機以外では復号化できない。したかって契約していないコンテンツは、スクランブル鍵Ｋｓを復号化するために必要なＫｗが得られないため受信できない事になる。マスター鍵Ｋｍは変更される事はないが、ワーク鍵Ｋｗは契約時とおよそ半年から１年程度で変更され、スクランブル鍵Ｋｓはおよそ数秒単位で更新される。このため契約していないコンテンツのワーク鍵Ｋｗが分かったとしても１年程度、スクランブル鍵Ｋｓが分かった場合は数秒程度しか視聴する事しかできなくなっている。また、図２の復号器１１６、復号器１１７、マスター鍵１１５、契約情報１１４、視聴判定器１１９はＩＣカードで実現されている。

【０００４】

また、図３のようにパーソナルコンピュータ（ＰＣ）に接続可能なＢＳデジタル放送の受信ボードが存在する。

【０００５】

【発明が解決しようとする課題】

コンテンツを録画する場合には、以下の問題が生じる。この問題を図3に示す場合を例に説明するが、その他、PCを含む情報処理装置内に受信ボードがある場合、テレビ受像機、セットトップボックス、ビデオレコーダの場合でも同様の問題が生じる。

【０００６】

図３のようにＢＳデジタル放送の受信ボードをパーソナルコンピュータ（ＰＣ）に接続した場合に、ＰＣで録画機を実現すると次のようになる。チューナ１１で受信したデジタルデータは、分離器１３で暗号化されたスクランブル鍵Ｋｓ、ワーク鍵Ｋｗや契約情報を分離して、ローカルバス２４を介してローカルＣＰＵ１５によりＩＣカード１６に送られる。ＩＣカード１６では、上述したように、ワーク鍵Ｋｗや契約情報を保存し、暗号化されたスクランプル鍵Ｋｓを復号化する。そしてコンテンツ復号器１２にスクランブル鍵Ｋｓを送り、暗号化されたコンテンツを復号化する。復号化されたコンテンツはコンテンツデコーダ１４でデコードされモニタやスピーカなどの出力装置３０に出力される。このとき、出力装置３０ではなくＰＣの表示制御装置６に直接出力することも考えられる。また、ＰＣのＨＤＤの様な記憶装置５に録画するには、分離器１３で分離したコンテンツをローカルバス２４よりバスＩ／Ｆ部２３に送られ、ＰＣの内部バスであるＰＣＩバス４を介してバスブリッジ２を経由し主記憶３に格納される。主記憶３にある程度コンテンツが蓄積されるとＣＰＵ１により、記憶装置５に格納される。ここで、記憶装置５に格納されたコンテンツは暗号化されておらず、ファイル操作を行うアプリケーションを用いると簡単にコピーができてしまい、コンテンツの著作権の保護が困難になる。

【０００７】

また、コンテンツの著作権を保護するためにコンテンツやスクランブル鍵Ｋｓを暗号化されたまま、記憶装置５に格納し再生するときに暗号を復号する事が考えられるがこれは、上述したようにワーク鍵Ｋｗが半年から１年程度で変更されてしまうため録画してから時間が経つとコンテンツを視聴できなくなってしまうと言った問題がある。

【０００８】

【課題を解決するための手段】

本発明の目的は、コンテンツの著作者等の権利の保護を図りつつ、視聴者側で適切な記憶媒体又は記憶装置でコンテンツを管理できるデータ受信装置及び情報処理装置を提供することである。

【０００９】

この目的を達成するために、本発明は、暗号化されたデータであって、前記データが時間の経過により内容が変更されるデータ復号鍵により復号化するデータ対象とし、第1の暗号鍵により暗号化された前記データを受信し、受信された前記データおよび第2の暗号鍵により暗号化された前記データ復号鍵の少なくとも一方を復号化し、復号化された前記データまたは前記データ復号鍵を、再暗号化鍵により暗号化し、前記暗号器と接続され、暗号化された前記データまたは前記データ復号鍵を、記憶媒体に記憶する。

【００１０】

また、本発明には、記憶媒体に記憶されたデータを再生することも含まれる。

【００１１】

【発明の実施の形態】

次に本発明の実施例について図面を用いて詳細に説明する。

図１は、本発明の１情報処理装置を示すブロック図である。図１において、１９はスクランブル鍵を再暗号化するＫｓ暗号器で、２０はデータ受信装置１０毎又は情報処理装置毎のユニークな識別情報である識別ＩＤ（Identifier）を格納する識別ＩＤ格納領域で、２１は乱数を発生させる乱数発生器で、１８はコンテンツのＩＤとＫｓ暗号器１９で暗号化されたスクランブル鍵を復号化する鍵を格納する鍵格納領域である。２２は再暗号化されたスクランブル鍵Ｋｓを暗号化されているコンテンツに多重化を行うＫｓ多重器である。１７は、再暗号化されたスクランブル鍵Ｋｓの復号を行う復号器である。

【００１２】

情報処理装置は、データを受信し復号化及び再暗号化を行うデータ受信装置１０と、データを視聴するための出力装置３０と、情報処理を実行する情報処理装置本体と、表示を行うためのＣＲＴ（Cathode-Ray Tube）７とを備える。尚、ＣＲＴ７は、液晶ディスプレイ、プラズマディスプレイ、ＥＬディスプレイ等のデータを表示する他の表示装置であってもよい。

【００１３】

情報処理装置本体は、演算処理を行うためのＣＰＵ（Central Processing Unit）１と、データやプログラムを記憶する主記憶３（例えば、ＲＡＭ（Random Access Memory）等）、バスブリッジ２と、データやプログラムを記憶する記憶装置５（例えば、ＨＤＤ等）、表示を制御するための表示制御装置６を備える。データ受信装置１０とＣＰＵ１と主記憶３とバスブリッジ２と記憶装置５と表示制御装置６とは相互にＰＣＩ（Peripheral Component Interconnect）バス４で接続されている。尚、記憶装置５は、フロッピーディスク、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ－ＲＡＭ、ＭＯ等のように、書き込み可能又は書き換え可能な記憶媒体であってもよい。記憶装置は、データ、情報を記憶できればよい。

【００１４】

なお、情報処理装置は、PC、ワークステーションの他、携帯電話を含む。

【００１５】

データ受信装置１０は、放送データを受信するためのチューナ１１と、暗号化されたコンテンツを復号化するコンテンツ復号器１２と、放送データを暗号化されたコンテンツと暗号化されたスクランブル鍵Ｋｓとに分離する分離器１３と、コンテンツをデコードするコンテンツデコーダ１４と、演算処理を行うためのローカルＣＰＵ１５と、ワーク鍵Ｋｗ及び契約情報を記憶すると共にワーク鍵Ｋｗによって暗号化されたスクランブル鍵Ｋｓを復号化するＩＣカード１６と、再暗号化されたスクランブル鍵Ｋｓを復号化する復号器１７と、再暗号化されたスクランプル鍵Ｋｓを復号化するための鍵とコンテンツＩＤとを記憶する鍵格納領域と、スクランブル鍵Ｋｓを再暗号化するＫｓ暗号器１９と、識別ＩＤを格納する識別ＩＤ格納領域２０と、乱数を発生する乱数発生器２１と、再暗号化されたスクランブル鍵Ｋｓを暗号化されたコンテンツに多重化するＫｓ多重器２２と、ＰＣＩバス４とインターフェースするためのバスＩ／Ｆ部２３とを備える。これら各機器は、ローカルバス２４によって、相互に接続される。尚、チューナ１１は、モデムやＴＡ等のようにネットワークを介して伝送されたデータを受信する受信機であってもよい。また、ＩＣカー

ド１６は、データ受信装置１０から分離（着脱）可能である。ワーク鍵Ｋｗは、ＩＣカード１６に記憶されるのが好ましいが、他の記録媒体（例えば、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等）に記憶されてもよいし、ネットワークによってアクセス可能なサーバに記憶されてもよい。ワーク鍵Ｋｗがサーバに記憶される場合は、ネットワークを介して、ワーク鍵Ｋｗを取得する。

【００１６】

次に、情報処理装置の処理内容を説明する。まず、ワーク鍵Ｋｗと契約情報は予めＩＣカード１６に保存されているとする。最初にコンテンツを記録する場合を説明する。チューナ１１により暗号化された放送データ（番組）を受信し、コンテンツ復号器１２を通り分離器１３で、受信された放送データを暗号化されたコンテンツと暗号化されたスクランブル鍵Ｋｓに分離する。分離された暗号化されたスクランブル鍵ＫｓはローカルＣＰＵ１５によりＩＣカード１６でワーク鍵Ｋｗによって復号化され、ローカルＣＰＵ１５で復号化されたスクランブル鍵ＫｓをＫｓ暗号器１９に転送する。Ｋｓ暗号器１９では、識別ＩＤ格納領域に格納されかつデータ受信装置１０毎のユニークな識別情報である識別ＩＤと乱数発生器２１で生成された乱数をもちいて暗号化する。ＣＰＵ１で指定した再暗号化した事を示すコンテンツＩＤを、バスブリッジ２とバスＩ／Ｆ部２３を介してＫｓ暗号器１９に転送しておく。再暗号化が行われるとＫｓ暗号器１９はコンテンツＩＤと再暗号化したスクランブル鍵ＫｓをＫｓ多重器２２に転送する。また、Ｋｓ暗号器１９は再暗号化されたスクランプル鍵Ｋｓを復号する時に用いる鍵とコンテンツＩＤとを対にして鍵格納領域１８に格納する。Ｋｓ多重器２２ではコンテンツＩＤと再暗号化したスクランブル鍵Ｋｓとを多重化し、バスＩ／Ｆ部２３に転送する。バスＩ／Ｆ部では、この多重化されたデータをＰＣＩバス４、バスブリッジ２を介して主記憶３に転送し、主記憶３にある程度データが貯まったら、ＣＰＵ１でＨＤＤ等の記憶装置５に格納する。

【００１７】

記録したコンテンツを再生する場合を説明する。記憶装置５に格納された多重化されたデータをＣＰＵ１で読み出しＰＣＩバス４を介してバスＩ／Ｆ部２３を通してコンテンツ復号器１２に入力する。多重化されたデータは、分離器１３で暗号化されたスクランブル鍵Ｋｓを分離しローカルＣＰＵ１５に送る。ローカルＣＰＵ１５では、再暗号化した事をしめすコンテンツＩＤを確認するとコンテンツＩＤと暗号化されたスクランブル鍵ＫｓをＫｓ復号器１７に転送する。Ｋｓ復号器１７はコンテンツＩＤを元に対応した再暗号化されたスクランブル鍵Ｋｓを復号するための鍵を鍵格納領域１８より読み出し、再暗号化されたスクランブル鍵Ｋｓをこの鍵と識別ＩＤを用いて復号化する。ローカルＣＰＵ１５はこのスクランブル鍵Ｋｓを受け取りコンテンツ復号器１２に設定して、暗号化されたコンテンツを復号化する。この復号されたコンテンツは、コンテンツデコーダ１４によりデコードされた後、出力装置３０に送られ視聴する事ができる。

【００１８】

このようにコンテンツを暗号化したままで、スクランブル鍵Ｋｓをデータ受信装置固有の識別ＩＤを用いて再暗号化しコンテンツと多重化して記録することで、例えファイルがコピーされても他の情報処理装置やデータ再生装置で再生しようとしても、識別ＩＤが異なるためスクランブル鍵Ｋｓを復号することができないため、コンテンツの著作権の保護が可能となる。また、鍵格納領域１８に格納される鍵は更新される事がないので再生する場合の時間による制限もなくなる。次に、本発明の特徴であるＫｓ暗号器１９について図４を用いて詳細に説明する。図４において、４１はスクランブル鍵Ｋｓを格納するスクランブル鍵Ｋｓレジスタで、４２はコンテンツのＩＤを格納するコンテンツＩＤレジスタで、４５はスクランブル鍵Ｋｓを再暗号化するスクランブル鍵暗号部で、４６は暗号化されたスクランブル鍵を復号するための鍵を生成する復号鍵生成部で、４７はスクランブル鍵Ｋｓを暗号化する鍵を生成する暗号鍵生成部で、４８はコンテンツＩＤと再暗号化されたスクランブル鍵Ｋｓを合成する合成部である。Ｋｓ暗号器１９は、スクランブル鍵Ｋｓレジスタ４１と、コンテンツＩＤレジスタ４２と、格納制御部４３と、スクランブル鍵暗号部４５と、復号鍵生成部４６と、暗号鍵生成部４７と、合成部４８とを備える。

【００１９】
次に、これらを用いて処理内容を説明する。スクランブル鍵レジスタ４１には、ＩＣカードで復号化されたスクランブル鍵Ｋｓがローカル ＣＰＵ１５により設定され、コンテンツＩＤレジスタ４２にはＣＰＵ１によってコンテンツＩＤが設定される。暗号鍵生成部４７では、識別ＩＤと乱数発生器２１で生成した乱数に所定の演算を施し暗号化するための鍵を得る。この暗号化するための鍵はスクランブル鍵暗号部４５に送られ、スクランブル鍵レジスタ４１に格納されているスクランブル鍵Ｋｓを暗号化して合成部４８に送られる。合成部４８では、暗号化されたスクランブル鍵Ｋｓとコンテンツ ＩＤレジスタ４２に格納されたコンテンツＩＤを合成して、Ｋｓ多重器２２に送る。ここで、コンテンツＩＤは、暗号化されていないためＣＰＵ１で確認できる事になる。これにより、再生を行う場合、記録されている多重化されたデータのコンテンツＩＤが確認できる。また、復号器生成部４６では、識別ＩＤと乱数発生器２１で生成した乱数に所定の演算を施し復号化するための鍵を得る。格納制御部４３では、この復号化するための鍵とコンテンツＩＤを対にして鍵格納領域１８に格納する。
【００２０】
尚、本発明は、放送電波を介して伝送された放送データを受信する場合に限られず、ネットワーク（インターネット、ローカルエリアネットワーク等）を介して伝送されたデータを受信する場合や、他の情報処理装置から伝送されたデータを受信する場合にも適用可能である。
【００２１】
次に、図５を用いて第２の実施例を説明する。図５において、３１はコンテンツを再生する時に用いる再生用分離器で、３２はコンテンツを記録するときに用いる記録用分離器である。第１の実施例では、コンテンツを記録している時には暗号化されたままコンテンツを転送するため暗号化されたコンテンツの復号化は行わなかった。つまりコンテンツ復号器１２は動作せずに分離器１３に転送されてくるデータは、暗号化されたままのコンテンツであり当然コンテンツデコーダ１４で復号させることはできない。つまり、記録中はコンテンツを視聴する事ができない。そこで図５の用に再生用分離器３１と記録用分離器３２を独立に持つ事により記録中のコンテンツの視聴を可能としている。
【００２２】
処理内容としては次の通りである。再生用分離器３１では、暗号化されたスクランブル鍵Ｋｓを分離してローカルＣＰＵ１５によりＩＣカードでスクランブル鍵Ｋｓを復号しコンテンツ復号器１２に設定して暗号化されたコンテンツの復号を行う。従って、再生用分離器３１から送られてくるコンテンツは復号されているためコンテンツデコーダ１４でデコードでき視聴が可能になる。また、記録用分離器では、復号されているコンテンツは必要ないため、チューナの出力よりデータを受け取り暗号化されたコンテンツを分離してＫｓ多重器２２に転送する事により記憶装置５への記録が可能となる。
【００２３】
次に、図６を用いて第３の実施例を説明する。図６において、５２は第１、第２の実施例におけるＫｓ復号器１７、Ｋｓ暗号器１９、識別ＩＤ格納領域２０、乱数発生器２１と鍵格納領域１８の機能を持つ取り外し可能なスクランブル鍵暗号復号カードである。スクランブル鍵暗号復号カード５２は、カードＩ／Ｆ部５１を介してローカルバス２４に接続されており、再暗号化されたスクランブル鍵ＫｓとコンテンツＩＤもカードＩ／Ｆ部５１を介してＫｓ多重器２２に接続されているので、Ｋｓ復号器１７とＫｓ暗号器１８のアクセスは第１、第２の実施例と同様に行える。スクランブル鍵暗号復号カード５２は、データ受信装置１０から分離（着脱）可能である。また、識別ＩＤは、スクランブル鍵暗号復号カード５１毎にユニークなＩＤにするのが好ましい。これにより、例えば記憶装置５に記録された多重化されたデータを、ＤＶＤ－ＲＡＭ、ＣＤ－Ｒ、ＣＤ－ＲＷの様な外部記憶装置８にコピーしてこの外部記憶装置８とスクランブル鍵暗号復号カード５１を本発明のデータ受信装置１０が接続されている情報処理装置であれば他の情報処理装置でもコンテンツの視聴が可能になる。また、スクランブル鍵暗号復号カード５１の機能をＩＣカード

１６に内蔵する事でカードの枚数を減らす事も容易に考えられる。

【００２４】

次に、図７を用いて第４の実施例を説明する。図７において、３４はコンテンツを再暗号化するコンテンツ暗号器で、３５は再暗号化されたコンテンツを復号する再暗号コンテンツ復号器である。

【００２５】

まず、コンテンツを記録する場合を説明する。チューナ１１により暗号化された放送データ（番組）を受信し、コンテンツ復号器１２を通り分離器１３で、暗号化されたコンテンツと暗号化されたスクランブル鍵Ｋｓに分離する。分離された暗号化されたスクランブル鍵ＫｓはローカルＣＰＵ１５によりＩＣカード１６で復号化され、ローカルＣＰＵ１５で復号化されたスクランブル鍵Ｋｓをコンテンツ復号器１２に設定する。コンテンツ復号器１２で復号されたコンテンツは分離器１３によりコンテンツデコーダ１４とコンテンツ暗号器３４に送られる。コンテンツデコーダ１４でコンテンツをデコードして出力装置３０に出力してコンテンツを視聴できる。コンテンツ暗号器３４では、データ受信装置毎のユニークな識別情報である識別ＩＤと乱数発生器２１で生成された乱数をもちいて暗号化する。

【００２６】

また、ＣＰＵ１で指定した再暗号化した事を示すコンテンツＩＤを、バスブリッジ２とバスＩ／Ｆ部２３を介してコンテンツ暗号器３４に転送しておく。再暗号化が行われるとコンテンツ暗号器３４はコンテンツＩＤと再暗号化したコンテンツをバスＩ／Ｆ部２３に転送する。また、コンテンツ暗号器３４は再暗号化されたコンテンツを復号する時に用いる鍵とコンテンツＩＤを鍵格納領域１８に格納する。バスＩ／Ｆ部では、この多重化されたデータをＰＣＩバス４、バスブリッジ２を介して主記憶３に転送し、主記憶３にある程度データが貯まったら、ＣＰＵ１でＨＤＤ等の記憶装置５に格納する。記録したコンテンツを再生する場合を説明する。記憶装置５に格納された再暗号化されたデータをＣＰＵ１で読み出しＰＣＩバス４を介してバスＩ／Ｆ部２３を通して再暗号コンテンツ復号器３５に入力する。この時コンテンツＩＤに対応した鍵を鍵格納領域１８から読み出し再暗号化されたコンテンツを復号して分離器１３に入力してコンテンツＩＤ等の余分なデータを削除してコンテンツデコーダ１４に転送する。コンテンツデコーダ１４によりデコードされ出力装置３０に送られ視聴する事ができる。また、コンテンツ暗号器３４で用いる暗号アルゴリズムを放送事業者がコンテンツを暗号化するときのアルゴリズムと同じにする事によりコンテンツ復号器１２と再暗号コンテンツ復号器３５を共通化する事も可能である。このように、この実施例でも記憶装置５に格納されるコンテンツは、暗号化されているため第１の実施例と同様の効果がある。

【００２７】

以上説明したように、本発明の第１～第４の実施例によれば、放送データを受信する装置において暗号化されたコンテンツを復号する暗号化された鍵を復号し再暗号化することで、記憶装置に暗号化されたままのコンテンツを格納でき、ファイル操作を行うことができるアプリケーションが動作するＰＣなどの情報処理装置に於いても、コンテンツの著作権の保護が可能でワーク鍵ｋｗが変更になってもコンテンツを視聴可能なデータ受信装置を提供できる。また、暗号化されたコンテンツを復号する暗号化された鍵を復号し再暗号化する機能を取り外しか可能な構造にする事により、別のデータ処理装置でもコンテンツの視聴が可能になる。

【００２８】

尚、上記第１～第４の実施例は、相互に組み合わせることが可能である。

上記第１～第４の実施例の各機器の処理は、ハードウェアで実行されてもよりし、プログラム（ソフトウェア）で実行されてもよい。そして、プログラムは、記憶媒体（例えば、フロッピーディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＭＯ等）に記憶されてもよいし、ネットワークを介してアクセス可能なサーバに記憶されてもよい。プログラムがサーバに記憶された場合は、ネットワークを介して、ダウンロードが可能である。

【００２９】
以上の実施の形態によれば、暗号化されたコンテンツが復号化できない状態で移動することができるため、コンテンツの著作者等の権利の保護を図りつつ、視聴者側で適切な記憶媒体や記憶装置でコンテンツを管理できるという効果を奏する。
【００３０】
次に図８を用いて第５の実施例を説明する。図８において５３は第４の実施例における鍵格納領域１８と識別ＩＤ２０の機能を持つ取り外し可能な鍵格納カードである。鍵格納カード５３は、カードＩ／Ｆ５４を介してコンテンツ暗号器３４と再暗号コンテンツ復号器３５に接続されているので、コンテンツ暗号器３４と再暗号コンテンツ復号器３５のアクセスは第４の実施例と同様に行える。また、第３の実施例で説明したように、識別ＩＤ２０を鍵格納カード５３毎にユニークなＩＤにしておけば、例えば記憶装置５に記録された多重化されたデータを、ＤＶＤ－ＲＡＭの様な外部記憶装置８にコピーしてこの外部記憶装置と鍵格納カード５３を本発明のデジタル放送データ転送処理装置１０が接続されているＰＣであれば他のＰＣでもコンテンツの視聴が可能になることは明らかである。
【００３１】
次に図９から１１を用いて第６の実施例を説明する。まず図９を用いて構成を説明する。図９において、６１と６２はそれぞれカードＩ／Ｆ５４を介してデータのやり取りを行う際に暗号通信の制御を行うデジタル放送データ転送処理装置１０側の暗号通信制御部で、鍵格納カード５３側のカード暗号通信制御部である。先述した、第３および５の実施例ではカードＩ／Ｆに鍵の情報がやり取りされ、カードＩ／Ｆのプロトコルがわかっている場合や規格化されていて一般に入手が可能な場合には、ユーザが信号をプローブすることで鍵を知ることが可能である。そこで、カードＩ／Ｆ部５４と鍵格納カード５３の間は暗号通信制御部６１とカード暗号通信制御部を用いてやり取りされるデータを暗号化することで鍵の情報などをユーザが簡単に入手できないようにする。
【００３２】
図１０を用いて、鍵を格納する場合の手順について説明する。ここで、Ｋｏは、公開鍵方式の公開鍵でデータを暗号化するときに使用される鍵で、Ｋｐは公開鍵方式の秘密鍵で暗号化されたデータを復号するときに使用される鍵で、Ｋｃは第４の実施例で述べた再暗号化されたコンテンツデータを復号するときに用いるコンテンツ鍵である。暗号通信制御部６１は、自身の認証データと予め保持している秘密鍵Ｋｐと対の公開鍵Ｋｏとを含んだ鍵格納指示を作成し、これを鍵格納カード５３に送信する（Ｔ１００１）。これを受けて鍵格納カード５３のカード暗号通信制御部６２はデジタル放送データ転送処理装置１０の認証を行う（Ｔ１００２）。それからカード暗号通信制御部６２は乱数などを用いてセッション鍵Ｋｓ１を生成し（Ｔ１００３）、これを鍵格納指示に含まれているＫｏを用いて暗号化して、送信元であるデジタル放送データ転送処理装置１０の暗号通信制御部６１に送信する（Ｔ１００４）。これを受けて暗号通信制御部６１は、暗号化されたセッション鍵Ｋｓ１を予め保持している秘密鍵Ｋｐを用いて復号し、セッション鍵Ｋｓ１を得る（Ｔ１００５）。それから乱数Ｋｓ２を生成して（Ｔ１００６）、この乱数Ｋｓ２をセッション鍵Ｋｓ１を用いて暗号化して鍵格納カード５３に送信する（Ｔ１００７）。鍵格納カード５３のカード暗号通信制御部６２では、セッション鍵Ｋｓ１を用いて暗号化された乱数Ｋｓ２を復号し、乱数Ｋｓ２を得る（Ｔ１００８）。そしてコンテンツの暗号化に必要な識別ＩＤ２０を乱数Ｋｓ２を用いて暗号化し暗号通信制御部６１に送信する（Ｔ１００９）。暗号通信制御部６１では、Ｋｓ２を用いて暗号化された識別ＩＤを復号し、識別ＩＤを得て（Ｔ１０１０）、コンテンツ暗号器３４よりコンテンツＩＤとコンテンツを復号するときに必要なライセンス鍵Ｋｃを得て（Ｔ１０１１）、これらをセッション鍵Ｋｓ１を用いて暗号化し鍵格納カード５３に送信する。そして鍵格納カード５３のカード暗号通信制御部６２でＫｓ１を用いて復号化し、コンテンツＩＤとライセンス鍵Ｋｃを得て、これらを鍵格納領域１８に格納する。このように、コンテンツの復号に必要な識別ＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃは、暗号化されてやり取りし、更にこれらの暗号に用いられるセッション鍵Ｋｓ１、乱数Ｋｓ２は、乱数などを用いて生成されるため暗号化されたデ

ータは毎回違うデータとなり、信号をプローブするだけでは鍵を知ることは困難となる。

【００３３】

図１１を用いて、コンテンツを復号（再生）する鍵を得る場合の手順について述べる。暗号通信制御部６１は、自身の認証データと予め保持している秘密鍵Ｋｐと対の公開鍵Ｋｏとを含んだ鍵送信指示を作成し、これを鍵格納カード５３に送信する（Ｔ１１０１）。これを受けて鍵格納カード５３のカード暗号通信制御部６２はデジタル放送データ転送処理装置１０の認証を行う（Ｔ１１０２）。それからカード暗号通信制御部６２は乱数などを用いてセッション鍵Ｋｓ１を生成し（Ｔ１１０３）、これを鍵格納指示に含まれているＫｏを用いて暗号化して、送信元であるデジタル放送データ転送処理装置１０の暗号通信制御部６１に送信する（Ｔ１１０４）。これを受けて暗号通信制御部６１は、暗号化されたセッション鍵Ｋｓ１を予め保持している秘密鍵Ｋｐを用いて復号し、セッション鍵Ｋｓ１を得る（Ｔ１１０５）。それから乱数Ｋｓ２を生成して（Ｔ１１０６）、この乱数Ｋｓ２をセッション鍵Ｋｓ１を用いて暗号化して鍵格納カード５３に送信する（Ｔ１１０７）。鍵格納カード５３のカード暗号通信制御部６２では、セッション鍵Ｋｓ１を用いて暗号化された乱数Ｋｓ２を復号し、乱数Ｋｓ２を得る（Ｔ１００８）。そしてコンテンツの復号化に必要な識別ＩＤ２０とライセンス鍵Ｋｃを乱数Ｋｓ２を用いて暗号化し暗号通信制御部６１に送信する（Ｔ１１０９）。暗号通信制御部６１では、Ｋｓ２を用いて暗号化された識別ＩＤとライセンス鍵Ｋｃを復号し、識別ＩＤとライセンス鍵Ｋｃを得て（Ｔ１１１０）、これらの識別ＩＤとライセンス鍵Ｋｃを再暗号コンテンツ復号器３５に送りコンテンツを復号化する。この場合も先述したように、信号をプローブするだけでは鍵を知ることは困難となる。

【００３４】

次に図１２を用いて第７の実施例を説明する。図１２において５７は、暗号化したコンテンツデータを格納するコンテンツ格納領域で、５５はコンテンツ格納領域に第６の実施例で説明した暗号通信を用いて識別ＩＤやコンテンツ鍵をやり取りする鍵格納カードの機能を具備した鍵格納領域付記憶装置で、５６は、コンテンツ格納領域５７や鍵格納領域や識別ＩＤをアクセスするためのカード・格納領域Ｉ／Ｆ部である。これらを用いて動作を説明する。最初にコンテンツを記録する場合を説明する。チューナ１１により暗号化された番組を受信し、コンテンツ復号器１２を通り分離器１３で、暗号化されたコンテンツデータと暗号化されたスクランブル鍵Ｋｓに分離する。分離された暗号化されたスクランブル鍵ＫｓはローカルＣＰＵ１５によりＩＣカード１６で復号化され、ローカルＣＰＵ１５で復号化されたスクランブル鍵Ｋｓをコンテンツ復号器１２に設定する。

【００３５】

コンテンツ復号器１２で復号されたコンテンツデータは分離器１３によりコンテンツデコーダ１４とコンテンツ暗号器３６に送られる。コンテンツデコーダ１４でコンテンツをデコードして出力装置３０に出力してコンテンツを視聴できる。コンテンツ暗号器３６では、暗号通信を用いて方送受信データ転送処理装置毎のユニークな識別情報である識別ＩＤ２０を取得し、これと乱数発生器２１で生成された乱数をもちいて暗号化する。ここで生成したコンテンツ鍵とコンテンツＩＤを暗号通信を用いて書き格納領域１８に格納する。コンテンツ暗号器３６は再暗号化されたコンテンツデータをカード・格納領域Ｉ／Ｆ部を介してコンテンツＩＤとともにコンテンツ領域５７に格納される。また、復号するときは鍵格納領域付記憶装置５５のコンテンツ格納領域５７に格納された暗号化されたコンテンツデータとコンテンツＩＤを再暗号コンテンツ復号器３７が読み出し、暗号通信を用いてコンテンツＩＤに対応したコンテンツ鍵と識別ＩＤをそれぞれ鍵格納領域１８と識別ＩＤ２０から読み出し、暗号化されたコンテンツデータを復号する。それから、復号化されたコンテンツデータは分離器１３を介してコンテンツデコーダ１４に入力され出力装置３０で出力されコンテンツを視聴することができる。

【００３６】

また、鍵格納領域１８はコンテンツを再暗号化するとその都度コンテンツ鍵が増えていくが、鍵格納領域１８は有限の容量しか持たないため一杯になってしまう場合がある。その

ときには鍵格納カードを複数枚で管理することになりユーザが管理するのに不便である。しかし、図１２の様な構成をとれば、コンテンツを格納する領域の容量により、鍵格納領域の容量を適当に決めることにより上記のような問題は少なくなり、またコンテンツと鍵は常に一緒にあるため鍵とコンテンツを分けて管理する必要がなくユーザにとって便利である。コンテンツデータをあるグループ毎にコンテンツ鍵１つに関連付けたり、コンテンツ格納領域をある単位毎に分けそこに格納されるコンテンツ毎に関連図けることにより鍵格納領域の容量を削減することも可能である。また、図１２のコンテンツ格納領域５７は、ＨＤＤや半導体記憶装置であったり、ＤＶＤ－ＲＡＭや磁気テープでもメディアのケースに電極などをつけ鍵格納領域や識別ＩＤを持たせることで鍵格納領域付記憶装置とすること可能である。

【００３７】

次に図１３を用いて第８の実施例を説明する。図１３において６９は暗号化コンテンツを復号するときに用いるコンテンツ鍵で、６８はコンテンツ鍵６９に対応した鍵インデックスで、６７は複数のコンテンツ鍵６９と鍵インデックス６８の対を格納する鍵格納領域で、４０は鍵インデックスを暗号化したり復号化したりする鍵インデックス暗号復号器である。

【００３８】

これらを用いて動作を説明する。最初にコンテンツを記録する場合を説明する。チューナ１１により暗号化された番組を受信し、コンテンツ復号器１２を通り分離器１３で、暗号化されたコンテンツデータと暗号化されたスクランブル鍵Ｋｓに分離する。分離された暗号化されたスクランブル鍵ＫｓはローカルＣＰＵ１５によりＩＣカード１６で復号化され、ローカルＣＰＵ１５で復号化されたスクランブル鍵Ｋｓをコンテンツ復号器１２に設定する。コンテンツ復号器１２で復号されたコンテンツデータは分離器１３によりコンテンツデコーダ１４とコンテンツ暗号器３８に送られる。コンテンツデコーダ１４でコンテンツをデコードして出力装置３０に出力してコンテンツを視聴できる。コンテンツ暗号器３８では、乱数発生器２１で生成された乱数を用いて鍵格納領域６７の複数あるコンテンツ鍵のどれを使用するかを決める鍵インデックスを生成し、暗号通信を用いてこの鍵インデックスを鍵格納カード６６に送信して、鍵インデックス６８に対応したコンテンツ鍵６９と識別ＩＤ２０を得る。ここで取得したコンテンツ鍵と識別ＩＤを用いてコンテンツデータを暗号化して、更に鍵インデックス暗号復号器４０である特定の鍵を用いて鍵インデックスを暗号化して、暗号化されたコンテンツデータとともにバスＩ／Ｆ部２３を介して主記憶３に転送し最終的には、記憶装置５または外部記憶装置８に格納する。また、鍵インデックス暗号復号器では、ある特定の鍵で暗号化すると暗号化された結果も鍵インデックスが同じであれば同じデータとなってしまうため鍵インデックスに乱数などの冗長なデータをつけて暗号化すれば結果も異なり鍵インデックスが解読される可能性は低くなる。次に記録したコンテンツを再生する場合を説明する。記憶装置５に格納された再暗号化されたデータをＣＰＵ１で読み出しＰＣＩバス４を介してバスＩ／Ｆ部２３を通して再暗号コンテンツ復号器３９に入力する。この時コンテンツデータとともに格納されている暗号化された鍵インデックスを鍵インデックスを鍵インデックス暗号復号器４０で特定の鍵で復号し、鍵インデックスを得る。それから暗号通信を用いて鍵インデックスを鍵格納カードに送信して、鍵インデックス６８に対応したコンテンツ鍵６９と識別ＩＤ２０を得る。そして、再暗号コンテンツ復号器でコンテンツデータを復号して分離器１３に入力してコンテンツＩＤ等の余分なデータを削除してコンテンツデコーダ１４に転送する。コンテンツデコーダ１４によりデコードされ出力装置３０に送られ視聴する事ができる。

【００３９】

このような構成にすると、鍵格納カードには新たなコンテンツ鍵を追加する必要がないので暗号化してコンテンツを格納する場合コンテンツの数が増えても、鍵格納カードは増える心配がなく、ユーザも１枚のカード管理すれば良いだけであるので鍵の管理が簡単になり便利である。また、鍵管理カード毎にコンテンツ鍵と識別ＩＤを変えることで暗号化のときに用いた鍵格納カードとは違う鍵格納カードを用いて再生しようとしても同じ鍵イン

デックスであってもコンテンツ鍵か違いまた識別ＩＤも異なるためコンテンツデータを復号することはできなので、著作権保護が可能となる。

【００４０】

以上説明したように、本発明の一実施態様によれば、放送データを受信する装置において暗号化されたコンテンツデータを復号する暗号化された鍵を復号し再暗号化することで、記憶装置に暗号化されたままのコンテンツデータを格納でき、ファイル操作を行うことができるアプリケーションが動作するＰＣなどのデータ処理装置に於いても、コンテンツデータの著作権の保護が可能でワーク鍵ｋｗが変更になってもコンテンツを視聴可能なデジタル放送データ転送処理装置を提供できる。また、暗号化されたコンテンツデータを復号する暗号化された鍵を復号し再暗号化する機能を取り外しか可能な構造にする事により、別のデータ処理装置でもコンテンツの視聴が可能になる。

【００４１】

【発明の効果】

本発明の構成により、暗号化されて送信されるコンテンツを保存し、再生することが可能になる。

【図面の簡単な説明】

【図１】本発明の第１の実施例の情報処理装置のシステム構成図である。

【図２】従来の限定受信方式のシステム構成図である。

【図３】デジタル放送データを受信し記録する情報処理装置の１システム構成図である。

【図４】本発明の第１の実施例のスクランブル鍵を再暗号化する暗号器のシステム構成図である。

【図５】本発明の第２の実施例の情報処理装置のシステム構成図である。

【図６】本発明の第３の実施例の情報処理装置のシステム構成図。

【図７】本発明の第４の実施例の情報処理装置のシステム構成図。

【図８】本発明の第５の実施例を示すブロック図である。

【図９】暗号通信を用いて鍵を格納するデータのやり取りの一例を示すためのシーケンス図である。

【図１０】暗号通信を用いて鍵を取得するデータのやり取りの一例を示すためのシーケンス図である。

【図１１】本発明の第６の実施例を示すブロック図である。

【図１２】本発明の第７の実施例を示すブロック図である。

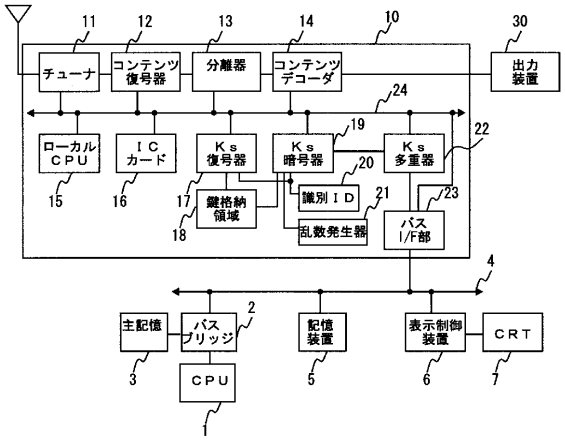
【図１３】本発明の第８の実施例を示すブロック図である。

【符号の説明】

１・・・ＣＰＵ、２・・・バスブリッジ、３・・・主記憶、４・・・ＰＣＩバス、５・・・記憶装置、６・・・表示制御部、７・・・ＣＲＴ、８・・・外部記憶装置、１０・・・デジタル放送データ転送処理装置、１１・・・チューナ、１２・・・コンテンツ復号器、１３・・・分離器、１４・・・コンテンツデコーダ、１５・・・ローカルＣＰＵ、１６・・・ＩＣカード、１７・・・Ｋｓ復号器、１８・・・鍵格納領域、１９・・・Ｋｓ暗号器、２０・・・識別ＩＤ、２１・・・乱数発生、２２・・・Ｋｓ多重器、２３・・・バスＩ／Ｆ部、２４・・・ローカルバス、３０・・・出力装置

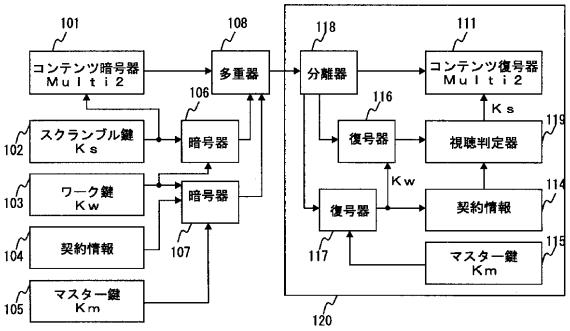
【図１】

【図１】



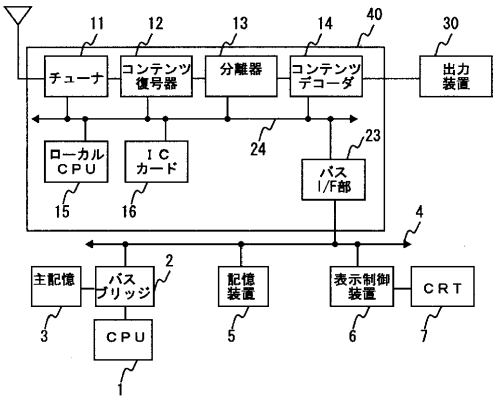
【図２】

【図２】



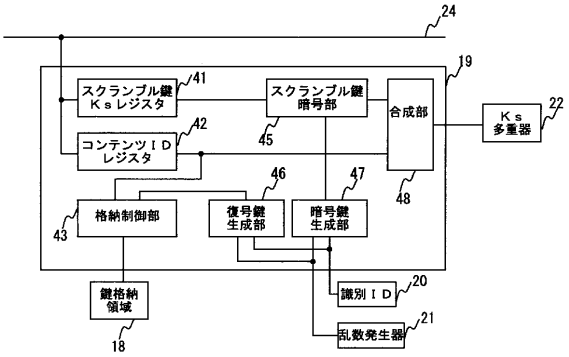
【図３】

【図３】

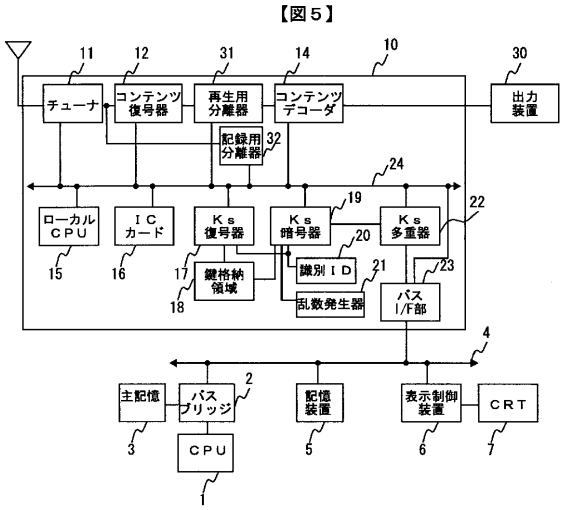


【図４】

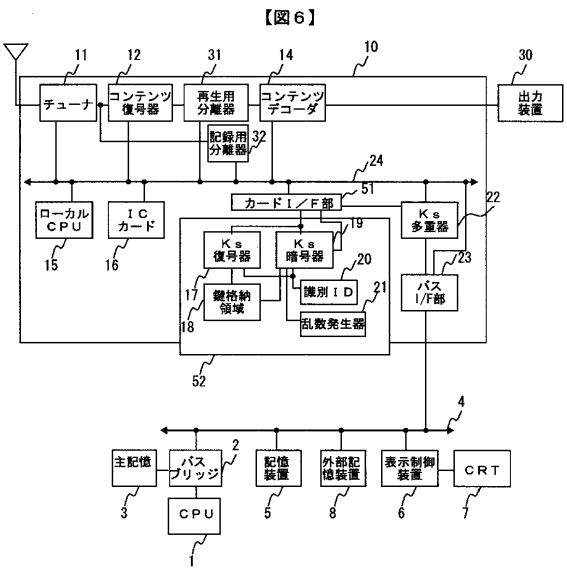
【図４】



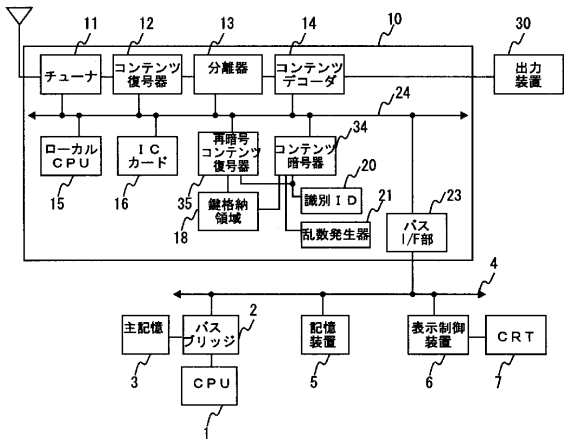
【図５】


【図５】
チューナ
コンテンツ復号器
再生用分離器
コンテンツデコーダ
出力装置
記録用分離器
ローカルCPU
ＩＣカード
Ｋｓ復号器
Ｋｓ暗号器
Ｋｓ多重器
鍵格納領域
識別ＩＤ
乱数発生器
バスI/F部
主記憶
バスブリッジ
CPU
記憶装置
表示制御装置
CRT

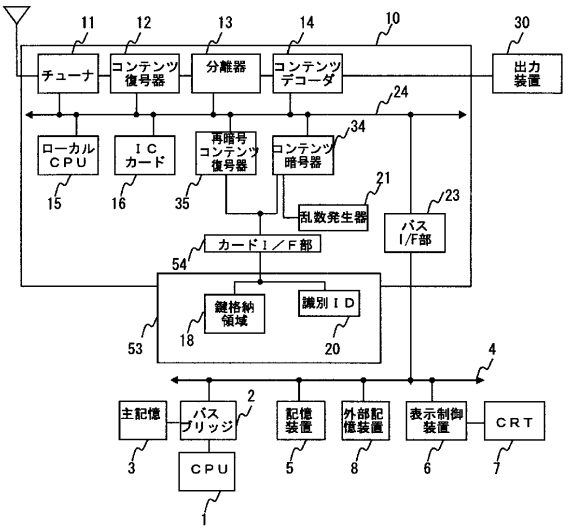
【図６】


【図６】
チューナ
コンテンツ復号器
再生用分離器
コンテンツデコーダ
出力装置
記録用分離器
カードＩ／Ｆ部
ローカルCPU
ＩＣカード
Ｋｓ復号器
Ｋｓ暗号器
Ｋｓ多重器
鍵格納領域
識別ＩＤ
乱数発生器
バスI/F部
主記憶
バスブリッジ
CPU
記憶装置
外部記憶装置
表示制御装置
CRT

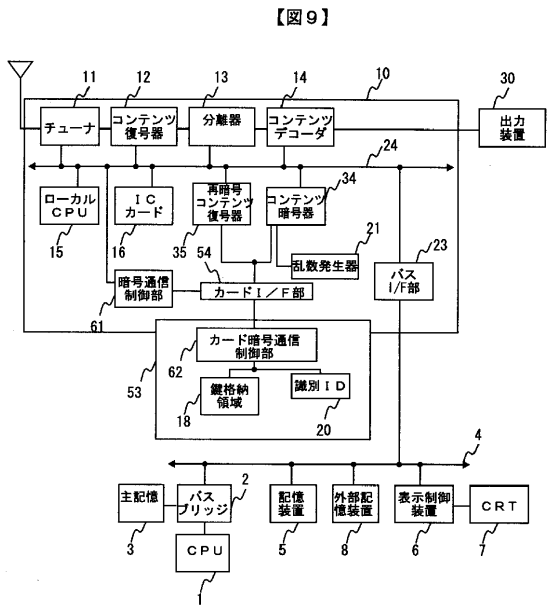
【図７】


【図７】
チューナ
コンテンツ復号器
分離器
コンテンツデコーダ
出力装置
ローカルCPU
ＩＣカード
再暗号コンテンツ復号器
コンテンツ暗号器
鍵格納領域
識別ＩＤ
乱数発生器
バスI/F部
主記憶
バスブリッジ
CPU
記憶装置
表示制御装置
CRT

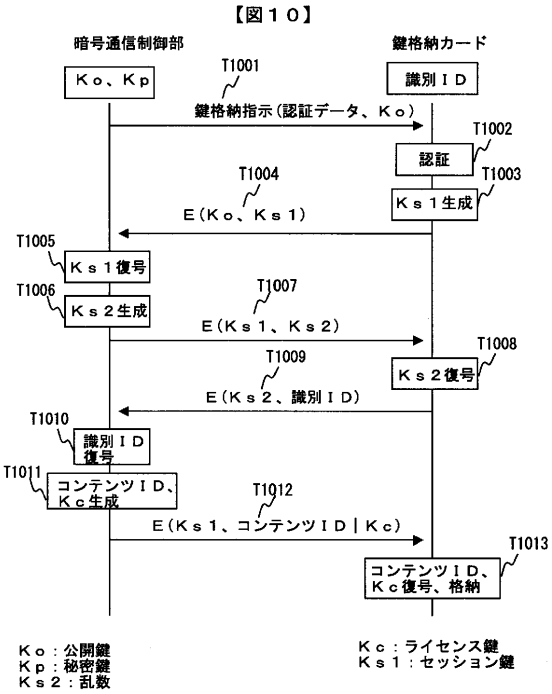
【図８】


【図８】
チューナ
コンテンツ復号器
分離器
コンテンツデコーダ
出力装置
ローカルCPU
ＩＣカード
再暗号コンテンツ復号器
コンテンツ暗号器
乱数発生器
バスI/F部
カードＩ／Ｆ部
鍵格納領域
識別ＩＤ
主記憶
バスブリッジ
CPU
記憶装置
外部記憶装置
表示制御装置
CRT

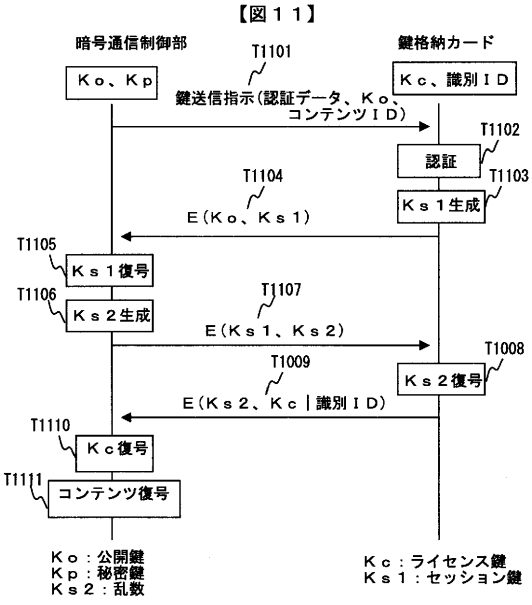
【図９】



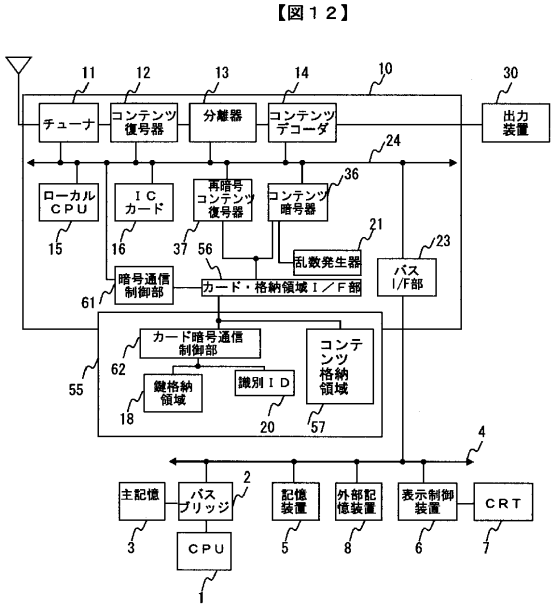
【図１０】



【図１１】

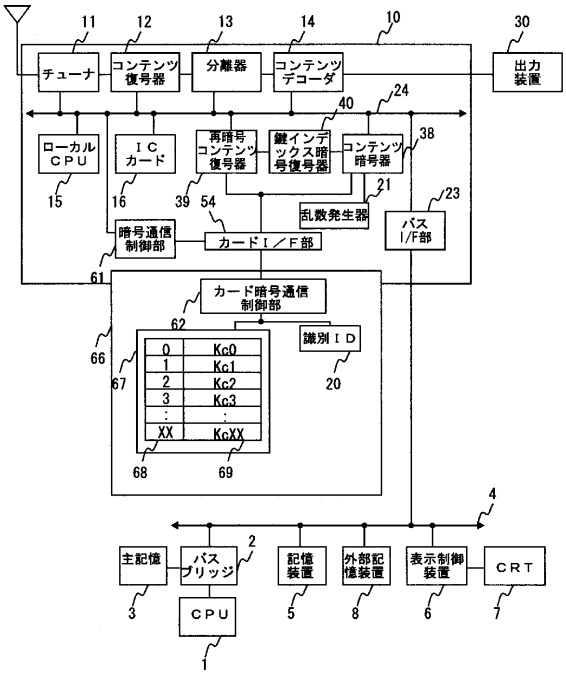


【図１２】



【図１３】

【図１３】


11
12
13
14
10
30
チューナ
コンテンツ復号器
分離器
コンテンツデコーダ
出力装置
24
40
ローカルCPU
ＩＣカード
再暗号コンテンツ復号器
鍵インデックス暗号復号器
コンテンツ暗号器
38
15
16
39
54
21
23
乱数発生器
バスI/F部
暗号通信制御部
カードＩ／Ｆ部
61
カード暗号通信制御部
62
識別ＩＤ
66
67
20
0 Kc0
1 Kc1
2 Kc2
3 Kc3
XX KcXX
68
69
4
主記憶
バスブリッジ
2
記憶装置
外部記憶装置
表示制御装置
CRT
CPU
3
5
8
6
7
1

フロントページの続き

(72)発明者　友兼　武郎
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　小檜山　智久
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

審査官　中里　裕正

(56)参考文献　特開平０２－０４１０５１（ＪＰ，Ａ）
特開平０８－０７９２３４（ＪＰ，Ａ）
特開平０８－１２５６５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08
H04L 9/14
H04N 7/16