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

特許第5046340号
(P5046340)

(45)発行日　平成24年10月10日(2012.10.10)　(24)登録日　平成24年7月27日(2012.7.27)

(51)Int.Cl.		F I		
H04N 7/167	(2011.01)	H04N	7/167	Z
H04N 5/91	(2006.01)	H04N	5/91	P
H04L 9/08	(2006.01)	H04L	9/00	601B
H04H 60/23	(2008.01)	H04L	9/00	601E
H04H 60/27	(2008.01)	H04H	60/23	

請求項の数 1　(全 18 頁)　最終頁に続く

(21)出願番号　特願2009-248579 (P2009-248579)
(22)出願日　平成21年10月29日 (2009.10.29)
(62)分割の表示　特願平10-525990の分割
　原出願日　平成9年10月28日 (1997.10.28)
(65)公開番号　特開2010-88121 (P2010-88121A)
(43)公開日　平成22年4月15日 (2010.4.15)
　審査請求日　平成21年11月27日 (2009.11.27)
(31)優先権主張番号　08/762,488
(32)優先日　平成8年11月27日 (1996.11.27)
(33)優先権主張国　米国 (US)

(73)特許権者　391000818
トムソン　コンシューマ　エレクトロニクス　インコーポレイテッド
THOMSON CONSUMER ELECTRONICS, INCORPORATED
アメリカ合衆国　インディアナ州　４６２９０－１０２４　インディアナポリス　ノース・メリデイアン・ストリート　１０３３０
(74)代理人　100115864
弁理士　木越　力
(74)代理人　100121175
弁理士　石井　たかし

最終頁に続く

(54)【発明の名称】ディジタル・ビデオ・データを処理する装置

(57)【特許請求の範囲】
【請求項１】
放送源から暗号化されたビデオ・データを受信して処理する装置であって、
前記放送源から受け取る暗号化コードを解読して、前記暗号化された放送ビデオ・データを解読する際に使用する暗号化キーを生成する手段と、
前記暗号化キーを第１の記憶手段に記憶されたアルゴリズムを使用することにより暗号化して暗号化された再生キーを生成する手段と、
前記暗号化された再生キーを前記暗号化されたビデオ・データと共に第２の記憶手段に保存する手段と、
前記第２の記憶手段から供給された前記暗号化された再生キーを解読して再生キーを生成する手段と、
前記解読された再生キーを使用して、前記第２の記憶手段から供給された前記暗号化されたビデオ・データを解読する手段と、
前記解読されたビデオ・データを出力する手段と、
を備える、前記装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ディジタル信号処理の分野に関し、特に、例えば、放送、衛星またはケーブルのビデオ・データを消費者用受像機によって保存するための、暗号化されたパケット・

データの条件付きアクセス処理、復号化およびフォーマット化に関する。

【背景技術】

【０００２】

ビデオ・データを処理し保存する場合、ディジタル・ビデオ・データは、既知の標準の要件に合うように符号化されるのが典型的である。そのように広く採用されている１つの標準は、ＭＰＥＧ２（Moving Pictures Expert Group）の画像符号化標準（以下、“ＭＰＥＧ標準”と称す）である。このＭＰＥＧ標準は、システム符号化部門（ＩＳＯ／ＩＥＣ１３８１８－１，１９９４年６月１０日）と、ビデオ符号化部門（ＩＳＯ／ＩＥＣ１３８１８－２，１９９５年１月２０日）とで構成され、以下にそれぞれ、“ＭＰＥＧシステム標準”および“ＭＰＥＧビデオ標準”と称す。ＭＰＥＧ標準に従って符号化されるビデオ・データはパケット化されたデータストリームの形式をとり、典型的に、多数の番組チャンネル（例えば、ケーブルテレビの１～１２５チャンネルに類似する）のデータ内容を含んでいる。例えば、ＨＢＯ^{TM}（登録商標）、Ｃｉｎｅｍａｘ^{TM}（登録商標）、Ｓｈｏｗｔｉｍｅ^{TM}（登録商標）のようなプレミアム番組チャンネルのデータ内容は通常、暗号化やスクランブルのような方法により、無許可のアクセスから保護される。これらの方法は、単独で繰返しまたは組合わせて、使用され、複数の保護レベルが与えられる。

【０００３】

デコーダでは、プレミアム・チャンネルへのアクセスは、典型的には、条件付きアクセス方式によって支配され、ユーザへの支払請求が管理され、ユーザの資格に基づき番組のデスクランブル（スクランブル解除）および暗号解読が規制される。条件付きアクセス方式は種々の方法で、アクセスが許可されているかを判断する。例えば、許可は、いわゆる「スマート・カード」に予めプログラムされるユーザの資格情報から、デコーダの内部で判定され、あるいは、ペイ・パー・ビュー（視聴した番組の本数に応じて料金を支払う）ケーブルテレビの場合のように、遠隔地で判定され、遠隔地から送られるユーザの資格情報を使用して、デコーダ内部で実行される。資格情報は典型的には、番組のスクランブル解除や暗号解読に使用されるデスクランブル・キーおよび暗号解読キーを発生するのに使用されるコード（符号）を含むが、資格情報はそのようなキー自体を含むこともある（例えば、特許文献１）。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】欧州特許出願公開第０７０４７８５Ａ２号明細書

【発明の概要】

【発明が解決しようとする課題】

【０００５】

暗号化された番組や暗号化されてない番組データの処理、並びに保存、支払請求その他に使用するための、関連する暗号化コードおよびスクランブル・コードの管理は、いくつかの問題を起こす。１つの問題は、視聴者が番組を、あとで見るために、暗号化された形式か暗号化されない形式で保存する場合に暗号化コードの安全保護（security）を維持する必要から起こる。更に別の問題は、番組の保存または再生について支払請求ができ且つ暗号化された番組や暗号化されてない番組データのコピー防止処理ができるシステムを提供することである。

【０００６】

これらの問題は、本発明によるシステムで処理される。以下、「暗号化」という言葉は、無許可の使用を防止する程度のスクランブル機能を含む。

【０００７】

暗号化された形式で番組を処理するデコーダ・システムで、暗号化コードの安全保護を維持するのに使用される１つの技術は、定期的または非定期的に、暗号化アルゴリズムおよび暗号化キーを変更することである。このようなアルゴリズムの変更は典型的に、暗号化システムの安全保護を守り且つコードの解読（code-breaking）や無許可の番組アクセ

スを防止するために、サービス・プロバイダによって開始される。ここで、発明者たちは、暗号化アルゴリズムと暗号化キーを変更するシステムを使用すると、暗号化された形式での番組の保存について問題が生じることを認識する。特に、暗号化された形式で、関連する放送暗号化キーと共に保存された番組は、ひとたび暗号化アルゴリズムが更新されると、解読されないこともある。新しい暗号化アルゴリズムは、それ以前に保存された暗号化キーと互換性がない。そのため、暗号化されて保存された番組は、ひとたびアルゴリズムが変更されると、暗号解読されず、使用できなくなる。

【課題を解決するための手段】

【０００８】

この問題を解決するために、別のアルゴリズムがデコーダの条件付きアクセス・システムに有利に組み込まれる。条件付きアクセス・システムは、局所的な保存源（例えば、記録媒体）から得られる番組に対するのとは異なる動作で、「生の」ソース（例えば、同時放送）から得られる番組にアクセスできるようにする。

【０００９】

暗号化された番組および暗号化コードを処理するための条件付きアクセス・プロセッサは、暗号化コードを解読して暗号化キーを供給するための第１のアルゴリズム手段を含む。条件付きアクセス・プロセッサはまた、暗号化キーを暗号化するための第２のアルゴリズムを含み、この第２の暗号化アルゴリズムは第１の暗号化アルゴリズムとは異なる。

【００１０】

本発明の特徴により、暗号化された番組データおよび関連する暗号化コードから、番組を表すデータストリームを発生する方法では、暗号化コードを解読し、第１のアルゴリズムを使用して暗号化キーを供給する。この暗号化キーは、第１の暗号化アルゴリズムとは異なる第２のアルゴリズムを使用して暗号化され、番組のデータストリームは、暗号化された番組データおよび暗号化された暗号化キーから形成される。

【００１１】

本発明の別の特徴により、番組を表すデータストリームを復号化する方法では、暗号化コードを解読するために第１と第２のアルゴリズムを選択する。暗号化コードは解読され、選択されたアルゴリズムを使用して暗号化キーを供給し、暗号化された番組は、この暗号化キーを使用して解読される。

【００１２】

本発明の更に別の特徴により、第１の暗号化アルゴリズムと暗号化コードを使用して暗号化された番組データを記録するための記録媒体のデータ・フォーマットが開示される。暗号化コードは、第１の暗号化アルゴリズムとは異なる第２の暗号化アルゴリズムを使用して、暗号化キーを暗号化することにより得られる。

【図面の簡単な説明】

【００１３】

【図１】番組を表すデータストリームをユーザが選択できる暗号化されたまたは暗号化されない形式で適応的に発生するための、本発明によるビデオ受信システムを示す。

【図２】選択可能な記録媒体に保存するのに適する、番組を表すデータストリームを供給すると共に、それに関連してユーザへの支払請求を実行するためのプロセス・フローチャートを示す。

【図３】選択可能な記録媒体に保存するのに適する、番組を表すデータストリームを供給すると共に、それに関連してユーザへの支払請求を実行するためのプロセス・フローチャートを示す。

【図４】暗号化された番組または暗号化されてない番組を選択し、選択された記憶装置から再生すると共に、番組の再生についてユーザに支払請求するためのプロセス・フローチャートを示す。

【発明を実施するための形態】

【００１４】

第１図は、番組を表すデータストリームを、ユーザが選択できる暗号化されたまたは暗

号化されない形式で適応的に発生するための、本発明によるビデオ受信システムである。開示されたシステムは、放送番組を表すＭＰＥＧ符号化されたトランスポート・ストリームを受け取るための、ＭＰＥＧと互換性のあるシステムに関連して説明されているが、これは例示的なものに過ぎない。本発明の原理は、他のタイプの符号化されたデータストリームを含む、ＭＰＥＧと互換性のない他のタイプのシステムにも応用される。更に、ここに開示されたシステムは、放送番組を処理するものとして説明されているが、これは例示的なものに過ぎない。「プログラム(program）；番組」という用語は、あらゆる形式のパケット化されたデータ、例えば、電話のメッセージ、コンピュータ・プログラム、インターネット・データその他の通信情報を表すためにも使用されている。

【００１５】

概略を述べると、第１図のビデオ受信システムにおいて、ビデオ・データで変調された搬送波はアンテナ１０で受信され、入力プロセッサ１５で処理される。その結果生じるディジタル出力信号は復調器２０で復調され、デコーダ３０で復号化される。デコーダ３０からの出力は、リモコン１２５からのコマンドに応答するトランスポート・システム２５で処理される。トランスポート・システム２５は、圧縮されたデータ出力を、保存し更に復号化しあるいは他の装置に送るために供給する。トランスポート・システム２５は、ユーザへの支払請求を管理し、且つユーザの資格に基づき番組のスクランブル解除および暗号解読を規制するために、条件付きアクセス方式を組み込んでいる。ビデオ受信機のユーザは、自分が見たい番組、保存したい番組、使用する記録媒体のタイプ、番組を暗号化された形式でそれとも暗号化されない形式で保存するのかを、リモコン１２５を使用して画面上のメニューにより選択する。トランスポート・システム２５はまた、暗号化されてない番組のデータストリームから暗号化コードをリアルタイムあるいは非リアルタイムで除去できるようにする機構を提供する。

【００１６】

ビデオ・デコーダとオーディオ・デコーダ８５と８０はそれぞれ、トランスポート・システム２５からの圧縮されたデータを復号化し、表示用の出力を供給する。データ・ポート７５は、システム２５から他の装置、例えば、コンピュータや高精細度テレビジョン（ＨＤＴＶ）受像機へ圧縮されたデータを伝送するためのインタフェースを提供する。記憶装置９０はシステム２５からの圧縮されたデータを記録媒体１０５に保存する。再生モードで記憶装置９０は、圧縮されたデータを、システム２５で処理し復号化し他の装置に伝送しあるいは別の記録媒体（図面を簡略にするために図示せず）に保存するために、記録媒体１０５から取り出すのをサポートする。システム２５内部にある条件付きアクセス・システムは、番組の保存、再生、または他の装置への伝送を含む更なる処理のための、暗号解読および支払請求をサポートする。トランスポート・システム２５の条件付きアクセス・システムは、放送源から受信する番組データを処理するために、局所的なソースから再生されるデータとは異なる暗号解読・支払請求機構を使用する。

【００１７】

第１図を詳細に考察すると、アンテナ１０で受信するビデオ・データで変調された搬送波は、入力プロセッサ１５でディジタル形式に変換され処理される。プロセッサ１５は、無線周波（ＲＦ）チューナ、および中間周波（ＩＦ）ミクサー、および入力ビデオ信号を更に処理するために比較的低い周波数にダウン・コンバートする増幅段を含んでいる。その結果生じるディジタル出力信号は復調器２０で復調され、デコーダ３０で復号化される。デコーダ３０からの出力はトランスポート・システム２５で更に処理される。

【００１８】

サービス検出器３３のマルチプレクサ（ＭＵＸ）３７は、選択器３５を介して、デコーダ３０からの出力を供給され、あるいはＮＲＳＳ（National Renewable Standards Committee）のスクランブル解除装置４０で更に処理されるデコーダ３０の出力を供給される。選択器３５は、挿入可能な、ＮＲＳＳと互換性のスクランブル解除カードの存在を検出し、カードが受像機内に現在挿入されている場合に限り、装置４０の出力をＭＵＸ３７に供給する（ＮＲＳＳの取り外し可能な条件付きアクセス・システムは、EIA草案　IS-67

9, Project PN-3639 で規定されている）。それ以外の場合には、選択器３５はデコーダ３０からの出力をＭＵＸ３７に供給する。挿入可能なカードが存在すると、ユニット４０は、例えば、追加的なプレミアム番組チャンネルのスクランブルを解除し、視聴者に追加的な番組サービスを提供することができる。注目すべきは、ＮＲＳＳユニット４０とスマート・カード・ユニット１３０（スマート・カード・ユニット１３０についてはあとで述べる）は、同じシステム２５のインタフェースを共有しており、一度に挿入できるのはＮＲＳＳカードまたはスマート・カードのいずれかに限られることである。あるいは、直列動作または並列動作を可能にするためにインタフェースを別々にしてもよい。

【００１９】

選択器３５からＭＵＸ３７に供給されるデータは、ＭＰＥＧシステム標準２．４項に規定される、ＭＰＥＧに準拠するパケット化されたトランスポート・データストリームの形式をとる。特定の番組チャンネルを含む個々のパケットはパケット識別子（ＰＩＤ：Packet Identifier）によって識別される。トランスポート・ストリームには、トランスポート符号化データの伝送と復号化をサポートする補助的なデータが含まれている。この補助的データの中には、パケット化されたデータストリームを含む全ての番組チャンネルの内容を再生するために、ＰＩＤを識別して個々のデータ・パケットを組み立てる際に使用する、番組に固有の情報（ＰＳＩ：Program Specific Information）が含まれている。受像機のユーザは、リモコン１２５を使用して画面上のメニューを選択して、見たい番組、保存したい番組、保存に使用する媒体、および番組を暗号化して保存するのかそれとも暗号化せずに保存するのか、を選択する。システム・コントローラ１１５は、インタフェース１２０を介して供給される選択情報を使用して、保存および表示用の番組を選択すると共に、選択された記憶装置と記録媒体に適するＰＳＩを発生するようにトランスポート・システム２５を構成する。コントローラ１１５は、システム２５の要素４５、４７、５０、６５、９５内部の制御レジスタの値をデータ・バスを介して設定し且つＭＵＸ３７と１１０を通る信号経路を制御信号Ｃで選択することにより、これらの要素（４５、４７、５０、６５、９５）を構成する。コントローラ１１５はまた、保存しあるいは処理する暗号化されてない番組データストリームから、暗号化コードをリアルタイムおよび非リアルタイムで除去できるようにプログラムできる。この特徴は、暗号化キーがシステム２５の外に出るのを防ぎそれにより第三者に利用されるのを制限することにより、暗号化の安全保護が高められる。

【００２０】

ＭＵＸ３７は、制御信号Ｃに応答して、選択ユニット３５からトランスポート・ストリームを選択するか、または再生モードで、ストア（記憶；保存）インタフェース９５を介して記憶装置９０から取り出されるデータストリームを選択する。通常の、非再生動作において、ユーザが見るために選択した番組を含んでいるデータ・パケットは、そのＰＩＤによって選択ユニット４５で識別される。パケットが暗号化されていることを、選択された番組パケットのヘッダ・データ内の暗号化指標が示している場合、選択ユニット４５はそのパケットを暗号解読ユニット５０へ供給する。そうでない場合、選択ユニット４５は暗号化されてないパケットをトランスポート・デコーダ４５に供給する。同様にして、ユーザが保存するために選択した番組を含んでいるデータ・パケットはそのＰＩＤによって選択ユニット４７で識別される。ユニット４７は、パケット・ヘッダの暗号化指標の情報に基づいて、暗号化されたパケットを暗号解読ユニット５０に供給するかまたは暗号化されてないパケットをＭＵＸ１１０に供給する。

【００２１】

選択ユニット４５と４７は検出フィルタを使用して、ＭＵＸ３７より供給される入来パケットのＰＩＤの値を、コントローラ１１５により、選択ユニット４５と４７内部の制御レジスタ内に予めロードされているＰＩＤの値とマッチさせる。予めロードされたＰＩＤは、選択ユニット４７および４５内で使用され、保存するデータ・パケット、およびビデオ画像を供給する際に復号化するデータ・パケットを識別する。予めロードされたＰＩＤはユニット４５および４７内のルックアップ・テーブル内に貯えられる。このＰＩＤルッ

クアップ・テーブルは、暗号化キーと予めロードされたＰＩＤを関連付けるユニット４５および４７内の暗号化キー・テーブルにメモリ・マップされる。メモリ・マップされたＰＩＤおよび暗号化キー・ルックアップ・テーブルにより、ユニット４５と４７は、予めロードされたＰＩＤを含んでいる暗号化されたパケットを、それに関連する、暗号化されたパケットの解読を可能にする暗号化キーとマッチさせることができる。暗号化されてないパケットは、それに関連する暗号化キーを持たない。選択ユニット４５と４７は、識別されたパケットおよびそれに関連する暗号化キーを暗号解読器５０に供給する。ユニット４５内のＰＩＤルックアップ・テーブルはデスティネーション(送信先)テーブルにメモリ・マップされる。送信先テーブルは、予めロードされたＰＩＤを含んでいるパケットを、それと対応する、パケット・バッファ６０内の送信先バッファの位置とマッチさせる。ユーザが見るためにまたは保存するために選択した番組に関連する、暗号化キーおよび送信先バッファの位置のアドレスは、割り当てられたＰＩＤと共に、コントローラ１１５によって、選択ユニット４５と４７の中へ予めロードされる。

【００２２】

暗号化キーは、ＩＳＯ７８１６－３に準拠するスマート・カード・システム１３０によって、入力データストリームから抽出される暗号化コードから発生される。暗号化キーの発生は、挿入可能なスマート・カード自体に予め貯えられる符号化された情報から決定される顧客の資格を条件とする（国際標準化機構の１９８９年の文書ＩＳＯ７８１６－３では、スマート・カード・システムについてのインタフェースおよび信号構成を規定している）。顧客の資格情報は、入力データストリーム内のコマンドによって挿入可能なスマート・カード上のコード化された情報を更新することにより、定期的に変更される。

【００２３】

ＩＳＯ７８１６－３に準拠する、挿入可能なスマート・カードは３つのアルゴリズム機能を有利に含んでいる。これらのアルゴリズム機能のうちの２つ（放送暗号化アルゴリズムと呼ばれる）は、トランスポート・システム２５の非再生モードで入力データストリームから抽出される放送暗号化コードから暗号化キーを発生するために割り当てられている。放送暗号化アルゴリズムは、スマート・カード１３０の内部で放送暗号化コードを解読することにより、暗号化キーを発生する。第３のアルゴリズム機能は、システム２５において、システム２５の保存・再生モードで取り出される放送暗号化キーを暗号化し解読するために使用される。再生アルゴリズムは放送暗号化キーを、挿入可能なスマート・カード自体の内部で、暗号化し解読する。しかしながら、他のシステムでは、再生アルゴリズム機能は、どこか他の場所に、例えばデコーダ内に、在る。

【００２４】

スマート・カード１３０内で使用されるこれら３つの暗号化アルゴリズムは種々のタイプのうちの任意のものでよく、再生アルゴリズムは放送アルゴリズムと同じタイプである必要はない。例示的な目的のために、放送および再生アルゴリズムは、商務省の米国技術情報サービスより提供された連邦情報標準（ＦＩＰＳ）で規定される、データ暗号化標準（ＤＥＳ）のアルゴリズム機能と見なされる。しかしながら、これらのアルゴリズム機能は、別のタイプ、例えば、Rivest-Shamir-Adlemann(ＲＳＡ)タイプの機能でもよい。

【００２５】

スマート・カード上に在る２つの放送暗号化アルゴリズムの各々は、入力データストリーム内の制御情報によって起動される。２つの放送暗号化アルゴリズムは、サービス・プロバイダがすべての顧客に対して放送暗号化アルゴリズムの変更を同時に行うことができるようにするために、スマート・カードの内部に収められている。サービス・プロバイダは、放送暗号化アルゴリズムの変更を行う際に、新しいアルゴリズムを有する新しいスマート・カードを、新しいアルゴリズムが使用されることを予定される日に先だって、すべての顧客に安全に発行する。その変更日に、サービス・プロバイダは同時に、放送データストリーム内の制御情報を更新することにより、新しいアルゴリズムに変更するようスマード・カードにコマンドし；新しいアルゴリズムで番組を暗号化し；そして更新された暗号化コードを放送データストリーム内に挿入する。暗号化システムの安全保護を守り且つ

コードの解読（code-breaking）および番組への無許可のアクセスを防止するために、アルゴリズムの変更は、定期的にあるいは希望されるたびに、サービス・プロバイダによって実施される。

【００２６】

発明者たちは、暗号化キーの変更を伴うこのような暗号化システムでは、暗号化された形式での番組の保存について問題を生じることを認めている。特に、関連する放送暗号化コードと共に、暗号化された形式で保存される番組は、ひとたびスマード・カードが変更されスマード・カードのアルゴリズムが更新されると、解読できないこともある。その理由は、スマート・カード上の新しいアルゴリズムは、前のバージョンのスマード・カードに関連する暗号化コードと互換性がないからである。その結果、新しいスマード・カードのアルゴリズムでは、必要とされる放送暗号化キーを、保存されている暗号化コードから取り出すことができない。これは、保存されている暗号化された番組は、ひとたびシステムのスマード・カードが変更されると、解読できず、使用できないことを意味する。

【００２７】

この問題を解決するために、第３の、異なるアルゴリズム（再生アルゴリズム）がスマート・カードに有利に組み込まれている。この第３のアルゴリズム機能（再生アルゴリズムと呼ばれる）は、システム２５の特定の動作モードで使用され、放送暗号化キーを暗号化し、システム２５の保存・再生モードにおいて、再生暗号化コードを形成する。

【００２８】

ひとたび再生アルゴリズムによって暗号化されると、再生暗号化コードは、暗号化された番組内容と共に、記録媒体に安全に保存される。暗号化された番組の再生時に、再生アルゴリズム機能は、保存されている暗号化コードを解読し、元の放送暗号化キーを取り出し、暗号化された番組内容を解読できるようにする。取り出された放送暗号化キーは、あとで述べるように、暗号化された番組内容パケットを解読するために、暗号解読ユニット５０で使用される。再生アルゴリズムは、２つの放送アルゴリズムほど頻繁に変更されず、スマート・カードの連続するバージョンでも変更されないままである。このため、保存されている暗号化された番組は、スマート・カードや放送暗号化アルゴリズムが変更されても、解読し使用することができる。

【００２９】

選択ユニット４５と４７により暗号解読ユニット５０に供給されるパケットは、データ暗号化標準（ＤＥＳ）に従って暗号化される。第１図のシステム２５の暗号解読ユニット５０はＤＥＳアルゴリズム機能を使用して、これらの暗号化されたパケットを解読する。システム２５の他の実施においては、暗号解読ユニット５０は他のアルゴリズム機能（例えば、以前述べたＲＳＡ機能）を代りに使用することもできる。暗号解読ユニット５０は既知の技術を利用し、暗号化されたパケットを、それに対応する、選択ユニット４５と４７を介してスマート・カード１３０より供給される暗号化キーを使用して解読する。ユニット５０からの解読されたパケット、および表示用の番組を含むユニット４５からの暗号化されてないパケットはデコーダ５５に供給される。ユニット５０からの解読されたパケット、および保存用の番組を含むユニット４７からの暗号化されてないパケットはＭＵＸ１１０に供給される。

【００３０】

ユニット６０は、コントローラ１１５でアクセスできるパケット・バッファを含んでいる。これらのバッファの１つは、コントローラ１１５で使用することを予定されるデータを保持するために割り当てられ、他の３個のバッファは、アプリケーション装置７５、８０、８５で使用することを予定されるパケットを保持するために割り当てられる。更に別のバッファ（あとで述べる代用バッファ）は暗号化コード・データの代りをするデータを保持するために使用される。コントローラ１１５とアプリケーション・インタフェース７０による、ユニット６０内のバッファに貯えられるパケットへのアクセスは、バッファ制御ユニット６５によって制御される。選択ユニット４５は、復号化するためにユニット４５で識別される各パケットについて、送信先フラグをユニット６５に供給する。これらの

フラグは、識別されたパケットについて、ユニット６０内の個々の送信先の位置を示し、制御ユニット６５によって内部メモリ・テーブルに貯えられる。制御ユニット６５は、ファーストイン・ファーストアウト（ＦＩＦＯ）の原理に基づきバッファ６０内に貯えられるパケットに関連する一連の読出し／書込みポインタを決定する。書込みポインタは、送信先フラグと連係して、ユニット４５または５０からの識別されたパケットを、ユニット６０内部の適正な送信先バッファ内の次の空いている位置に順次貯えられるようにする。読出しポインタは、コントローラ１１５とアプリケーション・インタフェース７０により、ユニット６０内の適正な送信先バッファからのパケットの順次読出しを可能にする。

【００３１】

ユニット４５と５０によりデコーダ５５に供給される、暗号化されてないパケットおよび解読されたパケットは、ＭＰＥＧシステム標準の第２．４．３．２項で規定されるトランスポート・ヘッダを含んでいる。デコーダ５５はこのトランスポート・ヘッダから、暗号化されてないパケットおよび解読されたパケットが適応化フィールド（ＭＰＥＧシステム標準に従う）を含んでいるかどうかを判断する。適応化フィールドにはタイミング情報、例えば、内容パケット（content packet）の同期化と復号化を可能にするプログラム・クロック・レファレンス（Program Clock Reference：ＰＣＲ）を含んでいる。タイミング情報パケット（すなわち、適応化フィールドを含んでいるパケット）を検出すると、デコーダ５５は、インタラプト（interrupt：割り込み、中断）機構内部のシステム・インタラプトを設定することにより、パケットが受信されたことをコントローラ１１５に合図する。更に、デコーダ５５は、ユニット６５内のタイミング・パケット送信先フラグを変更して、そのパケットをユニット６０に供給する。ユニット６５内の送信先フラグを変更することにより、ユニット６５は、デコーダ５５より供給されるタイミング情報パケットを、アプリケーション・バッファの位置にではなく、コントローラ１１５で使用するデータを保持するために割り当てられたユニット６０内のバッファの位置に転送する。

【００３２】

デコーダ５５で設定されたシステム・インタラプトを受け取ると、コントローラ１１５はタイミング情報とＰＣＲ値を読み取り、それを内部メモリに貯える。連続するタイミング情報パケットのＰＣＲ値は、システム２５のマスタークロック（２７ＭＨｚ）を調節するために使用される。連続するタイミング・パケットを受信する時間間隔の、ＰＣＲに基づく推定値とマスタークロックに基づく推定値との差（コントローラ１１５で発生される）が、システム２５のマスタークロック（図面を簡略にするために図示されていない）を調節するために使用される。コントローラ１１５はこの調節を行うために、時間間隔について得られた推定値の差を使用して、マスタークロックを発生するのに使用される電圧制御発振器の入力制御電圧を調節する。コントローラ１１５は、内部メモリにこのタイミング情報を貯えてから、システム・インタラプトをリセットする。

【００３３】

デコーダがユニット４５と５０から受け取る、オーディオ、ビデオ、キャプションその他の情報などの番組内容を含むパケットは、ユニット６５によって、デコーダ５５から、パケット・バッファ６０内の指定されたアプリケーション装置のバッファに向けられる。アプリケーション制御ユニット７０は、バッファ６０内の指定されたバッファから、オーディオ、ビデオ、キャプションその他のデータを順次取り出し、そのデータを対応するアプリケーション装置７５、８０、８５に供給する。アプリケーション装置は、オーディオ・デコーダ８０とビデオ・デコーダ８５と高速データ・ポート７５から成る。データ・ポート７５は、例えば、コンピュータ・プログラムのような高速データを供給するのに使用され、また例えば、ＨＤＴＶデコーダにデータを出力するのにも使用される。

【００３４】

ＰＳＩ情報を含んでいるパケットは、ユニット６０内のコントローラ１１５用のバッファのために予定されたものとして、選択ユニット４５によって認識される。番組内容を含んでいるパケットについて述べたのと同様にして、ＰＳＩパケットは、選択ユニット４５、５０、５５を介して、ユニット６５によりこのバッファに向けられる。コントローラ１

１５はユニット６０からＰＳＩを読み出し、それを内部メモリに貯える。

【００３５】

コントローラ１１５は第２図と第３図のプロセスを使用して、記録媒体１０５に保存するのに適する番組データストリームを発生し、且つその保存に対しユーザに支払請求する。コントローラ１１５はまた、第２図と第３図のプロセスを使用して、記録媒体１０５に保存するための再生暗号化コードを発生し、且つ保存される番組データストリームから元の放送暗号化コードを除去する。第２図と第３図のパケット識別および方向づけのプロセスは、以前説明した様に、コントローラ１１５、制御ユニット６５、およびユニット４５と４７の、ＰＩＤ，送信先および暗号化キーのルックアップ・テーブルによって管理される。

【００３６】

ＣＰＳＩ（Condensed Program Specific Information：圧縮されたプログラム固有の情報）は、保存される特定のプログラム（番組）に関する情報を含んでいるのに対して、ＰＳＩは、システム２５に入力されるデータストリーム内のすべての番組に関する情報を含んでいる。従ってＣＰＳＩは、ＰＳＩよりも必要とする記憶容量が少なく、費用も少ない。更に、一定の費用の制約のもとでは、ＣＰＳＩはＰＳＩよりも頻繁にデータストリーム内で繰り返され、取り出され、使用されて、番組内容の再生待ち時間が短縮される。

【００３７】

ＭＰＥＧシステム標準第２．４．４項に規定されるＰＳＩは、４つの暗号化されない情報要素（情報テーブル）から成り、それらは、Program Association Table（ＰＡＴ：プログラム関連付けテーブル）、Program Map Table（ＰＭＴ：プログラム・マップ・テーブル）、Network Information Table（ＮＩＴ：ネットワーク情報テーブル）およびConditional Access Table（ＣＡＴ：条件付きアクセス・テーブル）である。各テーブルは、特定のＰＩＤで認識されるデータ・パケットで形成される。ＰＭＴは、１つのプログラムを構成するパケット化された個々のデータストリームを識別するＰＩＤラベルを規定する。これらの個々のストリームは、ＭＰＥＧ標準で基本的ストリームと呼ばれる。基本的ストリームには、データストリーム、例えば、ビデオ、種々の言語のオーディオおよびキャプションのデータストリーム、が含まれる。ＰＡＴは、ＰＭＴを含んでいるパケットの識別と組立てを可能にするＰＩＤとプログラムの番号を関連付ける。ＮＩＴはオプションであり、例えば、衛星伝送チャンネルの周波数およびトランスポンダ・チャンネルのような物理的ネットワークのパラメータを規定するために構成され使用される。ＣＡＴは、ユーザの資格に依存する番組へのアクセスを支配する暗号化コードのような、条件付きアクセス情報を含んでいる。

【００３８】

第２図のステップ２０５で、コントローラ１１５（第１図）は、ステップ２００における開始に続くシステムのパワーアップにおいて初期設定の手順を行う。ステップ２０５で、コントローラ１１５は、ＰＡＴおよびＣＡＴテーブルについてＭＰＥＧで規定されるＰＩＤ値（ＰＩＤの１６進値はそれぞれ、０００００と０００１）を選択ユニット４５（第１図）のＰＩＤ検出フィルタにロードする。更に、コントローラ１１５は、ユニット４５の送信先テーブルを更新することにより、ＰＡＴパケットとＣＡＴパケットをユニット６０内のコントローラ・バッファに予め割り当てる。ユニット４５で検出されたＰＡＴおよびＣＡＴパケットは、ユニット６５の制御下で、デコーダ５５を介してユニット６０内のコントローラ・バッファに導かれる。ステップ２０５で、制御ユニット６５は、ＰＳＩパケットがユニット６０内に存在することを、ＰＳＩインタラプトによってコントローラ１１５に合図する。コントローラ１１５は、ＰＳＩインタラプトを受け取ると、ユニット６０内のその指定されたバッファに貯えられているパケットに繰返しアクセスし、完全なＣＡＴデータとＰＡＴデータを内部メモリに貯える。コントローラ１１５はこのプロセスを繰り返して、ＰＡＴから、ＰＭＴパケットとＮＩＴパケットを識別するＰＩＤを決定したあとで、完全なＰＭＴデータとＮＩＴデータを内部メモリに貯える。コントローラ１１５は、受像機が起動されている間、バッファ６０に連続的にアクセスし、ＰＳＩインタラプト

を受け取ると、ＰＳＩパケットを内部メモリに保存する。その結果、コントローラ１１５はその内部メモリに、システム２５に入力されるトランスポート・データストリームについての完全なＰＳＩを含むＰＡＴ、ＰＭＴ、ＮＩＴおよびＣＡＴデータを捕獲する。

【００３９】

第２図のステップ２１０で、ユーザが保存したいと思う番組、暗号化された形式で保存しようとする番組および保存用に使用する媒体と装置を識別する、ユーザが発生するデータ（ＳＰ、ＳＭ、ＳＥ）はコントローラ１１５（第１図）に入力される。ユーザは、種々の理由で、暗号化せずに保存するよりもむしろ、暗号化して保存することを選択するかも知れない。例えば、サービス・プロバイダは、ユーザがあとで作成するコピーの数を制限する手段として、暗号化した形式で保存するほうが安上がりになるようにすることもある。サービス・プロバイダはこれを行うために、予めスマート・カードに保存された資格情報によって、暗号化された番組へのアクセスをコントロールする。コントローラ１１５に入力される選択データは、インタフェース１２０を介して、ユーザがリモコン１２５で画面上のメニューを選択して入れられる。ステップ２１５で、入力選択データ（ＳＰ）に応答して、コントローラ１１５は、保存用に選択された番組のＰＩＤを、保存されているＰＳＩから取り出す。選択ユニット４７の検出フィルタに、コントローラ１１５により貯えられる番組のＰＩＤがロード（ｌｏａｄ）される。これにより、ユニット４７は、保存用に選択された番組を含んでいるパケットを識別できる。ステップ２１５で、コントローラ１１５はまた、ユニット６０の代用バッファにナル・データを予めロードする。ナル（null：空白、零）データは、暗号化された形式で放送され保存用に選択される番組において生じる放送暗号化コードの代りに使用されることになる。

【００４０】

第２図のステップ２１５で、選択ユニット４７（第１図）は、暗号化されてないパケットをＭＵＸ１１０に供給し、暗号化されたパケット（パケット・ヘッダ・データ内の暗号化指標で識別される）を、関連する放送暗号化キーと共に、暗号解読ユニット５０に供給する。放送暗号化キーは、以前説明したように、選択された番組（ＳＰ）に対してＣＡＴから得られる暗号化コードの解読によってスマート・カード１３０（第１図）で発生されたあとで、第２図のステップ２１５で、コントローラ１１５によって選択ユニット４７に供給される。しかしながら、もし選択データＳＥが、暗号化された保存をリクエスト（request）するならば、ユニット４７は、保存しようとする暗号化されたパケットをＭＵＸ１１０に送る。その結果、第２図のステップ２１５で、保存しようとする番組（ＳＰ）を含んでいるパケットは、選択データＳＥに応答して、暗号化された形式かまたは暗号化されない形式のいずれかで、ＭＵＸ１１０に供給される。

【００４１】

ステップ２１７～２２７で、コントローラ１１５は、システム２５に入力されるトランスポート・データストリームから捕獲される完全なＰＳＩ（Program Specific Information：プログラム固有の情報）から保存用に選択された番組に対して、ＣＰＳＩ（Condensed Program Specific Information：圧縮されたプログラム固有の情報）を形成する。もし選択データＳＥが、暗号化された保存をリクエストするならば、コントローラ１１５は、判定ステップ２１７に続いて、ステップ２２７を実行する。ステップ２２７で、コントローラ１１５は、スマート・カード・システム１３０における再生アルゴリズム機能を利用して、ステップ２１５で（放送暗号化コードの解読により）以前発生された放送暗号化キーを暗号化し、保存しようとする番組のための再生暗号化コードを形成する。ＣＰＳＩは、再生暗号化コードを含むように形成されるが、システム２５に入力されるトランスポート・データストリームのＰＳＩに最初から存在する放送暗号化コードを除外するように形成される。従って、保存用に予定される番組のために形成されるデータストリームから、それに関連する放送暗号化コードが除外される。これによって、第三者がアクセスできる取り出し可能な記録媒体に暗号化キーが保存されている場合、暗号化キーの安全保護が危うくされるのを防止する。ひとたび記録媒体上でキーにアクセスできると、キーの安全保護は、利用できるリバース・エンジニアリング（reverse engineering）とコード

解読（code-breaking）技術に依存する。本システムでは、多数レベルの安全保護を与えるために、放送暗号化キーが取り出されるような放送暗号化コードを保存しないようにすると共に、放送暗号化キーを、暗号化された形式で保存する。更に、たとえ保存された番組のキーが推定されても、放送暗号化アルゴリズムが定期的に変更される現在放送中の番組にはアクセスできない。

【００４２】

もし入力データＳＥが、暗号化された保存をリクエストしなければ、コントローラ１１５は、判定ステップ２１７に続いてステップ２２５を実行する。ステップ２２５で、コントローラ１１５は、システム２５に入力されるトランスポート・データストリームのＰＳＩから、保存用に予定される番組のＣＰＳＩを形成し、そのＣＰＳＩから暗号化コードを除外する。

【００４３】

ここで説明した暗号化システムは例示的なものに過ぎない。これに代る別の暗号化機構では、ＰＳＩ以外のデータストリーム情報地帯において放送および再生暗号化コードを伝送する。他の暗号化機構では、ＰＳＩを発生する場合とは異なる間隔で、暗号化コードの発生および挿入が要求される。もし放送暗号化コードがＰＳＩで伝送されなければ、保存される番組のために形成されるデータストリームからこれらのコードを除外するために、これらのコードの代りに他のデータを使用する必要がある。ＣＰＳＩが生じる間隔とは異なる間隔で放送暗号化コードに代るナル・データの使用についてはあとで述べる。具体的には、放送暗号化コードを、リアルタイムで、すなわち、例えば、放送暗号化コードがパケット・ヘッダで伝送されるときのパケット周波数で、置換することについては、ステップ２３７～２４９に関連して述べる。

【００４４】

ステップ２３０で、コントローラ１１５は、ＭＰＥＧシンタクス（ＭＰＥＧシステム標準の２．４．４．３～２．４．４．１１項）に従ってＣＰＳＩデータを各セクション別に形成する。ステップ２３０で、コントローラ１１５はまた、ヘッダ・データをＣＰＳＩデータ・セクションに付け加え、保存されるデータストリームの中へ挿入するためにＣＰＳＩデータをフォーマット化しそしてパケット化する。コントローラ１１５は、ＭＰＥＧシステム標準の２．４．３．２と２．４．３．３項に従ってコントローラ１１５の内部メモリに保存されているＰＳＩヘッダ・データからヘッダを作り出す。しかしながら、ＣＰＳＩのセクション・データは、それと対応するＰＳＩのセクション・データと長さが異なる。従って、「連続性カウント」指標と「ペイロード・ユニット開始」指標を含む新しいヘッダ・パラメータがコントローラ１１５で作り出され、ヘッダ・データ内部のそれぞれの指標フィールドに挿入される。コントローラ１１５で作り出される新しい連続性カウント指標は、例えば、ＣＰＳＩ要素について各ＰＩＤごとのパケットの数を、それと対応するＰＳＩ要素の各ＰＩＤごとのパケットの数の代りに、表す。コントローラ１１５で作り出される新しいペイロード・ユニット開始指標は、例えば、ＣＰＳＩセクションの最初のバイトを、それと対応するＰＳＩセクションの最初のバイトの代りに、識別する。

【００４５】

ステップ２３０に続き、第２図のフローチャートは第３図のステップ２３７に続く。ステップ２３７で、コントローラ１１５は、放送暗号化コードがＣＰＳＩ以外のデータストリーム・フィールドで伝送されるのかを判断する。具体的に、コントローラ１１５は、放送暗号化コードが、ＭＰＥＧと互換性のパケット・ヘッダの適応化フィールド（ＭＰＥＧシステム標準シンタクスの２．４．３．４項に従う）で伝送されるのかを判断する。もしそうであれば、コントローラ１１５はステップ２４９を実行して、パケット・ヘッダにおいて放送暗号化コードの代わりにナル・データを使用して、ＣＰＳＩパケットおよび番組内容パケットを含む複合データストリームを作り出す。暗号化コードの置換は、１パケットごとに、パケット周波数で行われる。

【００４６】

ステップ２４９で、ステップ２１５（第２図）の間にユニット６０内の代用バッファの

中へ予めロードされた代用パケット・データは、コントローラ１１５の制御下で、ユニット６０からＭＵＸ１１０（第１図）へ供給される。更に、ステップ２４９で、ステップ２３０で形成されたＭＰＥＧと互換性のパケット化されたセクション・データの形式をとるＣＰＳＩは、コントローラ１１５によってＭＵＸ１１０（第１図）に供給される。ユニット４７またはユニット５０からの番組内容パケット・データストリームも、ステップ２１５に関連して以前述べたように、ＭＵＸ１１０に供給される。ステップ２４９で、コントローラ１１５は、経路選択信号Ｃを使用してＭＵＸ１１０に入力される代用データと、番組内容データストリームと、ＣＰＳＩデータストリームを多重して、ＭＵＸによって保存インタフェースに出力される複合データストリームを作り出す。この複合データストリームには、番組内容パケットとＣＰＳＩパケットが含まれ、パケット・ヘッダにおいて放送暗号化コードの代りにナル・データが使用されている。

【００４７】

コントローラ１１５は、制御ユニット６５（第１図）からのＰＳＩインタラプト信号と代用タイミング信号に応答して、保存される番組のデータストリームの中へＣＰＳＩパケットとナル・データが同時に挿入されるようにする。ＰＳＩインタラプト信号は、ステップ２０５に関連して述べたように、バッファ６０内のＰＳＩパケットの存在を表示する。代用タイミング信号は、ナル・データの挿入と、パケット・ヘッダ内の放送暗号化コードの発生を同時に行わせる。このようにして、ＣＰＳＩのパケット化されたセクションはＰＳＩの位置へ挿入されて、対応するＰＳＩのセクションと入れ替り、放送暗号化コードが除去される。暗号化されてないＣＰＳＩデータは、保存用の番組（暗号化されるかまたは暗号化されない）を作り出すために、ＭＵＸ１１０に入力される番組内容（暗号化されたかまたは暗号化されてない）のデータストリームに挿入することができる。

【００４８】

注目すべきことに、ステップ２４９で実行された放送暗号化コードの置換は、ＭＰＥＧパケット・ヘッダの適応化フィールド以外のデータストリーム・フィールドで伝送されるコードにも行われる。更に、暗号化コードは、適応化フィールドが生じる間隔とは異なる間隔で置換される。例えば、ＭＰＥＧと互換性および非互換性の種々のデータストリームの位置で発生する暗号化コードに替えて、ナル・データが使用される。これらのデータストリームの位置には以下のものが含まれる：民間のDigital Satellite System（ＤＳＳ™：ディジタル衛星システム）内部の補助パケット；Packetized Elementary Stream（ＰＥＳ：パケット化された基本的ストリーム）のフィールド（ＭＰＥＧシステム標準シンタクス２．５．３．７～２．５．４．２項に従う）；Digital Storage Media Control Commands（ＤＳＭＣＣ：ディジタル記録媒体制御コマンド）のフィールド（ＭＰＥＧシステム標準シンタクス付録Ａに従う）；および他のデータ伝送プロトコル、例えば、標準化されたＣＥＢｕｓ制御プロトコル（Home Automation Standard：ホーム・オートメーション標準（ＣＥＢｕｓ）、ＥＩＡ／ＩＳ‐６０，１９８９年１２月）、に従ってフォーマット化される非ＭＰＥＧパケット。

【００４９】

もし暗号化コードがパケットで伝送され、その暗号化コード自体がそのパケットで唯一の重要性のあるデータ項目である場合、その暗号化コードを運んでいるパケットを出力データストリームから完全に省くこともできる。これを行うには、ＰＩＤ選択ユニット４５と４７（第１図）を介してそのパケットを廃棄するか、またはステップ２４９で実行される多重処理の間にそのパケットを削除する。しかしながら、出力データストリーム・シンタクス内部の、データ・レートとデータ構成に敏感なパラメータは、そのようなパケット・データの削除の結果生じるデータ・レートの変化を反映させるために、更新する必要がある。

【００５０】

ステップ２４９で、記憶インタフェース９５（第１図）は、ＣＰＳＩとナル・データを組み込んでいるパケット化されたデータストリーム（以下、ＣＰＳＩストリームと称す）の形式で保存される番組をＭＵＸ１１０から受け取る。ステップ２４９に続く、ステップ

２５４（第３図で）、システム２５内部の条件付きアクセス・システムにより、番組の保存（または他の装置への伝送）に対しユーザに支払請求をする。ユーザへの支払請求は、挿入可能なスマート・カード自体の内部に支払請求情報を記録して行われる。支払請求情報の保存は再生アルゴリズムを使用して開始されるが、支払請求は再生アルゴリズムの適用と同時に行われる必要はない。支払請求情報には、暗号化された放送番組をユーザが保存していることが表示される。この支払請求情報はあとで、サービス・プロバイダによって電話リンクを介してアクセスされ、従来の請求手順を経てユーザに請求される。他の請求方法も同じように実施可能である。例えば、スマート・カード内に予め保存されたクレジットの総額から差し引くこともできる。更に、スマート・カードは、リクエストされる保存のタイプに基づき、請求額を変えることもできる；例えば、保存される番組を一回だけコピーまたは再生できるようにする場合と、保存される番組を無制限にコピーしたり再生したりできるようにする場合とで、別の料金とすることもできる。リクエストされる保存のタイプは、ＣＰＳＩストリーム自体における指定されたコピー保護データの内部に符号化されるか、またはＣＰＳＩストリームの外部のパケット・データ内に符号化される。記録媒体１０５に保存するのに適する番組データストリーム（ＣＰＳＩストリーム）を発生し、且つその保存に対してユーザに支払請求するためにコントローラ１１５が使用する第２～３図のプロセスは、ステップ２５８で終了する。

【００５１】

ステップ２３７で、ＭＰＥＧと互換性のある適応化フィールドのパケット・ヘッダにおいて放送暗号化コードが伝送されていないとコントローラ１１５が判断すると、コントローラ１１５はステップ２４０～２４５を実行する。これらのステップは、ステップ２４９～２５８と同様であるが、ＭＵＸ１１０に入力されるデータストリームには、保存される番組を表す放送暗号化コードが存在しないので、ナル・データを挿入する必要はない。コントローラ１１５はステップ２４０を実行し、記憶インタフェース９５を介して保存用のＣＰＳＩストリームを作り出し、ステップ２４４を実行して、ステップ２４９と２５４に関連して説明したのと同様にして、保存に対してユーザに支払請求をする。第２～３図のこの部分のプロセスはステップ２４５で終了する。しかしながら、注目すべきことに、ステップ２４０と２４９で、このＣＰＳＩストリームは、インタフェース９５を経由する保存の代りに、インタフェース７０を経由する表示または情報伝達のような他の用途にも供給される。

【００５２】

ＭＵＸ１１０からのＣＰＳＩストリームは、インタフェース９５によりバッファされ、データ内のギャップをおよびビット・レートの変動を減少させる。その結果生じる、バッファされたデータは、記録媒体１０５に保存するのに適するように記憶装置９０で処理される。コントローラ１１５は、標準化されたＣＥＢｕｓ制御プロトコル（例えば、Home Automation Standard（ＣＥＢｕｓ），ＥＩＡ／ＩＳ‐６０，１９８９年１２月）を使用して、Ｉ／Ｏポート１００を経由してコマンドにより記憶装置９０（第１図）の動作を開始させ制御する。記憶装置９０は線型蓄積メディアＤＶＨＳ^{TM}（登録商標）タイプのデバイスであり、記録媒体１０５は線形順次アクセス・タイプのメディア（例えば、ビデオテープ）である。記憶装置９０は、既知のエラー符号化技術（例えば、チャンネル符号化、インタリービング、リード・ソロモン符号化）を使用して、インタフェース９５からのバッファされたデータストリームを符号化して、保存に適する符号化されたデータストリームを発生する。記憶装置９０は、その結果生じる、ＣＰＳＩを組み込まれている符号化されたデータストリームをテープ媒体１０５に貯える。

【００５３】

記憶装置９０は、第１図の実施例では線形の蓄積メディアにデータを貯えるＤＶＨＳ^{TM}デバイスとして説明したが、いかなるタイプの記憶装置でもよい。例えば、記憶装置９０は、ＲＡＭに、あるいは非線形の媒体に、データを貯えるソリッドステートまたは非線形タイプの装置である。非線形タイプの媒体は、非順次的アクセスに適応する媒体（例えば、ＣＤＲＯＭまたはＤＶＤのようなディスク媒体）である。記憶装置９０と記録媒体１

０５が非線形のあるいはソリッドステート・タイプの蓄積システムであれば、記憶装置９０はＣＰＳＩデータをＣＰＳＩストリームから分離し、そのＣＰＳＩデータを記録媒体の指定されたディレクトリ・セクションに貯える。これにより、ＣＰＳＩデータの保存の繰返しが回避され、且つ必要とされる記憶容量が減少されて有利である。記憶装置９０はＣＰＳＩストリームを、ＣＰＳＩデータの繰返しを一回以上組み込んで装置９０に入力された形式として貯えることもできる。

【００５４】

更に、第１図のシステム２５は、線形、非線形、ソリッドステート・タイプなど種々のタイプの複数の装置の動作をサポートする複数の記憶／取出し経路を組み込むこともできる。第１図に示すただ１つの記憶／取出し経路は、すでに説明したように、ユニット４７、９０、９５、１０５、１１０から成る。これらの要素を複製して並列記憶機能を作り出すことにより、システム２５は複数の記憶経路を組み込むように容易に拡張される。特定の記憶装置用に予定される記憶経路および番組は、以前述べたように、リモコン１２５で画面上のメニューを選択してからインタフェース１２０を経由してコントローラ１１５に入力されるユーザが発生するデータ（ＳＰ，ＳＭ）で選択される。

【００５５】

第１図のシステム２５は、第４図のプロセスを使用して再生モードで記憶装置９０と記録媒体１０５から番組を再生する。再生されたデータストリームはシステム２５で処理されて、例えば、表示または出力するために、アプリケーション装置７５、８０、８５に供給される。あるいは、番組データストリームは他の並列記憶装置（図面を簡略するために第１図に示されていない）に保存される。

【００５６】

ステップ５００の開始に続く、第４図のステップ５０５で、ユーザが発生するデータ（ＳＲ、ＳＭ）がシステム２５（第１図）のコントローラ１１５に入力され、再生する番組（ＳＲ）および再生する番組が取り出される記憶装置（ＳＭ）を識別する。ユーザが選択するデータは、リモコン１２５で画面上のメニューを選択してからインタフェース１２０を経由してコントローラ１１５に入力される。例示的な目的で、ユーザは再生しようとする番組を記憶装置９０（第１図）から選択するものと仮定する。

【００５７】

ステップ５１０で、コントローラ１１５は、以前述べたように、標準化されたＣＥＢｕｓ制御プロトコルを使用してＩ／Ｏポート１００を経由するコマンドにより、記録媒体１０５から記憶装置９０によって、選択された番組データストリームの再生を開始する。記憶装置９０は、記録媒体１０５から取り出されるエラー符号化されたデータを復号化し、それに対応する、記憶装置９０に最初に供給されたデータを再生する。記憶装置９０は、ＤＶＨＳ^{TM}線形タイプの記憶装置または別のタイプの記憶装置、例えば、ソリッドステートＲＡＭまたは非線形タイプのＤＶＤまたはＣＤＲＯＭタイプの装置である。ステップ５１０で、復号化され再生されたデータストリームは、記憶装置９０によって、インタフェース９５に転送される。このデータ転送は標準的なＣＥＢｕｓを経由してコントローラ１１５で制御され同期化される。記憶インフェース９５は記憶装置９０から受け取るデータをバッファし、データ・パケット間の時間的間隔を調節して、ＭＰＥＧと互換性のある且つＭＰＥＧビット・レート制約に従う、バッファされたデータ出力を供給する。

【００５８】

ステップ５１５で、コントローラ１１５はこのバッファされた出力を、経路選択信号Ｃを用いて、インタフェース９５（再生データストリーム）からＭＵＸ３７を介してＰＩＤ選択ユニット４５と４７に導く。ステップ５１５で、コントローラ１１５は、ステップ２４４と２５４（第３図）で指定するコピー保護データ内に符号化されたコピーについての制限（コピーを１回だけとるのかまたは無制限にとるのか）を、再生される番組が超過しているかどうか判断する。再生が許可されれば、ステップ５１５（第４図）で、コントローラ１１５は、選択された番組（ＳＲ）に対しステップ２２７（第２図）でＣＡＴから発生された再生暗号化コードを再生し、ステップ２１５（第２図）に関連して前述したよう

に、そのコードをスマート・カード・ユニット１３０に供給する。ステップ５１５（第４図）で、コントローラ１１５の制御下で、スマート・カード・ユニット１３０は、再生アルゴリズムを使用して、再生暗号化コードから元の放送暗号化キーを発生する。ステップ５１５で、コントローラ１１５により、放送暗号化キーは、ユニット４５と４７におけるＰＩＤ、デスティネーションおよび暗号化キーのルックアップ・テーブルに供給される。

【００５９】

ステップ５２０で、ユニット４５と４７およびシステム２５のその他のユニットは、再生データストリームを、ＭＵＸ１１０を介して保存するためにあるいはインタフェース７０を経由して利用するために、処理する。ユニット９５からの再生用データストリームと選択器３５から伝送されるデータストリームはいずれも、ＭＵＸ３７を介する選択に続いて、システム２５によって同じように処理される。これらのデータストリームはいずれも、暗号化キーの発生ステップとＣＰＳＩ処理ステップを除いて、伝送されたデータストリームについて以前述べたように処理される。再生モードで、スマート・カード１３０は、放送キー発生アルゴリズムの代りに、再生暗号化キー発生アルゴリズムを適用する。スマート・カード・ユニット１３０は、再生アルゴリズム機能を利用して、第２図のステップ２２７において再生符号化アルゴリズムで以前に符号化された暗号化コードを解読する。それにより、ユニット１３０は、再生用に選択された番組（ＳＲ）に対する元の放送暗号化キーを取り出す。この放送暗号化キーをＤＥＳ暗号解読ユニット５０が使用して、伝送されたデータストリームについて前述したように、続くステップ５２０（第４図）で、暗号化された番組内容パケットを解読する。しかしながら、ＭＵＸ３７を介して選択された再生データストリームはすでにＣＰＳＩを組み込んでいる。従って、ステップ５２０において、再生モードでコントローラ１１５は、第２～３図に関連して述べたＣＰＳＩの形成に関するステップを行わない。

【００６０】

ステップ５２０で、第４図に示す例示的な再生モードで、システム２５は再生データストリームをトランスポート復号化し、復号化されたデータを、表示するためにアプリケーション・デコーダ８０と８５に供給する。このモードで、システム２５は、ＭＰＥＧ標準に従って、再生データストリーム内にある最新の完全なＣＰＳＩデータを利用して、選択された番組ＳＲを表すトランスポート復号化されたデータストリームを供給する。

【００６１】

ＣＰＳＩを利用して、再生データストリームをトランスポート復号化する際に、第１図に関連して以前述べたのと同様にして、ＰＩＤフィルタ４５と４７、暗号解読器５０、デコーダ５５、バッファ６０および制御ユニット６５を使用する。トランスポート復号化されたデータストリーム（ＣＰＳＩを除く）は、インタフェース７０を経由して、ＭＰＥＧ復号化および画像再生のために、アプリケーション・デコーダ８０と８５に供給される。他のモードでは、システム２５は、ＣＰＳＩを組み込んでいる再生データストリームを他のアプリケーション装置（例えば、高速データ・ポート７５）へ供給する。再生データストリームをトランスポート復号化する際に、これらのアプリケーション装置あるいはあとに続く装置がＣＰＳＩを必要に応じて利用できる。もし再生データストリームを、例えば、記憶装置９０以外の第２の記憶装置に貯えようとするならば、ＭＵＸ１１０はそのデータストリーム（ＣＰＳＩを組み込んでいる）を、第２の記憶インタフェースを介して、第２の記憶装置に供給する。更に、この第２の記憶装置と第２のインタフェース（どちらも第１図に示されていない）はそれぞれ、記憶装置９０およびインタフェース９５と同様に動作し機能する。インタフェース７０からのデータは、アプリケーション・デコーダ８０と８５によりＭＰＥＧ復号化されて、それぞれデコーダ８０と８５におけるオーディオ再生装置とビデオ再生装置で再生される。

【００６２】

ステップ５２７（第４図）で、システム２５内部の条件付きアクセス・システムは番組の再生に対してユーザに支払請求する。再生アルゴリズムが適用されて支払請求情報が保存され、ユーザは、挿入可能なスマート・カードの内部で支払請求される。この支払請求

情報は、暗号化された放送番組をユーザが再生したことを表示する。支払請求情報はあとで、電話リンクを介してサービス・プロバイダによってアクセスされ、従来の請求手続きによりユーザに支払請求するために使用される。他の方法も、前に述べたように、同様に使用される。第４図の再生プロセスはステップ５３０で終了する。

【００６３】

第１図のアーキテクチャは唯一のものではない。本発明の原理に従い、他のアーキテクチャを使用して、同じ目的を達成することもできる。更に、第１図のアーキテクチャの各要素の機能および第２図～４図の処理ステップは、全部または一部、プログラムされたマイクロプロセッサのインストラクションの範囲内で実行される。また、本発明の原理は、ＭＰＥＧのＰＳＩテーブルで伝送されるものとして本明細書で述べたあらゆる情報を伝送するために、ＭＰＥＧと互換性または非互換性の電子的プログラム・ガイドを使用するあらゆるシステムに応用される。本発明の原理は、ＭＰＥＧと互換性のあるＰＳＩテーブルで伝送されるプログラム・ガイドまたはＰＳＩに限定されることなく応用される。

【符号の説明】

【００６４】

１０　アンテナ
１５　入力プロセッサ
２０　復調器
２５　トランスポート・システム
３０　デコーダ
３７　マルチプレクサ
４０　暗号解読装置
８０　オーディオ・デコーダ
８５　ビデオ・デコーダ
９０　記憶装置
９５　記憶インタフェース
１００　Ｉ／Ｏポート
１０５　記録媒体
１２５　リモコン１３０　スマート・カード

【図１】

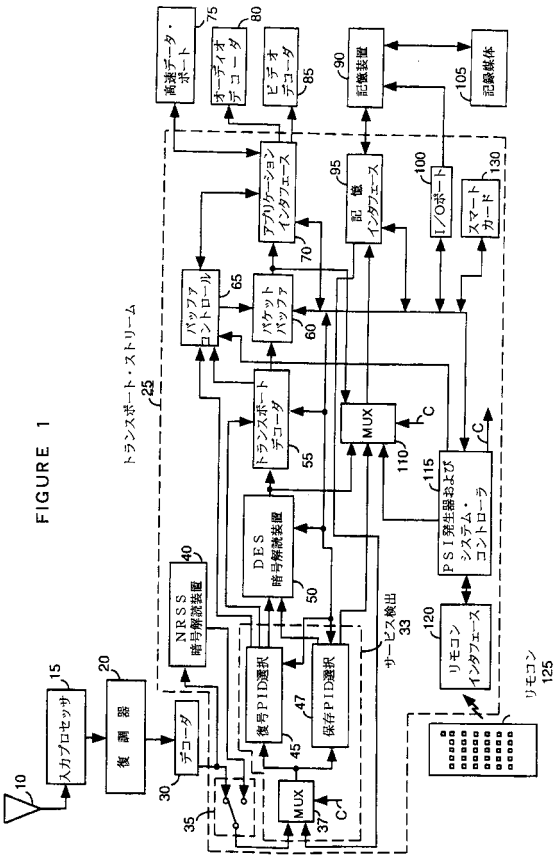
FIGURE 1
高速データ・ポート
オーディオデコーダ
ビデオデコーダ
記憶装置
記録媒体
アプリケーションインタフェース
記憶インタフェース
I／Oポート
スマートカード
バッファコントロール
パケットバッファ
トランスポート・ストリーム
トランスポートデコーダ
MUX
PSI発生器およびシステム・コントローラ
DES暗号解読装置
NRSS暗号解読装置
復号PID選択
保存PID選択
サービス検出
リモコンインタフェース
リモコン
入力プロセッサ
復調器
デコーダ

【図２】

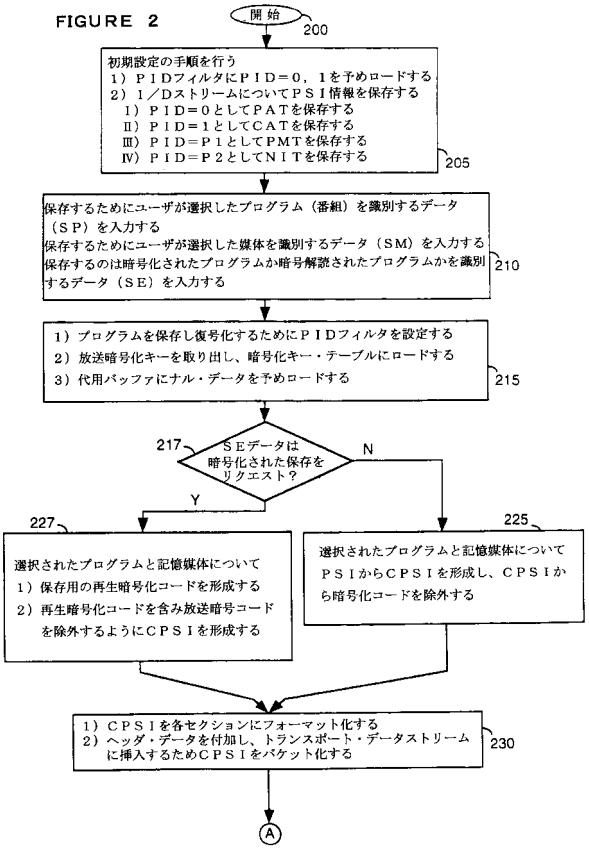
FIGURE 2
開始
200
初期設定の手順を行う
1）PIDフィルタにPID＝0，1を予めロードする
2）I／DストリームについてPSI情報を保存する
I）PID＝0としてPATを保存する
II）PID＝1としてCATを保存する
III）PID＝P1としてPMTを保存する
IV）PID＝P2としてNITを保存する
205
保存するためにユーザが選択したプログラム（番組）を識別するデータ（SP）を入力する
保存するためにユーザが選択した媒体を識別するデータ（SM）を入力する
保存するのは暗号化されたプログラムか暗号解読されたプログラムかを識別するデータ（SE）を入力する
210
1）プログラムを保存し復号化するためにPIDフィルタを設定する
2）放送暗号化キーを取り出し、暗号化キー・テーブルにロードする
3）代用バッファにナル・データを予めロードする
215
217
SEデータは暗号化された保存をリクエスト？
N
Y
227
選択されたプログラムと記憶媒体について
1）保存用の再生暗号化コードを形成する
2）再生暗号化コードを含み放送暗号コードを除外するようにCPSIを形成する
225
選択されたプログラムと記憶媒体についてPSIからCPSIを形成し、CPSIから暗号化コードを除外する
1）CPSIを各セクションにフォーマット化する
2）ヘッダ・データを付加し、トランスポート・データストリームに挿入するためCPSIをパケット化する
230
A

【図３】

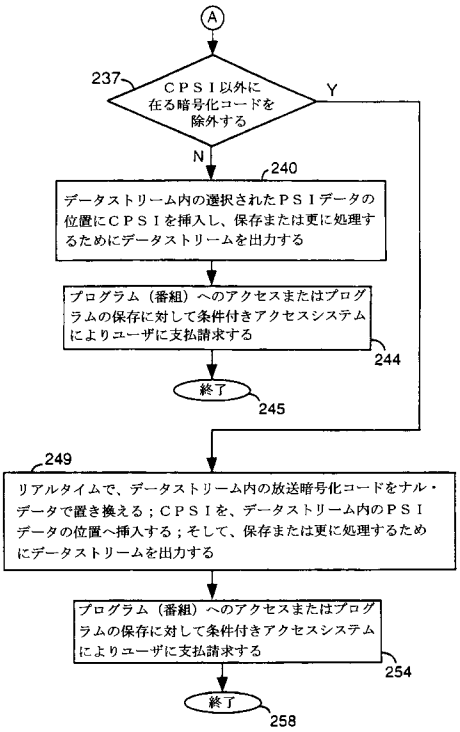
FIGURE 3
A
237
CPSI以外に在る暗号化コードを除外する
Y
N
240
データストリーム内の選択されたPSIデータの位置にCPSIを挿入し、保存または更に処理するためにデータストリームを出力する
プログラム（番組）へのアクセスまたはプログラムの保存に対して条件付きアクセスシステムによりユーザに支払請求する
244
終了
245
249
リアルタイムで、データストリーム内の放送暗号化コードをナル・データで置き換える；CPSIを、データストリーム内のPSIデータの位置へ挿入する；そして、保存または更に処理するためにデータストリームを出力する
プログラム（番組）へのアクセスまたはプログラムの保存に対して条件付きアクセスシステムによりユーザに支払請求する
254
終了
258

【図４】

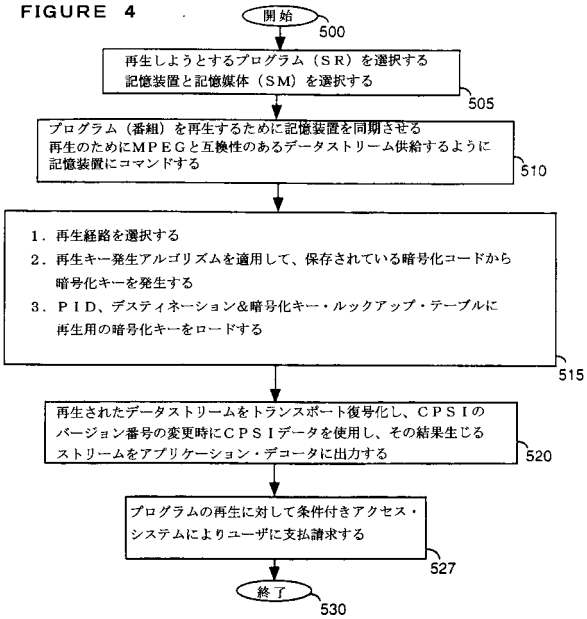
FIGURE 4
開始
500
再生しようとするプログラム（SR）を選択する
記憶装置と記憶媒体（SM）を選択する
505
プログラム（番組）を再生するために記憶装置を同期させる
再生のためにMPEGと互換性のあるデータストリーム供給するように記憶装置にコマンドする
510
1．再生経路を選択する
2．再生キー発生アルゴリズムを適用して、保存されている暗号化コードから暗号化キーを発生する
3．PID、デスティネーション&暗号化キー・ルックアップ・テーブルに再生用の暗号化キーをロードする
515
再生されたデータストリームをトランスポート復号化し、CPSIのバージョン番号の変更時にCPSIデータを使用し、その結果生じるストリームをアプリケーション・デコータに出力する
520
プログラムの再生に対して条件付きアクセス・システムによりユーザに支払請求する
527
終了
530

フロントページの続き

(51)Int.Cl.		FI	
H04H 60/18	***(2008.01)***	H04H	60/27
		H04H	60/18

(72)発明者 ブラツター, ハロルド
アメリカ合衆国 インデイアナ州 インデイアナポリス ブルースター・ロード ２２２０
(72)発明者 ホランダー, トーマス エドワード
アメリカ合衆国 インデイアナ州 インデイアナポリス ハバーフオード・アベニユー ６２３４
(72)発明者 ブリツジウオーター, ケビン エリオツト
アメリカ合衆国 インデイアナ州 インデイアナポリス サウス・ミユシング・ロード ２９０
(72)発明者 デイース, マイケル スコツト
アメリカ合衆国 インデイアナ州 ザイアンズビル インデイアン・バイプ・レーン １１０３

審査官 長谷川 素直

(56)参考文献 特開平２－４１０９０（ＪＰ, Ａ）
特開平２－４１０９１（ＪＰ, Ａ）
特開平８－２４２４３８（ＪＰ, Ａ）
特開平８－１９５７３５（ＪＰ, Ａ）
特開平８－７９２３４（ＪＰ, Ａ）
特開平４－１５０３３３（ＪＰ, Ａ）
特開平７－２８８７９８（ＪＰ, Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｎ ７／１６－７／１６７,
Ｈ０４Ｎ ５／９１－５／９５,
Ｈ０４Ｈ ６０／１８,
Ｈ０４Ｈ ６０／２３,
Ｈ０４Ｈ ６０／２７,
Ｈ０４Ｌ ９／０８