(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-531165
(P2005-531165A)
(43)公表日　平成17年10月13日(2005.10.13)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04N 7/16	H04N 7/16	Z	5B017
G06F 12/14	G06F 12/14	540C	5C064
H04L 9/08	G06F 12/14	540P	5J104
H04L 9/32	H04L 9/00	601Z	
	H04L 9/00	675B	

審査請求 未請求　予備審査請求 未請求　（全 54 頁）

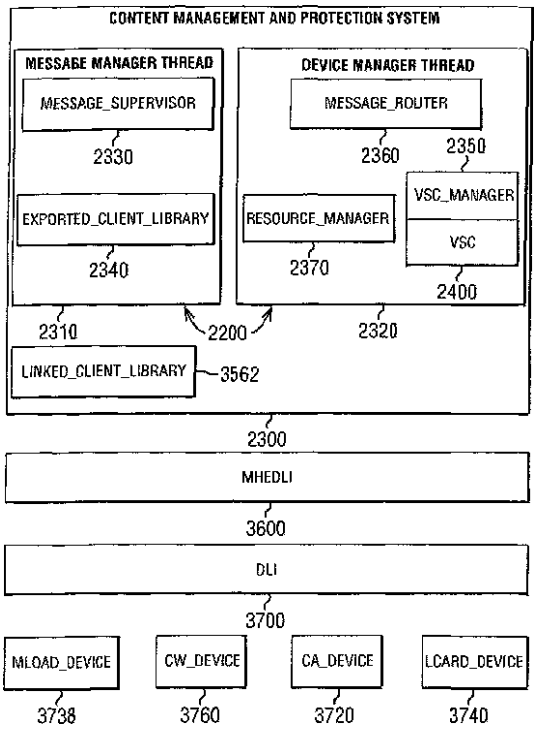
(21)出願番号　特願2003-551653 (P2003-551653)
(86)(22)出願日　平成14年12月12日 (2002.12.12)
(85)翻訳文提出日　平成16年6月11日 (2004.6.11)
(86)国際出願番号　PCT/IB2002/005774
(87)国際公開番号　WO2003/050661
(87)国際公開日　平成15年6月19日 (2003.6.19)
(31)優先権主張番号　01403228.8
(32)優先日　平成13年12月12日 (2001.12.12)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　エフ－９２１００　ブローニュ　ビヤンクール，　ケ　アルフォンス　ル　ガロ，　４６番地
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　レポリーニ，ダヴィド
フランス国，７５９０６　パリ，プラス・ラウル・ドトリー　３４，カナルプラス　テクノロジーズ　ソシエテ　アノニム内

最終頁に続く

(54)【発明の名称】データ処理

(57)【要約】
バーチャルスマートカード、バーチャルマネージャ、及びバーチャルスマートカード及び/またはバーチャルマネージャを有するデータ処理装置が開示される。



【特許請求の範囲】
【請求項１】
ペイロードと該ペイロードを含む暗号化されたデータの１つを選択する手段と、
前記選択されたペイロードまたは暗号化されたデータを格納する手段と、
前記格納された暗号化されたデータを前記ペイロードと置換する手段とを有するデータ処理装置。
【請求項２】
請求項１記載のデータ処理装置であって、さらに、
前記暗号化されたデータをスマートカードに送信する手段と、
前記スマートカードから前記暗号化されたデータに含まれるペイロードまたは該ペイロードが解読不能であることを示す応答を受信する手段とを有するデータ処理装置。
【請求項３】
請求項１または２記載のデータ処理装置であって、前記ペイロードと暗号化されたデータの１つを選択する手段は、前記ペイロードが利用可能である場合には前記ペイロードを選択し、そうでない場合には前記ペイロードを含む暗号化されたデータを選択するよう構成されることを特徴とするデータ処理装置。
【請求項４】
請求項１乃至３何れか一項記載のデータ処理装置であって、さらに、
前記ペイロードに関するデータの格納及び再生の少なくとも１つを実行する手段を有することを特徴とするデータ処理装置。
【請求項５】
請求項１乃至４何れか一項記載のデータ処理装置であって、さらに、
暗号化されたデータオブジェクトをさらなる暗号化されたデータオブジェクトにカプセル化する手段を有することを特徴とするデータ処理装置。
【請求項６】
請求項１乃至５何れか一項記載のデータ処理装置であって、さらに、
暗号鍵により前記格納されたペイロードまたは暗号化されたデータを暗号化する手段を有することを特徴とするデータ処理装置。
【請求項７】
請求項１乃至６何れか一項記載のデータ処理装置であって、さらに、
認証鍵により前記格納されたペイロードまたは暗号化されたデータを認証する手段を有することを特徴とするデータ処理装置。
【請求項８】
請求項１乃至７何れか一項記載のデータ処理装置であって、さらに、
通信暗号鍵により該装置とスマートカードとの通信を暗号化する手段を有することを特徴とするデータ処理装置。
【請求項９】
請求項１乃至８何れか一項記載のデータ処理装置であって、さらに、
通信認証鍵により該装置とスマートカードとの通信を認証する手段を有することを特徴とするデータ処理装置。
【請求項１０】
請求項１乃至９何れか一項記載のデータ処理装置であって、さらに、
少なくとも１つのセッションを確立する手段と、
前記または各セクションと各自のセッション識別子を関連付ける手段とを有することを特徴とするデータ処理装置。
【請求項１１】
請求項１乃至１０何れか一項記載のデータ処理装置であって、さらに、
暗号/認証鍵を生成するためマスタセッション鍵を利用する手段を有することを特徴とするデータ処理装置。
【請求項１２】

暗号鍵を格納する手段と、
該格納された暗号鍵を暗号化及び認証するためのそれぞれ暗号鍵及び認証鍵の１つを生成するため、マスタセッション鍵を利用する手段とを有することを特徴とするデータ処理装置。
【請求項１３】
請求項１１または１２記載のデータ処理装置であって、前記マスタセッション鍵を利用する手段は、前記マスタセッション鍵から暗号鍵と認証鍵の両方を生成するよう構成されることを特徴とするデータ処理装置。
【請求項１４】
請求項６乃至１３何れか一項記載のデータ処理装置であって、前記暗号/認証鍵は与えられたセッションに関し、前記利用する手段は前記マスタセッション鍵を前記対応するセッション識別子により多様化するよう構成されることを特徴とするデータ処理装置。
【請求項１５】
請求項１４記載のデータ処理装置であって、さらに、
さらなるセッションを暗号化/認証するため、前記暗号/認証鍵を利用する手段を有することを特徴とするデータ処理装置。
【請求項１６】
請求項６乃至１５何れか一項記載のデータ処理装置であって、さらに、
該装置の非暗号データに応じて前記暗号/認証鍵を生成する手段を有することを特徴とするデータ処理装置。
【請求項１７】
暗号鍵値が構成可能なデータを複数の場所に格納する手段を有することを特徴とするデータ処理装置。
【請求項１８】
請求項６乃至１７何れか一項記載のデータ処理装置であって、さらに、
前記鍵を複数の部分に分割する手段と
該複数の部分を複数の場所に格納する手段とを有することを特徴とするデータ処理装置。
【請求項１９】
請求項１７または１８記載のデータ処理装置であって、前記格納する手段は少なくとも部分的に受信機/デコーダに格納するよう構成されることを特徴とするデータ処理装置。
【請求項２０】
請求項１９記載のデータ処理装置であって、さらに、
前記複数の場所が前記受信機/デコーダに擬似ランダム的に分散されるよう前記複数の場所を選択する手段を有することを特徴とするデータ処理装置。
【請求項２１】
請求項１７乃至２０何れか一項記載のデータ処理装置であって、前記格納する手段は複数の物理的装置に格納するよう構成されることを特徴とするデータ処理装置。
【請求項２２】
請求項１７乃至２１何れか一項記載のデータ処理装置であって、さらに、
前記複数の場所の少なくとも１つが配置される実質的な乱数の領域を生成する手段を有することを特徴とするデータ処理装置。
【請求項２３】
請求項１乃至２２何れか一項記載のデータ処理装置であって、さらに
複数の場所からデータを読み出す手段と、
暗号鍵を生成するため前記データを合成する手段とを有するデータ処理装置。
【請求項２４】
大容量記憶装置を有するか、あるいは備えられる受信機/デコーダであって、
アクセス権の機能として、条件付アクセスデータペイロードと該条件付アクセスデータペイロードを含む暗号化された条件付アクセスデータの１つを選択する手段と、

前記大容量記憶装置にスクランブル化されたコンテンツと、前記選択された条件付アクセスデータペーロードまたは暗号化された条件付アクセスデータを格納する手段とを有することを特徴とする受信機/デコーダ。

【請求項２５】

請求項２４記載の受信機/デコーダであって、前記条件付アクセスデータペイロードは少なくとも１つの制御ワードであり、前記暗号化された条件付アクセスデータは少なくとも１つのエンタイトルメント制御メッセージであることを特徴とする受信機/デコーダ。

【請求項２６】

請求項２５記載の受信機/デコーダであって、前記少なくとも１つの制御ワードはエンタイトルメント制御メッセージからスマートカードにより生成されることを特徴とする受信機/デコーダ。

【発明の詳細な説明】

【発明の詳細な説明】

【０００１】

本発明は、バーチャルスマートカード、バーチャルスマートカードマネージャ、データ処理装置、条件付アクセスシステム、受信機/デコーダ、配信システム、データ処理方法、暗号鍵生成方法、暗号鍵値格納方法、コンピュータプログラムプロダクツ、コンピュータ読み出し可能な媒体及び信号に関する。本発明は、受信機/デコーダの条件付アクセスシステムに関する特定の適用を見出す。

【０００２】

デジタルテレビシステムは、アナログではなくデジタル形式により視聴者にテレビチャンネルを送信する。デジタルチャンネルは、送信機側でデジタルデータストリームに符号化され、デジタル受信機/デコーダを利用して受信機側で復号される。双方向性を実現するため、テレビチャンネルを送信する同一の媒体、あるいは電話接続のような異なる媒体を介し、アップリンクが提供されるかもしれない。さらに、デジタル音声、ソフトウェア及び対話型データのような様々なタイプのデータが配信可能であり、また実際に配信されている。ここで使われる「デジタルテレビシステム」という用語は、例えば、衛星、地上波、ケーブル及び他のシステムを含むものである。

【０００３】

ここで使われる「受信機/デコーダ」という用語は、ある手段により配信または送信される、好ましくはＭＰＥＧフォーマットでのテレビ及び/ラジオ信号のような符号化または非符号化信号を受信する受信機を意味するかもしれない。また、この用語は受信信号を復号化するデコーダを意味するかもしれない。このような受信機/デコーダの実施例として、例えば、物理的に異なる受信機と一緒に機能するデコーダや、ウェブブラウザ、ビデオレコーダやテレビのような付加的機能を有するデコーダのような「セットトップボックス」において受信信号を復号化する受信機と一体的に構成されるデコーダがあげられる。

【０００４】

ＭＰＥＧという用語は、国際的規格組織のワーキンググループである「Ｍｏｔｉｏｎ Ｐｉｃｔｕｒｅｓ Ｅｘｐｅｒｔ Ｇｒｏｕｐ」により開発されたデータ送信規格をいい、デジタルテレビアプリケーションのために開発され、文書ＩＳＯ１３８１８－１、ＩＳＯ１３８１８－２、ＩＳＯ１３８１８－３及びＩＳＯ１３８１８－４で提示されたＭＰＥＧ－２規格、ＭＰＥＧ－４及び他の考えられるＭＰＥＧ規格に限定されるものではない。本特許出願では、この用語は、デジタルデータ送信の分野に適用可能なＭＰＥＧフォーマットのすべての変形、変更または拡張を含む。

【０００５】

従来の受信機/デコーダでは、着脱可能に接続できるスマートカードが、暗号「秘密」（条件付アクセスデータの復号化に必要なマスタ及び他の利用鍵のような）安全な格納を提供し、暗号「秘密」に関して重要な暗号処理を実行する。典型的には、スマートカードの利用を要する受信機/デコーダの他のソフトウェア及びハードウェア要素への標準的（不変である場合）インタフェースを提供する専用のスマートカード読取器が使用される。

【０００６】
他の展開では、受信機/デコーダ内に取り付け、あるいは含まれた大容量記憶装置に受信したオーディオビジュアルコンテンツの記録（及び以降の再生）を可能にする受信機/デコーダのためのシステムが提案されてきた。そのようなシステムの多くは、セキュリティのためスクランブル形式でオーディオビジュアルコンテンツを格納し、特にセキュリティのため、上述のようなスマートカードを利用して、再生中にコンテンツのスクランブル解除を行う（スマートカードがコンテンツのライブ視聴中利用されるのと同様に）。
【０００７】
本発明は上記従来技術における問題点を解決するものである。
【０００８】
本発明の第１の特徴として、バーチャルスマートカードが提供される。
【０００９】
ここで使われる「スマートカード」という用語は、好ましくは、例えば、マイクロプロセッサ及び/またはメモリ記憶装置を処理し、特に、暗号処理を実行する任意の従来技術によるチップベース携帯カードタイプ装置を意味する。これには、ＰＣＭＣＩＡカード、ＳＩＭカードなどが含まれる。特に、「スマートカード」という用語は、特定の形状やサイズを意味するというより、むしろその携帯性及び/または暗号処理能力を意味するものであり、このためしばしばテレビデコーダシステムで利用されるような鍵状の装置などの他の物理的形状を有するチップ装置もまたこの用語に含まれる。
【００１０】
好ましくは、スマートカードは、少なくとも部分的にソフトウェアで、また部分的にハードウェアで、そして任意の適当なそれらの組み合わせで与えられる。例えば、暗号スキームにおいて広く利用される乱数発生器は、ハードウェア的に実現されうるが、そのより管理的機能はソフトウェア的に実現される。
【００１１】
バーチャルスマートカードを提供することにより、あるレベルのフレキシビリティを実際の物理的スマートカードの存在を要するシステムに与えることができる。
【００１２】
この重要な特徴はまた、バーチャルスマートカードを有するデータ処理装置の形式で与えられる。ここで使われる「データ」という用語は、一般に、記録形態及び信号形態（電気的あるいはそれ以外の形態）での情報を意味する。好ましくは、データはバーチャルスマートカードにより処理される。
【００１３】
この特徴はさらに、バーチャルスマートカードを提供するため、スマートカードをエミュレートする手段（プロセッサやそれに関連するメモリなど）を有するデータ処理装置の形式で与えられる。
【００１４】
スマートカードをエミュレートする手段は、好ましくは、暗号処理を実行する手段（同一あるいはさらなるプロセッサのような）と暗号データを格納する手段（同一あるいはさらなるメモリのような）を有する。暗号処理を実行する手段は、好ましくは、バーチャルスマートカードに等価な実際のスマートカードにおける対応する手段より高速であるものが選ばれ、これにより、実際のスマートカードに対してより良好なパフォーマンスを生み出すことが可能となる。同様に、暗号データを格納する手段は、実際のスマートカードにおける対応する手段より高速かつ/または大容量であり、これにより、さらなる良好なパフォーマンスを生み出すことができる。暗号処理を実行する手段は、例えば、受信機/デコーダのホストプロセッサであるかもしれないし、暗号データを格納する手段は、例えば、ホストプロセッサと関連付けられたRAMであるかもしれない。
【００１５】
これにより、広範囲の暗号タスクのバーチャルスマートカードでのエミュレート処理が可能となる。さらに、早送り再生モードでのコンテンツの良好なリアルタイムでのスクラ

ンブル解除を可能にするなどのような（従来のスマートカードでは不可能な、一般権利管理のような、制御ワードの解読に要する時間と、さらに他の時間を要する処理に費やされる時間が与えられる）、従来のスマートカードを上回る機能性を有するバーチャルスマートカードを実現することができる。

【００１６】

本発明の関連する特徴として、バーチャルスマートカードのより効率的な処理を可能にするバーチャルスマートカードマネージャが提供される。特に、本バーチャルスマートカードマネージャは、アブストラクションレイヤ（ａｂｓｔｒａｃｔｉｏｎ　ｌａｙｅｒ）をバーチャルスマートカードの機能の実現形態に与えるかもしれない。ここで使われる「マネージャ」という用語は、好ましくは、制御機能、インタフェース機能、データルーティング機能及び/または処理機能の少なくとも１つを有するものを意味する。

【００１７】

この重要な特徴はまた、バーチャルスマートカードマネージャを有するデータ処理装置の形式で独立に提供される。

【００１８】

本装置はさらに、好ましくは、バーチャルスマートカードとのインタフェースを提供し、バーチャルスマートカードの管理を簡素化する手段を有する。

【００１９】

この重要な特徴はまた独立に与えられる。本発明の関連する特徴では、バーチャルスマートカードとのインタフェースを提供する手段を有するデータ処理装置が提供される。再び、好ましくは、データはバーチャルスマートカードにより処理される。

【００２０】

上記装置はさらに、好ましくは、暗号データをバーチャルスマートカードと交換する手段を有する。このような暗号データを交換する手段は、暗号データをバーチャルスマートカードに送信する手段、あるいは暗号データをバーチャルスマートカードから受信する手段のどちらか、またはその両方を有するかもしれない。暗号データを送受信する手段は、例えば、後述のバーチャルスマートカードマネージャとバーチャルスマートカードとの間のイベント及び関数呼び出しであるかもしれない。

【００２１】

従って、バーチャルスマートカードの管理はさらに容易となるかもしれない。

【００２２】

本装置がさらにバーチャルスマートカードと等価な実際のスマートカードの存在を決定する手段を有する場合、本装置はさらに、好ましくは、暗号データを実際の等価なスマートカードと交換する手段を有する。バーチャルスマートカードは、これと等価な実際のスマートカードにより提供される特徴の一部を実現するかもしれないし、その逆もありうる。バーチャルスマートカードに等価な実際のスマートカードの存在を決定し、選択的に暗合データをこれと交換することにより、さらなるオプションがデータ処理に提供される。

【００２３】

本装置は、スマートカードを選択する手段を有するかもしれない。適切なスマートカードの選択により、システムにあるレベルのフレキシビリティを付加することが可能となる。

【００２４】

特に、本装置はさらに、選ばれたスマートカードを利用してデータを復号化する手段を有し、このスマートカードを選択する手段はデータの特徴に依存してスマートカードを選択するよう適応されている。この特徴とは、例えば、データの商業的な重要さ、データの持続期間（好ましくは、測定時間のような）、データサイズ、データが配布された程度であるかもしれない。従って、さらなるフレキシビリティの提供が可能となる。

【００２５】

データは、電子所世紀、ソフトウェア、ゲームなどの音声/画像あるいは他のコンテンツを有するものであってよい。ここで使われる「音声/画像」という用語は、好ましくは

、音声あるいは画像、それらを組み合わせたものを意味する。受信機/デコーダにより受信される放送信号に関して、この用語はテレビプログラムを構成する音声及び映像に密接に関連して送信されるサブタイトル、テレテキスト、同期データ及び他のデータを含むものであるかもしれない。

【００２６】

本装置はさらに、ペイロードとこのペイロードを含む暗号化されたデータの１つを選択する手段と、この選択されたペイロードあるいは暗号化されたデータを格納する手段と、この格納された暗号化されたデータをこのペイロードと取り替える手段とを有するようにしてもよい。例えば、これは、利用可能であるときには、コンテンツ管理メッセージ（ＣＭＭ）に暗号鍵（典型的には、当該暗号有効期間における制御ワード）をまず格納し、そうでないときには、当該暗号鍵を含む暗号化されたデータ（典型的には、関連するエンタイトルメント制御メッセージ）を格納し、その後、利用可のであるときには、この暗号化されたデータを対応する鍵と取り替えるというプロセスに対応する（後述のように）。

【００２７】

上記手段を提供することにより、格納時にペイロードを解読する必要を回避することができる（例えば、ペイロードを完全に含むデータがその時点で構築中である場合）。

【００２８】

この重要な特徴はまた独立に提供される。

【００２９】

本発明の関連する特徴によると、ペイロードと当該ペイロードを含む暗号化されたデータの１つを選択する手段と、この選択されたペイロードあるいは暗号化されたデータを格納する手段と、この格納された暗号化されたデータをペイロードと取り替える手段とを有するデータ処理装置が提供される。

【００３０】

上述のように、暗号化されたデータは、与えられたコンテンツのセクションをスクランブル解除するのに要する１以上の制御ワードのペイロードを有するエンタイトルメント制御メッセージ（ＥＣＭ）であってもよい。これにより、当該選択手段は、好ましくは、少なくとも１つの制御ワード及びエンタイトルメント制御メッセージの何れかを選択するよう適応される。

【００３１】

より詳細には、本装置はさらに、好ましくは、暗号化されたデータをスマートカードに送信する手段と、スマートカードからこの暗号化されたデータに含まれるペイロード、あるいはペイロードの解読が不可能であるということを示す応答を受信する手段とを有する。好ましくは、ペイロードと暗号化されたデータの何れかを選択する手段は、利用可能である場合にはペイロードを、そうでない場合にはペイロードに含まれる暗号化されたデータを選択するよう適応される。これはさらなるフレキシビリティを提供することができる。

【００３２】

さらに、本装置はさらに、好ましくは、ペイロードに関するデータの格納及び再生の少なくとも１つを実行する手段を有する。例えば、当該データは音声/画像コンテンツであってよく、当該ペイロードはこのコンテンツの一部に対する制御ワードを含むエンタイトルメント制御メッセージ（ＥＣＭ）であってもよい。通常、これは、コンテンツの格納または再生処理をコンテンツのスクランブル解除処理（あるいはスマートカードの使用を要する他の処理）と一体化することができる。

【００３３】

好ましくは、本装置はさらに、暗号化されたデータオブジェクトをさらなる暗号化されたデータオブジェクトにカプセル化する手段を有する。これにより、暗号化されたデータオブジェクトのさらなるセキュリティの向上につながり、１つのインタフェース及び/または適切なアブストラクションの提供を可能にすることにより、クライアントプロセスとの交代を簡素化しうる。さらに、本装置はさらに、好ましくは、前述の効果により、エン

タイトルメント制御メッセージをエンタイトルメント管理メッセージにカプセル化する手段を有する。

【００３４】

好ましくは、本装置はさらに、暗号鍵により格納されているペイロードまたは暗号化されたデータを暗号化する手段を有する。本装置はさらに、認証鍵により格納されているペイロードあるいは暗号化されたデータを認証する手段を有する。

【００３５】

好ましくは、本装置はさらに、通信暗号鍵により本装置とスマートカードとの通信を暗号化する手段と、通信認証鍵により本装置とスマートカードとの通信を認証する手段を有する。これにより、さらなるセキュリティが提供可能となる。

【００３６】

上記暗号及び認証鍵は、例えば、公開鍵暗号化方式により利用される公開鍵と秘密鍵とのペアから構成されるかもしれない。さらに、便宜上、通信暗号鍵は、暗号鍵と同一のもの、あるいは暗号鍵から導出されるものであってよく、同様に、通信認証鍵は、認証鍵と同一のもの、あるいは認証鍵から導出されるものであってもよい。

【００３７】

本装置はさらに、少なくとも１つのセッションを確立する手段と、当該セッションまたは各セッションを各自のセッション識別子と関連付ける手段を有するかもしれない。これにより、スマートカードあるいはカードの管理をさらに支援することが可能となる。

【００３８】

本装置はさらに、マスタセッション鍵を利用して暗号/認証鍵を、好ましくは前述のような鍵を生成する手段を有してもよい。当該生成手段は、好ましくは、入力としてもとのマスタセッション鍵と多様化値（好ましくは、整数）を受け取り、出力としてさらなる暗号鍵を生成する多様化関数を有する。さらに、多様化関数は、好ましくは、ある多様化値の範囲に対する出力が好ましくは実質的にすべての暗号的に強い鍵となるよう選ばれる。公開/秘密暗号システムでは、多様化関数は、好ましくは、出力の暗号強度を保証するためス数の様々な性質を利用する。

【００３９】

これにより、暗号/認証鍵、特に複数の鍵の生成が簡素化されうる。

【００４０】

この重要な特徴はまた独立に与えられる。本発明の関連する特徴によると、暗号鍵を格納する手段と、マスタセッション鍵を利用して当該格納された暗号鍵の暗号化及び認証をそれぞれ実行する暗号鍵と認証鍵の何れかを生成する手段を有する。

【００４１】

さらに、暗号/認証鍵は所与のセッションに関するものであってよく、この場合、当該生成手段は対応するセッション識別子によりマスタセッション鍵を多様化するよう適応されてもよい。これにより、任意の個数の鍵を生成する体系的かつシンプルな方法を提供することが可能となる。

【００４２】

本装置はさらに、暗号/認証鍵を利用してさらなるセッションを暗号化/認証する手段を有してもよい。例えば、同一の１つ以上の鍵を使って、ＨＤＶＲとＣＭＰＳとのセッションと、ＣＭＰＳとバーチャルスマートカードとのセッション（そのすべてが以下で説明される）が暗号化及び/または認証されうる。これにより、生成を要する鍵の個数を減らすことにより、計算負荷を低減することが可能となる。

【００４３】

本装置はさらに、好ましくは、受信機/デコーダにおける非暗号データに依存して、暗号/認証鍵を生成する手段を有する。この非暗号データは、好ましくは、受信機/デコーダに対して一意的なものであるか、あるいは他の対応する非暗号データと異なるものである。好ましくは、非暗号データは、暗号鍵の生成以外のさらなる利用を有し、好ましくは本来的に確率的なもの（すなわち、ある程度予測不可能なもの）である。

【００４４】
これにより、このような暗号/認証鍵のより迅速な生成が可能となる。
【００４５】
この重要な特徴はまた独立に与えられる。本発明の関連する特徴によると、受信機/デコーダの非暗号データに依存して暗号鍵を生成する手段を有するデータ処理装置が提供される。
【００４６】
好ましくは、本装置はさらに、乱数発生器、非暗号データにより乱数発生器にシードを提供する手段と、乱数発生器の出力に応じて鍵を生成する手段とを有する。これにより、既知の乱数発生器を利用した有用な鍵生成方法の提供が可能となる。
【００４７】
本装置はさらに、好ましくは、ランダムさ、予測不可能性、時間可変性及び空間可変性の少なくとも１つの性質を測定する手段と、当該あるいは各性質に応じた鍵を生成する手段を有する。好ましくは、受信機/デコーダの少なくとも３、５、１０、２０または５０の性質が測定される。これにより、得られる鍵のランダムさを促進することができる。
【００４８】
特に、鍵生成手段は、受信機/デコーダにより受信されるビットストリームの性質、受信機/デコーダ内のハードウェア環境の性質、受信機/デコーダ内のソフトウェア環境の性質、及び受信機/デコーダ外の環境の計測可能な性質の少なくとも１つに応じた鍵を生成するよう適応されてもよい。このような性質には、例えば、チューナーのビットエラーレート（ＢＥＲ）、信号レベル、受信機/デコーダソフトウェアの特定部分へのアクセス数、離調（ｄｅｔｕｎｅｄ）無線（ＲＦ）受信機の出力などが含まれる。
【００４９】
鍵生成手段は、鍵が必要となる前、好ましくは、受信機/デコーダの初期化あるいは再初期化（例えば、リブート後など）に応答して、鍵を生成するよう適応されてもよい。あるいは、またはさらに、本発明はさらに、鍵の供給を必要とする処理を実行するコマンドの呼び出しに応答して鍵を生成する手段を有してもよい。これらの特徴は、組み合わされて、あるいは単独で、よりフレキシブルな鍵生成を提供することができる。
【００５０】
ここで使われる「コマンド」という用語は、好ましくは、例えば、適切なデータキャリアへのルーチンの記録のような、メモリにおける電気パルスの形態、あるいはより恒久的な形態により、指定された機能を実行するようプログラムされたソフトウェアルーチンの物理的実現を意味する。好ましくは、ルーチンの実現は、プロセッサにより即座に実行可能なものであり、オブジェクトコードとして格納されている。この用語はまた、ルーチンを実行させるための物理的実現される指示の形式、あるいはルーチンを実行させるよう構成される、リモートプロシージャコール（ＲＰＣ）のような実際の信号の形式で、ルーチンの実際の呼び出しをカバーするよう拡張されてもよい。
【００５１】
本装置はさらに、暗号/認証鍵、好ましくは前述のような鍵を格納する手段を有してもよい。これにより、鍵の再生成の必要を避けることにより、システムの効率性を改善することが可能となる。本装置はさらに、例えば、鍵が利用可能なセキュリティレベルに対して価値があるとみなされる場合、鍵を格納するかどうか決定する手段を有してもよい。これにより、システムのセキュリティの向上が可能となる。
【００５２】
本装置はさらに、好ましくは、鍵の構成が可能なデータを複数の場所に格納する手段を有する。暗号鍵は、単なる暗号鍵値以上のものを有するかもしれないし、例えば、マスタ鍵、鍵生成アルゴリズム及び鍵多様化手段（例えば、セッションＩＤのような）の何れかを有するものであってよい。また、複数の場所は、好ましくは、相異なるり、かつ隣接していないものであり(少なくとも部分的に)、例えば、放送センター、加入者データセンター、スマートカード、受信機/デコーダなどの任意数の装置に存在するかもしれない。さ

らに、複数の場所は、受信機/デコーダ内のＥＥＰＲＯＭ、ＲＡＭ、フラッシュＲＡＭ、ハードディスク及びスマートカードの何れかを有するようにしてもよい。データはまた少なくとも部分的には装置自体に有効に格納されてもよく、データの露出を減らすことができる。さらに、例えば、１つの場所ではなく、複数の場所に鍵の構成を可能にするデータにより、システムの安全性が向上する。

【００５３】

この重要な特徴はまた単独で提供される。本発明の関連する特徴によると、鍵の構成を可能にするデータを複数の場所に格納する手段を有するデータ処理装置が提供される。

【００５４】

本装置は、鍵を複数の部分に分割する手段と、これら複数の部分を複数の場所に格納する手段とを有するようにしてもよい。当該分割手段は、暗号鍵を表すデータビットシーケンスを各自が小さなデータビットから構成される複数の部分に分割するよう調整されてもよく、当該複数の部分を格納する手段は、異なるアドレスにあるこれらの部分を記憶媒体に格納するよう調整されてもよい。好ましくは、これらの部分は、１、２、４、８、１６、３２あるいはそれ以上のビットから構成される。好ましくは、これら複数の部分の少なくとも２つ、好ましくはすべてが同じサイズを有する。

【００５５】

比較的大きなサイズの鍵に関して、より小さな（従って、気付くのが困難な）部分を生成することにより、鍵データはより容易に視界から隠すことができる。

【００５６】

これにより、当該格納手段は、受信機/デコーダに少なくとも部分的に格納するよう調整されるかもしれない。これにより、格納を簡素化し、外部記憶ソースへの依存を減らすことが可能となる。

【００５７】

好ましくは、本装置はまた、実質的な乱数の領域を複数の場所の少なくとも１つに生成する手段を有するようにしてもよい。暗号鍵はそれの明らかなランダムさによりときどき特定されうるため、鍵要素の実質的な乱数領域への格納は、より効率的に鍵を隠すことが可能である。

【００５８】

本装置はさらに、好ましくは、複数の領域から複数の鍵部分を読み出す手段と、暗号鍵を生成するためこれらの鍵部分を合成する手段とを有する。好ましくは、当該鍵部分合成手段は、複数の鍵部分に対して可逆な変換（線形代数変換の場合の逆行列処理のような）を実行するよう調整される。これにより、格納されている暗号鍵の再生を容易にすることが可能である。

【００５９】

本発明の関連する特徴によると、バーチャルスマートカードを提供するため、スマートカードをエミュレートするよう調整されたプロセッサとそれに関連したメモリを有するデータ処理装置が提供される。

【００６０】

好ましくは、本装置はさらに、バーチャルスマートカードを有する。プロセッサはまた暗号処理を実行するよう調整され、メモリは暗号データを格納するよう調整されてもよい。

【００６１】

本発明のさらなる関連する特徴によると、バーチャルスマートカードとのインタフェースを提供するよう調整されたプロセッサと関連したメモリを有するデータ処理装置が提供される。

【００６２】

プロセッサは、暗号データとバーチャルスマートカードを交換するよう調整され、あるいはバーチャルスマートカードと等価な実際のスマートカードの存在を決定するよう調整されてもよい。好ましくは、プロセッサはさらに、暗号データを実際の等価なスマートカ

ードと交換するよう調整される。

【００６３】

プロセッサはさらに、スマートカードを選ぶよう調整されてもよく、好ましくは、選ばれたスマートカードを利用してデータを復号化し、データの特性に応じてスマートカードを選択するよう調整されてもよい。好ましくは、プロセッサはさらに、ペイロード及び当該ペイロードを含む暗号化されたデータの１つを選び、選ばれたペイロードあるいは暗号化されたデータを格納し、この格納され暗号化されたデータをペイロードと置換するよう調整される。

【００６４】

本発明の関連する特徴によると、ペイロード及び当該ペイロードを含む暗号化されたデータの１つを選び、選ばれたペイロードあるいは暗号化されたデータを格納し、この格納された暗号化されたデータをペイロードと置換するよう調整されるプロセッサと関連したメモリを有するデータ処理装置が提供される。当該プロセッサは、少なくとも１つの制御ワードとエンタイトルメント制御メッセージの１つを選ぶよう調整されてもよい。さらに、プロセッサは、案が浮かされたデータをスマートカードに送信し、このスマートカードから暗号化されたデータに含まれるペイロード、あるいはペイロードが解読不可能であるということを示す応答を受信するよう調整されてもよい。好ましくは、プロセッサは、利用可能である場合にはペイロードを選択し、そうでない場合にはペイロードを含む暗号化されたデータを選択するよう調整される。

【００６５】

当該プロセッサは、ペイロードに関連したデータの格納あるいは再生を実行するよう調整されてもよい。プロセッサは、暗号化されたデータオブジェクトをさらなる暗号化されたデータオブジェクトにカプセル化するよう調整されてもよく、さらに、エンタイトルメント制御メッセージをエンタイトルメント管理メッセージにカプセル化するよう調整されてもよい。

【００６６】

好ましくは、プロセッサは、暗号鍵により格納されたペイロードあるいは暗号化されたデータを暗号化するよう調整され、認証鍵により格納されたペイロードあるいは暗号化されたデータを認証するよう調整されてもよい。また好ましくは、プロセッサは、通信暗号鍵により本装置とスマートカードとの通信を暗号化し、通信認証鍵により本装置とスマートカードとの通信を認証するよう調整されてもよい。

【００６７】

プロセッサは、少なくとも１つのセッションを確立し、当該または各セッションと各自のセッション識別子とを関連付けるよう調整されてもよい。プロセッサは、好ましくは、マスタセッション鍵を利用して暗号/認証鍵を生成するよう調整される。

【００６８】

本発明の関連する特徴によると、暗号鍵を（好ましくは、関連するメモリに）格納し、マスタセッション鍵を利用して格納されている暗号鍵をそれぞれ暗号化及び認証する暗号鍵と認証鍵の１つを生成するよう調整されたプロセッサと関連するメモリを有するデータ処理装置が提供される。

【００６９】

好ましくは、プロセッサは、マスタセッション鍵から暗号鍵と認証鍵の両方を生成するよう調整される。より好適には、プロセッサは、マスタセッション鍵を対応するセッション識別子により多様化するよう調整され、暗号/認証鍵を利用してさらなるセッションを暗号化/認証するよう調整されてもよい。

【００７０】

プロセッサは、好ましくは、受信機/デコーダに非暗号データに応じて暗号/認証鍵を生成するよう調整される。

【００７１】

本発明のさらなる特徴によると、受信機/デコーダに非暗号データに応じて暗号/認証鍵

を生成するよう調整されたプロセッサと関連するメモリを有するデータ処理装置が提供される。

【００７２】

好ましくは、本発明はさらに、乱数発生器を有し、プロセッサは非暗号データにより乱数発生器のシードを提供し、乱数発生器の出力に応じて鍵を生成するよう調整される。

【００７３】

好ましくは、本装置はさらに、ランダムさ、予測不可能性、時間可変性及び空間可変性の少なくとも１つの性質を測定する検出器を有し、プロセッサは当該または各性質に応じて鍵を生成するよう調整される。さらに、プロセッサは、受信機/デコーダにより受信されるビットストリームの性質、受信機/デコーダ内のハードウェア環境の性質、受信機/デコーダ内のソフトウェア環境の性質、及び受信機/デコーダ外の環境の計測可能な性質の少なくとも１つに応じて鍵を生成するよう調整されてもよい。

【００７４】

プロセッサは、鍵が必要となる前に鍵を生成するよう調整されてもよく、あるいは、またはさらに、プロセッサは、鍵の供給を要する処理を実行するコマンドの呼び出しに応答して、鍵を生成するよう調整されてもよい。

【００７５】

プロセッサは、暗号/認証鍵を格納するよう調整されてもよく、好ましくは、鍵を格納するか決定するよう調整される。プロセッサはさらに、鍵の構成が可能なデータを複数の場所に格納するよう調整されてもよい。

【００７６】

本発明の他の特徴によると、暗号鍵値の構成が可能なデータを複数の場所に格納するよう調整されるプロセッサと関連するメモリを有するデータ処理装置が提供される。

【００７７】

好ましくは、プロセッサは、鍵を複数の部分に分割し、これら複数の部分を複数の場所に格納するよう調整される。プロセッサはさらに、好ましくは、受信機/デコーダに少なくとも部分的に格納するよう調整される。さらに、プロセッサは、これら複数の場所が受信機/デコーダに擬似ランダム的に分布されるよう複数の場所を選ぶよう調整されてもよい。

【００７８】

プロセッサは、好ましくは、複数の物理的な装置に格納するよう調整され、実質的な乱数の領域をこれら複数の場所の少なくとも１つに生成するよう調整されてもよい。プロセッサはさらに、複数の場所からデータを読み出し、暗号鍵を生成するためデータを合成するよう調整されてもよい。

【００７９】

本発明のさらなる特徴によると、前述の装置を有する受信機/デコーダが提供される。

【００８０】

本発明のさらなる特徴によると、前述の装置を有する条件付アクセスシステムが提供される。

【００８１】

本発明の他の特徴によると、放送センターと前述の受信機/デコーダを有する放送システムが提供される。

【００８２】

本発明のさらなる特徴によると、前述の装置を有する放送システムが提供される。

【００８３】

本発明の他の特徴によると、バーチャルスマートカードを提供するため、スマートカードをエミュレートするステップを有するデータ処理方法が提供される。

【００８４】

好ましくは、本方法はさらに、バーチャルスマートカードを提供するステップを有する。スマートカードをエミュレートするステップは、好ましくは、暗号処理を実行するステ

ップと、暗号データを格納するステップとを有する。

【００８５】

本発明のさらなる特徴によると、バーチャルスマートカードとのインタフェースを提供するステップを有するデータ処理方法が提供される。

【００８６】

好ましくは、本方法は、暗号データをバーチャルスマートカードと置換するステップを有し、あるいは、またはさらに、バーチャルスマートカードと等価な実際のスマートカードの存在を決定するステップを有するかもしれない。好ましくは、本方法はさらに、暗号データを実際の等価なスマートカードと置換するステップを有する。

【００８７】

本方法はさらに、スマートカードを選択するステップを有してもよく、好ましくは、選択されたスマートカードを利用してデータを復号化するステップと、データの特性に応じてスマートカードを選択するステップを有する。好ましくは、本方法はさらに、ペイロード及び当該ペイロードを含む暗号化されたデータの１つを選択するステップと、選択されたペイロードあるいは暗号化されたデータを格納するステップと、格納された暗号化されたデータをペイロードと置換するステップとを有する。

【００８８】

本発明のさらなる特徴によると、ペイロード及び当該ペイロードを含む暗号化されたデータの１つを選択するステップと、選択されたペイロードあるいは暗号化されたデータを格納するステップと、格納された暗号化されたデータをペイロードと置換するステップとを有するデータ処理方法が提供される。

【００８９】

当該選択するステップは、少なくとも１つの制御ワードとエンタイトルメント制御メッセージの１つを選択するステップを有してもよい。本方法はさらに、暗号化されたデータをスマートカードに送信するステップと、スマートカードから暗号化されたデータに含まれるペイロード、あるいはペイロードが解読不可能であるということを示す応答を受信するステップとを有する。好ましくは、本方法は、利用可能である場合にはペイロードを選択し、そうでない場合にはペイロードを含む暗号化されたデータを選択するステップを有する。

【００９０】

本方法は、ペイロードに関連したデータの格納または再生を実行するステップを有する。本方法はさらに、暗号化されたデータオブジェクトをさらに暗号化されたデータオブジェクトにカプセル化するステップを有するようにしてもよく、当該カプセル化するステップはさらに、エンタイトルメント制御メッセージをエンタイトルメント管理メッセージにカプセル化するステップを有するようにしてもよい。

【００９１】

好ましくは、本方法はさらに、暗号鍵により格納されたペイロードあるいは暗号化されたデータを暗号化するステップを有し、認証鍵により格納されたペイロードあるいは暗号化されたデータを認証するステップを有するようにしてもよい。また、好ましくは、本方法は、通信暗号鍵により装置とスマートカードとの通信を暗号化するステップを有し、通信認証鍵により装置とスマートカードとの通信を認証するステップを有するようにしてもよい。

【００９２】

本方法は、少なくとも１つのセッションを確立するステップと、当該または各セッションを各自のセッション識別子と関連付けるステップとを有するようにしてもよい。好ましくは、本方法は、マスタセッション鍵を利用して暗号/認証鍵を生成するステップを有する。

【００９３】

本発明の関連する特徴によると、暗号鍵を格納するステップと、マスタセッション鍵を利用して格納された暗号鍵をそれぞれ暗号化及び認証する暗号鍵と認証鍵の１つを生成す

るステップを有するデータ処理方法が提供される。

【００９４】

好ましくは、本方法は、マスタセッション鍵から暗号鍵と認証鍵の両方を生成するステップを有する。より好ましくは、本方法は、マスタセッション鍵を対応するセッション識別子により多様化するステップを有してもよく、暗号/認証鍵を利用してさらなるセッションを暗号化/認証するステップを有してもよい。

【００９５】

好ましくは、本方法は、受信機/デコーダの非暗号データに応じて暗号/認証鍵を生成するステップを有する。

【００９６】

本発明のさらなる特徴によると、受信機/デコーダの非暗号データに応じて暗号/認証鍵を生成するステップを有する暗号鍵生成方法が提供される。

【００９７】

好ましくは、本方法はさらに、非暗号データにより乱数発生器にシードを提供するステップと、乱数発生器から出力を得るステップと、乱数発生器の出力に応じて鍵を生成するステップとを有する。

【００９８】

好ましくは、本方法はさらに、ランダムさ、予測不可能性、時間可変性及び空間可変性の少なくとも１つの性質を測定するステップを有し、本方法はさらに、当該または各性質に応じて鍵を生成するステップを有する。さらに、本方法は、受信機/デコーダにより受信されたビットストリームの性質、受信機/デコーダ内のハードウェア環境の性質、受信機/デコーダ内のソフトウェア環境の性質、及び受信機/デコーダ外の環境の計測可能な性質の少なくとも１つに応じて鍵を生成するステップを有するようにしてもよい。

【００９９】

本方法は、鍵が必要となる前に鍵を生成するステップを有し、あるいは、またはさらに、本方法は、鍵の供給が必要な処理を実行するためのコマンドの呼び出しに応答して鍵を生成するステップを有するようにしてもよい。

【０１００】

本方法は、暗号/認証鍵を格納するステップを有するようにしてもよく、好ましくは、さらに、鍵を格納するか決定するステップを有する。本方法はさらに、鍵の構成が可能なデータを複数の場所に格納するステップを有するようにしてもよい。

【０１０１】

本発明の関連する特徴によると、暗号鍵値の構成が可能なデータを複数の場所に格納するステップを有する暗号鍵値格納方法が提供される。

【０１０２】

好ましくは、本方法はさらに、鍵を複数の部分に分割するステップと、これら複数の部分を複数の場所に格納するステップとを有する。好ましくは、本方法はさらに、少なくとも部分的に受信機/デコーダに格納するステップを有する。さらに、本方法は、これら複数の場所が受信機/デコーダに擬似ランダム的に分布するよう複数の場所を選択するステップを有するようにしてもよい。

【０１０３】

好ましくは、本方法はさらに、複数の物理的な装置に格納するステップを有し、実質的な乱数の領域をこれら複数の場所の少なくとも１つに生成するステップを有するようにしてもよい。本方法は、複数の場所からデータを読み出すステップと、暗号鍵を生成するためデータを合成するステップを有するようにしてもよい。

【０１０４】

本発明のさらなる特徴によると、前述の方法を実行するよう調整されたコンピュータプログラムプロダクツが提供される。

【０１０５】

本発明のさらなる特徴によると、バーチャルスマートカードを有するコンピュータプロ

グラムプロダクツが提供される。

【０１０６】

バーチャルスマートカードを提供するため、スマートカードをエミュレートする手段を有するコンピュータプログラムプロダクツが提供される。

【０１０７】

当該スマートカードをエミュレートする手段は、好ましくは、暗号処理を実行する手段と、暗号データを格納する手段とを有する。

【０１０８】

本発明の他の特徴によると、バーチャルスマートカードマネージャを有するコンピュータプログラムプロダクツが提供される。

【０１０９】

本発明のさらなる特徴によると、バーチャルスマートカードとのインタフェースを提供する手段を有するコンピュータプログラムプロダクツが提供される。

【０１１０】

好ましくは、本コンピュータプログラムプロダクツはさらに、暗号データをバーチャルスマートカードにより交換する手段を有し、さらに、バーチャルスマートカードと等価な実際のスマートカードの存在を決定する手段を有するようにしてもよい。本コンピュータプログラムプロダクツはさらに、実際の等価なスマートカードにより暗号データを交換する手段を有するようにしてもよい。

【０１１１】

好ましくは、本コンピュータプログラムプロダクツは、スマートカードを選択する手段を有する。本コンピュータプログラムプロダクツはさらに、選択されたスマートカードを利用してデータを復号化する手段を有するようにしてもよく、当該スマートカードを選択する手段は、データの特性に応じてスマートカードを選択するよう調整される。

【０１１２】

好ましくは、本コンピュータプログラムプロダクツはさらに、ペイロードと当該ペイロードを含む暗号化されたデータの１つを選択する手段と、この選択されたペイロードあるいは暗号化されたデータを格納する手段と、格納された暗号化されたデータをペイロードにより置換する手段とを有する。

【０１１３】

本発明のさらなる特徴によると、ペイロードと当該ペイロードを含む暗号化されたデータの１つを選択する手段と、この選択されたペイロードあるいは暗号化されたデータを格納する手段と、格納された暗号化されたデータをペイロードにより置換する手段とを有するコンピュータプログラムプロダクツが提供される。

【０１１４】

当該選択手段は、少なくとも１つの制御ワードとエンタイトルメント制御メッセージの１つを選択するよう調整されてもよい。好ましくは、本コンピュータプログラムプロダクツはさらに、暗号化されたデータをスマートカードに送信する手段と、スマートカードから暗号化されたデータに含まれるペイロード、あるいはペイロードが解読不可能であることを示す応答を受信する手段とを有する。

【０１１５】

好ましくは、ペイロードと暗号化されたデータの１つを選択する手段は、利用可能である場合にはペイロードを選択し、そうでない場合にはペイロードを含む暗号化されたデータを選択するよう調整される。本コンピュータプログラムプロダクツはさらに、ペイロードに関連するデータの格納及び再生の少なくとも１つを実行する手段を有するようにしてもよい。

【０１１６】

好ましくは、本コンピュータプログラムプロダクツはさらに、暗号化されたデータオブジェクトをさらなる暗号化されたデータオブジェクトにカプセル化する手段を有し、このましくはさらに、エンタイトルメント制御メッセージをコンテンツ管理メッセージにカプ

セル化する手段を有する。

【０１１７】

好ましくは、本コンピュータプログラムプロダクツはさらに、暗号鍵により格納されたペイロードあるいは暗号化されたデータを暗号化する手段を有し、認証鍵により格納されたペイロードあるいは暗号化されたデータを認証する手段を有するようにしてもよい。

【０１１８】

好ましくは、本コンピュータプログラムプロダクツはさらに、通信暗号鍵により装置とスマートカードとの通信を暗号化する手段を有し、通信認証鍵により装置とスマートカードとの通信を認証する手段を有するようにしてもよい。

【０１１９】

好ましくは、本コンピュータプログラムプロダクツはさらに、少なくとも１つのセッションを確立する手段と、当該または各セッションと各自のセッション識別子を関連付ける手段とを有する。本コンピュータプログラムプロダクツはさらに、マスタセッション鍵を利用して暗号/認証鍵を生成する手段を有するようにしてもよい。

【０１２０】

本発明のさらなる特徴によると、暗号鍵を格納する手段と、マスタセッション鍵を多様化して格納された暗号鍵をそれぞれ暗号化及び認証するための暗号鍵と認証鍵の１つを生成する手段とを有するコンピュータプログラムプロダクツが提供される。

【０１２１】

当該生成手段は、マスタセッション鍵から暗号鍵と認証鍵の両方を生成するよう調整されてもよい。当該生成手段は、好ましくは、マスタセッション鍵を対応するセッション識別子により多様化するよう調整される。好ましくは、本コンピュータプログラムプロダクツはさらに、暗号/認証鍵を利用してさらなるセッションを暗号化/認証する手段を有し、さらに、受信機/デコーダにおける非暗号データに応じて暗号/認証鍵を生成する手段を有するようにしてもよい。

【０１２２】

本発明の他の特徴によると、受信機/デコーダにおける非暗号データに応じて暗号鍵を生成する手段を有するコンピュータプログラムプロダクツが提供される。

【０１２３】

本コンピュータプログラムプロダクツはさらに、乱数発生器と、非暗号データにより乱数発生器にシードを提供する手段と、乱数発生器の出力に応じて鍵を生成する手段とを有するようにしてもよい。

【０１２４】

本コンピュータプログラムプロダクツはさらに、ランダム製、予測不可能性、時間可変性及び空間可変性の少なくとも１つの性質を測定する手段と、当該あるいは各性質に応じて鍵を生成する手段とを有するようにしてもよい。特に、当該鍵生成手段は、受信機/デコーダにより受信されるビットストリームの性質、受信機/デコーダ内のハードウェア環境の性質、受信機/デコーダ内のソフトウェア環境の性質、及び受信機/デコーダ外の環境の測定可能な性質の少なくとも１つに応じて鍵を生成するよう調整されてもよい。

【０１２５】

当該鍵生成手段は、好ましくは、鍵が必要となる前に鍵を生成するよう調整されるが、あるいは、またはさらに、本コンピュータプログラムプロダクツは、鍵の供給が必要な処理を実行するためのコマンドの呼び出しに応答して鍵を生成する手段を有するようにしてもよい。

【０１２６】

好ましくは、本コンピュータプログラムプロダクツはさらに、暗号/認証鍵を格納する手段を有し、鍵を格納すべきか決定する手段を有するようにしてもよい。本コンピュータプログラムプロダクツはさらに、鍵を構成することが可能なデータを複数の場所に格納する手段を有するようにしてもよい。

【０１２７】

本発明のさらなる特徴によると、暗号鍵値を構成することが可能なデータを複数の場所に格納する手段を有するコンピュータプログラムプロダクツが提供される。

【０１２８】

好ましくは、本コンピュータプログラムプロダクツはさらに、鍵を複数の部分に分割する手段と、これら複数の部分を複数の場所に格納する手段とを有する。当該格納手段は、少なくとも部分的に受信機/デコーダに格納するよう調整されてもよい。好ましくは、本コンピュータプログラムプロダクツはさらに、複数の場所が受信機/デコーダに擬似ランダム的に分布するよう複数の場所を選択する手段を有する。

【０１２９】

好ましくは、当該格納手段は、複数の物理的装置に格納するよう調整される。好ましくは、本コンピュータプログラムプロダクツはさらに、実質的な乱数の領域を複数の場所の少なくとも１つに生成する手段を有し、複数の場所からデータを読み出す手段と、暗号鍵を生成するためデータを合成する手段とを有するようにしてもよい。

【０１３０】

本発明のさらなる特徴によると、前述のようなコンピュータプログラムプロダクツを有するコンピュータ世も出し可能な媒体が提供される。

【０１３１】

本発明のさらなる特徴によると、前述のようなコンピュータプログラムプロダクツを現実的に実現する信号が提供される。

【０１３２】

本発明の他の特徴によると、大容量記憶装置を有するか、あるいはそれに取り付けられ、アクセス権限の一機能として、条件付アクセスデータペイロードと当該条件付アクセスデータペイロードを含む暗号化されたアクセスデータの１つを選択する手段と、大容量記憶装置にスクランブル化されたコンテンツと、選択された条件付アクセスデータペイロードまたは暗号化された条件付アクセスデータを格納する手段とを有する受信機/デコーダが提供される。

【０１３３】

好ましくは、当該条件付アクセスデータペイロードはすくなくとも１つの制御ワードであり、当該暗号化された条件付アクセスデータは少なくともエンタイトルメント制御メッセージである。さらに好ましくは、受信機/デコーダは、少なくとも１つの制御ワードがエンタイトルメント制御メッセージからスマートカードにより生成されることを特徴とする。

【０１３４】

「スクランブル化」、「暗号化」「制御ワード」及び「鍵」という用語は、言語の簡単化のため様々な方法でここでは利用されてきた。しかしながら、「スクランブル化されたデータ」と「暗号化されたデータ」との間、あるいは「制御ワード」と「鍵」との間の基本的区別はなされないということを理解されたい。

【０１３５】

本発明はまた、ここで説明された方法の何れかの実行、及び/またはここで説明された装置の特徴の何れかの実現のためのコンピュータプログラム及びコンピュータプログラムプロダクツと、ここで説明された方法の何れかの実行、及び/またはここで説明された装置の特徴の何れかの実現のためのプログラムを格納したコンピュータ読み出し可能な媒体とを提供する。

【０１３６】

本発明はまた、ここで説明された方法の何れかの実行、及び/またはここで説明された装置の特徴の何れかの実現のためのコンピュータプログラムを具現化する信号と、そのような信号を送信する方法と、ここで説明された方法の何れかの実行、及び/またはここで説明された装置の特徴の何れかの実現のためのコンピュータプログラムをサポートするオペレーティングシステムを有するコンピュータプロダクツを提供する。

【０１３７】

本発明は、添付された図面を参照して実質的にここで説明されるような方法及び/または装置に拡張される。

【０１３８】

本発明の一特徴における任意の点が、任意の適当な組み合わせにより本発明の他の特徴に適用されるかもしれない。特に、方法の特徴は装置の特徴に適用されるかもしれないし、またその逆もありうる。

【０１３９】

さらに、ハードウェア的に実現される特徴は、一般にソフトウェア的に実現されるかもしれないし、またその逆もありうる。ここでのソフトウェア及びハードウェア的特徴に関する参照はそれに応じて解釈されるべきである。

【０１４０】

本発明の好適な特徴が、添付された図面を参照して実施例を通じて説明される。

[システムの概観]

図１において、デジタルテレビシステム５００の概要が示される。以下に説明されるように、システム５００は、放送センター１０００と、受信機/デコーダ２０００と、受信機/デコーダのソフトウェア/ハードウェアアーキテクチャ３０００と、対話型システム４０００と、条件付アクセスシステム５０００とを有する。

【０１４１】

システム５００は、既知のＭＰＥＧ－２圧縮システムを利用して圧縮されたデジタル信号を送信するほぼ従来のデジタルテレビシステム５０２を含む。より詳細には、放送センター１０００のＭＰＥＧ－２圧縮装置１０１０はデジタル信号ストリーム（典型的には、映像信号ストリーム）を受信する。圧縮装置１０１０は、リンク１０２０により多重化スクランブル化装置１０３０に接続される。

【０１４２】

多重化スクランブル化装置１０３０は、複数の入力信号を受信し、トランスポートストリームを収集し、圧縮されたデジタル信号を通信リンクを含む様々な形式をとりうるリンク１０２２を介し放送センターの送信機５１０に送信する。送信機５１０は、アップリンク５１４を介し衛星中継器５２０に電磁信号を送信し、そこで電気処理され、エンドユーザにより所有あるいはレンタルされているパラボナアンテナの従来形式で、概念的なダウンリンク５１６を介し地上受信機５１２に配信される。地上波放送、ケーブル送信、結合された衛星/ケーブルリンク、電話網などのデータ送信のための他の伝送チャンネルもまた可能である。

【０１４３】

受信機５１２により受信された新郷は、エンドユーザにより所有またはレンタルされ、エンドユーザのテレビ装置２０００に接続されている一体化された受信機/デコーダ２０００に送信される。受信機/デコーダ２０００は、圧縮されたＭＰＥＧ－２信号をテレビ装置１０００のテレビ信号に復号化する。分離タイプの受信機/デコーダが図１に示されているが、受信機/デコーダは一体化されたデジタルテレビの一部であってもよい。ここで使われる「受信機/デコーダ」という用語は、セットトップボックスのような独立タイプの受信機/デコーダや、受信機/デコーダを一体化したテレビを含む。

【０１４４】

受信機/デコーダ２０００には、音声、画像及び他のデータの記録が可能なハードディスク２１００が備えられている。これにより、受信機/デコーダにより受信されたプログラムの高度な記録及び再生機能が利用可能となり、電子番組ガイドデータのような受信機/デコーダに格納される多くの他のタイプのデータが利用可能となる。

【０１４５】

受信機/デコーダのコンテンツ管理保護システム（ＣＭＰＳ）２３００（図示せず）は、ハードディスク２１００（または他の記憶装置）上のデータの記録及び再生を確実かつフレキシブルに制御する能力を提供する。

【０１４６】

マルチチャンネルシステムでは、多重化装置１０３０は、多数のパラレルソースから受信した音声及び映像情報を処理し、送信機５１０とやり取りし、対応する複数のチャンネルに情報を配信する。音声及び映像情報に加えて、メッセージ、アプリケーションあるいは他のタイプのデジタルデータが、送信されるデジタル音声及び映像情報とインタレースされたチャンネルの一部あるいはすべてに取り入れられる。

【０１４７】

対話型システム４０００は、多重化装置１０３０と受信機/デコーダ２０００に接続され、一部は放送センターに、一部は受信機/デコーダに配置される。対話型システム４０００は、エンドユーザがバックチャンネル５７０を介し様々なアプリケーションとやり取りすることを可能にする。バックチャンネルは、例えば、ＰＳＴＮ（Ｐｕｂｌｉｃ Ｓｗｉｔｃｈｅｄ Ｔｅｌｅｐｈｏｎｅ Ｎｅｔｗｏｒｋ）チャンネル（例えば、モデムバックチャンネル）やＯＯＢ（Ｏｕｔ ｏｆ Ｂａｎｄ）チャンネルであってもよい。

【０１４８】

多重化装置１０３０と受信機/デコーダ２０００に接続され、一部は放送センターに、一部は受信機/デコーダに配置される条件付アクセスシステム５０００は、エンドユーザが１以上の放送提供者からのデジタルテレビ放送にアクセスすることを可能にする。商業的な供給（すなわち、放送提供者により販売される１以上のテレビプログラム）に関するメッセージの解読が可能なスマートカードを、受信機/デコーダ２０００に挿入することができる。受信機/デコーダ２０００とスマートカードを利用して、エンドユーザは加入者モードまたはペイパービュー（ｐａｙ－ｐｅｒ－ｖｉｅｗ）モードでの商業的な提供の購入が可能である。典型的には、対話型システム４０００により利用されるバックチャンネル５７０を利用してこれは可能である。

【０１４９】

上述のように、システムにより送信されるプログラムは多重化装置１０３０においてスクランブル化され、所与の送信に適用される条件及び暗号鍵がアクセス制御システム５０００により決定される。このようにスクランブル処理されたデータの送信は、有料テレビシステムの分野では周知である。典型的には、スクランブル処理されたデータは、当該データのスクランブル解除のための制御ワードと共に送信され、制御ワード自体はいわゆる使用鍵により暗号化され、暗号形式で送信される。

【０１５０】

その後、スクランブル処理されたデータと暗号化された制御ワードは、暗号化された制御ワードの解読と、その後の送信データのスクランブル解除を実行するため、受信機/デコーダに挿入されるスマートカードに記録されている使用鍵と等価なものにアクセスする受信機/デコーダ２０００により受信される。支払いを済ませた加入者は、例えば、配信されるマンスリーエンタイトルメント管理メッセージ（ＥＭＭ）において、送信の視聴を許可するため、暗号化された制御ワードの解読に必要な使用鍵を受信するであろう。

【０１５１】

図２は、圧縮されたデジタル信号の放送媒体としてケーブルネットワークを利用するデジタルテレビシステム５０４の他の実施例を示す。この図では、同一の要素は同一の番号により示されている。

【０１５２】

衛星中継器、送信及び受信機はケーブルネットワーク５５０により置き換えられている。さらに、本実施例では、受信機/デコーダ２０００と対話型システム４０００及び条件付アクセスシステム５０００との間のモデムバックチャンネルは、取り除かれ、ケーブルネットワーク５５０と条件付アクセスシステム５０００との間はリンク５５４により、ケーブルネットワーク５５０と対話型システム４０００との間はリンク５５６によりそれぞれ置き換えられている。これにより、受信機/デコーダ２０００は、放送センターからのデータの受信と同様のリンクを介しデータの送受信を可能にするケーブルモデムや他の手段を利用して、ケーブルネットワーク５５０を介しその他のシステムとの通信を実行する。

【０１５３】
ケーブルネットワーク５５０は、専用接続、インターネット、ローカルケーブル分散ネットワーク、無線接続あるいはこれらの任意の組み合わせのような任意の形態のワイドエリアネットワーク（ＷＡＮ）でありうる。本実施例では、ＨＦＣ（Ｈｙｂｒｉｄ　Ｆｉｂｅｒ　Ｃｏａｘ）ネットワークが使用される。受信機/デコーダ２０００とテレビシステムのその他の要素との様々な通信手段は互換性を有するということが認識される。
[条件付アクセスシステム]
図３を参照するに、条件付アクセスシステム５０００は、加入者認証システム（ＳＡＳ）５２００を有する。ＳＡＳ５２００は、各放送提供者に対して１つのＳＭＳが備えられる１以上の加入者管理システム（ＳＭＳ）１１００に、ＴＣＰ－ＩＰリンクまたは他のタイプのリンクであるリンク１０４４により接続される。あるいは、１つのＳＭＳが２つの商業的な運営者間で共有されてもよいし、１つの運営者が２つのＳＭＳを利用してもよい。
【０１５４】
「マザー（ｍｏｔｈｅｒ）」スマートカード５１１０を利用した暗号化ユニット５１００の形式での第１暗号化ユニットが、リンク１０４２によりＳＡＳに接続される。マザースマートカード５１１２を利用した暗号化ユニット５１０２の形式での第２暗号化ユニットが、リンク１０４０により多重化装置１０３０に接続されている。受信機/デコーダ２０００は、「ドーター（ｄａｕｇｈｔｅｒ）」スマートカード５５００を受け取る。受信機/デコーダは、通信サーバ１２００及びモデムバックチャンネル５７０を介しＳＡＳ５２００に直接接続される。ＳＡＳは、特に、加入権をリクエストに応じてドータースマートカードに送信する。
【０１５５】
好適な実施例の変形として、インターネットやケーブル接続がＰＳＴＮ５７０と通信サーバ１２００を補完あるいは置換する。
【０１５６】
スマートカードは、１以上の商業的運営者からの機密情報を含む。「マザー」スマートカードは、様々な種類のメッセージを暗号化し、「ドーター」スマートカードは、権利を有する場合にはメッセージの解読を行う。
【０１５７】
図３を参照するに、放送センターでは、デジタル映像信号が、ＭＰＥＧ－２圧縮装置１０１０を使ってまず圧縮される（あるいはビットレートの低減）。その後、この圧縮された信号は、他の圧縮データのような他のデータによる多重化のため、多重化スクランブル化装置１０３０に送信される。
【０１５８】
スクランブル化装置は、スクランブル処理で利用され、多重化装置１０３０のＭＰＥＧ－２ストリームに含まれる制御ワードを生成する。この制御ワードは、内部的に生成され、エンドユーザの一体化された受信機/デコーダ２０００によるプログラムのスクランブル解除を可能にする。
【０１５９】
プログラムの商品化方法を示すアクセス基準がまたＭＰＥＧ－２ストリームに付加される。プログラムは、多数の「加入者」モードの１つ、及び/または多数の「ペイパービュー（ＰＰＶ）」モードまたはイベントの１つで商品化されているかもしれない。加入者モードでは、エンドユーザは１以上の商業的な提供に加入するか、あるいはその中のすべてのチャンネルを視聴する権利が与えられた「セット」に加入する。ペイパービューモードでは、エンドユーザに所望のイベントの購入が可能となるものを与える。
【０１６０】
制御ワードとアクセス基準の両方を使って、エンタイトルメント制御メッセージ（ＥＣＫ）が構成される。これは、スクランブル処理されているプログラムに関し送信されるメッセージであり、当該メッセージは配信されるプログラムの制御ワード（プログラムのス

クランブル解除を可能にする）とアクセス基準を含む。このアクセス基準と制御ワードは、リンク１０４０を介し第２暗号化ユニット５１０２に送信される。このユニットにおいて、ＥＣＭが生成及び暗号化され、多重化スクランブル化装置１０３０に送信される。

【０１６１】

データストリームとして放送提供者により配信される各サービスは、相異なる多数の要素からなる。例えば、テレビプログラムは、映像要素、音声要素、サブタイトル要素などを含んでいる。サービスについてのこれらの各要素は、以降の配信のため個別にスクランブル化及び暗号化が実行される。サービスの各スクランブル化された要素に関して、独自のＥＣＭが必要とされる。

【０１６２】

多重化装置１０３０は、ＳＡＳ５２００からの暗号化されたＥＭＭと、第２暗号化ユニット５１０２からの暗号化されたＥＣＭと、圧縮装置１０１０からの圧縮されたプログラムからなる電気信号を受信する。多重化装置１０３０は、プログラムをスクランブル処理し、このスクランブル化されたプログラムと、暗号化されたＥＭＭと暗号化されたＥＣＭとを電気信号として、図１に示されるような衛星システムあるいは他の放送システムであるかもしれない放送システム６００に送信する。受信機/デコーダ２０００は、暗号化されたＥＭＭとＥＣＭによりスクランブル化されたプログラムを取得するためこの信号を逆多重化する。

【０１６３】

受信機/デコーダは、この放送信号を受信し、ＭＰＥＧ－２データストリームを抽出する。プログラムがスクランブル解除される場合、受信機/デコーダ２０００はＭＰＥＧ－２ストリームから対応するＥＣＭを抽出し、ＥＣＭをエンドユーザの「ドーター」スマートカード５５００にわたす。これは受信機/デコーダ２０００のハウジングにスロットインされる。ドータースマートカード５５００は、エンドユーザがＥＣＭを解読し、プログラムにアクセスする権利を有するか制御する。そうでない場合、プログラムがスクランブル解除不可であることを示す否定の状態が受信機/デコーダ２０００に送られる。他方、エンドユーザが当該権利を有する場合、ＥＣＭが解読され、制御ワードが抽出される。その後、デコーダ２０００は、この制御ワードを使ってプログラムのスクランブル解除を行う。ＭＰＥＧ－２ストリームは解凍され、テレビ装置１００００への持続的送信のため映像信号に変換される。

【０１６４】

プログラムがスクランブル化されていない場合、ＥＣＭはＭＰＥＧ－２ストリームと共に送信されず、受信機/デコーダ２０００はデータの解凍を行い、及びテレビ装置１００００への送信のため当該信号を映像信号に変換する。

【０１６５】

加入者管理システム（ＳＭＳ）１１００は、すべてのエンドユーザファイル、商業的提供（料金表や宣伝）、視聴購入、ＰＰＶの詳細、エンドユーザの利用及び認証に関するデータを管理するデータベース１１５０を含む。ＳＭＳはＳＡＳから物理的に離れていてもよい。

【０１６６】

ＳＭＳ１１００は、エンドユーザに送信されるエンタイトルメント管理メッセージ（ＥＭＭ）の変更あるいは生成を示すメッセージをＳＡＳ５２００に送信する。ＳＭＳ１１００はまた、ＥＭＭの変更あるいは生成ではなく、エンドユーザの状態変化（商品受注時にエンドユーザに与えられる認証あるいはエンドユーザへの課金額に関する）のみを示すメッセージをＳＡＳ５２００に送信する。ＳＡＳ５２００はまた、ＳＭＳ１１００にメッセージ（典型的には、コールバック情報や課金情報などの情報を要求する）をＳＭＳ１１００に送信し、これによりＳＡＳ５２００とＳＭＳ１１００との通信が双方向であるということが明らかとなる。

[受信機/デコーダ]

図４を参照するに、受信機/デコーダ２０００の様々な要素が機能ブロックに関し説明

される。

【０１６７】

例えば、デジタルセットトップボックス（ＤＳＴＢ）である受信機/デコーダ２０００は、中央ホストプロセッサ２００２とデジタルＴＶコプロセッサ２００４から構成され、これらは関連付けされたメモリ要素（図示せず）を有し、コプロセッサバス２００６により接続されている。コプロセッサ２００４は、ＵＳＢインタフェース２０７０と、シリアルインタフェース２０７２と、パラレルインタフェース（図示せず）と、モデム２０７４（図１のモデムバックチャンネル５７０に接続される）から入力データを受信し、デコーダのフロントパネル２０５４上のコンタクトを切り替えるよう調整される。

【０１６８】

受信機/デコーダは、さらに、赤外線遠隔制御２０８０（及び選択的にブルートゥースイネーブル装置のような他の無線周辺機器２０８２から）から入力を受信するよう構成され、銀行スマートカード２０６０と加入者スマートカード２０６２をそれぞれ読み取るよう構成される２つのスマートカード読取器２０５０と２０５２を処理する。加入者スマートカード読取器２０５２は、暗号化された放送信号がスクランブル解除されるのを可能とするのに必要な制御ワードを逆多重化/スクランブル解除/再多重化ユニット２０１０に供給するため挿入された加入者カード２０６２と条件付アクセスユニット（図示せず）と関与する。デコーダはまた、復調/スクランブル解除ユニット２０１０によるフィルタリング及び逆多重化前に、衛星送信を受信及び復調する従来のチューナー２０１６と復調器２０１２とを含む。第２チューナー２０１８と第２復調器２０１４がまた、第２チャンネルが第１と並行に受信及び復号化されるのを可能にするため備えられる。

【０１６９】

ハードディスク２１００がまた備えられ、受信機/デコーダにより受信及び生成されるプログラム及びアプリケーションデータの格納を可能にする。２つのチューナー２０１６と２０１８、２つの復調器２０１２と２０１４、スクランブル解除/復調/再変調装置２０１０、データデコーダ２０２４及び音声デコーダ２０２６に関して、最新の記録及び再生構成が備えられ、１以上のプログラムのさらなるプログラムの視聴中における同時記録を可能にし、パラレルに発生するハードディスク間、表示装置間、及び/または入出力間のより一般的な伝送が可能となる。

【０１７０】

受信機/デコーダにおける音声出力２０３８と映像出力２０４０は、ＰＣＭミキサ２０３０と、音声ＤＡＣ２０３４と、ＭＰＥＧ映像デコーダ２０２８と、グラフィックエンジン２０３２と、ＰＡＬ／ＳＥＣＡＭエンコーダ２０３６とによりそれぞれ供給される。他のあるいは補完的出力が与えられてもよい。

【０１７１】

本説明で使用されるように、好ましくは、アプリケーションは受信機/デコーダ２０００のハイレベルな機能を制御するためのコンピュータコードである。例えば、エンドユーザがテレビ装置（図示せず）の画面上のボタンオブジェクト画面のリモート制御２０８０に焦点をあわせ、チェックキーを押下すると、当該ボタンに関する指示シーケンスが実行される。アプリケーションとそれに関するミドルウェアがホストプロセッサ２００２により実行され、リモートプロシージャコール（ＲＰＣ）がコプロセッサバス２００６を介しデジタルＴＶコプロセッサ２００４に必要時に与えられる。

【０１７２】

対話型アプリケーションは、メニューを提示し、エンドユーザのリクエストによりコマンドを実行し、アプリケーションの目的に関連するデータを提供する。アプリケーションは常駐のアプリケーション、すなわち、受信機/デコーダ２０００のＲＯＭ（あるいはＦＬＡＳＨや他の不揮発性メモリ）に格納されているか、あるいは受信機/デコーダ２０００のＲＡＭ、ＦＬＡＳＨメモリまたはハードディスクに配信及びダウンロードされたものであるかもしれない。

【０１７３】

アプリケーションは、受信機/デコーダ２０００のメモリ領域に格納され、リソースファイルとして表される。リソースファイルは、グラフィックオブジェクト記述ユニットファイル、可変ブロックユニットファイル、指示シーケンスファイル、アプリケーションファイル及びデータファイルから構成される。

【０１７４】

受信機/デコーダは、少なくとも１つのＲＡＭ容量、ＦＬＡＳＨ容量及び少なくとも１つのＲＯＭ容量に分割されたメモリ（図示せず）を含むが、この物理的構成は論理構成とは異なるものである。メモリはさらに、様々なインタフェースと関連付けされたメモリ容量に分割されてもよい。１つの観点からは、メモリはハードウェアの一部としてみなすこともできるし、他の観点からは、メモリはハードウェアとは別に示されるシステム全体をサポートまたは含むものとしてみなされうる。

[受信機/デコーダのアーキテクチャ]

図５を参照するに、受信機/デコーダのソフトウェア/ハードウェアアーキテクチャ３０００は、ソフトウェアが任意の受信機/デコーダにおいて、任意のオペレーティングシステムにより実現可能となるよう構成された５つのソフトウェアレイヤを含む。様々なソフトウェアレイヤとして、アプリケーションレイヤ３１００、アプリケーションプログラミングインタフェース（ＡＰＩ）レイヤ３３００、バーチャルマシーンレイヤ３５００、デバイスインタフェースレイヤ３７００（しばしば「デバイスレイヤ」と短縮される）及びシステムソフトウェア/ハードウェアレイヤ３９００があげられる。

【０１７５】

アプリケーションレイヤ３１００は、受信機/デコーダに常駐あるいはダウンロードされるアプリケーション３１２０を含む。アプリケーション３１２０は、例えば、Ｊａｖａ（登録商標）、ＨＴＭＬ、ＭＨＥＧ－５あるいは他の言語で記述されたユーザにより使用される対話型アプリケーションであるかもしれないし、あるいは例えば、そのような対話型アプリケーションの実行のためのような、他の目的のため受信機/デコーダにより利用されるアプリケーションであるかもしれない。このレイヤはバーチャルマシーンレイヤにより与えられるオープンアプリケーションプログラミングインタフェース（ＡＰＩ）群に基づく。本システムは、処理中または要求に応じて、受信機/デコーダのハードディスク、フラッシュメモリまたはＲＡＭメモリへのアプリケーションのダウンロードを可能にする。アプリケーションコードは、ＤＳＭＣＣ（Ｄａｔａ　Ｓｔｏｒａｇｅ　Ｍｅｄｉａ　Ｃｏｍｍａｎｄ　ａｎｄ　Ｃｏｎｔｒｏｌ）、ＮＦＳ（Ｎｅｔｗｏｒｋ　Ｆｉｌｅ　Ｓｅｒｖｅｒ）のようなプロトコルあるいは他のプロトコルを利用して、圧縮または非圧縮フォーマットで送信されうる。

【０１７６】

ＡＰＩレイヤ３３００は、対話型アプリケーション開発のためハイレベルのユーティリティを提供する。ＡＰＩレイヤ３３００は、ハイレベルＡＰＩを構成する複数のパッケージを有する。これらパッケージは対話型アプリケーションの実行に必要なすべての機能を提供する。パッケージはアプリケーションによるアクセスが可能である。

【０１７７】

好適な実施例では、ＡＰＩはＪａｖａ（登録商標）、ＰａｎＴａｌｋまたは同様のプログラミング言語で記述されたアプリケーションに対して適応される。さらに、ＡＰＩは、ＨＴＭＬ及びＭＨＥＧ－５のような他のフォーマットの解釈を容易にする。これらの特徴の他に、ＡＰＩはまた、要件が指示するように着脱可能及び拡張可能な他のパッケージ及びサービスモジュールを有する。

【０１７８】

バーチャルマシーンレイヤ３５００は、言語インタプリタや様々なモジュール及びシステムから構成される。カーネル３６５０（図示せず）により管理されるこのレイヤは、受信機/デコーダでの対話型アプリケーションの受信及び実行に必要なすべてのものから構成される。

【０１７９】

デバイスインタフェースレイヤ３７００は、デバイスマネージャとソフトウェアデバイス（単に「デバイス」とだけ一般に呼ばれる）を含む。デバイスは、外部イベントや物理的インタフェースの管理に必要な論理リソースから構成されるソフトウェアモジュールである。デバイスマネージャによる制御のもと、デバイスインタフェースレイヤは、ドライバとアプリケーション間の通信チャンネルを管理し、拡張エラー例外チェックを提供する。管理される（ハードウェア）装置の例として、カード読取器３７２２（図示せず）、モデム３７３０（図示せず）、ネットワーク３７３２（図示せず）、ＰＣＭＣＩＡ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ Ｍｅｍｏｒｙ Ｃａｒｄ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ａｓｓｏｃｉａｔｉｏｎ）、ＬＥＤディスプレイなどがあげられる。プログラマーは、ＡＰＩレイヤが上記から装置の制御を行うため、このレイヤを直接処理する必要はない。

【０１８０】

システムソフトウェア/ハードウェアレイヤ３９００は、受信機/デコーダの製造業者により与えられる。システムのモダリティのため、及びよりハイレベルなオペレーティングシステムにより供給されるサービス（イベントスケジューリングやメモリ管理のような）はバーチャルマシーン及びカーネルの一部であるため、より上位のレイヤは特定のリアルタイムオペレーティングシステム（ＲＴＯＳ）や特定のプロセッサに制限されることはない。

【０１８１】

典型的には、バーチャルマシーンレイヤ３５００は、場合によってはデバイスインタフェースレイヤ３７００及び/またはＡＰＩ３３００と共に、受信機/デコーダの「ミドルウェア」と呼ばれる。

【０１８２】

図６を参照するに、図５の上半分に対応する受信機/デコーダ３０００のソフトウェアアーキテクチャ（アプリケーションレイヤ３１００、ＡＰＩレイヤ３３００及びバーチャルマシーンレイヤ３５００から構成される）がより詳細に説明される。

【０１８３】

対話型アプリケーションとは、例えば、電子プログラムガイド、テレバンキングアプリケーション及びゲームのような商品及びサービスを取得するため、ユーザがやり取りするアプリケーションである。

【０１８４】

アプリケーションレイヤ３１００には、アプリケーションマネージャ３１１０に加えて、２つのタイプのアプリケーションがある。ウェブブラウザ３１３０のようなＡＰＩ３３００に従う限りいつでも加えることが可能な対話型アプリケーションと、対話型アプリケーションの管理及びサポートを行う常駐のアプリケーションとがある。常駐のアプリケーションは、実質的に永続的なものであり、以下を含む。

・ブート　ブートアプリケーション３１４２は、受信機/デコーダの電源がオンされると、最初に始動されるアプリケーションである。ブートアプリケーションはまず、アプリケーションマネージャ３１１０をスタートし、その後、メモリマネージャ３５４４やイベントマネージャ３５４６のようなバーチャルマシーン３５００の「マネージャ」ソフトウェアモジュールをスタートする。

・アプリケーションマネージャ　アプリケーションマネージャ３１１０は、受信機/デコーダにおいて実行される対話型アプリケーションを管理する。すなわち、イベントの開始、中断、延期、再開及び処理が行われ、アプリケーション間の通信が処理される。アプリケーションマネージャ３１１０は、複数のアプリケーションの同時実行を可能にし、それらに対するリソースの配分が行われる。このアプリケーションはユーザに対して完全に明らかにされる。

・セットアップ　セットアップアプリケーション３１４４の目的は、主として最初に利用されるとき、受信機/デコーダを設定するためものである。セットアップアプリケーション３１４４は、テレビチャンネルの走査、日時の設定、ユーザ選好の確立などのようなアクションを実行する。しかしながら、セットアップアプリケーションは、受信機/デコー

ダの設定変更のため、ユーザによりいつでも利用可能である。
・ザッピング（Ｚａｐｐｉｎｇ） ザッピングアプリケーション３１４６は、プログラムアップ、プログラムダウン及び数字キーを利用したチャンネルの変更に使用される。例えば、バナー（パイロット）アプリケーションを通じて他の形式のザッピングが利用されるとき、ザッピングアプリケーションは中断される。
・コールバック コールバックアプリケーション３１４８は、受信機/デコーダのメモリに格納されている様々なパラメータ値を抽出し、モデムバックチャンネル１０７０（図示せず）を介し、あるいは他の手段によりこれらの値を商業的な運営者に返すのに利用される。

【０１８５】

アプリケーションレイヤ３１００の他のアプリケーションは、プログラムガイドアプリケーション３１３２、ペイパービューアプリケーション３１３４、バナー（パイロット）アプリケーション３１３６、ホームバンキングアプリケーション３１３８、ソフトウェアダウンロードアプリケーション３１４０及びＰＶＲ（Ｐｅｒｓｏｎａｌ Ｖｉｄｅｏ Ｒｅｃｏｒｄｅｒ）アプリケーション３１５４（以下参照）を有する。

【０１８６】

上述のように、アプリケーションプログラミングインタフェース（ＡＰＩ）レイヤ３３００は、複数のパッケージを含む。これらは、例えば、バーチャルマシーンの基本的機能にアクセスするのに利用される基本システムパッケージ３３１０と、ＤＡＶＩＣパッケージ３３２０と、主要なソフトウェアベンダーに特有のソフトウェアアーキテクチャの機能へのアクセスに利用される独自パッケージ３３３０とを含む。

【０１８７】

より詳細に考察されると、バーチャルマシーン３５００は以下を含む。
・言語インタプリタ３５１０ 異なるインタプリタが読み込み対象のアプリケーションのタイプに従いインストールされうる。これらには、Ｊａｖａ（登録商標）インタプリタ３５１２、ＰａｎＴａｌｋインタプリタ３５１４、ＨＴＭＬインタプリタ３５１６、ＭＨＥＧ－５インタプリタ３５１８などが含まれる。
・サービス情報（ＳＩ）エンジン ＳＩエンジン３５４０は、共通のＤＶＢ（Ｄｉｇｉｔａｌ Ｖｉｄｅｏ Ｂｒｏａｄｃａｓｔｉｎｇ）あるいはＰＳＩＰ（Ｐｒｏｇｒａｍ Ｓｙｓｔｅｍ Ｉｎｏｆｍｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）テーブルをロード及びモニタし、これらをキャッシュに置く。ＳＩエンジン３５４０は、これらに含まれるデータを必要とするアプリケーションによるテーブルへのアクセスが可能にする。
・スケジューラ３５４２ 当該モジュールは、各自のイベントキューを有する各スレッドによる割り込み型（ｐｒｅ－ｅｍｐｔｉｖｅ）マルチスレッドスケジューリングを可能にする。
・メモリマネージャ３５４４ 当該モジュールは、メモリへのアクセスを管理する。これはまた、自動的に必要なときにメモリ内のデータを圧縮し、自動的にガーベッジを回収する。
・イベントマネージャ３５４６ 当該モジュールは、優先度に応じたイベントのトリガーを可能にする。これは、タイマやイベントグラビング（ｅｖｅｎｔ ｇｒａｂｂｉｎｇ）を管理し、アプリケーションによる互いのイベントの送信を可能にする。
・ダイナミックリンカ（Ｄｙｎａｍｉｃ Ｌｉｎｋｅｒ）３５４８ 当該モジュールは、本来のＪａｖａ（登録商標）関数から生じるアドレスの決定を可能にし、ＲＡＭにダウンロードされたＪａｖａ（登録商標）クラスからもともとのメソッドをロードし、ダウンロードされた本来のコードからのＲＯＭへのコールを決定する。
・グラフィックスシステム３５５０ 当該システムは、オブジェクト指向であり、最適化されている。それは、グラフィックウィンドウ及びオブジェクト管理と共に、複数言語のサポートによるベクトルフォントエンジンを有する。
・クラスマネージャ３５５２ 当該モジュールは、クラスをロードし、任意のクラス参照問題を解決する。

・ファイルシステム３５５４　当該モジュールは、複数のＲＯＭ、フラッシュ、ＲＡＭ及びＤＳＭＣＣ容量による階層ファイルシステムの管理のためコンパクト化及び最適化されている。フラッシュ完全性が任意の事態に対して保証される。
・セキュリティマネージャ３５５６　当該モジュールは、アプリケーションを認証し、セットトップボックスのセンシティブメモリ及び他の領域へのアプリケーションのアクセスを制御する。
・ダウンローダ（ｄｏｗｎｌｏａｄｅｒ）３５５８　当該モジュールは、常駐のファイルと同様にアクセスされるダウンロードファイルにより、遠隔ＤＳＭＣＣカルーセル（ｃａｒｏｕｓｅｌ）から、あるいはＮＦＳプロトコルを介した自動的データロード処理を利用する。メモリのクリーンアップ、圧縮及び認証処理がまた提供される。

【０１８８】
さらに、ＤＡＶＩＣリソース通知モデルは、クライアントリソースは効率的に管理されるようサポートされる。

【０１８９】
カーネル３６５０は、バーチャルマシーン３５００及びデバイスインタフェースレイヤ３７００（図示せず）上で実行される様々なプロセスを管理する。効率性及び信頼性のため、カーネルはオペレーティングシステムのためのＰＯＳＩＸ規格の関連する部分を実現する。

【０１９０】
カーネルの制御のもと、バーチャルマシーン（Ｊａｖａ（登録商標）及びＰａｎＴａｌｋアプリケーションを実行する）は、大容量記憶サーバ３８５０（図示せず）のようなオペレーティングしすてむの他の「サーバ」要素とは別に、自身のスレッドを実行する。アプリケーション３１２０がマルチスレッド環境を利用できるように、システムコールのパラメータとしてわたされるスレッドＩＤの要求のような対応する用意がＡＰＩレイヤ３３００においてなされる。

【０１９１】
複数のスレッドを用意することにより、より高い安定性が得られる。例えば、バーチャルマシーン３５００がある理由のため動作を停止する場合、デバイスへのアクセスを試みるアプリケーションによる長期でのクラッシュやブロッキングにより、ハードディスクサーバのようなシステムの他のスピードが重視される要素の継続的動作が可能となる。

【０１９２】
バーチャルマシーン３５００とカーネル３６５０と共に、ハードディスクビデオレコーダ（ＨＤＶＲ）モジュール３８５０が、ハードディスク２２１０の記録及び再生機能あるいは他の装着されている大容量記憶要素の処理のため提供される。サーバは、記録を処理する２つのスレッド３８５４と３８５６と、再生を処理する１つのスレッド３８５８と、大容量記憶要素とのインタフェースのためのファイルシステムライブラリ３８５２とを有する。

【０１９３】
ハードディスクビデオレコーダ（ＨＤＶＲ）３８５０のスレッド３８５４、３８５６及び３８５８の適当な１つにより、例えば、ユーザの「記録」ボタンの押下に応答して、パーソナルビデオレコーダ（ＰＶＲ）アプリケーション３１５４のようなクライアントからのコマンド（特定のプログラムの録画開始のためのコマンドのような）が受信される。

【０１９４】
次に、当該スレッドは録画あるいは再生対象のビットストリームを扱う受信機/デコーダの要素を設定及び同期化するため、サービス装置３７３６（図７に示される）とやり取りする。並行して、スレッドはまた、ハードディスク２２１０（図示せず）の適当な場所で記録または再生処理を調整するファイルシステムライブラリ３８５２とやり取りする。

【０１９５】
ファイルシステムライブラリ３８５２はその後、（ＦＩＦＯバッファを介し）送信すべきサブトランスポートストリーム（ＳＴＳ）と、当該ストリームをどのハードディスクに

格納すべきかを大容量記憶装置３７２８に通知するコマンドを大容量記憶装置３７２８（図７にも示される）に送信する。ハードディスクへのクラスタ割り当て及び一般的ファイル管理がファイルシステムライブラリ３８５２により実行され、大容量記憶装置自身はより下位レベルの処理に関するものである。

【０１９６】

上記サービス装置３７３６は、それが受信機/デコーダの物理的要素と関連していないという点で、装置間において一意的なものである。サービス装置３７３６は代わりに、様々なサブデバイスを協調させることの困難さから、受信機/デコーダのチューナー、逆多重化装置、再多重化装置及びハードディスク装置などの様々な装置を１つの「インスタンス」にグループ化するハイレベルインタフェースを提供する。

【０１９７】

図７を参照するに、図５の下半分に対応する受信機/デコーダ３０００のソフトウェアアーキテクチャ（デバイスインタフェースレイヤ３７００とシステムソフトウェアハードウェアレイヤ３９００から構成される）がより詳細に説明される。

【０１９８】

デバイスレイヤに備えられるさらなる装置として、条件付アクセス装置３７２０と、図４の２つの（または潜在的にはそれ以上の）チューナー２０１６と２０１８に対応するチューナー装置３７２４と、ビデオ装置３７３４と、Ｉ／Ｏポート装置３７２６と、上記のサービス装置３７３６及び大容量記憶装置３７２８があげられる。

【０１９９】

広い意味では、２つの異なる装置が共通の物理的ポートに接続されるように、
装置とは論理インタフェースを定義するものとみなされる。装置は装置間において通信するかもしれないし、すべての装置はまたカーネル３６５０の制御のもと動作する。

【０２００】

装置のサービスを利用する前に、プログラム（アプリケーション指示シーケンスのような）は「クライアント」として、すなわち、装置またはデバイスマネージャ３７１０への論理的アクセス方法として宣言される必要がある。マネージャは、装置へのアクセス合計と呼ばれるクライアント数をクライアントに与える。装置は複数のクライアントを有することができ、各装置のクライアント数は装置のタイプに応じて特定される。クライアントは、プロシージャ「Ｄｅｖｉｃｅ：Ｏｐｅｎ　Ｃｈａｎｎｅｌ」により装置に導入される。このプロシージャはクライアント数をクライアントに割り当てる。クライアントは、プロシージャ「Ｄｅｖｉｃｅ：Ｃｌｏｓｅ　Ｃｈａｎｎｎｅｌ」によりデバイスマネージャ３７１０のクライアントリストから抽出される。

【０２０１】

デバイスマネージャ３７１０により与えられる装置へのアクセスは、同期あるいは非同期であるかもしれない。同期アクセスでは、プロシージャ「Ｄｅｖｉｃｅ：Ｃａｌｌ」が利用される。これは、即座に利用可能となるデータや、所望の応答を待機しない機能へのアクセス手段である。非同期アクセスでは、プロシージャ「Ｄｅｖｉｃｅ：Ｉ／Ｏ」が利用される。これは、例えば、多重送信を検出するためチューナー周波数を走査したり、あるいはＭＰＥＧストリームからテーブルを再入手したりなど、応答の待機に関しないデータアクセス手段である。リクエストされた結果が利用可能であるとき、その到達を信号化するイベントがエンジンのキューに積まれる。さらなるプロシージャ「ＤＥｖｉｃｅ：Ｅｖｅｎｔ」は、予期せぬイベントを管理する手段を提供する。

【０２０２】

受信機/デコーダの第２実施例では、受信機/デコーダのアーキテクチャの下半分が図８に示されるレイヤにより置き換えられる。

【０２０３】

本実施例では、拡張されたデバイスレイヤインタフェース（ＥＤＬＩ）３６００がバーチャルマシーン３５００（図示せず）とデバイスインタフェースレイヤ３７００との間に備えられ、アブストラクションデバイスインタフェース３８００がデバイスインタフェー

スレイヤ３７００とシステムソフトウェア/ハードウェアレイヤ３９００との間に備えられる。それ以外で、同様の要素は同様の参照番号で示される。

【０２０４】

拡張されたデバイスレイヤインタフェース（ＥＤＬＩ）３６００は、バーチャルマシーン３５００とデバイスインタフェースレイヤ３７００との間の専用インタフェースを提供し、一般にマルチスレッドサポートをデバイスインタフェースレイヤに提供する。ＥＤＬＩの機能として、非同期イベントのミドルウェアの適切なスレッドへのルーティング（デバイスインタフェースレイヤはそれ自体マルチスレッド処理をサポートする必要はないため）と、スレッド間のメッセージのルーティングがあげられる。

【０２０５】

アブストラクションデバイスインタフェース３８００は、システムソフトウェア/ハードウェアレイヤ３９００においてデバイスインタフェースレイヤ３７００とデバイスドライバ３９１０との間のさらなるインタフェースを提供する。このようなインタフェースを提供することによって、大規模かつ複雑なデバイスレイヤ３７００はより大きな程度まで独立したハードウェアとすることができる。

[コンテンツ管理保護システム（ＣＭＰＳ）]

図９を参照するに、上述のコンテンツ管理保護システム（ＣＭＰＳ）２３００は、放送センター１０００と受信機/デコーダ２０００との間に分散されている。ＣＭＰＳの受信機/デコーダ要素は、物理的スマートカード（関連するスマートカード読取器を有する）とバーチャルスマートカードの形態で、共にバーチャルスマートカードマネージャ（より詳細に後述されるような）の制御のもと与えられるが、この好適な実施例の変形では、ＣＭＰＳの受信機/デコーダ要素は単にソフトウェア的あるいはハードウェア的に、さらにその両方の組み合わせにより実現される。ＣＭＰＳは、認証されたユーザのみが所定の利用規則に従ってコンテンツの記録及び再生を実行することができるということを保証することができる。ＣＭＰＳはさらに、コピー制御や時間シフト制約のような、コンテンツ所有者及び/または販売者により定義された他の規則が添付されるということを保証するかもしれない。

【０２０６】

コンテンツ管理保護システムの重要部分は、与えられたコンテンツ（プログラムまたは送信のような）に関するコンテンツ管理情報を含み、そのようなプログラムまたは送信の前に送信されると特別な利用規則メッセージ（ＵＲＭ）である。本質的には、利用規則メッセージは、コンテンツの再生に関する利用制約を課すものであり、プログラム内の別々の「チャプタ（ｃｈａｐｔｅｒ）」のようなコンテンツの特定部分のみ、あるいはコンテンツ全体に対するものである。典型的な利用規則として、時間シフト処理、早送り処理、記録したものが再生可能である回数及び利用可能な再生モードに関する制約があげられる。以下で後述されるより詳細な他の重要な特徴は、与えられたプログラムに関するＵＲＭが対応するコンテンツまたは条件付アクセス情報（異なる場所から及び異なる時間に）とは独立に送信されるかもしれない。

【０２０７】

第２のメッセージクラスであるＣＭＰＳエンタイトルメント管理メッセージ（ＣＭＰＳ　ＥＭＭまたはＣＭＰ＿ＥＭＭ）がアクセス権利をＣＭＰＳに送信するため与えられる。ＣＭＰＳ　ＥＭＭは、他で参照される条件付アクセスエンタイトルメント管理メッセージ（ＥＭＭまたはＣＡＳ＿ＥＭＭ）と等価であるが、送信されたアクセス権利は「従来の」ＥＭＭと同様に、放送プログラムデータよりもプログラムデータのローカルな格納に関する。

【０２０８】

図９に示される好適な実施例では、多重化スクランブル化装置１０３０が、ＣＭＰＳ　ＥＭＭ５６４１とＵＲＭ５６１２を受信し、これらをスクランブル解除されたコンテンツ（プログラムデータ）８１０を有するビットストリームにより多重化し、得られたスクランブル化されたコンテンツ８００を放送システム６００を介し配信する。その後、受信機

/デコーダはスクランブル化されたコンテンツ８００を受信し、ＣＭＰＳ　ＥＭＭ及びＵＲＭをＣＭＰＳ２３００と条件付悪背うシステム５０００に必要に応じて削除及びわたす。しかしながら、本好適な実施例では、ＣＭＰＳ　ＥＭＭとＵＲＭはＣＭＰＳにより内部的に処理される。

【０２０９】

ＵＲＭは、本好適な実施例の変形ではＥＣＭ使用鍵と同一のＵＲＭ使用鍵により暗号化される。ＵＲＭ使用鍵と等価なものが、ＵＲＭの解読のため受信機/デコーダＣＭＰＳスマートカード（図示せず）に維持される。さらなる変形では、ＵＲＭは暗号化されず、データの完全さを保証するため暗号的に署名される。他の実施例では、ＵＲＭに含まれる値が潜在的には他の情報と共に暗号鍵を導出するためのシード値として使われる。ＣＭＰ＿ＥＭＭのような暗号化されたユニットがそのような鍵（またはその派生物）により暗号化可能となり、このことはＵＲＭにより改ざんが、例えば、ＣＭＰ＿ＥＭＭの解読を防ぐことを意味する。

【０２１０】

上述ように、受信機/デコーダを利用したユーザによる記録及び/または再生を可能にする使用権利は、ＣＭＰＳエンタイトルメント管理メッセージ（ＣＭＰＳ　ＥＭＭまたはＣＭＰ＿ＥＭＭ）の形式で与えられる。すなわち、ＣＭＰＳ　ＥＭＭは、従来のＥＭＭと同様の構成を有することが可能であるが、一般にはより鍵志向な（ｋｅｙ－ｏｒｉｅｎｔｅｄ）なもの、すなわち、ＣＭＰ＿ＥＭＭが典型的にはコンテンツやサービスに関する鍵を埋め込むものである。記録されたコンテンツを再生する権利は、一般にＵＲＭに符号化された商業的な規則に依存するものであり、既に取得されている使用権利にもまた依存する。そのような権利は、例えば、１回限りの支払い（衝動買い）や視聴契約に対する対価として与えられる。様々なレベルのアクセス権がまた任意のコンテンツに関して与えられる。これによりユーザは、例えば、コンテンツを一度だけ再生する権利に対する第１料金を支払うことができるし、あるいは制限なしの再生に対する第２のより高額な料金を支払うことが可能となる。ＣＭＰ＿ＥＭＭは典型的には、受信機/デコーダＣＭＰＳスマートカードに格納されるが、他に例えば、ハードディスクの安全に暗号化された領域に格納されてもよい。

【０２１１】

好適な実施例では、記録したものを再生する権利は、記録後（「ペイパービュー」モデル）あるいは記録前（「視聴契約」モデル）取得されうる。前者の場合、コンテンツの記録後、ユーザは条件付アクセスシステムにコンテンツを再生する権利の取得を所望しているということを指示する。この指示が視聴契約管理システムにより認証される場合、適切なＣＭＰＳエンタイトルメント管理メッセージ（「ＣＭＰ＿ＥＭＭ」が双方向リンクを介して受信機/デコーダに送信される。

【０２１２】

ＣＭＰＳシステムにより提供される多くの効果の１つは、プログラムを記録及び再生するアクセス権利は、従来システムと同様に、プログラムを単に視聴するアクセス権利とは全く独立なものであるということである。従って、ユーザは、プログラムの視聴が可能であるが、録画及び再生は不可であるという状況を有することが可能である。その逆に、ユーザは、プログラムの視聴は不可であるが、プログラムの記録は可能であり、必要な権利の取得及び再生は可能である。

【０２１３】

図１０に示されるインターネット配信モデルに特に典型的な本好適な実施例の変形では、スクランブル化されたコンテンツ（「ＣＯＮＴＥＮＴ＊」）、ＣＭＰＳ　ＥＭＭ（「ＣＭＰ＿ＥＭＭ」）及びＵＲＭ（「ＵＲＭ」）はすべて、第１パーティ７００、第２パーティ７０２及び第３パーティ７０４から受信機/デコーダ２０００に独立に送信される。例えば、第１、第２及び第３パーティはマルチアクセスポータル（ＭＡＰ）であり、スクランブル化されたコンテンツ８００、ＣＭＰＳ　ＥＭＭ５６１４及びＵＲＭ５６１２はそれぞれ、例えば、配信ストリーム、他のブロードバンド接続またはダイヤルアップ接続を介

し送信されるようにしてもよい。典型的には、プログラム提供者（第２パーティ１２０２）は、プログラムコンテンツ（「ＣＯＮＴＥＮＴ」）を多重化/スクランブル化装置に送信し、スクランブル化されたコンテンツ１３００（ＣＯＮＴＥＮＴ＊）が保証され、通常の方法により受信機/デコーダ２０００に送信される。上記及び好適な実施例における情報配信の独立性は、コンテンツ配信、商業的提供の提示及びしよう権利送信の様々な役割が異なる役者により演じられるという事実を反映している。

【０２１４】

図１１及び図１２を参照するに、ＣＭＰＳ２３００を利用したコンテンツの記録及び再生を行う受信機/デコーダ２０００での実現形態が説明される。

【０２１５】

記録モードでのＣＭＰＳの構成を示す図１１では、エクスポートクライアントライブラリ（ＡＰＩ）、メッセージスーパーバイザ及びリソースマネージャから構成されるＣＭＰＳサーバモジュール（コア）２２００が、ＣＭＰＳリンククライアントライブラリ３５６２、バーチャルスマートカードマネージャ（ＶＳＣマネージャ）２３５０、ＭＬＯＡＤ装置３７３８、ＬＣＡＲＤ装置３７４０及びＨＤＶＲモジュール３８５０に加えて示されている。デバイスレイヤインタフェース３７００がまた示される。

【０２１６】

ＣＭＰＳコア２２００が受信機/デコーダミドルウェアに備えられ、リンククライアントライブラリ３５６２を介しＨＤＶＲモジュール３８５０とのインタフェースを提供する。ＣＭＰＳコア２２００はまた、ＭＬＯＡＤ装置３７３８、ＬＣＡＲＤ装置３７４０（条件付アクセススマートカードを収容する）、及びＲＣＡＲＤ装置３４４２（図示されず、選択的なＣＭＰＳスマートカードを収容する）とのインタフェースを提供する。

【０２１７】

詳細に後述される記録モードでのＣＭＰＳシステムの動作において、プログラムデータストリームで受信されたＥＣＭ５６０２は、ＭＬＯＡＤ装置により分離され、その後ＣＭＰＳリソースマネージャにより条件付アクセススマートカードにルーティングされる。その後、ＥＣＭから導出された制御ワード５６００は、適切な場合には（好ましくは、プログラムデータストリームで受信されるが、他のルートを介して受信されてもよい）、対応するＵＲＭとＣＭＰＳ　ＥＭＭに加えて、バーチャルスマートカードにルーティングされる。

【０２１８】

バーチャルスマートカードマネージャ２３５０は、その後必要に応じて実際のまたはバーチャル名ＣＭＰＳスマートカード２４００（図示せず）を利用して、制御ワードや他のデータのＣＭＭ５６１０への変換を管理し、さらなる処理のため、ＣＭＭをＣＭＰＳコアに転送する。好適な実施例では、安全な認証されたチャンネル（ＳＡＣ）が、この制御ワードと他のセンシティブなデータの送信のため様々なソフトウェア及びハードウェア要素間で利用される。バーチャルスマートカードマネージャ２３５０とバーチャルスマートカード２４００は詳細に後述される。

【０２１９】

その後、ＣＭＭは、対応するコンテンツデータと共にディスクに格納されるように、ＨＤＶＲコントローラ３３５０にわたされる。ＥＣＭが解読不能であるイベントでは（典型的には、ユーザが適切な権利を有しないことに起因する）、アクセス権が利用可能になる以降の時点でＥＣＭの制御ワードでの将来的な変換を可能にするよう、ＥＣＭが制御ワードの代わりにＣＭＭ構成に格納される。ＥＣＭのＣＭＭへの上記カプセル化はまた、より詳細に後述される。

【０２２０】

本好適な実施例の変形では、コンテンツはスクランブル解除され、記録段階で再スクランブル化される。この場合、新たなコンテンツ鍵（ローカル制御ワードに等しい）が生成及びＣＭＭに格納される。さらなる変形では、コンテンツは、さらなるスクランブル化/暗号鍵を含むＣＭＭの第２レベルを要する、スーパースクランブル処理される（すなわち

、典型的にはより強力な暗号化方法によりさらにスクランブル化される）。この場合、トリプルＤＥＳは、適切に強力化された暗号化方法として、１６８ビットの鍵の長さにより利用可能となる。

【０２２１】

再生モードでのＣＭＰＳの構成を示す図１２では、エキスポートクライアントライブラリ、メッセージスーパーバイザ及びリソースマネージャから構成されるＣＭＰＳコア２２００が、ＣＭＰＳリンククライアントライブラリ３５６２と、バーチャルスマートカードマネージャ（ＶＳＣマネージャ）２３５０と、ＨＤＶＲモジュール３８５０とを加えて示される。

【０２２２】

以下で詳述される再生モードでのＣＭＰＳシステムの動作では、ＨＤＶＲモジュール３８５０により転送されるＣＭＭが、所望の制御ワードを生成するためバーチャルスマートカードマネージャ２３５０の制御のもと復号化され、その後、ＨＤＶＲモジュール３８５０に転送される。上述のように、ＣＭＭが復号化された制御ワードよりむしろカプセル化されたＥＣＭを含む場合、ＣＭＰＳは再びＥＣＭの解読を試み、成功した場合にはＣＭＭを適当な制御ワードにより埋め込む。

【０２２３】

図１３に示されるように、コンテンツをディスクに記録するプロセスがより機能的な視点から説明される。図１３において、各ＥＣＭ５６０２は条件付アクセススマートカードの解読段階５５５０にわたされ、グローバルな使用鍵K_G ５６０６を使用して解読される。その後、解読された制御ワード５６００はＣＭＰＳスマートカードの暗号化段階２２０２にわたされ、対応するＵＲＭ５６１２及びＣＭＰＳ　ＥＭＭ５６１４によりコンテンツ管理メッセージ（ＣＭＭ）に合成され、その後、ローカル使用鍵K_L ５６０８を利用して全体として再暗号化される。変更されていないスクランブル処理されたコンテンツと得られた複数のＣＭＭは、ハードディスク２１００の１つのファイル内のそれぞれコンテンツ部分２１１０と管理データ部分２１１２に格納される。本好適な実施例の変形では、別々のファイルが各部分の格納に利用される。

【０２２４】

図１４に再び示されるディスクからコンテンツを再生する逆のプロセスでは、スクランブル化されたコンテンツ１３００が、ハードディスク２１００のファイルのコンテンツ部分２１１０から読み出され、スクランブル解除装置２０１０に供給される。並行して、ＣＭＭが別の管理データ部分２１１２から読み出され、ＣＭＰＳスマートカードの暗号化段階２２０４に供給される。ＣＭＭはローカル使用鍵５６０８により解読され、ＵＲＭ５６１２、ＣＭＰＳ　ＥＭＭ５６１４及び制御ワード５６００に分割される。ＣＭＰＳモジュールがプログラムを視聴する権利をユーザが保持していると決定すると（ＵＲＭおよびＣＭＰＳ　ＥＭＭに基づき）、制御ワード５６００はコンテンツのスクランブル解除を可能にするため適当な時点でスクランブル解除装置２０１０に送信される。

【０２２５】

さらに、本システムは、可能な限りのセキュリティとスピードを保持しながら、すべてのセッションに必要なマスタ及び従属暗号及び/または認証鍵のすべてを生成及び格納する手段を提供する。これらの鍵の生成と格納の両方に関するプロセスがより詳細に以下で説明される。

【０２２６】

ＨＤＶＲ３８５０を利用した記録プロセスがより詳細に説明される。

【０２２７】

プログラムを記録する時点で、ＨＤＶＲは、管理データ（例えば、ｈｄｖｒ＿ｆｉｌｅ．ｍａｎａｇｅｍｅｎｔ＿ｄａｔａ）及びコンテンツ自身（例えば、ｈｄｖｒ＿ｆｉｌｅ．ｃｏｎｔｅｎｔ＿ｄａｔａ）という主として２つの部分からなる構成を有するファイルを生成する。

【０２２８】

ファイルの第１部分は、（特に）ＣＭＰＳにより生成及び処理されるローカルメッセージ（コンテンツ管理メッセージ－ＣＭＭ）に対応し、コンテンツの使用規則をそれに関連するスクランブル解除された鍵（言い換えると、制御ワード）と共に含んでいる。第１部分はまた、ビットストリームの時間オフセットをファイルのデータオフセットにマッピングするインデックスからなるインデックステーブルを有する。

【０２２９】

第２部分は、与えられたプログラムの様々な要素（映像、音声、サブタイトルなど）に対応する部分トランスポートストリーム（ｐＴＳ）から構成され、配信において共通のスクランブル化ケー式ＤＶＢ＿ＣＳに従いスクランブル化されたままである。本好適な実施例の変形では、管理データ及びコンテンツは少なくとも２つの別々のファイルに格納される。さらなる変形では、コンテンツはスクランブル解除され、再スクランブル化されるか（好ましくは、与えられた受信機/デコーダに一意的なローカル鍵により）、あるいはさらなるより安全な暗号化レベルでスーパースクランブル化される（適当な長さの鍵長によるトリプルＤＥＳのような）。

【０２３０】

ＣＭＰＳは、各暗号化期間においてＣＭＭを生成するため、それ自身の管理及び制御メッセージによる同期化を担う。このＣＭＭは、その後、ｈｄｖｒ＿ｆｉｌｅ．ｍａｎａｇｅｍｅｎｔ＿ｄａｔａ部分への挿入のため、ＨＤＶＲに送信される。ＣＭＰＳはまた、チャプタのスタートポイントや時間シフトモードでの記録の認証された最大範囲のような、コンテンツ（ｈｄｖｒ＿ｄａｔａ）の管理に関するある情報量を通信する。

【０２３１】

図１５において、これが概略的に示される。ＵＲＭ、ＣＭＰ＿ＥＭＭ及びＣＷがＣＭＰＳに入力される。ｈｄｖｒ＿ｄａｔａがＣＭＰＳ３００からＨＤＶＲ３５０にわたされる。

【０２３２】

上述のように、ファイルのｈｄｖｒ＿ｆｉｌｅ．ｍａｎａｇｅｍｅｎｔ＿ｄａｔａはまた、ビットストリームの時間オフセットをファイルのデータオフセットにマッピングするインデックスからなるインデックステーブルを有する。インデックステーブルには、ＨＤＶＲにより自動的に挿入されるＨＤＶＲインデックスと、ユーザのコマンドに応じて挿入されるユーザインデックスの２つのタイプのインデックスが含まれる。

【０２３３】

ＨＤＶＲインデックスは、ビットストリームの周期的な時間オフセットに対応するインターバルでＨＤＶＲにより位置決めされ、記録されたファイルの再生エントリポイントとして利用される。本好適な実施例では、ＨＤＶＲインデックスは、プログラムの記録中自動的にＨＤＶＲにより生成される。

【０２３４】

ユーザインデックスはまた再生エントリポイントであり、プログラムの記録時、または記録されたプログラムの再生中にユーザにより設定される。

【０２３５】

インデックステーブルは、各ＨＤＶＲインデックス及びユーザインデックスを適当なＣＭＭにマッピングするポインタを有し、ＨＤＶＲ及びユーザインデックスによりインデックスされたポイントでの格納されているビットストリームの解読を可能にする。

【０２３６】

例えば、ファイルまたは対応するビットストリームにおけるポイントの検索、早送り、巻き戻し及びスキップのような「トリックモード」の処理のような、記録されたコンテンツの処理は、インデックステーブルに格納されたＨＤＶＲ及びユーザインデックスを利用する。

[ＨＤＶＲを利用した再生]

記録されたコンテンツの利用時点で、記録されたＣＭＭに与えられた使用規則を加入者により取得され、ＣＭＰＳスマートカードあるいは受信機/デコーダ内の安全な場所に格

納された権利を比較することにより、ＣＭＰＳは関連する権利の有効性を保証する（バーチャルスマートカードの制御のもと）。好ましくは、この機構は、リクエストに応じて無効なアクションを記述した可能なエラーメッセージ（状態）とは別に、ＨＤＶＲアプリケーションに対し明確さを保つ。さらに、好ましくは、あるメッセージ、特に遠隔制御に関する無効なアクション（例えば、「トリック」モードの早送りがシーケンスにおいて認証されていないとき、画面に警告が表示される）は、マンマシーンインタフェースアプリケーションを利用してユーザに中継される。

【０２３７】

コンテンツ内のナビゲーションを容易にするため、ＣＭＰＳスマートカードに固有な処理時間による制限なく、スクランブル解除装置を新たなＣＷによりリロードすることができる。このため、ＨＤＶＲアプリケーションは、ＣＭＭが有するＣＷの効果的な利用の前に、複数のＣＭＭの前処理をサーバに依頼することができる。これを実行するため、ＨＤＶＲは、現在位置の一方の側で、チャプタ、インデックス及び暗号化期間に関するＣＭＭの異なるバッファを生成する。ＣＭＰＳのリクエストで、ＨＤＶＲはさらに、映像ファイルのｈｄｖｒ＿ｆｉｌｅ．ｍａｎａｇｅｍｅｎｔ＿ｄａｔａ部分に再挿入される更新されたＣＭＭを抽出する。

【０２３８】

ＨＤＶＲにより要求される主要なデータは、コンテンツの利用（チャプタの開始ラベル、ナビゲーション制約、最大記録範囲など）と共に、ＣＭＰＳサーバにおける処理のため送信されるＣＭＭバッファの状態を比較して、ナビゲーション及び使用制約情報から構成される。ある管理情報（ｈｄｖｒ＿ｄａｔａ）は、情報がＵＲＭにおいて明確に伝えられる場合に、コンテンツの記録（典型的には、チャプタの開始ラベル）時点でＵＲＭから取得するようにしてもよい。映像ファイルのｈｄｖｒ＿ｆｉｌｅ＿ｍａｎａｇｅｍｅｎｔ＿ｄａｔａ部分のオーバーロードを避けるため、利用制約（ナビゲーション、チャプタのモーラルコードなど）についての情報のような他のデータが、ＣＭＭを介しコンテンツの再生時にＣＭＰＳにより通信されるようにしてもよい。

【０２３９】

メッセージ交換、及び特に関連するデータ構造が説明される。

【０２４０】

ＨＤＶＲとＣＭＰＳとの間での交換プロトコルで生じるデータ量が特定される。交換プロトコルは、主として、ＣＭＭを送るＣＭＭ＿ｍｅｓｓａｇｅメッセージと、ナビゲーション情報とコンテンツの利用に関する制約とに関する。その構造は以下のとおりである。

【０２４１】

【表１】

ﾃﾞｰﾀ構造	記述
struct CMM_message {	
struct CMM,	格納対象のすべての CMM
struct CMM.navigation,	ﾅﾋﾞｹﾞｰｼｮﾝに関するﾃﾞｰﾀ
struct CMM.hdvr_rules	制約に関するﾃﾞｰﾀ
}	

次に、ＣＭＭは以下に詳細に示される異なる構成を有する。

【０２４２】

ＣＭＭ＿ｍｅｓｓａｇｅは、特に、コンテンツ内のナビゲーションに関する情報から構成される。ナビゲーション及び制約データが暗号化されるＣＭＭとは反対に、ＨＤＶＲによる直接的な解釈のため、これらのデータはＣＭＭ＿ｍｅｓｓａｇｅにおいて明確に与え

られる。ＣＭＭの一般的な構成が以下に与えられる（その符号化及び署名とは独立に）。

【０２４３】

【表２】

ﾃﾞｰﾀ構造	記述
struct CMM{	
struct CMM.navigation,	ﾅﾋﾞｹﾞｰｼｮﾝに関するﾃﾞｰﾀ
struct CMM.hdvr_rules,	制約に関するﾃﾞｰﾀ
struct CMM.content_key,	ｺﾝﾃﾝﾂ鍵(符号化)
struct CMM.private_data	ﾌﾟﾗｲﾍﾞｰﾄﾃﾞｰﾀ(使用規則)
}	

コンテンツ内のナビゲーションデータは見出しを参照し、以下に与えられる。

【０２４４】

【表３】

ﾃﾞｰﾀ構造	記述
struct CMM.navigation{	
total_chapter_number,	ｺﾝﾃﾝﾂのﾁｬﾌﾟﾀ総数
chapter_index	ﾁｬﾌﾟﾀ番号
}	

無効なアクション及び時間シフト制約に関するコンテンツ利用制限についてのデータが以下で与えられる。

【０２４５】

【表４】

ﾃﾞｰﾀ構造	記述
struct CMM.hdvr_rules{	
trick_mode_bitmap,	無効ﾋﾞﾃﾞｵﾚｺｰﾀﾞｱｸｼｮﾝ
time_shifting_duration,	最大記録長
content_rating	ﾓｰﾗﾙﾚﾍﾞﾙ(現在ﾁｬﾌﾟﾀの)
}	

[ＣＭＰＳの内部構造]

図１６を参照して、ＣＭＰＳがより詳細に説明される。図１１及び図１２に示されるように、ＣＭＰＳは、ＣＭＰＳコア２２００とリンククライアントライブラリ３５６２から構成される。ＣＭＰＳコア２０００自身は、ＣＭＰＳメッセージマネージャスレッド２３１０とＣＭＰＳデバイスマネージャスレッド２３２０から構成される。

【０２４６】

概略すると、ＣＭＰＳメッセージマネージャスレッドは、受信機/デコーダ上で実行するアプリケーション（例えば、ＨＤＶＲ３８５０）に対するＣＭＰＳの機能へのインタフ

ェースを提供し、ＣＭＰＳデバイスマネージャスレッド２３２０は、様々な関連する装置（ＭＬＯＡＤ装置、ＣＷ装置、ＬＣＡＲＤ装置など）とのインタフェースを提供する。

【０２４７】

リンククライアントライブラリ３５６２は、ＣＭＰＳの初期化に要する機能を含む。特に、リンククライアントライブラリは、ＣＭＰＳメッセージマネージャ２３１０とＣＭＰＳデバイスマネージャ２３２０のスレッドの生成のための機能を提供する。

【０２４８】

ＣＭＰＳメッセージマネージャスレッド２３１０は、エクスポートクライアントライブラリ２３４０とメッセージスーパーバイザも銃る２３３０を有する。

【０２４９】

エクスポートクライアントライブラリ２３４０は、ＣＭＰＳによりサポートされているアプリケーションメッセージを特定し、メッセージスーパーバイザモジュール２３３０はそのようなメッセージを受信し、それらの有効性を検証する（有効でない場合にはエラーを返す）。メッセージマネージャスレッド２３１０は、同期及び非同期両方のメッセージ処理をサポートする。

【０２５０】

デバイスマネージャスレッドの機能がより詳細に説明される。

【０２５１】

前述のように、ＣＭＰＳデバイスマネージャスレッド２３２０は、メッセージルータモジュール２３６０と、リソースマネージャ２３７０と、バーチャルスマートカード（ＶＳＣ）２４００と、バーチャルスマートカードマネージャ（ＶＳＣマネージャ）２３５０とを有する。バーチャルスマートカードとバーチャルスマートカードマネージャはより詳細に後述される。

【０２５２】

メッセージルータモジュール２３６０は、デバイスマネージャスレッド２３２０内のメッセージのキュー処理（必要に応じて）とルーティング処理を扱う。メッセージマネージャスレッド２３１０のメッセージスーパーバイザ２３３０が有効なアプリケーションメッセージを受信すると、対応する非同期アプリケーションメッセージをメッセージルータ２３６０に送信する。その後、メッセージルータ２３６０は、受信したアプリケーションメッセージが有効であると確認し（有効でない場合には、エラーを発生させる）、さらなる処理のためメッセージをリソースマネージャ２３７０にわたす。そのようなアプリケーションメッセージがリソースマネージャ２３７０により処理されると、応答メッセージがメッセージルータ２３６０とメッセージマネージャスレッド２３１０を介し適切なクライアントにわたされる。

【０２５３】

メッセージマネージャ２３１０とデバイスマネージャ２３２０のスレッド間の通信、及びリソースマネージャ２３７０と装置間の通信が、上述のＥＤＬＩ３６００を介し有効とされる。

【０２５４】

上述のように、リソースマネージャ２３７０は以下を含む様々な装置と通信する。

・ＭＬＯＡＤ装置３７３８は、復号化されたＭＰＥＧストリームから関連する条件付アクセスデータ（ＥＣＭ、ＥＭＭなど）を抽出するのに利用される。

・ＣＡ装置３７２０は、ＥＣＭマネージャを構成し（視聴契約モデルでの記録の場合）、必要に応じて、関連テーブルのＰＩＤの変更に利用される（そのような関連テーブルは、プログラムを構成する様々な要素とそれら関連するＥＣＭのＰＩＤとの対応を提供する）。

・ＣＷ装置３７６０は、制御ワードのスクランブル解除装置への挿入に利用される。

・ＬＣＡＲＤ装置３７４０は、条件付アクセススマートカードとの通信に利用される。

[セッション管理]

ＣＭＰＳデバイスマネージャスレッド２３２０とＣＭＰＳ（ＨＤＶＲのような）のクラ

イアントとの間の通信がセッションを利用して実現される。ＣＭＰＳデバイスマネージャとクライアントとの間では、レコーダとプレーヤーという２つのタイプのセッションが提供される。以下で詳細に示されるように、適切なメッセージの交換に応答して、ＣＭＰＳデバイスマネージャスレッド２３２０により新しいセッションが生成される。

【０２５５】

コンテンツの記録がレコーダセッションではカプセル化され、記録されたコンテンツの再セガプレーヤーセッションではカプセル化される。前述のように、図１１はレコーダセッションにおける典型的なデータフローを概略的に示し、図１２はプレーヤーセッションの典型的なデータフローを概略的に示している。任意の時点において、ＣＭＰＳは、本好適な実施例の変形ではプレーヤー及びレコーダ両方のタイプのさらなるセッションが関連するハードウェアの考察に従い提供されるが、１つのプレーヤーセッションと２つのレコーダセッションを扱うことができる。

【０２５６】

図１７は、新たな記録セッションの生成及び管理を示す。この図では、ステップ７００２から７０２６は以下の説明で示されるように、ＣＭＰＳシステムの要素と他のとの間で交換されるメッセージに対応する。

【０２５７】

ステップ７００２において、クライアントは、記録セッションをオープンするリクエストを送信し、その後、デバイスマネージャスレッドにより正式にオープンされる。ステップ７００４において、ＣＭＰＳメッセージマネージャにより一意的なセッション識別子（「ＳｅｓｓｉｏｎＩＤ」）を含む適当な承認が返される。このセッションに関するすべての以降の通信には、このセッション識別子が含まれる。

【０２５８】

ステップ７００６において、クライアントは、記録セッション内の記録シーケンスをオープンするためのリクエストをＣＭＰＳメッセージマネージャに送信する。ステップ７００８において、ＣＭＰＳメッセージマネージャは、ＣＭＰＳデバイスマネージャからファイル識別子（「ファイルＩＤ」）をリクエストする。その後、ＣＭＰＳデバイスマネージャは、ステップ７０１０により示されるように、ＶＳＣマネージャにおいて記録セッションを開始する。ステップ７０１２において、ＣＭＰＳデバイスマネージャは、ファイルＩＤを取得するためのリクエストをＣＭＰＳメッセージマネージャに対して承認する。以降、ステップ７０１４において、記録シーケンスがオープンされたという承認がＣＭＰＳメッセージマネージャからクライアントに送信される。

【０２５９】

ステップ７０１６において、クライアントは、ＣＭＰＳメッセージマネージャにバーチャルマシーンからＥＣＭに関して記録されたプログラムのＰＭＴテーブルの一部を取得させる。ステップ７０１８において、クライアントはこの実行が成功したということを確認する。

【０２６０】

ステップ７０２０において、実際のコンテンツの記録を開始するリクエストがクライアントにより送信される。その後、ＣＭＰＳメッセージマネージャは対応するリクエストをＣＭＰＳデバイスマネージャに送信する（ステップ７０２２）。ステップ７０２４において、後者は前者に対するこのリクエストを承認し、ステップ７０２６においてＣＭＰＳメッセージマネージャはクライアントによるリクエストを承認する。

【０２６１】

その後、正式な記録処理が開始され、正式な記録処理が終了するまで、さらなるメッセージが受信機/デコーダのＣＭＰＳ、ＨＤＶＲ及び他のシステムとの間で繰り返し送信される。この記録処理の「ループ」は、図１８を参照して以下で説明される。このループの終了に続くさらなるステップが、図１７を参照してまず説明される。

【０２６２】

記録処理中の任意の時点において、クライアントは正式な記録処理終了するリクエスト

をＣＭＰＳメッセージマネージャに送信するかもしれない（ステップ７０２８）。ステップ７０３０において、ＣＭＰＳメッセージマネージャは、記録処理が終了されるべきであるということをＣＭＰＳデバイスマネージャに通知し、ステップ７０３２において、ＣＭＰＳデバイスマネージャは当該記録セッションがクローズされるべきであるということをＶＳＣマネージャに通知する。ステップ７０３４において、ＣＭＰＳデバイスマネージャは、記録処理を終了させるためのリクエストの実行が成功したということをＣＭＰＳメッセージマネージャに確認させる。ステップ７０３６において、このことはＣＭＰＳメッセージマネージャによりクライアントに通知される。

【０２６３】

ステップ７０３８において、クライアントはＣＭＰＳメッセージマネージャに記録シーケンスをクローズするよう要求し、ステップ７０４０において、後者はこれが実行されたことを前者に確認させる。

【０２６４】

最後に、ステップ７０４２において、クライアントは、ＣＭＰＳメッセージマネージャに記録セッションをクローズするよう要求し、ステップ７０４４において、ＣＭＰＳメッセージマネージャはこれが実行されたことをクライアントに確認させる。

【０２６５】

図１８を参照するに、正式な記録処理が説明される。特に、ステップ７１０２、７１０４及び７１０６は記録処理の「ループ」の核心を示している。ステップ７１０２において、ＭＬＯＡＤ装置により抽出される次のＥＣＭが、ＥＤＬＩによりデバイスマネージャスレッド２３２０のリソースマネージャに送信される。その後、リソースマネージャはＥＣＭをＬＣＡＲＤ装置（条件付アクセススマートカードへのアクセスを提供する）に送信し、それに対してＬＣＡＲＤ装置から符号化された制御ワードを受信する（再び仲介としてＥＤＬＩを利用して）。ステップ７１０４において、このように得られた制御ワードは、必要に応じて、対応するコンテンツ（以下で説明されるＣＭＭの生成と共に）のライブでのスクランブル解除を可能にするため、ミドルウェアに（再びＥＤＬＩを介し）転送される。ステップ７１０６において、制御ワードは、必要に応じて、他の記録処理セッションのためのＣＭＭの生成を可能にするため、ＶＳＣマネージャに転送される。

【０２６６】

ステップ７１０８において、クライアントは、現在の記録セッションのための記録処理を開始するリクエストをＣＭＰＳメッセージマネージャに送信する。ステップ７１１０において、対応するリクエストがＣＭＰＳメッセージマネージャからＣＭＰＳデバイスマネージャに送信される。ステップ７１１２において、ＣＭＰＳデバイスマネージャは、ＣＭＰＳデバイスマネージャに対するリクエストを承認し、ステップ７１１４において、記録処理を開始するためクライアントによりなされたリクエストを承認し、記録処理の開始を確認する。ステップ７１１６と７１１８は、以前のように、ＭＬＯＡＤ装置からの次のＥＣＭの受信（ステップ７１１６）と、条件付アクセススマートカード（図示せず）によるＥＣＭの復号化と、他の関心を有するパーティへの制御ワードのリターン（ステップ７１１８）とに関する。ステップ７１２０において、ＣＭＰＳデバイスマネージャは、新しいＥＣＭセクションがＥＤＬＩから受信されたということをＣＭＰＳメッセージマネージャに通知する。ステップ７１２２において、これがＣＭＰＳメッセージマネージャによりクライアントに通知される。

【０２６７】

ステップ７１２４において、クライアントは、この新しいＣＭＭに対するリクエストをＣＭＰＳメッセージマネージャに送信する。ステップ７１２６において、ＣＭＰＳメッセージマネージャはこのリクエストをＣＭＰＳデバイスマネージャに送信する。以降、ステップ７１２８において、ＣＭＭを生成する（制御ワードと当該コマンドを有するデバイスマネージャスレッド２３２０のリソースマネージャにより供給される他の関連する情報）コマンドがＶＳＣマネージャに送信され、ＣＭＭがＶＳＣマネージャ（図示せず）によりデバイスマネージャに返される。ステップ７１３０において、ＣＭＰＳデバイスマネージ

ャは、ＣＭＭが取得されたということをＣＭＰＳメッセージマネージャに承認し、ステップ７１３２において、このことがクライアントに確認される。

【０２６８】

プレーヤーセッションでのメッセージの交換は、当該プレーヤーセッションをオープンするための一連の初期メッセージと、ＣＭＭのＣＭＰＳへの送信を処理するためのメイン「ループ」メッセージ（制御ワードは上述のようなバーチャルスマートカードにより直接設定される）と、セッションをクローズするためのメッセージの最終的交換とによる、上述のメッセージと同一の構成に広く従う。従って、プレーヤーセッションのメッセージのさらなる説明はここではなされない。

[バーチャルスマートカード]

前述のバーチャルスマートカード（ＶＳＣ）２４００は、ＲＣＡＲＤ装置３４４２に挿入可能なＣＭＰＳスマートカードの機能のソフトウェアエミュレーションである。

【０２６９】

ＶＳＣは以下の機能を提供する。

・ＥＣＭからのＣＭＭの生成
・ＣＭＭからのコンテンツの抽出
・ＣＭＭから抽出された制御ワードのリターン
・セッション鍵の生成
・セッション鍵によるメッセージの暗号化及び解読
・制御ワードの生成（ローカル再スクランブル処理が実行される）

ＶＳＣは、受信機/デコーダのミドルウェアにある暗号ライブラリを利用して、ＣＭＰＳスマートカードのこれら基本的機能をソフトウェア的にエミュレートする。この暗号ライブラリはバーチャルマシーンの別のモジュールとして与えられるが、好適な実施例の変形では、ＶＳＣマネージャ自体に、あるいは受信機/デコーダの他の部分や添付された暗号スマートカードに与えられる。実際のスマートカードの基板上のプロセッサとメモリをエミュレートするのに、ホストプロセッサと関連するメモリが利用される。本好適な実施例では、ＣＭＰＳデバイスマネージャスレッド２３２０のリソースマネージャモジュール２３７０がＶＳＣマネージャと通信し、そしてＶＳＣマネージャがＶＳＣと通信する。その後、リソースマネージャ２３７０は、必要に応じて、システムの他の部分に結果を返すため、メッセージマネージャと通信する。

【０２７０】

ＶＳＣは、暗号化、署名検証及びセッション生成のための３つ一意的な鍵を有する。本好適な実施例では、これらの鍵は、必要とされる限り、セッションをオープンするための第１のリクエストに応答して生成される。本好適な実施例の変形では、これらの鍵は、ＶＳＣの生成時に（例えば、リブート後の受信機/デコーダの初期化により）早期に生成される。

【０２７１】

ＣＭＰＳスマートカードが存在するとき、上記鍵はＣＭＰＳシステムによりＣＭＰＳスマートカードから取得される。あるいは、後述のように、受信機/デコーダのランダムな性質を効果的に利用することにより鍵は生成される。

【０２７２】

ＶＳＣ２４００が上記列挙されたＣＭＭ関連の機能を実行する方法が簡潔に説明される。

【０２７３】

ＶＳＣは、ＶＳＣマネージャ２３５０を介しＣＭＰＳリソースマネージャスレッド２３２０から受信する２つのデータ要素からＣＭＭを生成する。第１要素は公開情報を含み、第２要素は複数または１つのＥＣＭから抽出された制御ワードを含む（図２４に関する以下の説明を参照せよ）。本好適な実施例の変形では、第２要素はまた、ＵＲＭから長う出されたデータを含む。

【０２７４】

ＶＳＣは、これら２つの要素を連結し、この連結された要素を参照して暗号署名を計算する。この署名は、ペイロード（すなわち、制御ワード及び/またはＥＣＭ、署名及びパディング（ｐａｄｄｉｎｇ））の暗号化前にメッセージに（必要ならば、メッセージを一様な長さにするため、複数のパディングバイトと共に）添付される。本好適な実施例では、メッセージの署名を計算及びチェックを行うため、ＣＢＣ－ＭＡＣ暗号テクニックが利用される。この署名はメッセージ自身及び共有される対象鍵に応じて生成される。

【０２７５】

再生中、ＶＳＣ２４００は、ペイロードの解読、パディングの削除、解読されたメッセージ（及び公開情報）の添付された書名を利用した確認により、ＣＭＰＳスレッドを介しクライアントによりわたされたＣＭＭから制御ワード（またはＥＣＭ）を抽出する。その後、この抽出された制御ワードは、制御ワード装置３７６０を利用したＶＳＣによりスクランブル解除装置に直接ロードされる。本好適な実施例の変形では、不明瞭な状況での参照のため、キーハンドル（キーＩＤ）がクライアントに返される。

【０２７６】

本好適な実施例の変形では、ＶＳＣは、前述のように、ＵＲＭからの情報をＣＭＭに格納する代わりに、ＵＲＭの形式で送信された情報を含むテーブルを生成及び格納する。この情報は、ファイル識別子と、これに関する権利と制限（ＵＲＭから抽出された）を含む。ユーザが格納されたプログラムの再生を所望するとき、当該プログラムに関する権利と制限が記憶装置からコンテンツデータを読み出すことなくアクセスされるかもしれない。

[バーチャルスマートカードマネージャ]

ＶＳＣマネージャ２３５０は、ＣＭＰＳスマートカードがバーチャルスマートカード（ＶＳＣ）または実際のスマートカード（ＲＣＡＲＤ装置により表現されるような）の形態である場合、ＣＭＰＳスマートカードの機能をカプセル化する。ＶＳＣマネージャは、（特に）ルーティング機能を実行し、またある管理機能をも実行する。ＶＳＣマネージャはまた、ＶＳＣに有効に送信されるメッセージを定義する。

【０２７７】

上述のルーティングの役割に従って、ＶＳＣマネージャは、あるタスクに対し実際のスマートカードまたはＶＳＣを利用するか決定する機能を提供する（本好適な構成では、バーチャルＣＭＰＳスマートカードと実際のＣＭＰＳスマートカードの両方が与えられる）。この決定は、受信機/デコーダの１以上の特徴（それに対するロードを含む）及び/または処理されるコンテンツデータの１以上の特徴に応じて実行されてもよい。例えば、コンテンツは、実際のスマートカードにより与えられるより強力なセキュリティの恩恵を受けることが望ましいくらいに、あるいはＶＳＣにより与えられるより高速な処理が要するくらいに、比較的商業的に価値あるものであるかもしれない。

【０２７８】

ＶＳＣマネージャにより提供されるハイレベルの機能としては、ＶＳＣインスタンスを生成する機能、ＶＳＣを無効にする無効化装置（ＶＳＣに割り当てられたリソースを開放する）、及びＶＳＣモジュールが現在あるか決定するクエリ機能が含まれる。本好適な実施例では、１つのバーチャルスマートカードのみが任意の時点において存在しうるが、本好適な実施例の変形では、複数のインスタンスが可能である。

【０２７９】

ＶＳＣマネージャ（ＶＳＣ及び/または実際のＣＭＰＳスマートカードと類似した）により提供されるローレベルの機能としては、データオブジェクトの生成、複製、無効化、格納、ロード及び消去のための機能、暗号化及び解読機能、署名の生成及び利用、パッキングの追加及び削除を含む上述のようなＣＭＭの構築機能、以下で詳細に説明されるような乱数の生成及び鍵の生成及び/または導出機能が含まれる。

【０２８０】

ＶＳＣマネージャはまた、デバイスマネージャスレッド２３２０とＶＳＣとの間のセッションの生成及び無効化のための機能を提供する。各新しいセッションには生成時に一意的な識別子（「ＳＥｓｓｉｏｎＩＤ」）が割り当てられ、以降、ＶＳＣマネージャにわた

されるメッセージは関連するセッションのＳｅｓｓｉｏｎＩＤを特定する。前述のように、これらのセッションは、ＣＭＰＳとクライアントとの間の通信に利用されるセッションと異なる（しかし類似な）ものである。これらＣＭＰＳクライアントセッションと対照的に、レコーダセッション、プレーヤーセッション及び管理セッションの合計３つのタイプのセッションが与えられる。このうち、レコーダセッションとプレーヤーセッションは典型的には、ＣＭＰＳとクライアントとの間の対応するレコーダセッション及びプレーヤーセッションにおいて生成される。

【０２８１】

より詳細には、レコーダセッションは、プログラムデータの格納と共に、ローカル制御（すなわち、ＣＭＭ）のメッセージの生成のため利用される。プレーヤーセッションは記録されたコンテンツの再生中利用される。これらのセッションにおいて利用される機能としては、クライアント（例えば、ＨＤＶＲ）によりＶＳＣに送信されるＣＭＭからの制御ワードの抽出に関するものや、ＣＷ装置を介したスクランブル解除装置への挿入に関するものが含まれる。本好適な実施例の変形では、スクランブル解除能力を有するデジタルテレビや制御ワードをロードするＨＤＶＲのような、安全性を有する認証されたチャンネルを利用することにより、制御ワードは他のエンティティ（ｅｎｔｉｔｙ）に転送される。

【０２８２】

管理セッションでは、ＶＳＣの基本的機能、すなわち、擬似乱数シーケンスの生成のような機能などが利用可能である。

【０２８３】

ＶＳＣマネージャとＶＳＣまたは実際のＣＭＰＳスマートカードとの間の通信は安全性を有することが要求される。マスタセッション鍵はこの目的のために使用される。鍵の生成に関するセッションにおいて後述されるように、１以上要求される異なるセッション鍵を導出するため、マスタセッション鍵はＳｅｓｓｉｏｎＩＤにより多様化される。このマスタセッション鍵はまた、例えば、制御ワードがそれをＣＷ装置３７６０にわたすＨＤＶＲにわたされる実施例では、ＨＤＶＲとの安全な通信を確立するのに利用されてもよい。

【０２８４】

ＶＳＣとＶＳＣマネージャは、ＣＭＰＳデバイスマネージャスレッドの一部を形成するものとして説明及び例示（図１６において）されてきたが、必要に応じて、ＣＭＰＳシステム内の他の場所に配備されてもよい。

[鍵生成]

図１９及び図２０を参照するに、鍵を生成する様々な手段が説明される。

【０２８５】

上述のように、本好適な実施例では、乱数発生器の操作や既存の鍵を多様化することにより、様々な鍵が生成される。

【０２８６】

図１９は、新たなマスタセッション鍵８１００が生成される前者のプロセスを示す。受信機/デコーダの様々な要素８１１０（この場合、チューナー、システムクロック及びオペレーティングシステム）と、これらの要素の様々な測定可能な性質８１２０（例えば、チューナーの平均ビットエラーレート、与えられた信号の信号レベル、現在のシステム時刻、最近のリセットからデバイスレイヤインタフェースになされたアクセス数）とが、一列に並んだ正規化フィルタ８１３０と、一列に並んだビットスクランブル化装置８１４０と、排他的ＯＲオペレータ（ＸＯＲ）８１５０と、乱数発生器８１６０に加えて示される。

【０２８７】

可能である場合はいつでも、要素８１１０の性質８１２０は、好ましくは、経時的に変動する効果的な乱数及び/または予測不可能な値として、その能力に応じて選択される。適切な場合には、各性質８１２０は、何れかの性質が優勢にならないように、乱数のシードと同一のビット幅に正規化される（言い換えると、好適な実施例の場合と同様に、３２ビットの乱数シードに対しては３２ビットの数が生成される）。

【０２８８】
以降、各性質の正規化された値は、各性質に対する値の異なるビットを効果的に交換するビットスクランブル化装置により性質ごとに異なる方法によりスクランブル処理される。測定された性質の予測不可能性は少数の下位ビットにのみ制限される場合、例えば、ビットスクランブル処理は３２ビット空間にこの予測不可能性を効果的に分散させる。
【０２８９】
最後に、排他的ＯＲオペレータが第１のビットスクランブル処理された値と第２のビットスクランブル処理された値とを合成し、その結果を第３のビットスクランブル処理された値などと合成する。
【０２９０】
このように生成された乱数シードは乱数発生器に供給され、その後所望のビット長を有する所望の暗号鍵を生成する（必要ならば、任意の個数の固定長の乱数を付け加えることにより）。
【０２９１】
本好適な実施例の変形では、正規化、ビットスクランブル化及び排他的ＯＲの一部あるいはすべての段階がなく、例えば、いくつかのケースでは、単純な和をとるというような性質の合成のための異なる方法と置き換えられる。
【０２９２】
図２０では、鍵多様化装置８２００が、典型的なマスタセッション鍵８２１０とセッションＩＤ８２２０の入力と、導出されたセッション鍵８２３０の出力と共に示される。
【０２９３】
本質的には、鍵多様化装置は、強力な暗号鍵の性質を利用した式を利用して（典型的には、様々な素数の性質を利用して）、セッションに一意的なセッション鍵８２３０を生成するため、セッションＩＤ８２２０に依存してマスタセッション鍵８２１０を操作する。鍵多様化装置に関する制約として、実質的にすべての異なるセッションＩＤの入力が一意的なセッション鍵８２３０を生成し、セッション鍵８２３０はその暗号解読が容易にマスタセッション鍵８２１０を生成できないくらい十分強力なものである。
【０２９４】
図１９及び図２０に示される要素は例示的なものであり、実際の物理的装置に必ずしも対応するものでないということは注意すべきである。実際、好適な実施例では、正規化及びビットスクランブル関数、排他的ＯＲ演算及び乱数生成のすべてが、上述のホストプロセッサ２００２により実行される。本好適な実施例の変形では、少なくとも１つのさらなるプロセッサが、ホストコンピュータへの負荷を減らすため、これらの機能を実行する。
[鍵格納]
図２１を参照するに、暗号鍵を安全に格納及び再生する手段が説明される。
【０２９５】
図２１において、鍵スプリッタ８３１０、格納アクセス装置８３２０及び鍵再合成装置８３３０が、格納アクセス装置８３２０と従来のＲＡＭ要素８３５０とを接続するデータバス８３４０と、ハードディスクユニット２１００と、ＥＥＰＲＯＭ要素８３６０とＦＬＡＳＨ　ＲＡＭ要素８３７０と共に示される。
【０２９６】
暗号鍵を格納するため、例えば、鍵は鍵スプリッタ８３１０に供給され、各自があるビット数を有する適当な数の部分に分割される。本好適な実施例では、便宜上、これら部分のすべては８ビット（１バイト）の同一のサイズを有するが、本好適な実施例の他の変形では、これらの部分は、より小さいサイズ及び/またはより大きいサイズを有し、互いに異なるサイズを有するようにしてもよい。８ビットより小さいサイズは一般的に操作に不便であるが、より良好な安全性を提供することができる。
【０２９７】
これら鍵部分はその後格納アクセス装置８３２０に格納される。実際、この装置は、大容量記憶装置３７２８（ハードディスクのための）などの様々な記憶装置８３５０、２１

００、８３６０及び８３７０と通信するための様々なソフトウェア装置から構成される。
【０２９８】
本好適な実施例では、これら部分をどこに格納すべきかについての場所の正確な選択は、呼び出すプロセスにより提供される鍵識別子（例えば、８ビットに限定して）に依存して格納アクセス装置により生成される。各場所指定装置は、異なる鍵部分の上書きを回避するため、特定の鍵識別子に一意的なものである必要がある。本好適な実施例では、適切な複雑さを有する式が、鍵識別子と鍵部分番号に依存して各格納場所の計算に利用される。本好適な実施例の変形では、様々なテーブル（ＶＳＣの初期化あるいは再初期化時に生成される）が、格納場所の追跡に利用され、格納された鍵部分のそれぞれが鍵識別子及び/または鍵部分番号から導出された鍵により、それが格納されるように、暗号化されてもよい。
【０２９９】
鍵を読み込む対応するプロセスが、鍵識別子を特定する呼び出しを行うプロセスからコマンドにより初期化され、格納アクセス装置にまず格納場所（上述のような）を計算させ、鍵部分のすべてをロードさせる。
【０３００】
その後、鍵部分は鍵再合成装置８３３０に転送され、鍵が再構成され、呼び出したプロセスに出力される。
【０３０１】
鍵格納のための上記方法に対するさらなる改良は、鍵部分が格納されるメモリのランダム化（及び好ましくは、格納されないさらなるメモリのランダム化）である。暗号鍵はしばしば明らかなランダムさのため検出されるため、例えば、侵害者により鍵が再構成される確率を減らすことができる。
【０３０２】
図２２と図２３は、鍵格納機構の動作をより詳細に示す。
【０３０３】
図２２は、４８ビット暗号鍵８４００（１６進数形式で示される）と、鍵部分８４１０、８４１２、８４１４、８４１６及び８４１８と、ランダム化されたメモリ領域８４２０とを示し、鍵８４００の構成要素部分への分割（均等でないサイズの場合）と、これら部分の示された場所のランダム化されたメモリ領域８４２０への格納を示す。
【０３０４】
図２３は、複数の装置を利用した同一の鍵の格納を示す（１つだけのメモリ領域を利用した図２２に示される例と対照的に）。
【０３０５】
図２３において、４８ビット暗号鍵８５００、それの構成要素部分８５１０、８５１２、８５１４、８５１６及び８５１８と、ＥＥＰＲＯＭ要素８５２０と、ハードディスクユニット２１００とフラッシュＲＡＭ要素８５３０が示される。ここで、異なる部分８５１０、８５１２、８５１４、８５１６及び８５１８の異なる装置８５２０、２１００及び８５３０への割り当てが示される。
[ＥＣＭのＣＭＭへのカプセル化]
図２４を参照するに、ＥＣＭのＣＭＭへのカプセル化がより詳細に説明される。
【０３０６】
図２４は、第１及び第２ケースでのＣＭＭ生成ステップ８６００とコンテンツ再生ステップ８６１０を示す（それぞれ破線の左側と右側）。様々なシナリオにおいて、条件付アクセスシステム５０００、ＣＭＭ５６１０及びＣＭＭの鍵フィールドが示される。
【０３０７】
第１ステップ８６００において、ユーザは、少なくとも１つのＣＭＭが必要とされるコンテンツ（テレビプログラムのような）を記録している。どちらの場合でも、与えられたＣＭＭ５６１０に対する関連するＥＣＭが相変わらず要求される。
【０３０８】

第１のケースは、ユーザにＣＭＭを要するコンテンツを視聴するアクセス権が与えられている情況を示す。この場合、条件付アクセスシステム５０００は、ＣＭＰＳシステムにＥＣＭに含まれる制御ワードを返し、ＣＭＭの関連するフィールド８６２０が制御ワードにより埋められる。

【０３０９】

しかしながら第２のケースでは、ユーザは記録されているコンテンツへのアクセス権を所持しない。条件付アクセスシステム５０００からのＤＥＮＹ信号に応答して、関連するＥＣＭが解読された制御ワードのために通常用意されているフィールド８６２０に格納される。この点で、ユーザはコンテンツの視聴が不可であり、アクセス権が拒絶され続ける限り、ＣＭＭは意図されるような機能は行わない。ＥＣＭをＣＭＭにカプセル化するため、リソースマネージャ２３７０は、図１１を参照して上述されたプロシージャにおいて、ＣＭＭを生成するリクエストに対するパラメータとして、制御ワードでなくＥＣＭをＶＳＣマネージャ２３５０を介しＶＳＣ２４００にわたす。

【０３１０】

第２ステップ８６１０において、ユーザはステップ８６００において前に記録されたコンテンツを再生しようとする。これまでに、コンテンツへのアクセス権が以前になくなっていて、適切に取得されたと仮定される。ＣＭＰＳシステムの通常の機能に従って、クライアント（典型的には、ＨＤＶＲシステム）は処理のためＣＭＰＳシステムにＣＭＭを転送する。

【０３１１】

第１のケースでは、ＣＭＰＳシステムは、通常通りＣＭＭ５６１０の関連するフィールド８６２０から制御ワードを抽出し、コンテンツの視聴を可能にするよう制御ワードをスクランブル解除装置（図示せず）に自動供給する。

【０３１２】

第２のケースでは、ＣＭＰＳシステムは、ＣＭＭ５６１０からＥＣＭを抽出し、再びそれを条件付アクセスシステム５０００に転送する。さらなる解読エラーのイベントで、ＣＭＰＳシステムはエラーを通知し、コンテンツを再生する以降の試みにおいて同一の試みを行うであろう。しかしながら、このとき、解読処理は成功する。制御ワードはコンテンツを解読できるスクランブル解除装置２０１０と、当該制御ワードを利用して上述のような格納のためクライアントに送信される新しいＣＭＭ５６１０を生成するＶＳＣにわたされる。

【０３１３】

ここで、上述のシステムはＥＣＭ及び制御ワード以外の他のデータ形式に適用可能である。さらに、第２ステップ８６１０がＣＭＭの検証が即座に実行される効果を有する当該コンテンツの再生中動作するものとして説明されたが、それはまた、例えば、早朝や適切な権利を与えるＥＭＭの受信に応答して、他の任意の時点で「バックグラウンドで」動作することができる。

【０３１４】

ＥＣＭのＣＭＭへのカプセル化はまた、ＨＤＶＲと条件付アクセスシステムとの間の独立性の度合いを提供することができる。例えば、複数の条件付アクセスシステムが受信機/デコーダに備えられる場合、これは特に有益である。この場合、以前のように、それらの１つが適切な権利を受け取るまで、様々な条件付アクセスシステムからのＥＣＭを埋め込むことができ、ＣＭＰＳがＥＣＭを決定することが可能となる。

【０３１５】

上述の様々な機能の実現形態の正確な詳細と、ハードウェアとソフトウェア間の分散は、実現する者の選択の問題であり、詳細には説明されない。しかしながら、受信機/デコーダにおいて必要な処理を実行することができる専用の集積回路は商業的に利用可能であり、容易に設計可能である。これらの集積回路は、ハードウェアアクセラレータの基礎として利用可能であり、より好ましくは、必要とされる様々な処理を実現するため、専用のハードウェアアクセラレータを生成するよう変更される。これにより、ソフトウェアの実

行に要する処理パワーを減少させることができる。しかしながら、必要とされる処理は、十分な処理パワーが利用可能である場合、ソフトウェア的に実現されてもよい。

【０３１６】

モジュールと他の要素が、各要素により提供される特徴及び機能と共に、選択的かつ好ましい特徴に関して、モジュール及び他の要素が説明された。与えられる情報及び詳細により、これらの特徴と正確な詳細の実際の実現形態は実現する者に任される。一例として、あるモジュールはソフトウェア的に実現可能であり、好ましくは、Ｃプログラミング言語で記述され、アプリケーションの実行に利用されるプロセッサ上で実行できるようにコンパイルされる。しかしながら、構成要素の中には別のプロセッサ上で実行されるものもあるし、構成要素の一部あるいはすべてが専用ハードウェアにより実現されてもよい。

【０３１７】

上記モジュール及び構成要素は単なる例示のためのものであり、本発明は様々な方法で実現されてもよく、特に、構成要素の一部は類似の機能を実行する他の要素に合成されるか、あるいは一部は簡素化された実現形態では省略されてもよい。各機能のハードウェア及びソフトウェアによる実現は、構成要素間で、及び単一の構成要素内で自由に混合されてもよい。

【０３１８】

ハードウェア、コンピュータソフトウェアなどにより実行される機能は、電気信号などで、あるいは電気信号などを利用して実行されるということは容易に理解されるであろう。ソフトウェアの実現形態はＲＯＭに格納されてもよいし、あるいはＦＬＡＳＨに収められてもよい。

【０３１９】

本発明は、単なる例により上記のように説明されたが、本発明の範囲内で詳細の変更が可能であるということは理解されるであろう。

【０３２０】

説明、（適切である場合）クレーム及び図面に開示された各特徴は独立に、または任意の適当な組み合わせにより与えられるかもしれない。

【図面の簡単な説明】

【０３２１】

【図１】図１は、衛星デジタルテレビシステムの概観である。

【図２】図２は、ケーブルデジタルテレビシステムの概観である。

【図３】図３は、より詳細に示されたヘッドエンドを有するシステムの全体図である。

【図４】図４は、受信機/デコーダの要素アーキテクチャの概略である。

【図５】図５は、受信機/デコーダのソフトウェアアーキテクチャの図である。

【図６】図６は、図５の上半分をより詳細に示す図である。

【図７】図７は、図５の下半分をより詳細に示す図である。

【図８】図８は、図５の下半分の他の実施例を示す図である。

【図９】図９は、コンテンツ管理保護システムの概観である。

【図１０】図１０は、コンテンツ管理保護システムを利用した分散システムの概観である。

【図１１】図１１は、データの記録を調整する受信機/デコーダのコンテンツ管理保護システムの実施形態の概略である。

【図１２】図１２は、データの再生を調整する受信機/デコーダのコンテンツ管理保護システムの実施形態の概略である。

【図１３】図１３は、コンテンツ管理保護システムを利用したデータの記録処理を示したものである。

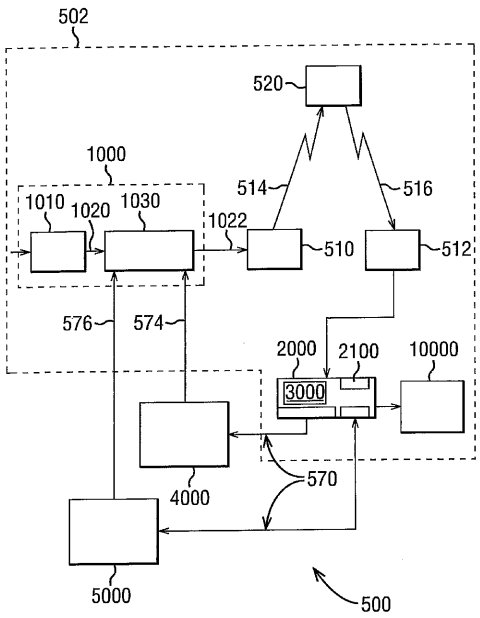
【図１４】図１４は、コンテンツ管理保護システムを利用したデータの再生処理を示したものである。

【図１５】図１５は、コンテンツ管理保護システムとハードディスクビデオレコーダとの間の関係を示したものである。

【図１６】図１６は、コンテンツ管理保護システムのより詳細な概略である。
【図１７】図１７は、コンテンツ管理保護システムの異なる要素間のコマンドフローを示したものである。
【図１８】図１８は、コンテンツ管理保護システムの異なる要素間のコマンドフローをさらに示したものである。
【図１９】図１９は、乱数発生器を利用した暗号鍵を生成するシステムの概略である。
【図２０】図２０は、鍵多様化装置を利用した暗号鍵を生成するシステムの概略である。
【図２１】図２１は、暗号鍵を格納及び抽出するシステムの概略である。
【図２２】図２２は、上記システムに従い暗号鍵を格納するプロセスを示したものである。
【図２３】図２３は、暗号鍵を格納するプロセスをさらに示したものである。
【図２４】図２４は、エンタイトルメント制御メッセージ（ＥＣＭ）のコンテンツ管理メッセージ（ＣＭＭ）へのカプセル化を示したものである。

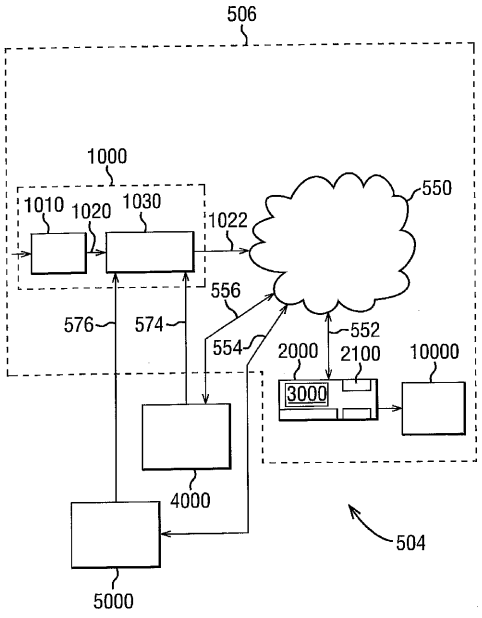
【図１】

FIG. 1

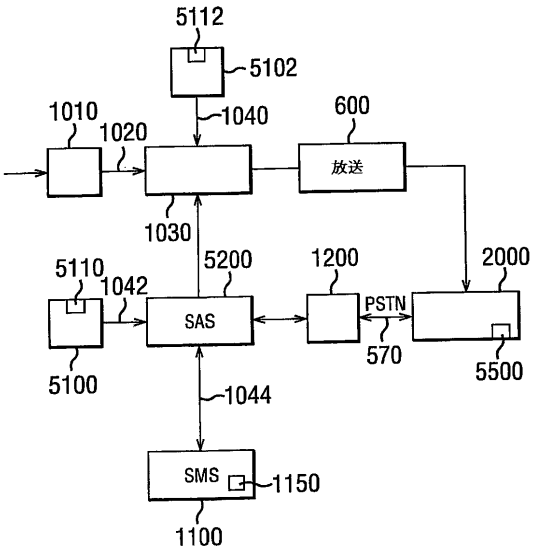


【図２】

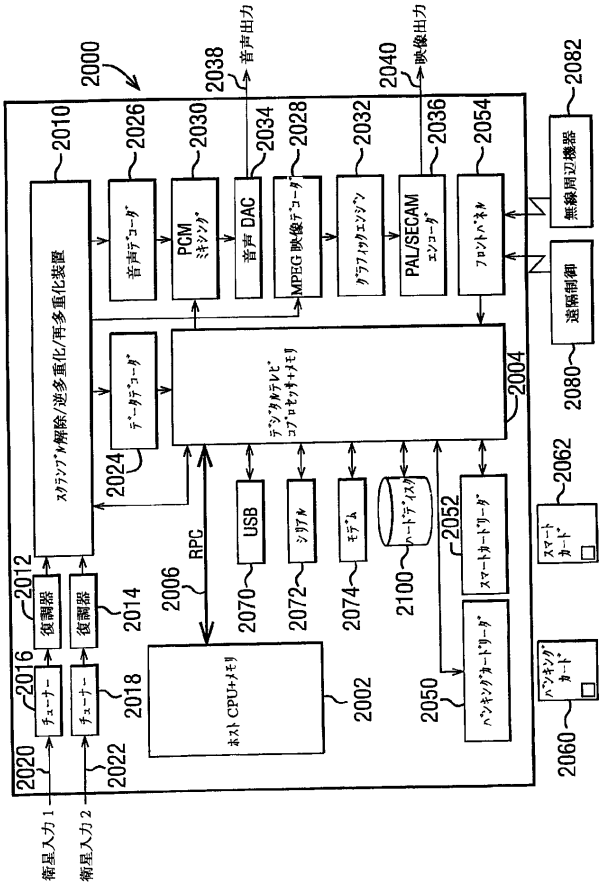
FIG. 2



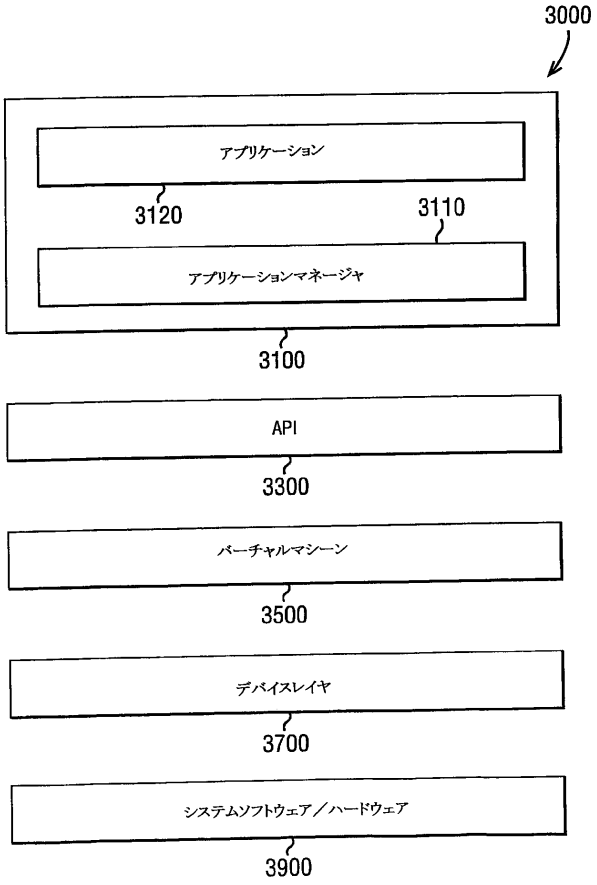
【図３】


5112
5102
1010
1020
1040
600
放送
1030
5110
1042
5200
1200
2000
SAS
PSTN
570
5500
5100
1044
SMS
1150
1100

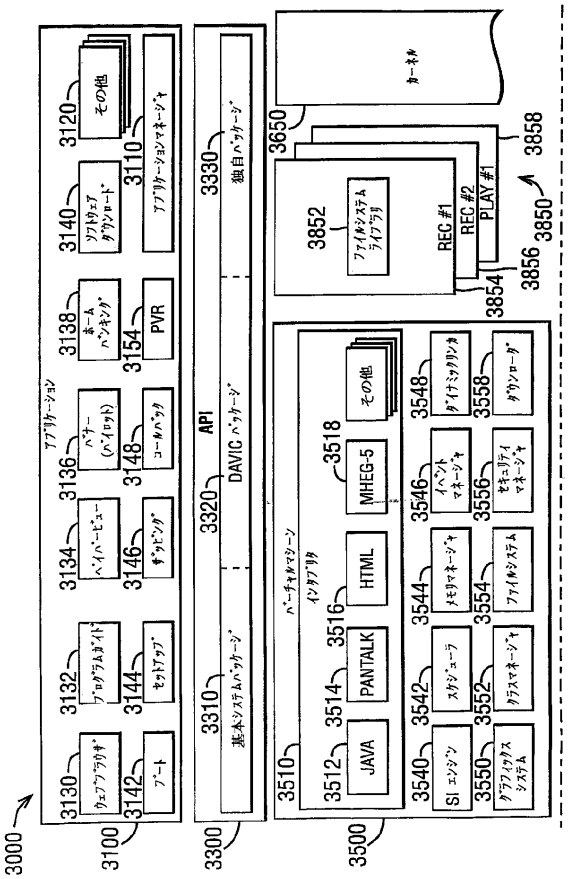
【図４】


2000
2038
音声出力
2040
映像出力
2082
無線周辺機器
遠隔制御
2080
2010
2026
2030
2034
2028
2032
2036
2054
音声デコーダ
PCM
音声 DAC
MPEG 映像デコーダ
PAL/SECAM
フロントパネル
2004
2062
2012
2014
2006
RPC
2070
2072
2074
2100
2052
2024
2002
2050
2060
2016
2018
2020
2022
衛星入力 1
衛星入力 2
USB
RPC

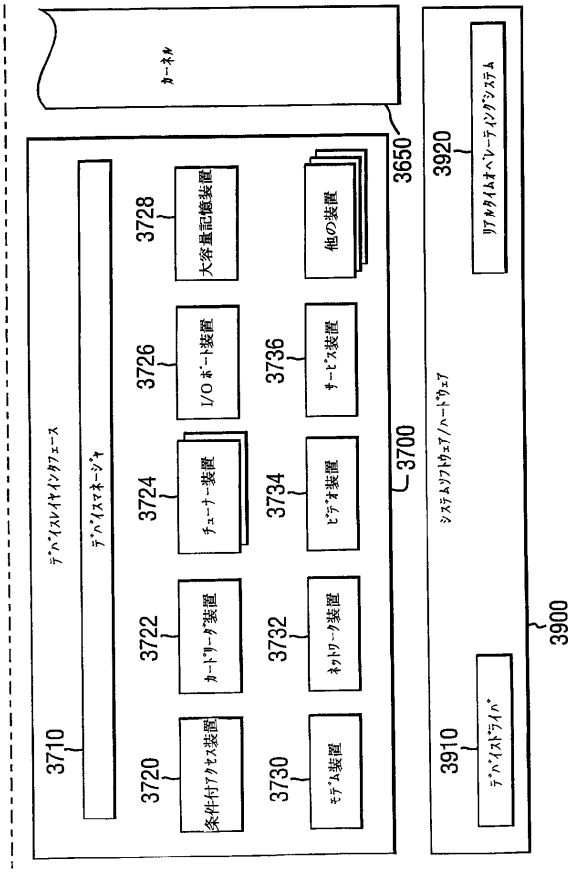
【図５】


3000
アプリケーション
3120
3110
アプリケーションマネージャ
3100
API
3300
バーチャルマシーン
3500
デバイスレイヤ
3700
システムソフトウェア／ハードウェア
3900

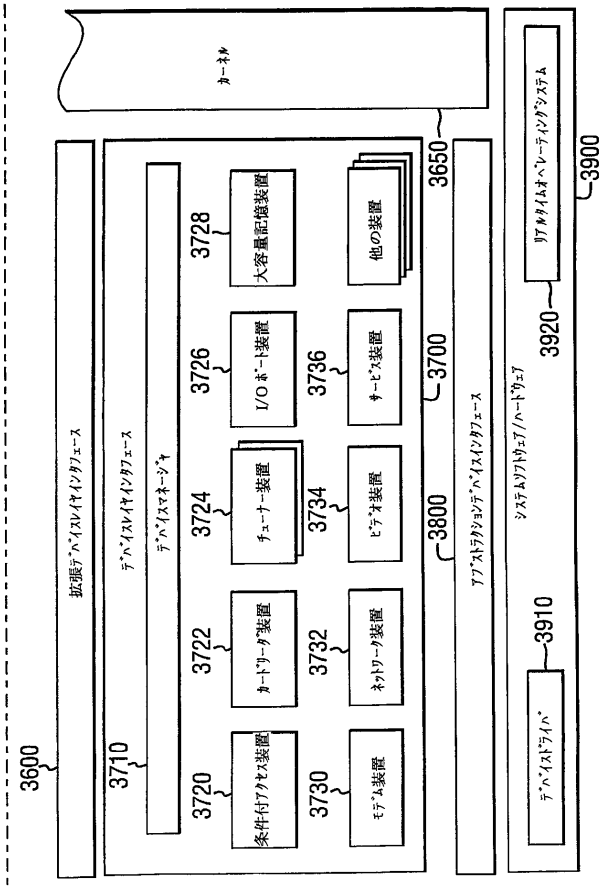
【図６】


3000
3100
3300
3500
3120
3110
3140
3138
3154
3136
3148
3134
3146
3132
3144
3130
3142
3310
3320
3330
3650
3858
3852
3850
3856
3854
3510
3512
3514
3516
3518
3540
3542
3544
3546
3548
3550
3552
3554
3556
3558
JAVA
PANTALK
HTML
MHEG-5
REC #1
REC #2
PLAY #1

【図７】

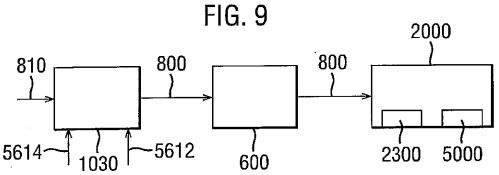


【図８】



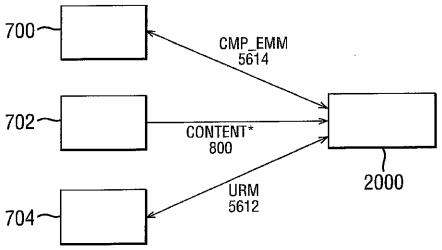
【図９】

FIG. 9

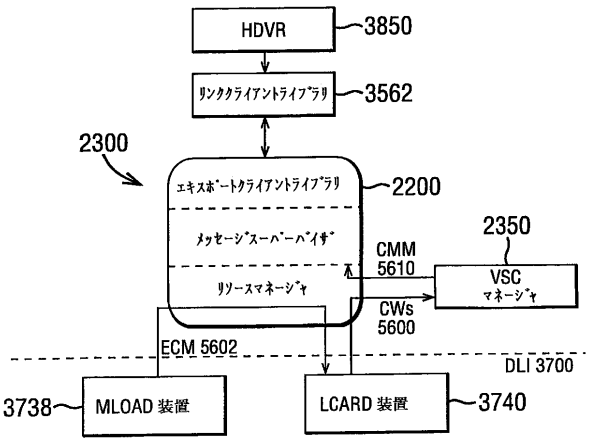


【図１０】

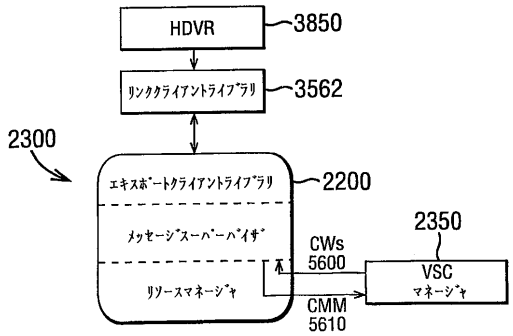
FIG. 10



【図１１】

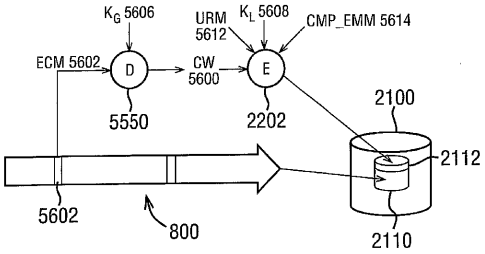


【図１２】



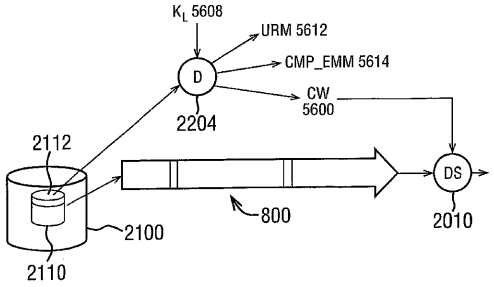
【図１３】

FIG. 13



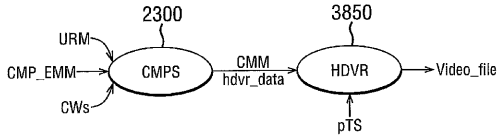
【図１４】

FIG. 14

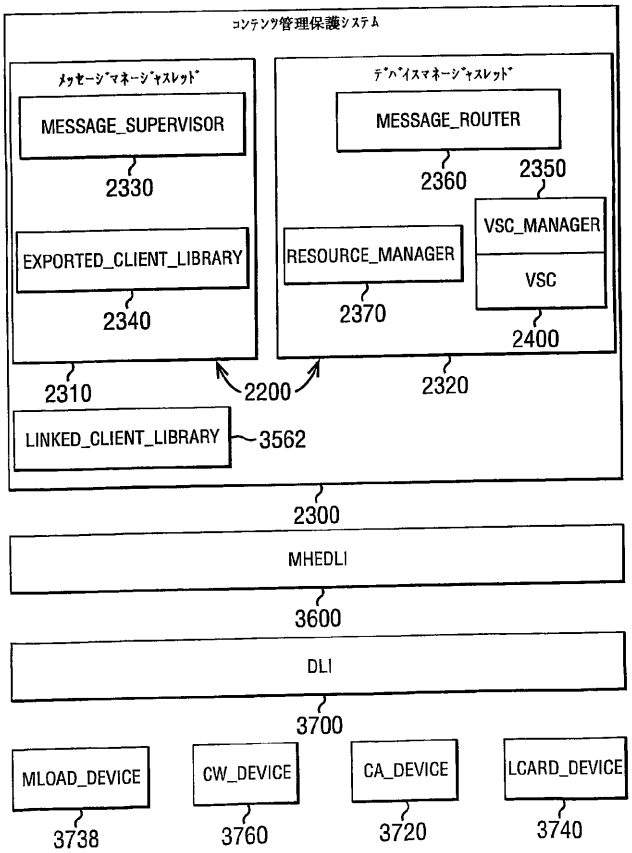


【図１５】

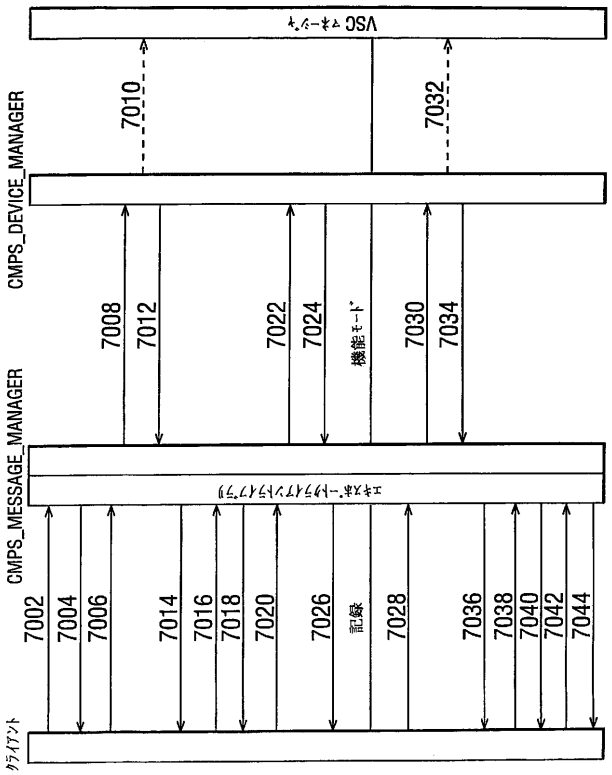
FIG. 15



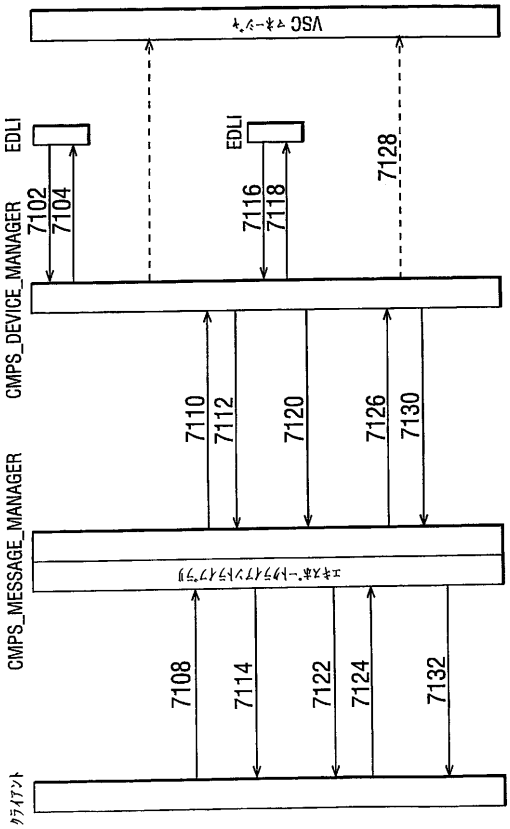
【図１６】



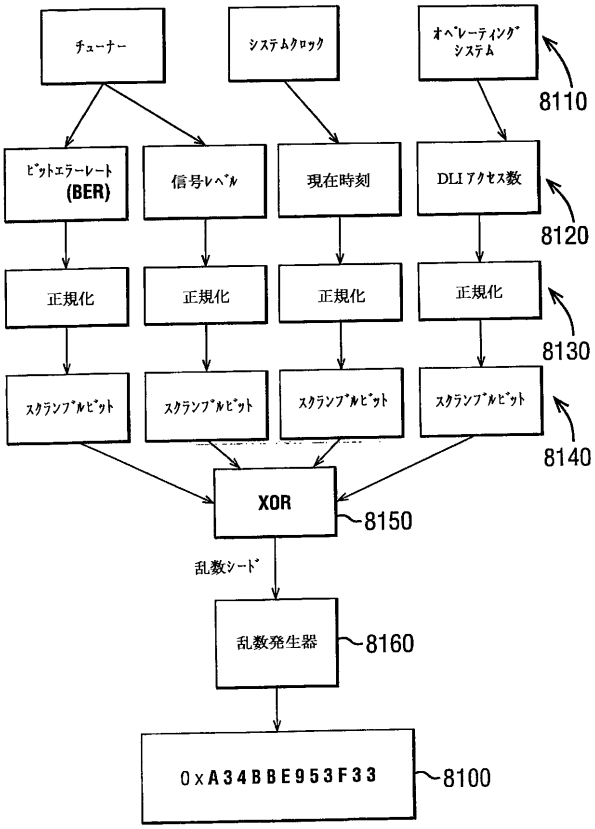
【図１７】



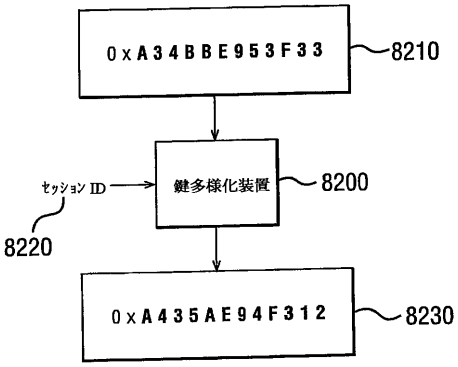
【図１８】



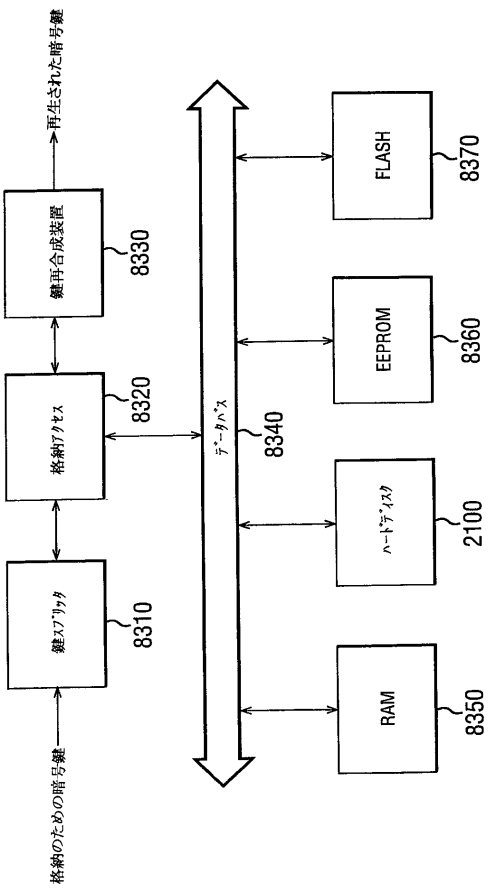
【図１９】



【図２０】

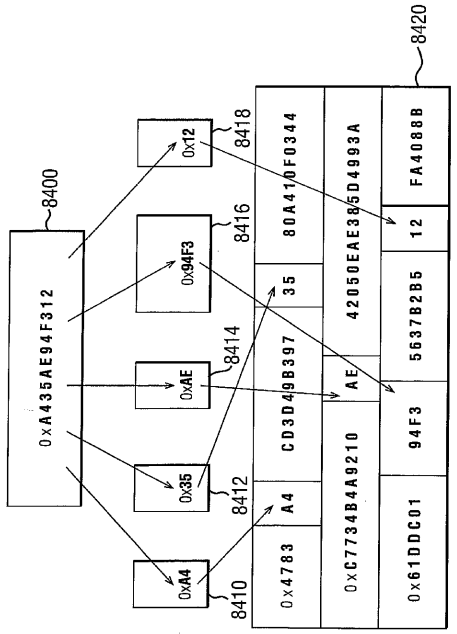


【図２１】

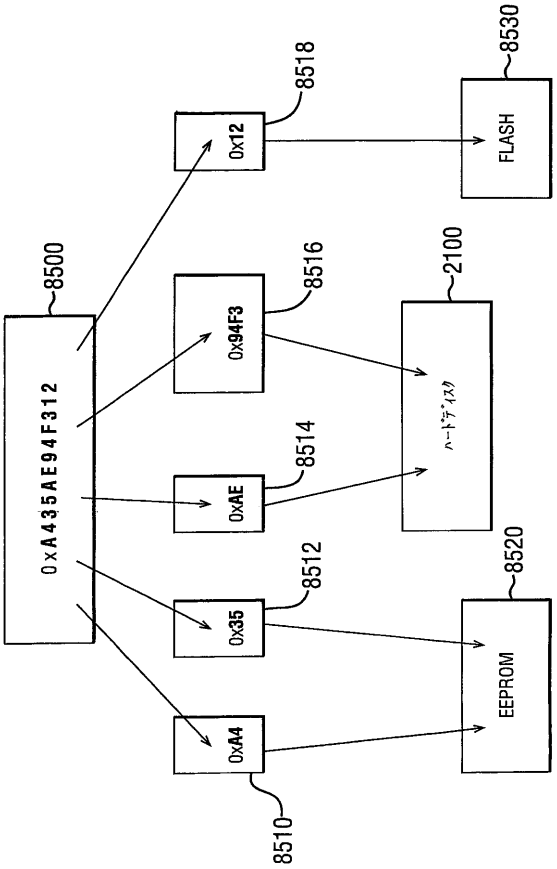


【図２２】

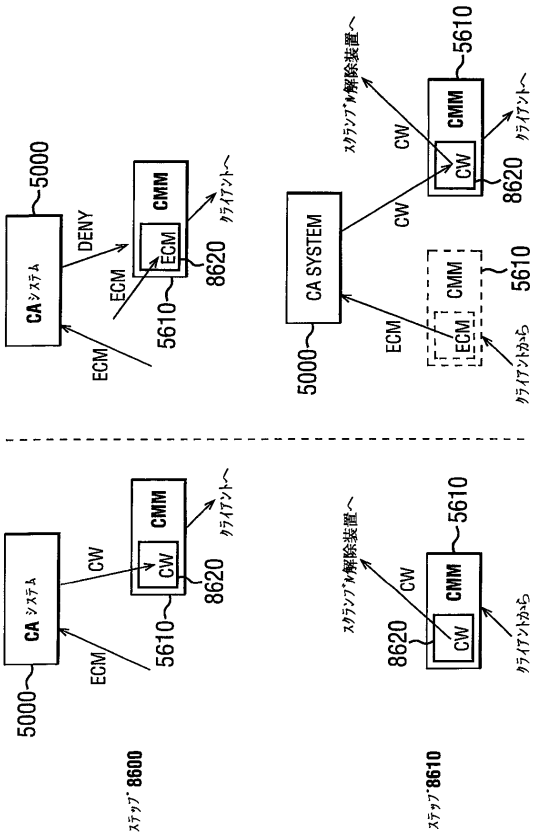
FIG. 22



【図２３】



【図２４】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/IB 02/05774

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04N G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 128 605 A (MOMIKI SHUNICHI ET AL) 3 October 2000 (2000-10-03) column 4, line 33 - line 55 column 7, line 66 -column 8, line 44 column 10, line 57 -column 11, line 18 column 14, line 9 -column 15, line 23 claims 1-3; figures 5,6,8	1,4-9, 11,12,24
X	EP 0 936 530 A (SIEMENS NIXDORF INF SYST) 18 August 1999 (1999-08-18)	12,13,17
A	column 3, line 22 -column 4, line 11 column 6, line 18 -column 7, line 39 column 10, line 7 -column 11, line 39 column 19, line 3 -column 20, line 9 figures 1,2,5-7,10-13	14-16

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 September 2003	24/09/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Paraf, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/05774

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 93212 A (BILLSTROM LEIF OLOV ;MUIR JOHN RICHARD (US); LENNARTSSON KURT UNO) 6 December 2001 (2001-12-06)	12,13,17
A	page 8, line 20 -page 9, line 9 page 13, line 8 -page 14, line 19 claims 1-6,11-14,21; figures 3,5-7,10	14-16
A	EP 0 658 054 A (NEWS DATACOM LTD) 14 June 1995 (1995-06-14) column 5, line 17 -column 7, line 25 claims 1,2,7; figures 1,2	1,2,17

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr ial Application No
PCT/IB 02/05774

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6128605 A	03-10-2000	EP 0715241 A2	05-06-1996
		JP 8287014 A	01-11-1996
		US 2002052850 A1	02-05-2002
		US 2002112173 A1	15-08-2002
		US 6408390 B1	18-06-2002
		US 2001013021 A1	09-08-2001
		US 5867579 A	02-02-1999
		US 6424715 B1	23-07-2002
		US 2002059238 A1	16-05-2002
		US 6002772 A	14-12-1999
EP 0936530 A	18-08-1999	EP 0936530 A1	18-08-1999
WO 0193212 A	06-12-2001	AU 7505101 A	11-12-2001
		WO 0193212 A2	06-12-2001
EP 0658054 A	14-06-1995	IL 107967 A	05-12-1996
		AT 171331 T	15-10-1998
		AU 684112 B2	04-12-1997
		AU 8034294 A	15-06-1995
		CA 2137608 A1	10-06-1995
		DE 69413361 D1	22-10-1998
		EP 0658054 A2	14-06-1995
		HK 1012811 A1	12-05-2000
		JP 7288522 A	31-10-1995
		US 5590200 A	31-12-1996

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 ブーク，ジャン－ベルナール
フランス国，７５９０６ パリ，プラス・ラウル・ドトリー ３４，カナルプラス テクノロジーズ ソシエテ アノニム内
(72)発明者 アンジェル，ミシェル
フランス国，７５００４ パリ，ブールヴァール・モルラン ４

Ｆターム(参考) 5B017 AA06 BA07 CA14 CA16
5C064 BA01 BB02 BC06 BC16 BC17 BC22 BC23 BC25 BD02 BD08
BD09
5J104 AA16 NA40