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

特許第4819059号
(P4819059)

(45)発行日　平成23年11月16日(2011.11.16)　(24)登録日　平成23年9月9日(2011.9.9)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
G06Q 50/00	(2006.01)	H04L	9/00	601E
H04N 7/167	(2011.01)	G06F	17/60	142
H04N 7/173	(2011.01)	H04N	7/167	Z
		H04N	7/173	630

請求項の数 21　(全 20 頁)

(21)出願番号　特願2007-536692 (P2007-536692)
(86)(22)出願日　平成17年8月31日 (2005.8.31)
(65)公表番号　特表2008-516551 (P2008-516551A)
(43)公表日　平成20年5月15日 (2008.5.15)
(86)国際出願番号　PCT/US2005/031171
(87)国際公開番号　WO2006/041590
(87)国際公開日　平成18年4月20日 (2006.4.20)
審査請求日　平成20年8月5日 (2008.8.5)
(31)優先権主張番号　10/962,830
(32)優先日　平成16年10月11日 (2004.10.11)
(33)優先権主張国　米国 (US)

(73)特許権者　593181638
ソニー　エレクトロニクス　インク
アメリカ合衆国　ニュージャージー州　07656　パークリッジ　ソニー　ドライブ　1
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100109070
弁理士　須田　洋之
(74)代理人　100151987
弁理士　谷口　信行

最終頁に続く

(54)【発明の名称】デスクランブル方法及びデスクランブル装置

(57)【特許請求の範囲】
【請求項１】
スクランブルされたデジタルコンテンツを、加入者端末装置内でデスクランブルするデスクランブル方法において、
上記加入者端末装置の第１のコンポーネントによって、デジタル権利管理を行い、デスクランブルされたフォーマットのデジタルコンテンツにアクセスするために必要な権利を、該加入者端末装置が使用可能であるかを判定するステップと、
上記第１のコンポーネントから論理的に分離され、独立した、上記加入者端末装置の第２のコンポーネントによって、デジタルコンテンツにアクセスするために必要な全ての権利を、該加入者端末装置が使用可能であるとの判定に応じて、スクランブルされたデジタルコンテンツをデスクランブルするために用いられるサービスキーを平文化するために用いられるキーを導出するステップとを有し、
上記キーを導出するステップは、固有キーを用いて暗号化されたデータを平文化し、その後、該平文化されたデータをハッシュ処理し、該キーを生成するステップを含むことを特徴とするデスクランブル方法。
【請求項２】
上記第１のコンポーネントは、メインの中央処理装置（ＣＰＵ）であり、上記第２のコンポーネントは、デスクランブラであることを特徴とする請求項１記載のデスクランブル方法。
【請求項３】

上記キーを導出する前に、デジタルコンテンツにアクセスするために権利が必要であり、上記加入者端末装置が該権利を現在使用できない場合、該加入者端末装置の加入者に権利を購入するための入力を促すステップを更に有する請求項１記載のデスクランブル方法。

【請求項４】

上記加入者に入力を促すステップは、上記加入者端末装置と通信するディスプレイ装置に表示され、選択可能なフィールドを含む画像を生成するステップを含むことを特徴とする請求項３記載のデスクランブル方法。

【請求項５】

上記キーを導出する前に、上記選択可能なフィールドの選択に応じて、上記加入者端末装置に送信される選択された権利の要求であるメッセージをヘッドエンドに送信するステップを更に有する請求項４記載のデスクランブル方法。

【請求項６】

上記選択可能なフィールドの選択は、上記加入者がアクセスできる制御ユニットによって実行されることを特徴とする請求項５記載のデスクランブル方法。

【請求項７】

上記デジタル権利管理を行うステップは、それぞれがデジタルコンテンツの再生を制御する複数の必要な権利を分析するステップを含むことを特徴とする請求項１記載のデスクランブル方法。

【請求項８】

上記キーは、ハッシュ値であることを特徴とする請求項１記載のデスクランブル方法。

【請求項９】

スクランブルされたデジタルコンテンツを受信し、デスクランブルするデスクランブル装置において、

上記デジタルコンテンツにアクセスするために各権利が必要かを判定するデジタル権利管理（ＤＲＭ）機能を実行するプロセッサと、

上記デジタルコンテンツにアクセスするために必要な各権利が予め保存されているとの判定に基づいて、一回のみ書込可能なメモリ内に保存されている固有キーを用いて、スクランブルされたデジタルコンテンツをデスクランブルし、該デジタルコンテンツを再生するために用いられる少なくとも１つのサービスキーを平文化するためのキーを生成するために用いられる暗号化情報を平文化するデスクランブラとを備え、

前記デスクランブラは、少なくとも第１の処理ブロック及び第２の処理ブロックを有する処理ブロックのシーケンスであって、キーのラダー接続を構成する処理ブロックのシーケンスを備え、上記第１の処理ブロックは、上記固有キーによって、暗号化されている複数のキーを平文化し、複数の平文化キーを生成し、上記第２の処理ブロックは、複数の平文化キーを用いて一方向ハッシュ処理を行い、上記キーを生成するデスクランブル装置。

【請求項１０】

上記プロセッサ及びデスクランブラは、単一の集積回路内に設けられていることを特徴とする請求項９記載のデスクランブル装置。

【請求項１１】

上記キーのラダー接続ラは、上記スクランブルされたデジタルコンテンツをデスクランブルするための上記少なくとも１つのサービスキーを再生するためのキーを生成するよう構成されていることを特徴とする請求項９記載のデスクランブル装置。

【請求項１２】

上記デスクランブラは、プロセッサを含まず、それぞれが専用機能を有する上記処理ブロックのシーケンスによって実現されることを特徴とする請求項１１記載のデスクランブル装置。

【請求項１３】

上記処理ブロックのシーケンスの第１の処理ブロックは、固有キーによって暗号化された複数のキーを平文化し、複数の平文化キーを生成することを特徴とする請求項１２記載

のデスクランブル装置。
【請求項１４】
上記処理ブロックのシーケンスの第２の処理ブロックは、複数の平文化キーの少なくとも１つと、少なくとも１つの予め算出されたハッシュ値とを用いて、一方向ハッシュ処理を行い、キーを生成することを特徴とする請求項１３記載のデスクランブル装置。
【請求項１５】
上記処理ブロックのシーケンスの第３の処理ブロックは、供給されるスクランブルされたデジタルコンテンツをデスクランブルし、デスクランブルされたデジタルコンテンツを生成することを特徴とする請求項１４記載のデスクランブル装置。
【請求項１６】
上記キーは、ハッシュ値であることを特徴とする請求項１２記載のデスクランブル装置。
【請求項１７】
当該デスクランブル装置は、伝送媒体を介して、ディスプレイと、ハードディスク記録ユニットと、加入者端末装置とに接続され、上記デスクランブラは、複数の処理ブロックに接続され、デスクランブルされたデジタルコンテンツを受信し、上記伝送媒体を介して上記加入者端末装置に伝送するために、該デジタルコンテンツを再暗号化する暗号化ロジックを備えることを特徴とする請求項１１記載のデスクランブル装置。
【請求項１８】
供給されるスクランブルされたコンテンツをデスクランブルする集積回路装置において、
デジタル権利管理（ＤＲＭ）機能を実行する第１のコンポーネントと、
固有キーを保存する一回のみ書込可能なメモリを含み、ＤＲＭ機能から完全に独立して動作する第２のコンポーネントとを備え、
上記第２のコンポーネントは、少なくとも第１の処理ブロック及び第２の処理ブロックを有する処理ブロックのシーケンスであって、キーのラダー接続を構成する処理ブロックのシーケンスによって実現され、
上記第２のコンポーネントは、動作可能な状態にある場合、上記第１の処理ブロックにおいて、上記固有キーを用いて暗号化情報を平文化し、第２の処理ブロックにおいて、平分化され当該情報をハッシュ化し、上記コンテンツにアクセスするために必要な各権利が当該集積回路装置内に保存されているとの判定に基づいて、スクランブルされたコンテンツをデスクランブルするために用いられる少なくとも１つのサービスキーを平文化するために用いられるキーを生成することを特徴とする集積回路装置。
【請求項１９】
上記第１のコンポーネント及び第２のコンポーネントは、単一の集積回路内に設けられていることを特徴とする請求項１８記載の集積回路装置。
【請求項２０】
上記第１のコンポーネントは、プロセッサであることを特徴とする請求項１８記載の集積回路装置。
【請求項２１】
上記第２のコンポーネントは、それぞれが専用機能を有し、処理ブロックのシーケンスによって実現されるデスクランブラであり、少なくとも１つのサービスキーを再生するキーを生成するようキーのラダー接続は構成されることを特徴とする請求項２０記載の集積回路装置。
【発明の詳細な説明】
【関連出願】
【０００１】
本出願は、２００２年１１月５日に出願された米国仮特許出願番号６０／４２４，３８１号の優先権を主張して２００３年3月１２日に出願された米国特許出願番号１０／３８８，００２号の一部継続出願である。

【技術分野】
【０００２】
本発明の実施の形態は、デジタル通信に関する。詳しくは、一回のみ書込可能なキーを用いてデジタル権利管理を行うデスクランブル方法及びデスクランブル装置に関する。
【背景技術】
【０００３】
デジタル通信システムは、アナログ通信システムに代わって急速に普及しつつある。同様に、インターネットとワールドワイドウェブの爆発的な普及により、例えばＭＰ３フォーマットのオーディオファイルやその他のコンテンツを含むダウンロード可能なオーディオビジュアルファイルも広く普及している。
【０００４】
同時に、このようなデジタル通信システムへの急速な移行に伴い、デジタル記録装置も大きく進化している。高品質の記録及びアナログ技術において知られている世代間の劣化（すなわち、連続するコピーによりデータ品質が順次劣化していくこと）を生じることなくコピーを作成するデジタル記録装置の例として、デジタルバーサタイルディスク（Digital versatile disk：以下、ＤＶＤという）レコーダ、デジタルＶＨＳビデオテープレコーダ（以下、Ｄ－ＶＨＳ ＶＴＲという。）、ＣＤ－ＲＯＭレコーダ（例えば、ＣＤ－Ｒ及びＣＤ－ＲＷ）、ＭＰ３記録装置、及びハードディスクを利用した記録装置等が知られている。
【０００５】
デジタル通信システム及びデジタル記録装置の普及により、例えば映像及び音楽制作業者等のコンテンツ提供業者は、著作権等により保護されるべき素材が正当な許可なく自由にコピーされないよう工夫する必要がある。このために、このようなコンテンツのプロバイダからデジタルコンテンツを受信するセットトップボックスでは、デジタル権管理方式が採用されている。
【０００６】
「デジタル権利管理」（Digital Rights Management：ＤＲＭ）は、コンテンツ所有者又はコンテンツプロバイダの何れかによって付与された権利に基づいてデジタルコンテンツを適切に扱うためのメカニズムである。従来、ＤＲＭは、放送コンテンツへの単純な限定受信を実現するために構成されていた。この処理は、暗号コプロセッサ又は例えば、中央演算処理装置（central processing unit：ＣＰＵ）と連携して動作するスマートカード等の周辺のハードウェアによって実行されていた。この構成によって、デジタルコンテンツを加入者にある程度安全に配信できていたが、個別のセキュリティ回路は高コストであり、配信後のデジタルコンテンツの保護は不完全であり、コンテンツ所有者又はコンテンツプロバイダによって課される新たな規則に従ってプログラムを変更することが困難である等の問題があった。近年のセットトップボックスは、将来の視聴のためにコンテンツを保存でき、また、例えば、イーサネット（登録商標）、ＩＥＥＥ１３９４又はＨＤＭＩ等のデジタルインタフェースを介して、ネットワーク内の他の機器にコンテンツを供給することができる。この結果、コンテンツを取り扱うための規則は、複雑になっている。そこで、新たに導入されるコンテンツの取り扱いのための規則に柔軟且つ動的に対応すると共に、平文化キーの安全性を低コストで確保する技術が望まれている。
【発明を実施するための最良の形態】
【０００７】
本発明は、様々な実施の形態として、コンテンツプロバイダから受信したデジタルコンテンツに関する権利を制御する装置、システム及び方法を提供する。「コンテンツプロバイダ」の具体例としては、以下に限定されるものではないが、地上波放送業者、ケーブル運営事業者、直接放送衛星（direct broadcast satellite：ＤＢＳ）事業者、インターネットを介してダウンロードされるコンテンツを提供する業者及び又はコンテンツの他のソースが含まれる。このような制御は、キー生成ロジックから独立しているが、キー生成ロジックと連携して動作する加入者端末装置にロードされたデジタル権利管理ロジックによ

って実現される。

【０００８】

詳しくは、デジタル権利管理ロジックの機能は、デスクランブラによって内部的に行われるキー生成処理から独立している。ＤＲＭは、加入者端末装置のメインプロセッサによって実行される。ＤＲＭの更新情報は、加入者端末装置にダウンロードできる。キー生成は、デスクランブラによって実行され、デスクランブラは、非プロセッサのハードウェアであってもよく、したがって、ＤＲＭ機能から完全に独立しており、独立した暗号プロセッサを設ける必要はない。ハードウェアベースの機密保護技術は、解読及びリバースエンジニアリングがより困難であるため、この手法により、ソフトウェアのみを用いてＤＲＭ及びキー生成の両方を実行する手法に比べて、コンテンツに関してより高いレベルの安全性が確保される。

【０００９】

以下の説明では、特定の用語を用いて本発明の特徴を説明する。例えば、用語「コンポーネント」又は「ロジック」は、１つ以上の機能を実行するように構成されたハードウェア及び／又はソフトウェアを表している。「ハードウェア」の具体例としては、以下に限定されるものではないが、集積回路、例えば、プロセッサ（例えば、マイクロプロセッサ、特定用途向け集積回路、デジタルシグナルプロセッサ、マイクロコントローラ等）、有限状態マシン、組合せロジック等がある。

【００１０】

「ソフトウェア」の具体例には、アプリケーション、アプレット、ルーチン又はサブルーチンの形式を有する一連の実行可能な命令が含まれる。ソフトウェアは、例えば、プログラマブル電子回路、半導体記憶装置、例えば、揮発性メモリ（例えば、ランダムアクセスメモリ等）、不揮発性メモリ、（例えば、あらゆる種類の読出専用メモリ（ＲＯＭ）、フラッシュメモリ）、フロッピー（登録商標）ディスク、オプティカルディスク（例えば、コンパクトディスク又はデジタルビデオディスク（ＤＶＤ））、ハードディスクドライブディスク、テープ状記録媒体等、マシンにより読取可能な如何なる媒体に格納してもよい。

【００１１】

本明細書において、用語「処理ブロック」とは、平文化、暗号化、ハッシュ処理等の専用機能を有するハードウェア及び／又はソフトウェアを表す。

【００１２】

図１は、コンテンツ配信システム１００の例示的な実施の形態を示している。コンテンツ配信システム１００は、１つ以上のコンテンツプロバイダから、第１の伝送媒体１０５（例えば、電線、光ファイバ、ケーブル、無線シグナリング回路等）を介して、プログラムデータを含む情報を受信する加入者端末装置１１０を備える。プログラムデータは、例えば、デジタルビットストリームとして伝送してもよい。加入者端末装置１１０は、例えば、セットトップボックス、又はテレビジョン、コンピュータ、オーディオ再生装置（例えば、デジタルラジオ）、録音機器（例えば、ＭＰ３プレーヤ）、ビデオ録画機器（例えば、デジタルレコーダ）等に組み込まれた１つ以上のコンポーネントを始めとして、如何なる製品として動作してもよい。

【００１３】

本発明の一実施の形態では、加入者端末装置１１０は、埋め込みアーキテクチャに基づき、すなわち、加入者端末装置１１０は、デジタル権利管理（ＤＲＭ）及びデスクランブル処理の両方をサポートする、固定された内部ロジックを有するセットトップボックスとして実現される。図１では、この内部ロジックをデジタルデバイス１１５として表している。

【００１４】

加入者端末装置１１０は、セットトップボックスとして実現される場合、第２の伝送媒体１２０を介して、コンテンツ配信システム１００の他のコンポーネントに接続してもよい。第２の伝送媒体１２０は、コンテンツ配信システム１００の加入者端末装置１１０と

、他のコンポーネントとの間でプログラムデータを伝送する。

【００１５】

コンテンツ配信システム１００は、加入者端末装置１１０に対応する製品の種類に応じて、オーディオシステム１３０、デジタルＶＣＲ１４０、ハードディスク記録ユニット１５０、ディスプレイ１６０、制御ユニット１７０及び第２の加入者端末装置１８０のうちの１つ以上を含んでいてもよい。

【００１６】

ここでは、図１に示すように、プログラムデータがオーディオファイルを含む場合、オーディオシステム１３０は、オーディオ再生及び記録機能を提供する。例えば、Ｄ－ＶＨＳビデオテープレコーダであるデジタルＶＣＲ１４０及びハードディスク記録ユニット１５０は、プログラムデータの記録及び再生に用いられる。オーディオシステム１３０、デジタルＶＣＲ１４０及びハードディスク記録ユニット１５０は、第２の伝送媒体１２０を介して、加入者端末装置１１０と、コンテンツ配信システム１００の他のコンポーネント、例えば、ディスプレイ１６０、制御ユニット１７０及び第２の加入者端末装置１８０と通信する。

【００１７】

ディスプレイ１６０は、高精細テレビジョンディスプレイ、モニタ又はデジタルビデオ信号を処理できる他の装置を備えていてもよい。制御ユニット１７０は、第２の伝送媒体１２０を介して通信を行うことができる。制御ユニット１７０を用いて、コンテンツ配信システム１００のコンポーネントの一部又はそれぞれの動作を調整及び制御することができる。

【００１８】

第２の加入者端末装置１８０は、住居内、事務所又は他の任意の設備内に設置された様々なコンポーネントへのデータの再伝送をサポートするホームエンターテインメントネットワークの一部であってもよい。

【００１９】

ここでは、加入者端末装置１１０には、ＤＲＭ機能を有するデジタルデバイス１１５が埋め込まれているが、分離型安全管理アーキテクチャに基づいて、加入者端末装置１１０を構成してもよい。ここでは、加入者端末装置１１０にデジタルデバイス１１５が実現された着脱可能なスマートカードを挿入して使用するような構成としてもよい。

【００２０】

図２Ａに示すように、加入者端末装置１１０は、供給される情報２００、すなわち、デジタルコンテンツに含まれるプログラムデータ２１０を処理するデジタルデバイス１１５を備える。「プログラムデータ」２１０は、少なくとも（１）システム情報２２０と、（２）デジタルコンテンツ２３０、すなわち画像、ドキュメント（ウェブページ、英数字テキスト等）、オーディオ、ビデオ又はこれらの任意の組合せとを含む。デジタルコンテンツ２３０は、スクランブルされていてもよく、クリアなフォーマットであってもよい。更に、本発明の一実施の形態では、プログラムデータ２１０は、権利付与制御メッセージ（Entitlement Control Message：ＥＣＭ）２４０及び／又は権利付与管理メッセージ（ＥＭＭ）２５０を含んでいてもよい。

【００２１】

プログラムデータが供給されると、図２Ｂに例示的に示すようなデータ伝送の順序で、システム情報２２０が処理される。「システム情報」２２０には、番組名２２２、放送時刻２２４、コンテンツソース２２６、必要な復号アルゴリズム２２８、アクセス基準２６０等の情報を含ませることができる。「アクセス基準」２６０は、デジタルコンテンツ２３０の再生、再伝送及び／又は記録の手法及び日時等に関して、デジタルデバイス１１５及び他のコンポーネント（例えば、図１に示すオーディオシステム１３０、デジタルＶＣＲ１４０、ハードディスク記録ユニット１５０、ディスプレイ１６０）を制御する情報（本明細書では、「アクセス要求」と呼ぶ。）である。包括的に言えば各アクセス要求は、加入者端末装置１１０が特定の処理を実行する権限を有しているかを決定する制約的なパ

ラメータである。

【００２２】

実例として、第１のアクセス要求は、Ｘ＞１として、デジタルコンテンツ２３０を「Ｘ」回再生できることを示していてもよい。第２のアクセス要求は、デジタルコンテンツ２３０が、所定の期間のみ再生できるペイパープレイ（pay per play：ＰＰＰ）又はペイパービュー（pay per view：ＰＰＶ）用のスクランブルされたデジタルコンテンツであることを示していてもよい。第３のアクセス要求は、デジタルコンテンツ２３０を記録できない（記録「０」回）」又は「Ｘ」回だけ記録できることを示していてもよい。

【００２３】

これに代えて、通常、特定のチャンネル又はサービスへのアクセスを規制するために用いられるＥＣＭ２４０の一部として又はＥＣＭ２４０と共に、アクセス要求２６０を送信してもよい。ＥＣＭ２４０は、供給されるスクランブルされたデジタルコンテンツをデスクランブルするためのキー（例えば、制御ワード）を含んでいてもよい。

【００２４】

ＥＭＭ２５０を用いて、デジタルデバイス１１５にアクセス権（「権利情報」とも呼ぶ。）２７０を配信してもよい。権利情報２７０には、例えば、以下に限定されるものではないが、キー、デジタル証明書、加入者端末装置１１０の再生、再伝送、記録機能を指定するアクセスパラメータ等も含まれる。通常ＥＭＭ２５０は、デジタルコンテンツ２３０より先に受信され、（図に示すように）帯域内で伝送してもよく、又は、例えば、側波帯チャンネルを介して、帯域外で伝送してもよい。これらの権利情報２７０は、対応するデジタルコンテンツ２３０の受信の前にダウンロードしてもよい。

【００２５】

もちろん、他の制御情報２８０をＥＭＭ２５０に含ませてもよい。例えば、ＥＭＭ２５０の他の制御情報２８０は、加入者端末装置１１０の特定の種類及び／又は製造業者を示すビット値であるリムーバブルデバイス識別子（ＩＤ）を含んでいてもよい。また、ＥＭＭ２５０の制御情報２８０は、ＥＭＭ２５０のデータ長を示すビット値であるレングスフィールドを含んでいてもよい。更に、ＥＭＭ２５０の制御情報２８０は、１つ以上のＥＭＭ２５０のキーが不当に変更されていないことを確認するために署名されるマルチビット権利タグ値であるキー識別子を含んでいてもよい。

【００２６】

ＥＭＭ２５０の制御情報２８０は、更に、デジタルデバイス１１５の製造業者を特定する所定の値（例えば、１６ビット等の１つ以上のビット）である製造業者識別子（製造業者ＩＤ）、コンテンツ配信システムプロバイダ及び選択された伝送方式（例えば、要求されたプログラムデータを供給するケーブル、衛星、地上波、インターネット）を特定する値であるサービスプロバイダＩＤ、ＣＡ制御システムのプロバイダを特定する値である限定受信（ＣＡ）プロバイダＩＤ、又は、キーの長さが２つ以上のパケットに亘る場合、情報のパケットを並べ替えるために用いられ、及びある方式では、様々な制御情報の期限を示すためにも用いることができるシーケンス番号等のうちの１つ以上を含んでいてもよい。

【００２７】

加入者端末装置１１０は、スクランブルされたフォーマットのデジタルコンテンツ２３０を受信した場合、プログラムデータ２１０内のアクセス要求２６０と、加入者端末装置１１０が実際に有している権利情報２７０とを比較する。このような比較は、後に詳細に説明するように、デジタルデバイス１１５内で実行される。

【００２８】

本発明の一実施の形態においては、例えば、加入者端末装置１１０にスクランブルされたコンテンツをクリアな形式で表示するために、デジタルコンテンツ２３０に関連しているアクセス要求２６０と、以前に加入者端末装置１１０に割り当てられている権利情報２７０とが比較される。権利情報２７０は、例えば、ホームボックスオフィス（Home Box Office：ＨＢＯ）等の所定のコンテンツプロバイダからのコンテンツを視聴／再生する権

利を加入者端末装置１１０が有していることを示すものであってもよい。また、権利情報２７０は、デジタルコンテンツをデスクランブルするために必要な１つ以上のキーを含んでいてもよい。権利情報２７０は、加入者端末装置１１０がデジタルコンテンツ２３０をデスクランブルすることができる期間を定義してもよい。

【００２９】

このように、一実施の形態では、デジタル権利管理（ＤＲＭ）機能によって、アクセス要求２６０及び権利情報２７０を用いて、デジタルデバイス１１５が特定の番組を視聴することを許可されているかを判定する。この例示的な実施の形態では、例えば、テレビジョン放送され、又は購入された映画等のオーディオ／ビジュアルコンテンツを再生するメカニズムを説明しているが、本発明は、オーディオのみ又は画像のみのコンテンツ（例えば、デジタル化された音楽ファイル、デジタルピクチャ等）のデスクランブルにも適用できる。

【００３０】

図３に示すように、コンテンツ配信システム１００の詳細な例示的な実施の形態は、一方向又は双方向のネットワーク３２０を介して、加入者端末装置１１０及び通信するヘッドエンドサーバ（又は「ヘッドエンド」３１０）を備える。

【００３１】

本発明の実施の形態では、ヘッドエンド３１０は、デコーダとして動作する加入者端末装置１１０のデジタルデバイス１１５に関する全ての権利を保守する。また、他の実施の形態によって権利を保守することもできる。

【００３２】

ヘッドエンド３１０は、例えば、デジタルデバイス１１５内に保存され又はデジタルデバイス１１５によって生成されたルートキー３５０を用いて、暗号化ロジック２４０によって暗号化された１つ以上の（Ｎ個の）サービスキー３３０_{1}～３３０_{N}である権利情報を配信する。このルートキー３５０は、例えば、１つ以上のキー、デジタルコンテンツ２３０の一部、後述する固有キー、又はこれらの任意の組合せ等の情報の集合に基づいて決定される「ルートキー」であってもよい。説明を明瞭にするために、サービスキー３３０_{1}～３３０_{N}を包括的に「サービスキー（Service Key）」又は「ＳＫ」３３０と呼ぶこととする。サービスキー３３０は、ルートキー３５０を用いて暗号化され（「Ｅ（ＳＫ）３３５」と表す）、ネットワーク３２０を介して、加入者端末装置１１０に供給され、ローカルで保存される。

【００３３】

後述するように、サービスキー３３０は、暗号化された形式で保存され、必要に応じて、ストレージからロードされる。このローディングに応じて、デジタルデバイス１１５は、ルートキー３５０、及び例えば、後述するように、デジタルデバイス１１５のストレージ要素に保存されている固有キーを用いて、暗号化サービスキー３３０の何れかを平文化する。

【００３４】

本発明の実施の形態では、デジタルデバイス１１５は、プリント回路カード、マルチチップモジュール、又は単一のチップとして実現してもよい。この実施の形態では、デジタルデバイス１１５は、プロセッサ３６０と、任意のメモリ３７０と、供給されるコンテンツを安全に処理する集積回路（ＩＣ）であるデスクランブラ３８０と、インタフェース３９０とを備える。メモリ３７０は、暗号化サービスキー３３５及び／又はプロセッサ３６０等によって実行されるＤＲＭ機能３７５を保存するために用いてもよい。したがって、メモリ３７０は、不揮発性メモリであっても、揮発性メモリであっても、これらを組み合わせたメモリであってもよい。

【００３５】

一実施の形態では、デスクランブラ３８０は、ストレージ要素４００と、平文化ブロック４１０と、デスクランブルロジック４２０とを備える。デスクランブラ３８０は、プロセッサも、ファームウェアも、ソフトウェアも含まず、すなわち、非プロセッサベースの

デスクランブラであってもよい。すなわち、デスクランブラ３８０内では、ソフトウェア命令もコードも実行されない。暗号の処理（例えば、平文化、ハッシュ処理等）は、平文化ブロック４１０によって実行され、本発明の一実施の形態では、平文化ブロック４１０は、平文化のための単一のキー機能だけを用いるハードウェア回路又は状態マシンとして実現される。本発明の他の実施の形態では、平文化ブロック４１０は、供給されるスクランブルされたコンテンツをデスクランブルする（又はデスクランブルを補助する）ための少なくとも１つのサービスキー３３０$_i$（１＜ｉ＜Ｎ）を再生するためのキー（例えば、ルートキー３５０）を生成するキーのラダー接続を構成する処理ブロックのシーケンスとして実現してもよい（図５Ａ参照）。

【００３６】

１つ以上の固有のキーを、ここでは、「固有キー」４３０と呼び、固有キー４３０は、製造時に、ストレージ要素４００にプログラミングしてもよい。例えば、一実施の形態では、ストレージ要素４００は、一回のみ書込可能なメモリとして、デスクランブラ３８０内に組み込んでもよい。そして、加入者端末装置１１０を製造する際、ストレージ要素４００をプログラミングする。この実施の形態によって、ストレージ要素４００に元々ロードされている固有キー４３０を不正に読み取り、又は上書きすることができなくなる。加入者端末装置１１０のシリアル番号と、固有キー４３０との間の関係をデスクランブラ３８０にロードし、保存して、後にヘッドエンド３１０が使用できるようにしてもよい。

【００３７】

本発明の一実施の形態においては、サービスキー３３０は、コンテンツを直接デスクランブルするためのデスクランブルキーとして使用される。本発明の他の実施の形態においては、サービスキー３３０は、スクランブルされたデジタルコンテンツと共に帯域内で受信され、後のデスクランブルのために用いられる１つ以上のデスクランブルキーを平文化するために用いられる。サービスキー３３０が２つ以上のキーを含む場合、異なる公開暗号アルゴリズム及び秘密暗号アルゴリズムを用いて各サービスキー３３０$_1$～３３０$_N$を暗号化してもよい。これらの異なる専用のアルゴリズムは、複製されたハードウェアを無効化するための、著作権保護のメカニズムであるとみなすことができる。

【００３８】

更に、図３に示すように、ヘッドエンド３１０は、ＥＭＭのチャンネル又は「サービス層」毎に、１つ以上のサービスキー３３０を提供してもよい。サービスキー３３０は、暗号化され、Ｅ（ＳＫ）３３５が生成され、加入者端末装置１１０内に、例えば、メモリ３７０又はプロセッサ３６０のオンチップメモリ内にローカルに保存される。これにより、プロセッサ３６０は、異なるチャンネルを選局する際、必要に応じて、サービスキー３３０を使用することができる。

【００３９】

この実施の形態では、一方向（非ＩＰＰＶの）の放送ネットワークを想定しているが、本発明は、双方向の対話型ネットワークに適用してもよく、この場合、特定のサービス、例えば、ＩＰＰＶ又はＶＯＤ購入又は他の何らかの非購読型サービスのためのサービスキー３３０が要求される。新たなサービスへのアクセスの許可は、ローカルで制御される暗号プロセッサの代わりにヘッドエンド３１０が行うため、特定のサービスキー３３０$_i$を要求するために戻りチャンネル３２１が使用される。

【００４０】

ＩＰＰＶプログラムを同時に大量に購入するために生じるヘッドエンド３１０におけるオーバーロード問題を回避するため、無料プレビュー期間を定め、実際の視聴の前にＩＰＰＶプログラムを販売してもよい。この実施の形態では、加入者端末装置１１０は、個々のショー又は映画毎に、サービスキーを要求でき、これを事前に配信することができる。例えば、ＤＯＣＳＩＳモデム又は帯域外送信機／受信機等の戻りチャンネル３２１を有するケーブルシステム等の対話型ネットワーク（図４参照）では、プログラムキー（ＲＰＫ）メッセージの要求を加入者端末装置１１０からヘッドエンド３１０に送信することができる。これに代えて、加入者端末装置１１０は、アクセスした各プログラムについて、実

時間でサービスキー３３０を要求することもできる。

【００４１】

図４は、ヘッドエンド３１０にサービスキーを要求し、及びサービスキーを受信する図３の加入者端末装置１１０のより詳細な構成を示している。本発明の一実施の形態では、例えば、権利付与制御メッセージ（ＥＣＭ）又は電子番組ガイド（ＥＰＧ）に関連するメタデータ等のプログラムデータ２１０が、コンテンツプロバイダから加入者端末装置１１０に提供される。プログラムデータ２１０は、少なくとも所望のチャンネル又はサービスの識別子（「チャンネル又はサービスＩＤ」と呼ばれる。）を示す。プログラムデータ２１０がＩＰＰＶ又はＶＯＤプログラムである場合、プログラムデータ２１０は、更に、プログラム識別子（ＰＩＤ）を含んでいてもよい。

【００４２】

ＭＰＥＧデマルチプレクサ５１０は、メッセージプロセッサとして動作し、チャンネル又はサービスＩＤを抽出する。チャンネル又はサービスＩＤは、プロセッサ３６０にルーティングされ、プロセッサ３６０は、送信機／受信機ロジックとして動作するインタフェース（以下送信機／受信機ロジックともいう）３９０と協働して、ＲＳＫメッセージを生成し、戻りチャンネル３２１を介してヘッドエンド３１０にルーティングする。

【００４３】

図には示さないが、ヘッドエンドは、ＲＰＫメッセージを処理する。ＲＰＫメッセージは、加入者端末装置１１０のアドレスと、視聴されるチャンネルを特定するために必要な情報とを含んでいてもよい（これらは、全て、モーションピクチャエキスパートグループ「ＭＰＥＧ」システム及び機密保護されていないプロセッサによって既に処理されているプログラム情報から入手される）。ＲＰＫメッセージは、必要ならば、例えば、ＩＰＰＶ又はＶＯＤ要求等のサービス攻撃を防御及び防止するために、暗号化してもよい。

【００４４】

ヘッドエンドは、ＲＰＫメッセージを受信すると、アクセスコントロールリスト（加入者端末装置１１０の各権利情報のリストを示す）にアクセスし、加入者端末装置１１０が、特定のサービスキー（例えば、ＳＫ３３０$_i$）を受け取ることを許可されているかを確認する。これが許可されている場合、ヘッドエンドは、加入者端末装置１１０にＥ（ＳＫ）３３５$_i$（デスクランブラ３８０内のストレージ要素４００に保存されている固有キー４３０に部分的に基づいてルートキー３５０のコピーを用いて暗号化されたＳＫ３３０$_i$）を送信する。

【００４５】

これに応じて、インタフェース３９０は、Ｅ（ＳＫ）３３５$_i$を受信し、プロセッサ３６０にルーティングする。プロセッサ３６０は、Ｅ（ＳＫ）３３５$_i$内部又は外部のメモリ３７０に保存してもよく、ＳＫ３３５$_i$をデスクランブラ３８０に供給し、供給されるスクランブルされたコンテンツを実時間でデスクランブルしてもよい。メモリ３７０は、例えば、Ｅ（ＳＫ）３３５$_i$をローカルで保存することが望ましい場合に用いられる任意の要素である。

【００４６】

Ｅ（ＳＫ）３３５$_i$は、シード情報と共にルートキー３５０を生成し、ルートキー３５０は、ＥＭＭ又は他の制御情報を介して加入者端末装置１１０に供給され、保存される。これらの権利情報は、後に、プロセッサ３６０又はデスクランブラ３８０内で実現される処理ロジックによって処理されるＤＲＭによって、アクセス要求と比較される。ＤＲＭは、メモリ３７０又はプロセッサ３６０のオンチップ内部メモリから実行される。

【００４７】

デスクランブラ３８０は、プログラムデータ２１０のスクランブルされたデジタルコンテンツを受信すると、このデジタルコンテンツをデスクランブルし、このコンテンツがＭＰＥＧフォーマットで圧縮されている場合、このコンテンツは、更にＭＰＥＧデコーダ５２０に供給される。ＭＰＥＧデコーダ５２０は、デジタルコンテンツを伸長し、伸長されたデジタルコンテンツを、ＤＶ端子（ＤＶＩ）リンク又はネットワークインタフェース（

例えば、ＩＥＥＥ１３９４リンク）を介して、テレビジョン受像機に表示するためにデジタル／アナログ（Ｄ／Ａ）コンバータにルーティングする。

【００４８】

図４に示すように、プロセッサ３６０、メモリ３７０、デスクランブラ３８０、送信機／受信機ロジック３９０、ＭＰＥＧデマルチプレクサ５１０及びＭＰＥＧデコーダ５２０は、バス接続又は他の通信方式（例えば、ワイヤ、光ファイバ等）を介して相互接続された２つ以上の集積回路に実装してもよい。これに代えて、これらの全てのコンポーネントを単一の集積回路上に実装してもよい。

【００４９】

この実施の形態では、$SK330_i$は、所定の期間のみ有効である。デジタルデバイス１１５は、ヘッドエンドからネットワークを介して供給された$E(SK)335_i$をメモリ３７０に保存でき、これにより、加入者端末装置１１０は、$SK330_i$が有効な期間内であれば、サービスキーを再び要求することなく、サービスに再アクセスすることができる。

【００５０】

$SK330_i$は、番組の放送期間のみ有効であってもよく、又は選択された期間、例えば、所定の数時間のみ有効であってもよい。より長い期間のキーを用いることによって、$E(SK)330_i$が加入者端末装置１１０のメモリ３７０に保存されれば、このキーを容易に使用できるようになるため、加入者端末装置とヘッドエンドとの間で行われる全体的なトランザクションの数を減少させることができる。現在のサービスキー（例えば、ＳＫ）の期間に応じて、次のサービスキー（SK_{next}）をＳＫと共に配信してもよい。これに代えて、加入者端末装置１１０は、ＳＫの有効期間（例えば、ＳＫの持続期間）が終了したことを検出した後に、SK_{next}を要求してもよい。異なる実施の形態として、加入者の加入期間に亘ってサービスキーを有効にしてもよい。

【００５１】

サービスは、個別に任意に販売してもよく、パッケージとして販売してもよい。これらのサービスは、それぞれがサービスＩＤによって特定される階層的な構造を有していてもよい。例えば、基本的なサービスが提供される基本層と、より多くのサービスを提供する中間層と、異なるプレミアサービスを提供する上位層とを設けてもよい。これらの階層的なサービスの層のそれぞれについて、個別にサービスキーを設定してもよい。

【００５２】

要約すれば、図３及び図４に示すように、図４に示すデジタルデバイス１１５は、デジタルデバイス１１５の製造時又は加入者端末装置の製造時にロードされる固有キー４３０を含むデスクランブラ３８０を備える。ルートキー３５０によって暗号化されたサービスキー330_iである$E(SK)335_i$は、加入者端末装置１１０に供給され、デジタルデバイス１１５に暗号化された形式で保存される。これに代えて、加入者端末装置１１０は、サービスキーをローカルに保存せず、加入者端末装置１１０がチャンネルを選局する都度、サービスキーを要求してもよい。更に、ルートキー３５０を生成するためのシード情報６２０を提供してもよい。

【００５３】

通常、権利情報は、例えば、図３に示すヘッドエンド３１０のキーサーバ等、制御権限を有する機関によって保持される。デジタルデバイス１１５のプロセッサ３６０は、どのデジタルデバイス１１５がデスクランブルを許可されているかを特定するメッセージ（例えば、ＥＣＭ及び／又はＥＭＭ）を受信でき、これにより視聴者に視聴オプションを正しく表示することができる。その後、プロセッサ３６０は、選択されたチャンネルのサービスキーを要求又は生成でき、既に受信され、以前に保存されている権利情報と、加入者端末装置１１０に保存されているアクセス要求とが比較される。

【００５４】

図５Ａは、図３の加入者端末装置１１０内に実現されるデスクランブラ３８０の第１の例示的な実施の形態である。例えば、一連のキー等の制御情報が供給されると、第１の処

理ブロック６１０は、ルートキー３５０を算出する。ルートキー３５０は、後述するように、情報（「シード情報」６２０と呼ばれる。）を編集して生成される。特に本発明の一実施の形態では、ルートキー３５０は、第１の処理ブロック６１０によって、最初にシード情報６２０を処理し、すなわち、固有キー４３０を用いて、一連の暗号化されたキーのシード情報６２０を平文化することによって生成される。これらのキーのそれぞれは、加入者端末装置のグループを表す。平文化（ＤＥＣ）は、ＤＥＳ、ＡＥＳ、ＩＤＥＡ、３ＤＥＳ等の対称キー暗号機能に基づいて実行される。

【００５５】

その後、第２の処理ブロック６３０は、平文化キー６２５に対して、一方向ハッシュ処理を行う。これらのハッシュ処理は、図６Ａ～図６Ｃに示すように、ツリー状のハッシュ構造に基づく。

【００５６】

具体的には、図６Ａに示すハッシュ処理の第１の実施の形態では、平文化キー６２５（キー６２６～６２９）をハッシュ処理し、対応するハッシュ値ＫＥＹＨ１～ＫＥＹＨ４（７００、７０２、７０４、７０６）を生成する。この実施の形態では、説明を明瞭にするため、４個の平文化キー、すなわち、Key_1～Key_4を選択している。なお、キーの数は、これより多くても少なくてもよい。更に、ツリー階層は、ここに示すような２つのハッシュ値に代えて、３つ以上のハッシュ値に基づくハッシュブロック演算を含んでいてもよい。また、キー（又はハッシュ値の和）の数が奇数の場合、対を構成するためにそのキー（又はハッシュ値の和）に、定数を用いてもよい。

【００５７】

ハッシュ値７００、７０２、７０４、７０６の対は、別のハッシュ関数に組み合わされて演算され、ハッシュ値の和ＨＶＳ１（７１０）及びＨＶＳ２（７１２）が算出される。例えば、ＫＥＹＨ１（７００）及びＫＥＹＨ２（７０２）を結合し、ハッシュ処理してＨＶＳ１（７１０）を算出し、ＫＥＹＨ３（７０４）及びＫＥＹＨ４（７０６）を結合し、ハッシュ処理してＨＶＳ２（７１２）を算出する。これに続いて、ＨＶＳ１（７１０）及びＨＶＳ２（７１２）を結合し、ハッシュ処理して、この実施の形態では、ルートキー３５０となる第２のレベルのハッシュ値を生成する。ハッシュ値を「結合する」とは、これらの値に数学的演算を施すことを意味する。数学的演算の具体例としては、連結、剰余加算及び他の演算も含まれる。

【００５８】

他の実施の形態におけるハッシュ処理では、図６Ｂに示すように、ルートキー３５０は、図５Ａの第１の処理ブロックが、最初に、固有キー４３０によって暗号化されている少なくとも１つのキー（例えば、$Key_1$６２６）を平文化することによって生成される。このような平文化は、ストレージ要素４００に初期的に格納されている固有キー４３０を用いて実行される。次に、図５Ａの第２の処理ブロックは、復元されたKey_1（６２６）に一方向ハッシュ処理を実行し、ＫＥＹＨ１（７００）を生成する。このハッシュ処理の速度を最適化するために、ＫＥＹＨ２（７０２）及びＨＶＳ２（７１２）の値を予め算出し、図５Ａの第２の処理ブロック６３０に供給してルートキー３５０を生成してもよい。

【００５９】

本発明の更に他の実施の形態では、図６Ｃに示すように、第２の処理ブロック６３０は、シード値（例えば、$Key_1$６２６）に対し、一方向ハッシュ処理を繰り返し実行することによって、ルートキー３５０を生成する。もちろん、他のメカニズムを用いてルートキー３５０を生成してもよい。

【００６０】

図５Ａに示すルートキー３５０は、第３の処理ブロック６４０にロードされ、デジタルデバイス、特にデスクランブルロジック４２０にロードされたスクランブルされたデジタルコンテンツ２３０をデスクランブルするために用いられるサービスキー３３０を復元するために用いられる暗号化サービスキー３３５を平文化するために用いられる。デスクラ

ンブルロジック４２０は、スクランブルされたコンテンツに３ＤＥＳ演算を実行するように構成してもよい。この演算により、コンテンツは、クリアなフォーマットになり、図４に示すように、デスクランブルロジック４２０からＭＰＥＧデコーダに供給され、又はオプションとして、Ｄ／Ａ変換器、ＤＶＩインタフェース又はＩＥＥＥ１３９４に供給される。

【００６１】

デスクランブラ３８０は、デスクランブルロジック４２０から供給されたデスクランブルされたコンテンツを再暗号化する。デスクランブルされたコンテンツは、暗号化ロジック６５０にロードされ、ルートキー３５０を用いて暗号化される。再暗号化コンテンツは、例えば、第２の加入者端末装置等、コンテンツ配信システムの他のコンポーネントに供給される。

【００６２】

図５Ｂは、図３の加入者端末装置１１０内に実現されるデスクランブラ３８０の第２の例示的な実施の形態を示している。例えば、一連のキー等の制御情報が供給されると、第１及び第２の処理ブロック６１０、６３０は、上述のように、シード情報６２０から、ルートキー３５０を算出する。

【００６３】

ルートキー３５０は、暗号化サービスキー３３５を平文化する第３の処理ブロック６４０ではなく、デスクランブルロジック４２０にロードされ、スクランブルされたデジタルコンテンツ２３０をデスクランブルするために用いられる。デスクランブルロジック４２０は、スクランブルされたコンテンツに３ＤＥＳ演算を実行するように構成してもよい。この演算により、コンテンツは、クリアなフォーマットになり、デスクランブルロジック４２０から、ＭＰＥＧデコーダ、Ｄ／Ａ変換器、ＤＶＩインタフェース又はＩＥＥＥ１３９４等に供給される。

【００６４】

デスクランブラ３８０は、デスクランブルロジック４２０から供給されたデスクランブルされたコンテンツを再暗号化する。デスクランブルされたコンテンツは、暗号化ロジック６５０にロードされ、ルートキー３５０を用いて暗号化される。再暗号化コンテンツは、例えば、第２の加入者端末装置又はコンテンツ配信システムの他のコンポーネントに供給される。

【００６５】

図５Ｃは、図３の加入者端末装置１１０内に実現されるデスクランブラ３８０の第３の例示的な実施の形態を示している。デスクランブラ３８０には、入力を制御する制御情報２８０及び／又はホームキージェネレータ（home key generator：ＨＫＧ）メッセージ６８５が入力される。第１の処理ブロック６６０は、制御情報２８０を処理し、スクランブルされたデジタルコンテンツ２３０をデスクランブルするために用いられるキー６６５を生成する。

【００６６】

本発明の一実施の形態では、制御情報２８０は、（１）デジタルデバイスの製造業者を特定する「製造業者ＩＤ」、（２）コンテンツ配信システムプロバイダ及び選択された伝送方式（例えば、要求されたプログラムデータを供給するケーブル、衛星、地上波、インターネット）を特定する「サービスプロバイダＩＤ」、（３）キーの長さが２つ以上のパケットに亘る場合、情報のパケットを並べ替えるために用いられ、及びある方式では、様々な制御情報の期限を示すためにも用いることができる「シーケンス番号」のうちの１つ以上が含まれる。

【００６７】

ここに示すように、キー６６５は、上述のように、第２の処理ブロック６７０にロードされ、スクランブルされたデジタルコンテンツ２３０をデスクランブルするために用いられるサービスキー６７６を復元するために使用にされる暗号化サービスキー６７５を平文化する。デスクランブルされたコンテンツ６８０は、ディスプレイ装置にルーティングさ

れて表示され、及び再暗号化ロジック６５０に入力される。

【００６８】

同時にデスクランブラ３８０には、入力ＨＫＧメッセージ６８５が入力される。サービスプロバイダＩＤ及び他の可能なデータ（例えば、シーケンス番号、識別子等）から構成されるＨＫＧメッセージ６８５は、第３の処理ブロック６９０によって処理され、デスクランブルされたコンテンツ６８０を再暗号化するためのキー６９２が生成される。ここで、キー６９２は、暗号キーとして暗号化ロジック６５０に供給してもよく、又は、上述のように、第４の処理ブロック６９５にロードし、デスクランブルされたコンテンツ６８０を暗号化するために用いられるキー６９７を復元してもよい。

【００６９】

図７Ａ及び図７Ｂは、図３及び図４のデジタルデバイスのプロセッサ３６０によって実行されるデジタル権利管理（digital rights management：ＤＲＭ）の処理の例示的な実施の形態のフローチャートを示している。この例示的な実施の形態では、ＤＲＭは、プロセッサ３６０の内部メモリ（又はオフチップメモリ）に保存されており、デスクランブラによって処理されるキー生成から独立して、権利情報（例えば、ペイパープレイ／ペイパータイム）を調整する。したがって、デスクランブラとの通信インタフェースが維持されれば、再プログラミング可能であるＤＲＭは、デジタルデバイスのためのメインＣＰＵとして示されているプロセッサ３６０によって処理される。

【００７０】

図７Ａに示すように、まず、加入者がクリアなフォーマットのコンテンツにアクセスするためにＤＲＭが要求されているか否かに関する第１の判定を行う（ステップ８００）。これに該当する場合、コンテンツが再生条件に基づいてアクセスされているか（既に保存されているコンテンツへのアクセス）、ブロードキャスト、マルチキャスト又はユニキャストとして、ソース（例えば、ヘッドエンド）から送信されたコンテンツに基づいているかを判定する（ステップ８０５）。送信されたコンテンツの受信時のＤＲＭ処理は、後述するように、再生時のものと同じであってもよい。或いは、ここに説明するように、ＤＲＭを符号化し、保存されているコンテンツを再生する場合と、伝送媒体を介してコンテンツを受信した場合とで、異なる処理を実行してもよい。

【００７１】

コンテンツが再生条件に基づいてアクセスされる場合、例えば、ＤＲＭ解析を継続し、コンテンツについて、如何なる権利情報が必要であるかを判定する（ステップ８１０、８１５、８２０）。例えば、再生に関するこれらの権利情報には、以下に限定されるものではないが、デジタルコンテンツの再生を制御する情報（例えば、ペイパービュー「ＰＰＶ」権利情報８１０、ペイパープレイ「ＰＰＰ」権利情報８１５、所定の製造業者種類のデジタルデバイス等）が含まれる。

【００７２】

伝送媒体を介して受信したコンテンツにアクセスする場合、例えば、コンテンツがパッケージ又はサービスの他の層の一部であるか、無料プレビューであるか、記録可能であるか、特定のインタフェースのみに出力されるものであるか等、他の種類の権利情報を解析してもよい。

【００７３】

図７Ｂに示す処理では、以前に取得したデジタルコンテンツから、アクセス要求、すなわち、制御情報、例えば、使用の期限及び／又は条件、許可される再生の回数、必要なキー等を入手し、既にロードされている権利情報と比較する（ステップ８５０、８５５）。これらの権利情報には、以下に限定されるものではないが、再生の回数、所有しているキー等が含まれる。

【００７４】

プログラムデータによって提供されるアクセス要求が、プレロードされた権利付与情報と異なっている場合、加入者に対し、適切な権利情報を購入するか否かに関する入力を促す（ステップ８６０、８６５）。具体例として加入者端末装置のディスプレイの画面に、

選択可能なフィールドを有するポップアップメニューを表示することによって、「プロンプト」を実現してもよい。プレロードされた権利情報を購入する場合、加入者は、適切なフィールドを選択し、エンティティ（例えば、ヘッドエンド、コンテンツ配信業者、指定されたキーサーバ等のコンテンツの本来のソース）にメッセージを送信し、加入者のデジタルデバイスに所望の権利情報を受け取る。この処理を行わなければ、アクセスは、拒否される。

【００７５】

一方、アクセス要求と、権利情報とが一致していれば、この権利情報に基づいて、デスクランブル処理が実行される。例えば、権利情報が最大再生数の制限（例えば、再生２回）を指定しており、デジタルコンテンツが未だ１回しか再生されていないことをカウント値が示している場合、残る１回の再生について、デスクランブル処理が実行され、デジタルコンテンツがデスクランブルされる。

【００７６】

具体的には、デスクランブル処理において、例えば、デジタルデバイスにロードされている暗号化フォーマットのキー等の情報の集合を用いて、キー（例えば、ルートキー）が導出される（ステップ８７０）。特にルートキーは、特定の加入者端末装置に固有の固有キーによるデータ暗号化を含む情報から導出される。このキーは、デジタルデバイスにロードされている暗号化されたサービスキーを平文化するように適応化してもよい（ステップ８７５）。この実施の形態では、復元されたサービスキーを用いて、プログラムデータによって提供されるスクランブルされたデジタルコンテンツをデスクランブルする（ステップ８８０）。この他の場合、アクセスは、拒否される。

【００７７】

以上、特定の例示的な具体例を参照して、本発明を説明した。しかしながら、添付の請求の範囲に示す本発明の範囲から逸脱することなく、上述の実施の形態を様々に修正及び変形できることは、明らかである。すなわち、本発明の説明及び図面は例示的なものであり、本発明を限定するために示したものではない。

【図面の簡単な説明】

【００７８】

【図１】加入者端末装置を含むコンテンツ配信システムの第１の例示的な実施の形態を示す図である。

【図２Ａ】図１の加入者端末装置のデジタルデバイスに供給される情報に関連するデータ構造の例示的な実施の形態を示す図である。

【図２Ｂ】図１の加入者端末装置のデジタルデバイスに供給される情報に関連するデータ構造の例示的な実施の形態を示す図である。

【図３】図１のコンテンツ配信システムにおけるヘッドエンドと加入者端末装置との間の通信の実施の形態をより詳細に示す図である。

【図４】図３のデジタルデバイスの例示的な実施の形態を示す図である。

【図５Ａ】図１のデジタルデバイス内に実現されるデスクランブラの第１の例示的な実施の形態を示す図である。

【図５Ｂ】図１のデジタルデバイス内に実現されるデスクランブラの第２の例示的な実施の形態を示す図である。

【図５Ｃ】図１のデジタルデバイス内に実現されるデスクランブラの第３の例示的な実施の形態を示す図である。

【図６Ａ】ルートキーを生成するための処理の第１の例示的な実施の形態を示す図である。

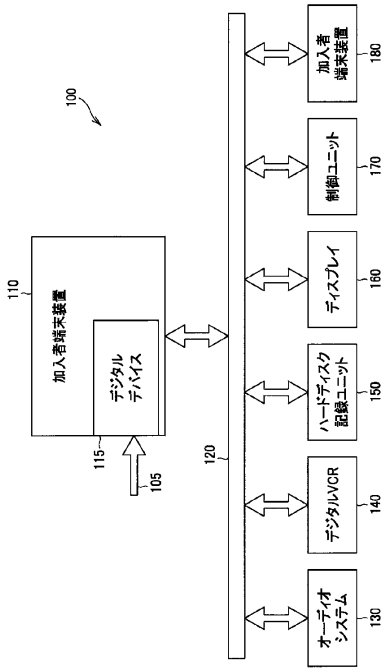
【図６Ｂ】ルートキーを生成するための処理の第２の例示的な実施の形態を示す図である。

【図６Ｃ】ルートキーを生成するための処理の第３の例示的な実施の形態を示す図である。

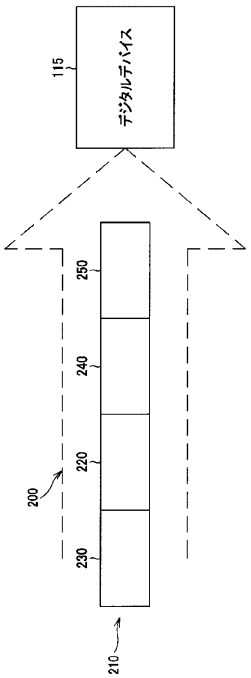
【図７Ａ】図１のデジタルデバイス内の他のコンポーネントと連携するデジタル権利管理

ロジックの処理の例示的なフローチャートである。
【図７Ｂ】図１のデジタルデバイス内の他のコンポーネントと連携するデジタル権利管理ロジックの処理の例示的なフローチャートである。

【図１】



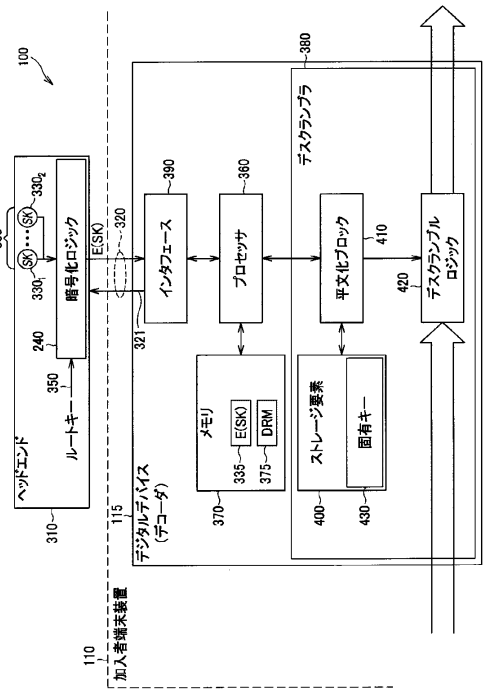
【図２Ａ】



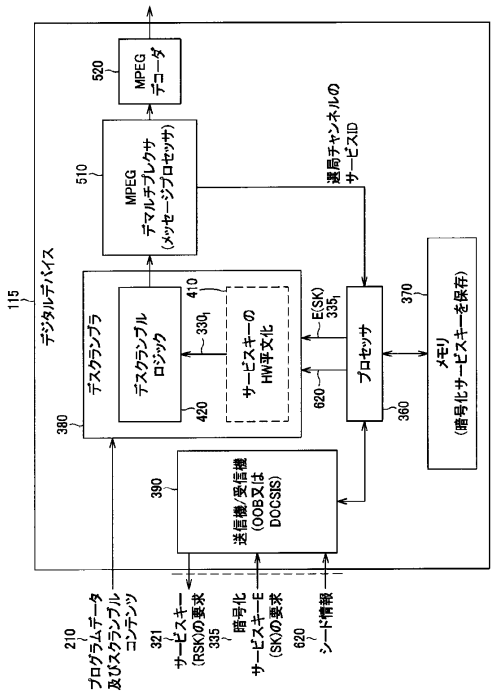
【図２Ｂ】


権利情報
他の制御情報
ECM
番組名
放送時刻
コンテンツソース
復号アルゴリズム
アクセス基準
…
デジタルコンテンツ
270
280
250
222
224
226
228
260
240
220
230

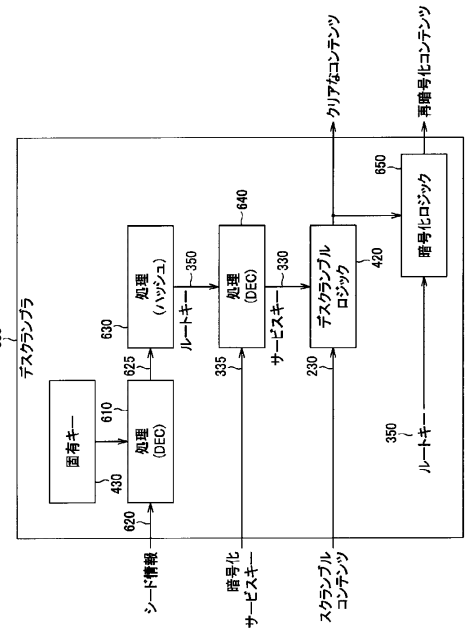
【図３】


100
ヘッドエンド
310
ルートキー
350
240
330
暗号化ロジック
E(SK)
320
321
デジタルデバイス（デコーダ）
115
加入者端末装置
110
インタフェース
390
プロセッサ
360
メモリ
370
E(SK)
335
DRM
375
デスクランブラ
380
ストレージ要素
400
固有キー
430
平文化ブロック
410
デスクランブルロジック
420

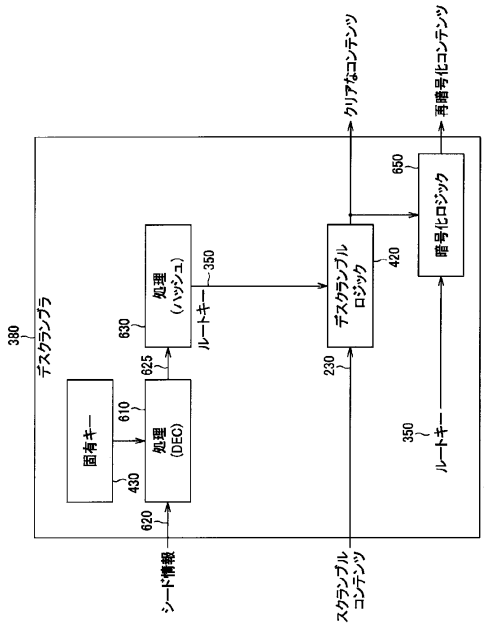
【図４】


210
プログラムデータ及びスクランブルコンテンツ
321
サービスキー（RSKの要求）
335
暗号化サービスキー（SKの要求）
620
シード情報
115
デジタルデバイス
380
デスクランブラ
420
デスクランブルロジック
410
サービスキーのHW平文化
510
MPEG デマルチプレクサ（メッセージプロセッサ）
520
MPEG デコーダ
390
送信機/受信機（OOB又はDOCSIS）
E(SK)
335
620
プロセッサ
360
370
メモリ（暗号化サービスキーを保存）
選局チャンネルのサービスID

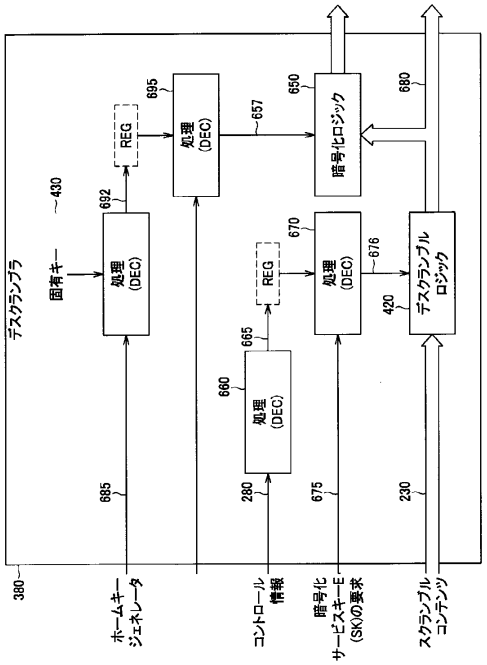
【図５Ａ】


380
デスクランブラ
固有キー
430
処理（DEC）
620
610
シード情報
処理（ハッシュ）
625
630
ルートキー
350
処理（DEC）
640
335
暗号化サービスキー
デスクランブルロジック
420
230
スクランブルコンテンツ
クリアなコンテンツ
暗号化ロジック
650
再暗号化コンテンツ
350
ルートキー

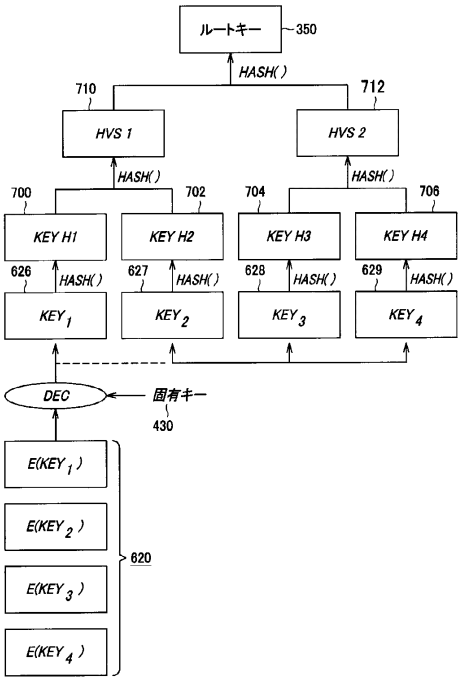
【図５Ｂ】



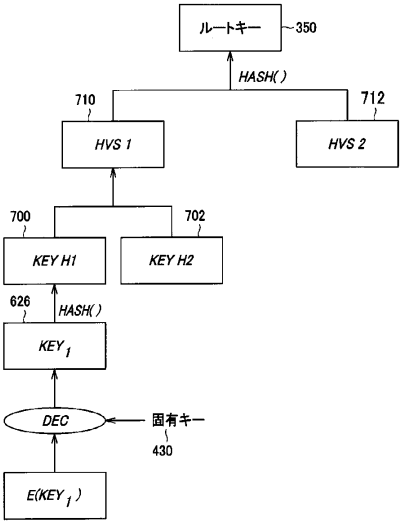
【図５Ｃ】



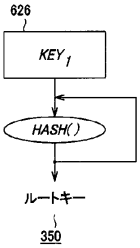
【図６Ａ】



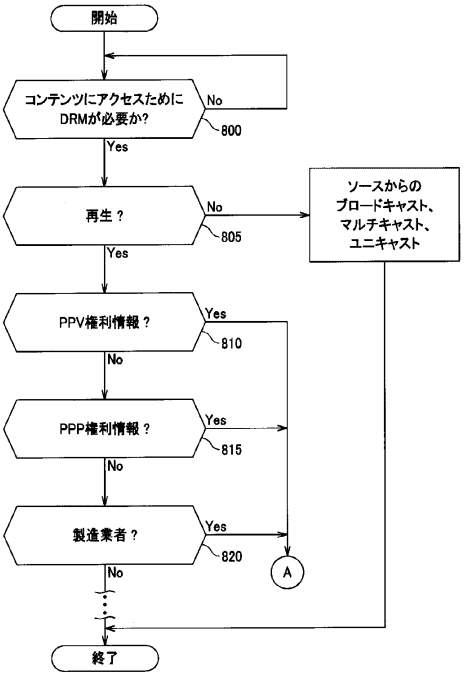
【図６Ｂ】



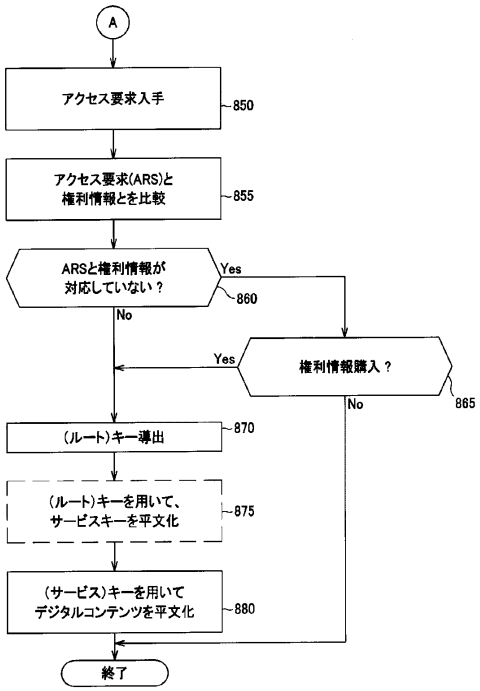
【図６Ｃ】


626
KEY 1
HASH( )
ルートキー
350

【図７Ａ】


開始
コンテンツにアクセスためにDRMが必要か?
No
800
Yes
再生？
No
805
ソースからのブロードキャスト、マルチキャスト、ユニキャスト
Yes
PPV権利情報？
Yes
810
No
PPP権利情報？
Yes
815
No
製造業者？
Yes
820
A
No
終了

【図７Ｂ】


A
アクセス要求入手
850
アクセス要求(ARS)と権利情報とを比較
855
ARSと権利情報が対応していない？
Yes
860
No
Yes
権利情報購入？
No
865
(ルート)キー導出
870
(ルート)キーを用いて、サービスキーを平文化
875
(サービス)キーを用いてデジタルコンテンツを平文化
880
終了

フロントページの続き

(72)発明者　キャンデロール、ブラント、エル.
アメリカ合衆国　カリフォルニア州　９２０２９－６５０２　エスコンディード　クァイル　グレン　ウェイ　１０１２４

審査官　石田　信行

(56)参考文献　特表２００２－５４０７３６（ＪＰ，Ａ）
国際公開第２００４／０４２９９５（WO，Ａ１）
特表２００６－５０６０２９（ＪＰ，Ａ）
特表２００８－５１４１２３（ＪＰ，Ａ）
特表２００３－５１８８４１（ＪＰ，Ａ）
特開平１１－３３１８０５（ＪＰ，Ａ）
特開平１０－１６４０５２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/08
G09C　1/00
H04N　7/167
H04N　7/173
G06Q　50/00