(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-74686
(P2006-74686A)
(43)公開日　平成18年3月16日(2006.3.16)

(51)Int.Cl.		F I			テーマコード（参考）
H04N 7/167	(2006.01)	H04N	7/167	Z	5B017
G06F 21/24	(2006.01)	G06F	12/14	540A	5C025
H04N 5/44	(2006.01)	G06F	12/14	550A	5C064
H04L 9/10	(2006.01)	H04N	5/44	Z	5J104
		H04L	9/00	621Z	

審査請求 未請求　請求項の数 12　ＯＬ　（全 13 頁）

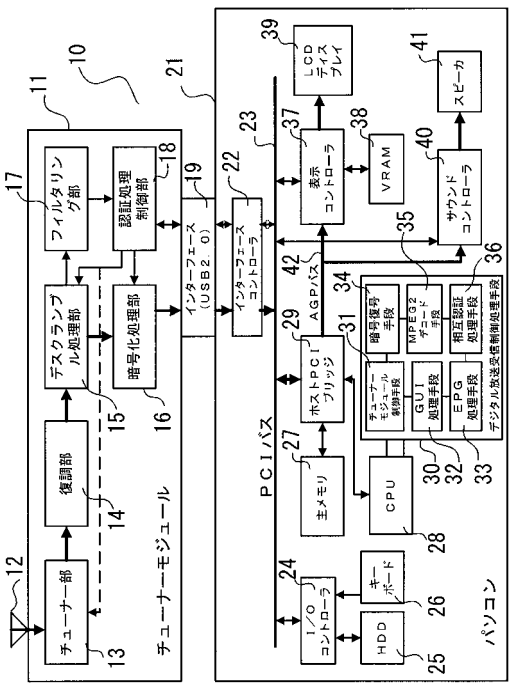
(21)出願番号　特願2004-258610 (P2004-258610)
(22)出願日　平成16年9月6日 (2004.9.6)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100109900
弁理士　堀口　浩
(72)発明者　木村　琢二
東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内

Ｆターム(参考)　5B017 AA06 BA07 BA09 CA16
5C025 BA25 DA01
5C064 BA07 BB02 BC16 BC20 BC22 BD08 BD09
5J104 AA01 AA07 JA03 KA02 KA04 NA02 NA05 NA38 PA05

(54)【発明の名称】チューナーモジュール、デジタル放送受信装置、およびデジタル放送番組コンテンツ保護方法

(57)【要約】
【課題】　デジタル放送から受信した放送番組コンテンツの不正に複製、転送を防止し、著作権を保護するチューナーモジュール、デジタル放送受信装置、およびデジタル放送番組コンテンツ保護方法を提供する。
【解決手段】　デジタル放送受信装置は、チューナーモジュール１１とパソコン２１から構成される。チューナーモジュール１１は、受信したデジタル放送信号を選局、復調、符号誤り訂正して放送番組コンテンツ生成し、暗号化してパソコン２１に伝送する。また、デジタル放送信号に多重化されている認証パラメータを用いてパソコン２１と相互認証を行う。この認証パラメータの更新することにより、相互認証不成立とし、放送番組コンテンツの伝送を停止して、放送番組コンテンツの不正な受信を排除し、著作権の保護を図る。
【選択図】　図１



【特許請求の範囲】
【請求項１】
電子機器と接続して使用されるデジタル放送受信のチューナーモジュールであって、
受信したデジタル放送信号を選局するチューナー部と、
前記チューナー部で選局したデジタル放送信号を復調してトランスポート・ストリームを生成する復調部と、
前記トランスポート・ストリームからコンテンツ保護あるいは限定受信のために放送番組コンテンツに施されているスクランブルを解除するデスクランブル処理部と、
前記トランスポート・ストリームに多重化されている認証パラメータを抽出する手段と、
前記電子機器との間で前記認証パラメータを用いて相互認証する手段と、
前記デスクランブル処理部から出力されたトランスポート・ストリームの放送番組コンテンツを暗号化する手段と、
暗号化した前記放送番組コンテンツを前記電子機器に伝送するインターフェースとを具備し、
前記電子機器との相互認証の結果に基づいて、前記放送番組コンテンツの伝送を制御することを特徴とするチューナーモジュール。
【請求項２】
デジタル放送信号を受信するチューナーモジュールと電子機器とがインターフェースを介して接続される構成のデジタル放送受信装置において、
前記チューナーモジュールは、チューナー部で選局したデジタル放送信号を復調してトランスポート・ストリームを生成する復調部と、
前記トランスポート・ストリームから、コンテンツ保護あるいは限定受信のために放送番組コンテンツに施されているスクランブルを解除するデスクランブル処理部と、
前記トランスポート・ストリームに多重化されている認証パラメータを抽出する手段と、
前記電子機器との間で前記認証パラメータを用いて相互認証する手段と、
前記デスクランブル処理部から出力されたトランスポート・ストリームの放送番組コンテンツを暗号化する手段と、
暗号化した前記放送番組コンテンツを前記インターフェースを介して前記電子機器へ伝送する手段とを具備し、
前記電子機器は、前記チューナーモジュールと相互認証する手段と、
前記チューナーモジュールから前記インターフェースを介して、暗号化された前記放送番組コンテンツを受信する手段と、
前記暗号化された放送番組コンテンツの暗号を解除する手段と、
前記暗号を解除する手段から出力された放送番組コンテンツから映像、音声を復号する手段と、
前記映像、音声を復号する手段からの出力を表示装置およびスピーカに出力する手段とを具備し、
前記チューナーモジュールと前記電子機器は、相互認証を行い、前記相互認証の結果に基づいて、前記チューナーモジュールから前記電子機器への前記放送番組コンテンツの伝送を制御することを特徴とするデジタル放送受信装置。
【請求項３】
前記チューナーモジュールと前記電子機器の間で行う相互認証において、
前記チューナーモジュールは、前記認証パラメータから生成される第１の認証用パラメータを、前記電子機器は、あらかじめ保持している第２の認証用パラメータを用いることを特徴とする請求項２に記載のデジタル放送受信装置。
【請求項４】
前記チューナーモジュールと前記電子機器の間での相互認証の手順にて、前記インターフェースに伝送する放送番組コンテンツの暗号化鍵を共有し、前記暗号化鍵を用いて、放送番組コンテンツを暗号化することを特徴とする請求項２に記載のデジタル放送受信装置。

【請求項５】
前記トランスポート・ストリームに多重化されている認証パラメータが更新された場合、前記チューナーモジュールは、前記第１の認証用パラメータを更新し、前記第１の認証パラメータを用いて前記電子機器との相互認証を行った結果、認証が成立しなかった場合には、放送番組コンテンツの前記インターフェースでの伝送を停止して、前記電子機器からの放送番組コンテンツの視聴を制限することを特徴とする請求項３に記載のデジタル放送受信装置。
【請求項６】
前記電子機器は、前記デジタル放送受信ソフトウェアのアップデートを促す情報を前記表示装置およびスピーカから出力する手段を具備し、
前記相互認証の結果、認証が成立しなかった場合には、前記電子機器から前記デジタル放送受信ソフトウェアのアップデートを促す情報を出力することを特徴とする請求項２に記載のデジタル放送受信装置。
【請求項７】
デジタル放送信号を受信するチューナーモジュールと電子機器がインターフェースを介して接続される構成のデジタル放送受信装置において、
前記デジタル放送信号を選局、復調、誤り訂正したトランスポート・ストリームから、多重化された認証パラメータを抽出する手段と、
放送に多重された受信制御情報から、前記デジタル受信装置での放送番組コンテンツの受信を制限させられた、あるいは、制限させられることが予定されていることを検出する検出手段と、
前記電子機器が、前記検出手段の結果により、搭載されているデジタル放送受信ソフトウェアのアップデートを促す情報を出力する手段と、
を具備することを特徴とするデジタル放送受信装置。
【請求項８】
前記トランスポート・ストリームに多重化されている共通制御情報あるいは個別制御情報内のパラメータを調べることにより、放送番組コンテンツの伝送を停止させた、あるいは、停止させることが予定されていることを検出することを特徴とする請求項７に記載のデジタル放送受信装置。
【請求項９】
放送局から送信されるデジタル放送信号に認証パラメータを多重化する手段と、
受信したデジタル放送信号から多重化された認証パラメータを抽出する手段と、
前記認証パラメータを用いて、チューナーモジュールと電子機器との間で相互認証を行う手段と、
受信した放送番組コンテンツを暗号化して、前記電子機器に伝送する手段と、
前記相互認証の結果により前記電子機器への伝送を制御する制御手段とを備えたデジタル放送システムに係るデジタル放送番組コンテンツ保護方法において、
前記放送局が前記認証パラメータを定期的に、あるいは必要に応じて更新することで、前記チューナーモジュールと前記電子機器の間の相互認証の成立を制御し、
前記相互認証が成立しない場合には、前記チューナーモジュールは、前記放送番組コンテンツの前記電子機器への伝送を停止することを特徴とするデジタル放送番組コンテンツ保護方法。
【請求項１０】
前記電子機器に搭載されているデジタル放送受信ソフトウェアのアップデートを促す情報を出力する手段を具備し、
前記相互認証が成立しなかった場合には、前記デジタル放送受信ソフトウェアのアップデートを促す情報を出力する手段の指示に従って、更新された認証パラメータに対応したより耐タンパ性の高いデジタル放送受信ソフトウェアにアップデートすることで、前記相互認証を成立させることを特徴とする請求項９に記載のデジタル放送番組コンテンツ保護方法。

【請求項１１】
前記相互認証が成立した場合、前記認証パラメータを用いて、前記チューナーモジュールと前記電子機器との間で暗号化鍵の生成および共有を行い、
前記チューナーモジュールは、前記暗号化鍵を用いて、受信した放送番組コンテンツを暗号化して前記電子機器に伝送し、
前記電子機器は前記暗号化鍵を用いて放送番組コンテンツを復号することを特徴とする請求項９に記載の放送番組コンテンツ保護方法。
【請求項１２】
送出するデジタル放送信号に多重化する共通制御情報あるいは個別制御情報内に、前記デジタル放送受信装置での相互認証を不成立にする情報、もしくは相互認証の不成立が予定されている情報を付加し、
前記チューナーモジュールは前記相互認証手順の中で、前記視聴制限に関する情報を前記電子機器に伝送し、
前記電子機器は、前記視聴制限に関する情報を受信した場合には、前記電子機器に搭載されているデジタル放送受信ソフトウェアのアップデートを促す情報を出力することを特徴とする請求項９に記載のデジタル放送番組コンテンツ保護方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子機器と接続して使用するチューナーモジュール、デジタル放送受信装置、およびデジタル放送番組コンテンツ保護方法に関する。
【背景技術】
【０００２】
近年、パーソナルコンピュータ（以下、パソコンと云う）は、高度なＡＶ（Ａｕｄｉｏ Ｖｉｓｕａｌ）機能を搭載しており、ＴＶ放送受信用のチューナーモジュールをパソコンに接続することで、パソコンのＬＣＤディスプレイ上に放送番組コンテンツを表示させて視聴したり、放送番組コンテンツをＨＤＤに録画することが一般的になっている。また、ＴＶ放送はアナログ放送からデジタル放送に移行しており、パソコンに接続して使用されるチューナーモジュールも、デジタル放送用が望まれている。
【０００３】
ところが、デジタル放送では、放送番組コンテンツがデジタル化されて伝送、処理されることから、その画質や音声に劣化が殆どなく、その複製が容易であり、不正に複製、転送されて著作権が侵害される虞がある。一般的にパソコンは、外部機器とも容易に接続できるＵＳＢ２．０、ＰＣＩバスなどの汎用インターフェースを備えていること、およびソフトウェアも自由に選択して搭載することができることから、受信した放送番組コンテンツを不正に複製、転送される危険性が高いと云える。
【０００４】
従って、放送番組コンテンツの著作権の保護の対策として、チューナーモジュールをパソコン等の汎用インターフェースに接続して放送番組コンテンツを受信する場合、汎用インターフェース上を伝送する放送番組コンテンツ、およびＨＤＤなどに録画する放送番組コンテンツを暗号化したり、パソコンに搭載されるデジタル放送受信用ソフトウェアには、不正な改ざんが行われないように耐タンパ性を持たせることが要求される（例えば、特許文献１参照）。
【０００５】
従来のデジタル放送受信装置の構成を図７に示す。デジタル放送受信装置１００は、パソコン１２０とこのパソコン１２０に接続されたチューナーモジュール１０１から構成されている。アンテナ１０３からのデジタル放送信号は、チューナー部１０４に入力される。チューナー部１０４は、選局、復調、および符号誤り訂正を行い、トランスポート・ストリームを生成して、デスクランブル処理部１０５に入力する。デスクランブル処理部１０５は、トランスポート・ストリームに有料放送限定受信用に掛けられているスクランブ

ルを解除し、放送番組コンテンツを生成する。この放送番組コンテンツは、暗号化部１０６に入力されて暗号化された後、ＰＣＩバス１２１を介して、パソコン１２０に送付される。また、周辺制御部１０８は、ＣＡＳ（Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ）方式のＩＣカード１１０からＩＣカードＩ／Ｆ部１０９を介して、暗号化鍵を取得し、暗号化部１０６に出力する。暗号化部１０６は、この暗号化鍵を用いて放送番組コンテンツを暗号化する。

【０００６】

パソコン１２０が受け取った暗号化された放送番組コンテンツは、デジタル放送受信制御処理手段１２６の一つである暗号復号処理手段１２９にて暗号が復号され、ＭＰＥＧ２デコード手段１３１にてデコードされる。デコードされた放送番組コンテンツの映像データは表示コントローラ１３２に出力され、変換されてＬＣＤディスプレイ１３４に表示される。また、デコードされた放送番組コンテンツの音声データはサウンドコントローラ１３５にてＤ／Ａ変換され出力されて、スピーカ１３６を鳴動させる。

【特許文献１】特開２００１－４５４３２号公報（第７頁、図２）

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、従来のデジタル放送受信装置においては、耐タンパ性を備えたデジタル放送受信用ソフトウェアであっても、パソコンのようなオープンなアーキテクチャーで動作するソフトウェアあるかぎり改ざんされる危険性がある。デジタル放送受信用ソフトウェア内の暗号化鍵等が解読され、放送番組コンテンツの複製や公衆回線への転送等、不正に利用された場合、特定のデジタル放送受信用ソフトウェアがハッキング、改ざんされたことを察知しても、直ぐに放送番組の受信動作を停止させるなどの対策手段が無いという問題があった。

【０００８】

本発明は、上記問題を解決するためになされたものであり、あらかじめデジタル放送信号にインターフェースを介して接続される機器間の認証に用いるパラメータを多重化しておき、この認証パラメータをもとに、チューナーモジュールとパソコン本体の間で相互認証を行い、認証の結果によりチューナーモジュールからパソコン本体への放送番組コンテンツの伝送を制御することにより、放送局側で直ちに不正な利用がなされているデジタル放送受信装置の番組受信を排除することができる。このための放送番組コンテンツの著作権を保護するチューナーモジュール、デジタル放送受信装置およびデジタル放送番組コンテンツ保護方法を提供するものである。

【課題を解決するための手段】

【０００９】

上記の課題を解決するため、本発明によるチューナーモジュールは、電子機器と接続して使用されるデジタル放送受信のチューナーモジュールであって、受信したデジタル放送信号を選局するチューナー部と、前記チューナー部で選局したデジタル放送信号を復調してトランスポート・ストリームを生成する復調部と、前記トランスポート・ストリームからコンテンツ保護あるいは限定受信のために放送番組コンテンツに施されているスクランブルを解除するデスクランブル処理部と、前記トランスポート・ストリームに多重化されている認証パラメータを抽出する手段と、前記電子機器との間で前記認証パラメータを用いて相互認証する手段と、前記デスクランブル処理部から出力されたトランスポート・ストリームの放送番組コンテンツを暗号化する手段と、暗号化した前記放送番組コンテンツを前記電子機器に伝送するインターフェースとを具備し、前記電子機器との相互認証の結果に基づいて、前記放送番組コンテンツの伝送を制御することを特徴とする。

【００１０】

また、本発明によるデジタル放送受信装置は、デジタル放送信号を受信するチューナーモジュールと電子機器とがインターフェースを介して接続される構成のデジタル放送受信装置において、前記チューナーモジュールは、チューナー部で選局したデジタル放送信号

を復調してトランスポート・ストリームを生成する復調部と、前記トランスポート・ストリームから、コンテンツ保護あるいは限定受信のために放送番組コンテンツに施されているスクランブルを解除するデスクランブル処理部と、前記トランスポート・ストリームに多重化されている認証パラメータを抽出する手段と、前記電子機器との間で前記認証パラメータを用いて相互認証する手段と、前記デスクランブル処理部から出力されたトランスポート・ストリームの放送番組コンテンツを暗号化する手段と、暗号化した前記放送番組コンテンツを前記インターフェースを介して前記電子機器へ伝送する手段とを具備し、前記電子機器は、前記チューナーモジュールと相互認証する手段と、前記チューナーモジュールから前記インターフェースを介して、暗号化された前記放送番組コンテンツを受信する手段と、前記暗号化された放送番組コンテンツの暗号を解除する手段と、前記暗号を解除する手段から出力された放送番組コンテンツから映像、音声を復号する手段と、前記映像、音声を復号する手段からの出力を表示装置およびスピーカに出力する手段とを具備し、前記チューナーモジュールと前記電子機器は、相互認証を行い、該相互認証の結果に基づいて、前記チューナーモジュールから前記電子機器への前記放送番組コンテンツの伝送を制御することを特徴とする。

【００１１】

さらに、本発明によるデジタル放送受信装置は、デジタル放送信号を受信するチューナーモジュールと電子機器がインターフェースを介して接続される構成のデジタル放送受信装置において、前記デジタル放送信号を選局、復調、誤り訂正したトランスポート・ストリームから、多重化された認証パラメータを抽出する手段と、放送に多重された受信制御情報から、前記デジタル受信装置での放送番組コンテンツの受信を制限させられた、あるいは、制限させられることが予定されていることを検出する検出手段と、前記電子機器が、前記検出手段の結果により、搭載されているデジタル放送受信ソフトウェアのアップデートを促す情報を出力する手段と、を具備することを特徴とする。

【００１２】

さらにまた、本発明による放送番組コンテンツ保護方法は、放送局から送信されるデジタル放送信号に認証パラメータを多重化する手段と、受信したデジタル放送信号から多重化された認証パラメータを抽出する手段と、前記認証パラメータを用いて、チューナーモジュールと電子機器との間で相互認証を行う手段と、受信した放送番組コンテンツを暗号化して、前記電子機器に伝送する手段と、前記相互認証の結果により前記電子機器への伝送を制御する制御手段とを備えたデジタル放送システムに係るデジタル放送番組コンテンツ保護方法において、前記放送局が前記認証パラメータを定期的に、あるいは必要に応じて更新することで、前記チューナーモジュールと前記電子機器の間の相互認証の成立を制御し、前記相互認証が成立ない場合には、前記チューナーモジュールは、前記放送番組コンテンツの前記電子機器への伝送を停止することを特徴とする。

【発明の効果】

【００１３】

本発明によれば、放送局がデジタル放送信号に多重化する認証パラメータを更新することにより、電子機器とそれに接続されたチューナーモジュール間の相互認証の成立を制御することができ、これにより番組コンテンツの不正な利用が発覚した放送受信装置の番組受信を排除することが可能となり、放送番組コンテンツの著作権を保護することができる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の実施例を説明する。

【実施例】

【００１５】

以下、本発明によるチューナーモジュール、デジタル放送受信装置、およびデジタル放送番組コンテンツ保護方法の実施例について図１乃至図６を用いて説明する。なお、本発明は、以下の実施例に限定されるものではない。

【００１６】
図１は本発明の実施例に係るブロック図である。本発明の実施例に係わるデジタル放送受信装置は、パソコン（請求項に記載の電子機器の一実施例）２１とこのパソコン２１に接続して使用されるチューナーモジュール１１から構成されている。チューナーモジュール１１は、アンテナ１２から入力されたデジタル放送信号を選局するためのチューナー部１３と、このチューナー部１３により選局された信号を復調し、誤り符号訂正する復調部１４と、この復調部１４により復調された信号のスクランブルを解除するデスクランブル処理部１５と、このデスクランブル処理部１５によりスクランブル解除された信号を暗号化する暗号化処理部１６と、この暗号化処理部１６により暗号化された信号をパソコン２１へ伝送するインターフェース１９とを備えている。また、デジタル放送信号から認証パラメータを含むＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅ、個別制御情報）パケットなどを取り出すフィルタリング部１７と、接続されたパソコン２１との相互認証を処理する認証処理制御部１８を備えている。

【００１７】
パソコン２１は、ＣＰＵ２８、主メモリ２７、ホストＣＰＵブリッジ２９、Ｉ／Ｏコントローラ２４、ＨＤＤ２５、キーボード２６、インターフェースコントローラ２２、ＰＣＩバス２７、およびＡＧＰバス４２などの構成を備えている。また、ＬＣＤディスプレイ（請求項に記載の表示装置の一実施例）３９に放送番組コンテンツなどを表示させる表示コントローラ３７と、表示データを記憶するＶＲＡＭ３８と、スピーカ４１を鳴動させるためのサウンドコントローラ４０を備えている。また、パソコン２１に搭載されたデジタル放送受信ソフトウェアに従って、ＣＰＵ２１は、チューナーモジュール１１から受け取った暗号化された信号を復号する暗号復号手段３４と、この復号した信号をデコードするＭＰＥＧ２デコード手段３５と、チューナーモジュール１１と相互認証する相互認証処理手段３６と、ＥＰＧ（放送番組ガイド）処理手段３３と、チューナーモジュール制御手段３１と、ＧＵＩ（グラフィック・ユーザー・インターフェース）処理手段３２などから構成されるデジタル放送受信制御処理手段３０を備えている。

【００１８】
以下に本実施例の動作を図１を参照し、さらに詳しく説明する。アンテナ１２は、放送局あるいは放送衛星から送られてくるデジタル放送の電波を受信して、チューナー部１３に送出する。チューナー部１３は、その入力を中間周波数に変換し、ユーザーの視聴するチャンネルを選局し、選局した信号を復調部１４に送出する。復調部１４は、その信号をＡ／Ｄ変換し、ＱＰＳＫ（Ｑｕａｒｄｒａｔｕｒｅ Ｐｈａｓｅ Ｓｈｏｆｔ Ｓｅｙｉｎｇ）方式で変調されている信号を復調し、伝送経路等で発生した符号誤りを訂正して、ＭＰＥＧ２規格に準拠したトランスポート・ストリームを生成し、デスクランブル処理部１５に送出する。デスクランブル処理部１５は、このトランスポート・ストリームに有料放送番組の不正な視聴を防止して正規のユーザーのみが受信できるようにする受信限定方式によるスクランブルが施されている場合、このトランスポート・ストリームのスクランブルを解除する。なお、スクランブルの解除は、ＣＡＳ（Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ）方式のＩＣカードなどを使用して、正規のユーザーであることを認証し、スクランブル解除鍵を作成し、その解除鍵により、トランスポート・ストリームのスクランブルを解除し、有料放送番組の受信と視聴ができるようになっている。

【００１９】
暗号化処理部１６は、スクランブルが解除されたトランスポート・ストリームを暗号化し、汎用のインターフェース１９（実施例ではＵＳＢ２．０）を介して、パソコン２１に伝送する。放送番組コンテンツを含むトランスポート・ストリームを暗号化して後、インターフェース１９に伝送することにより、もし、インターフェース１９上のデータが盗み取られたとしても、暗号化されているため、不正な視聴や複製を防ぐことができる。

【００２０】
フィルタリング部１７は、トランスポート・ストリームに多重化されているＥＭＭパケットを取り出して、認証処理制御部１８に送出する。認証処理制御部１８は、ＥＭＭパケ

ットから認証パラメータを取得する。また、認証処理制御部１８は、この認証パラメータを用いて、パソコン２１との間で、相互認証処理と行い、伝送する放送番組コンテンツを暗号化するための暗号化鍵の共有を行う。相互認証が成立した場合、暗号化鍵を暗号化処理部に送出し、暗号化した放送番組コンテンツをパソコン２１に伝送することを許可する。

【００２１】

一方、相互認証が成立しない場合、チューナーモジュール１１は、放送番組コンテンツをパソコン２１に伝送することを停止し、パソコン２１は、デジタル放送受信用ソフトウェアのアップデートをユーザーに促す。なお、詳細な説明は省略するが認証処理制御部１８では、チューナーモジュール１１全体の制御等もあわせて行っている。

【００２２】

以下に、パソコン２１の動作を説明する。ユーザーから視聴するチャンネルの指示をＧＵＩ処理手段３２を介して受けたチューナーモジュール制御手段３１は、チューナーモジュール１１に対して、相互認証とチャンネル選局およびデジタル放送番組の受信を要求する。相互認証処理手段３６は、デジタル放送受信用ソフトウェアの該当バージョンに固有なデジタル放送受信ソフトウェア識別パラメータを用いて、チューナーモジュール１１の認証処理制御部１８との間で相互認証と暗号化鍵の共有を行う。

【００２３】

相互認証が成立した場合、暗号化された放送番組コンテンツをインターフェース１９、インターフェースコントローラ２２、ＰＣＩバス２３を介して受け取ることができる。暗号復号手段３４は、暗号化された放送番組コンテンツを復号し、ＭＰＥＧ２デコード手段３５に送出する。ＭＰＥＧ２デコード手段３５は、ＭＰＥＧ－２規格に基づいて圧縮された放送番組コンテンツを元の映像データと音声データに伸長し、映像データは表示コントローラ３７に、音声データはサウンドコントローラ４０にＡＧＰバス４２を介して送出する。表示コントローラ３７は、映像データをＶＲＡＭ３８に一時記憶させると共に、ＬＣＤディスプレイ３９に表示させる。サウンドコントローラ４０は、音声データをＤ／Ａ変換し、スピーカ４１を鳴動させる。ＥＰＧ処理手段３３は、放送番組コンテンツの中から放送番組ガイド情報を取り出して、番組一覧表の作成、選局、録音予約などに使用する。

【００２４】

相互認証が成立しない場合、パソコン２１は放送番組コンテンツを受け取ることができない。相互認証処理手段３６は、ＧＵＩ処理手段３０を介して、相互認証が成立せずデジタル放送を視聴できないため、デジタル放送受信用ソフトウェアのアップデートを促すメッセージをＬＣＤディスプレイ３９に表示して、ユーザーに知らせる。

【００２５】

次に、図２にデジタル放送信号に含まれるデータと情報の概要を示す。デジタル放送信号には、映像データと音声データに加えて、相互認証で用いる認証パラメータを含んだＥＭＭ情報などが多重化されている。

【００２６】

図３は、トランスポート・ストリームのフォーマットを示す。トランスポート・ストリームは、１８８バイトのトランスポート・ストリームパケット（以下、ＴＳパケットと云う）の連続した信号である。ＴＳパケットは、４バイト（３２ビット）のヘッダーと１８４バイトのペイロードから構成されており、ヘッダー内のＰＩＤ（Ｐａｃｋｅｔ ＩＤ）１３ビットにて、このＴＳパケットが何のＴＳパケットか（映像データ、音声データ、ＥＭＭ情報など）を区別している。デジタル受信装置１０は、このＰＩＤにもとに、必要なＴＳパケットをフィルタリングして、そのペイロードの情報を処理する。

【００２７】

以下に、図４のフローチャートを参照して、相互認証に用いる認証パラメータの取得手順について説明する。チューナーモジュールは、ＰＩＤ値が０ｘ０１のパケットをトランスポート・ストリームからフィルタリングし（ステップ４０１）、ＣＡＴ（Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ ｔａｂｌｅ）セッションのパケットを取り出す（ステップ４

０２）。ＣＡＴセッションデータから、ＣＡ（Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ）ディスクリプタ形式で記述されているＥＭＭパケットのＰＩＤを取り出す（ステップ４０３）。

【００２８】

チューナーモジュールは、このＥＭＭパケットのＰＩＤ値を用いて、トランスポート・ストリームからフィルタリングし（ステップ４０４）、ＥＭＭパケットを取り出し（ステップ４０５）、ＥＭＭセッションデータを取得する（ステップ４０５）。ＥＭＭセッションデータには、チューナーモジュール（受信機）のメーカー、機種、バージョン毎に割り当てられたＩＤとその認証パラメータ情報がセットで組み込まれている。チューナーモジュールは、このＥＭＭセッションデータから、当該チューナーモジュールのＩＤに対応する認証パラメータ情報を取り出す（ステップ４０７）。この認証パラメータ情報には、上記のＩＤに一致するチューナーモジュールのみが復号できる暗号が、あらかじめ掛けられている。チューナーモジュールは、この暗号化されている認証パラメータ情報を復号し、認証パラメータを取得する（ステップ４０８）。なお、本実施例では、認証パラメータがＥＭＭパケットに含まれることで説明したが、ＳＩ（Ｓｅｒｖｉｃｅ Ｉｎｆｏｍａｔｉｏｎ）情報に含まれてもよい。

【００２９】

次に、図５に示すフローチャートを参照して、本実施例によるチューナーモジュール１１とパソコン２１間の相互認証と暗号化鍵共有の手順について説明する。チューナーモジュール１１は、乱数を生成し（ステップ５０１）、相互認証処理と放送番組コンテンツの暗号化鍵作成のもとになる認証セッション鍵Ａを作成する（ステップ５０２）。また、図４を参照して説明した手順に従って、認証パラメータを取得し（ステップ５０３）、この認証パラメータを用いて、チューナーモジュール１１が相互認証用に保持しているチューナーモジュール識別パラメータ（請求項に記載の第１の認証用パラメータの一実施例）を更新する（ステップ５０４）。そして、認証セッション鍵Ａをデータにし、チューナーモジュール識別パラメータを鍵にして暗号化した（ステップ５０５）暗号化データをパソコン２１に伝送する。

【００３０】

一方、パソコン２１は、チューナーモジュール１１から受け取った暗号化データを、デジタル放送受信ソフトウェアがそのバージョン毎に固有に保持しているデジタル放送受信ソフトウェア識別パラメータ（請求項に記載の第２の認証用パラメータの一実施例）（ステップ５５１）を鍵にして復号し（ステップ５５２）、認証セッション鍵Ｂを作成する（ステップ５５３）。以上の手順にて、チューナーモジュール１１とパソコン２１の双方が、認証セッション鍵ＡとＢを作成する。そして、この双方の認証セッション鍵が、正しい鍵（同一の鍵）か否かを以下の手順にて相互認証する。

【００３１】

チューナーモジュール１１は、乱数を生成し（ステップ５０６）、相互認証処理に用いる認証用データＡを作成し（ステップ５０７）、その認証用データＡをパソコン２１に伝送するとともに、その認証用データＡを認証セッション鍵Ａを鍵にして暗号化する（ステップ５０９）。一方、パソコン２１は、乱数を生成し（ステップ５５４）、相互認証処理に用いる認証用データＢを作成し（ステップ５５５）、その認証用データＢをチューナーモジュール１１に伝送するとともに、その認証用データＢを認証セッション鍵Ｂを鍵にして暗号化する（ステップ５５６）。

【００３２】

チューナーモジュール１１は、パソコン２１から受信した認証用データＢを認証セッション鍵Ａを鍵にして暗号化し（ステップ５０８）、暗号化した認証用データＢをパソコン２１へ返送する。一方、パソコン２１は、チューナーモジュール１１から受信した認証用データＡを認証セッション鍵Ｂを鍵にして暗号化し（ステップ５５７）、暗号化した認証用データＡをチューナーモジュール１１へ返送する。チューナーモジュール１１は、自身の認証セッション鍵Ａにて暗号化した認証用データＡと、パソコン２１が認証セッション

鍵Ｂにて暗号化した認証用データＡとを比較する（ステップ５１０）。

【００３３】

一方、パソコン２１は、自身の認証セッション鍵Ｂにて暗号化した認証用データＢと、チューナーモジュールが認証セッション鍵Ａにて暗号化した認証用データＢとを比較する（ステップ５５８）。双方の比較結果の一致（Ｙｅｓ）の論理積をとり（ステップ５１５）、双方の比較結果が一致した場合、認証セッション鍵ＡとＢは同じと判断し、相互認証が成立する（ステップ５１６）。一方、双方の比較結果の少なくても一方が一致しない場合、認証セッション鍵ＡとＢに相違があると判断し、認証を成立させない。

【００３４】

相互認証が成立した場合、チューナーモジュール１１は、認証セッション鍵Ａを鍵にして暗号化した認証用データＢと、認証セッション鍵Ａを鍵にして暗号化した認証用データＡとの排他的論理和をとり（ステップ５１１）、その出力データを認証セッション鍵Ａを鍵にして暗号化し（ステップ５１２）、伝送する放送番組コンテンツの暗号化に用いる暗号セッション鍵Ａを作成する（ステップ５１３）。一方、パソコン２１は、認証セッション鍵Ｂを鍵にして暗号化した認証用データＡと、認証セッション鍵Ｂを鍵にして暗号化した認証用データＢとの排他的論理和をとり（ステップ５５９）、その出力データを認証セッション鍵Ｂを鍵にして暗号化し（ステップ５６０）、暗号化された放送番組コンテンツの復号に用いる暗号セッション鍵Ｂを作成する（ステップ５６１）。

【００３５】

以下に、図６のフローチャートを参照して、デジタル放送受信ソフトウェアのアップデートの要因、作業手順、および方法についてまとめて説明する。デジタル放送受信ソフトウェアのアップデートが発生する要因としては、１）デジタル放送受信ソフトウェアの改ざんを未然に防止するための定期的なアップデート、２）耐タンパ性を向上させたデジタル放送受信ソフトウェアの改良版へのアップデート、３）デジタル放送受信ソフトウェアの改ざんが察知された場合、改ざん対策版への緊急のアップデートなどがある（ステップ６０１）。

【００３６】

また、デジタル放送受信ソフトウェアのソフトウェアメーカー、および放送番組コンテンツを送信する放送局のアップデートの準備としては、１）デジタル放送受信ソフトウェアのアップデート版の作成とリリース準備、２）ユーザーへのアップデート実施の告知（メール、ホームページなど）、３）デジタル放送信号に多重化している認証パラメータの更新による相互認証不成立とユーザーへのアップデートの促しなどがある（ステップ６０２）。

【００３７】

更に、アップデートの方法としては、１）デジタル放送受信ソフトウェアを起動時、インターネットを介して自動確認、自動アップデート、２）ソフトウェアメーカーのホームページからダウンロードし、アップデート、３）電子メールによるアップデート、４）郵送メディアによるアップデート、５）デジタル放送のダウンロードサービスによるアップデート、などがある（ステップ６０３）。ユーザーは、上記のいずれかの方法によって、パソコン２１に搭載しているデジタル放送受信ソフトウェアをアップデートすることにより、放送番組コンテンツを継続して視聴することができる。

【００３８】

以上の本発明による実施例により、デジタル放送受信ソフトウェアの改ざんを察知した場合、認証パラメータを更新し、相互認証を不成立にさせることで、チューナーモジュールからパソコンへの放送番組コンテンツの伝送を行わないように制御し、これにより放送番組コンテンツの視聴を制限し、また放送番組コンテンツの不正な複製や公衆回線への転送等の不正な利用を防止して、著作権を保護することができる。また、定期的に、認証パラメータを更新することにより、デジタル放送受信ソフトウェアの不正な改ざんによる不正利用を未然に防止して、著作権を保護することができる。さらに、デジタル放送受信ソフトウェアを、より耐タンパ性を高めた改良版にアップデートすることにより、著作権の

保護をより高めることができる。さらにまた、デジタル放送受信ソフトウェアへのアップデートすることにより、放送番組コンテンツを継続して視聴する、あるいは再開することができる。

【図面の簡単な説明】

【００３９】

【図１】本発明の実施例におけるデジタル放送受信装置のブロック図。

【図２】本発明の実施例におけるデジタル放送信号の概要図。

【図３】本発明の実施例におけるトランスポート・ストリームのフォーマット図。

【図４】本発明の実施例における認証パラメータ取得の手順を示すフローチャート。

【図５】本発明の実施例における相互認証の手順を示すフローチャート。

【図６】本発明の実施例におけるデジタル放送受信ソフトウェアのアップデート処理を示すフローチャート。

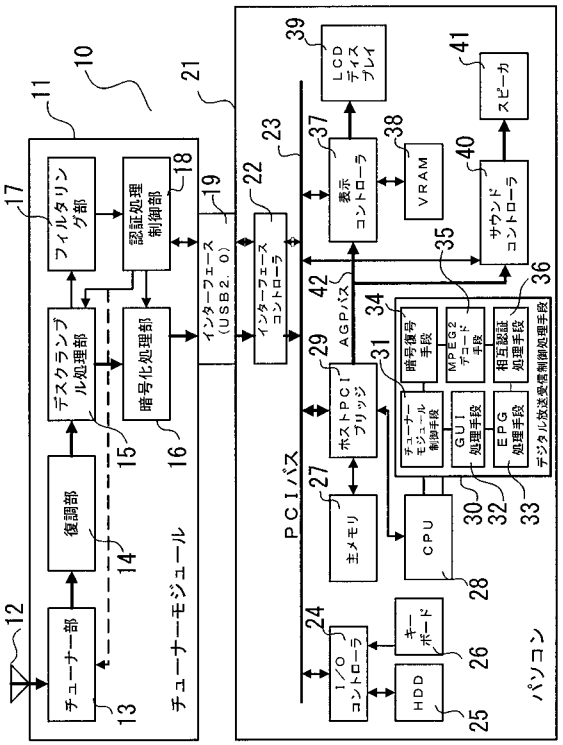
【図７】従来のデジタル放送受信装置の構成を示すブロック図。

【符号の説明】

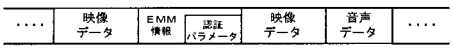
【００４０】

１０　デジタル放送受信装置
１１　チューナーモジュール
１２　アンテナ
１３　チューナー部
１４　復調部
１５　デスクランブル部
１６　暗号化処理部
１７　フィルタリング部
１８　認証処理制御部
１９　インターフェース
２１　パソコン
２２　インターフェースコントローラ
２３　ＰＣＩバス
２４　Ｉ／Ｏコントローラ
２５　ＨＤＤ
２６　キーボード
２７　主メモリ
２８　ＣＰＵ
２９　ホストＰＣＩブリッジ
３０　デジタル放送受信制御処理手段
３１　チューナーモジュール制御手段
３２　ＧＵＩ処理手段
３３　ＥＰＧ処理手段
３４　暗号復号手段
３５　ＭＰＥＧ２デコード手段
３６　相互認証手段
３７　表示コントローラ
３８　ＶＲＡＭ
３９　ＬＣＤディスプレイ
４０　サウンドコントローラ
４１　スピーカ
４２　ＡＧＰバス

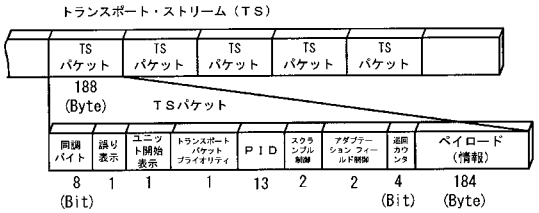
【図１】



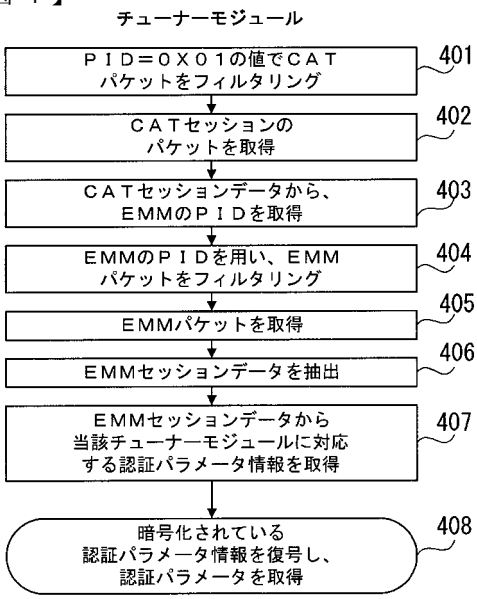
【図２】



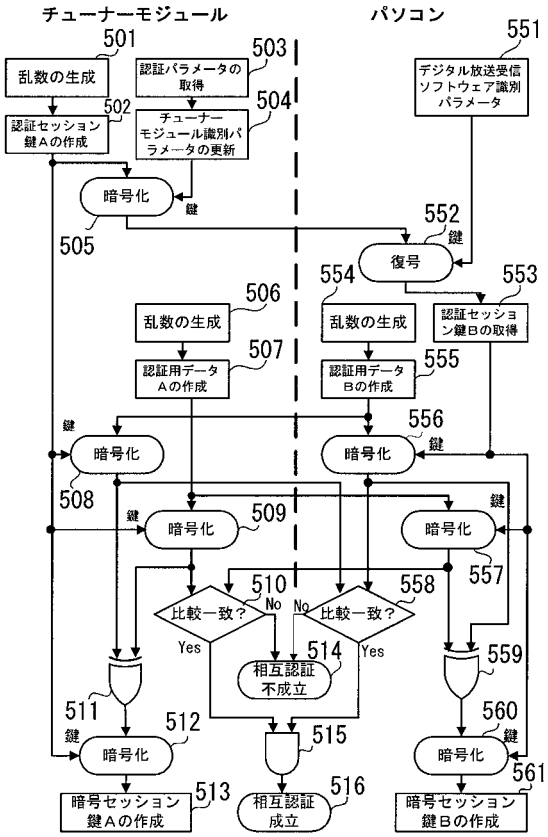
【図３】



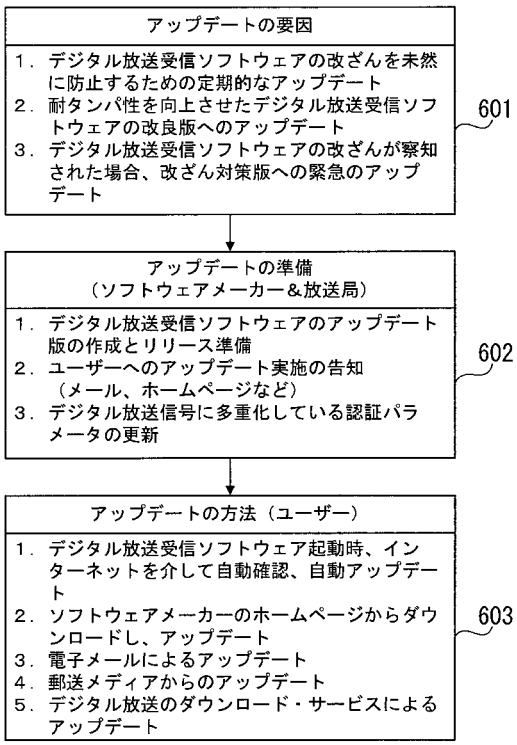
【図４】



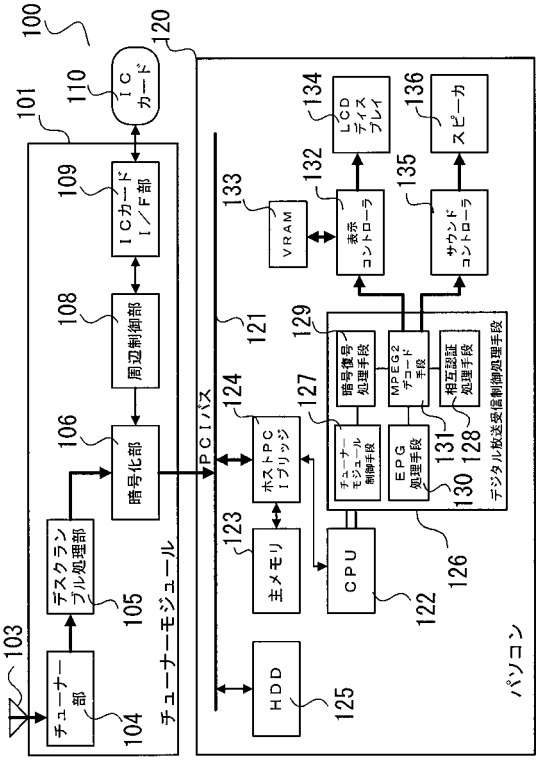
【図５】



【図６】



【図７】


100
101
103
104
105
106
108
109
110
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
チューナー部
デスクランブル処理部
暗号化部
周辺制御部
ICカードI／F部
ICカード
チューナーモジュール
PCIバス
ホストPCIブリッジ
主メモリ
HDD
CPU
VRAM
表示コントローラ
サウンドコントローラ
LCDディスプレイ
スピーカ
暗号復号処理手段
チューナーモジュール制御手段
EPG処理手段
MPEG2デコード手段
相互認証処理手段
デジタル放送受信制御処理手段
パソコン