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

特許第5173661号
(P5173661)

(45)発行日　平成25年4月3日(2013.4.3)　(24)登録日　平成25年1月11日(2013.1.11)

(51)Int.Cl.		F I		
H04N 5/91	(2006.01)	H04N	5/91	P
G11B 20/10	(2006.01)	G11B	20/10	H
		G11B	20/10	311

請求項の数 12　(全 18 頁)

(21)出願番号　特願2008-201188(P2008-201188)
(22)出願日　平成20年8月4日(2008.8.4)
(65)公開番号　特開2010-41333(P2010-41333A)
(43)公開日　平成22年2月18日(2010.2.18)
審査請求日　平成23年8月2日(2011.8.2)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】録画装置およびその制御方法

(57)【特許請求の範囲】

【請求項１】

スクランブルされたコンテンツを受信する受信手段と、

前記コンテンツのスクランブル鍵を暗号化したワーク鍵を取得する取得手段と、

前記ワーク鍵により前記スクランブル鍵を復号する復号手段と、

前記スクランブル鍵を用いて前記スクランブルを解除する解除手段と、

前記受信手段により受信された前記スクランブルされたコンテンツを記録媒体に記録し、前記復号手段により前記スクランブル鍵が復号可能になった後、前記記録媒体に記録した前記スクランブルされたコンテンツを読み出し、前記解除手段によって前記スクランブルを解除したコンテンツを前記記録媒体に記録する制御手段とを有することを特徴とする録画装置。

【請求項２】

前記制御手段は、前記復号手段により前記スクランブル鍵が復号可能になった後、前記受信手段により受信された前記スクランブルされたコンテンツの前記記録媒体への記録を継続するとともに、前記記録媒体に記録した前記スクランブルされたコンテンツの読み出しを開始して、前記解除手段によって前記スクランブルを解除したコンテンツの前記記録媒体への記録を開始することを特徴とする請求項1に記載された録画装置。

【請求項３】

前記制御手段は、前記復号手段により前記スクランブル鍵が復号可能になったことに応じて、前記受信手段により受信された前記スクランブルされたコンテンツの前記記録媒体

への記録を終了し、前記解除手段によって前記スクランブルを解除したコンテンツの前記記録媒体への記録を開始することを特徴とする請求項1に記載された録画装置。

【請求項４】

前記制御手段は、前記解除手段によって前記スクランブルを解除したコンテンツの前記記録媒体への記録が終了し、前記記録媒体に前記スクランブルされたコンテンツが記録されている場合は、前記記録媒体に記録した前記スクランブルされたコンテンツを読み出し、前記解除手段によって前記スクランブルを解除したコンテンツを前記記録媒体に記録するスクランブル解除処理を行うことを特徴とする請求項3に記載された録画装置。

【請求項５】

前記制御手段は、前記スクランブル解除処理が終了すると、前記記録媒体に記録した、前記スクランブルを解除した二つのコンテンツを結合することを特徴とする請求項4に記載された録画装置。

【請求項６】

さらに、前記ワーク鍵を取得するための情報を前記受信手段が受信する周期を測定する測定手段を有し、

前記制御手段は、前記周期に基づき、前記コンテンツの記録を開始する前に前記受信手段、前記取得手段および前記復号手段を動作させることを特徴とする請求項1に記載された録画装置。

【請求項７】

スクランブルされたコンテンツを受信する受信手段、前記コンテンツのスクランブル鍵を暗号化したワーク鍵を取得する取得手段、前記ワーク鍵により前記スクランブル鍵を復号する復号手段、前記スクランブル鍵を用いて前記スクランブルを解除する解除手段、および、制御手段を有する録画装置の制御方法であって、

前記制御手段が、前記受信手段により受信された前記スクランブルされたコンテンツを記録媒体に記録し、

前記復号手段により前記スクランブル鍵が復号可能になった後、前記制御手段が、前記記録媒体に記録した前記スクランブルされたコンテンツを読み出し、前記解除手段によって前記スクランブルを解除したコンテンツを前記記録媒体に記録することを特徴とする制御方法。

【請求項８】

前記復号手段により前記スクランブル鍵が復号可能になった後、前記制御手段が、前記受信手段により受信された前記スクランブルされたコンテンツの前記記録媒体への記録を継続するとともに、前記記録媒体に記録した前記スクランブルされたコンテンツの読み出しを開始して、前記解除手段によって前記スクランブルを解除したコンテンツの前記記録媒体への記録を開始することを特徴とする請求項7に記載された制御方法。

【請求項９】

前記復号手段により前記スクランブル鍵が復号可能になったことに応じて、前記制御手段が、前記受信手段により受信された前記スクランブルされたコンテンツの前記記録媒体への記録を終了し、前記解除手段によって前記スクランブルを解除したコンテンツの前記記録媒体への記録を開始することを特徴とする請求項7に記載された制御方法。

【請求項１０】

前記解除手段によって前記スクランブルを解除したコンテンツの前記記録媒体への記録が終了し、前記記録媒体に前記スクランブルされたコンテンツが記録されている場合、前記制御手段が、前記記録媒体に記録した前記スクランブルされたコンテンツを読み出し、前記解除手段によって前記スクランブルを解除したコンテンツを前記記録媒体に記録するスクランブル解除処理を行うことを特徴とする請求項9に記載された制御方法。

【請求項１１】

前記スクランブル解除処理が終了すると、前記制御手段が、前記記録媒体に記録した、前記スクランブルを解除した二つのコンテンツを結合することを特徴とする請求項10に記載された制御方法。

【請求項１２】
前記録画装置は、さらに、前記ワーク鍵を取得するための情報を前記受信手段が受信する周期を測定する測定手段を有し、
前記制御手段が、前記周期に基づき、前記コンテンツの記録を開始する前に前記受信手段、前記取得手段および前記復号手段を動作させることを特徴とする請求項7に記載された制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、スクランブルされたコンテンツの録画に関する。
【背景技術】
【０００２】
地上ディジタル放送は、無料放送であるが、コンテンツの著作権保護のためにスクランブルされる。コンテンツのスクランブルには、限定受信システム(conditional access system: CAS)を用いる。現在、限定受信システムとして、ICカードを用いるB-CAS方式のシステムが運用されている。
【０００３】
放送受信機において著作権を保護する方法はRMP (rights management and protection)と呼ばれ、暗号鍵を用いてコンテンツを暗号化する方法が用いられる。例えば、現行のB-CASの場合、スクランブル鍵、ワーク鍵、マスタ鍵の三段階の暗号鍵を用いる。また、後述する新RMP方式は、スクランブル鍵、ワーク鍵、デバイス鍵の三段階の暗号鍵を用いる（例えば、非特許文献1参照）。
【０００４】
スクランブル鍵は、安全性を向上するために数秒ごとに更新され、ワーク鍵を用いて暗号化されて送信される。暗号化スクランブル鍵は、ECM (entitlement control message)と呼ばれるデータに含まれる。
【０００５】
ワーク鍵もまた暗号化されて送信される。ワーク鍵を暗号化する鍵は、マスタ鍵またはデバイス鍵であり、RMPの方式によって何れかの鍵を用いる。暗号化ワーク鍵は、EMM (entitlement management message)と呼ばれるデータに含まれる。
【０００６】
マスタ鍵は、B-CASカードに記述される、カードごとに与えられた鍵である。一方、デバイス鍵は、装置メーカまたは機種に対して与えられた鍵であり、同一装置メーカまたは同一機種は同じデバイス鍵を有する。
【０００７】
放送局は、機種ごとに異なるデバイス鍵でワーク鍵を暗号化し、暗号化ワーク鍵をEMMに含めて送信する。暗号化ワーク鍵を一度に多数送信することはできないので、様々な機種に対応した暗号化ワーク鍵を順次送信することになる。つまり、放送局は、様々な機種に対応した暗号化ワーク鍵を含むEMMの順次送信を周期的に繰り返す。EMMの順次送信の一周期に要する時間は、送信するデータの数によって決まり、データの数は機種の数によって決まる。従って、EMMの順次送信の一周期に要する時間は、数秒間から数十秒間になる可能性がある。
【０００８】
従って、自機種向けの暗号化ワーク鍵を含むEMMを取得するには、最大、EMMの順次送信の一周期分の時間を必要とする。勿論、ワーク鍵を取得するまでの期間、コンテンツを復号することはできない。もし、録画を開始する時点で、録画機が記憶すワーク鍵がコンテンツを暗号化したスクランブル鍵に未対応であるとすると、録画機は、ワーク鍵を取得する必要がある。ワーク鍵の取得には、最大、EMMの順次送信の一周期分の時間が必要になり、録画の開始に間に合わない場合がある。
【０００９】

一方、電波産業会の標準規格「デジタル放送におけるアクセス制御方式」（ARIB STD-B25 5.1版）の第3部「受信時の制御方式（コンテンツ保護法式）」において、新たなコンテンツ保護方式（以下、新RMP方式）が追加規格化された。

【００１０】

新RMP方式においては、著作権侵害による被害を防ぐために、著作権を侵害する放送受信機（以下、不正受信機）が出現した場合、不正受信機を無効化する仕組みが検討されている。不正受信機の無効化は、コンテンツの暗号鍵と、正規の放送受信機（以下、正規受信機）の暗号鍵を更新することにより実現する。暗号鍵の更新を行うことができない不正受信機は、コンテンツの復号が不可能になる（特許文献1、非特許文献1参照）。

【００１１】

不正受信機の無効化をリボーク(revoke)、無効化処理をリボケーション(revocation)と呼ぶ。デバイス鍵は、リボケーションの実行により書き換えられることを想定し、例えばデバイス鍵の漏洩が生じた場合、古いデバイス鍵は無効化される。その場合、放送局、放送受信機の双方で、デバイス鍵を新鍵に更新する必要がある。

【００１２】

新RMP方式においては、放送受信機は機種ごとに異なるデバイス鍵を生成し、生成したデバイス鍵を用いてワーク鍵の復号を行う。デバイス鍵の生成には、放送局がそれに対応する機種IDを送信し、放送受信機が機種IDを受信する必要がある。機種IDもEMMを用いて送信され、やはり様々な機種向けに、EMMが順次送信される。従って、機種IDを取得するために、やはり、最大、EMMの順次送信の一周期分の時間を必要とする。

【００１３】

従って、機種IDを取得し、自機種向けの暗号化ワーク鍵を取得するまでの期間、録画機はコンテンツを復号することができず、コンテンツの録画を正常に行うことはできない。この期間、正しく復号されていないデータが記録媒体に記録されることになる。

【００１４】

【特許文献１】特開2007-006380公報

【非特許文献１】電波産業会標準規格「ディジタル放送におけるアクセス制御方式」（ARIB STD-B25 5.1版）

【発明の開示】

【発明が解決しようとする課題】

【００１５】

本発明は、コンテンツのスクランブルを解除できない期間を考慮して、コンテンツを記録することを目的とする。

【課題を解決するための手段】

【００１６】

本発明は、前記の目的を達成する一手段として、以下の構成を備える。

【００１７】

本発明にかかる録画装置は、スクランブルされたコンテンツを受信する受信手段と、前記コンテンツのスクランブル鍵を暗号化したワーク鍵を取得する取得手段と、前記ワーク鍵により前記スクランブル鍵を復号する復号手段と、前記スクランブル鍵を用いて前記スクランブルを解除する解除手段と、前記受信手段により受信された前記スクランブルされたコンテンツを記録媒体に記録し、前記復号手段により前記スクランブル鍵が復号可能になった後、前記記録媒体に記録した前記スクランブルされたコンテンツを読み出し、前記解除手段によって前記スクランブルを解除したコンテンツを前記記録媒体に記録する制御手段とを有することを特徴とする。

【００１８】

本発明にかかる制御方法は、スクランブルされたコンテンツを受信する受信手段、前記コンテンツのスクランブル鍵を暗号化したワーク鍵を取得する取得手段、前記ワーク鍵により前記スクランブル鍵を復号する復号手段、前記スクランブル鍵を用いて前記スクランブルを解除する解除手段、および、制御手段を有する録画装置の制御方法であって、前記制

御手段が、前記受信手段により受信された前記スクランブルされたコンテンツを記録媒体に記録し、前記復号手段により前記スクランブル鍵が復号可能になった後、前記制御手段が、前記記録媒体に記録した前記スクランブルされたコンテンツを読み出し、前記解除手段によって前記スクランブルを解除したコンテンツを前記記録媒体に記録することを特徴とする。

【発明の効果】

【００１９】

本発明によれば、コンテンツのスクランブルを解除できない期間を考慮して、コンテンツを記録することができる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明にかかる実施例の放送受信録画装置を図面を参照して詳細に説明する。

【００２１】

［概要］

実施例の放送受信録画装置（以下、録画機）は、スクランブルを解除して録画するモードが選択されていたとしても、一旦、スクランブルされたトランスポートストリーム（MPEG-2 TS）を復号せずに録画する。そして、暗号鍵を取得することができた時点で、スクランブルされたMPEG-2 TSの復号を開始し、最終的に、スクランブルを解除したプログラムストリーム（MPEG-2 PS）として記録媒体に録画する。

【実施例１】

【００２２】

［装置の構成］

図1は実施例の録画機の構成例を示すブロック図である。

【００２３】

録画機100は、放送波を受信し、放送されたコンテンツをハードディスクやDVDなどの記録媒体に録画する。

【００２４】

選局部102は、アンテナ101によって受信された放送波からユーザが所望するチャネルを選局する。復調部103は、選局部102によって選局されたチャネルの信号を復調する。

【００２５】

セレクタ104は、二つの端子AとBに入力された信号を選択的に出力する。端子Aはインタフェイス(IF)120が生成する信号を入力し、端子Bは復調部103が生成する信号を入力する。

【００２６】

伝送制御信号分離部113は、トランスポートストリーム(TS)から限定受信にかかわる情報（ECM、EMMを含む）を分離し、システム部109に入力する。復号部105は、スクランブル鍵を用いて、スクランブルされたコンテンツを復号する。分離部106は、多重化されたストリームから必要なストリームを取り出す。MPEGデコーダ107は、MPEGデータをデコードして映像信号と音声信号を取り出す。MPEGエンコーダ108は、映像信号と音声信号をMPEGフォーマットに再エンコードする。

【００２７】

システム部109は、マイクロプロセッサ(CPU)とメモリ(RAM)で構成される例えばマイクロコントローラである。システム部109のCPUは、RAMを作業領域としてプログラムを実行し、録画機100を制御する。CPUが実行するプログラムは、不揮発性のハードディスクや半導体メモリに格納され、たとえ録画機100の電源がオフになっても保持される。なお、システム部109の詳細は後述する。

【００２８】

システム部109は、CPUとそれが実行するプログラムの形態で実装されたスクランブル鍵復号部110、ワーク鍵復号部111、デバイス鍵生成部112を備える。スクランブル鍵復号部110は、ECMに含まれる暗号化スクランブル鍵をワーク鍵を用いて復号する。ワーク鍵復号

部111は、EMMに含まれる暗号化ワーク鍵をデバイス鍵を用いて復号する。デバイス鍵生成部112は、暗号鍵の生成アルゴリズムを備え、デバイスIDが入力されるとデバイス鍵を生成する。

【００２９】

インタフェイス(IF)120は、バスと制御回路で構成されるインタフェイスである。コントローラ121は、記録装置122のインタフェイスを制御するコントローラである。記録装置122は、ハードディスクドライブ(HDD)やDVDドライブなど、記録媒体にディジタル情報を記録し、記録媒体からディジタル情報を読み出す装置である。なお、記録装置122とコントローラ121は、データの書込転送と読出転送を実行する。複数の書込転送要求と、複数の読出転送要求が発生した場合、記録装置122とコントローラ121は、それら要求に対応する転送を時分割に処理して、複数の転送要求を同時に処理することが可能である。

【００３０】

出力回路123は、映像信号と音声信号を出力端子を介してディスプレイ124に出力する。ディスプレイ124は、映像信号が表す映像を表示し、音声信号を再生する。

【００３１】

［システム部の構成］

図2はシステム部109の構成例を示すブロック図である。

【００３２】

CPU150は、RAM151を作業領域として、プログラムとして記述された命令を順次処理する。

【００３３】

NVメモリ152は、プログラム、初期値などの各種データ、暗号鍵などを記憶するEEPROMなどの書換可能な不揮発性のメモリである。NVメモリ152には、録画機100を制御するプログラム、RMPを制御するプログラム、RMPで用いるデバイス鍵生成アルゴリズム、初期値などの各種データがファームウェアとして格納されている。

【００３４】

インタフェイス(IF)153は、録画機100が受信したデータを入力し、システム部109が生成したデータを出力するインタフェイスである。システムバス154は、上記構成を相互に接続し、上記構成の間のデータ転送を担うバスである。

【００３５】

［暗号鍵の更新］

上述したARIB STD-B25 5.1版は、ワーク鍵としてペアの暗号鍵を用意し、これらを順に切り替えて暗号鍵の更新操作を行う構成を開示する。本来、送信される暗号鍵と受信側で復号される暗号鍵の同期を取るために、ARIB STD-B25 5.1版が開示する方法に従うべきであるが、ここでは概念の説明に留め、簡略化した構成を説明する。

【００３６】

図3は暗号鍵の更新の概要を説明するタイミングチャートである。

【００３７】

図3において、番組のコンテンツCはスクランブル鍵で暗号化されている。暗号化ワーク鍵Kwcは、デバイス鍵Kdを用いて暗号化されたワーク鍵Kwである。デバイスIDは、ワーク鍵Kwを暗号化するデバイス鍵Kdと対応付けられている。暗号化ワーク鍵Kwcとデバイスは、EMMに含められ、コンテンツCとともに送信される。録画機100のCPU150は、デバイスIDをデバイス鍵生成部112に入力してデバイス鍵Kdを生成し、生成したデバイス鍵Kdを用いてワーク鍵復号部111により暗号化ワーク鍵Kwcを復号する。

【００３８】

暗号鍵の更新は次のように行われる。時刻R1において、EMMに含まれるデバイスIDがID(p)からID(p+1)に更新される。さらに、放送局において、ワーク鍵Kwの暗号化に用いるデバイス鍵KdがID(p+1)に対応する鍵に更新される。

【００３９】

CPU150は、受信したID(p+1)をデバイス鍵生成部112に入力して暗号鍵Kd(p+1)を生成す

る。これにより、例えばRAM151の所定領域に割り当られたレジスタKdrが記憶するデバイス鍵がKd(p)からKd(p+1)に更新される。

【００４０】

次に、時刻R2において、ワーク鍵がKw(k)からKw(k+1)に更新される。従って、時刻R2において、EMMに含まれる暗号化ワーク鍵はKd(p)[Kw(k)]からKd(p+1)[Kw(k+1)]に更新される。

【００４１】

CPU150は、受信した暗号化ワーク鍵Kd(p+1)[Kw(k+1)]をワーク鍵復号部111に入力してデバイス鍵Kd(p+1)によりワーク鍵を復号する。これにより、例えばRAM151の所定領域に割り当られたレジスタKwrが記憶するワーク鍵がKw(k)からKw(k+1)に更新される。

【００４２】

つまり、時刻R2において、放送局がスクランブル鍵を暗号化するワーク鍵がKw(k)からKw(k+1)に更新され、録画機100のレジスタKwrが記憶するワーク鍵もKw(k)からKw(k+1)に更新される。従って、送信側と受信側の双方でワーク鍵Kwが一致するので、コンテンツCをスクランブルするスクランブル鍵の復号は正常に継続され、番組のコンテンツCの視聴も正常に継続される。

【００４３】

［コンテンツの復号が正常に行えないケース］

図4は鍵の更新が正常に行われずにコンテンツCの復号が正常に行えないケースを説明するタイミングチャートである。なお、録画機は、番組の録画を時刻Sに開始するように予約録画設定されているものとする。

【００４４】

図3と同様に、時刻R1において、EMMに含まれるデバイスIDがID(p)からID(p+1)に更新され、時刻R2において、ワーク鍵がKw(k)からKw(k+1)に更新される。録画機は、時刻Sより前はパワーオフ状態にあり、放送の受信を休止していたとする。そして、録画機は、時刻Sにおいてパワーオン状態になり、予約録画を開始する。

【００４５】

時刻Sにおいて、スクランブル鍵の暗号化に用いられているワーク鍵はKw(k+1)、ワーク鍵Kw(k+1)の暗号化に用いられているデバイス鍵Kd(p+1)である。一方、録画機のレジスタKdrとKwrは、ワーク鍵Kw(k)とデバイス鍵Kd(p)を保持する。従って、送信側と受信側でワーク鍵Kwが一致しないので、コンテンツCをスクランブルするスクランブル鍵の復号は正常に行われず、番組のコンテンツCも正常に復号することができない。言い換えれば、録画機は、時刻Sにおいて、番組のコンテンツを正常に録画することができない。

【００４６】

その後、時刻Tにおいて、録画機のデバイスID(p+1)を含むEMMが送信され、録画機はデバイスID(p+1)によりデバイス鍵kd(p+1)を生成する。しかし、この時点では、録画機は更新後の暗号化ワーク鍵を受信していないので、更新後のワーク鍵を復号することができない。その後、時刻Uにおいて、録画機向けの暗号化ワーク鍵Kd(p+1)[Kw(k+1)]を含むEMMが送信される。この時点で、漸く、録画機は、更新後ワーク鍵Kw(k+1)を復号することができ、コンテンツCのスクランブル鍵を復号し、コンテンツCの復号が可能になる。

【００４７】

言い換えれば、録画機は、時刻SからUの期間、番組のコンテンツを正常に録画することができず、時刻U以降、番組のコンテンツを正常に録画することができる。その結果、予約録画された、時刻SからUの期間に相当する映像、音声は視聴不能な状態で記録されることになる。

【００４８】

［予約録画方法］

録画機100は、以下の動作を行うことにより、上記のコンテンツの復号が正常に行えないケースを回避して、予約録画が指示されたコンテンツを正常に録画する。

【００４９】

録画機100は、コンテンツを録画する際のフォーマットとして以下の三つの記録モードが設定可能である。

モードA：MPEG-2 PSフォーマット、DVDなどの記録媒体と互換性があり、スクランブルを解除したプログラムストリーム(PS)を記録する、

モードB：MPEG-2 TSフォーマット、スクランブルを解除せず、トランスポートストリーム(TS)をそのまま記録する、

モードC：MPEG-2 TSフォーマット、スクランブルを解除したトランスポートストリーム(TS)を記録する。

【００５０】

暗号鍵の更新によって、コンテンツの復号が正常に行えないケースが発生するのは、モードAの場合とモードCの場合である。以下では、モードAが設定された場合の録画機100の予約録画動作を説明する。

【００５１】

図5はモードAが設定された場合の録画機100の予約録画動作を説明するタイミングチャートである。

【００５２】

図4と同様に、時刻R1において、EMMに含まれるデバイスIDがID(p)からID(p+1)に更新され、時刻R2において、ワーク鍵がKw(k)からKw(k+1)に更新される。録画機100は、時刻Sより前はパワーオフ状態にあり、放送の受信を休止していたとする。なお、録画機100はパワーオフ状態にあっても、システム部109は、時刻を計時し、時刻Sに録画機100をパワーオンするなどの処理が行える程度に動作、機能していることは言うまでもない。

【００５３】

録画機100は、時刻Sにおいてパワーオン状態になり、モードAの予約録画を開始する。時刻Sにおいて、セレクタ104は端子Bに入力される信号を選択出力するようにセットされている。従って、アンテナ101と選局部102により受信された放送信号は復調部103によって復調され、復調部103が出力する信号は伝送制御信号分離部113に入力される。そして、システム部109は、伝送制御信号分離部113によって分離された限定受信に関する情報を入力する。同時に、復調部103が出力する信号はIF120に入力される。コントローラ121は、IF120を経由して、復調部103が復調したTSを受信し、TSを記録装置122の記録媒体に記録する。

【００５４】

図5において、CR1は、上記の動作により、スクランブルされたTSが記録媒体に記録される様子を示している。

【００５５】

時刻Sにおいて、TSのスクランブル鍵を暗号化しているワーク鍵Kw(k+1)と、レジスタKwrが記憶するワーク鍵Kw(k)は一致しない。従って、スクランブル鍵復号部110は、ワーク鍵設定エラーをCPU150に通知する。

【００５６】

時刻Tにおいて録画機100に対応するデバイスID(p+1)を含むEMMが、時刻Uにおいて録画機100に対応する暗号化ワーク鍵Kd(p+1)[Kw(k+1)]を含むEMMが送信される。従って、録画機100は、時刻Tにおいて、デバイスID(p+1)を受信してデバイス鍵Kd(p+1)を生成し、レジスタKdrを更新する。そして、時刻Uにおいて、暗号化ワーク鍵を受信してワーク鍵Kw(k+1)を復号し、レジスタKwrを更新する。

【００５７】

時刻Uにおいて、スクランブル鍵復号部110は、ECMに含まれるスクランブル鍵を、更新されたワーク鍵Kw(k+1)を用いて復号する。この時点で、スクランブル鍵の暗号化に使用されたワーク鍵Kwと、復号に用いるワーク鍵Kwが一致するので、スクランブル鍵復号部110は、スクランブル鍵を正常に復号することが可能になり、ワーク鍵設定エラーを解除する。

【００５８】

CPU150は、ワーク鍵設定エラーが解除されると、記録媒体に記録したストリームCR1を読み出し、ストリームCR1のスクランブルの解除とデコードを開始する。なお、コントローラ121と記録装置122は、ストリームCR1の記録、記録媒体に記録したストリームCR1の読み出し、および、後述するストリームCR2の記録を時分割により並列処理する。CPU150は、セレクタ104の選択出力を端子Aに切り替え、セレクタ104は、IF120が出力する信号を選択出力する。CPU150は、記録媒体から読み出したストリームCR1をIF120を介してセレクタ104の端子Aに入力する。

【００５９】

これにより、伝送制御信号分離部113は、ストリームCR1からコンテンツCを含むストリームを分離する。復号部105は、分離されたストリームのスクラブルを解除する。分離部106は、スクランブルが解除されたストリームからコンテンツCのストリームを分離する。MPEGデコーダ107は、分離されたストリームからコンテンツCをデコードする。MPEGエンコーダ108は、デコードされたコンテンツCをPSに再エンコードする。再エンコードされたPSは、IF120を経由して、コントローラ121と記録装置122によって記録媒体に記録される。

【００６０】

図5において、CR2は、上記の動作により、スクランブルが解除されたPSが記録媒体に記録される様子を示している。

【００６１】

図6はモードAが設定された場合の録画機100の予約録画動作を説明するフローチャートで、CPU150の制御によって実行される動作である。

【００６２】

CPU150は、録画予約された時刻Sになると、録画機100をパワーオンし、録画動作を開始する(S101)。そして、選局部102を制御して、チャネル設定を予約チャネルに設定し(S102)、セレクタ104の選択出力を端子Bに設定する(S103)。

【００６３】

次に、CPU150は、IF120とコントローラ121を制御して、復調部103が復調したTSの記録を開始し(S104)、TSはストリームCR1として記録媒体に記録される。

【００６４】

次に、CPU150は、スクランブル鍵復号部110からワーク鍵設定エラーが通知されているか否かの判定(S105)を繰り返す。スクランブル鍵復号部110は、レジスタKwrのワーク鍵Krによって、ECMに含まれるスクランブル鍵の復号に成功すると、ワーク鍵設定エラーを解除する。

【００６５】

ワーク鍵設定エラーが解除されると、CPU150は、セレクタ104の選択出力を端子Aに切り替える(S106)。そして、コントローラ121とIF120を制御して、記録媒体からのストリームCR1の読み出しを開始して、セレクタ104の端子Aに入力する(S107)。

【００６６】

この時点では、正しいデバイス鍵が生成され、正しいワーク鍵Kwが設定され、スクランブル鍵が復号されている。従って、復号部105は、ストリームCR1の先頭からスクランブルを解除することができる。CPU150は、分離部106、MPEGデコーダ107、MPEGエンコーダ108を制御して、スクランブルを解除したストリームCR1をPSに再エンコードする(S108)。そして、IF120とコントローラ121を制御して、記録媒体へのPS（ストリームCR2）の記録を開始する(S109)。

【００６７】

この後、録画機100は、録画終了時刻E1まで上記の録画動作を継続する。

【００６８】

CPU150は、録画終了時刻E1か否かの判定(S110)を繰り返し、録画終了時刻E1になると、ストリームCR1の記録を終了する(S111)。さらに、ストリームCR1の読み出しが完了したか否かを判定し(S112)、完了するとストリームCR1の読み出しからPSの再エンコードまでの処理を終了し(S113)、PS（ストリームCR2）の記録を終了する(S114)。録画機100の予約録

画動作は時刻E2において終了する。なお、ストリームCR1の読み出しが完了した後、記録媒体からストリームCR1を削除することが好ましい。

【００６９】

ここで、モードC、Bが設定された場合について、モードAの処理と異なる点を説明する。

【００７０】

モードCが設定された場合、CPU150は、ワーク鍵設定エラーが解除されると(S105)、ストリームCR1の読み出しを開始する(S107)。しかし、ストリームCR1のスクランブルを解除するだけで、PSに再デコードせずに、IF120に送る。そして、IF120とコントローラ121を制御して、スクランブルを解除したTSを記録媒体に記録する。つまり、スクランブルされたTSをバッファし、正しいスクランブル鍵を復号した後、スクランブルの解除を開始する点は、モードAの場合と同様である。

【００７１】

また、モードBが設定された場合は、スクランブルを解除する必要はないので、復調部103が復調したTS（限定受信に関する情報を含む）を記録媒体に記録するだけである。

【００７２】

このように、スクランブルを解除したフォーマットによる記録モードが設定された場合、受信したTSをバッファして、スクランブルが解除できるようになった（ワーク鍵を復号した）時点で、バッファしたTSのスクランブル解除を開始する。従って、録画機100がパワーオフ状態にある録画開始前に暗号鍵が更新された場合も、番組のコンテンツを正常に復号し、予約録画を指示された番組の映像、音声を視聴可能な状態で記録することができる。

【実施例２】

【００７３】

以下、本発明にかかる実施例2の放送受信機、録画機を説明する。なお、実施例2において、実施例1と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００７４】

図7はモードAが設定された場合の実施例2の録画機100の予約録画動作を説明するタイミングチャートである。

【００７５】

実施例1（図5）と同様に、時刻R1において、EMMに含まれるデバイスIDがID(p)からID(p+1)に更新され、時刻R2において、ワーク鍵がKw(k)からKw(k+1)に更新される。録画機100は、時刻Sより前はパワーオフ状態にあり、放送の受信を休止していたとする。

【００７６】

録画機100は、時刻Sにおいてパワーオン状態になり、モードAの予約録画を開始する。

【００７７】

図8、図9はモードAが設定された場合の実施例2の録画機100の予約録画動作を説明するフローチャートで、CPU150の制御によって実行される動作である。

【００７８】

CPU150は、録画予約された時刻Sになると、録画機100をパワーオンし、録画動作を開始する(S201)。そして、選局部102を制御して、チャネル設定を予約チャネルに設定し(S202)、セレクタ104の選択出力を端子Bに設定する(S203)。

【００７９】

次に、CPU150は、IF120とコントローラ121を制御して、復調部103が復調したTSの記録を開始し(S204)、TSはストリームCR1として記録媒体に記録される。

【００８０】

次に、CPU150は、スクランブル鍵復号部110からワーク鍵設定エラーが通知されているか否かの判定(S205)を繰り返す。スクランブル鍵復号部110は、レジスタKwrのワーク鍵Krによって、ECMに含まれるスクランブル鍵の復号に成功すると、ワーク鍵設定エラーを解除する（時刻U）。

【００８１】
ワーク鍵設定エラーが解除されると、この時点で、正しいデバイス鍵が生成され、正しいワーク鍵Kwが設定され、スクランブル鍵が復号されている。従って、復号部105は、復調されたTSのスクランブルを解除することができる。CPU150は、分離部106、MPEGデコーダ107、MPEGエンコーダ108を制御して、スクランブルを解除したTSをPSに再エンコードする(S206)。そして、IF120とコントローラ121を制御して、記録媒体へのPS（ストリームCR2）の記録を開始し(S207)、ストリームCR1の記録を終了する(S208)。つまり、時刻U以後、記録媒体には、受信中のTSのスクランブルが解除され、デコード、再エンコードされたPS（ストリームCR2）が記録される。
【００８２】
この後、録画機100は、録画終了時刻E1までPS（ストリームCR2）の録画動作を継続する。
【００８３】
CPU150は、録画終了時刻E1か否かの判定(S209)を繰り返し、録画終了時刻E1になると、PS（ストリームCR2）の記録を終了し(S210)、時刻SからUの間に記録したストリームCR1の処理を開始する。つまり、CPU150は、セレクタ104の選択出力を端子Aに切り替える(S211)。そして、コントローラ121とIF120を制御して、記録媒体からのストリームCR1の読み出しを開始して、セレクタ104の端子Aに入力する(S212)。
【００８４】
復号部105は、ストリームCR1の先頭からスクランブルを解除する。CPU150は、分離部106、MPEGデコーダ107、MPEGエンコーダ108を制御して、スクランブルを解除したストリームCR1をPSに再エンコードする(S213)。そして、IF120とコントローラ121を制御して、記録媒体へのPS（ストリームCR3）の記録を開始する(S214)。
【００８５】
次に、CPU150は、ストリームCR1の読み出しが完了したか否かを判定し(S215)、完了するとストリームCR1の読み出しからPSの再エンコードまでの処理を終了し(S216)、PS（ストリームCR3）の記録を終了する(S217)。
【００８６】
この時点で、記録媒体には二つのPS、ストリームCR2とCR3が存在することになる。ストリームCR3は時刻SからUのコンテンツに相当し、ストリームCR2は時刻U以後のコンテンツに相当する。CPU150は、コントローラ121を制御して、ストリームCR2の前にストリームCR3を結合して(S218)、一つのストリームCR2にする。その際、CPU150は、ストリームCR3とCR2が時間的に連続する結合点を検出し、二つのストリームを結合する。録画機100の予約録画動作は時刻E2において終了する。なお、読み出しが完了したストリームCR1、および、結合後のストリームCR3は記録媒体から削除することが好ましい。
【００８７】
このように、スクランブルを解除したフォーマットによる記録モードが設定された場合、受信したTSをバッファする。そして、スクランブルが解除できるようになった（ワーク鍵を復号した）時点で、TSのスクランブルを解除して、デコード、再エンコードしたPS(CR2)の記録を開始し、TSをバッファリングを終了する。そして、録画終了時刻にバッファしたTSのスクランブルを解除して、デコード、再エンコードしたPS(CR3)を記録する。さらに、CR2の前にCR3を結合して、一つのストリームにする。
【００８８】
従って、実施例1と同様に、録画機100がパワーオフ状態にある録画開始前に暗号鍵が更新された場合も、番組のコンテンツを正常に復号し、予約録画を指示された番組の映像、音声を視聴可能な状態で記録することができる。また、実施例2の場合は、記録媒体に対する書き込みと読み出しの並列処理が実施例1に比べて少なくなる。従って、実施例2は、記録装置122などのデータ転送帯域が小さいシステムにも適用することができる。
【実施例３】
【００８９】

以下、本発明にかかる実施例3の放送受信機、録画機を説明する。なお、実施例3において、実施例1、2と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００９０】

実施例3の録画機100は、EMMの順次送信の周期を測定して、測定結果に基づき予約録画動作を制御する。

【００９１】

［EMMの順次送信周期の測定］

EMMの順次送信周期の測定は、放送の視聴や録画が行われていない期間、言い換えれば録画機100がパワーオフ状態にある期間に定期的に実行される。また、放送の視聴状態において、視聴中のチャネルに関して、EMMの順次送信周期を測定し、測定結果を更新してもよい。

【００９２】

図10はEMMの順次送信周期の測定処理の一例を示すフローチャトで、CPU150は、放送の視聴や録画が行われていない期間に、定期的に、EMMの順次送信周期を測定する。

【００９３】

CPU150は、選局部102を制御して測定対象のチャネルを選局する(S301)。なお、EMMの順次送信周期の測定周期は、チャネルごとに異なる値を設定することも可能である。その場合、チャネルごとに、EMMの順次送信周期を測定し、測定結果をテーブルに格納する。

【００９４】

次に、CPU150は、自機種向けの暗号化ワーク鍵を含むEMMの受信を待ち(S302)、当該EMMを受信すると、カウンタまたはタイマをスタートする(S303)。

【００９５】

次に、CPU150は、再び、自機種向けの暗号化ワーク鍵を含むEMMの受信を待つ(S304)。そして、当該EMMを受信すると、カウンタまたはタイマをストップし(S305)、カウンタのカウント値またはタイマの計時時間を、EMMの順次送信周期として、RAM151またはNVメモリ152の所定領域に格納し(S306)、処理を終了する。なお、計時開始前に、カウンタまたはタイマは初期化されていることは言うまでもない。

【００９６】

［予約録画方法］

図11はモードAが設定された場合の実施例3の録画機100の予約録画動作を説明するタイミングチャートである。

【００９７】

実施例1（図5）と同様に、時刻R1において、EMMに含まれるデバイスIDがID(p)からID(p+1)に更新され、時刻R2において、ワーク鍵がKw(k)からKw(k+1)に更新される。また、録画機100には、時刻S2からの予約録画が設定されているとする。

【００９８】

図12はモードAが設定された場合の実施例3の録画機100の予約録画動作を説明するフローチャートで、CPU150の制御によって実行される動作である。

【００９９】

CPU150は、録画開始時刻S2よりも所定時間Soff前の時刻S1に録画機100をパワーオンする(S401)。そして、選局部102を制御して、チャネル設定を予約チャネルに設定して放送の受信を開始し(S402)、セレクタ104の選択出力を端子Bに設定する(S403)。

【０１００】

CPU150は、所定時間Soffに、EMMの順次送信周期の二倍の時間を設定とする。これは、デバイスIDの取得に一周期、さらに、暗号化ワーク鍵の取得に一周期かかるとしても充分な時間である。従って、CPU150は、時刻Tにおいてデバイスを取得し、時刻Uにおいて暗号化ワーク鍵を取得することができ、録画開始時刻S2以前にスクランブル鍵を復号することができる。

【０１０１】

CPU150は、録画開始時刻S2か否かの判定(S404)を繰り返し、録画開始時刻S2になると、受信したTSのスクランブルを解除し、デコード、再エンコードしたPS（ストリームCR2）の記録媒体への記録を開始する(S405)。

【０１０２】

この後、録画機100は、録画終了時刻E1までPS（ストリームCR2）の録画動作を継続する。

【０１０３】

CPU150は、録画終了時刻E1か否かの判定(S406)を繰り返し、録画終了時刻E1になると、PS（ストリームCR2）の記録（予約録画動作）を終了する(S407)。

【０１０４】

このように、録画開始時刻S2よりSoff時間（EMMの順次送信周期の二倍）前に放送の受信を開始するため、録画開始時刻S2には、必ず、スクランブルの解除が可能な状態にある。従って、録画開始時刻S2以後に、番組のコンテンツの復号が不能になることはなく、予約録画を指示された番組の映像、音声を視聴可能な状態で記録することができる。

【０１０５】

［他の実施例］

なお、本発明は、複数の機器（例えばコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置、制御装置など）に適用してもよい。

【０１０６】

また、本発明の目的は、上記実施例の機能を実現するコンピュータプログラムを記録した記録媒体または記憶媒体をシステムまたは装置に供給する。そして、そのシステムまたは装置のコンピュータ（CPUやMPU）が前記コンピュータプログラムを実行することでも達成される。この場合、記録媒体から読み出されたソフトウェア自体が上記実施例の機能を実現することになり、そのコンピュータプログラムと、そのコンピュータプログラムを記憶する、コンピュータが読み取り可能な記録媒体は本発明を構成する。

【０１０７】

また、前記コンピュータプログラムの実行により上記機能が実現されるだけではない。つまり、そのコンピュータプログラムの指示により、コンピュータ上で稼働するオペレーティングシステム(OS)および/または第一の、第二の、第三の、…プログラムなどが実際の処理の一部または全部を行い、それによって上記機能が実現される場合も含む。

【０１０８】

また、前記コンピュータプログラムがコンピュータに接続された機能拡張カードやユニットなどのデバイスのメモリに書き込まれていてもよい。つまり、そのコンピュータプログラムの指示により、第一の、第二の、第三の、…デバイスのCPUなどが実際の処理の一部または全部を行い、それによって上記機能が実現される場合も含む。

【０１０９】

本発明を前記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応または関連するコンピュータプログラムが格納される。

【図面の簡単な説明】

【０１１０】

【図１】実施例の録画機の構成例を示すブロック図、

【図２】システム部の構成例を示すブロック図、

【図３】暗号鍵の更新の概要を説明するタイミングチャート、

【図４】鍵の更新が正常に行われずにコンテンツの復号が正常に行えないケースを説明するタイミングチャート、

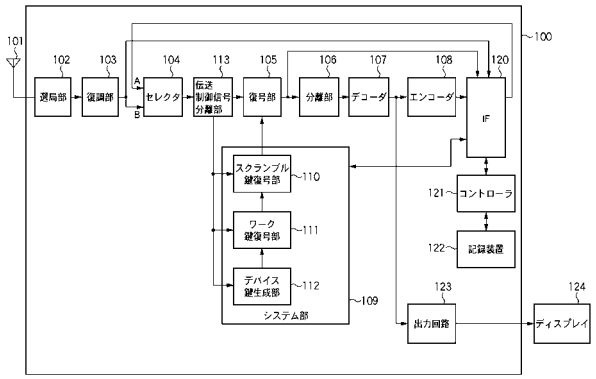
【図５】モードAが設定された場合の録画機の予約録画動作を説明するタイミングチャート、

【図６】モードAが設定された場合の録画機の予約録画動作を説明するフローチャート、

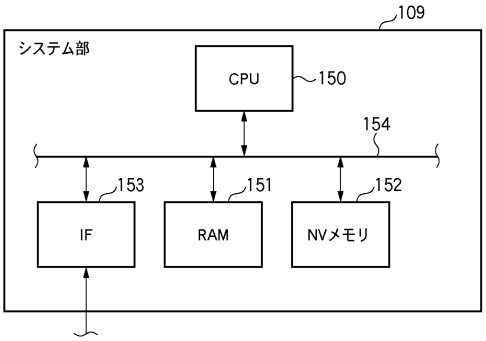
【図７】モードAが設定された場合の実施例2の録画機の予約録画動作を説明するタイミン

グチャート、
【図８】モードAが設定された場合の実施例2の録画機の予約録画動作を説明するフローチャート、
【図９】モードAが設定された場合の実施例2の録画機の予約録画動作を説明するフローチャート、
【図１０】EMMの順次送信周期の測定処理の一例を示すフローチャート、
【図１１】モードAが設定された場合の実施例3の録画機の予約録画動作を説明するタイミングチャート、
【図１２】モードAが設定された場合の実施例3の録画機の予約録画動作を説明するフローチャートである。

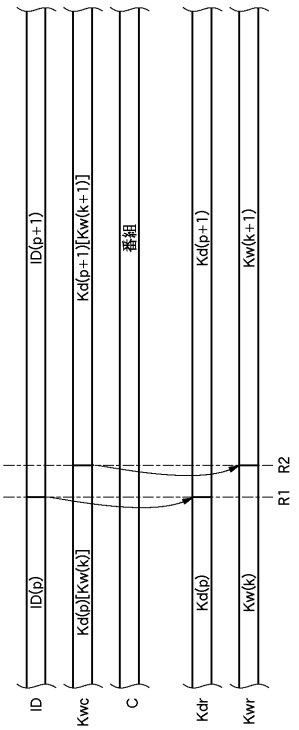
【図１】



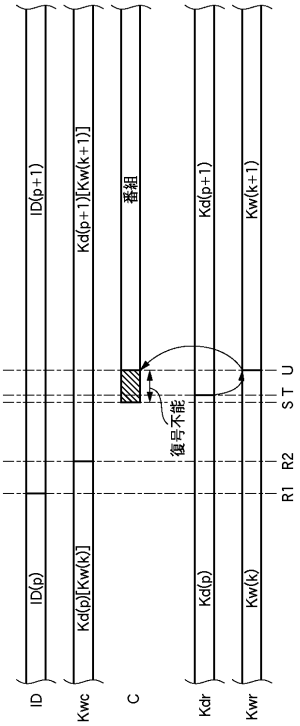
【図２】



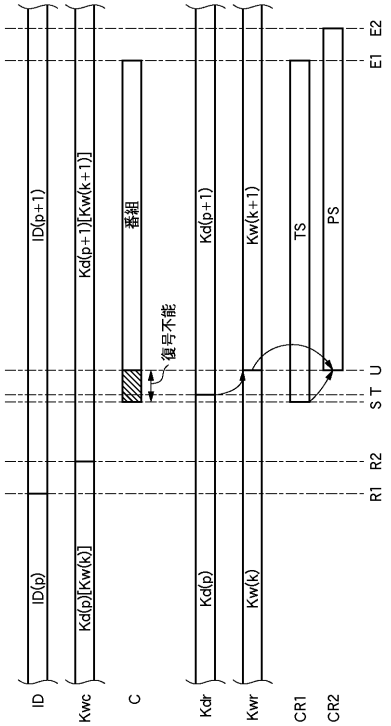
【図３】



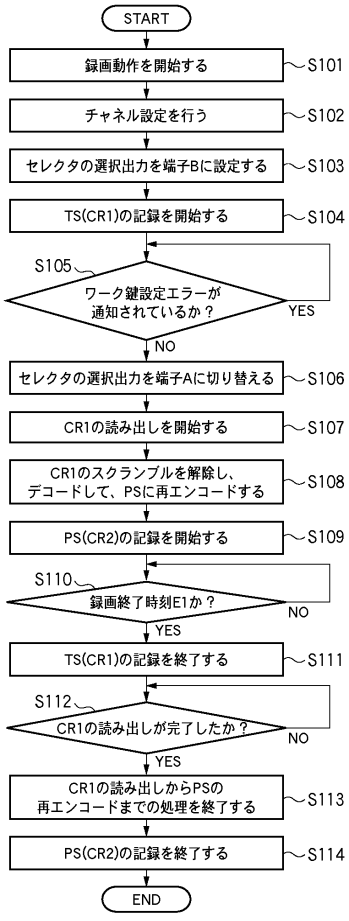
【図４】


ID(p+1)
Kd(p+1)[Kw(k+1)]
番組
Kd(p+1)
Kw(k+1)
ID(p)
Kd(p)[Kw(k)]
Kd(p)
Kw(k)
復号不能
S T U
R2
R1
ID
Kwc
C
Kdr
Kwr

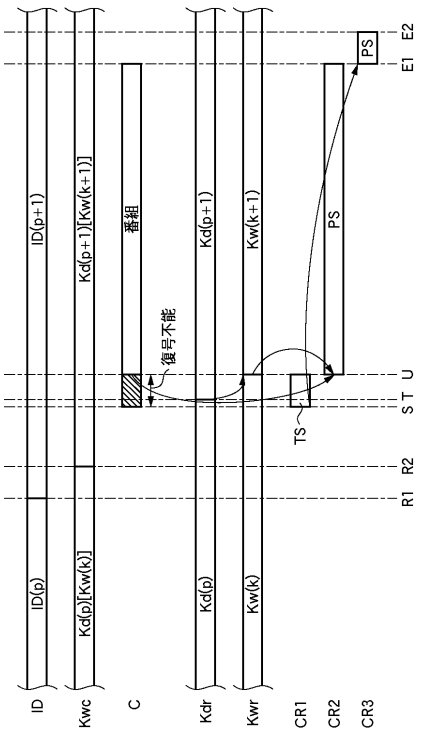
【図５】


E2
E1
ID(p+1)
Kd(p+1)[Kw(k+1)]
番組
Kd(p+1)
Kw(k+1)
TS
PS
復号不能
S T U
R2
R1
ID(p)
Kd(p)[Kw(k)]
Kd(p)
Kw(k)
ID
Kwc
C
Kdr
Kwr
CR1
CR2

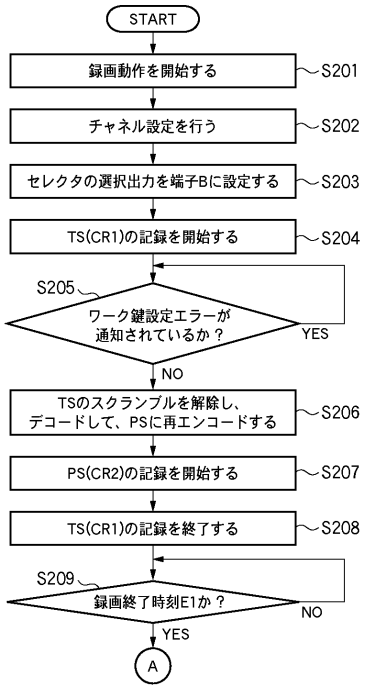
【図６】


START
録画動作を開始する
S101
チャネル設定を行う
S102
セレクタの選択出力を端子Bに設定する
S103
TS(CR1)の記録を開始する
S104
S105
ワーク鍵設定エラーが通知されているか？
YES
NO
セレクタの選択出力を端子Aに切り替える
S106
CR1の読み出しを開始する
S107
CR1のスクランブルを解除し、デコードして、PSに再エンコードする
S108
PS(CR2)の記録を開始する
S109
S110
録画終了時刻E1か？
NO
YES
TS(CR1)の記録を終了する
S111
S112
CR1の読み出しが完了したか？
NO
YES
CR1の読み出しからPSの再エンコードまでの処理を終了する
S113
PS(CR2)の記録を終了する
S114
END

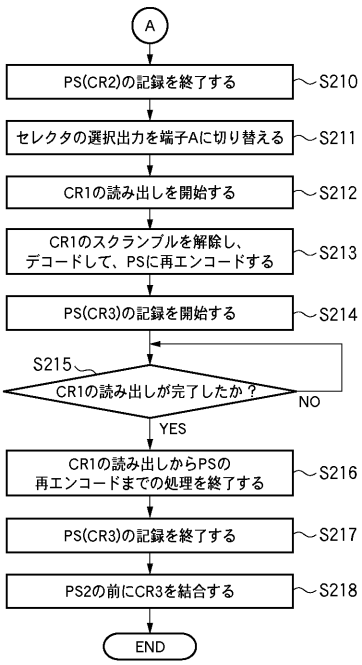
【図７】


PS
E2
E1
ID(p+1)
Kd(p+1)[Kw(k+1)]
番組
Kd(p+1)
Kw(k+1)
PS
復号不能
TS
S T U
R2
R1
ID(p)
Kd(p)[Kw(k)]
Kd(p)
Kw(k)
ID
Kwc
C
Kdr
Kwr
CR1
CR2
CR3

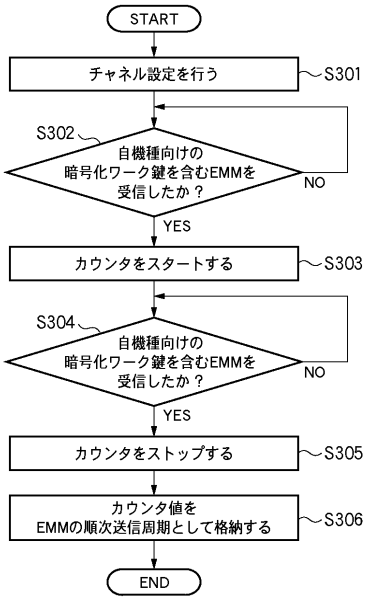
【図８】


START
録画動作を開始する
S201
チャネル設定を行う
S202
セレクタの選択出力を端子Bに設定する
S203
TS(CR1)の記録を開始する
S204
S205
ワーク鍵設定エラーが通知されているか？
YES
NO
TSのスクランブルを解除し、デコードして、PSに再エンコードする
S206
PS(CR2)の記録を開始する
S207
TS(CR1)の記録を終了する
S208
S209
録画終了時刻E1か？
NO
YES
A

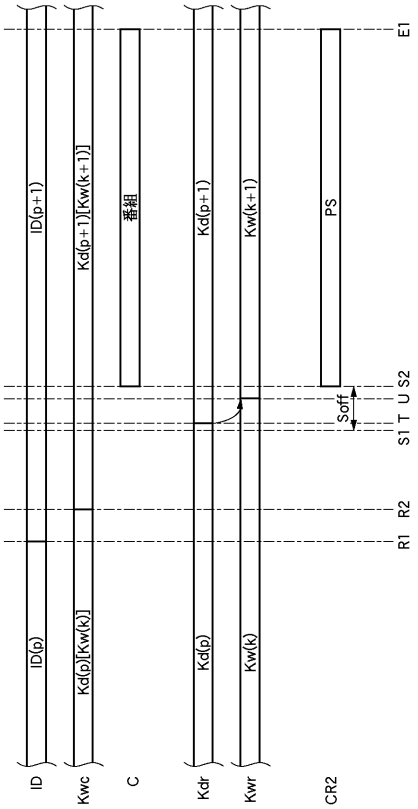
【図９】


A
PS(CR2)の記録を終了する
S210
セレクタの選択出力を端子Aに切り替える
S211
CR1の読み出しを開始する
S212
CR1のスクランブルを解除し、デコードして、PSに再エンコードする
S213
PS(CR3)の記録を開始する
S214
S215
CR1の読み出しが完了したか？
NO
YES
CR1の読み出しからPSの再エンコードまでの処理を終了する
S216
PS(CR3)の記録を終了する
S217
PS2の前にCR3を結合する
S218
END

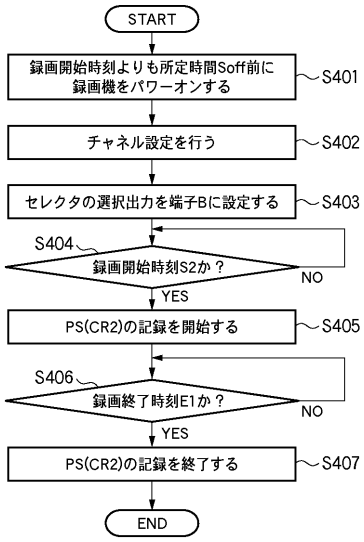
【図１０】


START
チャネル設定を行う
S301
S302
自機種向けの暗号化ワーク鍵を含むEMMを受信したか？
NO
YES
カウンタをスタートする
S303
S304
自機種向けの暗号化ワーク鍵を含むEMMを受信したか？
NO
YES
カウンタをストップする
S305
カウンタ値をEMMの順次送信周期として格納する
S306
END

【図１１】


E1
S2
U
T
S1
R2
R1
Soff
ID(p+1)
Kd(p+1)[Kw(k+1)]
番組
Kd(p+1)
Kw(k+1)
PS
ID(p)
Kd(p)[Kw(k)]
Kd(p)
Kw(k)
ID
Kwc
C
Kdr
Kwr
CR2

【図１２】


START
録画開始時刻よりも所定時間Soff前に
録画機をパワーオンする
S401
チャネル設定を行う
S402
セレクタの選択出力を端子Bに設定する
S403
S404
録画開始時刻S2か？
NO
YES
PS(CR2)の記録を開始する
S405
S406
録画終了時刻E1か？
NO
YES
PS(CR2)の記録を終了する
S407
END

フロントページの続き

(72)発明者　嵯峨　吉博
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　松永　稔

(56)参考文献　特開平０５－１４５９２２（ＪＰ，Ａ）
特開２００８－５２３６４５（ＪＰ，Ａ）
特開２００８－１５４０１４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　　５／９１
Ｇ１１Ｂ　２０／１０