(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2008-11547
(P2008-11547A)
(43)公開日　平成20年1月17日(2008.1.17)

(51)Int.Cl.		F I			テーマコード（参考）
H04H 60/15	(2008.01)	H04H	1/00	613	5C164
H04H 20/06	(2008.01)	H04H	1/00	208	5J104
H04H 20/74	(2008.01)	H04H	1/00	286	
H04H 20/79	(2008.01)	H04H	1/04	220	
H04H 60/23	(2008.01)	H04H	1/00	621	

審査請求 有　請求項の数 2　ＯＬ　（全 14 頁）　最終頁に続く

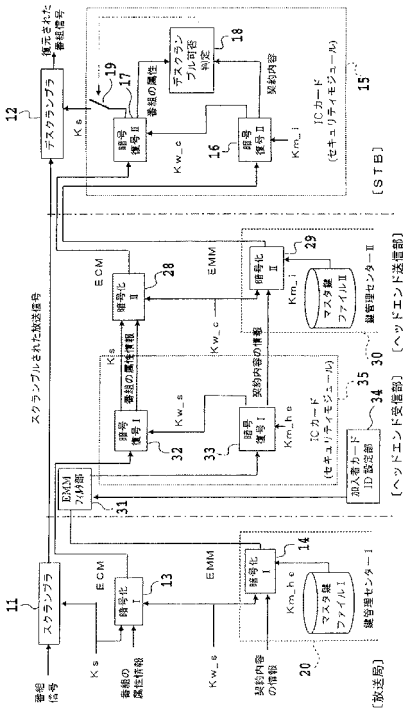
(21)出願番号　特願2007-198169 (P2007-198169)
(22)出願日　平成19年7月30日 (2007.7.30)
(62)分割の表示　特願平11-294575の分割
原出願日　平成11年10月15日 (1999.10.15)

(71)出願人　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　難波　誠一
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内

Ｆターム(参考)　5C164 FA03　PA24　PA25　SB03P SB06S SC02P
5J104 AA01　AA35　DA04　PA05

(54)【発明の名称】限定受信方式の処理装置及び処理方法

(57)【要約】
【課題】衛星放送波等の放送伝送路をＣＡＳを用いて伝送された放送信号を受信して、ＣＡＴＶ等の放送伝送路を別のＣＡＳを用いて再送信して放送する際に、限定受信の制御に用いられる情報を安全に転送すること。
【解決手段】衛星放送の番組信号はスクランブラ１１でスクランブルされ、デスクランブルせずに、ＳＴＢへ転送される。ＥＣＭとＥＭＭがヘッドエンドを介してＳＴＢに転送される。衛星放送の放送局側で関連情報がＳ－ＣＡＳ方式で暗号化され、得られたＥＣＭ，ＥＭＭはＣＡＴＶのヘッドエンド受信部で暗号復号手段３２，３３によって復号され、暗号化手段２８，２９によって、Ｃ－ＣＡＳ方式で再暗号化してＳＴＢへ転送される。セキュリティの観点から、全受信機に共通な鍵情報と各受信機に個別な情報とで暗号化の方法を別個とする。
【選択図】図１



【特許請求の範囲】
【請求項１】
放送信号をスクランブルアルゴリズムで暗号化するためのスクランブル鍵と、該スクランブル鍵及び全受信機に共通な番組属性情報を第１の暗号化アルゴリズムで暗号化するための第１のワーク鍵と、該第１のワーク鍵及び受信機ごとに個別の契約内容の情報を前記第１の暗号化アルゴリズムで暗号化するための第１のマスタ鍵とを用いた第１の限定受信方式を使用した第１の放送伝送路で放送された放送信号及び前記スクランブル鍵及び番組属性情報、第１のワーク鍵及び契約内容の情報を受信して、
複数の第２の放送伝送路で各々の第２のワーク鍵と第２のマスタ鍵と第２の暗号化アルゴリズムを用いる第２の限定受信方式を使用して再暗号化して、前記第２の放送伝送路において再送信する際に、前記第２の放送伝送路のヘッドエンドでの限定受信方式の処理方法であって、
前記スクランブルアルゴリズム及び前記スクランブル鍵を用いて暗号化された放送信号は、受信された信号をそのまま再送信し、
前記スクランブル鍵及び前記番組の属性情報は、該ヘッドエンドごとに個別でかつ該ヘッドエンドより第２の放送伝送路を通して受信する全受信機に共通な第１のマスタ鍵を用いて、該ヘッドエンドで前記第１のワーク鍵が外部に漏れないハードウェア構成を持ったセキュリティモジュールを用いて暗号復号して得られた、第１のワーク鍵を用いて暗号復号して得られたスクランブル鍵及び番組属性情報を、該ヘッドエンドにおいて生成した第２のワーク鍵と前記第２の暗号化アルゴリズムを用いて再暗号化して再送信し、
前記契約内容の情報は、前記第１のマスタ鍵を用いて該ヘッドエンドで暗号復号して得られた契約内容の情報を、前記第２のワーク鍵とともに、前記各々の第２の放送伝送路を通して受信する受信機ごとに個別な第２のマスタ鍵と第２の暗号化アルゴリズムを用いて再暗号化して再送信する、
各ステップを有することを特徴とする限定受信方式の処理方法。
【請求項２】
放送信号をスクランブルアルゴリズムで暗号化するためのスクランブル鍵と、該スクランブル鍵及び全受信機に共通な番組属性情報を第１の暗号化アルゴリズムで暗号化するための第１のワーク鍵と、該第１のワーク鍵及び受信機ごとに個別の契約内容の情報を前記第１の暗号化アルゴリズムで暗号化するための第１のマスタ鍵とを用いた第１の限定受信方式を使用した第１の放送伝送路で放送された放送信号及び前記スクランブル鍵及び番組属性情報、第１のワーク鍵及び契約内容の情報を受信して、
複数の第２の放送伝送路で各々の第２のワーク鍵と第２のマスタ鍵と第２の暗号化アルゴリズムを用いる第２の限定受信方式を使用して再暗号化して、前記第２の放送伝送路において再送信する、前記第２の放送伝送路のヘッドエンドに設けられた限定受信方式の処理装置であって、
前記スクランブルアルゴリズム及び前記スクランブル鍵を用いて暗号化された放送信号は、受信された信号をそのまま再送信する手段と、
前記スクランブル鍵及び前記番組の属性情報は、該ヘッドエンドごとに個別でかつ該ヘッドエンドより第２の放送伝送路を通して受信する全受信機に共通な第１のマスタ鍵を用いて、該ヘッドエンドで前記第１のワーク鍵が外部に漏れないハードウェア構成を持ったセキュリティモジュールを用いて暗号復号して得られた、第１のワーク鍵を用いて暗号復号して得られたスクランブル鍵及び番組属性情報を、該ヘッドエンドにおいて生成した第２のワーク鍵と前記第２の暗号化アルゴリズムを用いて再暗号化して再送信する手段と、
前記契約内容の情報は、前記第１のマスタ鍵を用いて該ヘッドエンドで暗号復号して得られた契約内容の情報を、前記第２のワーク鍵とともに、前記各々の第２の放送伝送路を通して受信する受信機ごとに個別な第２のマスタ鍵と第２の暗号化アルゴリズムを用いて再暗号化して再送信する手段と、
を備えたことを特徴とする限定受信方式の処理装置。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は限定受信方式における関連情報の処理装置に関するものである。特に衛星放送や地上放送など第１の放送伝送路で限定受信方式を用いて放送された信号を、ＣＡＴＶなどの第２の放送伝送路を用いる放送システムで限定受信方式を用いて再送信して放送する際に適用される限定受信方式における関連情報の処理装置に関するものである。なお、ここで、限定受信方式の持つ機能としては、有料放送を行うために信号をスクランブルして送信する場合の受信制御の機能の他に、信号をスクランブルするか否かにかかわらず、放送において受信機ごとに個別のメッセージを表示させるなど特定の受信機を選択して制御するための情報を伝達できる機能も対象とする。
【背景技術】
【０００２】
限定受信方式（以下、ＣＡＳと記す）の基本的なシステム構成を図２に示す。ここで、放送局内のスクランブラ１で番組信号をスクランブルする方法は、我国の衛星デジタル放送では、ブロック暗号方式が採用されているが、この暗号化の鍵、すなわち信号をスクランブルするための鍵（スクランブル鍵：以下Ｋｓと呼ぶ）は例えば、１秒単位の時間で変化させることにより不正受信に対する安全性を高めている。受信機側のデスクランブラ２で信号をデスクランブルするためには、このＫｓの情報を知る必要がある。このＫｓは放送局内の暗号化手段３において、その番組に関する属性情報とともに別な鍵（ワーク鍵：以下Ｋｗと呼ぶ）で暗号化され、番組情報（以下、ＥＣＭと呼ぶ）と呼ばれる関連情報（平成１０年郵政省令第５７号、平成１０年郵政省告示第２６０号参照）として受信機側に送られる。さらに、Ｋｗは安全性を保つために、例えば、１ケ月や１年といった単位で更新できるようになっている。このＫｗも電波のようなどこからでもアクセスできる媒体で伝送する場合には、暗号化して送る必要がある。従って、このＫｗは各受信機が契約している内容を示すための情報（契約内容の情報）とともに、個別情報（以下、ＥＭＭと呼ぶ）と呼ばれる関連情報として、受信機に送られる。このＥＭＭも電波などで伝送する場合には、不正に利用したり情報内容が改ざんされたりしないように暗号化手段４によって暗号化される。この暗号化のための鍵（マスタ鍵：以下Ｋｍと呼ぶ）は一般に受信機毎に異なる。これらの暗号の復号処理や受信判定の処理は受信機内に設けられた集積回路や、受信機本体から取り外し可能なセキュリティモジュールで行われるが、近年後者としてＣＰＵ内蔵のＩＣカード５を用いて実用化されるシステムが多い。このＩＣカードは、例えば、ＣＰＵと、後述するような所定の情報およびＣＰＵによりその機能が実現される各手段の制御手順が格納されているＥＥＰＲＯＭなどのメモリとを有する。すなわち、このＩＣカード５は、情報としてＫｍを有し、受信機内に取り付けられた状態で、このＫｍを用いて受信したＥＭＭから暗号復号手段６によって契約内容の情報とＫｗとを復号し、暗号復号手段７によって、受信したＥＣＭからＫｓとその番組に関する属性情報とを復号し、デスクランブル可否判定手段８によって、暗号復号手段６からの契約内容と、暗号復号手段７からの番組の属性情報とに基づいて当該放送（番組）のデスクランブルの可否を判定し、可能な場合は、暗号復号手段７からデスクランブラ２にＫｓを供給するためのスイッチ９を閉じる。これによって、デスクランブラ２によってデスクランブルされ復元された番組信号が得られる。
【０００３】
上述した鍵のうち、Ｋｗはその放送を受信する全ての受信機に対して共通であるが、Ｋｍは受信機ごとに異なっている。このとき、Ｋｍは同じ受信機へ向けて放送する事業者間では同じ鍵を用いて各受信機の契約内容の情報を暗号化することが受信機での処理を簡略化するために望ましい。すなわち、各放送事業者ごとの契約内容の情報はそれぞれの放送事業者で作成するが、これをＥＭＭとして受信機に送る際の暗号化に使用されるＫｍは放送事業者間で統一的に管理する必要がある（各放送事業者ごとに複製して管理すると、いずれかで漏れた場合には、追跡も困難と予想され、大きな影響が出ることになる）。このために、鍵管理センター１０と呼ばれる組織が放送局側に設けられ、ここで、暗号化手段

４を用いて各放送事業者が作成したＥＭＭの暗号化を統一して行うのが一般的である。

【０００４】

以上は単一の放送伝送路でのＣＡＳの基本的な構成であるが、次に、衛星放送等で放送された番組をＣＡＴＶのヘッドエンドで受信して、ＣＡＴＶに再送信する場合を考える。

【０００５】

図２に示したようなＣＡＳの構成は、例えば衛星放送のシステムでも、ＣＡＴＶのシステムでも共通である。しかし、衛星放送の系統とＣＡＴＶのシステムを接続する場合には、スクランブルの行い方と、関連情報の伝送、処理方法においていくつかの組み合わせが存在する。

【０００６】

信号をスクランブルして放送する場合には、信号をデスクランブルするために必要な前述の鍵（ＫｓやＫｗ）の情報を受信機まで送る必要がある。また、有料放送等のようにＣＡＳの機能を用いて放送を行う場合には、信号デスクランブル用の鍵の情報とともに、各受信者に各番組が契約されていて受信可能か否か、すなわちデスクランブルを行うか否かの判定を受信機で行えるようにするための情報を送る必要がある。このとき、一般にある番組を受信するために必要なＫｓやＫｗは全受信機に共通な情報であるが、契約を判定するための情報は受信機ごとに個別の情報項目である。これらの関連情報をＣＡＴＶに伝える方法が衛星放送事業者やＣＡＴＶ事業者の事業形態に大きく影響する。

【０００７】

衛星放送波等の第１の伝送路でＣＡＳを用いて放送された放送番組を受信して、ケーブル等の第２の伝送路に再送信する場合の代表的なシステム構成を図３及び図４に示す。

【０００８】

図３はＣＡＴＶのヘッドエンドで受信した衛星放送波の信号をそのまま、あるいは変調方式や伝送周波数のみを変換してケーブルに再送信するものである。図３において、１１はスクランブラ、１２はデスクランブラ、１３，１４は暗号化手段、１５は受信機のＳＴＢに設けられたＩＣカード、１６，１７は暗号復号手段、１８はデスクランブル可否判定手段、１９はスイッチ、２０は鍵管理センターであって、１１，１３，１４，２０は放送局側に設けられており、１２，１５，１６，１７，１８，１９は受信機側に設けられている。これらは図２で説明したものと同様である。なお、ＳＴＢ（セットトップボックス）は、受信機の基本機能を実現するための部分である。また、スイッチ１９はゲート回路でも良い（後述する各図におけるスイッチも同様である）。

【０００９】

この図３の場合、ＣＡＳは衛星放送のものをそのまま使用するので、受信機に対しては衛星放送波を直接受信する場合と同等の制御や、受信者管理を行うことができる。一方、ＣＡＴＶ事業者が衛星放送番組の再送信の他に、ヘッドエンドから独自の番組の有料放送を行うシステムも存在し、この場合、視聴者の利便性を考えると、再送信用番組と独自番組を同じ受信機で受信できることが望ましい。これは図３のようなシステムでは、ＣＡＴＶにおいて衛星放送のＣＡＳと同じ方式を用いることで実現できる（この系統は図３には示していない）。この場合のシステムでのマスタ鍵の管理は衛星放送側で統一的に行うことが基本となるので、ＣＡＴＶ事業者の事業の独立性に関して制限が出ることが想定される。従って、これが放送事業上問題になる場合には採用されにくい。

【００１０】

図４はＣＡＴＶのヘッドエンドで衛星放送等のＣＡＳ方式（以下Ｓ－ＣＡＳ方式と記す）の復元処理を行い、通常の信号に戻した後に、ＣＡＴＶの伝送路に送出する形態のシステムを示す。図４において、２１はデスクランブラ、２７はスクランブラ、２２，２３は暗号復号手段、２４はデスクランブル可否判定手段、２５はスイッチ、２６はヘッドエンド受信部に設けられたＩＣカード、２８，２９は暗号化手段、３０は鍵管理センターであって、１１，１３，１４，２０は放送局側に設けられており、２１，２２，２３，２４，２５，２６，２７，２８，２９，３０はヘッドエンドに設けられており、１２，１５，１６，１７，１８，１９は受信機側に設けられている。これらは図２で説明したものと同様

である。

【００１１】

図４に示す構成は、アナログの衛星放送の時代から実施されている形態である。以下では、衛星放送等の第１の伝送路ではデジタル信号で伝送するデジタル放送を考えるが、ケーブルへの再送信には従来からのアナログ伝送の場合と、デジタル伝送の場合があり、それぞれについて考える。アナログ伝送の場合、衛星放送等で信号にスクランブルがかけられている場合には、ヘッドエンドでデスクランブルを行い、その出力信号をスクランブルせずに再送信する場合と、そのＣＡＴＶシステムでＳ－ＣＡＳ方式とは別の方式（以下、Ｃ－ＣＡＳ方式と記す）でスクランブルを行って再送信する場合とがある。スクランブルを行う場合の構成は例えば図４のようになる。これは図２の基本的なシステムを衛星伝送路の部分とケーブル伝送路の部分で独立に設けて、縦続接続した形態である。この方式では、ＣＡＴＶ内は完全にＣＡＴＶ事業者が管理するが、衛星放送事業者はＣＡＴＶ内の加入者を個別に直接管理することはできない。すなわち、衛星放送事業者とヘッドエンドの間は当該ヘッドエンドに対応するマスタ鍵Ｋｍ_ｈｅ（ヘッドエンドのマスタ鍵）を持つＩＣカードを用いて、一括して受信制御を行い、復元された番組信号を再度Ｃ－ＣＡＳ方式でスクランブルして各加入者の受信機に送信する。

【発明の開示】

【発明が解決しようとする課題】

【００１２】

近年、ＣＡＴＶにおいても信号をデジタル伝送するデジタル放送化が始まっているが、デジタル放送では、放送される番組の数が増大するとともに、各種のデータと組み合せた新たな機能を持った放送が行われる。また、これらの放送に対して多様な課金を行うことが考えられる、従って、ケーブルで衛星デジタル放送等を再送信する場合、番組の視聴や運用の面で衛星放送事業者側の要求する多様な機能がどの程度各受信機（基本機能はＳＴＢに備えられている）で実現できるかが問題となる。特に、有料放送を行う場合に実現できる機能など、衛星放送等で放送された信号をケーブルでデジタル伝送により再送信する場合についての検討が不十分であった。

【００１３】

以下では、ＣＡＴＶで再送信する場合の限定受信方式の機能について検討する。

【００１４】

まず、信号のスクランブル方式については、衛星デジタル放送とケーブルデジタル放送とで同一の場合を扱うこととする。さらに、衛星放送を再送信する番組の信号のスクランブルは衛星の放送局側で行い、ケーブルデジタル放送のヘッドエンドではデスクランブルを行わず、そのまま再送信し、ＳＴＢでデスクランブルする場合を考える。このとき、Ｋｓを含む関連情報の伝送方式や暗号化方式は、衛星デジタル放送とケーブルデジタル放送とで等しい場合と異なる場合を考える。

【００１５】

（ａ）Ｃ－ＣＡＳ方式がＳ－ＣＡＳ方式と同一の場合

これは図３の場合に当たり、各ＳＴＢでＳ－ＣＡＳ方式と同じＩＣカードで受信することができるが、前述のように、ヘッドエンドでケーブル放送独自の番組をスクランブルして放送する場合、この契約のためのＥＭＭの暗号化は衛星放送側の鍵管理センターで行う必要があるなど事業の独立性の点が問題になる。しかし、技術的に特に大きな問題はないと考えられるので以下では扱わない。

【００１６】

（ｂ）Ｃ－ＣＡＳ方式とＳ－ＣＡＳ方式が異なる場合

これは図４の構成の場合に当たる。この図に示すような従来の形態は、チャンネルの少ないアナログ衛星放送のような場合には使用できるが、衛星デジタル放送等の多チャンネル、多機能の信号をＣＡＴＶに再送信して、衛星放送事業者側でＣＡＳを利用した多様なサービスをセキュリティ上の問題を生じることなく行うには機能が不十分である。ＣＡＴＶを介して各加入者を直接管理するには、各加入者宛ての衛星デジタル放送の関連情報を衛

星放送の放送局側でＳ－ＣＡＳ方式により暗号化し、ケーブルデジタル放送のヘッドエンドで復号し、得られた平文のＥＭＭをＣ－ＣＡＳ方式で再暗号化して送ることになる。このとき、一般的に考えると、ヘッドエンドの装置では、ＥＭＭが暗号がかかっていない状態で現れ、再度暗号化されることになる。このＥＭＭに含まれる情報のうち、Ｋｗは全受信機に共通のものであり、これが外部に漏れると、ここで考えているＣＡＳ方式全体のセキュリティが崩れることになる。

【００１７】

上述したＣＡＳ方式は受信側ではＫｗが外部から読み出し不可能なＩＣカード等のセキュリティモジュールの中でのみ現れ、セキュリティモジュールの外部にはそのＫｗを用いて復号処理した結果のＫｓのみ現れるようにできることが、安全性の根拠となっている（各受信機のＫｍを守っても、どこかでＫｗが知られれば意味がなくなる）。このＥＭＭの暗号復号処理は全国のケーブル局のヘッドエンドで行われるので、そのうちのいずれかのセキュリティ対策の十分でない局から漏れると、全衛星放送のセキュリティが崩れるので、極めて厳重に注意しなければならない。一方、ＥＭＭに含まれる情報の内、Ｋｗ以外の部分が外部に漏れる場合は、これらはあくまでもそのケーブル事業者に接続されている受信者で衛星デジタル放送に加入している人の情報であるので、他の放送事業者へ及ぼす影響は少ないと考えられる。

【００１８】

本発明は、衛星デジタル放送側の持つ限定受信方式の所要機能が、ケーブル側に転送されて実現され、しかもこの転送の際にセキュリティ（安全性）上の問題を生じない関連情報の伝送を可能にすることを目的としている。特に、衛星デジタル放送の事業者側でＣＡＴＶ内で衛星デジタル放送を受信している人をセキュリティを損なうことなく直接管理可能にすることを目的としている。

【課題を解決するための手段】

【００１９】

本発明では、第１に、ヘッドエンドにおいて関連情報を転送する際に、Ｋｗが外部に現れるとセキュリティが維持できなくなる点を解決するために、衛星デジタル放送の放送局とヘッドエンドとの間には、一般の受信機を対象とした関連情報伝送方式とは異なる方式を適用する。すなわち、あるケーブルデジタル放送局内で再送信される衛星デジタル放送を受信するためのＥＭＭを衛星デジタル放送局から送る場合に、ケーブル事業者のヘッドエンド向けの新たな関連情報伝送方式を適用する。

【００２０】

また、前述のように、ＣＡＴＶ内での信号スクランブル方式が衛星デジタル放送と同一である場合を対象としているので、特に、スクランブルされた信号のパケットをヘッドエンドで復号し、再スクランブルする必要はない。しかし、このデスクランブルの制御に用いるＫｓを含むＥＣＭの暗号化に関しては、前述のようにＥＣＭの暗号化に使用されるＫｗはセキュリティ上、Ｓ－ＣＡＳ方式とＣ－ＣＡＳ方式とで変える必要があり、最終的にはＳＴＢでＣ－ＣＡＳ方式の復号処理を行う必要がある。このため、ヘッドエンドでＳ－ＣＡＳ方式によるＥＣＭの暗号を復号し、再度Ｃ－ＣＡＳ方式による暗号化を行う。このとき、ケーブルでＥＣＭの再暗号化に使用するものをＫｗ＿ｃ、衛星側で使用しているものをＫｗ＿ｓとする。

【００２１】

ＥＭＭは、一般に、ＥＭＭ伝送の宛先（受信機、ＳＴＢ、デコーダ、ＩＣカード等のセキュリティモジュール等）の識別番号（以下では、代表的にカードＩＤと記す）、ＥＣＭの暗号化のための鍵であるＫｗ、各受信機の契約内容に関する情報（以下では、簡単に契約情報と記す）とで構成される。このＥＭＭに対して、本発明では、カードＩＤ（暗号化されない）と契約情報（受信機個別の鍵で暗号化される）を衛星放送側からＣＡＴＶへ転送し、Ｋｗは転送しないような関連情報の伝送処理方法を適用する。すなわち、各受信機の個別制御に必須な情報は転送するが、全受信機に共通で、漏れることによりセキュリティ上の影響が大きい項目には転送の処理を行わないことを特徴とする関連情報の伝送、処

理方法を適用する。

【００２２】

請求項１の発明は、放送信号をスクランブルアルゴリズムで暗号化するためのスクランブル鍵（図１，Ｋｓ）と、該スクランブル鍵及び全受信機に共通な番組属性情報を第１の暗号化アルゴリズム（図１、暗号化I）で暗号化するための第１のワーク鍵（図１，Ｋｗｓ）と、該第１のワーク鍵及び受信機ごとに個別の契約内容の情報を前記第１の暗号化アルゴリズムで暗号化するための第１のマスタ鍵（図１，Ｋｍ　ｈｅ）とを用いた第１の限定受信方式を使用した第１の放送伝送路で放送された放送信号及び前記スクランブル鍵及び番組属性情報、第１のワーク鍵及び契約内容の情報を受信して、複数の第２の放送伝送路で各々の第２のワーク鍵（図１，Ｋｗ　ｃ）と第２のマスタ鍵（図１，Ｋｍ　ｉ）と第２の暗号化アルゴリズム（図１、暗号化II）を用いる第２の限定受信方式を使用して再暗号化して、前記第２の放送伝送路において再送信する際に、前記第２の放送伝送路のヘッドエンドでの限定受信方式の処理方法であって、前記スクランブルアルゴリズム及び前記スクランブル鍵を用いて暗号化された放送信号は、受信された信号をそのまま再送信し、前記スクランブル鍵及び前記番組の属性情報は、該ヘッドエンドごとに個別でかつ該ヘッドエンドより第２の放送伝送路を通して受信する全受信機（図１、ＳＴＢ）に共通な第１のマスタ鍵（図１，Ｋｍ　ｈｅ）を用いて、該ヘッドエンドで前記第１のワーク鍵が外部に漏れないハードウェア構成を持ったセキュリティモジュール（図１，３５）を用いて暗号復号して得られた、第１のワーク鍵を用いて暗号復号して得られたスクランブル鍵及び番組属性情報を、該ヘッドエンドにおいて生成した第２のワーク鍵と前記第２の暗号化アルゴリズムを用いて再暗号化して再送信し、前記契約内容の情報は、前記第１のマスタ鍵を用いて該ヘッドエンドで暗号復号して得られた契約内容の情報を、前記第２のワーク鍵とともに、前記各々の第２の放送伝送路を通して受信する受信機ごとに個別な第２のマスタ鍵と第２の暗号化アルゴリズムを用いて再暗号化して再送信する各ステップを有することを特徴とする。

【００２３】

また請求項２の発明は、放送信号をスクランブルアルゴリズムで暗号化するためのスクランブル鍵（図１，Ｋｓ）と、該スクランブル鍵及び全受信機に共通な番組属性情報を第１の暗号化アルゴリズム（図１、暗号化I）で暗号化するための第１のワーク鍵（図１，Ｋｗ　ｓ）と、該第１のワーク鍵及び受信機ごとに個別の契約内容の情報を前記第１の暗号化アルゴリズムで暗号化するための第１のマスタ鍵（図１，Ｋｍ　ｈｅ）とを用いた第１の限定受信方式を使用した第１の放送伝送路で放送された放送信号及び前記スクランブル鍵及び番組属性情報、第１のワーク鍵及び契約内容の情報を受信して、複数の第２の放送伝送路で各々の第２のワーク鍵（図１，Ｋｗ　ｃ）と第２のマスタ鍵（図１，Ｋｍ　ｉ）と第２の暗号化アルゴリズム（図１、暗号化II）を用いる第２の限定受信方式を使用して再暗号化して、前記第２の放送伝送路において再送信する、前記第２の放送伝送路のヘッドエンドに設けられた限定受信方式の処理装置であって、前記スクランブルアルゴリズム及び前記スクランブル鍵を用いて暗号化された放送信号は、受信された信号をそのまま再送信する手段と、前記スクランブル鍵及び前記番組の属性情報は、該ヘッドエンドごとに個別でかつ該ヘッドエンドより第２の放送伝送路を通して受信する全受信機（図１、ＳＴＢ）に共通な第１のマスタ鍵（図１，Ｋｍ　ｈｅ）を用いて、該ヘッドエンドで前記第１のワーク鍵が外部に漏れないハードウェア構成を持ったセキュリティモジュール（図１，３５）を用いて暗号復号して得られた、第１のワーク鍵を用いて暗号復号して得られたスクランブル鍵及び番組属性情報を、該ヘッドエンドにおいて生成した第２のワーク鍵と前記第２の暗号化アルゴリズムを用いて再暗号化して再送信する手段（図１、２８）と、前記契約内容の情報は、前記第１のマスタ鍵を用いて該ヘッドエンドで暗号復号して得られた契約内容の情報を、前記第２のワーク鍵とともに、前記各々の第２の放送伝送路を通して受信する受信機ごとに個別な第２のマスタ鍵と第２の暗号化アルゴリズムを用いて再暗号化して再送信する手段（図１、２９）と、を備えたことを特徴とする。

【発明の効果】

【００２４】
本発明によれば、衛星放送等の第１の放送伝送路で第１の限定受信方式を使用して放送された信号を受信し、ＣＡＴＶ等の第２の放送伝送路に第２の限定受信方式を使用して再送信する際に、前記第２の放送伝送路からの信号を受信する受信機を個別に制御するための情報を含む関連情報を、安全性を損なうことなく転送することができる。
【発明を実施するための最良の形態】
【００２５】
図１は本発明の実施例を示す。この図に含まれる各構成要素の機能については、図２～図４で説明した要素に対応しているものは説明を省略または簡単にする。すなわち、１１はスクランブラ、１３，１４は暗号化手段、２０は鍵管理センターであって、これらは放送局側に設けられており、３１はＥＭＭフィルタ部、３２，３３は暗号復号手段、２８，２９は暗号化手段、３０は鍵管理センター、３４は加入者カードＩＤ設定部、３５はヘッドエンド受信部に設けられたＩＣカードであって、これらはヘッドエンドに設けられており、１２はデスクランブラ、１５はＩＣカード、１６，１７は暗号復号手段、１８はデスクランブル可否判定手段、１９はスイッチであって、これらは受信機側に設けられている。
【００２６】
この実施例では衛星放送の番組信号はスクランブラ１１でスクランブルされるが、ヘッドエンドではデスクランブルせずに、そのままＳＴＢへ転送される。従って、ＳＴＢのデスクランブラ１２では衛星放送のスクランブルをデスクランブルする必要があるので、これに必要なＥＣＭとＥＭＭがヘッドエンドを介してＳＴＢに転送される。この図１では衛星放送等の放送局側で関連情報がＳ－ＣＡＳ方式で暗号化され（暗号化I）、この暗号化により得られたＥＣＭ，ＥＭＭはＣＡＴＶのヘッドエンド受信部で暗号復号手段３２，３３によって復号され（詳細は後述するが、ＥＭＭに関しては、ＥＭＭフィルタ部３１によってフィルタリングされたＥＭＭのみが復号され）、暗号化手段２８，２９によって、Ｃ－ＣＡＳ方式で再暗号化（暗号化II）してＳＴＢへ転送される。ここで、前述のセキュリティの観点から、Ｓ－ＣＡＳ方式でのＫｗ（Ｋｗ_ｓ）とＣ－ＣＡＳ方式でのＫｗ（ＫＷ_ｃ）とは別個とする。
【００２７】
デジタル放送ではＥＣＭ，ＥＭＭ，ＥＭＭメッセージの各関連情報はセクションと呼ばれる図５のような構造で送信される。ＥＭＭについて、さらに具体的な構成例を示すと図６のようになる。関連情報は暗号化して伝送される。その暗号化される範囲についてはセキュリティの点で一般に公開されないが、少なくともセクションのヘッダ部は暗号化されない。また、ＥＭＭは大量に送信される情報の中から各受信機で自分宛の情報を抽出し、ＩＣカードにおいて暗号復号を行うが、この自分宛の情報の抽出は高速に行う必要があることから、カードＩＤ部は暗号化されない。従って、従来のＥＭＭのセクションでは、図６のカードＩＤ部のあとの契約情報「契約情報_ｉ」（ｉ番目のデコーダにおける契約情報）がｉ番目のマスタ鍵Ｋｍ_ｉで暗号化される。
【００２８】
一方、衛星放送事業者がＣＡＴＶ内で衛星デジタル放送に加入している人を直接管理するために以下に述べる方法でＥＭＭセクションを利用して転送を行う。すなわち、衛星放送事業者がＣＡＴＶ内で衛星デジタル放送に加入している人を直接管理するためにＥＭＭを各ＳＴＢに転送する必要があるが、このためには、ＣＡＴＶのヘッドエンドにおいて衛星放送の大量のＥＭＭから各ＣＡＴＶ内の加入者の分のＥＭＭを抽出して復号し、さらにＣ－ＣＡＳ方式で再暗号化する必要がある。これを行うには、該当するカードＩＤの全ＥＭＭを順次受信し、それぞれの対応するＫｍ_ｉを用いて順次暗号を復号する必要があるが、このＫｍ_ｉはセキュリティを維持するために外部からアクセスできないＩＣカードの内部のみに存在する前提になっている。従って、ヘッドエンドには、例えば、ＣＡＴＶ内の加入者分のＩＣカードを並列に置く必要がある。このような装置は現実的ではない。このため、以下に述べるような方法でＥＭＭセクションを利用して転送を行うこととする

。

【００２９】

図７は本発明で使用するＣＡＴＶヘッドエンド向けにＣＡＴＶ内の衛星放送の加入者のＥＭＭやＥＭＭ個別メッセージを送るためのセクションの例を示している。従来のＣＡＴＶ内ＥＭＭセクションは、図８のように、各カードＩＤ_ｉの後の契約情報_ｉはそれぞれ異なるＫｍ_ｉで暗号化される。これに対して、図７のＥＭＭセクションは各カードＩＤ_ｉの後の契約情報_ｉは同一のＫｍ_ｈｅ（ヘッドエンド用マスタ鍵）で暗号化される。

【００３０】

次に、図１の構成によってヘッドエンドで図７の形式によるセクションを受信して図８の従来の形式によるＣＡＴＶ用のセクションに変換する過程を説明する。ヘッドエンドには加入者カードＩＤ設定部３４を設け、ここで当該ＣＡＴＶ内で当該衛星デジタル放送に加入している、すなわち、衛星デジタル放送のＥＭＭを転送する必要のあるＳＴＢのカードＩＤを蓄積している。ここから各力一ドＩＤを順次ＥＭＭフィルタ部３１へ与えることにより、衛星放送波から各ＣＡＴＶ内の加入者のＥＭＭを抽出し、ヘッドエンド用ＩＣカード３５に順次転送して暗号復号処理を行なう。

【００３１】

このとき、ヘッドエンド用のＩＣカード内の処理プログラムは一般の衛星放送の直接受信用のＩＣカードとは異なる。すなわち、一般のＩＣカードからはＥＭＭの復号結果はＩＣカードの中に記憶され外部には現れないが、ヘッドエンド用のＩＣカードでは各受信者の契約情報を再度Ｃ－ＣＡＳ方式で暗号化してＳＴＢに送るために出力する必要がある。一般のＩＣカード（例えば図２の５）では、ＥＭＭを各ＩＣカードのＫｍ（Ｋｍ_ｉ）で復号すると、Ｋｗ_ｓとその受信者の契約情報_ｉが得られるがこれらはＩＣカードの中に記憶され、外部から読み出すことはできないようになっている。このＫｗ_ｓを用いてＥＣＭの暗号を復号するとＫｓと番組の属性情報が得られる。このＫｓはＩＣカードから出力されデスクランブラに供給されるが、番組の属性情報はＩＣカードの中で契約情報との照合のみに使用されＩＣカードから外部に出力されることはない。しかし、本発明によるヘッドエンド用のＩＣカードでは、図７に示すようなＥＭＭをヘッドエンド用のＫｍ（Ｋｍ_ｈｅ）で復号すると、Ｋｗ_ｓと当該ＣＡＴＶ内の各加入者の契約情報_ｉが得られる。この内、Ｋｗ_ｓはＩＣカードの中に記憶されるが、契約情報_ｉはＩＣカードからのレスポンスとして外部に出力される。ＥＣＭが受信されると、ヘッドエンド用ＩＣカードでは、記憶されているＫｗ_ｓを用いて暗号を復号し、Ｋｓと番組の属性情報を得る。これらはＩＣカードからのレスポンスとして外部に出力される。この出力されたＫｓと番組の属性情報は暗号化手段２８によってＣＡＴＶ用のＫｗ（Ｋｗ_ｃ）で暗号化され（暗号化II）、ＣＡＴＶのＥＣＭとして送出される。一方、ＥＭＭは各カードＩＤごとに、ヘッドエンド用ＩＣカードから出力された契約情報にＣＡＴＶのＫｗ_ｃを加えて暗号化手段２９によってＣＡＴＶのマスタ鍵Ｋｍ_ｉで暗号化して図８に示すようなＣＡＴＶのＥＭＭを構成して送出する。

【００３２】

なお、このＣＡＴＶで送出されるセクションの構成は、衛星デジタル放送を直接受信する場合のＥＭＭセクションと同一である。このため、ＳＴＢの機能や設計は衛星デジタル放送のＩＲＤと共通になり、受信機コストを下げることができる。

【００３３】

前述したように、ＣＡＴＶのヘッドエンドでは、そのＣＡＴＶ内で衛星デジタル放送に加入する全てのＳＴＢ宛てのＥＭＭを選別受信（フィルタリング）してＩＣカード３５に転送する。ＩＣカード３５に転送した後は、全て同じＫｍ（Ｋｍ_ｈｅ）で復号する。転送前の当該ＣＡＴＶ内での全加入者宛てのＥＭＭのフィルタリングは鍵管理上のセキュリティの問題はないが、フィルタリング処理は高速に行う必要がある。この部分は、ＣＡＴＶ事業者のヘッドエンドに置かれる装置であり、一般の受信機のように簡易のものである必要は少ないが、かなり大規模なものとなることが予想される。このため、カードＩＤ設定部とＥＭＭフィルタ部の処理を効率的に行うために、運用上、ＣＡＴＶ用のＳＴＢに用

いられるカードＩＤ（衛星デジタル放送の規格では４８ビット）の特定のビットをＣＡＴＶの事業者コードとすることが効果的である。すなわち、カードＩＤの特定のビットが一致するもののみ抽出してＩＣカード３５に転送すればよく、ＩＤの照合動作が極めて容易になる。また、ＩＣカードへの転送の時間を考慮して、衛星デジタル放送の送出側で、各ＣＡＴＶ内ＳＴＢ宛てのＥＭＭの送信間隔を一定時間以上空けて送出することが適当である。

【００３４】

なお、衛星放送局側から当該ＣＡＴＶ内で加入している受信機へのＥＭＭは衛星放送の伝送路を用いず、まとめて、通信回線等を用いてヘッドエンドまで届けることもできる。この場合には、ヘッドエンドで一括受信するので、衛星放送伝送路側の負担は軽くなるが、ＣＡＴＶ側でＥＭＭを確実に受信するための繰り返し伝送などの制御を行う必要がある（衛星放送波により配布する場合は、一般には予め繰り返し伝送されるので、ヘッドエンドでは受信したまま送出すればよい。）。

【００３５】

次に、各ＳＴＢでは、ケーブルを介して衛星デジタル放送事業者のチャンネルとＣＡＴＶ事業者のチャンネルを同一のＩＣカードで受信できるようにするためには、両チャンネルを受信するためのＥＭＭのカードＩＤは共通に管理する必要がある。しかし、カードＩＤに対する各カードのマスタ鍵Ｋｍ_ｉは衛星放送事業者とＣＡＴＶ事業者では独立なものを使用することができる。この場合、衛星放送事業者では、ＣＡＴＶ内で加入したＳＴＢに対しては、対応するヘッドエンド用のＫｍ_ｈｅのみ使用し、他のＫｍ_ｉは衛星を直接受信するＩＲＤに割り当てられることになる。

【００３６】

ところで、本発明では、ＣＡＴＶ内各受信者の衛星放送事業者への契約内容がヘッドエンドで暗号化されない状態で現れるので、ここでの不正が行われることが想定される。この影響は、前述したように、当該ＣＡＴＶ事業者内に限られ、衛星デジタル放送のＣＡＳ全体の安全性に関わることはないが、この安全性が問題になる場合には、衛星放送側の暗号をかけたままＥＭＭを処理する必要がある。図９はこれを実現するシステム構成例であり、放送局側で暗号化するＥＭＭについては、カードＩＤ部分はされず、他はＳ－ＣＡＳ方式でのＫｍｓ_ｉで暗号化されている。ヘッドエンドで受信した衛星放送からのＥＣＭ，ＥＭＭを復号することなく、さらに暗号化手段３６，３７，３８を用いてＣ－ＣＡＳ方式で暗号化（暗号化II）して再送信を行う。この場合、ＳＴＢにおけるＩＣカード１５（セキュリティモジュール）では、まず、暗号復号手段３９，４０を用いてＣ－ＣＡＳ方式でヘッドエンドからのＥＣＭ，ＥＭＭを復号（暗号復号II）し、この復号後のＥＭＭが衛星デジタル放送事業者のものである場合には、さらに暗号復号手段４１，４２を用いてＳ－ＣＡＳ方式の暗号復号（暗号復号II）を行う。この方式では、ＥＣＭはヘッドエンドで暗号復号せずに、そのままＣＡＴＶのＫｗ（Ｋｗ_ｃ）で暗号化して送出する。ＥＭＭについては、衛星放送から受信したものはＳ－ＣＡＳ方式で暗号化されている部分（Ｓ－ＣＡＳ方式でのｉ番目の受信機向けのＫｍであるＫｍｓ_ｉで暗号化されている）はそのまま再度Ｃ－ＣＡＳ方式で暗号化してケーブルに送出する。このときの鍵は、Ｃ－ＣＡＳ方式でのｉ番目の受信機向けのＫｍであるＫｍｃ_ｉである。この方式では、ＳＴＢのＩＣカード等のセキュリティモジュール内には、少なくともＣ－ＣＡＳ方式とＳ－ＣＡＳ方式の複数の暗号アルゴリズムとＫｍすなわちＫｍｃ_ｉとＫｍｓ_ｉを実装している必要がある。この方式では、さらに、ケーブル側でＫｗ_ｃで再暗号化したＥＣＭを復号するためのＫｗ_ｃをＳＴＢへ送る必要があり、暗号化手段３７によってＫｗ_ｃを送るためのＥＭＭを別途ヘッドエンドから加える。このＥＭＭは同じ衛星放送から転送されたＥＭＭと同じカードＩＤでＫｍｃ_ｉで暗号化して送る。ＳＴＢでは、自分宛のＥＭＭを受信すると、ＩＣカードに転送して暗号復号手段４０によってＫｍｃ_ｉで暗号復号する（暗号復号II）。受信したＥＭＭがＫｗ_ｃを伝送するためのものである場合には、ＩＣカードの中に記憶して、暗号復号手段３９によってＥＣＭの復号に用いる。受信したＥＭＭが衛星放送のＥＭＭを再暗号化したものである場合には、復号されたＥＭＭをさらに暗号復号手段４

２によってＫｍｓ_ｉで暗号復号して（暗号復号Ｉ）、後は衛星放送の直接受信と同様に衛星放送のＥＣＭを復号し、番組の属性情報と契約内容とからデスクランブル可否判定手段４３によってデスクランブルの可否を判定して、スイッチ４４を閉じてＫｓを出力する。この方式では、図９には示してないが、ＣＡＴＶ事業者独自の番組の制御も、ＳＴＢで暗号復号Ｉの処理を省略することにより同様に行うことができる。

【００３７】

限定受信方式の機能を利用すると、各受信機に向けて個別のメッセージを送り、画面に表示することができる。この場合、ＥＭＭメッセージのセクションを利用して送るが、伝送の効率を上げるために、各受信機に向けた個別のメッセージは表示する定型文の番号で送り、実際のメッセージ内容は別途定型文番号を付した全受信機に共通のメッセージとして送る方法がある。このような方法で衛星デジタル放送で特定の受信機にメッセージを送る場合、その受信機が再送信されているＣＡＴＶ内にあるときには、ヘッドエンドで関連情報を転送するしくみが必要である。これも例えば図１に示した実施例のシステムで伝送することができる。このとき、上記の全受信機に共通な定型文メッセージの内容は暗号化されない規格であるので、ヘッドエンドでは特段の処理を行うことなく、そのＥＭＭメッセージセクションをＣＡＴＶに転送できる。一方、各受信機ごとに異なる定型文の番号を示す個別のメッセージセクションはＥＭＭと同様にＫｍ_ｉで暗号化されているので、本質的に本発明で説明したＥＭＭの伝送の場合と変わらない。ただし、ＥＭＭメッセージの場合にはＥＣＭの暗号を復号するためのＫｗは送られないので、Ｋｗのセキュリティに関する事項は関係なくなり、ＥＭＭの転送の問題よりも容易に実現できる。

【図面の簡単な説明】

【００３８】

【図１】本発明の実施例のシステム構成を示す図である。

【図２】限定受信方式（ＣＡＳ）の基本的なシステム構成を示す図である。

【図３】従来のシステム構成を示す図である。

【図４】従来の他のシステム構成を示す図である。

【図５】デジタル放送で関連情報（ＥＣＭ，ＥＭＭ）を伝送するセクションの構成を示す図である。

【図６】ＥＭＭを伝送するセクションの構成例を示す図である。

【図７】本発明に使用するＥＭＭセクションの構成を示す図である。

【図８】受信機に伝送されるＥＭＭセクションの構成を示す図である。

【図９】本発明の実施例のシステム構成を示す図である。

【符号の説明】

【００３９】

１，１１　　スクランブラ

２，１２，２７　　デスクランブラ

３，４，１３，１４，２８，２９，３６，３７，３８　　暗号化手段

５，１５，３５　　ＩＣカード

６，７，１６，１７，２２，２３，３２，３３，３９，４０，４１，４２　　暗号復号手段

８，１８，２４，４３　　デスクランブル可否判定手段

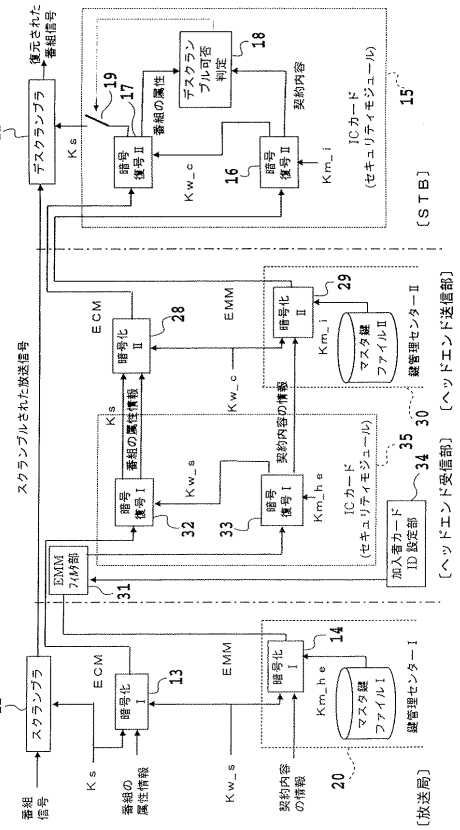
９，１９，２５，４４　　スイッチ

１０，２０，３０　　鍵管理センター

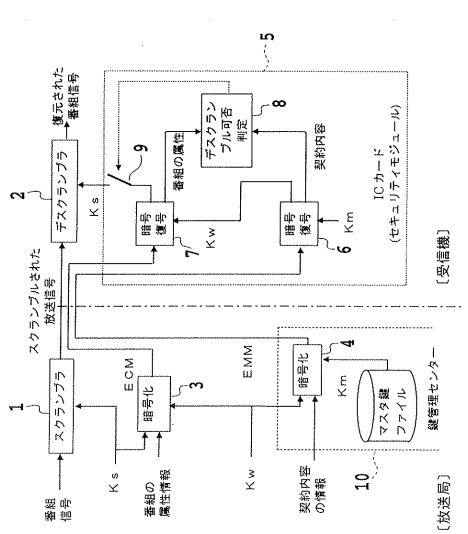
３１　　ＥＭＭフィルタ

３４　　加入者カードＩＤ設定部

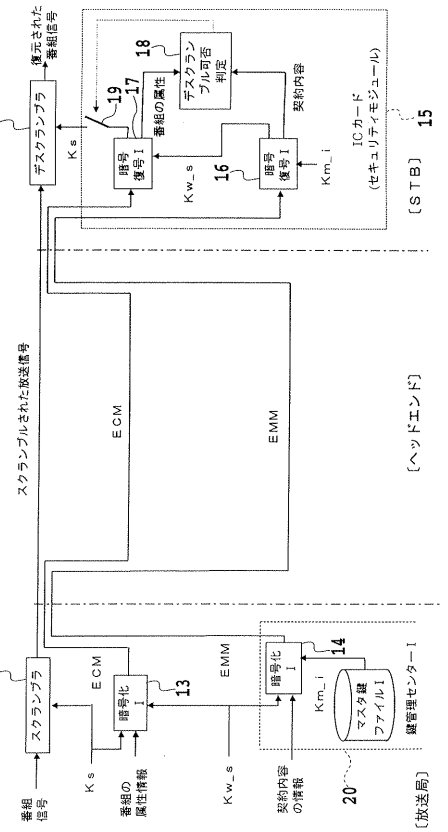
【図１】


スクランブルされた放送信号
番組信号
Ks
番組の属性情報
Kw_s
契約内容の情報
スクランブラ
ECM
暗号化Ⅰ
EMM
暗号化Ⅰ
Km_he
マスタ鍵ファイルⅠ
鍵管理センターⅠ
〔放送局〕
EMM用処理部
加入者カードID設定部
暗号化Ⅱ
Km_i
マスタ鍵ファイルⅡ
鍵管理センターⅡ
〔ヘッドエンド送信部〕
〔ヘッドエンド受信部〕
デスクランブラ
復元された番組信号
暗号復号Ⅰ
暗号復号Ⅱ
Kw_c
番組の属性
デスクランブル可否判定
契約内容
ICカード（セキュリティモジュール）
〔STB〕

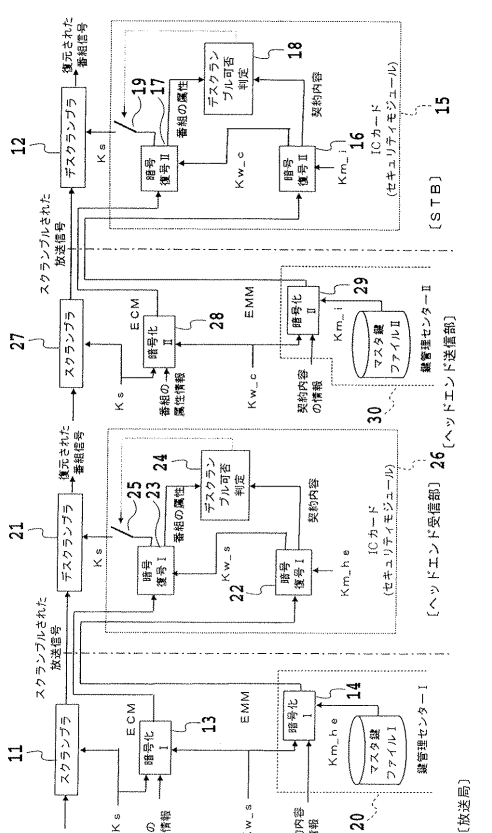
【図２】


スクランブルされた放送信号
番組信号
Ks
番組の属性情報
Kw
契約内容の情報
スクランブラ
ECM
暗号化
EMM
暗号化
Km
マスタ鍵ファイル
鍵管理センター
〔放送局〕
デスクランブラ
復元された番組信号
暗号復号
番組の属性
デスクランブル可否判定
契約内容
ICカード（セキュリティモジュール）
〔受信機〕

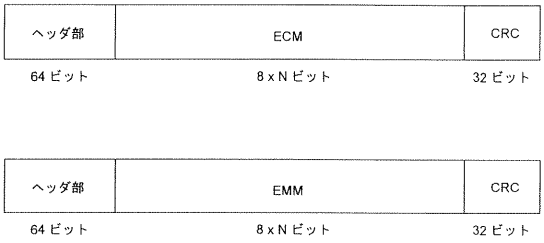
【図３】


スクランブルされた放送信号
番組信号
Ks
番組の属性情報
Kw_s
契約内容の情報
スクランブラ
ECM
暗号化Ⅰ
EMM
暗号化Ⅰ
Km_i
マスタ鍵ファイルⅠ
鍵管理センターⅠ
〔放送局〕
〔ヘッドエンド〕
デスクランブラ
復元された番組信号
暗号復号Ⅰ
Kw_s
番組の属性
デスクランブル可否判定
契約内容
ICカード（セキュリティモジュール）
〔STB〕

【図４】

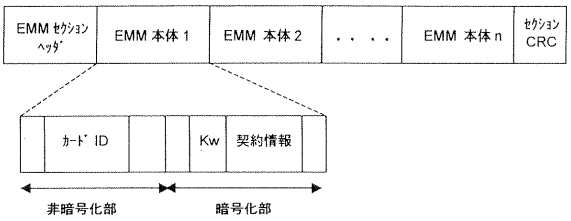

スクランブルされた放送信号
番組信号
Ks
番組の属性情報
Kw_s
契約内容の情報
スクランブラ
ECM
暗号化Ⅰ
EMM
暗号化Ⅰ
Km_he
マスタ鍵ファイルⅠ
鍵管理センターⅠ
〔放送局〕
スクランブラ
ECM
暗号化Ⅱ
EMM
暗号化Ⅱ
Km_i
マスタ鍵ファイルⅡ
鍵管理センターⅡ
〔ヘッドエンド送信部〕
〔ヘッドエンド受信部〕
デスクランブラ
復元された番組信号
暗号復号Ⅰ
暗号復号Ⅱ
Kw_c
番組の属性
デスクランブル可否判定
契約内容
ICカード（セキュリティモジュール）
〔STB〕

【図５】

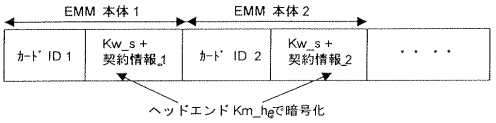


（平成 10 年郵政省告示第 260 号による）

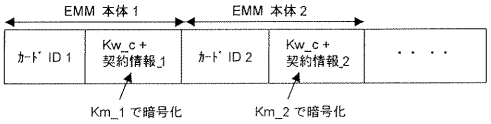
【図６】



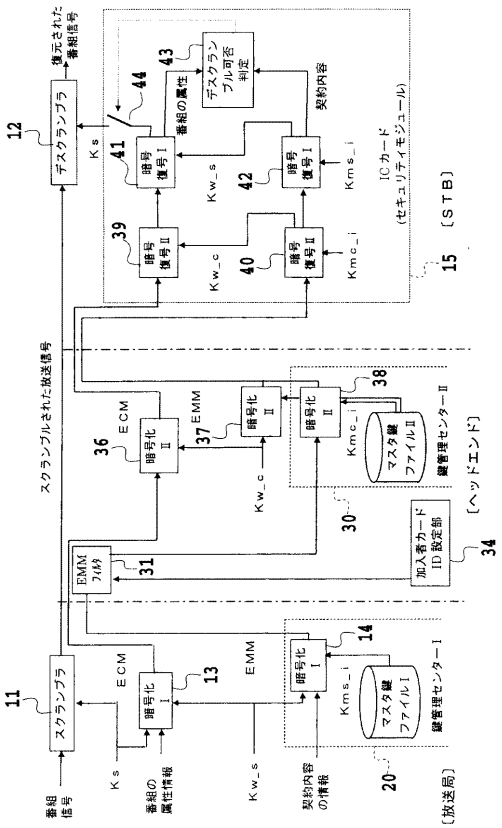
【図７】



【図８】



【図９】



フロントページの続き

(51)Int.Cl.			FI			テーマコード（参考）
H04L	***9/14***	***(2006.01)***	Ｈ０４Ｌ	9/00	６４１	
H04L	***9/18***	***(2006.01)***	Ｈ０４Ｌ	9/00	６５１	
H04N	***7/16***	***(2006.01)***	Ｈ０４Ｎ	7/16	Ｚ	