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

特許第5052616号
(P5052616)

(45)発行日　平成24年10月17日(2012.10.17)　(24)登録日　平成24年8月3日(2012.8.3)

(51)Int.Cl.			F I		
H04N	7/16	(2011.01)	H04N	7/16	Z
H04L	9/08	(2006.01)	H04L	9/00	601B
			H04L	9/00	601E

請求項の数 6　(全 19 頁)

(21)出願番号　特願2009-529877 (P2009-529877)
(86)(22)出願日　平成19年8月24日 (2007.8.24)
(86)国際出願番号　PCT/JP2007/066473
(87)国際公開番号　WO2009/028026
(87)国際公開日　平成21年3月5日 (2009.3.5)
審査請求日　平成21年12月21日 (2009.12.21)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100123434
弁理士　田澤　英昭
(74)代理人　100101133
弁理士　濱田　初音
(72)発明者　村山　修
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　虻川　雅浩
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】限定受信装置

(57)【特許請求の範囲】

【請求項１】

暗号化されているメディアデータを受信して、上記メディアデータを出力するとともに、暗号化されている鍵情報を受信し、上記鍵情報が設定済みのフィルタ条件と合致していれば、上記鍵情報を出力するフィルタリング手段と、上記フィルタリング手段に対して第１のフィルタ条件を設定する一方、上記フィルタリング手段から上記第１のフィルタ条件と合致している鍵情報が出力されると、上記鍵情報を復号する鍵情報復号手段と、上記鍵情報復号手段により復号された鍵情報を用いて、上記フィルタリング手段から出力されたメディアデータを復号するメディアデータ復号手段とを備えた限定受信装置において、他の限定受信装置から第２のフィルタ条件を受信すると、上記第２のフィルタ条件を上記フィルタリング手段に設定する一方、上記フィルタリング手段から上記第２のフィルタ条件と合致している鍵情報が出力されると、他の限定受信装置との通信が不可な状態であれば、他の限定受信装置との通信が可能な状態になるまで上記鍵情報を保持し、他の限定受信装置との通信が可能な状態になれば、上記鍵情報を他の限定受信装置に通知する鍵情報通知手段を設けたことを特徴とする限定受信装置。

【請求項２】

暗号化されているメディアデータを受信して、上記メディアデータを出力するとともに、暗号化されている鍵情報を受信し、上記鍵情報が設定済みのフィルタ条件と合致していれば、上記鍵情報を出力するフィルタリング手段と、上記フィルタリング手段に対して第１のフィルタ条件を設定する一方、上記フィルタリング手段から上記第１のフィルタ条件

と合致している鍵情報が出力されると、上記鍵情報を復号する鍵情報復号手段と、上記鍵情報復号手段により復号された鍵情報を用いて、上記フィルタリング手段から出力されたメディアデータを復号するメディアデータ復号手段とを備えた限定受信装置において、他の限定受信装置から第２のフィルタ条件を受信すると、上記第２のフィルタ条件を上記フィルタリング手段に設定する一方、上記フィルタリング手段から上記第２のフィルタ条件と合致している鍵情報が出力されると、他の限定受信装置との通信が不可な状態であれば、他の限定受信装置との通信が可能な状態になるまで上記鍵情報を保持し、他の限定受信装置との通信が可能な状態になれば、上記鍵情報を他の限定受信装置に通知する鍵情報通知手段と、上記鍵情報復号手段によって上記フィルタリング手段に設定された第１のフィルタ条件を他の限定受信装置に通知し、他の限定受信装置から上記第１のフィルタ条件と合致している鍵情報を取得する鍵情報取得手段とを設けたことを特徴とする限定受信装置。

【請求項３】

鍵情報通知手段は、他の限定受信装置から第２のフィルタ条件を受信すると、上記第２のフィルタ条件を他の限定受信装置と異なる別の限定受信装置に通知することを特徴とする請求項１または請求項２記載の限定受信装置。

【請求項４】

他の限定受信装置から受信する第２のフィルタ条件と同一のフィルタ条件を生成するフィルタ条件生成手段を設けたことを特徴とする請求項１または請求項２記載の限定受信装置。

【請求項５】

フィルタリング手段は、放送局の送信装置から第２のフィルタ条件が記述されているフィルタ条件リストを受信すると、上記フィルタ条件リストを鍵情報通知手段に出力し、

上記鍵情報通知手段は、上記フィルタリング手段から出力されたフィルタ条件リストに記述されている第２のフィルタ条件を抽出して、上記第２のフィルタ条件を上記フィルタリング手段に設定することを特徴とする請求項１または請求項２記載の限定受信装置。

【請求項６】

外部の通信機器を利用して、他の限定受信装置とフィルタ条件及び鍵情報を送受信することを特徴とする請求項１または請求項２記載の限定受信装置。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、暗号化されているメディアデータ（例えば、映像、音声、その他のデータ）と、そのメディアデータを復号する際に利用する鍵情報を受信する限定受信装置に関するものである。

【背景技術】

【０００２】

従来の限定受信装置として、例えば、デジタル放送の受信装置が挙げられる。

日本のデジタル放送における暗号化方式に関しては、ＡＲＩＢ（Ａｓｓｏｃｉａｔｉｏｎ ｏｆ Ｒａｄｉｏ Ｉｎｄｕｓｔｒｉｅｓ ａｎｄ Ｂｕｓｉｎｅｓｓｅｓ：社団法人 電波産業会）のコンテンツ保護方式に関する規格書「ＡＲＩＢ ＳＴＤ－Ｂ２５」で規定されている。

【０００３】

この規格書では、放送局から暗号化されているメディアデータと共通情報（ＥＣＭ：Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ）が受信機に送信され、また、その共通情報の暗号化を解く際に利用する個別情報（ＥＭＭ：Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅ）についても、暗号化されて放送局から受信機に送信される。

したがって、受信機が放送局から共通情報ＥＣＭと個別情報ＥＭＭを受信するまでは、メディアデータの暗号化を解くことができない。

【０００４】
図９は規格書「ＡＲＩＢ　ＳＴＤ－Ｂ２５」で規定されている放送局と受信機のやり取りを示す説明図である。
放送局から番組コンテンツ（例えば、映像や音声などのメディアデータ）が受信機に伝送される際、スクランブル鍵Ｋｓを用いて、番組コンテンツが暗号化される。
このスクランブル鍵Ｋｓは別のワーク鍵Ｋｗを用いて暗号化され、暗号化されたスクランブル鍵Ｋｓが制御データの一部である共通情報ＥＣＭとして受信機に伝送される。
また、ワーク鍵Ｋｗは別のデバイス鍵Ｋｄを用いて暗号化され、暗号化されたワーク鍵Ｋｗが制御データの一部である個別情報ＥＭＭとして受信機に伝送される。
【０００５】
上記の通り、番組コンテンツ、共通情報ＥＣＭ及び個別情報ＥＭＭについては、放送局から受信機に伝送されるが、デバイス鍵Ｋｄについては、放送局と受信機が共通に保有するようにしている。
受信機では、先ず、放送局から共通情報ＥＣＭと個別情報ＥＭＭを受信し、自身が保有するデバイス鍵Ｋｄを用いて、個別情報ＥＭＭからワーク鍵Ｋｗを獲得し、更に、ワーク鍵Ｋｗを用いて、共通情報ＥＣＭからスクランブル鍵Ｋｓを獲得することで、所望のメディアデータの暗号化を解くようにしている。
【０００６】
なお、ストリームの中から共通情報ＥＣＭを取得するためのフィルタ条件は、全ての受信機で共通であり、例えば、パケットＩＤやテーブルＩＤなどが該当する。
一方、ストリームの中から個別情報ＥＭＭを取得するためのフィルタ条件については、特定の受信機又は特定のグループの受信機毎に変えられるように、視聴設定されており、例えば、ＩＣカードのカードＩＤや、受信機の識別情報などが該当する。
したがって、放送局では、一部の受信機に視聴設定されているフィルタ条件にだけ合致するような個別情報ＥＭＭを送信すれば、一部の受信機のみが視聴可能な番組コンテンツを提供することが可能となる。
【０００７】
放送局では、個別情報ＥＭＭを周期的に受信機に送信するようにしているが、個別情報ＥＭＭの種類が増えると、一般的には、個々の個別情報ＥＭＭの再送周期が長くなる傾向がある。
受信機では、個々の個別情報ＥＭＭの再送周期が長くなると、予め設定されているフィルタ条件と合致する個別情報ＥＭＭを取得するまでに要する時間が長くなり、ワーク鍵Ｋｗを取得するまでに長時間を要することがある。
【０００８】
そのため、個別情報ＥＭＭの送出側である放送局では、時間的に十分に先行して個別情報ＥＭＭを伝送することが一般的であるが、例えば、受信機の電源が投入されていないような場合には、事前に個別情報ＥＭＭを受信して、ワーク鍵Ｋｗを取得しておくことはできない。
また、事前にワーク鍵Ｋｗを取得するために、番組コンテンツを視聴していない時間においても、受信機を常時又は定期的に起動するなどの方法も考えられるが、例えば、受信機が自動車に搭載されるような場合には、使用可能な電力に限りがあり、また、車の停車場所によっては、電波を良好に受信できないケースも考えられるため実用的ではない。
【０００９】
以下の特許文献１には、同一の個別情報ＥＭＭを必要とする家庭内の複数の限定受信装置が通信手段を有し、ある限定受信装置が個別情報ＥＭＭを受信すると、その個別情報ＥＭＭを他の限定受信装置に通知するようにして、各限定受信装置が、互いに補完しあう手法が開示されている。
ただし、この限定受信装置では、例えば、家庭内等の同一グループの限定受信装置を前提としており、同一のフィルタ条件で各限定受信装置が取得した個別情報ＥＭＭを補完しあうため、フィルタ条件が異なる限定受信装置との補完は不可能である。

また、個別情報ＥＭＭは、一般的に別の鍵で暗号化されているため、個別情報ＥＭＭ同士を共有して補完するためには、個別情報ＥＭＭの暗号化をその都度解く必要がある。

【先行技術文献】

【特許文献１】

【００１０】

特開２００１－２９８７２２号公報（段落番号［００２６］から［００２７］、図１）

【発明の概要】

【発明が解決しようとする課題】

【００１０】

従来の限定受信装置は以上のように構成されているので、設定されているフィルタ条件が他の限定受信装置に設定されているフィルタ条件と異なる場合、他の限定受信装置から事前に個別情報ＥＭＭを取得することができず、放送局から個別情報ＥＭＭが送信されるまで、ワーク鍵Ｋｗを取得することができないなどの課題があった。

【００１１】

この発明は上記のような課題を解決するためになされたもので、設定されているフィルタ条件が他の限定受信装置に設定されているフィルタ条件と異なる場合でも、事前に鍵情報を他の限定受信装置に与えることができる限定受信装置を得ることを目的とする。

また、この発明は、設定されているフィルタ条件が他の限定受信装置に設定されているフィルタ条件と異なる場合でも、他の限定受信装置から事前に鍵情報を取得することができる限定受信装置を得ることを目的とする。

【課題を解決するための手段】

【００１２】

この発明に係る限定受信装置は、鍵情報通知手段が、他の限定受信装置から第２のフィルタ条件を受信すると、第２のフィルタ条件をフィルタリング手段に設定する一方、そのフィルタリング手段から第２のフィルタ条件と合致している鍵情報が出力されると、他の限定受信装置との通信が不可な状態であれば、他の限定受信装置との通信が可能な状態になるまで上記鍵情報を保持し、他の限定受信装置との通信が可能な状態になれば、その鍵情報を他の限定受信装置に通知するようにしたものである。

また、鍵情報取得手段が、情報復号手段によってフィルタリング手段に設定された第１のフィルタ条件を他の限定受信装置に通知し、他の限定受信装置から第１のフィルタ条件と合致している鍵情報を取得するようにしたものである。

【発明の効果】

【００１３】

このことによって、設定されているフィルタ条件が他の限定受信装置に設定されているフィルタ条件と異なる場合でも、他の限定受信装置から事前に鍵情報を取得することができるなどの効果がある。

また、設定されているフィルタ条件が他の限定受信装置に設定されているフィルタ条件と異なる場合でも、事前に鍵情報を他の限定受信装置に与えることができる効果がある。

【図面の簡単な説明】

【００１４】

【図１】　この発明の実施の形態１による限定受信装置を示す構成図である。

【図２】　この発明の実施の形態１による限定受信装置Ａ，Ｂの処理内容を示すフローチャートである。

【図３】　この発明の実施の形態２による限定受信装置を示す構成図である。

【図４】　この発明の実施の形態３による限定受信装置を示す構成図である。

【図５】　この発明の実施の形態４による限定受信装置を示す構成図である。

【図６】　フィルタ条件リストの送信例を示す説明図である。

【図７】　この発明の実施の形態５による限定受信装置が利用する通信機器を示す構成図である。

【図８】　限定受信装置Ａと限定受信装置Ｂが通信機器を利用して、フィルタ条件や鍵情

報パケットを交換している様子を示す説明図である。
【図９】　規格書「ＡＲＩＢ　ＳＴＤ－Ｂ２５」で規定されている放送局と受信機のやり取りを示す説明図である。
【発明を実施するための形態】
【００１５】
以下、この発明をより詳細に説明するために、この発明を実施するための形態について、添付の図面に従って説明する。
実施の形態１.
図１はこの発明の実施の形態１による限定受信装置を示す構成図である。
この実施の形態１では、説明の便宜上、２台の限定受信装置Ａ，Ｂがフィルタ条件や鍵情報パケットを交換するものとして、図１は限定受信装置Ａの構成を表している。ただし、限定受信装置Ｂの構成は、限定受信装置Ａの構成と同じである。
【００１６】
図１において、限定受信装置Ａのフィルタ部１は例えば放送局から送信されたパケットを受信し、その受信パケットが暗号化されているメディアデータ（例えば、映像、音声、その他のデータ）を含んでいるメディアパケットであれば、そのメディアパケットをメディア復号部４に出力し、その受信パケットが鍵情報制御部３により設定されたフィルタ条件Ａ（例えば、個別情報ＥＭＭであるワーク鍵Ｋｗを取得するためのフィルタ条件Ａとしては、限定受信装置Ａに実装されているＩＣカードのカードＩＤや、限定受信装置Ａの識別情報などが該当し、共通情報ＥＣＭであるスクランブル鍵Ｋｓを取得するためのフィルタ条件Ａとしては、パケットＩＤやテーブルＩＤなどが該当する）と合致する鍵情報パケットであれば、その鍵情報パケットを鍵情報復号部２に出力する処理を実施する。なお、フィルタ部１はフィルタリング手段を構成している。
【００１７】
限定受信装置Ａの鍵情報復号部２は鍵情報制御部３に保有されている平文のデバイス鍵Ｋｄ（鍵情報用の鍵）を用いて、フィルタ部１から出力された鍵情報パケットに含まれている暗号化鍵であるワーク鍵Ｋｗを復号（暗号化の解除）するとともに、平文のワーク鍵Ｋｗを用いて、その鍵情報パケットに含まれている暗号化鍵であるスクランブル鍵Ｋｓを復号（暗号化の解除）して、平文のスクランブル鍵Ｋｓ（メディア用の鍵）を鍵情報制御部３に出力する処理を実施する。
この例では、鍵情報パケットに含まれる暗号化鍵は、情報漏洩の観点から周期的に変更されるワーク鍵Ｋｗとスクランブル鍵Ｋｓであるが、他の暗号鍵が鍵情報パケットに含まれて放送局から送信されるようにしてもよい。
【００１８】
限定受信装置Ａの鍵情報制御部３は予め平文のデバイス鍵Ｋｄとフィルタ条件Ａを保有し、そのデバイス鍵Ｋｄを鍵情報復号部２に出力するとともに、そのフィルタ条件Ａをフィルタ部１に設定する処理を実施する。また、鍵情報復号部２により復号された平文のスクランブル鍵Ｋｓをメディア復号部４に出力するとともに、そのフィルタ条件Ａを通信制御部５に出力する処理を実施する。
なお、鍵情報復号部２及び鍵情報制御部３から鍵情報復号手段が構成されている。
【００１９】
限定受信装置Ａのメディア復号部４は鍵情報制御部３から出力されたスクランブル鍵Ｋｓを用いて、フィルタ部１から出力されたメディアパケットをパケット単位に復号（暗号化の解除）し、平文のメディアパケットを出力する処理を実施する。なお、メディア復号部４はメディアデータ復号手段を構成している。
【００２０】
限定受信装置Ａの通信制御部５は限定受信装置Ｂ（他の限定受信装置）と情報交換を実施する通信機器であり、通信制御部５は限定受信装置Ｂから送信されたフィルタ条件Ｂ（例えば、個別情報ＥＭＭであるワーク鍵Ｋｗを取得するためのフィルタ条件Ｂとしては、限定受信装置Ｂに実装されているＩＣカードのカードＩＤや、限定受信装置Ｂの識別情報

などが該当し、共通情報ＥＣＭであるスクランブル鍵Ｋｓを取得するためのフィルタ条件Ｂとしては、パケットＩＤやテーブルＩＤなどが該当する）を受信すると、そのフィルタ条件Ｂを外部フィルタ制御部６に出力し、鍵情報制御部３から出力されたフィルタ条件Ａを限定受信装置Ｂに送信する処理を実施する。

また、通信制御部５はフィルタ部１からフィルタ条件Ｂと合致している鍵情報パケットＢ（例えば、ワーク鍵Ｋｗ、スクランブル鍵Ｋｓを含む）を受けると、その鍵情報パケットＢを限定受信装置Ｂに送信し、限定受信装置Ｂからフィルタ条件Ａと合致している鍵情報パケットＡ（例えば、ワーク鍵Ｋｗ、スクランブル鍵Ｋｓを含む）を受信すると、その鍵情報パケットＡを鍵情報復号部２に出力する処理を実施する。

【００２１】

限定受信装置Ａの外部フィルタ制御部６は通信制御部５から出力されたフィルタ条件Ｂをフィルタ部１に設定する処理を実施する。

なお、通信制御部５及び外部フィルタ制御部６から鍵情報通知手段が構成されている。

また、通信制御部５は鍵情報取得手段を構成している。

図２はこの発明の実施の形態１による限定受信装置Ａ，Ｂの処理内容を示すフローチャートである。

【００２２】

次に動作について説明する。

限定受信装置Ａの鍵情報制御部３は、予めデバイス鍵Ｋｄとフィルタ条件Ａを保有し、そのデバイス鍵Ｋｄを鍵情報復号部２に出力するとともに、そのフィルタ条件Ａをフィルタ部１に設定する（ステップＳＴ１）。

また、限定受信装置Ａの鍵情報制御部３は、そのフィルタ条件Ａを通信制御部５に出力する。

【００２３】

一方、限定受信装置Ｂの鍵情報制御部３は、予めデバイス鍵Ｋｄとフィルタ条件Ｂを保有し、そのデバイス鍵Ｋｄを鍵情報復号部２に出力するとともに、そのフィルタ条件Ｂをフィルタ部１に設定する（ステップＳＴ２）。

また、限定受信装置Ｂの鍵情報制御部３は、そのフィルタ条件Ｂを通信制御部５に出力する。

なお、限定受信装置Ａにおいては、フィルタ条件Ａが第１のフィルタ条件に相当し、フィルタ条件Ｂが第２のフィルタ条件に相当する。

一方、限定受信装置Ｂにおいては、フィルタ条件Ｂが第１のフィルタ条件に相当し、フィルタ条件Ａが第２のフィルタ条件に相当する。

【００２４】

限定受信装置Ａの通信制御部５は、鍵情報制御部３からフィルタ条件Ａを受けると、そのフィルタ条件Ａを限定受信装置Ｂに送信する（ステップＳＴ３）。

限定受信装置Ｂの通信制御部５は、鍵情報制御部３からフィルタ条件Ｂを受けると、そのフィルタ条件Ｂを限定受信装置Ａに送信する（ステップＳＴ４）。

【００２５】

限定受信装置Ａの通信制御部５は、限定受信装置Ｂから送信されたフィルタ条件Ｂを受信すると、そのフィルタ条件Ｂを外部フィルタ制御部６に出力する。

限定受信装置Ａの外部フィルタ制御部６は、通信制御部５からフィルタ条件Ｂを受けると、そのフィルタ条件Ｂをフィルタ部１に設定する（ステップＳＴ５）。

【００２６】

限定受信装置Ｂの通信制御部５は、限定受信装置Ａから送信されたフィルタ条件Ａを受信すると、そのフィルタ条件Ａを外部フィルタ制御部６に出力する。

限定受信装置Ｂの外部フィルタ制御部６は、通信制御部５からフィルタ条件Ａを受けると、そのフィルタ条件Ａをフィルタ部１に設定する（ステップＳＴ６）。

【００２７】

これにより、限定受信装置Ａは、自己宛のメディアパケットの暗号化を解く際に必要な

暗号鍵（フィルタ条件Ａと合致している暗号鍵（ワーク鍵Ｋｗ、スクランブル鍵Ｋｓ））と、限定受信装置Ｂがメディアパケットの暗号化を解く際に必要な暗号鍵（フィルタ条件Ｂと合致している鍵情報パケット（ワーク鍵Ｋｗ、スクランブル鍵Ｋｓを含む））の取得が可能になる。

また、限定受信装置Ｂは、自己宛のメディアパケットの暗号化を解く際に必要な暗号鍵（フィルタ条件Ｂと合致している暗号鍵（ワーク鍵Ｋｗ、スクランブル鍵Ｋｓ））と、限定受信装置Ａがメディアパケットの暗号化を解く際に必要な暗号鍵（フィルタ条件Ａと合致している鍵情報パケット（ワーク鍵Ｋｗ、スクランブル鍵Ｋｓを含む））の取得が可能になる。

以下、説明の便宜上、限定受信装置Ａの電源が落とされて、限定受信装置Ａが一時的にパケットを受信することができないものとする。

【００２８】

限定受信装置Ｂのフィルタ部１は、例えば、放送局から送信されたパケットを受信すると、その受信パケットが暗号化されているメディアデータを含んでいるメディアパケットであれば、そのメディアパケットをメディア復号部４に出力する。

また、限定受信装置Ｂのフィルタ部１は、その受信パケットが鍵情報制御部３により設定されたフィルタ条件Ｂと合致する鍵情報パケットＢであれば、その鍵情報パケットＢを鍵情報復号部２に出力する。

また、その受信パケットが外部ファイル制御部６により設定されたフィルタ条件Ａ（限定受信装置Ａから送信されたフィルタ条件Ａ）と合致する鍵情報パケットＡであれば、その鍵情報パケットＡを通信制御部５に出力する。

限定受信装置Ｂの通信制御部５は、フィルタ部１から鍵情報パケットＡを受けると、限定受信装置Ａの電源が投入されて、限定受信装置Ａとの通信が可能になるまで、その鍵情報パケットＡを保存する（ステップＳＴ７）。

【００２９】

限定受信装置Ｂの鍵情報復号部２は、フィルタ部１から鍵情報パケットＢを受けると、鍵情報制御部３に保有されている平文のデバイス鍵Ｋｄ（鍵情報用の鍵）を用いて、その鍵情報パケットＢに含まれている暗号化鍵であるワーク鍵Ｋｗの暗号化を解除する。

また、鍵情報復号部２は、平文のワーク鍵Ｋｗを用いて、その鍵情報パケットＢに含まれている暗号化鍵であるスクランブル鍵Ｋｓの暗号化を解除して、平文のスクランブル鍵Ｋｓ（メディア用の鍵）を鍵情報制御部３に出力する（ステップＳＴ８）。

限定受信装置Ｂの鍵情報制御部３は、鍵情報復号部２から平文のスクランブル鍵Ｋｓを受けると、そのスクランブル鍵Ｋｓをメディア復号部４に出力する。

【００３０】

限定受信装置Ｂのメディア復号部４は、鍵情報制御部３からスクランブル鍵Ｋｓを受けると、そのスクランブル鍵Ｋｓを用いて、フィルタ部１から出力されるメディアパケットをパケット単位に暗号復号（ｄｅｃｒｙｐｔ）し、復号済みの平文のメディアパケットを後段のメディア復号部（図示せず）等に出力する（ステップＳＴ９）。

なお、メディアパケットに含まれているメディアデータが符号化されている場合には、そのメディアデータのメディア復号（ｄｅｃｏｄｅ）等が行われる。

【００３１】

限定受信装置Ｂの通信制御部５は、限定受信装置Ａの電源が投入されて、限定受信装置Ａとの通信が可能になると、先に保存している鍵情報パケットＡを限定受信装置Ａに送信する（ステップＳＴ１０）。

限定受信装置Ａの通信制御部５は、限定受信装置Ｂから送信された鍵情報パケットＡを受信すると、その鍵情報パケットＡを鍵情報復号部２に出力する。

なお、限定受信装置Ｂの通信制御部５が鍵情報パケットＡを限定受信装置Ａに送信する際、その鍵情報パケットＡに含まれている暗号鍵を復号することなく、暗号化されている状態で送信するようにしているので、鍵情報の秘匿性を保つことができ、鍵情報の漏洩を防止することができる。

また、鍵情報の暗号復号に必要な計算量を抑制することができるため、実装に必要なハードウェアやソフトウェアのコスト及び動作中の消費電力を抑制することができる。

【００３２】

限定受信装置Ａの鍵情報復号部２は、通信制御部５から鍵情報パケットＡを受けると、鍵情報制御部３に保有されている平文のデバイス鍵Ｋｄ（鍵情報用の鍵）を用いて、その鍵情報パケットＡに含まれている暗号化鍵であるワーク鍵Ｋｗの暗号化を解除する。

また、鍵情報復号部２は、平文のワーク鍵Ｋｗを用いて、その鍵情報パケットＡに含まれている暗号化鍵であるスクランブル鍵Ｋｓの暗号化を解除して、平文のスクランブル鍵Ｋｓ（メディア用の鍵）を鍵情報制御部３に出力する（ステップＳＴ１１）。

限定受信装置Ａの鍵情報制御部３は、鍵情報復号部２から平文のスクランブル鍵Ｋｓを受けると、そのスクランブル鍵Ｋｓをメディア復号部４に出力する。

【００３３】

限定受信装置Ａのメディア復号部４は、鍵情報制御部３からスクランブル鍵Ｋｓを受けると、そのスクランブル鍵Ｋｓを用いて、フィルタ部１から出力されるメディアパケットをパケット単位に暗号復号（ｄｅｃｒｙｐｔ）し、復号済みの平文のメディアパケットを後段のメディア復号部（図示せず）等に出力する（ステップＳＴ１２）。

なお、メディアパケットに含まれているメディアデータが符号化されている場合には、そのメディアデータのメディア復号（ｄｅｃｏｄｅ）等が行われる。

【００３４】

図２の例では、限定受信装置Ａの電源が落とされている間、限定受信装置Ｂが鍵情報パケットＡを取得し、限定受信装置Ａの電源が投入されて、限定受信装置Ａとの通信が可能になると、直ちに、その鍵情報パケットＡを限定受信装置Ａに送信することにより、放送局から鍵情報パケットＡが送信される前の段階でも、限定受信装置Ａがメディアパケットの復号を開始することができるものについて示したが、逆に、限定受信装置Ｂの電源が落とされる場合には、限定受信装置Ｂの電源が落とされている間、限定受信装置Ａが鍵情報パケットＢを取得し、限定受信装置Ｂの電源が投入されて、限定受信装置Ｂとの通信が可能になると、直ちに、その鍵情報パケットＢを限定受信装置Ｂに送信するようにしてもよい。

【００３５】

また、図２の例では、限定受信装置Ａの電源が落とされている間、限定受信装置Ｂが鍵情報パケットＡを取得するものについて示したが、例えば、限定受信装置Ａの電源が投入されている状態でも、受信状態の悪化等が原因で、限定受信装置Ａが鍵情報パケットＡの取得に失敗する場合がある。

このような場合に備えて、限定受信装置Ｂが定常的に鍵情報パケットＡを取得して、その鍵情報パケットＡを限定受信装置Ａに送信するようにしてもよい。

【００３６】

また、図２の例では、２台の限定受信装置Ａ，Ｂがフィルタ条件や鍵情報パケットを交換するものについて示したが、３台以上の限定受信装置がフィルタ条件や鍵情報パケットを交換するようにしてもよい。

この場合、各限定受信装置は、自分宛のフィルタ条件と鍵情報パケットに加え、他の限定受信装置に設定されているフィルタ条件と鍵情報パケットを管理する必要がある。

【００３７】

以上で明らかなように、この実施の形態１によれば、他の限定受信装置からフィルタ条件を受信して、そのフィルタ条件をフィルタ部１に設定し、そのフィルタ部１から上記フィルタ条件と合致している鍵情報が出力されると、その鍵情報を他の限定受信装置に通知する一方、鍵情報制御部３によってフィルタ部１に設定されたフィルタ条件を他の限定受信装置に通知し、他の限定受信装置から上記フィルタ条件と合致している鍵情報を取得するように構成したので、フィルタ部１に設定されているフィルタ条件が他の限定受信装置に設定されているフィルタ条件と異なる場合でも、他の限定受信装置から事前に鍵情報を取得することができるなどの効果を奏する。

また、設定されているフィルタ条件が他の限定受信装置に設定されているフィルタ条件と異なる場合でも、事前に鍵情報を他の限定受信装置に与えることができる効果を奏する。

これにより、放送局から鍵情報の送信周期が長く、速やかに放送局から鍵情報を取得することができない場合でも、速やかにメディアパケットの復号を開始することができるため、動作開始後におけるメディアデータの復号や再生等の待ち時間を短縮することができる効果を奏する。

【００３８】

なお、この実施の形態１では、限定受信装置Ａ，Ｂの双方が、自己のフィルタ条件を他の限定受信装置に通知して、他の限定受信装置から上記フィルタ条件に合致する鍵情報パケットを受信する機能（以下、「鍵情報パケット取得機能」と称する）と、他の限定受信装置からフィルタ条件を受信し、そのフィルタ条件に合致する鍵情報パケットを他の限定受信装置に通知する機能（以下、「鍵情報パケット通知機能」と称する）とを備えているものについて示したが、例えば、限定受信装置Ａが鍵情報パケット取得機能のみを備え、限定受信装置Ｂが鍵情報パケット通知機能のみを備えるようにしてもよい。

【００３９】

この場合、限定受信装置Ａでは、外部フィルタ制御部６が不要になり、フィルタ部１が鍵情報パケットＢを通信制御部５に出力する機能が不要になる。

また、限定受信装置Ｂでは、鍵情報制御部３がフィルタ条件Ａを通信制御部５に出力する機能と、通信制御部５が鍵情報パケットＡを鍵情報復号部２に出力する機能とが不要になる。

ただし、この場合、限定受信装置Ａでは、電源が投入されると、直ちに限定受信装置Ｂから鍵情報パケットＡを取得して、メディアパケットの復号を開始することができるが、限定受信装置Ｂは、電源の投入時に限定受信装置Ａから鍵情報パケットＢを取得することができない。

【００４０】

また、この実施の形態１では、デジタル放送を例にして説明したが、衛星通信や、その他の暗号化データ通信に活用してもよい。

また、当該限定受信装置が唯一でないことが既知である場合、当該限定受信装置用の鍵情報は、外部の限定受信装置用の鍵情報にもなり得るため、それを外部に出力してもよい。

【００４１】

実施の形態２．

図３はこの発明の実施の形態２による限定受信装置を示す構成図であり、図において、図１と同一符号は同一または相当部分を示すので説明を省略する。

上記実施の形態１では、２台の限定受信装置Ａ，Ｂがフィルタ条件や鍵情報パケットを交換するものについて示したが、この実施の形態２では、３台の限定受信装置Ａ，Ｂ，Ｃがフィルタ条件や鍵情報パケットを交換するものについて説明する。

ここでは、３台の限定受信装置Ａ，Ｂ，Ｃがフィルタ条件や鍵情報パケットを交換するものについて説明するが、３台以上の限定受信装置がフィルタ条件や鍵情報パケットを交換するようにしてもよい。

【００４２】

限定受信装置Ａの通信制御部１１は図１の通信制御部５と同様の機能を有するほか、限定受信装置Ｃから送信されたフィルタ条件Ｃを受信すると、そのフィルタ条件Ｃを外部フィルタ制御部１２に出力し、鍵情報制御部３から出力されたフィルタ条件Ａを限定受信装置Ｃに送信する処理を実施する。

また、通信制御部１１は限定受信装置Ｂから送信されたフィルタ条件Ｂを限定受信装置Ｃに送信するとともに、限定受信装置Ｃから送信されたフィルタ条件Ｃを限定受信装置Ｂに送信する処理を実施する。

また、通信制御部１１はフィルタ部１からフィルタ条件Ｂと合致している鍵情報パケッ

トＢを受けると、その鍵情報パケットＢを限定受信装置Ｂに送信し、フィルタ部１からフィルタ条件Ｃと合致している鍵情報パケットＣを受けると、その鍵情報パケットＣを限定受信装置Ｃに送信する処理を実施する。

【００４３】

限定受信装置Ａの外部フィルタ制御部１２は通信制御部１１から出力されたフィルタ条件Ｂ，Ｃをフィルタ部１に設定するとともに、そのフィルタ条件Ｂ，Ｃを通信制御部１１に出力する処理を実施する。

なお、通信制御部１１及び外部フィルタ制御部１２から鍵情報通知手段が構成されている。

また、通信制御部１１は鍵情報取得手段を構成している。

【００４４】

次に動作について説明する。

この実施の形態２では、説明の便宜上、上記実施の形態１と同様に、限定受信装置Ａと限定受信装置Ｂがフィルタ条件や鍵情報パケットを交換して、メディアパケットの復号を開始したのち、停止中であった限定受信装置Ｃが限定受信装置Ａとの通信のみが可能な状態になったものとして説明する。

【００４５】

限定受信装置Ｃの通信制御部１１は、限定受信装置Ａとの通信が可能になると、フィルタ条件Ｃを限定受信装置Ａに送信する。

限定受信装置Ａの通信制御部１１は、限定受信装置Ｃから送信されたフィルタ条件Ｃを受信すると、そのフィルタ条件Ｃを外部フィルタ制御部１２に出力する。

【００４６】

限定受信装置Ａの外部フィルタ制御部１２は、通信制御部１１からフィルタ条件Ｃを受けると、そのフィルタ条件Ｃをフィルタ部１に設定する。

なお、フィルタ部１には、先にフィルタ条件Ａ，Ｂが設定されているので、全部でフィルタ条件Ａ，Ｂ，Ｃの設定がなされたことになる。

限定受信装置Ａの外部フィルタ制御部１２は、フィルタ条件Ｃをフィルタ部１に設定すると、先にフィルタ部１に設定しているフィルタ条件Ｂを通信制御部１１に出力する。

【００４７】

限定受信装置Ａの通信制御部１１は、外部フィルタ制御部１２から出力されたフィルタ条件Ｂと、鍵情報制御部３から出力されたフィルタ条件Ａとを限定受信装置Ｃに送信する。

限定受信装置Ｃの通信制御部１１は、限定受信装置Ａから送信されたフィルタ条件Ａ，Ｂを受信すると、そのフィルタ条件Ａ，Ｂを外部フィルタ制御部１２に出力する。

限定受信装置Ｃの外部フィルタ制御部１２は、通信制御部１１からフィルタ条件Ａ，Ｂを受けると、そのフィルタ条件Ａ，Ｂをフィルタ部１に設定する。

なお、限定受信装置Ｃのフィルタ部１には、鍵情報制御部３によってフィルタ条件Ｃも設定されるので、全部でフィルタ条件Ａ，Ｂ，Ｃの設定がなされることになる。

【００４８】

また、限定受信装置Ａの外部フィルタ制御部１２は、フィルタ条件Ｃをフィルタ部１に設定すると、そのフィルタ条件Ｃを通信制御部１１に出力する。

限定受信装置Ａの通信制御部１１は、外部フィルタ制御部１２からフィルタ条件Ｃを受けると、そのフィルタ条件Ｃを限定受信装置Ｂに送信する。

限定受信装置Ｂの通信制御部１１は、限定受信装置Ａから送信されたフィルタ条件Ｃを受信すると、そのフィルタ条件Ｃを外部フィルタ制御部１２に出力する。

限定受信装置Ｂの外部フィルタ制御部１２は、通信制御部１１からフィルタ条件Ｃを受けると、そのフィルタ条件Ｃをフィルタ部１に設定する。

なお、限定受信装置Ｂのフィルタ部１には、先にフィルタ条件Ａ，Ｂが設定されているので、全部でフィルタ条件Ａ，Ｂ，Ｃの設定がなされることになる。

【００４９】

これにより、限定受信装置Ａ，Ｂ，Ｃは、フィルタ条件Ａ，Ｂ，Ｃに対応する鍵情報パケットＡ，Ｂ，Ｃの取得が可能になる。

その後、例えば、限定受信装置Ａの電源が落とされて、限定受信装置Ａが一時的にパケットを受信することができなくなると、限定受信装置Ａの電源が落とされている間、限定受信装置Ｂ，Ｃが鍵情報パケットＡを取得することになる。

限定受信装置Ｂ，Ｃにおける鍵情報パケットＡの取得処理は、上記実施の形態１と同様であるため説明を省略する。

【００５０】

限定受信装置Ｂ，Ｃは、鍵情報パケットＡを取得したのち、限定受信装置Ａの電源が投入されて、限定受信装置Ａとの通信が可能になると、直ちに、その鍵情報パケットＡを限定受信装置Ａに送信する。

これにより、限定受信装置Ａが電源投入後に、放送局から周期的に伝送される鍵情報パケットＡを受信する前の段階でも、限定受信装置Ａがメディアパケットの復号を開始することができるようになる。

【００５１】

以上で明らかなように、この実施の形態２によれば、限定受信装置Ａが限定受信装置Ｂからフィルタ条件Ｂを受信すると、そのフィルタ条件Ｂを限定受信装置Ｃに通知し、限定受信装置Ｃからフィルタ条件Ｃを受信すると、そのフィルタ条件Ｃを限定受信装置Ｂに通知するように構成したので、上記実施の形態１よりも、各限定受信装置が他の限定受信装置の鍵情報パケットを代わりに取得できる確率を高めることができる効果を奏する。

【００５２】

なお、この実施の形態２では、外部フィルタ制御部１２が他の限定受信装置から送信されたフィルタ条件を保持し、通信制御部１１が外部フィルタ制御部１２から出力されたフィルタ条件を他の限定受信装置と異なる別の他の限定受信装置に送信するものについて示したが、フィルタ部１が他の限定受信装置から送信されたフィルタ条件を保持し、通信制御部１１がフィルタ部１から出力されたフィルタ条件を他の限定受信装置と異なる別の他の限定受信装置に送信するようにしてもよい。

【００５３】

実施の形態３．

図４はこの発明の実施の形態３による限定受信装置を示す構成図であり、図において、図１と同一符号は同一または相当部分を示すので説明を省略する。

限定受信装置Ａのフィルタ条件生成部２１は限定受信装置Ｂ（他の限定受信装置）から受信するフィルタ条件Ｂと同一のフィルタ条件Ｂを生成する処理を実施する。なお、フィルタ条件生成部２１はフィルタ条件生成手段を構成している。

図４は図１の限定受信装置にフィルタ条件生成部２１が追加されているものを示しているが、図３の限定受信装置にフィルタ条件生成部２１が追加されていてもよい。

【００５４】

次に動作について説明する。

上記実施の形態１，２では、例えば、限定受信装置Ａが限定受信装置Ｂからフィルタ条件Ｂを受信するものについて示したが、そのフィルタ条件Ｂと同一のフィルタ条件Ｂを生成するフィルタ条件生成部２１を設け、フィルタ条件生成部２１がフィルタ条件Ｂをフィルタ部１に設定するようにしてもよい。

【００５５】

例えば、フィルタ条件が所定の長さのバイト列であって、一定のルールにより生成されている場合、そのルールに当てはめる情報が取得可能であれば、限定受信装置Ａにおいて、他の限定受信装置Ｂと通信することなく、フィルタ条件Ｂを生成することができる。

以下、フィルタ条件生成部２１におけるフィルタ条件Ｂの生成例を説明する。

【００５６】

例えば、フィルタ条件の一部に、所有者固有のＩＤ等が割り振られている場合、残りのフィールドをワイルドカードとすることで、同一の所有者のフィルタ条件を網羅すること

ができる。
そこで、フィルタ条件生成部２１は、限定受信装置Ａに登録された所有者固有のＩＤを一部に含むフィルタ条件Ｂを生成し、そのフィルタ条件Ｂをフィルタ部１に設定する。これにより、同一所有者の鍵情報を取得することが可能となる。
【００５７】
また、メーカーや各メーカーの機種毎の固有番号が割り振られている場合も同様に、同一メーカーや、同一機種のフィルタ条件を生成することができ、同一メーカーや、同一機種の鍵情報を取得することが可能となる。
他にも、物理的な位置情報や、ＭＡＣアドレス等を利用して、フィルタ条件を生成することで、鍵情報を取得することが可能となる。
【００５８】
以上で明らかなように、この実施の形態３によれば、フィルタ条件生成部２１が限定受信装置Ｂから受信するフィルタ条件Ｂと同一のフィルタ条件Ｂを生成するように構成したので、限定受信装置Ｂからフィルタ条件Ｂを受信する通信処理を省略することができる効果を奏する。
【００５９】
なお、この実施の形態３では、通信制御部５が限定受信装置Ｂからフィルタ条件Ｂを受信する機能を残しているが、この機能を削除するようにしてもよい。
また、この実施の形態３では、フィルタ条件生成部２１が各種ＩＤを一部に含むフィルタ条件Ｂを生成するものについて示したが、各種ＩＤに基づいて何らかの計算を実施し、その計算結果を一部に含むフィルタ条件Ｂを生成するようにしてもよい。
【００６０】
実施の形態４．
図５はこの発明の実施の形態４による限定受信装置を示す構成図であり、図において、図１と同一符号は同一または相当部分を示すので説明を省略する。
限定受信装置Ａの外部フィルタ制御部３１はフィルタ部１により限定受信装置Ｂ，Ｃから受信するフィルタ条件Ｂ，Ｃと同一のフィルタ条件Ｂ，Ｃが記述されているフィルタ条件リストが受信された場合、そのフィルタ条件リストからフィルタ条件Ｂ，Ｃを抽出して、そのフィルタ条件Ｂ，Ｃをフィルタ部１に設定する処理を実施する。なお、外部フィルタ制御部３１は鍵情報通知手段を構成している。
図５は図１の限定受信装置に外部フィルタ制御部３１が適用されているものを示しているが、図３の限定受信装置に外部フィルタ制御部３１が適用されていてもよい。
図６はフィルタ条件リストの送信例を示す説明図である。
【００６１】
次に動作について説明する。
例えば、限定受信装置Ａ，Ｂ，Ｃのフィルタ条件を把握しているシステム管理者やメーカー等が、限定受信装置Ａ，Ｂ，Ｃのフィルタ条件Ａ，Ｂ，Ｃとして、“ＸＸＸ”、“ＹＹＹ”、“ＺＺＺ”が記述されているフィルタ条件リストを放送局の送信装置に通知する。
放送局の送信装置は、フィルタ条件リストの通知を受けると、図６に示すように、そのフィルタ条件リストをメディアパケットや鍵情報パケットと多重して限定受信装置Ａ，Ｂ，Ｃに送信する。
【００６２】
ここでは、放送局の送信装置がシステム管理者やメーカー等からフィルタ条件リストの通知を受けるものについて示したが、放送局の送信装置がフィルタ条件リストを生成するようにしてもよい。
なお、限定受信装置Ａ，Ｂ，Ｃのフィルタ部１には、予め、フィルタ条件リストを共通的に取得するためのフィルタ条件が設定されているものとする。
【００６３】
限定受信装置Ａ，Ｂ，Ｃのフィルタ部１は、放送局の送信装置から送信されたパケット

を受信すると、そのパケットの中からフィルタ条件リストを取得し、そのフィルタ条件リストを外部フィルタ制御部３１に出力する。
ただし、図６の例では、限定受信装置Ａについては、電源が入っておらず、フィルタ条件リストを取得することができない。
【００６４】
限定受信装置Ｂの外部フィルタ制御部３１は、フィルタ部１からフィルタ条件リストを受けると、そのフィルタ条件リストから他の限定受信装置Ａ，Ｃのフィルタ条件Ａ，Ｃを抽出して、そのフィルタ条件Ａ，Ｃをフィルタ部１に設定する。
限定受信装置Ｂの鍵情報制御部３は、上記実施の形態１と同様に、自装置用のフィルタ条件Ｂをフィルタ部１に設定する。
これにより、限定受信装置Ｂのフィルタ部１には、フィルタ条件Ａ，Ｂ，Ｃが設定され、フィルタ条件Ａ，Ｂ，Ｃに対応する鍵情報パケットＡ，Ｂ，Ｃの取得が可能になる。
【００６５】
また、限定受信装置Ｃの外部フィルタ制御部３１は、フィルタ部１からフィルタ条件リストを受けると、そのフィルタ条件リストから他の限定受信装置Ａ，Ｂのフィルタ条件Ａ，Ｂを抽出して、そのフィルタ条件Ａ，Ｂをフィルタ部１に設定する。
限定受信装置Ｃの鍵情報制御部３は、自装置用のフィルタ条件Ｃをフィルタ部１に設定する。
これにより、限定受信装置Ｃのフィルタ部１には、フィルタ条件Ａ，Ｂ，Ｃが設定され、フィルタ条件Ａ，Ｂ，Ｃに対応する鍵情報パケットＡ，Ｂ，Ｃの取得が可能になる。
【００６６】
限定受信装置Ｂ，Ｃにおける鍵情報パケットＡの取得処理は、上記実施の形態１と同様であるため説明を省略するが、限定受信装置Ｂ，Ｃは、鍵情報パケットＡを取得したのち、限定受信装置Ａの電源が投入されて、限定受信装置Ａとの通信が可能になると、直ちに、その鍵情報パケットＡを限定受信装置Ａに送信する。
これにより、放送局から鍵情報パケットＡが送信される前の段階でも、限定受信装置Ａがメディアパケットの復号を開始することができるようになる。
【００６７】
以上で明らかなように、この実施の形態４によれば、フィルタ部１によりフィルタ条件リストが受信された場合、そのフィルタ条件リストから他の限定受信装置のフィルタ条件を抽出して、そのフィルタ条件をフィルタ部１に設定するように構成したので、他の限定受信装置からフィルタ条件を受信する通信処理を省略することができる効果を奏する。
【００６８】
なお、この実施の形態４では、通信制御部５が他の限定受信装置からフィルタ条件を受信する機能を残しているが、この機能を削除するようにしてもよい。
【００６９】
また、この実施の形態４では、フィルタ部１がフィルタ条件リストを受信すると、外部フィルタ制御部３１がフィルタ条件リストから他の限定受信装置のフィルタ条件を抽出して、そのフィルタ条件をフィルタ部１に設定するものについて示したが、これに限るものではなく、次のようにしてもよい。
例えば、フィルタ部１により受信されたフィルタ条件リストが鍵情報パケットと一緒に暗号化されている場合には、鍵情報復号部２がフィルタ条件リストの暗号化を解除してから、鍵情報制御部３が平文のフィルタ条件リストに含まれている他の限定受信装置のフィルタ条件をフィルタ部１に設定するようにしてもよい。
【００７０】
実施の形態５．
上記実施の形態１では、限定受信装置Ａと限定受信装置Ｂがフィルタ条件や鍵情報パケットを交換するものについて示したが、限定受信装置Ａと限定受信装置Ｂが外部の通信機器を利用して、フィルタ条件や鍵情報パケットを交換するようにしてもよい。
図７はこの発明の実施の形態５による限定受信装置が利用する通信機器を示す構成図で

あり、図において、蓄積部４１は通信部４３により受信されたフィルタ条件や鍵情報パケットを一時的に蓄積するメモリである。

判定部４２はフィルタ条件や鍵情報パケットの蓄積や通信を判別する処理を実施する。

通信部４３は限定受信装置とフィルタ条件や鍵情報パケットを送受信する。

【００７１】

なお、通信機器は、専用の機器である必要はなく、例えば、携帯電話等に、当該通信機器の機能を追加するようにしてもよい。また、自動車の内部に限定受信装置が設置されている場合には、キーレスエントリー機能や、予め通信機能を持つリモコンなどに、当該通信機器の機能を追加するようにしてもよい。

【００７２】

図８は限定受信装置Ａと限定受信装置Ｂが通信機器を利用して、フィルタ条件や鍵情報パケットを交換している様子を示す説明図である。

なお、図８では、（ａ）（ｂ）（ｃ）が時系列順に並んでおり、通信機器を手にしているユーザが、２つの限定受信装置Ａ，Ｂ間を行き来する様子を示している。

図８中の噴出しは、限定受信装置又は通信機器の内部に保持されている情報を示している。

また、鍵情報Ａ１，鍵情報Ａ２は限定受信装置Ａ用の鍵情報が時系列的に変化している様子を示し、常に最新（添え字の値が大きい）の鍵情報を取得する必要がある。

【００７３】

次に動作について説明する。

まず、ユーザは、図８（ａ）において、通信機器を手にして、限定受信装置Ａの前に居る。

このとき、限定受信装置Ａは動作しており、通信制御部５が内部のフィルタ条件Ａを通信機器に通知する。

通信機器の判定部４２は、通信部４３が限定受信装置Ａから送信されたフィルタ条件Ａを受信すると、そのフィルタ条件Ａと同一のフィルタ条件が蓄積部４１に蓄積されていないことを確認し、同一のフィルタ条件が蓄積されていなければ、そのフィルタ条件Ａを蓄積部４１に蓄積する。

限定受信装置Ａは、図８（ａ）において、フィルタ条件Ａと合致している鍵情報パケットＡ１を取得するが、遠隔地にある限定受信装置Ｂは停止しており、鍵情報パケットＢ１を取得しない。

【００７４】

次に、ユーザは、図８（ｂ）において、限定受信装置Ａを停止させてから、通信機器を手にして限定受信装置Ｂの前に移動し、限定受信装置Ｂの使用を開始する。

このとき、限定受信装置Ｂの通信制御部５が内部のフィルタ条件Ｂを通信機器に通知する。

通信機器の判定部４２は、通信部４３が限定受信装置Ｂから送信されたフィルタ条件Ｂを受信すると、そのフィルタ条件Ｂと同一のフィルタ条件が蓄積部４１に蓄積されていないことを確認し、同一のフィルタ条件が蓄積されていなければ、そのフィルタ条件Ｂを蓄積部４１に蓄積する。

【００７５】

また、通信機器の判定部４２は、蓄積部４１にフィルタ条件Ａが蓄積されているので、通信部４３を介して、そのフィルタ条件Ａを限定受信装置Ｂに送信する。

これにより、限定受信装置Ｂの通信制御部５がフィルタ条件Ａを受信すると、上記実施の形態１と同様に、そのフィルタ条件Ａがフィルタ部１に設定される。

限定受信装置Ｂは、図８（ｂ）において、フィルタ条件Ａと合致している鍵情報パケットＡ２と、フィルタ条件Ｂと合致している鍵情報パケットＢ１とを取得する。

このとき、停止中である限定受信装置Ａは、鍵情報パケットＡ２を取得することができない。

また、通信機器は、フィルタ条件Ａが蓄積部４１に蓄積されているので、判定部４２が

通信部４３を介して、フィルタ条件Ａと合致している鍵情報パケットＡ２を取得し、その鍵情報パケットＡ２を蓄積部４１に蓄積する。

【００７６】

次に、ユーザは、図８（ｃ）において、限定受信装置Ｂを停止させてから、通信機器を手にして、再度、限定受信装置Ａの前に移動し、限定受信装置Ａの使用を開始する。

通信機器の判定部４２は、蓄積部４１に蓄積されている鍵情報パケットＡ２が、図８（ａ）において、限定受信装置Ａにより取得された鍵情報パケットＡ１より新しいことを確認すると、通信部４３を介して、その鍵情報パケットＡ２を直ちに限定受信装置Ａに送信する。

これにより、鍵情報パケットＡ２の伝送周期に関わらず、即座に、限定受信装置Ａの通信制御部５が最新の鍵情報パケットＡ２を取得する。

【００７７】

また、通信機器は、フィルタ条件Ｂが蓄積部４１に蓄積されているので、判定部４２が通信部４３を介して、フィルタ条件Ｂと合致している鍵情報パケットＢ２を取得し、その鍵情報パケットＢ２を蓄積部４１に蓄積する。

図８（ｃ）では、限定受信装置Ｂが停止中であるため、限定受信装置Ｂの使用が開始されたとき、通信機器が最新の鍵情報パケットＢ２を限定受信装置Ｂに送信する。

【００７８】

以上で明らかなように、この実施の形態５によれば、限定受信装置Ａと限定受信装置Ｂが外部の通信機器を利用して、フィルタ条件や鍵情報パケットを交換するように構成したので、限定受信装置Ａと限定受信装置Ｂが物理的に離れている位置に存在していても、間接的にフィルタ条件や鍵情報パケットを送受信することができる効果を奏する。

【００７９】

なお、この実施の形態５では、図８（ａ）において、限定受信装置Ａは自身が保有するフィルタ条件Ａを固有のものとして、鍵情報パケットＡ１を通信機器に通知していないが、同様の限定受信装置Ａが多数存在する場合には、通知を行うようにしてもよい。

これは図８（ｂ）において、限定受信装置Ｂが鍵情報パケットＢ２を通知するかどうかに関しても同様である。

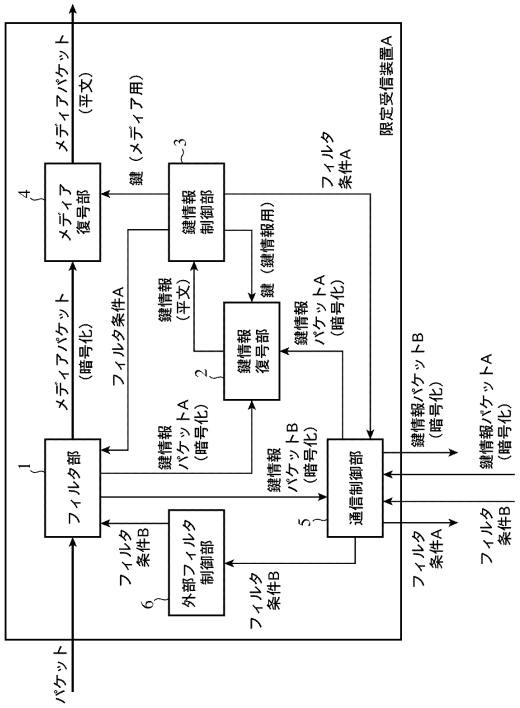
また、通信機器が限定受信装置と同様に、メディアパケットや鍵情報パケットのフィルタ機能を有していてもよい。

また、図８の例では、鍵情報パケットを受信できない状態として、電源が落とされている場合を示しているが、例えば、電源が投入されている状態でも、受信状態の悪化等が原因で鍵情報パケットを受信できない場合もある。

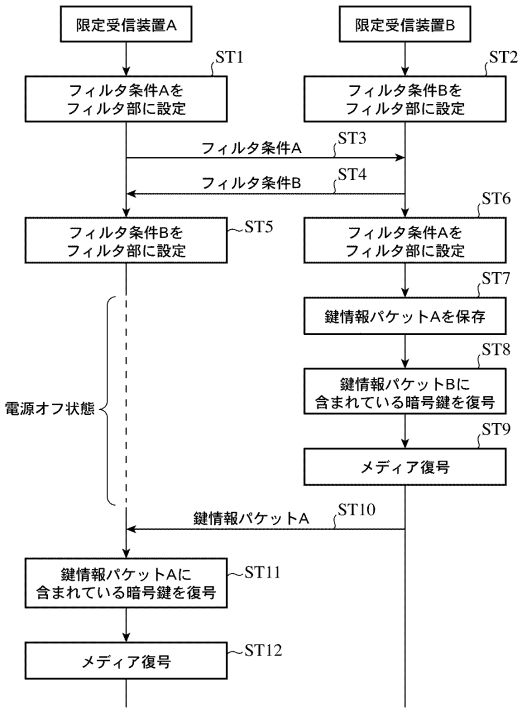
【００８０】

以上のように、この発明に係る限定受信装置は、暗号化されているメディアデータを受信すると、そのメディアデータの暗号化をリアルタイムに解く必要があるものなどに適している。

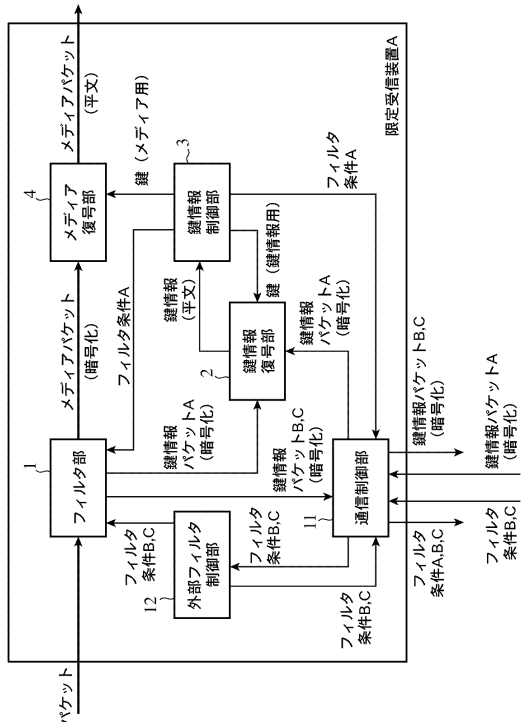
【図１】


限定受信装置A
パケット
メディアパケット（暗号化）
メディアパケット（平文）
フィルタ部
メディア復号部
鍵情報制御部
鍵情報復号部
通信制御部
外部フィルタ制御部
フィルタ条件A
フィルタ条件B
鍵情報パケットA（暗号化）
鍵情報パケットB（暗号化）
鍵（メディア用）
鍵（鍵情報用）
鍵情報（平文）
鍵情報パケットB（暗号化）
鍵情報パケットA（暗号化）

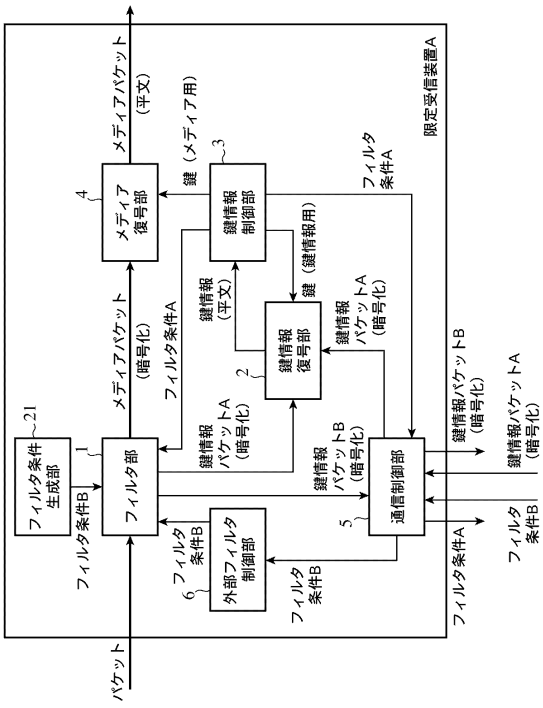
【図２】


限定受信装置A
限定受信装置B
フィルタ条件Aをフィルタ部に設定
フィルタ条件Bをフィルタ部に設定
フィルタ条件A
フィルタ条件B
電源オフ状態
鍵情報パケットAを保存
鍵情報パケットBに含まれている暗号鍵を復号
メディア復号
鍵情報パケットA
鍵情報パケットAに含まれている暗号鍵を復号
メディア復号
ST1
ST2
ST3
ST4
ST5
ST6
ST7
ST8
ST9
ST10
ST11
ST12

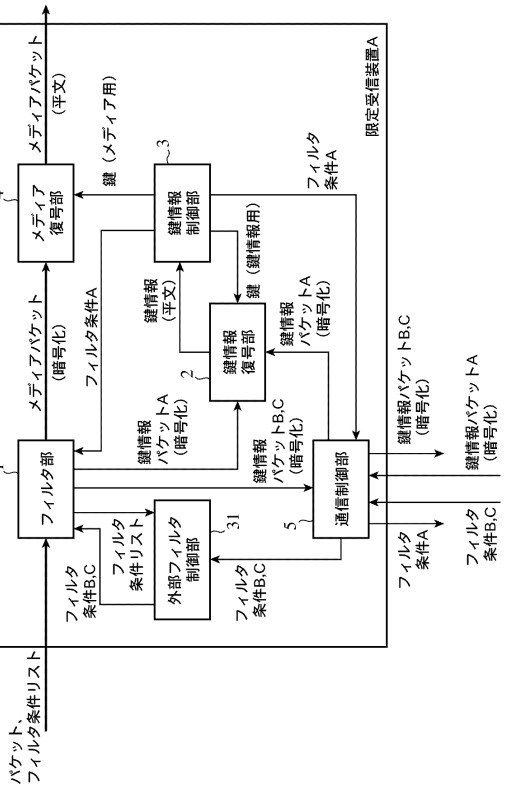
【図３】


限定受信装置A
パケット
メディアパケット（暗号化）
メディアパケット（平文）
フィルタ部
メディア復号部
鍵情報制御部
鍵情報復号部
通信制御部
外部フィルタ制御部
フィルタ条件A
フィルタ条件B,C
鍵情報パケットA（暗号化）
鍵情報パケットB,C（暗号化）
鍵（メディア用）
鍵（鍵情報用）
鍵情報（平文）

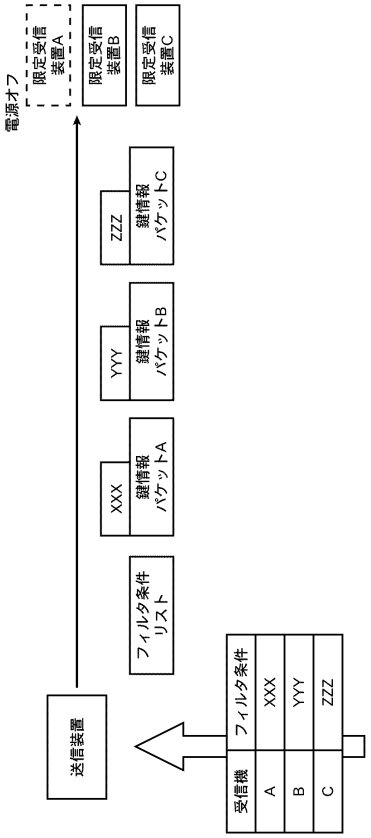
【図４】


限定受信装置A
パケット
メディアパケット（暗号化）
メディアパケット（平文）
フィルタ条件生成部
フィルタ部
メディア復号部
鍵情報制御部
鍵情報復号部
通信制御部
外部フィルタ制御部
フィルタ条件A
フィルタ条件B
鍵情報パケットA（暗号化）
鍵情報パケットB（暗号化）
鍵（メディア用）
鍵（鍵情報用）
鍵情報（平文）

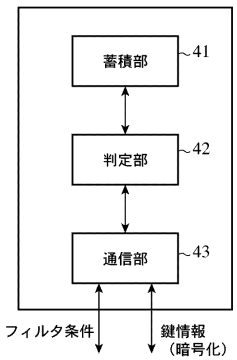
【図５】


限定受信装置A
メディアパケット（平文）
メディア復号部
4
鍵（メディア用）
鍵情報制御部
3
フィルタ条件A
メディアパケット（暗号化）
フィルタ条件A
鍵情報（平文）
鍵情報復号部
2
鍵（鍵情報用）
鍵情報パケットA（暗号化）
鍵情報パケットB,C（暗号化）
鍵情報パケットB,C（暗号化）
鍵情報パケットA（暗号化）
1
フィルタ部
通信制御部
5
フィルタ条件リスト
外部フィルタ制御部
31
フィルタ条件B,C
フィルタ条件B,C
フィルタ条件A
フィルタ条件B,C
パケット、フィルタ条件リスト

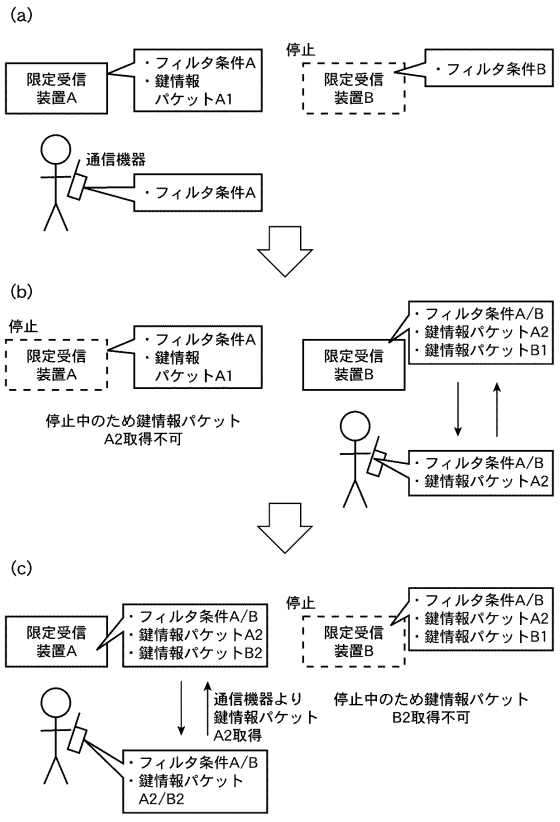
【図６】


電源オフ
限定受信装置A
限定受信装置B
限定受信装置C
ZZZ
鍵情報パケットC
YYY
鍵情報パケットB
XXX
鍵情報パケットA
フィルタ条件リスト
送信装置
受信機
フィルタ条件
A
B
C
XXX
YYY
ZZZ

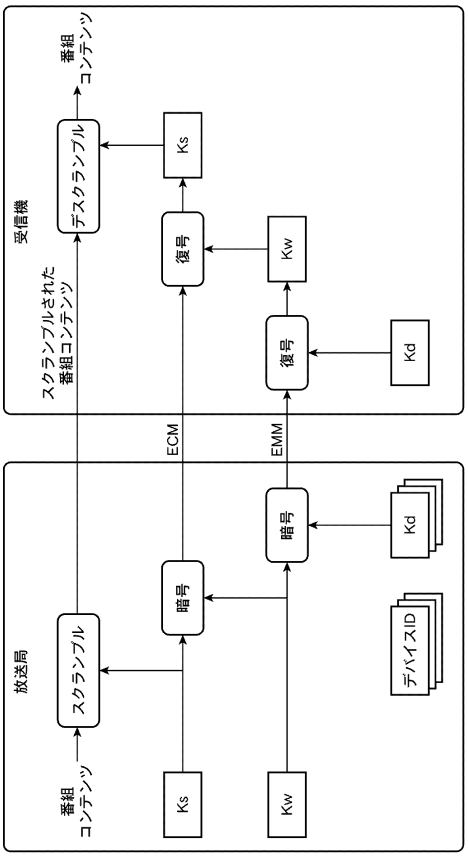
【図７】


蓄積部
41
判定部
42
通信部
43
フィルタ条件
鍵情報（暗号化）

【図８】


(a)
限定受信装置A
・フィルタ条件A
・鍵情報パケットA1
停止
限定受信装置B
・フィルタ条件B
通信機器
・フィルタ条件A
(b)
停止
限定受信装置A
・フィルタ条件A
・鍵情報パケットA1
停止中のため鍵情報パケットA2取得不可
限定受信装置B
・フィルタ条件A/B
・鍵情報パケットA2
・鍵情報パケットB1
・フィルタ条件A/B
・鍵情報パケットA2
(c)
限定受信装置A
・フィルタ条件A/B
・鍵情報パケットA2
・鍵情報パケットB2
停止
限定受信装置B
・フィルタ条件A/B
・鍵情報パケットA2
・鍵情報パケットB1
通信機器より鍵情報パケットA2取得
停止中のため鍵情報パケットB2取得不可
・フィルタ条件A/B
・鍵情報パケットA2/B2

【図９】


放送局
番組コンテンツ
スクランブル
暗号
暗号
Ks
Kw
Kd
デバイスID
ECM
EMM
受信機
スクランブルされた番組コンテンツ
デスクランブル
復号
復号
Ks
Kw
Kd
番組コンテンツ

フロントページの続き

(72)発明者　奥村　信義
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　坂田　憲司
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　後藤　嘉宏

(56)参考文献　特開２００７－１２９５７５（ＪＰ，Ａ）
特開２０００－１１５０９１（ＪＰ，Ａ）
国際公開第２００５／０９６１５７（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N　7/16
H04L　9/08