(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2006-148469
(P2006-148469A)
(43)公開日　平成18年6月8日(2006.6.8)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 9/08	(2006.01)	H04L 9/00	601B	5J104
H04L 12/22	(2006.01)	H04L 12/22		5K030
H04L 12/56	(2006.01)	H04L 12/56	260A	
		H04L 9/00	601E	

審査請求 未請求　請求項の数 5　OL　（全 13 頁）

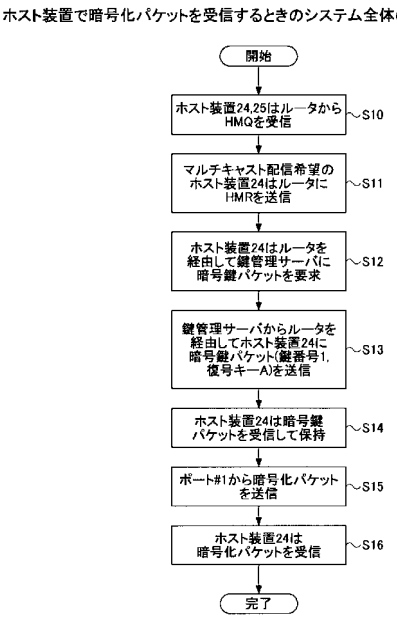
(21)出願番号　特願2004-334752 (P2004-334752)
(22)出願日　平成16年11月18日 (2004.11.18)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　安部　健一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　吉村　直政
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Fターム(参考)　5J104 EA16　PA05　PA07
5K030 GA15　HA08　HD03　JA11　KX28
LD06　LD19

(54)【発明の名称】マルチキャスト配信方法及びホスト装置及びルータ

(57)【要約】
【課題】　本発明は、配信要求を行ったホスト装置だけに復号キーを配信し、配信要求を行ったホスト装置だけでストリーミングの暗号化パケットを復号できるマルチキャスト配信方法及びホスト装置及びルータを提供することを目的とする。
【解決手段】　ストリーミングサーバ２０は鍵管理サーバ２１から通知された鍵番号とストリーミングを暗号化したデータを含む暗号化パケットをルータ２２に送信し、マルチキャスト配信を希望するホスト装置２４はルータに配信要求を行い、更に、ルータを介して鍵管理サーバに暗号鍵パケットを要求し、ルータは鍵管理サーバから送信される暗号鍵パケットを、配信要求を行ったホスト装置だけに送信し、ホスト装置は受信した暗号鍵パケットに含まれる鍵番号とルータからマルチキャスト配信される暗号化パケットに含まれる鍵番号が一致したとき、暗号鍵パケットに含まれる復号キーを用いて暗号化パケットに含まれるストリーミングを暗号化したデータを復号する。
【選択図】　図５



【特許請求の範囲】
【請求項１】
ストリーミングサーバからルータに送信されるストリーミングを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信方法であって、
前記ストリーミングサーバは鍵管理サーバから通知された鍵番号と前記ストリーミングを暗号化したデータを含む暗号化パケットを前記ルータに送信し、
マルチキャスト配信を希望するホスト装置は前記ルータに配信要求を行い、更に、前記ルータを介して前記鍵管理サーバに暗号鍵パケットを要求し、
前記ルータは前記鍵管理サーバから送信される前記暗号鍵パケットを、前記配信要求を行ったホスト装置だけに送信し、
前記ホスト装置は受信した暗号鍵パケットに含まれる鍵番号と前記ルータからマルチキャスト配信される暗号化パケットに含まれる鍵番号が一致したとき、前記暗号鍵パケットに含まれる復号キーを用いて前記暗号化パケットに含まれるストリーミングを暗号化したデータを復号することを特徴とするマルチキャスト配信方法。
【請求項２】
ストリーミングサーバからルータに送信されるストリーミングを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信システムのホスト装置であって、
前記ルータに配信要求を行い、更に、前記ルータを介して前記鍵管理サーバに暗号鍵パケットを要求する要求手段と、
受信した前記鍵管理サーバからの暗号鍵パケットに含まれる鍵番号と前記ルータからマルチキャスト配信される暗号化パケットに含まれる鍵番号が一致したとき、前記暗号鍵パケットに含まれる復号キーを用いて前記暗号化パケットに含まれるストリーミングを暗号化したデータを復号する復号手段を
有することを特徴とするホスト装置。
【請求項３】
ストリーミングサーバからルータに送信されるストリーミングを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信システムのルータであって、
マルチキャスト配信を希望するホスト装置からの配信要求と前記鍵管理サーバに対する暗号鍵パケットの要求があったのち、前記鍵管理サーバから送信される前記暗号鍵パケットを、前記配信要求を行ったホスト装置だけに送信する暗号鍵パケット送信手段を
有することを特徴とするルータ。
【請求項４】
請求項１記載のマルチキャスト配信方法において、
前記ストリーミングサーバは、所定時間毎に前記暗号鍵パケットの鍵番号を変更し、前記暗号鍵パケットの鍵番号を変更する前に前記暗号鍵パケットの鍵番号の変更情報を前記暗号化パケットに付加して前記ルータに送信し、
マルチキャスト配信を受信しているホスト装置は前記暗号鍵パケットの鍵番号の変更情報を受けて前記鍵管理サーバに変更後の暗号鍵パケットを要求し、
前記ルータは前記鍵管理サーバから送信される前記変更後の暗号鍵パケットを、前記暗号鍵パケットの要求を行ったホスト装置だけに送信し、
前記ホスト装置は受信した前記変更後の暗号鍵パケットを使用中の暗号鍵パケットと共に保持することを特徴とするマルチキャスト配信方法。
【請求項５】
請求項４記載のマルチキャスト配信方法において、
前記ホスト装置は前記ルータからマルチキャスト配信される暗号化パケットの鍵番号が変更されたとき前記使用中の暗号鍵パケットを削除することを特徴とするマルチキャスト配信方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、マルチキャスト配信方法及びホスト装置及びルータに関し、ストリーミングのマルチキャスト配信を行うマルチキャスト配信方法及びホスト装置及びルータに関する。
【背景技術】
【０００２】
図１は従来のマルチキャスト配信システムの一例のシステム構成図、図２は従来のマルチキャスト配信シーケンスを示す。図１において、ストリーミングサーバ１０はルータ１１に接続され、ルータ１１のポート＃１にＬＡＮ１２が接続され、ＬＡＮ１２にはホスト装置１３，１４が接続されている。
【０００３】
図２に示すように、ストリーミングサーバ１０は常時ルータ１１に対しストリーミングを配信している。ルータ１１のポート＃１配下のホスト装置１３，１４は定期的（例えば１２５ｓｅｃ毎）にルータ１１からマルチキャストの参加確認をするＨＭＱ（Ｈｏｓｔ Ｍｅｍｂｅｒｓｈｉｐ Ｑｕｅｒｙ）を受信している。
【０００４】
ホスト装置１３でルータ１１にマルチキャストを希望する場合、ホスト装置１３はルータ１１にＨＭＲ（Ｈｏｓｔ Ｍｅｍｂｅｒｓｈｉｐ Ｒｅｐｏｒｔ）を送信する。ＨＭＲを受信したルータ１１はポート＃１配下のＬＡＮ１２にストリーミングをマルチキャスト配信する。これにより、ルータ１１のポート＃１配下に接続されたホスト装置１３，１４はストリーミングを受信することができる。
【０００５】
ところで、特許文献１には、クライアント装置が収容されているルーティング装置に認証機能を持たせ、この認証機能付きルーティング装置にコンテンツサーバと暗号鍵パケット管理装置からコンテンツと復号鍵をマルチキャストで配信し、認証機能付きルーティング装置ではクライアント装置からの要求に対して認証を行い、認証が通った場合にのみクライアント装置に対しコンテンツ及び復号鍵の配信を行うことが記載されている。
【特許文献１】特開２００３－１７４４４０公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
従来のマルチキャスト配信システムでは、ストリーミングのマルチキャスト配信を希望しているのはホスト装置１３であるが、ルータ１１のポート＃１配下に接続されたホスト装置１４においてもストリーミングがマルチキャスト配信されてしまうという問題があった。
【０００７】
特許文献１の技術においても、認証機能付きルーティング装置はポート単位でクライアント装置に対しコンテンツ及び復号キーの配信を行うため、認証が通ったクライアント装置と同一ポートに接続されている他のクライアント装置にもコンテンツ及び復号キーが配信されてしまうという問題があった。
【０００８】
本発明は、上記の点に鑑みなされたものであり、配信要求を行ったホスト装置だけに復号キーを配信し、配信要求を行ったホスト装置だけでストリーミングの暗号化パケットを復号できるマルチキャスト配信方法及びホスト装置及びルータを提供することを目的とする。
【課題を解決するための手段】
【０００９】
請求項１に記載の発明は、ストリーミングサーバからルータに送信されるストリーミン

グを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信方法であって、
前記ストリーミングサーバは鍵管理サーバから通知された鍵番号と前記ストリーミングを暗号化したデータを含む暗号化パケットを前記ルータに送信し、
マルチキャスト配信を希望するホスト装置は前記ルータに配信要求を行い、更に、前記ルータを介して前記鍵管理サーバに暗号鍵パケットを要求し、
前記ルータは前記鍵管理サーバから送信される前記暗号鍵パケットを、前記配信要求を行ったホスト装置だけに送信し、
前記ホスト装置は受信した暗号鍵パケットに含まれる鍵番号と前記ルータからマルチキャスト配信される暗号化パケットに含まれる鍵番号が一致したとき、前記暗号鍵パケットに含まれる復号キーを用いて前記暗号化パケットに含まれるストリーミングを暗号化したデータを復号することにより、
配信要求を行ったホスト装置だけに復号キーを配信し、配信要求を行ったホスト装置だけでストリーミングの暗号化パケットを復号できる。

【００１０】

請求項２に記載の発明は、ストリーミングサーバからルータに送信されるストリーミングを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信システムのホスト装置であって、
前記ルータに配信要求を行い、更に、前記ルータを介して前記鍵管理サーバに暗号鍵パケットを要求する要求手段と、
受信した前記鍵管理サーバからの暗号鍵パケットに含まれる鍵番号と前記ルータからマルチキャスト配信される暗号化パケットに含まれる鍵番号が一致したとき、前記暗号鍵パケットに含まれる復号キーを用いて前記暗号化パケットに含まれるストリーミングを暗号化したデータを復号する復号手段を有し、
請求項３に記載の発明は、ストリーミングサーバからルータに送信されるストリーミングを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信システムのルータであって、
マルチキャスト配信を希望するホスト装置からの配信要求と前記鍵管理サーバに対する暗号鍵パケットの要求があったのち、前記鍵管理サーバから送信される前記暗号鍵パケットを、前記配信要求を行ったホスト装置だけに送信する暗号鍵パケット送信手段を有することにより、
配信要求を行ったホスト装置だけに復号キーを配信し、配信要求を行ったホスト装置だけでストリーミングの暗号化パケットを復号できる。

【００１１】

請求項４に記載の発明は、請求項１記載のマルチキャスト配信方法において、
前記ストリーミングサーバは、所定時間毎に前記暗号鍵パケットの鍵番号を変更し、前記暗号鍵パケットを変更する前に前記暗号鍵パケットの鍵番号の変更情報を前記暗号化パケットに付加して前記ルータに送信し、
マルチキャスト配信を受信しているホスト装置は前記暗号鍵パケットの鍵番号の変更情報を受けて前記鍵管理サーバに変更後の暗号鍵パケットを要求し、
前記ルータは前記鍵管理サーバから送信される前記変更後の暗号鍵パケットを、前記暗号鍵パケットの要求を行ったホスト装置だけに送信し、
前記ホスト装置は受信した前記変更後の暗号鍵パケットを使用中の暗号鍵パケットと共に保持することにより、
マルチキャスト配信を受信しているホスト装置ではストリーミングサーバが暗号鍵パケットを変更する前に変更後の暗号鍵パケットを保持することができる。

【００１２】

請求項５に記載の発明は、請求項４記載のマルチキャスト配信方法において、
前記ホスト装置は前記ルータからマルチキャスト配信される暗号化パケットの鍵番号が変更されたとき前記使用中の暗号鍵パケットを削除することにより、不要となった暗号鍵

パケットを削除することができる。

【発明の効果】

【００１３】

本発明によれば、配信要求を行ったホスト装置だけに復号鍵を配信し、配信要求を行ったホスト装置だけでストリーミングの暗号化パケットを復号できる。

【発明を実施するための最良の形態】

【００１４】

以下、図面に基づいて本発明の実施形態について説明する。

【００１５】

図３は、本発明のマルチキャスト配信方法を適用したシステムの一実施形態のシステム構成図を示す。同図中、ストリーミングサーバ２０と鍵管理サーバ２１は接続されており、ストリーミングサーバ２０は鍵管理サーバ２１から供給される暗号化鍵を用いて暗号化した暗号化パケットのストリーミングを常時ルータ２２に配信する。鍵管理サーバ２１は、鍵番号と復号鍵を管理しており、鍵管理サーバ２１はストリーミングサーバ２０との間でＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）を使って鍵番号を同期させている。ルータ２２のポート＃１にはＬＡＮ２３が接続され、ＬＡＮ２３にはホスト装置２４，２５が接続されている。

【００１６】

ルータ２２は例えば１２５ｓ周期で定期的にマルチキャストの参加確認を行うＨＭＱを送信しており、ルータ２２のポート＃１配下のホスト装置２４，２５は定期的にルータ２２からのＨＭＱを受信する。マルチキャスト配信を希望するホスト装置２４，２５のいずれかはルータ２２にＨＭＲを送信する。ルータ２２はＨＭＲを受信したポート＃１からＬＡＮ２３に暗号化パケットを送信する。

【００１７】

図４は、本発明のマルチキャスト配信方法で使用されるホスト装置２４，２５の一実施形態のブロック図を示す。同図中、ホスト装置３０は、パケット受信部３１と、ＩＧＭＰ（Ｉｎｔｅｒｎｅｔ Ｇｒｏｕｐ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）受信部３２と、暗号化パケット受信部３３と、暗号鍵パケット受信部３４と、非プロトコルパケット受信部３５と、制御部３６内のＩＧＭＰ処理部３７、復号処理部３８、パケット処理部３９を有している。

【００１８】

パケット受信部３１はＬＡＮ２３に接続されており、ルータ２２から送信されたパケットを受信してＩＧＭＰ受信部３２、暗号化パケット受信部３３、暗号鍵パケット受信部３４、非プロトコルパケット受信部３５それぞれに供給する。

【００１９】

パケット受信部３１で受信されたパケットのうちＩＧＭＰパケットはＩＧＭＰ受信部３２で受信され、ＩＧＭＰ処理部３７にて処理される。また、暗号化パケットは暗号化パケット受信部３３で受信され、復号処理部３８にて復号されたのちパケット処理部３９に供給される。また、暗号鍵パケットは暗号鍵パケット受信部３４で受信されて復号処理部３８に供給される。また、非プロトコルパケットは非プロトコルパケット受信部３５で受信されてパケット処理部３９に供給される。

【００２０】

図５は、ホスト装置で暗号化パケットを受信するときのシステム全体のフローチャートを示す。同図中、ステップＳ１０で例えばホスト装置２４は、定期的にルータ２２からのＨＭＱを受信する。マルチキャスト配信を希望するホスト装置２４はステップＳ１１でルータ２２にＨＭＲを送信する。

【００２１】

ステップＳ１２でＨＭＲを送信したホスト装置２４は、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ：ホストとサーバ間のデータを暗号化した通信）等を用いルータ２２，ストリーミングサーバ２０を経由して鍵管理サーバ２１に暗号鍵パケットを要求する

。

【００２２】

ステップＳ１３で鍵管理サーバ２１はＳＳＬ等を用いストリーミングサーバ２０，ルータ２２を経由して暗号鍵パケット（鍵番号１、復号キーＡ）を、ＨＭＲの送信及び暗号鍵パケット要求を行ったホスト装置２４だけに送信する。ステップＳ１４でホスト装置２４は暗号鍵パケット（鍵番号１、復号キーＡ）を受信して保持する。

【００２３】

ステップＳ１５でルータ２２はＨＭＲを受信したポート＃１からＬＡＮ２３に暗号化パケットを送信する。ステップＳ１６でホスト装置２４はルータ２２からの暗号化パケットを受信する。

【００２４】

図６に、ＨＭＲの構成を示す。同図中、ＨＭＲは、送信先アドレス（ＤＡ：送信先のＭＡＣアドレス）、送信元アドレス（ＳＡ：送信元のＭＡＣアドレス）、次のデータがＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）であることを示すＴｙｐｅ０８００、データ、ＦＣＳ（Ｆｒａｍｅ　Ｃｈｅｃｋ　Ｓｅｑｕｅｎｃｅ）で構成される。データはＩＰヘッダとＩＧＭＰヘッダで構成される。

【００２５】

ＨＭＲを受信したルータ２２ではＨＭＲ内の送信元アドレス（ＳＡ）によってＨＭＲを送信したホスト装置２４を知り、その後、鍵管理サーバ２１からの暗号鍵パケットをＨＭＲの送信元であるホスト装置２４だけに送信することができる。

【００２６】

図７に、暗号化パケットの構成を示す。同図中、暗号化パケットは、鍵番号、更新フラグ、マルチキャスト暗号化データで構成される。更新フラグは値０が鍵番号の更新が不要であることを示し、値１が鍵番号の更新が必要であることを示す。

【００２７】

図８は、ホスト装置で暗号化パケットを復号するときのフローチャートを示す。同図中、ステップＳ３０でホスト装置は保持している暗号鍵パケットの鍵番号と、受信した暗号化パケット内の鍵番号を比較する。双方の鍵番号が一致した場合（ホスト装置２４の場合）、ステップＳ３１でマルチキャスト送信された暗号化パケットを保持している復号キー（例えば復号キーＡ）で復号し、ステップＳ３２でストリーミングを見ることができる。双方の鍵番号が一致しない場合（ホスト装置２５の場合）、ステップＳ３３でストリーミングを見ることができない。

【００２８】

暗号鍵パケットの更新について説明する。暗号化パケットの鍵番号を更新する時間を予め設定する。例えば送信開始からｍ（例えばｍ＝６０）分毎に鍵番号を更新するように設定する。ストリーミングサーバ２０は鍵番号１で更新フラグ０の暗号化パケットを送信して、鍵番号を更新するｎ分前（例えばｎ＝３）に、鍵番号１で更新フラグ１の暗号化パケットを送信する。その後ｎ分間、鍵番号１で更新フラグ０の暗号化パケットを送信したのち、鍵番号２で更新フラグ０に切り替えて暗号化パケットを送信する。

【００２９】

図９は、ホスト装置で暗号鍵パケットを更新するときのフローチャートを示す。同図中、ステップＳ４０でホスト装置２４は、更新フラグ１の暗号化パケットを受信したか否かを判別する。更新フラグ１の暗号化パケットを受信した場合、ホスト装置２４はステップＳ４１でＳＳＬ等を用いルータ２２，ストリーミングサーバ２０を経由して鍵管理サーバ２１に暗号鍵パケットの更新を要求する。

【００３０】

ステップＳ４２で鍵管理サーバ２１はＳＳＬ等を用いストリーミングサーバ２０，ルータ２２を経由して暗号鍵パケット（鍵番号２、復号キーＢ）を暗号鍵パケットの更新要求があったホスト装置２４だけに送信する。ステップＳ４３でホスト装置２４は暗号鍵パケット（鍵番号２、復号キーＢ）を受信して暗号鍵パケット（鍵番号１、復号キーＡ）と共

に保持する。
【００３１】
一方、ステップＳ４０で更新フラグ１の暗号化パケットを受信していない場合、ホスト装置２４は暗号鍵パケットの更新を要求することなく処理を終了する。
【００３２】
これによって、マルチキャスト配信を受信しているホスト装置２４ではストリーミングサーバ２０が暗号鍵パケットを変更する前に変更後の暗号鍵パケットを保持することができる。
【００３３】
図１０は、暗号鍵パケットを削除するときのホスト装置のフローチャートを示す。同図中、ステップＳ５０で例えばホスト装置２４は複数の暗号鍵パケットを保持しているか否かを判別し、複数の暗号鍵パケットを保持している場合、ステップＳ５１でホスト装置２４は新たな暗号化パケット（鍵番号２で更新フラグ０の暗号化パケット）を受信したか否かを判別する。新たな暗号化パケット（鍵番号２で更新フラグ０の暗号化パケット）を受信した場合、ステップＳ５２でホスト装置２４は不要となった暗号鍵パケット（鍵番号１、復号キーＡ）を削除する。
【００３４】
複数の暗号鍵パケットを保持していない場合、または、新たな暗号化パケット（鍵番号２で更新フラグ０の暗号化パケット）を受信していない場合、ホスト装置２４はこの処理を終了する。
【００３５】
図１１及び図１２は、本発明のマルチキャスト配信方法の動作シーケンスの一実施形態を示す。同図中、ストリーミングサーバ２０は鍵管理サーバ２１に鍵番号を要求し、鍵番号１が通知されたのち、時刻ｔ１からルータ２２に対し鍵番号１で更新フラグ０の暗号化パケットの送信を開始する。また、ルータ２２はＨＭＱを定期的にホスト装置２４、２５に対し送信する。時刻ｔ２にホスト装置２４はルータ２２にＨＭＲを送信すると、時刻ｔ３にルータ２２は鍵番号１で更新フラグ０の暗号化パケットをホスト装置２４、２５に対し送信する。
【００３６】
時刻ｔ４にホスト装置２４がＳＳＬを用いて鍵管理サーバ２１に暗号鍵パケットを要求すると、時刻ｔ５に鍵管理サーバ２１はＳＳＬを用いてホスト装置２４に暗号鍵パケット（鍵番号１、復号キーＡ）を送信する。
【００３７】
これにより、ホスト装置２４ではルータ２２から送信される鍵番号１で更新フラグ０の暗号化パケットの復号が可能となる。また、ホスト装置２５では暗号鍵パケット（鍵番号１、復号キーＡ）がないため、ルータ２２から送信される鍵番号１で更新フラグ０の暗号化パケットの復号が不可能である。
【００３８】
ストリーミングサーバ２０は時刻ｔ６にルータ２２に対し鍵番号１で更新フラグ１の暗号化パケットの送信し、この暗号化パケットはルータ２２からホスト装置２４，２５に送信される。この後、ストリーミングサーバ２０は鍵管理サーバ２１に鍵番号を要求し、時刻ｔ７に鍵管理サーバ２１から新たな鍵番号（鍵番号２）を受信する。
【００３９】
図１２において、時刻ｔ８にホスト装置２４はＳＳＬ等を用い鍵管理サーバ２１に暗号鍵パケットの更新を要求し、時刻ｔ９に鍵管理サーバ２１から新たな暗号鍵パケット（鍵番号２、復号キーＢ）を受信する。
【００４０】
その後、ストリーミングサーバ２０は時刻ｔ１０にルータ２２に対し鍵番号２で更新フラグ０の暗号化パケットの送信を開始し、この時点でホスト装置２４は古い暗号鍵パケット（鍵番号１、復号キーＡ）を削除し、これ以降、ホスト装置２４ではルータ２２から送

信される鍵番号２で更新フラグ０の暗号化パケットを新たな暗号鍵パケット（鍵番号２、復号キーＢ）の復号キーＢを用いて復号する。

【００４１】

なお、ステップＳ１１，Ｓ１２が請求項または付記記載の要求手段に対応し、ステップＳ３１が復号手段に対応し、ステップＳ１３が暗号鍵パケット送信手段に対応し、ステップＳ４１が変更後暗号鍵パケット要求手段に対応し、ステップＳ４３が保持手段に対応し、ステップＳ５２が削除手段に対応する。

（付記１）

ストリーミングサーバからルータに送信されるストリーミングを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信方法であって、

前記ストリーミングサーバは鍵管理サーバから通知された鍵番号と前記ストリーミングを暗号化したデータを含む暗号化パケットを前記ルータに送信し、

マルチキャスト配信を希望するホスト装置は前記ルータに配信要求を行い、更に、前記ルータを介して前記鍵管理サーバに暗号鍵パケットを要求し、

前記ルータは前記鍵管理サーバから送信される前記暗号鍵パケットを、前記配信要求を行ったホスト装置だけに送信し、

前記ホスト装置は受信した暗号鍵パケットに含まれる鍵番号と前記ルータからマルチキャスト配信される暗号化パケットに含まれる鍵番号が一致したとき、前記暗号鍵パケットに含まれる復号キーを用いて前記暗号化パケットに含まれるストリーミングを暗号化したデータを復号することを特徴とするマルチキャスト配信方法。

（付記２）

ストリーミングサーバからルータに送信されるストリーミングを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信システムのホスト装置であって、

前記ルータに配信要求を行い、更に、前記ルータを介して前記鍵管理サーバに暗号鍵パケットを要求する要求手段と、

受信した前記鍵管理サーバからの暗号鍵パケットに含まれる鍵番号と前記ルータからマルチキャスト配信される暗号化パケットに含まれる鍵番号が一致したとき、前記暗号鍵パケットに含まれる復号キーを用いて前記暗号化パケットに含まれるストリーミングを暗号化したデータを復号する復号手段を

有することを特徴とするホスト装置。

（付記３）

ストリーミングサーバからルータに送信されるストリーミングを前記ルータの同一ポートに接続されている複数のホスト装置にマルチキャスト配信するマルチキャスト配信システムのルータであって、

マルチキャスト配信を希望するホスト装置からの配信要求と前記鍵管理サーバに対する暗号鍵パケットの要求があったのち、前記鍵管理サーバから送信される前記暗号鍵パケットを、前記配信要求を行ったホスト装置だけに送信する暗号鍵パケット送信手段を

有することを特徴とするルータ。

（付記４）

付記１記載のマルチキャスト配信方法において、

前記ストリーミングサーバは、所定時間毎に前記暗号鍵パケットの鍵番号を変更し、前記暗号鍵パケットの鍵番号を変更する前に前記暗号鍵パケットの鍵番号の変更情報を前記暗号化パケットに付加して前記ルータに送信し、

マルチキャスト配信を受信しているホスト装置は前記暗号鍵パケットの鍵番号の変更情報を受けて前記鍵管理サーバに変更後の暗号鍵パケットを要求し、

前記ルータは前記鍵管理サーバから送信される前記変更後の暗号鍵パケットを、前記暗号鍵パケットの要求を行ったホスト装置だけに送信し、

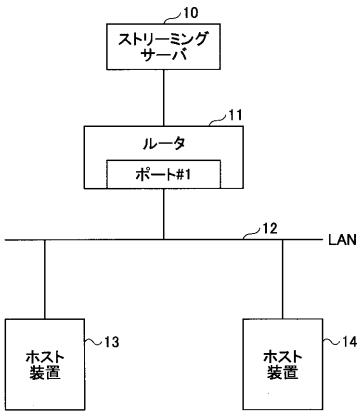
前記ホスト装置は受信した前記変更後の暗号鍵パケットを使用中の暗号鍵パケットと共

に保持することを特徴とするマルチキャスト配信方法。
（付記５）
付記４記載のマルチキャスト配信方法において、
前記ホスト装置は前記ルータからマルチキャスト配信される暗号化パケットの鍵番号が変更されたとき前記使用中の暗号鍵パケットを削除することを特徴とするマルチキャスト配信方法。
（付記６）
付記２記載のホスト装置において、
マルチキャスト配信を受信しているホスト装置は前記暗号化パケットに付加された前記暗号鍵パケットの鍵番号の変更情報を受けて前記鍵管理サーバに変更後の暗号鍵パケットを要求する変更後暗号鍵パケット要求手段と、
前記鍵管理サーバから送信される前記変更後の暗号鍵パケットを受信して使用中の暗号鍵パケットと共に保持する保持手段を
有することを特徴とするホスト装置。
（付記７）
付記６記載のホスト装置において、
前記ルータからマルチキャスト配信される暗号化パケットの鍵番号が変更されたとき前記保持手段の使用中の暗号鍵パケットを削除する削除手段を
有することを特徴とするホスト装置。
【図面の簡単な説明】
【００４２】
【図１】従来のマルチキャスト配信システムの一例のシステム構成図である。
【図２】従来のマルチキャスト配信シーケンス図である。
【図３】本発明のマルチキャスト配信方法を適用したシステムの一実施形態のシステム構成図である。
【図４】本発明のマルチキャスト配信方法で使用されるホスト装置２４，２５の一実施形態のブロック図である。
【図５】ホスト装置で暗号化パケットを受信するときのシステム全体のフローチャートである。
【図６】ＨＭＲの構成を示す図である。
【図７】暗号化パケットの構成を示す図である。
【図８】ホスト装置で暗号化パケットを復号するときのフローチャートである。
【図９】ホスト装置で暗号鍵パケットを更新するときのフローチャートである。
【図１０】暗号鍵パケットを削除するときのホスト装置のフローチャートである。
【図１１】本発明のマルチキャスト配信方法の動作シーケンスである。
【図１２】本発明のマルチキャスト配信方法の動作シーケンスである。
【符号の説明】
【００４３】
２０　ストリーミングサーバ
２１　鍵管理サーバ
２２　ルータ
２３　ＬＡＮ
２４，２５　ホスト装置
３１　ホスト装置
３２　ＩＧＭＰ受信部
３３　暗号化パケット受信部
３４　暗号鍵パケット受信部
３５　非プロトコルパケット受信部
３６　制御部
３７　ＩＧＭＰ処理部

３８　復号処理部
３９　パケット処理部

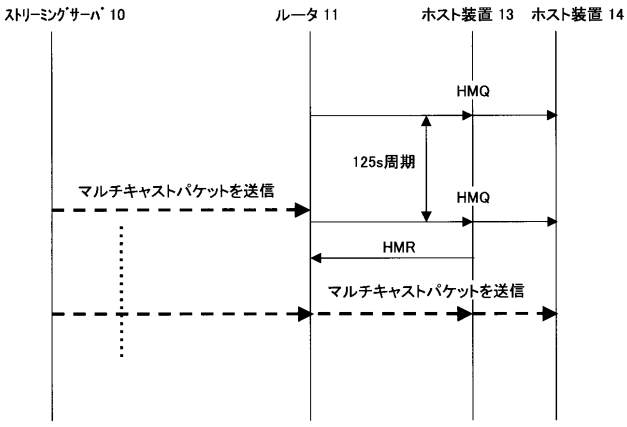
【図１】

従来のマルチキャスト配信システムの一例のシステム構成図



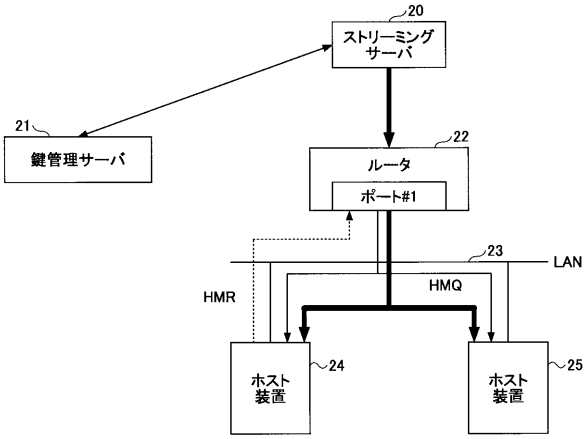
【図２】

従来のマルチキャスト配信シーケンス図



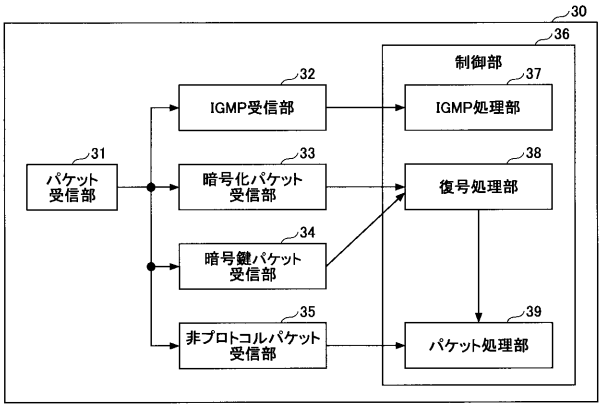
【図３】

本発明のマルチキャスト配信方法を適用したシステムの一実施形態のシステム構成



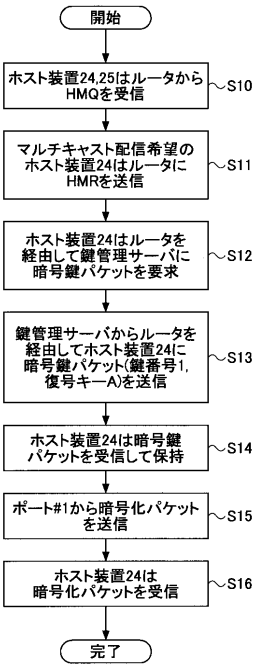
【図４】

本発明のマルチキャスト配信方法で使用されるホスト装置24，25の一実施形態のブロック図



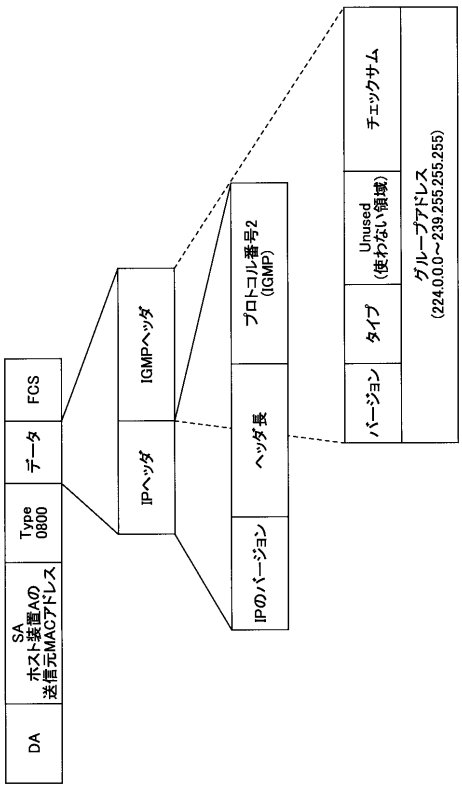
【図５】

ホスト装置で暗号化パケットを受信するときのシステム全体のフローチャート



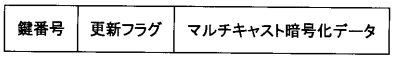
【図６】

HMRの構成を示す図



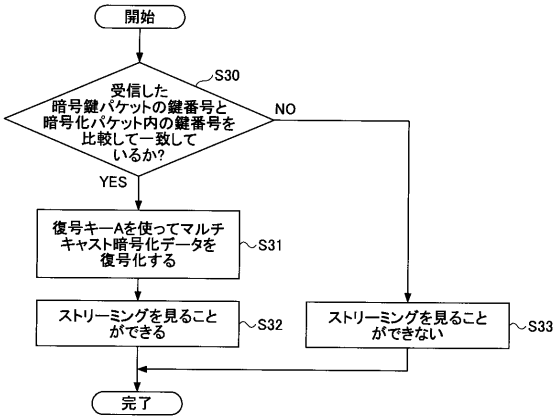
【図７】

暗号化パケットの構成を示す図



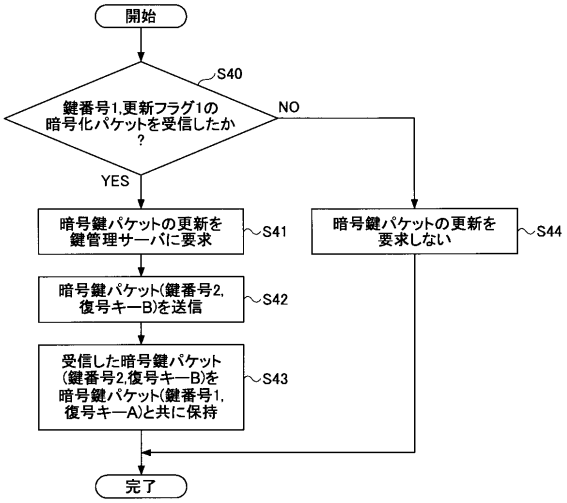
【図８】

ホスト装置で暗号化パケットを復号するときのフローチャート



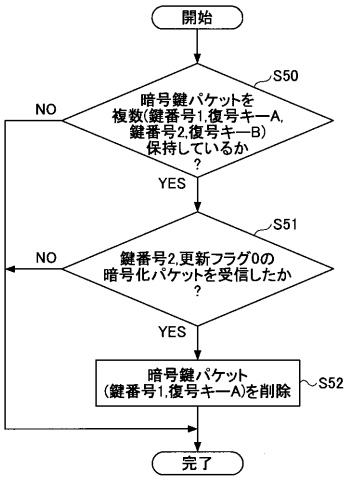
【図９】

ホスト装置で暗号鍵を更新するときのフローチャート



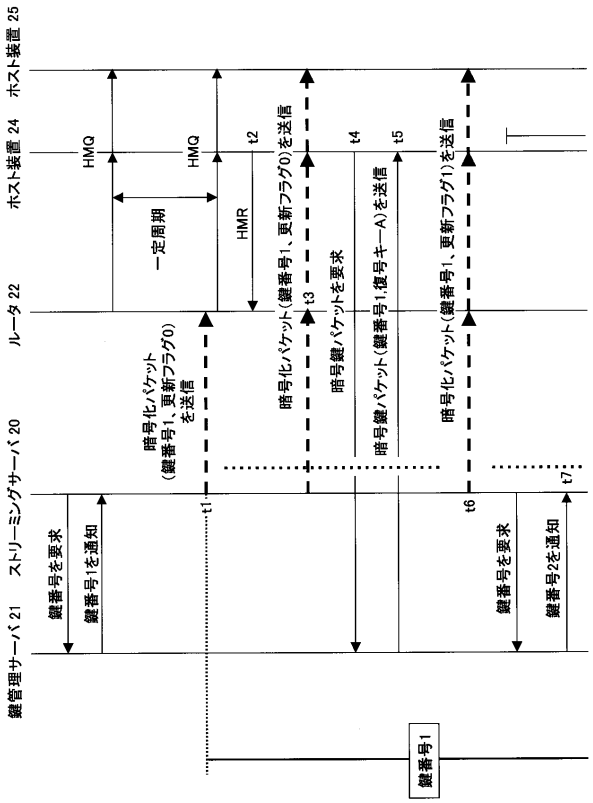
【図１０】

暗号鍵を削除するときのホスト装置のフローチャート



【図１１】

本発明のマルチキャスト配信方法の動作シーケンス



【図１２】

本発明のマルチキャスト配信方法の動作シーケンス