(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2004-266342
(P2004-266342A)
(43)公開日　平成16年9月24日(2004.9.24)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601B	5J104
	H04L	9/00	601E	

審査請求 未請求　請求項の数 18　OL　（全 23 頁）

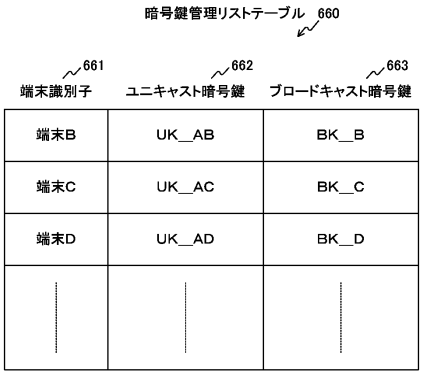
(21)出願番号　特願2003-26543(P2003-26543)
(22)出願日　平成15年2月3日(2003.2.3)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100112955
弁理士　丸島　敏一
(72)発明者　鈴木　英之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Fターム(参考)　5J104 AA16　EA02　EA17　EA19

(54)【発明の名称】無線アドホック通信システム、端末、その端末における復号方法、暗号化方法及びブロードキャスト暗号鍵配布方法並びにそれらの方法を端末に実行させるためのプログラム

(57)【要約】
【課題】無線アドホック通信システムにおいて、ブロードキャスト暗号鍵の管理を自律分散して行う。
【解決手段】無線アドホック通信システムにおける各端末は暗号鍵管理リストテーブル６６０を備える。この暗号鍵管理リストテーブル６６０では、ＭＡＣアドレス等の端末識別子６６１に関連付けられて、その端末識別子６６１により識別される端末との間のユニキャスト通信に用いられるユニキャスト暗号鍵６６２およびその端末識別子６６１により識別される端末がブロードキャスト通信を行う際に用いられるブロードキャスト暗号鍵６６３が保持される。これにより、ブロードキャスト通信を行う端末毎にブロードキャスト暗号鍵が設けられ、ブロードキャスト暗号鍵の管理が各端末により自律分散して行われる。
【選択図】　図５



【特許請求の範囲】
【請求項１】
複数の端末により構成される無線アドホック通信システムであって、
ブロードキャストフレームのペイロードを暗号化して当該ブロードキャストフレームを送信する第１の端末と、
前記ブロードキャストフレームを受信して当該ブロードキャストフレームのペイロードを復号する第２の端末とを具備し、
前記第１の端末は前記第１の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを暗号化し、
前記第２の端末は前記第１の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する
ことを特徴とする無線アドホック通信システム。
【請求項２】
前記第２の端末は、
前記第１の端末の端末識別子と前記第１の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも有する暗号鍵管理リストテーブルと、受信したブロードキャストフレームの始点端末識別子に含まれる前記第１の端末の端末識別子により前記暗号鍵管理リストテーブルを検索して対応する前記第１の端末のブロードキャスト暗号鍵を抽出する手段と、
抽出された前記第１の端末のブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手段とを備える
ことを特徴とする請求項１記載の無線アドホック通信システム。
【請求項３】
前記第１の端末は、
前記第１の端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、
ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持された前記第１の端末のブロードキャスト暗号鍵により暗号化する手段と、
暗号化された前記ブロードキャストフレームを送信する手段とを備える
ことを特徴とする請求項１記載の無線アドホック通信システム。
【請求項４】
他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、
受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手段と、
抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手段と
を具備することを特徴とする端末。
【請求項５】
他の端末の端末識別子に対応して前記他の端末との間のユニキャスト暗号鍵および前記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、
受信したフレームの終点端末識別子がブロードキャストアドレスであれば当該フレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を暗号鍵として抽出し、前記受信したフレームの終点端末識別子がブロードキャストアドレス以外であれば当該フレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵を前記暗号鍵として抽出する手段と、
抽出された前記暗号鍵により前記フレームのペイロードを復号する手段と
を具備することを特徴とする端末。

【請求項６】
自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、
ブロードキャストフレームのペイロードを前記ブロードキャスト暗号鍵により暗号化する手段と、
暗号化された前記ブロードキャストフレームを送信する手段と
を具備することを特徴とする端末。
【請求項７】
自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、
他の端末の端末識別子に対応して前記他の端末との間のユニキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、
送信しようとするフレームがブロードキャストフレームであれば前記生成鍵テーブルの前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを暗号化し、送信しようとする前記フレームがユニキャストフレームであれば当該ユニキャストフレームの終点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵により前記ユニキャストフレームのペイロードを暗号化する手段と、
暗号化された前記フレームを送信する手段と
を具備することを特徴とする端末。
【請求項８】
送信先端末のユニキャスト暗号鍵により自端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、
前記暗号化された自端末の端末識別子およびブロードキャスト暗号鍵を前記送信先端末に送信する手段と
を具備することを特徴とする端末。
【請求項９】
他の端末の端末識別子に対応して前記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、
送信先端末のユニキャスト暗号鍵により前記暗号鍵管理リストを暗号化する手段と、
前記暗号化された暗号鍵管理リストを前記送信先端末に送信する手段と
を具備することを特徴とする端末。
【請求項１０】
他の端末から当該他の端末の端末識別子およびブロードキャスト暗号鍵を受信する手段と、
自端末のブロードキャスト暗号鍵により前記他の端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、
前記暗号化された他の端末の端末識別子およびブロードキャスト暗号鍵をブロードキャスト配布する手段と
を具備することを特徴とする端末。
【請求項１１】
他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末におけるブロードキャストフレームの復号方法であって、
受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手順と、
抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手順と
を具備することを特徴とするブロードキャストフレームの復号方法。
【請求項１２】
自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末におけるブロー

ドキャストフレームの暗号化方法であって、
ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、
暗号化された前記ブロードキャストフレームを送信する手順と
を具備することを特徴とするブロードキャストフレームの暗号化方法。
【請求項１３】
第１の端末と第２の端末との間のユニキャスト暗号鍵により暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、
前記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、
第２の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により暗号化する手順と、
前記暗号化された第２の端末の端末識別子およびブロードキャスト暗号鍵を前記第１の端末に送信する手順と
を具備することを特徴とする前記第２の端末におけるブロードキャスト暗号鍵配布方法。
【請求項１４】
第１の端末と第２の端末との間のユニキャスト暗号鍵により暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、
前記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、
前記第１の端末の端末識別子およびブロードキャスト暗号鍵を第２の端末のブロードキャスト暗号鍵により暗号化する手順と、
前記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を第３の端末に送信する手順と
を具備することを特徴とする前記第２の端末におけるブロードキャスト暗号鍵配布方法。
【請求項１５】
他の端末の端末識別子と前記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末において、
受信したブロードキャストフレームの始点端末識別子を含む前記暗号鍵管理リストを前記暗号鍵管理リストテーブルから検索して対応する前記ブロードキャスト暗号鍵を抽出する手順と、
抽出された前記ブロードキャスト暗号鍵により前記ブロードキャストフレームのペイロードを復号する手順と
を端末に実行させることを特徴とするプログラム。
【請求項１６】
自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末において、
ブロードキャストフレームのペイロードを前記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、
暗号化された前記ブロードキャストフレームを送信する手順と
を端末に実行させることを特徴とするプログラム。
【請求項１７】
第１の端末と第２の端末との間のユニキャスト暗号鍵により暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、
前記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、
第２の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により暗号化する手順と、
前記暗号化された第２の端末の端末識別子およびブロードキャスト暗号鍵を前記第１の端末に送信する手順と
を前記第２の端末に実行させることを特徴とするプログラム。

【請求項１８】
第１の端末と第２の端末との間のユニキャスト暗号鍵により暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、
前記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を前記ユニキャスト暗号鍵により復号する手順と、
前記第１の端末の端末識別子およびブロードキャスト暗号鍵を第２の端末のブロードキャスト暗号鍵により暗号化する手順と、
前記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を第３の端末に送信する手順と
を前記第２の端末に実行させることを特徴とするプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、無線アドホック通信システムに関し、特に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化して秘匿性を保つ無線アドホック通信システム、当該システムにおける端末、および、これらにおける処理方法ならびに当該方法をコンピュータ（端末）に実行させるプログラムに関する。
【０００２】
【従来の技術】
電子機器の小型化、高性能化が進み、簡単に持ち運び利用することが可能となったことから、必要になったその場で端末をネットワークに接続し、通信を可能とする環境が求められている。その一つとして、必要に応じて一時的に構築されるネットワーク、すなわち無線アドホックネットワーク技術の開発が進められている。この無線アドホックネットワークでは、特定のアクセスポイントを設けることなく、各端末（例えば、コンピュータ、携帯情報端末（ＰＤＡ：Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｃｅ）、携帯電話等）が自律分散して相互に接続される。このような無線アドホック通信システムにおいても、重要な情報の送受やプライベートなやりとりが第三者に傍受されることなく安心して行えるように暗号化等による秘匿性が求められている。
【０００３】
一般に、通信内容を暗号化するためには、暗号化および復号化の両者で同じ共通鍵を用いる共通鍵暗号方式と、暗号化には公開鍵を用いて復号化には秘密鍵を用いる公開鍵暗号方式の二つの暗号方式が用いられている。共通鍵暗号方式は、暗号化および復号化を高速に行うことが可能であるが、通信の当事者同士が事前に何らかの方法で共通鍵を共有しておく必要がある。一方、公開鍵暗号方式は、共通鍵暗号方式に比べると処理が遅いが、当事者間同士で鍵を共有する必要がないという利点がある。そこで、共通鍵暗号の高速性と公開鍵暗号の利便性を組み合わせるハイブリッド方式が一般的に用いられている。具体的には、公開鍵暗号方式を用いて共通鍵を暗号化して送信し、当事者間で共有した共通鍵で実際の通信データの暗号化を行うことになる。
【０００４】
この通信データの暗号化のための共通鍵は、用途に応じてユニキャスト暗号鍵とブロードキャスト暗号鍵とに分類される。ユニキャスト暗号鍵は、二つの端末間のユニキャスト通信において用いられるものであり、その二つの端末以外には知らされない共通鍵である。一方、ブロードキャスト暗号鍵は、ある端末からのブロードキャスト通信を各端末において復号化するために用いられるものであり、ブロードキャスト通信にかかわる全ての端末間で共有される共通鍵である。従って、ブロードキャスト暗号鍵は、ユニキャスト暗号鍵と比較して一般に、秘匿性を維持することが難しくなる。
【０００５】
そのため、従来の通信システムにおいては、ブロードキャスト暗号鍵はネットワーク上の特定の装置において一元管理され、ブロードキャストグループにおけるブロードキャスト暗号鍵の秘匿性が図られている。例えば、モバイルデバイスに対してネットワーク所有者

であるワイヤレスキャリアがブロードキャスト暗号鍵を予め設定しておくことにより、ブロードキャストメッセージを暗号化する技術が提案されている（例えば、特許文献１参照。）。

【０００６】

【特許文献１】

特表２００２－５０１３３４号公報（図１）

【０００７】

【発明が解決しようとする課題】

従来の通信システムではブロードキャスト暗号鍵は一元管理されているが、無線アドホック通信システムにおいては端末は常に移動し、端末の参入および脱退が頻繁に行われ、ブロードキャストグループを構成する端末を固定することができない。また、無線媒体の性質上、そのような一元管理を行う装置への通信路が常に確保されているとは限らないため、一元管理に適さない。

【０００８】

そこで、本発明の目的は、無線アドホック通信システムにおいて、ブロードキャスト暗号鍵の管理を自律分散して行うことにある。特に、本発明は、ネットワークを構成する全ての無線端末が管理情報（例えば、ビーコン等）を送信する無線ネットワークにおいて有用である。

【０００９】

【課題を解決するための手段】

上記課題を解決するために本発明の請求項１記載の無線アドホック通信システムは、複数の端末により構成される無線アドホック通信システムであって、ブロードキャストフレームのペイロードを暗号化して当該ブロードキャストフレームを送信する第１の端末と、上記ブロードキャストフレームを受信して当該ブロードキャストフレームのペイロードを復号する第２の端末とを具備し、上記第１の端末は上記第１の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを暗号化し、上記第２の端末は上記第１の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する。これにより、端末毎にブロードキャスト暗号鍵を自律分散して設定可能にするという作用をもたらす。

【００１０】

また、本発明の請求項２記載の無線アドホック通信システムは、請求項１記載の無線アドホック通信システムにおいて、上記第２の端末が、上記第１の端末の端末識別子と上記第１の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも有する暗号鍵管理リストテーブルと、受信したブロードキャストフレームの始点端末識別子に含まれる上記第１の端末の端末識別子により上記暗号鍵管理リストテーブルを検索して対応する上記第１の端末のブロードキャスト暗号鍵を抽出する手段と、抽出された上記第１の端末のブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手段とを備える。これにより、ブロードキャストフレームの始点端末識別子に応じてブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

【００１１】

また、本発明の請求項３記載の無線アドホック通信システムは、請求項８記載の無線アドホック通信システムにおいて、上記第１の端末が、上記第１の端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持された上記第１の端末のブロードキャスト暗号鍵により暗号化する手段と、暗号化された上記ブロードキャストフレームを送信する手段とを備える。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

【００１２】

また、本発明の請求項４記載の端末は、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リス

トテーブルと、受信したブロードキャストフレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手段と、抽出された上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手段とを具備する。これにより、端末毎にブロードキャスト暗号鍵を自律分散して設定しておいて、ブロードキャストフレームの始点端末識別子に応じてブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

【００１３】

また、本発明の請求項５記載の端末は、他の端末の端末識別子に対応して上記他の端末との間のユニキャスト暗号鍵および上記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、受信したフレームの終点端末識別子がブロードキャストアドレスであれば当該フレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を暗号鍵として抽出し、上記受信したフレームの終点端末識別子がブロードキャストアドレス以外であれば当該フレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵を上記暗号鍵として抽出する手段と、抽出された上記暗号鍵により上記フレームのペイロードを復号する手段とを具備する。これにより、受信したフレームの終点端末識別子に応じてブロードキャスト暗号鍵およびユニキャスト暗号鍵を使い分けることを可能にするという作用をもたらす。

【００１４】

また、本発明の請求項６記載の端末は、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、ブロードキャストフレームのペイロードを上記ブロードキャスト暗号鍵により暗号化する手段と、暗号化された上記ブロードキャストフレームを送信する手段とを具備する。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

【００１５】

また、本発明の請求項７記載の端末は、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルと、他の端末の端末識別子に対応して上記他の端末との間のユニキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、送信しようとするフレームがブロードキャストフレームであれば上記生成鍵テーブルの上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを暗号化し、送信しようとする上記フレームがユニキャストフレームであれば当該ユニキャストフレームの終点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵により上記ユニキャストフレームのペイロードを暗号化する手段と、暗号化された上記フレームを送信する手段とを具備する。これにより、送信するフレームの終点端末識別子に応じてブロードキャスト暗号鍵およびユニキャスト暗号鍵を使い分けることを可能にするという作用をもたらす。

【００１６】

また、本発明の請求項８記載の端末は、送信先端末のユニキャスト暗号鍵により自端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、上記暗号化された自端末の端末識別子およびブロードキャスト暗号鍵を上記送信先端末に送信する手段とを具備する。これにより、自端末のブロードキャスト暗号鍵を自端末の管理の下で配布するという作用をもたらす。

【００１７】

また、本発明の請求項９記載の端末は、他の端末の端末識別子に対応して上記他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルと、送信先端末のユニキャスト暗号鍵により上記暗号鍵管理リストを暗号化する手段と、上記暗号化された暗号鍵管理リストを上記送信先端末に送信する手段とを具備する。これにより、自端末の管理するブロードキャスト暗号鍵群（暗号鍵管理リスト

）を自律分散して配布するという作用をもたらす。

【００１８】

また、本発明の請求項１０記載の端末は、他の端末から当該他の端末の端末識別子およびブロードキャスト暗号鍵を受信する手段と、自端末のブロードキャスト暗号鍵により上記他の端末の端末識別子およびブロードキャスト暗号鍵を暗号化する手段と、上記暗号化された他の端末の端末識別子およびブロードキャスト暗号鍵をブロードキャスト配布する手段とを具備する。これにより、他の端末のブロードキャスト暗号鍵を自律分散して配布するという作用をもたらす。

【００１９】

また、本発明の請求項１１記載のブロードキャストフレームの復号方法は、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末におけるブロードキャストフレームの復号方法であって、受信したブロードキャストフレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手順と、抽出された上記ブロードキャスト暗号鍵により上記ブロードキャストフレームのペイロードを復号する手順とを具備する。これにより、ブロードキャストフレームの始点端末識別子に応じて復号化に使用するブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

【００２０】

また、本発明の請求項１２記載のブロードキャストフレームの暗号化方法は、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末におけるブロードキャストフレームの暗号化方法であって、ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、暗号化された上記ブロードキャストフレームを送信する手順とを具備する。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

【００２１】

また、本発明の請求項１３記載のブロードキャスト暗号鍵配布方法は、第１の端末と第２の端末との間のユニキャスト暗号鍵により暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、第２の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により暗号化する手順と、上記暗号化された第２の端末の端末識別子およびブロードキャスト暗号鍵を上記第１の端末に送信する手順とを具備する。これにより、第１の端末と第２の端末との間で互いのブロードキャスト暗号鍵を配布するという作用をもたらす。

【００２２】

また、本発明の請求項１４記載のブロードキャスト暗号鍵配布方法は、第１の端末と第２の端末との間のユニキャスト暗号鍵により暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、上記第１の端末の端末識別子およびブロードキャスト暗号鍵を第２の端末のブロードキャスト暗号鍵により暗号化する手順と、上記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を第３の端末に送信する手順とを具備する。これにより、第１の端末のブロードキャスト暗号鍵を第３の端末にブロードキャスト配布するという作用をもたらす。

【００２３】

また、本発明の請求項１５記載のプログラムは、他の端末の端末識別子と上記他の端末のブロードキャスト暗号鍵との組からなる暗号鍵管理リストを少なくとも一つ有する暗号鍵管理リストテーブルを備える端末において、受信したブロードキャストフレームの始点端末識別子を含む上記暗号鍵管理リストを上記暗号鍵管理リストテーブルから検索して対応する上記ブロードキャスト暗号鍵を抽出する手順と、抽出された上記ブロードキャスト暗

号鍵により上記ブロードキャストフレームのペイロードを復号する手順とを端末に実行させるものである。これにより、ブロードキャストフレームの始点端末識別子に応じて復号化に使用するブロードキャスト暗号鍵を選択可能にするという作用をもたらす。

【００２４】

また、本発明の請求項１６記載のプログラムは、自端末のブロードキャスト暗号鍵を保持する生成鍵テーブルを備える端末において、ブロードキャストフレームのペイロードを上記生成鍵テーブルに保持されたブロードキャスト暗号鍵により暗号化する手順と、暗号化された上記ブロードキャストフレームを送信する手順とを端末に実行させるものである。これにより、ブロードキャスト通信を行う際に端末毎に異なるブロードキャスト暗号鍵によりブロードキャストフレームを暗号化することを可能にするという作用をもたらす。

【００２５】

また、本発明の請求項１７記載のプログラムは、第１の端末と第２の端末との間のユニキャスト暗号鍵により暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、第２の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により暗号化する手順と、上記暗号化された第２の端末の端末識別子およびブロードキャスト暗号鍵を上記第１の端末に送信する手順とを上記第２の端末に実行させるものである。これにより、第１の端末と第２の端末との間で互いのブロードキャスト暗号鍵を配布するという作用をもたらす。

【００２６】

また、本発明の請求項１８記載のプログラムは、第１の端末と第２の端末との間のユニキャスト暗号鍵により暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を受信する手順と、上記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を上記ユニキャスト暗号鍵により復号する手順と、上記第１の端末の端末識別子およびブロードキャスト暗号鍵を第２の端末のブロードキャスト暗号鍵により暗号化する手順と、上記暗号化された第１の端末の端末識別子およびブロードキャスト暗号鍵を第３の端末に送信する手順とを上記第２の端末に実行させるものである。これにより、第１の端末のブロードキャスト暗号鍵を第３の端末にブロードキャスト配布するという作用をもたらす。

【００２７】

【発明の実施の形態】

次に本発明の実施の形態について図面を参照して詳細に説明する。

【００２８】

図１は、本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末３００の構成例を示す図である。無線端末３００は、通信処理部３２０と、制御部３３０と、表示部３４０と、操作部３５０と、スピーカ３６０と、マイク３７０と、メモリ６００とを備え、これらの間をバス３８０が接続する構成となっている。また、通信処理部３２０にはアンテナ３１０が接続されている。通信処理部３２０は、アンテナ３１０を介して受信した信号からネットワークインターフェース層（データリンク層）のフレームを構成する。また、通信処理部３２０は、ネットワークインターフェース層のフレームをアンテナ３１０を介して送信する。

【００２９】

制御部３３０は、無線端末３００全体を制御する。例えば、通信処理部３２０により構成されたフレームを参照して所定の処理を行う。また、制御部３３０は、タイマ３３５を有し、所定のイベントからの経過時間を計時する。表示部３４０は、所定の情報を表示するものであり、例えば、液晶ディスプレイ等が用いられ得る。操作部３５０は、無線端末３００に対して外部から操作指示を行うためのものであり、例えば、キーボードやボタンスイッチ等が用いられ得る。スピーカ３６０は、音声を出力するものであり、無線端末３００の利用者に対して注意を喚起したり他の端末と音声情報のやりとりを行うために用いられる。マイク３７０は、無線端末３００に対して外部から音声入力を行うものであり、他

の端末と音声情報のやりとりを行ったり操作指示を行うために用いられる。

【００３０】

メモリ６００は、属性証明書の発行端末に関する情報を保持する属性証明書発行端末リストテーブル６１０と、無線端末３００自身のアクセス権限を示す属性証明書を保持する属性証明書テーブル６２０と、無線端末３００自身の生成鍵に関する情報として自端末の公開鍵と秘密鍵と公開鍵証明書とブロードキャスト暗号鍵とを保持する生成鍵テーブル６５０と、他の端末との間のユニキャスト暗号鍵および他の端末のブロードキャスト暗号鍵を保持する暗号鍵管理リストテーブル６６０とを格納する。

【００３１】

図２は、本発明の実施の形態における属性証明書発行端末リストテーブル６１０の構成例である。この属性証明書発行端末リストテーブル６１０は、過去に属性証明書を発行した実績のある端末に関する情報を保持するものであり、属性証明書発行端末の端末識別子６１１のそれぞれに対応して、公開鍵証明書６１２を保持している。端末識別子６１１は、ネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）におけるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス等を用いることができる。公開鍵証明書６１２は、対応する端末識別子６１１により識別される端末の公開鍵証明書である。公開鍵証明書とは、証明書所有者（サブジェクト）の本人性を証明するものであり、証明書所有者の公開鍵を含む。この公開鍵証明書は証明書発行者たる認証局（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）によって署名される。

【００３２】

図３は、属性証明書発行端末リストテーブル６１０に保持される公開鍵証明書６１２のフォーマット７１０を示す図である。この公開鍵証明書のフォーマット７１０は、大きく分けて、署名前証明書７１１と、署名アルゴリズム７１８と、署名７１９とから構成される。署名前証明書７１１は、シリアル番号７１２と、発行者７１４と、有効期限７１５と、所有者７１６と、所有者７１６と、所有者公開鍵７１７とを含む。

【００３３】

シリアル番号７１２は、公開鍵証明書のシリアル番号であり、認証局によって採番される。発行者７１４は、公開鍵証明書の発行者たる認証局の名前である。この発行者７１４とシリアル番号７１２とにより公開鍵証明書は一意に識別される。有効期限７１５は、公開鍵証明書の有効期限である。所有者７１６は、公開鍵証明書の所有者の名前である。所有者公開鍵７１７は、所有者７１６の公開鍵である。

【００３４】

署名７１９は公開鍵証明書に対する認証局による署名であり、署名アルゴリズム７１８はこの署名７１９のために使用された署名アルゴリズムである。署名アルゴリズムは、メッセージダイジェストアルゴリズムと公開鍵暗号アルゴリズムの２つにより構成される。メッセージダイジェストアルゴリズムは、ハッシュ関数（要約関数）の一つであり、署名前証明書７１１のメッセージダイジェストを作成するためのアルゴリズムである。ここで、メッセージダイジェストとは、入力データ（署名前証明書７１１）を固定長のビット列に圧縮したものであり、拇印や指紋（フィンガープリント）等とも呼ばれる。メッセージダイジェストアルゴリズムとしては、ＳＨＡ－１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ１）、ＭＤ２（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　＃２）、ＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　＃５）等が知られている。公開鍵暗号アルゴリズムは、メッセージダイジェストアルゴリズムにより得られたメッセージダイジェストを認証局の秘密鍵により暗号化するためのアルゴリズムである。この公開鍵暗号アルゴリズムとしては、素因数分解問題に基づくＲＳＡや離散対数問題に基づくＤＳＡ等が知られている。このように、署名前証明書７１１のメッセージダイジェストを認証局の秘密鍵により暗号化したものが署名７１９となる。

【００３５】

従って、この公開鍵証明書の署名７１９を認証局の公開鍵により復号することによってメ

ッセージダイジェストが得られる。公開鍵証明書の利用者は、署名前証明書７１１のメッセージダイジェストを自身で作成し、それを認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、署名前証明書７１１の内容が改ざんされていないことを検証できる。

【００３６】

図４は、属性証明書テーブル６２０に保持される属性証明書のフォーマット７２０を示す図である。この属性証明書は、大きく分けて、属性証明情報７２１と、署名アルゴリズム７２８と、署名７２９とから構成される。属性証明情報７２１は、所有者公開鍵証明書識別子７２３と、発行者７２４と、シリアル番号７２２と、有効期限７２５とを含む。

【００３７】

所有者公開鍵証明書識別子７２３は、属性証明書の所有者の公開鍵証明書を識別するためのものである。具体的には、公開鍵証明書７１０（図３）の発行者７１４とシリアル番号７１２とにより識別する。発行者７２４は、属性証明書の発行者たる属性認証局（ＡＡ：Ａｔｔｒｉｂｕｔｅ ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ）の名称である。シリアル番号７２２は、属性証明書のシリアル番号であり、属性証明書の発行者たる属性認証局によって採番される。このシリアル番号７２２と発行者７２４とにより属性証明書は一意に識別される。有効期限７２５は、属性証明書の有効期限である。

【００３８】

署名７２９は属性証明書に対する属性認証局による署名であり、署名アルゴリズム７２８はこの署名７２９のために使用された署名アルゴリズムである。署名アルゴリズムの内容については、前述の公開鍵証明書の署名アルゴリズム７１８と同様であり、属性証明情報７２１のメッセージダイジェストを属性認証局の秘密鍵により暗号化したものが署名７２９となる。

【００３９】

従って、この属性証明書の署名７２９を属性認証局の公開鍵により復号することによってメッセージダイジェストが得られる。属性証明書の利用者は、属性証明情報７２１のメッセージダイジェストを自身で作成し、それを属性認証局の公開鍵により復号されたメッセージダイジェストと比較することにより、属性証明情報７２１の内容が改ざんされていないことを検証できる。

【００４０】

なお、本明細書では、端末権限認証証明書の一例として属性証明書について説明するが、例えば、ＸＭＬ言語等により端末権限を記述しておき、権限を有する機関がそれに署名を付することにより作成されたようなものであっても本発明における端末権限認証証明書として機能し得る。

【００４１】

図５は、本発明の実施の形態における暗号鍵管理リストテーブル６６０の構成例である。この暗号鍵管理リストテーブル６６０は、復号化に用いられるブロードキャスト鍵および暗号化ならびに復号化に用いられるユニキャスト鍵を保持するものであり、他の端末の端末識別子６６１に対応して当該他の端末との間のユニキャスト暗号鍵６６２および当該他の端末のブロードキャスト暗号鍵６６３を保持する暗号鍵管理リストを少なくとも一つ有する。

【００４２】

端末識別子６６１は、上述の通り他の端末を一意に識別するものであり、一例としてＭＡＣアドレス等を用いることができる。ユニキャスト暗号鍵６６２は、対応する端末識別子６６１を有する端末との間のユニキャスト通信のために定められた共通鍵である。このユニキャスト暗号鍵６６２を表すために、例えば、端末Ａと端末Ｂとの間で使用されるユニキャスト暗号鍵を「ＵＫ＿ＡＢ」等と表記する。また、ブロードキャスト暗号鍵６６３は、対応する端末識別子６６１を有する端末がブロードキャスト通信を行うために定められた共通鍵である。このブロードキャスト暗号鍵６６３を表すために、例えば、端末Ｂからのブロードキャスト通信において使用されるブロードキャスト暗号鍵を「ＢＫ＿Ｂ」等と

表記する。

【００４３】

なお、これらユニキャスト暗号鍵およびブロードキャスト暗号鍵に用いられる共通鍵アルゴリズムとしては、５６ビットの鍵の長さを有するＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）、１２８ビット、１９２ビットおよび２５６ビットの３通りの鍵の長さを有するＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）等が知られている。

【００４４】

図６は、本発明の実施の形態におけるブロードキャスト暗号鍵およびユニキャスト暗号鍵の機能を示す図である。ブロードキャスト暗号鍵は、ブロードキャスト通信を行う各端末毎に定められるものであり、ブロードキャスト送信端末における暗号化およびブロードキャスト受信端末における復号化の両者で共通に用いられる共通鍵である。例えば、端末Ａのブロードキャスト暗号鍵（ＢＫ＿Ａ）は、端末Ａがブロードキャスト通信を送信する際の暗号化に使用され、端末Ａ以外の端末が端末Ａからのブロードキャスト通信を受信する際の復号化に使用される。

【００４５】

一方、ユニキャスト暗号鍵は、端末対毎に定められるものであり、端末対における通信の暗号化および復号化の両者で共通に用いられる共通鍵である。例えば、端末Ａと端末Ｂの間のユニキャスト暗号鍵（ＵＫ＿ＡＢ）は、端末Ａが端末Ｂにユニキャスト通信を送信する際の暗号化および端末Ｂが端末Ａからのユニキャスト通信を受信する際の復号化に使用されるだけでなく、端末Ｂが端末Ａにユニキャスト通信を送信する際の暗号化および端末Ａが端末Ｂからのユニキャスト通信を受信する際の復号化にも使用される。

【００４６】

図７は、本発明の実施の形態における経路テーブル６８０の構成例である。この経路テーブル６８０は、終点端末にフレームを到達させるための転送先端末に関する情報を保持するものであり、終点端末の端末識別子６８１に対応してフレームの転送先端末の端末識別子６８２および有効時間６８３を保持する経路リストを少なくとも一つ有する。

【００４７】

終点端末識別子６８１および転送先端末識別子６８２における端末識別子は、上述の通り他の端末を一意に識別するものである。ある端末に最終的にフレームを配送するために、次にどの端末にフレームを転送すべきであるかを示している。

【００４８】

無線アドホック通信システムにおいては、ネットワーク構成が時々刻々と変化する可能性がある。従って、経路テーブル６８０に保持される情報も古くなる可能性がある。そこで、有効時間６８３によって、対応する情報の鮮度を管理する。例えば、情報更新時もしくは情報更新からの経過時間を有効時間６８３に記録していくことにより、所定時間以上経過した情報を削除もしくは更新することが考えられる。これらの時間を計時するために制御部３３０のタイマ３３５が使用される。

【００４９】

図８は、本発明の実施の形態におけるブロードキャスト通信およびユニキャスト通信に用いられるフレーム構成を示す図である。フレーム８００は、ヘッダ部８０１と、ペイロード部８０２とから構成される。また、ヘッダ部８０１は、始点端末識別子８０３と、終点端末識別子８０４と、送信端末識別子８０５と、受信端末識別子８０６と、フレーム種別８０７と、属性証明書の有無８０８とを含む。始点端末識別子８０３は、このフレームを最初に発信した端末の端末識別子である。なお、端末識別子は、前述のようにネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネット（登録商標）におけるＭＡＣアドレス等を用いることができる。終点端末識別子８０４は、このフレームの最終宛先の端末の端末識別子である。

【００５０】

送信端末識別子８０５および受信端末識別子８０６は、フレームを中継する際に用いられ

る。無線アドホック通信システムにおいては、ネットワーク内の全ての端末が直接通信できるとは限らず、電波の届かない端末へフレームを送信したい場合には他の端末を介してマルチホップにより通信経路を確立しなければならない。この場合にフレームの送受信を行う端末間で使用されるのが送信端末識別子８０５および受信端末識別子８０６である。フレーム種別８０７は、フレームの種別を示すものである。

【００５１】

ペイロード部８０２には通信の内容であるデータ８０９が格納される。このペイロード部８０２が、ユニキャスト暗号鍵およびブロードキャスト暗号鍵による暗号化および復号化の対象となる。

【００５２】

次に本発明の実施の形態における無線アドホック通信システムの動作について図面を参照して説明する。本発明の実施の形態では、端末がネットワーク資源に接続する際に端末間で属性証明書を用いて相互認証（図９）を行い、互いの認証に成功した後にセッション鍵の配布、ユニキャスト暗号鍵の生成、および、ブロードキャスト暗号鍵の配布を行う（図１３）。これら図９および図１３における各処理は、無線端末３００における制御部３３０により実現される。

なお、相互認証に用いられる属性証明書は、予め適切に発行されて、各端末の属性証明書テーブル６２０（図１）に保持されていることを前提とする。また、属性証明書の検証に必要な属性証明書発行端末の公開鍵は、各端末の属性証明書発行端末リストテーブル６１０の公開鍵証明書６１２（図２）に予め設定されていることを前提とする。

【００５３】

図９は、本発明の実施の形態における相互認証の手順を示す図である。本発明の実施の形態における無線アドホック通信システムでは、各端末は定期的にビーコンを送信し、他の端末に対して自己の存在を知らせる。以下では、端末Ｂのビーコンをトリガーとして端末Ａが認証要求を行うものと仮定するが、最終的に相互に認証が行われればよく、何れの端末のビーコンをトリガーとしてもよい。

【００５４】

まず、端末Ｂが、ビーコン２１１１を送信しているものとする（２１１）。このビーコン２１１１のフレーム構成は図１０の通りである。ビーコンフレーム８１０は、図８で説明したフレーム８００の構成に基づくものであり、ヘッダ部８１１およびペイロード部８１２に分けられる点も同様である。各端末識別子８１３乃至８１６も図８の各端末識別子８０３乃至８０６と同様である。ビーコンフレーム８１０では、終点端末識別子８１４にはブロードキャストアドレス（例えば、全てのビットに１）が設定される。フレーム種別８１７は、ここでは、ビーコンフレームであることを示す。属性証明書の有無８１８は、ネットワーク資源にアクセスする権限を示す属性証明書をビーコンフレームの送信元端末が有しているか否かを示すものである。属性証明書を有していない旨をこの属性証明書の有無８１８が示している場合には、相互認証を進めることはできず、例えば、属性証明書の取得を促す等の処置を採ることが考えられる。

【００５５】

端末Ａは、端末Ｂから送信されたビーコン２１１１を受信すると（１１１）、ビーコンフレーム８１０の属性証明書の有無８１８をチェックする。端末Ｂが属性証明書を有していると判断すると、端末Ａは端末Ｂに対して端末Ａを認証するよう認証要求メッセージ１１２２を送信する（１１２）。この認証要求メッセージ１１２２のフレーム構成は図１１の通りである。認証要求フレーム８７０は、図８で説明したフレーム８００の構成に基づくものであり、ヘッダ部８７１およびペイロード部８７２に分けられる点も同様である。各端末識別子８７３乃至８７６も図８の各端末識別子８０３乃至８０６と同様である。フレーム種別８７７は、ここでは、認証要求フレームであることを示す。

【００５６】

また、この認証要求フレーム８７０では、ペイロード部８７２のデータ８７９として、送信元である端末Ａの公開鍵証明書８７９１および属性証明書８７９２が含まれる。端末Ａ

の公開鍵証明書８７９１は端末Ａの生成鍵テーブル６５０に予め格納されたものであり、端末Ａの属性証明書８７９２は端末Ａの属性証明書テーブル６２０に予め格納されたものである。

【００５７】

端末Ｂは、端末Ａから送信された認証要求メッセージ１１２２を受信すると、その内容から端末Ａを認証する（２１２）。具体的には、属性証明書発行端末リストテーブル６１０の公開鍵証明書６１２（図２）から属性認証局の公開鍵を抽出して、この公開鍵によって認証要求メッセージ１１２２に含まれる属性証明書８７９２の署名７２９（図４）を復号することにより署名時のメッセージダイジェストを得る。そして、属性証明書８７９２の属性証明情報７２１（図４）のメッセージダイジェストを新たに生成する。この新たに生成されたメッセージダイジェストが署名時のメッセージダイジェストと一致していることを確認する。もしこれらが一致しないとすれば、属性証明書は署名後に改ざんされた可能性があり、属性証明書の検証は失敗となる。両者が一致している場合には、さらに認証要求メッセージ１１２２に含まれる属性証明書８７９２の所有者公開鍵証明書識別子７２３（図４）が、認証要求メッセージ１１２２に含まれる公開鍵証明書８７９１の発行者７１４およびシリアル番号７１２（図３）に一致することを確認する。これが一致すれば、公開鍵証明書の所有者である端末Ａは属性証明書の所有者であることが確認できる。もしこれらが一致しなければ、属性証明書の所有者は端末Ａではなく、属性証明書の検証は失敗となる。

【００５８】

端末Ａの認証（２１２）に成功すると、端末Ｂは端末Ａの認証に成功したことを通知する認証成功メッセージ２１３１を端末Ａに送信する（２１３）。この認証成功メッセージ２１３１の認証応答フレーム構成は図１２の通りである。認証応答フレーム８８０は、図８で説明したフレーム８００の構成に基づくものであり、ヘッダ部８８１およびペイロード部８８２に分けられる点も同様である。各端末識別子８８３乃至８８６も図８の各端末識別子８０３乃至８０６と同様である。認証成功メッセージ２１３１の場合、フレーム種別８８７は認証成功フレームとなる。この認証応答フレーム８８０では、さらに応答理由種別８８８を含むが、認証成功の場合は特に必要はない。

【００５９】

なお、端末Ａの属性証明書の検証（２１２）に失敗すると、端末Ｂは端末Ａの認証に成功したことを通知する認証失敗メッセージを端末Ａに送信することになる。この認証失敗メッセージの認証応答フレーム構成は図１２により説明した通りである。但し、認証失敗メッセージの場合、フレーム種別８８７は認証失敗フレームとなり、応答理由種別８８８には認証に失敗した理由として属性証明書のメッセージダイジェスト不一致、属性証明書失効等の事由がコード化されて示される。これら。認証成功メッセージ２１３１または認証失敗メッセージは端末Ａにおいて受信されて確認される（１１３）。

【００６０】

端末Ａの属性証明書の検証（２１２）に成功すると、さらに端末Ｂは端末Ａに対して端末Ｂを認証するよう認証要求メッセージ２１４１を送信する（２１４）。この認証要求メッセージ２１４１のフレーム構成は上述の図１１と同様であり、送信元である端末Ｂの公開鍵証明書８７９１および属性証明書８７９２が含まれる。

【００６１】

端末Ａは、端末Ｂから送信された認証要求メッセージ２１４１を受信すると、その内容から端末Ｂを認証する（１１４）。この認証の内容は、既に説明した端末Ｂにおける端末Ａの認証（２１２）と同様であり、属性証明書の検証、および、属性証明書の所有者の確認等を行う。

【００６２】

端末Ｂの認証（２１２）に成功すると、端末Ａは端末Ｂの認証に成功したことを通知する認証成功メッセージ１１５２を端末Ｂに送信する（１１５）。この認証成功メッセージ１１５２の認証応答フレーム構成は上述の図１２と同様である。また、端末Ｂの属性証明書

の検証（２１２）に失敗した場合には、端末Ａは端末Ｂの認証に成功したことを通知する認証失敗メッセージを端末Ｂに送信することになる。この認証失敗メッセージの認証応答フレーム構成も図１２により説明した通りである。これら認証成功メッセージ１１５２または認証失敗メッセージは端末Ｂにおいて受信されて確認される（２１５）。

【００６３】

このようにして、端末Ａおよび端末Ｂにおいて互いの端末の認証に成功すると相互認証は完了し、次に暗号鍵の配布を行う。

【００６４】

図１３は、本発明の実施の形態における暗号鍵配布の手順を示す図である。ここで、端末Ａ（１００）は新規にネットワークに参入しようとしている端末であり、端末Ｂ（２００）は既にネットワークに参入している属性証明書発行端末である。

【００６５】

まず、端末Ａは、端末Ｂとの間で通信を行うためのセッション鍵を生成する（１２１）。このセッション鍵は、端末Ａと端末Ｂとの間の共通鍵であり、乱数を用いて生成することができる。端末Ａは、このセッション鍵を端末Ｂの公開鍵により暗号化してセッション鍵配布メッセージ１２２２として端末Ｂに送信する（１２２）。このセッション鍵配布メッセージ１２２２のセッション鍵配布フレーム構成は図１４の通りである。セッション鍵配布フレーム８２０は、図８で説明したフレーム８００の構成に基づくものであり、ヘッダ部８２１およびペイロード部８２２に分けられる点も同様である。各端末識別子８２３乃至８２６も図８の各端末識別子８０３乃至８０６と同様である。フレーム種別８２７はセッション鍵配布フレームとなる。ペイロード部８２２のデータ８２９にはセッション鍵８２９１が含まれる。

【００６６】

なお、このセッション鍵配布フレームのペイロード部８２２は、ユニキャスト暗号鍵またはブロードキャスト暗号鍵による暗号化または復号化の対象とはならず、受信端末の公開鍵で暗号化され、受信端末の秘密鍵で復号化される。端末Ａは、相互認証の段階で端末Ｂの公開鍵証明書を受信しているため、その所有者公開鍵７１７（図３）により端末Ｂの公開鍵を得ることができる。

【００６７】

端末Ｂは、端末Ａから送信されたセッション鍵配布メッセージ１２２２を受信すると、セッション鍵８２９１を端末Ｂの秘密鍵により復号化する（２２２）。これにより、端末Ａおよび端末Ｂの間で同一のセッション鍵を共有したことになる。

【００６８】

その後、端末Ａおよび端末Ｂは、セッション鍵からユニキャスト暗号鍵（ＵＫ＿ＡＢ）を生成する（１２３、２２３）。このユニキャスト暗号鍵は、セッション鍵をそのまま利用してもよく、また、このセッション鍵を種（シード）としてハッシュ関数により新たにユニキャスト暗号鍵を生成するようにしてもよい。このようにして得られた端末Ａと端末Ｂとの間のユニキャスト暗号鍵（ＵＫ＿ＡＢ）は、両端末の暗号鍵管理リストテーブル６６０の対応するユニキャスト暗号鍵６６２（図５）に格納される。

【００６９】

次に、端末Ａは、予め生成していた端末Ａのブロードキャスト暗号鍵（ＢＫ＿Ａ）と端末Ａの端末識別子との対を端末Ｂとの間のユニキャスト暗号鍵（ＵＫ＿ＡＢ）により暗号化してブロードキャスト鍵配布メッセージ１２４２として端末Ｂに送信する（１２４）。このブロードキャスト鍵配布メッセージ１２４２のブロードキャスト鍵配布フレーム構成は図１５の通りである。ブロードキャスト鍵配布フレーム８３０は、図８で説明したフレーム８００の構成に基づくものであり、ヘッダ部８３１およびペイロード部８３２に分けられる点も同様である。各端末識別子８３３乃至８３６も図８の各端末識別子８０３乃至８０６と同様である。フレーム種別８３７はブロードキャスト鍵配布フレームとなる。ペイロード部８３２のデータ８３９には端末識別子８３９１とブロードキャスト暗号鍵８３９２との対が含まれる。端末Ａは、端末Ａのブロードキャスト暗号鍵（ＢＫ＿Ａ）８３９２

を生成鍵テーブル６５０に保持している。また、ブロードキャスト鍵配布メッセージ１２４２のペイロード部８３２の暗号化に用いるユニキャスト暗号鍵（ＵＫ＿ＡＢ）は暗号鍵管理リストテーブル６６０のユニキャスト暗号鍵６６２（図５）に保持している。

【００７０】

端末Ｂは、端末Ａからブロードキャスト鍵配布メッセージ１２４２を受信すると、ブロードキャスト鍵配布メッセージ１２４２のペイロード部８３２を端末Ａとの間のユニキャスト暗号鍵（ＵＫ＿ＡＢ）により復号化する（２２４）。これにより、端末Ａのブロードキャスト暗号鍵と端末識別子とを取得する。そして、この端末Ａのブロードキャスト暗号鍵を端末Ａの端末識別子と関連付けて、暗号鍵管理リストテーブル６６０のブロードキャスト暗号鍵６６３（図５）に格納する。

【００７１】

そして、端末Ｂは、端末Ａのブロードキャスト暗号鍵（ＢＫ＿Ａ）と端末Ａの端末識別子との対を端末Ｂのブロードキャスト暗号鍵（ＢＫ＿Ｂ）により暗号化してブロードキャスト鍵配布メッセージ２２４４として他の端末にブロードキャスト送信する（２２５）。このブロードキャスト鍵配布メッセージ２２４４のブロードキャスト鍵配布フレーム構成は上述した図１５の通りであるが、終点端末識別子８３４にはブロードキャストアドレス（例えば、全てのビットに１）が設定される。

【００７２】

端末Ｂからのブロードキャスト鍵配布メッセージ２２４４を受信した他の端末４００（例えば、端末Ｃや端末Ｄ）は、ブロードキャスト鍵配布メッセージ２２４４のペイロード部８３２を端末Ｂのブロードキャスト暗号鍵（ＢＫ＿Ｂ）により復号化する（４２５）。これにより、端末Ａのブロードキャスト暗号鍵と端末識別子とを取得する。そして、この端末Ａのブロードキャスト暗号鍵を端末Ａの端末識別子と関連付けて、暗号鍵管理リストテーブル６６０のブロードキャスト暗号鍵６６３（図５）に格納する。

【００７３】

さらに、端末Ｂは、端末Ｂの暗号鍵管理リストテーブル６６０に含まれるブロードキャスト暗号鍵６６３の全てをそれぞれの端末識別子６６１と対にして、端末Ａとの間のユニキャスト暗号鍵（ＵＫ＿ＡＢ）により暗号化してブロードキャスト鍵配布メッセージ２２６１として端末Ａに送信する（２２６）。このブロードキャスト鍵配布メッセージ２２６１のブロードキャスト鍵配布フレーム構成は上述した図１５の通りであるが、ペイロード部８３２には端末識別子８３９１およびブロードキャスト暗号鍵８３９２の対が複数含まれる可能性がある。

【００７４】

端末Ｂからブロードキャスト鍵配布メッセージ２２６１を受信した端末Ａは、ブロードキャスト鍵配布メッセージ２２６１のペイロード部８３２を端末Ｂとの間のユニキャスト暗号鍵（ＵＫ＿ＡＢ）により復号化する（１２６）。これにより、他の端末のブロードキャスト暗号鍵と端末識別子との対を取得する。そして、これら他の端末のブロードキャスト暗号鍵をそれぞれの端末の端末識別子と関連付けて、暗号鍵管理リストテーブル６６０のブロードキャスト暗号鍵６６３（図５）に格納する。

【００７５】

次に本発明の実施の形態における無線アドホック通信システムの各端末の暗号鍵選択アルゴリズムについて図面を参照して説明する。

【００７６】

図１６は、本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。図８のフレームにおいて、ブロードキャストフレームでは終点端末識別子８０４がブロードキャストアドレスであるので（ステップＳ９２１）、自端末のブロードキャスト暗号鍵によりペイロード部８０２を暗号化する（ステップＳ９２２）。一方、ブロードキャストフレームでなければ終点端末識別子８０４がブロードキャストアドレス以外であるので（ステップＳ９２１）、終点端末識別子８０４と一致する端末識別子６６１に対応するユニキャスト暗号鍵６６２を図５の暗号鍵管理リストテーブル６６０から抽出し

て、そのユニキャスト暗号鍵によりペイロード部８０２を暗号化する（ステップＳ９２３）。その後、暗号化されたフレームは下位層に送出される（ステップＳ９２４）。

【００７７】

図１７は、本発明の実施の形態におけるフレーム受信の際の暗号鍵選択アルゴリズムを示す図である。図８のフレームにおいて、終点端末識別子８０４がブロードキャストアドレスであれば（ステップＳ９１１）、始点端末識別子８０３と一致する端末識別子６６１に対応するブロードキャスト暗号鍵６６３を図５の暗号鍵管理リストテーブル６６０から抽出して、そのブロードキャスト暗号鍵によりペイロード部８０２を復号化する（ステップＳ９１２）。

【００７８】

終点端末識別子８０４がブロードキャストアドレスでなく（ステップＳ９１１）、自端末の端末識別子であれば（ステップＳ９１３）、始点端末識別子８０３と一致する端末識別子６６１に対応するユニキャスト暗号鍵６６２を図５の暗号鍵管理リストテーブル６６０から抽出して、そのユニキャスト暗号鍵によりペイロード部８０２を復号化する（ステップＳ９１４）。ステップＳ９１２またはステップＳ９１４において復号化されたフレームは上位層において処理される（ステップＳ９１５）。

【００７９】

一方、終点端末識別子８０４がブロードキャストアドレスでなく（ステップＳ９１１）、自端末の端末識別子でもなければ（ステップＳ９１３）、そのフレームは次点の端末へ転送される（ステップＳ９１６）。次点の端末は、フレーム８００の終点端末識別子８０４（図８）と一致する終点端末識別子６８１を経路テーブル６８０（図７）から抽出して、対応する転送先端末識別子６８２を参照することにより知ることができる。

【００８０】

このように、本発明の実施の形態によれば、暗号鍵管理リストテーブル６６０において端末識別子６６１に関連付けてブロードキャスト暗号鍵６６３を保持しておくことにより、端末毎に異なるブロードキャスト暗号鍵を適用することができる。これらブロードキャスト暗号鍵は、ブロードキャスト通信を行う端末自身が生成して図１３のシーケンス等を用いて配布するものである。従って、無線アドホック通信システムのようにブロードキャスト暗号鍵の一元管理が適さない環境において、ブロードキャスト暗号鍵の管理を各端末において自律分散して行うことができる。

【００８１】

なお、本発明の実施の形態は、ネットワークに属する全ての端末へ均等に配送するブロードキャストに関するものであるが、この「ブロードキャスト」の語句は厳格に解釈されるものではなく、「マルチキャスト」を含む広い概念として解釈されるべきものである。

【００８２】

また、ここでは本発明の実施の形態を例示したものであり、本発明はこれに限られず、本発明の要旨を逸脱しない範囲において種々の変形を施すことができる。

【００８３】

また、ここで説明した処理手順はこれら一連の手順を有する方法として捉えてもよく、これら一連の手順をコンピュータに実行させるためのプログラム乃至そのプログラムを記憶する記録媒体として捉えてもよい。

【００８４】

【発明の効果】

以上の説明で明らかなように、本発明によると、無線アドホック通信システムにおいて、ブロードキャスト暗号鍵の管理を自律分散して行うことができるという効果が得られる。

【図面の簡単な説明】

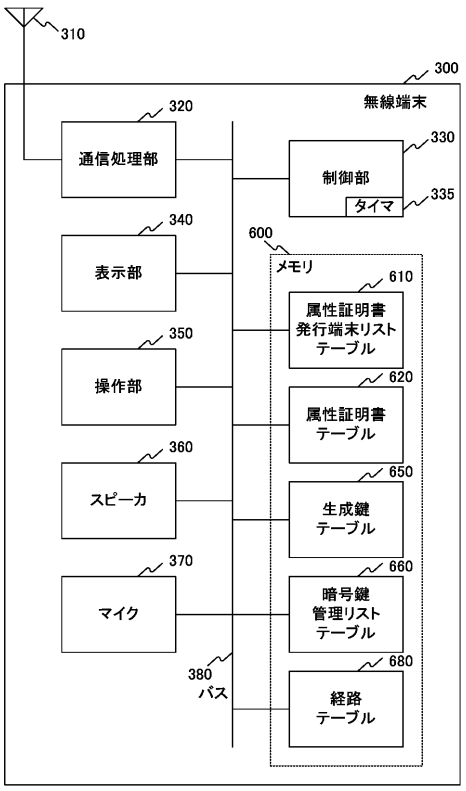
【図１】本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末３００の構成例を示す図である。

【図２】本発明の実施の形態における属性証明書発行端末リストテーブル６１０の構成例を示す図である。

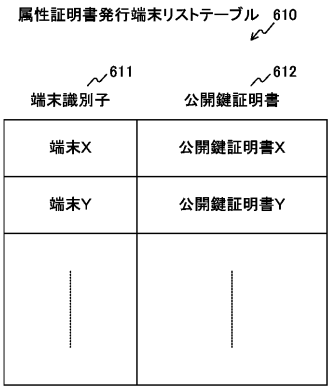
【図３】本発明の実施の形態における属性証明書発行端末リストテーブル６１０に保持される公開鍵証明書６１２のフォーマット７１０を示す図である。
【図４】本発明の実施の形態における属性証明書テーブル６２０に保持される属性証明書のフォーマット７２０を示す図である。
【図５】本発明の実施の形態における暗号鍵管理リストテーブル６６０の構成例を示す図である。
【図６】本発明の実施の形態におけるブロードキャスト暗号鍵およびユニキャスト暗号鍵の機能を示す図である。
【図７】本発明の実施の形態における経路テーブル６８０の構成例を示す図である。
【図８】本発明の実施の形態におけるブロードキャスト通信およびユニキャスト通信に用いられるフレーム構成を示す図である。
【図９】本発明の実施の形態における相互認証の手順を示す図である。
【図１０】本発明の実施の形態におけるビーコンフレーム８１０の構成例を示す図である。
【図１１】本発明の実施の形態における認証要求フレーム８７０の構成例を示す図である。
【図１２】本発明の実施の形態における認証応答フレーム８８０の構成例を示す図である。
【図１３】本発明の実施の形態における暗号鍵配布の手順を示す図である。
【図１４】本発明の実施の形態におけるセッション鍵配布フレーム８２０の構成例を示す図である。
【図１５】本発明の実施の形態におけるブロードキャスト鍵配布フレーム８３０の構成例を示す図である。
【図１６】本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。
【図１７】本発明の実施の形態におけるフレーム送信の際の暗号鍵選択アルゴリズムを示す図である。
【符号の説明】
３００　無線端末
３１０　アンテナ
３２０　通信処理部
３３０　制御部
３３５　タイマ
３４０　表示部
３５０　操作部
３６０　スピーカ
３７０　マイク
３８０　バス
４００　端末
６００　メモリ
６１０　属性証明書発行端末リストテーブル
６２０　属性証明書テーブル
６５０　生成鍵テーブル
６６０　暗号鍵管理リストテーブル
６８０　経路テーブル
７１０　公開鍵証明書
７２０　属性証明書
８００　フレーム
８１０　ビーコンフレーム
８２０　セッション鍵配布フレーム

８３０　ブロードキャスト鍵配布フレーム
８７０　認証要求フレーム
８８０　認証応答フレーム

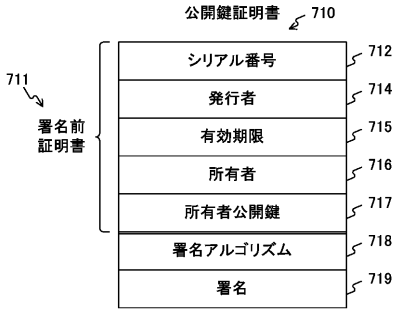
【図１】



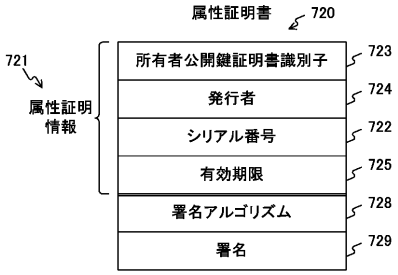
【図２】



【図３】



【図４】

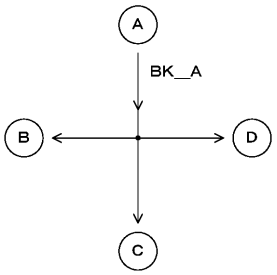


【図５】

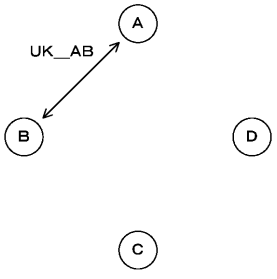
暗号鍵管理リストテーブル 660

661 端末識別子	662 ユニキャスト暗号鍵	663 ブロードキャスト暗号鍵
端末B	UK_AB	BK_B
端末C	UK_AC	BK_C
端末D	UK_AD	BK_D
⋮	⋮	⋮

【図６】



(a) ブロードキャスト鍵



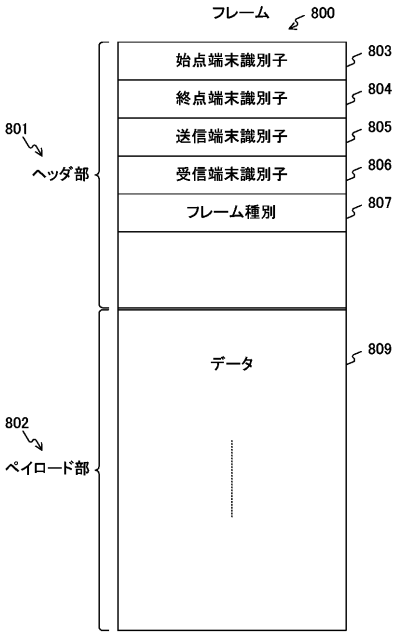
(b) ユニキャスト鍵

【図７】

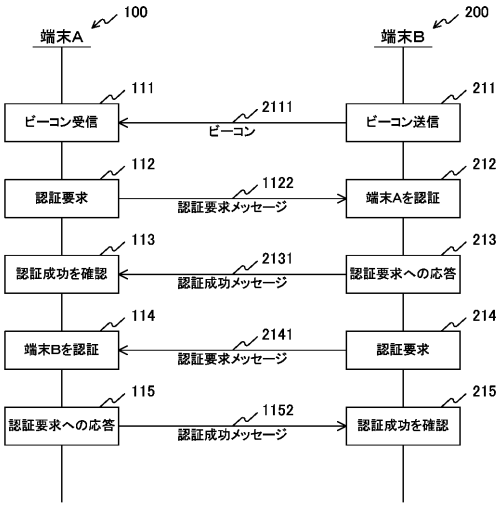
経路テーブル 680

681 終点端末識別子	682 転送先端末識別子	683 有効時間
端末B	端末B	1:30
端末C	端末B	0:50
端末D	端末B	0:30
⋮	⋮	⋮

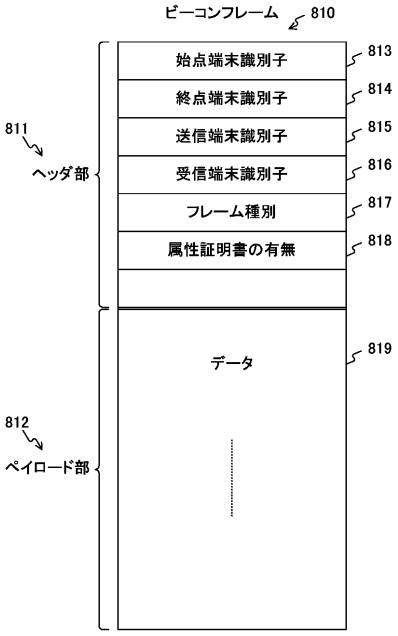
【図８】



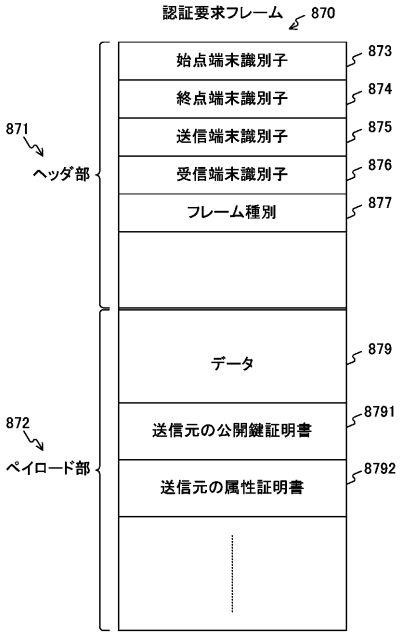
【図９】



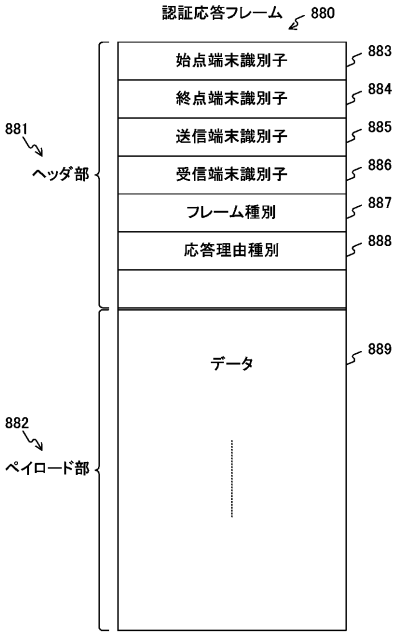
【図１０】



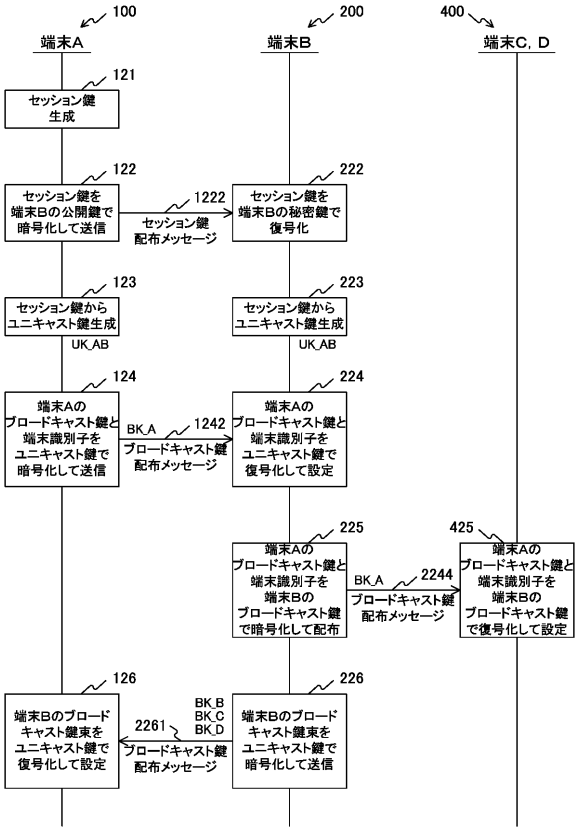
【図１１】



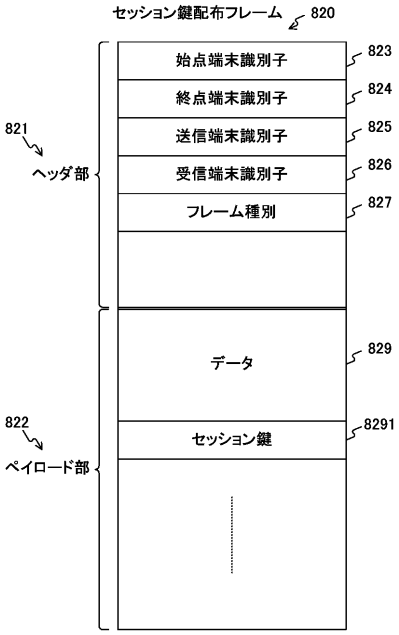
【図１２】



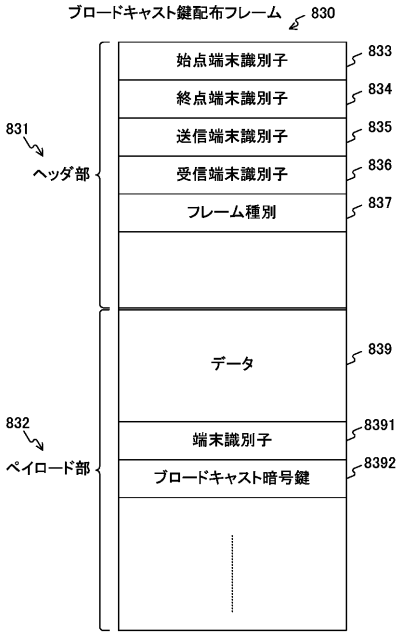
【図１３】



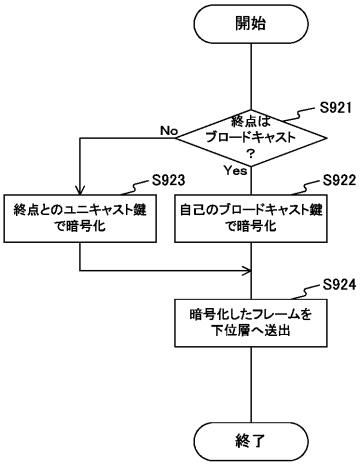
【図１４】



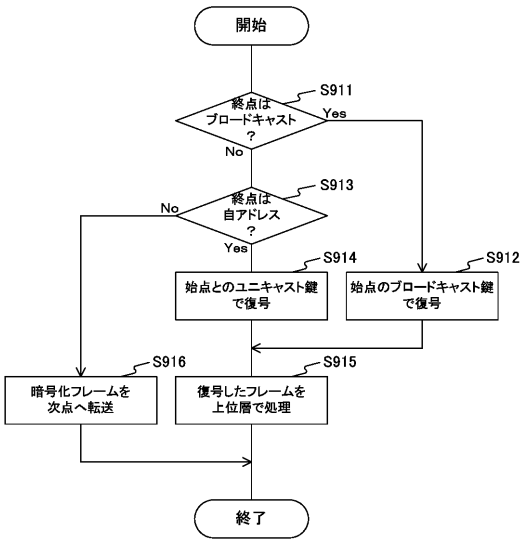
【図１５】


ブロードキャスト鍵配布フレーム
830
始点端末識別子
833
終点端末識別子
834
送信端末識別子
835
受信端末識別子
836
フレーム種別
837
831
ヘッダ部
データ
839
端末識別子
8391
ブロードキャスト暗号鍵
8392
832
ペイロード部

【図１６】


開始
終点は
ブロードキャスト
？
S921
No
Yes
S923
終点とのユニキャスト鍵
で暗号化
S922
自己のブロードキャスト鍵
で暗号化
S924
暗号化したフレームを
下位層へ送出
終了

【図１７】


開始
終点は
ブロードキャスト
？
S911
Yes
No
終点は
自アドレス
？
S913
No
Yes
S914
始点とのユニキャスト鍵
で復号
S912
始点のブロードキャスト鍵
で復号
S916
暗号化フレームを
次点へ転送
S915
復号したフレームを
上位層で処理
終了