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

特許第5270937号
(P5270937)

(45)発行日　平成25年8月21日(2013.8.21)　(24)登録日　平成25年5月17日(2013.5.17)

(51)Int.Cl.　　F I
H04W 12/06 (2009.01)　　H04W 12/06
H04W 84/20 (2009.01)　　H04W 84/20
H04W 12/04 (2009.01)　　H04W 12/04

請求項の数 12　(全 17 頁)

(21)出願番号　特願2008-68354(P2008-68354)
(22)出願日　平成20年3月17日(2008.3.17)
(65)公開番号　特開2009-225182(P2009-225182A)
(43)公開日　平成21年10月1日(2009.10.1)
審査請求日　平成23年3月16日(2011.3.16)

前置審査

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

最終頁に続く

(54)【発明の名称】通信装置及びその制御方法

(57)【特許請求の範囲】
【請求項１】
通信装置であって、
他の通信装置との間で形成される通信ネットワークにおける役割を、所定のプロトコルを用いて自動的に決定する決定手段と、
前記決定手段によって自装置の役割が第１の役割に決定された場合、通信ネットワークを形成するための通信パラメータを前記他の通信装置に提供する提供手段と、
前記決定手段によって自装置の役割が第２の役割に決定された場合、前記他の通信装置から通信ネットワークを形成するための通信パラメータを受信する受信手段と、
前記決定手段によって自装置の役割が第１の役割に決定された場合、前記他の通信装置を認証する認証装置として機能する認証手段と、
前記決定手段によって自装置の役割が第２の役割に決定された場合、前記他の通信装置による認証を受ける被認証装置として機能する被認証手段と、を有し、
前記提供手段により提供された通信パラメータに基づいて形成された前記通信ネットワークから前記他の通信装置が離脱した後、該通信ネットワークに前記他の通信装置が再び接続する場合、前記決定手段による前記所定のプロトコルを用いた役割の決定を省略し、先の接続の際に前記決定手段によって前記所定のプロトコルを用いて決定された役割に従って、前記認証手段は、前記認証装置として前記他の通信装置との認証処理を再実行して、前記通信ネットワークにおいて暗号通信するための暗号鍵を共有する共有処理を行う、
ことを特徴とする通信装置。

【請求項２】
前記他の通信装置との間で、前記通信パラメータ設定後のデータ通信の際に使用する暗号方式についてのネゴシエーションを行い、該ネゴシエーションの結果に基づいて前記認証を行うか否かを判断することを特徴とする請求項１に記載の通信装置。
【請求項３】
前記ネゴシエーションの結果、前記通信ネットワークを構成する全ての通信装置において同一のグループ鍵の共有処理を実施する暗号方式を使用することが判別された場合には、前記認証を行い、前記グループ鍵を用いない暗号方式を使用することが判別された場合には、前記認証を行わないことを特徴とする請求項２に記載の通信装置。
【請求項４】
前記グループ鍵は、前記通信パラメータを用いたネットワークが構築された後、周期的に更新されることを特徴とする請求項３に記載の通信装置。
【請求項５】
前記グループ鍵は、前記通信パラメータを用いたネットワークが構築された後、該ネットワークに参加する通信装置の数の変更に応じて更新されることを特徴とする請求項３に記載の通信装置。
【請求項６】
前記提供手段による通信パラメータの提供を行う場合は、提供先装置のリストを配布する配布手段を有することを特徴とする請求項１から５のいずれか１項に記載の通信装置。
【請求項７】
前記決定手段によって自装置の役割が第１の役割に決定しなかった場合、他の通信装置から配布される、該他の通信装置が既に前記通信パラメータの提供を行った提供先装置のリストを受信する手段を有し、
前記受信したリストに基づいて、認証処理を行う装置を選択することを特徴とする請求項１から５のいずれか１項に記載の通信装置。
【請求項８】
開始信号を受信する手段と、
前記開始信号に対応する処理を判定する手段と、
前記判定に応じて、処理を選択する選択手段と、
を更に有することを特徴とする請求項１から７のいずれか１項に記載の通信装置。
【請求項９】
前記選択手段による選択に応じて、通信パラメータを共有するための処理を行わず認証処理を行う場合と、前記通信パラメータを共有するための処理を行ってから、認証処理を行う場合との何れかを実行する、
ことを特徴とする請求項８に記載の通信装置。
【請求項１０】
前記提供手段により提供された通信パラメータに基づいて形成された前記通信ネットワークから前記他の通信装置が離脱した後、該通信ネットワークに前記他の通信装置が再び接続する際に、前記提供手段による通信パラメータの提供を行わない場合であっても、前記認証手段は、前記他の通信装置との認証処理において前記認証装置として認証を行う、ことを特徴とする請求項１から９のいずれか１項に記載の通信装置。
【請求項１１】
通信装置の制御方法であって、
決定手段が、他の通信装置との間で形成される通信ネットワークにおける役割を、所定のプロトコルを用いて自動的に決定する決定工程と、
提供手段が、前記決定工程において自装置の役割が第１の役割に決定された場合、通信ネットワークを形成するための通信パラメータを前記他の通信装置に提供する提供工程と、
受信手段が、前記決定工程において自装置の役割が第２の役割に決定された場合、前記他の通信装置から通信ネットワークを形成するための通信パラメータを受信する受信工程

と、
認証手段が、前記決定工程において自装置の役割が第１の役割に決定された場合、認証装置として、前記他の通信装置を認証する認証工程と、
被認証手段が、前記決定工程において自装置の役割が第２の役割に決定された場合、被認証装置として、前記他の通信装置による認証を受ける被認証工程と、
を有し、
前記提供工程において提供された通信パラメータに基づいて形成された前記通信ネットワークから前記他の通信装置が離脱した後、該通信ネットワークに前記他の通信装置が再び接続する場合、前記決定工程における前記所定のプロトコルを用いた役割の決定を省略し、先の接続の際に前記決定工程において前記所定のプロトコルを用いて決定された役割に従って、前記認証工程において、前記認証装置として前記他の通信装置との認証処理を再実行して、前記通信ネットワークにおいて暗号通信するための暗号鍵を共有する共有処理を行う、
ことを特徴とする制御方法。
【請求項１２】
請求項１１に記載の通信装置の制御方法をコンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数の通信装置で構築されるネットワークにおける通信装置及びその制御方法に関する。
【背景技術】
【０００２】
従来、例えばIEEE802.11a/b/g/n/iなど、所謂IEEE802.11規格シリーズに基づいた無線ＬＡＮ接続を行う際の通信パラメータは多数存在し、尚且つ、設定値のバリエーションが多い。よって、その通信パラメータ設定を簡便にするための方法が提案されている。
【０００３】
特定の基地局を持つインフラストラクチャモードのネットワークでは、ネットワークを構成する無線通信装置は基地局により管理されている。よって、ネットワークを構成するための通信パラメータは、基地局から無線通信装置に配布される。
【０００４】
一方、特定の基地局を持たないアドホックモードのネットワークでは、全ての無線通信装置が対等な立場にある。よって、どの無線通信装置が通信パラメータの提供元となるかを決定する技術が必要であり、通信パラメータ提供元決定技術が提案されている（例えば、特許文献１、特許文献２参照）。
【特許文献１】特開2006-309458号公報
【特許文献２】特開2006-311138号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、例えば通信パラメータのセキュリティ設定として、無線ＬＡＮの暗号化方式の規格であるＷＰＡなどを選択した場合、通信パラメータ提供の方向性とは別に接続認証処理として、鍵共有アルゴリズムの起動方向を決定しなければならない。ＷＰＡはWi-Fi Protected Accessの略である。
【０００６】
よって、特定の基地局を持たず、全ての無線通信装置が対等な関係にあるアドホックモードのネットワークの場合、どの無線通信装置が接続認証処理を行うかを決定しなければならないという問題が依然として残っている。
【０００７】
本発明は、通信パラメータの提供元又は提供先として判別された通信装置が、その判別

に応じて、認証側又は被認証側として認証処理を行うことを目的とする。
【課題を解決するための手段】
【０００８】
本発明は、通信装置であって、他の通信装置との間で形成される通信ネットワークにおける役割を、所定のプロトコルを用いて自動的に決定する決定手段と、前記決定手段によって自装置の役割が第１の役割に決定された場合、通信ネットワークを形成するための通信パラメータを前記他の通信装置に提供する提供手段と、前記決定手段によって自装置の役割が第２の役割に決定された場合、前記他の通信装置から通信ネットワークを形成するための通信パラメータを受信する受信手段と、前記決定手段によって自装置の役割が第１の役割に決定された場合、前記他の通信装置を認証する認証装置として機能する認証手段と、前記決定手段によって自装置の役割が第２の役割に決定された場合、前記他の通信装置による認証を受ける被認証装置として機能する被認証手段と、を有し、前記提供手段により提供された通信パラメータに基づいて形成された前記通信ネットワークから前記他の通信装置が離脱した後、該通信ネットワークに前記他の通信装置が再び接続する場合、前記決定手段による前記所定のプロトコルを用いた役割の決定を省略し、先の接続の際に前記決定手段によって前記所定のプロトコルを用いて決定された役割に従って、前記認証手段は、前記認証装置として前記他の通信装置との認証処理を再実行して、前記通信ネットワークにおいて暗号通信するための暗号鍵を共有する共有処理を行う、ことを特徴とする。
【発明の効果】
【００１０】
本発明によれば、通信パラメータの提供元として動作する通信装置が、認証側として認証処理を行うことができる。また、認証側として認証処理を行った他の通信装置が再接続の際には認証側として認証処理を行うので再接続の利便性を向上することができる。
【発明を実施するための最良の形態】
【００１１】
以下、図面を参照しながら発明を実施するための形態について詳細に説明する。
【００１２】
［第１の実施形態］
まず、本発明を実施するのに好適な事例におけるハードウェア構成について説明する。図１は、通信パラメータの自動設定アプリケーションを備えた無線通信装置の構成を表すブロック図である。ここで、本実施形態における通信パラメータとは、ネットワーク識別子（ＳＳＩＤ）、暗号鍵、認証方式、周波数チャネル等である。
【００１３】
１０１は無線通信装置、１０２は通信パラメータの設定制御及び無線機能の制御などを行う制御部、１０３は各種情報を記憶する記憶部である。１０４は無線通信を行うための無線部、１０５は表示などを行う表示部であり、ＬＣＤやＬＥＤのように視覚で認知可能な情報の出力や、スピーカなどの音出力が可能な機能を有する。１０６は通信パラメータ設定を開始するトリガを与える設定ボタン、１０７はアンテナ制御部、１０８はアンテナである。
【００１４】
以上が無線通信装置のハードウェア構成である。尚、このハードウェア構成は本発明における実施形態の一つの事例であり、必ずしもこのハードウェア構成を有していなければいけないものではない。本発明の精神を適用できるハードウェア構成であれば全て本発明の範囲内である。
【００１５】
図２は、図１に示す無線通信装置によって構成される通信ネットワークの構成の一例を示す図である。図２に示すように、IEEE802.11規格シリーズに準拠した無線ＬＡＮの無線通信機能を備えた無線通信装置２１（以下、端末Ａ）、無線通信装置２２（以下、端末Ｂ）、無線通信装置２３（以下、端末Ｃ）が存在する。

【００１６】
ここで、端末Ａ、端末Ｂ、端末Ｃは図１に示す無線通信装置としての機能を有し、全て同等の無線通信能力を有し、アドホックモードのネットワークを構成している。ここで、アドホックモードとは、基地局（アクセスポイント）を介さず、端末間で直接通信を行う通信形態である。アドホックモードのネットワークを構築後、定められた通信パラメータ提供元決定アルゴリズムに基づいて、通信パラメータの設定処理における役割（通信パラメータの提供元端末、又は提供先端末）を決定する。
【００１７】
尚、本実施形態では、通信パラメータ提供元決定アルゴリズムについては、例えば特開2006-311138号公報に記載のプロトコルを用いることができるが、本発明はこの方法に限定されるわけではない。端末Ａが通信パラメータの提供元端末として決定され、端末Ｂ及び端末Ｃが通信パラメータの提供先端末として決定されるものとする。図２に示す例では、端末Ｂ及び端末Ｃが端末Ａから通信パラメータを提供されている様子を示している。
【００１８】
図３は、図２に示す端末Ａで実行される通信制御方法を説明するためのフローチャートである。まず、ユーザが設定ボタン１０６を押下することで、通信パラメータ設定機能が有効化される。具体的には、自端末で通信パラメータ設定機能が有効になったことを示すために、例えば無線ＬＡＮで用いられるビーコン情報に特定の識別子を付与する。また、通信パラメータ設定機能が有効になったことをユーザに通知するために、表示部１０５に「通信パラメータ設定作業中」などと表示させる（Ｆ３０１）。これにより、ユーザの利便性が向上する。
【００１９】
次に端末Ａは、通信パラメータ設定機能が有効になった端末Ｂ及び端末Ｃとの間で予め定めた通信パラメータ提供方向決定処理を実施する。この処理により、端末Ａが通信パラメータ提供元端末と決定されたものとする（Ｆ３０２）。
【００２０】
次に、通信パラメータ提供元端末と決定された端末Ａは、通信パラメータ提供先端末と決定された端末Ｂ又は端末Ｃから、通信開始要求として通信パラメータ設定開始要求を受信する（Ｆ３０３）。
【００２１】
ここで、端末Ａは、通信パラメータ設定後（即ち、ネットワーク構築後）のデータ通信の際に使用する暗号方式、認証方式についてのネゴシエーションを、相手装置（例えば、端末Ｂ）との間で実施する（Ｆ３０４）。無線ＬＡＮにおける暗号・認証方式としては、いくつかのバリエーションが存在するが、この暗号・認証方式は２つに大別できる。まず、一つ目は通信パラメータ提供元端末から通信パラメータとして提供暗号鍵を、そのまま送信データを暗号化するための暗号鍵として利用する場合である（第１の暗号・認証方式）。
【００２２】
次に、二つ目は通信パラメータとして引き渡された暗号鍵を種として、受信元及び送信元とで認証処理を行い、新たなセッション鍵を生成して、そのセッション鍵を用いて送信データを暗号化する場合である（第２の暗号・認証方式）。
【００２３】
何れの場合も、通信パラメータ提供時に通信パラメータを暗号化する鍵と、通信パラメータ設定処理終了後に実際のデータ通信で用いる暗号鍵とは、異なることが望ましい。
【００２４】
尚、IEEE802.11i規格シリーズでは、一つ目の方式は従来のＷＥＰ鍵に相当し、二つ目の方式はＴＫＩＰ、ＣＣＭＰに相当する。ここで、ＷＥＰはWired Equivalent Privacyの略である。ＴＫＩＰはTemporal Key Integrity Protocolの略で、ユーザ認証機能を備え、パケット毎又は周期的に暗号鍵の変更が可能でメッセージ改ざん防止機能を有する。ＣＣＭＰ（Counter mode with Cipher block chaining Message authentication code Prot

ocol）はデータの改ざんを検出することが可能である。

【００２５】

ネゴシエーションの結果、新たなセッション鍵を生成するような場合には、端末間でグループ鍵の共有処理も行うこととなる。そのため、第１の実施形態では、暗号・認証方式を区別するために、グループ鍵の共有処理を実施するか、しないかを判断基準とするものとして説明する（Ｆ３０５）。実際には、上記ネゴシエーションによってどの暗号・認証方式を用いるかが決定されるので、決定された暗号・認証方式に基づいて、Ｆ３０６以下の処理が行なわれるか、Ｆ３１４の処理が行なわれるかが決定される。

【００２６】

尚、本実施形態における説明では、暗号・認証方式についてのネゴシエーション結果に基づいて上記判断を行うものとして説明したが、暗号方式、認証方式のいずれかに基づいて上記判断を行ってもよい。

【００２７】

ここで、セッション鍵とは、主にユニキャスト通信に用いる暗号鍵であって、端末Ａと端末Ｂの組、および端末Ａと端末Ｃの組で異なるセッション鍵を用いても良いし、同一のセッション鍵を用いても良い。

【００２８】

一方、グループ鍵とは、マルチキャスト通信及びブロードキャスト通信に用いる暗号鍵であり、ネットワークを構成する全ての端末（本実施の形態では、端末Ａと端末Ｂと端末Ｃ）において同一である。尚、セッション鍵とグループ鍵を同一の鍵として、全ての通信をグループ鍵で行っても良い。

【００２９】

グループ鍵はパケットの送信元となりうる端末毎にそれぞれ有してもよく、本実施の形態ではネットワークを構成する端末は３つあるため、それぞれの端末はグループ鍵を３つずつ持っても良い。また、ネットワークとして唯一のグループ鍵を有するものとしてもよい。

【００３０】

まず、Ｆ３０５に示す判断処理において、グループ鍵の共有処理を実施する方式を採用した場合の説明を行う。

【００３１】

グループ鍵共有処理を実施する方式の場合、端末Ａと端末Ｂとは接続認証プロセスにおける役割（接続認証側か被接続認証側か）を決定する必要がある。ここで、接続認証側をオーセンティケーター（Authenticator）と称し、被接続認証側をサプリカント（Supplicant）と称している。

【００３２】

第１の実施形態では、通信パラメータ提供方向決定処理により、通信パラメータ提供元端末と決定された端末Ａが接続認証側機能を担当するオーセンティケーターとなる。そして、通信パラメータ提供先端末に決定された端末Ｂ又は端末Ｃが被接続認証側機能を担当するサプリカントとなる。

【００３３】

通信パラメータを提供するに当たっては、セキュリティを保つために、通信パラメータの暗号化及び通信パラメータ提供元と提供先端末間での認証処理が行われる。そこで、端末Ａは、暗号・認証処理のために必要な乱数を生成する（Ｆ３０６）。ここで生成した乱数は、セッション鍵生成のために用いる乱数として使用するために、記憶しておく。

【００３４】

引き続き、端末Ａは端末Ｂとの間で、提供する通信パラメータを暗号化するための暗号鍵の共有処理及び認証処理を行う（Ｆ３０７）。Ｆ３０７に示す処理過程で、端末Ｂが生成した通信パラメータ提供時の暗号・認証処理に必要な乱数が端末Ｂから送信される。端末Ａと端末Ｂは、互いに生成した乱数を用いて通信パラメータ提供用の暗号鍵の共有処理を行う。

【００３５】
尚、後述するように、端末Ｂは、端末Ａとの間で共有された暗号鍵を、提供された通信パラメータを復号化するために用いる。つまりここでの暗号鍵の共有処理とは、端末Ａが提供する通信パラメータを暗号化するための暗号鍵を有し、端末Ｂが提供された通信パラメータを復号化するための暗号鍵を有するため、端末Ａと端末Ｂとの間で所定のプロトコル処理を行うことを示す。
【００３６】
次に、端末Ａ自身で生成した乱数と、端末Ｂから受信した乱数と、端末Ａが保有している暗号鍵の種と、に基づいて通信用のセッション鍵を生成する（Ｆ３０８）。
【００３７】
そして、端末Ａは、アドホックモードのネットワークを構成するのに必要な通信パラメータを、Ｆ３０７で端末Ｂとの間で共有した暗号鍵を用いて暗号化し、端末Ｂに対して送信する（Ｆ３０９）。その際、Ｆ３０８で生成したセッション鍵も併せて送信する。こうして、端末Ａと端末Ｂとの間でセッション鍵が共有される。以降の説明で用いるセッション鍵の共有処理とは、端末Ａが生成したセッション鍵を端末Ｂへ送信し、端末Ｂがそれを受信する処理を示す。
【００３８】
但し、ここでセッション鍵を端末Ｂへ送信しても端末Ｂが第１の実施形態に必要な機能を備えていない場合も考えられる。その場合、端末Ｂは端末Ａから送信されたセッション鍵を読み捨て、従来どおりの処理を行う。
【００３９】
Ｆ３０９で送信したセッション鍵は、端末Ａと端末Ｂとの間でユニキャスト通信を行う際に有効な暗号鍵である。次に端末Ａは、アドホックモードのネットワークを構成する端末全てに有効になるグループ鍵をセッション鍵で暗号化し、端末Ｂへ送信する（Ｆ３１０）。こうして、端末Ａと端末Ｂとの間でグループ鍵が共有される。このように、グループ鍵の共有処理とは、端末Ａがセッション鍵で暗号化したグループ鍵を端末Ｂへ送信し、端末Ｂがそれを受信する処理を示す。第１の実施形態ではグループ鍵を端末Ｂへ送信するのみであるが、端末Ａが既に別の端末との間で通信パラメータ設定処理を実施済みである場合、そのパラメータ設定処理を実施済みの端末全てとの間でグループ鍵の共有処理を行う。
【００４０】
この時点で、無線接続に必要な通信パラメータは一通りそろったことになる。よって、端末Ｂから設定完了通知が送信されてくるため、端末Ａはそれを受信する（Ｆ３１１）。このとき、表示部１０５に「無線ネットワークへの接続完了」などと表示させても良い。これにより、ユーザの利便性が向上する。
【００４１】
以上の処理により、端末Ａと端末Ｂとの間でアドホックモードのネットワークの通信が確立する。
【００４２】
次に、通信パラメータ設定処理を継続し、他の端末に対しても通信パラメータの提供を行うかを判断し（Ｆ３１２）、継続すると判断した場合、処理フローをＦ３０３から別の端末との間で実施する。また、継続しない場合、Ｆ３０１で設定した通信パラメータ設定機能が有効になったことを示す表示を終了する（Ｆ３１３）。
【００４３】
ここで、Ｆ３０５に示す判断処理で、グループ鍵共有処理を実施する方式を採用しなかった場合を説明する。
【００４４】
グループ鍵共有処理を実施しない方式の場合は、端末Ａから端末Ｂへ通信パラメータとして提供された暗号鍵をそのまま適用するのみでよい。即ち、端末Ａと端末Ｂとは、接続認証プロセスにおける接続認証側か被接続認証側かどうかの決定は特に不要である。通信

パラメータを提供するに当たっては、通信パラメータの暗号化及び提供元端末と提供先端末間での認証処理が行われる。そこで、端末Ａは、前記暗号・認証処理のために必要な乱数を生成する（Ｆ３１４）。

【００４５】

次に、端末Ａは端末Ｂとの間で、提供する通信パラメータを暗号化するための暗号鍵の共有処理及び認証処理を行う（Ｆ３１５）。引き続き、端末Ａはアドホックモードのネットワークを構成するのに必要な通信パラメータを、Ｆ３１５で端末Ｂとの間で共有した暗号鍵を用いて暗号化し、端末Ｂに向けて送信する（Ｆ３１６）。

【００４６】

以上の処理により、グループ鍵の共有処理を実施しない場合の通信パラメータ設定処理が完了し、端末Ａと端末Ｂとの間で同一の通信パラメータが共有できたので、そのパラメータを用いてネットワークを構築することができる。

【００４７】

図４は、図２に示す端末Ｂ又は端末Ｃの通信制御方法を説明するためのフローチャートである。ここでは、端末Ｂについて説明を行う。

【００４８】

まず、端末Ｂにおいても端末Ａと同様に、設定ボタン１０６が押下されることにより、通信パラメータ設定機能が有効化される。上述のように、自端末において通信パラメータ設定機能が有効になったことを示すために、例えば無線ＬＡＮで用いられるビーコン情報に特定の識別子を付与する。また、通信パラメータ設定機能が有効になったことをユーザに通知するために、表示部１０５に「通信パラメータ設定作業中」などと表示させる（Ｆ４０１）。これにより、ユーザの利便性が向上する。

【００４９】

次に端末Ｂは、通信パラメータ設定機能が有効になった端末Ａ及び端末Ｃとの間で、予め定めた通信パラメータ提供方向決定処理を実施する。この提供方向決定処理により、端末Ａが通信パラメータ提供元端末と決定された場合、端末Ｂは通信パラメータ提供先端末（受信端末）と決定される（Ｆ４０２）。

【００５０】

次に、上述の提供方向決定処理により通信パラメータ受信端末と決定された端末Ｂは、通信パラメータ提供元端末と決定された端末Ａへ通信パラメータ設定開始要求を送信する（Ｆ４０３）。

【００５１】

ここで端末Ｂは、通信パラメータ設定処理を開始する際に、まずは、通信パラメータ設定後のデータ通信の際に使用する暗号・認証方式についてのネゴシエーションを、端末Ａとの間で実施する（Ｆ４０４）。端末Ａのフローチャートと同様に、端末Ｂにおいても、暗号・認証方式を区別するために、グループ鍵共有処理を実施するか、しないかを判断基準とする（Ｆ４０５）。

【００５２】

まず、Ｆ４０５に示す判断処理において、グループ鍵共有処理を実施する方式を採用した場合について説明を行う。

【００５３】

グループ鍵共有処理を実施する方式の場合、端末Ａと端末Ｂとは接続認証プロセスにおける接続認証側か被接続認証側か否かを決定する必要がある。ここで、通信パラメータ提供方向決定処理により、通信パラメータ提供元端末と決定された端末Ａが接続認証側機能を担当するオーセンティケーターとなる。そして、通信パラメータ提供先端末に決定された端末Ｂ又は端末Ｃは、被接続認証側機能を担当するサプリカントとなる。

【００５４】

端末Ａが通信パラメータを提供するに当たっては、通信パラメータの暗号化及び通信パラメータ提供元と提供先端末間での認証処理が行われる。そこで、端末Ｂは、前記暗号・認証処理のために必要な乱数を生成する（Ｆ４０６）。

【００５５】
引き続き、端末Ｂは、端末Ａとの間で、提供される通信パラメータを復号化するための暗号鍵の共有処理及び認証処理を行う（Ｆ４０７）。Ｆ４０７に示す処理過程で、端末Ａが生成した通信パラメータ提供時の暗号・認証処理に必要な乱数が端末Ａから送信される。端末Ａと端末Ｂは、互いに生成した乱数を用いて通信パラメータ提供用の暗号鍵の共有処理を行う。
【００５６】
その後、アドホックモードのネットワークを構成するのに必要な通信パラメータが端末Ａから端末Ｂに向けて送信されるので、端末Ｂはそれを受信する（Ｆ４０８）。なお、通信パラメータは、Ｆ４０７で端末Ａと端末Ｂ間で共有された暗号鍵によって暗号化されている。
【００５７】
また、端末Ａからは、端末Ｂと端末Ａとの間でのみ有効なセッション鍵（図３のＦ３０８にて端末Ａが生成）も通信パラメータとして送信される。
【００５８】
Ｆ４０８で受信したセッション鍵は、端末Ａと端末Ｂとの間でユニキャスト通信を行う際に有効な暗号鍵である。次に端末Ｂは、アドホックモードのネットワークを構成する全端末で有効になるグループ鍵を端末Ａから受信する（Ｆ４０９）。なお、グループ鍵は、Ｆ４０８で端末Ａから提供されたセッション鍵により暗号化されている。こうして、端末Ａと端末Ｂとの間でグループ鍵が共有される。
【００５９】
この時点で、無線通信に必要な通信パラメータは一通りそろったため、端末Ｂは端末Ａへ設定完了通知を送信する（Ｆ４１０）。このとき、表示部１０５に「無線ネットワークへの接続完了」などと表示させても良い。これによりユーザの利便性が向上する。
【００６０】
以上の処理により、端末Ａと端末Ｂとの間でアドホックモードのネットワークの通信が確立するので、Ｆ４０１で設定した通信パラメータ設定機能が有効になったことを示す表示を終了する（Ｆ４１１）。
【００６１】
ここで、Ｆ４０５に示す判断処理においてグループ鍵共有処理を実施する方式を採用しなかった場合について説明を行う。
【００６２】
グループ鍵共有処理を実施しない方式の場合は、端末Ａから端末Ｂへ通信パラメータとして提供された暗号鍵をそのまま適用するのみで良い。即ち、端末Ａと端末Ｂとは、接続認証プロセスにおける接続認証側か被接続認証側かの決定は特に不要である。
【００６３】
端末Ａが通信パラメータを提供するに当たっては、通信パラメータの暗号化及び提供元と提供先端末間での認証処理が行われる。そこで、端末Ｂは、前記暗号・認証処理のために必要な乱数を生成する（Ｆ４１２）。
【００６４】
次に端末Ｂは、端末Ａとの間で、提供される通信パラメータを復号化するための暗号鍵の共有処理及び認証処理を行う（Ｆ４１３）。
【００６５】
そして、端末Ａから、アドホックモードのネットワークを構成するのに必要な通信パラメータが端末Ｂに向けて送信されるので、端末Ｂはそれを受信する（Ｆ４１４）。尚、通信パラメータは、Ｆ４１３で端末Ａと端末Ｂ間で共有された暗号鍵によって暗号化されている。
【００６６】
以上の処理により、グループ鍵共有処理をしない場合の通信パラメータ設定処理が完了し、端末Ａと端末Ｂとの間で同一の通信パラメータが共有できたので、そのパラメータを

用いてネットワークを構築することができる。

【００６７】

図５は、図２に示すネットワーク構成における通信制御方法を示すシーケンスチャートである。まず、端末Ａ、端末Ｂ及び端末Ｃで、それぞれ通信パラメータ設定機能を有効にするために設定ボタン１０６が押下される。設定ボタン１０６が押下されることにより、通信パラメータ設定機能が有効となり、予め定められた通信パラメータ提供方向決定処理を実施する（Ｓ５０１）。

【００６８】

この通信パラメータ提供方向決定処理により、端末Ａが通信パラメータ提供端末に決定され（Ｓ５０３）、端末Ｂ及び端末Ｃが通信パラメータ受信端末と決定される（Ｓ５０２，Ｓ５０４）。

【００６９】

次に、通信パラメータ受信端末と決定された端末Ｂから、通信パラメータ設定開始要求が、通信パラメータ提供端末と決定された端末Ａへ送信される（Ｓ５０５）。引き続き、通信パラメータ設定開始手続きが端末Ａと端末Ｂとの間で行われる（Ｓ５０６）。

【００７０】

通信パラメータ設定開始手続きに引き続き、端末Ａと端末Ｂとの間で、通信パラメータ設定後（即ち、ネットワーク構築後）のデータ通信時に使用する暗号・認証方式についてのネゴシエーションが行われる（Ｓ５０７）。ここでは、図３及び図４を用いて説明したグループ鍵共有処理の実施の有無によって処理が区別される。

【００７１】

Ｓ５０７において、グループ鍵の共有処理を行う暗号・認証方式が選択された場合、本来であれば通信パラメータ設定処理に引き続いて実施される接続認証処理及びセッション鍵の共有処理を、通信パラメータ設定処理の中で同時に実行する（Ｓ５０８）。これにより、通信パラメータの設定処理後に接続認証処理及びセッション鍵の共有処理を行う場合と比べ、ネットワーク形成までに要する時間を短縮することができる。

【００７２】

セッション鍵が定まると、アドホックモードのネットワークにおいてマルチキャスト通信、及びグループキャスト通信に使用するグループ鍵を、セッション鍵を用いて端末Ａから端末Ｂへ向けて配信する（Ｓ５０９）。

【００７３】

以上の処理により、端末Ａと端末Ｂとの間で無線接続に必要な通信パラメータは一通り共有されるため、通信パラメータ設定完了通知が、端末Ａから端末Ｂへ送信される（Ｓ５１０）。こうして端末Ａと端末Ｂ間で共通の通信パラメータが設定され、アドホックモードのネットワークが確立される。

【００７４】

次に、端末Ａと端末Ｂとの間で、通信パラメータ設定及び新規ネットワーク構築が完了した後に、端末Ｃがネットワークに参加する場合を、図５を用いて引き続き説明する。

【００７５】

まず、端末Ｃは、上述のＳ５０４で既に通信パラメータ受信端末と決定されているので、通信パラメータ受信端末と決定された端末Ｃから、通信パラメータ設定開始要求が、通信パラメータ提供端末と決定された端末Ａへ送信される（Ｓ５１１）。次に、通信パラメータ設定開始手続きが端末Ａと端末Ｃとの間で行われる（Ｓ５１２）。

【００７６】

通信パラメータ設定開始手続きに引き続き、端末Ａと端末Ｃとの間で、通信パラメータ設定後（即ち、ネットワーク構築後）のデータ通信時に使用する暗号・認証方式についてのネゴシエーションが行われる（Ｓ５１３）。ここでも、図３及び図４を用いて説明したグループ鍵共有処理の実施の有無によって処理が区別される。

【００７７】

Ｓ５１３において、グループ鍵の共有処理を行う暗号・認証方式が選択された場合につ

いて説明する。この場合、本来であれば通信パラメータ設定処理に引き続いて実施される接続認証処理及びセッション鍵共有処理を、通信パラメータ設定処理の中で同時に実行する（Ｓ５１４）。これにより、通信パラメータの設定処理後に接続認証処理及びセッション鍵の共有処理を行う場合と比べ、ネットワーク形成までに要する時間を短縮することができる。

【００７８】

セッション鍵が定まると、アドホックモードのネットワークにおいてマルチキャスト通信、及びグループキャスト通信に使用するグループ鍵を、セッション鍵を用いて端末Ａから端末Ｃへ向けて配信する（Ｓ５１５）。

【００７９】

以上の処理により、端末Ａと端末Ｃとの間で無線接続に必要な通信パラメータは一通り共有される。そのため、通信パラメータ設定完了通知が端末Ａから端末Ｃへ送信され（Ｓ５１６）、端末Ｃは、端末Ａと端末Ｂとが構築しているアドホックモードのネットワークに参加する。

【００８０】

ここで、ネットワーク内の端末が共通で用いるグループ鍵が常に同一であると、悪意のある第三者や、かつてネットワークに参加していた端末が容易にネットワークに参加することが可能となり、セキュリティ上の危険がある。よって、周期的なタイマや、通信パラメータ提供を受ける端末が増加、減少する度に、グループ鍵を更新しても良い。

【００８１】

図５に示す例では、端末Ｃが新たにネットワークに参加した時点で、端末Ａは端末Ｂ及び端末Ｃとの間でグループ鍵共有を行う（Ｓ５１７）。このようにネットワーク内の端末が増加もしくは減少した際にグループ鍵の共有処理を実行することにより、グループ鍵が更新されるため、セキュリティを向上することができる。

【００８２】

このように、本実施形態では、通信パラメータ設定処理の役割（通信パラメータの提供元端末、又は提供先端末）の判別に応じて、セッション鍵の共有処理における役割（認証側、又は被認証側）を決定する。これにより、通常であれば通信パラメータ設定処理の後に行う必要があるセッション鍵の共有処理を通信パラメータ設定処理の中で実行することができるため、接続完了までの時間を短縮することができる。また、通信パラメータ提供元端末が認証側端末となることにより、グループ鍵の更新を容易に行うことができ、セキュリティが向上する。

【００８３】

［第２の実施形態］

次に、図面を参照しながら本発明に係る第２の実施形態を詳細に説明する。第１の実施形態では、端末Ａと端末Ｂ又は端末Ｃが通信パラメータを設定し、接続が完了するまでを説明した。第２の実施形態では、端末Ａと端末Ｂ又は端末Ｃとの間で既に通信パラメータの設定が完了している場合の再接続を説明する。

【００８４】

尚、第２の実施形態におけるハードウェア構成は、第１の実施形態で用いた図１に示す構成と同様である。また、第２の実施形態におけるネットワーク構成例も第１の実施形態で用いた図２に示す構成と同様である。端末Ａと端末Ｂ及び端末Ｃ間でネットワークを形成するまでの処理は第1の実施形態と同様であるため、ここでの説明を省略する。

【００８５】

図６は、図２に示す端末Ａの、第２の実施形態における通信制御方法を説明するためのフローチャートである。まず、通信パラメータ提供元端末である端末Ａが通信パラメータ提供先端末である端末Ｂから通信開始要求を受信する（Ｆ６０１）。この通信開始要求は、通信パラメータ設定処理だけでなく、通常の接続認証処理でも使用されるものとする。通信開始要求を受信した端末Ａは、通信パラメータ設定処理の開始を要求されたか接続認証処理の開始を要求されたかを判別するため、その送信元へ向けて処理識別要求を送信す

る（Ｆ６０２）。
【００８６】
処理識別要求に対して端末Ｂからその応答である処理識別応答が返答される。この応答の種別が通信パラメータ設定用か否かで処理を分岐する（Ｆ６０３）。
【００８７】
次に、処理識別応答が通常の接続認証処理を示している場合について説明する。まず、通常の接続認証処理である場合、通信パラメータ送信元であった端末Ａが接続認証側機能を担当するオーセンティケータとして端末Ｂを認証し、端末Ｂとの間でセッション鍵の共有処理を実施する（Ｆ６０４）。
【００８８】
このセッション鍵共有処理に引き続き、端末Ａはアドホックモードのネットワークに参加する全ての端末との間で、マルチキャスト通信又はブロードキャスト通信時に使用されるグループ鍵の共有処理を実行する（Ｆ６０５）。ここで、端末Ａが新しく通信パラメータを提供した端末が増加している場合も考えられるため、端末Ａはこれまでに通信パラメータを提供した端末に対して、提供先端末のリストを配布する（Ｆ６０６）。このリストは、端末Ａがネットワークから離脱した後の接続認証側機能を担う端末を決定する際に使用される。
【００８９】
一方、Ｆ６０３において、処理識別応答が通信パラメータ設定用を示している場合について説明する。この場合、既に図３を用いて説明した通信パラメータ設定処理を実施する（Ｆ６０７）。
【００９０】
次に、通信パラメータ設定が終了した時点で、上述の通信パラメータを提供した提供先端末のリストを更新する（Ｆ６０８）。その後、ネットワークに参加している全ての端末との間でグループ鍵共有処理を実施し（Ｆ６０９）、更新したリストを、各端末に配布する（Ｆ６１０）。
【００９１】
以上により、アドホックモードのネットワークを構成する全ての端末で、グループ鍵が更新され、それぞれの端末情報を保有することができる。また、表示部１０５に、「無線ネットワークへの接続完了」などと表示させても良く、ユーザの利便性が向上する。
【００９２】
図７は、図２に示す端末Ｂ又は端末Ｃの、第２の実施形態における通信制御方法を説明するフローチャートである。ここでは、端末Ｂの場合について説明を行う。
【００９３】
通信パラメータ受信端末である端末Ｂは、通信パラメータ提供元端末である端末Ａへ、通信開始要求を送信する（Ｆ７０１）。通信開始要求は、通信パラメータ設定処理だけでなく、通常の接続認証処理でも使用される。端末Ｂは、通信開始要求を受信した端末Ａから、通信パラメータ設定処理の開始を要求されたか接続認証処理の開始を要求されたかを判別するための処理識別要求を受信する。
【００９４】
但し、通信パラメータの提供元端末であった端末Ａが既にネットワーク上に存在しない場合もある。その場合、ある一定期間のタイムアウト及び所定の再送回数だけリトライを行い、端末Ａがネットワーク上に存在するか否かを判定する（Ｆ７０２）。
【００９５】
ここで、端末Ａからの応答が無い場合、端末Ａがネットワーク上に存在しないものと判断し、端末Ｂは端末Ａから受信した通信パラメータの提供先端末のリストを参照し、通信開始要求の送信先を選選択する。例えば端末Ｄを新たな接続先として設定する（Ｆ７０３）。
【００９６】
そして端末Ｂは、選択された通信開始要求の送信先端末Ｄへ向けて、通信開始要求を送

信する（Ｆ７０４）。その後、通信開始要求を受信した端末Ｄからの処理識別要求の受信を待機する。ここで、端末Ｄも存在しない場合、通信パラメータの提供先端末リストから再度端末を選択し、通信開始要求を送信する。こうして、処理識別要求を受信するか、このリストが空になるまで処理を続ける。

【００９７】

処理識別要求の受信元によって処理は変わらないため、ここでは、端末Ａから処理識別要求を受信したものとして説明を行う。

【００９８】

端末Ｂは、処理識別応答として通常の接続認証処理である旨を応答する。この場合は、端末Ａが接続認証側機能を担うオーセンティケータとして端末Ｂを認証する。そして端末Ｂは端末Ａとの間でセッション鍵の共有処理を実施する（Ｆ７０５）。セッション鍵共有処理に引き続き、端末Ｂは端末Ａとの間で、アドホックモードのネットワーク全体でマルチキャスト通信又はブロードキャスト通信時に使用するグループ鍵の共有処理を実行する（Ｆ７０６）。

【００９９】

ここで、端末Ａが新しく通信パラメータを提供した端末が増加している場合も考えられるため、端末Ａから提供先端末のリストを受信する（Ｆ７０７）。

【０１００】

以上により、アドホックモードのネットワークを構成する全ての端末においてグループ鍵が更新され、それぞれの端末情報を保有する。このとき、表示部１０５に「無線ネットワークへの接続完了」などと表示させても良く、ユーザの利便性が向上する。

このように、通信パラメータの提供元端末（認証側）が、提供先端末のリストをネットワーク内の端末に配布することにより、上記提供元端末がネットワークから離脱した場合であっても、新たな認証側端末を決定することができる。

【０１０１】

以上、本発明の好適な実施形態を説明したが、これは本発明の説明のための例示であって、本発明の範囲をこの実施形態のみに限定する趣旨ではない。本発明の要旨を逸脱しない範囲で、実施形態は種々に変形することが可能である。

【０１０２】

また、IEEE802.11シリーズに準拠の無線ＬＡＮシステムを例に挙げて説明したが、通信形態は必ずしもIEEE802.11準拠の無線ＬＡＮに限定されないことは言うまでもない。

【０１０３】

また、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（ＣＰＵ若しくはＭＰＵ）が記録媒体に格納されたプログラムコードを読出し実行する。これによっても、本発明の目的が達成されることは言うまでもない。

【０１０４】

この場合、コンピュータ読み取り可能な記録媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記録媒体は本発明を構成することになる。

【０１０５】

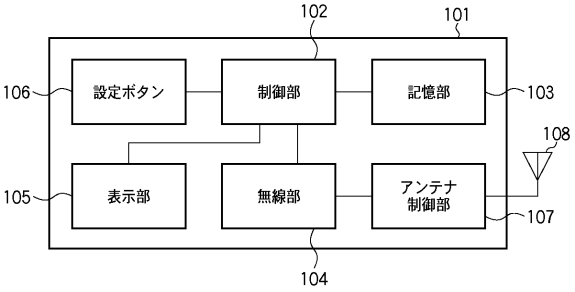
このプログラムコードを供給するための記録媒体として、例えばフレキシブルディスク，ハードディスク，光ディスク，光磁気ディスク，ＣＤ－ＲＯＭ，ＣＤ－Ｒ，磁気テープ，不揮発性のメモリカード，ＲＯＭなどを用いることができる。

【０１０６】

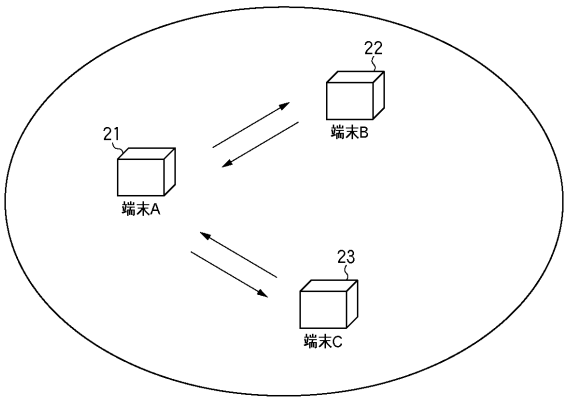
また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、次の場合も含まれることは言うまでもない。即ち、プログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）などが実際の処理の一部又は全部を行い、その処理により前述した実施形態の機能が実現される場合である。

【０１０７】
更に、記録媒体から読出されたプログラムコードがコンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込む。その後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部又は全部を行い、その処理により前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【図面の簡単な説明】
【０１０８】
【図１】通信パラメータの自動設定アプリケーションを備えた無線通信装置の構成を表すブロック図である。
【図２】図１に示す無線通信装置によって構成されるネットワークの構成の一例を示す図である。
【図３】図２に示す端末Ａで実行される通信制御方法を説明するためのフローチャートである。
【図４】図２に示す端末Ｂ又は端末Ｃの通信制御方法を説明するためのフローチャートである。
【図５】図２に示すネットワーク構成における通信制御方法を示すシーケンスチャートである。
【図６】図２に示す端末Ａの、第２の実施形態における通信制御方法を説明するためのフローチャートである。
【図７】図２に示す端末Ｂ又は端末Ｃの、第２の実施形態における通信制御方法を説明するフローチャートである。
【符号の説明】
【０１０９】
１０１　無線通信装置
１０２　制御部
１０３　記憶部
１０４　無線部
１０５　表示部
１０６　設定ボタン
１０７　アンテナ制御部
１０８　アンテナ

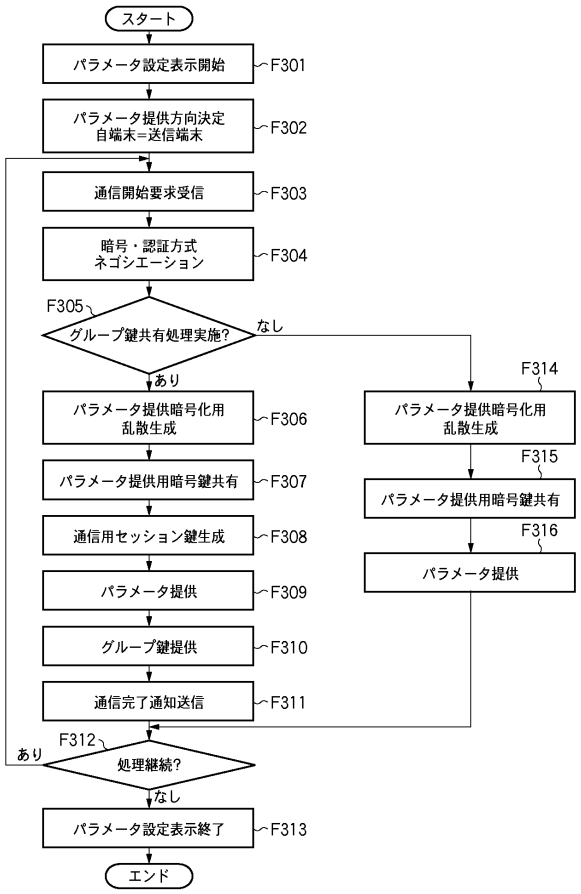
【図１】


102
101
106
設定ボタン
制御部
記憶部
103
108
105
表示部
無線部
アンテナ
制御部
107
104

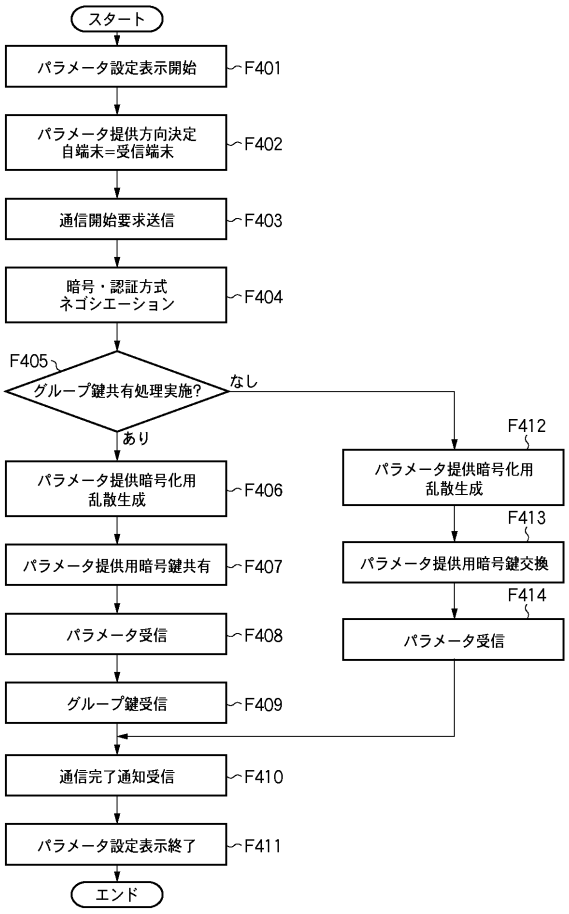
【図２】


22
端末B
21
端末A
23
端末C

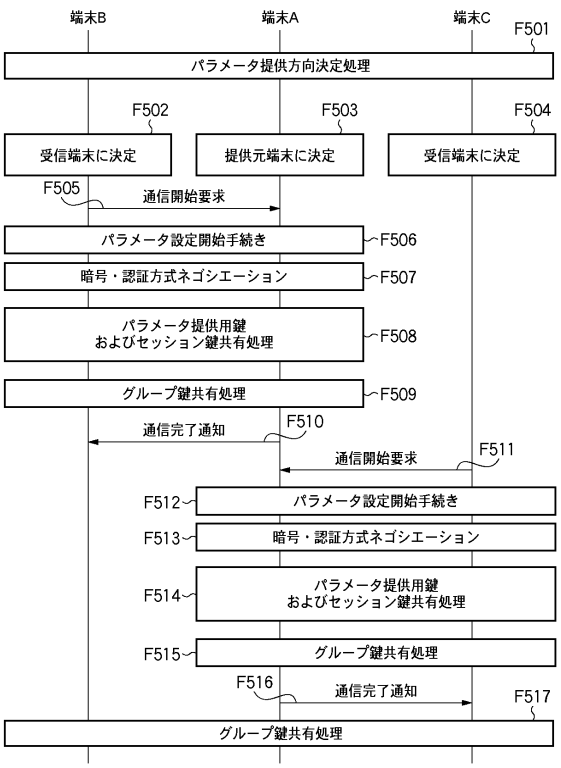
【図３】


スタート
パラメータ設定表示開始
F301
パラメータ提供方向決定
自端末=送信端末
F302
通信開始要求受信
F303
暗号・認証方式
ネゴシエーション
F304
F305
グループ鍵共有処理実施?
なし
あり
パラメータ提供暗号化用
乱散生成
F306
パラメータ提供用暗号鍵共有
F307
通信用セッション鍵生成
F308
パラメータ提供
F309
グループ鍵提供
F310
通信完了通知送信
F311
F312
処理継続?
あり
なし
パラメータ設定表示終了
F313
エンド
F314
パラメータ提供暗号化用
乱散生成
F315
パラメータ提供用暗号鍵共有
F316
パラメータ提供

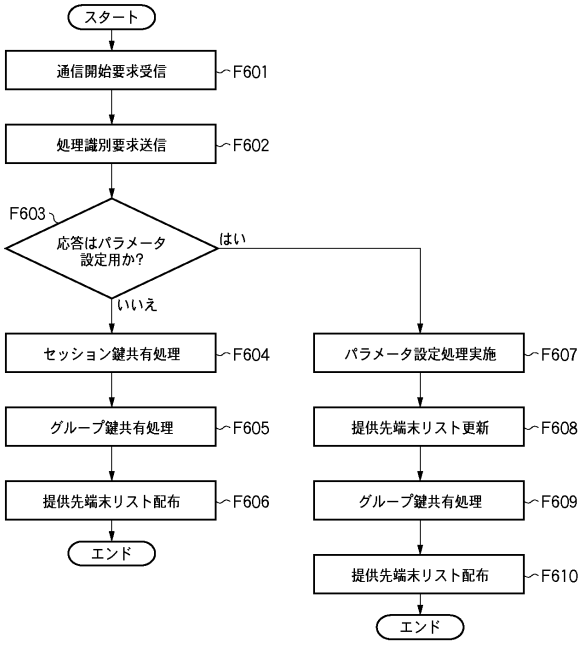
【図４】


スタート
パラメータ設定表示開始
F401
パラメータ提供方向決定
自端末=受信端末
F402
通信開始要求送信
F403
暗号・認証方式
ネゴシエーション
F404
F405
グループ鍵共有処理実施?
なし
あり
パラメータ提供暗号化用
乱散生成
F406
パラメータ提供用暗号鍵共有
F407
パラメータ受信
F408
グループ鍵受信
F409
通信完了通知受信
F410
パラメータ設定表示終了
F411
エンド
F412
パラメータ提供暗号化用
乱散生成
F413
パラメータ提供用暗号鍵交換
F414
パラメータ受信

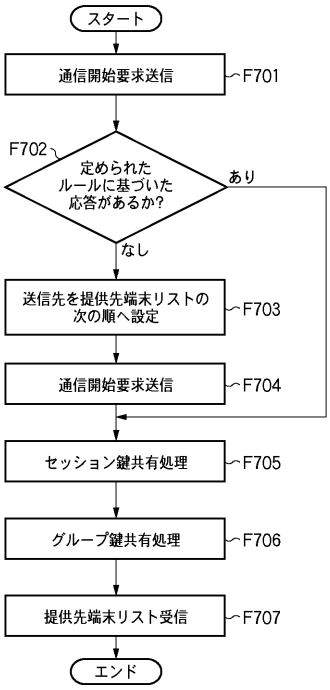
【図５】


端末B
端末A
端末C
F501
パラメータ提供方向決定処理
F502
受信端末に決定
F503
提供元端末に決定
F504
受信端末に決定
F505
通信開始要求
パラメータ設定開始手続き
F506
暗号・認証方式ネゴシエーション
F507
パラメータ提供用鍵
およびセッション鍵共有処理
F508
グループ鍵共有処理
F509
通信完了通知
F510
通信開始要求
F511
F512
パラメータ設定開始手続き
F513
暗号・認証方式ネゴシエーション
F514
パラメータ提供用鍵
およびセッション鍵共有処理
F515
グループ鍵共有処理
F516
通信完了通知
F517
グループ鍵共有処理

【図６】


スタート
通信開始要求受信
F601
処理識別要求送信
F602
F603
応答はパラメータ設定用か?
はい
いいえ
セッション鍵共有処理
F604
グループ鍵共有処理
F605
提供先端末リスト配布
F606
エンド
パラメータ設定処理実施
F607
提供先端末リスト更新
F608
グループ鍵共有処理
F609
提供先端末リスト配布
F610
エンド

【図７】


スタート
通信開始要求送信
F701
F702
定められたルールに基づいた応答があるか?
あり
なし
送信先を提供先端末リストの次の順へ設定
F703
通信開始要求送信
F704
セッション鍵共有処理
F705
グループ鍵共有処理
F706
提供先端末リスト受信
F707
エンド

フロントページの続き

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

審査官　北元　健太

(56)参考文献　特開２００７－２５１９２２（ＪＰ，Ａ）
遠藤資訓，これがホントの無線ＬＡＮだ！，NETWORK WORLD，日本，(株)ＩＤＧジャパン，２００５年　5月　1日，第10巻，第５号，pp.82－92
V. Varadharajan et al., Security for cluster based ad hoc networks, Computer Communications, Elsevier B.V., ２００４年　3月２０日，vol.27, no.5, pp.488－501

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　　４／００　－　９９／００
Ｈ０４Ｂ　　７／２４　－　　７／２６