(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2006-60578
(P2006-60578A)
(43)公開日　平成18年3月2日(2006.3.2)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/28	(2006.01)	H04L	12/28	300M	5K033
H04Q 7/38	(2006.01)	H04L	12/28	307	5K067
		H04B	7/26	109A	
		H04B	7/26	109R	

審査請求 未請求　請求項の数 7　OL　（全 12 頁）

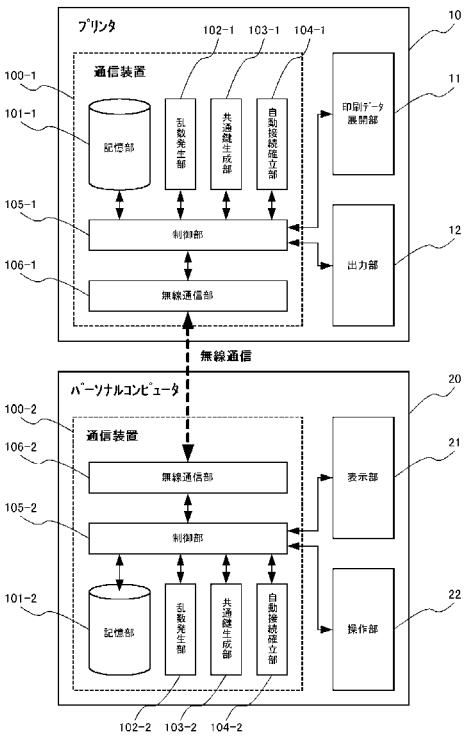
(21)出願番号　特願2004-241078 (P2004-241078)
(22)出願日　平成16年8月20日 (2004.8.20)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目１７番２２号
(74)代理人　100071054
弁理士　木村　高久
(72)発明者　石村　卓也
埼玉県岩槻市府内三丁目７番１号　富士ゼロックスプリンティングシステムズ株式会社内

Fターム(参考)　5K033 AA08 CC01 DA02 DA19 DB12 EC01
5K067 AA21 AA30 BB21 BB37 DD17 DD23 EE02 EE25 GG01 HH22 HH23 HH24 HH36 KK15

(54)【発明の名称】無線通信システムおよび通信装置および通信制御方法および通信制御プログラム

(57)【要約】
【課題】
無線ＬＡＮ独自設定を自動化できるようにした無線通信システムおよび通信装置および通信制御方法および通信制御プログラムを提供する。
【解決手段】
プリンタ１０およびパーソナルコンピュータ２０双方の自動接続確立部（１０４－１、１０４－２）が通信制御を行うことでセッションが確立する。まず、プリンタ１０から無線通信部１０６－１を介してＳＳＩＤが送出され、該ＳＳＩＤをパーソナルコンピュータ２０が無線通信部１０６－２にて受信し、その後数回のデータ授受が行われＪｏｉｎが確立すると、ＤＨ（Diffie-Hellman）鍵共有方式によりＷＥＰキーの生成および交換が行われ認証結果正常後、無線ＬＡＮ通信が開始される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
無線端末間でアクセスポイントを介さないアドホックネットワークを構築して通信を行う無線通信システムにおいて、
前記無線端末は、
通信相手先無線端末から定期的に発生されるビーコン信号を受信する受信手段と、
前記受信手段で受信したビーコン信号に含まれるネットワーク識別情報を抽出する抽出手段と、
前記抽出したネットワーク識別情報を自動設定する設定手段と、
前記設定手段で設定されたネットワーク識別情報を用いて前記通信相手先無線端末に通信要求を送信することでセッションを確立するセッション確立手段と
を具備することを特徴とする無線通信システム。
【請求項２】
前記無線端末と前記通信相手先無線端末は、
共通の素数と原始元を保持する保持手段と、
乱数発生手段と、
前記乱数発生手段で発生された乱数および前記保持手段に保持された素数と原始元を用いて前記無線端末と前記通信相手先無線端末との間で通信を行うことにより共通暗号鍵を生成する共通暗号鍵生成手段と
を具備することを特徴とする請求項１記載の無線通信システム。
【請求項３】
前記通信相手先無線端末は、
複数台の前記無線端末からの通信要求を受信した際に予め設定された情報に基づいて前記無線端末に対して選択的に通信許可信号を送信する通信調停手段
を具備することを特徴とする請求項１記載の無線通信システム。
【請求項４】
前記通信相手先無線端末は、
前記共通暗号鍵を通信要求をした無線端末の識別情報と対応して記憶する記憶手段
を更に具備し、
前記無線端末との再接続処理に際して、前記記憶手段に記憶された共通暗号鍵および識別情報を用いて接続を確立する
ことを特徴とする請求項１乃至３いずれかに記載の無線通信システム。
【請求項５】
無線端末間でアクセスポイントを介さないアドホックネットワークを構築して通信を行う通信装置において、
通信相手先無線端末から定期的に発生されるビーコン信号を受信する受信手段と、
前記受信手段で受信したビーコン信号に含まれるネットワーク識別情報を抽出する抽出手段と、
前記抽出したネットワーク識別情報を自動設定する設定手段と、
前記設定手段で設定されたネットワーク識別情報を用いて前記通信相手先無線端末に通信要求を送信することでセッションを確立するセッション確立手段と、
前記通信相手先無線端末と共通の素数と原始元を保持する保持手段と、
乱数発生手段と、
前記乱数発生手段で発生された乱数および前記保持手段に保持された素数と原始元を用いて前記通信相手先無線端末との間で通信を行うことにより共通暗号鍵を生成する共通暗号鍵生成手段と
を具備し、
前記セッション確立手段で確立したセッションで前記共通暗号鍵を用いて通信を行う
ことを特徴とする通信装置。
【請求項６】

無線端末間でアクセスポイントを介さないアドホックネットワークを構築して通信を行う通信制御方法において、
前記無線端末は、
通信相手先無線端末から定期的に発生されるビーコン信号を受信手段で受信し、
前記受信手段で受信したビーコン信号に含まれるネットワーク識別情報を抽出手段で抽出し、
前記抽出したネットワーク識別情報を設定手段で自動設定し、
前記設定手段で設定されたネットワーク識別情報を用いて前記通信相手先無線端末に通信要求を送信することでセッション確立手段でセッションを確立し、
前記無線端末間で共通の素数と原始元を保持手段で保持し、
乱数発生手段で発生された乱数および前記保持手段に保持された素数と原始元を用いて前記無線端末と前記通信相手先無線端末との間で通信を行うことにより共通暗号鍵を共通暗号鍵生成手段で生成し、
前記セッション確立手段で確立したセッションで前記共通暗号鍵を用いて通信を行う
ことを特徴とする通信制御方法。
【請求項７】
無線端末間でアクセスポイントを介さないアドホックネットワークを構築して通信を行う通信制御をコンピュータに実行させる通信制御プログラムであって、
通信相手先無線端末から定期的に発生されるビーコン信号を受信する受信ステップと、
前記受信ステップで受信したビーコン信号に含まれるネットワーク識別情報を抽出する抽出ステップと、
前記抽出したネットワーク識別情報を自動設定する設定ステップと、
前記設定ステップで設定されたネットワーク識別情報を用いて前記通信相手先無線端末に通信要求を送信することでセッションを確立するセッション確立ステップと、
前記無線端末間で共通の素数と原始元を保持する保持ステップと、
乱数発生ステップと、
前記乱数発生ステップで発生された乱数および前記保持手段に保持された素数と原始元を用いて前記無線端末と前記通信相手先無線端末との間で通信を行うことにより共通暗号鍵を生成する共通暗号鍵生成ステップと
を含み、
前記セッション確立ステップで確立したセッションで前記共通暗号鍵を用いて通信を行う
ことを特徴とする通信制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、中継機器（アクセスポイント）の介在なしに、無線端末（ステーション）同士で構成される接続形態（アドホックネットワーク）において、データの授受を行う無線通信システムおよび通信装置および通信制御方法および通信制御プログラムに係わり、詳しくは、無線ＬＡＮ独自設定を自動化できるようにした無線通信システムおよび通信装置および通信制御方法および通信制御プログラムに関する。
【背景技術】
【０００２】
近年、ＰＣ（Personal Computer）、ＰＤＡ（Personal Digital Assistance）、プリンタなど複数の端末を無線接続し、ＬＡＮ（Local Area Network）を構築する技術として無線ＬＡＮが知られている。その規格の一つにＩＥＥＥ８０２．１１（IEEE802.11a/b/g）がある。
【０００３】
このＩＥＥＥ８０２．１１規格で無線ＬＡＮを構成する最も基本的な構成要素には、無線端末（ステーション）のみで構成されるアドホックネットワークと、中継機器（アクセ

スポイント）を介してステーション同士や有線ＬＡＮ上の機器と通信を行うインフラストラクチャネットワークとがある。

【０００４】

無線ＬＡＮ接続する場合、認証にはＳＳＩＤ（Service Set Identifier）、暗号にはＷＥＰ（Wired Equivalent Privacy）など無線ＬＡＮ独自の設定を事前に実施する必要がある。

【０００５】

これら特別な設定操作を必要とすることなく、無線ＬＡＮ接続するための設定を自動的に実行する技術として特許文献１の「通信装置および方法、記録媒体、並びにプログラム」が開示されている。

【０００６】

この特許文献１の発明は、ステーションがＩＣ（Integrated Circuit）カードに記録されているローカルネットワーク情報を読み出し、該情報に従いネットワーク設定を実行することで、ユーザによる特別な設定操作を必要とすることなく、無線接続のための設定を自動的に行うことができるといった技術について言及されている。

【特許文献１】特開２００３－１２９８７２号

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、特許文献１の発明は、ネットワーク設定を記憶しておくＩＣカードなどの記録媒体や、該ＩＣカードから設定の読み出しを行う読出装置を備える必要があるという問題があった。

【０００８】

ところで従来、無線ＬＡＮで構成したネットワークにおいては、煩わしいケーブルの呪縛がない（ケーブルレス）、端末の設置や移動が自由などといった利点がある反面、設定操作が煩雑であるという点やセキュリティの脆弱性が問題となっていた。

【０００９】

そして、無線ＬＡＮのセキュリティを強化する機能としては大きく（ａ）アクセス制御、（ｂ）データの暗号化の２種類が挙げられる。

【００１０】

例えば前者（ａ）には、ＭＡＣ（Media Access Control）アドレスフィルタリング機能、ＲＡＤＩＵＳ（Remote Authentication Dial-In User Service）サーバによるユーザ認証機能などがあるが、ＭＡＣアドレス登録の場合は、ＭＡＣアドレスは無線のフレーム上に平文で記載されているため、ツールを用いて簡単に取得できてしまいなりすましが可能になる。

【００１１】

また、ＲＡＤＩＵＳサーバを用いた場合は、アクセスポイントに接続してきたユーザをＲＡＤＩＵＳサーバが認証し、アクセスの可否を判断するといったものなので、アドホックネットワークには適用できない。

【００１２】

一方、後者（ｂ）には、ＷＥＰによる暗号化などがあるが、ＷＥＰはＲＣ４（Ron’s Code 4）という暗号化アルゴリズムを採用しており、データの秘匿、改竄・偽造・なりすましの防止などの機能を持っている。しかしながら、ＷＥＰキーが手動で設定された後、変更されなければ、全てのステーションが同じキーを使用して接続と認証を繰り返すことになるため、悪意のあるユーザがＷＥＰキーを不正に入手し、暗号解読法を駆使してＷＥＰキーを盗用する可能性がある。

【００１３】

この他、ＩＰｓｅｃ（IP Security）などで通信時のＩＰパケットを暗号化するといった方法も挙げられるが、この場合ステーションの処理負荷が増えるという問題がある。

【００１４】

そこで、本発明は上記問題点に鑑みてなされたものであり、無線ＬＡＮ独自設定をセッション確立時にステーション同士で自動的に行う無線通信システムおよび通信装置および通信制御方法および通信制御プログラム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】

【００１５】

上記目的を達成するため、請求項１の発明は、無線端末間でアクセスポイントを介さないアドホックネットワークを構築して通信を行う無線通信システムにおいて、前記無線端末は、通信相手先無線端末から定期的に発生されるビーコン信号を受信する受信手段と、前記受信手段で受信したビーコン信号に含まれるネットワーク識別情報を抽出する抽出手段と、前記抽出したネットワーク識別情報を自動設定する設定手段と、前記設定手段で設定されたネットワーク識別情報を用いて前記通信相手先無線端末に通信要求を送信することでセッションを確立するセッション確立手段とを具備することを特徴とする。

【００１６】

また、請求項２の発明は、請求項１の発明において、前記無線端末と前記通信相手先無線端末は、共通の素数と原始元を保持する保持手段と、乱数発生手段と、前記乱数発生手段で発生された乱数および前記保持手段に保持された素数と原始元を用いて前記無線端末と前記通信相手先無線端末との間で通信を行うことにより共通暗号鍵を生成する共通暗号鍵生成手段とを具備することを特徴とする。

【００１７】

また、請求項３の発明は、請求項１の発明において、前記通信相手先無線端末は、複数台の前記無線端末からの通信要求を受信した際に予め設定された情報に基づいて前記無線端末に対して選択的に通信許可信号を送信する通信調停手段を具備することを特徴とする。

【００１８】

また、請求項４の発明は、請求項１乃至３の発明において、前記通信相手先無線端末は、前記共通暗号鍵を通信要求をした無線端末の識別情報と対応して記憶する記憶手段を更に具備し、前記無線端末との再接続処理に際して、前記記憶手段に記憶された共通暗号鍵および識別情報を用いて接続を確立することを特徴とする。

【００１９】

また、請求項５の発明は、無線端末間でアクセスポイントを介さないアドホックネットワークを構築して通信を行う通信装置において、通信相手先無線端末から定期的に発生されるビーコン信号を受信する受信手段と、前記受信手段で受信したビーコン信号に含まれるネットワーク識別情報を抽出する抽出手段と、前記抽出したネットワーク識別情報を自動設定する設定手段と、前記設定手段で設定されたネットワーク識別情報を用いて前記通信相手先無線端末に通信要求を送信することでセッションを確立するセッション確立手段と、前記通信相手先無線端末と共通の素数と原始元を保持する保持手段と、乱数発生手段と、前記乱数発生手段で発生された乱数および前記保持手段に保持された素数と原始元を用いて前記通信相手先無線端末との間で通信を行うことにより共通暗号鍵を生成する共通暗号鍵生成手段とを具備し、前記セッション確立手段で確立したセッションで前記共通暗号鍵を用いて通信を行うことを特徴とする。

【００２０】

また、請求項６の発明は、無線端末間でアクセスポイントを介さないアドホックネットワークを構築して通信を行う通信制御方法において、前記無線端末は、通信相手先無線端末から定期的に発生されるビーコン信号を受信手段で受信し、前記受信手段で受信したビーコン信号に含まれるネットワーク識別情報を抽出手段で抽出し、前記抽出したネットワーク識別情報を設定手段で自動設定し、前記設定手段で設定されたネットワーク識別情報を用いて前記通信相手先無線端末に通信要求を送信することでセッション確立手段でセッションを確立し、前記無線端末間で共通の素数と原始元を保持手段で保持し、乱数発生手段で発生された乱数および前記保持手段に保持された素数と原始元を用いて前記無線端末と前記通信相手先無線端末との間で通信を行うことにより共通暗号鍵を共通暗号鍵生成手

段で生成し、前記セッション確立手段で確立したセッションで前記共通暗号鍵を用いて通信を行うことを特徴とする。

【００２１】

また、請求項７の発明は、無線端末間でアクセスポイントを介さないアドホックネットワークを構築して通信を行う通信制御をコンピュータに実行させる通信制御プログラムであって、通信相手先無線端末から定期的に発生されるビーコン信号を受信する受信ステップと、前記受信ステップで受信したビーコン信号に含まれるネットワーク識別情報を抽出する抽出ステップと、前記抽出したネットワーク識別情報を自動設定する設定ステップと、前記設定ステップで設定されたネットワーク識別情報を用いて前記通信相手先無線端末に通信要求を送信することでセッションを確立するセッション確立ステップと、前記無線端末間で共通の素数と原始元を保持する保持ステップと、乱数発生ステップと、前記乱数発生ステップで発生された乱数および前記保持手段に保持された素数と原始元を用いて前記無線端末と前記通信相手先無線端末との間で通信を行うことにより共通暗号鍵を生成する共通暗号鍵生成ステップとを含み、前記セッション確立ステップで確立したセッションで前記共通暗号鍵を用いて通信を行うことを特徴とする。

【発明の効果】

【００２２】

本発明によれば、無線ＬＡＮ通信を行うためのＳＳＩＤ設定やＷＥＰキー設定などの無線ＬＡＮ独自の設定をセッション確立時にステーション同士で自動的に行うように構成したため、無線ＬＡＮ設定時における煩雑な操作が必要無くなる。

【００２３】

また、無線ＬＡＮ経路上に暗号鍵が流れることなく安全に暗号鍵を共有することができるので、セキュリティが向上する。

【発明を実施するための最良の形態】

【００２４】

以下、この発明に係わる無線通信システムおよび通信装置および通信制御方法および通信制御プログラムの実施例について添付図面を参照して詳細に説明する。

【実施例１】

【００２５】

図１は、本発明に係わる実施形態の一実施例を示す図であり、本発明に係わる通信装置を適用したプリンタ１０およびパーソナルコンピュータ２０の内部構成を示す図である。

【００２６】

同図に示されるプリンタ１０およびパーソナルコンピュータ２０は、アクセスポイントを介さずに機器同士が直接無線通信を行なう。いわゆる、アドホックモードによる通信が可能であり、それぞれ本発明に係わる通信装置１００が内部に設けられている。

【００２７】

この通信装置１００の通信制御によりプリンタ１０とパーソナルコンピュータ２０間の通信はＩＥＥＥ８０２．１１規格に準拠した無線ＬＡＮ通信を行う。なお、本発明においては、無線通信時におけるＷＥＰによる暗号化処理に際して、その暗号鍵となるＷＥＰキーの生成および交換処理にＤＨ（Diffie-Hellman）鍵共有方式を採用する。

【００２８】

プリンタ１０は、パーソナルコンピュータ２０と無線通信を行うことが可能で、パーソナルコンピュータ２０から印刷指示を受け付けると、該印刷指示に基づき印刷処理を行う。また、プリンタ１０は内部に通信装置１００－１と、パーソナルコンピュータ２０から送信される印刷指示に含まれる印刷データを解釈しデータ展開する印刷データ展開部１１と、該印刷データ展開部１１において展開されたデータを出力する出力部１２とを具備して構成される。

【００２９】

パーソナルコンピュータ２０は、液晶ディスプレィ等の表示用デバイスと、キーボードおよびマウス等の入力用デバイスを備えており、表示用デバイスに表示された無線接続可

能ステーションを入力デバイスにより選択するといった操作が行える。また、パーソナルコンピュータ２０は内部に通信装置１００－２と、上述した表示デバイスにあたる表示部２１と、上述した入力デバイスにあたる操作部２２とを具備して構成される。

【００３０】

ここで、プリンタ１０およびパーソナルコンピュータ２０に設置される通信装置１００について説明する。なお、通信装置１００－１および通信装置１００－２は、設定状況等により動作的な相違は多少あるものの、その他の点においては略同一の機能を有する通信装置１００である。

【００３１】

通信装置１００は各種処理機能部として、ＤＨ鍵共有方式による暗号鍵生成に際して使用する素数Ｐおよび原始元ｇを記憶する記憶部１０１と、ＤＨ鍵共有方式による暗号鍵生成に際して使用する乱数を発生する乱数発生部１０２と、上記乱数発生部１０２から取得した情報に基づきＤＨ鍵共有方式により暗号鍵を生成する共通鍵生成部１０３と、事前に設定されたＳＳＩＤ（ネットワーク識別情報）等を用いて自動で無線ＬＡＮ接続を確立する自動接続確立部１０４と、通信装置１００を統括制御する制御部１０５と、無線で他装置との通信を可能とするインターフェース装置である無線通信部１０６とを具備して構成される。

【００３２】

上述した記憶部１０１で記憶する素数Ｐおよび原始元ｇはプリンタ１０およびパーソナルコンピュータ２０で共通の値にする。以上が本発明に係わるプリンタ１０およびパーソナルコンピュータ２０の内部構成である。

【００３３】

図２は、図１に示したプリンタ１０およびパーソナルコンピュータ２０における通信制御方法の動作を説明するシーケンスチャート図である。

【００３４】

上述したプリンタ１０およびパーソナルコンピュータ２０間の接続確立は、Ｂｅａｃｏｎ、ＰｒｏｂｅＲｅｓｐｏｎｓｅパケットの受け渡しにより実施される。まず、プリンタ１０の自動接続確立部１０４－１が無線通信部１０６－１を介してＢｅａｃｏｎパケットを定期的に送出する（ステップＳ１０１）。このＢｅａｃｏｎパケットは図３に示すようにＳＳＩＤを含む情報から構成されている。このＳＳＩＤは、記憶部１０１－１において事前に保持される。

【００３５】

一方、パーソナルコンピュータ２０はＢｅａｃｏｎパケット受信待ち状態であり、プリンタ１０から送出されたＢｅａｃｏｎパケットを無線通信部１０６－２にて受信した場合には（ステップＳ１０２）、受信したＢｅａｃｏｎパケットから自動接続確立部１０４－２にてＳＳＩＤを抽出するとともに（ステップＳ１０３）、ＰｒｏｂｅＲｅｓｐｏｎｓｅを生成し送信する（ステップＳ１０４）。このとき、複数のステーションからＢｅａｃｏｎパケットが送出されていた場合は、事前に登録した優先情報に従った自動選択、電波強度の強いステーションが優先される自動選択、または表示用デバイスに無線接続可能端末を表示し手動による選択などが挙げられる。

【００３６】

パーソナルコンピュータ２０からのＰｒｏｂｅＲｅｓｐｏｎｓｅを無線通信部１０６－１にて受信したプリンタ１０は、自動接続確立部１０４－１において自装置への接続要求と認識すると、パーソナルコンピュータ２０との通信を受け付け（ステップＳ１０５）、無線通信部１０６－１を介して通信可能のＡｃｋｏｎｗｌｅｄｇｅを返信する（ステップＳ１０６）。そして、パーソナルコンピュータ２０は無線通信部１０６－２を介してＡｃｋｏｎｗｌｅｄｇｅを受信する（ステップＳ１０７）。これにより、プリンタ１０およびパーソナルコンピュータ２０間のＪｏｉｎが確立する。

【００３７】

上述したステップＳ１０７までの処理がＪｏｉｎ確立処理であり、ステップＳ１０８以

降の処理で共通暗号鍵生成処理を説明する。

【００３８】

Ｊｏｉｎが確立すると、パーソナルコンピュータ２０の乱数発生部１０２－２において、乱数Ｘを生成する（ステップＳ１０８）。その結果を受けて共通鍵生成部１０３－２は、乱数Ｘと記憶部１０１－２より取り出した素数Ｐと原始元ｇとを用いて計算式「ａ＝ｇ＾Ｘ（ｍｏｄ　Ｐ）」を計算する（ステップＳ１０９）。そして、パーソナルコンピュータ２０の自動接続確立部１０４－２が無線通信部１０６－２を介して、計算の結果得られた値ａをプリンタ１０へと送信する（ステップＳ１１０）。

【００３９】

一方、プリンタ１０は無線通信部１０６－１を介して値ａを受信すると（ステップＳ１１１）、パーソナルコンピュータ２０と同様に乱数発生部１０２－１において、乱数Ｙを生成する（ステップＳ１１２）。その結果を受けて共通鍵生成部１０３－１は、乱数Ｙと記憶部１０１－１より取り出した素数Ｐと原始元ｇとを用いて計算式「ｂ＝ｇ＾Ｙ（ｍｏｄ　Ｐ）」を計算する（ステップＳ１１３）。そして、プリンタ１０の自動接続確立部１０４－１が無線通信部１０６－１を介して、計算の結果得られた値ｂをパーソナルコンピュータ２０へと送信する（ステップＳ１１４）。

【００４０】

続いて、プリンタ１０は、共通鍵生成部１０３－１で上記値を用いて計算式「ａ＾Ｙ（ｍｏｄ　Ｐ）」若しくは「ｇ＾（ＸＹ）（ｍｏｄ　Ｐ）」を計算することで共通暗号鍵を生成する（ステップＳ１１５）。

【００４１】

また、パーソナルコンピュータ２０は無線通信部１０６－２を介して値ｂを受信すると（ステップＳ１１６）、共通鍵生成部１０３－２で上記値を用いて計算式「ｂ＾Ｘ（ｍｏｄ　Ｐ）」若しくは「ｇ＾（ＸＹ）（ｍｏｄ　Ｐ）」を計算することで共通暗号鍵を生成する（ステップＳ１１７）。

【００４２】

なお、計算式「ａ＾Ｙ（ｍｏｄ　Ｐ）」および「ｂ＾Ｘ（ｍｏｄ　Ｐ）」および「ｇ＾（ＸＹ）（ｍｏｄ　Ｐ）」は同一の計算結果が得られる。

【００４３】

上述したステップＳ１１７までの処理が共通暗号鍵生成処理であり、上記説明したようにＤＨ鍵共有方式により暗号鍵を生成するため、無線ＬＡＮ経路上に暗号鍵が流れることなく安全に暗号鍵を共有することができるので、セキュリティが向上する。

【００４４】

上述した共通暗号鍵生成処理が終了すると、次に認証処理を行う（ステップＳ１１８）。具体的には、上述した共通暗号鍵生成処理で生成された共通暗号鍵を用いて、プリンタ１０およびパーソナルコンピュータ２０それぞれの制御部１０５がＳＳＩＤ等を含む認証情報の暗号化を行う。そして、自動接続確立部１０４がその暗号化された認証情報のやり取りを行うことで認証処理が行われる。

【００４５】

認証結果正常の場合には、プリンタ１０とパーソナルコンピュータ２０間での無線通信が開始され、例えば、パーソナルコンピュータ２０からプリンタ１０へ印刷指示が行われるなどして、一連の通信処理（セッション）が行われる（ステップＳ１１９）。該セッションが終了すると（ステップＳ１２０）、プリンタ１０は、ＳＳＩＤを含むＢｅａｃｏｎの送出を再び開始する。

【００４６】

以上説明したように本発明においては、無線ＬＡＮ通信を行うための認証処理におけるＳＳＩＤ設定や暗号化処理におけるＷＥＰキー設定などの無線ＬＡＮ独自の設定をセッション確立時にステーション同士で自動的に行うように構成したため、無線ＬＡＮ設定時における煩雑な操作が必要無くなる。

【００４７】

また、無線ＬＡＮ経路上に暗号鍵が流れることなく安全に暗号鍵を共有することができるので、セキュリティが向上する。

【００４８】

なお、上記実施例においては、本発明をアドホックネットワークに適用した場合を説明したが、これに限られず、中継機器（アクセスポイント）を介して接続されるインフラストラクチャネットワークに適用してもよい。

【実施例２】

【００４９】

上記実施例１では、プリンタ１０とパーソナルコンピュータ２０がピアツーピア（peer to peer）で接続されている場合を説明したが、実施例２においては、プリンタ１０を複数台のステーション（パーソナルコンピュータ２０）で共有して使用する場合の実施形態について説明する。

【００５０】

図４は、本発明に係わる通信装置１００を適用したプリンタ１０および複数台のパーソナルコンピュータ（２０ａ、２０ｂ：以下、２０と総称する）で構成した無線ＬＡＮネットワークの全体構成を示す図である。なお、実施例１を説明した上記図１に示したものと同じ符号のものは略同様に動作し内部構成も同一であるため、その説明は省略する。パーソナルコンピュータ２０ａおよびパーソナルコンピュータ２０ｂは実施例１を説明した上記図１のパーソナルコンピュータ２０と同一のものである。

【００５１】

図５は、図４に示したプリンタ１０およびパーソナルコンピュータ２０における通信制御方法の動作を説明するシーケンスチャート図である。なお、ここでは、パーソナルコンピュータ２０ａの各処理機能部については、符号の最後に「－２」を付加し、パーソナルコンピュータ２０ｂの各処理機能部については、符号の最後に「－３」を付加して説明する。例えば、パーソナルコンピュータ２０ａの制御部は、１０５－２で示し、パーソナルコンピュータ２０ｂの制御部は１０５－３で示す。

【００５２】

上述したプリンタ１０およびパーソナルコンピュータ２０間の接続確立は、Ｂｅａｃｏｎ、ＰｒｏｂｅＲｅｓｐｏｎｓｅパケットの受け渡しにより実施される。まず、プリンタ１０の自動接続確立部１０４－１が無線通信部１０６－１を介してＢｅａｃｏｎパケットを定期的に送出する（ステップＳ２０１）。このＢｅａｃｏｎパケットは図３に示すようにＳＳＩＤを含む情報から構成されている。このＳＳＩＤは、記憶部１０１－１において事前に保持される。

【００５３】

一方、パーソナルコンピュータ２０ｂはＢｅａｃｏｎパケット受信待ち状態であり、プリンタ１０から送出されたＢｅａｃｏｎパケットを無線通信部１０６－３にて受信した場合には（ステップＳ２０２）、受信したＢｅａｃｏｎパケットから自動接続確立部１０４－３にてＳＳＩＤを抽出するとともに（ステップＳ２０３）、ＰｒｏｂｅＲｅｓｐｏｎｓｅを生成し送信する（ステップＳ２０４）。このとき、複数のステーションからＢｅａｃｏｎパケットが送出されていた場合は、事前に登録した優先情報に従った自動選択、電波強度の強いステーションが優先される自動選択、または表示用デバイスに無線接続可能端末を表示し手動による選択などが挙げられる。

【００５４】

パーソナルコンピュータ２０ｂからのＰｒｏｂｅＲｅｓｐｏｎｓｅを無線通信部１０６－１にて受信したプリンタ１０は、自動接続確立部１０４－１において自装置への接続要求と認識すると、パーソナルコンピュータ２０ｂとの通信を受け付け（ステップＳ２０５）、Ｂｅａｃｏｎパケットの送出を停止するとともに（ステップＳ２０６）、無線通信部１０６－１を介して通信可能のＡｃｋｏｎｗｌｅｄｇｅを返信する（ステップＳ２０７）。そして、パーソナルコンピュータ２０ｂは無線通信部１０６－３を介してＡｃｋｏｎｗｌｅｄｇｅを受信する（ステップＳ２０８）。これにより、プリンタ１０およびパーソナ

ルコンピュータ２０ｂ間のＪｏｉｎが確立する。

【００５５】

また、パーソナルコンピュータ２０ａも同様に、プリンタ１０からＢｅａｃｏｎパケットを無線通信部１０６－２にて受信し（ステップＳ２１２）、受信したＢｅａｃｏｎパケットから自動接続確立部１０４－２にてＳＳＩＤを抽出するとともに（ステップＳ２１３）、ＰｒｏｂｅＲｅｓｐｏｎｓｅを生成し送信するが（ステップＳ２１４）、プリンタ１０においては、既にパーソナルコンピュータ２０ｂとＪｏｉｎを確立しているため、このＰｒｏｂｅＲｅｓｐｏｎｓｅを無視する。さらに、プリンタ１０は、Ｂｅａｃｏｎパケットの送出も停止するため、パーソナルコンピュータ２０ａとはＪｏｉｎの確立を行えない状態になる。これにより、他装置による割り込み処理を禁止することができる。すなわち、パーソナルコンピュータ２０ａを通信待ち状態とすることができる。

【００５６】

Ｊｏｉｎが確立したプリンタ１０およびパーソナルコンピュータ２０ｂ間では、上記実施例１で説明した処理と同様の共有暗号鍵生成処理（ステップＳ２０９）および認証処理（ステップＳ２１０）が行われ、認証結果正常の場合には、パーソナルコンピュータ２０ｂの制御部１０５－３が共有暗号鍵生成処理で生成された共通暗号鍵を用いてＭＡＣアドレスの暗号化を行い、無線通信部１０６－３を介してプリンタ１０へと送信する（ステップＳ２１１）。そして、暗号化されたＭＡＣアドレスを無線通信部１０６－１を介して受信したプリンタ１０は、制御部１０５－１において共通暗号鍵を用いて復号化するとともに（ステップＳ２１２）、記憶部１０１－２に共通暗号鍵とＭＡＣアドレスを関連付けてセッション情報として登録する（ステップＳ２１３）。このセッション情報は、一連のセッションが終了し、再び、プリンタ１０およびパーソナルコンピュータ２０ｂ間で通信を開始する際に使用されるもので、このセッション情報を使うことで通信開始が容易となる。

【００５７】

セッション情報の登録処理後、例えば、パーソナルコンピュータ２０ｂからプリンタ１０へ印刷指示が行われるなどして、一連の通信処理（セッション）が行われ（ステップＳ２１４）、該セッションが終了すると（ステップＳ２１５）、プリンタ１０は、ＳＳＩＤを含むＢｅａｃｏｎの送出を再び開始する（ステップＳ２１６）。

【００５８】

ここで、Ｂｅａｃｏｎパケット受信待ち状態のパーソナルコンピュータ２０ａは、プリンタ１０から送出されたＢｅａｃｏｎパケットを無線通信部１０６－２にて受信し、Ｊｏｉｎ確立などの所定の処理を経て接続確立後、一連の通信処理が終了すると（ステップＳ２１８）、プリンタ１０は再び、Ｂｅａｃｏｎの送出を行う。

【００５９】

上述したように実施例２においては、複数台のステーション（パーソナルコンピュータ２０）から特定のステーション（プリンタ１０）に対して同時に通信要求が行われても、プリンタ１０にアービトレーション機能を組み込むことで最適な通信順序を提供できる。

【００６０】

なお、上記実施例２で説明したプリンタ１０のアービトレーション機能の優先順位は、事前に登録した優先情報に従った自動選択、電波強度の強いステーションが優先される自動選択、または表示用デバイスに無線接続可能端末を表示し手動による選択などが挙げられるが、これに限られず、最適な通信順序を提供できるのであれば特に方法は問わない。

【００６１】

また、上記実施例１および上記実施例２においては、本発明に係わる通信装置をプリンタ１０およびパーソナルコンピュータ２０に適用することにより実施する場合を説明したが、上記説明した通信制御処理をコンピュータにインストールされた通信制御プログラムにより実行するように構成してもよい。

【００６２】

この他、本発明は、上記および図面に示す実施例に限定することなく、その要旨を変更

しない範囲内で適宜変形して実施できるものである。例えば、本発明に係わる通信装置をパーソナルコンピュータ、プリンタ以外にも適用できることはいうまでもない。

【産業上の利用可能性】

【００６３】

本発明の無線通信システムおよび通信装置および通信制御方法および通信制御プログラムは、アドホックネットワークにおいて通信を行う通信装置全般に適用可能であり、特に、無線ＬＡＮ独自設定を自動化したため、モバイル端末などを出先で有効に利用することができる。

【図面の簡単な説明】

【００６４】

【図１】本発明に係わる通信装置を適用したパーソナルコンピュータ２０およびプリンタ１０の内部構成を示す図である。

【図２】図１に示したパーソナルコンピュータ２０およびプリンタ１０における通信制御方法の動作を説明するシーケンスチャート図である。

【図３】Ｂｅａｃｏｎパケットの構成内容の一例を示す図である。

【図４】実施例２おける本発明に係わる全体構成を示す図である。

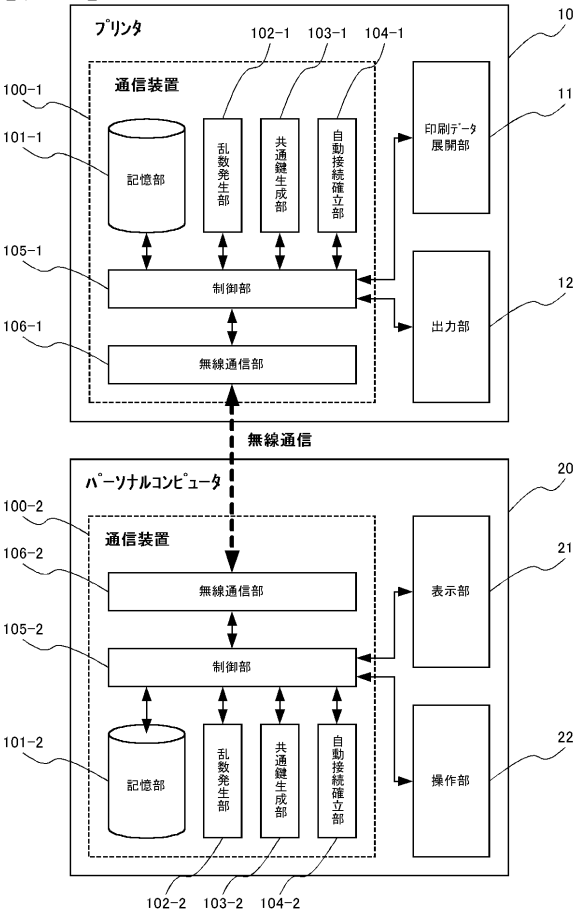
【図５】実施例２における通信制御方法の動作を説明するシーケンスチャート図である。

【符号の説明】

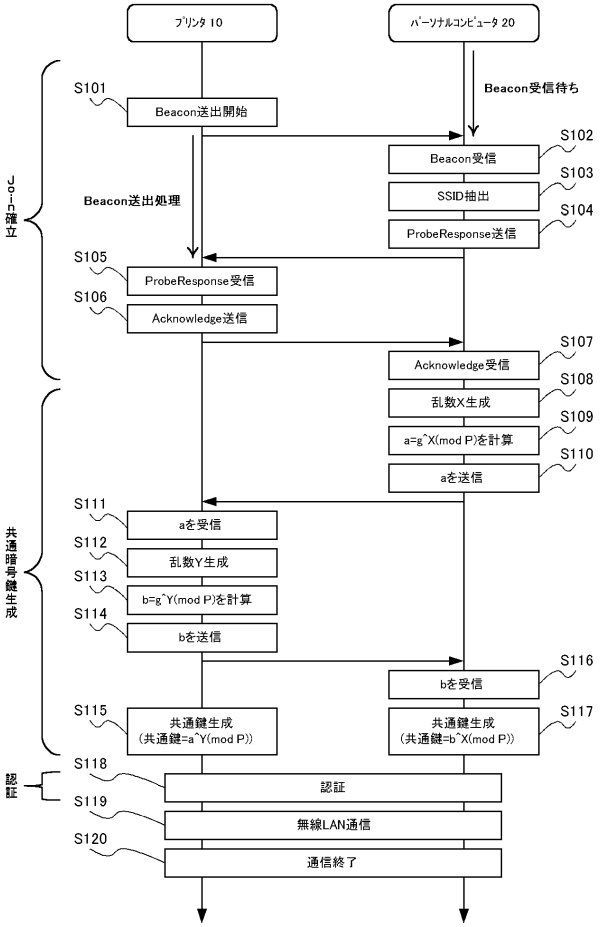
【００６５】

１０　プリンタ
１１　印刷データ展開部
１２　出力部
２０　パーソナルコンピュータ
２１　表示部
２２　操作部
１００　通信装置
１０１　記憶部
１０２　乱数発生部
１０３　共通鍵生成部
１０４　自動接続確立部
１０５　制御部
１０６　無線通信部

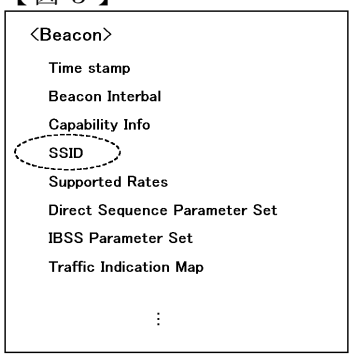
【図１】


プリンタ
10
102-1
103-1
104-1
通信装置
100-1
101-1
記憶部
乱数発生部
共通鍵生成部
自動接続確立部
印刷データ展開部
11
105-1
制御部
出力部
12
106-1
無線通信部
無線通信
パーソナルコンピュータ
20
100-2
通信装置
106-2
無線通信部
表示部
21
105-2
制御部
101-2
記憶部
乱数発生部
共通鍵生成部
自動接続確立部
操作部
22
102-2
103-2
104-2

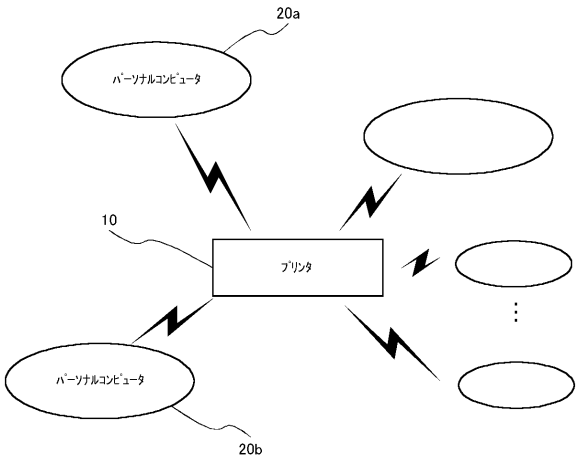
【図２】


プリンタ 10
パーソナルコンピュータ 20
Beacon受信待ち
S101
Beacon送出開始
S102
Beacon受信
S103
SSID抽出
S104
ProbeResponse送信
Beacon送出処理
Join確立
S105
ProbeResponse受信
S106
Acknowledge送信
S107
Acknowledge受信
S108
乱数X生成
S109
a=g^X(mod P)を計算
S110
aを送信
共通暗号鍵生成
S111
aを受信
S112
乱数Y生成
S113
b=g^Y(mod P)を計算
S114
bを送信
S116
bを受信
S115
共通鍵生成
(共通鍵=a^Y(mod P))
S117
共通鍵生成
(共通鍵=b^X(mod P))
認証
S118
認証
S119
無線LAN通信
S120
通信終了

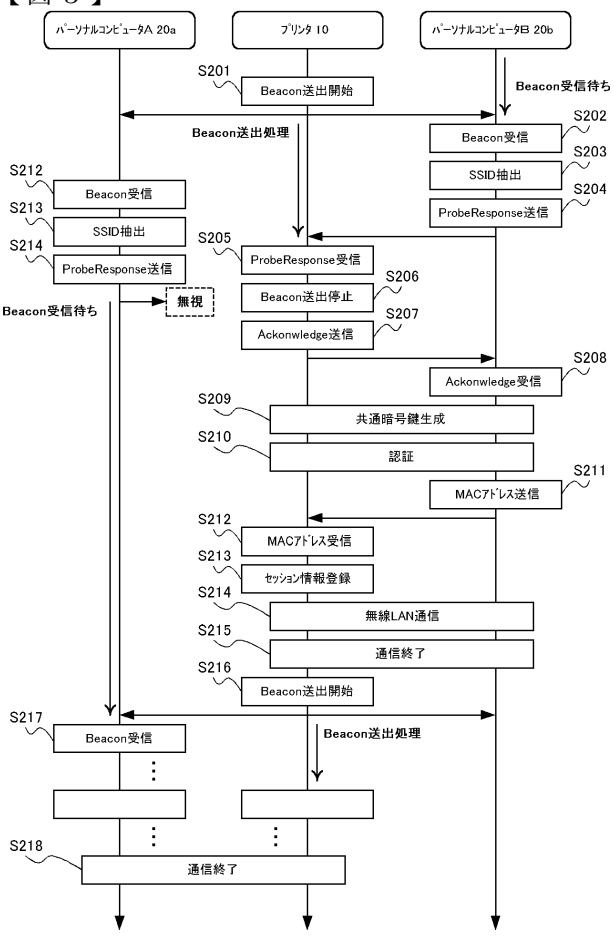
【図３】


<Beacon>
Time stamp
Beacon Interbal
Capability Info
SSID
Supported Rates
Direct Sequence Parameter Set
IBSS Parameter Set
Traffic Indication Map
⋮

【図４】


20a
パーソナルコンピュータ
10
プリンタ
パーソナルコンピュータ
20b

【図５】


パーソナルコンピュータA 20a
プリンタ 10
パーソナルコンピュータB 20b
Beacon受信待ち
S201
Beacon送出開始
Beacon送出処理
S202
Beacon受信
S203
SSID抽出
S204
ProbeResponse送信
S212
Beacon受信
S213
SSID抽出
S214
ProbeResponse送信
S205
ProbeResponse受信
S206
Beacon送出停止
Beacon受信待ち
無視
S207
Ackonwledge送信
S208
Ackonwledge受信
S209
共通暗号鍵生成
S210
認証
S211
MACアドレス送信
S212
MACアドレス受信
S213
セッション情報登録
S214
無線LAN通信
S215
通信終了
S216
Beacon送出開始
S217
Beacon受信
Beacon送出処理
S218
通信終了