(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3870081号
(P3870081)
(45)発行日　平成19年1月17日(2007.1.17)　(24)登録日　平成18年10月20日(2006.10.20)

(51)Int.Cl.		F I		
H04L 12/28	(2006.01)	H04L	12/28	300Z
G06F 13/00	(2006.01)	G06F	13/00	510A
G06F 21/20	(2006.01)	G06F	15/00	330C

請求項の数 8　(全 11 頁)

(21)出願番号　特願2001-385869(P2001-385869)
(22)出願日　平成13年12月19日(2001.12.19)
(65)公開番号　特開2003-188885(P2003-188885A)
(43)公開日　平成15年7月4日(2003.7.4)
審査請求日　平成16年4月16日(2004.4.16)

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　100090538
弁理士　西山　恵三
(74)代理人　100096965
弁理士　内尾　裕一
(72)発明者　荒井　俊次
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　矢頭　尚之

最終頁に続く

(54)【発明の名称】通信システム及びサーバ装置、ならびに制御方法及びそれを実施するためのコンピュータプログラム、該コンピュータプログラムを格納する記憶媒体

(57)【特許請求の範囲】

【請求項１】

クライアント装置を接続する複数のアクセスポイントと、サーバ装置を有する通信システムにおいて、

前記サーバ装置は、

第１のアクセスポイントに接続するクライアント装置を認証する認証手段と、

前記認証手段による認証結果に応じて、前記クライアント装置が接続する前記第１のアクセスポイントに暗号キーを通知する通知手段と、

第２のアクセスポイントから通知されたクライアント装置の識別情報に基づいて、前記クライアント装置は既に認証済みか否かを判別する判別手段と、を有し、

前記通知手段は、前記判別手段により前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、上記第１のアクセスポイントに上記暗号化キーを消去するよう指示することを特徴とする通信システム。

【請求項２】

サーバ装置において、

第１のアクセスポイントに接続するクライアント装置を認証する認証手段と、

前記認証手段による認証結果に応じて、前記クライアント装置が接続する前記第１のアクセスポイントに暗号キーを通知する通知手段と、

第２のアクセスポイントから通知されたクライアント装置の識別情報に基づいて、前記

クライアント装置は既に認証済みか否かを判別する判別手段と、を有し、
前記通知手段は、前記判別手段により前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、上記第１のアクセスポイントに上記暗号化キーを消去するよう指示することを特徴とするサーバ装置。
【請求項３】
前記認証手段による認証結果に応じて、前記第１のアクセスポイントと前記クライアント装置間の通信に暗号通信に使われる暗号化キーを生成する生成手段を有し、
上記通知手段が上記第２のアクセスポイントに通知する暗号化キーは、上記生成手段により暗号化キーを生成した際に記憶した暗号化キー、もしくは、上記第１のアクセスポイントから受信した暗号化キーであることを特徴とする請求項２に記載のサーバ装置。
【請求項４】
前記通知手段は、前記判別手段により前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、前記判別手段により前記クライアント装置は未承認であると判別されると、新規の暗号化キーを前記第２のアクセスポイントに通知することを特徴とする請求項２に記載のサーバ装置。
【請求項５】
クライアント装置を接続する複数のアクセスポイントと、サーバ装置を有する通信システムの制御方法において、
前記サーバ装置は、
第１のアクセスポイントに接続するクライアント装置を認証する認証工程と、
前記認証工程における認証結果に応じて、前記クライアント装置が接続する前記第１のアクセスポイントに暗号キーを通知する通知工程と、
第２のアクセスポイントから通知されたクライアント装置の識別情報に基づいて、前記クライアント装置は既に認証済みか否かを判別する判別工程と、を有し、
前記通知工程では、前記判別工程において前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、上記第１のアクセスポイントに上記暗号化キーを消去するよう指示することを特徴とする通信システムの制御方法。
【請求項６】
サーバ装置の制御方法において、
第１のアクセスポイントに接続するクライアント装置を認証する認証工程と、
前記認証工程における認証結果に応じて、前記クライアント装置が接続する前記第１のアクセスポイントに暗号キーを通知する通知工程と、
第２のアクセスポイントから通知されたクライアント装置の識別情報に基づいて、前記クライアント装置は既に認証済みか否かを判別する判別工程と、を有し、
前記通知工程では、前記判別工程において前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、上記第１のアクセスポイントに上記暗号化キーを消去するよう指示することを特徴とするサーバ装置の制御方法。
【請求項７】
請求項６に記載のサーバ装置の制御方法を実行させるようにコンピュータを動作させることを特徴とするコンピュータプログラム。
【請求項８】
請求項７に記載のコンピュータプログラムを格納したことを特徴とする、コンピュータにより読み取り可能な記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】

本発明は、クライアント端末がアクセスポイントを介して通信する際に使用する暗号キーをサーバ装置が上記アクセスポイントに通知する通信システムに関する。

【０００２】

【従来の技術】

従来、無線ＬＡＮシステムでは、クライアント端末は、ネットワーク上にあるアクセスポイントとの無線通信を介してネットワークと接続していた。

【０００３】

また、クライアント端末はアクセスポイントを介し、ネットワーク上にある認証サーバからネットワークへの接続の認証を受ける無線ＬＡＮシステムがあった。

【０００４】

そして、クライアント端末が認証サーバから認証を受けると、クライアント端末及び認証サーバはＷＥＰ暗号化方式の暗号キーを生成し、認証サーバは生成された暗号キーをアクセスポイントに通知していた。クライアント端末とアクセスポイントはＷＥＰ暗号化方式の暗号キーを用いて暗号化されたデータを送受信することによりセキュアな無線通信を行うことができた。

【０００５】

【発明が解決しようとする課題】

ところで、アクセスポイントの通信可能範囲は限られており、クライアント端末は自由に移動可能である。したがって、クライアント端末がアクセスポイント▲１▼の通信可能範囲からアクセスポイント▲２▼の通信可能範囲に移動すると、クライアント端末は再度、アクセスポイント▲２▼との無線通信を介して認証サーバによるネットワークへの接続の認証を受け、クライアント端末及び認証サーバにおいて新たなＷＥＰキーを生成し、認証サーバは新たなＷＥＰキーをアクセスポイント▲２▼に通知しなければならなかった。

【０００６】

そこで、本発明では、クライアント端末が、最初にネットワークへの接続を行ったアクセスポイントとは異なるアクセスポイントの通信可能範囲に移動した場合に、移動先のアクセスポイントを介した通信が可能になるまでの時間を短縮することを目的とする。

【０００７】

また、クライアント端末が、最初にネットワークへの接続を行ったアクセスポイントとは異なるアクセスポイントの通信可能範囲に移動した場合に、移動先のアクセスポイントを介した通信を可能にするための処理を削減することを目的とする。

【０００８】

【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は、クライアント装置を接続する複数のアクセスポイントと、サーバ装置を有する通信システムにおいて、記サーバ装置は、第１のアクセスポイントに接続するクライアント装置を認証する認証手段と、前記認証手段による認証結果に応じて、前記クライアント装置が接続する前記第１のアクセスポイントに暗号キーを通知する通知手段と、第２のアクセスポイントから通知されたクライアント装置の識別情報に基づいて、前記クライアント装置は既に認証済みか否かを判別する判別手段と、を有し、前記通知手段は、前記判別手段により前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、上記第１のアクセスポイントに上記暗号化キーを消去するよう指示することを特徴とする通信システムを提供する。

【０００９】

また、サーバ装置において、第１のアクセスポイントに接続するクライアント装置を認証する認証手段と、前記認証手段による認証結果に応じて、前記クライアント装置が接続する前記第１のアクセスポイントに暗号キーを通知する通知手段と、第２のアクセスポイントから通知されたクライアント装置の識別情報に基づいて、前記クライアント装置は既に認証済みか否かを判別する判別手段と、を有し、前記通知手段は、前記判別手段により前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知

した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、上記第１のアクセスポイントに上記暗号化キーを消去するよう指示することを特徴とするサーバ装置を提供する。

【００１０】

また、クライアント装置を接続する複数のアクセスポイントと、サーバ装置を有する通信システムの制御方法において、前記サーバ装置は、第１のアクセスポイントに接続するクライアント装置を認証する認証工程と、前記認証工程における認証結果に応じて、前記クライアント装置が接続する前記第１のアクセスポイントに暗号キーを通知する通知工程と、第２のアクセスポイントから通知されたクライアント装置の識別情報に基づいて、前記クライアント装置は既に認証済みか否かを判別する判別工程と、を有し、前記通知工程では、前記判別工程において前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、上記第１のアクセスポイントに上記暗号化キーを消去するよう指示することを特徴とする通信システムの制御方法を提供する。

【００１１】

また、サーバ装置の制御方法において、第１のアクセスポイントに接続するクライアント装置を認証する認証工程と、前記認証工程における認証結果に応じて、前記クライアント装置が接続する前記第１のアクセスポイントに暗号キーを通知する通知工程と、第２のアクセスポイントから通知されたクライアント装置の識別情報に基づいて、前記クライアント装置は既に認証済みか否かを判別する判別工程と、を有し、前記通知工程では、前記判別工程において前記クライアント装置は認証済みであると判別されると、第１のアクセスポイントに通知した前記暗号キーと同じ暗号キーを前記第２のアクセスポイントに通知し、上記第１のアクセスポイントに上記暗号化キーを消去するよう指示することを特徴とするサーバ装置の制御方法を提供する。

【００１２】

また、上記サーバ装置の制御方法を実行させるようにコンピュータを動作させることを特徴とするコンピュータプログラムを提供する。

【００１３】

また、上記コンピュータプログラムを格納したことを特徴とする、コンピュータにより読み取り可能な記憶媒体を提供する。

【００１９】

【発明の実施の形態】

以下に、本発明の一実施の形態について説明する。

【００２０】

図１は本実施の形態のシステムの構成図である。

【００２１】

１０１はネットワークであり、アクセスポイントＡ１０３、アクセスポイントＢ１０４が接続されている。尚、図１では２つのアクセスポイントが図示されているが、設置数はこれに限らない。また、アクセスポイントＡ１０３、アクセスポイントＢ１０４はそれぞれ、通信可能範囲１０６、１０７に存在するクライアント端末１０５と無線通信することができる。また、本実施の形態では、無線通信の方式としてＩＥＥＥ８０２．１１、ＩＥＥＥ８０２．１１ｂ、及びＩＥＥＥ８０２．１１ａなどの標準に基づく無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を利用する。

【００２２】

１０５はクライアント端末であり、アクセスポイントＡ１０３やアクセスポイントＢ１０４との無線通信を介してネットワーク１０１に接続する。尚、図１には図示されていないが、クライアント端末１０５は複数存在してもよい。

【００２３】

１０２は認証サーバであり、ネットワーク１０１に接続するクライアント端末１０５を認証するとともに、ＷＥＰ（Wired Equivalent Privacy）暗号化方式で用いられる暗号キー

を生成する。
【００２４】
図２はアクセスポイントＡ１０３のブロック図である。
【００２５】
尚、アクセスポイントＢ１０４も同様である。
【００２６】
２０１は無線部であり、無線データを送受信する。無線部２０１は送信部２１０、受信部２１１、アンテナ２１２からなる。
【００２７】
２０２は信号処理部であり、受信部２１１で受信した信号を検波し、デジタル信号に変換するとともに、データ処理部２０３から送られてくるデジタル信号を無線で送信するために変調する。また、信号処理部２０２はデータ処理部２０３から送られてくるデータを無線送信用のデータとするためにヘッダ等を添付したり、受信したデータからヘッダ等をはずしてデータ処理部２０３へ送ったりする機能を有する。
【００２８】
２０３はデータ処理部であり、ネットワークインターフェース２０８からのデータにＷＥＰ暗号化方式で暗号処理を施す送信データ処理部２０５と、暗号化されたデータを復号化する受信データ処理部２０６からなる。
【００２９】
２０４は制御部であり、新たなクライアント端末１０５の存在を判定したり、アクセスポイントＡ１０３全体の制御を行ったりする。
【００３０】
２０７は記憶部であり、ＷＥＰ暗号化処理を行うための暗号キーや、クライアント端末１０５のＩＤ等の情報を記憶する。
【００３１】
２０８はネットワークインターフェース部であり、アクセスポイントＡ１０３とネットワーク１０１とのインターフェースである。
【００３２】
図３はクライアント端末１０５のブロック図である。
【００３３】
尚、本実施の形態のクライアント端末１０５は無線通信カードで構成される。
【００３４】
また、図２に示したアクセスポイントＡ１０３と同様の機能には同番号が付してある。
【００３５】
３０１はデータ通信インターフェースであり、パーソナルコンピュータ等の情報処理装置と接続し、データ通信を行う。
【００３６】
３０２は記憶部であり、ＷＥＰ暗号化処理を行うのための暗号キーや、クライアント端末１０５のＩＤ等、アクセスポイントＡ１０３やアクセスポイントＢ１０４との無線通信に必要な情報を記憶する。尚、本実施の形態では、クライアント端末１０５のＩＤとして、ＭＡＣアドレス（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ａｄｄｒｅｓｓ）を使用する。
【００３７】
以下、本実施の形態におけるシステム全体の動作について、図面を参照して説明する。
【００３８】
まず、クライアント端末１０５がアクセスポイントＡ１０３を介してネットワーク１０１に初めて接続する際の手順について図４のシーケンス図を参照して説明する。
【００３９】
クライアント端末１０５は、無線ＬＡＮにおけるオープン認証を行い、アクセスポイントＡ１０３と接続する（Ｓ４０１）。

【００４０】
アクセスポイントＡ１０３は、クライアント端末１０５のＩＤを取得する（Ｓ４０２）。
【００４１】
アクセスポイントＡ１０３は、クライアント端末１０５のＩＤを認証サーバ１０２へ通知する（Ｓ４０３）。
【００４２】
認証サーバ１０２は、アクセスポイントＡ１０３から通知されたＩＤに基づき、クライアント端末１０５がネットワーク１０１に接続するための認証を既に終了しているか否かを判定する（Ｓ４０４）。ここでは、クライアント端末１０５は初めての接続であり、認証が終了していないので、認証は終了していないと判定される。
【００４３】
認証サーバ１０２は、クライアント端末１０５に対してユーザ名とパスワードの入力を要求する（Ｓ４０５）。
【００４４】
クライアント端末１０５は、ユーザ名とパスワードを入力する（Ｓ４０６）。
【００４５】
クライアント端末１０５は、ステップＳ４０６で入力されたユーザ名やパスワードの秘匿性を高めるためにＯｎｅ－Ｗａｙ　Ｈａｓｈという可逆性のない数値処理を行い、そのＯｎｅ－Ｗａｙ　Ｈａｓｈデータを認証サーバ１０２へ通知する（Ｓ４０７）。
【００４６】
認証サーバ１０２は、ステップＳ４０７にて通知されたＯｎｅ－Ｗａｙ　Ｈａｓｈのデータと認証サーバ１０２内のデータベースに保存されたネットワーク１０１との接続を許可するユーザに関するデータ群とを照合する。照合の結果、一致するものがあれば、クライアント端末１０５のネットワーク１０１への接続を認証するとともに、クライアント端末１０５のＩＤを記憶する（Ｓ４０８）。
【００４７】
クライアント端末１０５と認証サーバ１０２は、ＷＥＰセッションキーと呼ばれる暗号キーを生成する（Ｓ４０９）。ここで、ＷＥＰセッションキーとは、ＷＥＰ暗号化方式で用いられ、クライアント端末１０５のトラフィックの暗号化にのみ有効な暗号キーである。
【００４８】
認証サーバ１０２は、生成したＷＥＰセッションキーをクライアント端末１０５のＩＤと関連づけて記憶するとともに、アクセスポイントＡ１０３へ通知する（Ｓ４１０）。
【００４９】
アクセスポイントＡ１０３は、ブロードキャストキーをＷＥＰセッションキーで暗号化し（Ｓ４１１）、暗号化ブロードキャストキーをクライアント端末１０５に送信する（Ｓ４１２）。尚、ブロードキャストキーとは、アクセスポイントＡ１０３が複数のクライアント端末１０５に同報するデータを暗号化する際に用いる暗号キーである。
【００５０】
クライアント端末１０５は、ステップＳ４０９にて生成したＷＥＰセッションキーを用いて暗号化ブロードキャストキーを復号化し、ブロードキャストキーを取得する（Ｓ４１３）。
【００５１】
アクセスポイントＡ１０３とクライアント端末１０５は、ＷＥＰ暗号化手順を起動する（Ｓ４１４、Ｓ４１５）。
【００５２】
そして、アクセスポイントＡ１０３は、１つのクライアント端末１０５との通信（Ｐｏｉｎｔ－ｔｏ－ｐｏｉｎｔ通信）では、ＷＥＰセッションキーで暗号化したデータを送受信することによりセキュアな無線通信を行う（Ｓ４１６）。また、アクセスポイントＡ１０３は、複数のクライアント端末１０５との同報通信（Ｐｏｉｎｔ－ｔｏ－ｍｕｌｔｉｐｏｉｎｔ通信）では、ブロードキャストキーで暗号化したデータを送受信することによりセ

キュアな無線通信を行う（Ｓ４１６）。
【００５３】
次に、一度、アクセスポイントＡ１０３を介してネットワーク１０１への接続の認証が終了しているクライアント端末１０５が、アクセスポイントＡ１０３の通信可能範囲１０６からアクセスポイントＢ１０４の通信可能範囲１０７に移動して、アクセスポイントＢ１０４を介してネットワーク１０１と接続する場合の動作を図５のシーケンス図を用いて説明する。
【００５４】
クライアント端末１０５が、アクセスポイントＡ１０３の通信可能範囲１０６外に移動し、アクセスポイントＡ１０３と通信できない状態になる（Ｓ５０１）。そして、クライアント端末１０５が、アクセスポイントＢ１０４の通信可能範囲１０７内に移動し、アクセスポイントＢ１０４と通信可能な状態になったとする。
【００５５】
クライアント端末１０５は、オープン認証を行い、アクセスポイントＢ１０４と接続する（Ｓ５０２）。
【００５６】
アクセスポイントＢ１０４は、クライアント端末１０５のＩＤを取得する（Ｓ５０３）。
【００５７】
アクセスポイントＢ１０４は、クライアント端末１０５のＩＤを認証サーバ１０２へ通知する（Ｓ５０４）。
【００５８】
認証サーバ１０２は、ステップＳ５０４にて通知されたＩＤと、記憶されている既に認証済みのクライアント端末のＩＤと、に基づき、クライアント端末１０５が、ネットワーク１０１に接続するための認証を既に終了しているか否かを判定する（Ｓ５０５）。ここでは、クライアント端末１０５は、ステップＳ４０８（図４）にて既にアクセスポイントＡ１０３を経由してネットワーク１０１への接続の認証が終了し、クライアント端末１０５のＩＤが記憶されているので、認証は終了していると判定される。
【００５９】
認証サーバ１０２は、アクセスポイントＡ１０３に、記憶部２０７に記憶してあるクライアント端末１０５との無線通信に使用するＷＥＰセッションキーを消去するように指示する（Ｓ５０６）。
【００６０】
認証サーバ１０２は、ステップＳ４１０（図４）にてクライアント端末１０５のＩＤと対応づけて記憶されているＷＥＰセッションキーをアクセスポイントＢ１０４に通知する（Ｓ５０７）。
【００６１】
アクセスポイントＢ１０４は、ステップＳ５０７にて通知されたＷＥＰセッションキーでブロードキャストキーを暗号化し（Ｓ５０８）、暗号化ブロードキャストキーをクライアント端末１０５に送付する（Ｓ５０９）。
【００６２】
クライアント端末１０５は、ステップＳ４０９（図４）で生成したＷＥＰセッションキーで暗号化ブロードキャストキーを復号化し、ブロードキャストキーを取得する（Ｓ５１０）。
【００６３】
アクセスポイントＢ１０４とクライアント端末１０５は、それぞれＷＥＰ暗号化手順を起動する（Ｓ５１１、Ｓ５１２）。
【００６４】
そして、アクセスポイントＢ１０４は、１つのクライアント端末１０５との通信（Ｐｏｉｎｔ－ｔｏ－ｐｏｉｎｔ通信）では、クライアント端末１０５とアクセスポイントＡ１０３との通信で使われていたＷＥＰセッションキーと同じＷＥＰセッションキーで暗号化し

たデータを送受信することによりセキュアな無線通信を行う（Ｓ５１３）。また、アクセスポイントＢ１０３は、複数のクライアント端末１０５との同報通信（Ｐｏｉｎｔ－ｔｏ－ｍｕｌｔｉｐｏｉｎｔ通信）では、ブロードキャストキーで暗号化したデータを送受信することによりセキュアな無線通信を行う（Ｓ５１３）。

【００６５】

尚、本実施の形態では、ステップＳ５０７において、認証サーバ１０２内に記憶されているＷＥＰセッションキーをアクセスポイントＢ１０４に通知するようにしたが、アクセスポイントＡ１０３内に記憶されているＷＥＰセッションキーを認証サーバ１０２を介してアクセスポイントＢ１０４に通知するようにしてもよい。

【００６６】

尚、上記説明では、クライアント端末１０５を無線通信カードとして説明したが、パーソナルコンピュータやＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔｓ）に上記無線通信カードと同じ機能が内蔵されているものとしてもよい。

【００６７】

また、本発明の目的は、上記したクライアント端末、アクセスポイント、認証サーバ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憶した記憶媒体を、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（又はＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読みだして実行することによっても、達成されることは言うまでもない。

【００６８】

この場合、記憶媒体から読み出されたプログラムコード自体が本実施の形態の機能を実現することとなり、そのプログラムコードを記憶した記憶媒体は本発明を構成することとなる。

【００６９】

プログラムコードを供給するための記憶媒体としては、ＲＯＭ、フロッピーディスク、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等を用いることができる。

【００７０】

また、コンピュータが読みだしたプログラムコードを実行することにより、本実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ等が実際の処理の一部又は全部を行い、その処理によって本実施の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。

【００７１】

さらに、記憶媒体から読み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拡張機能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き込まれた後、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、その処理によって本実施の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。

【００７２】

【発明の効果】

以上説明したように、本発明によれば、クライアント装置が最初に接続を行ったアクセスポイントとは異なるアクセスポイントの通信可能範囲に移動した場合の、移動先のアクセスポイントを介した通信が可能になるまでの時間の短縮、サーバ装置の処理削減を、セキュリティを保持した上で可能とすることができる。

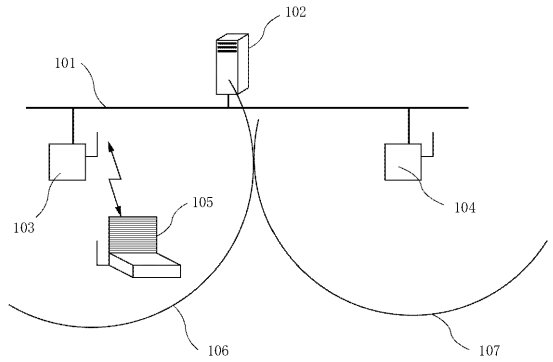
【００７３】

即ち、クライアント装置の移動前、移動後においても、アクセスポイントへの暗号化キーの通知はサーバ装置が行うので、セキュリティ管理を一元管理でき、また、移動前に接続していたアクセスポイントに暗号キーの消去を指示するので、セキュリティを保持した上で上記時間の短縮、処理の削減を実現できる。

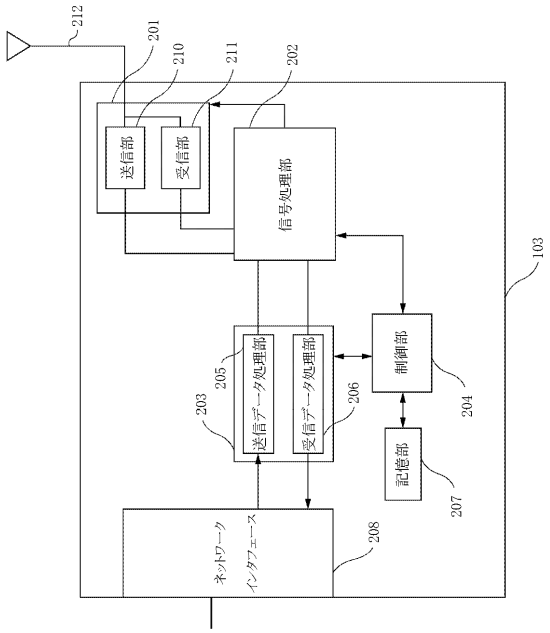
【図面の簡単な説明】

【図１】本発明の一実施の形態におけるシステムの構成図である。
【図２】本発明の一実施の形態におけるアクセスポイントのブロック図である。
【図３】本発明の一実施の形態におけるクライアント端末のブロック図である。
【図４】本発明の一実施の形態におけるシステムの動作を表すシーケンス図である。
【図５】本発明の一実施の形態におけるシステムの動作を表すシーケンス図である。
【符号の説明】
１０１　ネットワーク、
１０２　認証サーバ
１０３、１０４　アクセスポイント
１０５　クライアント端末
１０６　アクセスポイントＡ１０３の通信可能範囲
１０７　アクセスポイントＢ１０４の通信可能範囲

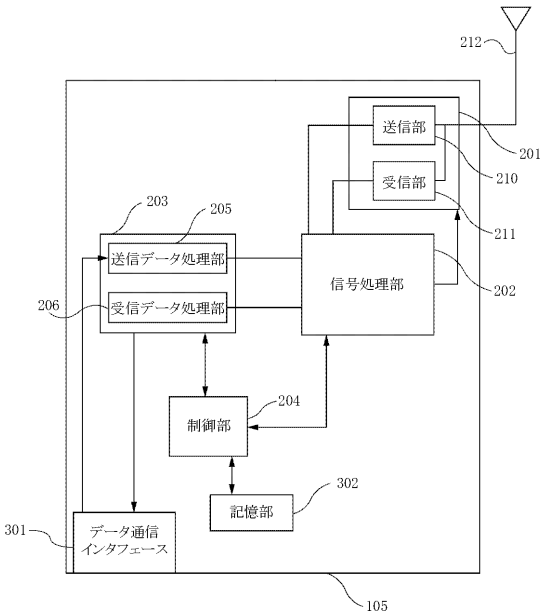
【図１】



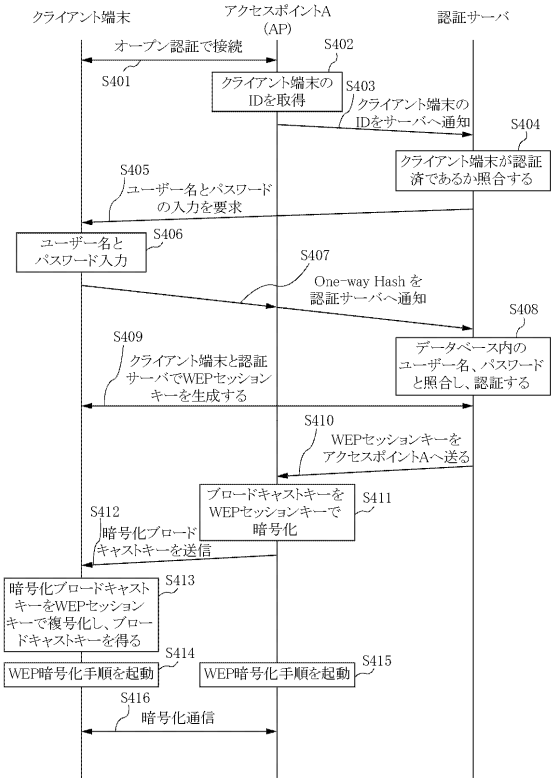
【図２】



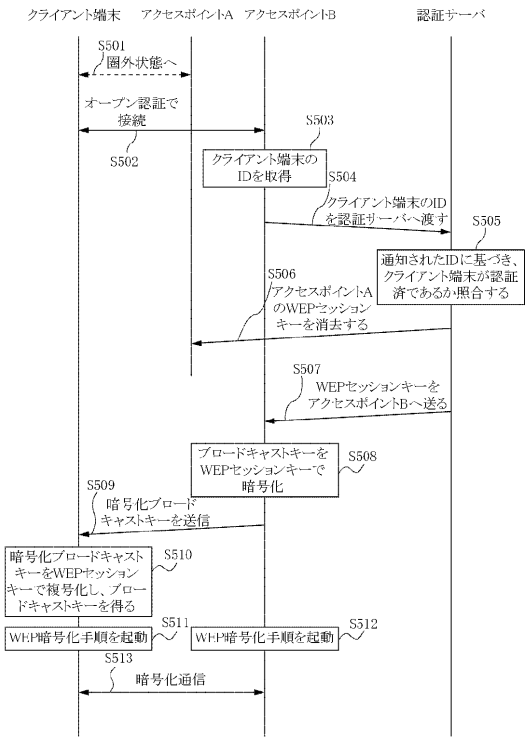
【図３】


212
送信部
201
受信部
210
211
203
205
送信データ処理部
信号処理部
202
206
受信データ処理部
204
制御部
302
記憶部
301
データ通信
インタフェース
105

【図４】


クライアント端末
アクセスポイントA
(AP)
認証サーバ
オープン認証で接続
S401
S402
クライアント端末の
IDを取得
S403
クライアント端末の
IDをサーバへ通知
S404
クライアント端末が認証
済であるか照合する
S405
ユーザー名とパスワード
の入力を要求
ユーザー名と
パスワード入力
S406
S407
One-way Hash を
認証サーバへ通知
S408
データベース内の
ユーザー名、パスワード
と照合し、認証する
S409
クライアント端末と認証
サーバでWEPセッション
キーを生成する
S410
WEPセッションキーを
アクセスポイントAへ送る
ブロードキャストキーを
WEPセッションキーで
暗号化
S411
S412
暗号化ブロード
キャストキーを送信
暗号化ブロードキャスト
キーをWEPセッション
キーで複号化し、ブロー
ドキャストキーを得る
S413
WEP暗号化手順を起動
S414
WEP暗号化手順を起動
S415
S416
暗号化通信

【図５】


クライアント端末
アクセスポイントA
アクセスポイントB
認証サーバ
S501
圏外状態へ
オープン認証で
接続
S502
S503
クライアント端末の
IDを取得
S504
クライアント端末のID
を認証サーバへ渡す
S505
通知されたIDに基づき、
クライアント端末が認証
済であるか照合する
S506
アクセスポイントA
のWEPセッション
キーを消去する
S507
WEPセッションキーを
アクセスポイントBへ送る
ブロードキャストキーを
WEPセッションキーで
暗号化
S508
S509
暗号化ブロード
キャストキーを送信
暗号化ブロードキャスト
キーをWEPセッション
キーで複号化し、ブロー
ドキャストキーを得る
S510
WEP暗号化手順を起動
S511
WEP暗号化手順を起動
S512
S513
暗号化通信

フロントページの続き

(56)参考文献 特開２００１－２５８０５９（ＪＰ，Ａ）
特開平１０－１４５３６９（ＪＰ，Ａ）
特開２００１－１１１５４３（ＪＰ，Ａ）
特開２００１－１１１５４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/28
G06F 13/00
G06F 21/20
H04Q 7/38