(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3970079号
(P3970079)
(45)発行日　平成19年9月5日(2007.9.5)　(24)登録日　平成19年6月15日(2007.6.15)

(51)Int.Cl.		F I		
H04L 12/28	(2006.01)	H04L	12/28	300Z
H04Q 7/38	(2006.01)	H04B	7/26	109R
H04L 9/32	(2006.01)	H04L	9/00	675D

請求項の数 14　(全 19 頁)

(21)出願番号　特願2002-110491 (P2002-110491)
(22)出願日　平成14年4月12日 (2002.4.12)
(65)公開番号　特開2003-304258 (P2003-304258A)
(43)公開日　平成15年10月24日 (2003.10.24)
審査請求日　平成17年2月18日 (2005.2.18)

(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　100125254
弁理士　別役　重尚
(74)代理人　100118278
弁理士　村松　聡
(74)代理人　100138922
弁理士　後藤　夏紀
(74)代理人　100136858
弁理士　池田　浩
(74)代理人　100135633
弁理士　二宮　浩康

最終頁に続く

(54)【発明の名称】アクセスポイント、無線通信装置及びそれらの制御方法

(57)【特許請求の範囲】

【請求項１】

無線通信装置のアクセス制御を行うアクセスポイントにおいて、

着脱式の記憶装置に保存されたアカウントデータを読み出し、記憶する記憶手段と、

前記記憶手段に記憶されているアカウントデータに基づいて無線通信装置を認証する認証手段と、を有し、

前記認証手段は、前記着脱式の記憶装置に保存されているアカウントデータの中の現在時刻に対応するアカウントデータを用いて前記認証処理を行うことを特徴とするアクセスポイント。

【請求項２】

請求項１において、

前記アクセスポイントは、複数の無線通信機能に対応した無線通信拡張インターフェースを有し、

前記無線通信拡張インターフェースに選択的に無線通信カードを装着することで異なる無線通信機能による無線通信装置との無線通信を可能とすることを特徴とするアクセスポイント。

【請求項３】

請求項２において、

前記アクセスポイントは、前記無線通信拡張インターフェースを複数有することを特徴とするアクセスポイント。

【請求項４】
請求項１において、
前記アクセスポイントは、有線のネットワークに接続するための有線インターフェースを有し、
前記無線通信装置と前記有線ネットワーク間の通信経路選択処理を実行する制御部により、前記認証手段による認証のエミュレーション処理を実行することを特徴とするアクセスポイント。
【請求項５】
請求項１において、
着脱式の記憶装置に保存されたアカウントデータが更新されたことを判別する判別手段と、
前記判別手段による判別に基づいて、前記記憶手段に記憶されているアカウントデータを書き換える書換手段と、
を有することを特徴とするアクセスポイント。
【請求項６】
請求項５において、
前記判別手段は、前記着脱式の記憶装置が接続されたときの時刻に対応するアカウントデータが更新されたことを判別することを特徴とするアクセスポイント。
【請求項７】
請求項１において、
前記アクセスポイントは、有線ネットワークに接続するための有線インターフェースを有し、
前記記憶手段は、前記有線ネットワーク経由で受信した認証用のアカウントデータも記憶することを特徴とするアクセスポイント。
【請求項８】
請求項１において、
前記着脱式の記憶装置には、前記アクセスポイントが管理する全てのアカウントデータが保存されることを特徴とするアクセスポイント。
【請求項９】
請求項１において、
前記着脱式の記憶装置には、前記無線通信装置と無線ネットワーク接続するためのネットワーク識別情報が保存されることを特徴とするアクセスポイント。
【請求項１０】
請求項１において、
前記アクセスポイントは、複数の無線通信インターフェースと、
前記アカウントデータに応じて、利用する無線通信インターフェースを選択する選択手段と、を有することを特徴とするアクセスポイント。
【請求項１１】
無線通信装置において、
認証機能を有するアクセスポイントが無線通信装置を認証する際に使用するアカウントデータが保存されている着脱式の記憶装置を装着するインターフェースと、
前記インターフェースに装着された着脱式の記憶装置に保存されているアカウントデータの中の現在時刻に対応するアカウントデータを編集する編集手段と、
前記編集手段により編集したアカウントデータを使用して前記アクセスポイントとの認証処理を実行する認証手段と、
を有することを特徴とする無線通信装置。
【請求項１２】
アクセスポイントの制御方法において、
着脱式の記憶装置に保存されたアカウントデータを読み出し、メモリに記憶する記憶工程と、

前記記憶工程において前記メモリに記憶されたアカウントデータに基づいて無線通信装置を認証する認証工程と、を有し、

前記認証工程において、前記着脱式の記憶装置に保存されているアカウントデータの中の現在時刻に対応するアカウントデータを用いて前記認証処理を行うことを特徴とする制御方法。

【請求項１３】

アクセスポイントが無線通信装置を認証する際に使用するアカウントデータが保存されている着脱式の記憶装置を装着するインターフェースを有する無線通信装置の制御方法において、

前記インターフェースに装着された着脱式の記憶装置に保存されているアカウントデータの中の現在時刻に対応するアカウントデータを編集する編集工程と、

前記編集工程において編集したアカウントデータを使用して前記アクセスポイントとの認証処理を実行する認証工程と、

を有することを特徴とする制御方法。

【請求項１４】

請求項１２もしくは請求項１３に記載された制御方法を実行す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ＬＡＮ（８０２．１１）やBluetooth等の無線通信機能を有する無線通信装置を認証し、セキュリティを考慮したネットワーク構築を実現する場合に好適なアクセスポイント、無線通信装置、それらの制御方法に関する。

【０００２】

【従来の技術】

従来より、無線ＬＡＮやBluetoothでは、その通信媒体として電波を用いるため、通信先の制限が難しいという問題があった。このため、これらの規格では、通信先毎に暗号鍵を変更することで、たとえパケットをのぞき見られても、それを解読できないようにするといった防御手段が採用されてきた。防御手段の中でも802.1x（ＥＡＰ）と呼ばれる認証・暗号化手段は、Microsoft社がWindows（登録商標）プラットフォームで採用したこともあり、無線通信認証・暗号化手段のデファクトスタンダードとなりつつある。

【０００３】

無線ＬＡＮ（８０２．１１）における802.1x方式は、クライアントの端末がネットワーク接続要求を行う際、ＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）を利用してイントラネット内に設けられた認証サーバ（RADIUSサーバ等）とデータ通信を行い、認証サーバからクライアントへのチャレンジを実施する。クライアントは、このチャレンジに対しアカウント（利用者を識別するための情報）名とパスワードを入力し、そのセットが認証サーバ内のデータと一致すれば、認証サーバは128bitの暗号鍵をアクセスポイントとクライアントに返す。このようなプロセスを経てクライアントが認証をパスすると、それ以降の無線通信は、入手した128bitの暗号鍵をＷＥＰキーとして、クライアントとアクセスポイントとの両者で利用することで暗号化される。

【０００４】

また、Bluetoothでは、ＰＡＮプロファイルにおいてセキュリティ向上のためには802.1x認証・暗号化手段を用いることが推奨されている。Bluetoothの場合は、無線媒体である電波を暗号化するための鍵の生成は、Bluetooth方式で通信を行うデバイス間の相互認証によって自動的に生成されるため、認証サーバから受け取った暗号鍵情報を、無線ＬＡＮで言うところのＷＥＰキーのような電波そのものの暗号化鍵としては利用できないが、無線媒体として電波を生成する前段階で、パケットを暗号化する際の鍵として利用することで、二重に暗号化し通信のセキュリティを向上させることができる。

【０００５】

この８０２．１ｘ方式の認証・暗号化プロセスでは、認証を実施するための認証サーバがネットワーク内に存在し、認証サーバでクライアントのアカウントを集中管理する。このため、８０２．１ｘ方式を用いれば、クライアントがどこにいても、認証サーバとのＴＣＰ／ＩＰによる通信が実現可能であれば、同一のアカウント・パスワードを用いてイントラネット等のネットワークに接続することができる。

【０００６】

【発明が解決しようとする課題】

しかしながら、上記従来技術においては下記のような問題があった。上述した８０２．１ｘ方式による認証・暗号化プロセスを用いることで、クライアントは無線通信を用いた安全なネットワーク接続を実現できる。但し、そのためにはネットワーク内に認証サーバが設置され、且つ認証サーバには予めクライアントのアカウントが登録されている必要がある。即ち、８０２．１ｘ方式は、比較的規模の大きなイントラネット等での運用を想定した方式であり、無線によるネットワーク接続を行うクライアントも認証サーバ上にアカウントを持ったメンバに限定されるといった制限があった。

【０００７】

このため、認証サーバにアカウントの無い外来者が参加するミーティングを行う場合や、イントラネットへの接続手段がない社外の会議室でのミーティングを行う場合は、８０２．１ｘ方式による認証・暗号化プロセスを利用した無線通信による安全なネットワークを構築できないという不具合があった。なお、この際に、認証・暗号化を無くした無線通信は実現可能であるが、セキュリティの面から大きな問題がある。また、手作業による無線通信用パラメータの再設定を実施すれば、無線通信の暗号化は可能であるが、クライアントはイントラネット内で通常利用する８０２．１ｘ方式のアカウント・パスワードの入力による自動接続とは、全く異なる接続操作を手動で行わなければならず、操作が煩雑であり、利便性が損なわれる。

【０００８】

本発明は、上述した点に鑑みなされたものであり、安全な無線ネットワークを、簡易なシステム構成で簡単かつ柔軟に構築することを可能にすることを目的とする。

【０００９】

【課題を解決するための手段】

上記目的を達成するため、本発明のアクセスポイントは、無線通信装置のアクセス制御を行うアクセスポイントにおいて、着脱式の記憶装置に保存されたアカウントデータを読み出し、記憶する記憶手段と、前記記憶手段に記憶されているアカウントデータに基づいて無線通信装置を認証する認証手段と、を有し、前記認証手段は、前記着脱式の記憶装置に保存されているアカウントデータの中の現在時刻に対応するアカウントデータを用いて前記認証処理を行うことを特徴とする。

【００１０】

また、本発明の無線通信装置は、無線通信装置において、認証機能を有するアクセスポイントが無線通信装置を認証する際に使用するアカウントデータが保存されている着脱式の記憶装置を装着するインターフェースと、前記インターフェースに装着された着脱式の記憶装置に保存されているアカウントデータの中の現在時刻に対応するアカウントデータを編集する編集手段と、前記編集手段により編集したアカウントデータを使用して前記アクセスポイントとの認証処理を実行する認証手段と、を有することを特徴とする。

【００１１】

また、本発明のアクセスポイントの制御方法は、アクセスポイントの制御方法において、着脱式の記憶装置に保存されたアカウントデータを読み出し、メモリに記憶する記憶工程と、前記記憶工程において前記メモリに記憶されたアカウントデータに基づいて無線通信装置を認証する認証工程と、を有し、前記認証工程において、前記着脱式の記憶装置に保存されているアカウントデータの中の現在時刻に対応するアカウントデータを用いて前記認証処理を行うことを特徴とする。

【００１２】

また、本発明の無線通信装置の制御方法は、アクセスポイントが無線通信装置を認証する際に使用するアカウントデータが保存されている着脱式の記憶装置を装着するインターフェースを有する無線通信装置の制御方法において、前記インターフェースに装着された着脱式の記憶装置に保存されているアカウントデータの中の現在時刻に対応するアカウントデータを編集する編集工程と、前記編集工程において編集したアカウントデータを使用して前記アクセスポイントとの認証処理を実行する認証工程と、を有することを特徴とする。

【００１６】

【発明の実施の形態】

先ず、本発明の実施の形態の詳細を説明する前に、本発明の実施の形態で実現しようとする目的を列挙する。本発明の実施の形態では、Windows(登録商標)プラットフォーム等の８０２．１ｘ認証・暗号化システムを搭載したクライアントデバイスによるＰＡＮを無線通信によって構築しようとする際に、安全且つ柔軟なＰＡＮを簡単に構築可能とする。また、ＰＡＮ構築の際に、利用する無線通信手段を簡単に選択可能とする。また、ＰＡＮ構築の際に用いる無線通信手段を複数同時に利用可能とし、異なる無線通信手段で構成されたＰＡＮを簡単に構築可能とする。また、ＰＡＮに参加可能なある無線通信手段におけるクライアント数を増加させる。

【００１７】

また、無線通信手段によって構築したＰＡＮを、イントラネットやインターネットなどの基幹ネットワークに接続する場合、不正なアクセスを相互に禁止する。また、本アクセスポイントを製品化する場合のコストを低減する。また、ＰＡＮ構築時にクライアントのテンポラリな参加や代理参加等の柔軟な参加を許容する。また、ＰＡＮに参加するクライアントを、本アクセスポイントに集中的に接続し、クライアント管理を本アクセスポイントで統合的に実施可能とする。また、ＰＡＮに参加するクライアントを、本アクセスポイント内の無線通信拡張カードに選択的に接続し、クライアント配分等の管理を本アクセスポイントで実現可能とする。また、アカウント管理用の着脱式不揮発性メモリ装置に関する管理を容易にする。

【００１８】

また、本アクセスポイントを用いてＰＡＮを構成する際のアカウントデータの作成をローカルで柔軟に実施可能とし、クライアントやＰＡＮ構築時間の管理を柔軟に実施可能とする。また、本アクセスポイントを複数利用するか、アクセスポイント内に複数の無線通信拡張カードを挿入して、複数のＰＡＮを構築する際に、各ＰＡＮのクライアントを各々に対応したアクセスポイントに自動接続する。また、本アクセスポイントに複数のＰＡＮ構築用アカウントが与えられた場合に、構築すべきＰＡＮ用アカウントを自動判定し、ＰＡＮを構築する。

【００１９】

次に、本発明の実施の形態の特徴的な構成及び作用を列挙する。本発明の実施の形態は、８０２．１ｘ認証に必要な認証サーバをアクセスポイント内に取り込み、且つ認証サーバ用アカウントデータを着脱式の不揮発性メモリ装置から供給することで、Windows（登録商標）プラットフォーム等の８０２．１ｘ認証・暗号化システムを搭載したクライアントデバイスによるＰＡＮを、無線通信によって構築しようとする際に、安全且つ柔軟なＰＡＮを簡単に構築可能とする。また、アクセスポイント内部の無線通信機能を拡張カードによって提供し、且つ拡張カードを簡単に変更可能とすることで、ＰＡＮ構築の際に利用する無線通信手段を、簡単に選択可能とする。

【００２０】

また、アクセスポイント内部に無線通信機能拡張用カードインターフェースを複数装備し、同インターフェースに通信手段の異なるカードを装着することによって、ＰＡＮ構築の際に用いる無線通信手段を複数同時に利用可能とし、異なる無線通信手段で構成されたＰＡＮを簡単に構築可能とする。更に、同インターフェースに802.11b等の無線通信カードを複数装着することによって、１枚のカードで対応できるユーザ数を越えたクライアント

数によるＰＡＮの構築やクライアントの負荷分散を実現可能とする。また、本アクセスポイントを経由して基幹ネットワークへ接続する無線通信クライアントに対してユーザ毎のルーティングやフィルタリングを行うことで、不正なアクセスを相互に禁止する。また、単一のＣＰＵ及び周辺回路で、本アクセスポイントの有するルーティング機能と認証用サーバエミュレーション機能を実現することで、製品化する場合のコストを低減する。

【００２１】

また、クライアントは自身のアカウントデータを、着脱式の不揮発性メモリ装置のデータから入手するか、またはネットワーク経由で予めクライアントデバイス内の不揮発性メモリにダウンロードして入手し、入手したアカウントをＰＡＮ参加の際に利用することで、ＰＡＮ構築時にテンポラリなクライアントの参加や代理参加等の柔軟な参加を許容する。

【００２２】

また、アクセスポイントとクライアントデバイスグループが、無線ＬＡＮによるＰＡＮ構築時に利用するESS ID情報を、アカウントデータと共に、着脱式の不揮発性メモリ装置のデータから入手するか、またはネットワーク経由で予めクライアントデバイス内の不揮発性メモリにダウンロードして入手し、アクセスポイントとクライアントデバイス群で構成するＰＡＮ毎にESS IDを変えることで、ＰＡＮに参加するクライアント群を、あるアクセスポイントに集中的に接続し、クライアント管理をアクセスポイントで統合的に実施する。

【００２３】

また、複数の無線通信拡張カードを内蔵したアクセスポイントとクライアントデバイスグループが、無線ＬＡＮによるＰＡＮ構築時に利用する複数のESS ID情報を、アカウントデータと共に、着脱式の不揮発性メモリ装置のデータから入手するか、またはネットワーク経由で予めクライアントデバイス内の不揮発性メモリにダウンロードして入手し、アクセスポイント内の各無線通信拡張カードと対応するクライアントデバイス群で構成するＰＡＮ毎にESS IDを変えることで、ＰＡＮに参加するクライアント群を、アクセスポイント内のある無線通信拡張カードに選択的に接続し、クライアント配分等の管理をアクセスポイント上で実現する。

【００２４】

また、アカウントデータの管理用に利用する着脱式の不揮発性メモリ装置を、アクセスポイントとクライアントデバイスで共通に利用することで、１式のアカウント管理用着脱式不揮発性メモリ装置を管理するだけで本発明によるＰＡＮを運用する。また、クライアントデバイスとして主に利用されるパーソナルコンピュータやＰＤＡで稼働し、着脱式不揮発性メモリ装置内のデータやアクセスポイントやクライアントデバイス内の不揮発性メモリ装置にアカウントデータを登録するアカウント作成プログラムを用意することで、本発明によるＰＡＮ構成時のアカウントデータ作成をローカルで柔軟に実施可能とし、クライアントやＰＡＮ構築時間の管理を柔軟に実施する。

【００２５】

また、クライアントデバイスとして主に利用されるパーソナルコンピュータやＰＤＡで稼働し、着脱式不揮発性メモリ装置内のデータやアクセスポイントやクライアントデバイス内の不揮発性メモリ装置にアカウントデータとESS IDを登録するアカウント作成プログラムを用意することで、本アクセスポイントを複数利用するか、複数の無線通信拡張カードをアクセスポイント内に内蔵して、本発明による複数のＰＡＮを構築する際に、各ＰＡＮのクライアントを各々に対応したアクセスポイントや無線通信拡張カードに自動接続する。

【００２６】

また、アクセスポイント内に内蔵したリアルタイマクロック情報と、着脱式の不揮発性メモリ装置またはアクセスポイント内部の不揮発性メモリに保存され供給されるＰＡＮ構築の時間情報とを比較し、時間情報が一致したアカウントデータに基づいてアクセスポイントの無線通信パラメータを自動設定し、そのパラメータに基づいてネットワーク接続を行うことで、アクセスポイントに複数のＰＡＮ構築用アカウントが与えられた場合に、構築

すべきＰＡＮ用アカウントを自動判定し、ＰＡＮを構築する。

【００２７】

また、８０２．１ｘ認証に必要な認証サーバをアクセスポイント内に取り込み、且つ認証サーバ用アカウントデータを、ネットワーク経由でアクセスポイント内の不揮発性メモリに一旦蓄積した後、不揮発性メモリから認証サーバ用アカウントデータを供給することで、Windows(登録商標)プラットフォーム等の８０２．１ｘ認証・暗号化システムを搭載したクライアントデバイスによるＰＡＮを、無線通信によって構築しようとする際に、安全且つ柔軟なＰＡＮを、簡単に構築可能とする。

【００２８】

以下、本発明の第１の実施の形態乃至第３の実施の形態を図面に基づいて詳細に説明する。

【００２９】

［第１の実施の形態］

図１は本発明の第１の実施の形態に係るネットワークシステムの構成を示す概念図であり、本発明の特徴を最も良く表す図である。ネットワークシステムは、ＩＣカードスロット２を備えたアクセスポイント１と、クライアントとなるパーソナルコンピュータ（ＰＣ）３、４、５、６と、Personal Digital Assistants (ＰＤＡ)７、８、９と、無線通信手段１０、１１、１２、１３、１４、１５、１６から構成されている。

【００３０】

アクセスポイント１は、無線ＬＡＮ（８０２．１１）やBluetooth等の無線通信手段による安全なネットワークを構築する本発明の主たる特徴を有するものであり、利用者との接続点である。ＩＣカードスロット２は、着脱式の不揮発性メモリが挿入されるものであり、アクセスポイント１に内蔵された認証サーバ機能に対して着脱式の不揮発性メモリよりアカウントデータを供給する。クライントパソコン３、４、５、６は、アクセスポイント１によってＰＡＮに接続される。ＰＤＡ７、８、９は、アクセスポイント１によってＰＡＮに接続される。無線通信手段１０、１１、１２、１３、１４、１５、１６は、アクセスポイント１と各クライアントパソコン３、４、５、６、７、８、９を接続する８０２．１１やBluetooth等の無線通信機能を有する。

【００３１】

図２は上記アクセスポイント１の内部構造を示すブロック図である。アクセスポイント１は、無線通信の電波生成部（RF）２０、無線通信制御回路（Base Band）２１、Media Access Control (ＭＡＣ)回路等を含むアクセスポイントコントローラ２２、アクセスポイントコントローラ２２と認証サーバ２４を結ぶ通信手段であるところのＴＣＰ／ＩＰ２３、RADIUS等の認証サーバ２４、認証サーバ２４に対してアカウントデータを供給するためのインターフェースであるＩＣカードスロット２５、ＩＣカードスロット２５を介して認証サーバ２４へ供給するアカウントデータを保持する着脱式のＩＣカード（着脱式不揮発性メモリ装置）２６を備えている。

【００３２】

本構成において、クライアントパソコン３、４、５、６やＰＤＡ７、８、９がネットワークを構成しようとする際、従来技術で述べた８０２．１ｘ等のユーザ認証を用いれば、安全な無線ネットワークを構築可能である。しかしながら、上述したように８０２．１ｘ等のユーザ認証には、アクセスポイント１とＴＣＰ／ＩＰで接続された認証サーバが必須である。この問題を解決するため、本発明では、図２に示すように認証サーバ２４をアクセスポイント１内に取り込む。更に、認証サーバ２４用のアカウントデータを、ＩＣカード（着脱式不揮発性メモリ装置）２６に保存しておき、便宜に応じて、ＩＣカードスロット２５を介してＩＣカード（着脱式不揮発性メモリ装置）２６内のアカウントデータを認証サーバ２４へ読み込んで利用する。

【００３３】

即ち、本アクセスポイント１との安全な無線通信によるネットワークを確立しようとするクライアントパソコン３は、認証サーバへのアカウントを有していないと仮定する。この

場合、通常は、ネットワーク管理者へのアカウント申請等の手続きを経てアカウントが生成されるが、本発明においては、クライアントパソコン３の所有者は、アクセスポイント１のＩＣカードスロット（図１の２、図２の２５）に挿入されたＩＣカード（着脱式不揮発性メモリ装置）２６を取り出して、自身のクライアントパソコンに装備されたＩＣカードスロットへ挿入し、本発明のプログラムを起動することで、ＩＣカード（着脱式不揮発性メモリ装置）２６上にアカウントを作成することができる。

【００３４】

図３はクライアントデバイスで稼働するアカウントデータベース更新プログラム（アカウント作成プログラム）の動作を示すフローチャートである。図３に示すように、アカウントデータベース更新プログラムでは、新規アカウントデータの作成か既存アカウントデータの編集かによって処理の流れが異なる。既存アカウントデータの編集の場合は、現在時刻に使用されるべきアカウントファイルが自動的にオープンされ、その内容に関して変更が実施できる。こうすることで、クライアントパソコン４、５、６やＰＤＡ７、８、９が既にアカウントを有するＰＡＮを構築しており、そこに新たにクライアントパソコン３が参加するような場合に、容易にクライアントパソコン３のアカウントを作成して、ＰＡＮに参加させることができる。なお、このアカウントデータベース更新プログラムの実行は、クライアントパソコン３に限らず、その他のクライアントパソコン４、５、６やＰＤＡ７、８、９でも実行可能である。

【００３５】

図３のフローチャートをステップ順に説明すると、先ず、クライアントデバイスでは、新規アカウントデータの作成か既存アカウントデータの編集かを判断する（ステップＳ３１）。既存アカウントデータの編集の場合は、使用中のアカウントデータを変更する編集か否かを判断する（ステップＳ３２）。使用中のアカウントデータを変更する編集でない場合は、本処理を終了する。使用中のアカウントデータを変更する編集の場合は、クライアントデバイスのＩＣカードスロットに挿入された着脱式不揮発性メモリ装置から現在時刻に対応するアカウントデータを読み出し（ステップＳ３３）、アカウントデータを変更する（ステップＳ３４）。他方、新規アカウントデータの作成の場合は、ＰＡＮ構築に必要な人数と各々の種別（例えば、ＰＡＮへのアクセス権を付与する者と付与しない者の区別など）、ＰＡＮ構築の時間等の新規条件を入力し（ステップＳ３５）、アカウントデータを入力する（ステップＳ３６）。ステップＳ３４またはステップＳ３６の処理後は、更新されたアカウントデータを不揮発性メモリ装置へ書き込む（ステップＳ３７）。

【００３６】

図４はアカウントデータを更新した後に本発明で述べるアクセスポイント１に着脱式不揮発性メモリ装置２６を再挿入した際のアクセスポイント１の動作を示すフローチャートである。図４に示すように、アクセスポイント１は、挿入された不揮発性メモリ装置２６に現在使用中のアカウントデータの更新版が存在する場合には、速やかに更新されたアカウントデータを読み出して、アクセスポイント自身のメモリ上にコピーしたアカウントデータを置き換える。

【００３７】

図４のフローチャートをステップ順に説明すると、先ず、アクセスポイント１のＩＣカードスロット２５に着脱式不揮発性メモリ装置２６が挿入されたか否かを判断する（ステップＳ４１）。着脱式不揮発性メモリ装置２６が挿入された場合は、現在時間に対応する着脱式不揮発性メモリ装置２６内のアカウントデータを読み出す（ステップＳ４２）。次に、更新アカウントデータが存在するか否かを判断する（ステップＳ４３）。更新アカウントデータが存在しない場合は、本処理を終了する。更新アカウントデータが存在する場合は、現在認証に使用中のアカウントデータを更新アカウントデータに置き換える（ステップＳ４４）。

【００３８】

図５はアクセスポイント１の内部構成を示すブロック図であり、本発明の特徴を最も良く表す図である。アクセスポイント１は、ルータ回路３０、認証サーバ回路３１、クライア

ントデータベース用ＰＣカードインターフェース３２、不揮発性メモリカード３３、無線通信ボードインターフェース（クライアント用拡張コネクタ１）３４、無線通信ボードインターフェース（クライアント用拡張コネクタ２）３５、無線通信ボードインターフェース（クライアント用拡張コネクタ３）３６、無線通信ボードインターフェース（クライアント用拡張コネクタ４）３７、有線ＬＡＮインターフェース（ホスト接続用１００／１０ＢａｓｅＴ）３８、Bluetooth拡張ボード３９、802.11b拡張ボード４０、802.11a拡張ボード４１を備えている。

【００３９】

ルータ回路３０は、アクセスポイント１に接続されたクライアントパソコン３、４、５、６、ＰＤＡ７、８、９間のＴＣＰ／ＩＰによるトラフィックや、イントラネットやインターネット等の基幹ネットワークへのトラフィックに対してパケットフィルタやルーティング（通信経路選択）を実現する。認証サーバ回路３１は、８０２．１ｘ等の認証を行う。ＰＣカードインターフェース３２は、認証サーバ回路３１へアカウントデータを供給する不揮発性メモリカード３３のインターフェースである。不揮発性メモリカード３３は、認証サーバ回路３１へ供給するアカウントデータを保持する。無線通信ボードインターフェース３４、３５、３６、３７は、無線通信手段毎に異なる無線通信ボードを接続するためのインターフェースである。

【００４０】

有線ＬＡＮインターフェース３８は、アクセスポイント１とイントラネットやインターネット等の基幹ネットワークを接続するためのインターフェースである。Bluetooth拡張ボード３９は、無線通信手段の一つであるBluetooth方式に対応し、無線通信ボードインターフェース３４、３５、３６、３７に挿入することでアクセスポイント１にBluetoothによる無線通信機能を提供する。802.11b拡張ボード４０は、無線通信手段の一つである802.11b方式に対応し、無線通信ボードインターフェース３４、３５、３６、３７に挿入することでアクセスポイント１に802.11bによる無線通信機能を提供する。802.11a拡張ボード４１は、無線通信手段の一つである802.11a方式に対応し、無線通信ボードインターフェース３４、３５、３６、３７に挿入することでアクセスポイント１に802.11aによる無線通信機能を提供する。

【００４１】

図５に示すように、本発明によるアクセスポイントは、無線通信ボードインターフェース３４、３５、３６、３７に無線通信拡張ボード３９、４０、４１を挿入することで無線通信を実現する。このため、無線通信ボードインターフェース３４、３５、３６、３７は、複数の無線方式に対応するために柔軟性に富む構成を取る必要がある。

【００４２】

図６は無線通信ボードインターフェースの構成を示すブロック図である。無線通信ボードインターフェースは、無線通信ボードインターフェースコネクタ（アクセスポイントコネクタ）５０と、無線ＬＡＮ　ＲＦ５１１、無線ＬＡＮ　ＢＢ（Base Band）５１２、無線ＬＡＮアクセスポイントコントローラ５１３を備え、無線ＬＡＮの規格である802.11方式に対応した無線ＬＡＮ拡張ボード５１と、ＣＰＵ５２１、Bluetoothモジュール５２２、ＵＡＲＴ（Universal Asynchronous Receiver Transmitter：汎用非同期送受信回路）５２３、ＦＰＧＡ（Field Programmable Gate Array）５２４、ＲＡＭ５２５、ＲＯＭ５２６、ＦＩＦＯ（First In First Out）メモリ５２７、ＦＩＦＯメモリ５２８を備え、Bluetoothに対応したBluetooth拡張ボード５２に対応するように構成されている。

【００４３】

図６によれば、無線ＬＡＮ拡張ボード５１が、上記ルータ回路３０と接続されるインターフェースは、有線ＬＡＮインターフェース規格である802.3uとシリアルポート（RS232C）であり、Bluetooth拡張ボード５２が、上記ルータ回路３０と接続されるインターフェースは、ＦＩＦＯメモリ５２７、５２８を介したバス接続とシリアルポート（RS232C）である。このように、接続する無線通信手段によって、無線通信ボードインターフェースコネクタ５０に要求される仕様は異なる場合があるため、本発明のアクセスポイント１では、

無線ＬＡＮ拡張ボード５１、Bluetooth拡張ボード５２のいずれにも対応できるように双方のインターフェース仕様を網羅した信号に対応する。

【００４４】

更に、本発明のアクセスポイント１には、複数の無線通信ボードインターフェースコネクタ５０を装備することにより、異なる無線通信拡張ボードの混載や同一無線通信ボードの複数搭載を実現する。異なる無線通信拡張ボードの混載によって、図１におけるクライアントパソコン３、４、５、６の利用する無線通信手段１０、１１、１２、１３が８０２．１１ｂ方式であり、ＰＤＡ７、８、９の利用する無線通信手段１４、１５、１６がBluetooth方式であるような場合にも、１台のアクセスポイントで安全な無線通信ネットワークを構築することができる。

【００４５】

また、同一無線通信ボードの複数搭載によって、１台当たりの無線通信拡張ボードがサポート可能なクライアント数の制限をなくすことが可能となる。例えば、Bluetooth方式の無線通信拡張ボード３９、５１を４個の無線通信ボードインターフェース３４、３５、３６、３７に挿入することによって、Bluetooth方式のPicoネット生成上の上限であるクライアント数７名という制限を無くし、各ボード７名ずつ、計２８名による無線通信ネットワークを生成することができる。無線ＬＡＮ方式の場合も、論理上の無線通信拡張ボード４０、４１、５２のクライアント対応数の上限は２５５クライアントと問題のないレベルであるが、実際には、無線通信拡張ボード４０、４１、５２の処理能力の問題から、無線通信拡張ボード１枚当たり、１０～１５クライアント程度の制限が発生する。この場合も無線ＬＡＮ対応の無線通信拡張ボード４０、４１、５２を複数、無線通信ボードインターフェース３４、３５、３６、３７に挿入することで、クライアント数制限を緩和することができる。

【００４６】

図７は本発明のアクセスポイント１のルータ回路３０、認証サーバ回路３１、不揮発性メモリ用ＰＣカードインターフェース３２、無線通信ボードインターフェース３４、３５、３６、３７、有線ＬＡＮインターフェース３８部分の詳細構成を示すブロック図である。アクセスポイント１は、無線通信拡張ボード用インターフェース（APC1）７１、無線通信拡張ボード用インターフェース（APC2）７２、無線通信拡張ボード用インターフェース（APC3）７３、無線通信拡張ボード用インターフェース（APC4）７４、スイッチコントローラ７５、ＭＡＣ(Media Access Control)７６、ＲＡＭ７７、ＲＯＭ７８、ＣＰＵ７９、ＭＡＣ８０、ＰＨＹ（Physical Layer Protocol）８１、カードバス８２、電源８３を備えている。なお、図７全体をまとめてメインボードと称する。

【００４７】

図７に示すように、本発明のアクセスポイント１は、複数の無線通信拡張ボード用インターフェース（APC1・７１、APC2・７２、APC3・７３、APC4・７４）を備え、それらの各々に802.3uインターフェース、バスインターフェース、シリアルインターフェース（RS232C）を有することによって、いずれのコネクタにも上述した無線通信拡張ボード３９、４０、４１を挿入することが可能である。

【００４８】

ここで、本発明の特徴の一つとして、図５に示した認証サーバ回路３１をアクセスポイント１内に内蔵する点が挙げられるが、同機能を実現する最も簡単な方法は、図２に示した認証サーバ２４のために専用のＣＰＵやメモリからなる回路を与えて認証サーバ回路３１を構築し、認証サーバ回路３１とルータ回路３０をＴＣＰ／ＩＰに対応した802.3uのインターフェースで連結する方法である。しかし、このような方法を採ると、ＣＰＵとメモリから成る回路を重複して持つことになり無駄が多い。このため、本発明では、認証サーバ機能をルータ回路３０でエミュレーションすることでハードウェアリソースの無駄を省いている。即ち、図７におけるＣＰＵ７９部分で、ルーティング等のネットワークアプリケーションと、認証サーバエミュレーション（RADIUSサーバエミュレーション）をコンカレント（並列）に実行することで、効率の良いハードウェアを実現する。

【００４９】
図８は本発明のアクセスポイント１のルータ回路３０、認証サーバ回路３１、ＰＣカードインターフェース３２、無線通信ボードインターフェース３４、３５、３６、３７、有線ＬＡＮインターフェース３８から成るメインボード部分と、Bluetooth拡張無線通信ボード３９、無線ＬＡＮ拡張無線通信ボード４０、４１の各部分で実行されるソフトウェア処理のスタック構造を示す図である。
【００５０】
図８に示すように、認証サーバエミュレーションであるRADIUSサーバエミュレーションはメインボード上で実行される。また、認証サーバエミュレーションをメインボードで行うが故に、メインボード上のＣＰＵには高いパフォーマンスが要求される。このパフォーマンスを有効利用するため、図８に示すようにBluetooth拡張無線通信ボード３９（図５参照）上では、負荷の重いＬＡＮプロファイルによるＴＣＰ／ＩＰへの対応は行わず、メインボード上でBNEP上にＴＣＰ／ＩＰのソフトウェア階層を付加する。このような対応を行うことで、Bluetooth拡張無線通信ボード３９では、比較的処理の軽いＰＡＮプロファイルを実行すれば良くなるため、Bluetooth拡張無線通信ボードの有する通信性能を有効に利用することができる。
【００５１】
また、無線ＬＡＮ（８０２．１１）とBluetoothの両無線通信手段をＴＣＰ／ＩＰレベルで統合する目的は、両者をＴＣＰ／ＩＰの階層で揃えることによって、その上位に位置するネットワークアプリケーションが実際の無線通信手段に関わらず共通に利用できるためと、認証サーバへのアクセス手段をＴＣＰ／ＩＰに統一するためである。
【００５２】
以上説明したように、第１の実施の形態によれば、８０２．１ｘ方式に準拠した無線通信認証手段を用いて、安全な無線ネットワークを、簡易なシステム構成で簡単かつ柔軟に構築することができる。このようなＰＡＮ構築のニーズは、会議等でテンポラリに安全なネットワークを構築したい場合等に最適である。
【００５３】
［第２の実施の形態］
上記第１の実施の形態で述べたように、本発明におけるアクセスポイント１は、各種の無線通信方式に柔軟に対応可能な無線通信部と基幹ネットワークへも接続可能なルータ回路３０、認証サーバ回路３１、認証サーバ回路３１にアカウントデータを供給するＰＣカードインターフェース３２をコンパクトな筐体に装備し、クライアントデバイス３、４、５、６、７、８、９との安全な無線ネットワークを簡易な構成で柔軟に実現できることを特徴としている。
【００５４】
上記第１の実施の形態では、８０２．１ｘベースの認証を行うためのクライアントデータを認証サーバに供給する手段、データを更新する手段、また、アクセスポイント側の無線通信手段選定の柔軟性を確保するための手段について述べてきた。これに対し、第２の実施の形態では、本発明におけるクライアントデバイス（クライアントパソコン、ＰＤＡ）側の例について述べる。
【００５５】
図９は第２の実施の形態に係るクライアントデバイスとしてのＰＤＡの構造を示す外観図であり、本発明の特徴を最も良く表す図である。クライアントデバイス（ＰＤＡ）６０は、無線通信に対応したものである。ＣＦカードスロット６１は、ＰＤＡ６０の筐体に装備されている。ＣＦカード６２は、ＣＦカードスロット６１に挿入することでＰＤＡ６０へクライアントデータを供給する着脱式不揮発性メモリ装置である。
【００５６】
上記第１の実施の形態では、アクセスポイント１へ認証サーバ用アカウントデータを供給する着脱式不揮発性メモリ装置上のアカウントデータは、クライアントデバイスで稼働するアカウントデータベース更新プログラムによって、容易に更新可能であることを述べた

。アカウントデータベース更新プログラムで作成したアカウントデータは、アクセスポイント１だけでなく、クライアントデバイス（ＰＤＡ）６０でも利用可能である。この場合、アクセスポイント１側では全クライアントのデータをまとめて管理すればよいが、クライアントデバイス（ＰＤＡ）６０は各々異なるアカウントを利用して接続を行わなければならないため、どのアカウントが利用可能であるかを判定する必要がある。

【００５７】

図１０はクライアントデバイス（ＰＤＡ）６０でＣＦカード（着脱式不揮発性メモリ装置）６２からアカウントデータを取得する際の処理を示すフローチャートである。図１０に示すように、クライアントデバイス６０が、ＣＦカード（着脱式不揮発性メモリ装置）６２からアカウントデータを取得する際は、現在利用中のアカウントデータをクライアントデバイス６０上のメモリへ読み出した後（ステップＳ１０１）、読み出したアカウントデータに未使用のアカウントデータが含まれているか否かをチェックする（ステップＳ１０２）。もし、未使用アカウントデータが存在しない場合は、新たにアカウントデータを追加し（ステップＳ１０３）、ステップＳ１０４へ移行する。未使用アカウントデータが存在する場合は、アカウントデータの追加を行わず、ステップＳ１０４へ移行する。

【００５８】

上記ステップＳ１０２でＹＥＳの場合または上記ステップＳ１０３の処理後、未使用アカウントデータを取得し（ステップＳ１０４）、そのアカウントデータをクライアントデバイス（ＰＤＡ）６０のメモリに保存する。更に、利用したアカウントデータには使用済みフラグを付加した後（ステップＳ１０５）、更新したアカウントデータをＣＦカード（着脱式不揮発性メモリ装置）６２へ書き込み（ステップＳ１０６）、次のクライアントデバイス（ＰＤＡ）６０のアカウントデータ読み出しに備える。

【００５９】

なお、アカウントデータの追加を実施した場合は、アカウントデータの更新を実施したＣＦカード（着脱式不揮発性メモリ装置）６２をアクセスポイント１に挿入し、上記図４で示したアカウントデータの更新処理を実施することで、更新されたアカウントデータをアクセスポイント１に反映する。アカウントデータの追加を実施しない場合は、アクセスポイント１に保存されているアカウントデータは変更する必要が無いため、ＣＦカード（着脱式不揮発性メモリ装置）６２のアクセスポイント１への挿入作業を実施する必要はない。

【００６０】

また、無線ＬＡＮをあるアクセスポイントとクライアントに限定して構築する際、ESS ID（Extended Service Set Identity：アクセスポイントがカバーするエリアを無線端末が移動する際に自動的に接続を切り替えるローミングの設定などで利用）をネットワーク毎に変更することは一般的であるが、本発明では、ESS ID情報をアカウントデータと共に着脱式不揮発性メモリ装置に保存しておき、ＰＡＮ構築時に読み出したESS ID情報に基づいて無線ＬＡＮネットワークを構築することで、所望のアクセスポイントとクライアントデバイス、または、所望のアクセスポイント内の拡張無線通信カードとクライアントデバイスをネットワーク接続することができる。なお、アクセスポイントに内蔵したリアルタイマクロック情報と、着脱式不揮発性メモリ装置から供給されるＰＡＮ構築の時間を示す情報とを比較し、前記両情報が一致したアカウントデータに基づいてアクセスポイントの無線通信パラメータを自動設定する。

【００６１】

図１１はアカウントデータと関連付けたESS ID情報の例を示す図である。この例では、ESS ID "106efc"に関連付けられた７クライアントが、同じ"106efc"のESS IDを有するアクセスポイントに接続される。また、ESS ID "152e42"に関連付けられた２クライアントは、"152e42"のESS IDを有するアクセスポイントに接続される。同様に、本発明における１台のアクセスポイント内部に異なる無線通信手段または同一の無線通信手段に対応する拡張無線通信カードを複数有するアクセスポイントでは、上述したアカウントデータに関連づけられたESS ID情報を用いることで、アクセスポイント内部の拡張無線通信カードとク

ライアントデバイスのネットワーク接続が可能となる。

【００６２】

以上説明したように、第２の実施の形態によれば、上記第１の実施の形態と同様に、安全な無線ネットワークを、簡易なシステム構成で簡単かつ柔軟に構築することができる。

【００６３】

［第３の実施の形態］

第１及び第２の実施の形態で述べたように、本発明におけるアクセスポイント内の認証サーバ回路及びクライアントデバイスは、それらで構築するＰＡＮ用のアカウントデータやESS ID等の情報を着脱式不揮発性メモリ装置で入手することを特徴としている。しかし、これらの情報は着脱式不揮発性メモリ装置からだけではなく、ネットワーク経由でアクセスポイントやクライアントデバイス内に内蔵された不揮発性メモリに事前に取り込んで使用することも可能である。

【００６４】

このためには、ＰＡＮを構築しようとするユーザがアカウントデータベース作成プログラムを起動してアカウントデータを作成し、作成したデータを、電子メールに添付して送付し、各クライアントデバイスのユーザが添付データの保存作業を行うか、P2P等のファイル共有プログラムを用いて共有フォルダにアカウントデータを置き、それを各クライアントデバイスユーザが事前にダウンロードし、保存しておくことが必要である。

【００６５】

これらの手段を用いれば、着脱式不揮発性メモリ装置を用いずにアカウントデータやESS IDを入手することが可能である。但し、アクセスポイント自体は、電子メールアドレスを有しておらず、且つネットワークに常時接続されているとは限らないため、アカウントデータの管理は、ネットワーク経由の保存と着脱式不揮発性メモリ装置による供給を併用することが望ましい。

【００６６】

以上説明したように、第３の実施の形態によれば、上記第１の実施の形態と同様に、安全な無線ネットワークを、簡易なシステム構成で簡単かつ柔軟に構築することができる。

【００６７】

［他の実施の形態］

なお、上記実施の形態では、図１に示すような構成のネットワークシステムを例に挙げたが、本発明はこれに限定されるものではなく、クライアントデバイスの設置台数、クライアントデバイスの種類等は任意とすることが可能である。

【００６８】

また、本発明は、複数の機器から構成されるシステムに適用しても、１つの機器からなる装置に適用してもよい。上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憶した記憶媒体等の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（またはＣＰＵやＭＰＵ）が記憶媒体等の媒体に格納されたプログラムコードを読み出し実行することによっても、本発明が達成されることは言うまでもない。

【００６９】

この場合、記憶媒体等の媒体から読み出されたプログラムコード自体が上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憶媒体等の媒体は本発明を構成することになる。プログラムコードを供給するための記憶媒体等の媒体としては、例えば、フロッピー（登録商標）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、或いはネットワークを介したダウンロードなどを用いることができる。

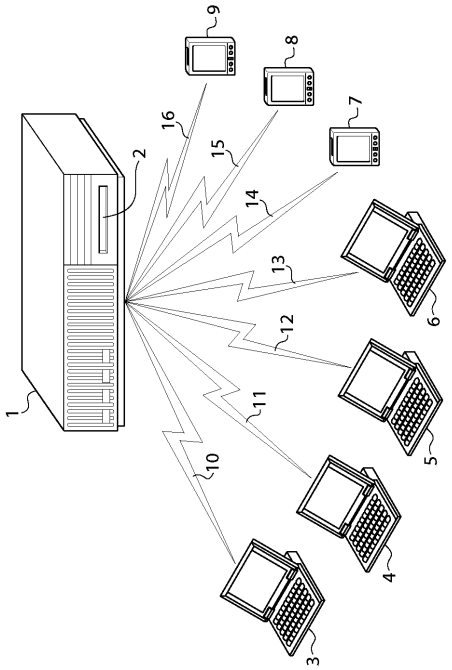
【００７０】

また、コンピュータが読み出したプログラムコードを実行することにより、上述した実施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などが実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合も、本発明に含まれることは言うまでもない。

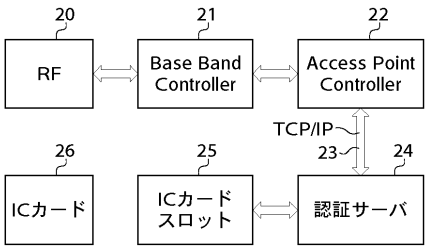
【００７１】
更に、記憶媒体等の媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合も、本発明に含まれることは言うまでもない。
【００７２】
以上説明したように、上記各実施の形態によれば、安全な無線ネットワークを、簡易なシステム構成で簡単かつ柔軟に構築することができる。このようなネットワーク構築のニーズは、会議等でテンポラリに安全なネットワークを構築したい場合等に最適である。
【発明の効果】
以上説明したように、本発明によれば、着脱式の記憶装置に保存されたアカウントデータの中の現在時刻に対応したアカウントデータを用いることにより、アクセスポイントと無線通信装置間の認証を行うことができる。従って、時間毎のネットワークの構築や管理を安全且つ容易に行うことができる。
【図面の簡単な説明】
【図１】本発明の第１の実施の形態に係るネットワークシステムの構成を示す概念図である。
【図２】第１の実施の形態に係るアクセスポイントの内部構造を示すブロック図である。
【図３】第１の実施の形態に係るアカウント作成プログラムの処理内容を示すフローチャートである。
【図４】第１の実施の形態に係るアクセスポイントのアカウントデータベース更新手順を示すフローチャートである。
【図５】第１の実施の形態に係るアクセスポイントの機能構成を示すブロック図である。
【図６】第１の実施の形態に係るアクセスポイント内部に設けた拡張無線通信コネクタと８０２．１１及びBluetooth拡張無線ボードの関係を示すブロック図である。
【図７】第１の実施の形態に係るアクセスポイントのルータ回路の構成を示すブロック図である。
【図８】第１の実施の形態に係るアクセスポイントのソフトウェア階層構造を示す図である。
【図９】本発明の第２の実施の形態に係るクライアントデバイスの構成を示す外観図である。
【図１０】第２の実施の形態に係るクライアントデバイスのアカウントデータ取得処理を示すフローチャートである。
【図１１】第２の実施の形態に係るアカウントデータベースにおけるアカウントデータとESS IDの記録形態を示す図である。
【符号の説明】
１　アクセスポイント
２　ＩＣカードスロット
３～６　クライントパソコン
７～９　ＰＤＡ
１０～１６　無線通信手段
２０　無線通信の電波生成部
２１　無線通信制御回路
２２　アクセスポイントコントローラ
２４　認証サーバ
２５　ＩＣカードスロット
２６　着脱式不揮発性メモリ装置
３０　ルータ回路
３１　認証サーバ回路

３２　ＰＣカードインターフェース
３３　不揮発性メモリカード
３４～３７　無線通信ボードインターフェース
３８　有線ＬＡＮインターフェース
３９　Bluetooth拡張ボード
４０　802.11b拡張ボード
４１　802.11a拡張ボード
５０　無線通信ボードインターフェース
５１　802.11無線通信拡張ボード
５２　Bluetooth無線通信拡張ボード
６０　ＰＤＡ
６１　ＣＦカードスロット
６２　着脱式不揮発性メモリ装置

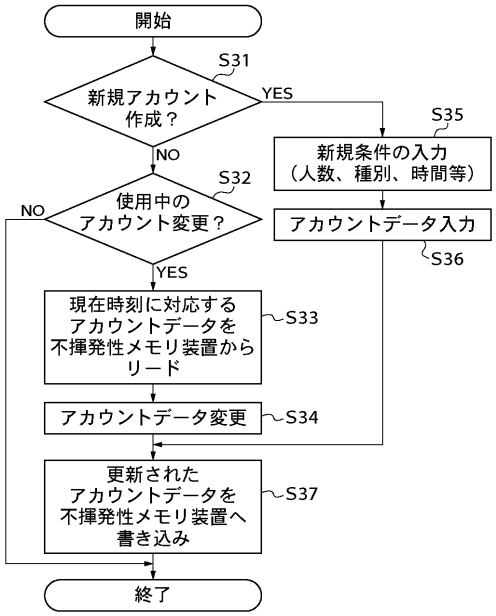
【図１】



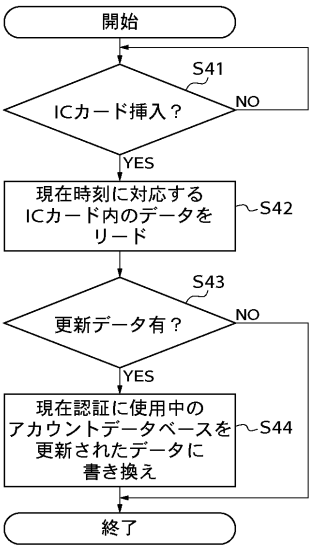
【図２】



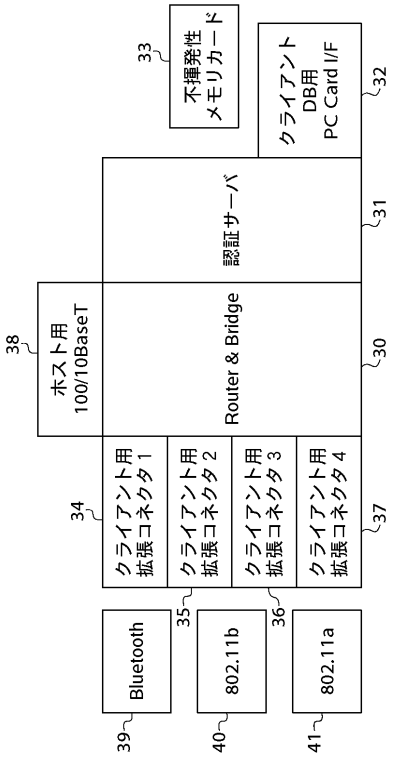
【図３】


開始
新規アカウント作成？
S31
YES
NO
新規条件の入力（人数、種別、時間等）
S35
使用中のアカウント変更？
S32
NO
YES
アカウントデータ入力
S36
現在時刻に対応するアカウントデータを不揮発性メモリ装置からリード
S33
アカウントデータ変更
S34
更新されたアカウントデータを不揮発性メモリ装置へ書き込み
S37
終了

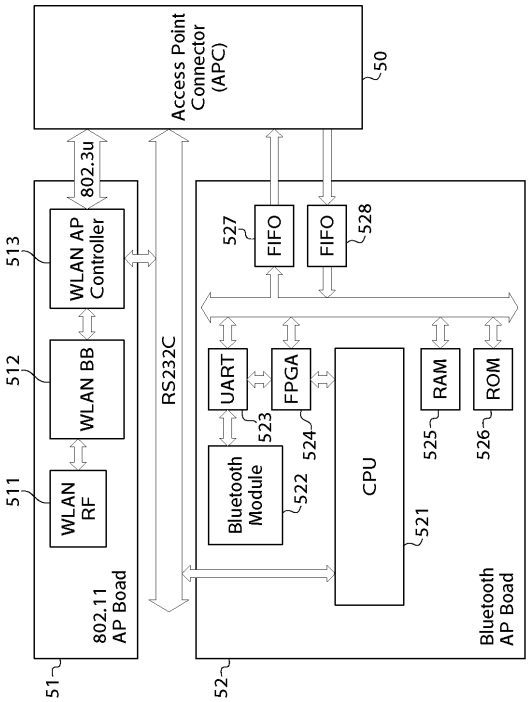
【図４】


開始
ICカード挿入？
S41
NO
YES
現在時刻に対応するICカード内のデータをリード
S42
更新データ有？
S43
NO
YES
現在認証に使用中のアカウントデータベースを更新されたデータに書き換え
S44
終了

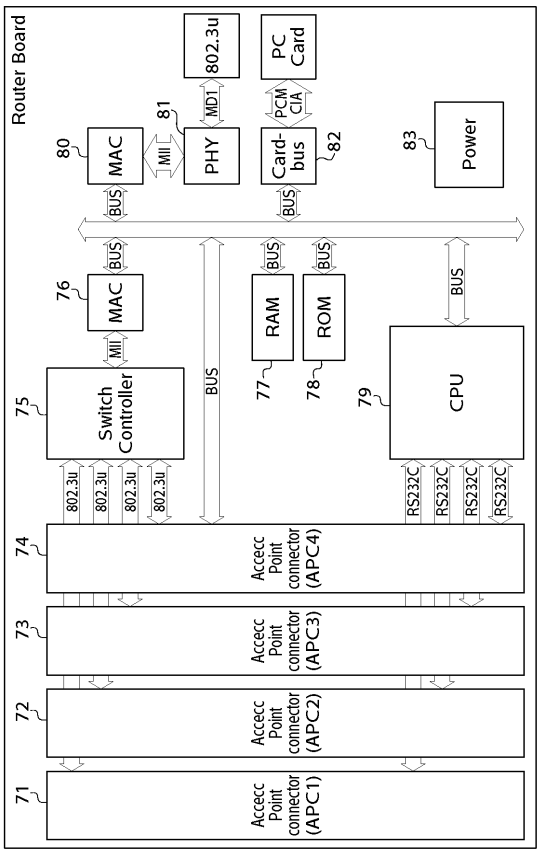
【図５】


33
不揮発性メモリカード
クライアントDB用PC Card I/F
32
認証サーバ
31
38
ホスト用100/10BaseT
Router & Bridge
30
34
クライアント用拡張コネクタ1
クライアント用拡張コネクタ2
クライアント用拡張コネクタ3
クライアント用拡張コネクタ4
37
35
36
Bluetooth
802.11b
802.11a
39
40
41

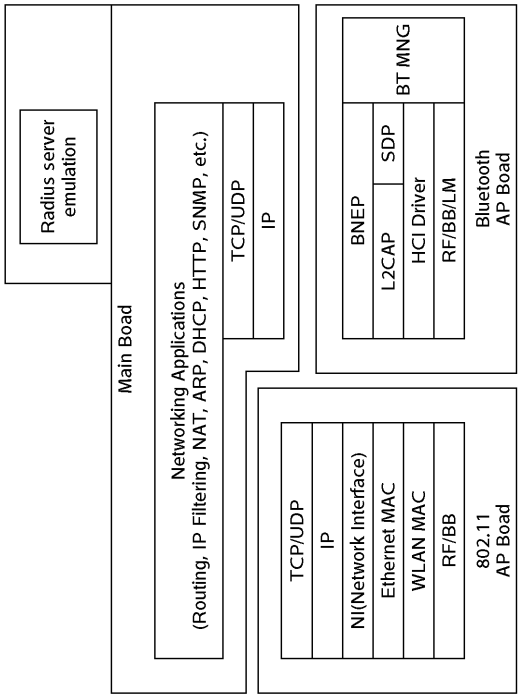
【図６】


Access Point Connector (APC)
50
802.3u
513
WLAN AP Controller
512
WLAN BB
511
WLAN RF
802.11 AP Boad
51
RS232C
527
FIFO
528
FIFO
UART
523
FPGA
524
Bluetooth Module
522
CPU
521
525
RAM
526
ROM
Bluetooth AP Boad
52

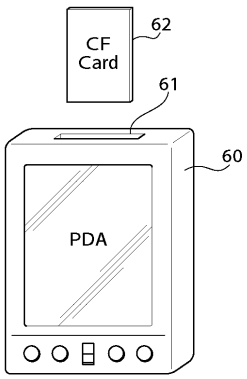
【図７】


Router Board
802.3u
PC Card
MD1
PCM CIA
81
80
MAC
MII
PHY
Card-bus
82
83
Power
BUS
76
MAC
RAM
ROM
77
78
79
CPU
75
Switch Controller
802.3u
RS232C
74
Accecc Point connector (APC4)
73
Accecc Point connector (APC3)
72
Accecc Point connector (APC2)
71
Accecc Point connector (APC1)

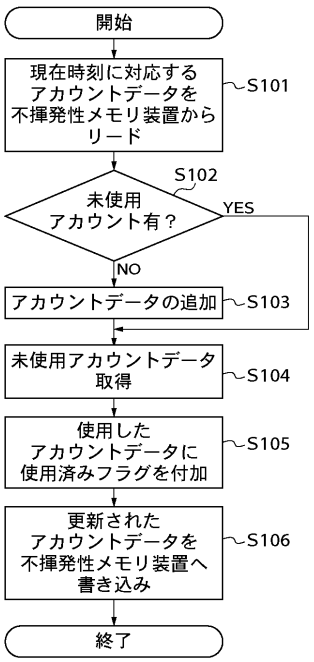
【図８】


Radius server emulation
Main Boad
Networking Applications
(Routing, IP Filtering, NAT, ARP, DHCP, HTTP, SNMP, etc.)
TCP/UDP
IP
BT MNG
BNEP
SDP
L2CAP
HCI Driver
RF/BB/LM
Bluetooth AP Boad
TCP/UDP
IP
NI(Network Interface)
Ethernet MAC
WLAN MAC
RF/BB
802.11 AP Boad

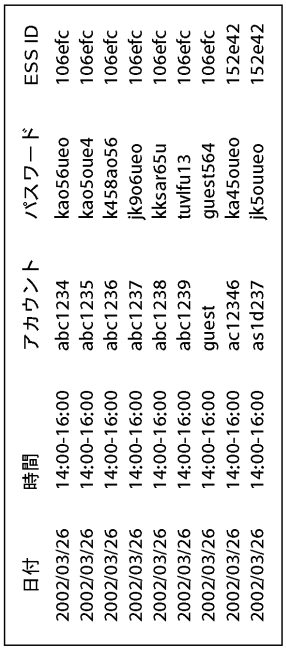
【図９】


CF Card
62
61
60
PDA

【図１０】


開始
現在時刻に対応するアカウントデータを不揮発性メモリ装置からリード
S101
S102
未使用アカウント有？
YES
NO
アカウントデータの追加
S103
未使用アカウントデータ取得
S104
使用したアカウントデータに使用済みフラグを付加
S105
更新されたアカウントデータを不揮発性メモリ装置へ書き込み
S106
終了

【図１１】



日付	時間	アカウント	パスワード	ESS ID
2002/03/26	14:00-16:00	abc1234	kao56ueo	106efc
2002/03/26	14:00-16:00	abc1235	kao5oue4	106efc
2002/03/26	14:00-16:00	abc1236	k458ao56	106efc
2002/03/26	14:00-16:00	abc1237	jk9o6ueo	106efc
2002/03/26	14:00-16:00	abc1238	kksar65u	106efc
2002/03/26	14:00-16:00	abc1239	tuvftu13	106efc
2002/03/26	14:00-16:00	guest	guest564	106efc
2002/03/26	14:00-16:00	ac12346	ka45oueo	152e42
2002/03/26	14:00-16:00	as1d237	jk5ouueo	152e42

フロントページの続き

(72)発明者　立川　博英
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　矢頭　尚之

(56)参考文献　特開２００１－１８９７２２（ＪＰ，Ａ）
特開２００２－０４４７３８（ＪＰ，Ａ）
特開２００２－１５５１１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/28
H04L 9/32
H04Q 7/38