(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年9 月21 日 (21.09.2006)

PCT

(10) 国際公開番号
WO 2006/098116 A1

(51) 国際特許分類:
*H04Q 7/38* (2006.01) *H04L 12/28* (2006.01)

(21) 国際出願番号: PCT/JP2006/302995

(22) 国際出願日: 2006 年2 月21 日 (21.02.2006)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2005-072129 2005 年3 月15 日 (15.03.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 角丸 貴洋 (KAKUMARU, Takahiro) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 鈴木 弘男 (SUZUKI, Hiroh); 〒1030023 東京都中央区日本橋本町２丁目３番１号 茶の木屋ビル 鈴木国際特許事務所 Tokyo (JP).

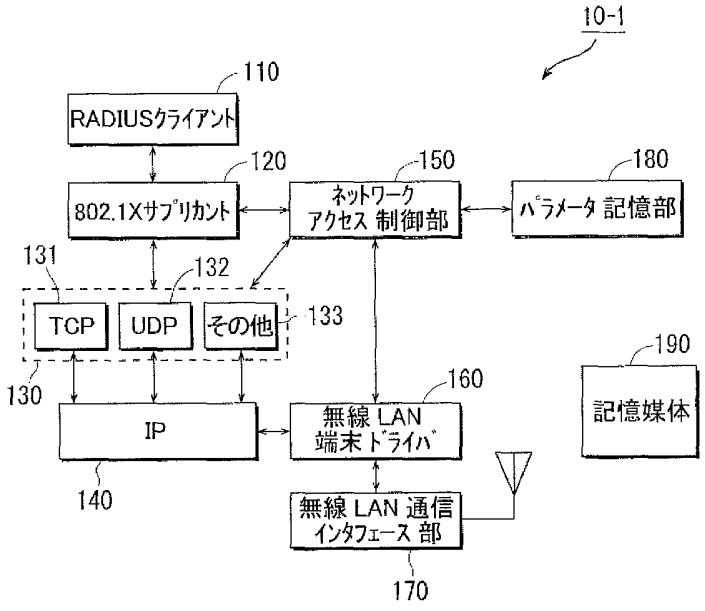
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG,

[続葉有]

(54) Title: AUTHENTICATION METHOD IN RADIO COMMUNICATION SYSTEM, RADIO TERMINAL DEVICE AND RADIO BASE STATION USING THE METHOD, RADIO COMMUNICATION SYSTEM USING THEM, AND PROGRAM

(54) 発明の名称: 無線通信システムにおける認証方式、それを備える無線端末装置と無線基地局、それらを用いた無線通信システム及びプログラム




110... RADIUS CLIENT
120... 802.1X SUPPLICANT
150... NETWORK ACCESS CONTROL UNIT
180... PARAMETER STORAGE UNIT
133... OTHERS
160... RADIO LAN TERMINAL DRIVER
170... RADIO LAN COMMUNICATION INTERFACE UNIT
190... STORAGE MEDIUM

(57) **Abstract:** For communication with a base station on an IP network, radio terminals (10-1 to 10-6) have a function for encapsulating and releasing encapsulation of a packet for preparatory authentication defined in the IEEE 802.11i at a RADIUS client unit (110) by an authentication packet communicable on the IP network. For communication with the radio terminals on the IP network, the base station (30) has a function for encapsulating and releasing encapsulation of a packet for preparatory authentication defined in the IEEE 802.11i at a RADIUS server (320) by an authentication packet communicable on the IP network. Thus, it is possible to provide an authentication method in a radio communication system enabling a preparatory authentication between a radio terminal and a base station even between different IP sub-networks. There are also disclosed a radio terminal device and a radio base station using this authentication method, a radio communication system using them, and a program.

(57) 要約: ＩＰネットワーク上で基地局とやり取りするために、無線端末（１０－１～１０－６）は、ＩＥＥＥ　８０２．１１ｉで規定される事前認証のためのパケットをＲＡＤＩＵＳクライ

[続葉有]

WO 2006/098116 A1

CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

アント部（１１０）にてＩＰネットワーク上で通信可能である認証パケットでカプセル化及びカプセル化を解く機能を、一方、前述同様のやり取りを無線端末と行うために、基地局（３０）は、ＩＥＥＥ　８０２．１１ｉで規定される事前認証のためのパケットをＲＡＤＩＵＳサーバ部（３２０）にてＩＰネットワーク上で通信可能である認証パケットでカプセル化及びカプセル化を解く機能をそれぞれ保持することで、異なるＩＰサブネットワーク間においても無線端末及び基地局間での事前認証を可能とする無線通信システムにおける認証方式、この認証方式を備える無線端末装置と無線基地局、それらを用いた無線通信システム、及びプログラム。

# 明 細 書

## 無線通信システムにおける認証方式、それを備える無線端末装置と無線基地局、それらを用いた無線通信システム及びプログラム

### 技術分野

[0001] 本発明は、無線通信システムにおける認証方式、この認証方式を備える無線端末装置と無線基地局、それらを用いた無線通信システム、及びプログラムに関し、特にIP(Internet Protocol)ネットワーク上において予め認証処理を実行することができる無線通信システムにおける認証方式、この認証方式を備える無線端末装置と無線基地局、それらを用いた無線通信システム、及びプログラムに関する。

### 背景技術

[0002] 近年、無線LANセキュリティの脆弱性が指摘されている。つまり、無線LANに用いられるWEP(Wired Equivalent Privacy)キーによって暗号化されたデータも解析されてしまう可能性があると同時に、WEPキーが解析されることによって、無線LANを介するすべてのデータ通信まで解析されてしまう危険性があることが指摘されている。

[0003] これらの危険性をできるだけ排除するために、IEEE(Institute of Electrical and Electronic Engineers) 802.11iというIEEE 802.11無線LANのセキュリティを強化するための規格が規定されている。(IEEE P802.11i/D10.0、"Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements"、米国、2004年、8.4.6.1 Pre-authentication and RSNA Key Managementの項、参照)。

[0004] IEEE 802.11iは、IEEE 802.11無線LANシステムの無線区間における前記のような脆弱性を解決するために、IEEE 802.1Xに基づいたアクセス制御、安全なセッション管理、動的な鍵交換や鍵管理、WEP暗号化アルゴリズムをより強化した無線区間のデータ暗号化アルゴリズムなどを規定している。(IEEE 802.1X、"Port-Based Network Access Control"、米国、2001年、6. Principles of o

perationの項、参照)。

[0005] IEEE 802. 1Xは、ユーザー認証及び鍵交換のフレームワークを規定している。IEEE 802. 11iでは、新たに鍵交換方式である4ウェイハンドシェイク及びグループキーハンドシェイク、鍵の用途を決める鍵階層(Key hierarchy)、無線区間の暗号化アルゴリズム(CipherSuites)を定義している。

[0006] 図1は、通常のIEEE 802. 11i及びIEEE 802. 1Xを利用した場合の無線LAN接続シーケンスを示している。

[0007] 図1に示すように、無線端末が基地局を介してデータ通信が可能となるまでには、IEEE 802. 11ネゴシエーション(802. 11 Authentication、Assocaition)、IEEE 802. 1X認証(EAP[Extensible Authentication Protocol]認証)、IEEE 802. 11i鍵交換(4ウェイハンドシェイク、グループキーハンドシェイク)を必要とする。

[0008] IEEE 802. 1X認証を成功裏に完了することにより、無線端末と基地局は端末と基地局及び認証サーバ以外知りえないペアワイズマスターキー(Pairwise Master Key 以下、PMKと記す)を共有する。

[0009] このPMKは以後、無線端末と基地局間におけるデータ通信を暗号化するための鍵を決定する処理である鍵交換において通信内容の暗号化、通信内容の改竄確認のために使用される。PMKはIEEE 802. 1X認証の結果、無線端末と認証サーバの両者によって共有され、認証サーバから基地局に対して認証成功を通知するとともにPMKも一緒に通知することにより、無線端末と基地局で共有される。

[0010] 図2のネットワーク構成における無線端末1は、移動性を有しているので現在接続している基地局2から新しい基地局3に移動することができる。

[0011] 通常、無線端末1が新しい基地局3においてもこれまで接続していた基地局2によって提供されていたサービスを受けようとする場合、新しい基地局3に対してもう一度接続ネゴシエーション、つまり、IEEE 802. 11ネゴシエーション、IEEE 802. 1X認証、IEEE 802. 11i鍵交換シーケンスを必要とする。

[0012] しかし、基地局間を移動する毎に前述シーケンスを行うことによって、その期間はネットワークとの通信が断絶されてしまうため、提供するサービスに影響を及ぼしかねな

い。この問題を解決するために、前述シーケンスを簡略化する方式がIEEE 802．11iにてPMKキャッシュとして提案されている。

[0013] 図3は、前述PMKキャッシュを使用した場合の無線LAN接続シーケンスを示している。

[0014] PMKキャッシュは、一度、成功裏に認証が完了し接続した基地局に対して無線端末及び前述基地局がそのときに取得したPMKを保持しておき、再び同じ基地局に接続するときに保持しておいたPMKを利用して、IEEE 802．1X認証の処理を省略する仕組みとなっている。

[0015] 無線端末は、前述基地局に対して以前取得したPMKを識別するための識別子をAssociation RequestフレームもしくはReassociation Requestフレームにて含むことにより基地局に対してPMKキャッシュを利用したい旨を通知する。

[0016] PMKを識別するための識別子を含むAssociation RequestフレームもしくはReassociation Requestフレームを受信した基地局は、同様に自身で保持している前述無線端末のためのPMKが存在するならば引き続きIEEE 802．1X認証ではなくIEEE 802．11i鍵交換シーケンスを行う。

[0017] その際、IEEE 802．11i鍵交換シーケンスの一番目のフレームにおいて選択したPMK識別子を含めることにより無線端末と基地局での確認が行われる。

[0018] なお、前述無線端末のためのPMKが存在しないならば通常通り引き続きIEEE 802．1X認証を開始する。このようにPMKキャッシュを利用することによりIEEE 802．1X認証シーケンスを省略することが可能となる。

[0019] しかし、前述PMKキャッシュの問題点として、一度成功裏に認証が完了し接続した基地局との接続においてのみ有効であるということが挙げられる。

[0020] この点を一部解決するために、現在接続している基地局を介して新しく接続する基地局と事前にIEEE 802．1X認証を行うことでPMKを取得しておくことによって、一度も接続したことのない基地局に対してもPMKキャッシュを利用できるようにする方式が同様にIEEE 802．11iにて事前認証（Preauthentication）として提案されている。

[0021] 図4は、前述事前認証を使用した場合の無線LAN接続シーケンスを示している。

[0022] 無線端末は現在接続している基地局とは成功裏に認証が完了し動的に設定された鍵を用いて暗号化されたデータ通信が行えている状態である。

[0023] この状態で無線端末は新しく接続しようとする基地局、つまり事前認証の対象となる基地局が報知しているビーコンを取得することにより前述基地局を検出し、事前認証を開始する。事前認証は、IEEE 802.1Xプロトコルおよびステートマシンを利用し、イーサフレームのイーサタイプを通常は88－8Eを使う代わりに88－C7を使うことで事前認証であること識別する。

[0024] イーサタイプ88－C7のフレームを受信した基地局は、あて先アドレスに記述されたMACアドレスを保持する装置に対して前述フレームを転送する。

[0025] また事前認証のフレームはあて先アドレスに事前認証の対象である基地局のBSSIDを指定し、基本サービスセットの範囲には現在接続している基地局のBSSIDを指定することで、無線端末は現在接続している基地局を介して事前認証の対象である基地局と事前認証を行うことが可能となる。

[0026] なお、事前認証の対象である基地局のBSSIDは事前認証の対象である基地局が報知しているビーコンから取得される。また、認証自体はIEEE 802.1X認証と同じであり、成功裏に認証が完了することで無線端末と事前認証の対象である基地局とで新たなPMKが共有される。PMKが共有されると、無線端末は事前認証済みの新たな基地局との接続ネゴシエーションにPMKキャッシュを利用することができる。

[0027] しかし、前述事前認証の問題点として、現在接続している基地局と事前認証の対象である基地局が同じブロードキャストドメインのネットワーク、言い換えると同じIPサブネットワーク内にのみ適用可能である、ということが挙げられる。つまり、IPサブネットワークを越えて基地局が位置する場合には適用できないということである。

## 発明の開示

## 発明が解決しようとする課題

[0028] 第1の問題点は、ブロードキャストドメイン（サブネットワーク）内でしか事前認証を行うことができないということである。その理由は、従来の事前認証システムではブロードキャストドメインを超えた事前認証について何ら考慮されていないためである。

[0029] 第2の問題点は、事前認証の対象となる基地局を識別するためのIPアドレスを、事

前認証を行おうとする無線端末は取得することができないということである。その理由は、第1の問題点の理由と同じである。

[0030] 本発明は、無線端末が現在接続している基地局が所属するブロードキャストドメインを超えて存在する基地局に対する事前認証を行い得る無線通信システムを提供することができる。

[0031] また、本発明は、無線端末が現在接続している基地局から他の基地局へ移動する場合に、移動先の基地局が移動元の基地局と異なるブロードキャストドメインに所属している場合でも、認証処理によるデータ通信不可期間を減少させ得る無線通信システムを提供することができる。

[0032] さらに、本発明は、事前認証のための情報も含むネットワーク接続のための情報を動的に取得／設定し得る無線通信システムを提供することができる。

## 課題を解決するための手段

[0033] 本発明による無線通信システムは、無線端末から基地局を介してネットワーク接続する際に認証サーバによる認証を必要とする通信システムであって、前記無線端末から別の基地局に対してIPネットワークを介して事前に認証を行う手段を前記無線端末及び前記基地局に備えている。

[0034] 本発明による基地局は、ネットワーク接続する際に認証サーバによる認証を必要とする無線端末を当該認証結果に応じて前記ネットワークへの接続を行う基地局であって、すでに接続されているネットワーク側を介した前記無線端末からのIPネットワーク上でやり取りされる事前認証を処理する手段を備えている。

[0035] 本発明による無線端末は、基地局を介してネットワーク接続する際に認証サーバによって認証を必要とする無線端末であって、接続されたネットワークを介してIPデータ通信を行うことが可能である基地局に対する事前認証を要求する手段を備えている。

[0036] 本発明による無線端末は、また、基地局に対応する情報を基地局管理サーバもしくは設定情報サーバから取得する手段を備えている。また、複数の無線通信手段を備えている。

[0037] 本発明による基地局管理サーバは、基地局に対するIPアドレス情報を保持しているサーバであって、無線端末からの基地局IPアドレス取得要求に対して該当する基

地局のIPアドレスを返す手段を備えている。

[0038] 本発明による設定情報サーバは、無線端末において無線ネットワーク接続に必要となる情報を保持しているサーバであって、無線端末からの取得要求に対して自身で保持している情報を返す手段を備えている。

[0039] すなわち、本発明の無線通信システムは、無線端末が基地局を介してネットワーク接続する際に認証サーバによって認証を必要とし、すでに接続しているネットワークを介して無線端末が基地局に対して事前認証を行う場合において、事前認証のやり取りをIPネットワーク上で行うことによって解決しようとするものである。

[0040] 本発明の無線通信システムでは、無線端末において保持する事前認証の対象とする基地局のIPアドレスから事前認証を行うことが可能となる。

[0041] あるいは、本発明の無線通信システムでは、基地局管理サーバにおいて保持する基地局に対応するIPアドレスを、無線端末が基地局管理サーバから基地局に対応するIPアドレスを取得して事前認証を行うことが可能である。

[0042] あるいは、本発明の無線通信システムでは、設定情報サーバにおいて保持するネットワーク接続に関する情報を、無線端末が設定情報サーバから取得してネットワーク接続に利用もしくは事前認証に利用することが可能である。

[0043] ここでの事前認証とは、例えば、IEEE 802.11iのPMKキャッシュを利用するための事前認証であり、IEEE 802.1X認証を現在接続しているIPネットワークを介して行ってしまうことにより予めPMKを共有しておくことであって、実際の無線LAN接続時には、IEEE 802.11ネゴシエーション及び鍵交換のみを行うことで無線LAN接続が可能である。

[0044] 本発明では、LAN回線またはWAN回線にてネットワークに接続して伝送媒体に無線を利用した基地局と、同じくLAN回線またはWAN回線にてネットワークに接続して伝送媒体に無線を利用した基地局と、LAN回線またはWAN回線に基地局を介して伝送媒体に無線を利用してネットワーク接続する無線端末と、LAN回線またはWAN回線に接続して基地局を介した無線端末からの認証要求を処理する認証サーバとから構成されている。

[0045] 無線端末は基地局を介して接続するためにユーザー認証もしくは相互認証を必要

とし、前記認証をすでに接続されているネットワークを介して行ってしまうことが可能である無線ネットワークシステムにおいて、無線端末と基地局がIPネットワーク上で事前認証を行うことができるようにすることによって、無線端末と基地局が異なるIPサブネットワーク内に存在しているときでも事前認証を行うことが可能となる。

## 発明の効果

[0046] 上記各態様を有する本発明は、下記の効果を奏する。

[0047] 第1の効果は、無線端末はIPサブネットワークが異なる基地局に対してもIEEE 802.11iのPMKキャッシュを利用するための事前認証を行うことができることにある。この結果、IPサブネットワークを越えて無線端末が初めて接続する基地局に移動した場合でもPMKキャッシュを利用することで接続ネゴシエーション処理を減らすことができ、接続に待たされる時間も減少される。その理由は、事前認証のためのやり取りをIPネットワーク上で行うことができるようにIP通信が可能である認証プロトコル処理手段を無線端末及び基地局にて備えるためである。

[0048] 第2の効果は、無線端末において事前認証の対象とする基地局のIPアドレスを予め設定しておく必要がないということにある。この結果、ユーザーによる設定間違いの減少や基地局のIPアドレスが変更になった場合の対応、沢山の設定をする煩わしさの減少などの効果が得られる。その理由は、無線端末においては動的に取得可能な手段を備え、管理しているサーバにその都度問い合わせることにより動的に取得することが可能であるためである。

## 図面の簡単な説明

[0049] [図1]図1は、従来のIEEE 802.11i及びIEEE 802.1Xを利用した場合の無線LAN接続動作を示すシーケンスチャート図である。

[図2]図2は、従来の無線通信システムの構成を示すブロック図である。

[図3]図3は、従来のIEEE 802.11i規定のPMKキャッシュを利用した場合の無線LAN接続動作を示すシーケンスチャート図である。

[図4]図4は、従来のIEEE 802.11i規定の事前認証(preauthentication)を利用した場合の無線LAN接続動作を示すシーケンスチャート図である。

[図5]図5は、本発明の第1の形態による無線通信システムの構成を示すブロック図で

ある。

[図6]図6は、図5に示す無線端末10－1の構成を示すブロック図である。

[図7]図7は、図5に示す基地局30の構成を示すブロック図である。

[図8]図8は、本発明の第1の形態における動作を示すシーケンスチャート図である。

[図9]図9は、本発明の第1の形態におけるデータの流れを示すブロック図である。

[図10]図10は、図6に示す無線端末構成における動作を示すシーケンスチャート図である。

[図11]図11は、図7に示す基地局構成における動作を示すシーケンスチャート図である。

[図12]図12は、本発明の第2の形態による無線通信システムの構成を示すブロック図である。

[図13]図13は、図12に示す無線端末10－2の構成を示すブロック図である。

[図14]図14は、本発明の第3の形態による無線通信システムの構成を示すブロック図である。

[図15]図15は、図14に示す無線端末10－3の構成を示すブロック図である。

[図16]図16は、本発明の第4の形態による無線通信システムの構成を示すブロック図である。

[図17]図17は、図16に示す無線端末10－4の構成を示すブロック図である。

[図18]図18は、本発明の第5の形態による無線通信システムの構成を示すブロック図である。

[図19]図19は、図18に示す無線端末10－5の構成を示すブロック図である。

[図20]図20は、本発明の第6の形態における無線通信システムの構成を示すブロック図である。

## 発明を実施するための最良の形態

[0050] 次に、本発明を実施するための幾つかの好ましい最良の形態について添付の図面を参照して詳細に説明する。

[0051] 以降の説明において、本発明の特徴を明確にするために、関連した公知機能及び構成に関する具体的な説明は省略する。

（第1の形態）

図5は、本発明の第1の形態による無線通信システムの構成を示す図である。

[0052] 図5を参照すると、第1の形態による無線通信システムは、LAN（Local Area Network）回線またはWAN（Wide Area Network）回線などを結ぶネットワーク40と、LAN回線またはWAN回線に接続された基地局20、基地局30と、基地局20を介して伝送媒体に無線を利用してネットワークに接続する無線端末10－1と、基地局20及び30とLAN回線またはWAN回線で接続されネットワークに接続しようとしている無線端末10－1に対する接続の可否を判断する認証サーバ50と、認証サーバとLAN回線またはWAN回線で接続されネットワークに接続しようとしている無線端末10－1に対する接続の可否に関する情報を保持する管理装置60とから構成されている。

[0053] 基地局20は、IEEE 802.11に基づく基地局としての機能を保持し、無線端末10－1とネットワーク40に接続された装置との間でのデータ通信を中継する動作を行う。

[0054] 基地局20は、IEEE 802.11i及びIEEE 802.1Xに基づく基地局としての機能及びIEEE 802.1Xで規定されるオーセンティケータ（Authenticator）の機能を保持し、無線端末10－1からの接続ネゴシエーション要求に応じて接続ネゴシエーションを行い、接続ネゴシエーション完了後、無線端末10－1に対してネットワーク接続のためのIEEE 802.1Xに基づく認証を開始する。

[0055] 基地局20は、無線端末10－1からの認証情報を認証サーバ50に転送することにより、つまり無線端末10－1に対する認証可否は認証サーバ50で行い、基地局20は認証サーバ50から受信するネットワーク接続のための認証結果に伴い、無線端末毎のアクセス制御を行う。

[0056] 基地局20は、認証サーバ50からの認証成功通知と共に、以後の基地局20と無線端末10－1との間のデータ通信を暗号化するための情報の基となるPMKを受信すると、無線端末10－1に対して認証成功を通知した後に、その後のデータ通信を暗号化するための鍵をやり取りするために4ウェイハンドシェイク及びグループキーハンドシェイクを行い、データ通信を暗号化するための鍵が設定され、無線通信区間での

暗号化されたデータ通信が可能となる。

[0057] 基地局20は、IEEE 802.11iに基づくPMKキャッシュの機能を保持し、一度認証が成功した無線端末毎のPMKを保持しておき再び前述無線端末との(再)接続ネゴシエーションにおいて無線端末10－1からPMKキャッシュを利用する旨通知があった場合は自身が保持しているPMKの中から適するものを選択し利用することによってIEEE 802.1X認証を省略し引き続き無線端末10－1と4ウェイハンドシェイク及びグループキーハンドシェイクを行い、データ通信を暗号化するための鍵が設定され、無線区間が暗号化されたデータ通信が可能となる。

[0058] 基地局30は、基地局20の機能に加え、認証サーバ及び認証プロキシサーバそして認証クライアントとしての機能を保持し、事前認証のためのIEEE 802.1X認証フレームをIPネットワーク上での通信(以下、単にIP通信と言う)が可能である認証パケットでカプセル化してトンネリング処理を実行することが可能である。また、カプセル化された認証パケットからカプセル化を解き、IEEE 802.1X認証フレームを取り出す処理も可能である。

[0059] 無線端末10－1から受信したIEEE 802.1X認証パケットをIP通信が可能である認証パケットでカプセル化してトンネリングすることによりIPネットワークを介して認証サーバとの間の通信を行う方法が一般的であるが、それに加え、IP通信が可能である認証パケットでカプセル化してトンネリングすることにより無線端末10－1との間でIPネットワークを介したIEEE 802.1X認証パケットのやり取りが可能である。IP通信が可能である認証プロトコルとしては、RADIUS(Remote Authentication Dial in User Service)プロトコル等がある。

[0060] 無線端末10－1は、IEEE 802.11に基づく端末の機能を保持し、基地局20を介してネットワーク40に接続された装置とインターネットプロトコル(IP)を用いて通信が可能である。

[0061] また、無線端末10－1は、IEEE 802.11i及びIEEE 802.1Xに基づく端末としての機能及びIEEE 802.1Xで規定されるサプリカント(Supplicant)の機能を保持し、データ通信が可能となる前に、基地局20基地局30と無線物理層を用いて接続ネゴシエーションを行い、接続ネゴシエーション完了後、IEEE 802.1Xによるユ

ーザー認証を必要とし、ユーザー認証完了後、その後のデータ通信を暗号化するための鍵をやり取りするために4ウェイハンドシェイク及びグループキーハンドシェイクを行い、データ通信を暗号化するための鍵が設定された時点で、本ネットワークの一端末として動作する。

[0062] IEEE 802.1X認証時には、ユーザーID及びパスワードを必要とするかもしれないし、保持している自身のユーザー証明書を用いるかもしれない。どちらを使用するかはネットワーク接続のための認証時に選択される認証方式しだいである。

[0063] 無線端末10－1は、IEEE 802.11iに基づくPMKキャッシュの機能を保持し、一度認証が成功した基地局のPMKを保持しておき、再び前述基地局との(再)接続ネゴシエーションにおいてPMKキャッシュを使用する旨通知し、前述基地局においてもPMKキャッシュに対応している場合は、前述基地局に対応するPMKを使用して、IEEE 802.1X認証を省略し引き続き基地局と4ウェイハンドシェイク及びグループキーハンドシェイクを行い、データ通信を暗号化するための鍵が設定され、無線区間が暗号化されたデータ通信が可能となる。

[0064] 無線端末10－1は、認証クライアントとしての機能を保持し、事前認証のためのIEEE 802.1X認証フレームをIP通信が可能である認証パケットでカプセル化してトンネリング処理を実行することにより基地局30との間でIPネットワークを介したIEEE 802.1X認証パケットのやり取りが可能である。また、カプセル化された認証パケットからカプセル化を解き、IEEE 802.1X認証フレームを取り出す処理も可能である。通常、IEEE 802.1X認証時及びIEEE 802.11iで規定されている事前認証時には、無線LANのMACフレーム上でIEEE 802.1X認証パケットの送受信を行う。

[0065] 認証サーバ50は、無線端末10－1が基地局20との接続ネゴシエーション後もしくは基地局30との事前認証時にネットワーク接続のための認証を行う際に、基地局20、30に代わって無線端末10－1の認証を行う。認証サーバ50は、基地局からのユーザー認証要求に応じて、無線端末10－1のユーザー認証を自身で保持しているユーザー情報を利用し、もしくは管理装置60と通信することで行い、ユーザー認証結果を基地局20、30へ通知する。

[0066] 認証サーバ50は、ユーザー認証結果が成功である場合、IEEE 802.1X認証の

結果得られる無線端末と認証サーバ間においてのみ共有されるPMKを、ユーザー認証結果と共に基地局20、30に対して通知する。認証サーバ50は、基地局20、30と認証に関する通信及び無線端末10－1との暗号化データ通信に使用するPMKの通知を行い、ユーザー情報の認証に関する通信を管理装置60と行う。認証サーバ50は、ネットワーク接続のための認証方式によっては、無線端末10－1から渡される証明書を検証することによってユーザー認証を行う。

[0067] 管理装置60は、無線端末10－1を使用しているユーザーのアカウント及びパスワードを管理している。この機能は認証サーバ50内に含まれるかもしれない。

[0068] 図6は、図5の無線端末10－1の構成を示すブロック図である。

[0069] 図6において、無線端末10－1は、RADIUSクライアント110と、802．1Xサプリカント120と、プロトコル処理部130と、IPプロトコル処理部140と、ネットワークアクセス制御部150と、無線LAN端末ドライバ160と、無線LAN通信インタフェース部170と、パラメータ記憶部180と、記憶媒体190とから構成されている。

[0070] これらの手段は概略、次のように動作する。

[0071] RADIUSクライアント110は、802．1Xサプリカント120から受け取ったIPサブネットワークを越えた事前認証のためのIEEE 802．1X認証パケットをRADIUSパケットでカプセル化し802．1Xサプリカント120へ受け渡す。また802．1Xサプリカントから受け取ったRADIUSパケットでカプセル化された事前認証のためのIEEE 802．1X認証パケットをカプセル化から解き、802．1Xサプリカントへ受け渡す。

[0072] なお、RADIUSクライアント110は、IP通信が可能である他の認証プロトコルを実現するクライアントでもかまわない。

[0073] 802．1Xサプリカント120は、802．1Xオーセンティケータ宛、及び802．1Xオーセンティケータからの IEEE 802．1Xパケットを、ネットワークアクセス処理部を介して送信及び受信する。

[0074] 802．1Xサプリカント120は、IEEE 802．1X認証に必要な認証処理を行う機能を保持する。IEEE 802．11iで規定されるPMKキャッシュの機能を保持し、一度成功裏に認証が完了したときのPMKをキャッシュしておく機能を備える。また、PMKは同時に複数保持することも可能であり、接続する基地局毎に適切に使い分けることが

可能である。また、IEEE 802．11iで規定される事前認証(preauthentication)に加え、RADIUSパケットでカプセル化して送受信される事前認証のためのIEEE 802．1X認証機能を備える。認証に必要となる情報及び認証開始・切断などの要求をネットワークアクセス制御部150から受ける。

[0075] プロトコル処理部130は、IPプロトコル処理部140から受け取ったデータを適切に処理し、必要に応じて処理したデータをアプリケーションへ受け渡す。また、アプリケーションから受け取ったデータを適切に処理し、IPプロトコル処理部140へ送信のために引き渡す。

[0076] プロトコル処理部140は、TCP処理部131、UDP処理部132、それ以外のプロトコル処理部133で構成され、前述各処理部はそれぞれ特定のプロトコルに対する処理を行う。例えば、UDP／IPでやり取りされる認証プロトコルのパケットは、UDP処理部132において適切に処理される。

[0077] IPプロトコル処理部140は、無線LAN端末ドライバ160から受け取ったIEEE 802．3プロトコルフレームを適切に処理し、必要に応じてプロトコル処理部130へ引き渡す。また、プロトコル処理部130から受け取ったフレームをIEEE 802．3プロトコルに処理し、送信するために無線LAN端末ドライバ160へ引き渡す。

[0078] ネットワークアクセス制御部150は、接続先及び接続タイミングなどネットワーク接続に関する制御を行う。無線LAN端末ドライバ160に対しては無線LAN接続ネゴシエーションの制御を、802．1Xサプリカント120に対しては認証開始などの制御を、プロトコル処理部130、IPプロトコル処理部140に対しては通信先アドレスなどに関する制御を行う。また、ネットワーク接続において必要な情報の指示／提供もネットワークアクセス制御部150は行う。ネットワーク接続に必要となる情報はパラメータ記憶部180から取得する。

[0079] 無線LAN端末ドライバ160は、IEEE 802．11の端末としての機能を実現するためのMAC処理を行う。つまり、基地局との接続ネゴシエーション処理を行うためのIEEE 802．11パケットの生成及び解析を行う。また、無線LAN通信インタフェース部170から受信したIEEE 802．11パケットをTCP／IPやUDP／IPなどのIEEE 802．3プロトコルに変換しプロトコル処理部130に渡す。逆に、プロトコル処理部130か

ら受信したIEEE 802.3プロトコルのフレームをIEEE 802.11パケットでカプセル化し無線LAN通信インタフェース部170を介して送信する。

[0080] 無線LAN端末ドライバ160は、無線LAN通信インタフェース部170から受信したIEEE 802.1Xパケットを802.1Xサプリカント120へ渡し、802.1Xサプリカント120から送信要求されたIEEE 802.1Xパケットを無線LAN通信インタフェース部170を介して送信する。

[0081] 無線LAN通信インタフェース部170は、無線LAN端末ドライバ160から受けとったデータを無線で送信する処理を行う。

[0082] また、無線LAN通信インタフェース部170は、受信したデータを無線LAN端末ドライバ160へ渡す処理を行う。無線LAN通信インタフェース部170は、主に、基地局20、30との通信の際に用いられる。

[0083] パラメータ記憶部180は、ネットワーク接続に必要となる情報を保持している。例えば、接続する基地局を識別するためのESSIDとESSIDに対応するセキュリティ設定情報(IEEE 802.1X認証のためのユーザー情報やEAP－TLS、EAP－TTLS、PEAP、EAP－SIMなどの認証方式、TKIPやAESなどの暗号化方式)を保持している。

[0084] また、パラメータ記憶部180は、基地局のESSIDもしくはBSSIDに対応するIPアドレスの対応表を保持している。パラメータ記憶部180にて保持される値はネットワークアクセス制御部150によって使用される。

[0085] 無線端末10－1が図示せぬCPU(中央処理装置)及びRAM(リードオンリーメモリ)を含むコンピュータの場合、CPUは記憶媒体190に格納されたプログラムを実行することで、上述した各部の処理を実現する。

[0086] 図7は、図5の基地局30の構成を示すブロック図である。

[0087] 図7において、基地局30は、RADIUSクライアント部310と、RADIUSサーバ部320と、802.1Xオーセンティケーター330と、プロトコル処理部340と、IPプロトコル処理部350と、ブリッジ部360と、有線LAN通信インタフェース部370と、ネットワークアクセス制御部380と、無線LAN APドライバ390と、無線LAN通信インタフェース部400と、記憶媒体410とから構成されている。

[0088] これらの手段は概略、次のように動作する。

[0089] RADIUSクライアント部310は、無線端末10－1とのIEEE 802.1X認証においてIEEE 802.1X認証を認証サーバ50へ転送するために使用される。

[0090] RADIUSクライアント部310は、802.1Xオーセンティケーター330から受け取ったIEEE 802.1XパケットをRADIUSパケットでカプセル化し802.1Xオーセンティケーター330へ受け渡す。また802.1Xオーセンティケーター330から受け取ったRADIUSパケットでカプセル化されたIEEE 802.1Xパケットをカプセル化から解き、802.1Xオーセンティケーター330へ受け渡す。なお、RADIUSクライアント部310は、IP通信が可能である他の認証プロトコルを実現するクライアント機能でもかまわない。

[0091] RADIUSサーバ部320は、802.1Xオーセンティケーター330から受け取ったIPサブネットワークを越えた事前認証のためのIEEE 802.1XパケットをRADIUSパケットでカプセル化し802.1Xオーセンティケーター330へ受け渡す。また802.1Xオーセンティケーター330から受け取ったRADIUSパケットでカプセル化された事前認証のための802.1Xパケットをカプセル化から解き、802.1Xオーセンティケーター330へ受け渡す。

[0092] なお、RADIUSサーバ部320は、IP通信が可能である他の認証プロトコルを実現するサーバ機能でもかまわない。

[0093] 802.1Xオーセンティケーター330は、802.1Xサプリカント宛、及び802.1Xサプリカントからの IEEE 802.1Xパケットを、ネットワークアクセス処理部を介して送信及び受信する。

[0094] 802.1Xオーセンティケーター330は、IEEE 802.1X認証に必要な認証処理を行う機能を保持する。IEEE 802.11iで規定されるPMKキャッシュの機能を保持し、無線端末10－1に対して一度成功裏に認証が完了したときのPMKをキャッシュしておく機能を備える。また、PMKは同時に複数保持することも可能であり、接続してくる無線端末毎に適切に使い分けることが可能である。また、IEEE 802.11iで規定される事前認証（preauthentication）に加え、RADIUSパケットでカプセル化して送受信される事前認証のためのIEEE 802.1X認証機能を備える。

[0095] プロトコル処理部340は、IPプロトコル処理部350から受け取ったデータを適切に処理し、必要に応じて処理したデータをアプリケーションへ受け渡す。また、アプリケーションから受け取ったデータを適切に処理し、IPプロトコル処理部350へ送信のために引き渡す。

[0096] プロトコル処理部340は、TCP処理部341、UDP処理部342、それ以外のプロトコル処理部343で構成され、前述各処理部はそれぞれ特定のプロトコルに対する処理を行う。例えば、UDP／IPでやり取りされる認証プロトコルのパケットは、UDP処理部342において適切に処理される。

[0097] IPプロトコル処理部350は、ブリッジ部360から受け取ったIEEE 802.3プロトコルフレームを適切に処理し、必要に応じてプロトコル処理部340へ引き渡す。また、プロトコル処理部340から受け取ったフレームをIEEE 802.3プロトコルに処理し、送信するためにブリッジ360へ引き渡す。

[0098] ブリッジ部360は、IPプロトコル処理部350から受け取った送信データを送信先によって有線LAN通信インタフェース部370、もしくは無線LAN APドライバ390へ振り分ける処理を行う。

[0099] 基地局30は、有線LAN通信インタフェース部370から受け取ったデータを自身で処理せずに転送する場合は、無線LAN APドライバ390へ、または無線LAN APドライバ390から受け取ったデータを自身で処理せず転送する場合は、有線LAN通信インタフェース部370へそのまま受け渡す動作を行う。自身で処理するデータについてはIPプロトコル処理部350へ受け渡す。

[0100] 有線LAN通信インタフェース部370は、ネットワーク40に接続しており、ブリッジ部360から受け取ったデータをネットワーク40に送信する処理を行う。

[0101] また、有線LAN通信インタフェース部370は、ネットワーク40から受信したデータをブリッジ部360へ受け渡す処理を行う。

[0102] 有線LAN通信インタフェース部370は、IEEE 802.1X認証時には無線端末10－1とのIEEE 802.1XパケットをRADIUSパケットとして認証サーバと送受信する際に用いられ、また有線側に接続されている端末との通信の際にも用いられる。

[0103] ネットワークアクセス制御部380は、自身つまり基地局30へ接続しようとするもしくは

接続している無線端末10－1の接続に関する制御を行う。無線LAN APドライバ390に対しては、無線LAN接続ネゴシエーションの制御を、802．1Xオーセンティケーター330に対しては認証開始などの制御を、プロトコル処理部340、IPプロトコル処理部350、ブリッジ部360に対しては通信先アドレスやデータのルーティングなどに関する制御を行う。また、無線端末10－1からのネットワーク接続要求に対して必要な情報の指示／提供もネットワークアクセス制御部380は行う。

[0104] 無線LAN APドライバ390は、IEEE 802．11の基地局としての機能を実現するためのMAC処理を行う。つまり、無線端末10－1との接続ネゴシエーション処理を行うためのIEEE 802．11パケットの生成及び解析を行う。また、無線LAN通信インタフェース部400から受信したIEEE 802．11パケットをTCP／IPやUDP／IPなどのIEEE 802．3プロトコルに変換しブリッジ部360に渡す。逆に、ブリッジ部360から受信したIEEE 802．3プロトコルのフレームをIEEE 802．11パケットでカプセル化し無線LAN通信インタフェース部400を介して送信する。

[0105] 無線LAN APドライバ390は、無線LAN通信インタフェース部400から受信したIEEE 802．1Xパケットを802．1Xオーセンティケーター330へ渡し、802．1Xオーセンティケーター330から送信要求されたIEEE 802．1Xパケットを無線LAN通信インタフェース部400を介して送信する。

[0106] 無線LAN通信インタフェース部400は、無線LAN APドライバ390から受け取ったデータを無線で送信する処理を行う。また、無線LAN通信インタフェース部400は、受信したデータを無線LAN APドライバ390へ渡す処理を行う。無線LAN通信インタフェース部400は、主に、無線端末10－1との通信の際に用いられる。

[0107] 基地局30が図示せぬCPU（中央処理装置）及びRAM（リードオンリーメモリ）を含むコンピュータの場合、CPUは記憶媒体410に格納されたプログラムを実行することで、上述した各部の処理を実現する。

[0108] 次に、図8の無線通信システムの全体的な動作の流れを示すシーケンスチャート図、図9の無線通信システムを構成する装置間のデータの流れを示すネットワーク構成図、図10の無線端末10－1の動作を示すフローチャート図、図11の事前認証の対象となる基地局30の動作を示すフローチャート図及び図5～図7を参照して本実施

の形態における全体の動作について詳細に説明する。

[0109] 尚、図10に示す処理は無線端末10－1を構成するコンピュータのCPUが記憶媒体190のプログラムをRAMに移して実行することで実現され、図11に示す処理は基地局30を構成するコンピュータのCPUが記憶媒体410のプログラムをRAMに移して実行することで実現される。

[0110] まず、基地局20を介して無線端末10－1がネットワーク40に接続して通信を行うには、無線端末10－1と基地局20との間でネゴシエーションを行いデータ通信が可能となる(図8のC1、図9の(1)、図10のステップA1、ステップA2)。

[0111] 無線端末10－1と基地局20との間のネゴシエーションは、IEEE 802．11接続ネゴシエーションのみでWEPキーによる暗号化通信であるかもしれないし、IEEE 802．1X認証の結果接続が許可され動的に設定されたWEPキーによる暗号化通信であるかもしれないし、もしくはWPA(Wi－Fi Protected Access)によるよりセキュリティが強化された接続であるかもしれない。

[0112] 次に、無線端末10－1は現在接続している基地局20とは別の事前認証の対象とする基地局30の存在を前述基地局30が報知している情報を取得することによって検出する(図8のC2、図9の(5)、図10のステップA3)。無線端末10－1においては、無線LAN通信インタフェース部170から受信した前述報知情報が無線LAN端末ドライバ160を介してネットワークアクセス制御部150へ受け渡される。例えば、前記基地局30が報知しているビーコンもしくはプローブレスポンスには自身のネットワークを識別するESSIDやBSSID及び基地局名などが含まれている。

[0113] 無線端末10－1は、事前認証の対象とする基地局30に対して現在接続している基地局20を介して本発明の事前認証を行うことを決定すると、事前認証の対象とする基地局30が報知している情報から取得した情報(ESSID、BSSIDなど)を元に、図6のネットワークアクセス制御部150はパラメータ記憶部180に記憶されているESSIDもしくはBSSIDとIPアドレスとの対応表から事前認証の対象とする基地局30のIPアドレスを取得する(図10のステップA4)。例えば、パラメータ記憶部180にはあるESSIDに対するIPアドレスが、もしくはあるBSSIDに対するIPアドレスが記憶されており、事前認証の対象とする基地局のBSSIDに対応するIPアドレスを取得する。

[0114] 無線端末10－1は、事前認証の対象とする基地局30のIPアドレスを取得すると、事前認証の対象とする基地局30に対して事前認証を開始する(図8のC3、図10の(5)、図10のステップA5)。

[0115] 無線端末10－1においては、ネットワークアクセス制御部150から802．1Xサプリカント120に対して前述基地局30に対して事前認証を開始する旨を指示する。

[0116] 802．1Xサプリカント120は、事前認証を開始するためのIEEE 802．1Xフレームを生成し、RADIUSクライアント部110を通してRADIUSパケットを生成し、前述取得したIPアドレス宛にプロトコル処理部130、IPプロトコル処理部140、無線LAN端末ドライバ160及び無線LAN通信インタフェース部170を介して現在接続している基地局20に対して送信する。以後、無線端末10－1においては、事前認証のためのIEEE 802．1XパケットはRADIUSパケットでカプセル化され送信されるという上記の流れで行われるものとする。

[0117] また、送信したRADIUSパケットに対する応答として受信したRADIUSパケットは、上記とまったく逆の流れにおいて802．1Xサプリカント120に届けられる。例えば、無線LAN区間において基地局のBSSIDを示すフィールドには現在接続している基地局のMACアドレスを指定し、IPヘッダーのあて先IPアドレスには事前認証の対象とする基地局のIPアドレスが指定され、RADIUSパケットが含まれたパケットである。

[0118] 前述RADIUSパケットを受信した現在無線端末10－1が接続している基地局20は、前述IPアドレスへ配送されるように適切に配送処理を行う(図8のC4、図9の(2)、図11のステップB1)。

[0119] ネットワーク40を介して前述RADIUSパケットを受信した事前認証の対象となる基地局30は、無線端末10－1の識別子を要求するためにIEEE 802．1XパケットであるEAP－Request／IdentityパケットをRADIUSパケットでカプセル化して、無線端末10－1と同様にネットワーク40を介して無線端末10－1が接続している基地局20を経由して返信する(図8のC5、図9の(2)，(1)、図11のステップB2)。

[0120] 事前認証の対象となる基地局30においては、有線LAN通信インタフェース部370より受信したRADIUSパケットをブリッジ部360、IPプロトコル処理部350、プロトコル処理部340を介して802．1Xオーセンティケーター330と受け渡され、RADIUSサ

ーバ部320においてRADIUSパケットのカプセル化が解かれ事前認証のためのIEEE 802. 1Xフレームが802. 1Xオーセンティケーター330へ届けられる。

[0121] 802. 1Xオーセンティケーター330は、まず最初に無線端末10－1の識別子を要求するためにIEEE 802. 1XフレームであるEAP－Request／Identityパケットを送信する(図8、図11のステップB2)。

[0122] 送信時は、受信時とは逆に、RADIUSサーバ部320においてRADIUSパケットへのカプセル化が行われ、RADIUSパケットをプロトコル処理部40、IPプロトコル処理部350、ブリッジ部360、有線LAN通信インタフェース部370を介して送信元である無線端末10－1へ届けられる。

[0123] 以後、事前認証の対象となる基地局30においては、上記の流れで事前認証のためのIEEE 802. 1Xフレームの送受信が行われる。

[0124] 以降、無線端末10－1と事前認証の対象となる基地局30との間でやり取りされるRADIUSパケットでカプセル化された事前認証のためのIEEE 802. 1Xフレームのやり取りは、通常のIEEE 802. 1X認証のやり取りと同様に行われる。

[0125] また、前述IEEE 802. 1X認証のやり取りは認証方式、例えばEAP－TLS、EAP－TTLS、PEAP、EAP－AKAなど利用する認証によって異なるのも通常のIEEE 802. 1X認証のやり取りと同様である。

[0126] 事前認証の対象となる基地局30において、無線端末10－1の認証を基地局自身では行わずに認証サーバ50において代わりに行ってもらうために、802. 1Xオーセンティケーター330において受信したIEEE 802. 1Xフレームを認証サーバ50とやり取りするためにRADIUSクライアント部310を介してRADIUSパケットとして認証サーバ50との送受信を行う。

[0127] 認証サーバ50は、基地局30に代わって無線端末10－1の認証を行う。認証サーバ50は、基地局からのユーザー認証要求に応じて、無線端末10－1のユーザー認証を自身で保持しているユーザー情報を利用し、もしくは管理装置60と通信することで行い、ユーザー認証結果を基地局30へ通知する。

[0128] 認証サーバ50は、ユーザー認証結果が成功である場合、IEEE 802. 1X認証の結果得られる無線端末10－1と認証サーバ50間においてのみ共有されるPMKを、

ユーザー認証結果と共に基地局30に対して通知する(図8のC6、図11のステップB4)。

[0129] 事前認証の対象となる基地局30は、認証サーバ50から無線端末10－1に対する認証結果を受信すると、これまでと同様、RADIUSパケットでカプセル化された形で事前認証のためのIEEE 802.1X認証結果通知を無線端末10－1に対して、これまた同様にネットワーク40、基地局20を介して送信する(図8のC7、図10のステップA6、図11のステップB5)。

[0130] 事前認証のためのIEEE 802.1X認証が成功であるとともに、認証が成功した無線端末10－1に対するPMKを受信した基地局30においては、RADIUSクライアント部310にてIEEE 802.1X認証成功通知とPMKが分割され802.1Xオーセンティケーター330に受け渡される。無線端末10－1に対しては、IEEE 802.1X認証成功通知のみをRADIUSサーバ部320を介してRADIUSパケットでカプセル化した形で無線端末10－1へ送信する。PMKに関しては無線端末10－1へ転送せず、自身でキャッシュしておく(図8のC8、図10のステップA6、図11のステップB6)。

[0131] 現在接続している基地局20を介して事前認証の対象とする基地局30からの事前認証成功通知を受信した無線端末10－1は、前述事前認証のためのIEEE 802.1X認証の過程で取得したPMKを自身でキャッシュし、事前認証の対象とする基地局30が報知する情報(ESSIDやBSSIDなど)と前述キャッシュしたPMKとの対応を保持しておく(図8のC8、図10のステップA6)。

[0132] 無線端末10－1は、IEEE 802.11iで規定されるPMKキャッシュを利用するために必要となる無線端末10－1自身のMCアドレスをIEEE 802.1X認証フレームをカプセル化するためのRADIUSパケットに含めることにより基地局30に対して通知する。

[0133] 無線端末10－1は、前述事前認証を行った基地局30の存在を、前述基地局30が報知する情報から検出し、現在接続している基地局20から前述事前認証を行った基地局30へ移動することを決定すると、無線端末10－1は、前述事前認証を行った基地局30に対して接続ネゴシエーションを開始する(図8のC9、図10のステップA7,A8、図11のステップB7)。

[0134] 無線端末10－1と事前認証を行った基地局30との接続ネゴシエーションは、IEEE 802．11i規定のPMKキャッシュを利用することができる。つまり、無線端末10－1は基地局30に対するIEEE 802．11(再)アソシエーション要求において前述事前認証にてキャッシュしておいたPMKを識別するためのIDをRSN IE(Robust Security？ Network Information Element)と共に指定する。無線端末10－1は、PMKを複数同時に保持することが可能であるため、前述PMKをキャッシュするときに対応付けて保持している基地局の情報(ESSIDやBSSID)を参考にして、適切なPMKを選択することが可能である。また、IEEE 802．11(再)アソシエーション要求において同時に複数のPMK IDを含むこともできる。この場合、後述するが基地局30が選択したPMK IDを利用して引き続き鍵交換が行われる。

[0135] 無線端末10－1と接続ネゴシエーション中の基地局30は、RSN IE／PMK IDを含むIEEE 802．11(再)アソシエーション要求を受信すると、IEEE 802．11(再)アソシエーション応答を無線端末10－1に対して返信する(図8のC10)。

[0136] 前述の基地局30は、無線端末10－1とのRADIUSパケットを介したIEEE 802．1X認証時に、無線端末10－1から通知されたMCAアドレスと、無線端末10－1との間で行われた事前認証を介して取得済みであって、無線端末自身でキャッシュしているPMKとを用いて、予め無線端末10－1を識別するためのPMK IDを生成済みである。このPMK IDは、無線端末10－1がPMKキャッシュを使用して接続する場合に、どのPMKを使用するかについての識別を行うために使用される。

[0137] 前述の基地局30は、自身でキャッシュしているPMKを識別するための各IDと無線端末10－1からIEEE 802．11(再)アソシエーション要求において受信したPMK IDを比較し、一致するものがあった場合は該PMK IDで識別されるPMKを使用して引き続き鍵交換を行う(図11のステップB8，B9)。

[0138] 鍵交換においては、4ウェイハンドシェイクの最初のメッセージであるEAPOL－Keyフレームにおいて選択したPMK IDを含んで無線端末10－1へ送信する(図8のC11)。

[0139] PMK IDを含んだEAPOL－Keyフレームを受信した無線端末10－1は、IEEE 802．11(再)アソシエーション要求において指定したPMK IDと一致していること

を、もしくは複数指定したPMK IDから基地局によって選択されたPMK IDを確認する(図8のC12)。

[0140] 以降は、引き続き通常の4ウェイハンドシェイク及びグループキーハンドシェイク処理を行うことにより最終的に暗号化通信のための鍵が設定され、暗号化されたデータ通信が可能となる。

[0141] この時点で、別途他の基地局に対して本発明の事前認証を行うことも可能であり、この場合も同様に前述他の基地局との接続においてもPMKキャッシュを使用した無線LAN接続が可能となる。

[0142] 図10のステップA6において、事前認証が失敗した旨通知を受けた場合、無線端末10－1は前述事前認証に失敗した基地局に無線LAN接続する時には、通常のIEEE 802.11接続ネゴシエーション、IEEE 802.1X認証、鍵交換が行われることになり、その後、暗号化されたデータ通信が行われる(図10のステップA11、A12、A13、A10)。

[0143] 事前認証によってPMKをキャッシュする無線端末10－1及び基地局30は、それぞれキャッシュしたPMKに対して保持期間を持っているかもしれない。保持期間を過ぎて利用されなかったPMKは破棄されるかもしれない。つまり、保持期間を過ぎた後にPMKキャッシュを利用して無線LAN接続ネゴシエーションを行おうとした場合、基地局30においてはPMKがすでに破棄されているために通常の接続ネゴシエーションが要求されることになるかもしれないし、無線端末10－1においてはPMKがすでに破棄されているためにPMKキャッシュでの接続を行うことができないかもしれない。

[0144] 図8のアクセス要求は、EAPOL－Startフレームを含む代わりに、基地局30が事前認証を開始することが判断できるフレーム、例えばアクセス要求に事前認証を開始する旨内容が伴うアクセス要求フレームであってもよい。

[0145] 第1の形態における説明では、認証サーバは1つであったが、基地局毎に異なる認証サーバを使用して認証を行うような構成でもかまわない。

[0146] 次に、第1の形態による効果について説明する。

[0147] 第1の形態では、無線端末及び事前認証の対象となる基地局それぞれにおいてIE

EE 802. 1X認証フレームをIP通信可能な認証パケットでカプセル化することによってIPネットワーク上でお互いに通信することが可能であるように構成されているため、IEEE 802. 11i規定の事前認証ではIPサブネットワーク内においてのみしか事前認証ができないのに対して、IPネットワーク上で無線端末及び事前認証の対象となる基地局がお互いに通信可能であれば、事前認証を遂行することができる。このため、無線LAN接続ネゴシエーションの量を減らすことができ、無線LAN通信断となる期間を短くすることが可能となる。

[0148] また、第1の形態では、さらに、無線端末においてパラメータ記憶部180を備え基地局に対するIPアドレスの対応を予め保持できるように構成されているため、事前認証の対象とする基地局30のIPアドレスを識別することができる。

(第1の形態の変形例)

次に、第1の形態の変形例について図7を参照して詳細に説明する。

[0149] 図7を参照すると、第1の形態の変形例は、図7の802. 1Xオーセンティケーター330及びRADIUSサーバ部320の動作において第1の形態と一部異なる以外は、第1の形態と同様の構成となっている。

[0150] 基地局30における802. 1Xオーセンティケーター330は、無線端末10－1の802. 1Xサプリカント120とやり取りされる事前認証のためのRADIUSパケットの処理動作においてのみ、第1の形態とは一部異なる。

[0151] 802. 1Xオーセンティケーター330は、第1の形態では、事前認証のためのRADIUSパケットを受け取るといったんRADIUSサーバ部320へ受け渡し、RADIUSパケットのカプセル化を解いたIEEE 802. 1Xパケットとして受け取り、受け取ったIEEE 802. 1Xパケットを認証サーバ50へ転送するためにRADIUSクライアント部310においてRADIUSパケットにして転送処理を、またその逆、認証サーバ50から応答されたRADIUSパケットをRADIUSクライアント部310においてIEEE 802. 1Xパケットにし、無線端末10－1の802. 1Xサプリカント120へ送信するためにRADIUSサーバ部320へ受け渡す処理をしていたが、第1の形態の変形零では、事前認証のためのRADIUSパケットを受け取るとRADIUSサーバ部320へ受け渡した後、RADIUSサーバ部320はRADIUSプロキシーとしての動作を行い、つまりプロキシー

動作として必要な処理を行った後、RADIUSパケットのまま802．1Xオーセンティケーター330に返される。802．1Xオーセンティケーター330は、前述RADIUSパケットを認証サーバ50へ転送する。認証サーバ50から返信されたRADIUSパケットはRADIUSプロキシーとして動作しているRADIUSサーバ部320を介した後、そのまま無線端末10－1へ送信される。

[0152] RADIUSサーバ部320は、第1の形態では、事前認証のためのRADIUSパケットのカプセル化及びその逆の処理をしていたが、第1の形態の変形例では、RADIUSプロキシーサーバとして動作する点が大きく異なる。

[0153] RADIUSサーバ部320は、802．1Xオーセンティケーター330から受け取ったRADIUSパケットに対してプロキシー動作としての処理を施した後、RADIUSパケットのまま802．1Xオーセンティケーター330へ受け渡す。

[0154] RADIUSサーバ部320は、認証サーバ50から最終的に認証成功を通知するパケットを受信した場合、認証成功を通知するパケットに付随するPMK情報については無線端末10－1へ転送せずに、認証成功を通知するパケットと分離し、認証成功を通知するパケットについては無線端末10－1へ転送し、PMKは別に802．1Xオーセンティケーター330へ受け渡す。なお、RADIUSサーバ部320は、IP通信が可能である他の認証プロトコルを実現するサーバ機能でもかまわない。

[0155] 第1の形態の変形例において、第1の形態と異なる点は、基地局30における802．1Xオーセンティケーター330及びRADIUSサーバ部320の動作に関してである。そこで、以下ではこれらの異なる点についてのみ説明する。

[0156] 無線端末10－1の構成及び動作は第1の形態と同様であり、まず最初の基地局20に対して適切に接続ネゴシエーションを行い接続し、事前認証の対象とする基地局30を何らかの方法で検出すると前述基地局に対して本発明の事前認証を開始する旨要求するパケットを送信する。

[0157] 事前認証開始を要求するパケットを受信した基地局30は、無線端末10－1に対してIDを要求するパケットを送信する。

[0158] 基地局30においては、有線LAN通信インタフェース部370、ブリッジ部360、IPプロトコル処理部350、プロトコル処理部340を介して802．1Xオーセンティケーター3

30はRADIUSパケットでカプセル化された事前認証開始を要求するパケットを受け取る。このRADIUSパケットはRADIUSサーバ部320においてカプセル化が解かれて、802．1Xオーセンティケーター330は無線端末10－1からの事前認証開始要求に対して、IDを要求するパケットにて応答する。

[0159] 前述RADIUSパケットでカプセル化された事前認証開始を要求するパケットは、802．1Xオーセンティケーター330が事前認証を開始することが判断可能であるパケットがRADIUSパケットでカプセル化されている形式かもしれないし、RADIUSパケット自体に含まれる属性値などにおいて事前認証の開始を要求していることを示しているRADIUSパケットであるかもしれない。

[0160] 無線端末10－1は、RADIUSパケットでカプセル化されたIDを要求する事前認証パケットを受信すると、RADIUSパケットでカプセル化された自身のIDを挿入した事前認証パケットにて基地局へ応答する。

[0161] 基地局30は、前述RADIUSパケットでカプセル化された無線端末の利用者のIDが挿入された事前認証パケットを受信すると、RADIUSプロキシパケットである旨を示す属性を付与し、また認証サーバ50との安全な通信をするための処理を施して認証サーバ50へ転送する。認証サーバ50から返信されたRADIUSプロキシパケットに対しても同様に、RADIUSプロキシパケットである旨を示す属性をこの場合は取り除き、無線端末10－1との安全な通信をするための処理を施して無線端末10－1へ転送する。

[0162] 以降、無線端末10－1、基地局30、認証サーバ50において認証方式によってやり取りする内容は異なるが、IEEE 802．1X認証と同様に事前認証が行われる。

[0163] 最終的に、PMKが含まれる属性を伴った認証成功を示すRADIUSパケットを認証サーバ50から受信した基地局30は、PMKが含まれる属性はRADIUSパケットから取り除き、無線端末10－1へ転送する。PMKはPMKキャッシュによる接続を可能とするために自身にキャッシュされる。

[0164] 以降、前述無線端末10－1が基地局30へ無線LAN接続ネゴシエーションを行うときに、前述キャッシュされたPMKを使用してPMKキャッシュを利用した接続が可能となる。

[0165] 次に、第1の形態の変形例による効果について説明する。

[0166] 第1の形態の変形例では、基地局30において無線端末10－1と基地局30の間のRADIUSパケットに対して基地局30と認証サーバ50の間のRADIUSパケットを生成し直す必要がないように構成されているため、基地局30におけるRADIUSパケットの処理を少なくすることができる。

(第2の形態)

次に、本発明の第2の形態について添付の図面を参照して詳細に説明する。

[0167] 図12は、第2の形態による無線通信システムの構成を示す図である。

[0168] 図12を参照すると、前述した第1の形態及びその変形例による無線通信システムの構成とは、基地局管理サーバ70を要している点で異なる。

[0169] 基地局管理サーバ70は、基地局のBSSIDやESSID、基地局名などに対応するIPアドレスを管理している。無線端末などからIPアドレス解決要求を受信すると、自身で保持している基地局のBSSIDやESSID、基地局名などとIPアドレスとの対応表から、IPアドレス解決要求の対象である基地局に対応するIPアドレスを返す。

[0170] なお、基地局管理サーバ70とIPアドレス解決要求を送信する端末間のプロトコルは、DNS(Dynamic Name Service)プロトコルに似た独自プロトコルかもしれないし、HTTP(Hyper Text Transfer Protocol)もしくはHTTPS(Hyper Text Transfer Protocol over SSL)を利用したプロトコルであるかもしれない。

[0171] 図13において、第2の形態による無線端末10－2の構成は、上述した第1の形態及びその変形例による無線端末10－1の構成に加え、基地局アドレス解決部200を要する点で異なる。

[0172] 基地局アドレス解決部200は、図12における基地局管理サーバ70と通信を行い、基地局のIPアドレスを解決する役割を担う。

[0173] 基地局アドレス解決部200は、ネットワークアクセス処理部150からIPアドレスのわかっていない基地局のBSSIDアドレスを渡されると、前述BSSIDアドレスに対するIPアドレスを基地局管理サーバ70へ問い合わせる。基地局管理サーバ70から取得したIPアドレスをネットワークアクセス処理部150へ返す。

[0174] また、基地局アドレス解決部200は、BSSIDアドレスに対するIPアドレスを問い合

わせるだけではなく、ESSIDからIPアドレスを問い合わせる機能も併せ持つ。また、基地局が報知している情報から基地局の基地局名が取得できる場合、基地局アドレス解決部200は、基地局名からIPアドレスを問い合わせる機能も併せ持つ。なお、基地局アドレス解決部200と基地局管理サーバ70間のプロトコルは、DNSプロトコルに似た独自プロトコルかもしれないし、HTTPもしくはHTTPSを利用したプロトコルであるかもしれない。

[0175] 図13において、第2の形態による無線端末10－2の動作は、上述した第1の形態及びその変形例における無線端末10－1の動作と比較して、ネットワークアクセス処理部150において若干異なる。第1の形態及びその変形例では、事前認証の対象とする基地局のIPアドレスをパラメータ記憶部180から取得していたが、第2の形態では、基地局が報知している情報（BSSIDやESSID、基地局名など）からIPアドレスを解決するよう基地局アドレス解決部200に対して要求し、基地局アドレス解決部200の問い合わせによって取得したIPアドレスを用いて、ネットワークアクセス処理部150は本発明の事前認証の動作に入る。また、ネットワークアクセス処理部150は取得したIPアドレスをパラメータ記憶部180に格納しておくことが可能である。

[0176] 第2の形態は、無線端末10－2における上述の事前認証の対象とする基地局のIPアドレスの取得方法が異なるのみで他の動作に関しては、上述した第1の形態及びその変形例における無線端末10－1の動作と同様である。また、基地局20、30、認証サーバ50、管理装置60に関しては上述した第1の形態及びその変形例におけるそれらと構成及び動作は同様である。

[0177] また、第2の形態は、上述した第1の形態及びその変形例のどちらにも組み合わせることが可能である。

[0178] 次に、第2の形態による効果について説明する。

[0179] 第1の形態およびその変形例では、無線端末10において予め基地局のIPアドレスを保持していなければいけなかったが、第2の形態では基地局アドレス解決部200を備えるように構成されているため、動的に基地局のIPアドレスを取得することが可能である。このため、予め無線端末10－2において基地局のIPアドレスを設定しておく必要がないという効果が得られる。

（第3の形態）

次に、本発明の第3の形態について添付の図面を参照して詳細に説明する。

[0180] 図14は、第3の形態における無線通信システムの構成を示す図である。

[0181] 図14を参照すると、前述した第1及びその変形例における無線通信システムの構成とは、設定情報サーバ80を要している点で異なる。

[0182] 設定情報サーバ80は、無線端末が基地局に対して無線LAN接続する際に必要となる情報の組を保持している。無線端末などから設定情報取得要求を受信すると、無線端末に対する無線LAN接続に必要な情報の組を返す。

[0183] 前述無線LAN接続に必要な情報にはESSIDとESSIDが設定されている基地局に接続するために必要となるセキュリティ情報（WPAなどの接続方式からWEP、TKIP、AESなどの暗号化方式、IEEE 802．1Xの認証方式及び各認証方式に必要となる設定、及びパスフレーズなどを含む）及びIP接続に必要となる情報（無線端末のIPアドレス、ネットマスク、ゲートウェイアドレス、DNSアドレスやDHCP設定など）などが含まれている。

[0184] また、各基地局に対する設定には、本発明の事前認証への対応の不可も含まれており、対応している場合は、基地局に対する接続先であるIPアドレスも含まれている。なお、無線LAN接続に必要な情報の組は複数含まれていてもよい。

[0185] また、設定情報サーバ80と設定情報取得要求を送信する端末間のプロトコルは、HTTP（Hyper Text Transfer Protocol）もしくはHTTPS（Hyper Text Transfer Protocol over SSL（Secure Sockets Layer））を利用したプロトコルであるかもしれないし、独自に規定したプロトコルであるかもしれない。実際にやり取りされる情報は、XML（Extensible Markup Language）言語に従い、＜network＞＜wlan＞＜essid＞ap1＜／essid＞＜assoc＞wpa＜／assoc＞＜enc＞tkip＜／enc＞＜bssid＞aaaaaaaaaaaa＜／bssid＞＜ip＞0．0．0．0＜／ip＞＜／wlan＞＜network＞などのように記述される。

[0186] 図15において、第3の形態における無線端末10－3の構成は、上述した第1の形態及びその変形例における無線端末10－1の構成に加え、設定情報ダウンロード部210を要する点で異なる。

[0187] 設定情報ダウンロード部210は、図14における設定情報サーバ80と通信を行い、無線端末において無線LAN接続のために必要となる設定情報を取得し、パラメータ記憶部に格納する役割を担う。設定情報ダウンロード部210は、ネットワークアクセス処理部150から特定の設定情報サーバ80から設定情報をダウンロードする旨指示を受けると、前述特定の設定情報サーバ80に対して設定情報取得要求を設定情報サーバ80へ行う。設定情報サーバ80から取得した無線LAN接続のために必要となる設定情報をパラメータ記憶部180へ格納し、ネットワークアクセス処理部150へ設定情報の取得が完了した旨を通知する。

[0188] なお、無線LAN接続に必要な情報の組は複数含まれていてもよい。

[0189] また、設定情報サーバ80と設定情報取得要求を送信する端末間のプロトコルは、HTTP(Hyper Text Transfer Protocol)もしくはHTTPS(Hyper Text Transfer Protocol over SSL(Secure Sockets Layer))を利用したプロトコルであるかもしれないし、独自に規定したプロトコルであるかもしれない。実際にやり取りされる情報は、XML(Extensible Markup Language)言語に従い、＜network＞＜wlan＞＜essid＞ap1＜／essid＞＜assoc＞wpa＜／assoc＞＜enc＞tkip＜／enc＞＜bssid＞aaaaaaaaaaaa＜／bssid＞＜ip＞0. 0. 0. 0＜／ip＞＜／wlan＞＜network＞などのように記述される。

[0190] 図15において、第3の形態による無線端末10－3の動作は、上述した第1の形態及びその変形例による無線端末10－1の動作と比較してネットワークアクセス処理部150において若干異なる。第1の形態及びその変形例では、無線LAN接続情報及び事前認証の対象とする基地局の情報つまりIPアドレスを予め記述されたパラメータ記憶部180から取得していた動作が、第3の形態では、ネットワークアクセス処理部150が、まず設定情報ダウンロード部210に対してネットワークアクセス処理部150が指定する特定の設定情報サーバ80から無線LAN接続のため、及び本発明の事前認証のための設定情報をダウンロードする旨を要求し、設定情報ダウンロード部210が設定情報サーバ80から取得した設定情報をパラメータ記憶部180に格納し、格納が完了した旨がネットワークアクセス処理部150へ通知され、パラメータ記憶部180に格納された情報を用いて無線LAN接続及び本発明の事前認証を開始する。事前

認証を開始した後の動作に関しては、上述した第1の形態及びその変形例における動作と同様である。

[0191] 第3の形態における無線端末10－3の動作は、最初の基地局にすでに接続されネットワーク40に接続された端末とのデータ通信が可能である状態であり、第3の形態における無線端末10－3は設定情報サーバ80と図15の無線LAN通信インタフェース部170を介して設定情報の取得動作を行う。

[0192] また、最初の基地局に接続するための無線LAN接続情報は予めパラメータ記憶部180に格納されている必要がある。

[0193] なお、最初の基地局への接続動作と、設定情報サーバ80からの設定情報の取得動作と、本発明の事前認証に関する開始動作のタイミングについては、必ずしも全て連続で行う必要はない。前述各動作における前提条件としては、最初の基地局への接続動作に関してはすでにパラメータ記憶部180に接続するための情報が格納されている必要があり、設定情報サーバ80からの設定情報の取得動作に関しては何かしらネットワークに接続済みである必要があり、本発明の事前認証に関する開始動作のタイミングについては、事前認証の対象とする基地局に対する情報がすでにパラメータ記憶部180に格納されている必要があるということだけである。

[0194] つまり、次のようにいくつかの動作タイミングが考えられる。

[0195] 第3の形態における無線端末10－3は、最初ある基地局へ接続しており、あるタイミングでネットワークアクセス制御部150より設定情報サーバ80からの設定情報の取得要求の指令が出されると設定情報ダウンロード部210は設定情報サーバ80より設定情報を取得しパラメータ記憶部180へ取得して情報を格納し、ネットワークアクセス制御部150へ格納した旨通知する。その後、ネットワークアクセス制御部150は任意のタイミングでパラメータ記憶部180へ格納された情報を用いて本発明の事前認証を開始することが可能である。

[0196] 別のタイミングとしては、無線端末10－3は、最初ある基地局へ接続しており、あるタイミングでネットワークアクセス制御部150より設定情報サーバ80からの設定情報の取得要求の指令が出されると設定情報ダウンロード部210は設定情報サーバ80より設定情報を取得しパラメータ記憶部180へ取得して情報を格納し、ネットワークアク

セス制御部150へ格納した旨通知する。その後、ネットワークアクセス制御部150は現在接続している基地局から切断し、前述設定情報サーバ80から取得した情報を利用して別の基地局へ接続し直してから本発明の事前認証を開始するかもしれない。

[0197] 第3の形態は、上述の事前認証の対象とする基地局のIPアドレスを含むネットワーク接続情報に加えて、10－3が接続可能である基地局に対するネットワーク接続情報の取得手段を備え、取得手段を用いた取得方法が前述した第1の形態、その変形例、及び第2の形態における無線端末の動作と異なるのみで、他の動作に関しては第1の形態、その変形例、及び第2の形態における無線端末の動作と同様である。また、基地局20、30、認証サーバ50、管理装置60に関しては前述した第1の形態、その変形例、及び第2の形態におけるそれらと構成及び動作とも同様である。

[0198] 第3の形態において、無線端末10－3が設定情報サーバから設定情報を取得するときに相互認証が可能であるHTTPSを利用してもよく、その場合、無線端末にて保持しているユーザー証明書を設定情報サーバに対して提供することも可能である。設定情報サーバは無線端末から提供されたユーザー証明書に基づき、設定情報を返す内容を変更したり、設定情報を渡してもよいかどうかの可否を判断して設定情報を返したり返さなかったりすることが可能である。

[0199] また、第3の形態は、前述した第1の形態、その変形例、及び第2の形態のどれにも組み合わせることが可能であり、さらに第1及び第2の形態を組み合わせた形態、及び第1の形態の変形例及び第2の形態を組み合わせた形態のどちらにも組み合わせることが可能である。

[0200] 次に、第3の形態による効果について説明する。

[0201] 第3の形態では、事前認証の対象となる／ならない基地局のどちらも含むネットワーク接続するための情報（事前認証の対象となる基地局のIPアドレスを含む）を無線端末が現在接続しているネットワークを介して設定情報サーバから取得できるように構成されているため、無線LAN接続のためのネットワーク情報を動的に取得することができる。このため、予め無線端末に接続するための多くの基地局に対する情報を設定しておく必要がなく、また動的に設定してくれるため手動で設定する煩わしさ及び

設定間違いなどを減らしてくれる効果が得られる。

（第4の形態）

次に、本発明の第4の形態について添付の図面を参照して詳細に説明する。

[0202] 図16は、第4の形態による無線通信システムの構成を示す図である。

[0203] 図16を参照すると、上述の第3の形態による無線通信システムの構成とは、設定情報サーバ80が有線LAN通信インタフェース以外のインタフェース部（赤外線通信インタフェース、可視光通信インタフェース、HomeRF通信インタフェース、Bluetooth通信インタフェースなど）81を要している点で異なる。

[0204] 第4の形態による設定情報サーバは、第3の形態による設定情報サーバに加え、有線LAN通信インタフェース以外の無線通信インタフェース部（赤外線通信インタフェース、可視光通信インタフェース、HomeRF通信インタフェース、Bluetooth通信インタフェースなど）81を要している。第4の形態においては、第3の形態における設定情報を、無線通信インタフェース部220を介して無線端末10－4とやり取りするという動作のみ異なり、その他の動作に関しては第3の形態における動作と同様である。

[0205] なお、設定情報サーバ80は、有線LAN通信インタフェースを介してネットワーク40に接続されていても接続されていなくてもよい。

[0206] 図17において、第4の形態における無線端末10－4の構成は、第3の形態における無線端末10－3の構成（図15参照）に加え、無線LAN通信インタフェース部170とは異なる無線通信インタフェース部220を要する点で異なる。

[0207] 第4の形態においては、第3の形態におけるような、設定情報サーバとのやり取りを無線LAN経由で行うのではなく、無線通信インタフェース部220を介して取得動作をするという点が異なる。

[0208] 図16に図示の設定情報サーバ80においても、無線端末10－4と同様に、自身で備える無線通信インタフェース部を介して無線端末10－4からの設定情報取得要求に応える。

[0209] なお、ネットワークアクセス処理部150が設定情報ダウンロード部210に対して設定情報ダウンロードの指示を出し、設定情報ダウンロード部210が設定情報サーバ80から取得した設定情報をパラメータ記憶部210へ格納し、格納が完了した旨をネット

ワークアクセス処理部150へ通知され、パラメータ記憶部180へ格納された情報を用いて無線LAN接続及び本発明の事前認証を開始するという動作は、上述した第3の形態における動作と同様である。また、事前認証を開始した後の動作に関しては、前述した第1の形態及びその変形例における動作と同様である。

[0210] 第4の形態における無線端末10－4の動作は、上述した第3の形態における無線端末10－3の動作と異なり、設定情報を無線通信インタフェース部220から取得するため、第4の形態における無線端末10－4は予め無線LAN接続に接続されている必要はない。

[0211] 第4の形態は、上述の事前認証の対象とする基地局のIPアドレスを含むネットワーク接続情報に加えて、無線端末10－4が接続可能である基地局に対するネットワーク接続情報の取得手段に無線通信インタフェース部220を用いる点が上述した第3の形態における動作と異なるのみで、他の動作に関しては上述した第3の形態における無線端末10－3の動作と同様である。また、基地局20、30、認証サーバ50、管理装置60に関しては既述の第1の形態、その変形例、第2の形態、及び第3の形態のそれらと構成及び動作は同様である。

[0212] また、第4の形態は、第1の形態、その変形例、第2の形態、及び第3の形態のどれにも組み合わせることが可能であり、さらに、それら各形態の任意の組み合わせにも組み合わせることが可能である。

[0213] 次に、第4の形態における効果について説明する。

[0214] 第4の形態では、無線端末及び設定情報サーバにおいて無線LAN通信インタフェース部もしくは有線LAN通信インタフェース部の他に別途無線通信インタフェース部を備えるように構成されているため、無線通信インタフェース部を介して設定情報のやり取りができる。このため、無線端末においては無線LAN接続していない状態でも設定情報を取得することが可能である。また設定情報サーバにおいては通信インタフェース部の特性を利用して、例えばある特定の範囲内でしか通信できない場合、その特性を活かして特定の無線端末とのみ通信したりすることが可能である。

（第5の形態）

次に、本発明の第5の形態について添付の図面を参照して詳細に説明する。

[0215] 図18は、第5の形態による無線通信システムの構成を示す図である。

[0216] 図18を参照すると、上述した第4の形態による無線通信システムの構成とは、無線通信インタフェース部の代わりに設定情報サーバ80が設定情報の内容を含むバーコードの出力表示手段82を要している点で異なる。

[0217] 第5の形態における設定情報サーバは、第3の形態における設定情報サーバに加え、出力表示手段82を要している。第5の形態においては、上述の第3の形態における設定情報を、第5の形態において備える設定情報の内容を含むバーコードの出力表示手段82を介して無線端末に対して出力結果を読み取らせるという動作のみ異なり、その他の動作に関しては第4の形態における動作と同様である。

[0218] 第5の形態における無線端末10－5は、第4の形態における無線端末10－4の構成とは無線通信インタフェース部220がバーコードリーダ読み取り手段230である点が異なる。

[0219] 図19において、第5の形態における無線端末10－5の構成は、第4の形態における無線端末10－4の構成と比較して、無線通信インタフェース部220がバーコードリーダ読み取り手段230である点が異なる。第5の形態においては、上述した第4の形態における、設定情報サーバとのやり取りを無線通信インタフェース部経由で行うのではなく、第5の形態において備えるバーコードリーダ読み取り手段230を介して取得するという点が異なる。

[0220] 図18における設定情報サーバ80においても、無線端末10－5と同様に、自身で備える設定情報の内容を含むバーコードの出力表示手段82を介して無線端末10－5に設定情報を提示する。

[0221] なお、ネットワークアクセス処理部150が設定情報ダウンロード部210に対して設定情報ダウンロードの指示を出し、設定情報ダウンロード部210が設定情報サーバ80から取得した設定情報をパラメータ記憶部180へ格納し、格納が完了した旨がネットワークアクセス処理部150に通知され、パラメータ記憶部180へ格納された情報を用いて無線LAN接続、及び本発明の事前認証を開始するという動作は、上述の第4の形態によるものと同様である。

[0222] また、事前認証を開始した後の動作に関しては、前述までの各形態における動作と

同様である。

[0223] なお、設定情報サーバ80は、設定情報の内容を含むバーコードの出力表示結果を自身で表示するのみではなく、別途媒体、例えば紙などのように印刷することが可能である媒体に写すことにより、設定情報サーバの存在位置に関わらず配布したりすることが可能である。

[0224] また、第5の形態は、前述までの各形態のどれにも組み合わせることが可能であり、さらに、それら各形態の任意の組み合わせにも組み合わせることが可能である。

[0225] 次に、第5の形態による効果について説明する。

[0226] 第5の形態では、無線端末においてはバーコード読み込み部を備え、設定情報サーバにおいてはバーコード出力表示手段を備えるように構成されているため、設定情報サーバの存在位置に関わらず設定情報を含むバーコードが記録された媒体を利用することが可能である。

(第6の形態)

次に、本発明の第6の形態について添付の図面を参照して詳細に説明する。

[0227] 図20は、第6の形態による無線通信システムの構成を示す図である。

[0228] 図20を参照すると、第3の形態における無線通信システムの構成(図14参照)とは、携帯電話網90、携帯電話網90とインターネット40とを繋ぐゲートウェイ91、および無線端末を携帯電話網へ接続するための基地局92を要している点で異なる。

[0229] 携帯電話網90は、携帯電話網における閉じたネットワークにおいてデータ通信を可能とする。携帯電話網90に接続するためには、基地局92よりアクセスする必要がある。

[0230] ゲートウェイ91は、前述携帯電話網90とインターネット40間でデータ通信を可能にするためのゲートウェイである。

[0231] 基地局92は、携帯電話網90へアクセスするために必要となる基地局としての機能を保持し、携帯電話網への接続機能を有する無線端末10－6と携帯電話網90に接続された装置との間でのデータ通信を中継する動作を行う。

[0232] 第6の形態における無線端末10－6は、無線端末の無線通信インタフェース部220(図17参照)が基地局92を介して携帯電話網90へ接続する機能を有する点で上

述の第4の形態における無線端末10－4と異なる。

[0233] 第6の形態における無線端末10－6の動作は上述した第5の形態における無線端末10－5の動作と略同様である。すなわち、設定情報の取得を携帯電話網への接続機能を有する無線通信インタフェース220を介して設定情報を取得する動作が異なるのみであり、それ以外の動作はまったく同様である。

[0234] 第6の形態における無線端末10－6から送信される設定情報取得要求は、基地局92を介して携帯電話網90を通り、ゲートウェイ91によってインターネット40へ届き設定情報サーバ80へ届けられる。無線端末10－6へ返す設定情報データはその逆の経路で届けられる。

[0235] また、第6の形態は、前述までの各形態のどれにも組み合わせることが可能であり、さらに、それら各形態の任意の組み合わせにも組み合わせることが可能である。

## 産業上の利用可能性

[0236] 本発明によれば、無線LANや有線LANの端末または基地局において、無線LANによるデータ通信を行う前にネットワーク接続のための認証が必要となる装置に適用可能であり、特に基地局間を頻繁に移動する状況において特に有効である。

# 請求の範囲

[1] 無線端末から基地局を介してネットワーク接続する際に認証サーバによる認証を必要とする通信システムであって、前記無線端末から前記基地局に対して接続中のネットワークを介して事前に認証を行うことによって前記無線端末が前記基地局を介してネットワーク通信を開始する際に、接続手続きの一部を省略することができる通信システムであって、前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングすることを特徴とする通信システム。

[2] 前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングする手段を有する基地局は、前記カプセル化された事前認証のためのIPパケットをIPパケットのまま認証サーバへ転送し、且つ、認証サーバから返送されたIPパケットをIPパケットのまま前記無線端末へ転送することを特徴とする請求項1に記載の通信システム。

[3] 前記IPパケットのまま無線端末へ転送する基地局は、前記認証サーバからの認証成功通知とともに通知されるPMKを認証成功通知から分離し、認証成功通知のみを無線端末へ転送することを特徴とする請求項2に記載の通信システム。

[4] 前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングする手段を有する無線端末は、前記基地局の接続情報を取得する手段を有することを特徴とする請求項1または請求項3に記載の通信システム。

[5] 前記基地局の接続情報を取得する手段として、前記無線端末が自身で保持している基地局情報から取得することを特徴とする請求項4に記載の通信システム。

[6] 前記基地局の接続情報を取得する手段として、前記基地局の設定情報を管理しているサーバを有し、前記基地局の設定情報を管理しているサーバと通信することによって設定情報を取得することを特徴とする請求項4または請求項5に記載の通信システム。

[7] 前記基地局の接続情報を取得する手段として、無線LAN通信インタフェースを介して通信することを特徴とする請求項6に記載の通信システム。

[8] 前記基地局の接続情報を取得する手段として、無線LAN通信インタフェースとは別の無線通信インタフェースを介して通信することを特徴とする請求項6に記載の通信

システム。

[9] 前記基地局の接続情報を取得する手段として、携帯電話網への接続機能を有する無線通信インタフェースを介して通信することを特徴とする請求項6に記載の通信システム。

[10] 前記接続情報として、前記基地局のIPアドレスであることを特徴とする請求項7から請求項9のいずれかに記載の通信システム。

[11] 前記接続情報として、前記基地局への接続ネゴシエーションにて必要となる情報であることを特徴とする請求項7から請求項9に記載のいずれかの通信システム。

[12] ネットワーク接続する際に認証サーバによる認証を必要とする無線端末を当該認証結果に応じて前記ネットワークへの接続を行う基地局であって、前記無線端末から接続中のネットワークを介して事前に認証を行うことによって前記無線端末に対してネットワーク通信を開始する際に、接続手続きの一部を省略する基地局であって、前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングすることを特徴とする基地局。

[13] 前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングする手段を有する基地局は、前記カプセル化された事前認証のためのIPパケットをIPパケットのまま認証サーバへ転送し、且つ、認証サーバから返送されたIPパケットをIPパケットのまま前記無線端末へ転送することを特徴とする請求項12に記載の基地局。

[14] 基地局を介してネットワーク接続する際に認証サーバによる認証を必要とする無線端末であって、前記基地局に対して接続中のネットワークを介して事前に認証を行うことによって前記基地局を介してネットワーク通信を開始する際に、接続手続きの一部を省略することができる無線端末であって、前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングすることを特徴とする無線端末。

[15] 前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングする手段を有する無線端末は、前記基地局の接続情報を取得する手段を有することを特徴とする請求項14に記載の無線端末。

[16] 前記基地局の接続情報を取得する手段として、自身で保持している基地局情報から取得することを特徴とする請求項15に記載の無線端末。

[17] 前記基地局の接続情報を取得する手段として、前記基地局の設定情報を管理しているサーバを有し、前記基地局の設定情報を管理しているサーバと通信することによって設定情報を取得することを特徴とする請求項15または請求項16に記載の無線端末。

[18] 前記基地局の接続情報を取得する手段として、無線LAN通信インタフェースを介して通信することを特徴とする請求項17に記載の無線端末。

[19] 前記基地局の接続情報を取得する手段として、無線LAN通信インタフェースとは別の無線通信インタフェースを介して通信することを特徴とする請求項17に記載の無線端末。

[20] 前記基地局の接続情報を取得する手段として、携帯電話網への接続機能を有する無線通信インタフェースを介して通信することを特徴とする請求項19に記載の無線端末。

[21] 前記接続情報として、前記基地局のIPアドレスであることを特徴とする請求項18から請求項20のいずれかに記載の無線端末。

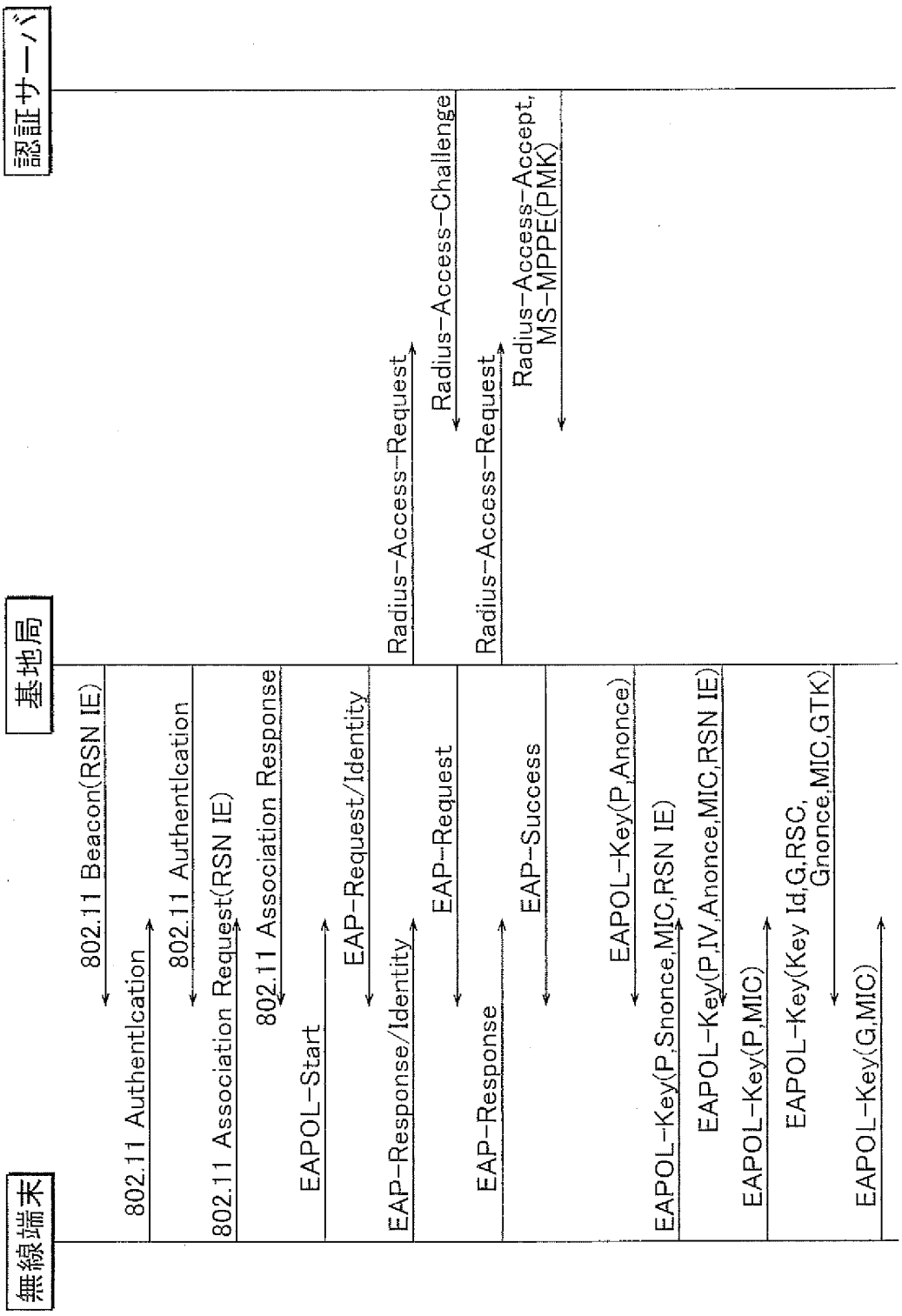
[22] 前記接続情報として、前記基地局への接続ネゴシエーションにて必要となる情報であることを特徴とする請求項18から請求項20のいずれかに記載の無線端末。

[23] 無線端末から基地局を介してネットワーク接続する際に認証サーバによる認証を必要とする通信システムに用いられる制御方法であって、前記無線端末から前記基地局に対して接続中のネットワークを介して事前に認証を行うことによって前記無線端末が前記基地局を介してネットワーク通信を開始する際に、接続手続きの一部を省略することができる通信システムに用いられる制御方法であって、前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングすることを特徴とする制御方法。

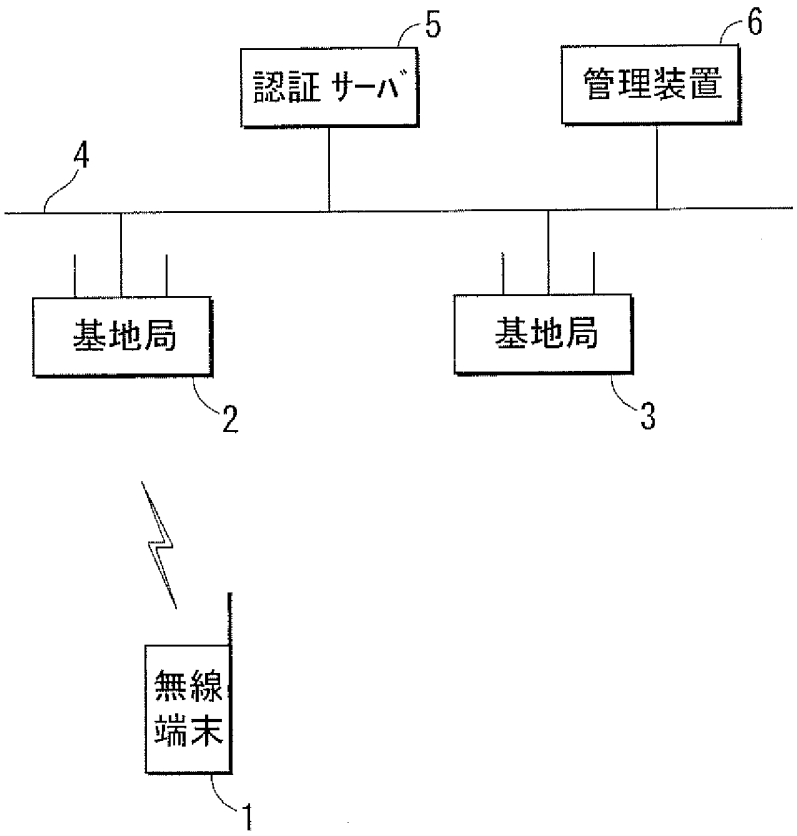
[24] 無線端末から基地局を介してネットワーク接続する際に認証サーバによる認証を必要とする通信システムに用いられる制御方法のプログラムであって、前記無線端末から前記基地局に対して接続中のネットワークを介して事前に認証を行うことによって

前記無線端末が前記基地局を介してネットワーク通信を開始する際に、接続手続きの一部を省略することができる通信システムに用いられる制御方法のプログラムであって、前記事前に行う認証フレームをIPパケットによりカプセル化してIPネットワーク上をトンネリングすること処理を実行させるためのプログラム。

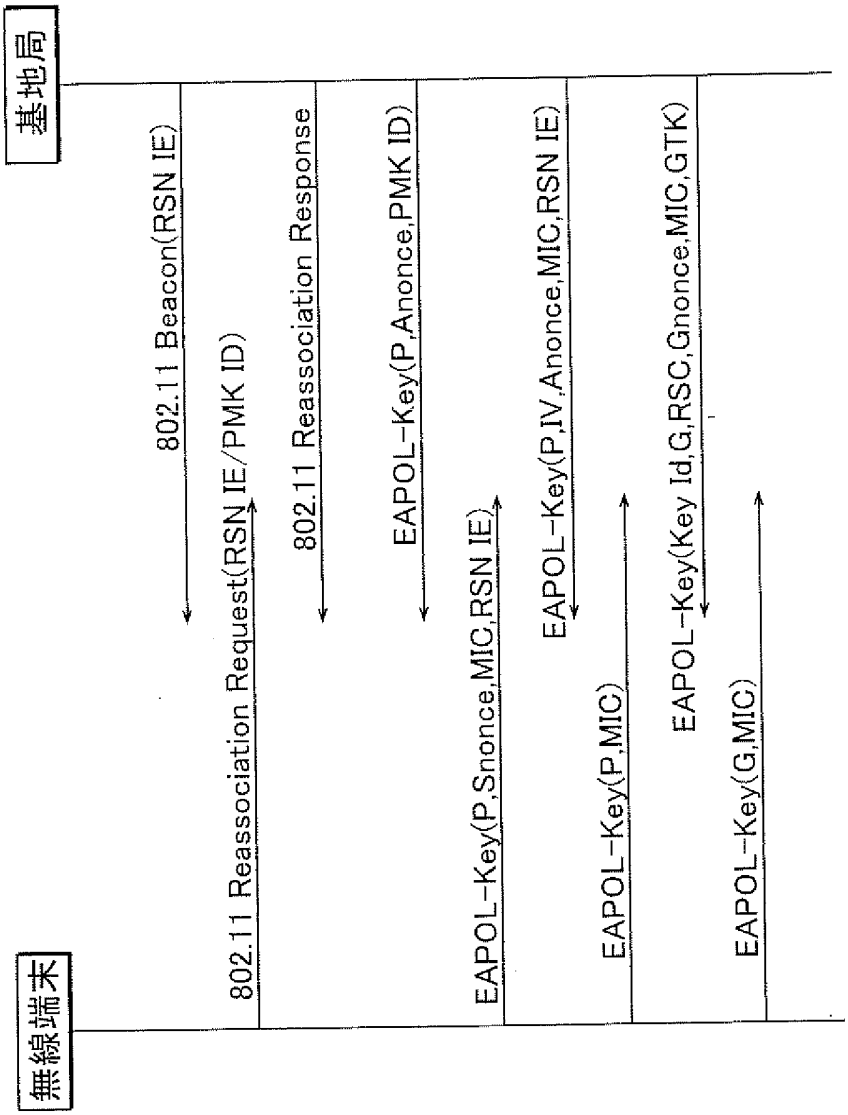
[図1]


無線端末
基地局
認証サーバ
802.11 Beacon(RSN IE)
802.11 Authentication
802.11 Authentication
802.11 Association Request(RSN IE)
802.11 Association Response
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
Radius-Access-Request
Radius-Access-Challenge
EAP-Request
Radius-Access-Request
Radius-Access-Accept,
MS-MPPE(PMK)
EAP-Response
EAP-Success
EAPOL-Key(P,Anonce)
EAPOL-Key(P,Snonce,MIC,RSN IE)
EAPOL-Key(P,IV,Anonce,MIC,RSN IE)
EAPOL-Key(P,MIC)
EAPOL-Key(Key Id,G,RSC,
Gnonce,MIC,GTK)
EAPOL-Key(G,MIC)

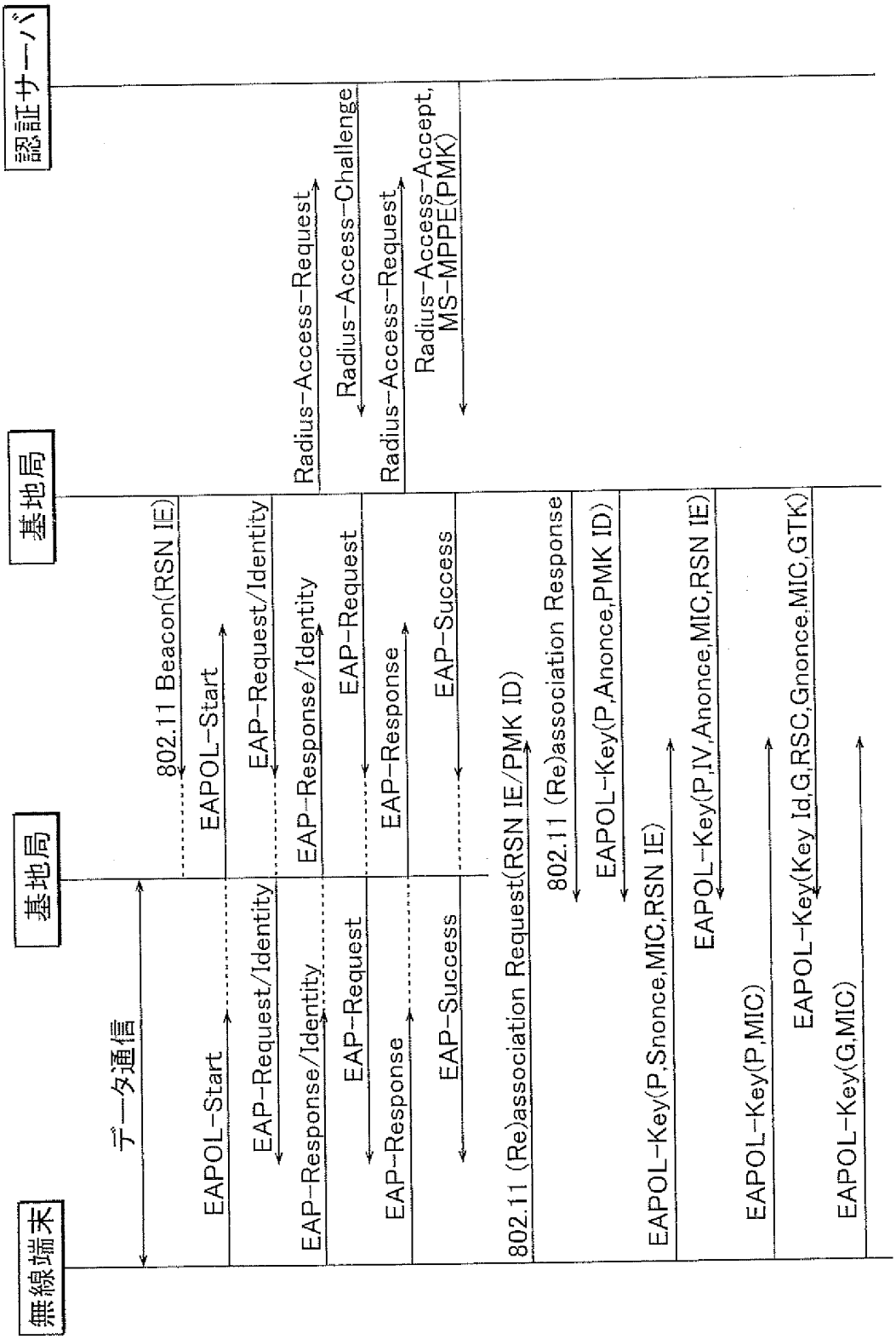
[図2]



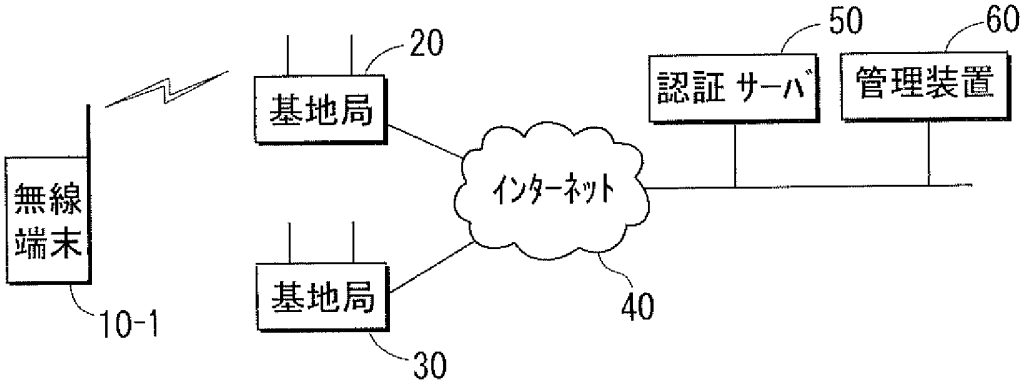
[図3]


基地局
無線端末
802.11 Beacon(RSN IE)
802.11 Reassociation Request(RSN IE/PMK ID)
802.11 Reassociation Response
EAPOL-Key(P,Anonce,PMK ID)
EAPOL-Key(P,Snonce,MIC,RSN IE)
EAPOL-Key(P,IV,Anonce,MIC,RSN IE)
EAPOL-Key(P,MIC)
EAPOL-Key(Key Id,G,RSC,Gnonce,MIC,GTK)
EAPOL-Key(G,MIC)

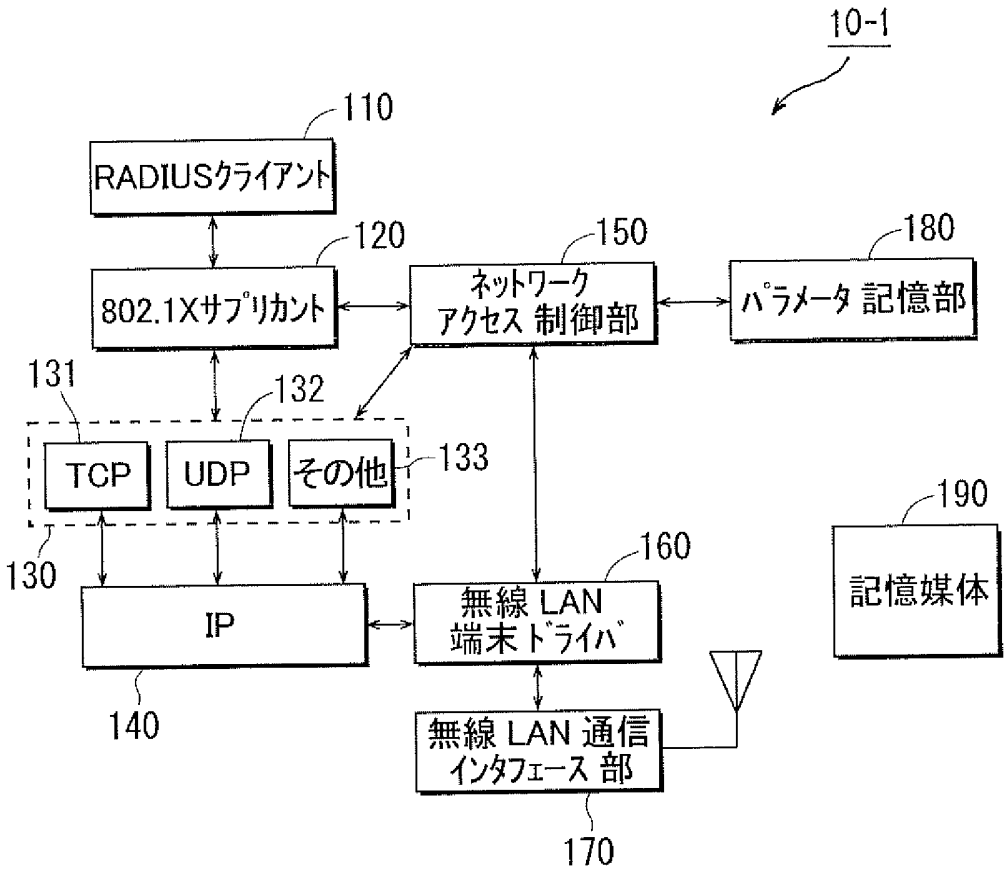
[図4]


無線端末
基地局
基地局
認証サーバ
データ通信
802.11 Beacon(RSN IE)
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
Radius-Access-Request
Radius-Access-Challenge
EAP-Request
EAP-Response
Radius-Access-Request
Radius-Access-Accept,
MS-MPPE(PMK)
EAP-Success
802.11 (Re)association Request(RSN IE/PMK ID)
802.11 (Re)association Response
EAPOL-Key(P,Anonce,PMK ID)
EAPOL-Key(P,Snonce,MIC,RSN IE)
EAPOL-Key(P,IV,Anonce,MIC,RSN IE)
EAPOL-Key(P,MIC)
EAPOL-Key(Key Id,G,RSC,Gnonce,MIC,GTK)
EAPOL-Key(G,MIC)

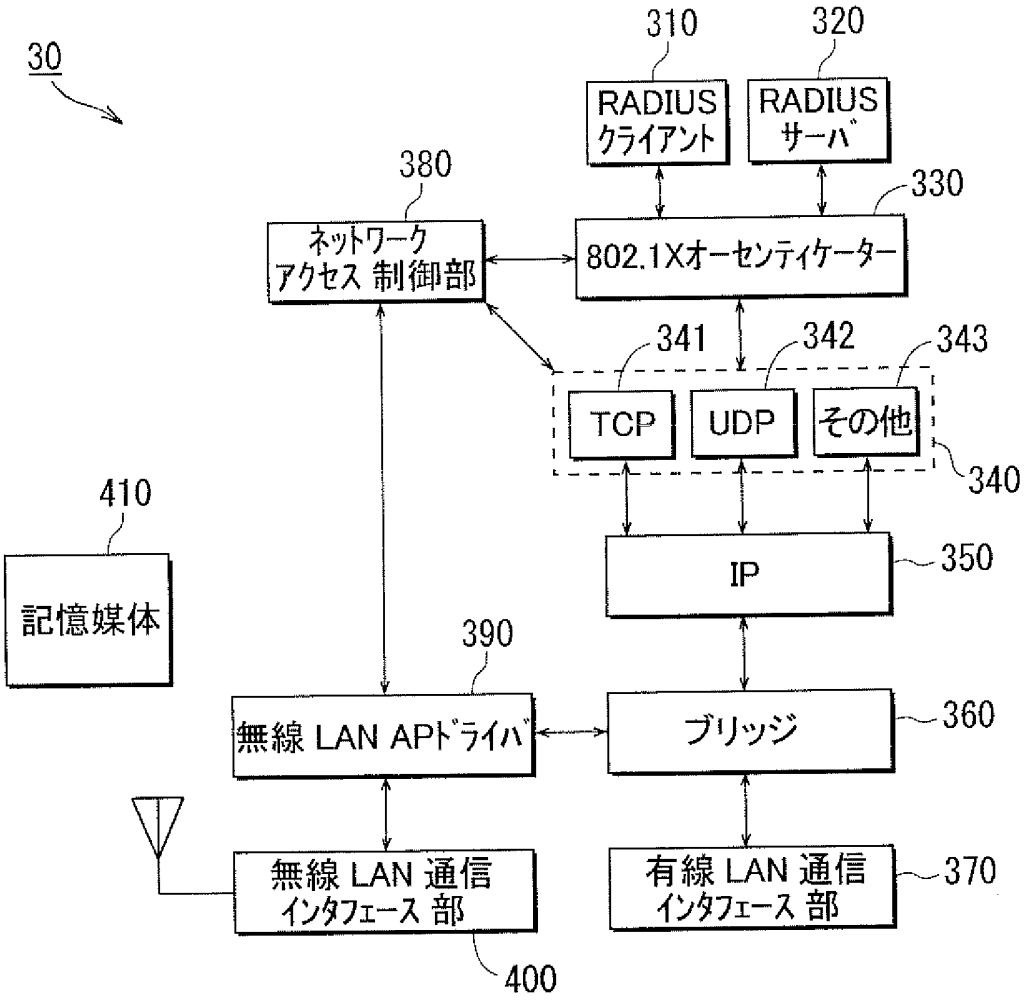
[図5]


無線
端末
10-1
基地局
20
基地局
30
インターネット
40
認証 サーバ
50
管理装置
60

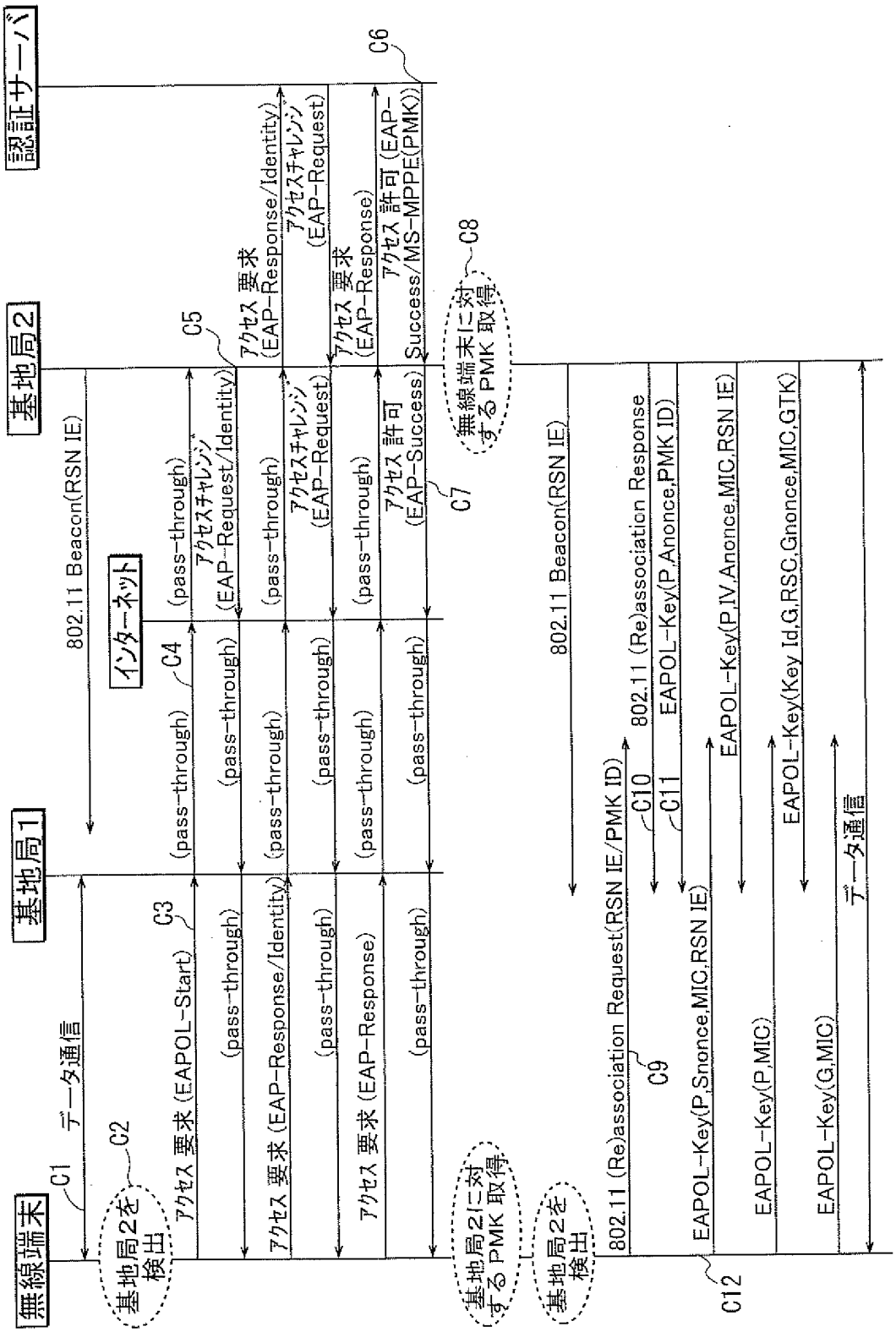
[図6]


10-1
110
RADIUSクライアント
120
802.1Xサプリカント
150
ネットワーク
アクセス 制御部
180
パラメータ 記憶部
131
132
TCP
UDP
その他
133
130
IP
140
160
無線 LAN
端末ドライバ
無線 LAN 通信
インタフェース 部
170
190
記憶媒体

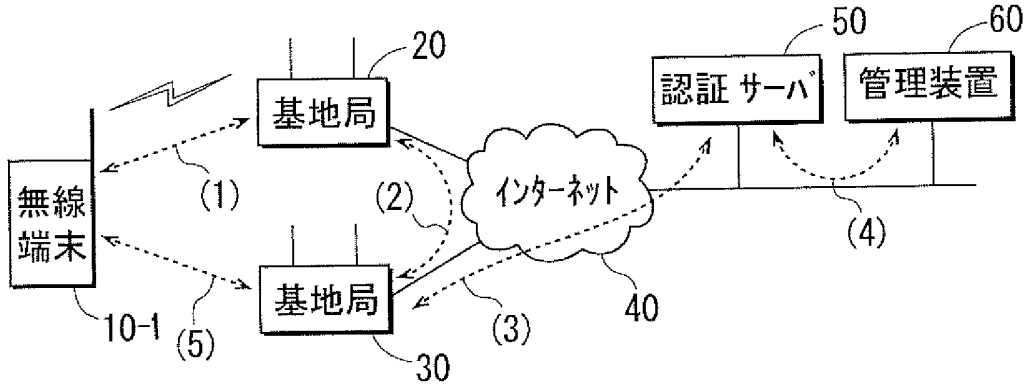
[図7]


30
310
320
RADIUS クライアント
RADIUS サーバ
380
330
ネットワーク アクセス 制御部
802.1Xオーセンティケーター
341
342
343
TCP
UDP
その他
340
410
IP
350
記憶媒体
390
無線 LAN APドライバ
ブリッジ
360
無線 LAN 通信 インタフェース 部
有線 LAN 通信 インタフェース 部
370
400

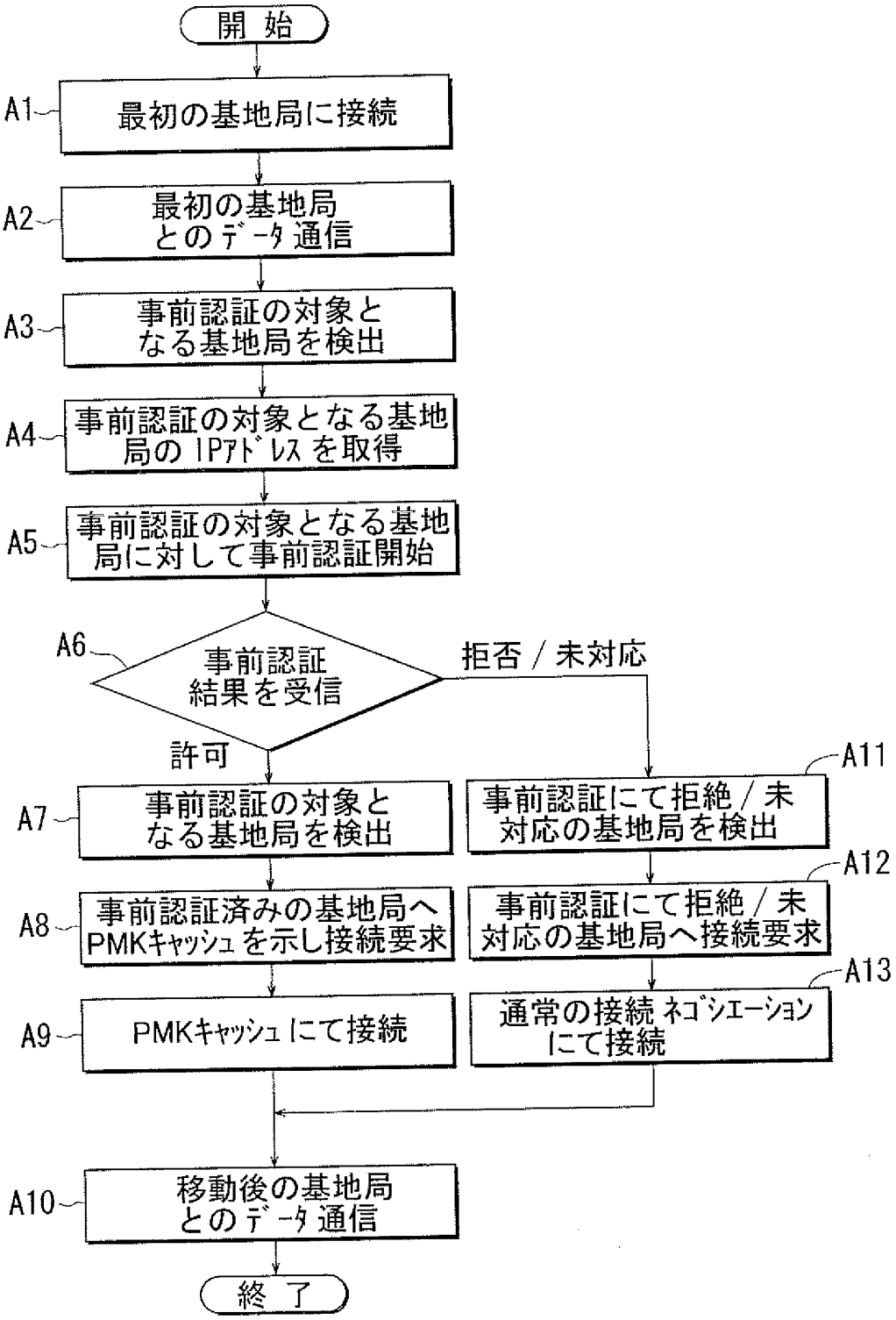
[図8]


無線端末
基地局1
基地局2
インターネット
認証サーバ
C1
データ通信
C2
基地局2を検出
C3
アクセス 要求 (EAPOL-Start)
802.11 Beacon(RSN IE)
C4
(pass-through)
アクセス 要求 (EAP-Response/Identity)
C5
アクセスチャレンジ (EAP-Request/Identity)
アクセス 要求 (EAP-Response/Identity)
アクセスチャレンジ (EAP-Request)
アクセス 要求 (EAP-Response)
C6
アクセス許可 (EAP-Success/MS-MPPE(PMK))
C7
アクセス許可 (EAP-Success)
C8
無線端末に対する PMK 取得
基地局2に対する PMK 取得
基地局2を検出
802.11 Beacon(RSN IE)
C9
802.11 (Re)association Request(RSN IE/PMK ID)
C10
802.11 (Re)association Response
C11
EAPOL-Key(P,Anonce,PMK ID)
C12
EAPOL-Key(P,Snonce,MIC,RSN IE)
EAPOL-Key(P,IV,Anonce,MIC,RSN IE)
EAPOL-Key(P,MIC)
EAPOL-Key(Key Id,G,RSC,Gnonce,MIC,GTK)
EAPOL-Key(G,MIC)
データ通信

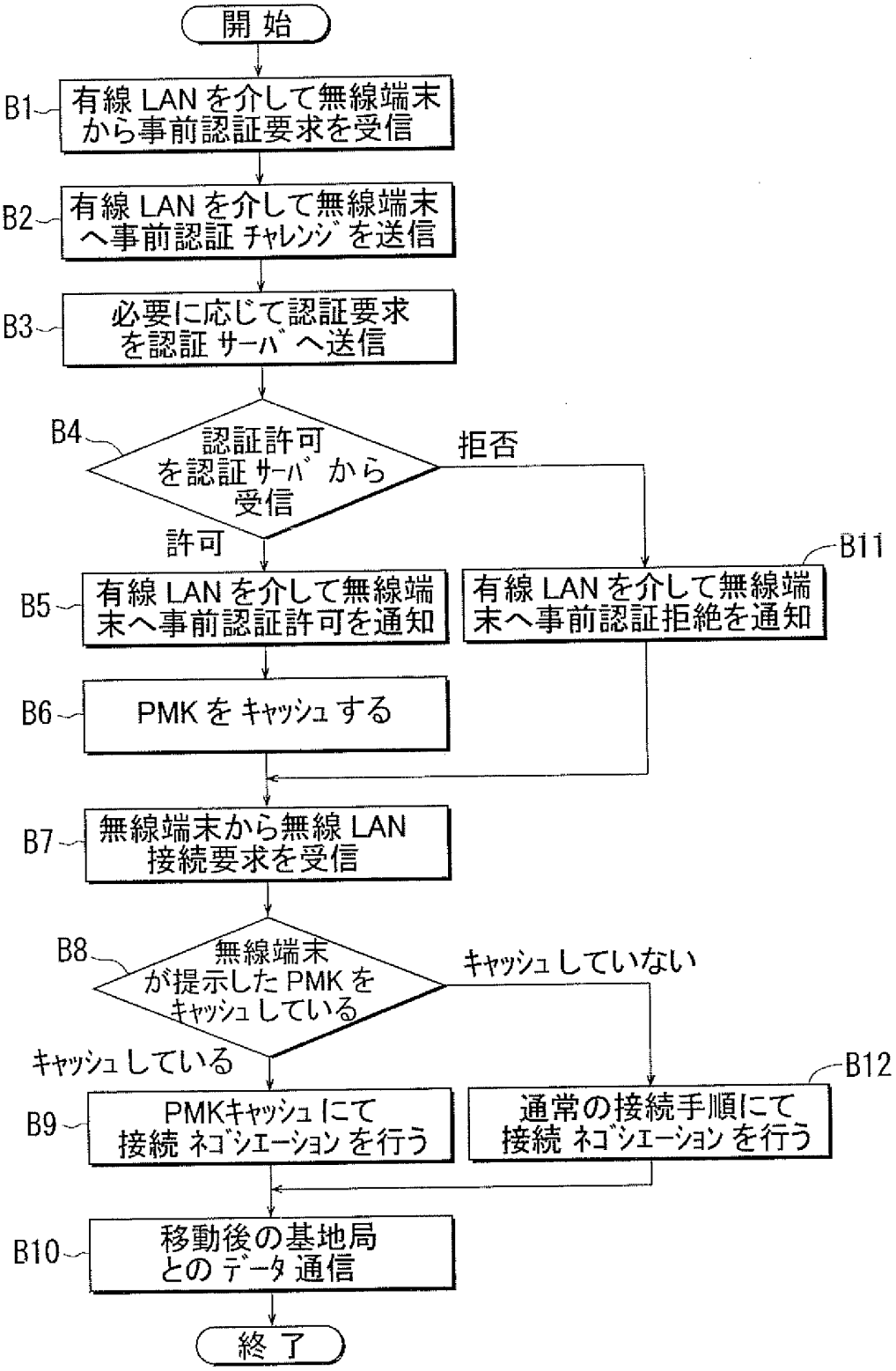
[図9]



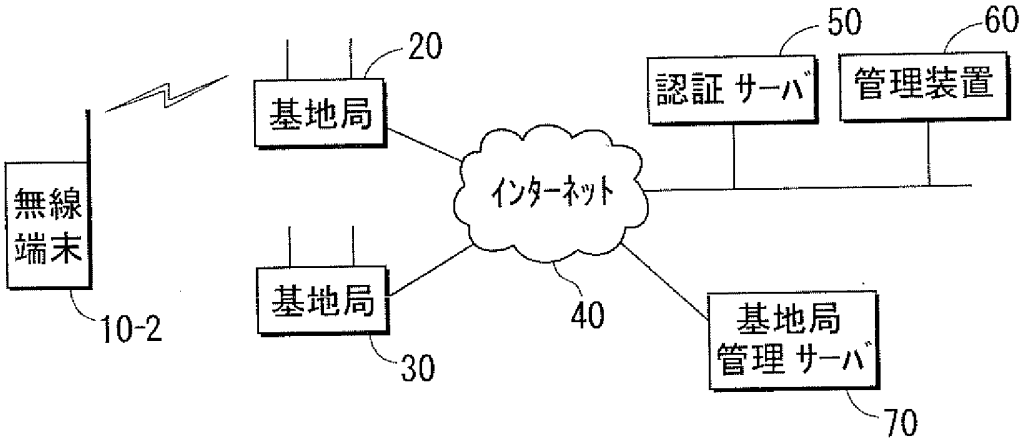
[図10]


開 始
A1
最初の基地局に接続
A2
最初の基地局
とのﾃﾞｰﾀ通信
A3
事前認証の対象と
なる基地局を検出
A4
事前認証の対象となる基地
局のIPｱﾄﾞﾚｽを取得
A5
事前認証の対象となる基地
局に対して事前認証開始
A6
事前認証
結果を受信
拒否 / 未対応
許可
A7
事前認証の対象と
なる基地局を検出
A8
事前認証済みの基地局へ
PMKｷｬｯｼｭを示し接続要求
A9
PMKｷｬｯｼｭにて接続
A10
移動後の基地局
とのﾃﾞｰﾀ通信
終 了
A11
事前認証にて拒絶 / 未
対応の基地局を検出
A12
事前認証にて拒絶 / 未
対応の基地局へ接続要求
A13
通常の接続ﾈｺﾞｼｴｰｼｮﾝ
にて接続

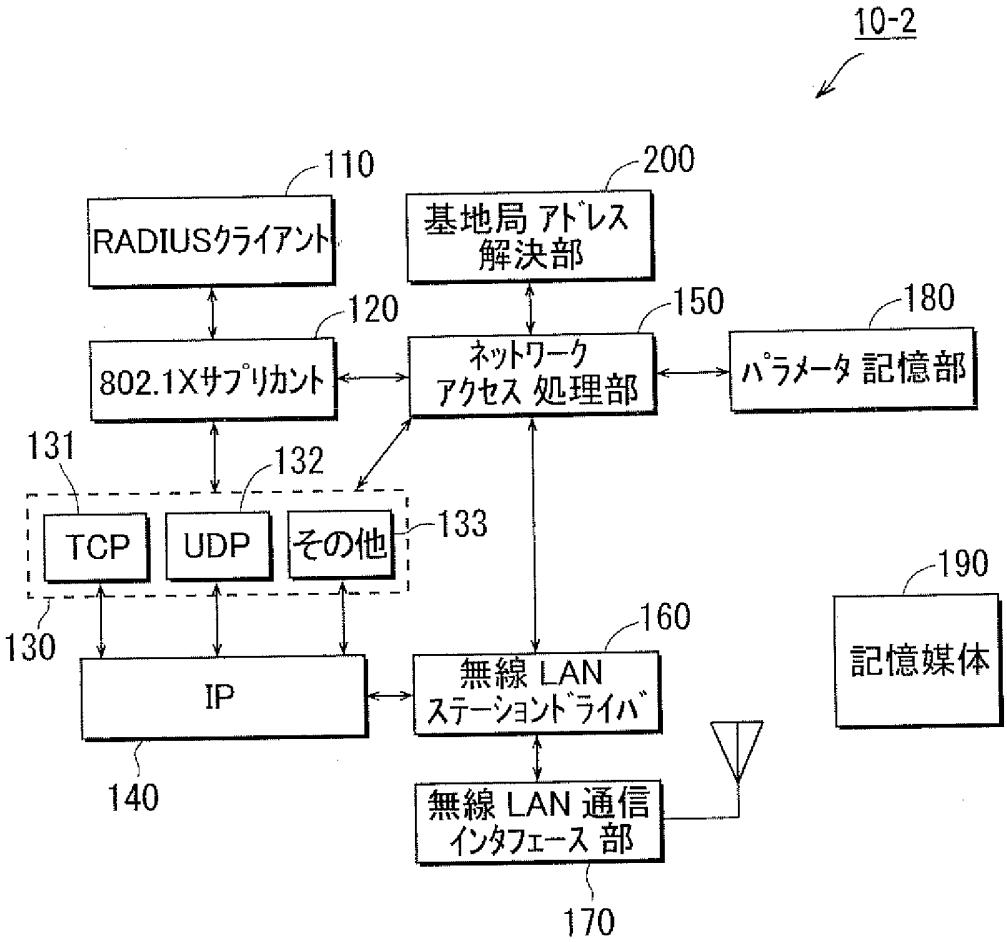
[図11]


開始
B1
有線LANを介して無線端末から事前認証要求を受信
B2
有線LANを介して無線端末へ事前認証チャレンジを送信
B3
必要に応じて認証要求を認証サーバへ送信
B4
認証許可を認証サーバから受信
拒否
許可
B11
有線LANを介して無線端末へ事前認証拒絶を通知
B5
有線LANを介して無線端末へ事前認証許可を通知
B6
PMKをキャッシュする
B7
無線端末から無線LAN接続要求を受信
B8
無線端末が提示したPMKをキャッシュしている
キャッシュしていない
キャッシュしている
B12
通常の接続手順にて接続ネゴシエーションを行う
B9
PMKキャッシュにて接続ネゴシエーションを行う
B10
移動後の基地局とのデータ通信
終了

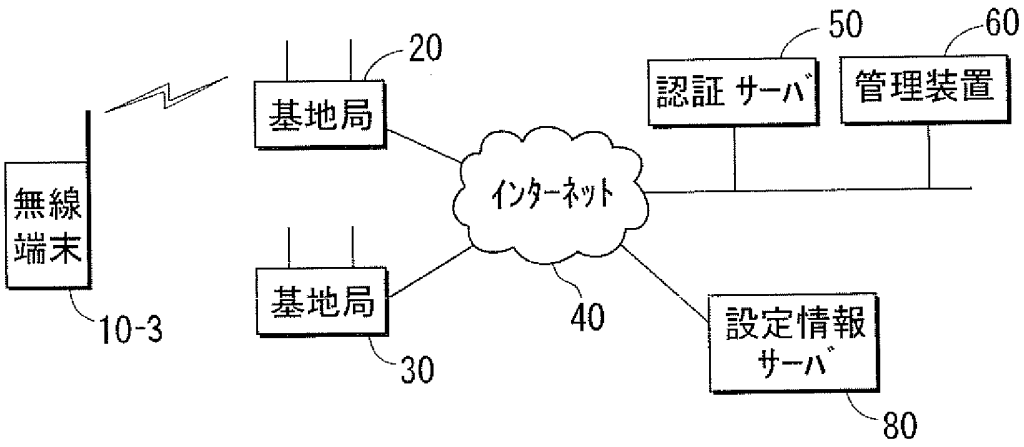
[図12]


無線
端末
10-2
基地局
20
基地局
30
インターネット
40
認証 サーバ
50
管理装置
60
基地局
管理 サーバ
70

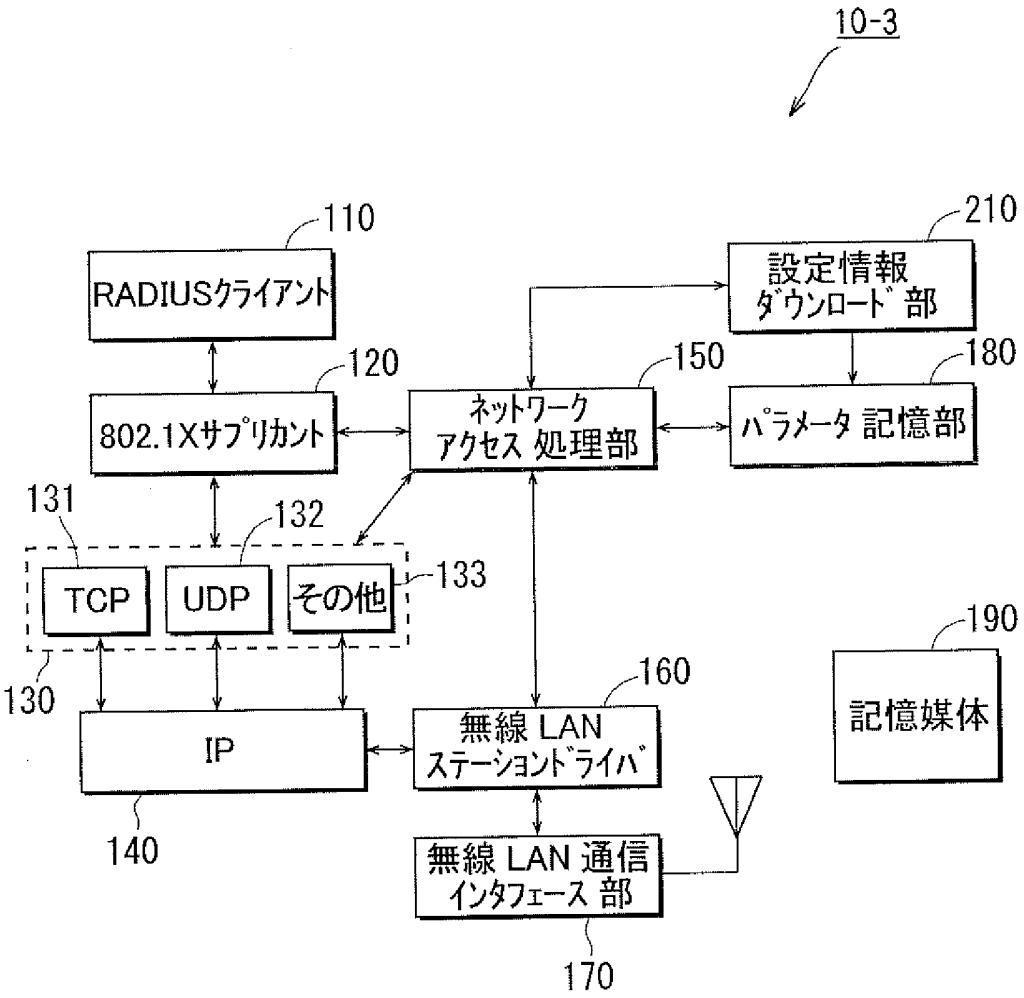
[図13]


10-2
RADIUSクライアント
110
基地局 アドレス
解決部
200
802.1Xサプリカント
120
ネットワーク
アクセス 処理部
150
パラメータ 記憶部
180
131
132
TCP
UDP
その他
133
130
IP
140
無線 LAN
ステーションドライバ
160
無線 LAN 通信
インタフェース 部
170
記憶媒体
190

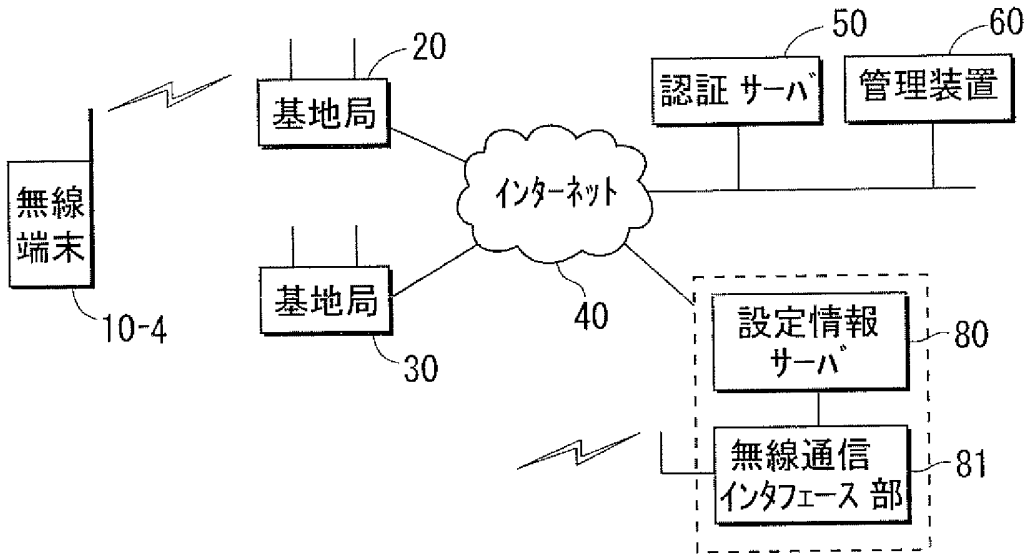
[図14]


無線端末
10-3
基地局
20
基地局
30
インターネット
40
認証 サーバ
50
管理装置
60
設定情報サーバ
80

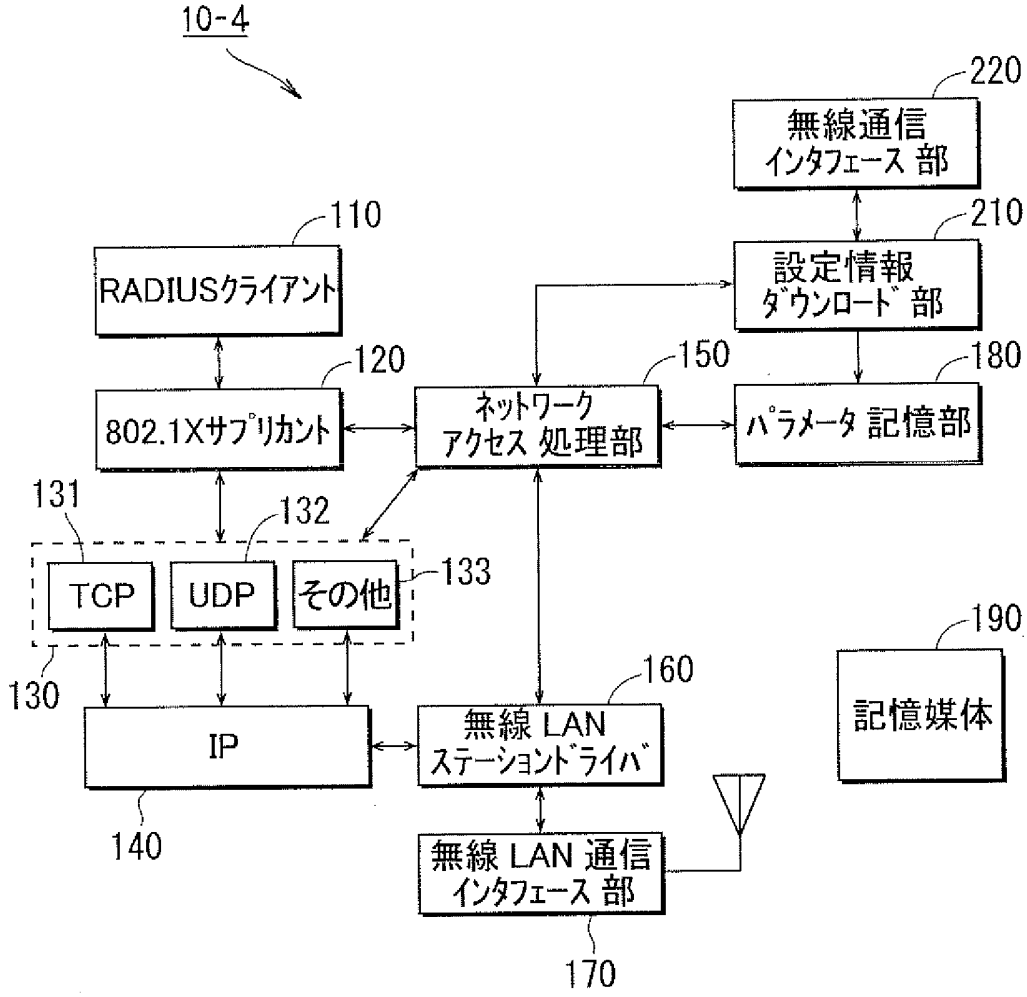
[図15]


10-3
RADIUSクライアント
110
802.1Xサプリカント
120
131
132
TCP
UDP
その他
133
130
IP
140
ネットワーク アクセス 処理部
150
設定情報 ダウンロード 部
210
パラメータ 記憶部
180
記憶媒体
190
無線 LAN ステーションドライバ
160
無線 LAN 通信 インタフェース 部
170

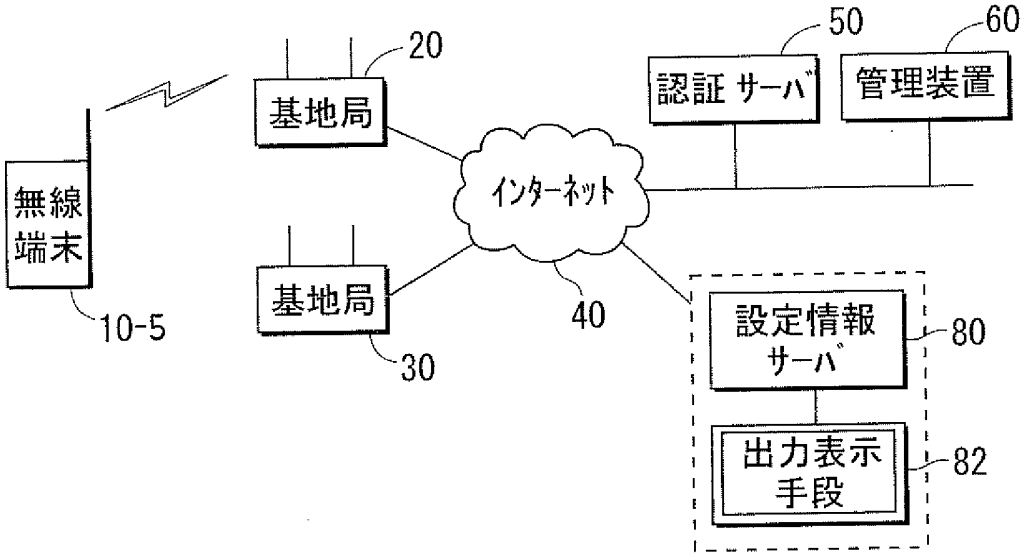
[図16]


50
60
20
認証 サーバ
管理装置
基地局
無線
端末
インターネット
基地局
40
10-4
30
設定情報
サーバ
80
無線通信
インタフェース 部
81

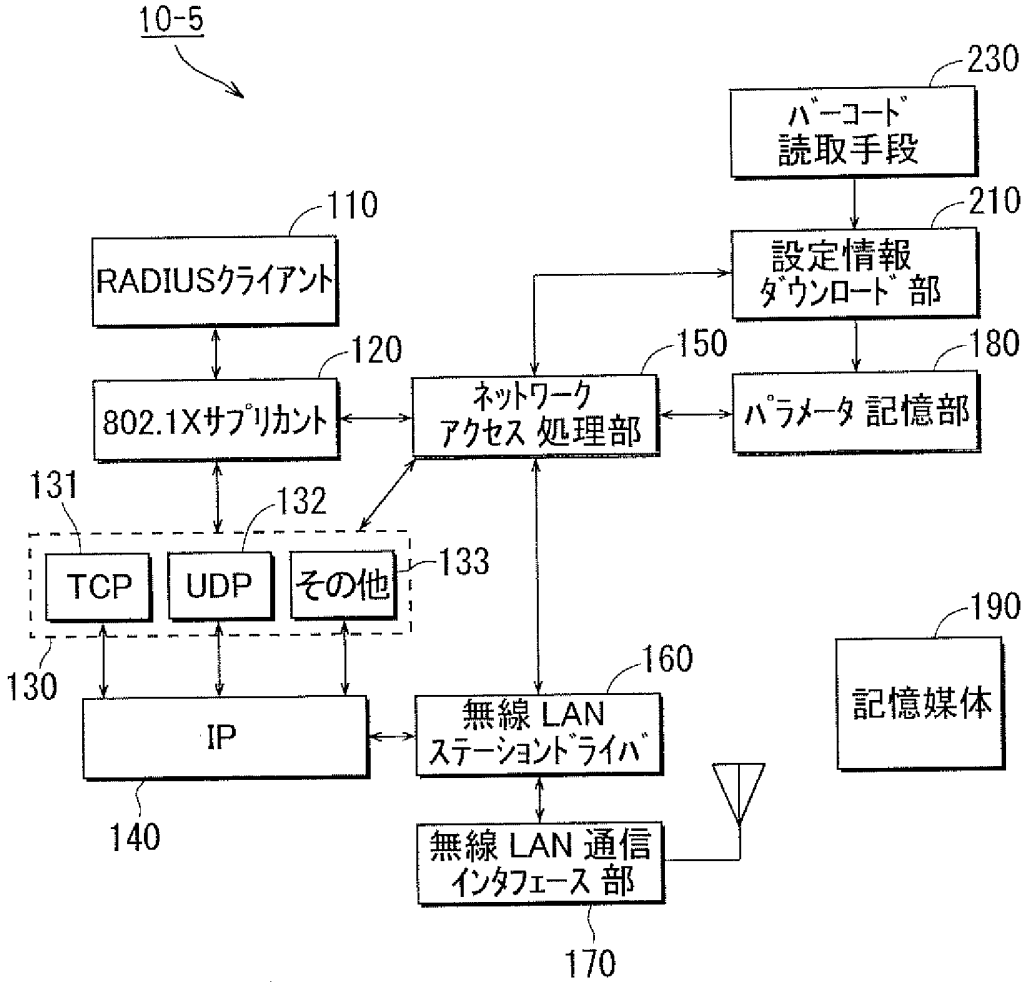
[図17]


10-4
220
無線通信
インタフェース 部
110
210
RADIUSクライアント
設定情報
ダウンロード 部
120
150
180
802.1Xサプリカント
ネットワーク
アクセス 処理部
パラメータ 記憶部
131
132
TCP
UDP
その他
133
190
130
160
記憶媒体
IP
無線 LAN
ステーションドライバ
140
無線 LAN 通信
インタフェース 部
170

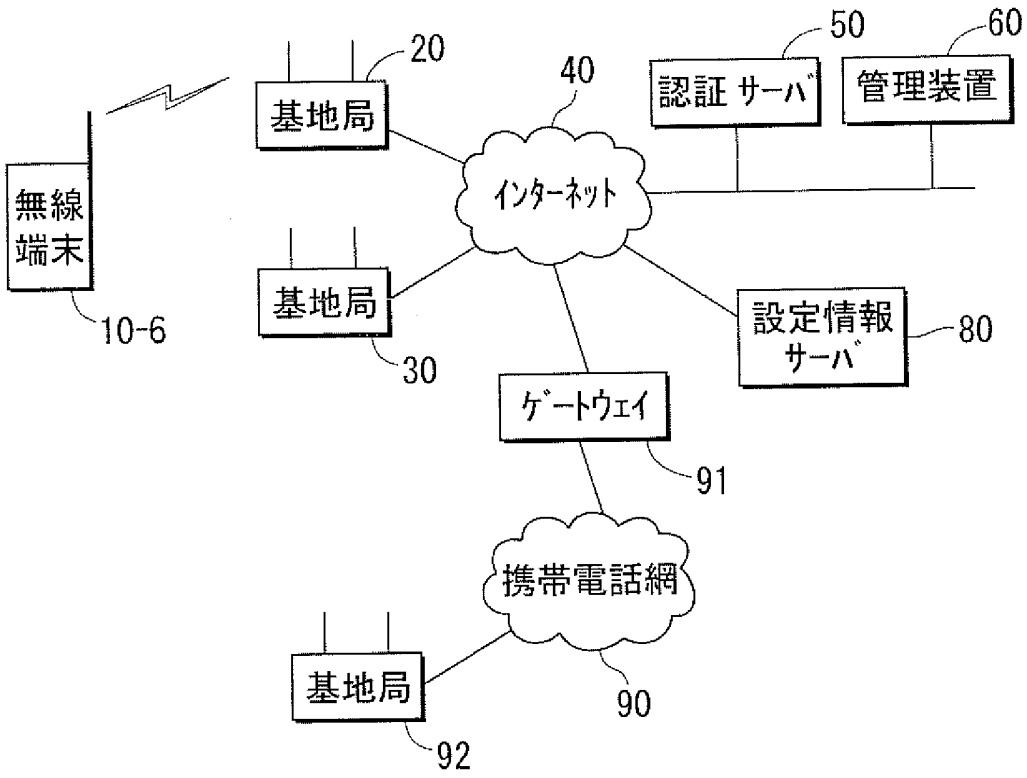
[図18]


無線端末
10-5
基地局
20
基地局
30
インターネット
40
認証サーバ
50
管理装置
60
設定情報サーバ
80
出力表示手段
82

[図19]


10-5
バーコード読取手段
230
RADIUSクライアント
110
設定情報ダウンロード部
210
802.1Xサプリカント
120
ネットワークアクセス処理部
150
パラメータ記憶部
180
131
132
TCP
UDP
その他
133
130
IP
140
無線LANステーションドライバ
160
記憶媒体
190
無線LAN通信インタフェース部
170

[図20]


無線端末
10-6
基地局
20
基地局
30
インターネット
40
認証サーバ
50
管理装置
60
設定情報サーバ
80
ゲートウェイ
91
携帯電話網
90
基地局
92

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/302995

A. CLASSIFICATION OF SUBJECT MATTER
***H04Q7/38***(2006.01), ***H04L12/28***(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04B7/24-7/26, H04Q7/00-7/38, H04L12/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | JP 2003-333639 A (Docomo Communications Laboratories U.S.A. Inc.), 21 November, 2003 (21.11.03), Par. Nos. [0029] to [0037], [0067] to [0081]; Figs. 1 to 7 & US 2003/0193910 A1 | 1-24 |
| Y | JP 2003-284117 A (Docomo Communications Laboratories U.S.A. Inc.), 03 October, 2003 (03.10.03), Par. Nos. [0013], [0037], [0049] to [0050]; Figs. 1 to 16 & US 2003/0148777 A1 & EP 1339250 A2 & EP 1526752 A2 | 1-24 |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 07 June, 2006 (07.06.06) | 20 June, 2006 (20.06.06) |
| Name and mailing address of the ISA/ Japanese Patent Office<br>Facsimile No. | Authorized officer<br>Telephone No. |

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2006/302995

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | JP 2004-007576 A (Docomo Communications Laboratories U.S.A. Inc.), 08 January, 2004 (08.01.04), Full text; all drawings & US 2003/0192309 A1 | 1-24 |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３０２９９５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　*H04Q7/38*(2006.01)，*H04L12/28*(2006.01)

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04B7/24-7/26，H04Q7/00-7/38，H04L12/28

最小限資料以外の資料で調査を行った分野に含まれるもの

| | |
|---|---|
| 日本国実用新案公報 | １９２２－１９９６年 |
| 日本国公開実用新案公報 | １９７１－２００６年 |
| 日本国実用新案登録公報 | １９９６－２００６年 |
| 日本国登録実用新案公報 | １９９４－２００６年 |

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Y | JP 2003-333639 A(ドコモ　コミュニケーションズ　ラボラトリーズ　ユー・エス・エー　インコーポレーティッド)2003.11.21<br>段落[0029]～[0037]、[0067]～[0081]及び図1～7<br>& US 2003/0193910 A1 | 1-24 |
| Y | JP 2003-284117 A(ドコモ　コミュニケーションズ　ラボラトリーズ　ユー・エス・エー　インコーポレーティッド)2003.10.03<br>段落[0013]、[0037]、[0049]～[0050]及び図1～16<br>& US 2003/0148777 A1 & EP 1339250 A2 & EP 1526752 A2 | 1-24 |

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

| | |
|---|---|
| 国際調査を完了した日<br>０７．０６．２００６ | 国際調査報告の発送日<br>２０．０６．２００６ |
| 国際調査機関の名称及びあて先<br>日本国特許庁（ＩＳＡ／ＪＰ）<br>郵便番号１００－８９１５<br>東京都千代田区霞が関三丁目４番３号 | 特許庁審査官（権限のある職員）　５Ｊ　２９５６<br>久松　和之<br>電話番号　０３－３５８１－１１０１　内線　３５３４ |

Ｃ（続き）．　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| A | JP 2004-007576 A(ドコモ　コミュニケーションズ　ラボラトリーズ　ユー・エス・エー　インコーポレーティッド)2004.01.08<br>全文、全図 & US 2003/0192309 A1 | 1-24 |