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

特許第4806028号
(P4806028)

(45)発行日　平成23年11月2日(2011.11.2)　(24)登録日　平成23年8月19日(2011.8.19)

(51)Int.Cl.		F I		
H04W 12/06	(2009.01)	H04Q	7/00	183
H04W 8/26	(2009.01)	H04Q	7/00	161
H04W 80/04	(2009.01)	H04Q	7/00	602

請求項の数 26　(全 16 頁)

(21)出願番号	特願2008-539393 (P2008-539393)
(86)(22)出願日	平成18年10月27日 (2006.10.27)
(65)公表番号	特表2009-515448 (P2009-515448A)
(43)公表日	平成21年4月9日 (2009.4.9)
(86)国際出願番号	PCT/EP2006/067895
(87)国際公開番号	WO2007/051768
(87)国際公開日	平成19年5月10日 (2007.5.10)
審査請求日	平成20年5月7日 (2008.5.7)
(31)優先権主張番号	102005052718.3
(32)優先日	平成17年11月4日 (2005.11.4)
(33)優先権主張国	ドイツ(DE)
(31)優先権主張番号	102006004868.7
(32)優先日	平成18年2月2日 (2006.2.2)
(33)優先権主張国	ドイツ(DE)

(73)特許権者　390039413
シーメンス　アクチエンゲゼルシヤフト
Ｓｉｅｍｅｎｓ　Ａｋｔｉｅｎｇｅｓｅｌｌｓｃｈａｆｔ
ドイツ連邦共和国　Ｄ－８０３３３　ミュンヘン　ヴィッテルスバッハープラッツ　２
Ｗｉｔｔｅｌｓｂａｃｈｅｒｐｌａｔｚ　２，　Ｄ－８０３３３　Ｍｕｅｎｃｈｅｎ，　Ｇｅｒｍａｎｙ
(74)代理人　100061815
弁理士　矢野　敏雄
(74)代理人　100099483
弁理士　久野　琢也

最終頁に続く

(54)【発明の名称】モビリティキーを提供する方法とサーバ

(57)【特許請求の範囲】

【請求項１】

ホームエージェントに関するモビリティシグナリングメッセージを暗号化により保護するための少なくとも１つのモビリティキーを提供する方法において：

（ａ）モバイル加入者端末装置（１）とアクセスネットワーク（４）との間に無線コネクションを確立し、加入者を認証するために、中間ネットワーク（９）の認証プロキシサーバ（８Ｃ）が、加入者識別子を包含する少なくとも１つの認証メッセージを前記アクセスネットワーク（４）と前記加入者のホームネットワーク（１２）との間で転送し、前記ホームネットワーク（１２）の認証サーバ（１１）による認証が成功したと識別すると、前記認証プロキシサーバ（８Ｃ）は前記加入者識別子を記憶し；

（ｂ）加入者識別子を包含する、加入者端末装置（１）に由来する登録リクエストメッセージを前記ホームエージェント（８Ｂ）が受信し；

（ｃ）前記登録リクエストメッセージ内に包含されている加入者識別子を包含する、モビリティキーに関するキーリクエストメッセージを前記ホームエージェント（８Ｂ）から所属の前記認証プロキシサーバ（８Ｃ）に送信し；

（ｄ）前記キーリクエストメッセージ内に包含されている加入者識別子が前記認証プロキシサーバ（８Ｃ）に記憶されている加入者識別子のうちの１つと一致する場合には、前記認証プロキシサーバ（８Ｃ）がモビリティキーを前記ホームエージェント（８Ｂ）に提供し、前記中間ネットワーク（９）は、前記ホームネットワーク（１２）によって支援されないホームＭＩＰ（Mobile Internet Protocol）機能を提供して、前記ＭＩＰを基礎とす

るマクロモビリティを実現する、
ことを特徴とする、モビリティキーを提供する方法。
【請求項２】
前記認証プロキシサーバ（８Ｃ）はモビリティキーをランダムに生成する、請求項１記載の方法。
【請求項３】
前記ホームネットワーク（１２）の前記認証サーバ（１１）は、認証の成功の際に、認証メッセージ内に包含されているＭＳＫキーを前記認証プロキシサーバ（８Ｃ）を介して前記アクセスネットワーク（４）の認証クライアント（６Ｃ）に伝送する、請求項１記載の方法。
【請求項４】
前記認証プロキシサーバ（８Ｃ）は前記モビリティキーを、伝送された前記ＭＳＫキーから導出する、請求項３記載の方法。
【請求項５】
前記モビリティキーは、伝送された前記ＭＳＫキーの一部を形成する、請求項４記載の方法。
【請求項６】
前記モビリティキーは、伝送された前記ＭＳＫキーと同一である、請求項４記載の方法。
【請求項７】
前記モビリティキーを、暗号キー導出関数または暗号ハッシュ関数によって導出する、請求項４記載の方法。
【請求項８】
前記認証メッセージをＲＡＤＩＵＳデータ伝送プロトコルに従い伝送する、請求項１記載の方法。
【請求項９】
前記認証メッセージをＤＩＡＭＥＴＥＲデータ伝送プロトコルに従い伝送する、請求項１記載の方法。
【請求項１０】
前記アクセスネットワーク（４）をＷｉＭａｘアクセスネットワーク（ＡＳＮ）によって形成する、請求項１記載の方法。
【請求項１１】
前記中間ネットワーク（９）をＷｉＭａｘ中間ネットワーク（ＣＳＮ）によって形成する、請求項１記載の方法。
【請求項１２】
前記ホームネットワーク（１２）を３ＧＰＰネットワークによって形成する、請求項１記載の方法。
【請求項１３】
前記ホームネットワークをＷＬＡＮネットワークによって形成する、請求項１記載の方法。
【請求項１４】
前記加入者識別子をネットワークアクセス識別子ＮＡＩによって形成する、請求項１記載の方法。
【請求項１５】
前記加入者識別子を前記加入者のホームアドレスによって形成する、請求項１記載の方法。
【請求項１６】
前記モビリティキーを付加的に前記アクセスネットワーク（４）のＰＭＩＰクライアント（６Ｂ）に提供する、請求項１記載の方法。
【請求項１７】

複数の中間ネットワーク（９）が前記アクセスネットワーク（４）と前記ホームネットワーク（１２）との間に存在する、請求項１記載の方法。

【請求項１８】

前記ホームエージェント（８Ｂ）は前記ホームネットワーク（１２）または前記中間ネットワーク（９）のうちの１つに設けられている、請求項１７記載の方法。

【請求項１９】

前記認証プロキシサーバ（８Ｃ）は前記ホームネットワーク（１２）または前記中間ネットワーク（９）のうちの１つに設けられている、請求項１７記載の方法。

【請求項２０】

モビリティシグナリングメッセージを暗号化により保護するためにモビリティキーを提供する認証プロキシサーバ（８Ｃ）において、

加入者を認証するために、前記認証プロキシサーバ（８Ｃ）は、加入者識別子を包含する少なくとも１つの認証メッセージをアクセスネットワーク（４）と前記加入者のホームネットワーク（１２）との間で転送し、前記ホームネットワーク（１２）の認証サーバ（１１）による認証が成功したと識別すると、前記認証プロキシサーバ（８Ｃ）は、それぞれの前記加入者の前記加入者識別子を記憶し、ホームエージェント（８Ｂ）からのモビリティキーに関するキーリクエストメッセージの受信後に、該キーリクエストメッセージ内に包含されている加入者識別子が記憶されている前記加入者識別子のうちの１つと一致する場合にはモビリティキーを提供することを特徴とする、認証プロキシサーバ（８Ｃ）。

【請求項２１】

モビリティキーをランダムに生成する、請求項２０記載の認証プロキシサーバ。

【請求項２２】

ホームネットワーク（１２）の認証サーバ（１１）と接続されている、請求項２０記載の認証プロキシサーバ。

【請求項２３】

前記モビリティキーを、ホームネットワーク（１２）の認証サーバ（１１）によって出力されたＭＳＫキーから導出する、請求項２０記載の認証プロキシサーバ。

【請求項２４】

ホームネットワーク（１２）は３ＧＰＰネットワークである、請求項２０記載の認証プロキシサーバ。

【請求項２５】

ホームネットワーク（１２）はＷＬＡＮネットワークである、請求項２０記載の認証プロキシサーバ。

【請求項２６】

ＷｉＭａｘ認証プロキシサーバである、請求項２０記載の認証プロキシサーバ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、移動無線ネットワークのホームエージェントに関するモビリティシグナリングメッセージを暗号化により保護するためのモビリティキーを提供する方法とプロキシサーバに関する。

【０００２】

ＴＣＰ／ＩＰプロトコルを用いるインターネットはモバイルの分野に関するより高度のプロトコルを開発するためのプラットフォームを提供する。インターネットプロトコルは広く普及しているので、相応のプロトコル拡張によってモバイル環境に関してより多くの利用者を開拓することができる。しかしながら従来のインターネットプロトコルは本来的にモバイルの用途的のために構想されていない。従来のインターネットのパケット交換においては固定のコンピュータ間でパケットが交換されており、これらのパケットのネットワークアドレスは変化せず、またこれらのパケットが異なるサブネットワーク間でローミングされることもない。モバイルコンピュータを備えた無線ネットワークにおいては、モ

バイルコンピュータＭＳが種々のネットワークにリンクされることが多い。ＤＨＣＰ（Dynamic Host Configuration Protocol）は、相応のサーバを用いてネットワーク内のコンピュータへのＩＰアドレスおよび別のコンフィギュレーションパラメータの動的な割り当てを実現する。ネットワークにリンクされるコンピュータにはＤＨＣＰプロトコルにより自由なＩＰアドレスが自動的に割り当てられる。モバイルコンピュータにＤＨＣＰがインストールされると、このコンピュータはＤＨＣＰプロトコルによるコンフィギュレーションを支援するローカルネットワークの範囲内で動作しなければならない。ＤＨＣＰプロトコルでは動的なアドレス設定が実現される。すなわち自由なＩＰアドレスが自動的に所定の時間にわたり割り当てられる。この時間の経過後に、モバイルコンピュータによるリクエストが新たに行われるか、ＩＰアドレスを別のやり方で割り当てることができる。ＤＨＣＰによりマニュアルによるコンフィギュレーションを行うことなくモバイルコンピュータをネットワークにリンクさせることができる。その前提として単にＤＨＣＰサーバが提供されれば良い。モバイルコンピュータはローカルネットワークのサービスを利用することができ、例えば中央に記憶されているデータファイルを利用することができる。しかしながら、モバイルコンピュータ自体がサービスを提供する場合には、潜在的なサービスユーザがそのモバイルコンピュータを発見することはできない。何故ならば、そのモバイルコンピュータのＩＰアドレスはモバイルコンピュータがリンクされるネットワーク毎に変わるからである。同様のことは、ＩＰコネクションの確立中にＩＰアドレスが変わる場合にも発生する。これによりコネクションが中断される。したがってモバイルＩＰの場合にはモバイルコンピュータに他のネットワークにおいても保持されるＩＰアドレスが割り当てられる。従来のＩＰネットワーク切り換えにおいては、ＩＰアドレス調整を相応に適合させることが必要であった。しかしながら、端末機器においてＩＰコンフィギュレーションおよびルーティングコンフィギュレーションを常に適合させることはマニュアルでは殆ど不可能である。従来の自動的なコンフィギュレーションメカニズムにおいては、確立中のコネクションがＩＰアドレスの変更の際に遮断される。ＭＩＰプロトコル（ＲＦＣ２００２，ＲＦＣ２９７７，ＲＦＣ３３４４，ＲＦＣ３８４６，ＲＦＣ３９５７，ＲＦＣ３７７５，ＲＦＣ３７７６，ＲＦＣ４２８５）はモバイル端末装置のモビリティを支援する。従来のＩＰプロトコルにおいては、モバイル端末装置にアドレッシングされたデータパケットを正確にルーティングするためにＩＰサブネットワークを切り換える場合、モバイル端末装置はその都度自身のＩＰアドレスを適合させなければならなかった。確立中のＴＣＰコネクションを維持するために、モバイル端末装置は自身のＩＰアドレスを保持しなければならない。何故ならば、アドレス変更によりコネクションは遮断されるからである。ＭＩＰプロトコルは、モバイル端末装置ないしモバイルノード（ＭＮ）が２つのＩＰアドレスを所有することを許可することによってこの矛盾を解消する。ＭＩＰプロトコルにより２つのアドレス間、すなわち恒久的なホームアドレスと一時的な気付アドレス（Care-of-Address）との間のトランスパレントなコネクションが実現される。気付アドレスはその時点においてモバイル端末装置にアクセスすることができるＩＰアドレスである。

【０００３】

ホームエージェント（Home Agent）は、モバイル端末装置が本来のホームネットワーク内に存在しない場合のこのモバイル端末装置のエージェントである。ホームエージェントにはモバイルコンピュータの現在地に関する情報が恒常的に通知される。ホームエージェントは通常の場合、モバイル端末装置のホームネットワーク内のルータの構成要素である。モバイル端末装置がホームネットワーク外に存在する場合には、ホームエージェントはモバイル端末装置がログインできる機能を提供する。この場合、ホームエージェントはモバイル端末にアドレッシングされたデータパケットをモバイル端末の現在のサブネットワークに転送する。

【０００４】

フォーリンエージェント（Foreign Agent）は、モバイル端末装置が移動しているサブネットワーク内に存在する。フォーリンエージェントは到来したデータパケットをモバイル端末装置ないしモバイルコンピュータに転送する。フォーリンエージェントはいわゆる

フォーリンネットワーク（訪問先のネットワーク）内に存在する。フォーリンエージェントも通常の場合ルータの構成要素である。フォーリンエージェントはモバイル端末装置とそのモバイル端末装置のホームエージェントとの間で全ての事務モバイルデータパケットをルーティングする。フォーリンエージェントはホームエージェントから送信、トンネリングされたＩＰデータパケットをアンパックし、そのデータをモバイル端末装置に転送する。

【０００５】

モバイル端末装置のホームアドレスは、モバイル端末装置に恒常的にアクセスすることができるアドレスである。ホームアドレスはホームエージェントと同一のアドレスプレフィクスを有する。気付アドレスはモバイル端末装置がフォーリンネットワークにおいて使用するＩＰアドレスである。

【０００６】

ホームエージェントはいわゆるモビリティ結合テーブル（MBT: Mobility Binding Table）を管理する。このテーブル内のエントリは、モバイル端末装置の２つのアドレス、すなわちホームアドレスと気付アドレスを相互に対応付け、データパケットを相応にリルートするために使用される。ＭＢＴテーブルはホームアドレス、気付アドレス、この対応付けが有効である期間（ライフタイム）についての情報に関するエントリを含む。図１は、従来技術によるモビリティ結合テーブルの一例を示す。フォーリンエージェント（ＦＡ）は訪問者リストないしビジターリスト（ＶＬ：Visitor List）を有し、このリストはその時点においてフォーリンエージェントのＩＰネットワーク内に存在するモバイル端末装置に関する情報を包含する。図２は、従来技術によるその種の訪問者リストの一例を示す。

【０００７】

モバイルコンピュータをネットワークにリンクできるようにするために、モバイルコンピュータは先ず自身がホームネットワーク内にいるのか外部ネットワーク内にいるのかを識別しなければならない。付加的にモバイル端末装置は、サブネットワーク内のどのコンピュータがホームエージェントもしくはフォーリンエージェントであるかを識別しなければならない。これらの情報はいわゆるエージェント発見（Agent Discovery）によって求められる。

【０００８】

続く登録によってモバイル端末装置は自身の現在地を自身のホームエージェントに通知することができる。このためにモバイルコンピュータないしモバイル端末装置はホームエージェントに目下の気付アドレスを送信する。登録のためにモバイルコンピュータは登録リクエスト（Registration-Request）ないし登録要求をホームエージェントに送信する。ホームエージェント（ＨＡ）は気付アドレスをリストに登録し、登録リプレイ（Registration Reply）ないし登録応答により応答する。もっともこの場合、安全性に関する問題が存在する。原理的には各コンピュータはホームエージェントに登録リクエストを送信することができるので、簡単にホームエージェントに、コンピュータは別のネットワーク内を移動しているかのように認識させることができてしまう。つまり外部のコンピュータはモバイルコンピュータないしモバイル端末装置の全てのデータパケットを受け取ることも可能であり、このことを送信器が識別することもない。これを阻止するために、モバイルコンピュータおよびホームエージェントには共通の秘密キーを使用する。モバイルコンピュータが自身のホームネットワークに戻ると、このモバイルコンピュータはホームエージェントにおける登録が抹消される。何故ならばモバイルコンピュータは全てのデータパケットを自身で受け取ることができるからである。モバイル無線ネットワークは殊に以下のセキュリティ特性を有していなければならない。

【０００９】

情報も対するアクセスは所望の通信パートナに対してのみ許可される。すなわち伝送されるデータに対する不所望な傍受者によるアクセスは許可されない。すなわちモバイル無線ネットワークは秘匿性（Confidentiality）の特性を有していなければならない。さらに真正性が与えられていなければならない。真正性（Authenticity）により通信パートナ

は、所望の通信パートナとの通信が実際に確立されたか否か、もしくは部外者が通信パートナと称しているか否かを一義的に識別することができる。認証をメッセージ毎またはコネクション毎に実施することができる。コネクションを基礎として認証が行われる場合には、セッションの開始時に一度だけ通信パートナが識別される。セッションの更なる経過に関しては、後続のメッセージが依然として相応の送信器に由来することが前提とされる。通信パートナの同定が確定されている場合であっても、すなわち通信パートナが認証されている場合であっても、通信パートナは全てのリソースへのアクセスが許可されない、もしくはネットワークを介する全てのサービスの利用が許可されない場合が発生する可能性がある。この場合においては、相応の許可は通信パートナの先行する認証を前提とする。

【００１０】

モバイルデータネットワークにおいては、メッセージがエアインタフェースを介して比較的長い区間にわたり伝送され、したがって潜在的な攻撃者はこれらのメッセージに容易にアクセスすることができる。したがってモバイル無線データネットワークにおいてはセキュリティの観点が非常に重要である。データネットワークにおける安全性を高めるための実際の手段は暗号化技術である。暗号化によって、権限のない第三者がデータにアクセスできることなく、信頼性が低い通信経路、例えばエアインタフェースを介してデータを伝送することができる。暗号化のためにデータ、すなわちいわゆる平文が暗号化アルゴリズムにより暗号文に変換される。暗号化された文を信頼性が低いデータ伝送チャネルを介して伝送し、続けて復号ないし解読することができる。非常に有望な無線アクセス技術としてＷｉＭａｘ（Worldwide Interoperability for Microwave Access）が新たな標準として提案されており、これはＩＥＥＥ８０２．１６無線伝送に関して使用される。ＷｉＭａｘにより送信局は１００Ｍｂｉｔ／秒のデータレートで５０ｋｍまでの領域をカバーすることができる。

【００１１】

図３は、ＷｉＭａｘ無線ネットワークに関する基準モデルを示す。モバイル端末装置ＭＳはアクセスネットワーク（ＡＳＮ：Access Serving Network）内に存在する。アクセスネットワークＡＳＮは少なくとも１つの訪問先ネットワーク（ＶＣＳＮ：Visited Connectivity Service Network）ないし中間ネットワークを介してホームネットワークＨＣＳＮ（Home Connectivity Service Network）と接続されている。異なるネットワークはインタフェースないし基準点Ｒを介して相互に接続されている。移動局ＭＳのホームエージェントＨＡはホームネットワークＨＣＳＮまたは訪問先ネットワークＶＣＳＮ内に存在する。

【００１２】

ＷｉＭａｘは移動局自体がＭＩＰクライアント機能を実現するモバイルＩＰ、いわゆるクライアントＭＩＰ（ＣＭＩＰ）と、ＭＩＰクライアント機能がＷｉＭａｘアクセスネットワークによって実現されているプロキシＭＩＰ（ＰＭＩＰ）の２つの実現バリエーションを支援する。このためにＡＳＮ内に設けられている機能はプロキシノード（ＰＭＮ）またはＰＭＩＰクライアントと称される。これによって自身ではＭＩＰを支援しない移動局によってもＭＩＰを使用することができる。

【００１３】

図４はホームエージェントが訪問先ネットワーク内に存在する場合の従来技術によるプロキシＭＩＰにおけるコネクション確立を示す。

【００１４】

モバイル端末装置と基地局との間の無線コネクションが確立された後に、先ずアクセス認証が行われる。認証、許可および課金の機能はいわゆるＡＡＡサーバによって行われる（ＡＡＡ：Authentication Authorization and Accounting）。モバイル端末装置ＭＳとホームネットワーク（ＨＡＡＡ）のＡＡＡサーバとの間では認証メッセージが交換され、この認証メッセージによりホームエージェントのアドレスおよび認証キーが取得される。ホームネットワーク内の認証サーバは加入者のプロフィールデータを有する。ＡＡＡサー

バはモバイル端末装置の加入者識別子を包含する認証リクエストメッセージを受け取る。ＡＡＡサーバはアクセス認証の成功後に、モバイル端末装置ＭＳとアクセスネットワークＡＳＮの基地局との間のデータ伝送区間を保護するためにＭＳＫキー（ＭＳＫ：Master Session Key）を生成する。このＭＳＫキーはホームネットワークのＡＡＡサーバから中間ネットワークＣＳＮを介してアクセスネットワークＡＳＮに伝送される。

【００１５】

アクセス認証後には、図４から見て取れるように、ＤＨＣＰプロキシサーバがアクセスネットワークＡＳＮにおいてコンフィギュレートされる。ＩＰアドレスおよびホストコンフィギュレーションが既にＡＡＡ応答メッセージに含まれている場合には、全ての情報がＤＨＣＰプロキシサーバにダウンロードされる。

【００１６】

認証および許可の成功後に、移動局ないしモバイル端末装置ＭＳはＤＨＣＰ発見リメッセージ（discovery message）を送信し、またＩＰアドレス割り当てが行われる。

【００１７】

アクセスネットワークＡＳＮがＰＭＩＰもＣＭＩＰモビリティも支援する場合には、Ｒ３モビリティコンテキストメッセージが送信されることによってフォーリンエージェントがＡＳＮハンドオーバ機能を通知する。ＰＭＩＰしか支援しないネットワークではこれを省略することができる。ホームアドレスが読み出された後に、このホームアドレスがＰＭＩＰクライアントに転送される。

【００１８】

続いてＭＩＰ登録が行われる。登録の際にホームエージェントには、モバイル端末装置の現在地に関する情報が通知される。登録のためにモバイルコンピュータは目下の気付アドレスを包含する登録リクエストをホームエージェントに送信する。ホームエージェントは気付アドレスを自身が管理するリストに登録し、登録応答（Registration Reply）により応答する。原理的には各コンピュータはホームエージェントに登録リクエストを送信することができるので、簡単にホームエージェントに、コンピュータは別のネットワーク内を移動しているかのように認識させることができてしまう。これを阻止するために、モバイルコンピュータもホームエージェントも共通の秘密キー、すなわちＭＩＰキーを使用する。ホームエージェント（ＨＡ）がＭＩＰキーを知らない場合には、ホームエージェントはＭＩＰキーを設定し、このためにホームＡＡＡサーバと通信する。

【００１９】

図４に示されているコネクション確立が終了した後に、モバイル端末装置はホームアドレスを受け取り、ホームエージェントに登録される。

【００２０】

もっともホームＡＡＡサーバがＷｉＭａｘプロトコルによって予期される属性ないしデータを供給しない場合には、図４に示されているコネクション確立は実現されない。例えば、ホームＡＡＡサーバが３ＧＰＰサーバまたはＷｉＭａｘインターワーキングを支援しないその他のＡＡＡサーバである場合には、このホームＡＡＡサーバはＭＩＰ登録のために必要とされるデータ属性、殊にホームアドレスおよび暗号化キーを提供することができない。したがってホームエージェントＨＡはＭＩＰキー（ＭＳＫ：Master Session Key）を受け取らず、加入者を拒絶する。

【００２１】

したがって本発明の課題は、ホームネットワークの認証サーバがＭＩＰ登録を支援しないモバイル無線ネットワークのためのモバイルキーの供給方法を提供することである。

【００２２】

本発明によればこの課題は、請求項１に記載されている特徴を有する方法によって解決される。

【００２３】

本発明は、ホームエージェントに関するモビリティシグナリングメッセージを暗号化により保護するための少なくとも１つのモビリティキーを提供する方法に関し、この方法は

以下のステップを有する：モバイル加入者端末装置とアクセスネットワークとの間に無線コネクションを確立し、中間ネットワークの認証プロキシサーバは加入者を認証するために、加入者識別子を包含する少なくとも１つの認証メッセージをアクセスネットワークと加入者のホームネットワーク間で転送し、認証が成功すると、ホームネットワークの認証サーバによって加入者識別子をそれぞれ記憶し；

加入者識別子を包含する、加入者端末装置に由来する登録リクエストメッセージをホームエージェントによって受信し；

登録リクエストメッセージ内に包含されている加入者識別子を包含する、モビリティキーに関するキーリクエストメッセージをホームエージェントから所属の認証プロキシサーバに送信し；

キーリクエストメッセージ内に包含されている加入者識別子が認証プロキシサーバによって記憶されている加入者識別子のうちの１つと一致する場合には、認証プロキシサーバによってモビリティキーをホームエージェントに対して提供する。

【００２４】

本発明による方法の有利な実施形態においては、モビリティキーが認証プロキシサーバによってランダムに生成される。

【００２５】

本発明による方法の有利な実施形態においては、ホームネットワークの認証サーバが、認証の成功の際に、認証メッセージ内に包含されているＭＳＫキーを認証プロキシサーバを介してアクセスネットワークの認証クライアントに伝送する。

【００２６】

本発明による方法の択一的な実施形態においては、モビリティキーが認証プロキシサーバによってランダムに生成されるのではなく、伝送されたＭＳＫキーから認証プロキシサーバによって導出される。

【００２７】

本発明による方法の有利な実施形態においては、モビリティキーが伝送されたＭＳＫキーの一部を形成する。

【００２８】

本発明による方法の択一的な実施形態においては、モビリティキーが伝送されたＭＳＫキーと同一である。

【００２９】

本発明による方法の実施形態においては、認証メッセージがＲＡＤＩＵＳデータ伝送プロトコル（radius data transmission protocol）に従い伝送される。

【００３０】

本発明による方法の択一的な実施形態においては、認証メッセージがＤＩＡＭＥＴＥＲデータ伝送プロトコル（diameter data transmission protocol）に従い伝送される。

【００３１】

本発明による方法の有利な実施形態においては、アクセスネットワークがＷｉＭａｘアクセスネットワークＡＳＮによって形成される。

【００３２】

本発明による方法の有利な実施形態においては、中間ネットワークがＷｉＭａｘ中間ネットワークＣＳＮによって形成される。

【００３３】

本発明による方法の第１の実施形態においては、ホームネットワークが３ＧＰＰネットワークである。

【００３４】

本発明による方法の択一的な実施形態においては、ホームネットワークがＷＬＡＮ加入者のためのＡＡＡインフラストラクチャを提供するネットワークによって形成される（ＷＬＡＮネットワーク）。

【００３５】

本発明による方法の有利な実施形態においては、加入者識別子がネットワークアクセス識別子ＮＡＩ（Network Access Identifier）によって形成される。

【００３６】

本発明による方法の択一的な実施形態においては、加入者識別子が加入者のホームアドレスによって形成される。

【００３７】

本発明による方法の有利な実施形態においては、モビリティキーが付加的に、アクセスネットワークのＰＭＩＰクライアントに提供される。

【００３８】

本発明による方法の有利な実施形態においては、アクセスネットワークとホームネットワークとの間に複数の中間ネットワークが存在する。

【００３９】

本発明による方法の第１の実施形態においては、ホームエージェントがホームネットワーク内に存在する。

【００４０】

本発明による方法の択一的な実施形態においては、ホームエージェントが中間ネットワーク内に存在する。

【００４１】

本発明による方法の第１の実施形態においては、認証プロキシサーバがホームネットワーク内に設けられている。

【００４２】

本発明による方法の択一的な実施形態においては、認証プロキシサーバが中間ネットワークの内の１つに設けられている。

【００４３】

さらに本発明はモビリティシグナリングメッセージを暗号化により保護するためにモビリティキーを提供する認証プロキシサーバを提供し、この認証プロキシサーバは、加入者の認証の成功後にそれぞれの加入者の加入者識別子を記憶し、ホームエージェントからのモビリティキーに関するキーリクエストメッセージの受信後に、キーリクエストメッセージ内に包含されている加入者識別子が記憶されている加入者識別子のうちの１つと一致する場合にはモビリティキーを提供する。

【００４４】

以下では、本発明の本質をなす特徴を説明するために添付の図面を参照しながら本発明による方法および本発明による認証プロキシサーバの有利な実施形態を説明する。ここで、

図１は、従来技術によるモビリティ結合テーブルの例を示す。

図２は、従来技術による訪問者リストの例を示す。

図３は、ＷｉＭａｘ無線ネットワークに関する基準ネットワーク構造を示す。

図４は、従来技術による、従来のＷｉＭａｘネットワークにおけるコネクション確立を示す。

図５は、本発明による方法の有利な実施形態によるネットワーク構造を示す。

図６は、本発明による方法の機能を説明するためのフローチャートを示す。

図７は、本発明による方法の機能を説明するための別のフローチャートを示す。

図８は、本発明による方法の機能を説明するためのチャートを示す。

【００４５】

図５から見て取れるように、モバイル端末装置１は無線インタフェース２を介してアクセスネットワーク４の基地局３に接続されている。モバイル端末装置１は任意のモバイル端末装置、例えばラップトップ、ＰＤＡ、移動電話またはその他のモバイル端末装置である。アクセスネットワーク４の基地局３はデータ伝送線路５を介してアクセスネットワークゲートウェイ６と接続されている。アクセスゲートウェイコンピュータ６には有利には別の機能、殊にフォーリンエージェント６Ａ、ＰＭＩＰクライアント６Ｂ、ＡＡＡクライ

アントサーバ６ＣおよびＤＨＣＰプロキシサーバ６Ｄが組み込まれている。フォーリンエージェント６Ａはルータであり、このルータはモバイル端末装置１のためのルーティングサービスを提供する。モバイル端末装置１へのデータパケットはトンネリングされ伝送され、またフォーリンエージェント６Ａによってアンパックされる。

【００４６】

アクセスネットワーク４のゲートウェイ６はインタフェース７を介して中間ネットワーク９のコンピュータ８と接続されている。コンピュータ８はＤＨＣＰサーバ８Ａ、ホームエージェント８ＢおよびＡＡＡプロキシサーバ８Ｃを含む。ホームエージェント８Ｂはモバイル端末装置１が本来のホームネットワーク内に存在しない場合には、このモバイル端末装置１のエージェントである。ホームエージェント８Ｂにはモバイルコンピュータの現在地に関する情報が常に通知される。モバイル端末装置１に対するデータパケットは先ずホームエージェントに伝送され、このホームエージェントからトンネリングされて、フォーリンエージェント６Ａに転送される。反対に、モバイル端末装置１から送信されるデータパケットを直接的にそれぞれの通信パートナに送信することができる。モバイル端末装置１のデータパケットは発信者アドレスとしてのホームアドレスを包含する。ホームアドレスはホームエージェント８Ｂと同一のプレフィクス、すなわちネットワークアドレスおよびサブネットワークアドレスを有する。モバイル端末装置１のホームアドレスに送信されるデータパケットはホームエージェント８Ｂによって受信され、トンネリングされてホームエージェント８Ｂからモバイル端末装置１の気付アドレスに伝送され、最終的にトンネルのエンドポイントにおいて、すなわちフォーリンエージェント６Ａまたはモバイル端末装置自体によって受信される。

【００４７】

中間ネットワーク９のコンピュータ８は別のインタフェース１０を介してホームネットワーク１２の認証サーバ１１と接続されている。ホームネットワークは例えばＵＭＴＳのための３ＧＰＰネットワークである。択一的な実施形態においては、サーバ１１はＷＬＡＮネットワークの認証サーバである。図５に示されている認証サーバ１１はＭＩＰ登録を支援しない。

【００４８】

本発明の方法によれば、コンピュータ８のＡＡＡプロキシサーバ８Ｃがホームネットワーク１２のＡＡＡサーバ１１がＭＩＰ（ＣＭＩＰ／ＰＭＩＰ）は支援されないことを識別すると、ホームエージェント８Ｂに関するモビリティシグナリングメッセージを暗号化により保護するためにモビリティキーが提供される。ＡＡＡプロキシサーバ８ＢはＣＭＩＰ／ＰＭＩＰが支援されていないことを例えば、このＡＡＡプロキシサーバの問合せに基づいてホームネットワーク１２のサーバ１１からＭＩＰ属性が供給されないことにより識別する。モビリティシグナリングメッセージを暗号化により保護するために、ＰＭＩＰのケースに関してホームエージェント８Ｂとモバイル端末装置１に対する共通のモビリティキー（ＭＩＰキー）が必要とされるか、ＰＭＩＰのケースに関してホームエージェント８ＢとＰＭＩＰクライアント６Ｂに対する共通のモビリティキーが必要とされる。ホームネットワーク１２がＷｉＭａｘインターワーキング能力を有する場合には、ホームエージェント８ＢがこのＭＩＰキーをホームネットワーク１２のＡＡＡサーバから受け取る。もっとも図５に示されているようにＡＡＡサーバ１１が、ホームエージェント８Ｂの相応の問合せに対して、必要とされるＭＩＰ属性を提供できない場合には、本発明による方法が実施される。図５に示されている場合のように、３ＧＰＰ－ＡＡＡサーバ１１がホームエージェント８Ｂの問合せを解釈できないために、この３ＧＰＰ－ＡＡＡサーバ１１はモビリティシグナリングメッセージを保護するための相応の暗号化キーを提供できない。本発明による方法においては、ホームネットワーク１２のＷｉＭａｘ能力を有する認証サーバ１１は変更されないままであり、モビリティキーはＡＡＡプロキシサーバ８Ｃによってホームエージェント８Ｂに提供される。ホームネットワーク１２の認証サーバ１１はモビリティキーを提供しないということが識別された後では、いわゆるプロキシホームＭＩＰ機能が起動され、このＡＡＡセッションに関して局所的なデータセットが認証プロキシサーバ８

Ｃによって生成される。すなわち本発明によれば、ＰＭＩＰ／ＣＭＩＰに必要とされる機能がホームネットワーク１２の認証サーバ１１によって提供されるのではなく、３ＧＰＰネットワークの認証サーバ１１とアクセスネットワーク４のゲートウェイ６との間の通信経路内に存在する中間ネットワーク９のＡＡＡプロキシサーバによって提供される。

【００４９】

図６は、本発明による方法の実施形態において、モバイル端末装置１を認証するためのフローチャートを示す。

【００５０】

開始ステップＳ０の後にステップＳ１においては、先ずモバイル端末装置１とアクセスネットワーク４の基地局３との間に無線コネクションが確立される。

【００５１】

続いてステップＳ２においては、アクセスネットワーク４とホームネットワーク１２との間で認証メッセージが中間ネットワーク９の認証プロキシサーバ８Ｃによって転送される。認証メッセージはそれぞれのモバイル端末装置１を識別するための加入者識別子を包含する。加入者識別子は例えばネットワークアクセス識別子ＮＡＩである。択一的に、加入者識別子は例えばモバイル端末装置１のホームアドレスによって形成される。ＡＡＡプロキシサーバから転送された認証メッセージはホームネットワーク１２の認証サーバ１１に到達する。ホームネットワーク１２の認証サーバ１１は加入者の認証を行う。認証が成功すると、認証サーバ１１は相応のメッセージを中間ネットワーク９の認証プロキシサーバ８Ｃを介してアクセスネットワーク４に送信する。ステップＳ３においては、中間ネットワーク９の認証プロキシサーバ８Ｃが、ホームネットワーク１２の認証サーバ１１による認証は問題なく終了したか否かを検査する。認証プロキシサーバ８Ｃはこのことを例えば認証サーバ１１の相応の成功通知（success notification）において識別する。認証プロキシサーバ８Ｃがホームネットワーク１２からアクセスネットワーク４に伝送されるメッセージに基づき、加入者の認証は問題なく終了したことを識別すると、ステップＳ４において認証プロキシサーバ８Ｃによって相応の加入者識別子が抽出され、中間記憶される。

【００５２】

プロセスはステップＳ５において終了する。したがってＡＡＡプロキシサーバ８Ｃは、その認証が問題なく終了している加入者ないしモバイル端末装置１の全ての加入者識別子を記憶する。

【００５３】

図７から見て取れるように、開始ステップＳ６の後にホームエージェント８Ｂが後の時点において登録リクエストメッセージを受け取ると、ホームエージェント８ＢがステップＳ８において相応のキーリクエストメッセージを認証プロキシサーバ８Ｃに送信する。受け取った登録リクエストメッセージには、モバイル端末装置１の加入者識別子が包含されている。これに基づき生成される、ホームエージェント８Ｂの認証プロキシサーバ８Ｃへの相応のキーリクエストメッセージは同様にこの加入者識別子を包含する。認証プロキシサーバ８ＣはステップＳ９において、キーリクエストメッセージ内に包含されている加入者識別子がステップＳ４においてこの認証プロキシサーバによって記憶された加入者識別子のうちの１つと一致するか否かを検査する。一致する場合には、認証プロキシサーバ８ＣがステップＳ１０においてモビリティ保護メッセージを暗号的に保護するためのモビリティキーを提供する。認証プロキシサーバ８Ｃは提供されたモビリティキーをホームエージェント８Ｂに伝送する。有利には、モビリティキーが中間ネットワーク４の認証クライアントサーバ６Ｄにも伝送される。プロセスはステップＳ１１において終了する。

【００５４】

本発明による方法の第１の実施形態においては、ステップＳ１０において提供されたモビリティキーが認証プロキシサーバ８Ｃによってランダムに生成される。択一的な実施形態においては、モビリティキー（ＭＩＰキー）が認証プロキシサーバ８Ｃによって、この認証プロキシサーバ８Ｃが認証サーバ１１からアクセスネットワーク４に転送したＭＳＫ

（Master Session Key）キーから導出される。ＭＩＰキーをＭＳＫキーから任意のキー導出関数、例えばハッシュ関数に従い導出することができる。ハッシュ関数は任意の大きさのデータをいわゆる指紋（fingerprint）に低減する。この種のハッシュ関数の例はＳＨＡ－Ｉを表す。最大で2^{64}ビットのデータが１６０ビットにマッピングされる。択一的なハッシュ関数はＭＤ５である。ＭＤ５はＳＨＡ－Ｉのように入力を５００ビットの大きさのブロックに分割し、１２８ビットの大きさのハッシュ値を形成する。

【００５５】

択一的な実施形態においては、提供されるモビリティキーが認証プロキシサーバ８Ｃによって受信されたＭＳＫキー１２の一部によって形成される。

【００５６】

別の択一的な実施形態においては、提供されたモビリティキーが伝送されたＭＳＫキーと同一である。

【００５７】

有利な実施形態において認証メッセージはラディウス（ＲＡＤＩＵＳ）プロトコルまたはディアメータ（ＤＩＡＭＥＴＥＲ）プロトコルに従い伝送される。

【００５８】

本発明による方法においては、ホームＭＩＰ機能がホームネットワーク１２によって支援されない場合には、中間ネットワーク９がこのホームＭＩＰ機能を提供する。これによって、ＭＩＰを支援しないホームネットワーク、例えば３ＧＰＰネットワークにおいても、ＭＩＰを基礎とするマクロモビリティを実現することができる。種々のアクセスネットワーク４間のハンドオーバを実現するために、ＭＩＰがアクセスネットワーク４および中間ネットワーク９において使用される。フォーリンエージェント６ＡのＭＩＰ登録の際に、中間ネットワーク９のホームエージェント８Ｂが所属の認証プロキシサーバ８Ｃのモビリティキーを問い合わせる。ホームエージェント８Ｂは相応の加入者識別子、すなわち例えばネットワークアクセス識別子ＮＡＩ（Network Access Identifier）またはモバイル端末装置１のホームアドレスを使用する。相応のデータセットが生成されている場合には、このキーリクエストメッセージが認証プロキシサーバ８Ｃによって局所的に応答される。認証プロキシサーバ８Ｃがそれぞれのキーを提供できるようにするために、この認証プロキシサーバ８Ｃは、ホームネットワーク１２の認証サーバ１１とアクセスネットワーク４におけるオーセンティケータとの間においてモバイル端末装置１の認証中に交換されるメッセージを解釈できるように設計されている。

【００５９】

図５に示されているように、ホームエージェント８Ｂは有利には中間ネットワーク９内に存在する。択一的な実施形態においてはホームエージェント８Ｂがホームネットワーク１２内に存在する。

【００６０】

本発明による方法の択一的な実施形態においては、モバイルＩＰ機能としてモバイルＩＰＶ６［ＲＦＣ３７７５］が使用される。

【００６１】

本発明による方法の有利な実施形態においては、モビリティキーがホームエージェント８Ｂによって一度だけ認証プロキシサーバからのキーリクエストメッセージを用いて問合せられる。

【００６２】

本発明による方法でもって、例えばＷｉＭａｘネットワークのためのＷＬＡＮまたは３ＧＰＰサーバのようなレガシー（Legacy）ＡＡＡサーバがＷｉＭＡＸネットワークによって予期されるＣＭＩＰ／ＰＭＩＰ機能を提供しないにもかかわらず、このサーバを使用することができる。本発明による方法でもって、ホームネットワーク１２においてレガシーＡＡＡサーバが使用されるにもかかわらずＰＭＩＰベースのマクロモビリティが実現される。したがってＷＬＡＮまたは３ＧＰＰネットワークのネットワークプロバイダはＰＭＩＰを一般的に自身で支援する必要は無く、またそれにもかかわらず自身の顧客にＷｉＭａ

ｘ無線ネットワークを用いるローミング／インターワーキングを実現させる。殊に本発明による方法でもって、ＰＭＩＰ支援により端末装置もモバイルＩＰの支援なしでＷｉＭａｘインターワーキングを実現することができる。殊に本発明による方法は、現在規定されているＷＬＡＮダイレクトＩＰアドレス（WLAN-direct-IP-Access）と同様にＷｉＭａｘ－３ＧＰＰインターワーキングを実現することができる。

【００６３】

図８は、本発明による方法の有利な実施形態のメッセージフローチャートを示す。アクセス認証中にホームネットワーク、例えば３ＧＰＰネットワークの認証サーバがホームエージェントアドレスを供給しない場合には、訪問先のネットワークの認証サーバが中間ネットワークのホームエージェントに関するホームアドレスを適用し、中間ネットワークのホームエージェント８Ｂによるモビリティキーの後のリクエストに対する状態を適用する。状態データは加入者識別子を包含する。図４に示されているステップ１６ｂ，１７ａ、すなわちホームエージェント８Ｂによるホームネットワーク１２の認証サーバ１１に対するモビリティキーのリクエストおよび所属の応答は本発明による方法では省略される。本発明による方法においては、加入者識別子を包含するキーリクエストメッセージが中間ネットワーク９の認証プロキシサーバ８Ｃによって応答される。したがって本発明による方法は、ホームネットワークによる支援がなくともＷｉＭａｘネットワークにおけるマクロモビリティ管理を実現する。

【図面の簡単な説明】

【００６４】

【図１】従来技術によるモビリティ結合テーブルの例を示す。

【図２】従来技術による訪問者リストの例を示す。

【図３】ＷｉＭａｘ無線ネットワークに関する基準ネットワーク構造を示す。

【図４】従来技術による、従来のＷｉＭａｘネットワークにおけるコネクション確立を示す。

【図５】本発明による方法の有利な実施形態によるネットワーク構造を示す。

【図６】本発明による方法の機能を説明するためのフローチャートを示す。

【図７】本発明による方法の機能を説明するための別のフローチャートを示す。

【図８】本発明による方法の機能を説明するためのチャートを示す。

【図１】

従来技術

モビリティ結合テーブル

ホームアドレス	気付アドレス	ライフタイム (ms)
131.192.180.42	129.142.23.42	100
213.123.24.140	172.23.142.49	150
・・・	・・・	・・・

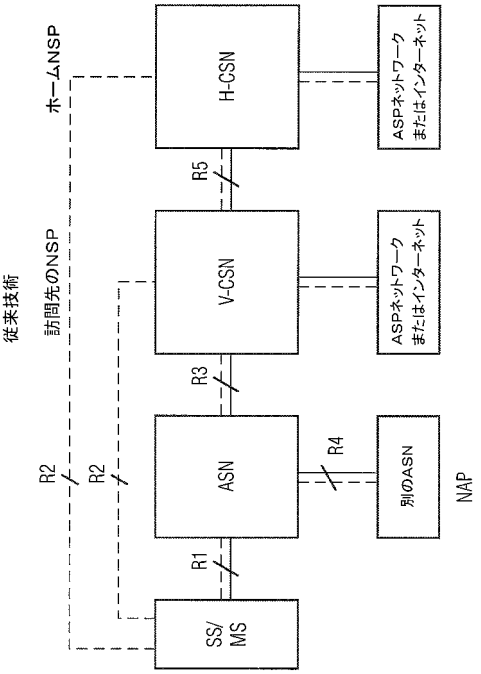
【図２】

従来技術

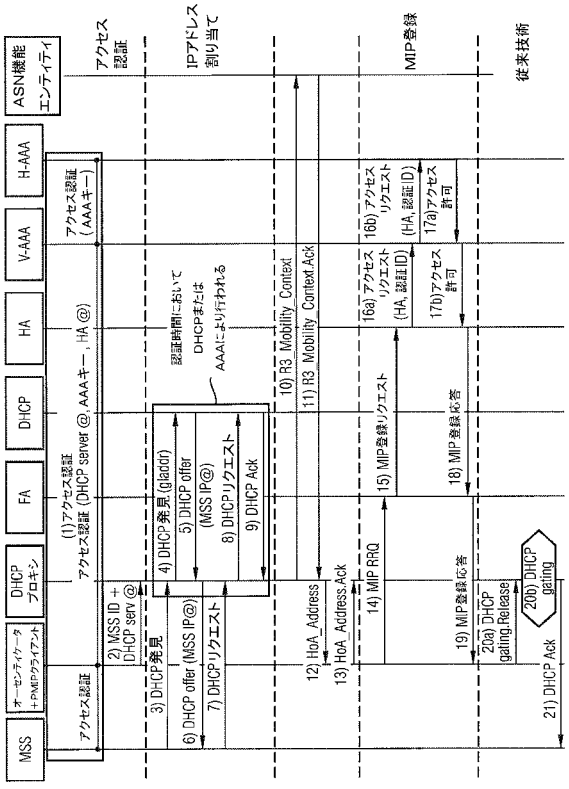
訪問者リスト

ホームアドレス	ホームエージェントアドレス	メディアアドレス	ライフタイム
131.192.180.42	129.142.23.42	08-00-46-26-75-6A	100
213.123.24.140	172.23.142.49	00-02-B3-77-43-00	150
・・・	・・・	・・・	・・・

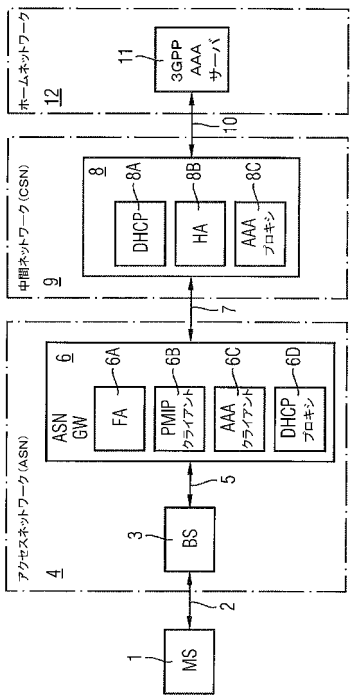
【図３】



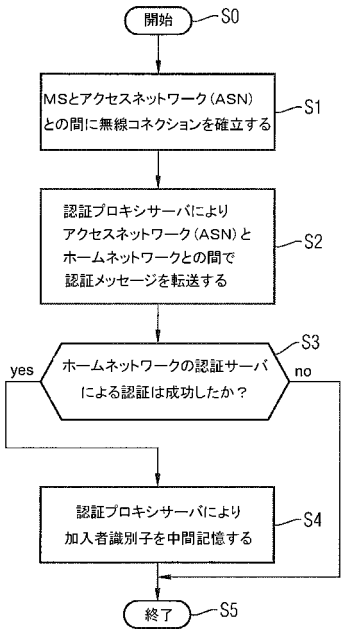
【図４】



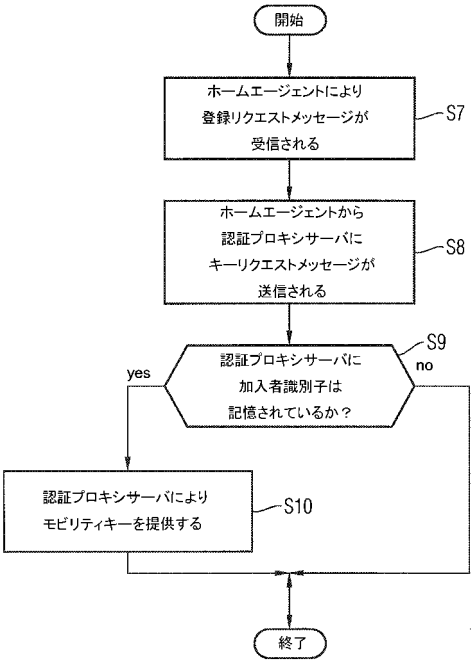
【図５】



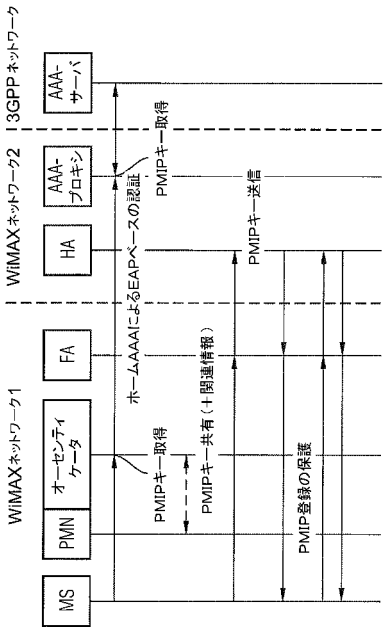
【図６】


開始
S0
MSとアクセスネットワーク（ASN）との間に無線コネクションを確立する
S1
認証プロキシサーバにより アクセスネットワーク（ASN）と ホームネットワークとの間で 認証メッセージを転送する
S2
yes
ホームネットワークの認証サーバによる認証は成功したか？
S3
no
認証プロキシサーバにより 加入者識別子を中間記憶する
S4
終了
S5

【図７】


開始
ホームエージェントにより 登録リクエストメッセージが 受信される
S7
ホームエージェントから 認証プロキシサーバに キーリクエストメッセージが 送信される
S8
yes
認証プロキシサーバに 加入者識別子は 記憶されているか？
S9
no
認証プロキシサーバにより モビリティキーを提供する
S10
終了

【図８】


3GPPネットワーク
AAA-サーバ
WiMAXネットワーク2
AAA-プロキシ
HA
WiMAXネットワーク1
FA
オーセンティケータ
PMN
MS
ホームAAAによるEAPベースの認証
PMIPキー取得
PMIPキー送信
PMIPキー取得
PMIPキー共有（＋関連情報）
PMIP登録の保護

フロントページの続き

(74)代理人 100128679
弁理士 星 公弘
(74)代理人 100135633
弁理士 二宮 浩康
(74)代理人 100114890
弁理士 アインゼル・フェリックス＝ラインハルト
(72)発明者 ライナー ファルク
ドイツ連邦共和国 エヒング ホラーナー シュトラーセ ２３アー
(72)発明者 ディルク クレーゼルベルク
ドイツ連邦共和国 ミュンヘン ペスタロッツィシュトラーセ ２７
(72)発明者 マクシミリアン リーゲル
ドイツ連邦共和国 ニュルンベルク マックスフェルトシュトラーセ ２４アー

審査官 稲葉 崇

(56)参考文献 特表２００７－５３５２２５（ＪＰ，Ａ）
国際公開第２００５／０６９５６７（WO，Ａ１）
MADJID NAKHJIRI，INTERNET DRAFT，スイス，IETF，２００５年 １月，P1-9

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B 7/24-7/26
H04W 4/00-99/00
H04L 12/00-12/26
H04L 12/50-12/66
H04L 12/28,12/44-12/46
G09C 1/00-5/00
H04K 1/00-3/00
H04L 9/00-9/04