(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4510682号
(P4510682)
(45)発行日　平成22年7月28日(2010.7.28)　(24)登録日　平成22年5月14日(2010.5.14)

(51)Int.Cl.　　F I
H04W 40/34 (2009.01)　　H04L 12/56　100D
H04L 12/56 (2006.01)　　H04L 12/56　H

請求項の数 23　(全 17 頁)

(21)出願番号　特願2005-110465(P2005-110465)
(22)出願日　平成17年4月7日(2005.4.7)
(65)公開番号　特開2006-121647(P2006-121647A)
(43)公開日　平成18年5月11日(2006.5.11)
審査請求日　平成19年5月8日(2007.5.8)
(31)優先権主張番号　093123263
(32)優先日　平成16年8月3日(2004.8.3)
(33)優先権主張国　台湾(TW)

(73)特許権者　504376348
合勤科技股▼ふん▲有限公司
台湾台北縣新竹科学園區創新二路６號
(74)代理人　100091683
弁理士　▲吉▼川　俊雄
(74)代理人　100075247
弁理士　最上　正太郎
(72)発明者　陳志成
台湾新竹市東區湖濱里１０鄰明湖路４７８之６號
(72)発明者　林俐▼い▲
台湾台北市南京東路５段１６３號６Ｆ～６
(72)発明者　劉義文
台湾台北縣中和市連城路２６３巻２７弄６號３Ｆ

最終頁に続く

(54)【発明の名称】移動式ＶＰＮのエージェントをダイナミックに割り当てる方法及び装置

(57)【特許請求の範囲】
【請求項１】
移動式VPNのエージェントをダイナミックに割り当てる方法であって、少なくとも一つの外部ネットワークと内部ネットワークとの間にバーチャルプライベートネットワーク（Virtual Private Network, VPN）を構築することにより、少なくとも一つのモバイルノード（Mobile Node, MN）が前記外部ネットワークで安全にローミングできるようにする方法において、
下記のステップを含むプログラムを順次実行することを特徴とする上記の方法。
（ａ）　前記モバイルノードが前記内部ネットワークから前記外部ネットワークにローミングを行う際に、前記モバイルノードから外部ホームアドレスリクエスト及びホームエージェントのアドレスリクエストが含まれている登録要求情報をローカルの外部ホームエージェントに送信するように、DHCPサーバから前記モバイルノードへ接続用アドレスを送信するステップ。
（ｂ）　前記外部ホームエージェントから外部AAAサーバに授権確認要求情報を送信し、これにより、前記外部AAAサーバが選定の対象となる少なくとも一つの外部ホームエージェントのネットワークアクセス識別子（Network Access Identifier, NAI）を前記授権確認要求情報に書きこんだ後にホームAAAサーバに転送するステップ。
（ｃ）　前記外部ホームエージェントは前記外部ネットワークに接続され、前記ホームAAAサーバにより前記外部ホームエージェントと、前記モバイルノードとの間のセキュリティアソシエーション（Security Association）を構築すると共に、ホームエージェントリク

エスト情報を生成して前記外部ホームエージェントに送信するステップ。
（ｄ） 前記外部ホームエージェントが、外部ホームアドレスを前記モバイルノードに割り当てると共に、外部ホームアドレス及び自身のアドレスをホームエージェントの授権確認応答情報に設定して、前記ホームAAAサーバに送信するステップ。
（ｅ） 前記ホームAAAサーバが、前記外部ホームアドレスを前記モバイルノードの接続用アドレスとして前記ホームエージェントにログインし、ログイン終了後に、前記ホームエージェントが、前記外部ホームエージェントに授権確認応答情報を送信する権限を前記ホームAAAサーバに授けるステップ。
及び
（ｆ） 前記外部ホームエージェントが、前記授権確認応答情報から前記外部ホームアドレス及びホームエージェントアドレスを含む授権登録返信情報を取得して前記モバイルノードに転送し、その後、前記モバイルノードが前記外部ネットワークでローミングする際に、前記外部ホームアドレスを用いて前記外部ホームエージェントのアドレスログインできるようにするステップ。
【請求項２】
前記モバイルノードが、ワイヤレスネットワーク装置が設けられた携帯式パソコンである、請求項１に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項３】
前記モバイルノードが前記外部ネックワークで初回のローミングを行うステップに先立って、
前記DHCPサーバから連続してアドバータイズメントアンドチャレンジ（Advertisement & Challenge）情報を前記外部ネットワークに送信してネットワークでローミングしている前記モバイルノードの有無を確認し、ローミングしている前記モバイルノードが検出された場合には、自動的にモバイルIPアドレスを前記モバイルノードに割り当てるステップ、及び
前記モバイルノードが前記モバイルIPアドレスを前記接続用アドレス（CoA）として用い、前記外部ホームエージェントに前記ログイン要求を送信するステップを実行する、
請求項１に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項４】
前記登録要求情報には、更に前記ホームAAAサーバによって授権されるべき認証情報及び前記モバイルノードのネットワークアクセス識別子（NAI）が含まれている、 請求項1に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項５】
前記外部ホームアドレス及び外部ホームエージェントアドレスの登録要求情報には、これらのアドレスが全て0、0、0、0と設定されている、請求項1に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項６】
前記モバイルノードが前記外部ネットワークで初回のローミングを行うステップの後に、外部エージェントが、前記登録要求情報を受信した後に、前記モバイルノードのホームアドレスリクエストフラッグ及び前記ホームエージェントリクエストフラッグが設定されている特徴ベクトルの属性値ペア（MIP‐Feature‐Vector Attribute Value Pair）を生成するステップ、及び
前記特徴ベクトルの属性値ペアを前記授権確認要求情報内に設定するステップをさらに含む、請求項1に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項７】
、前記外部ホームエージェントによって授権確認要求情報を送信するステップの後に、
前記ホームAAAサーバが、前記外部AAAサーバから転送されてきた前記授権確認要求を受信した後に、前記授権確認要求に設定されたMN‐AAA‐セキュリティパラメータインデックス（Security Parameters Index）により前記モバイルノードが授権認証を行う際に用いるセキュリティ対策を確認するステップを含む、請求項1に記載の移動式VPNのエージェン

トをダイナミックに割り当てる方法。
【請求項８】
前記ホームAAAサーバによってセキュリティアソシエーションを構築するステップが、
前記ホームAAAサーバにより少なくとも128ビットのランダムなキー（Key Materials）を生成し、前記キーを用いた計算によりセッションキー（Session Key）を生成してセキュリティアソシエーションのセキュリティ性を確認するステップ、及び
前記セッションキーをホームエージェントの要求情報に設定するステップをさらに含む、請求項1に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項９】
前記ホームAAAサーバによってセキュリティアソシエーションを構築するステップでは、ホームエージェントの要求情報が前記外部AAAサーバを介して前記外部ホームエージェントに転送される、請求項1に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項１０】
前記ホームAAAサーバによってセキュリティアソシエーションを構築するステップでは、ホームエージェントの要求情報が前記モバイルノードと前記外部ホームエージェント間のキー及びセッションキーを含む、請求項1に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項１１】
前記外部ホームエージェントによって前記モバイルノードに外部ホームアドレスを割り当てるステップでは、前記ホームエージェントの授権確認応答情報が前記外部AAAサーバを介して前記ホームAAAサーバに転送される、請求項1に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項１２】
前記外部ホームエージェントによって登録返信情報を前記モバイルノードに転送するステップが、更に、
前記モバイルノードが前記外部ホームアドレスとVPNゲートウェイの接続線交点を用いて前記モバイルノードと前記VPNゲートウェイ間でIPsecチャンネルを構築するステップを含む、請求項1に記載の移動式VPNのエージェントをダイナミックに割り当てる方法。
【請求項１３】
移動式VPNの外部エージェントをダイナミックに割り当てる装置であって、少なくとも一つの外部ネットワークと内部ネットワークとの間にバーチャルプライベートネットワーク（Virtual Private Network, VPN）を構築することにより、少なくとも一つのモバイルノード（Mobile Node, MN）が前記外部ネットワークでセキュリティにローミングできるようにする装置において、
下記の構成要素を含むことを特徴とする上記の装置。
（Ａ） 前記内部ネットワーク内に設けられ、前記モバイルノードの前記内部ネットワークにおけるローミングログインを管理する内部ホームエージェント（Internal Home Agent, i－HA）。
（Ｂ） 前記外部ネットワーク内に設けられ、前記モバイルノードの前記外部ネットワークにおけるローミングログインを管理する少なくとも一つの外部ホームエージェント（External Home Agent, x－HA）。
（Ｃ） 前記内部ネットワークと前記外部ホームエージェントとの間にインターネット通信セキュリティプロトコル（IPsec）チャンネルを構築することが可能であり、これにより、前記モバイルノードが前記外部ネットワークでローミングする際に、安全に前記内部ネットワークに接続することができるVPNゲートウェイ。
（Ｄ） 前記モバイルノードのローミングログインを行うために、前記モバイルノードに近い外部ホームエージェントをダイナミックに割り当てる少なくとも一つのエージェント割り当て装置。
（Ｅ） 前記外部ネットワークに設けられ、前記モバイルノードが前記外部ネットワーク

で初回のローミングを行う際に、接続用アドレスとして自動的にIPアドレスを割り当て、これにより前記外部ホームエージェント、前記AAAサーバ及び前記内部ホームエージェントに対してローミングログインを行い、前記VPNゲートウェイとの間にIPsecチャンネルを構築した後に、前記モバイルノードが外部ネットワークでローミングする際に、最も近い前記外部ホームエージェントにログインするだけで済むようにする少なくとも一つのDHCPサーバ。

【請求項１４】

前記外部ネットワークが複数のサブネットワークを含む、請求項１３に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項１５】

前記モバイルノードは、ワイヤレスネットワーク装置が設けられた携帯式パソコンである、請求項１３に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項１６】

前記VPNゲートウェイと前記エージェント割り当て装置がDMZ（DeMilitarized Zone）内に設けられ、前記DMZ（60）は、インターネットのバックにある実態領域であり、ファイアウォールに対してバックエンドシステムとデータを保護する第2層のファイアウォールの前に位置している、請求項13に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項１７】

前記VPNゲートウェイと前記エージェント割り当て装置がDMZ内に設けられ、前記DMZ（60）は、インターネットのバックにある実態領域であり、ファイアウォールに対してバックエンドシステムとデータを保護する第2層のファイアウォールの前に位置していることを特徴とする、請求項13に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項１８】

前記DMZは、内部ルータを介して前記内部ネットワークに接続され、かつ外部ルータを介して前記外部ネットワークに接続される請求項１７に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項１９】

前記エージェント割り当て装置は、AAAサーバ、DHCPサーバ又はDNSサーバを用いることができる、請求項13に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項２０】

前記エージェント割り当て装置は、前記AAAサーバを用いて前記外部ホームエージェントを割り当てるだけでなく、ローミング領域内の複数のエージェント（Agents）間にセキュリティアソシエーション（Security Association, SA）を構築すると共に、キー配布センター（Key Distribution Center, KDC）として用いることができる、請求項１９に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項２１】

前記エージェントは、ダイヤメータベースオンプロトコル（Diameter Base on Protocol）を用いたAAAサーバである、請求項20に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項２２】

前記内部ネットワークに接続された少なくとも一つのサブネットワークにおいて、前記モバイルノードが、前記サブネットワークでローミングする際に、前記内部フォーリンエージェントを介して前記内部ホームエージェントにローミングログインできるようにする少なくとも一つの内部フォーリンエージェント（Internal Foreign Agent, i－FA）を含む、請求項13に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【請求項２３】

前記内部ネットワーク又は前記外部ネットワークに設けられ、ワイヤレスで前記モバイル

ノードに接続するためのワイヤレス基地局（Wireless Access Point）を含む、請求項１３に記載の移動式VPNの外部エージェントをダイナミックに割り当てる装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、移動式VPN（Mobile Virtual Private Network）のダイナミックホームエージェント（Home Agent）の指定（Assignment）方法とシステムに関し、特に、インターネット通信セキュリティ協定（IPSec）のフレーム上のVPNにおいて、外部エージェントを動的に指定することによりモバイルノードのログインを提供する方法とシステムに関する。

【背景技術】

【０００２】

バーチャル専用ネットワーク（Virtual Private Network、以下VPNと略称する）は、広域ネットワーク（例えば、インターネット）を利用することにより、リモート使用者のコンピュータとホームネットワークのサーバとの間で専用のネットワーク通路を構築し、データの伝送を行い、クロースしている個人LANの内部にいるようなセキュリティを提供する。

【０００３】

VPNは安全性を確認するために、下記の基本要求を求める：

1．ユーザー検証：VPNは必ず使用者の身分を認証し、しかも予め権限が授けられた使用者のみがログインすることが可能であるという規律を厳格に守らねばならない。

2．アドレス管理：VPNは必ず使用者に専用のネットワーク上のアドレスを割り当て、しかもアドレスのセキュリティ性を確保しなければならない。

3．データの暗号化：インターネットにおける権限が授けられていない他の使用者がデータ情報を読み取ることができないことを確保するように、インターネットを介して伝送されるデータを暗号化しなければならない。

4．暗号化キーの管理：VPNは必ず使用者側のコンピュータとサーバとの暗号化したキーを生成且つ更新することができなければならない。

5．多種協定の支援：VPNは必ずインターネットにおけるIP、IPX、PPTP（点対点通路協定）、L2TP（第2層通路協定）あるいはIPSec（インターネット通信セキュリティ協定）などを含んだ一般な使用の基本協定を支援することができなければならない。

【０００４】

インターネット通信協定（IP）は、コンピュータネットワーク（例えば、インターネット）上で資料を伝送するための通信協定であるが、然しながら、IPはいかなるセキュリティ性メカニズムを定義していない。そのため、インターネットエンジニアリング任務推進グループ（Internet Engineering Task Force、以下IETFと略称する）は、「Request for Comments（RFC）」2401通信標準の中で、IPSec協定を定義した。これは、IP流量を暗号化する方法であり、ネットワーク通信を保護することにより、資料の変更、第三者の盗視、真似、盗み取り及び再アドバータイズメントを防止する標準である。

【０００５】

然しながら、無線ネットワーク技術の迅速な発展のため、無線伝送ネットワークが如何に移動式VPNを構築することは、すでに非常に重要な研究課題となっている。無線技術を応用した移動式（Mobile）VPNは、IETFでもMobile IPv4（IETF RFC3344）協定標準をも定義したが、前記Mobile IPv4標準には、まだ解決する必要のある問題がいくつか存在している。

【０００６】

例えば、一つのモバイルノード（Mobile Node、以下MNと略称する）（例えば、無線ネットワーク設備が装備された行動コンピュータ）は、一つイントラネット（Intranet）でローミングする時に、一つのホームエージェント（Home Agent、HA）により一つの移動IP（Mobile IP、以下MIPと略称する）を前記MNにMN指定する。前記MNが前記イントラネットから一つの外部ネットワーク（Internet）までローミングした時に、例えば、家あるいは

外地の支社にいる時に、前記MNは現地の一つの外地エージェント（Foreign Agent、FA）から、一つのIPSecをセキュリティベースとするVPNゲートウェイ（VPN Gateway）に進入して、前記ホームエージェント（HA）にログインすることにより、前記VPNゲートウェイに前記外地エージェント（FA）に対してIPSec通路を構築させる。

【０００７】

前記MNは、ローミングしている外部ネットワークの中から一つの新しい中継アドレス（Care of Address、以下CoAと略称する）を得ることができ、しかも前記VPNゲートウェイに前記MNが毎回新しいサブネットワークまでローミングした時に、IPSec通路を更新させることを要求する。しかしながら、前記VPNゲートウェイに進入した全てのデータパケット情報がすべてIPSecセキュリティ標準に暗号化されるが、前記外地エージェント（FA）はこれらの暗号化されたデータパケットを解読することができないため、前記外地エージェント（FA）がこれらのIP情報を伝送することができない。

【０００８】

上述した問題を解決するために、IETFのMobile IPv4のワーキンググループ（Working Group、WG）は、一部固定の機械（Mechanism）を利用してVPNユーザーの国際スキーマ無しローミング（International Seamless Roaming、ISR）を支援する方法を提案した。

【０００９】

前記方法は、前記イントラネットにおけるホームエージェント（HA）を一つのイントラネットホームエージェント（Internal Home Agent、以下、i－HAと略称する）として定義して、前記外部ネットワーク（External Network）の中に一つの外部ホームエージェント（External Home Agent、以下、x－HAと略称する）を構築し、前記i－HAは前記イントラネットが前記MNのローミング状況を管理（Mobility Management）するために使われるが、前記x－HAは、前記MNが前記外部ネットワークまでローミングした時に、前記MNのローミング状況を管理するために使われる。

【００１０】

余った前記x－HAは、既に構築されたIPSec tunnelをx－MIP tunnelの下に覆い、既に構築されたIPSec tunnelへ変更する必要がないため、前記MNが前記VPNゲートウェイにより一つの新しいCoAを獲得した後、前記VPNゲートウェイが構築したIPSec通路が破壊されることがない。そのため、前記外部エージェント（FA）は前記x－MIPの情報を解読することができるので、この方法を使う場合、Mobile IPv4標準とIPSec標準を改正する必要がなく、一部のモバイルノードが必要とする中継アドレス（CoA）を変更するだけでよい。

【００１１】

IETFに定義された移動式VPN標準フレームを示す図1に示したように、図1において、一つのi－HA11を通じて一つのイントラネット10の中でローミングしているMN1がある。前記MN1が前記イントラネット10から一つの外部ネットワーク20に移動した時に、前記MN1は必ず一つのx－HA21にログインして、新しいCoAを獲得する。前記x－HA21は、更に一つのVPNゲートウェイ22に、前記x－HA21に接続するIPSec通路を構築することを要求する。最後に、前記VPNゲートウェイ22は、再び前記i－HA11に前記MN1のVPN－TIA（VPN Tunnel Inner Address）をログインすることにより、構築された前記IPSec通路を前記i－HA11に接続して、外部ネットワーク20及びイントラネット10からすべてローミングすることができるバーチャル専用ネットワーク（VPN）を形成する。

【００１２】

図2　は、前記移動式VPNが構築した通路の情報の構造を示す図であり、前記MN1がイントラネット10から外部ネットワーク20までローミングした通路信号データパケット30であり、中に、一層の原始データパケット（Original Packet）31が含まれており、前記原始データパケット31の前に一層の内部移動IP（i－MIP）の通路情報32（前記i－HA11から前記VPNゲートウェイ22まで）が覆われており、また、前記内部移動IP通路情報32の外に更に一層のIPSec通路情報33（前記VPNゲートウェイ22から前記x－HA21まで）が覆われており、前記IPSec通路情報33の外に更に一層の外部移動IP（x－MIP）の通路情報34（前記x－HA21から前記MN1の中継アドレスまで）が覆われている。

【００１３】
しかしながら、よく知られているIETFの方法において、2つの問題が発生し得る。第1は、前記x‐HA21が何処にあるのが最も適切であるか？第2は、前記x‐HAは安全であると信じることが出来るのか？
【００１４】
このよく知られているIETFの方法では、前記外部ネットワーク20の中に一つ固定（Static）のx‐HA21を構築するため、もし前記外部ネットワーク20の中に複数のサブネットワーク（Subnet）が含まれている場合に、前記x‐HA21の地点の選定は、ローミングするサブネットワークの間における前記外部エージェント（FA）と前記x‐HA21との間の中継伝送（Handoff）の時間遅れ、及びローミングするサブネットワークの間における端末から端末まで（End‐to‐End）の時間遅れに影響を与える。尚且つ、前記x‐HA21は、VPNゲートウェイ22に制御されない外部ネットワーク20の中にあるため、前記x‐HA21は本当にIPSecのセキュリティ標準に合っていると信じることができるのか？
【００１５】
即ち、本願の発明者は、上記した従来の移動式VPNの要求及び問題点を解決するために、研究に特に専念して学んだ知識を応用して、移動式VPNのダイナミックエージェント（x‐HA）の指定方法及びシステムを提案した。前記方法及びシステムにより、前記MNに接近するホームエージェント（HA）を前記x－HAとして動的に指定することができるため、ローミングするネットワークの間の中継伝送（Handoff）の遅れ及び端末から端末まで（End‐to‐End）の遅れを最少に減少させ、しかもVPNのIPSecセキュリティ制御を完全に結合することが可能であり、合理的であり、且つ上記した欠点を有効に改善することができる発明である。
【発明の開示】
【発明が解決しようとする課題】
【００１６】
本発明の目的は、外部ネットワークでローミングする間で、前記モバイルノードに近い外部ホームエージェントを前記モバイルノードのログインエージェントとして指定することにより、前記モバイルノードが同じ外部ネットワークの中でローミングする時に、（前記外部ホームエージェントにログインするだけでよい、前記イントラネットの内部ホームエージェントにログインする必要がない‐IETFの方法でもよい）、このようにローミングする時のエージェント間の中継伝送（Handoff）の遅れ及び端末から端末まで（End‐to‐End）の遅れを最少に減少させ、しかもVPNのIPSecセキュリティ制御を完全に結合することができる移動式VPNのダイナミックエージェントの指定方法及びシステムを提供することである。
【００１７】
上述の目的を達成するため、本発明は主に、少なくとも一つの外部ネットワークと一つのイントラネットとの間でVPNを構築することができる移動式VPNのダイナミックエージェントの指定方法を提供する。前記方法はまず、一つのモバイルノードが前記外部ネットワークの中でローミングする時に、一つのDHCPサーバにより一つのIPアドレスが割り当てられ、前記モバイルノードの中継アドレスとして前記外部ホームエージェントにログインの請求を発信する。前記外部ホームエージェントは、一つの外地AAAサーバに授権確認リクエスト情報を発信することにより、前記外地AAAサーバが少なくとも一つの外部ホームエージェントのネットワークアクセス標示を前記授権確認リクエスト情報の中に記入してから一つのホームAAAサーバに転送する。続いて、前記ホームAAAサーバがMNの認証に成功した後、前記外部ホームエージェントと前記モバイルノードとの間のセキュリティアソシエーションを設立し、さらに一つのホームエージェントリクエスト情報を生成し、前記外部ホームエージェントに発信する。前記外部ホームエージェントは前記モバイルノードのために一つの外部ホームアドレスを指定し、前記外地ホームアドレス及び自身のアドレスを一つのホームエージェント回答情報の中に設定して、前記ホームAAAサーバに発信する。それから、前記ホームAAAサーバは、前記外部ホームアドレスを前記モバイルノードの中

継アドレスとして使い、前記内部ホームエージェントにログインする。ログインが終了された後、前記内部ホームエージェントは前記ホームAAAサーバに権限を授け、授権確認回答情報が前記外部ホームエージェントに発信される。最後に、前記外部ホームエージェントは、前記授権確認回答情報の中から前記外部ホームアドレス及び前記ホームエージェントアドレスを含んだ登録返信情報を獲得して、前記モバイルノードに転送する。その後、前記モバイルノードは前記外部ネットワークでローミングする時に、前記外部ホームアドレスを利用して、前記ホームエージェントアドレスのホームエージェントにログインすればよい。

【００１８】

本発明は更に、少なくとも一つの外部ネットワークと一つのイントラネットとの間にVPNを構築することにより、少なくとも一つのモバイルノードが前記外部ネットワークの中で安全にローミングすることができるようにする移動式VPNのダイナミック外部エージェントを指定するシステムを提供する。前記システムは、一つのイントラネットホームエージェント、少なくとも一つの外部ホームエージェント、一つのVPNゲートウェイ、少なくとも一つのエージェント指定器及び少なくとも一つのDHCPサーバを備えている。その中に、前記イントラネットホームエージェント（ｉ－HA）は、前記モバイルノードが前記イントラネットの中でローミングするログインを管理するためのものであり、前記外部ホームエージェント（ｘ－HA）は、前記モバイルノードが前記外部ネットワークの中でローミングするログインを管理するものであり、前記VPNゲートウェイは、前記イントラネットと前記外部ホームエージェントの間で、一つのインターネット通信セキュリティ協定（IPSec）通路を構築することが可能であり、前記エージェント指定器は、前記モバイルノードに近い任意の外部ホームエージェントを動的に指定して、前記外部ホームエージェントに前記モバイルノードのローミングログインを行わせる。また、前記DHCPサーバは、前記モバイルノードが第1回目で前記外部ネットワークでローミングする時に、前記外部ホームエージェントに一つのIPアドレスを自動的に割り当て、前記AAAサーバ及び前記内部ホームエージェントがローミングログインを行うことにより、前記VPNゲートウェイとの間のIPSec通路を構築した後、前記モバイルノードが外部ネットワーク内でローミングする場合、前記モバイルノードが最も近い前記外部ホームエージェントにログインするだけで済むようにするためのものである。

【課題を解決するための手段】

【００１９】

本発明が予定の目的を達成するために採用した技術、手段及び作用を理解するために、本発明に関する以下の詳細説明と図面を参照されたい。本発明の目的、特徴と利点がこれよってより一層深く且つ具体的に理解されることを信じる。しかしながら、図面は参照の提供及び説明のために使われるものであり、本発明を制限するものではない。

【００２０】

図3に示す本発明に係る移動式VPNのシステムの構成図を参照されたい。本発明は主に、外部ネットワークの中でモバイルノード（MN）80に最も近いホームエージェント（HA）を一つの外部ホームエージェント（ｘ－HA）54として能動的に指定することにより、前記MN80を前記x－HA54へログインさせて、移動式バーチャル専用ネットワーク（Mobile VPN）のIPSec通路の構築を完成させる。

【００２１】

本発明は、外部ネットワーク領域内に使用されるDHCPサーバ、AAA（Authentication、Authorization and Accounting）サーバ或いはDNSサーバなどを利用して、前記ｘ－HAを動的に指定することにより、外部ネットワークの中で前記MN80に最も近いホームエージェント（HA）を選択して前記ｘ－HA54として指定することができる。また、前記ｘ－HA54は前記MN80に最も近いので、前記ｘ－HA54と前記MN80との間の遅れが最低限に減らされる。前記外部ネットワークにおけるサブネットワーク（inter－Subnet）間の端末から端末までの中継伝送（Handoff）も更に速くなり、しかも外部ネットワークにある別のホームエージェント（HA）を負荷のバランス調整に使うこともできる。

【００２２】
然しながら、最も重要なことはやはり、前記x－HA54のセキュリティメカニズムの問題である。そのため、AAAサーバを使って前記x－HA54を指定した方がよい。例えば、私達はDiameter基礎協定（Diameter Base on Protocol）（IETF RFC3588）を前記AAAサーバとして採用し、前記x‐HAを指定することができるだけではなく、ローミングする時に移動と変化の複数のエージェント（Agents）の間で、セキュリティアソシエーション（Security Association、以下SAと略称する）を構築し、キーの配分センター（Key Distribution Center、KDC）とすることもできる。
【００２３】
図3において、一つのイントラネット（Intranet）40及び少なくとも一つの外部ネットワーク（Internet）50が示されている。前記イントラネット40は、保護を受ける個人ネットワーク（Protected Private Network）であり、一つのDHCPサーバ41及び一つの内部ルータ（Interior Router）42と接続されている。前記内部ルータ42は、一つのDMZ60と接続されている。前記DMZ60は、インターネットの後方の実体領域であり、ファイアウォールに直面して、保護末端システムと資料の第2のファイアウォールの前に位置する。また、前記DMZ60には、一つの（以下、AAAHと略称する）61と、一つのVPNゲートウェイ62及び一つの外部ルータ（Exterior Router）51と接続されており、前記外部ルータ51は前記外部ネットワーク50（Internet）へ接続されている。
【００２４】
前記イントラネット40の中に、複数のサブネットワーク（Subnet）43が含まれている可能性がある。すべてのサブネットワーク43は、少なくとも一つの無線基地（Wireless Access Point、WAP）44へ接続されて、少なくとも一つの前記MN80を無線連結するために使われる。前記イントラネット40の中に、更に一つのi‐HA45及び一つの内部外地エージェント（Internal Foreign Agent、 以下、i‐FAと略称する）46が設置されている。図3に示したように、前記i‐HA45が第1のサブネットワーク（Subnet 1）の上に接続されており、前記i‐FA46が第2のサブネットワーク（Subnet 2）の上に接続されており、前記DHCPサーバ41が第3のサブネットワーク（Subnet 3）の上に接続されている。
【００２５】
前記MN80がイントラネット40でローミングするログインフローチャート及びタイミングチャートを示す図4と図5を併せて参照されたい。前記DHCPサーバ41の機能は主に、ネットワークにおけるすべてのコンピュータのIPアドレスを動的に割り当てるためのものであるので、前記DHCPサーバ41は一つのアドバータイズメント&探索情報100を絶えずに発信し、ネットワークの上に新しいコンピュータの接続コード（S200）があるか否かをサーチする。
【００２６】
そのため、前記MN80が前記イントラネット40の他のサブネットワークまでローミングした時に、例えば、第2のサブネットワーク（Subnet 2）から第3のサブネットワーク（Subnet 3）までローミングした時に、前記DHCPサーバ41は前記MN80を発見し、前記MN80がIPアドレスのリクエスト情報105をDHCPサーバ41に発信し、その時に前記DHCPサーバ41は一つの新しいダイナミックIPアドレス110を前記MN80に割り当てる（S205）。
【００２７】
前記MN80は、新しいIPアドレスを一つの中継アドレス （CoA）として、前記内部ホームエージェント（i‐HA）45に一つのログインリクエスト（Registration Request, 以下Reg‐Reqと略称する）情報115を発信する（S210）。前記i‐HA45は元々前記MN80を認識しているため、ログインを行うことになり、しかも前記MN80に一つのログイン応答（Registration Reply、以下、Ｒｅｇ‐Replyと略称する）情報120を応答し（S215）て、イントラネットのローミングログインプロセスを完成させる。
【００２８】
再び図3を参照されたい。前記外部ネットワーク（Internet）50は保護を受けていない公衆ネットワーク（Unprotected Public Network）であり、その中に複数の外部ネットワ

ークが含まれている可能性がある。図3に示したように、第1の外部ネットワークと第2の外部ネットワークが存在し、各外部ネットワークの中に更に複数のサブネットワークが含まれる可能性がある。しかも、それぞれが一つの外地AAAサーバ（Foreign AAA Server、以下AAAFとの略称する）53、一つのx‐HA54、一つの外部外地ホームエージェント（External Foreign Agent、以下、x‐FAと略称する）55、一つのDHCPサーバ56及び少なくとも一つの無線基地（WAP）57と接続されている。

【００２９】

図6、図7及び図8を併せて参照されたい。これらは、前記MN80が外部ネットワークでローミングするときの、ログインフローチャートとタイミングチャートを示している。前記MN80がイントラネット40から前記外部ネットワーク50までローミングした時に、同様に、現地の前記DHCPサーバ56は自動的に一つのダイナミックIPアドレスを前記MN80に割り当てる（S400）。前記MN80は前記IPアドレスを一つの中継アドレス（CoA）300として利用し、前記x‐HA54に一つのReg‐Req情報305を発信する（S405）。

【００３０】

前記Reg‐Req情報305の中に、一つのホームアドレス（Home Address、以下HoAと略称する）、一つのHAアドレス、一つ前記AAAH61に権限が授けられる認証コンサルタント及び一つのMNのネットワークアクセス標示（Network Access Identifier、 NAI）などが含まれるべきである。

【００３１】

然も、前記x‐HA54が受け取った前記Reg‐Req情報305の中に、前記HoAと前記HAアドレスとがすべて0．0．0．0と設定されるべきであり、前記MN80が前記外部ネットワークの中から一つの外部ホームアドレス（External Home Address、以下x‐HoAと略称する）を獲得したいことを表す。そのため、前記x‐HA54は一つの特徴ベクトル（MIP‐Feature‐Vector）の属性値対（Attribute Value Pair、以下、AVPと略称する）を生成する。その中に、MN80のホームアドレスリクエスト（Home‐Address‐Requested）、及びホームエージェントリクエスト（以下、Home‐Agent‐Requestedと称する）と一つの共同アドレスリクエスト（以下、Co‐Located‐Mobile‐Node‐Requested）が設定されており、フラグ（Flag）は「1」である。

【００３２】

この時、前記x‐HA45は、前記MIP‐Feature‐Vector AVPを一つの授権リクエスト（AA‐Mobile‐Node‐Request、以下AMRと略称する）情報310の中に設定し、Reg‐Req情報の中から必要なデータを獲得し、関連のAVPに加え、前記AMR情報310を現地の前記AAAF53に発信する（S410）。

【００３３】

前記AAAF53は、まず前記MIP‐Feature‐Vector AVPの中のHome‐Agent‐Requestedのフラグビット（Flag bit）が「1」であるか否かをチェックする。

【００３４】

「1」である場合、前記AAAF53は、ローミングしている外部ネットワーク中の一つのx‐HA54を前記MN80のホームエージェント（HA）として指定することを許可するように、前記AAAH61に要求する。そのため、前記AAAF53は受け取ったAMR情報310中の前記MIP‐Feature‐Vector AVPの中に一つの外地のホームエージェント適用（以下、Foreign‐Home‐Agent‐Availableと称する）フラグを設定し、しかも、一つの候補のホームエージェントホストコンピュータ（以下、MIP‐Candidate‐Home‐Agent‐Hostと称する）AVPの中に少なくとも一つの候補のx‐HA54のネットワークアクセス標示（NAI）を記入し、その後前記AAAF53は、更に前記AMR情報310を前記AAAH61へ伝送する（S415）。

【００３５】

前記AAAH61が前記AAAF53から伝送されたAMR情報310を受け取った後、前記MN80にReg‐Req情報305を与えなければならない。そのため、前記AAAH61は前記AMR情報310の中に設定された一つのセキュリティパラメータインディクス（MN‐AAA‐SPI、Security Paremeters Index）を通じて、前記MN80は何らかのセキュリティ対策、（例えば、暗号化演算方と

長期シェアキー）を特定する。

【００３６】

もし前記AAAH61は授権に成功すれば、前記AMR情報310のMIP‐Feature‐Vector AVP中の前記Home‐Agent‐Requestedのフラグビット及び前記Foreign‐Home‐Agent‐Availableのフラグビットはすべて「1」であるか否かをチェックする。「1」であれば、MNが一つのx－HA54をローミングしている外部ネットワークの領域に指定することを要求していることを意味する。前記AAAH61は、ローミングしている外部ネットワークの領域の中に前記x－HA54とMNとの間のセキュリティアソシエーション（SA）を構築する（S420）。

【００３７】

そのため、前記AAAH61は、少なくとも128ビットの乱数キー（一般的にはNoncesと称されるKey Materials）を生成し、前記Noncesを利用して一つの通信キー（Session Key）を計算し生成することができる。これにより、セキュリティアソシエーション（SA）のセキュリティ性を確保することができる。

【００３８】

前記x‐HA54及び前記AAAF53が発信した前記AMR情報310の中のMIP‐Feature‐Vector AVPは、MN80とホームエージェント（HA）との間のキーリクエスト（Key‐Requested）も含んでいる。前記通信キー（Session Key）は、Diameter協定（Diameter Protocol）のAAAサーバを通じて、セキュリティにx－HA54に伝送される。

【００３９】

これは、IPSec標準或いは通信層セキュリティ（Transport Layer Security、TLS）標準（IETF RFC 2246）は、保護Diameterノード（サーバ、客先とエージェントを含む）の間の通信データに強制的に応用されているからである。しかしながら、前記通信キー（Session Key）をネットワーク保護協定のない中に暴露してしまうことを避けるために、前記通信キー（Session Key）が直接MN80上伝送されなく、前記MN80にのみ前記キー（Nonces）を与える。

【００４０】

そのため、前記AAAH61は、再び一つのホームエージェントリクエスト（Home‐Agent‐MIP‐Request、 以下HARと略称する）情報315を生成し、通信キー（Session Key）及びReg‐Req情報をHAR情報315中の前記関連のAVPの中に装入し、前記AAAF53を通じて前記候補のx－HA54に伝送する（S425）。前記AAAF53は主に、代理サーバ（Proxy）の役割を果たすものである。そのため、前記x－HA54は、前記HAR情報315中の関連のAVPの中から前記x－HA54とMN80のキー（Nonces）を獲得することができる。

【００４１】

前記x‐HA54は、受け取ったHAR情報315の中に前記MN80のアドレス（以下、MIP‐Mobile‐Node‐Addressと称する）AVPが含まれていない場合で、しかも前記MIP‐Feature‐Vector AVP中のHome‐Agent‐Address‐Requestedのフラグビットが「1」に設定されている場合、前記x‐HA54は自動的に前記MN80のために一つのx‐HoAを指定し、前記MIP‐Mobile‐Node‐Address AVPの中に設定し、しかも前記x‐HA54が自動的に自身のアドレスを前記MIP‐Home‐Agent‐Address AVPの中に設定する。

【００４２】

引き続いて、前記x－HA54は前記MN80と前記x‐HA54との間の前記通信キー（Session Key）を保存し、前記キー（Nonces）を一つの登録応答（Reg‐Reply）にコピーし、その後前記x－HA54は一つのホームエージェント回答（Home‐Agent‐MIP‐Answer、以下HAAと略称する）情報320を生成し、前記AAAF53を通じて、更に前記AAAH61へ伝送する（S430）。前記HAA情報320は、少なくとも一つの前記キー（Nonces）が含まれているログイン応答（以下、MIP‐Reg‐Reply）AVP、一つの結果コード（Result‐Code）AVP、一つの前記MN80x‐HoAが含まれているMIP‐Mobile‐Node‐address AVP、及び一つの前記x‐HA54アドレスが含まれているMIP‐Home‐Agent‐Address AVPを含んでいる。

【００４３】

前記AAAH61は、前記x‐HA54が前記AAAF53を通じて伝送されて来た前記HAA情報320を受

け取った後、前記AAAH61が前記MIP‐Mobile‐Node‐address AVPの中から前記MN80のx‐HoAを獲得し、MIP‐Home‐Agent‐Address AVPの中から前記x‐HA54のアドレスを獲得することになる。

【００４４】

それから、前記AAAH61は、新しいHAR情報325を作成し、さらに前記x‐HoA及びx－HAのアドレスをそれぞれMIP‐Mobile‐Node‐Address及びMIP‐Home‐Agent‐Address AVPの中に記入し、そして、前記AAAH61が前記HAR情報325を発信して、前記i－HA45にログインする（S435）。

【００４５】

前記i－HA45が前記HAR情報325を受け取った後、前記i－HA45は前記HAR情報325中のAVPから前記x－HoAを獲得した後、獲得したx－HoA54のアドレスを前記MN80の公共のCoAとしてログインすることにより、前記i－HA45が前記HAR情報325を認識してから一つの新しいHAA情報330を作成して前記AAAH61に伝送する（S440）。

【００４６】

それから、前記AAAH61は、前記i‐HA45が発信した前記HAA情報330を受け取った後、その中の前記結果コード（Result‐Code）AVPにより授権に成功したことを表示することができる。そのため、前記AAAH61は、一つの授権回答（AA‐Mobile‐Node‐Answer、以下AMAと略称する）情報335を生成し、前記AAAF53を通じて前記x‐HA54へ伝送する（S445）。前記AMA情報335の中に、DIAMETER成功の結果コード（Result‐Code）、前記MIP‐Home‐Agent‐Address AVP、前記MIP‐Mobile‐Node‐address AVP及び前記MIP‐Reg‐Reply AVPが含まれており、これらのAVPが受け取った前記HAA情報330の中から複製される。

【００４７】

前記x－HA54が前記AAAH61から伝送されてきた前記AMA情報335を受け取った後、前記結果コード（Result‐Code）AVPにより授権に成功したことを表示することができるので、前記x－HA54は前記AMA情報335のMIP‐Reg‐Reply AVPの中から一つのReg‐Reply情報340を獲得し、前記Reg‐Reply情報340を前記MN80に伝送する（S450）。そうしなければ、前記x‐HA54がAMA情報335をそっと捨てることになる。

【００４８】

一旦前記MN80が前記Reg‐Reply情報340を受け取ったら、前記MN80は前記新しいx‐HoA、前記x‐HAのアドレス及び前記キー（Nonces）を獲得することができる。それから、前記MN80は受け取ったキー（Nonces）及び前記AAAH61と同様な離散計算方法及び長期シェアキー（Longterm Shared Key）により、正確な通信キー（Session Key）を算出する。

【００４９】

そのため、前記MN80が前記AAAH61により権利が授けられた後、更に前記x‐HA54及びx‐HA45によりMobile IPv4セキュリティ標準でログインした後、前記x‐HoAを前記VPNゲートウェイと連結することにより、前記MN80と前記VPNゲートウェイとの間でIPSec通路345を構築して（S455）、イントラネットにあると同様なセキュリティ通信を回復させる。

【００５０】

前記x－HA54の指定が完成された後、ローミングしている外部ネットワークの中の各現地のホームエージェント（HA）の間のセキュリティアソシエーション（SA）の構築も完成されることになる。その時に、前記MN80は前記AAAサーバを通す必要がなく、直接MIPｖ4標準を使って前記現地のx‐HA54にログイン通信を行うことができる。即ち、前記MN80は前記外部ネットワークから一つの新しい中継アドレス（CoA）を獲得した後、イントラネット内部にローミングしているように、指定されたx‐HA54にログインするだけでよい、前記ｉ‐HA45にログインする必要がなくなる。

【００５１】

さらに、同じ前記外部ネットワークにおいて、IPSec通路を再建する必要がなくなる。但し、前記通信キー（Session Key）は寿命のあるものであり、寿命が終了したら、前記Diameterをベースとした AAAサーバを通じて新しい通信キー（Session Key）を生成することになる。また、もし前記MN80が他の外部ネットワークへ移動した場合、また現地の一つ

の新しいx－HAにログインをリクエストしなければならないときに、上記した全てのプロセスが再び行われることにより、前記x‐HAが再び指定され、IPSec通路も再建されることになる。

【産業上の利用可能性】

【００５２】

即ち、本発明は、上記開示した技術に基づいて、ダイナミック指定のx‐HAでスタティックx‐HAを取替える技術を提供するため、ローミングする時のホームエージェント（HA）の間の伝送中継（Handoff）の遅れ及び端末から端末まで（End to End）の遅れが著しく減少されることになり、さらに、本発明はDiameter MIPｖ4を中継のホームエージェント（HA）の間で構築されたセキュリティアソシエーション（SA）に応用するため、前記x‐HAは信頼できるものである。しかも、前記x‐HA及びｉ－HAに対するログイン動作が同時に完成されるため、本発明は移動式VPNのシステムプラットフォームを実現した。本発明は、当業者の設計とまったく異なり、全体の使用価値を向上させることができる。また、本発明は、リクエストする前に出版物での公開及び公開使用が見つからなかったので、発明特許の要求を満たしており、法律に従って発明特許リクエストを提出する。

【００５３】

なお、上記開示した図面、説明は、本発明の実施の形態とするものであり、この技術に精通する当業者がすべて上記した説明に基づいて様々な改良を行うことが可能である。しかしながら、このような改良は本発明の発明精神及びそれに定められた特許の範囲内に属するべきである。

【図面の簡単な説明】

【００５４】

【図１】IETF定義の移動式VPNの標準フレームを示す図である。

【図２】上記移動式VPNが構築した通路の情報構造を示す図である。

【図３】本発明に係る移動式VPNのシステムフレームを示す図である。

【図４】図3に示したシステムにおいて、MNがイントラネットでローミングするログインフローチャートである。

【図５】上記MNがイントラネットでローミングするログインフローチャートである。

【図６】上記MNが外部ネットワークでローミングするログインフローチャートである。

【図７】上記MNが外部ネットワークでローミングする時のタイミングチャートの前半部分である。

【図８】上記MNが外部ネットワークでローミングする時のタイミングチャートの後半部分である。

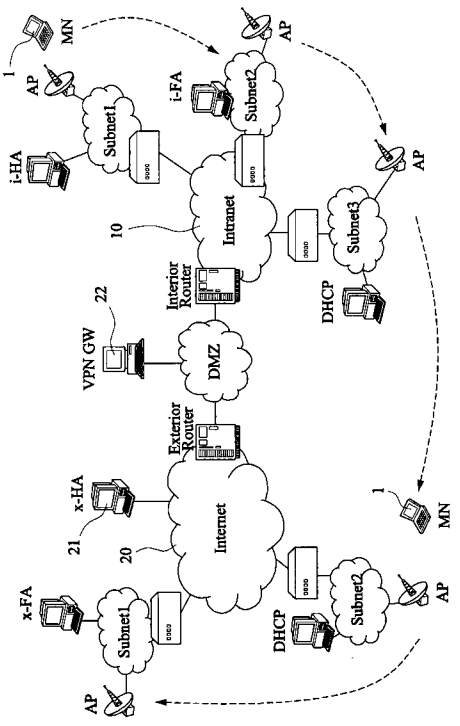
【符号の説明】

【００５５】

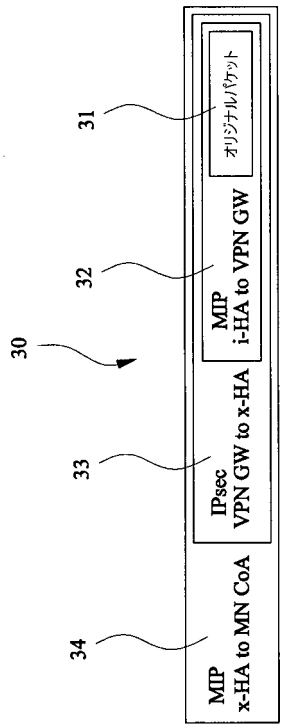
40　イントラネット
41　DHCPサーバ
42　内部ルータ
43　サブネットワーク
44　無線基地
45　内部ホームエージェント
46　内部外地エージェント
50　外部ネットワーク
51　外部ルータ
53　外地AAAサーバ
54　外部ホームエージェント
55　外部外地エージェント
56　DHCPサーバ
57　無線基地
60　DMZ

61 ホームAAAサーバ
62 VPNゲートウェイ
80 モバイルノード

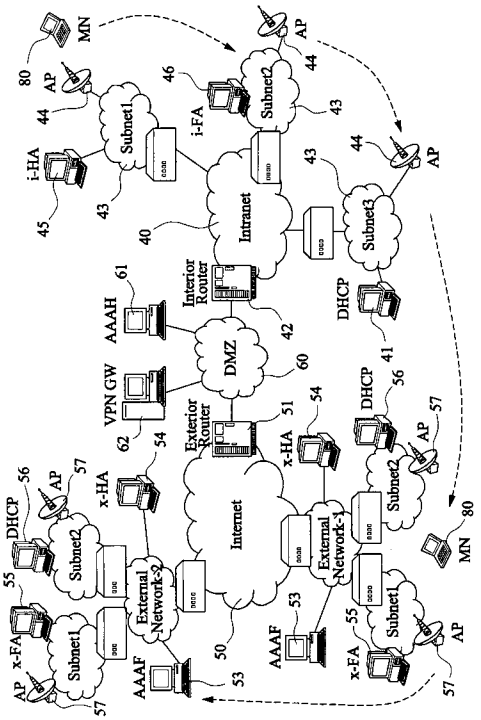
【図１】



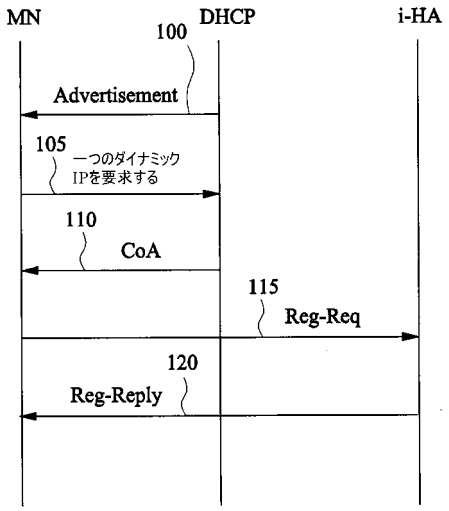
【図２】



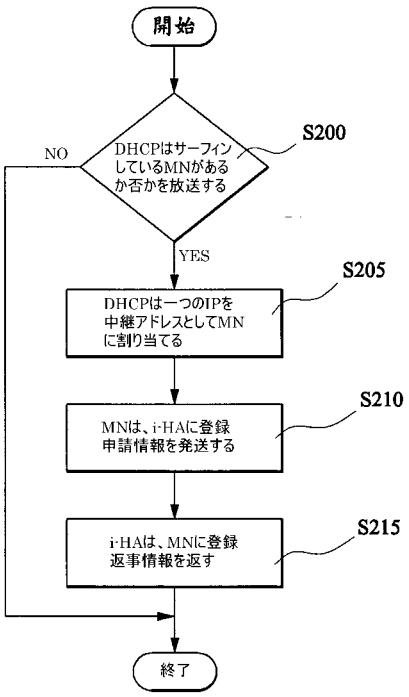
【図３】


MN
AP
i-HA
Subnet1
i-FA
Subnet2
Intranet
Subnet3
Interior Router
AAAH
DMZ
DHCP
VPN GW
Exterior Router
x-HA
Internet
External Network-1
External Network-2
x-FA
AAAF

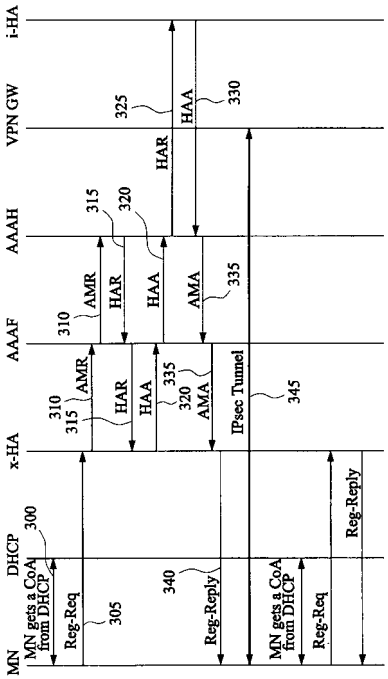
【図４】


MN
DHCP
i-HA
100
Advertisement
105
一つのダイナミック IPを要求する
110
CoA
115
Reg-Req
120
Reg-Reply

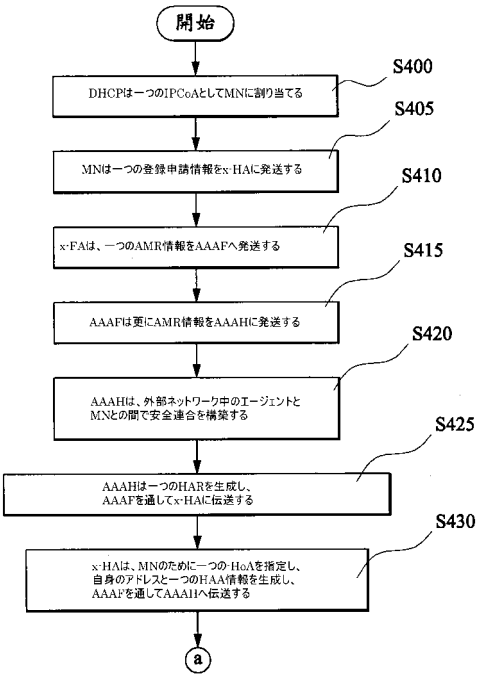
【図５】


開始
DHCPはサーフィンしているMNがあるか否かを放送する
S200
NO
YES
DHCPは一つのIPを中継アドレスとしてMNに割り当てる
S205
MNは、i-HAに登録申請情報を発送する
S210
i-HAは、MNに登録返事情報を返す
S215
終了

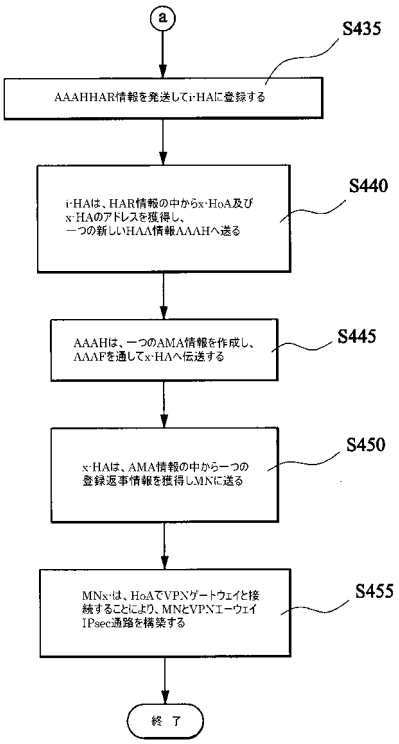
【図６】


i-HA
VPN GW
AAAH
AAAF
x-HA
DHCP
MN
HAA
HAR
AMR
AMA
IPsec Tunnel
Reg-Reply
Reg-Req
MN gets a CoA from DHCP

【図７】


開始
DHCPはーつのIPCoAとしてMNに割り当てる
S400
MNはーつの登録申請情報をx-HAに発送する
S405
x-FAは、一つのAMR情報をAAAFへ発送する
S410
AAAFは更にAMR情報をAAAHに発送する
S415
AAAHは、外部ネットワーク中のエージェントと
MNとの間で安全連合を構築する
S420
AAAHは一つのHARを生成し、
AAAFを通してx-HAに伝送する
S425
x-HAは、MNのために一つのHoAを指定し、
自身のアドレスと一つのHAA情報を生成し、
AAAFを通してAAAHへ伝送する
S430
a

【図８】


a
AAAHHAR情報を発送してr-HAに登録する
S435
r-HAは、HAR情報の中からx-HoA及び
x-HAのアドレスを獲得し、
一つの新しいHAA情報AAAHへ送る
S440
AAAHは、一つのAMA情報を作成し、
AAAFを通してx-HAへ伝送する
S445
x-HAは、AMA情報の中から一つの
登録返事情報を獲得しMNに送る
S450
MNx-は、HoAでVPNゲートウェイと接
続することにより、MNとVPNエーウェイ
IPsec通路を構築する
S455
終了

フロントページの続き

審査官　矢頭　尚之

(56)参考文献　特開２００２－０４４１４１（ＪＰ，Ａ）
特開２００４－２６６３１０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　４０／３４
Ｈ０４Ｌ　１２／５６