(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3811064号
(P3811064)
(45)発行日　平成18年8月16日(2006.8.16)　(24)登録日　平成18年6月2日(2006.6.2)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330C
H04Q 7/38 (2006.01)　　H04B 7/26 109S

請求項の数 17　(全 9 頁)

(21)出願番号　特願2001-508140(P2001-508140)
(86)(22)出願日　平成11年7月2日(1999.7.2)
(65)公表番号　特表2003-503803(P2003-503803A)
(43)公表日　平成15年1月28日(2003.1.28)
(86)国際出願番号　PCT/EP1999/004625
(87)国際公開番号　WO2001/003402
(87)国際公開日　平成13年1月11日(2001.1.11)
審査請求日　平成14年3月18日(2002.3.18)

前置審査

(73)特許権者　398012616
ノキア　コーポレイション
フィンランド　エフイーエンー０２１５０
エスプー　ケイララーデンティエ　４
(74)代理人　100059959
弁理士　中村　稔
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100065189
弁理士　宍戸　嘉一
(74)代理人　100074228
弁理士　今城　俊夫

最終頁に続く

(54)【発明の名称】認証方法及びシステム

(57)【特許請求の範囲】

【請求項１】

ＧＰＲＳネットワークである第１ネットワーク（２）の加入者を、ＶＡＳプラットホームに対する認証サーバー機能が設けられたインターネットプロトコル（ＩＰ）ネットワークである第２ネットワークにおいて識別するための認証方法であって、

ａ）ゲートウェイ装置（５）において上記第２ネットワーク（９）のＩＰアドレスを上記加入者に割り当て、

ｂ）上記ゲートウェイ装置（５）において上記第２ネットワーク（９）における加入者のＩＰアドレスと加入者の認識との間のマッピングに関する情報を発生し、そして

ｃ）上記ゲートウェイ装置（５）によって上記マッピングを上記第２ネットワークに送信する、

という段階を含み、上記加入者は、ＶＡＳプラットホームにおいて上記マッピング情報に基づいて識別されることを特徴とする認証方法。

【請求項２】

上記マッピング情報は、上記第２ネットワークにおける上記アドレスと加入者の認識との間の上記マッピングが変化したときに、上記ゲートウェイ装置（５）によって上記第２ネットワークに送信される請求項１に記載の認証方法。

【請求項３】

上記加入者の認識は、加入者のＩＭＳＩ及び／又はＭＳＩＳＤＮである請求項１又は２に記載の認証方法。

【請求項４】
上記マッピング情報は、アクセス要求メッセージにおいて上記ゲートウェイ装置（５）によって送信される請求項１ないし３のいずれかに記載の認証方法。
【請求項５】
上記アクセス要求メッセージは、ＲＡＤＩＵＳアクセス要求メッセージである請求項４に記載の認証方法。
【請求項６】
上記認証サーバー機能は、ＶＡＳプラットホームに含まれる請求項１に記載の認証方法。
【請求項７】
上記認証サーバー機能は、専用の認証サーバーによって与えられる請求項１に記載の認証方法。
【請求項８】
上記マッピング情報は、ＧＧＳＮにおいて認証クライアント機能により発生される請求項１ないし７のいずれかに記載の認証方法。
【請求項９】
上記マッピング情報は、移動ターミナルのサービス特有の課金及び／又はアドレッシングに対して使用される請求項１ないし８のいずれかに記載の認証方法。
【請求項１０】
ＧＰＲＳネットワークである第１ネットワーク（２）の加入者（１）をインターネットプロトコル（ＩＰ）ネットワークである第２ネットワーク（９）において識別するための認証システムであって、
ａ）ゲートウェイ装置（５）を備え、このゲートウェイ装置は、上記第２ネットワーク（９）のＩＰアドレスを上記加入者（１）に割り当てるための割り当て手段（５１）と、上記第２ネットワーク（９）の上記ＩＰアドレスと加入者認識との間のマッピングに関する情報を発生しそしてそのマッピング情報を上記第２ネットワーク（９）に送信するための認証クライアント手段（５２）とを含み、そして
ｂ）上記第２ネットワーク（９）に設けられそして上記マッピング情報をロギング及び維持するように構成された認証サーバー（８）を更に備え、
ｃ）上記認証サーバー（８）は、上記第２ネットワーク（９）に設けられたＶＡＳプラットホーム（７）のサーバーであり、このＶＡＳプラットホーム（７）は、上記マッピング情報に基づいて上記加入者（１）を識別するよう構成されたことを特徴とする認証システム。
【請求項１１】
上記ゲートウェイ装置は、ＧＧＳＮ（５）である請求項１０に記載の認証システム。
【請求項１２】
上記認証クライアント手段（５２）は、ＲＡＤＩＵＳクライアントである請求項１０又は１１に記載の認証システム。
【請求項１３】
上記認証サーバー（８）は、ＲＡＤＩＵＳサーバーである請求項１０ないし１２のいずれかに記載の認証システム。
【請求項１４】
上記加入者認識は、ＩＭＳＩ又はＭＳＩＳＤＮである請求項１０ないし１３のいずれかに記載の認証システム。
【請求項１５】
上記認証クライアント手段（５２）は、上記マッピング情報をアクセス要求メッセージにおいて上記認証サーバー（８）へ送信するように構成される請求項１０ないし１４のいずれかに記載の認証システム。
【請求項１６】
ＧＰＲＳネットワークである第１ネットワーク（２）をインターネットプロトコル（Ｉ

Ｐ）ネットワークである第２ネットワーク（９）に接続するためのゲートウェイ装置において、
ａ）上記第２ネットワーク（９）のＩＰアドレスを上記第１ネットワーク（２）の加入者（１）に割り当てるための割り当て手段（５１）と、
ｂ）上記第２ネットワーク（９）の上記ＩＰアドレスと加入者認識との間のマッピングに関する情報を発生し、そして上記マッピング情報を上記ＩＰネットワーク（９）に送信するための認証クライアント手段（５２）と、
を備え、この認証クライアント手段(52)はＲＡＤＩＵＳクライアントであることを特徴とするゲートウェイ装置。
【請求項１７】
上記認証クライアント手段（５２）は、上記マッピング情報をアクセス要求メッセージにおいて送信するように構成された請求項１６に記載のゲートウェイ装置。
【発明の詳細な説明】
【０００１】
【技術分野】
本発明は、第１ネットワークの加入者を第２ネットワークにおいて識別するための認証方法及びシステムに係る。
【０００２】
【背景技術】
ＧＰＲＳ（汎用パケット無線サービス）システムでは、パケットモード技術を使用して高速及び低速データ及びシグナリングが効率的に転送される。ＧＰＲＳは、ネットワーク及び無線リソースの使用を最適化する。標準的なデータプロトコルをベースとするアプリケーションがサポートされ、そしてＩＰネットワークとのインターワーキングが定義される。ＧＰＲＳは、間欠的及びバーストデータの転送から大量データの時々の送信までをサポートするように構成される。課金は、通常、転送されるデータの量に基づいて行われる。
【０００３】
ＧＰＲＳは、ＧＳＭ移動ネットワークに２つの新たなネットワークノードを導入する。サービングＧＰＲＳサポートノード（ＳＧＳＮ）は、移動交換センター（ＭＳＣ）と同じハイアラーキーレベルにあって、移動ステーション（ＭＳ）の個々の位置を追跡しそしてセキュリティ機能及びアクセス制御を遂行する。ＳＧＳＮは、フレームリレーでベースステーションシステムに接続される。ゲートウェイＧＳＮ（ＧＧＳＮ）は、外部パケット交換ネットワークとのインターワーキングを与え、そしてＩＰベースのＧＰＲＳバックボーンネットワークを経てＳＧＳＮに接続される。ＧＳＭシステムのＨＬＲ（ホーム位置レジスタ）は、ＧＰＲＳ加入者情報で改善され、そしてＶＬＲ（ビジター位置レジスタ）は、ＧＰＲＳ及び非ＧＰＲＳサービス及び機能の更に効率的な整合に対して改善することができ、例えば、ＳＧＳＮを経て更に効率的に遂行できる回路交換コールのページングや、複合ＧＰＲＳ及び非ＧＰＲＳ位置更新に対して改善することができる。
【０００４】
ＧＰＲＳサービスにアクセスするために、ＭＳは、先ず、ＧＰＲＳアタッチを実行することによりその存在をネットワークに知らせる。このオペレーションは、ＭＳとＳＧＳＮとの間に論理的リンクを確立し、そしてＭＳがＳＧＳＮを経てのページング及び到来するＧＰＲＳデータの通知を使用できるようにする。ＧＰＲＳデータを送信及び受信するために、ＭＳは、それが使用することを望むパケットデータアドレスをアクチベートしなければならない。このオペレーションは、ＭＳを対応するＧＧＳＮに知らしめ、そして外部データネットワークとのインターワーキングを開始することができる。ユーザデータは、カプセル化及びトンネル化として知られている方法でＭＳと外部データネットワークとの間で透過的に転送され、この場合、データパケットは、ＧＰＲＳ特有のプロトコル情報が設けられ、そしてＭＳとＧＧＳＮとの間で転送される。この透過的な転送方法は、ＧＰＲＳ移動ネットワークが外部データプロトコルを解釈する必要性を低減し、そして付加的なインターワーキングプロトコルを将来容易に導入できるようにする。

【０００５】
移動加入者が、ＩＰネットワークにより提供される付加価値サービス（ＶＡＳ）にアクセスしたい場合には、サービス特有の課金が、移動オペレータに対する対応ＶＡＳプラットホームの必須の特徴である。これは、オペレータが、例えばアクセスされたＷＭＬ内容又はＵＲＬ（均一リソースロケータ）及び供給されたメッセージに基づいて課金を実行できるサービスプラットホームを必要とすることを意味する。しかしながら、ＧＰＲＳネットワーク又は他の移動パケット交換ネットワークに接続されたＶＡＳプラットホームにおけるＭＳ識別は、普通のものではない。その理由は、ＶＡＳプラットホームは、あるソースアドレスからＩＰパケットしか受信しないが、これが、通常、ＭＳの動的なＩＰアドレスに過ぎず、従って、そのＭＳを識別するのに全く充分ではないからである。更に、付加的なＨＬＲ問い合わせを防止するためにメッセージングサービス（例えば、マルチメディアメッセージング）にとって特に重要なＭＳＩＳＤＮ（移動ステーションＩＳＤＮ番号）も必要とされる。

【０００６】
既知のＭＳ識別は、例えば、ユーザ名、パスワード又は暗号キーを使用することにより実行される。しかしながら、これらの形式の解決策は、移動オペレータにとって操作及び管理が複雑である。更に、これら解決策は、通常、それら自身のマネージメントシステム及びデータベースを必要とするが、これは、ＩＭＳＩ（国際移動加入者認識）又はＭＳＩＳＤＮがＣＤＲ（コール詳細記録）のキーである移動オペレータの既存のビリングシステム又は課金システムに必ずしも適合しない。
或いは又、ＨＬＲにおいて認証サービスを遂行することもできる。しかしながら、この解決策は、既に極めて厳しいノードであるＨＬＲに顕著な負荷上昇を招く。

【０００７】
【発明の開示】
それ故、本発明の目的は、ＶＡＳプラットホームが、そのＶＡＳプラットホームのサービスにアクセスするＭＳを識別できるようにする認証方法及びシステムを提供することである。
この目的は、第１ネットワークの加入者を第２ネットワークにおいて識別するための認証方法であって、上記第２ネットワークのアドレスを上記加入者に割り当て、上記第２ネットワークにおける加入者のアドレスと加入者の認識との間のマッピングに関する情報を発生し、そして上記マッピングを上記第２ネットワークに送信するという段階を含む認証方法によって達成される。

【０００８】
更に、上記目的は、第１ネットワークの加入者を第２ネットワークにおいて識別するための認証システムであって、ゲートウェイ装置を備え、このゲートウェイ装置は、上記第２ネットワークのアドレスを上記加入者に割り当てるための割り当て手段と、上記第２ネットワークの上記アドレスと加入者認識との間のマッピングに関する情報を発生しそしてそのマッピング情報を上記第２ネットワークに送信するための認証クライアント手段とを含み、そして更に、上記第２ネットワークに設けられそして上記マッピング情報をロギング及び維持するように構成された認証サーバーを備えた認証システムによって達成される。
更に、上記目的は、第１ネットワークを第２ネットワークに接続するためのゲートウェイ装置において、上記第２ネットワークのアドレスを上記第１ネットワークの加入者に割り当てるための割り当て手段と、上記第２ネットワークの上記アドレスと加入者認識との間のマッピングに関する情報を発生し、そして上記マッピング情報を上記ＩＰネットワークに送信するための認証クライアント手段とを備えたゲートウェイ装置によって達成される。

【０００９】
従って、第２ネットワークのアドレスと加入者認識との間のマッピング情報が発生されて第２ネットワークに供給される。これにより、クライアント－サーバー接続が達成され、これは、第２ネットワークの動的アドレスの実際の加入者認識を第２ネットワークへとハ

ンドオーバーできるようにする。第２ネットワークは、第２ネットワークのアドレスと加入者認識とのマッピングを使用して加入者を識別する。
第１ネットワーク、例えばＧＧＳＮは、第２ネットワークのアドレスと加入者認識との間のマッピングに関する情報を含むので、マッピングが変化した場合に新たなマッピングデータを第２ネットワークに送信することができる。
【００１０】
上記加入者認識は、加入者のＩＭＳＩ及び／又はＭＳＩＳＤＮであるのが好ましい。従って、マルチメディアメッセージングサービスは、ＭＳＩＳＤＮを使用して受信者を識別し、そして受信者は、マルチメディアメッセージングサービスセンターにより与えられるＭＳＩＳＤＮに基づいてメッセージの送信者を識別することができ、ＨＬＲ問合せは、もはや必要とされない。更に、ＭＳＩＳＤＮ又はＩＭＳＩは、加入者を識別してサービス特有の課金を実行するために課金機能によって使用される。
マッピング情報は、アクセス要求メッセージ、例えば、ＲＡＤＩＵＳアクセス要求メッセージにおいて送信することができる。
【００１１】
認証サーバー機能がＶＡＳプラットホームに対して設けられ、アクセス要求メッセージがＶＡＳプラットホームの認証サーバー機能へ送信され、そして移動ターミナルがＶＡＳプラットホームにおいてマッピング情報に基づいて識別されるのが好ましい。この場合に、認証サーバー機能がＶＡＳプラットホームに含まれてもよいし、或いは認証サーバー機能が専用の認証サーバーによって与えられてもよい。
ゲートウェイ装置がＧＧＳＮである場合には、マッピング情報は、ＧＧＳＮの認証クライアント機能によって発生される。
マッピング情報は、サービス特有の課金に使用することもできる。
認証サーバーは、第２ネットワークに設けられたＶＡＳプラットホームに対するＲＡＤＩＵＳサーバーでよく、この場合、ＶＡＳプラットホームは、マッピング情報に基づいて加入者を識別するように構成される。
【００１２】
【発明を実施するための最良の形態】
以下、添付図面を参照して、本発明の好ましい実施形態を詳細に説明する。
本発明による認証方法及びシステムの好ましい実施形態を、第１ネットワークの一例であるＧＰＲＳネットワークと、第２ネットワークの一例であるＩＰネットワークとに基づいて以下に説明する。
図１に示すように、移動ターミナル又は移動ステーション（ＭＳ）１は、ＧＳＭネットワーク２に無線接続され、該ネットワークは、次いで、ＧＰＲＳバックボーンネットワークのＳＧＳＮ３に接続される。ＧＰＲＳバックボーンネットワークは、課金サーバー４と、ＧＧＳＮ５を備え、これは、ＩＰネットワーク９、例えば、特定のオペレータのイントラネット又はインターネットに接続される。
【００１３】
ＧＧＳＮ５は、ＩＰネットワーク９へのアクセスを与えるアクセスポイントユニット（ＡＰ）５１を備え、これは、ＩＰネットワーク９に接続されるべきＭＳにＩＰアドレスを割り当てるように構成される。更に、ＧＧＳＮ５は、ＩＰネットワーク９へ発生されるアクセス要求に対して必要なパラメータを与えるように構成された認証クライアントユニット５２を備えている。更に、この認証クライアントユニット５２は、ＩＰネットワーク９の所望のＶＡＳへ供給されるユーザ名及びパスワードパラメータの取り扱いを明瞭化及び指定するよう構成される。
図１に示す好ましい実施形態によれば、ＩＰネットワーク９は、オペレータのイントラネットバックボーンであり、これは、アドレス割り当てサーバー６、例えば、ＲＡＤＩＵＳ（リモート認証ダイヤルインユーザサービス）サーバーや、ＤＨＣＰ（ダイナミックホストコンフィギュレーションプロトコル）サーバー又はＤＮＳ（ドメイン名サーバー）等を含む。このアドレス割り当てサーバー６は、ＧＧＳＮ５からのアクセス要求に、アクセス

受け入れ又はアクセス拒絶メッセージで応答するように構成される。更に、アドレス割り当てサーバー６は、ＩＰネットワーク９においてホスト構成及びアドレス割り当てを遂行する。

【００１４】

更に、ＩＰネットワーク９、例えば、オペレータのイントラネットは、付加価値サービス（ＶＡＳ）プラットホーム７を備えている。このようなＶＡＳプラットホームの一例は、ＭＳ１のような要求を発している加入者へマルチメディアメッセージを供給するためのマルチメディアメッセージセンター（ＭＭＳＣ）である。更に、ＶＡＳプラットホームの別の例は、対応する均一リソースロケーター（ＵＲＬ）に基づいてワールドワイドウェブ（ＷＷＷ）へのアクセスを与えるワイヤレスアプリケーションプロトコル（ＷＡＰ）である。

本発明の好ましい実施形態によれば、ＶＡＳプラットホーム７に対する専用の認証サーバー８がＩＰネットワーク９に設けられる。この認証サーバー８は、ＶＡＳプラットホーム７へのアクセス要求を受け入れるか又は拒絶するＲＡＤＩＵＳサーバーである。更に、認証サーバー８は、ＧＧＳＮ５の認証クライアント５２、例えば、ＲＡＤＩＵＳクライアントから受け取ったアクセス要求又はそれに対応する移動加入者認識をロギング又は記憶するように構成される。従って、ＧＧＳＮ５の認証クライアント５２は、アドレス割り当てサーバー又は特定の認証サーバー８と通信して、認証クライアント－サーバー接続が確立されるようにする。

【００１５】

特に、認証クライアント５２は、マッピング情報を組み込むか又はそれをアクセス要求に追加し、それに基づいて、ＩＰネットワーク９からサービスを要求するＭＳの実際のＭＳＩＳＤＮ及び／又はＩＭＳＩを認証サーバー８において導出することができる。マッピング情報は、現在ＩＰアドレス、ＭＳＩＳＤＮ及び／又はＩＭＳＩ、或いはその組合せ又は短縮バージョンを含み、これに基づいて、ＭＳＩＳＤＮ及び／又はＩＭＳＩを現在のＩＰアドレスから導出することができる。ＭＳＩＳＤＮは、ＧＧＳＮ５によりＧＳＭネットワーク２からＳＧＳＮ３を経て得ることができる。

従って、ＧＧＳＮ５の認証クライアントユニット５２は、ＩＰアドレスと、ＭＳＩＳＤＮ及び／又はＩＭＳＩとの間のマッピングに関する情報を与える。このマッピングが変更される場合には、認証クライアントユニット５２は、ＩＰネットワーク９の認証サーバー８に新たなマッピング情報を送信する。これにより、ＭＳＩＳＤＮ及び／又はＩＭＳＩが常にＶＡＳプラットホーム７に得られる。

【００１６】

ＭＳＩＳＤＮは、ＳＧＳＮ３からＧＧＳＮ５へ供給される付加的なＧＴＰパラメータとして与えることができる。ＩＭＳＩは、これもＳＧＳＮ３からＧＧＳＮ５へ供給されるＴＩＤから導出することができる。

ＧＧＳＮ５は、ＩＰネットワーク９とインターワーキングするためのＧＳＭ　ＧＰＲＳデータネットワークのアクセスポイントとして機能する。この場合に、ＧＰＲＳネットワークは、他のＩＰネットワーク又はサブネットワークのように見える。ＩＰネットワーク９へのアクセスは、ユーザ認証、ユーザ許可、ＭＳとＩＰネットワーク９との間の端－端暗号化、ＩＰネットワーク９のアドレススペースに属するダイナミックＩＰアドレスの割り当てといった特定の機能を伴う。より詳細には、ＩＰネットワーク９へのアクセスを要求するＭＳ１には、オペレータアドレッシングスペースに属するアドレスが与えられる。このアドレスは、契約時に与えられるか（この場合は、スタティックアドレスである）又はＰＤＰ（パケットデータプロトコル）コンテキストアクチベーションにおいて与えられる（この場合は、ダイナミックアドレスである）。このアドレスは、ＩＰネットワーク９とＧＧＳＮ５との間及びＧＧＳＮ５内でのパケット転送に使用される。

【００１７】

ＧＰＲＳバックボーンネットワークを経てＩＰネットワーク９へ行われるアクセスオペレーションの一例を、図２を参照して以下に説明する。

図２は、例示的なアクセスオペレーション中に実行されるシグナリング及び処理動作を示す情報流及び処理図である。図２によれば、ＭＳ１は、「ＰＤＰコンテキストアクチベート要求」メッセージをＳＧＳＮ３へ送信し、これは、ＮＳＡＰＩ（ネットワークレイヤーサービスアクセスポイント識別子）のようなプロトコルコンフィギュレーションオプション及びパラメータを含む。次いで、ＳＧＳＮ３は、ＭＭ（移動管理）コンテキストに記憶されたＩＭＳＩを、ＭＳから受け取ったＭＳＡＰＩと合成することにより、要求されたＰＤＰコンテキストに対するＴＩＤを形成し、ここで、ＳＧＳＮは、ＨＬＲからＭＳＩＳＤＮをフェッチする。その後、ＳＧＳＮ３は、「ＰＤＰコンテキスト形成要求」メッセージをＧＧＳＮ５へ送信し、これは、ＡＰＮ（アクセスポイント名）、ＴＩＤ及びＭＳＩＳＤＮのようなパラメータを含む。ＧＧＳＮ５のＡＰユニット５１は、ＭＳ１に対するＩＰアドレスを割り当て、そして認証クライアントユニット５２は、アクセス要求に対して要求されるパラメータを認証サーバー８に組み込む。より詳細には、認証クライアントユニット５２は、割り当てられたＩＰアドレスとＭＳＩＳＤＮ／ＩＭＳＩとの間のマッピングを指示するマッピングデータを発生する。

【００１８】

ＧＧＳＮ５は、ＩＰアドレス及びマッピングデータを含むアクセス要求を、ＶＡＳプラットホーム７に対して設けられた認証サーバー８へ送信する。次いで、認証サーバー８は、受け取った要求を受け入れ又は拒絶する。更に、認証サーバー８は、ＩＰアドレス及びマッピングデータを含む要求をロギングする。従って、ＶＡＳプラットホーム７は、認証サーバー８に記憶されたアクセス要求に含まれたマッピングデータに基づいてＭＳ１を識別することができる。

ＧＧＳＮ５は、「ＰＤＰコンテキスト形成応答」メッセージをＳＧＳＮ３に返送し、ここで、原因値が、認証の結果、即ちアクセス拒絶又は受け入れに基づいてセットされる。「ＰＤＰコンテキスト形成応答」メッセージにおいて受け取られる原因値に基づいて、ＳＧＳＮ３は、「ＰＤＰコンテキストアクチベート受け入れ」メッセージ又は「ＰＤＰコンテキストアクチベート拒絶」メッセージをＭＳ１に送信する。

【００１９】

従って、上記アクセス手順により、ＶＡＳプラットホーム７は、ＩＰアドレスと、アクセスしているＭＳのＩＭＳＩ及びＭＳＩＳＤＮとを受け取ることができ、マルチメディアメッセージングサービスのアドレッシングは、ＭＳＩＳＤＮをベースとすることができ、そしてサービス特有の課金を行うことができる。

要約すれば、本発明は、第１ネットワークの加入者を第２ネットワークにおいて識別するための認証方法及びシステムであって、第２ネットワークのアドレスが加入者に割り当てられる方法及びシステムに係る。第２ネットワークのアドレスと加入者認識との間のマッピングに関する情報が発生されて第２ネットワークに送信される。これにより、第１ネットワークと第２ネットワークとの間に認証サーバー接続が形成され、加入者認識を第２ネットワークへハンドオーバーすることができる。従って、第２ネットワークのＶＡＳプラットホームは、第２ネットワークのアドレス及び加入者の認識を受け取ることができ、従って、ＶＡＳプラットホームの加入者アクセスサービスを課金及び／又はアドレッシングの目的で識別することができる。

【００２０】

上述した認証方法及びシステムは、移動ネットワークとＩＰネットワーク、或いは電話ネットワーク（例えば、ＩＳＤＮ、ＰＳＴＮ）と閉又は開データネットワークのような２つのネットワーク間のゲートウェイ装置に適用できることに注意されたい。更に、認証サーバー８及び認証クライアントユニット５２は、ＲＡＤＩＵＳサーバー及びクライアントに限定されるものではない。又、互いに同様の又は異なる多数のＶＡＳプラットホームを第２ネットワークに同時にアタッチできることにも注意されたい。

好ましい実施形態の上記説明及び添付図面は、本発明を単に例示するものに過ぎない。従って、本発明の好ましい実施形態は、特許請求の範囲内で変更し得るものである。

【図面の簡単な説明】

【図１】　本発明の好ましい実施形態によりＩＰネットワークに接続されたＧＰＲＳネットワークのブロック図である。
【図２】　本発明の好ましい実施形態によりＩＰネットワークにアクセスするオペレーションを示す情報流及び処理図である。

【図１】

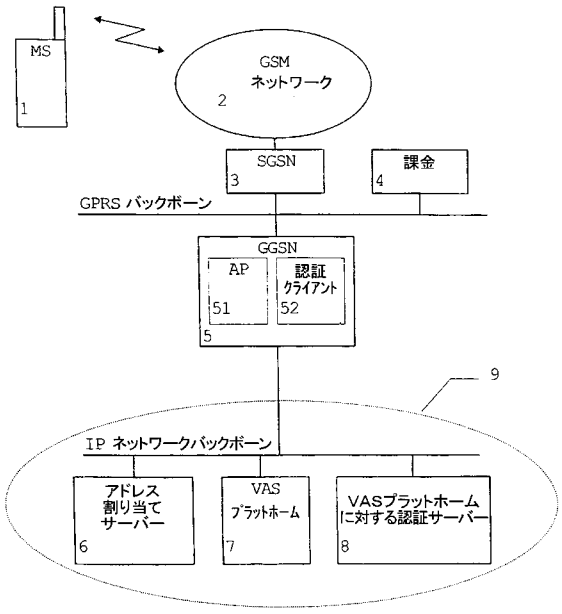

Fig. 1

【図２】

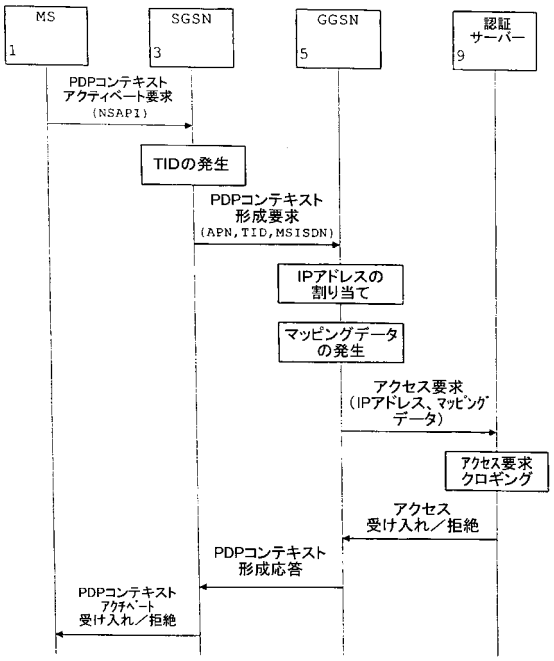

Fig. 2

フロントページの続き

(74)代理人 100084009
弁理士 小川 信夫
(74)代理人 100086771
弁理士 西島 孝喜
(74)代理人 100084663
弁理士 箱田 篤
(72)発明者 ヴィティカイネン ティモ
フィンランド エフイーエン－０２６６０ エスプー シニタイスクンポルク ４アー３

審査官 宮司 卓佳

(56)参考文献 特開平０９－１１４８９１（ＪＰ，Ａ）
特開平１１－１７７６０２（ＪＰ，Ａ）
枝洋樹、今井拓司，パソコンＩＤ宣言 認証技術 固有番号と認証回路で個別の端末を確実に識別，日経エレクトロニクス，日経ＢＰ社，１９９９年 4月 5日，第７４０号，p.105-p.113

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20
H04Q 7/38
H04L 9/00