(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3772831号
(P3772831)
(45)発行日　平成18年5月10日(2006.5.10)　(24)登録日　平成18年2月24日(2006.2.24)

(51)Int.Cl.		F I		
H04Q 7/38	(2006.01)	H04B	7/26	109R
G06F 21/20	(2006.01)	G06F	15/00	330B
G09C 1/00	(2006.01)	G09C	1/00	640E

請求項の数 16　(全 9 頁)

(21)出願番号	特願2002-515860 (P2002-515860)
(86)(22)出願日	平成13年7月30日 (2001.7.30)
(65)公表番号	特表2004-505570 (P2004-505570A)
(43)公表日	平成16年2月19日 (2004.2.19)
(86)国際出願番号	PCT/US2001/023764
(87)国際公開番号	WO2002/011469
(87)国際公開日	平成14年2月7日 (2002.2.7)
審査請求日	平成15年2月13日 (2003.2.13)
(31)優先権主張番号	09/630,425
(32)優先日	平成12年8月1日 (2000.8.1)
(33)優先権主張国	米国 (US)

(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　100086368
弁理士　萩原　誠
(72)発明者　ステファノ　ファシーン
アメリカ合衆国　テキサス州　７５２２９－２６２２　ダラス　ダルトモーア　３４２１
(72)発明者　フランク　ル
アメリカ合衆国　テキサス州　７５０６３　アービング　ウェスト　ロイヤル　レーン　ナンバー２１２　２７１５

最終頁に続く

(54)【発明の名称】ＳＩＰ（セッション開始プロトコル）メッセージを用いるＵＭＴＳ（ユニバーサル移動通信システム）認証の実行方法

(57)【特許請求の範囲】

【請求項１】

ＳＩＰ（セッション開始プロトコル）メッセージを使用するサーバに対して利用者エージェントの認証を行う方法において、前記方法が、

前記利用者エージェントから前記サーバへＳＩＰ要求を送信するステップと、

前記ＳＩＰ要求に応答して前記サーバから前記利用者エージェントへ認証要求を送信するステップであって、前記認証要求には、前記認証がＵＭＴＳ（ユニバーサル移動通信システム）ＡＫＡ（認証及び基本協定）メカニズムを用いて実行される旨の情報が含まれるステップと、

前記ＵＭＴＳ　ＡＫＡメカニズムに従って、前記認証要求に応答して前記利用者エージェントから前記サーバへ認証応答を送信するステップと、

前記認証応答に照らして前記認証が成功すると考えられる場合、前記ＳＩＰ要求に応答して、呼び出されたＳＩＰ処理手順を前記サーバ上で実行するステップと、を有することを特徴とする方法。

【請求項２】

請求項１に記載の方法において、前記ＳＩＰ要求が、ＳＩＰ　ＩＮＶＩＴＥ（送信勧誘）要求またはＳＩＰ　ＲＥＧＩＳＴＥＲ（登録）要求のうちの一方を含むことを特徴とする方法。

【請求項３】

請求項１に記載の方法において、前記認証要求が、ＳＩＰ４０１不許可コードまたはＳＩ

Ｐ４０７プロキシ認証要求コードのうちの一方を含むことを特徴とする方法。
【請求項４】
請求項３に記載の方法において、前記認証要求がＵＭＴＳ　ＡＫＡ　ＲＡＮＤ（ランダムな呼び掛け）およびＡＵＴＮ（認証トークン）ベクトルとを含むことを特徴とする方法。
【請求項５】
請求項４に記載の方法において、前記ＲＡＮＤおよびＡＵＴＮベクトルがＳＩＰ　WWW-認証またはプロキシ-認証応答ヘッダ・フィールドの中に含まれることを特徴とする方法。
【請求項６】
請求項１に記載の方法において、前記認証応答が、ＵＭＴＳ　ＡＫＡ　ＲＥＳ（応答）コードまたはＡＵＴＳ（同期失敗パラメータ）コードまたはエラーコードのうちの１つを含むことを特徴とする方法。
【請求項７】
請求項６に記載の方法において、ＳＩＰ認証またはプロキシ-認証ヘッダ・フィールドの中に前記認証応答が含まれることを特徴とする方法。
【請求項８】
請求項１に記載の方法において、前記呼び出された処理手順が、ＳＩＰ２００コードを含む確認応答を含むことを特徴とする方法。
【請求項９】
機械により読出し可能なプログラム記憶装置であって、前記機械により実行可能な命令を示すプログラムを有形のものとして具現化して、ＳＩＰメッセージを使用するサーバに対して利用者エージェントの認証を行う方法を実行するプログラム記憶装置において、前記方法が、
前記利用者エージェントから前記サーバへＳＩＰ要求を送信するステップと、
前記ＳＩＰ要求に応答して前記サーバから前記利用者エージェントへ認証要求を送信するステップであって、前記認証要求には、前記認証がＵＭＴＳ（ユニバーサル移動通信システム）ＡＫＡ（認証及び基本合意）メカニズムを用いて実行される旨の情報が含まれるステップと、
前記ＵＭＴＳ　ＡＫＡメカニズムに従って、前記認証要求に応答して前記利用者エージェントから前記サーバへ認証応答を送信するステップと、
前記認証応答に照らして前記認証が成功すると考えられる場合、前記ＳＩＰ要求に応答して、呼び出されたＳＩＰ処理手順を前記サーバ上で実行するステップと、を有することを特徴とする装置。
【請求項１０】
請求項９に記載の記憶装置において、前記ＳＩＰ要求が、ＳＩＰ　ＩＮＶＩＴＥ要求またはＳＩＰ　ＲＥＧＩＳＴＥＲ要求のうちの一方を含むことを特徴とする装置。
【請求項１１】
請求項９に記載の記憶装置において、前記認証要求が、ＳＩＰ４０１不許可コードまたはＳＩＰ４０７プロキシ認証要求コードのうちの一方を含むことを特徴とする装置。
【請求項１２】
請求項１１に記載の記憶装置において、前記認証要求がＵＭＴＳ　ＡＫＡ　ＲＡＮＤ（ランダムな呼び掛け）およびＡＵＴＮ（認証トークン）ベクトルとを含むことを特徴とする装置。
【請求項１３】
請求項１２に記載の記憶装置において、前記ＲＡＮＤおよびＡＵＴＮベクトルがＳＩＰ　WWW-認証またはプロキシ-認証応答ヘッダ・フィールドの中に含まれることを特徴とする装置。
【請求項１４】
請求項９に記載の記憶装置において、前記認証応答が、ＵＭＴＳ　ＡＫＡ　ＲＥＳ（応答）コードまたはＡＵＴＳ（同期失敗パラメータ）コードまたはエラーコードのうちの１つ

を含むことを特徴とする装置。
【請求項１５】
請求項１４に記載の記憶装置において、ＳＩＰ認証またはプロキシ-認証ヘッダ・フィールドの中に前記認証応答が含まれることを特徴とする装置。
【請求項１６】
請求項９に記載の記憶装置において、前記呼び出された処理手順が、ＳＩＰ２００コードを含む確認応答を含むことを特徴とする装置。
【発明の詳細な説明】
【０００１】
（技術分野）
本発明はＳＩＰ（セッション開始プロトコル）メッセージを使用する認証の実行技法に関する。さらに詳細には、本発明はＳＩＰメッセージを使用するＵＭＴＳ（ユニバーサル移動通信システム）の認証実行技法に関する。
【０００２】
（背景技術）
ＳＩＰはＵＮＩ（ユーザからネットワークへのインターフェース）、すなわち、移動通信加入者とＣＳＣＦ（呼状態制御機能）間のインターフェースを介する、Ｒ００（リリース２０００）のプロトコルとして選択されている。そして、最新のＵＭＴＳ　ＡＫＡ（認証及び基本合意）はＲ００ＵＭＴＳの認証メカニズムに対する１つの提案である。
【０００３】
ＳＩＰは、１９９９年３月に発行された、ＩＥＴＦ（インターネット・エンジニアリング・タスク・フォース）のドラフト規格ＲＦＣ２５４３（コメント要求）で定められたものであり、ＵＭＴＳ　ＡＫＡは、３ＧＰＰ（第３世代パートナー・プロジェクト）仕様ＴＳ３３．１０２（バージョン３．５．０、リリース１９９９、２０００年７月発行）で定められたものである。このドラフト規格内容の全体及び上記仕様内容の全体は本願明細書に参考文献として取り入れられている。
【０００４】
上記ドラフト規格に記載されているように：セッション開始プロトコル（ＳＩＰ）は、１以上の参加者とのセッションの作成、変更、終了を行うためのアプリケーション層制御（信号）プロトコルである。このセッションには、インターネット・マルチメディア会議、インターネット電話、及び、マルチメディア配信が含まれる。セッションのメンバーは、マルチキャストを介して、あるいは、ユニキャスト関係のメッシュを介して、もしくは、上記の組み合わせを介して交信を行うことができる。
【０００５】
セッションの作成に使用されるＳＩＰの送信勧誘は、１組の互換性のある媒体タイプについて参加者の合意を可能とするセッション記述を担持する。ＳＩＰは、プロキシ要求と、ユーザの現在位置に対するリダイレクト要求によりユーザのモビリティをサポートする。ユーザは当該現在位置の登録を行うことが可能となる。ＳＩＰは特定のいずれの会議制御プロトコルにも拘束されない。ＳＩＰは、下位層のトランスポート・プロトコルから無関係となるようには設計されていないため、追加能力を備えた拡張を行うことが可能である。
【０００６】
しかし、ＳＩＰメッセージを介して認証を実行するためのＵＭＴＳ　ＡＫＡ処理手順の利用は上記ドラフト規格には開示されていない。
【０００７】
さらに、移動ＩＰ電話をサポートするＩＰマルチメディア（ＩＭ）サブシステムでは、加入者認証メカニズムの標準化を行う必要がある。このような認証メカニズムは標準化されてはいない。しかしながら、ＵＭＴＳ　ＡＫＡ処理手順がこの選択された認証メカニズムとなることが最も予想される。したがって、ＳＩＰプロトコルを用いるＵＭＴＳ　ＡＫＡを実行する技法を定める必要がある。

【０００８】
（発明の開示）
したがって、本発明の目的は、ＵＭＴＳ　ＡＫＡ処理手順を用いる認証を実行し、ＳＩＰメッセージを介して対応するＵＭＴＳパラメータを担持する技法を提供することである。ＳＩＰメッセージ内に含まれる適当なフィールドを持つ新しいＵＭＴＳ　ＡＫＡ認証モードを作成することにより、上記認証を実行するか、或いは、ＳＩＰメッセージの既存の認証モード（ダイジェスト・モードやＰＧＰモードなど）の再使用と適合化とにより上記認証を実行するかのいずれかを行うことが可能である。
【０００９】
ＩＭサブシステムの場合、本発明の別の目的として、ＵＥ（ユーザ用装置）とＣＳＣＦとの間の呼制御プロトコルとして使用して、認証パラメータの担持に選択されるＳＩＰメッセージの利用がある。
【００１０】
本発明のさらに別の目的として、ＩＭサブシステムにおける認証手続のための可能なソリューションとしてＵＭＴＳ　ＡＫＡメカニズムを再使用するという目的がある。
【００１１】
本発明のさらなる目的として、ＩＭサブシステムにおける加入者認証ＵＭＴＳ　ＡＫＡメカニズムを利用するために、ＳＩＰメッセージとヘッダ・フィールドのいずれを使用して、ＵＭＴＳ認証パラメータを担持するようにするかを定め、さらに、ＳＩＰヘッダ・フィールドの中にＵＭＴＳ認証パラメータを含める方法を定めるという目的がある。
【００１２】
添付図面と関連して読むとき、実施態様例についての以下の詳細な説明と請求項とから、本発明の上述の目的及び本発明のより良い理解が明らかになる。これらはすべて本発明の開示の一部を形成するものである。上述及び以下に記載の例示された開示は、本発明の実施態様例の開示に焦点を合わせたものであり、同開示は例示及び実施例による開示にすぎず、本発明はこれに限定されるものではない旨を明瞭に理解されたい。本発明の精神と範囲は添付の請求項の文言によってのみ限定されるものである。
【００１３】
（発明を実施するための最良の形態）
本発明の詳細な説明を始める前に、以下のことを述べておく必要がある。異なる図面においても、適切な場合、同じ参照番号及び記号が類似の構成要素を示すために使用される。さらに、以下の詳細な記述では、例示のサイズ／モデル／値／範囲を示す場合があるが、本発明はこれらに限定されるものではない。さらに、本発明を不明瞭なものとしないように、実施例と説明との簡略化のために図面に示されていないエレメントもある。
【００１４】
図１は、ＳＩＰ　ＵＡとＣＳＣＦ間のデータ・フローの一例を示す。但し、ＣＳＣＦの代わりにプロキシ・サーバを使用してもよい。セキュリティ・ポリシに応じて、ＵＭＴＳ　ＡＫＡを実行する必要がある場合（呼設定時や登録時など）、ＵＥ内のＵＡにより、ＣＳＣＦまたはプロキシに対するＲＥＧＩＳＴＥＲ要求またはＩＮＶＩＴＥ要求が送信される。ＣＳＣＦまたはプロキシは、２００　ＯＫメッセージの送信により登録を受け入れるか、４０１不許可応答の送信により認証を求めることができる。
【００１５】
前述の３ＧＰＰ仕様によれば、ＵＭＴＳ　ＡＫＡ処理手順を実行するためには、ユーザの認証のための２つのパラメータ（ＲＡＮＤとＡＵＴＮ）をユーザへ送信する必要があり、次いでユーザがこれに応答を行う。
【００１６】
したがって、４０１応答には、必要な認証方式と関連するパラメータを含むＷＷＷ認証応答ヘッダ・フィールドが含まれる。本発明に基づくＵＭＴＳ　ＡＫＡ処理手順の実行時に、ＷＷＷ認証ヘッダにはＲＡＮＤ（ランダムな呼び掛け）とＡＵＴＮ（認証トークン）とが含まれる。

【００１７】
４０１応答後、ＵＡは新しいＲＥＧＩＳＴＥＲ要求またはＩＮＶＩＴＥ要求の送信を行うことが可能であり、この要求は認証ヘッダ・フィールドに適切な認証情報を含むことが望ましい。本発明に基づくＵＭＴＳ　ＡＫＡ処理手順の場合、認証ヘッダにはＲＥＳまたはＡＵＴＳあるいはエラーコードが含まれる（例えば、ＭＡＣ（メッセージ認証コード）が無効であると考えられる場合、エラー・メッセージを送信することができる）。
【００１８】
ＩＮＶＩＴＥ要求の提示後のプロキシ認証を示す図２を参照すると、ＵＡによるＣＳＣＦへのＩＮＶＩＴＥ要求送信時に、ＣＳＣＦは４０７プロキシ認証要求応答の送信により認証を要求することができる。上記４０７応答には、必要な認証方式及び関連するパラメータを含むプロキシ認証応答ヘッダ・フィールドが含まれる。
【００１９】
４０７応答の受信後、ＵＡはＡＣＫ（肯定）応答を送信し、ＩＮＶＩＴＥ要求を反復することができ、この反復要求の中には、プロキシ-認証ヘッダ・フィールド内の適切な認証情報が含まれる。
【００２０】
ＵＭＴＳ　ＡＫＡ処理手順の場合には、プロキシ認証ヘッダはWWW認証ヘッダと同じ情報を含み、プロキシ-認証ヘッダは認証ヘッダと同じ情報を含む。この処理手順は、ＵＡが要求を送信するとき（呼の開始時など）にだけ利用できるので、登録時に認証用として代用することはできない。
【００２１】
ＲＥＧＩＳＴＥＲ要求、２００　ＯＫメッセージ、及び、４０１不許可応答、並びに、その他のパラメータ及びエレメントがすべて明瞭に前述のＲＦＣ２５４３ドラフト規格に定められていることを付記しておく。
【００２２】
前述のドラフト規格にはＳＩＰ認証の３つの異なる技法、すなわち、ＨＴＴＰ“基本”認証メカニズムと、ＨＴＴＰ“ダイジェスト”認証メカニズムと、ＰＧＰ（かなり良好なプライバシー）認証メカニズムとが定義されている。ＨＴＴＰ認証メカニズムは１９９９年７月に発行されたＩＥＴＦドラフト規格ＲＦＣ２６１７に定められている。このドラフト規格の内容はその全体が本願明細書に参考文献として取り入れられている。
【００２３】
ＳＩＰ認証のこれら３つの異なる技法は使用可能ではあるが、簡略化のため、代わりにＵＭＴＳ　ＡＫＡ技法を好適に使用することが可能である。さらに、ＳＩＰ規格におけるフォーマットの改訂を必要とせずに、これら３つの異なるＳＩＰ認証技法に使用されるエレメントの代わりにＵＭＴＳ　ＡＫＡエレメントの利用も可能である。
【００２４】
したがって、本発明によれば、４０１応答には、ＵＭＴＳ　ＡＫＡ認証ベクトル、すなわち、ＲＡＮＤ（ランダムな呼び掛け）とＡＵＴＮ（認証トークン）とを含むWWW認証応答ヘッダ・フィールドが含まれる。
【００２５】
４０１応答後、ＵＥは、認証ヘッダ・フィールドに適切な認証情報を含むことが望ましい新しいＲＥＧＩＳＴＥＲ／ＩＮＶＩＴＥ要求の送信を行う。ＭＡＣ（メッセージ認証コード）が無効であると考えられた場合、認証応答（ＲＥＳ）、同期失敗パラメータ（ＡＵＴＳ）、エラーコードを送信してもよい。
【００２６】
呼設定用として、以下に解説するように、４０７プロキシ認証要求応答を利用してＵＭＴＳ　ＡＫＡパラメータを担持するようにしてもよいことを付記しておく。
【００２７】
本発明は、ＳＩＰメッセージの中にＵＭＴＳ　ＡＫＡパラメータを担持する２つの方法を定めるものである。

【００２８】
上述したように、ＳＩＰ規格により、認証用の３つの異なる技法すなわち、ＨＴＴＰ基本認証法、ＨＴＴＰダイジェスト認証法、ＰＧＰ認証メカニズムが定義されている。
【００２９】
したがって、必要なフィールドを用いて新しい認証モード、ＵＭＴＳ　ＡＫＡモードを定めることも可能である。或いは、ＵＭＴＳ　ＡＫＡ処理手順の実行のために既存のモードの再使用と適合化を行ってもよい。
【００３０】
ＩＭサブシステムにおいて認証を行うためにＵＭＴＳ　ＡＫＡ処理手順を使用可能にするために、ＳＩＰメッセージ内にＵＭＴＳ　ＡＫＡパラメータを含める方法を定める必要がある。新しい認証方法またはモードを導入してＳＩＰメッセージの中にＵＭＴＳ　ＡＫＡパラメータを含めるようにしてもよい。本発明による新しい認証モードについて以下に説明する。この新しい認証モードには、できるだけ短くしたヘッダが含まれる。
【００３１】
ＵＭＴＳ　ＡＫＡ処理手順の場合、WWW認証応答ヘッダは、ＲＡＮＤとＡＵＴＮの双方を担持できるものでなければならない。したがって、単純なフォーマットの１例として以下のようなフォーマットを使用することができる：

```
WWW-Authenticate ='WWW-Authenticate' ':' 'UMTS' RAND AUTN
RAND ='RAND' '='RAND-value
AUTN ='AUTN' '='AUTN-value
```

【００３２】
ＲＡＮＤ値とＡＵＴＮ値の双方について１６進フォーマットを用いてもよい。
【００３３】
ＵＭＴＳ　ＡＫＡ処理手順の場合、認証ヘッダはＲＥＳ値またはＡＵＴＳ値を担持できなければならない。したがって、単純なフォーマットの１例として、以下のようなフォーマットを使用することができる：

```
Authorization ='Authorization' ':' 'UMTS'RES|AUTS|AUTH-REJECT
RES ='RES' '=' RES-value
AUTS ='AUTS' '=' AUTS-value
AUTH-REJECT ='AUTH-REJECT' '=' error-code
```

ＲＥＳ値とＡＵＴＳ値の双方について１６進フォーマットを用いてもよい。
【００３４】
プロキシ認証応答ヘッダは、WWW認証応答ヘッダの役割と実質的に同じ役割を果たす。同様のフォーマットの１例として以下のようなフォーマットを使用することができる：

```
Proxy-Authenticate ='Proxy-Authenticate' ':' 'UMTS' RAND AUTN
RAND ='RAND' '=' RAND-value
AUTN ='AUTN' '=' AUTN-value
```

【００３５】
同様に、プロキシ-認証応答ヘッダは、認証応答ヘッダの役割と実質的に同じ役割を果たす。したがって、同様のフォーマットの１例として以下のようなフォーマットを使用することができる：
【００３６】

```
Proxy-Authorization ='Proxy-Authorization' ':' 'UMTS'RES|AUTS|AUTH-REJECT
RES ='RES' '=' RES-value
AUTS ='AUTS'  '=' AUTS-value
AUTH-REJECT = 'AUTH-REJECT' '=' error-code
```

【００３７】
したがって、ＩＭサブシステムにおいて利用するための本発明による認証メカニズムの場合、新しい認証モードとしてＵＭＴＳ　ＡＫＡ認証の利用が可能となる。
【００３８】

ＨＴＴＰの基本メカニズムとダイジェスト認証メカニズムとはＳＩＰドラフト規格で利用するために定めたものであるため、以下に述べるように、ダイジェスト・メカニズム用として予約されたＳＩＰメッセージの部分を本発明に基づいて別様に利用して、ＵＭＴＳ　ＡＫＡパラメータを担持することも可能である。

【００３９】

例えば、正式にはダイジェスト・メカニズムにより使用される“ｎｏｎｃｅ”フィールドを用いて、ＵＭＴＳ　ＡＫＡを連結したＲＡＮＤ値とＡＵＴＮ値を１６進フォーマットで担持するようにすることも可能である。ｎｏｎｃｅフィールドの内容は実施構成に依存するため、フィールドの長さはＲＡＮＤ値とＡＵＴＮ値を担持できるほど十分に長いものでなければならない。そうでない場合、ドラフト規格で定められている不透明な“フィールド”が使用されてＵＭＴＳ　ＡＫＡパラメータの一部分が担持されるようになる可能性がある。

【００４０】

ドラフト規格で定められた“応答”フィールドはＵＭＴＳ　ＡＫＡ　ＲＥＳエレメント用として使用される。同期エラーが生じた場合、ＡＵＴＳが“応答”フィールドの中に含まれることになる。“応答”フィールドの第１のキャラクタは該応答がＲＥＳ、ＡＵＴＳまたはエラーコードを含むことを示すことができる。ＲＥＳとＡＵＴＳとは１６進フォーマットで表されたものであってもよい。

【００４１】

正式にはダイジェスト・モード用として使用されるＳＩＰメッセージを利用する認証では、正式にはダイジェストの計算にどのアルゴリズムを用いるか（デフォルトでＭＤ５を用いることができる）を指定する“アルゴリズム”フィールドは、本発明によれば、このアルゴリズムがＵＭＴＳ　ＡＫＡ処理手順であるという情報を受け手に提供するために使用することができ、このようにして、受け手は、ｎｏｎｃｅフィールドが実際にはＲＡＮＤとＡＵＴＮとを担持していることを理解することになる。

【００４２】

上述したように、ＰＧＰメカニズムは、ＳＩＰドラフト規格で使用する認証用として定められたものである。代替用として、本発明に基づいてこのモードを用いてＵＭＴＳ　ＡＫＡパラメータを担持することができる。すなわち：

【００４３】

“ｎｏｎｃｅ”フィールドはＲＡＮＤ値とＡＵＴＮ値とを担持することが可能である。“ＰＧＰ＝ａｌｇｏｒｉｔｈｍ”は、これがＵＭＴＳ　ＡＫＡ処理手順であるという情報を受け手に与えることができる。

【００４４】

この結果は“ＰＧＰ-サイン”の中に含まれる。このフィールドは２００ビット以上の長さとなる場合もあるので、このフィールドの第１のビットのいくつかを用いて、ＲＥＳ、ＡＵＴＳまたはエラーコードなどの結果のタイプを指定することができる。

【００４５】

以上が実施態様例の説明の結論である。本発明のいくつかの実施例に関して本発明を説明したが、本発明の原理の精神と範囲内に属する他の多数の変形及び実施態様を当業者が考案可能であることを理解されたい。特に、本発明の精神から逸脱することなく、上述の開示、図面、及び、添付の請求項の範囲内で、構成要素部分および／または上記組み合わせ構成の構成の合理的な変形例及び変更例が可能である。構成要素部分および／または構成の変形例及び変更例に加えて、別の利用例も当業者には明らかである。

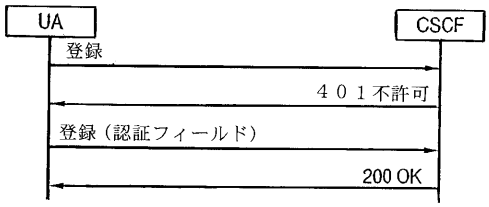
【図面の簡単な説明】

以下は図面についての簡単な説明を表すものである。

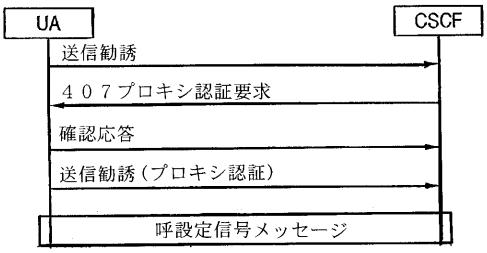
【図１】　ＳＩＰ　ＵＡ（ユーザー・エージェント）とＣＳＣＦ間のデータ・フローの一例を示す。

【図２】　ＳＩＰ　ＵＡとＣＳＣＦと間のデータ・フローの一例を示す。

【図１】


UA
CSCF
登録
４０１不許可
登録（認証フィールド）
200 OK

【図２】


UA
CSCF
送信勧誘
４０７プロキシ認証要求
確認応答
送信勧誘（プロキシ認証）
呼設定信号メッセージ

フロントページの続き

(72)発明者　ジョルジー　ウルフナー
ハンガリー　ブダペスト　エッチ－１０２５　スゼェプボルジー　ウト　４エー

審査官　高木　進

(56)参考文献　特開２００２－０８４２７６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04Q 7/00-7/38
G09C 1/00
G06F 21/20