(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5582544号
(P5582544)
(45)発行日　平成26年9月3日(2014.9.3)　(24)登録日　平成26年7月25日(2014.7.25)

(51)Int.Cl.　　F I
G06F 21/41 (2013.01)　　G06F 21/20 141
G06F 21/31 (2013.01)　　G06F 21/20 131A

請求項の数 21　(全 23 頁)

(21)出願番号　特願2011-524213 (P2011-524213)
(86)(22)出願日　平成21年7月22日 (2009.7.22)
(65)公表番号　特表2012-509517 (P2012-509517A)
(43)公表日　平成24年4月19日 (2012.4.19)
(86)国際出願番号　PCT/EP2009/005329
(87)国際公開番号　WO2010/022826
(87)国際公開日　平成22年3月4日 (2010.3.4)
審査請求日　平成23年2月24日 (2011.2.24)
(31)優先権主張番号　08015346.3
(32)優先日　平成20年8月29日 (2008.8.29)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　508342183
エヌイーシー　ヨーロッパ　リミテッド
ＮＥＣ　ＥＵＲＯＰＥ　ＬＴＤ.
ドイツ連邦共和国、６９１１５　ハイデルベルク、クアフュルステン・アンラーゲ　３６
(74)代理人　100097157
弁理士　桂木　雄二
(72)発明者　サントス、フーゴ
ドイツ連邦共和国　６９１１５　ハイデルベルク、フェーレンツシュトラーセ　６
(72)発明者　ジラオ、ジョアオ
ドイツ連邦共和国　６７０６３　ルードヴィッヒスハーフェン、ザイラーシュトラーセ　２３

最終頁に続く

(54)【発明の名称】ネットワークプロバイダ経由でサービスプロバイダへのネットワークアクセスをユーザに提供するシステムおよびその動作方法

(57)【特許請求の範囲】
【請求項１】
ネットワークプロバイダ（ＮＰ）と、サービスプロバイダ（ＳＰ）と、ユーザ装置と、を有するシステムの動作方法において、
サービスプロバイダ（ＳＰ）にアクセスすることを求めるユーザの要求によって、ユーザ装置とネットワークプロバイダ（ＮＰ）との間にコネクションを確立し、
ネットワークプロバイダ（ＮＰ）の要求に応じて、ユーザのアイデンティティプロバイダ（ＩｄＰ）がユーザ装置を認証し、
サービスプロバイダ（ＳＰ）または第三者がアクセス料金の支払側であるという情報をネットワークプロバイダ（ＮＰ）に与えるように、アイデンティティプロバイダ（ＩｄＰ）からネットワークプロバイダ（ＮＰ）へデータを送信し、
ネットワークプロバイダ（ＮＰ）が、ネットワークプロバイダ（ＮＰ）経由でサービスプロバイダ（ＳＰ）へのネットワークアクセスをユーザ装置に提供する
ことを特徴とする、前記システムの動作方法。
【請求項２】
ネットワークプロバイダ（ＮＰ）が支払側にアクセス料金を課金することをさらに含むことを特徴とする請求項１に記載の方法。
【請求項３】
ネットワークプロバイダ（ＮＰ）が課金情報を含むオブリゲーション情報を生成することをさらに含むことを特徴とする請求項１または２に記載の方法。

【請求項４】
オブリゲーション情報を生成するポリシー決定技術が、ＸＡＣＭＬ技術であることを特徴とする請求項３に記載の方法。
【請求項５】
アイデンティティプロバイダ（ＩｄＰ）が、サービスプロバイダ（ＳＰ）であることを特徴とする請求項１ないし４のいずれか１項に記載の方法。
【請求項６】
認証ステップ中に、ネットワークプロバイダ（ＮＰ）が、ユーザ装置に対して、自己のアイデンティティプロバイダ（ＩｄＰ）を指定するよう要求することを特徴とする請求項１ないし５のいずれか１項に記載の方法。
【請求項７】
ネットワークプロバイダ（ＮＰ）は、ユーザ装置が自己のアイデンティティプロバイダ（ＩｄＰ）を指定できるページへユーザ装置をリダイレクトすることを特徴とする請求項１ないし６のいずれか１項に記載の方法。
【請求項８】
ユーザ装置が、アイデンティティプロバイダ（ＩｄＰ）に対して認証を行うことを特徴とする請求項１ないし７のいずれか１項に記載の方法。
【請求項９】
アイデンティティプロバイダ（ＩｄＰ）からネットワークプロバイダ（ＮＰ）へ送信されるデータが、ネットワークプロバイダ（ＮＰ）によって作成されたコンテキスト、ユーザのポリシー、および／または、アクセスされるサービスプロバイダ（ＳＰ）のアイデンティティに基づくことを特徴とする請求項１ないし８のいずれか１項に記載の方法。
【請求項１０】
ネットワークプロバイダ（ＮＰ）とアイデンティティプロバイダ（ＩｄＰ）が、支払側を選択するためにネゴシエーションを行うことを特徴とする請求項１ないし９のいずれか１項に記載の方法。
【請求項１１】
支払側が、コンテキストおよび／またはユーザポリシーに基づいて選択されることを特徴とする請求項１０に記載の方法。
【請求項１２】
アイデンティティプロバイダ（ＩｄＰ）が、認証の後、ネットワークプロバイダ（ＮＰ）へユーザ装置をリダイレクトすることを特徴とする請求項１ないし１１のいずれか１項に記載の方法。
【請求項１３】
ネットワークプロバイダ（ＮＰ）が、ポリシー施行ポイント（ＰＥＰ）として作用して、ポリシー決定要求を生成し、アイデンティティプロバイダ（ＩｄＰ）にコンタクトし、アイデンティティプロバイダ（ＩｄＰ）が、ポリシー決定ポイント（ＰＤＰ）として作用することを特徴とする請求項１ないし１２のいずれか１項に記載の方法。
【請求項１４】
ネットワークプロバイダ（ＮＰ）が、課金オブリゲーション情報またはアイデンティティプロバイダ（ＩｄＰ）によって提供された情報について、支払側との間でネゴシエーションおよび／または確認を行うことを特徴とする請求項１ないし１３のいずれか１項に記載の方法。
【請求項１５】
ネゴシエーションおよび／または確認ステップ中に、支払および／またはサービスアクセスオプションが微調整されることを特徴とする請求項１４に記載の方法。
【請求項１６】
ネットワークプロバイダ（ＮＰ）および支払側またはサービスプロバイダ（ＳＰ）が両者とも、Ｐ３Ｐポリシーに関してサービスプロビジョニングのエッジを提供することを特徴とする請求項１ないし１５のいずれか１項に記載の方法。

【請求項１７】
Ｐ３Ｐポリシーが、サービス水準パラメータの決定および／またはアクセス条件のネゴシエーションのために使用されることを特徴とする請求項１６に記載の方法。
【請求項１８】
支払側またはサービスプロバイダ（ＳＰ）のアクティビティがフィルタおよび課金情報に集中し、ネットワークプロバイダ（ＮＰ）のアクティビティは支払に集中することを特徴とする請求項１ないし１７のいずれか１項に記載の方法。
【請求項１９】
ユーザに関する他の個人情報をネットワークプロバイダ（ＮＰ）および／またはサービスプロバイダ（ＳＰ）に提供することにより、パーソナライズ機能を向上させ、および／または、サービスプロバイダ（ＳＰ）またはネットワークプロバイダ（ＮＰ）によって要求される情報を提供することを特徴とする請求項１ないし１８のいずれか１項に記載の方法。
【請求項２０】
ネットワークプロバイダ（ＮＰ）が、ネットワークアクセスのためのＷＬＡＮを提供することを特徴とする請求項１ないし１９のいずれか１項に記載の方法。
【請求項２１】
ネットワークプロバイダ（ＮＰ）と、サービスプロバイダ（ＳＰ）と、ユーザ装置と、ユーザのアイデンティティプロバイダ（ＩｄＰ）と、を有し、
前記サービスプロバイダ（ＳＰ）にアクセスすることを求めるユーザの要求によって、前記ユーザ装置と前記ネットワークプロバイダ（ＮＰ）との間にコネクションを確立し、
前記ネットワークプロバイダ（ＮＰ）の要求に応じて、前記アイデンティティプロバイダ（ＩｄＰ）が前記ユーザ装置を認証し、
前記サービスプロバイダ（ＳＰ）または第三者がアクセス料金の支払側であるという情報を前記ネットワークプロバイダ（ＮＰ）に与えるように、前記アイデンティティプロバイダ（ＩｄＰ）から前記ネットワークプロバイダ（ＮＰ）へデータを送信し、
前記ネットワークプロバイダ（ＮＰ）が、前記ネットワークプロバイダ（ＮＰ）経由で前記サービスプロバイダ（ＳＰ）へのアクセスを前記ユーザ装置に提供する
ことを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、請求項１に記載のネットワークプロバイダ（ＮＰ）経由でサービスプロバイダ（ＳＰ）へのネットワークアクセスをユーザに提供するプロセスに関する。
【背景技術】
【０００２】
現在、ネットワークアクセスは、それ自体がサービスとして扱われている。サービスプロバイダ（ＳＰ）にアクセスするために、ユーザは、ネットワークプロバイダ（ＮＰ）との間でセッションを確立し、十分な情報、あるいは、アクセスに課金するために必要な課金データを提供する必要がある。特許文献１は、現在の配備において実行される課金を示している。例えば、現在のＷｉＦｉホットスポット配備では、このセッションは、ＮＰに対する認証を通じて確立される。この確立は通常、ユーザが最初に外部ウェブページにアクセスしようとするときにユーザに提示されるポータルを通じて行われる。ＮＰは、ユーザに課金するために必要な課金情報も維持管理する。この情報は、ユーザの最初のアクセス中にアカウントが作成されたときに提供されたデータである。この課金情報は、ユーザとＮＰとの間の既存の契約のサブスクリプション情報であっても（例えばオペレータモデル）、クレジットカード番号や口座番号のような課金のためのバンキング情報であってもよい。
【０００３】
ユーザがホットスポットにアクセスするのは、複数のサービスを利用するため（これは

通常のインターネットモデルとして記述可能である）の場合もあれば、企業ＶＰＮへのアクセス、オンラインチェックインの実行、道順／地図の検索、書籍の購入、電子メールのチェック等のような単一のサービスを目的とする場合もある。本研究が対象とするのは後者、すなわち、単一のサービスにアクセスする場合である。従来の配備はインターネットモデルに有利である。この場合、ユーザは、アカウントの作成や課金情報の提供を主要な負担とはみなさない。しかし、この手順は、ユーザが単一のサービスにアクセスする場合には、特に次のことを考慮すると、実際的でない。すなわち、ユーザが単一のサービスにアクセスする際には、移動中、旅行中、および、スマートフォンのような限定的なインターネットデバイスの使用中であることが非常に多い。

【０００４】

いま述べた現在の傾向においては、ユーザは、新規電子メールや地図サービスでの道順のチェック、近所のレストランの検索、あるいは単に自動的なコンテキスト更新（すなわち、「私はいま街にいます」）のように非常にノマディックな形で、少量のデータのために各サービスにコンタクトする。これらの場合、ホットスポットサービスを使用すると、ユーザは、ネットワークプロバイダおよび目的のサービスプロバイダに対する認証のために、個人情報を２度提供することを要求されることになる。さらに、ユーザは、例えば自分のクレジットカード番号のようなデリケートな個人情報を、潜在的に未知の当事者の可能性のあるＮＰと共有しなければならない。これらの点は両方とも、ユーザにとって共通の欠点であり、ユーザは、サービスプロバイダにコンタクトすることを控えがちとなる。

【０００５】

したがって、本発明の技術的背景は次のようにまとめることができる。

・最近の傾向：
　－　アクセス設定の負担からユーザを解放する
　－　シンプルさを保つ：１つのボタンを押せばサービスが得られる
　－　多くのサービスを組み合わせて自分のサービスを作る
　－　一部のサービスは散発的であり、本質的に非常に特殊である
　　・例：「近所のレストランを検索」、「街まで道案内」、「映画の券を予約」
・現実：
　－　ユーザは依然として自分でアクセスする必要がある
　　・　複雑なホットスポットのアクセス手順
　　・　広帯域／低遅延サービス需要に適さない常時接続ＵＭＴＳ
　－　サービス集約のためにはプロバイダ間の合意が要求されることが多いが、そのような合意は利用可能でないことが多い
　－　ユーザは、アクセスしたいサービスとは無関係に、インターネットへの汎用接続を確立する

【０００６】

特許文献２には、通信サービスのためのポリシーベースの課金方法および装置が開示されている。この文献は、測定されたサービス品質水準および所定のＳＬＡに基づいて、通話に課金する方法を記載している。

【０００７】

特許文献３は、電話ネットワークにおいて使用するための統合課金システムおよび方法を示している。この文献は、通話、ボイスメール等のような複数のサービスに関する課金が、共通のユーザ課金に集約される方法を記載している。

【０００８】

特許文献４は、無線通信デバイスに対するサービスを認証する方法および装置を示している。この文献が特に対象としているのは、ローカルなコンテキスト（この場合には、使用されている実際のホットスポット）がリモートエンティティの決定における変数となる方法である。

【０００９】

特許文献５は、無線ＬＡＮサービス経由の企業アクセスに対する二重認証を除去する方

法および装置を示している。この方法によれば、ユーザの企業固有のクレデンシャルを用いて、単一の認証が実行可能となる。しかし、この方法は、企業ＶＰＮサーバへの制限されたアクセスを提供するために、ネットワークプロバイダと企業との間で合意を行う必要がある。

【００１０】

特許文献６は、無線ホットスポットへのアクセスを可能にし制御することを記載している。これに関して、従来の認証は、無線ユーザとネットワークプロバイダとの間で個人データが交換されることを要求する。

【先行技術文献】

【特許文献】

【００１１】

【特許文献１】米国特許第６８６２４４４Ｂ２号明細書
【特許文献２】米国特許第６７２１５５４Ｂ２号明細書
【特許文献３】米国特許第６２６６４０１Ｂ１号明細書
【特許文献４】米国特許出願公開第２００４／０１５２４４７Ａ１号明細書
【特許文献５】米国特許出願公開第２００５／０２１０２８８Ａ１号明細書
【特許文献６】米国特許出願公開第２００４／０２０３６０２Ａ１号明細書

【発明の概要】

【発明が解決しようとする課題】

【００１２】

本発明の目的は、ネットワークアクセスを提供するプロセスにおいて、単一のサービスを対象としてネットワークにアクセスするために使用可能なシンプルなネットワークアクセスプロセスを提供するような改良およびさらなる展開を行うことである。

【課題を解決するための手段】

【００１３】

本発明によれば、上記の目的は、請求項１の構成を備えた方法によって達成される。この請求項に記載の通り、本プロセスは、以下のことを特徴とする。すなわち、

サービスプロバイダ（ＳＰ）にアクセスすることを求めるユーザの要求によって、ユーザとネットワークプロバイダ（ＮＰ）との間にコネクションを確立し、

ネットワークプロバイダ（ＮＰ）の要求に応じて、ユーザのアイデンティティプロバイダ（ＩｄＰ）がユーザを認証し、

サービスプロバイダ（ＳＰ）または第三者がアクセス料金の支払側であるという情報をネットワークプロバイダ（ＮＰ）に与えるように、アイデンティティプロバイダ（ＩｄＰ）からネットワークプロバイダ（ＮＰ）へデータを送信し、

ネットワークプロバイダ（ＮＰ）が、ネットワークプロバイダ（ＮＰ）経由でサービスプロバイダ（ＳＰ）へのアクセスをユーザに提供する。

【００１４】

本発明によって認識されたこととして、非常にシンプルなネットワークアクセスプロセスにより、ネットワークプロバイダが、ユーザのアイデンティティプロバイダによって設定された第三者にアクセス料金を課金することを可能にするメカニズムが実現される。本発明は、サービスプロバイダまたは第三者が、その一部または全部の顧客のアクセス料金を負担することができるという特徴を備え、ユーザが直面する利用可能性の負担を低減することにより、ビジネスを拡大し、既存のネットワークプロバイダに対する新規な収益源を作り出す。サービスプロバイダまたは第三者がアクセス料金の支払側であることにより、ユーザはネットワークプロバイダの契約者である必要がないので、ネットワークアクセスは非常にシンプルになる。

【００１５】

好ましくは、前記プロセスは、ネットワークプロバイダ（ＮＰ）が支払側にアクセス料金を課金することをさらに含む。この場合、前記プロセスは、ネットワークプロバイダ（ＮＰ）が課金情報を含むオブリゲーション（obligation）を生成することを含んでもよい

。好ましくは、オブリゲーションを生成するポリシー決定技術はＸＡＣＭＬ技術である。いずれの場合でも、通常の利用可能性障壁が低減され、ユーザは、ネットワークプロバイダに直接に個人データを提供しないので、ネットワークにアクセスする際の懸念が少なくなる。

【００１６】

非常にシンプルな場合、アイデンティティプロバイダ（ＩｄＰ）はサービスプロバイダ（ＳＰ）であってもよい。

【００１７】

有利な態様として、認証ステップ中に、ネットワークプロバイダ（ＮＰ）が、ユーザに対して、自己のアイデンティティプロバイダ（ＩｄＰ）を指定するよう要求する。この場合、ネットワークプロバイダ（ＮＰ）は、ユーザが自己のアイデンティティプロバイダ（ＩｄＰ）を指定できるページへユーザをリダイレクトしてもよい。このステップ中に、ユーザは、アイデンティティプロバイダ（ＩｄＰ）に対して認証を行う。

【００１８】

好ましくは、アイデンティティプロバイダ（ＩｄＰ）からネットワークプロバイダ（ＮＰ）へ送信されるデータは、ネットワークプロバイダ（ＮＰ）によって作成されたコンテキスト、ユーザのポリシー、および／または、アクセスされるサービスプロバイダ（ＳＰ）のアイデンティティに基づく。支払側を選択するため、ネットワークプロバイダ（ＮＰ）とアイデンティティプロバイダ（ＩｄＰ）は、コンテキスト、ユーザのポリシー、および／または、アクセスされるサービスプロバイダ（ＳＰ）のアイデンティティを考慮してネゴシエーションをしてもよい。すなわち、支払側は、コンテキストおよび／またはユーザのポリシーに基づいて選択されてもよい。

【００１９】

認証ステップの後、アイデンティティプロバイダ（ＩｄＰ）は、好ましくは、ネットワークプロバイダ（ＮＰ）へユーザをリダイレクトする。

【００２０】

サービスアクセスのためのアクセス制御に関して、好ましくは、ネットワークプロバイダ（ＮＰ）は、ポリシー施行ポイント（Policy Enforcement Point，ＰＥＰ）として作用して、ポリシー決定要求を生成し、アイデンティティプロバイダ（ＩｄＰ）にコンタクトする。アイデンティティプロバイダ（ＩｄＰ）はポリシー決定ポイント（Policy Decision Point，ＰＤＰ）として作用することになる。この要求は、ＰＤＰが決定に到達することを可能にするコンテキスト情報を含んでもよい。

【００２１】

有利な態様として、ネットワークプロバイダ（ＮＰ）は、課金オブリゲーションまたはアイデンティティプロバイダ（ＩｄＰ）によって提供された情報について、支払側との間でネゴシエーションおよび／または確認を行う。前記ネゴシエーションおよび／または確認ステップ中に、支払および／またはサービスアクセスオプションを微調整してもよい。このステップは、支払側およびネットワークプロバイダ（ＮＰ）に非常に強く依存するので、どのようにそれを実現するかについては多くの相異なる可能性がある。

【００２２】

効率的な条件ネゴシエーションに関して、ネットワークプロバイダ（ＮＰ）および支払側またはサービスプロバイダ（ＳＰ）は両者とも、Ｐ３Ｐポリシーに関してサービスプロビジョニングの境界を提供する。このようなポリシーは通常、ユーザデータをどのように処理するかを伝えるために使用されるが、その使用は、サービス水準パラメータを決定するために拡張できる。Ｐ３Ｐを選択するもう１つの理由として、このポリシーは公開を意図しているので、ネットワークプロバイダ（ＮＰ）およびサービスプロバイダ（ＳＰ）の不正も抑制することがある。すなわち、Ｐ３Ｐポリシーは、サービス水準パラメータの決定および／またはアクセス条件のネゴシエーションのために使用可能である。

【００２３】

また、効率的でシンプルなネットワークアクセスに関して、支払側またはサービスプロ

バイダ（ＳＰ）はフィルタおよび課金情報に集中し、ネットワークプロバイダ（ＮＰ）は支払に集中してもよい。フィルタおよび課金情報、ならびに支払への集中の程度は、アプリケーションによって異なる。

【００２４】

また、ユーザに関する他の個人情報をネットワークプロバイダ（ＮＰ）および／またはサービスプロバイダ（ＳＰ）に提供することにより、パーソナライズ機能を向上させ、および／または、サービスプロバイダ（ＳＰ）またはネットワークプロバイダ（ＮＰ）によって要求される情報を提供してもよい。

【００２５】

非常にシンプルなネットワークアクセスに関して、ネットワークプロバイダ（ＮＰ）が、ネットワークアクセスのためのＷＬＡＮを提供してもよい。

【００２６】

本発明は、ネットワークプロバイダ（ＮＰ）が、ユーザのアイデンティティプロバイダ（ＩｄＰ）によって設定された第三者にアクセス料金を課金することを可能にするメカニズムを提供する。この決定は、コンテキストおよびユーザポリシーに基づいて実行される可能性もあるが、ほとんどの場合、サービスプロバイダ（ＳＰ）自身が、コストを負担する当事者となると予想される。この能力は、アイデンティティ管理プロトコルによるネットワークプロバイダとアイデンティティプロバイダとの間のインタラクションを拡張することによって利用可能となる。これにより、アイデンティティブローカ（Identity Broker，ＩｄＢ）が課金オブリゲーションを設定することが可能となる。この課金オブリゲーションは、ネットワークプロバイダがサービスプロバイダとの間でさらにネゴシエーションおよび確認をして、最終的にネットワークアクセスに課金するために使用する。原理的には、これらのメカニズムは、ユーザに関する他の情報をＮＰやＳＰに提供するためにも使用可能であり、それにより、パーソナライズ機能の向上、ＳＰまたはＮＰによって要求されるコンテキスト情報の提供等が行われる。

【００２７】

本発明の好ましい側面は以下の通りである。

・ネットワークプロバイダは、ユーザ認証中のサービスアクセスに関してサービスプロバイダに課金できる

・ユーザは、アクセス制御プロトコルに対するプライバシーポリシーを選択できる

・ネットワークプロバイダおよびサービスプロバイダは、アイデンティティ管理システムとは独立に、ネットワークアクセスに対する条件のネゴシエーションをすることができる

・新しいビジネスモデルに基づく

【００２８】

本研究は、ユーザが既に、アクセスしているサービスプロバイダ（航空会社グループ、オンラインショップ等）の顧客である場合がほとんどである、ということを考慮している。この場合、ユーザエクスペリエンスを向上させるために、サービスプロバイダ自身が、通常は自己のサービスへの付加価値として、ユーザに代わってアクセス料金を負担する場合が多く、またビジネスの観点からはそれが望ましい。これは、アクセスされるサービスに関して統一的な表示をユーザに提示することによって、サービスプロバイダに営業上の強みを与える。すなわち、ネットワークプロバイダとのコネクションを確立してからサービスにアクセスするという手順の代わりに、ユーザは、サービスに「直接に」アクセスすることで、サービスがどこでも利用可能であるという意識を生み出す。これは、サービスプロバイダおよびネットワークプロバイダの双方にとって有効に作用する。というのは、通常の利用可能性障壁が低減され、ユーザは、ＮＰに直接に個人データを提供しないので、ネットワークにアクセスする際の懸念が少なくなるからである。

【００２９】

本発明を好適な態様で実施するにはいくつもの可能性がある。このためには、一方で請求項１に従属する諸請求項を参照しつつ、他方で図面により例示された本発明の好ましい

実施形態についての以下の説明を参照されたい。図面を用いて本発明の好ましい実施形態を説明する際には、本発明の教示による好ましい実施形態一般およびその変形例について説明する。

【図面の簡単な説明】

【００３０】

【図１】アイデンティティプロバイダに対する認証後、課金情報を取得し、最後にサービスプロバイダにアクセスするという従来のネットワークアクセスを例示する図である。

【図２】アイデンティティプロバイダがコンテキストから課金当事者としての第三者を設定することが可能な、サービス結合課金の設定を例示する図である。

【図３】本発明の一実施形態によるネットワークアクセス提供プロセスを例示する図である。

【図４】本発明の一実施形態によるプロセスの要部を例示する図である。

【図５】本発明の一実施形態によるプロセスの要部を例示する図である。

【図６】本発明の一実施形態によるプロセスの要部を例示する図である。

【図７】本発明の一実施形態による基本プロセスを例示する図である。

【図８】本発明の一実施形態による，より詳細なプロセスを例示する図である。

【図９】本発明の別の実施形態を例示する図である。

【発明を実施するための形態】

【００３１】

図１は、アイデンティティプロバイダ（ＩｄＰ）に対する認証後、課金情報を取得し、最後にサービスプロバイダ（ＳＰ）にアクセスするという従来のネットワークアクセスを例示する図である。

【００３２】

図１において、ホットスポットで提供されるような従来のネットワークアクセスに対する１つのありふれた拡張として、次のようなものが考えられる。ネットワークへのユーザの最初のアタッチメントの一部として、ユーザは、アイデンティティプロバイダに対して認証を行うことにより、ネットワークプロバイダ（ＮＰ）は、アクセスに課金するための十分な課金情報を取得できる。この情報は、ユーザがネットワークプロバイダに対する有効なサブスクリプションを有するかどうかであってもよいし、ネットワークプロバイダがユーザに課金するために使用可能なバンキング情報（クレジットカード番号、銀行口座等）であってもよい。このモデルは、ネットワークにアクセスするユーザの意図に基づいており、この意図は、サービスへのアクセスによって決まる。

【００３３】

このモデルでは、ユーザは、ＮＰとの間で追加的なトランザクション（例えば契約の締結）を実行しなければならない。すなわち、このトランザクションに要求される個人情報とは別に、ユーザは、課金のために自己のバンキングの詳細（クレジットカード番号）もＮＰに提示する必要が生じる。

【００３４】

図２は、アイデンティティプロバイダがコンテキストから課金当事者としての第三者を設定することが可能な、サービス結合課金の設定を例示している。

【００３５】

本発明は、次の２つの点で、従来型のアクセスを拡張するものである。

・ユーザのアクションのコンテキストを保存する。もとの意図（サービスプロバイダにアクセスする）が、ポリシー作成プロセスに挿入される。また、位置のような追加的コンテキスト情報がＮＰによって追加されてもよい。ＮＰのアイデンティティは既に、ＮＰとＩｄＰとの間の通信から導出されている。

・アイデンティティプロバイダから課金情報を取得してユーザに直接に課金する代わりに、ネットワークプロバイダが、課金情報を含むオブリゲーションを生成する。

【００３６】

アイデンティティプロバイダＩｄＰへのこの問合せにより、ＩｄＰは、ＮＰによって作

成されたコンテキスト、ユーザのポリシー、アクセスされるサービスプロバイダのアイデンティティ等に基づいて課金情報を提供できる。

【００３７】

ＮＰがここで規定されるメカニズムをすべてサポートするとは限らない段階的な配備ストラテジをサポートするためには、ＩｄＰがＮＰの能力を推論するようにしてもよい。この場合、ＮＰが第三者への課金の委任をサポートするかどうかを推論してもよい。

【００３８】

ＮＰがこの能力をサポートしない場合には、ＮＰとＳＰとの間の仲介（ブローカー）を提供する新しい機能を導入することによって、このモデルは依然として配備することが可能である。このようなブローカーを規定することは本明細書の目的ではないが、原理的には、このブローカーは、課金限度に関する情報をＳＰから取得できる。この情報は、金額や期間のように単純であっても、（利用パターンに基づいて）より複雑であってもよく、ＮＰに対して、クレジットカード番号のような、課金に必要なバンキング情報を提供する。

【００３９】

他方、完全に準拠したＮＰは、アクセスに対して課金すべき当事者のアイデンティティと、この情報に関するユーザ制限とを受信できる。可能性の１つとして、課金情報は、最大のデータ総量や期限のような所定の適用有効性を有し、ユーザ自身が、不正なアプリケーションや類似の状況を低減するように、各アクセスをどのくらい利用するかの制限をしたい場合もある。課金・請求メカニズムは、ユーザのアイデンティティをＮＰから保護するためのプライバシープロトコルで強化されることも可能である。

【００４０】

アイデンティティ管理フレームワークを通じて、ＮＰは、課金当事者（ほとんどの場合には、アクセスされるＳＰ）との間にコネクションを確立でき、それにより、ＩｄＰによって提供された情報の確認および／またはネゴシエーションを行う。

【００４１】

このコンセプトは、一般化されたローミングサポートを提供するためにさらに拡張できる。ここで、アクセスされるサービスプロバイダ（ＳＰ）は、ユーザのホームネットワークプロバイダ（Home Network Provider，ＨＮＰ）である。この場合、ＨＮＰは、在圏ネットワークプロバイダ（Visited Network Provider）とともに課金を負担してから、従来のローミングで行われるのと同様に、ユーザに課金することになる。しかし、このコンセプトを採用すると、高度に動的なローミングフェデレーションが生じ得る。その場合、在圏ネットワークプロバイダとホームネットワークプロバイダとの間にはあらかじめ締結した合意が存在しない。その能力は、本明細書で提示される一般的な条件ネゴシエーションに委ねられる。

【００４２】

このコンセプトをサポートする４つの使用事例を以下に提示する。

【００４３】

オンラインチェックイン（マイレージサービス会員(Frequent flyer)）

ジョン・ドウ氏は、外国に滞在していて、地元の喫茶店で朝食をとっている。彼にとって運がよいことに、地域電話会社がＷｉＦｉホットスポットサービスを提供している。帰りのフライトが午後にあるので、この際、この機会を利用して、オンラインチェックインを行う。旅行に利用した航空会社グループのマイレージサービスの会員なので、そのクレデンシャルを用いて認証を行う。マイレージサービス会員であることの利益の１つとして、フライト時刻を取得しオンラインチェックインを行うためのネットワークアクセスの支払が挙げられる。そこで、航空会社のＩｄＰは、クレデンシャルと、その航空会社を支払側とする課金オブリゲーションとをネットワークプロバイダに提供する。ユーザは、自分の携帯電話を用いて、オンラインチェックインを完了することができる。

【００４４】

企業ＶＰＮアクセス

企業は、従業員のために企業ＶＰＮサービスにアクセス料金を支払う機能を提供する場合がある。同じメカニズムを用いて、ユーザは、企業のＩｄＰに対して認証を行う。その場合、ＩｄＰは、ユーザがＶＰＮへのコネクションを確立する際に、必要なクレデンシャルおよび課金オブリゲーションをネットワークプロバイダに提供する。このメカニズムは、モバイル端末が強力なデジタルアイデンティティ（例えばＴＰＭによるもの）を有する場合には、さらに拡張できる。その場合、このサービスは、企業のハードウェアの認証を通じて利用することも可能である。

【００４５】

Ａｍａｚｏｎ（登録商標）、オンラインショッピング

売上高を向上させるため、Ａｍａｚｏｎ（登録商標）は、顧客がある一定額の購入をする際に、ネットワークアクセス費用の負担を申し出ることによって、インターネットアクセスを拡大することが可能である。さらに、従来の顧客に対しては、顧客の購入履歴に基づいて、ユーザがストアを閲覧するために使用可能な一定の時間を提供してもよい。この提供は、時間等に基づいて、アクセス料金をＡｍａｚｏｎ（登録商標）が負担しない場合にはユーザが負担するように制限される。この配備は、ネットワークプロバイダとサービスプロバイダ（Ａｍａｚｏｎ（登録商標））との間での動的なネゴシエーションを利用して、ユーザプロファイルに基づいて最大の継続時間およびコストを設定する。認証およびネゴシエーションの標準的手段を使用し、Ａｍａｚｏｎ（登録商標）をアイデンティティプロバイダとして使用し、Ａｍａｚｏｎ（登録商標）の「Flexible Payments Service」のようなＡｍａｚｏｎ（登録商標）自身のウェブサービスを追加することによって、現在の技術を用いた配備が可能となる。

【００４６】

Ｎｅｔｆｌｉｘ（登録商標）、オンデマンドビデオサービス

Ｎｅｔｆｌｉｘ（登録商標）によれば、ユーザは、映画や、お気に入りのＴＶ番組の最新の回をレンタルし、自分の装置にコンテンツをストリーミングすることにより、自宅などＮｅｔｆｌｉｘ（登録商標）アカウントにアクセスできるところなら好きなところでそのビデオを見ることができる。しかし、高い帯域幅要求のため、このサービスはＵＭＴＳのようなモバイルネットワークには適していない。その理由には、技術的理由（メディアの特性）と経済的理由（定額制が利用可能でない場合）の両方がある。同時に、ユーザがかなりの時間を過ごすホテル（ホテルの部屋を含む）、空港、駅、喫茶店等のレジャーエリアにはホットスポットが特に普及している。このようなサービスにアクセスするには、ユーザは、通常であれば、Ｎｅｔｆｌｉｘ（登録商標）契約に加えて、ホットスポットアクセスのための高額な料金を支払わなければならない。この使用事例では、ユーザ、例えば顧客との会議に向かう出張中で疲れたビジネスマンは、ホテルのバーでお気に入りの連続ドラマを確認したり、自室で寝る前に映画を見たりすることができる。これはすべて、彼のＮｅｔｆｌｉｘ（登録商標）契約の一部である。彼は、どのホットスポットに接続しても、そのホットスポットで複雑で高価な契約に煩わされずにコンテンツにアクセスできる。また、インタフェースは彼のためにパーソナライズされているので、ホットスポットや場所に関係なく、インタフェースは、ＳＰによって提供される慣れているインタフェースである。Ｎｅｔｆｌｉｘ（登録商標）は、バックグラウンドで、前の使用事例と同様にＮＰへのトランスポートコストを負担し、より包括的な一連の契約クラスをユーザに提供する。

【００４７】

図３は、ネットワークプロバイダ（ＮＰ）経由でサービスプロバイダ（ＳＰ）へのネットワークアクセスをユーザに提供するプロセスの一実施形態を例示している。本具体例では、一般性を失うことなく、マイレージサービス会員の使用事例に注目することにする。なお、本具体例は、ｈｔｔｐサーバを通じて利用可能なウェブサービスにアクセスするために通常のＷｉＦｉホットスポットを使用する場合である。

【００４８】

サービスアクセスに関する手順を、認証、アクセス制御、および条件ネゴシエーション

という３つの異なる部分に分けることができる。

【００４９】

ユーザの端末は使用可能状態であり、ネットワークアクセスが公衆ホットスポットを用いて設定されている（これは、端末のサポートソフトウェアによって自動的に行われているとしてもよい）と仮定する。アイデンティティプロバイダをも利用した、より複雑な発見メカニズムもまた、このセットアップ段階の一部であってもよい。

【００５０】

（１）ユーザが http://airline.com にアクセスを試みる

ユーザは、ブラウザを開き、航空会社のウェブサイト（本具体例では、http://airline.com）を開こうと試みる。サービスとの間にＨＴＴＰコネクションが確立される。しかし、ホットスポットは透過型プロキシを使用しており、ＨＴＴＰコネクションはすべて、ゲートウェイにおけるポリシールールによって、このプロキシにリダイレクトされる。このプロセスは、従来のホットスポット技術と同様である。

【００５１】

（２）認証が要求される

ユーザは現在認証されていないので、プロキシは、ユーザが自分のアイデンティティプロバイダを指定できるページへユーザをリダイレクトする。ここで、ホットスポットゲートウェイは、ユーザごとに、そのユーザのセッションに基づいて、ユーザが認証済みか否かを確認できると仮定する。ＮＰのページで、ユーザは、自分の航空会社／マイレージサービスのアイデンティティプロバイダを指定する。その後、ユーザは、マイレージサービスのログインページへリダイレクトされる。

【００５２】

別法として、ユーザは、自分のマイレージサービス会員アイデンティティについて知っている第三者アイデンティティプロバイダを指定してもよい。

【００５３】

（３）認証およびプライバシーオプション選択

ユーザは、アイデンティティプロバイダで自己の認証クレデンシャルを入力し、追加のプライバシーオプションがあれば指定する。これらは、条件ネゴシエーションがアイデンティティプロバイダによって行われるかネットワークプロバイダによって行われるを含めて、ネットワークプロバイダがアクセス可能な情報の量を制限するために使用可能である。本具体例では、ユーザは、追加のプライバシーオプションを指定していない。

【００５４】

（４）アクセス制御

ユーザを識別する認証コンテキストを取得した後、プロキシは、ユーザのＩｄＰに情報を問い合わせることができる。プロキシは、自分自身によって施行されるポリシーを設定するために、ＩｄＰに問合せを行う。この問合せにおいて、ネットワークプロバイダが最初のコンテキストを提供する。このコンテキストは、サービス（いまの場合はＨＴＴＰ）およびユーザが到達しようと試みたＵＲＬを含む。ＩｄＰからのＰＤＰ（ポリシー決定ポイント）応答として取得される情報は、オブリゲーション情報を含む。この情報により、プロキシは、支払人と、アクセス権限への制約（例えば、当該マイレージサービスドメインへの通信のみが許可される）とを確認できる。このネットワークアクセスに対する支払人を確認するため、アイデンティティプロバイダは以下のステップに従う。

【００５５】

・ユーザがアクセスしているＵＲＬが、マイレージサービスの範囲内のＵＲＬであるか確認する。

・ネットワークプロバイダのアイデンティティで既知の信頼チェインをチェックする。ユーザと全く同様に、航空会社は、ネットワークプロバイダが信頼でき、ユーザのデータに対する正当なハンドラであることを確かめなければならない。

【００５６】

これら２つのステップがＩｄＰによって正しく処理されると、ＩｄＰは、航空会社財務

部のアイデンティティをこの通信の支払側として、そのアイデンティティをネットワークプロバイダに応答する。

【００５７】

（５）ポリシー決定チェック

応答を受信すると、ネットワークプロバイダは自ら、その情報が、現在設定されているポリシーと、および設定されている信頼水準と両立可能か（特に、このトランザクションの支払側を信頼してもよいかどうか）を確認する。ネットワークプロバイダは、航空会社財務部のアイデンティティを支払側として読み出し、合意のある主要なクレジット会社によって支持されていることを確認する（なお、ネットワークプロバイダの財務部自体が相手方と合意を有していてもよいが、課金プロセスを支える信用は、本明細書に記載される手順にとって本質的ではない）。

【００５８】

（６）条件ネゴシエーション

次にネットワークプロバイダは、予想される料金を航空会社財務部に通知する。その後、支払額および支払時期について合意するために両者によるネゴシエーションが行われる。ここで、両者間における条件の事前設定等、サービスプロバイダにとって課金処理簡略化およびコスト低減となるいくつかの可能性がある。また、このネゴシエーションおよび課金は、第三者課金ブローカを通じて行うことが可能であるとも考えられる。このブローカは、さまざまな国のコストや通貨等に関する情報を維持管理する。ＳＰによって提供される（いまの場合は、航空会社の財務部によって仲介される）応答の一部は、通信の限度および可能な最大時間、最大データ量、および最高支払額を含むとよい。

【００５９】

（７）サービスアクセス

最後に、ユーザは、航空会社のウェブサイトにアクセスすることができる。

【００６０】

例示した実施形態をより良く理解するため、以下に各ステップを再度まとめる。

（１）サービスへのアクセスおよびハイジャック

ユーザがＳＰに接続し、ｈｔｔｐはハイジャックされる（ホットスポットと同様）。

（２）アイデンティティプロバイダの認証

ユーザは認証のためにＩｄＰへリダイレクトされる。

（３）サービスアクセスのためのアクセス制御

トランスポートまたはネットワークプロバイダがＩｄＰとの間でアクセス条件を確認する。

（３ａ）任意：条件ネゴシエーション

トランスポートまたはネットワークプロバイダがＳＰとの間で課金オプションを確認し、アクセス条件を微調整する。

（４）サービスへのアクセス、およびアクセス確認

任意：ＳＰは、ユーザがＮＰのサービスアクセス条件下でサービスにアクセスしたことがあるかどうかをチェックすることができる。

【００６１】

以下、本発明によるプロセスの一実施形態をさらに詳細に説明する。

【００６２】

１）サービスへのアクセスおよびハイジャック

このステップで用いられる技術は周知である。まず、多くのホットスポットで行われているのと同様に、透過型プロキシを用いてｈｔｔｐコネクションをハイジャックする。すると、ユーザにはホットスポットのウェブページが提示される。ユーザが自己のＩｄＰ情報を提示するか、またはそれが自動的に取得されて、ユーザはＩｄＰへリダイレクトされる。

【００６３】

２）アイデンティティプロバイダの認証

このステップにおいても、技術は周知である。ＩｄＰは、ユーザのみが有する情報、例えば、ログインおよびパスワードを要求することによって、またはＳＩＭカード認証によって、ユーザの真正性を調べる。

【００６４】

３）サービスアクセスのためのアクセス制御

ユーザのＩｄＰを知ると、ＮＰは、アクセスについて問い合わせることができる。ＮＰは、ＰＥＰ（ポリシー施行ポイント）として作用して、ポリシー決定要求を生成し、ＩｄＰにコンタクトする。ＩｄＰはＰＤＰとして作用することになる（アクセス制御フレームワークの一例として、ＯＡＳＩＳ　ＸＡＣＭＬ（http://www.oasis-open.org/committees/xacml/ で入手可能）を参照）。この要求は、ＰＤＰが決定に到達することを可能にするコンテキスト情報を含む。また、ＩｄＰは、ステップ２）で取得されるアサーションのような、ＮＰがユーザを有することの証明を施行してもよい。要求を処理した後、ＩｄＰは、以下で説明するようなオブリゲーションを含むポリシー決定を提供する。このオブリゲーションは、支払およびプロトコルのネゴシエーション段階に関する情報を含んでもよい。ＮＰがこの要求におけるすべての情報に満足した場合、ステップ４）は省略できる。

【００６５】

上記の例のオブリゲーションは、ＩｄＰからの応答の一部であるが、ネゴシエーション段階がどのようにして始まり得るかに関する情報（これは、ユーザおよびＳＰエンドポイントを指定するために使用できる）、支払に関する情報（ここでは、ＳＰが支払ってもよい金額）（１回払い、料率、価額、課金情報）、およびその料率でサービスに対して施行されることになる制約、を含む。

【００６６】

このオブリゲーションの例は、読みやすくするために簡略化してあり、スキーマ定義を通らないであろう。属性のデータ値はシリアライズしなければならない。

【００６７】

４）条件ネゴシエーション

このステップは、ＳＰおよびＮＰに非常に強く依存するので、どのようにそれを実現するかについては多くの相異なる可能性がある。

【００６８】

このステップでは、ＳＰおよびＮＰの両者が、支払およびサービスアクセスオプションを微調整できる。前項で指定された属性のすべてが当てはまるが、ＱｏＳ等の他の属性を追加することも可能である。

【００６９】

３）に含まれるオブリゲーションの提供する情報が少ないほど、より強力な条件ネゴシエーションを必要とする。ステップ３）が満足な場合、このステップは省略できる。ＳＰおよびＮＰは、サービスプロビジョニングに対する最低限のバインディングを選択する。これにより、ＳＰのためのコストおよびＮＰでのリソースが低減されるからである。

【００７０】

上記の例では、ＮＰおよびＳＰは両者とも、Ｐ３Ｐ（Platform for Privacy Preferences）ポリシーに関してサービスプロビジョニングの境界を提供する。このようなポリシーは通常、ユーザデータをどのように処理するかを伝えるために使用されるが、ここでは、サービス水準パラメータを決定するためにそのようなポリシーの使用を拡張する。Ｐ３Ｐを選択するもう１つの理由として、このポリシーは公開を意図しているので、ＮＰおよびＳＰの不正も抑制することがある。

【００７１】

Ｐ３Ｐを用いた例からわかるように、ＳＰはフィルタおよび課金情報（実際の情報ではなく、権限のある当事者にとってどこでそれが取得可能かということ）に集中し、ＮＰは支払に集中する。

【００７２】

図４および図５を参照。

【００７３】
ＳＰからポリシーを取得した後、ＮＰは、それが自己のポリシーと両立可能かどうかをチェックする。両立可能な場合、指定されたアクセス制限が配備され、ユーザはＳＰにコンタクトすることが許可される。ＳＰがＮＰの提案に同意しない場合には、ユーザがＳＰのページに到達した後、ＳＰはアクセスをローカルに拒否できる。
【００７４】
なお、ＳＰおよびＮＰは、同時に相互にプライバシーポリシーのネゴシエーションをすることも可能であるが、これは本発明の範囲外である。
【００７５】
このステップの他の可能性には、ネゴシエーションステップに対する独自仕様のソリューションも含まれる。
【００７６】
５）サービスへのアクセス、およびアクセス確認
上記のステップがすべて完了した後、ユーザがＳＰのウェブサイトにログインすれば、ＳＰはＮＰへの支払を許可することができる。ログイン手順は、ＩｄＰに対する前の認証に基づくことができるので、ユーザにとって透過的となる。
【００７７】
図６を参照。
【００７８】
以下、本発明の一実施形態を再び、より詳細に説明する。
【００７９】
図３は、メッセージが交換されるプロトコルの実施例の図を示している。プロトコルフローは、上記の具体例に従っているが、このセクションでは一般化され、さらに詳細に記載されている。
【００８０】
この場合、相異なる動作プロバイダによって所有される相異なる機器がこれらの交換中に相互作用するので、標準化が特に重要である。ＳＡＭＬ仕様が、ＨＴＴＰとともに用いるために必要なバインディングおよびプロファイル拡張を既に定義している。同じ能力を提供するＳＩＰに対する拡張がＩＥＴＦ［ＳＩＰ　ＳＡＭＬ］に提案されている。他のトランスポートは、標準化のために特定の拡張を必要とする場合がある。
【００８１】
サービスアクセス
サービスへのアクセスは、サービス固有のプロトコルを用いて実行される。ほとんどの場合、上記の具体例のように、これはＨＴＴＰを通じて行われるが、ローミングをサポートするためのＳＩＰに基づくサービスのような他のサービスも排除されない。システムは、他のサービスプロトコルに対するアイデンティティプロバイダからのサポートに強く依存する。しかし、ＳＩＰに対する［ＳＩＰ　ＳＡＭＬ］のように、（ＨＴＴＰ以外の）他のサービスとともに使用するために必要なＳＡＭＬのバインディングおよびプロファイル拡張が、引き続き導入される。
【００８２】
サービスアクセスのため、ここで処理されるメッセージは、使用されるサービスプロトコルの最初のメッセージであると仮定する。このメッセージは、ＨＴＴＰの場合であればＨＴＴＰ　ＧＥＴ、ＳＩＰではＳＩＰ　ＲＥＧＩＳＴＥＲメッセージ、等となる。
【００８３】
サービスアクセスメッセージの横取りおよび処理
このステップもまた本明細書の範囲外であるので、ネットワークプロバイダがユーザのＩｄＰを知るためのメカニズムは指定しない。しかし、以下で、従来の技術および新しい標準化作業に基づく２つの提案を示す。一方はＨＴＴＰの場合であり、他方はＳＩＰの場合である。
【００８４】

ほとんどのホットスポットと同様、サービスアクセスメッセージは、サービスアクセスに対する支払のいくつかの選択肢をユーザに提示するために、ネットワークプロバイダによって横取りされる。ここでは、ネットワークプロバイダが、ユーザのアイデンティティプロバイダを識別するオプションを含む場合を提案する。ＨＴＴＰでは、これは、ユーザをあるウェブページへリダイレクトすることになる。このウェブページで、ユーザは、フォームに入力することにより、自己のＩｄＰをネットワークプロバイダに対して示すことができる。ＳＩＰでは、同じ機能を、ＳＩＰ　ＵＡによって挿入される特別のヘッダによって提供できる。この挿入は、接続失敗時に、あるいはインターネットアクセスの欠如をアプリケーションが検出できる場合には事前に、行われる。この特別のＳＩＰヘッダの使用についてさらに詳細な説明は、［ＳＩＰ　ＳＡＭＬ］ＩＥＴＦ草案で見ることができる。

【００８５】

他のタイプのサービストランスポートの場合、ユーザのＩｄＰをＮＰに通知するための適切なメカニズムを導入しなければならない。

【００８６】

ＩｄＰ認証リダイレクト

以下では、ＨＴＴＰ、ＳＩＰ、あるいはその他のプロトコルのいずれが使用されるかをもはや指定せず、一般的な場合を考える。実際、交換されるメッセージは、ＨＴＴＰやＳＩＰ、あるいはその他のトランスポートプロトコルとは独立である。これらのプロトコルをこれらの２つのバインディングにどのように適用するかについての詳細に関して、読者は、［ＳＡＭＬ］仕様または［ＳＩＰ　ＳＡＭＬ］草案を参照されたい。サービスが異なる種類のものである場合、適切なＳＡＭＬのプロファイルおよびバインディングを検討しなければならない。バインディングおよびプロファイルが存在すれば、以下の説明が当てはまる。

【００８７】

ＮＰは、ユーザのＩｄＰを知った後、認証問合せ手順を開始できる。ＮＰはＳＡＭＬ認証要求メッセージを作成し、それをＩｄＰへのメッセージに埋め込む。多くのプロファイルでは、これにより、ユーザが処理すべきリダイレクトメッセージが得られる。ＮＰは、その認証要求を有するＩｄＰへユーザをリダイレクトする。

【００８８】

認証および任意のプライバシーオプション選択

通常のＳＡＭＬモデルと全く同様に、ＩｄＰに認証コンテキストが既に存在するのでなければ、ユーザは、ＩｄＰに対して認証を行わなければならない。実際の方法は定義されていないが、例えば、ログインおよびパスワードや、証明書を用いたチャレンジ－レスポンスが使用可能である。

【００８９】

このステップにおいても、ユーザは、利用可能であれば、自己のプライバシーオプションを選択できる。このようなオプションは、サービス品質や、サービスへのアクセスにも影響を及ぼす可能性がある。このステップの目的は、プライバシー拡張を容易にすることである。その場合、ユーザは、アクセス制御プロセスの一部として、アイデンティティプロバイダに自己のコンテキストの一部を提供しないことを選択してもよい。

【００９０】

当該コンテキスト情報は、ユーザのデバイス情報、デバイスの位置、ネットワーク事業者のローカル情報、アクセスされるサービス、およびその他多くを含んでもよい。

【００９１】

ＩｄＰは、ＮＰがユーザのポリシーに従うかどうかを確認する監査ツールとして作用することができる。

【００９２】

プロキシ認証リダイレクト（認証応答）

ユーザが認証された後、ＳＡＭＬモデルによれば、ＩｄＰは、今度はユーザをＮＰへリ

ダイレクトして戻すことになる。このＳＡＭＬメッセージに含まれる情報は、認証コンテキストと、ユーザが選択したプライバシーオプションとに関するものである。

【００９３】

現在、プライバシーオプションは、ＳＡＭＬの一部として標準化されていないので、それらをユーザの属性とみなすことにする。それらを通常の属性アサーションとしてＳＡＭＬメッセージに埋め込むことができる。

【００９４】

プライバシーポリシー自体は、多くの方法で指定できる。簡単のため、Ｗ３Ｃ　Ｐ３Ｐ［Ｐ３Ｐ］の使用を仮定する。これは、情報の開示および処理を記述するためのシンプルなメカニズムである。

【００９５】

メッセージが受信されると、プロキシは、ＳＡＭＬ認証応答メッセージ内のアサーション中の署名と、認証コンテキスト内の認証方法が承諾可能かどうかとを確認する。その後、Ｐ３Ｐポリシーと、それらのポリシーがＮＰにとって承諾可能であるかどうかとを確認する。

【００９６】

ＮＰは、これがアクセス制御部にとって十分ではないと判断した場合、認証ステップに戻り、再認証をさせる。ただし、認証要求には自己のＰ３Ｐポリシー提案を埋め込む。プライバシーポリシーに関するＮＰの想定がユーザに通知されるべきであることを除き、この時点までの他のすべてのことが継続されることになる。

【００９７】

プライバシーポリシーがユーザおよびＮＰの双方の要求に従う場合、サービスへのユーザのアクセスの処理を続行できる。

【００９８】

ポリシー決定問合せ

ネットワークへのアクセスを可能にするため、ＮＰは、ユーザが正しい権限、または支払方法を有することをＩｄＰとの間で確認しなければならない。このステップでは、汎用のアクセス制御フレームワークである［ＸＡＣＭＬ］を利用する。ＸＡＣＭＬの選択は、ＳＡＭＬとの長期の関係によるものである。ＳＡＭＬおよびＸＡＣＭＬはともに、ＸＡＣＭＬのポリシー決定問合せおよびポリシー決定応答のトランスポート、ポリシー決定の仕様および処理を提供する。

【００９９】

ＸＡＣＭＬポリシー決定問合せは、ポリシーが評価される際のコンテキストと、ポリシー決定ポイント（ＰＤＰ）（いまの場合はＩｄＰ）でのみインスタンス化可能ないくつかの変数とを含む。

【０１００】

コンテキスト情報の例として、以下のものが挙げられる。

－　ユーザがアクセスしようとしているサービスに関する情報
－　ユーザまたはＮＰによって与えられる、ユーザの位置
－　ユーザのデバイス／アプリケーションに関する情報
－　その他

【０１０１】

ポリシー要求内の変数に関しては次の通り。

－　年齢、性別、選好等のようなユーザの属性
－　時刻、日付、地域／タイムゾーン
－　課金プロバイダに関する情報
　・優先順のリスト
　・名称、提携先、グループ等
　・国
　・財務データ

－　その他
【０１０２】
ＰＤＰ（ＩｄＰ）は、このメッセージを受信すると、自己の内部ポリシーに従ってそれを処理する。そのようなポリシーは、アクセスコンテキストをユーザ属性（例えば、サブスクリプション、課金プロバイダ、および選好）にどのように結合するかに関する情報を含んでもよい。これらのポリシーに従って応答が作成される。これは、ＸＡＣＭＬオブリゲーションのような、決定における追加情報を含んでもよい。決定は、ＮＰがアクセス要求の承諾（ＡＣＣＥＰＴ）、ネゴシエーション（ＮＥＧＯＴＩＡＴＥ）、または拒否（ＲＥＪＥＣＴ）を行うのに十分でなければならない。メッセージはＮＰによって署名される。
【０１０３】
課金オブリゲーション定義
このセクションでは、ＸＡＣＭＬポリシー決定応答内の課金情報およびパラメータを含む仕様を提案する。このオブリゲーションは、ＳＡＭＬアサーションのようなデータ、または、ＳＡＭＬアーティファクトのような情報へのポインタを含むことができる。ポインタは、ポリシーが施行される前に解決されなければならない。
【０１０４】
このアサーションに含まれる情報は、
－　課金プロバイダネゴシエーションポイント（プロトコルを含む）を含まなければならない
または
－　直接課金情報（すなわち、クレジットカード詳細等）を含まなければならない。
－　情報は、課金プロバイダまたは他の適当な認定ソースによって表明されなければならない
－　プロバイダに関する次のような情報を含んでもよい
・名称、アドレス等
・提携先、グループ等（例えば、クレジットカード、ｐａｙｐａｌ（登録商標）、銀行、事業者等）
・認定
－　最大リスク因子（支払限度額等）を含んでもよい
【０１０５】
ポリシー決定応答
ポリシー施行ポイント（ＰＥＰ）（いまの場合はＮＰ）は、ＩｄＰから決定を受信する。この場合も、この決定は、ＳＡＭＬ　ＸＡＣＭＬに従って処理されなければならない。これは署名確認を含む。
【０１０６】
応答が、承諾（ＡＣＣＥＰＴ）またはネゴシエーション（ＮＥＧＯＴＩＡＴＥ）の肯定応答を含む場合、ＮＰは、オブリゲーションセクションが存在するかどうかをチェックしなければならない。その後、ＮＰは、決定のオブリゲーションに対して自己のポリシーエンジンを作用させ、これが満足かどうかを確認できる。この時点で、決定がサービスアクセスの処理の継続である場合、アクセスに対する条件ネゴシエーションが必要な場合もある。
【０１０７】
条件ネゴシエーション
次に、ＮＰは、ネットワークアクセスサービスの課金に必要な情報およびその他のパラメータを列挙したＰ３Ｐポリシーを準備することができる。パラメータとしては以下のものが挙げられる。
－　ユニット、セッション、契約あたりの価格
－　リスク管理
・支払前の最大転送データ

・最小許容支払額
・頭金
－　ＳＰとＮＰとの間の契約の場合や、新たなフェデレーションを設定するための合意情報
－　サービスに対する制限
・時間、帯域幅、サービス等

【０１０８】
ＩｄＰから受信されるユーザの認証アサーションは、プロセスにおけるユーザおよびＩｄＰの関与を証明するために、最初のネゴシエーションメッセージに含まれてもよい。このパラメータは、ＳＰによって、Ｐ３Ｐポリシーにおいて要求される場合もある。

【０１０９】
これらのパラメータは、Ｐ３ＰポリシーとともにＳＰとの間で交換される。そして、ＳＰは、自己の値を提案し、合意が達成されるまで、他のパラメータを提示してもよい。

【０１１０】
合意が達成できない場合、例えば、２つの連続する交換で変化がない場合、この方法ではサービスは達成できず、提案がユーザに提示されてもよい（すなわち、ユーザが自分で支払をしなければならない）。

【０１１１】
そうでない場合、プロセスは次のステップに進む。

【０１１２】
サービスプロバイダリダイレクト（権限のあるサービスアクセス）
ＮＰは、支払について確認した後、ユーザをＳＰへリダイレクトする。これは、ＳＰが認証を要求する場合には、ＩｄＰへの新たな呼び出しを必要とするかもしれないが、システムのＳＳＯは、ユーザインタラクションなしでこれが行われることを許可すべきである。
ユーザはサービスにアクセスする。

【０１１３】
サービスプロバイダ合意妥当性検査
オプションとして、ネゴシエーションが終結した後、またはＩｄＰのトリガによって、ＳＰは、ユーザおよびアクセスサービスプロビジョニングの条件をＮＯ　ＳＨＯＷステートメントとともに列挙したエントリを作成する。このエントリは、タイマと関連づけることができる。このタイマは、ユーザがある一定時間後にサービスにアクセスしない場合に、このエントリをＦＡＩＬＥＤステートメントでマークする。

【０１１４】
ユーザが最初にＳＰにアクセスすると、ＳＰは、このエントリにＣＯＭＳＵＭＥＤとタグ付けすることができる。オプションとして、ＳＰは、サービスが実際にこのように利用されたことをユーザに対して証明するために、ＳＰへのユーザログイン時にＩｄＰから受信した認証アサーションを保存することにしてもよい。このステップは、ユーザがこのようにサービスを利用するためにＳＰによって信用される場合に有益である。第３のシナリオ、すなわちローミングは、これが起こる典型的な使用事例である。

【０１１５】
ＮＰがＳＰに課金すると、ＳＰは、エントリのステータスをチェックして、課金に異議を唱えることができる。

【０１１６】
システムのこのセクションの実装は、ＳＰのリスク管理メカニズムに依存する。

【０１１７】
図７は、本発明の一実施形態の重要な特徴を例示している。
・ユーザがサービスにアクセスし、ホットスポットプロバイダによるリダイレクトを通じてアイデンティティプロバイダ（ＩｄＰ）に対して認証を行う
・ユーザポリシーは、ホットスポットプロバイダによって問合せを受けると、ＳＰを支

払人として設定する
・サービスプロバイダとホットスポットプロバイダとの間のネゴシエーションにより、課金の詳細を設定する
【０１１８】
図８は、さらなる詳細および利点を例示している。
・ユーザが、サービスプロバイダ（ＳＰ）のブックマークを選び、近くのホットスポットを選択する（自動でもよい）
・ＩｄＰが、ホットスポットのポリシー問合せを通じてＳＰのアイデンティティを知る
・ＩｄＰは、ユーザがＳＰとのサブスクリプションを有することを知る
【０１１９】
ＳＰは、ＩｄＰによって提供されるポリシーに基づいて、ユーザのネットワークアクセスに対して課金される。
・コンセプトの利点：
－　収益：ホットスポットが、より多くの顧客によってアクセスされる
－　顧客ベースの拡大：ＳＰが、より多くのユーザを獲得する。付加価値サービス
－　信頼：ユーザが、一貫したシンプルなサービスの表示を得る
【０１２０】
図９は、ステップの動きを例示している。
【０１２１】
以下、本発明の重要な側面について要約する。
・アイデンティティ管理とアクセス制御技術との新たな組合せにより、ネットワークトランスポートの第三者支払が可能となる。
・ユーザに対するプライバシーオプションを含むように認証段階を拡張する。
・Ｐ３Ｐポリシーの新たな応用により、ＮＰとＳＰとの間でアクセス条件のネゴシエーションを行う
・ネットワークプロバイダは、ユーザ認証中のサービスアクセスに対してサービスプロバイダに課金できる。
・ユーザは、アクセス制御プロトコルに対するプライバシーポリシーを選択できる。
・ネットワークプロバイダとサービスプロバイダは、アイデンティティ管理システムとは独立に、ネットワークアクセスに対する条件のネゴシエーションをすることができる
・新規なビジネスモデルに基づく
【０１２２】
従来技術と比較した本発明の利点は次の通りである。
【０１２３】
特許文献６、特許文献４、および特許文献１に対して、本発明は、支払人の認証および設定の両方をアイデンティティプロバイダに委任するようにこれらのメカニズムを拡張し、それにより、Ｉｄブローカに保存された事前設定情報に基づいてサービスごとのポリシーを効果的に設定できる。ネットワークプロバイダは、ネットワークアクセスに対してサービスプロバイダに課金でき、ユーザ認証中に支払人のアイデンティティを確認し、それによりユーザのプライバシーを保護する。これは、ＮＰに個人データを開示しない。現在のモデルでは、ユーザは、ネットワークプロバイダおよびサービスプロバイダとの間で個別に、自己のそれぞれの契約またはサブスクリプションを利用できるだけである。
【０１２４】
さらに、課金メカニズムの共通理解をのぞき、プロバイダ間の事前合意（ＳＬＡ）やその他の知識は不要である。特許文献５に記載されているようなメカニズムでは、限定的なサービスにしかアクセスできず、この場合、ホットスポットプロバイダは、事前合意を通じて、特殊な認証およびユーザに利用可能なサービスについて知っている。本発明には、このような制限は何ら課されない。
【０１２５】
特許文献３および特許文献２に記載されているような従来の技術は、特定のサービスサ

ポートをシステムに組み込まずにさらに拡張される。このため、本発明者によって提示されるもの以外にも、任意の変更を、現在および将来の課金方法に組み込むことが可能である。具体的には、本発明によって使用されるプロトコルでは、動的なポリシー構築に基づいて、ＮＰとＳＰとの間で新たな種類のオブリゲーションを定義することが可能である。

【０１２６】

本発明は、ユーザのアイデンティティへのリンクを提供し、その後に課金プロバイダへのリンクを提供するために設定されるアイデンティティ管理システムにある程度依存する。しかしこれは強い要件ではない。というのは、この役割は、サービス合意に応じて、ＳＰまたは他の第三者が引き受けることができるからである。

【０１２７】

上記の説明および添付図面の記載に基づいて、当業者は本発明の多くの変形例および他の実施形態に想到し得るであろう。したがって、本発明は、開示した具体的実施形態に限定されるものではなく、変形例および他の実施形態も、添付の特許請求の範囲内に含まれるものと解すべきである。本明細書では特定の用語を用いているが、それらは総称的・説明的意味でのみ用いられており、限定を目的としたものではない。

【図１】

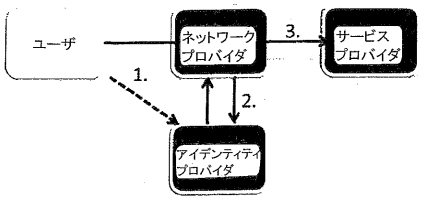

Fig. 1

【図２】

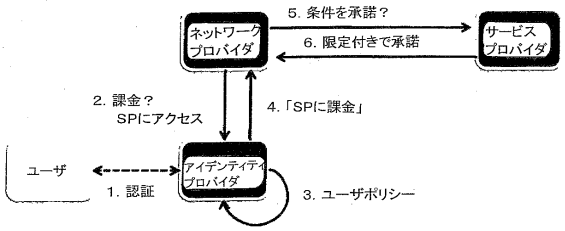

Fig. 2

【図３】

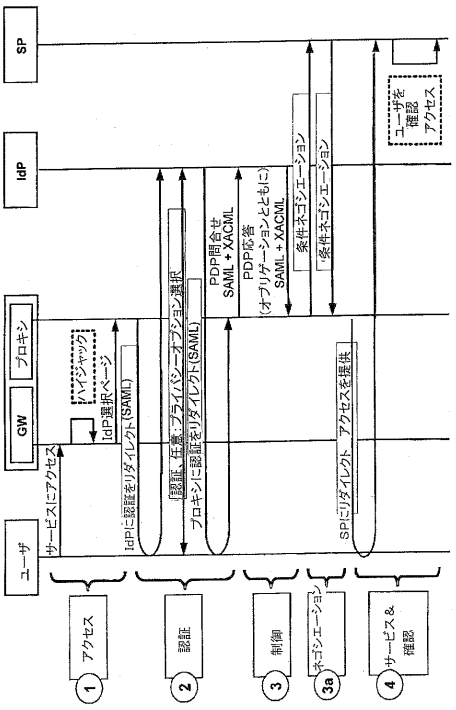

Fig. 3

【図４】

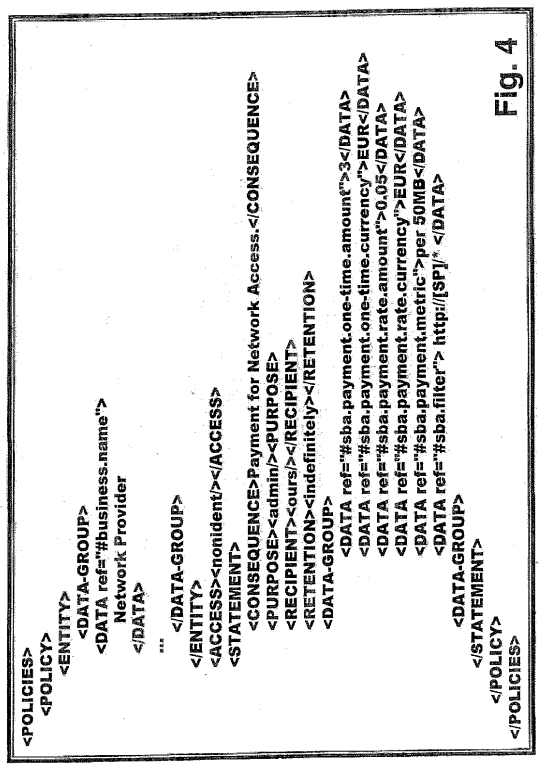

Fig. 4

【図５】

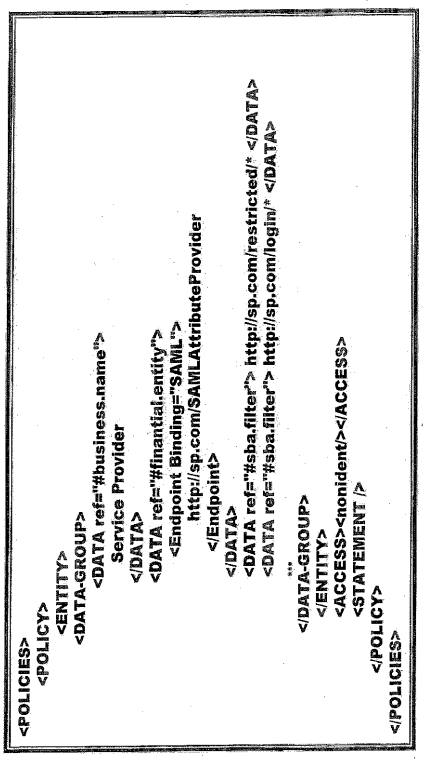

Fig. 5

【図６】

```
<Obligations>
  <Obligation
      ObligationId="eu:neclab:nw:sba:obligation"
      FulfillOn="Permit">
      <AttributeAssignment
          AttributeId="eu:neclab:nw:sba:obligation:subject"
          DataType="urn:oasis:names:tc:SAML:2.0:assertion:NameID">
          <saml:NameID
                  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                  Format="http://www.w3.org/2001/XMLSchema#anyURI">
                  temporary-subject@sp.com
          </saml:NameID>
      </AttributeAssignment>
      <AttributeAssignment
                  AttributeId="eu:neclab:nw:sba:obligation:negotiation:endpoint"
                  DataType="urn:oasis:names:tc:SAML:2.0:metadata:Endpoint">
                  <md:NegotiationService
   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata:Endpoint"
                          Binding="SOAP">
                          https://idp.com:8444/SAMLNegotiation
                  </md:NegotiationService>
      </AttributeAssignment>
      <AttributeAssignment
                  AttributeId="eu:neclab:nw:sba:obligation:negotiation:payment:one-
time:amount"
                  DataType="http://www.w3.org/2001/XMLSchema#integer">
                  10
      </AttributeAssignment>
      <AttributeAssignment
                  AttributeId="eu:neclab:nw:sba:obligation:negotiation:payment:one-
time:currency"
                  DataType="http://www.w3.org/2001/XMLSchema#string">
                  EUR
      </AttributeAssignment>
      <AttributeAssignment
   AttributeId="eu:neclab:nw:sba:obligation:negotiation:payment:rate:amount"
                  DataType="http://www.w3.org/2001/XMLSchema#double">
                  0.1
      </AttributeAssignment>
      <AttributeAssignment
   AttributeId="eu:neclab:nw:sba:obligation:negotiation:payment:rate:currency"
                  DataType="http://www.w3.org/2001/XMLSchema#string">
                  EUR
      </AttributeAssignment>
      <AttributeAssignment
      AttributeId="eu:neclab:nw:sba:obligation:negotiation:payment:metric"
      DataType="eu:neclab:nw:sba:obligation:negotiation:payment:metric:type">
                  perHour
      </AttributeAssignment>
      <AttributeAssignment
                  AttributeId="eu:neclab:nw:sba:obligation:negotiation:payment:method"
                  DataType="eu:neclab:nw:sba:obligation:negotiation:payment:method:type">
                  VISA
      </AttributeAssignment>
      <AttributeAssignment
                  AttributeId="eu:neclab:nw:sba:obligation:negotiation:payment:data"
                  DataType="http://www.w3.org/2001/XMLSchema#string">
                  1111 2222 3333 4444, 20/2010, 123
      </AttributeAssignment>
      <AttributeAssignment
                  AttributeId="eu:neclab:nw:sba:obligation:filter"
                  DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                  http://sp.com/restricted/*
      </AttributeAssignment>
      <AttributeAssignment
                  AttributeId="eu:neclab:nw:sba:obligation:filter"
                  DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                  http://sp.com/login/*
      </AttributeAssignment>
  </Obligation>
</Obligations>
```

Fig. 6

【図７】

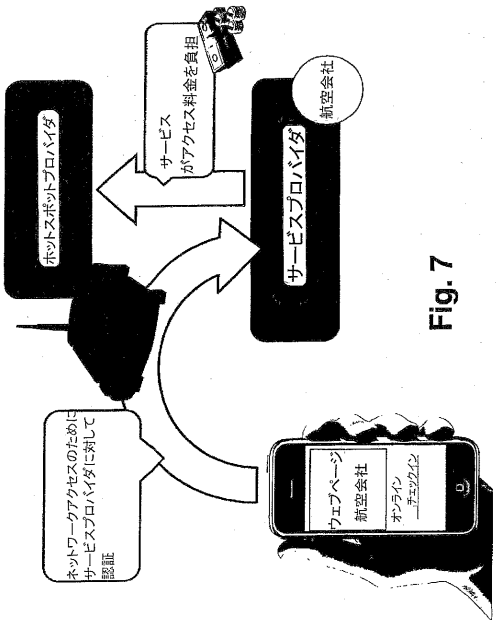

Fig. 7

【図８】

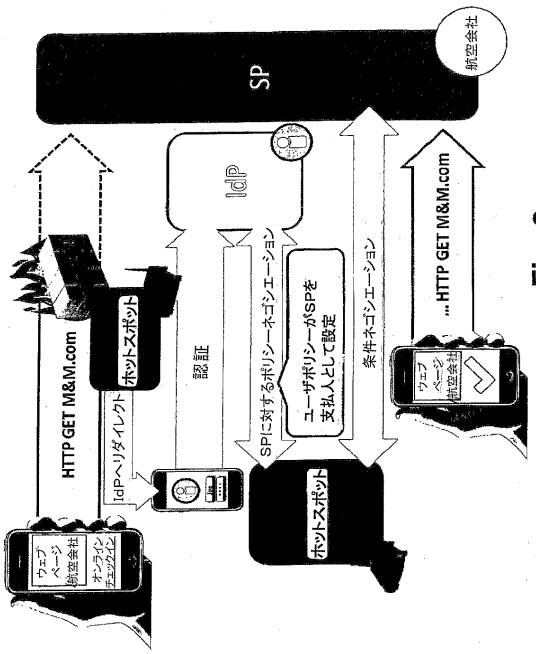

Fig. 8

【図９】

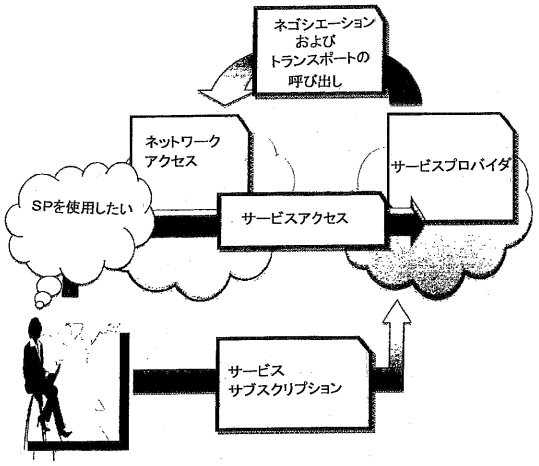

Fig. 9

フロントページの続き

審査官　▲吉▼田　耕一

(56)参考文献　特開２００４－３５５０７３（ＪＰ，Ａ）
特開平１１－２９６５８３（ＪＰ，Ａ）
特開２００２－１３２７２７（ＪＰ，Ａ）
特開２００７－０４８２４１（ＪＰ，Ａ）
特開２００４－２５８８７２（ＪＰ，Ａ）
米国特許出願公開第２００５／０２１０２８８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４１
Ｇ０６Ｆ　２１／３１