

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4722056号  
(P4722056)

(45) 発行日 平成23年7月13日(2011.7.13)

(24) 登録日 平成23年4月15日(2011.4.15)

(51) Int. Cl. F I  
G06F 21/20 (2006.01) G06F 15/00 330A

請求項の数 10 (全 18 頁)

(21) 出願番号	特願2006-545640 (P2006-545640)	(73) 特許権者	502303739
(86) (22) 出願日	平成16年11月10日(2004.11.10)		オラクル・インターナショナル・コーポレーション
(65) 公表番号	特表2007-521580 (P2007-521580A)		アメリカ合衆国、94065 カリフォルニア州、レッドウッド・ショアーズ、オラクル・パークウェイ、500
(43) 公表日	平成19年8月2日(2007.8.2)	(74) 代理人	100064746
(86) 国際出願番号	PCT/US2004/037461		弁理士 深見 久郎
(87) 国際公開番号	W02005/062155	(74) 代理人	100085132
(87) 国際公開日	平成17年7月7日(2005.7.7)		弁理士 森田 俊雄
審査請求日	平成19年9月14日(2007.9.14)	(74) 代理人	100083703
(31) 優先権主張番号	60/530,599		弁理士 仲村 義平
(32) 優先日	平成15年12月17日(2003.12.17)	(74) 代理人	100096781
(33) 優先権主張国	米国 (US)		弁理士 堀井 豊
(31) 優先権主張番号	10/890,786		
(32) 優先日	平成16年7月13日(2004.7.13)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 個別化およびアイデンティティ管理のための方法および装置

(57) 【特許請求の範囲】

【請求項1】

方法であって、

第1のアクセスプロバイダから第1のサービスプロバイダに向けられた第1のメッセージを受信するステップを含み、前記第1のメッセージは前記第1のアクセスプロバイダのユーザの第1の識別子に関連付けられ、

第2の識別子を得るステップと、

前記第1のメッセージから前記第1の識別子を分離するステップと、

前記第1のメッセージを前記第2の識別子に関連付けるステップと、

前記第2の識別子に関連付けられた前記第1のメッセージを前記第1のサービスプロバイダに送信するステップと、

前記第2の識別子に関連付けられた個別化情報を検索するステップと、

前記個別化情報の第1のサブセットを前記第1のサービスプロバイダに送信するステップと、

第2のアクセスプロバイダから前記第1のサービスプロバイダに向けられた第2のメッセージを受信するステップとを含み、前記第2のメッセージは前記第2のアクセスプロバイダの前記ユーザの第3の識別子に関連付けられ、前記方法はさらに、

前記第3の識別子が前記第1の識別子にマップされていることを判断するステップと、

前記第2のメッセージから前記第3の識別子を分離するステップと、

前記第2のメッセージを前記第2の識別子に関連付けるステップと、

10

20

前記第 2 の識別子に関連付けられた前記第 2 のメッセージを前記第 1 のサービスプロバイダに送信するステップと、

前記個別化情報の第 1 のサブセットを前記第 1 のサービスプロバイダに送信するステップとを含む、方法。

【請求項 2】

前記個別化情報を送信するステップは、前記個別化情報の部分にアクセスするという前記第 1 のサービスプロバイダからの要求の受信に回答するものである、請求項 1 に記載の方法。

【請求項 3】

前記第 1 のアクセスプロバイダから第 2 のサービスプロバイダに向けられた第 3 のメッセージを受信するステップを含み、前記第 3 のメッセージは前記第 1 の識別子に関連付けられ、前記方法はさらに、

前記第 3 のメッセージから前記第 1 の識別子を分離するステップと、

前記第 3 のメッセージを前記第 2 の識別子に関連付けるステップと、

前記第 2 の識別子に関連付けられた前記第 3 のメッセージを前記第 2 のサービスプロバイダに送信するステップと、

前記個別化情報の第 2 のサブセットを前記第 2 のサービスプロバイダに送信するステップとを含む、請求項 1 または 2 に記載の方法。

【請求項 4】

前記第 1 のアクセスプロバイダから第 2 のサービスプロバイダに向けられた第 3 のメッセージを受信するステップを含み、前記第 3 のメッセージは前記第 1 の識別子に関連付けられ、前記方法はさらに、

前記第 3 のメッセージから前記第 1 の識別子を分離するステップと、

第 4 の識別子を得るステップと、

前記第 3 のメッセージを前記第 4 の識別子に関連付けるステップと、

前記第 4 の識別子に関連付けられた前記第 3 のメッセージを前記第 2 のサービスプロバイダに送信するステップと、

前記個別化情報の第 2 のサブセットを前記第 2 のサービスプロバイダに送信するステップとを含む、請求項 1 または 2 に記載の方法。

【請求項 5】

個別化情報を受信するステップと、

前記個別化情報を前記第 2 の識別子に関連付けるステップと、

前記第 2 の識別子に関連付けられた前記個別化情報を記憶するステップとをさらに含む、請求項 1 ~ 4 のいずれか 1 項に記載の方法。

【請求項 6】

セッションを前記第 2 の識別子に関連付けるステップと、

前記第 1 または第 2 のメッセージを前記セッションに関連付けるステップと、

セッション管理情報に向けられたメッセージを評価するステップとを含み、前記セッション管理情報は、前記ユーザと前記サービスプロバイダとの間における情報のやり取りの状態を表わすデータを含み、前記方法はさらに、

前記第 1 のアクセスプロバイダから、前記第 1 または第 2 のサービスプロバイダに向けられた 1 つ以上の付加的なメッセージを受信するステップを含み、前記 1 つ以上の付加的なメッセージは前記第 1 の識別子に関連付けられ、前記方法はさらに、

前記第 1 のアクセスプロバイダから受信した、前記第 1 または第 2 のサービスプロバイダに向けられた前記付加的なメッセージの各々について、前記付加的なメッセージを前記セッションに関連付け、セッション管理情報のために前記付加的なメッセージの各々を評価するステップと、

前記セッション管理情報を記憶するステップとを含む、請求項 1 に記載の方法。

【請求項 7】

前記第 2 の識別子が前記セッションに関連付けられていることを判断するステップと、

10

20

30

40

50

前記セッションに関連付けられた前記セッション管理情報を検索するステップと、  
前記セッション管理情報を前記第1または第2のサービスプロバイダに送信するステップとをさらに含む、請求項6に記載の方法。

【請求項8】

前記第1のサービスプロバイダに向けられた前記第1のメッセージを受信するステップは、第1のアイデンティティプロバイダにおいて前記第1のメッセージを受信するステップを含み、

前記第1のサービスプロバイダに向けられた前記第2のメッセージを受信するステップは、第2のアイデンティティプロバイダにおいて前記第2のメッセージを受信するステップを含み、

前記第3の識別子が前記第1の識別子にマップされていると判断するステップは、前記第2のアイデンティティプロバイダから、データストレージにアクセスするステップを含み、前記データストレージは、前記第1のアクセスプロバイダで利用されるユーザアドレスを前記第2のアクセスプロバイダで利用されるユーザアドレスにマップするユーザ識別マッピングを含む、請求項1に記載の方法。

【請求項9】

方法であって、

第1のモバイルネットワークオペレータから第1のサービスプロバイダに向けられた第1のメッセージを受信するステップを含み、前記第1のメッセージはユーザの第1のMSISDNに関連付けられ、前記方法はさらに、

識別子を得るステップと、

前記識別子を認証するステップと、

前記第1のメッセージから前記第1のMSISDNを分離するステップと、

前記第1のメッセージを前記識別子に関連付けるステップと、

前記識別子に関連付けられた前記第1のメッセージを、前記識別子が認証されたという印とともに前記第1のサービスプロバイダに送信するステップと、

前記ユーザの嗜好を示す個別化情報を検索するステップと、

前記個別化情報を前記第1のサービスプロバイダに送信するステップと、

第2のモバイルネットワークオペレータから第1のサービスプロバイダに向けられた第2のメッセージを受信するステップとを含み、前記第2のメッセージは前記ユーザの第2のMSISDNに関連付けられ、前記方法はさらに、

前記第2のMSISDNが前記第1のMSISDNにマップされていることを判断するステップと、

前記第2のメッセージから前記第2のMSISDNを分離するステップと、

前記第2のメッセージを前記識別子に関連付けるステップと、

前記識別子に関連付けられた前記第2のメッセージを、前記識別子が認証されたという印とともに前記第1のサービスプロバイダに送信するステップと、

前記個別化情報を前記第1のサービスプロバイダに送信するステップとを含む、方法。

【請求項10】

システムであって、

第1のアクセスプロバイダから受信した第1のメッセージからユーザの第1の識別子を分離し、前記ユーザの第2の識別子を得、前記第2の識別子を前記第1のメッセージに関連付けるよう構成される第1のアイデンティティ構成要素と、

第2のアクセスプロバイダから受信した第2のメッセージからユーザの第3の識別子を分離し、前記ユーザの第2の識別子を得、前記第2の識別子を前記第2のメッセージに関連付けるよう構成される第2のアイデンティティ構成要素と、

前記第1のメッセージの受信に回答して、前記第2の識別子を認証し、前記第2の識別子が認証されたという印を前記第1のメッセージに関連付け、前記第2メッセージの受信に回答して、前記第3の識別子が前記第1の識別子にマップされていることを判断し、前記第2の識別子を認証し、前記第2の識別子が認証されたという印を前記第2メッセージ

10

20

30

40

50

に関連付けるよう構成された認証構成要素と、

前記第2の識別子に関連付けられた個別化情報を検索する検索構成要素と、

前記第2の識別子、前記印、および個別化情報のサブセットに関連付けられた前記メッセージをサービスプロバイダに送信する通信インターフェイスとを含む、システム。

【発明の詳細な説明】

【技術分野】

【0001】

関連する出願の相互参照

この出願は、2003年12月17日に出願され、「個別化およびアイデンティティ管理のための方法および装置 (“Method and Apparatus for Personalization and Identity Management”)」と題され、引用によりこの明細書中に援用される米国仮出願第60/530,599号の利益を主張する。

【0002】

発明の背景

この発明は、概して、電子ビジネスにおけるアイデンティティ管理に関する。より特定的には、この発明は、移動空間などにおける異なる位置および異なる装置からアクセスされ得るアイデンティティ管理、認証、ユーザ嗜好およびプロフィールに関する。

【背景技術】

【0003】

ユーザアイデンティティを管理するためにさまざまな技術が用いられてきた。典型的には、ネットワークアプリケーションまたはサーバにアクセスするために、ユーザはユーザを識別するアイデンティティ情報をアプリケーションまたはサーバプロバイダに提供する。次いで、ユーザには、アプリケーションまたはサーバにアクセスするのに用いることのできるログイン識別子が与えられる。場合によっては、アプリケーション/サーバはまた、ユーザの嗜好を記憶するユーザプロフィールを作成し得る。アプリケーションプロバイダは、ユーザがアプリケーションにアクセスするのに用いているクッキーまたは認証トークンをアプリケーション(たとえば、ウェブブラウザ)または装置(たとえば、ユーザの機械)に送信し得る。こうして、ユーザが次回ネットワークアプリケーションにアクセスする場合に備えて、ログイン識別、ユーザ嗜好、トランザクション履歴などの情報を蓄えることができる。しかしながら、ユーザの個別化情報(ユーザ嗜好、トランザクション履歴など)は、異なるプロバイダ間では共有できない。加えて、ユーザ識別はサービスプロバイダには知られている。

【発明の開示】

【発明が解決しようとする課題】

【0004】

他の既存の技術により、ユーザが1つのログイン識別子を用いて複数のアプリケーションにアクセスすることが可能となる。この技術の一例は、オラクル(Oracle)のシングル・サインオン・オファリング(Single Sign-On Offerings)などのシングル・サイン・オン(SSO)である。SSOは、プログラムコードにおいて「ハードコードされた(hard coded)」特定のSSOを有するアプリケーション間における1つのセッションに対して有効である。SSOは単一のセッションにのみ有効であるので、アプリケーションの個別化はSSOによってはもたらされない。さらに、ユーザアイデンティティは、すべてのアプリケーションに知られている。

【0005】

別の既存のアプローチには、マイクロソフト(Microsoft)(登録商標)のパスポート技術などのような、異なるサービスプロバイダ間での集中的なアイデンティティ管理の使用が含まれる。サービスプロバイダは、アイデンティティ(identity)/認証(authentication)プロバイダによるユーザの認証を可能にするプログラムコードをアプリケーションに含まなければならない。次いで、顧客は、単一のアイデンティティ/認証プロバイダを用いてサービスにログオンする。これにより、プライバシーの問題や違反のリスクが増

10

20

30

40

50

大するおそれがある。さらに、サービスプロバイダは、アイデンティティ / 認証プロバイダに連結される。これは、いくつかのサービスプロバイダ、特に電気通信、モバイルネットワークオペレータ (MNO) および銀行業務用プロバイダにとっては容認できない市場独占のリスクとして受取られる可能性がある。

【 0 0 0 6 】

別のアプローチとして、プロバイダ間で分散して単一のサインオンを提供し得る連合型アイデンティティ管理が挙げられる。このような1つの連合にはリバティ・アライアンス・プロジェクト (Liberty Alliance Project) (<http://www.projectliberty.org>) があり、概要を、<http://www.projectliberty.org/specs/liberty-architecture-overview-v1.0.pdf> に見出すことができる。連合型アイデンティティ管理は、当該連合のメンバによるユーザの認証が当該連合の他のメンバについての認証として機能することを可能にする。しかしながら、ユーザアイデンティティをマスキングするか、または、プロバイダ間でユーザ嗜好もしくは他のユーザ個別化情報を共有することを可能にする機構は提供されない。

10

【 課題を解決するための手段 】

【 0 0 0 7 】

発明の概要

個別化およびアイデンティティ管理のための方法およびシステムが開示される。一実施例においては、当該方法は、モバイルネットワークオペレータまたは無線ネットワークプロバイダなどのアクセスプロバイダからサービスプロバイダのためのメッセージを受信するステップを含む。当該メッセージは、アクセスプロバイダのユーザの第1の識別子に関連付けられる。第2の識別子が得られる。第1の識別子は当該メッセージから分離され、第2の識別子は当該メッセージに関連付けられる。第2の識別子に関連付けられたメッセージがサービスプロバイダに送信される。いくつかの実施例においては、第2の識別子が認証されたという印 (indication) が、また、サービスプロバイダに送信され得る。

20

【 0 0 0 8 】

いくつかの実施例においては、当該方法は、第2の識別子に関連付けられる個別化情報を検索し、個別化情報のサブセットをサービスプロバイダに送信するステップを含み得る。一例として、個別化情報は、ユーザ嗜好、ユーザ装置特徴、ユーザ装置能力、ユーザ装置設定、ユーザ装置アドレスおよび他のユーザ個別化情報を含み得る。当該方法は、情報が送信される前にサービスプロバイダが個別化情報を有する許可を得ているという判断を随意に含み得る。個別化情報は、ユーザ、サービスプロバイダから受信されていてもよく、および / またはユーザ履歴から得られていてもよい。

30

【 0 0 0 9 】

代替的には、または加えて、当該方法はまた、セッションを第2の識別子に関連付け、アクセスプロバイダから受信したメッセージを当該セッションに関連付けるステップを含み得る。アクセスプロバイダから受信したメッセージおよび1つ以上の付加的なメッセージは、第1の識別子に関連付けられているが、セッション管理情報について評価され得る。サービスプロバイダへの接続が失われ、再設定された場合、セッション管理情報は将来の検索のために記憶され得る。

40

【 0 0 1 0 】

アクセスプロバイダからメッセージを受信した後、メッセージは、サービスプロバイダのために第2のアクセスプロバイダから受信され得る。当該メッセージは、ユーザの第3の識別子に関連付けられ得る。次いで、当該方法は、第3の識別子が第1の識別子にマップされると判断するステップを含み得る。第3の識別子は当該メッセージから分離され、第2の識別子は当該メッセージに関連付けられる。第2の識別子に関連付けられる第2のメッセージはサービスプロバイダに送信される。

【 0 0 1 1 】

代替的な実施例においては、当該方法は、サービスプロバイダのためにモバイルネットワークオペレータからメッセージを受信するステップを含み得る。受信されたメッセージ

50

は、ユーザのMSISDNに関連付けられ得る。識別子が得られ、認証される。当該MSISDNはメッセージから分離され、得られた識別子はメッセージに関連付けられる。次いで、当該メッセージは、当該識別子が認証されたという印とともにサービスプロバイダに送信される。ユーザの嗜好を示す個別化情報もサービスプロバイダに送信される。

【0012】

第3の実施例においてシステムが開示される。当該システムは、アクセスプロバイダから受信したメッセージからユーザの第1の識別子を分離するよう構成されたアイデンティティ構成要素を含む。アイデンティティプロバイダはまた、アクセスプロバイダのユーザのための識別子を得、第2の識別子を当該メッセージに関連付けるよう構成される。当該システムはさらに、第2の識別子を認証し、第2の識別子が認証されたという印を当該メ  
10  
ッセージに関連付けるよう構成された認証構成要素を含む。通信インターフェイスは、第2の識別子に関連付けられるメッセージと、印とをサービスプロバイダに送信するよう構成される。

【0013】

明細書および添付の図面の残りの部分を参照することにより、この発明の性質および利点をさらに理解することができるだろう。

【0014】

この発明に従った具体的な実施例が添付の図面に示される。

【発明を実施するための最良の形態】

【0015】

発明の詳細な説明

以下の説明においては、この発明を完全に理解できるようにするために、説明の目的で多数の特定の詳細が述べられる。しかしながら、これらの特定の詳細のうちいくつかがなくともこの発明が実施可能であることが、当業者には明らかとなるだろう。他の場合には、周知の構造および装置がブロック図の形で示される。

【0016】

図1は、アイデンティティ管理をユーザに提供するのに用いられ得るシステムの具体的な実施例を示す。ユーザは、アクセスプロバイダ102を用いてネットワークにアクセスし得る。当該ネットワークは、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、無線ネットワークまたは他の種類のネットワークであってもよい  
30  
。こうして、アクセスプロバイダ102は、インターネットサービスプロバイダ、モバイルネットワークオペレータ(MNO)、または無線通信ネットワークに対する他の種類のプロバイダ、すなわち、無線ネットワークに対するプロバイダ(たとえば、汎用のパケット無線サービス(GPRS)ネットワーク、WiFiネットワーク、2.5G、EDGE、UMTS、3G、CDMA、FOMAなど)であってもよい。いくつかの実施例においては、ユーザは、移動可能な装置からネットワークにアクセスし得る。一例として、携帯機器は、ラップトップ、携帯情報端末(PDA)、携帯電話または他の種類の装置であり得る。他の実施例においては、ユーザ装置は相対的に据置き型であってもよく、たとえばパーソナルコンピュータなどであってもよい。

【0017】

ユーザは、アクセスプロバイダ102によって提供されるネットワークアクセスを用いて、1つ以上のサービスプロバイダ108、110と情報をやり取りし得る。異なる種類のさまざまなサービスがサービスプロバイダ108、110によって提供され得る。たとえば、サービスプロバイダ108、110は、電子メールサービス、音声メールサービス、メッセージングサービス(たとえば、テキストメッセージング、インスタントメッセージング、MMS、音声チャットなど)またはアプリケーションサービスを提供し得る。一例として、アプリケーションサービスは、ユーザが商品またはサービスを購入することを可能にするウェブサイト、或る人がどこに居るか、出席しているかまたは空いているかを見出すためのアプリケーション、データをリポジトリ(repository)と同期させるためのアプリケーション、データ、アプリケーションもしくは装置のライフサイクルを規定/管  
40  
50

理するためのアプリケーション、または、特定のドメインにアクセスするためのアプリケーションを含み得る。サービスプロバイダ108、110によって他の種類の広範囲のサービスも提供され得ることが認識される筈である。

【0018】

ユーザ装置（図示せず）は、そこにアクセスプロバイダ102がメッセージを送信することを可能にする関連する識別子を有する。一例として、識別子は、ネットワークインターフェイスカード（NIC）、移動識別番号（MIN）、移動局ISDN（MSISDN）、EMI、SIM情報またはUSIM情報であり得る。アクセスプロバイダ102を介してユーザ装置からサービスプロバイダ108、110に送信されたメッセージは、一般に、サービスプロバイダ108、110がメッセージをユーザに送り返すことができるようにメッセージに関連付けられた識別子を有する。しかしながら、場合によっては、プライバシーまたは他の理由のために、ユーザは、サービスプロバイダにその識別子を知られることを望まない可能性がある。たとえば、携帯電話のユーザが、サービスプロバイダ108、110にユーザの移動識別番号を知られることを望まない可能性がある。

10

【0019】

アイデンティティプロバイダ104は、サービスプロバイダ108、110からユーザのアドレスをマスキングするのに用いられてもよい。以下にさらに詳細に説明されるように、アイデンティティプロバイダ104は、ユーザのために異なる識別子を獲得し得る。アイデンティティプロバイダ104は、ユーザから送信されたメッセージから第1の識別子を分離し、代わりに、当該メッセージを第2の識別子と関連付け得る。次いで、第2の識別子に関連付けられたメッセージは、メッセージが宛てられたサービスプロバイダ108、110に送信され得る。場合によっては、アイデンティティプロバイダ104はまた、第2の識別子を認証し得、第2の識別子が認証されたという印を当該メッセージとともに送信し得る。サービスプロバイダ108、110は、メッセージをユーザまで戻すようアイデンティティプロバイダ104にルーティングする。次いで、アイデンティティプロバイダは、サービスプロバイダ108、110から受信したメッセージに関連付けられた第2の識別子を第1の識別子と置換え、当該メッセージを、ユーザに届けるためにアクセスプロバイダ102に送信し得る。こうして、ユーザは、いかなる識別情報、たとえばユーザ装置アドレス、名前、電子メールアドレス、電話番号または他の識別情報をも提供することなく、サービスプロバイダ108、110とのトランザクションを実行し得る。

20

30

【0020】

図2は、アイデンティティプロバイダ104の具体的な実施例を示す。アイデンティティプロバイダ104はアイデンティティマネージャ204を含む。アイデンティティマネージャ204は、ユーザ識別（user identification）をサービスプロバイダ108、110からマスキングする目的で、ユーザのための識別子を得るのに用いられ得る。場合によっては、ユーザアドレスのために新しい識別子が作成され得る。他の場合には、アイデンティティマネージャ204は、ユーザのために識別子が既に存在していると判断し得る。たとえば、マスキングするのに用いられる識別子は、ユーザの別の識別子に既に割当てられているかもしれない。別の例として、識別子は、同じユーザ（たとえば、複数のアクセスプロバイダおよび/または装置を用いるユーザ）のために付加的な複数の識別子に割当てられてもよく、その各々が当該識別子にマップされている。同じ識別子を用いて、複数のサービスプロバイダ108、110にアクセスし得る。代替的には、各々のサービスプロバイダのために異なる識別子を得て、ユーザのアイデンティティをサービスプロバイダからマスキングし得る。

40

【0021】

次いで、アイデンティティマネージャ204は、マスキングするために用いられる識別子を認証マネージャ206に送って、当該識別子を認証し得る。これは、アクセスプロバイダから受信した信用証明書に基づいてなされてもよい。信用証明書は、トークン、クッキー、デジタル証明書、SIM認証または他の種類のトークンを含み得る。場合によっては、チャレンジ応答をユーザ装置に送信してユーザを認証し得る。識別子が認証された後

50

、認証マネージャ 206 は、当該識別子が認証されたことをアイデンティティマネージャ 204 に通知し得る。次いで、アイデンティティマネージャ 206 は、識別子に関連付けられたメッセージを、当該識別子が認証されたというインジケータ (indicator) とともに伝送し得る。

【0022】

一実施例においては、アイデンティティマネージャ 204 は、アクセスプロバイダ 102 からメッセージを受信し、ユーザアイデンティティをマスキングし、識別がマスキングされた状態でメッセージをサービスプロバイダ 110 に送信し得る。アイデンティティマネージャ 204 はまた、メッセージに関連付けられたマスキングされた識別子をアクセスプロバイダのためのユーザのアイデンティティと置換えることにより、サービスプロバイダ 108、110 から受信したメッセージをユーザにルーティングするのに用いられてもよい。こうして、マスキングされた識別子が 1 つ以上のアクセスプロバイダのために複数のユーザアイデンティティにマップされると、アイデンティティマネージャ 204 は、メッセージを送信するのに用いるために現在の識別子を追跡し得る。

【0023】

他の実施例においては、ユーザについてのマスキングされた識別子を得るのにアイデンティティマネージャ 204 を用い得るセッション/個別化マネージャ 202 などの中継器にメッセージが送信され得る。こうして、アイデンティティプロバイダ 104 は、アクセスプロバイダ 102 からメッセージを受信し、アイデンティティマネージャ 102 からマスキングされた識別子を得、ユーザのアクセスプロバイダの識別子をマスキングされた識別子と置換え、メッセージをサービスプロバイダ 108、110 に送信するために、セッション/個別化マネージャ 202 または他の種類の中継器を随意に含み得る。上述のとおり、アイデンティティマネージャ 102 はマスキングされた識別子を認証し得、こうして、セッション/個別化マネージャ 202 (または他の種類の中継器) がまた、マスキングするのに用いられる識別子が認証されたという印をメッセージとともに送信し得る。セッション/個別化マネージャ 202 または他の種類の中継器はまた、識別子をユーザのアクセスプロバイダの識別と置換えることにより、サービスプロバイダ 108、110 から受信したメッセージをユーザに再度ルーティングするのに用いられ得る。

【0024】

セッション/個別化マネージャ 202 はまた、ユーザが異なるアクセスプロバイダに切替えるかまたは異なる装置を用いてサービスプロバイダ 108 にアクセスする場合に、複数のサービスプロバイダ 108、110 間でのユーザ個別化情報の共有および/またはセッション管理の実行のために用いられてもよい。ユーザが移動する (roams) (アクセスプロバイダを切替える) かまたは第 2 の装置を用いてサービスプロバイダにアクセスする場合にセッション管理を如何に実行し得るかについての詳細な説明は、「異なるアクセス機構間のローミングおよびネットワーク技術 ("ROAMING ACROSS DIFFERENT ACCESS MECHANISMS AND NETWORK TECHNOLOGIES")」と題された出願連続番号第 X X / X X X X, X X X (代理人番号 021756-000900US) において見出すことができ、その詳細が引用によりこの明細書中に援用される。

【0025】

ユーザに割当てられた識別子は、サービスプロバイダ 108、110 のためのセッションに関連付けられてもよい。所定の期間に亘って受信されたユーザからサービスプロバイダ 108、110 へのメッセージ (サービスプロバイダとのユーザセッション) はセッションに関連付けられ得る。セッションマネージャ 202 は、セッション管理情報についてのメッセージを評価し得る。セッション管理情報は、ユーザとサービスプロバイダとの間における情報のやり取りの状態を表わすデータ、状態またはセッション内のユーザ嗜好および/または他の種類のセッション情報を含み得る。以下により詳細に記載されるように、セッション管理情報は、ユーザによるさまざまな種類のローミング (たとえば、一時停止および再開、接続/断続的な切断/切断ならびに複数装置のローミング) をサポートするのに用いられてもよい。セッション/個別化マネージャ 202 は、データストレージ 2

10

20

30

40

50



08を用いてセッション管理情報を記憶し得る。

【0026】

加えて、セッション/個別化マネージャ202はユーザ個別化情報を管理し得る。セッション/個別化マネージャ202は、識別子に関連付けられる個別化情報をデータストレージ208から検索し得る。個別化情報のサブセットはサービスプロバイダ108、110に送信され得る。場合によっては、当該サブセットは個別化情報のすべてを含み得るが、他の場合には、サービスプロバイダ108、110に適用可能であるかまたはサービスプロバイダ108、110が有する許可を得た個別化情報だけが送信され得る。ユーザのアイデンティティをマスキングするために各サービスプロバイダ108、110のための異なる識別子が提供される実施例においては、個別化情報が複数のサービスプロバイダ108、110間で共有され得るように、当該個別化情報が識別子のすべてにマップされ得る。代替的には、一般的な個別化情報のサブセットは複数の識別子の各々にマップされ得るが、アプリケーション専用の個別化情報は、特定のアプリケーションのサービスプロバイダ108、110に対する識別子にのみマップされ得る。

10

【0027】

個別化情報は、異なる種類のさまざまな情報を含み得る。たとえば、個別化情報は、一般的なユーザ嗜好、アプリケーションに関連する嗜好もしくは他の個別化情報、たとえば支払情報もしくは嗜好(たとえば、Mコマース、電子財布、もしくはユーザ嗜好を特定する他の情報および支払いをするのに用いられるアカウント)、アプリケーション設定、アカウント情報、コンタクト/アドレスブック情報、または他の種類のアプリケーション専用 20の情報を含み得る。個別化情報はまた、装置に関連する情報、たとえば装置設定、どこで/如何にコンタクトすべきかについての統一されたメッセージング(UM)プライオリティリスト、またはプライバシールールを含み得る。個別化情報の他の例には、ユーザ信用証明書、嗜好およびプライバシー設定を含むサービスに対するユーザ契約、ユーザ装置(たとえば、装置特徴/能力、装置設定、装置アドレスなど)、ネットワーク/アクセス機構特徴(たとえば、マルチチャネル、マルチモーダル、音声など)、ならびに、嗜好を記憶した他の種類の情報またはユーザについての他の情報が含まれる。ユーザ個別化情報はユーザによって明確に設定または提供され得る。代替的に、または付加的には、セッション/個別化マネージャ202は、ユーザとサービスプロバイダ108、110との間で送信されるメッセージから嗜好または個別化情報を引出し得る。セッション/個別化マネ 30ージャ202が個別化管理を引出す実施例においては、プライバシー嗜好(Privacy Preferences)のためのプラットフォーム(P3P)は、メッセージによって伝送されている情報の種類を判定するよう、いくつかのアプリケーションのために用いられてもよい。

20

30

【0028】

セッション/個別化マネージャ202は、ユーザがサービスプロバイダとのセッションを開始した時、または、進行中のセッション中などの、嗜好情報を用いてユーザに関する文脈を設定するような他の時に、個別化情報をサービスプロバイダ108、110に送信し得る。個別化情報は、同様にまたは代替的には、サービスプロバイダ108、110から要求を受信することに対応して送信され得る。たとえば、セッション/個別化マネージャ202は、識別子に関連付けられた1つ以上のクッキーをサービスプロバイダ108、110から既に受信していてもよい。セッション/個別化マネージャ202は、クッキーをユーザ装置に転送するのではなく、クッキーをデータストレージ208に記憶し得る。サービスプロバイダがクッキーを要求した場合、セッション/個別化マネージャ202は、データストレージ208からクッキーを検索し、当該クッキーをサービスプロバイダ108、110に送信し得る。こうして、セッション/個別化マネージャ202は、サービスプロバイダのためのクッキープロキシとして機能し得る。他の種類の個別化情報がまた、サービスプロバイダ108、110の要求によって送信されてもよい。

40

【0029】

さまざまな技術を用いて、サービスプロバイダ108、110が許可された個別化情報だけを受信することを確実にすることができる。たとえば、サービスプロバイダは、背景

50

色などのアプリケーション設定を示す個別化情報にアクセスできるが、アイデンティティ情報にはアクセスできない。したがって、個別化情報を送信する前に、セッション/個別化マネージャ202は、サービスプロバイダ108、110が個別化情報を有する許可を得たかどうかを判断し得る。セッション/個別化マネージャ202は、情報を（たとえば、「ポップアップ」メッセージを介して）送信する前にユーザからの許可を要求し得るか、または、（ユーザによってデフォルトまたは設定された）ルールを調べて、どんな種類の情報が送信され得るか判断し得る。いくつかの実施例においては、サービスプロバイダ108、110はデータストレージ208にアクセスし得るが、当該情報は、サービスプロバイダ108、110が許可された情報しか閲覧、検索または変更できないようにフィルタにかけられ得る。また、他の機構を用いて、個別化情報の無許可のアクセスまたは送信を防止し得る。

10

#### 【0030】

代替的な実施例において、アイデンティティプロバイダ104が図2に示されるのとは異なり得ることが認識される筈である。たとえば、アイデンティティプロバイダ104は認証マネージャ206を含み得ないが、代わりに、第3のパーティによって提供される認証マネージャを用い得る。別の例として、セッション/個別化マネージャ202は別個の構成要素であり得るか、または、セッションもしくは個別化管理の両方ではなくいずれかしか提供し得ない。第3の例として、セッション管理情報を記憶するのに用いられるデータストレージとは異なるデータストレージを用いて、個別化情報を記憶し得る。他の代替例も企図される。

20

#### 【0031】

支払プロバイダとの情報のやり取りのための具体的な一実施例が挙げられるが、ここでは、ユーザがアイデンティティプロバイダ104を用いてアイデンティティをマスキングし得る。ユーザは、アイデンティティをマスキングするために、図1で説明されるようなアイデンティティマネージャを用いて商用サイトにログインし得る。ユーザが購入する商品を選択し、支払の準備ができると、業者は、ユーザのマスキングされたアイデンティティを支払プロバイダに送信し得る。業者はまた、他の個別化情報、嗜好情報またはプロフィール情報を送信し得る。次いで、支払プロバイダが、3ドメインセキュアプロトコルなどのプロトコルを用いてユーザのための認証を獲得し得る。いくつかの実施例においては、アイデンティティマネージャを用いてユーザを認証し得る。こうして、支払プロバイダは、ユーザが認証されたことだけを知り得るが、ユーザアイデンティティ、支払許可またはアカウント情報を知ることはできない。必要であれば、支払プロバイダは、トランザクションを許可するのに必要な確認または他の情報について、アイデンティティマネージャを介してユーザと情報をやり取りし得る。完了し次第、支払プロバイダは、アイデンティティマネージャがサービスプロバイダによって設定された請求書を発行することを要求し得る。次いで、アイデンティティプロバイダ104は、支払金額についての請求書をユーザに送信し得るか、または、アクセスプロバイダの請求書と組合せるために請求書情報をアクセスプロバイダ102に送信し得る。代替的には、支払プロバイダは、アイデンティティマネージャを用いてユーザに請求書通知を送信（たとえば、電子メールを送信）し得る。

30

40

#### 【0032】

図3は、ユーザがアクセスプロバイダを切替えた場合にユーザのためにマスキングする識別（identification）をサポートするのに用いられ得る例示的なシステム300を示す。ユーザは、さまざまな状況においてアクセスプロバイダ302から第2のアクセスプロバイダ304に切替え得る。たとえば、ユーザは、異なるネットワークにローミングする携帯機器（たとえば、携帯電話）を用いていてもよい。別の例として、ユーザは、ある種類のアクセスプロバイダ（たとえば、汎用のパケット無線サービス（GPRS）アクセスプロバイダ）から、第2の種類のアクセスプロバイダ（たとえば、WiFiプロバイダ）に切替え得る。ユーザは、第1の装置から、ネットワークにアクセスするのに別のアクセスプロバイダを用いる第2の装置に切替えた場合、アクセスプロバイダも切替える可能性

50

がある。ユーザはまた、他のさまざまな場合、たとえば、あるWi-Fiネットワークから別のネットワークに切替えるかまたはWi-Fiから3GもしくはGPRSに切替える場合に、アクセスプロバイダを切替える。時として、ユーザが異なるアクセスプロバイダに切替える場合、異なるアクセスプロバイダのためのユーザのアイデンティティが同じままである可能性がある。一例として、あるMNOネットワークから第2のMNOネットワークにローミングする場合、ユーザの識別（たとえば、MSISDN番号）は同じままである。他の場合、ユーザは、たとえば、装置を切替えるかまたは異なる種類のアクセスプロバイダに切替える場合、アイデンティティを変更する可能性がある。

#### 【0033】

図3は、アクセスプロバイダ302、304がともに同じアイデンティティプロバイダ306を用いてアイデンティティ管理を行なう実施例を示す。ユーザがアクセスプロバイダ302、304を切替えた後、アイデンティティマネージャ306は、第2のアクセスプロバイダからサービスプロバイダ310のための1つ以上のメッセージを受信する。第2のアクセスプロバイダについてのユーザアイデンティティが第1のアクセスプロバイダについてのアイデンティティから変わっていなければ、アイデンティティマネージャ306は、ユーザからサービスプロバイダ310に送信されたメッセージからユーザのアクセスプロバイダの識別を引き続き分離し、（メッセージがアクセスプロバイダ302から受信されたときに得られた）ユーザのアクセスプロバイダの識別にマップされたマスキングされた識別子をメッセージに関連付け得る。サービスプロバイダ310から識別子に送信されたメッセージは、ユーザのアクセスプロバイダの識別を用いて、第2のアクセスプロバイダ304を介してユーザにルーティングされる。

#### 【0034】

多くの場合、ユーザのアイデンティティは、第1のアクセスプロバイダ302から第2のアドレスプロバイダ304に切替えた場合、変化するだろう。いくつかの実施例においては、アクセスプロバイダ302、304は、1つのメンバ（アクセスプロバイダ302）についてのユーザアイデンティティのための認証が異なるメンバ（アクセスプロバイダ304）によって維持されるアイデンティティのための認証として機能することに当該アクセスプロバイダ302、304が同意している連合体のメンバであり得る。こうして、（たとえば、アイデンティティマネージャ204の構成要素における）アイデンティティプロバイダ104は、ユーザが有する識別子のマッピングをさまざまなアクセスプロバイダ302、304で維持し得る。アイデンティティプロバイダ104がこの情報を維持するので、アクセスプロバイダ302、304は、他のアクセスプロバイダでは、ユーザが有するアイデンティティを知り得ない。ユーザは、アイデンティティプロバイダ306にマッピングのうちのいくらかを提供し得る。

#### 【0035】

第2のアクセスプロバイダ304を介してユーザの第3の識別子（第2のアクセスプロバイダが用いる識別子）に関連付けられたメッセージを受信した後、アイデンティティプロバイダ306は、第3の識別子が、第1のアクセスプロバイダ302から受信したメッセージに関連付けられる第1の識別子にマップされると判断する。次いで、アイデンティティプロバイダ306は、第3の識別子をメッセージから分離し、第1の識別子にマップされたマスキングされた識別子と第2のメッセージを関連付ける。マスキングされた識別子に関連付けられたメッセージはサービスプロバイダ310に送信される。

#### 【0036】

いくつかの実施例においては、ユーザは装置を切替えるが、同じアクセスプロバイダを用い得る。これらの実施例においては、第3の識別子に関連付けられるメッセージは、同じアクセスプロバイダから送信されていてもよい。アイデンティティプロバイダ306はマッピングを用いて、第1の識別子に関連付けられるマスキングされた識別子も第3の識別子のアイデンティティをマスキングするのに用いられるべきであると判断し得る。加えて、先に記載されたように、いくつかの実施例においては、アイデンティティプロバイダ306はまた、セッションおよび/または個別化管理を提供し得る。ユーザがアクセス

10

20

30

40

50

プロバイダ302、304を切替えた（かまたは、異なるアドレスに切替えた）場合、サービスプロバイダ310への接続が終了させられてもよい。第2のアクセスプロバイダによって接続が再度確立された後、アイデンティティプロバイダ306は、マスキングされた識別子がサービスプロバイダとのセッションに関連付けられると判断し得る。次いで、アイデンティティプロバイダ306はサービスプロバイダ310にセッション管理情報を送信（または利用可能に）し得る。こうして、ユーザは、接続を終了させたのと同じ状態、またはほぼ同じ状態で、サービスプロバイダ310との情報のやり取りを再開し得る。

**【0037】**

図4は、ユーザがアクセスプロバイダを切替えた場合にユーザのためにマスキングする識別をサポートするのに用いられ得るシステム400の第2の具体的な実施例を示す。この実施例においては、アクセスプロバイダ402、404は異なるアイデンティティプロバイダ406、408を用いる。アクセスプロバイダ402、404は、ユーザが有するアイデンティティをさまざまなアクセスプロバイダ302、304に関連付けるマッピング情報にアイデンティティプロバイダ406、408がアクセスすることを可能にする連合協定（federation agreement）を有し得る。当該システムは、アクセスプロバイダ402、404がともに到達可能なデータストレージ410を含む。データストレージ410は、ユーザのアイデンティティ間における、さまざまなアクセスプロバイダでの、サービスプロバイダとの情報のやり取りのために用いられる1つ以上のマスキングされた識別子へのマッピングを記憶するのに用いられ得る。

**【0038】**

アイデンティティプロバイダ406が、アクセスプロバイダ402に関連付けられる第1の識別子のためのマスキングされた識別子を得た後、アイデンティティプロバイダ406は、第1の識別子からマスキングされた識別子へのマッピングをデータストレージ410に記憶し得る。こうして、第2のアイデンティティプロバイダ408は、（第2のアクセスプロバイダによって用いられる）第3の識別子に関連付けられるアクセスプロバイダ404からメッセージを受信すると、最初にデータストレージ410を調べて、マスキングされた識別子が第3の識別子に割当てられているかどうか判断し得る。いくつかの実施例においては、データストレージ410は、ユーザが有する異なるアイデンティティを異なるアクセスプロバイダ402、402でマップし得る。これらの実施例においては、第3の識別子に関連付けられるマスキングされた識別子の探索により、（第1のアクセスプロバイダが用いられる）第1の識別子に割当てられたマスキングされた識別子を戻し得る。代替的には、アクセスプロバイダ404は、ユーザの第3の識別子に関連付けられる異なるアイデンティティをすべて用いてデータストレージを探索し得る。次いで、アクセスプロバイダ404は、第1の識別子にマップされた同じマスキングされた識別子を用いて、サービスプロバイダ412とのトランザクションからユーザの第3の識別子をマスキングし得る。

**【0039】**

アイデンティティプロバイダ406、408によって割当てられたマスキングされた識別子を、ユーザが有するアイデンティティに、1つ以上のアクセスプロバイダ402、404でマップするマッピングに加えて、データストレージ410または異なるデータストレージはまた、識別子にマップされたセッションまたは個別化情報を記憶し得る。こうして、アイデンティティプロバイダ408は、必要または要求に応じて、セッションおよび個別化情報をサービスプロバイダ412に送信し得る。代替的には、アイデンティティプロバイダ406、408は、他のアイデンティティプロバイダによって記憶されたセッション/個別化情報に直接アクセスすることができない。これらの実施例においては、第2のアイデンティティプロバイダ408は、第1のアイデンティティプロバイダ406がセッションおよび個別化情報を第2のアイデンティティプロバイダ408またはサービスプロバイダ412に送信することを要求し得る。

**【0040】**

図5は、アクセスプロバイダを介してユーザがアクセスし得る例示的な無線ネットワー

10

20

30

40

50

クを示す。無線ネットワーク技術は、無線ワイドエリアネットワーク（WWAN）、無線ローカルエリアネットワーク（WLAN）および無線パーソナルエリアネットワーク（WPAN）の技術を含む。WWAN技術は、典型的には、携帯電話およびそれに関連する技術、たとえばGSM、GPRS、CDPD、CDMA、TDMA、WCDMAなどを含む。WWANネットワークは高出力の長距離ネットワークであり、典型的には、数キロメートル以上のオーダのアクセス範囲を有する。他方、WLAN技術は中出力の中距離ネットワークであり、数十メートルのオーダのアクセス範囲を有し、WPANネットワークは低出力の短距離ネットワークであり、典型的には約10メートル以下のアクセス範囲を有する。WLAN技術の例にはIEEE 802.11(a)、(b)、(e)および(g)の技術が含まれ、WPAN技術の例には、ブルートゥース（Bluetooth）（登録商標）、HomeRF、IrDAおよびIEEE 802.15の技術が含まれる。無線ネットワーク以外のネットワークがアクセスプロバイダを介してユーザにアクセス可能にされ得ることが理解されるべきである。

10

#### 【0041】

図6は、アイデンティティプロバイダ（または、アイデンティティプロバイダの構成要素）が実現され得るコンピュータシステム600の一実施例を示す。図示されるコンピュータシステム600は、バス655を介して電氣的に結合され得るハードウェア要素を含む。ハードウェア要素は、1つ以上の中央処理装置（CPU）605、1つ以上の入力装置610（たとえば、マウス、キーボードなど）、および1つ以上の出力装置615（たとえば、表示装置、プリンタなど）を含み得る。コンピュータシステム600はまた、1つ以上の記憶装置620を含み得る。一例として、記憶装置620は、ディスクドライブ、光学記憶装置、固体記憶装置、たとえば、プログラム可能、フラッシュ更新可能などであり得るランダムアクセスメモリ（「RAM」）および/または読出専用メモリ（「ROM」）であり得る。

20

#### 【0042】

コンピュータシステム600は、コンピュータ読取可能な記憶媒体リーダ625、通信システム630（たとえば、モデム、ネットワークカード（無線または有線）、赤外線通信装置など）、およびワーキングメモリ640を付加的に含み得るが、これらは、上述のRAMおよびROM装置を含み得る。いくつかの実施例においては、コンピュータシステム600はまた、DSP、特殊用途のプロセッサなどを含み得る処理加速ユニット（processing acceleration unit）635を含み得る。

30

#### 【0043】

コンピュータ読取可能な記憶媒体リーダ625はさらに、リモートの、ローカルな、固定された、および/または取外し可能な記憶装置に加えて、コンピュータ読取可能情報を一時的および/またはさらには永続的に含むための記憶媒体をともに（または、随意には記憶装置620と組合せて）包括的に表わすコンピュータ読取可能記憶媒体に接続され得る。通信システム630は、データをネットワークおよび/または他のいずれかのコンピュータと交換することを可能にし得る。

#### 【0044】

コンピュータシステム600はまた、オペレーティングシステム645および/またはアプリケーションプログラムなどの他のコード650を含むワーキングメモリ640内に現在位置するものとして示されるソフトウェア要素を含み得る。アプリケーションプログラムは、アイデンティティプロバイダ、アイデンティティプロバイダの構成要素および/またはこの発明の方法を実現し得る。コンピュータシステム600の代替的な実施例が、上述したものからの多数の変形例を有し得ることが認識されるべきである。たとえば、カスタマイズされたハードウェアが用いられてもよく、および/または特定の要素がハードウェア、（アプレットなどのポータブルソフトウェアを含む）ソフトウェアもしくはその両方において実現されてもよい。さらに、ネットワーク入出力装置などの他の演算装置への接続が用いられてもよい。

40

#### 【0045】

50

図7は、ユーザ識別をマスキングするのに用いられ得る具体的な方法を示す。当該方法は、702でサービスプロバイダのためのメッセージを受信することから始まり得る。当該メッセージは、第1のユーザ識別子に関連付けられ、ユーザ装置のアクセスをネットワークに提供するアクセスプロバイダから受信され得る。ユーザアイデンティティをマスキングするのに用いられる第2の識別子が704で得られる。第2の識別子は、アイデンティティプロバイダ(たとえば、アイデンティティマネージャ204の構成要素)によって704で得られ得る。第2の識別子が予め得られていて、第1の識別子にマップされていてもよく、または第3の識別子が、ユーザにも関連付けられる第1の識別子にマップされていてもよい。代替的には、新しい識別子が作成され、第2の識別子のために用いられてもよい。

10

**【0046】**

メッセージに関連付けられる第1の識別子は706で当該メッセージから分離され、得られた第2の識別子が708でその場所においてメッセージに関連付けられる。こうして、第2の識別子を用いて、アイデンティティプロバイダに戻るようメッセージをルーティングし得るが、これにより第2の識別子を第1の識別子と置換え、ユーザに転送するためにアクセスプロバイダに送信することとなる。第2の識別子がメッセージに関連付けられた後、当該メッセージは710でサービスプロバイダに送信される。

**【0047】**

いくつかの実施例においては、セッションおよび/または個別化情報がまた、712で検索され得る。セッション情報は、得られた第2の識別子に関連付けられるセッションについてのセッション情報であってもよい。セッション情報は、ユーザが、セッション情報によって示される以前の状態でセッションプロバイダとの情報のやり取りを開始し得るように、714でサービスプロバイダに送信され得る。ユーザ嗜好、装置能力および他のユーザ個別化情報を特定する個別化情報がまた、714でサービスプロバイダに送信され得る。代替的には、サービスプロバイダは、識別子に関連付けられる個別化情報(または個別化情報のサブセット)にアクセスし得る。

20

**【0048】**

図8は、ユーザがアクセスプロバイダを切換えた場合にアイデンティティ管理を実行するのに用いられ得る具体的な方法を示す。702で第1のアクセスプロバイダから1つ以上のメッセージを受信した後、あるメッセージが、802で第2のアクセスプロバイダから受信され得る。当該メッセージは、第1のアクセスプロバイダが用いる同じユーザ識別子に関連付けられ得る。たとえば、このことは、ユーザが異なるネットワークにローミングするか、または、ユーザが、異なるアクセスプロバイダを用いてネットワークにアクセスする異なる装置に切換える場合に起こる可能性がある。代替的には、第2のアクセスプロバイダから受信したメッセージに関連付けられるユーザの第3の識別子は、第1のアクセスプロバイダから受信したメッセージに関連付けられる第1の識別子とは異なってもよい。802でメッセージが受信された後、第3の識別子が、702で第1のアクセスプロバイダから受信したメッセージに関連付けられる第1の識別子にマップされるという判断が下され得る。

30

**【0049】**

第3の識別子は、806でメッセージから分離される。第1の識別子に関連付けられるメッセージのための、704で得られたマスキングされた識別子は、第2のアクセスプロバイダからのメッセージに関連付けられる。次いで、メッセージが、801でサービスプロバイダに送信される。随意には、セッションおよび/または個別化情報も812で送信され得る。

40

**【0050】**

上述の説明においては、例示の目的で、方法が特定の順序で説明された。代替的な実施例においては、当該方法を記載されたものとは異なる順序で実行し得ることが認識されるべきである。加えて、当該方法は、記載されたものよりも少ないか、追加されているかまたは異なるブロックを含み得る。上述の方法が、ハードウェア構成要素によって実行され

50

得るかまたは機械実行可能命令 (machine-executable instructions) のシーケンスにおいて実現され得ることも認識されるはずであるが、当該機械実行可能命令は、当該命令でプログラミングされる汎用または特殊用途のプロセッサまたは論理回路などの機械に当該方法を実行させるのに用いられ得る。これらの機械実行可能命令は、1つ以上の機械読取可能媒体、たとえば、CD-ROMもしくは他の種類の光ディスク、フロッピー（登録商標）ディスク、ROM、RAM、EPROM、EEPROM、磁気もしくは光学カード、フラッシュメモリ、または電子命令を記憶するのに好適な他の種類の機械読取可能媒体に記憶され得る。代替的には、当該方法は、ハードウェアとソフトウェアとの組合せによって実行され得る。

【0051】

10

この発明の例示的で現在好ましい実施例をこの明細書中に詳細に説明してきたが、この発明の概念がさまざまに具体化および使用され得、添付の特許請求の範囲が、先行技術によって限定されている場合を除いて、このような変形例を含むものと解釈されるよう意図されることが理解されるべきである。

【図面の簡単な説明】

【0052】

【図1】アイデンティティ管理を用いるシステムの具体的な実施例を示す図である。

【図2】図1のアイデンティティプロバイダの具体的な実施例を示す図である。

【図3】アイデンティティ管理を用いるシステムの第2の具体的な実施例を示す図である。

20

【図4】アイデンティティ管理を用いるシステムの第3の具体的な実施例を示す図である。

【図5】現在利用可能ないくつかのモバイルネットワーク技術の簡単な比較を示す図である。

【図6】アイデンティティプロバイダが実現され得るコンピュータシステムを示すブロック図である。

【図7】ユーザ識別をマスキングする方法を示すフロー図である。

【図8】アクセスプロバイダを切替えるユーザのためのアイデンティティ管理を示すフロー図である。

【図1】

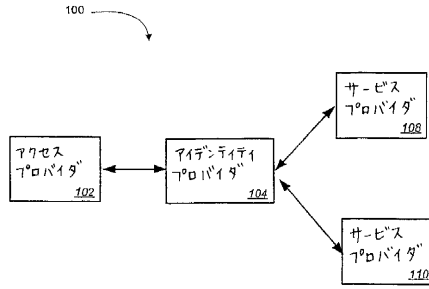


Fig. 1

【図2】

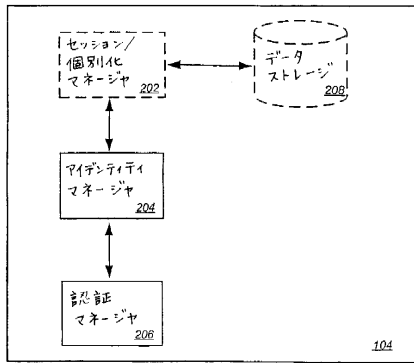


Fig. 2

【図3】

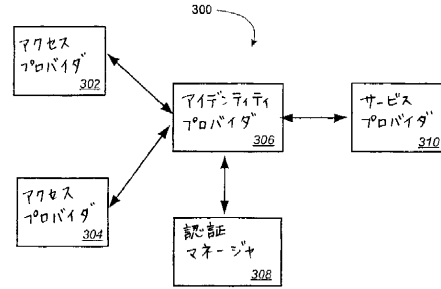


Fig. 3

【図4】

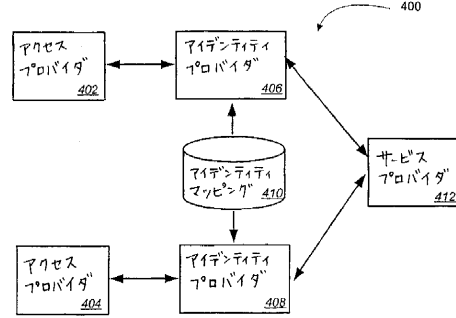


Fig. 4

【図5】

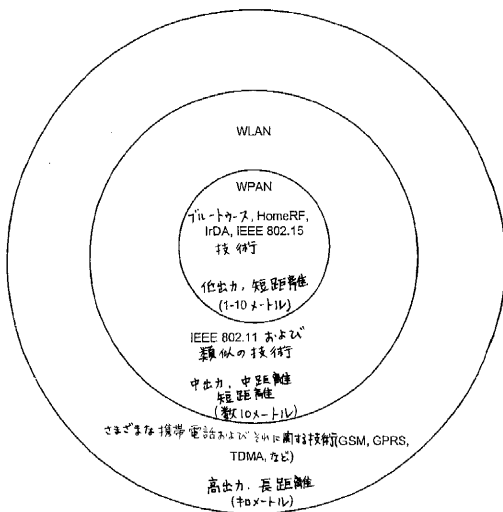


Fig. 5

【図6】

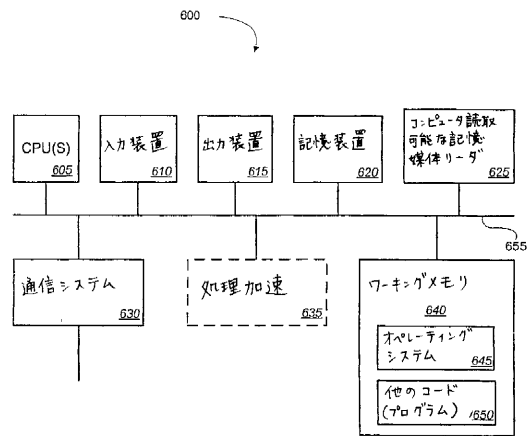


Fig. 6



【 図 7 】

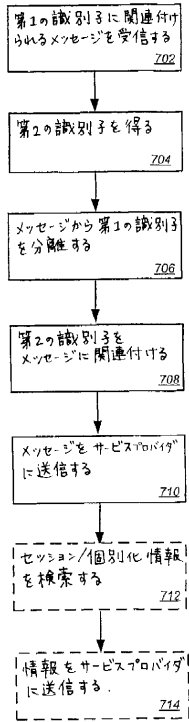


Fig. 7

【 図 8 】

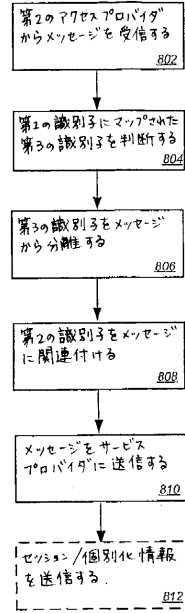


Fig. 8

---

フロントページの続き

(74)代理人 100098316

弁理士 野田 久登

(74)代理人 100109162

弁理士 酒井 将行

(72)発明者 マーズ, スティーブン・エイチ

アメリカ合衆国、9 4 5 3 9 カリフォルニア州、フリーモント、ネズ・パース・コート、1 0 9  
3

審査官 間野 裕一

(56)参考文献 国際公開第02/102016(WO, A2)

国際公開第02/33516(WO, A2)

国際公開第01/65380(WO, A1)

特開平11-120238(JP, A)

米国特許出願公開第2003/0140225(US, A1)

(58)調査した分野(Int.Cl., DB名)

G06F 21/20