(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5714690号
(P5714690)

(45)発行日　平成27年5月7日(2015.5.7)　(24)登録日　平成27年3月20日(2015.3.20)

(51)Int.Cl.		F I	
G06F 21/41	(2013.01)	G06F	21/41
G06F 21/33	(2013.01)	G06F	21/33
G06F 21/62	(2013.01)	G06F	21/62
G06F 21/10	(2013.01)	G06F	21/10

請求項の数 10　(全 16 頁)

(21)出願番号	特願2013-500154 (P2013-500154)
(86)(22)出願日	平成23年3月15日 (2011.3.15)
(65)公表番号	特表2013-522773 (P2013-522773A)
(43)公表日	平成25年6月13日 (2013.6.13)
(86)国際出願番号	PCT/US2011/028509
(87)国際公開番号	WO2011/115984
(87)国際公開日	平成23年9月22日 (2011.9.22)
審査請求日	平成26年3月5日 (2014.3.5)
(31)優先権主張番号	12/726,779
(32)優先日	平成22年3月18日 (2010.3.18)
(33)優先権主張国	米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】複数のウェブサービスにわたって認証を実施するプラグ可能なトークンプロバイダモデル

(57)【特許請求の範囲】

【請求項１】

コンピューティングデバイスにおいて実行される、プラグ可能なトークンプロバイダモデルを通じて複数のウェブサービスにわたってメッセージレベルの認証を行う方法であって、

クライアントアプリケーションのウェブサービスコンポーネントからウェブサービス要求を受け取るステップと、

前記要求されたウェブサービスに関連付けられたメタデータを突き止めるステップであって、前記メタデータが、前記要求されたウェブサービスの実行及び認証に関連付けられる情報を含む、ステップと、

前記メタデータを解析して複数のバインディングエントリにするステップと、

前記要求されたウェブサービスに資格情報が関連付けられているとき、前記資格情報を取得するステップと、

前記資格情報に基づいて、前記複数のバインディングエントリから適切なバインディングエントリを選択するステップであって、前記複数のバインディングエントリは、前記ウェブサービス要求が行われるリソースの識別子と、ウェブサービスメッセージに含まれるべき動作及び行為情報と、前記リソースによってサポートされる認証種類と、前記リソースに対応するセキュリティポリシー情報と、前記セキュリティポリシー内のトークン発行元識別子に基づくトークンプロバイダ識別情報とのうちの少なくとも１つを含む、ステップと、

前記取得した資格情報に関連付けられるトークンを取得するステップと、
前記取得したトークンと前記選択したバインディングエントリとに基づいて、前記要求されたウェブサービスを認証するステップと、
前記認証が成功したとき、前記要求されたウェブサービスを実施するステップと
を含む、方法。
【請求項２】
前記クライアントアプリケーション内のウェブサービスコンポーネント及びトークンプロバイダコンポーネントは、前記要求されたウェブサービスを定式化し理解するビジネス論理を動作させるコンポーネントとは分離される、請求項１に記載の方法。
【請求項３】
前記トークンプロバイダコンポーネントは、前記クライアントアプリケーションと対話するトークン発行元を表し、ＵＲＩと名前とのうちの一方によって識別される、請求項２に記載の方法。
【請求項４】
メタデータを維持するメタデータモデルコンポーネントは、前記ウェブサービスコンポーネントから取得されるウェブサービスメタデータとウェブサービスセキュリティ（ＷＳＳ）ポリシー情報とのうちの一方を用いて、前記トークンプロバイダコンポーネントを参照する、請求項３に記載の方法。
【請求項５】
前記メタデータモデルコンポーネントはさらに、メタデータ情報と、前記メタデータを供給するウェブサービスの識別子とのマッピングを維持する、請求項４に記載の方法。
【請求項６】
前記メタデータモデルコンポーネントが、前記メタデータを解析して、前記複数のバインディングエントリを維持し、前記メタデータが一度だけ取得され解析されるように、前記解析されたメタデータを保持する請求項４に記載の方法。
【請求項７】
ウェブサービスマネージャコンポーネントは、
前記メタデータモデルコンポーネントから前記メタデータを取得し、
前記複数のバインディングエントリをサイクルし、
前記要求されたウェブサービスと、関連付けられた認証種類とに基づいて、前記複数のバインディングエントリのうちの１つを選択し、
実際のウェブサービス要求を構築する
ように構成される、請求項４に記載の方法。
【請求項８】
資格情報マネージャコンポーネントは、前記ウェブサービスマネージャコンポーネントによって供給されるユーザ識別子に基づいて、前記要求されたウェブサービスに関連付けられた資格情報サービスを識別するように構成される、請求項７に記載の方法。
【請求項９】
プラグ可能なトークンプロバイダモデルを通じて複数のウェブサービスにわたってメッセージレベルの認証を行うためのコンピューティングデバイスであって、
プロセッサと、
前記プロセッサに接続され、クライアントアプリケーションを格納するメモリと
を備え、前記クライアントアプリケーションは、
少なくとも１つのウェブサービスコンポーネントと；
前記クライアントアプリケーションと対話するトークン発行元を表す、少なくとも１つのトークンプロバイダコンポーネントと；
ウェブサービスからメタデータを取得するメタデータモデルコンポーネントであって、前記メタデータは、要求されたウェブサービスの実行及び認証に関連付けられる情報を含む、メタデータモデルコンポーネントと；
前記メタデータモデルコンポーネントから前記メタデータを取得し、

前記メタデータモデルコンポーネントによって前記メタデータから解析された複数のバインディングエントリをサイクルすることであって、前記複数のバインディングエントリは、ウェブサービス要求が行われるリソースの識別子と、ウェブサービスメッセージに含まれるべき動作及び行為情報と、前記リソースによってサポートされる認証種類と、前記リソースに対応するセキュリティポリシー情報と、前記セキュリティポリシー内のトークン発行元識別子に基づくトークンプロバイダ識別情報とのうちの少なくとも１つを含み、

前記要求されたウェブサービスと、関連付けられた認証タイプとに基づいて、前記複数のバインディングエントリのうちの１つを選択し、

実際のウェブサービス要求を構築する

ように構成されたウェブサービスマネージャコンポーネントと；

を含む、コンピューティングシステム。

【請求項１０】

プラグ可能なトークンプロバイダモデルを通じて複数のウェブサービスにわたってメッセージレベルの認証を行うためのプログラムであって、コンピュータに、

クライアントアプリケーションのローカルウェブサービスコンポーネントから、ウェブサービスのコールのペイロードを受け取るステップと、

前記コールのベース識別子を抽出するステップと、

ウェブサービスのメタデータを要求しているメタデータモデルコンポーネントにコールするステップと、

前記メタデータを取得すると、前記メタデータ内の利用可能なバインディングをサイクルするステップであって、前記メタデータ内の前記利用可能なバインディングは、前記ウェブサービス要求が行われるリソースの識別子と、ウェブサービスメッセージに含まれるべき動作及び行為情報と、前記リソースによってサポートされる認証種類と、前記リソースに対応するセキュリティポリシー情報と、前記セキュリティポリシー内のトークン発行元識別子に基づくトークンプロバイダ識別情報とのうちの少なくとも１つを含む、ステップと、

前記要求されたウェブサービスに関連付けられた資格情報に応じて、要求される動作と認証種類とに基づいて適切なバインディングを選択するステップと、

実際のウェブサービスが構築されるように前記資格情報に関連付けられたトークンをフェッチするステップと

を実行させる、プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、複数のウェブサービスにわたってメッセージレベルの認証を行うプラグ可能なトークンプロバイダモデルを対象とする。

【背景技術】

【０００２】

クライアントアプリケーションがより複雑になってくるにつれて、かかるアプリケーションが相互作用する（interact with）ウェブサービスの数も増大してきている。多くのウェブサービスは、サーバに対して認証されたセッションを利用している。認証の標準方法のいくつかは、ＩＷＡ（Ｉｎｔｅｇｒａｔｅｄ　Ｗｉｎｄｏｗｓ（登録商標）　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）認証、ＭＴＬＳ（ｍｕｔｕａｌ　ｔｒａｎｓｐｏｒｔ　ｌｅｖｅｌ　ｓｅｃｕｒｉｔｙ）を用いたクライアント証明書ベースの認証、および様々な形態のメッセージレベルの認証の使用を含む。今日、ウェブサービスでは、ＷＳＳ（Ｗｅｂ　Ｓｅｒｖｉｃｅ　Ｓｅｃｕｒｉｔｙ）プロトコルを用いたメッセージレベルの認証が、その拡張性のため、増大する傾向にある。ＷＳＳメッセージ自体が、ケルベロスチケット、Ｘ．５０９証明書、またはＸＭＬトークン（例えば、ＳＡＭＬトークン）由来の認証トークンを担持することができる。

【０００３】
ウェブサービス実装は、認証トークンプロバイダを共有することができる。しかし、メッセージレベルの認証に使用されるトークン自体は、典型的には異なり、これは、トークンが有効化される対象のウェブサービスのターゲット名が異なることがあるからである。さらに、トークンプロバイダは、標準に基づいた、ライブラリを用いた独自の実装（ｐｒｏｐｒｉｅｔａｒｙ　ｉｍｐｌｅｍｅｎｔａｔｉｏｎ）、またはプロトコルを用いた独自の実装である場合がある。
【０００４】
したがって、通信クライアントが様々なウェブサービスで容易に認証を行うことができるように、異なる技術の統合を可能とする、利用可能な単一のインターフェイスが存在しない。さらに、企業サービスと、クラウドベースのサービスとの一体化に伴い、様々なウェブ技術を組み込み、それらのウェブ技術を認証することができる拡張可能なフレームワークで動作することが、企業クライアントの課題となっている。
【発明の概要】
【０００５】
この概要は、以下の詳細な説明でさらに説明する概念の抜粋を簡略化した形で示すものである。この概要は、特許請求する主題の重要な特徴または本質的な特徴を排他的に特定するためのものでも、特許請求する主題の範囲を決定する一助となるものでもない。
【０００６】
諸実施形態は、複数のウェブサービスにわたってメッセージレベルの認証を行うプラグ可能なトークンプロバイダモデルを対象とする。クライアントアプリケーション内のウェブサービス実装、およびトークンプロバイダ実装は、ウェブ要求を定式化し（ｆｏｒｍｕｌａｔｅ）理解するビジネス論理を動作させる実際のコンポーネントとは分離させることができる。ウェブサービスコンポーネントは、実行すべきウェブサービスを要求し、そのウェブサービスメッセージの本体を供給することができ、一方共通フレームワークは、それぞれのトークンに関連付けられた定義を含むウェブサービスメタデータを維持することができる。フレームワークは、認証トークンを実際にフェッチし、ウェブ要求を実施するトークンプロバイダ実装をさらに維持することができる。
【０００７】
上記およびその他の特徴および利点は、以下の詳細な説明を読み、関連する図面を検討することによって、明白となるであろう。前述の概要、および以下の詳細な説明はともに、説明のためのものであり、特許請求する態様を限定するものではないことを理解されたい。
【図面の簡単な説明】
【０００８】
【図１】複数のウェブサービスにわたってメッセージレベルの認証を行う諸実施形態を実装することができる、例示の統合通信システムを示す図である。
【図２】複数のウェブサービスにわたってメッセージレベルの認証を行うプラグ可能なモデルを実装するために使用することができる、クライアントアプリケーション内の様々なコンポーネント、および例示のサーバを示す概念図である。
【図３】諸実施形態によるクライアントアプリケーション内の、関連するコンポーネント、インターフェイス、および相互作用を示す図である。
【図４】諸実施形態によるシステムを実装することができる、ネットワーク化された環境を示す図である。
【図５】諸実施形態を実装することができる、例示のコンピューティング動作環境のブロック図である。
【図６】諸実施形態によるメッセージレベルの認証によってウェブサービスを提供する工程の論理流れ図である。
【発明を実施するための形態】
【０００９】

上記で簡単に説明したように、複数のウェブサービスにわたってメッセージレベルの認証を行うプラグ可能なトークンプロバイダモデルは、クライアントアプリケーション内のウェブサービス実装、およびトークンプロバイダ実装を、ウェブ要求を定式化し理解するビジネス論理を動作させる実際のコンポーネントとは分離させることによって、実装することができる。以下の詳細な説明では、本明細書の一部を成す添付の図面を参照し、これらの図面には、特定の実施形態または例が例示によって示されている。本開示の趣旨または範囲から逸脱することなく、上記の態様を組み合わせること、他の態様を使用すること、および構造の変更を行うことができる。したがって、以下の詳細な説明は、限定の意味で理解すべきではなく、本発明の範囲は、添付の特許請求の範囲、およびそれらの等価物によって規定される。

【００１０】

諸実施形態について、パーソナルコンピュータのオペレーティングシステムで実行するアプリケーションプログラムと共に実行するプログラムモジュールの一般的な例を取って説明するが、これらの態様は、他のプログラムモジュールと組み合わせて実装することもできることが、当業者には理解されよう。

【００１１】

一般に、プログラムモジュールは、ルーチン、プログラム、コンポーネント、データ構造、および特定のタスクを実施する、または特定の抽象データ型を実装する他の種類の構造を含む。さらに、諸実施形態は、ハンドヘルドデバイス、マルチプロセッサシステム、マイクロプロセッサベースの、またはプログラム可能なコンシューマエレクトロニクス、ミニコンピュータ、メインフレームコンピュータ、およびそれらに匹敵するコンピューティングデバイスを含めて、他のコンピュータシステム構成で実施することができることが、当業者には理解されよう。諸実施形態はまた、タスクが、通信ネットワークを介してリンクされたリモートプロセッシングデバイスによって実施される分散コンピューティング環境においても実施することができる。分散コンピューティング環境では、プログラムモジュールは、ローカルメモリ記憶装置、およびリモートメモリ記憶装置のどちらにも配置することができる。

【００１２】

諸実施形態は、コンピュータ実施工程（方法）、コンピューティングシステム、またはコンピュータプログラム製品、もしくはコンピュータ可読媒体などの製造物品として実装することができる。コンピュータプログラム製品は、コンピュータシステムによって可読であり、かつコンピュータ、またはコンピューティングシステムに例示の工程（複数可）を実施させる命令を含むコンピュータプログラムを符合化するコンピュータ記憶媒体でよい。コンピュータ可読記憶媒体は、例えば、１つまたは複数の揮発性コンピュータメモリ、不揮発性メモリ、ハードドライブ、フラッシュドライブ、フロッピー（登録商標）ディスク、またはコンパクトディスク、およびそれらに匹敵する媒体を介して実装することができる。

【００１３】

本明細書全体を通して、用語「プラットフォーム」とは、ウェブサービス、および関連するネットワーク通信を管理するソフトウェアコンポーネントと、ハードウェアコンポーネントとの組合せとすることができる。プラットフォームの例には、それだけに限られるものではないが、複数のサーバを介して実行されるホストサービス、単一のサーバで実行されるアプリケーション、およびそれらに匹敵するシステムが含まれる。用語「サーバ」とは、一般に、典型的にはネットワーク化された環境で１つまたは複数のソフトウェアプログラムを実行するコンピューティングデバイスを指す。しかし、サーバはまた、ネットワーク上でサーバとして見られる１つまたは複数のコンピューティングデバイスで実行される仮想サーバ（ソフトウェアプログラム）として実装することもできる。これらの技術、および例示の動作に関して、以下でより詳細に説明する。

【００１４】

図１は、複数のウェブサービスにわたってメッセージレベルの認証を行う諸実施形態を

実装することができる、例示の統合通信システム１００を示す。統合通信システムは、加入者に、幅広い範囲の能力およびサービスを提供することができる、最新の通信システムの一例である。統合通信システムは、インスタントメッセージング、プレゼンス、音声ビデオ会議、ウェブ会議、および類似の機能を促進するリアルタイム通信システムである。

【００１５】

統合通信（「ＵＣ」）システム１００では、ユーザは、ＵＣシステムのクライアントデバイスである、様々なエンドデバイス（１０２、１０４）を介して通信することができる。各クライアントデバイスは、音声通信、ビデオ通信、インスタントメッセージング、アプリケーション共有、データ共有などのための、１つまたは複数の通信アプリケーションを実行することが可能である。エンドデバイスは、その進歩した機能に加えて、ソーシャルネットワークへの参加、ウェブベースのドキュメント共有、検索、およびそれらに匹敵する機能など、様々なウェブサービスを促進するアプリケーションを実行することができる。さらに、これらのクライアントデバイスによって、ＰＢＸを介した「ＰＳＴＮ」（Ｐｕｂｌｉｃ Ｓｗｉｔｃｈｅｄ Ｔｅｌｅｐｈｏｎｅ Ｎｅｔｗｏｒｋ）への接続など、外部接続を介することによって、従来の電話通話、および類似の通信もやはり促進することができる。クライアントデバイスには、任意の種類のスマートフォン、携帯電話、通信アプリケーションを実行する任意のコンピューティングデバイス、スマート自動車コンソール、および追加の機能を有する先進の電話装置が含まれ得る。

【００１６】

ＵＣネットワーク（複数可）１１０は、異なるタスクを実施するいくつかのサーバを含むことができる。例えば、ＵＣサーバ１１４は、登録、プレゼンス、およびルーティングの機能を実現する。ルーティング機能では、システムは、ユーザに対するコールを、デフォルトおよび／またはユーザ設定のポリシーに基づいて、ユーザに割り当てられたクライアントデバイスのいずれにも回す（ｒｏｕｔｅ）ことが可能である。例えば、ユーザが通常の電話を利用できない場合、そのコールをユーザの携帯電話に転送することができ、そのコールに応答できない場合は、いくつかのボイスメールから選択して使用することができる。エンドデバイスは、追加の通信モードを扱うことができるので、ＵＣサーバ１１４は、アクセスサーバ１１２を介して、これらの追加の通信モード（例えば、インスタントメッセージング、ビデオ通信など）へのアクセスを実現することができる。アクセスサーバ１１２は、境界ネットワークに駐在し、ＵＣネットワーク（複数可）１１０を介して、他のユーザと追加の通信モードのうちの１つで接続することが可能である。ＵＣサーバ１１４は、上述の機能の組合せを実施するサーバ、または特定の機能だけを実現する専用サーバを含むことができる。例えば、プレゼンス機能を実現するホームサーバ、ルーティング機能を実現するルーティングサーバなどである。同様に、アクセスサーバ１１２は、ファイアウォール保護および接続などの複数の機能を実現する、または特定の機能だけを実現することができる。

【００１７】

Ａ／Ｖ（Ａｕｄｉｏ／Ｖｉｄｅｏ）会議サーバ１１８は、内部または外部ネットワークを介して、音声および／またはテレビ会議を促進することによって、そうした会議を実現する。仲介サーバ１１６は、シグナリングおよびメディアを、ＰＳＴＮまたは携帯電話網など他の種類のネットワークに、またはそこから取り次ぐ。仲介サーバ１１６はまた、ＳＩＰ（Ｓｅｓｓｉｏｎ Ｉｎｉｔｉａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）のユーザエージェントとして働く。

【００１８】

ＵＣシステムでは、ユーザは、１つまたは複数のＩＤを有することができ、ＩＤは必ずしも電話番号に限られるわけではない。ＩＤは、統合されたネットワークに依存して、電話番号、ＳＩＰ（Ｓｅｓｓｉｏｎ Ｉｎｉｔｉａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）ＵＲＩ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｉｄｅｎｔｉｆｉｅｒ）、または他の任意の識別子など、いかなる形も取ることができる。ＵＣシステムでは、いかなるプロトコルも使用することができるが、ＳＩＰが一般に使用されている方法である。

【００１９】
ＳＩＰは、１人または複数の参加者とのセッションを確立、変更、および終了するための、アプリケーション層制御（シグナリング）プロトコルである。ＳＩＰを用いて、インターネット電話通話、マルチメディア配信、およびマルチメディア会議を含めた、２パーティ、マルチパーティ、またはマルチキャストセッションを確立することができる。ＳＩＰは、下位のトランスポート層とは独立して設計される。
【００２０】
ＳＩＰクライアントは、「ＴＣＰ」（Ｔｒａｎｓｐｏｒｔ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）を用いて、ＳＩＰサーバ、および他のＳＩＰエンドポイントに接続することができる。ＳＩＰは主に、音声コールまたはビデオコールを開始または切断する際に使用される。しかし、ＳＩＰは、セッションの開始が要求されるいかなるアプリケーションにも使用することができる。これらのアプリケーションには、イベントサブスクリプションおよびイベント通知、ターミナルモビリティなどが含まれる。音声通信および／またはビデオ通信は、典型的には別個のセッションプロトコル、典型的には「ＲＴＰ」（Ｒｅａｌ Ｔｉｍｅ Ｐｒｏｔｏｃｏｌ）を介して行われる。
【００２１】
ＵＣシステムは、ソーシャルネットワーク、マルチモード企業通信、ウェブベースの共有サービス、および類似の環境のためのプラットフォームを提供することができる。加入者がかかる環境に参加すると、加入者は、１つまたは複数の外部サーバ（例えば１２２、１２４、および１２６）によって、またはＵＣシステム内部のサーバの１つによって管理されているウェブサービスを利用することができる。これらのサービスのいくつかでは、資格情報（ｃｒｅｄｅｎｔｉａｌ）に基づいた認証が要求されることがある。かかるサービスは、各クライアントアプリケーション内に実装されたウェブサービスコンポーネントによって促進することができる。諸実施形態によるシステムでは、クライアントアプリケーション内のウェブサービス実装、およびトークンプロバイダ実装は、ウェブサービスの実行を管理するウェブサービスマネージャコンポーネントとは分離させることができる。ウェブサービスマネージャコンポーネントは、ウェブサービスメタデータ、トークンプロバイダ実装、資格情報マネージャ、およびウェブ要求を実施するための関連するインターフェイスを維持する共通フレームワークの一部でよい。より詳細な例について、以下で論じる。
【００２２】
図１の例示のシステムでは、仲介サーバ、Ａ／Ｖサーバ、および類似の装置など、特定のコンポーネントを用いて説明してきたが、諸実施形態は、これらのコンポーネントまたはシステム構成に限られるものではなく、より少ない、または追加のコンポーネントを使用している他のシステム構成でも実装することができる。複数のウェブサービスにわたってメッセージレベルの認証を行うプラグ可能なモデルを使用したシステムの機能はまた、コンポーネントの能力、およびシステム構成に依存して、システムのコンポーネント間で異なるように分散させることもできる。さらに、諸実施形態は、統合通信システムに限られるものではない。本明細書で論じる手法は、ネットワーク化通信環境におけるいかなるデータ交換にも、本明細書に記載の原理を用いて応用することができる。
【００２３】
図２は、複数のウェブサービスにわたってメッセージレベルの認証を行うプラグ可能なモデルを実装するために使用することができる、クライアントアプリケーション内の様々なコンポーネント、および例示のサーバを示す概念図２００である。図２に示すように、諸実施形態によるシステムでは、ユーザ２２８は、クライアント２３０を介して様々なウェブサービスプロバイダと相互作用することができる。クライアント２３０は、１つまたは複数のアプリケーションを実行するコンピューティングデバイス、１つまたは複数のコンピューティングデバイスで実行されるアプリケーション、または分散された形で実行され、ユーザ２２８によってコンピューティングデバイスを介してアクセスされるサービスを指すことがある。典型的なシステムクライアント２３０は、そのクライアントのネット

ワーク内の通信を管理する１つまたは複数のサーバ（例えば、サーバ２４４）と通信することができる。ウェブサービスのいくつかは、サーバ２４４で利用可能なリソースを介して提供することができる。他のウェブサービスは、サーバ２４６で利用可能なリソースを介して提供することができ、これらのサーバ２４６は、ネットワークの内部にあっても、または外部にあってもよい。

【００２４】

クライアント２３０が相互作用するトークン発行元は、このモデルでは、トークンプロバイダコンポーネント２３４によって表すことができる。トークンプロバイダコンポーネント２３４は、そのＵＲＩ（Ｕｎｉｖｅｒｓａｌ Ｒｅｓｏｕｒｃｅ Ｉｄｅｎｔｉｆｉｅｒ）または名前で一意に識別することができ、これらのトークンプロバイダコンポーネント２３４は、メタデータモデルコンポーネント２４０によって、ウェブサービスコンポーネント２３２からフェッチされたウェブサービスメタデータ、またはＷＳＳポリシー情報を用いて参照することができる。

【００２５】

メタデータモデルコンポーネント２４０は、ウェブサービス（複数可）に関連付けられた情報を維持する働きをする。メタデータは、ＷＳＤＬ－メタデータまたはＷＳ－ＭＥＸのような標準の機構を使用してフェッチすることができる。メタデータを取得すると、メタデータモデルコンポーネント２４０は、メタデータ情報と、そのメタデータを供給するウェブサービスの識別子（例えば、「ＵＲＬ」（Ｕｎｉｖｅｒｓａｌ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）とのマッピングを維持することができる。メタデータモデルコンポーネント２４０はまた、アプリケーションが開始する度に、解析および取得サイクルが繰り返されないように、メタデータ情報をファイル、または類似の保持記憶域に保持することができる。

【００２６】

諸実施形態による、ウェブサービス要求およびウェブサービス応答を実施および／または消化する（ｃｏｎｓｕｍｅ）コンポーネントは、下位のトークンプロバイダ、およびメタデータフレームワークに依存しなくてもよい。これらのコンポーネントは、行われるウェブサービスコールのペイロード（例えば、ウェブサービスの「ＳＯＡＰ」（Ｓｉｍｐｌｅ Ｏｂｊｅｃｔ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）」では本体）を単に供給することができる。特定のコールが行われると、ウェブサービスマネージャコンポーネント２３８は、そのコールのベース識別子を抽出し、メタデータモデルコンポーネント２４０にコールして、ウェブサービスメタデータを要求する。メタデータを取得すると、ウェブサービスマネージャコンポーネント２３８は、メタデータ中の利用可能な完全なバインディングをサイクルし、要求された動作と、資格情報マネージャコンポーネント２３６によって供給される資格情報に依存した認証種類とに基づいて、適切なものを選択することができる。次いで、トークンプロバイダコールを行ってトークンをフェッチすることができ、ウェブサービスマネージャコンポーネント２３８は、これらの情報を組み合わせて、実際のウェブサービス要求（例えば、ＳＯＡＰ要求）を構築することができる。

【００２７】

資格情報マネージャコンポーネント２３６は、ユーザ識別子を用いて、資格情報サービス（「ログオンサービス」としても知られる）を識別することができる。資格情報サービスを実装している他のコンポーネントによって、資格情報マネージャコンポーネント２３６に対して行われるコールは、コールが行われる状況において、識別子を特定することができる。資格情報マネージャコンポーネント２３６は、複数の種類の資格情報を扱うことができる。諸実施形態によるシステムで使用することができる資格情報の例には、それだけに限られるものではないが、ユーザ名／パスワード、証明書、個人識別番号、およびそれらに匹敵するものが含まれる。資格情報マネージャコンポーネント２３６は、ユーザに資格情報を照会するか、またはシステム内固有の資格情報の任意のものを発行することができる。システム内固有の資格情報には、その時点でオペレーティングシステムにログインしたユーザの資格情報が含まれ得、この資格情報は、システムコールによってフェッチ

することができる。資格情報を照会すべき場合は、ユーザインターフェイスに、プロンプトを表示するコマンドを与えることができる。このプロンプトは、ユーザがキャンセルを実行可能にすることによって、または資格情報を供給して応答することによって解除することができる。

【００２８】

資格情報マネージャコンポーネント２３６に資格情報が供給されると、この資格情報をコンポーネントのデータモデルに保存して、後に使用することができる。モデルへの保存は、揮発性でよく、アプリケーションをシャットダウンする、または別のユーザがそのアプリケーションにログインすると、消去される。資格情報は、暗号化後、不揮発性メモリに記憶することもでき、オペレーティングシステムコールが、この目的で使用される。資格情報マネージャコンポーネント２３６が利用可能なあらゆる資格情報について、このコンポーネントは、（識別子によって表される）各サービスと、そのサービスのサクセスレコード間のサクセスレコードマップの実行中コピーを維持することができる。サクセスレコードは、「不明」、「成功」、または「失敗」の３つの状態のうちの１つにあることになる。「不明」状態は、特定の資格情報が資格情報サービスによって使用されたことがない場合に、設定され得る。そのサービスからの資格情報マネージャに対するその後のいかなるコールも、この資格情報を与えることができる。「成功」状態のサクセスレコードは、資格情報に対するサービスの成功使用例を記録することができ、失敗が報告されるまで、そのサービスは、同じ資格情報を使用することができる。資格情報マネージャコンポーネント２３６に対して、成功したサービス識別子を求めてさらにコールすることによって、「成功」の資格情報を返すことができる。「失敗」状態は、サービスの資格情報に対するログオン失敗を記録することができる。かかる資格情報は、システムがリセットされるまで、そのサービスで再度使用することができない。

【００２９】

さらに、資格情報マネージャコンポーネント２３６は、レジストリ、ファイル、および／または資格情報マネージャＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍｍｉｎｇ　Ｉｎｔｅｒｆａｃｅ）のようなシステムリソースを使用することによって、アプリケーションを再起動しても、資格情報を保持することができる。資格情報は、セキュリティのために暗号化することができる。ウェブサービストランスポートコンポーネント２４２は、サーバ２４４で実行されるものなどの他のアプリケーション／サービスとの通信インターフェイスとなることができる。

【００３０】

クライアント２３０のコンポーネントと、外部リソースとの間でメッセージ（コール）の交換について、ＳＯＡＰおよびＷＳＳなどの例示のプロトコルについて上記で説明してきた。ＳＯＡＰ（Ｓｉｍｐｌｅ　Ｏｂｊｅｃｔ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）は、コンピュータネットワークにおいて、ウェブサービスの実装に関する構造化された情報を交換するためのプロトコル仕様である。このプロトコルは、ＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）をそのメッセージ形式として利用し、通常は他のアプリケーション層プロトコルに依存し、最も顕著には、ＲＰＣ（Ｒｅｍｏｔｅ　Ｐｒｏｃｅｄｕｒｅ　Ｃａｌｌ）、およびＨＴＴＰを用いて、メッセージ交渉、およびメッセージ伝達を行う。ＳＯＡＰメッセージは、以下の３つの部分、すなわちメッセージの内容、およびその内容をどのように処理するかを定義するエンベロープと、ＳＯＡＰノードがメッセージ経路に沿って処理すべきアプリケーションに関連する情報を含むヘッダと、メッセージの最終的な受信者向けの情報を含む本体とを含むことができる。

【００３１】

ＳＯＡＰアーキテクチャは、メッセージ形式、メッセージ交換パターン、下位のトランスポートプロトコルのバインディング、メッセージ処理モデル、およびプロトコル拡張用のいくつかの仕様層を含む。ＷＳＳ（Ｗｅｂ　Ｓｅｒｖｉｃｅｓ　Ｓｅｃｕｒｉｔｙ）はフレキシブルであり、ＳＯＡＰに対して、ウェブサービスにセキュリティ機構を適用する機能豊富な拡張性を有する。ＷＳＳは、以下の３つの主な機構、すなわちＳＯＡＰメッセ

ージに署名して完全性を保証する方式、ＳＯＡＰメッセージを暗号化して機密性を保証する方式、およびセキュリティトークンを付与する方式について記述している。この仕様では、様々な署名形式、暗号化アルゴリズム、信頼領域（ｔｒｕｓｔ　ｄｏｍａｉｎ）、およびセキュリティトークンモデル（例えば、Ｘ．５０９証明書、ケルベロスチケット、ユーザＩＤ／パスワード資格情報、ＳＡＭＬアサーション、およびカスタム定義トークン）が可能となっている。

【００３２】

図３を参照すると、諸実施形態による、クライアントアプリケーション内の関連するコンポーネント、インターフェイス、および相互作用の例３００が示されている。先に論じたように、クライアントが相互作用するトークン発行元は、クライアントのトークンプロバイダコンポーネント３６６、３６８、３７０によって表すことができる。トークンプロバイダコンポーネント３６６、３６８、３７０は、メタデータモデルコンポーネント３６４によって、ウェブサービスコンポーネント３５２、３５４、３５６、および３５８からフェッチされたウェブサービスメタデータ、またはＷＳＳポリシー情報を用いて参照することができる。図３に示すように、特定の目的に特殊化できる汎用実装を持たせることによって、複数のトークンプロバイダを実装することができる。いくつかの実施形態によるクライアントアプリケーションでは、トークンプロバイダコンポーネント３６６、３６８、３７０は、トークンが与えられることになるターゲットが供給されたときに、そのターゲットに対応するトークンを供給するＧｅｔＴｏｋｅｎ（）インターフェイス（３７８、３８０、および３８２）を公開（ｅｘｐｏｓｅ）することができる。トークンは、有効である限り、キャッシュに入れることができ、有効期限後、トークンプロバイダに対するコールが行われたときに、自動的に更新することができる。トークンプロバイダコンポーネント３６６、３６８、３７０は、メタデータモデルコンポーネント３６４のＲｅｇｉｓｔｅｒＴｏｋｅｎＰｒｏｖｉｄｅｒ（）インターフェイス３７６にコールすることによって、メタデータモデルコンポーネント３６４に登録することができる。登録によって、トークン発行元の名前（例えば一意の名前）またはＵＲＩを供給することができる。

【００３３】

メタデータモデルコンポーネント３６４は、ウェブサービス（複数可）に関連付けられた情報を維持する働きをする。メタデータ情報は、解析し、一連のバインディングエントリとして維持することができる。各バインディングエントリは、ウェブサービス要求が行われる実際のエンドポイントＵＲＩ、ウェブサービスのＳＯＡＰ動作情報および行為情報、エンドポイントで支持される認証種類、エンドポイントに対応するセキュリティポリシー情報、および／またはセキュリティポリシーのトークンプロバイダに基づいたトークン発行元ＵＲＩを含むことができる。

【００３４】

ＧｅｔＴｏｋｅｎ（）インターフェイス（３７８、３８０、３８２）コールが行われると、トークンプロバイダコンポーネントが取得することができる異なる種類のトークンを支持するように、セキュリティポリシー情報を含めることができる。例えば、セキュリティポリシーは、トークンプロバイダコンポーネントが、トークン発行元に対してＲｅｑｕｅｓｔＳｅｃｕｒｉｔｙＴｏｋｅｎコールを実際に生成するために使用することができる動作環境キーを有することができる。メタデータを取得すると、メタデータモデルコンポーネント３６４は、アプリケーションが開始する度に、解析および取得サイクルが繰り返されないように、メタデータ情報をファイル、または類似の保持記憶域に保持することができる。

【００３５】

ウェブサービスマネージャコンポーネント３６０は、そのＥｘｅｃｕｔｅＷｅｂＲｅｑｕｅｓｔ（）インターフェイス３７２を介して、特定のウェブサービスを求めるコールを受け取り、そのコールのベース識別子を抽出することができる。次いで、ウェブサービスマネージャコンポーネント３６０は、メタデータモデルコンポーネント３６４のＧｅｔＭｅｔａｄａｔａ（）インターフェイス３７４にコールして、ウェブサービスメタデータを

要求することができる。メタデータを取得すると、ウェブサービスマネージャコンポーネント３６０は、メタデータ中の利用可能な完全なバインディングをサイクルし、要求された動作と、資格情報マネージャコンポーネントによって供給される資格情報に依存した認証種類とに基づいて、適切なものを選択することができる。次いで、トークンプロバイダコールを行って関連するトークンをフェッチすることができ、ウェブサービスマネージャコンポーネント３６０は、これらの情報を組み合わせて、実際のウェブサービス要求を構築することができる。特定の要求について、メタデータモデルコンポーネント３６４で利用可能なメタデータがない場合、メタデータモデルコンポーネント３６４は、関連するウェブサービスに対してダウンロードコールを行うことができる。先に論じたように、ウェブサービストランスポートコンポーネント３６２は、クライアント内のコンポーネントと、他のコンピューティングデバイスで実行される他のアプリケーション／サービスとの間のインターフェイスサービスを提供する。

【００３６】

図１、２、および３の例示のシステムを、特定のサーバ、クライアントデバイス、ソフトウェアモジュール、および相互作用について説明してきた。諸実施形態は、これらの例示の構成によるシステムに限られるものではない。複数のウェブサービスにわたってメッセージレベルの認証を行うプラグ可能なトークンプロバイダモデルは、より少ない、または追加のコンポーネントを使用し、かつ他のタスクを実施する構成でも実装することができる。さらに、特定のプロトコル、コール、およびインターフェイスについて、上述の諸実施形態に関して論じてきた。諸実施形態はやはり、それらの例に限定されるものではない。他のプロトコル、交換、インターフェイスを、本明細書に記載の原理を用いて同様に実装することができる。

【００３７】

図４は、諸実施形態を実装することができる、例示のネットワーク化された環境である。複数のウェブサービスにわたって認証を行うプラグ可能なトークンプロバイダモデルを実現するプラットフォームは、ホストサービスなど、１つまたは複数のサーバ４１４を介して実行されるソフトウェアを介して実装することができる。このプラットフォームは、ネットワーク（複数可）４１０を介して、スマートフォン４１３、ラップトップコンピュータ４１２、またはデスクトップコンピュータ４１１など（「クライアントデバイス」）の個々のコンピューティングデバイスのクライアントアプリケーションと通信することができる。

【００３８】

上記で論じたように、クライアントデバイス４１１～４１３のいずれかで実行されるクライアントアプリケーションは、別個のウェブサービスコンポーネント、トークンプロバイダコンポーネント、ウェブサービス管理コンポーネント、および資格情報管理コンポーネントを含むことができる。これらのコンポーネントは、上記で説明したように、メタデータモデルによって、ウェブサービス要求に関する認証を管理することができる。サーバ４１４の１つまたは複数のサーバ、あるいは単一のサーバ４１６で実行される通信サービスまたはアプリケーションは、クライアントデバイス４１１～４１３を介して、ユーザからの要求（複数可）を受け取り、関連するデータをデータストア（複数可）４１９から直接、またはデータベースサーバ４１８を介して受け取り、要求されたウェブサービスをユーザ（複数可）に提供することができる。

【００３９】

ネットワーク（複数可）４１０は、いかなるトポロジのサーバ、クライアント、インターネットサービスプロバイダ、および通信媒体も備えることができる。諸実施形態によるシステムは、静的トポロジ、または動的トポロジを有することができる。ネットワーク（複数可）４１０には、例えば企業ネットワークなどのセキュリティで保護されたネットワーク、無線オープンネットワーク、またはインターネットなどのセキュリティで保護されていないネットワークが含まれ得る。ネットワーク（複数可）４１０はまた、ＰＳＴＮ（Ｐｕｂｌｉｃ　Ｓｗｉｔｃｈｅｄ　Ｔｅｌｅｐｈｏｎｅ　Ｎｅｔｗｏｒｋ）または携帯電

話網など、他のネットワークを介した通信をコーディネートすることができる。さらに、ネットワーク（複数可）４１０は、ブルートゥースまたは類似のものなどの近距離無線ネットワークを含むことができる。ネットワーク（複数可）４１０は、本明細書に記載のノード間での通信を実現する。限定ではなく、例によって示すものであるが、ネットワーク（複数可）４１０には、アコースティック、ＲＦ、赤外線、および他の無線媒体などの無線媒体が含まれ得る。

【００４０】

他の多くの構成のコンピューティングデバイス、アプリケーション、データソース、およびデータ配信システムを使用して、複数のウェブサービスにわたてメッセージレベルの認証を行うフレームワークを実装することができる。さらに、図４で論じるネットワーク化された環境は、単なる例示の目的のものにすぎない。諸実施形態は、例示のアプリケーション、モジュール、または工程に限られるものではない。

【００４１】

図５および関連する考察は、諸実施形態を実装することができる適切なコンピューティング環境の簡潔で一般的な説明を行うためのものである。図５を参照すると、コンピューティングデバイス５００など、諸実施形態によるアプリケーション用の例示のコンピューティング動作環境のブロック図が示されている。基本の構成では、コンピューティングデバイス５００は、諸実施形態によるクライアントアプリケーションを実行するクライアントデバイスでよく、少なくとも１つの処理装置５０２、およびシステムメモリ５０４を含む。コンピューティングデバイス５００はまた、プログラムを実行する際に協働する複数の処理装置を含むことができる。コンピューティングデバイスの正確な構成、および種類に依存して、システムメモリ５０４は、揮発性（ＲＡＭなど）、不揮発性（ＲＯＭ、フラッシュメモリなど）、またはそれら２つの何らかの組合せでよい。システムメモリ５０４は、典型的には、本件特許出願人によるＷＩＮＤＯＷＳ（登録商標）オペレーティングシステムなど、プラットフォームの動作を制御するのに適したオペレーティングシステム５０５を含む。システムメモリ５０４はまた、プログラムモジュール５０６、通信クライアントアプリケーション５２２、およびコンポーネント５２４など、１つまたは複数のソフトウェアアプリケーションを含むことができる。

【００４２】

通信クライアントアプリケーション５２２は、コンピューティングデバイス５００の他のアプリケーションおよび／またはモジュールと、要求されたウェブサービスに関連するサーバとの間の通信を促進するいかなるアプリケーションでもよい。コンポーネント５２４には、先に論じたように、ウェブサービスコンポーネント、トークンプロバイダ、ウェブサービスマネージャ、資格情報マネージャ、およびメタデータモデルが含まれ得る。ウェブサービス要求は、コンポーネント間の相互作用によって遂行されるメッセージレベルの認証によって実施することができる。通信クライアントアプリケーション５２２は、別個のアプリケーションでも、またはクライアントデバイスに高機能の通信サービスを提供する、ホストサービスの一体型モジュールでもよい。この基本の構成を、破線５０８内のコンポーネントによって図５に例示する。

【００４３】

コンピューティングデバイス５００は、追加の特徴または機能を有することができる。例えば、コンピューティングデバイス５００はまた、例えば、磁気ディスク、光ディスク、またはテープなどの（取外し可能な、かつ／または取外し不可能な）追加のデータ記憶装置を含むことができる。かかる追加の記憶装置は、図５では、取外し可能な記憶装置５０９、および取外し不可能な記憶装置５１０によって示してある。コンピュータ可読記憶媒体には、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなど、情報を記憶する任意の方法または技術で実装される、揮発性、および不揮発性の、取外し可能な媒体、および取外し不可能な媒体が含まれ得る。システムメモリ５０４、取外し可能な記憶装置５０９、および取外し不可能な記憶装置５１０は全て、コンピュータ可読記憶媒体の例である。コンピュータ可読記憶媒体には、それだけに限られるもので

はないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、または他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤ（ｄｉｇｉｔａｌ　ｖｅｒｓａｔｉｌｅ　ｄｉｓｋ）、または他の光記憶装置、磁気テープ、磁気ディスク記憶装置、または他の磁気記憶装置、あるいは所望の情報を記憶するために使用することができ、かつコンピューティングデバイス５００によってアクセスすることができる他の任意の媒体が含まれる。かかるコンピュータ可読記憶媒体はいずれも、コンピューティングデバイス５００の一部となることができる。コンピューティングデバイス５００はまた、キーボード、マウス、ペン、音声入力装置、タッチ入力装置、およびそれらに匹敵する入力装置などの入力装置（複数可）５１２を有することができる。ディスプレイ、スピーカ、プリンタ、および他の種類の出力装置などの出力装置（複数可）５１４もやはり、含めることができる。これらの装置は、当技術分野で周知であり、本明細書で詳細に論じる必要はない。

【００４４】

コンピューティングデバイス５００はまた、分散コンピューティング環境の有線または無線ネットワーク、衛星リンク、携帯電話リンク、近距離ネットワーク、およびそれらに匹敵する機構などを介して、このデバイスを他のデバイス５１８と通信可能とする通信接続部５１６を含むことができる。他のデバイス５１８には、通信アプリケーション実行するコンピュータデバイス（複数可）、他のウェブサーバ、およびそれらに匹敵する装置が含まれ得る。通信接続部（複数可）５１６は、通信媒体の一例である。通信媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータをその中に含むことができる。限定ではなく、例によって示すものであるが、通信媒体には、有線ネットワーク、または直接有線接続などの有線媒体、およびアコースティック、ＲＦ、赤外線、および他の無線媒体などの無線媒体が含まれる。

【００４５】

例示の諸実施形態はまた、方法を含む。これらの方法は、本明細書に記載の構造を含めて、多くの方策で実施することができる。かかる方策の１つは、本明細書に記載の種類の装置の機械動作によって実施される。

【００４６】

任意選択による別の方策は、実施すべき方法の個々の操作の１つまたは複数のための方策であり、１人または複数の人間のオペレータがいくつかを実施する。これらの人間のオペレータは、互いに併存している（ｃｏｌｌｏｃａｔｅ）必要はなく、各自がプログラムの一部を実施する機械に向かっていればよい。

【００４７】

図６は、諸実施形態による、メッセージレベルの認証によってウェブサービスを提供する工程（ｐｒｏｃｅｓｓ）６００の論理流れ図を示す。工程６００は、高機能の通信システムに参加するクライアントアプリケーションの一部として実装することができる。

【００４８】

工程６００は、クライアントアプリケーション内のウェブサービスコンポーネントからのウェブサービス要求を、ウェブサービスマネージャコンポーネントで受け取る動作６１０から開始する。動作６２０で、ウェブサービスマネージャコンポーネントは、要求されたウェブサービスに関連付けられたメタデータを突き止めることができる。判定動作６３０で、ウェブサービスマネージャコンポーネントが、資格情報が必要であると判定した場合、処理は動作６４０に進み、ここで、資格情報マネージャコンポーネントから資格情報が取得される。そうでない場合には、処理は、動作６７０にスキップすることができ、ここで要求されたウェブサービスが、ウェブサービスマネージャコンポーネントの管理下で提供される。資格情報マネージャコンポーネントは、単一のユーザＩＤを複数ウェブサービスと関連付けることによって、または複数のユーザＩＤを単一のウェブサービスと関連付けることによって、複数種の資格情報を扱うことができる。

【００４９】

資格情報（複数可）の取得後、動作６５０で、取得した資格情報（複数可）に関連付けられたトークンを、トークンプロバイダコンポーネントから要求することができる。メタ

データは、サービスごとにトークンをフェッチするように設定可能に処理することができる。ウェブサービスごとにトークンプロバイダコンポーネントがあってもよく（サービスごとのトークンプロバイダ）、これらのトークンプロバイダコンポーネントと、ウェブサービスとは、静的にバインディングされるか、または動的にバインディングされる。この後、動作６６０が続き、ここで、ウェブサービスマネージャコンポーネントは、要求されたウェブサービスの認証を、受け取ったトークンに基づいて監督する。認証が成功した場合、動作６７０で、要求されたウェブサービスを提供することができる。

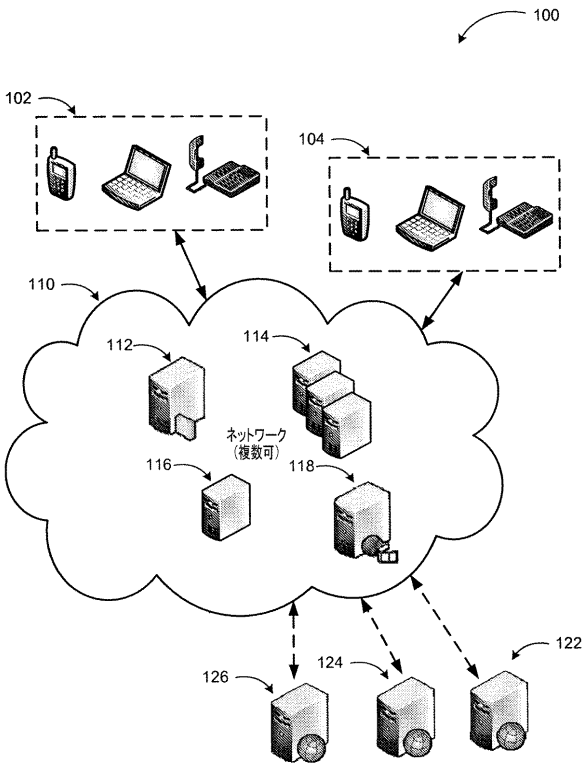
【００５０】

工程６００に含まれる動作は、例示の目的である。複数のウェブサービスにわたってメッセージレベルの認証を行うプラグ可能なトークンプロバイダモデルは、より少ない、または追加のステップを含む類似の工程によって実施することができ、また、本明細書に記載の原理を用いて、異なる動作順序でも同様に実施することができる。

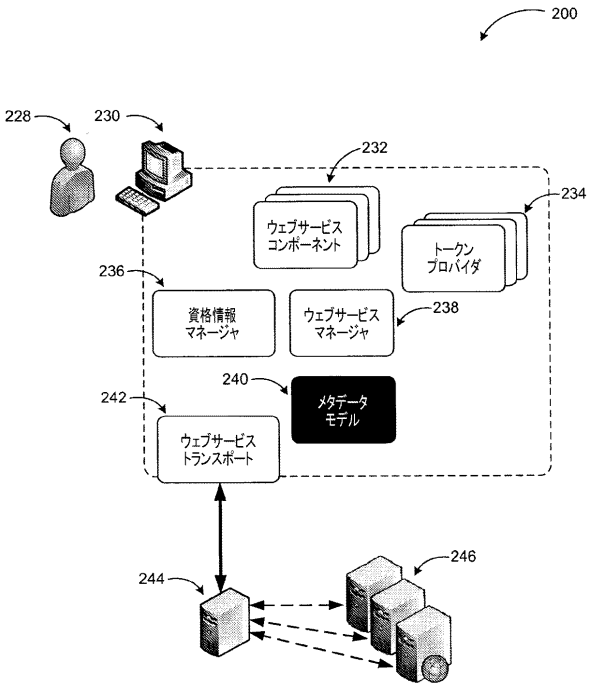
【００５１】

上述の仕様、例、およびデータは、諸実施形態の組成の製造および使用について完全に説明するためのものである。構造上の特徴および／または方法的行為に特定の言語で本主題を説明してきたが、添付の特許請求の範囲に規定される主題は、必ずしも上述の特定の特徴または行為に限られるものではないことを理解されたい。そうではなく、上述の特定の特徴および行為は、特許請求の範囲、および諸実施形態を実装する例示の形態として開示するものである。

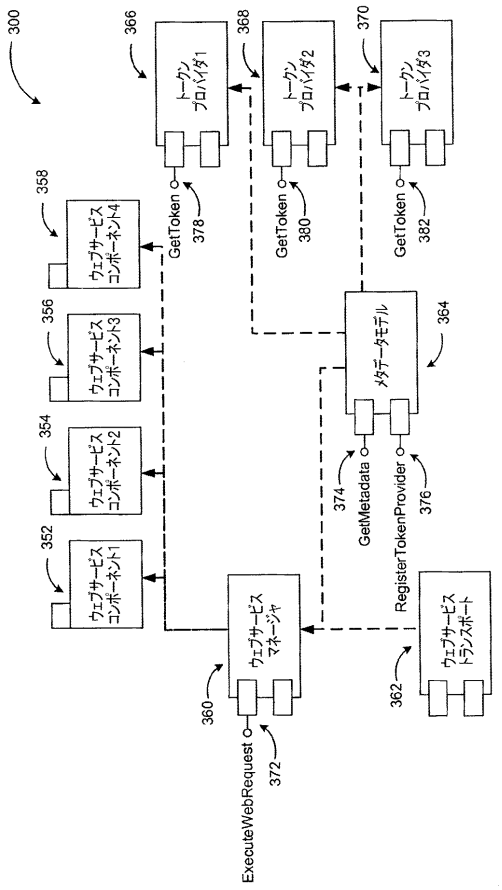
【図１】



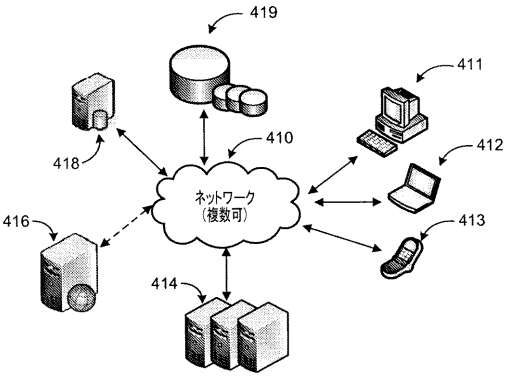
【図２】



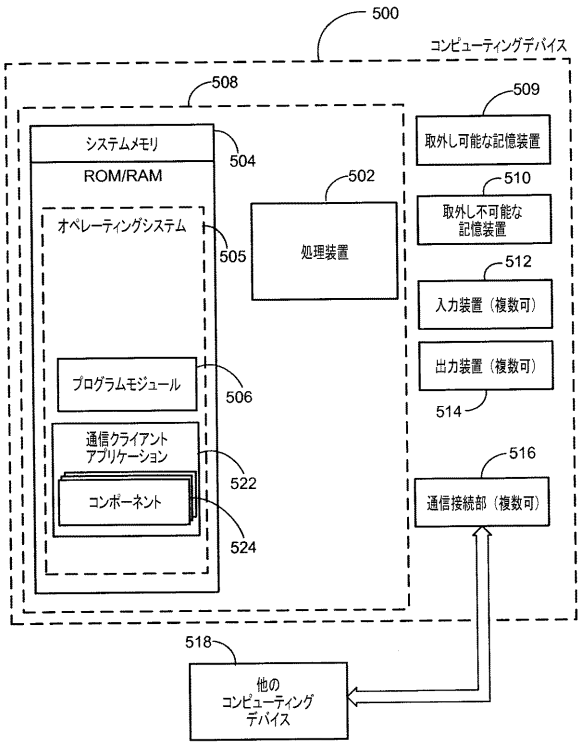
【図３】


300
366
トークンプロバイダ1
368
トークンプロバイダ2
370
トークンプロバイダ3
358
ウェブサービスコンポーネント4
356
ウェブサービスコンポーネント3
354
ウェブサービスコンポーネント2
352
ウェブサービスコンポーネント1
GetToken
378
GetToken
380
GetToken
382
メタデータモデル
364
GetMetadata
374
RegisterTokenProvider
376
ウェブサービスマネージャ
360
ウェブサービストランスポート
362
ExecuteWebRequest
372

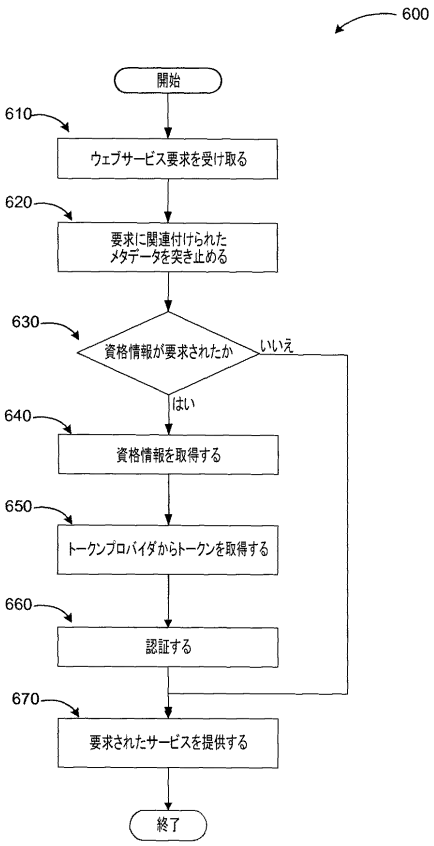
【図４】


419
411
418
410
412
ネットワーク
（複数可）
416
413
414

【図５】


500
コンピューティングデバイス
508
システムメモリ
ROM/RAM
504
オペレーティングシステム
505
プログラムモジュール
506
通信クライアントアプリケーション
522
コンポーネント
524
処理装置
502
509
取外し可能な記憶装置
510
取外し不可能な記憶装置
512
入力装置（複数可）
出力装置（複数可）
514
516
通信接続部（複数可）
518
他のコンピューティングデバイス

【図６】


600
開始
610
ウェブサービス要求を受け取る
620
要求に関連付けられたメタデータを突き止める
630
資格情報が要求されたか
いいえ
はい
640
資格情報を取得する
650
トークンプロバイダからトークンを取得する
660
認証する
670
要求されたサービスを提供する
終了

フロントページの続き

(72)発明者　ランジス　ナラヤナン
アメリカ合衆国　９８０５２－６３９９　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション　エルシーエー－インターナショナル　パテンツ内
(72)発明者　ルイ　リアン
アメリカ合衆国　９８０５２－６３９９　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション　エルシーエー－インターナショナル　パテンツ内
(72)発明者　スリバトサ　スリニバサン
アメリカ合衆国　９８０５２－６３９９　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション　エルシーエー－インターナショナル　パテンツ内

審査官　脇岡　剛

(56)参考文献　国際公開第２００８／１３０７６０（WO，Ａ１）
特開２００９－１５１７５５（ＪＰ，Ａ）
特開２００５－３２２２３４（ＪＰ，Ａ）
特開２００５－２０２９７２（ＪＰ，Ａ）
特開２００９－１９３４３５（ＪＰ，Ａ）
特表２０１０－５０６５１１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４１
Ｇ０６Ｆ　２１／１０
Ｇ０６Ｆ　２１／３３
Ｇ０６Ｆ　２１／６２