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

特許第5334332号
(P5334332)

(45)発行日　平成25年11月6日(2013.11.6)　(24)登録日　平成25年8月9日(2013.8.9)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/20	131A
G06F 21/32	(2013.01)	G06F	21/20	131D
G06F 21/33	(2013.01)	G06F	21/20	132
H04L 9/32	(2006.01)	G06F	21/20	133
		H04L	9/00	673A

請求項の数 9　(全 19 頁)　最終頁に続く

(21)出願番号　特願2010-504132 (P2010-504132)
(86)(22)出願日　平成20年3月18日 (2008.3.18)
(65)公表番号　特表2010-525448 (P2010-525448A)
(43)公表日　平成22年7月22日 (2010.7.22)
(86)国際出願番号　PCT/US2008/057375
(87)国際公開番号　WO2008/130760
(87)国際公開日　平成20年10月30日 (2008.10.30)
審査請求日　平成23年3月15日 (2011.3.15)
(31)優先権主張番号　60/912,986
(32)優先日　平成19年4月20日 (2007.4.20)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　12/024,901
(32)優先日　平成20年2月1日 (2008.2.1)
(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　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100153028
弁理士　上田　忠

最終頁に続く

(54)【発明の名称】ウェブサービスリソースにアクセスするためのリクエスト専用認証

(57)【特許請求の範囲】

【請求項１】

保護されたウェブサービスリソースへのアクセスを制御するコンピュータシステムであって、前記コンピュータシステムは、

通信ネットワークを介して通信を行う通信装置と、

前記通信装置に通信接続されたプロセッサと、

コンピュータ実行可能命令を格納したメモリであって、前記コンピュータ実行可能命令が前記プロセッサによって実行されるときに、前記プロセッサに、

前記通信ネットワークを介してクライアントコンピュータから前記保護されたウェブサービスリソースにアクセスするための第１のリクエストを受信するステップであって、前記第１のリクエストは、第１の認証レベルと関連付けられる、受信するステップと、

前記第１のリクエストを受信すると、前記第１のリクエストを評価し、前記通信ネットワークの種類、前記第１のリクエストに関連付けられるオブジェクトの種類およびプロパティ、ならびに前記第１のリクエストに関連付けられる前記クライアントコンピュータの証明書のうちの少なくとも１つを評価することにより、前記保護されたウェブサービスリソースにアクセスするために認証が必要かどうかを判定するステップと、

前記プロセッサにより前記認証が必要であると判定された場合、前記第１のリクエストを処理するためには少なくとも１つの認証プロセスを完了しなければならないことを示す、前記プロセッサにより作成された第１のフォルトを応答するステップと、

前記クライアントコンピュータが、第１の要因に従って、かつ第１の認証トークンを

用いて、認証サービスにより認証された後、前記クライアントコンピュータから前記第１の認証トークンを受信するステップであって、前記第１の認証トークンは、前記クライアントコンピュータが前記第１の要因に従って認証されたことを示す、受信するステップと、

前記受信した第１の認証トークンに基づいて前記第１の要因に従った認証が前記第１の認証レベルに対して十分であると判定された後、前記保護されたウェブサービスリソースにアクセスするための前記第１のリクエストを許可するステップと、

前記通信ネットワークを介して前記クライアントコンピュータから前記保護されたウェブサービスリソースにアクセスするための第２のリクエストを受信するステップであって、前記第２のリクエストは、第２の認証レベルに関連付けられ、前記第２の認証レベルは、前記第１の認証レベルより高いものである、受信するステップと、

前記第２の認証レベルには不十分となる前記第１の要因に従った前記第１の認証トークンに基づいて、前記保護されたウェブサービスリソースにアクセスするための前記第２のリクエストを拒否するステップと、

前記プロセッサにより前記認証が必要であると判定された場合、前記第２のリクエストを処理するためには少なくとも１つの追加の認証プロセスを完了しなければならないことを示す、前記プロセッサにより作成された第２のフォルトを応答するステップと、

前記クライアントコンピュータが、第２の要因に従って、かつ第２の認証トークンを用いて、前記認証サービスにより認証された後、前記クライアントコンピュータから前記第２の認証トークンを受信するステップであって、前記第２の要因は、前記第１の要因とは異なるが、前記第１の要因に従った認証から所定時間経過後は前記第１の要因を含み、前記第２の認証トークンは、前記クライアントコンピュータが前記第２の要因に従って認証されたことを示す、受信するステップと、

前記受信した第２の認証トークンに基づいて前記第２の要因に従った認証が前記第２の認証レベルに対して十分であると判定された後、前記保護されたウェブサービスリソースにアクセスするための前記第２のリクエストを許可するステップと

を含む方法を実行させる、メモリと

を備えることを特徴とするウェブサービスコンピュータシステム。

【請求項２】

前記第１の要因は、パスワード、セキュリティクエスチョンの回答、生体識別子、オブジェクト、およびクライアント特定情報を含むグループから選択されることを特徴とする請求項１に記載のコンピュータシステム。

【請求項３】

前記受信した第１の認証トークンに基づいて前記第１の要因に従った認証が前記第１の認証レベルに対して十分であると判定することは、

前記認証サービスの公開鍵を用いて前記第１の認証トークンを復号することと、

前記第１の認証トークンの前記認証サービスによって行われた申告がアクセスの条件を満たすと判定することと

を含むことを特徴とする請求項１に記載のコンピュータシステム。

【請求項４】

前記第２のリクエストを許可するステップは、前記第２の認証トークンの評価に基づくことを特徴とする請求項１に記載のコンピュータシステム。

【請求項５】

コンピュータ上のプロセッサによって実行されると、保護されたリソースへのアクセスを制御する方法を前記プロセッサに実行させるためのコンピュータ実行可能命令を記録したコンピュータ可読記憶媒体であって、前記方法は、

クライアントコンピュータから、ウェブサービスの前記保護されたリソースを特定するための第１のリクエストを受信するステップであって、前記第１のリクエストは、第１の認証レベルと関連付けられる、受信するステップと、

前記第１のリクエストを受信すると、前記第１のリクエストを評価し、前記通信ネット

ワークの種類、前記第１のリクエストに関連付けられるオブジェクトの種類およびプロパティ、ならびに前記第１のリクエストに関連付けられる前記クライアントコンピュータの証明書のうちの少なくとも１つを評価することにより、前記保護されたウェブサービスリソースにアクセスするために認証が必要かどうかを判定するステップと、
前記第１のリクエストを処理するためには前記第１の認証レベルを満たさなければならないことを示す、前記ウェブサービスにより作成されたフォルトを応答するステップと、
第１の要因に従って認証サービスから認証された後に、前記クライアントコンピュータから第１の認証トークンを受信するステップと、
前記第１の認証トークンを使用して、前記クライアントコンピュータが、前記第１の要因に従って認証されたかどうかを判定するステップと、
前記認証が、前記第１のリクエストを許可するのに十分である前記第１の認証レベルを満たすかどうかを判定するステップと、
前記認証が十分である場合、前記第１のリクエストを許可するステップと、
前記認証が前記第１のリクエストを許可するのに十分ではない場合、前記第１のリクエストを拒否するステップと、
前記クライアントコンピュータから、前記ウェブサービスの前記保護されたリソースを特定するための第２のリクエストを受信するステップであって、前記第２のリクエストは、第２の認証レベルと関連付けられ、かつ前記第１の認証トークンを含む、受信するステップと、
前記第１の認証トークンが前記第２のリクエストを許可するのに十分であるかどうかを判定するステップと、
前記第２の認証レベルが、前記第１の認証レベル以下である場合、前記第２のリクエストを許可するステップと、
前記第２の認証レベルが、前記第１の認証レベルより高い場合、前記第２のリクエストを拒否するステップと、
前記前記第２の要求が拒否された場合、前記クライアントコンピュータが前記認証サービスによって第２の要因によって認証された後、第２の認証トークンを前記クライアントコンピュータから受信し、前記第２の認証トークンを使用して、前記クライアントコンピュータが、前記第２の要因に従って認証されたかどうかを判定するステップであって、前記第２の要因は、前記第１の要因とは異なるが、前記第１の要因に従った認証から所定時間経過後は前記第１の要因を含む、判定するステップと
を備えることを特徴とするコンピュータ可読記憶媒体。

【請求項６】
前記認証トークンは、公開鍵暗号化を用いて暗号化されることを特徴とする請求項５に記載のコンピュータ可読記憶媒体。

【請求項７】
前記方法は、前記認証が十分である場合、前記第１または前記第２のリクエストを許可した後に前記保護されたリソースへのアクセスを許可するステップをさらに備えることを特徴とする請求項５に記載のコンピュータ可読記憶媒体。

【請求項８】
前記第１のリクエストを拒否するステップおよび前記第２のリクエストを拒否するステップは、拒否することを、メッセージを用いて前記クライアントコンピュータに送信するステップを含み、前記メッセージは、前記クライアントコンピュータを認証するように構成された前記認証サービスについての情報を含むことを特徴とする請求項５に記載のコンピュータ可読記憶媒体。

【請求項９】
前記第１のリクエストを拒否するステップおよび前記第２のリクエストを拒否するステップは、Ｓｉｍｐｌｅ　Ｏｂｊｅｃｔ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌに従ってフォルトメッセージを送信するステップを含み、前記第１の認証トークンを受信するステップおよび前記第２の認証トークンを受信するステップは、Ｗｅｂ　Ｓｅｒｖｉｃｅｓ　Ｔｒｕ

ｓｔ仕様書に従ってＷｅｂ　Ｓｅｒｖｉｃｅｓ　Ｔｒｕｓｔ　Ｒｅｑｕｅｓｔ　Ｓｅｃｕｒｉｔｙ　Ｔｏｋｅｎ　Ｒｅｓｐｏｎｓｅ　Ｍｅｓｓａｇｅを受信するステップを含むことを特徴とする請求項５に記載のコンピュータ可読記憶媒体。

【発明の詳細な説明】

【背景技術】

【０００１】

ユーザーが、インターネットなどのネットワークを経由して保護されたリモートリソースにアクセスを試みる場合、ユーザーは、通常、リモートリソースを制御するサーバによって発行されるポリシーステートメントに従う。ポリシーステートメントは、リソースとの通信を開始するのに必要な一連の認証ルールおよび認可ルールを与える。例えば、ポリシーステートメントは、リソースにアクセスする前に、ユーザーにパスワードを与えるように要求することがある。ユーザーが正しいパスワードを与えた場合、ユーザーの身元が認証されて、リソースへのアクセスが許可される。

【０００２】

単一の認証形式が保護されたリソースとの通信を開始するのに十分である状況では、ポリシーステートメントの認証方法は有効に機能するが、ポリシーステートメントは、動的環境においてあまり機能しない。動的環境において、クライアントと保護されたリソースとの間の通信の開始時に、単一のインスタンスの認証では十分でないことがある。例えば、ユーザーが保護されたリソースを有するウェブサイトにアクセスを試みる場合は、ユーザーにとって、最初にパスワードを入力して認証を与えることで十分である。しかしながら、いったんユーザーがウェブサイトにアクセスすると、ユーザーは、自分のパスワードを変更し、ディレクトリを更新し、高度に保護されたリソースにアクセスし、またはシステム管理者グループなどの高レベルのアクセスグループの権限を要求することを試みる。このような場合、ユーザーは、単に情報を閲覧するだけではなく、それ以上を行うことを要求する。このような行為は、保護されたリソースに大きな損害を与える可能性がある。

【０００３】

一部の認証方法は、リソースとの通信を可能にする前に認証を要求する。しかしながら動的環境において、保護されたリソースへのアクセスを要求する実リクエストが受信されるまでに、どのような認証ルールおよび認可ルールが適用されるかを判定するのは困難である。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】米国特許出願第１２／０２４８９５号明細書　上述の引用の開示はすべて、参照することにより本明細書に組み込まれる。

【発明の概要】

【課題を解決するための手段】

【０００５】

本開示の実施形態は、メッセージ専用の認証に対するシステム、方法、およびデータ構造に関する。一態様は、保護されたウェブサービスリソースへのアクセスを制御するコンピュータシステムである。コンピュータシステムは、通信装置、プロセッサ、およびメモリを含む。通信装置は、通信ネットワーク経由で通信を行う。プロセッサは、通信装置に通信接続される。メモリは、プロセッサによって実行された場合、コンピュータシステムに、保護されたウェブサービスリソースへのアクセスを制御する方法を実行させることができるプログラム命令を格納する。その方法は、まず、クライアントから第１のリクエストを受信して通信ネットワークからの保護されたウェブサービスリソースにアクセスし、第１の要因に従ってクライアントが認証されたと判定し、第１の要因に従った認証に基づいて、保護されたウェブサービスリソースにアクセスする第１のリクエストを許可し、通信ネットワークからの保護されたウェブサービスリソースにアクセスする第２のリクエストをクライアントから受信し、第２のリクエストを許可するには不十分となる第１の要因

に従った認証に基づいて、保護されたウェブサービスリソースにアクセスする第２のリクエストを拒否し、第２の要因に従ってクライアントが認証されたと判定し、および第２の要因に従った認証に基づいて、保護されたウェブサービスリソースにアクセスする第２のリクエストを許可することを含む。

【０００６】

別の態様は、ウェブサービスリソースへのアクセスをクライアントに認証する方法である。その方法は、（ｉ）認証されるクライアントからリクエストを受信すること、（ｉｉ）チャレンジメッセージをクライアントに送信すること、（ｉｉｉ）チャレンジメッセージへの確認応答をクライアントから受信すること、（ｉｖ）確認応答が所定の基準に合うと判定すること、（ｖ）認証されるリクエストがさらに認証を要求すると判定すること、（ｖｉ）第２のチャレンジメッセージ、第２の確認応答、および第２の所定の基準を用いて（ｉｉ）から（ｉｖ）までを繰り返すこと、（ｖｉｉ）認証メッセージをクライアントに送信することを含む。

【０００７】

追加的な態様は、コンピュータによって実行されたときに、保護されたリソースへのアクセスを制御する方法を実行するコンピュータ実行可能命令を含むコンピュータ読み取り可能媒体に関連する。その方法は、保護されたウェブサービスのリソースを特定するリクエストをクライアントから受信し、認証サービスから認証を要求する応答をクライアントに送信し、認証サービスから認証された後にクライアントから認証トークンを受信し、認証トークンがリクエストを許可するのに十分であるかどうかを判定し、認証トークンが十分な場合はリクエストを許可し、認証トークンがリクエストを許可するのに十分でない場合はリクエストを拒否することから成る。

【０００８】

実施形態は、コンピュータプロセス、コンピュータシステム、もしくはコンピュータプログラム製品またはコンピュータ読み取り可能媒体などの製造品として実装できる。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読み取り可能で、コンピュータプロセスを実行する命令のコンピュータプログラムを暗号化するコンピュータ記憶媒体とすることができる。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読み取り可能で、コンピュータプロセスを実行する命令のコンピュータプログラムを暗号化する搬送波上の伝播信号とすることもできる。

【０００９】

本発明の概要は、以下の発明の詳細な説明でさらに説明される簡易な形式において概念の１つの選択を導入するために与えられる。本発明の概要は、特許請求の範囲の対象事項での重要な特徴または不可欠な特徴を特定することを意図せず、または特許請求の範囲の対象事項の範囲を限定するように用いられることを意図しない。

【図面の簡単な説明】

【００１０】

【図１】動的認証を実行するように構成された例示的なシステムのブロック図である。

【図２】認証が要求されるかどうかを動的に判定する例示的な方法を示すフロー図である。

【図３】クライアントを認証する例示的な方法を示すフロー図である。

【図４】保護されたリソースへのアクセスを動的に制御する例示的な方法を示すフロー図である。

【図５】保護されたリソースへのアクセスを制御する例示的な方法を示すフロー図である。

【図６】本開示の態様を実装する例示的なコンピュータシステムのブロック図である。

【発明を実施するための形態】

【００１１】

本開示は、特定の実施形態を示す添付図を用いて、例示的な実施形態をより完全に説明する。しかしながら他の態様は、多くの異なる形式で実装することができ、本開示の特定

の実施形態の内容（inclusion）は、それらの態様を本明細書に説明される実施形態に限定するものとして解釈されてはならない。むしろ、図に示した実施形態は、完全で、かつ意図する範囲を十分に当業者に伝える開示を与えるために含められている。図を参照する場合、全体を通じて示した同種の構造および要素は、同種の参照符号を用いて指定される。

【００１２】

本開示の一部の実施形態は、メッセージ専用の認証に対するシステムおよび方法に関する。一態様は、クライアントが保護されたリソースへのアクセスを許可される前に、認証が必要であるかどうかを判定する方法である。

【００１３】

一般的には、認証は、コンピュータシステム、クライアント、システム、または人物などによって行われる身元申告の信憑性を検証するプロセスである。コンピュータシステムの認証は、典型的には、コンピュータシステムの元またはソースの確認を含む。元またはソースの確認は、通常、製造場所および製造時期、ネットワーク上の位置、物理的位置、識別番号などの固有の身元を申告するコンピュータシステムについての情報を、固有の身元についての周知の情報と比較することによって行われる。

【００１４】

しかしながら、人物を認証する動作は、例えば、その人物の身元の確認を伴う。認証に用いることができる多くの異なる識別特性がある。人物を特定する１つの方法は、生体識別子の検出に関与する。この認証方法は、身元を申告する人物に、身元を申告する人物のＤＮＡ、指紋パターン、網膜パターンなどの固有の特徴の形式で検証を行うことを要求する。人物の身元を検証することができる別の方法は、その人物が知るものによって行われる。この認証方法は、身元を申告する人物に、パスワード、暗証番号などの個人情報の形式で検証を行うことを要求する。さらに人物の身元を検証することができる別の方法は、その人物が有するものによって行われる。この認証方法は、身元を申告する人物に、キー、セキュリティカード、セキュリティトークン、クレジットカードなどのオブジェクトの形式で検証を行うことを要求する。これらの認証方法は、個々に、または多元的な認証として知られるプロセスにおいて一緒に用いることができる。

【００１５】

一般的に、クライアントを認証する場合、プロセスは、クライアントを認証するか、またはクライアントを用いる人物の身元を認証するかのいずれかを含む。一実施形態において、クライアントは、ウェブブラウザとすることができる。別の実施形態において、クライアントは、リモート手続き呼び出しを行うように構成されたプログラム、もしくは保護されたリソースとの通信を行う任意の他のアプリケーションまたはプログラムとすることができる。

【００１６】

動的環境において、認証の種類およびクライアントを認証するルールは、保護されたリソースにアクセスするために行われるリクエストの種類によって異なる。例えば、保護されたリソースの閲覧を要求するメッセージは、保護されたリソースの変更を要求するメッセージよりは複雑な認証を必要としない。一実施形態において、保護されたリソースは、特定のユーザーのみがアクセスできる私的ウェブサイトである。別の実施形態において、保護されたリソースは、私的電子メールグループ、保護されたデータ、保護された方法、保護された手続き、保護された動作、もしくは特定のユーザーまたはクライントに限定しなければならない任意の他の種類の保護された情報または機能とすることができる。

【００１７】

図１は、リクエスト専用の動的認証を実行するように構成された例示的なシステム１００のブロック図である。図示された実施形態において、システム１００は、クライアント１０２、ウェブサービス１０４、および認証サービス１０８を含む。ウェブサービス１０４は、保護されたリソース１０６を含む。この実施形態において、クライアント１０２は、保護されたリソース１０６にアクセスすることを望む。しかしながら保護されたリソー

ス１０６は、未認証のクライアントによるアクセスから保護されている。クライアント１０２、ウェブサービス１０４、および認証サービス１０８は、ネットワーク１１０経由で通信を行うように構成される。ネットワーク１１０はデータ通信路である。一実施形態において、ネットワーク１１０はインターネットである。他の実施形態において、ネットワーク１１０は、ローカルエリアネットワーク、イントラネット、無線ネットワーク、もしくはあるコンピュータシステムから別のコンピュータシステムにデータを送るように構成された任意の他の通信路である。

【００１８】

一実施形態において、クライアント１０２は、コンピュータシステムである。他の実施形態において、クライアント１０２は、ネットワーク１１０経由でデータを送るように構成された任意のコンピュータシステムである。クライアント１０２の１つの例は、図６に示したコンピュータシステム６００である。クライアント１０２は、ウェブサービス１０４と通信接続されて、ネットワーク１１０を経由して認証サービス１０８に接続される。一部の実施形態において、クライアント１０２は、メッセージをウェブサービス１０４に送信することによって保護されたリソース１０６にアクセスすることができる。別の実施形態において、クライアント１０２は、メッセージを、保護されたリソース１０６に直接送信する。

【００１９】

一実施形態において、ウェブサービス１０４は、ウェブサーバ、ウェブサービスを運用するなどのコンピュータシステム（例えば、図６に示したコンピュータシステム６００）である。一般的に、ウェブサービス１０４は、データ通信プロトコルを用いて、ネットワーク１１０を経由してアクセスすることができる実用的な機能を与える。ウェブサービスを用いて数多くの実用的な機能を与えることができる。一実施形態において、ウェブサービス１０４はサーバである。別の実施形態において、ウェブサービス１０４は、ネットワーク１１０に通信接続されたコンピュータシステム上で動作するコンピュータシステムのアプリケーションである。一部の実施形態において、ウェブサービス１０４は、参照可能なエンティティ、プロセッサ、またはウェブサービスのメッセージがアドレスに指定することができるリソースである。

【００２０】

一般的に、ウェブサービス１０４の一部の実施形態は、保護されたリソース１０６に関連するクライアント１０２から送信されたメッセージ用のネットワーク１１０を監視する。メッセージが受信されたときに、ウェブサービス１０４は、クライアント１０２の認証を要求するリクエストをメッセージが含むかどうかを判定する。保護されたリソース１０６にアクセスするのをクライアント１０２に許可する前に、クライアント１０２を認証することは、保護されたリソース１０６へのアクセスを制御するのに必要となる場合がある。ウェブサービス１０４が、認証が必要であると判定した場合、ウェブサービス１０４は、クライアント１０２を認証サービス１０８に導く。

【００２１】

図示された実施形態において、ウェブサービス１０４は、保護されたリソース１０６を含む。保護されたリソースは、例えば、ウェブサービス１０４によって実行される機能と、唯一認証されたクライアントによってアクセス、使用、または変更することができるウェブサービス１０４によって格納されるデータとを含む。例えば、ウェブサービス１０４がグループ分散リストを保持するサービスを提供する場合、グループ分散リストは、唯一認証されたクライアントによってアクセス、使用、または変更することができる保護されたリソースである。別の例として、保護されたリソース１０６は、ディレクトリ内のエントリである。別の実施形態において、保護されたリソース１０６は、データベース内のレコードである。別の実施形態において、保護されたリソース１０６は、メモリ記憶装置に格納されたファイルまたはファイルの一部である。他の実施形態は、保護されたリソース１０６の他の形式を用いる。

【００２２】

一実施形態において、認証サービス１０８は、ネットワーク１１０に通信接続されたサーバなどのコンピュータシステム（例えば、図６に示したコンピュータシステム６００）である。別の実施形態において、認証サービス１０８は、ネットワーク上に配置されたソフトウェアアプリケーションを実行するコンピュータシステムである。認証サービス１０８は、クライアント１０２を認証するように構成される。認証サービス１０８の１つの例は、セキュリティトークンサービスのエンドポイントである。図示された実施形態は、ウェブサービス１０４から明確に分離した認証サービス１０８の例を示すが、他の実施形態において、認証サービス１０８およびウェブサービス１０４は、同じサーバ上で動作する。

【００２３】

クライアント１０２が、保護されたリソース１０６へのクライアントのメッセージ内に含まれるリクエストを実行するのを認証された場合、ウェブサービス１０４は、要求された動作の結果をクライアント１０２に送る。しかしながら、他の実行可能な実施形態において、認証サービス１０８は、ネットワーク１１０経由で直接ウェブサービス１０４との通信を行い、例えば、ウェブサービス１０４から認証リクエスト受信し、または認証の証拠をウェブサービス１０４に送信する。

【００２４】

認証に加えて、クライアントが認証されるだけでなく認可されることを要求することによって、保護されたリソースへのアクセスを制御することが望ましい場合がある。

【００２５】

図２は、認証が要求されるかどうかを動的に判定する例示的な方法２００を示すフロー図である。方法２００は、動作２０２、２０４、２０６、２０８、および２１０を含む。方法２００は、リソースリクエストが行われる間に動作２０２から開始する。一実施形態において、動作２０２は、保護されたリソース１０６にアクセスする要求を含むメッセージを、クライアント１０２からウェブサービス１０４に送ることに関与する。一部の実施形態において、メッセージは、リモート手続き呼び出しである。別の実施形態において、リクエストは、クライアントとリソース間での電子メールまたは任意の他の種類の電気通信の形式をとることがある。別の実施形態において、動作２０２は、ウェブサービス通信に一般に用いられるような、Ｃｒｅａｔｅリクエスト、Ｇｅｔリクエスト、Ｐｕｔリクエスト、Ｄｅｌｅｔｅリクエスト、またはＥｎｕｍｅｒａｔｅリクエストをウェブサービス１０４に送信するクライアント１０２に関与する。

【００２６】

リソースリクエストが行われた後に、動作２０４は、リクエストを評価して、認証が必要であるかどうかを判定するために実行される。一実施形態において、ウェブサービスは、保護されたリソースにクライアントから送信されたメッセージを分析して、メッセージがクライアントに認証を与えるように要求するリクエストを含むかどうかを判定する。一実施形態において、保護されたリソースにアクセスを試みるクライアントは、リクエストに対して要求された認証をクライアントがすでに与えた場合には、認証を与える必要がない。別の実施形態において、クライアントは、リソースが認証を要求する誰もが利用できる公的リソースである場合、認証を与える必要がない。別の実施形態において、たとえリソースが保護されていても、メッセージが保護されたリソースに損害を与えることができないなどの、認証を要求しないリクエストを含む場合、認証は要求されない。ウェブサービス１０４が、動作２０４において認証が要求されないと判定した場合、　動作２０６が実行される。認証が要求された場合、動作２０８が実行される。

【００２７】

１つの例において、ウェブサービス１０４は、多数の要件を評価することによって認証が要求されるかどうかを判定する。これらの要件は、リクエストを運ぶ（ローカルエリアネットワークかリモートアクセスなどの）媒体、リクエストが関係するオブジェクトの種類、リクエストが関係するオブジェクトのプロパティ、すでにリクエストとともに含まれる証明書の品質を含む。証明書の品質に関して、例えば、証明書が別の組織からのユーザ

ーに対するものである場合、ユーザーがアクセスを試みるリソース次第で追加的な証明書が要求されることがある。

【００２８】

認証が要求されない場合、動作２０６を実行して要求されたリソースへのアクセスを許可する。ウェブサービスは、例えば、リソースの表現をクライアントに送信すること、要求された動作を保護されたリソース上で実行すること、または要求された動作の結果をクライアントに送信することによって、保護されたリソースへのアクセスを許可する。

【００２９】

しかしながら、認証が要求された場合、動作２０８を実行して認証を行う。クライアントの認証は、図３との関連でさらに説明する。クライアントに認証を与えるように要求する状況の例は、クライアントが私的ウェブサイト、私的電子メールグループ、保護されたデータ、保護された方法、保護された手続き、保護された動作、もしくは任意の他の種類の保護された情報または機能にアクセスまたは変更を試みるインスタンスを含む。一部の実施形態において、ウェブサービス１０４は、クライアント１０２をチャレンジして認証を与える。あるいは、ウェブサービス１０４は、クライアントを（認証サービス１０８などの）認証サービスに導く。認証サービス１０８を、ウェブサービス１０４に配置し、ウェブサービスから他の場所に配置し、または分散ネットワークの場合はその両方に配置することができる。クライアントを認証する例示的な方法は、図３を用いて説明される。

【００３０】

クライアントが認証された後に動作２０６が実行されて、ウェブサービスの保護されたリソースへのアクセスがクライアントに許可される。一実施形態において、クライアントが認証トークンを認証サービスからウェブサービスに与えた後に、アクセスが許可される。ウェブサービスは、例えば、リソースをクライアントに送信し、要求された動作を保護されたリソース上で実行し、保護されたリソースを要求された動作を実行するように導く。または、要求された動作の結果をクライアントに送信することによって、保護されたリソースへのアクセスを許可する。

【００３１】

クライアントを認証してはならないと判定した場合、動作２１０が、保護されたリソースに対してアクセスが拒否される間に実行される。１つの例において、認証サービス１０８が、保護されたリソースにアクセスするために必要な認証トークンを与えないために、アクセスが拒否される。

【００３２】

図３は、クライアントを認証する例示的な方法３００を示すフロー図である。一実施形態において、方法３００は、図２に示した動作２０８と一致する。方法３００は、認証に対するリクエストが行われる間に、動作３０２から開始する。一実施形態において、動作３０２は、クライアント１０２から認証サービス１０８に送信されるメッセージ、および認証のリクエストを受信する認証サービス１０８に関与する。

【００３３】

図示された実施形態において、認証のリクエストを受信した後に、動作３０４が実行されて、認証チャレンジと通信を行う。一実施形態において、認証サービス１０８は、クライアント１０２へのチャレンジと通信を行って、クライアントまたはユーザーの身元の信憑性を確かめる。一部の実施形態において、チャレンジは、パスワードを要求し、セキュリティクエスチョンの回答を要求し、ＤＮＡサンプル、指紋パターン、網膜パターン、生体識別子の他の形式、クライアントを用いる人物の他の固有の識別子を要求し、キー、セキュリティカード、セキュリティトークン、クレジットカードなどのオブジェクトまたはクライアントを用いる人物に固有の他のオブジェクトの形式で検証を要求し、製造場所および製造時期、ネットワーク上の位置、物理的位置、識別番号などのクライアントの特定情報を要求し、または認証目的で用いることができる任意の他の種類の情報を要求する形式をとる。

【００３４】

図示された実施形態において、いったんチャレンジが交信されると、動作３０６が実行されて、チャレンジへの確認応答を受信する。動作３０６は、動作３０４において要求された情報、サンプル、識別子などを与えて、それを認証サービス１０８に送ることに関与する。一実施形態において、クライアント１０２のユーザーが入力装置（例えば、図６に示した入力装置６１４）を用いて、識別情報をクライアント１０２に与えて、次に情報を認証サービス１０８に送る。一部の実施形態において、（入力装置の形式でもある）センサーが用いられる。例えば、ユーザーは、指を指紋スキャナに置いて、指紋を走査する。指紋データは、次に、認証サービス１０８に転送される。キーボード、マウス、タッチパッド、マイクロフォン、ペン、生体センサー、スキャナ、カードリーダー、化学物質検出器などを含むさまざまな種類の入力装置を用いることができる。他の実施形態において、データがクライアント１０２に入力されて、次に認証サービス１０８に送られる。

【００３５】

図示された実施形態において、いったん確認が交信されると、動作３０８を実行して、確認応答を検証する。一実施形態において、認証サービスは、クライアント１０２から受信された確認応答を、申告された身元についての周知の情報と比較する。例えば、認証サービス１０８は、データベースに格納されたデータを読み出し、そのデータを確認応答データと比較する。認証サービス１０８は、次に、確認応答が、すでに格納されたデータと一致するどうかを判定する。一致する場合、確認応答が検証されて、動作３１２が実行される。一致しない場合、確認応答が検証されずに、動作３１０が実行される。

【００３６】

受信された確認応答が周知の情報と一致しない場合、動作３１０が実行されて、要求されたリソースに対してアクセスを拒否する。別の実施形態において、認証サービス１０８が代わりに動作３０４に戻って、認証を再試行する。このような実施形態において、３度の再試行などの複数の再試行が許可される。再試行が成功しない場合、動作３１０が実行されて、保護されたリソースへのアクセスが拒否される。

【００３７】

受信された確認応答が周知の情報と一致する場合、動作３１２が実行されて、追加的な認証が必要であるかどうかを判定する。一実施形態において、認証サービス１０８は、強固な認証形式、すなわち、クライアントに複数の認証形式を与えるように要求する多元的な認証が要求されるかどうかを判定する。多元的な認証が必要な場合、方法３００は、動作３０４にもどって、第２のチャレンジと通信を行う。動作３０４、３０６、３０８、および３１０または３１２がその後、要求通りに何度でも繰り返される。しかしながら、繰り返される場合、認証チャレンジは、認証サービスからすでに発行されたチャレンジとは異なる形式をとる。例えば、認証サービスが最初にクライアントにパスワードを与えるように要求した場合、認証サービスは、２回目またはその次の回の検証の間にクライアントにスマートカードまたは生体スキャナを用いるように要求することがある。一部の実施形態において、認証サービス１０８が単に同じ情報を何度も要求しないように、認証の形式がすでに用いた形式とはある程度異なるのであれば、任意の形式の認証を用いることができる。多くの状況において、同じ情報を繰り返して要求することは、追加的な認証値を与えない。しかしながら、一部の状況において、前回のチャレンジ以来、かなりの時間が経過した場合などに、要求を繰り返して用いることができる。

【００３８】

これ以上認証が要求されない場合、動作３１４が実行されて、認証トークンを発行する。認証サービス１０８は、クライアントが認証されたことの証拠としてクライアントが用いるセキュリティトークンを、クライアントに戻す。認証トークンは、クライアント１０２からウェブサービス１０４に送信される。ウェブサービス１０４は、次に、クライアント１０２に、最初に要求された保護されたリソースへのアクセスを許可する。

【００３９】

図４は、保護されたリソースへのアクセスを動的に制御する例示的な方法４００を示すフロー図である。一実施形態において、方法４００は、保護されたリソース１０６にアク

セスを試みるなどの、クライアント１０２から受信されたメッセージに応答して、ウェブサービス１０４によって実行される。方法４００は、リクエストメッセージが受信された間に、動作４０４から開始する。一実施形態において、ウェブサービス１０４は、保護されたリソース１０６に関連するクライアント１０２からリクエストを受信する。いくつかの例として、リクエストは、保護されたリソースを閲覧し、保護されたリソースにアクセスし、または保護されたリソースを変更するためのリクエストである。

【００４０】

図示された実施形態において、動作４０６がその次に実行されて、リクエストメッセージが認証を要求するリクエストを含むかどうかを判定する。一実施形態において、ウェブサービス１０４は、リクエストを分析して、リクエスト内に含まれる分析したリクエストがクライアントの認証を要求するかどうかを判定する。一部の実施形態において、保護されたリソースにアクセスを試みるクライアントは、例えば、クライアントがリクエストに対してすでに要求された認証を与えた場合、リソースが公的でありすべてに利用できる場合、リクエストの種類が認証を要求しないリクエストを含む場合、またはリクエストの種類およびそれに関連付けられたリクエストが保護されたリソースに損害を与えることができない場合に、認証を与える必要がない。認証が要求されない場合、動作４１４がその次に実行されて、要求された動作を行う。

【００４１】

図示された実施形態において、メッセージ内に含まれるリクエストが認証を要求する場合、動作４０８がその次に実行されて、認証が要求されたことを伝える。一実施形態において、動作４０８は、メッセージをウェブサービス１０４からクライアント１０２に送信して、要求された動作を実行するために認証が必要であることをクライアントに通知することに関与する。一実施形態において、ウェブサービス１０４は、クライアント１０２を、図３を用いて説明されたような認証に対する認証サービス１０８に導く。例えば、メッセージは、認証プロバイダへのアドレスを含む。クライアントは、アドレスを用いて認証プロバイダを見つけ、認証の受信を試みる。別の実施形態において、方法３００は、メッセージが、クライアント１０２に認証情報を与えるように要求するクライアント１０２へのチャレンジを含むように、ウェブサービス１０４によって実行される。

【００４２】

図示された実施形態において、クライアントが認証に成功した場合、動作４１０が実行されて、認証トークンが受信される。図３を用いて説明したように、成功した認証の結果は、認証トークンの受信である。そのトークンは、ウェブサービス１０４を通過して、認証の証拠を与える。ウェブサービス１０４は、トークンを評価して、トークンが有効であるかを検証する。

【００４３】

一部の実施形態において、トークンの評価は、２つのステップに関与する。第１のステップは、公開キー暗号化に関与する。ウェブサービス１０４が、認証サービス１０８の公開キーを用いてトークンを復号することができる場合、ウェブサービス１０４は、トークンが認証サービス１０８によって発行されたと判定する。第２のステップは、認証サービス１０８によって行われたクライアント１０２についての申告が、アクセスに対する１または複数の条件を満たすかどうかを判定することを含む。

【００４４】

例えば、特定の保護されたリソース１０６がアクセスされるために、ウェブサービス１０４は、３つの特定の認証プロセスが実行されて、クライアント１０２を認証サービス１０８に認証することを要求することがある。結果として、ウェブサービス１０４は、クライアント１０２から受信されたトークンを評価して、クライアント１０２が３つの認証プロセスのすべてを完了したことを表明する認証サービス１０８によって、トークンが３つの申告を含むかを検証する。他の実施形態において、任意の数の認証プロセスが要求される。一部の実施形態において、要求された認証プロセスの数および種類は、行われたリクエストの種類に関連する。例えば、高いリスクを伴うリクエストは、より厳密な認証プロ

セスを要求することが多い。

【００４５】

一部の実施形態において、成功して完了した多くの認証プロセスは、認証レベルと呼ばれる。一部の実施形態において、保護されたリソース１０６に関与するリスクの低い動作は、１または２つの認証レベルなどの、低い認証レベルしか要求しない。一部の実施形態において、リスクの高い動作は、３から５つの認証レベルなどの、高い認証レベルを要求する。単一の保護されたリソースは、行われる要求次第でさまざまな認証レベルと関連付けることができる。例えば、保護されたリソースから情報を読み出す要求は、一部の状況において低い認証レベルしか要求しないが、保護されたリソースから情報を削除する要求は、中程度または高い認証レベルを要求することがある。他の状況において、保護されたリソースから情報を読み出す要求は、情報が機微または秘密である場合に高い認証レベルを要求することがある。

【００４６】

図示された実施形態において、認証の有効な証拠が与えられない場合、または与えられた認証が評価されて、不十分であると判定された場合、動作４１１が実行されて、保護されたリソースへのアクセスが拒否される。一部の実施形態において、メッセージがクライアント１０２に送信されて、クライアント１０２に拒否を通知する。一部の実施形態において、メッセージは、クライアント１０２を認証サービス１０８に導くなどの、適切な認証を得る方法についての情報も含む。

【００４７】

図示された実施形態において、認証の証拠が与えられて、有効と検証された場合、動作４１２において要求された動作が実行される。つまり、保護されたリソースへのアクセスが許可される。一部の実施形態において、動作４１４がその次に実行されて、要求が処理されたことを要求側に通知する。例えば、ウェブサービス１０４は、保護されたリソースに関連するリクエストが処理されたことをクライアント１０２に通知するメッセージを送信する。他の例において、ウェブサービス１０４は、リソース１０６の代表をクライアント１０２に送信し、要求された動作を保護されたリソース１０６上で実行し、または要求された動作の結果をクライアント１０２に送信することによって、保護されたリソースへのアクセスを許可する。

【００４８】

図示された実施形態において、動作４１６がその次に実行されて、追加的なメッセージの受信を監視する。例えば、ウェブサービス１０４は、リソース１０６に関連するクライアント１０２からの追加的な通信を監視する。クライアント１０２が追加的なメッセージをリソース１０６に送信した場合、方法４００は、動作４０４に戻って、動作４０４、４０６、および４０８を介して新しいメッセージが追加的な認証を要求するかどうかを評価する。クライアントが、この時点ですでに認証されたとしても、動的環境においてクライアントは、強固な認証形式、すなわち、クライアントが送信するメッセージおよびリクエストの種類次第で多元的な認証を与えなければならないことがある。これ以上メッセージが受信されない場合、方法４００は終了する。

【００４９】

図５は、保護されたリソースへのアクセスを制御する例示的な方法５００を示すフロー図である。方法５００は、クライアント１０２、ウェブサービス１０４、認証サービス１０８、および保護されたリソース１０６に関与する。認証サービス１０８は、ウェブサービス１０４から明確に分離したエンティティとして示されるが、一部の実施形態において、認証サービス１０８およびウェブサービス１０４は、同じコンピュータシステム上で動作する。一実施形態において、保護されたリソース１０６は、ウェブサービス１０４上に配置される。さらに別の実施形態において、保護されたリソース１０６は、別のウェブサービス、サーバ、コンピュータ、または他のコンピュータシステム上に配置される。通信５１２において、クライアント１０２は、保護されたリソース１０６のリクエストをサブミットする。ウェブサービス１０４は、このリクエストを受信する。通信５１４において

、ウェブサービス１０４は、認証が必要であると判定して、リクエストを処理するために少なくとも１つの認証プロセスが完了されなければならないことを示すフォルトを用いて応答する。実現可能な実施形態において、フォルトは、ＳＯＡＰ１．２仕様書に定義されるように、ＳＯＡＰ(Simple Object Access Protocol)フォルトの形式をとることができる。他の実施形態において、フォルトは、任意の他の種類のデータ通信プロトコルの形式をとることができる。追加的実施形態において、ウェブサービス１０４からのフォルトは、セキュリティトークンサービスのエンドポイントなどの認証サービス１０８へのアドレスを含む。

【００５０】

通信５１６において、クライアント１０２は、必要な認証プロセスが完了したことを申告する、セキュリティトークンのリクエストを認証サービス１０８に送信する。一実施形態において、このリクエストは、ＷＳ－Ｔｒｕｓｔ仕様書によって定義されたＷＳ－Ｔｒｕｓｔ(Web Services Trust)Ｒｅｑｕｅｓｔ Ｓｅｃｕｒｉｔｙ Ｔｏｋｅｎ Ｒｅｓｐｏｎｓｅ Ｍｅｓｓａｇｅの形式をとる。他の実施形態において、リクエストは、他のプロトコルの形式をとることができる。通信５１８において、認証サービス１０８は、身元の確認のためにチャレンジを用いてクライアント１０２に応答する。一部の実施形態において、チャレンジは、図３に関して説明されたチャンレンジの形式をとる。通信５２０において、クライアント１０２は、身元の確認を用いて応答する。一部の実施形態において、身元の確認は、図３に関して説明された確認の形式をとる。通信５２２において、認証サービス１０８は、身元の確認のために追加的チャレンジを用いてクライアント１０２に応答する。一実施形態において、このチャレンジは、失敗した身元の確認に応答する。さらに他の実施形態において、このチャレンジは、多元的な認証を行うのに必要である。通信５２４において、クライアント１０２は、追加的な身元の確認を用いて認証サービス１０８に応答する。このプロセスは、通信５２６におけるチャレンジとチャレンジ５２８の確認を用いてもう一度繰り返すことができる。チャレンジと確認のセットは３回実行されるように示しているが、他の実施形態において、これらのチャレンジおよび応答の通信は、任意の回数繰り返される。認証サービス１０８がクライアント１０２の身元を確認した後に、認証サービス１０８は、通信５３０において、要求されたセキュリティトークンをクライアント１０２に発行する。

【００５１】

通信５３２において、クライアント１０２は、保護されたリソースの元のリクエストをセキュリティトークンとともに再サブミットする。ウェブサービス１０４は、リクエストを検査して、リクエストが元のリクエストと同じであることを保証して、セキュリティトークンを有効にしてリクエストが有効であることを保証する。通信５３４において、ウェブサービス１０４は、クライアント１０２によって行われたリクエストを処理する。一部の実施形態において、この処理は、保護されたリソース１０６をフェッチングおよび／または更新することに関与する。通信５３６において、保護されたリソース１０６のフェッチおよび／または更新の結果は、ウェブサービス１０４に戻される。通信５３８において、ウェブサービス１０４は、クライアント１０２によって行われたリクエストに応答する。

【００５２】

テーブル１：認証チャレンジスキーマを参照すると、リクエストを処理するためにメッセージ専用認証プロセスが要求されることを示すデータ構造が与えられる。一部の実施形態において、図５に関して説明された通信は、ｗｈｅｎ ａ Ｗｅｂ ｓｅｒｖｉｃｅや、Ｗｅｂ ｓｅｒｖｉｃｅ １０４などの、テーブル１に定義されたデータ構造の形式で交信されて、メッセージ専用プロセスがリクエストを開始したユーザーを認証するために要求されると判定する。一実施形態において、サービスは、ＳＯＡＰ１．２仕様書に定義されるように、ＳＯＡＰフォルトを戻す。一部の実施形態において、従来のＳＯＡＰフォルトとは違って、メッセージ専用認証プロトコルが要求されることを表示するのに用いられるＳＯＡＰフォルトは、元のリクエストの詳細およびリクエストと関連付けるために判

明した任意の認証プロセスがウェブサービスによって読み出される識別子を含むコンテキストヘッダを含む。別の実施形態において、戻ったＳＯＡＰフォルトは、リクエストが行われる代わりにユーザーの身元を示すＤｅｔａｉｌ要素も含む。これは、追加的に認証される身元である。さらに別の実施形態において、Ｄｅｔａｉｌ要素はその上または選択的に、ユーザーがリクエストと関連付けられたそれぞれの認証プロセスを成功して完了したことを確認するセキュリティトークンをユーザーに発行することができる、認証サービス１０８などの認証サービスのアドレスを与える。一部の実施形態において、認証サービスのアドレスは、ウェブサービスのアドレスと同じである。他の実施形態において、認証サービスのアドレスは、ウェブサービスのアドレスとは異なる。

【００５３】

テーブル１：認証チャレンジスキーマ

テーブル１に示したスキーマは、Ｃｈａｌｌｅｎｇｅ要素およびＡｕｔｈｅｎｔｉｃａｔｉｏｎＣｈａｌｌｅｎｇｅ要素を含む。Ｃｈａｌｌｅｎｇｅ要素を用いて、要求された認証データを与えるためにユーザーにチャレンジするのに必要な情報をクライアントに転送する。一部の実施形態において、クライアントは、チャレンジデータをユーザーに表示するウェブブラウザとすることができ、チャレンジに応答してユーザーにデータを与えるように促す。例えば、チャレンジ要素は、クライアント１０２を導いて、ユーザーにパスワードを入力するように促すテキストボックスを表示することができる。他の実施形態は、図３を用いて説明したように、セキュリティクエスチョンへの回答を要求し、ＤＮＡサンプル、指紋パターン、網膜パターン、またはクライアントを用いる人物の他の固有の識別子を要求し、キー、セキュリティカード、セキュリティトークン、クレジットカードなどのオブジェクトまたはクライアントを用いる人物に固有の他のオブジェクトの形式で、ユーザーに認証を与えるように促す。実行可能な実施形態において、認証チャレンジスキーマは、スキーマのラッパーとして機能するＡｕｔｈｅｎｔｉｃａｔｉｏｎＣｈａｌｌｅｎｇｅ要素を含む。

【００５４】

テーブル２：認証チャレンジレスポンススキーマを参照すると、認証チャレンジに応答するデータ構造が与えられる。認証サービス１０８などの認証サービスは、情報を認証するためにチャレンジをユーザーに発行する。一部の実施形態において、チャレンジは、ＷＳ－Ｔｒｕｓｔ仕様書の１０節に定義されたチャレンジフレームワークに従って行われる。認証サービスがユーザーの身元を認証するために追加的な情報を要求した場合、認証サービスは、ＷＳ－Ｔｒｕｓｔ仕様書によって定義されたような応答を用いて、セキュリティトークンメッセージのリクエストに応答する。

【００５５】

テーブル２：認証チャレンジレスポンススキーマ

認証チャレンジレスポンススキーマは、レスポンス要素およびＡｕｔｈｅｎｔｉｃａｔｉｏｎＣｈａｌｌｅｎｇｅＲｅｓｐｏｎｓｅ要素を含む。レスポンス要素は、クライアントから要求される認証サービスの認証情報を特定する。この情報は、認証サービスによって用いられ、例えば、クライアントを認証するためにどのようなチャレンジをクライアントに送信しなければならないかを判定する。ＡｕｔｈｅｎｔｉｃａｔｉｏｎＣｈａｌｌｅｎｇｅＲｅｓｐｏｎｓｅ要素は、スキーマのラッパーとして機能する。

【００５６】

図６は、本開示の態様を実装する例示的なコンピュータシステム６００のブロック図である。一実施形態において、コンピュータシステム６００は、クライアント１０２である。別の実施形態において、コンピュータシステム６００は、ウェブサービス１０４である。別の実現可能な実施形態において、コンピュータシステム６００は認証サービス１０８である。実施形態の最も基本的な構成において、コンピュータシステム６００は、典型的には、少なくとも１つの処理ユニット６０２およびメモリ６０４を含む。コンピュータシステムの正確な構成および種類によって、メモリ６０４は、（ＲＡＭなどの）揮発性メモリ、（ＲＯＭ、フラッシュメモリなどの）不揮発性メモリ、またはその２つの組み合わせ

のメモリとすることができる。この最も基本的な構成は、図６の点線６０６によって示される。さらに、コンピュータシステム６００は、付加的な特徴／機能を有することもできる。例えば、コンピュータシステム６００は、磁気ディスクまたは光ディスク、磁気テープまたは光テープを含む付加的な（取り外し可能および／または取り外し不能）装置も含むことができるが、これに限定されない。このような付加的な記憶装置は、図６の取り外し可能な記憶装置６０８および取り外し不能な記憶装置６１０によって示される。コンピュータ記憶媒体は、コンピュータ読み取り可能命令、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の、情報を記憶する任意野方法または技術に実装される揮発性および不揮発性、取り外し可能および取り外し不能媒体を含む。メモリ６０４、取り外し可能記憶装置６０８、および取り外し不能記憶装置６１０は、コンピュータ記憶媒体のすべての例である。コンピュータ記憶媒体は、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 disks)または他の光記憶装置、磁気カセット、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、もしくは望ましい情報を格納するために用いることができて、コンピュータシステム６００によってアクセスすることができる任意の他の媒体を含むが、これに限定されない。このような任意のコンピュータ記憶媒体は、コンピュータシステム６００の一部とすることができる。

【００５７】

コンピュータシステム６００は、コンピュータシステムに他の装置との通信を行うようにさせることができる通信接続６１２も含むことができる。通信接続６１２は、通信媒体の例である。通信媒体は、典型的には、コンピュータ読み取り可能命令、データ構造、プログラムモジュール、もしくは搬送波などの変調データ信号の他のデータまたは他の転送機構を実施して、任意の情報配信媒体を含む。用語「変調データ信号」は、１または複数の信号の特性セットもしくは信号内の情報を暗号化するような方法によって変更される信号を意味する。一例として、通信媒体は、有線ネットワークまたは直接有線接続、および音響、ＲＦ、赤外線などの無線媒体、および他の無線媒体を含むが、これに限定されない。本明細書に用いられるコンピュータ読み取り可能媒体の用語は、記憶媒体と通信媒体の両方を含む。

【００５８】

コンピュータシステム６００は、キーボード、マウス、ペン、音声入力装置、タッチ入力装置などの入力装置６１４も有することができる。一部の実施形態において、入力装置は、その上（または選択的に）、例えば、生体識別子、センサー、検出器、カードリーダーなどを含む。ディスプレイ、スピーカ、プリンタなどの出力装置６１６も含むことができる。これらのすべての装置は、当業者にはよく知られており、ここで詳細に論じる必要はない。

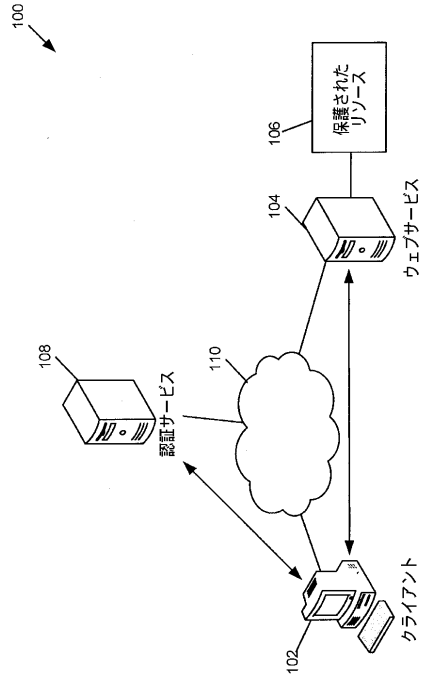
【００５９】

一部の実施形態において、メモリ６０４は、１または複数の動作システム６２０、アプリケーションプログラム６２２、他のプログラムモジュール６２４、およびプログラムデータ６２６を含む。一部の実施形態において、グローバルデータ、クライアント特定データ、および転送ルールは、メモリ６０４、取り外し可能な記憶装置６０８、取り外し不能な記憶装置６１０、または本明細書に記載の任意の他のコンピュータ記憶媒体にそれぞれ格納できる。

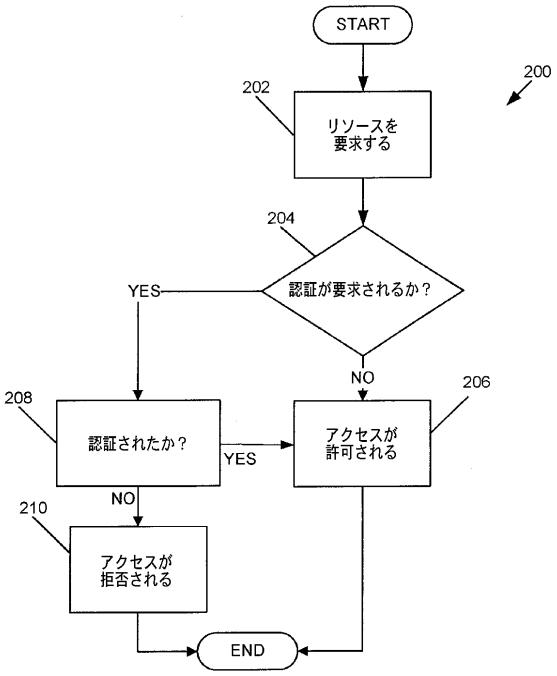
【００６０】

実施形態は、構造的特徴、方法論的動作、およびそれらの動作を含むコンピュータ読み取り可能媒体に専用の言語で記載されているが、添付図に定義されたように、実現可能な実施形態は、必ずしも記載された特定の構造、動作、または媒体に限定されないことを理解されたい。当業者は、本発明の精神および範囲内である他の実施形態または改良を認める。従って、特定の構造、動作、または媒体は、単に具体的な実施形態として開示される。

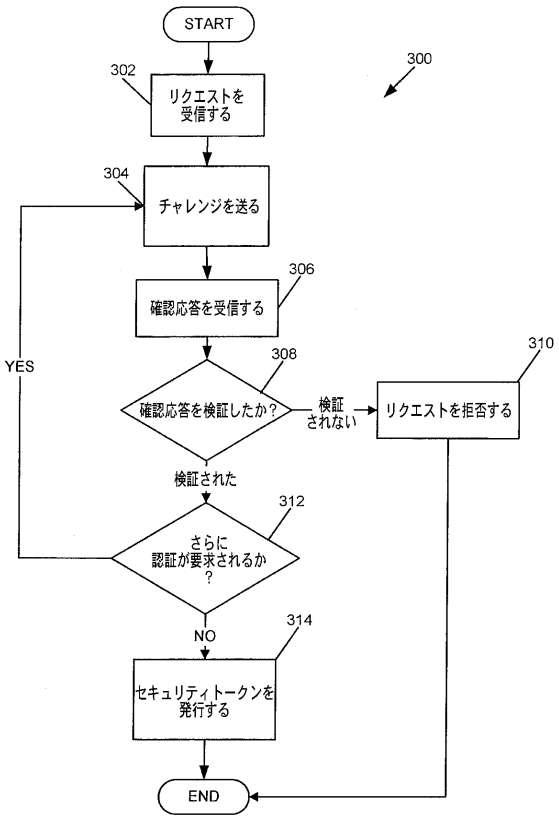
【図１】


100
保護された
リソース
106
104
ウェブサービス
108
認証サービス
110
102
クライアント

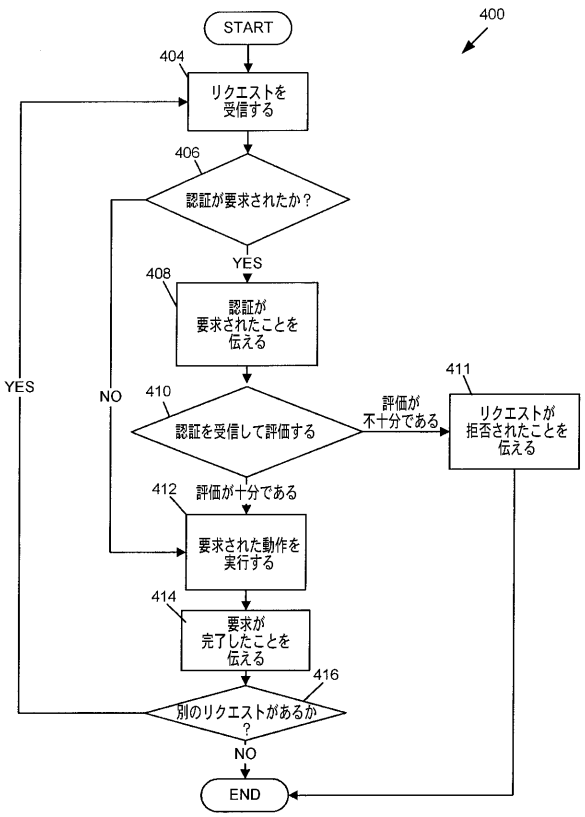
【図２】


START
200
202
リソースを
要求する
204
認証が要求されるか？
YES
NO
206
208
認証されたか？
YES
アクセスが
許可される
NO
210
アクセスが
拒否される
END

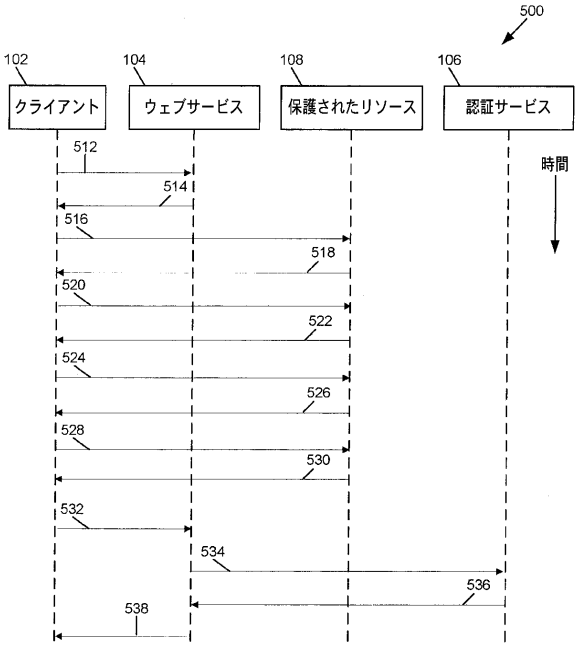
【図３】


START
300
302
リクエストを
受信する
304
チャレンジを送る
306
確認応答を受信する
308
確認応答を検証したか？
検証
されない
310
リクエストを拒否する
YES
検証された
312
さらに
認証が要求されるか
？
NO
314
セキュリティトークンを
発行する
END

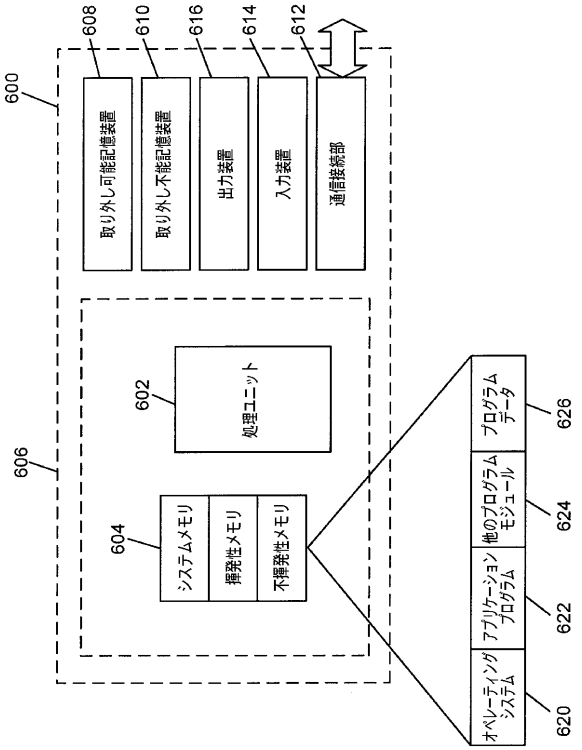
【図４】


START
400
404
リクエストを
受信する
406
認証が要求されたか？
YES
NO
408
認証が
要求されたことを
伝える
410
認証を受信して評価する
評価が
不十分である
411
リクエストが
拒否されたことを
伝える
412
評価が十分である
要求された動作を
実行する
414
要求が
完了したことを
伝える
416
別のリクエストがあるか
？
YES
NO
END

【図５】


500
102
104
108
106
クライアント
ウェブサービス
保護されたリソース
認証サービス
時間
512
514
516
518
520
522
524
526
528
530
532
534
536
538

【図６】


600
608
610
616
614
612
取り外し可能記憶装置
取り外し不能記憶装置
出力装置
入力装置
通信接続部
602
処理ユニット
606
604
システムメモリ
揮発性メモリ
不揮発性メモリ
プログラムデータ
626
他のプログラムモジュール
624
アプリケーションプログラム
622
オペレーティングシステム
620

フロントページの続き

(51)Int.Cl. FI
H04L 9/00 673D

(74)代理人 100120112
弁理士 中西 基晴
(74)代理人 100147991
弁理士 鳥居 健一
(74)代理人 100119781
弁理士 中村 彰吾
(74)代理人 100162846
弁理士 大牧 綾子
(74)代理人 100173565
弁理士 末松 亮太
(74)代理人 100138759
弁理士 大房 直樹
(74)代理人 100091063
弁理士 田中 英夫
(74)代理人 100077481
弁理士 谷 義一
(74)代理人 100088915
弁理士 阿部 和夫
(72)発明者 クレイグ マクマートリー
アメリカ合衆国 98052 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 インターナショナル パテンツ内
(72)発明者 アレキサンダー ティー. ワイネルト
アメリカ合衆国 98052 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 インターナショナル パテンツ内
(72)発明者 ヴァディム メレシュク
アメリカ合衆国 98052 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 インターナショナル パテンツ内
(72)発明者 マーク イー. ガバーラ
アメリカ合衆国 98052 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 インターナショナル パテンツ内

審査官 石田 信行

(56)参考文献 特開2007－079992（JP, A）
特開2006－309595（JP, A）
特開2005－301424（JP, A）
特開2006－236281（JP, A）
特開2007－049343（JP, A）
特開2004－234415（JP, A）
特開2002－288138（JP, A）

(58)調査した分野(Int.Cl., DB名)
G06F 21／31
G06F 21／32
G06F 21／33

H04L 9/32