(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7079798号
(P7079798)

(45)発行日　令和4年6月2日(2022.6.2)

(24)登録日　令和4年5月25日(2022.5.25)

(51)国際特許分類
Ｇ０６Ｆ　21/31　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/31

請求項の数　32　（全28頁）

(21)出願番号　特願2019-570081(P2019-570081)
(86)(22)出願日　平成30年5月16日(2018.5.16)
(65)公表番号　特表2020-524847(P2020-524847A)
(43)公表日　令和2年8月20日(2020.8.20)
(86)国際出願番号　PCT/IB2018/053436
(87)国際公開番号　WO2018/234886
(87)国際公開日　平成30年12月27日(2018.12.27)
審査請求日　令和3年5月14日(2021.5.14)
(31)優先権主張番号　15/626,881
(32)優先日　平成29年6月19日(2017.6.19)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　508045099
シトリックス・システムズ・インコーポレイテッド
Ｃｉｔｒｉｘ　Ｓｙｓｔｅｍｓ，Ｉｎｃ．
アメリカ合衆国、フロリダ州　３３３０９、フォート・ローダーデール、ウエスト・サイプレス・クリーク・ロード　８５１
(74)代理人　110002675
特許業務法人ドライト国際特許事務所
(72)発明者　フェン　フアン
英国　ＣＢ４　０ＦＹ　ケンブリッジシャー　ケンブリッジ　サイエンス　パーク　１０１
(72)発明者　ジャン－リュック　ジロー
英国　ＣＢ４　０ＦＹ　ケンブリッジシャー
最終頁に続く

(54)【発明の名称】　クラウドサービスにおける動的な柔軟な認証のためのシステム及び方法

(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よって、リソースにアクセスするための要求をクライアントデバイスから受信し、
前記コンピューティングデバイスによって、前記要求に対応するコンテキスト情報を決定し、
前記コンピューティングデバイスによって、前記コンテキスト情報に基づいてスコアを決定し、
前記コンピューティングデバイスによって、前記スコアに基づいて前記要求に認証レベルを割り当て、
前記コンピューティングデバイスによって、前記認証レベルに基づいて、前記コンピューティングデバイスから発行された初期トークンと、１つ以上の認証サービスのＩＤと、認証パラメータとを有する認証チャレンジを生成し、
前記コンピューティングデバイスによって、前記クライアントデバイスへの前記認証チャレンジの送信に応答して、前記クライアントデバイスから更新されたトークンを受信し、
前記更新されたトークンは、前記１つ以上の認証サービスに対する前記クライアントデバイスのユーザの認証を示す情報を前記初期トークンに含めることによって生成され、前記ユーザの前記認証は、少なくとも１つの認証プロトコルと、前記認証チャレンジへの応答の前記認証パラメータとを用いて達成され、前記認証を示す情報は、前記認証チャレンジに応答してなされた前記クライアントデバイスからの認証要求に対する応答の一部として

前記１つ以上の認証サービスによって前記初期トークンに含まれ、
前記コンピューティングデバイスによって、前記更新されたトークンで示された前記１つ以上の認証サービスに対する前記クライアントデバイスの前記ユーザの前記認証に基づいて、前記クライアントデバイスに前記リソースへのアクセスを提供する、
ことを含む方法。
【請求項２】
前記コンピューティングデバイスによって前記初期トークンを保存することをさらに含む、請求項１に記載の方法。
【請求項３】
前記コンピューティングデバイスによって、
少なくとも１つの認証スキームを実行するための認証サービスを識別し、
前記認証パラメータに前記認証サービスのＩＤを含める、
ことをさらに含む、請求項１に記載の方法。
【請求項４】
前記認証チャレンジの受信により、前記クライアントデバイスによって、前記初期トークンを有する認証要求を送信し、
前記クライアントデバイスによって、前記少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する前記更新されたトークンを受信する、
ことをさらに含む、請求項３に記載の方法。
【請求項５】
前記更新されたトークンの受信により、前記クライアントデバイスによって、前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されたか否かを判断し、
前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されたという判断により、前記更新されたトークンを前記コンピューティングデバイスに送信する、
ことをさらに含む、請求項４に記載の方法。
【請求項６】
前記更新されたトークンに含まれる１つ以上のアサーションが前記少なくとも１つの認証プロトコルを満たすという判断により、前記コンピューティングデバイスによって、前記リソースにアクセスするための前記要求を許可することをさらに含む、請求項５に記載の方法。
【請求項７】
前記リソースにアクセスするための前記要求を許可すると、前記コンピューティングデバイスによって、前記更新されたトークンを破棄することをさらに含む、請求項６に記載の方法。
【請求項８】
前記リソースにアクセスするための前記要求を許可すると、前記コンピューティングデバイスによって、前記初期トークンを破棄することをさらに含む、請求項６に記載の方法。
【請求項９】
前記コンピューティングデバイスによって、
前記更新されたトークンに関連付けられたタイムスタンプが規定の制限時間内にあるか否かを判断し、
前記タイムスタンプが前記規定の制限時間内にあるという判断により、前記リソースにアクセスするための前記要求を許可する、
ことをさらに含む、請求項６に記載の方法。
【請求項１０】
前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されていないという判断により、前記更新されたトークンを所定の認証サービスに送信することをさらに含む、請求項５に記載の方法。
【請求項１１】
前記初期トークンは、前記要求に含まれる１つ以上の認証資格情報のうち成功した認証を

示す初期アサーションを有する、請求項１に記載の方法。
【請求項１２】
前記要求は、前記ユーザを識別するユーザ情報を有する、請求項１に記載の方法。
【請求項１３】
前記リソースは、セルフサービスパスワードリセットサービスである、請求項１に記載の方法。
【請求項１４】
前記初期トークンは、前記１つ以上の認証サービスによる前記少なくとも１つの認証プロトコルの実行の動作を指定する情報を含む、請求項１に記載の方法。
【請求項１５】
前記認証を示す情報は、少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する、請求項１に記載の方法。
【請求項１６】
プロセッサと、
コンピューティングシステムでユーザを認証するための方法を前記プロセッサに実施させるプログラミング命令を有する非一時的なコンピュータ読み取り可能な記憶媒体と、を備え、
前記プログラミング命令は、
ユーザに関連付けられたコンピューティングデバイスから、リソースサービスに関連付けられたリソースにアクセスするためのアクセス要求を受信し、
前記アクセス要求に対応するコンテキスト情報を決定し、
前記コンテキスト情報に基づいてスコアを決定し、
前記スコアに基づいて前記アクセス要求に認証レベルを割り当て、
前記認証レベルを用いて、前記ユーザを認証するための認証プロトコルであって、少なくとも１つの認証スキームを有する認証プロトコルを識別し、
前記識別された認証プロトコルに対応する初期トークンと認証パラメータとを有する認証チャレンジを生成し、
前記認証チャレンジを前記コンピューティングデバイスに送信するための命令を有する、コンピューティングシステム。
【請求項１７】
前記プログラミング命令は、前記初期トークンを保存するための命令をさらに有する、請求項１６に記載のコンピューティングシステム。
【請求項１８】
前記コンピューティングシステムは、１つ以上の認証サービスを備えており、
前記プログラミング命令は、さらに、
前記１つ以上の認証サービスのうち、前記少なくとも１つの認証スキームを実行する認証サービスを識別し、
前記認証パラメータに前記識別された認証サービスのＩＤを含めるための命令を有する、請求項１６に記載のコンピューティングシステム。
【請求項１９】
前記プログラミング命令は、前記コンピューティングデバイスに、
前記初期トークンを有する認証要求を送信させ、
前記少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する更新されたトークンを受信させるための命令をさらに有する、
請求項１８に記載のコンピューティングシステム。
【請求項２０】
前記プログラミング命令は、前記コンピューティングデバイスに、
前記更新されたトークンの受信により、前記識別された認証プロトコルに含まれるすべての認証スキームが実行されたか否かを判断し、
前記識別された認証プロトコルに含まれるすべての認証スキームが実行されたという判断

により、前記更新されたトークンを前記リソースサービスに送信すること、を実行させるための命令をさらに有する、
請求項１９に記載のコンピューティングシステム。
【請求項２１】
前記プログラミング命令は、前記更新されたトークンに含まれる１つ以上のアサーションが前記識別された認証プロトコルを満たすという判断により、前記リソースにアクセスするための前記アクセス要求を前記プロセッサに許可させるための命令をさらに有する、請求項２０に記載のコンピューティングシステム。
【請求項２２】
前記プログラミング命令は、前記リソースにアクセスするための前記アクセス要求を許可すると、前記プロセッサに前記更新されたトークンを破棄させるための命令をさらに有する、請求項２１に記載のコンピューティングシステム。
【請求項２３】
前記プログラミング命令は、前記リソースにアクセスするための前記アクセス要求を許可すると、前記プロセッサに前記初期トークンを破棄させるための命令をさらに有する、請求項２１に記載のコンピューティングシステム。
【請求項２４】
前記プログラミング命令は、前記プロセッサに、
前記更新されたトークンに関連付けられたタイムスタンプが規定の制限時間内にあるか否かを判断させ、
前記タイムスタンプが前記規定の制限時間内にあるという判断により、前記リソースにアクセスするための前記アクセス要求を許可させるための命令をさらに有する、請求項２１に記載のコンピューティングシステム。
【請求項２５】
前記初期トークンは、前記アクセス要求に含まれる１つ以上の認証資格情報のうち成功した認証を示す初期アサーションを有する、請求項１６に記載のコンピューティングシステム。
【請求項２６】
前記アクセス要求は、前記ユーザを識別するユーザ情報を有する、請求項１６に記載のコンピューティングシステム。
【請求項２７】
前記アクセス要求に対応する前記コンテキスト情報を決定することは、前記ユーザ情報に基づいて前記コンテキスト情報を決定することを含む、請求項２６に記載のコンピューティングシステム。
【請求項２８】
前記コンテキスト情報は、前記ユーザの１つ以上の特性、前記リソースの１つ以上の特性、または前記コンピューティングデバイスの１つ以上の特性のうちの１つ以上を有する、請求項１６に記載のコンピューティングシステム。
【請求項２９】
プロセッサと、
コンピューティングシステムでユーザを認証するための方法を前記プロセッサに実施させるプログラミング命令を有する非一時的なコンピュータ読み取り可能な記憶媒体と、を備え、
前記プログラミング命令は、
リソースにアクセスするための要求をクライアントデバイスから受信し、
前記要求に対応するコンテキスト情報を決定し、
前記コンテキスト情報に基づいてスコアを決定し、
前記スコアに基づいて前記要求に認証レベルを割り当て、
前記認証レベルに基づいて、コンピューティングデバイスから発行された初期トークンと、１つ以上の認証サービスのＩＤと、認証パラメータとを有する認証チャレンジを生成し、

前記クライアントデバイスへの前記認証チャレンジの送信に応答して、前記クライアントデバイスから更新されたトークンを受信し、前記更新されたトークンは、前記１つ以上の認証サービスに対する前記クライアントデバイスのユーザの認証を示す情報を前記初期トークンに含めることによって生成され、前記ユーザの前記認証は、少なくとも１つの認証プロトコルと、前記認証チャレンジへの応答の前記認証パラメータとを用いて達成され、前記認証を示す情報は、前記認証チャレンジに応答してなされた前記クライアントデバイスからの認証要求に対する応答の一部として前記１つ以上の認証サービスによって前記初期トークンに含まれ、
前記更新されたトークンで示された前記１つ以上の認証サービスに対する前記クライアントデバイスの前記ユーザの前記認証に基づいて、前記クライアントデバイスに前記リソースへのアクセスを提供するための命令を有する、コンピューティングシステム。
【請求項３０】
前記プログラミング命令は、前記クライアントデバイスに、
前記初期トークンを有する認証要求を送信させ、
少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する前記更新されたトークンを受信させるための命令をさらに有する、請求項２９に記載のコンピューティングシステム。
【請求項３１】
前記プログラミング命令は、前記クライアントデバイスに、
前記更新されたトークンの受信により、前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されたか否かを判断し、
前記少なくとも１つの認証プロトコルに含まれるすべての認証スキームが実行されたという判断により、前記更新されたトークンを前記プロセッサに送信すること、を実行させるための命令をさらに有する、請求項２９に記載のコンピューティングシステム。
【請求項３２】
前記プログラミング命令は、前記更新されたトークンに含まれる１つ以上のアサーションが前記少なくとも１つの認証プロトコルを満たすという判断により、前記リソースにアクセスするための前記要求を前記プロセッサに許可させるための命令をさらに有する、請求項３０に記載のコンピューティングシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
本出願は、２０１７年６月１９日に出願された米国特許出願第１５／６２６，８８１号の優先権を主張し、その開示は参照により本明細書に組み込まれる。
【０００２】
本開示は、一般にクラウドコンピューティングシステムに関する。より詳細には、本発明は、強化されたセキュリティを可能にするクラウド環境におけるユーザ認証のためのシステムおよび方法の実施に関する。
【背景技術】
【０００３】
クラウドコンピューティングにより、ユーザは、ユーザのローカルコンピュータ上ではなく、遠隔地にあるコンピュータ上で実行されるアプリケーションまたはサービスを利用することができる。例えば、クライアントコンピュータからサーバコンピュータにデータを転送することにより、クラウドでデータが処理される。サーバコンピュータでは、処理されたデータをクライアントコンピュータに返す前にデータが処理される。このようにして、クライアントコンピュータは、処理タスクをクラウド内のコンピュータにオフロードする。クラウドコンピューティングには多くの利点があるが、クラウド環境のリソースへのアクセスを制御するためのユーザの認証は、システム管理者にとって大きな課題である。
【０００４】

当初、ユーザ名とパスワードは、デジタル情報とリソースへのアクセスを保護するための有効な手段として機能していた。ユーザ名とパスワードの代替手段として、より強力な形式の「要素」認証も使用することができる。「要素」認証は、個人、企業、および政府のデジタル情報への不正アクセスを防止する安全な方法を提供する。二要素認証、三要素認証、および四要素認証では、接触型のスマートカード、生体認証デバイス、知識ベース認証、ＩＤ検証サービス、およびワンタイムパスワードトークンなどのツールを使用する。認証の「要素」は、「あなたが持っているもの」である物理的な人間以外のデバイスと、「あなたが何か」である人間の生体認証と、「あなたが知っている何か」である人間の記憶と、「他の誰かがあなたについて知っている何か」である公的記録または第三者検証サービスなどの個人的な検証と、に分類される。通常、管理者とシステム所有者は、ユーザまたはネットワークベースのシステムを認証する１つの方法または場合によっては２つの方法のみを提供する。

【０００５】

さらに、サーバは、クライアントを認証するための認証モデルで構成することにより、アプリケーションまたはリソースのユーザまたはクライアントを認証することができる。しかしながら、認証モデルの現在の厳格なポリシー構造により、サーバを構成可能な認証モデルのタイプまたは機能が制限されることがある。具体的には、現在の認証モデルは、ユーザアクセスに対して画一的なアプローチをとるように構成されている。種々の認証モデルおよび／またはアプリケーションは、インストールされて作動するか、アンインストールされてシステムに存在しないかのいずれかである。システム所有者または管理者が、組織もしくはシステム所有者の要件またはポリシーに基づいて動的または自動的にログオン環境を制御するための中間的な態様も柔軟性もない。しかしながら、例えば、単一のコンピュータシステムには、システム内の様々なリソースに対して様々なレベルのアクセス権を有する様々な種類のユーザが含まれる。システム内のユーザとリソースは様々であるため、管理者は複数の認証メカニズムを使用して異なるリソースを保護することを望むであろう。しかしながら、複数の認証メカニズムを保守することは、管理者とシステム全体に多大な負担を与えてしまう可能性がある。

【発明の概要】

【０００６】

クラウドコンピューティングシステム内のリソースへのアクセスを要求するユーザを認証するためのシステムおよび方法を実施する。当該方法は、リソースサービスによって、ユーザに関連付けられたコンピューティングデバイスからリソースサービスに関連付けられたリソースにアクセスするためのアクセス要求を受信し、アクセス要求に対応するコンテキスト情報を決定し、決定されたコンテキスト情報を用いて、ユーザを認証するための認証プロトコルを識別する。認証プロトコルは、少なくとも１つの認証スキームを有する。当該方法は、さらに、認証チャレンジを生成し、認証チャレンジをコンピューティングデバイスに送信する。認証チャレンジは、識別された認証プロトコルに対応する初期トークンと認証パラメータとを有する。シナリオによっては、リソースサービスは初期トークンを保存する。シナリオによっては、コンテキスト情報は、ユーザの１つ以上の特性、リソースの１つ以上の特性、および／またはコンピューティングデバイスの１つ以上の特性を有する。

【０００７】

シナリオによっては、当該方法は、さらに、少なくとも１つの認証スキームを実行するための認証サービスを識別し、認証パラメータに認証サービスのＩＤを含める。コンピューティングデバイスは、認証チャレンジを受信すると、識別された認証サービスに、初期トークンを有する認証要求を送信する。次いで、認証サービスは、少なくとも１つの認証スキームを実行し、更新されたトークンをコンピューティングデバイスに送信する。更新されたトークンは、少なくとも１つの認証スキームの実行時のユーザ認証のステータスを示すアサーションを有する。コンピューティングデバイスは、更新されたトークンを受信すると、識別された認証プロトコルに含まれるすべての認証スキームが実行されたか否かを

判断し、識別された認証プロトコルに含まれるすべての認証スキームが実行された場合、リソースサービスに更新されたトークンを送信する。コンピューティングデバイスは、識別された認証プロトコルに含まれるすべての認証スキームが実行されていない場合、更新されたトークンを第２の認証サービスに送信する。

【０００８】

そのようなシナリオまたは他のシナリオでは、更新されたトークンに含まれる１つ以上のアサーションが識別された認証プロトコルを満たす場合、リソースサービスは、リソースにアクセスするためのアクセス要求を許可する。これらのシナリオまたは他のシナリオでは、リソースサービスは、リソースにアクセスするためのアクセス要求を許可すると、更新されたトークンおよび／または初期トークンを破棄する。そのようなシナリオまたは他のシナリオでは、リソースサービスは、更新されたトークンに関連付けられたタイムスタンプが規定の制限時間内にあるか否かを判断し、タイムスタンプが規定の制限時間内にある場合にのみ、リソースにアクセスするためのアクセス要求を許可する。

【０００９】

シナリオによっては、初期トークンは、アクセス要求に含まれる１つ以上の認証資格情報のうち成功した認証を示す初期アサーションを有する。

【００１０】

シナリオによっては、アクセス要求は、ユーザを識別するユーザ情報を有し、アクセス要求に対応するコンテキスト情報を決定することは、ユーザ情報に基づいてコンテキスト情報を決定することを含む。

【００１１】

決定されたコンテキスト情報を用いてユーザを認証するための認証プロトコルを識別するいくつかのシナリオでは、決定されたコンテキスト情報に基づいて認証レベルを決定し、認証レベルに対応する認証プロトコルを識別する。

【図面の簡単な説明】

【００１２】

以下の図面を参照して実施形態を説明するが、図面全体を通して、同様の参照符号は同様の特徴を表す。

【図１】例示的なネットワークおよびコンピューティング環境の図である。

【図２】例示的なコンピューティングデバイスの図である。

【図３】例示的なクラウドコンピューティング環境の図である。

【図４】クラウド環境内のリソースへのアクセスを許可する前にユーザを認証するための例示的な方法を示すフローチャートである。

【図５】クラウドコンピューティング環境のセルフサービスパスワードリセットサービスへのアクセスを要求するユーザを認証するための例示的な方法を示すメッセージフロー図である。

【発明を実施するための形態】

【００１３】

本明細書で一般的に説明され、添付図面に示された実施形態の構成要素は、多種多様な異なる構成で配置および設計され得ることが容易に理解されよう。したがって、図示されている様々な実施形態の以下のより詳細な説明は、本開示の範囲を限定するものではなく、様々な実施形態の単なる代表例である。実施形態の様々な態様が図面に提示されているが、特に明示しない限り、図面は必ずしも縮尺通りに描かれていない。

【００１４】

本発明は、その精神または本質的な特徴から逸脱することなく、他の特定の形態で具現化することができる。説明された実施形態は、あらゆる点で単なる例示にすぎず、限定的に解釈してはならない。したがって、本発明の範囲は、添付の特許請求の範囲によって示されるのであって、この詳細な説明には、なんら拘束されない。特許請求の範囲の均等物の意味および範囲内における変更はすべて本発明の範囲内に包含されるべきである。

【００１５】

本明細書全体を通して、特徴、利点、または類似の用語への言及は、本発明で実現され得る特徴および利点のすべてが本発明の任意の単一の実施形態であるべきであることを意味しない。むしろ、特徴および利点に言及する用語は、実施形態に関連して説明される特定の特徴、利点、または特性が本発明の少なくとも１つの実施形態に含まれることを意味すると理解される。したがって、本明細書全体にわたる特徴および利点、ならびに類似の言語の議論は、必ずしもそうではないが、同じ実施形態を指す場合がある。

【００１６】

さらに、本発明の記載された特徴、利点、および特性は、１つ以上の実施形態において任意の適切な方法で組み合わせることができる。当業者は、本明細書の説明に照らして、特定の実施形態の１つ以上の特定の特徴または利点なしで本発明が実施可能であることを認識するであろう。他の例では、本発明のすべての実施形態で示されていない特定の実施形態において、追加の特徴および利点が認識される場合がある。

【００１７】

本明細書全体を通して、「一実施形態」（one embodiment）、「実施形態」（an embodiment）、または同様の文言への言及は、示された実施形態に関連して説明された特定の特徴、構造、または特性が本発明の少なくとも１つの実施形態に含まれることを意味する。したがって、本明細書全体を通して、「一実施形態では」（in one embodiment）、「実施形態では」（in an embodiment）という文言、および同様の文言は、必ずしもそうではないが、すべて同じ実施形態を指す場合がある。

【００１８】

本文書で用いられている単数形「a」、「an」、および「the」は、文脈上特に明記されていない限り、複数形の言及を含む。別段に定義されない限り、本明細書で用いられているすべての技術用語および科学用語は、当業者によって一般に理解されるのと同じ意味を有する。本文書で用いられている「含む／有する」（comprising）という用語は「含むが、それに限定されない」（including, but not limited to）ことを意味する。

【００１９】

本明細書で用いられている「機密情報」（sensitive information）という用語は、ユーザまたはエンティティのプライバシーおよび／またはセキュリティを保護するために不正アクセスから保護されるべきデータを指す。例として、アクセス認証情報（access credentials）、個人情報、医療情報、財務情報、社会保障情報などの固有識別子、生体認証データ、企業秘密、顧客およびサプライヤ情報、従業員データなどが挙げられる。

【００２０】

用語「認証資格情報」（authentication credential）は、コンピューティングシステムへのアクセスを得るためにユーザが提示することができるユーザに固有の電子トークンまたは他のオブジェクトを指す。認証資格情報の例として、ユーザ名、パスワード、生体認証、セキュリティ質問への回答、前述のいずれかの組み合わせなどが挙げられるが、これらに限定されない。

【００２１】

ここで図１を参照すると、本明細書で説明する実施形態が実現される例示的なコンピューティング環境を示す概略ブロック図が示されている。図１は、１つ以上のサーバ１０６Ａ～１０６Ｎ（本明細書では概して「サーバ１０６Ａ～Ｎ」と称する。）と通信する１つ以上のクライアントマシン１０２Ａ～１０２Ｎ（本明細書では概して「クライアントマシン１０２Ａ～Ｎ」と称する。）を備えるコンピューティング環境１０１の一実施形態を示す。クライアントマシン１０２Ａ～Ｎとサーバ１０６Ａ～Ｎとの間にはネットワーク１０４が設置されている。

【００２２】

一実施形態では、コンピューティング環境１０１は、サーバ１０６Ａ～Ｎとクライアントマシン１０２Ａ～Ｎとの間に設置されたアプライアンスを備えてもよい（ここでは図示せず。）。このアプライアンスはクライアント／サーバ接続を管理しており、場合によっては複数のバックエンドサーバ間でクライアント接続の負荷を分散することができる。例え

ば、当該アプライアンスは、クラウドベースの環境でサーバ１０６Ａ～Ｎがホストするコンピューティングリソース（クラウドハードウェアおよびソフトウェアリソース）へのアクセスのため、クライアントマシン１０２Ａ～Ｎとサーバ１０６Ａ～Ｎとの間の通信リンクを提供するクラウド管理サーバおよび／またはクラウドコネクタである。管理サーバは、例えば、とりわけ、フロリダ州フォートローダーデールのCitrix Systems, Inc.によるCLOUDSTACK、またはOPENSTACKを実行する。クラウドハードウェアおよびソフトウェアリソースは、プライベートおよび／またはパブリックコンポーネントを有する。例えば、クラウドは、１つ以上の特定の顧客またはクライアントコンピュータによって使用され、および／またはプライベートネットワークを介して使用されるプライベートクラウドとして構成される。他の実施形態では、パブリッククラウドまたはパブリックプライベートクラウドは、オープンまたはクローズドネットワークを介して他の顧客によって使用される。

【００２３】

クライアントマシン１０２Ａ～Ｎについて、いくつかの実施形態では、単一のクライアントマシンまたは単一グループのクライアントマシンと称することができ、一方、サーバ１０６Ａ～Ｎは、単一のサーバまたは単一グループのサーバと称される。一実施形態では、単一のクライアントマシンが複数のサーバと通信し、一方、別の実施形態では、単一のサーバが複数のクライアントマシンと通信する。さらに別の実施形態では、単一のクライアントマシンが単一のサーバと通信する。

【００２４】

クライアントマシン１０２Ａ～Ｎは、いくつかの実施形態では、以下の用語のいずれか１つによって言及することができる：クライアントマシン；クライアント；クライアントコンピュータ；クライアントデバイス；クライアントコンピューティングデバイス；ローカルマシン；リモートマシン；クライアントノード；エンドポイント；エンドポイントノード；または第２のマシン。サーバ１０６Ａ～Ｎは、いくつかの実施形態では、以下の用語のいずれか１つによって言及される：サーバ；ローカルマシン；リモートマシン；サーバファーム；ホストコンピューティングデバイス；または第１のマシン。

【００２５】

一実施形態では、クライアントマシン１０２Ａ～Ｎのうちの１つ以上は仮想マシンであり得る。仮想マシンは任意の仮想マシンとすることができ、いくつかの実施形態では、仮想マシンは、Citrix Systems、IBM、VMwareにより開発されたハイパーバイザまたは他のハイパーバイザによって管理される任意の仮想マシンであり得る。他の実施形態では、仮想マシンは任意のハイパーバイザによって管理され、一方、さらに他の実施形態では、仮想マシンはサーバで実行するハイパーバイザまたはクライアントマシンで実行するハイパーバイザによって管理され得る。

【００２６】

クライアントマシン１０２Ａ～Ｎは、いくつかの実施形態では、以下のいずれか１つのアプリケーションを実行、動作、または提供することができる：ソフトウェア；プログラム；実行可能な命令；仮想マシン；ハイパーバイザ；Ｗｅｂブラウザ；Ｗｅｂベースのクライアント；クライアント・サーバアプリケーション；シンクライアントコンピューティングクライアント；ＡｃｔｉｖｅＸコントロール；Ｊａｖａ（登録商標）アプレット；ソフトＩＰ電話のようなVoice over Internet Protocol(ＶｏＩＰ)通信に関連するソフトウェア；ビデオおよび／またはオーディオをストリーミングするためのアプリケーション；リアルタイムデータ通信を容易にするためのアプリケーション；ＨＴＴＰクライアント；ＦＴＰクライアント；Ｏｓｃａｒクライアント；Ｔｅｌｎｅｔクライアント；その他の実行可能な命令のセット。さらに他の実施形態は、サーバ１０６Ａ～Ｎまたは他の遠隔設置されたマシン上でリモート実行するアプリケーションによって生成されたアプリケーション出力を表示する１つ以上のクライアントマシン１０２Ａ～Ｎを備える。これらの実施形態では、クライアントマシン１０２Ａ～Ｎは、アプリケーションウィンドウ、ブラウザ、または他の出力ウィンドウにアプリケーション出力を表示することができる。一実施形態

では、アプリケーションはデスクトップであるが、他の実施形態では、アプリケーションはデスクトップを生成するアプリケーションである。

【００２７】

サーバ１０６Ａ～Ｎは、いくつかの実施形態では、シンクライアントまたはリモートディスプレイプロトコルを使用するリモートプレゼンテーションクライアントまたは他のクライアントプログラムを実行して、サーバ上で実行されるアプリケーションによって生成されたディスプレイ出力を取得し、アプリケーション表示出力をリモートクライアントマシン１０２Ａ～Ｎに送信する。シンクライアントまたはリモートディスプレイプロトコルは、以下のプロトコルのいずれか１つである：フロリダ州フォートローダーデールのCitrix Systems, Inc.によって製造されたIndependent Computing Architecture(ＩＣＡ)プロトコル；または、ワシントン州レドモンドのMicrosoft Corporationによって製造されたRemote Desktop Protocol(ＲＤＰ)。

【００２８】

コンピューティング環境１０１は、サーバ１０６Ａ～Ｎが論理的にグループ化されてサーバファームとなるように、２つ以上のサーバ１０６Ａ～Ｎを備えてもよい。サーバファームは、サーバファーム内で地理的に分散して論理的にグループ化されたサーバを設けてもよいし、またはサーバファーム内で互いに近接して論理的にグループ化されたサーバを設けてもよい。サーバファーム内で地理的に分散したサーバは、いくつかの実施形態では、ＷＡＮ、ＭＡＮ、またはＬＡＮを用いて通信することができる。ここで、異なる地理的地域を以下のように特徴付けることができる：異なる大陸；一大陸での異なる地域；異なる国；異なる州；異なる都市；異なるキャンパス；異なる部屋；または、前述の地理的位置の任意の組み合わせ。いくつかの実施形態では、サーバファームは単一のエンティティとして管理され、一方、他の実施形態では、サーバファームは複数のサーバファームを設けてもよい。

【００２９】

一部の実施形態では、サーバファームは、実質的に同様のタイプのオペレーティングシステムプラットフォームを実行するサーバ１０６Ａ～Ｎを備えてもよい（例えば、ワシントン州レドモンドのMicrosoft Corporation製のWINDOWS NT（登録商標）、UNIX（登録商標）、LINUX、またはSNOW LEOPARD）。他の実施形態では、サーバファームは、第１のタイプのオペレーティングシステムプラットフォームを実行する第１のサーバグループと、第２のタイプのオペレーティングシステムプラットフォームを実行する第２のサーバグループとを備えてもよい。他の実施形態では、サーバファームは、異なるタイプのオペレーティングシステムプラットフォームを実行するサーバを備えてもよい。

【００３０】

サーバ１０６Ａ～Ｎは、いくつかの実施形態では、任意のサーバタイプとすることができる。例えば、サーバは、以下のサーバタイプのいずれかである：ファイルサーバ；アプリケーションサーバ；Ｗｅｂサーバ；プロキシサーバ；アプライアンス；ネットワークアプライアンス；ゲートウェイ；アプリケーションゲートウェイ；ゲートウェイサーバ；仮想化サーバ；展開サーバ；ＳＳＬ ＶＰＮサーバ；ファイアウォール；Ｗｅｂサーバ；アプリケーションサーバまたはマスターアプリケーションサーバ；アクティブディレクトリを実行するサーバ；または、ファイアウォール機能、アプリケーション機能、もしくは負荷分散機能を提供するアプリケーション加速プログラムを実行するサーバ。いくつかの実施形態では、サーバは、リモート認証ダイヤルインユーザサービスを含むＲＡＤＩＵＳサーバであってもよい。サーバがアプライアンスを有する実施形態では、当該サーバは、以下のメーカーのいずれか１つによって製造されたアプライアンスであり得る：Citrix Application Networking Group；Silver Peak Systems, Inc.；Riverbed Technology, Inc.；F5 Networks, Inc.；またはJuniper Networks, Inc.。いくつかの実施形態は、第１のサーバ１０６Ａを有し、第１のサーバ１０６Ａは、１つ以上のクライアントマシン１０２Ａ～Ｎから要求を受信し、当該要求を第２のサーバ１０６Ｂに転送し、クライアントマシン１０２Ａ～Ｎにより生成された要求に第２のサーバ１０６Ｂからの応答で応える。第

１のサーバ１０６Ａは、クライアントマシン１０２Ａ～Ｎが利用可能なアプリケーションの一覧と、アプリケーションの一覧内で識別されたアプリケーションをホストするアプリケーションサーバに関連するアドレス情報とを取得することができる。次いで、第１のサーバ１０６Ａは、ウェブインターフェイスを使用してクライアントの要求に対する応答を提示し、クライアントマシン１０２Ａ～Ｎと直接通信して、クライアントマシン１０２Ａ～Ｎに、識別されたアプリケーションへのアクセスを提供することができる。

【００３１】

サーバ１０６Ａ～Ｎは、いくつかの実施形態では、以下のアプリケーションのいずれか１つを実行することができる：シンクライアントプロトコルを使用してアプリケーションディスプレイデータをクライアントに送信するシンクライアントアプリケーション；リモートディスプレイプレゼンテーションアプリケーションなど。別の実施形態は、以下のようなアプリケーションサーバであるサーバを備える：Microsoft Corporationが製造したMICROSOFT EXCHANGEなどの電子メールサービスを提供する電子メールサーバ；Ｗｅｂサーバまたはインターネットサーバ；デスクトップ共有サーバ；コラボレーションサーバ；または他のタイプのアプリケーションサーバ。さらに他の実施形態は、以下のタイプのホスト型サーバアプリケーションのいずれか１つを実行するサーバを備える：Citrix Online Division, Inc.が提供するGOTOMEETING；カリフォルニア州サンタクララのWebEx, Inc.が提供するWEBEX；または、Microsoft Corporationが提供するMicrosoft Office LIVE MEETING。

【００３２】

クライアントマシン１０２Ａ～Ｎは、いくつかの実施形態では、サーバによって提供されるリソースへのアクセスを求めるクライアントノードであり得る。他の実施形態では、サーバ１０６Ａ～Ｎは、ホストリソースへのアクセスをクライアントマシン１０２Ａ～Ｎに提供する。サーバ１０６Ａ～Ｎは、いくつかの実施形態では、１つ以上のクライアントマシン１０２Ａ～Ｎまたはサーバ１０６Ａ～Ｎと通信するようにマスターノードとして機能する。いくつかの実施形態では、マスターノードは、要求されたアプリケーションをホストするサーバに関連付けられたアドレス情報を識別し、１つ以上のクライアントまたはサーバに提供することができる。さらに他の実施形態では、マスターノードは、サーバファーム、クライアントマシン、クライアントノードのクラスター、またはアプライアンスであり得る。

【００３３】

１つ以上のクライアントマシン１０２Ａ～Ｎおよび／または１つ以上のサーバ１０６Ａ～Ｎは、コンピューティング環境１０１内のマシンとアプライアンスとの間に設置されたネットワーク１０４を介してデータを送信することができる。ネットワーク１０４は、１つ以上のサブネットワークを有してもよく、コンピューティング環境１０１内に含まれるクライアントマシン１０２Ａ～Ｎ、サーバ１０６Ａ～Ｎ、コンピューティングマシンおよびアプライアンスの任意の組み合わせの間に設置することができる。いくつかの実施形態では、ネットワーク１０４として以下のいずれかを採用することができる：ローカルエリアネットワーク（ＬＡＮ）；メトロポリタンエリアネットワーク（ＭＡＮ）；広域ネットワーク（ＷＡＮ）；クライアントマシン１０２Ａ～Ｎとサーバ１０６Ａ～Ｎとの間に位置する複数のサブネットワークから構成されるプライマリネットワーク；プライベートサブネットワークを有するプライマリパブリックネットワーク；パブリックサブネットワーク４を有するプライマリプライベートネットワーク；または、プライベートサブネットワークを有するプライマリプライベートネットワーク。さらに別の実施形態は、以下のネットワークタイプのいずれかを採用し得るネットワーク１０４を備える：ポイントツーポイントネットワーク；ブロードキャストネットワーク；電気通信ネットワーク；データ通信ネットワーク；コンピュータネットワーク；ＡＴＭ（非同期転送モード）ネットワーク；ＳＯＮＥＴ（同期型光ネットワーク）ネットワーク；ＳＤＨ（同期デジタル階層）ネットワーク；ワイヤレスネットワーク；有線ネットワーク；または、ワイヤレスリンクが赤外チャネルまたは衛星帯であり得るワイヤレスリンクを有するネットワーク１０４。ネットワー

ク１０４のネットワークトポロジーは、実施形態によって異なってよく、ネットワークトポロジーの候補として以下が挙げられる：バスネットワークトポロジー；スター型ネットワークトポロジー；リングネットワークトポロジー；リピーターベースのネットワークトポロジー；または層状スターネットワークトポロジー（tiered-star network topology）。追加の実施形態は、プロトコルを使用してモバイルデバイス間で通信する携帯電話ネットワークのネットワーク１０４を備える。そのようなプロトコルとして以下のいずれか１つを採用することができる：ＡＭＰＳ；ＴＤＭＡ；ＣＤＭＡ；ＧＳＭ（登録商標）；ＧＰＲＳ ＵＭＴＳ；またはモバイルデバイス間でデータを送信可能な他のプロトコル。

【００３４】

ここで図２を参照すると、コンピューティングデバイス２００の例示的なアーキテクチャの詳細なブロック図が提供されている。ここで、図１に示すクライアントマシン１０２Ａ～Ｎおよびサーバ１０６Ａ～Ｎは、コンピューティングデバイス２００の任意の実施形態として配置および／または実行することができる。したがって、コンピューティングデバイス２００の以下の説明は、図１のクライアントマシン１０２Ａ～Ｎおよび／またはサーバ１０６Ａ～Ｎを理解するのに十分である。

【００３５】

コンピューティングデバイス２００の構成要素は、図２に示された構成要素よりも多くても少なくてもよい。しかしながら、図示されている構成要素は、本解決手段を実施する例示的な実施形態を開示するのに十分である。図２のハードウェアアーキテクチャは、クラウドコンピューティング環境における機密情報の格納および／または送信を容易にするように構成された代表的なコンピューティングデバイスの一実施形態を表す。したがって、図２のコンピューティングデバイス２００は、以下で説明するように、複数の認証サービスを介して、（ａ）ユーザコンテキストに基づいて適切な認証プロトコルを決定し、（ｂ）当該認証プロトコルに基づいてユーザを認証する方法の少なくとも一部を実施する。

【００３６】

コンピューティングデバイス２００の一部またはすべての構成要素は、ハードウェア、ソフトウェア、および／またはハードウェアとソフトウェアとの組み合わせとして実現することができる。ハードウェアには、１つ以上の電子回路が含まれるが、これらに限定されない。電子回路には、受動素子（例えば、抵抗器およびコンデンサ）および／または能動素子（例えば、増幅器および／またはマイクロプロセッサ）が含まれ得るが、これらに限定されない。受動素子および／または能動素子は、本明細書に記載の方法、手順、または機能のうちの１つ以上を実行するように構成され、配置され、および／またはプログラムされ得る。

【００３７】

図２に示すように、コンピューティングデバイス２００は、ユーザインターフェイス２０２と、中央処理装置（「ＣＰＵ」）２０６と、システムバス２１０と、システムバス２１０を介してコンピューティングデバイス２００の他の部分に接続されてアクセス可能なメモリ２１２と、システムバス２１０に接続されたハードウェアエンティティ２１４とを備える。ユーザインターフェイスは、入力デバイス（例えば、キーパッド２５０）および出力デバイス（例えば、スピーカー２５２、ディスプレイ２５４、および／または発光ダイオード２５６）を設けることができ、コンピューティングデバイス２００の動作を制御するためのユーザソフトウェア相互作用を促進する。

【００３８】

ハードウェアエンティティ２１４の少なくとも一部は、メモリ２１２へのアクセスおよび使用を伴うアクションを実行する。メモリ２１２として、ＲＡＭ、ディスクドライバおよび／またはコンパクトディスク読み取り専用メモリ（「ＣＤ－ＲＯＭ」）を採用し得る。ハードウェアエンティティ２１４は、コンピュータ読み取り可能な記憶媒体２１８を有するディスクドライブユニット２１６を備える。コンピュータ読み取り可能な記憶媒体２１８には、本明細書に記載の方法、手順、または機能のうちの１つ以上を実行する命令２２０（例えば、ソフトウェアコード）の１つ以上のセットが格納されている。命令２２０は

、コンピューティングデバイス２００による実行中に、メモリ２１２内および／またはＣＰＵ２０６内に完全にまたは少なくとも部分的に常駐するようにしてもよい。メモリ２１２およびＣＰＵ２０６はまた、機械読み取り可能な媒体を構成することができる。本明細書で使用される「機械読み取り可能な媒体」という用語は、命令の１つ以上のセット２２０を格納する単一の媒体または複数の媒体（例えば、集中型または分散型データベース、および／または関連するキャッシュおよびサーバ）を指す。本明細書で使用される「機械読み取り可能な媒体」という用語はまた、コンピューティングデバイス２００による実行のための命令２２２のセットを格納、符号化、または搬送することができ、且つ、コンピューティングデバイス２００に、本明細書で説明される方法のいずれか１つ以上を実行させる任意の媒体も指している。

【００３９】

シナリオによっては、ハードウェアエンティティ２１４は、複数の認証サービスを介して、認証プロトコルに基づくユーザの認証を促進するようにプログラムされた電子回路（例えば、プロセッサ）を有する。これに関して、当該電子回路は、コンピューティングデバイス２００にインストールされたソフトウェアアプリケーション２２４にアクセスして実行することができることを理解されたい。ソフトウェアアプリケーション２２４の機能は、議論が進むにつれて明らかになるだろう。

【００４０】

ここで図３を参照すると、本明細書で説明される１つ以上の例示的な態様を実施するために用いられる例示的なクラウドコンピューティングシステムが示されている。クラウドコンピューティング環境３００の構成要素は、図３に示されている構成要素よりも多くても少なくてもよい。しかしながら、図示されている構成要素は、本解決手段を実施する例示的な実施形態を開示するのに十分である。コンピューティング環境３００の一部またはすべての構成要素は、ハードウェア、ソフトウェア、および／またはハードウェアとソフトウェアとの組み合わせとして実現することができ、本明細書で説明する方法、手順、または機能のうち１つ以上を実行するように構成され、および／またはプログラムされ得る。

【００４１】

図３に示すように、クラウドコンピューティング環境３００は、パブリッククラウドサービスおよびリソースを提供するための外部クラウドサービスプロバイダ３１４を備える。クラウドコンピューティング環境は、さらに、リモートコンピューティングデバイス３０２と、クラウドコネクタ３１０を有する内部クラウド３０６とを備える。クラウドコネクタ３１０は、内部クラウド３０６と外部クラウドサービスプロバイダ３１４との間の通信を促進する。

【００４２】

システム３００は、クラウドコンピューティング環境の形態をとっており、エンティティのいくつかのリソースが外部で管理され、外部クラウドサービスプロバイダのクラウド内に位置する一方で、エンティティの他のリソースはエンティティによって内部的に管理され（内部リソース３０８）、エンティティの独自のサーバ内または他のコンピューティングデバイス内に配置される。本明細書で使用される「内部」という用語のバリエーションは、エンティティ自体によって管理され、および／またはエンティティによって制御され外部クラウドサービスプロバイダによって制御されない１つ以上のコンピューティングデバイスに格納されたリソースを指す。一例として、リソースは、エンティティに関連付けられた許可ユーザによるリモートアクセスのために、エンティティのオンプレミスサーバに格納される。例えば、特定のソフトウェアアプリケーション（例えば、内部アプリケーション）は、雇用主によって制御および管理されたサーバに格納され、1人以上の従業員によってアクセス可能である。本明細書で使用される「外部」という用語のバリエーションは、外部クラウドサービスプロバイダによって管理され、および／または外部クラウドサービスプロバイダによって制御された１つ以上のコンピューティングデバイスに格納されたリソースを指す。一例として、外部リソースは、エンティティに関連付けられた許可ユーザによるアクセスのために、外部クラウドサービスプロバイダのクラウドベースのサ

ーバに格納される。このような例では、外部リソースもエンティティに関連付けられる。リソース（外部および／または内部）には、ネットワーク、ファイル、データ、コンピューティングデバイス、アプリケーション、モジュール、クラウドサービス、機能、または他のエンティティが含まれるが、これらに限定されない。

【００４３】

クラウドコンピューティング環境３００は、パブリッククラウドサービスおよびリソースを提供する外部クラウドサービスプロバイダ３１４を備える。外部クラウドサービスプロバイダ３１４は、ユーザがインターネットを介してアクセスすることができるコンピューティングデバイスに格納されたリソースを有している（図示せず。）。外部クラウドサービスプロバイダ３１４は、外部クラウドサービスプロバイダ３１４の一部ではないかもしれないエンティティの異なる施設にある特定の内部コンピューティングデバイスから別の内部コンピューティングデバイスに情報を転送することもできる。例として、特定の地理的位置にあるプライベートクラウドの一部であるコンピューティングデバイスは、外部クラウドを介して、別の地理的位置にあるエンティティのプライベートクラウド（または、当該エンティティの別のプライベートクラウドでもよい。）の一部でもある別のコンピューティングデバイスに情報を送信することができる。

【００４４】

外部クラウドサービスプロバイダ３１４は、構成サービス、オンプレミスのアクティブディレクトリのシングルサインオンパスワードサービス、１つ以上の認証サービス、セルフサービスパスワードリセットサービス、オンプレミスのアクティブディレクトリアクセスサービス、データストアアクセスサービスなどの様々なリソースを設けることができる。

【００４５】

一実施形態では、構成サービス３１６（「構成サービス」とも称する。）は、外部クラウドサービスプロバイダ３１４（および／または内部アプリケーション）のクラウド内のすべてのサービス間通信を処理する。構成サービス３１６は、外部クラウドサービスプロバイダのすべてのサービスのリストを保持および管理し、それらが提供する機能を含むアドレスまたはエンドポイントをアドバタイズできるようにする。あるサービスが構成サービスに正常に登録されて初めてアクティブになり、他のサービスやアプリケーションと通信可能となる。完了すると、構成サービス３１６は、アクティブで且つ登録されたすべてのサービスのリストをアクティブなサービスとして共有する。構成サービス３１６は、任意のサービスディレクトリまたはリストおよび関連情報を構成ストレージに格納する。構成ストレージは、図１および図２に関連して説明したものなど、任意の種類および形式のストレージおよび／またはメモリを有している。各サービスに関連する情報は、構成ストレージに個別にまたは一緒に格納され、任意の種類の形式で格納される。一実施形態では、構成サービス３１６は、アクセス認証情報、暗号化キー、機密情報などを格納してもよい。

【００４６】

一実施形態では、クラウドコンピューティング環境（例えば、クラウドコンピューティング環境３００）のユーザは、地理的に離れた内部コンピューティングデバイスにインストールされた内部リソースへのアクセス、および／または、外部サーバにある外部リソースへのアクセス、または当該外部リソースの使用を望んでいる。ユーザは、外部クラウドサービスを介して、内部リソースおよび／または外部リソースと接続し、および／またはそうでなければ通信することができる。場合によっては、内部リソースおよび／または外部リソースへのアクセスを提供する前に、ユーザを認証する必要がある。そのような場合、内部リソースおよび／または外部リソースに関連付けられたリソースサービス３２０は、以下でさらに詳細に説明するように、ユーザを認証するための認証ポリシーまたはプロトコルを決定する。一実施形態では、リソースサービス３２０は、１つ以上の内部リソースおよび／または外部リソースに関連付けられる。例えば、リソースサービス３２０は、ユーザから、１つ以上の内部リソースおよび／または外部リソースにアクセスするための要求を受信し、要求されたアクセスを許可する前に当該ユーザを認証する。シングルサインオンプロセスの場合、リソースサービス３２０は、認証すると、個々のリソースへの認証

資格情報の提供をユーザに要求することなく、複数のリソースまたはサービスへのアクセスを許可する。ユーザからのアクセス要求を受信すると、リソースサービス３２０は、ルールセットを用いて、ユーザを認証するための適切な認証プロトコルを決定する。認証プロトコルは、限定されないが、ユーザ固有、デバイス固有、リソース固有の認証ルール（以下で説明。）に対応する認証ルールまたはルールセットに基づいて決定される。一実施形態では、リソースサービス３２０はトークン発行者サービスを設けてもよい。トークン発行者は、様々なエンタープライズ／リソースサービスに対して、承認情報、認証情報、トークンなどのアサーションなどを発行する。

【００４７】

認証プロトコルの例として、アグリゲート認証プロトコル、カスケード認証プロトコル、条件付き認証プロトコル、領域ベースの（realm-based）認証プロトコルなどが挙げられるが、これらに限定されない。認証を達成するためのアグリゲート認証プロトコルには、すべて満たさなければならない複数の個別の認証スキームが含まれる。例えば、２要素認証スキームには、パスワードベースの認証スキームとハードウェアトークンベースの認証スキームの両方を含めることができる。カスケード認証プロトコルでは、いくつかの特定の認証スキームのうち１つのみを満たすようユーザに要請する。通常、これらの認証スキームは、ユーザがこれらのうち１つに対して正常に認証されるまで順番に試行される。他の実施形態では、条件付き認証プロトコルは、認証スキームの順序付けられたリストを備える。最初の認証スキームについて正常に認証された後、システムはその特定のユーザに対して他の認証スキームが必要か否かを判断する。その場合、すべての要件が満たされるまで続行される。これにより、ロジックによっては、ユーザの認証要件が異なることとなる。例えば、特定のグループに属しているユーザが他の認証スキームについてさらに認証する必要がないように、複雑な動作が可能である。別の実施形態では、領域ベースの認証プロトコルは、各認証スキームが単一の領域にマッピングされた認証スキームのリストを備える。ユーザは、認証時に明示的に領域を指定する。これにより、特定の認証スキームが強制的に使用される。ユーザは、使用する認証スキームを決定する。

【００４８】

一実施形態では、認証プロトコルは、潜在的に任意の数の認証スキームを有してもよく、ここで提供される例は、認証スキームの性質または配置を完全に網羅するものではない。認証プロトコルは、種々のタイプの認証スキームを有し、または、これらの認証スキームと関連付けられる。認証スキームの例として、知識ベース認証、第２要素認証、生体ベース認証、パスワードベース認証、証明書ベース認証、拡張認証プロトコル（ＥＡＰ）およびその開発（例：ＰＥＡＰ［保護された拡張認証プロトコル］、ＥＡＰ－ＴＬＳ［トンネル層セキュリティ］、ＥＡＰ－ＴＴＬＳ［トンネルトランスポート層セキュリティ］、ＥＡＰ－ＦＡＳＴ［セキュアトンネリングを利用した柔軟な認証］）、Microsoftチャレンジハンドシェイク認証プロトコル（ＭＳ－ＣＨＡＰ［ｖ１およびｖ２］）、デバイスベースまたはネットワーク識別子ベースの認証（例：メディアアクセス制御［ＭＡＣ］アドレス、インターネットプロトコルアドレス、シリアル番号など）、非暗号化または暗号化されたキーまたはトークン、キー共有、外部デバイス認証（例：ＵＳＢキーベースのロック解除、スマートカード）、ローカルまたは非ローカルパスワード、ネットワークキー、時間ベースのアプローチなどが挙げられるが、これらに限定されない。なお、本明細書で開示する態様に従って、他のログイン／認証方法も実行可能である。さらに、本明細書のイノベーションに関連する種々の実施形態は、セキュリティおよび管理に関連する態様のためにActive Directory（商標）を使用することができる。

【００４９】

認証プロトコルには、それぞれが別個の認証サービスまたはモジュール３１８によって実行またはインスタンス化される１つ以上の認証メカニズム、スキーム、またはプロセスの定義または識別が含まれ得ることが理解されよう。代替方法として、および／または、追加の方法として、認証サービス３１８は、１つ以上の認証メカニズム、スキーム、またはプロセスを実行してもよい。各認証サービス３１８は、実行可能またはインスタンス化可

能なソフトウェア機能、手順、オブジェクトまたはクラスなどの関連ソフトウェア、ハードウェアまたはファームウェアコンポーネント、および構成および認証確認用の関連データ構造またはデータベース情報を有してよい。したがって、認証プロトコルは、ハードウェアまたはハードウェアで実行される実行可能な命令の任意の組み合わせを有してよい。認証プロトコルは、アプリケーション、ライブラリ、スクリプト、プロセス、サービス、タスク、または任意の種類と形式の実行可能な命令を有してよい。認証プロトコルは、ＡＰＩまたは関数呼び出しなどの任意のタイプおよび形式のインターフェイスを介して、本明細書で説明する機能と動作を提供してもよい。認証プロトコルは、アプライアンスおよび／またはサーバなどのデバイス上で１つ以上のサービスとして実行される。認証フレームワークは、Ｗｅｂサービスインターフェイスなどのインターフェイスを提供する。

【００５０】

例えば、パスワード認証サービスは、ユーザによって提供されたパスワードを認証するためのパスワードベースの認証スキームを実行する。別の例では、知識ベースの認証サービスは、ユーザによって提供された様々な応答を認証するための知識ベース認証スキームを実行する。さらに別の例では、認証サービスにはＣＡＰＴＣＨＡモジュール（例：コンピュータと人間を区別する完全に自動化された公開チューリングテスト）が含まれる。これは、ユーザが人間であるか否かを判断するためにコンピューティングで使用される一種のチャレンジレスポンステストである。認証サービスのデータストア、データベースまたはデータ構造は、ユーザを認証するための情報を含んでおり、認証サービスによって提供される認証スキーム用の複数の資格情報、データまたは属性を有している。そのような例として以下が挙げられるが、これらに限定されない：生体指紋情報；生体虹彩情報、顔認識画像または定義；音声認識情報；パスフレーズ；１つ以上のハードウェア、ソフトウェアまたはファームウェアトークンの登録；携帯電話、タブレット、コンピュータシステム、他のデバイスなどのユーザ関連デバイスの登録；質問への回答、個人情報（private information）、電話番号、住所、日付、関係の詳細などを含む秘密データなどの個人情報（personal information）の登録；証明書または認証局の情報；スマートカード登録；クラウドコンピューティング認証サービス、ソーシャルネットワーク認証情報、クラウドメールサービスなどのサードパーティ認証サービスの登録または参照；地理情報；および本明細書で提示される様々な認証プロトコルでの使用に適した他の認証スキームに必要な情報など。認証サービスによって提供される認証スキームの資格情報、データまたは属性は、ユーザ登録時にユーザ、管理者などによってデータストア、データベース、またはデータ構造に追加され、アクティブディレクトリまたは他の適切な形式で維持される。

【００５１】

一実施形態では、認証サービスはリソースサービス３２０に含まれ、その認証サービスに関連する認証スキームは、リソースサービス３２０によって実行される。別の実施形態では、１つ以上の認証サービスは、クラウドコンピューティング環境３００内の他のサービスまたはリソースの一部であってもよい。別の実施形態では、リソースサービスが認証サービスに含まれる。一実施形態では、認証サービス３１８は、トークン発行者サービスを有する。

【００５２】

一実施形態では、アクティブディレクトリは、認証サービスおよび／またはリソースサービスである。別の実施形態では、外部リソースおよび／または内部リソースは、それ自体のトークン発行者サービスに関連付けられている。例えば、（図５に関して）以下で説明するように、セルフサービスパスワードリセット（「ＳＳＰＲ」）はトークン発行者サービスを有する。

【００５３】

一実施形態では、外部クラウドサービスプロバイダ３１４は、セルフサービスパスワードリセット（「ＳＳＰＲ」）サービス（ここでは図示せず。）を有する。ＳＳＰＲサービスは、保護されたシステム、ネットワーク、ファイル、サーバなどの別のリソースにアクセスするために用いられたアクセス認証情報をユーザがリセットすることを許可するリソー

スに対応する。アクセス認証情報には、パスワード、スマートカードピン、生体認証データ、または他の認証メカニズムが含まれる。アクセス認証情報のリセットを希望するユーザは、何らかの方法で自分自身を認証するように求められる。ユーザが認証テストに合格すると、ユーザは自身のアクセス認証情報をリセットし、それを用いてリソースにアクセスすることを許可される。リソース内の情報またはアクセスに対するユーザの権利は、ユーザに関連付けられた許可設定を介して制御される。

【００５４】

クラウドコンピューティング環境３００は、リモートコンピューティングデバイス３０２（例えば、クライアントデバイス）も備え、これは、パーソナルコンピュータ、ラップトップ、タブレット、スマートフォンなどであり、上述のコンピューティングデバイスの１つ以上の構成要素を有する。場合によっては、リモートコンピューティングデバイス３０２はユーザの個人用デバイスである（例えば、ユーザがリモートコンピューティングデバイス３０２を所有している。）。そのような場合、リモートコンピューティングデバイス３０２は、内部クラウドの一部ではないかもしれないが、ユーザが認証された後は、内部クラウドにログインおよび／またはそうでなければアクセスすることができる。他の例では、リモートコンピューティングデバイス３０２は、内部クラウドを管理および制御するエンティティによって所有されてもよい（例えば、会社提供のラップトップ）。そのような場合、ユーザが当該エンティティの施設内の端末にリモートコンピューティングデバイス３０２を接続させると、リモートコンピューティングデバイス３０２は内部クラウドの一部となり得る。そうでない場合、ユーザが当該エンティティの施設外（例えば、ユーザの自宅）でリモートコンピューティングデバイス３０２を使用すると、リモートコンピューティングデバイス３０２は、内部クラウドの一部にはならないかもしれないが、ユーザが認証された後に（例えば、仮想プライベートネットワーク（ＶＰＮ）接続を介して）内部クラウドにログインおよび／またはそうでなければアクセスすることができる。

【００５５】

リモートコンピューティングデバイス３０２は、リモートコンピューティングデバイス３０２にインストールされたクライアントソフトウェアである受信機３０４を有する。受信機３０４によって、リモートコンピューティングデバイス３０２が内部および／または外部クラウドサービスにアクセスすることが可能となる。一例として、リモートコンピューティングデバイス３０２は、受信機３０４を用いて、内部および／または外部クラウドに格納されたアプリケーション、仮想デスクトップ、およびデータに安全にアクセスすることができる。受信機３０４の一例として、フロリダ州フォートローダーデールのCitrix Systems, Inc.によって開発されたCitrix Receiverがある。

【００５６】

クラウドコンピューティング環境３００の内部クラウドはまた、内部クラウドから外部クラウドに送信されているメッセージを分析および／または傍受するクラウドコネクタ３１０を有する。一実施形態では、クラウドコネクタ３１０は、内部クラウドの一部でなくてもよい。クラウドコネクタは、パブリッククラウドのサービスと内部リソース３０８との間の通信を容易にする。

【００５７】

ここで図４を参照すると、クラウド環境内のリソースへのアクセスを提供する前にユーザを認証および認可するための例示的な方法４００が示されている。例示的なクラウド環境３００は図３に示されている。プロセス４００は、システム１００などのシステムによって実行される。例えば、１つ以上の実施形態において、図４に示されるプロセス４００および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、図１～図２の任意のデバイス）によって実行される。他の実施形態では、図４に示されるプロセスおよび／またはその１つ以上のステップは、非一時的なコンピュータ読み取り可能なメモリなどのコンピュータ読み取り可能な媒体に格納されたコンピュータ実行可能な命令で具現化される。代替方法として、または、追加の方法として、プロセス４００のステップのいずれかは、クライアントデバイス、ゲートウェイデバイス、クラウドコネクタ、リソ

ースサービス、認証サービス、外部クラウドプロバイダおよび関連サービス、および／またはサードパーティサーバまたはコンピューティングデバイスで実行される。

【００５８】

クラウド環境のリソースサービスが、当該リソースサービスに関連付けられたリソースにアクセスするための要求（「アクセス要求」）を受信すると、プロセスが４０２で開始する。一実施形態では、リソースサービスは、クライアントデバイスおよび／またはリモートコンピューティングデバイスの受信機を介して要求を受信する。別の実施形態では、リソースサービスはまた、例えばロードバランサ、またはクラウド環境の別のデバイスを介して、ユーザ情報を含む要求を受信する。一実施形態では、アクセス要求はユーザ情報を含む。ここで、ユーザ情報とは、リソースへのアクセスを要求しているユーザを識別するために用いられるユーザに関する情報を指す。例として、ユーザ名、クライアントデバイスＩＤ、ユーザＩＤ番号、パスワードなどが挙げられるが、これらに限定されない。リソースサービスは、ユーザ情報を用いて、例えばクラウドコンピューティングシステムまたはリソースに登録されているユーザのアクティブディレクトリを使用して、アクセスを要求しているユーザを識別する。

【００５９】

アクセス要求を受信すると、リソースサービスは、当該アクセス要求および識別されたユーザに対応するコンテキスト情報を４０４で決定し、識別し、および／または読み出す。アクセス要求に対応するコンテキスト情報は、アクセスを要求しているユーザ、クライアントデバイス、アクセス対象のリソース、またはそれらの組み合わせの１つ以上の特性に関する情報を指す。コンテキスト情報の例として以下を挙げることができるが、これらに限定されない：地理的位置、相対位置、ネットワーク位置などのユーザの位置；デバイスの種類、ネットワーク、または設備（例えば、タブレット、ラップトップ、デスクトップ、端末、スマートフォンなど）または特定のデバイス、モデル、メーカー、シリアル番号など、ユーザがリソースへのアクセスを要求する際に用いたクライアントデバイスに関する情報；オペレーティングシステムのタイプまたはバージョン、セキュリティ構成、動作の状態、特定のセキュリティソフトウェアのインストールまたは構成を含むソフトウェア構成状態など、ユーザがリソースへのアクセスを要求する際に用いたデバイスまたはソフトウェアコンポーネントの特性；システム管理者によって割り当てられたユーザクラス、またはユーザの職務もしくは機能など、ユーザのカテゴリ、クラス、グループ、またはタイプ；リソースによって提供されるデータのタイプ、処理のタイプ、ファイル形式や、リソースに関連付けられたセキュリティのレベルなど、リソースのカテゴリ、クラスまたはタイプ。他の適切なコンテキスト情報および／または特性は当業者にとって明らかであり、本明細書に記載の実施形態は特定の特性に限定されない。

【００６０】

コンテキスト情報は、アクセス要求に関連付けられ、含まれ、および／またはアクセス要求から暗示され、上述のようにアクセスが要求された時点での１つ以上の特性を定義する。例えば、コンテキスト情報の一部またはすべてを、アクセス要求の１つ以上のデータ項目としてアクセス要求に含めることができる。例えば、当該要求は、クライアントデバイスに関連付けられたトークン、ユーザおよび／またはクライアントデバイスのＩＤ、ユーザおよび／またはクライアントデバイスの位置、またはユーザに関連付けられた他の情報を有する。あるいは、コンテキスト情報は、アクセス要求に基づいて（例えば、ユーザＩＤに基づいて）認識され、暗示され、決定され、またはそうでなければ推論され得る。一実施形態では、コンテキスト情報の一部またはすべては、アクティブディレクトリ、サービス、サーバ、システム管理者などの別のデバイスから受信される。例えば、ユーザの特性、アクセス要求の特性、リソースの特性、アクセス要求の受信方法、アクセス要求のネットワークルートもしくはトレース、または、ユーザとリソースサービスとの仲介者からの情報などのアクセス要求に関するサードパーティ情報を用いて、ユーザコンテキストを決定することができる。追加の方法として、または、代替方法として、コンテキスト情報をアクセス要求に全体的または部分的に含めることができる。

【００６１】
コンテキスト情報のソースの例として以下を挙げることができる：ネットワークルート；ネットワークアドレス；ネットワークの位置；ネットワーク仲介情報；ソフトウェアの種類、バージョンおよび／または構成情報などのユーザ側のソフトウェア情報；デバイスタイプ（携帯電話、ラップトップ、タブレット、インターネットカフェデバイスなど）、構成および／またはバージョンまたはモデル情報などのユーザデバイス情報；ユーザによる要求の頻度；最近の認証要求の結果（許可または阻止）などの最近の要求情報；ユーザの年齢、状況などのユーザの個人情報；ユーザの身体的または精神的能力；ユーザの地理的位置；地理上のユーザの動き；匿名サービス、プロキシ、仮想プライベートネットワークサービスなど、ユーザとリソースサービスとの間の仲介者の使用；ユーザによって、またはユーザとのネットワーク通信の一部として使用されるシステムのセキュリティレベル；ユーザとやり取りする情報の暗号化レベルなど。
【００６２】
リソースサービスは、ルールセットにアクセスすることによって要求されたリソースへのアクセスを許可する前に、４０６で、ユーザ情報および／または現在のコンテキスト情報を用いて、ユーザを認証するための適切な認証プロトコルを識別する。一実施形態では、各リソースおよび／またはリソースサービスは、それ自体のルールセットに関連付けられている。代替方法として、および／または、追加の方法として、１つ以上のリソースおよび／またはリソースサービスが同一のルールセットに関連付けられてもよい。
【００６３】
一実施形態では、ルールセットは、ユーザＩＤおよび／またはコンテキスト情報に基づいてアクセス要求に適切な認証レベルを識別し、当該認証レベルを少なくとも１つの認証プロトコルに関連付けるための論理ルールを含む。例えば、ルールセットは、コンテキスト情報全体に基づいて、リソースへのアクセスを要求しているユーザを認証するために必要な保証のレベルまたは程度として、特定の認証レベルを提供する。したがって、特定のコンテキストタイプおよび／または値は、他のコンテキストタイプおよび／または値よりも高いレベルの保証を要するように事前に決定され、それに応じてコンテキスト情報全体に対する認証レベルが選択される。言い換えれば、認証レベルは、ユーザＩＤおよび／またはコンテキスト情報に含まれる様々な要素の関数であり、様々な要素の例として、ユーザの位置、ユーザの役割、リソースタイプなどが挙げられるが、これらに限定されない。例えば、場所に関係なくシステム管理者に高い認証レベルを割り当てることができるが、公共の場所からリソースへのアクセス要求があった場合にのみ、別のユーザに高い認証レベルを割り当てることができる。別の例では、１日の特定の時間帯に、またはユーザの位置が認可された企業の場所であると判断された場合に、リソースへのアクセス要求に低い認証レベルを割り当てることができる。いくつかの他の例では、認証レベルは最後に成功した認証要求以降の時間を考慮に入れてもよい。さらに別の例では、認証レベルの決定にリソース情報を用いることもできる。例えば、ゲームアプリケーションではセキュリティ要件を低くし（リスクインデックスが低い。）、一方、銀行サービスではセキュリティ要件を高くする（リスクインデックスが高い。）。進化するセキュリティ要件もこの方法を使ってサポートされ得る（例えば、新しいポリシーにより写真共有サービスのセキュリティ要件が増加する。）。別の例として、ユーザは、それぞれ特定のリスクの可能性がある金額のオンライン取引、例えば、取引金額（例えば、１００．００ドル未満に対して低い認証レベル、１０００．００ドル未満に対して中間認証レベル、または１０００．００ドルを超える場合に高い認証レベル）のオンライン取引の完了を試みることができる。人口統計プロファイルデータもまた、セキュリティ要件を決定する際のコンテキスト入力として利用される。
【００６４】
認証レベル（高、低、中など）の選択または定義は例として提供されるものであり、他の適切な認証レベル、値、および／または値の範囲が、本明細書で説明する原理から逸脱することなく定義されることは理解されるであろう。例えば、ユーザＩＤおよび／または収

集されたコンテキスト情報に基づいて、アクセス要求に０～１０の認証レベルを割り当てることができる。ここで、０は最低の認証レベルを示し、１０は最高の認証レベルを示す。認証レベルの割り当ては、例えば、個々のコンテキスト情報エレメント（または要素）にスコアを割り当て、これらの個々のスコアを組み合わせてアクセス要求の認証レベルを取得するか、他の適切な方法によって行われる。

【００６５】

一実施形態において、ルールセットは、様々な認証レベルを少なくとも１つの認証プロトコルに関連付けてもよく、各認証プロトコルは、特定の保証レベルで認証を達成するための１つ以上の認証スキームを有する。したがって、認証プロトコルは、認証レベルにふさわしいと事前に決定された認証の保証のレベルまたは程度を提供するように定義または選択される。認証プロトコルは、多要素アグリゲート認証プロトコルなどの非常に高度なセキュリティ方法から、単純なパスワード入力など、セキュリティは低下するが、より便利で社会的に受け入れられる方法までさまざまである。さらに、認証プロトコルに含まれる認証スキームは、必要な認証レベルに応じて異なる。例えば、第１の知識ベース認証スキームは、ユーザに回答させるための３つの質問を有し、第２の知識ベース認証スキームは、ユーザに回答させるための５つの異なる質問を有する。別の例では、認証プロトコルは、同一の認証スキームに対して異なる信頼レベルを要する。例えば、知識ベース認証スキームを含む認証プロトコルでは、ユーザへの５つの質問に対する応答を提出するようユーザに求める。ユーザが５問中４問に正しく答えると、第１の認証プロトコルが満たされるが、第２の認証プロトコルでは、ユーザが認証スキームに応答する必要があるが、当該認証プロトコルを満たすためには５問すべてに正しく答える必要がある。

【００６６】

一実施形態では、ルールセットは、例えば管理者によって、動的に決定および／または事前に決定される。一実施形態では、管理者は、認証レベルおよび／または認証プロトコルを決定するためのルールセットを作成する。一実施形態では、管理者は、新しい認証ルール、レベルおよび／またはプロトコルを作成し、既存のルールセットを変更または削除し、リソースユーザグループおよび/または個々のユーザに認証レベルを割り当て、および再割り当てし、ユーザ登録を削除などする。例えば、管理者は、様々な認証スキームを組み合わせて新しい認証プロトコルを作成し、当該プロトコルを認証レベルに割り当てる。必要に応じて、または、希望に応じて、管理者は、すでに定義済みのスキームに加えて、新しい認証スキームをインポートまたは作成する。管理者は、認証スキームの特性をカスタマイズし、様々な認証プロトコルに対するスキームの合否基準を設定する。管理者は、新しい認証スキームおよび／またはプロトコルを特定のリソース、個々のユーザおよび／またはユーザグループに適用または関連付けることを選択可能である。

【００６７】

図４に戻って参照すると、適切な認証プロトコルが識別されると、リソースサービスは、識別された認証プロトコルに含まれる認証スキームを実行するために必要な１つ以上の認証サービスを４０８で識別する。例えば、識別された認証プロトコルは、知識ベースの認証サービスによって実行される第１認証スキームと、第２要素認証サービスによって実行される第２認証スキームと、生体認証サービスによって実行される第３生体ベース認証スキームとを有する。一実施形態では、１つ以上の認証スキームは同一の認証サービスによって実行されてもよい。代替方法として、および／または、追加の方法として、１つ以上の認証サービスが１つの認証スキームを実行してもよい。一実施形態では、１つ以上の認証スキームが、認証サービスおよび／またはリソースサービスによって実行される。

【００６８】

次に、リソースサービスは、認証チャレンジを４１０で生成し、当該認証チャレンジを、アクセス要求をしたクライアントデバイスの受信機に送信する。一実施形態では、認証チャレンジは初期トークンを有する。初期トークンは、ユーザＩＤ、要求されているアクション／リソース、タイムスタンプ、および他の有用な情報などのステートメントを含む初期アサーションを有する。一実施形態では、識別された認証プロトコルに含まれる１つ以

上の認証スキームが既に実行されたとリソースサービスが判断した場合、リソースサービスは、初期アサーションにそのような実行済みの認証スキームのステータスも含める。認証チャレンジおよび／または初期アサーションは、識別された認証プロトコルを実行するための認証パラメータを有してよいが、特に限定されない。認証パラメータには、識別された認証プロトコルに含まれる認証スキームに関連する情報、位置（ユニフォームリソースロケータ、ＩＰアドレスなど）および／または識別された認証プロトコルに含まれる識別された認証スキームの実行に必要な認証サービスのＩＤ、識別された認証プロトコルに関連付けられた要件および／またはルール（例えば、認証を実行すべき順序、各認証サービスによってどのように成功する認証が実行されるべきかの説明、認証サービスから要求された応答の種類など）、結果のアサーションを認証サービスおよび／またはリソースサービスに返す方法、などが含まれるが、これらに限定されない。認証チャレンジの形式とパラメータは柔軟であり、様々な認証シナリオに対応するように調整される。例えば、Ｗｅｂブラウザベースのアプリケーション用に提供される認証チャレンジには、ＨＴＴＰリダイレクトが含まれる。認証チャレンジは、現在または今後既知の方法を用いて一時的なものとなるように設計されている。一実施形態では、リソースサービスは、初期トークン、認証チャレンジ、および／または初期アサーションを格納する。

【００６９】

一実施形態では、リソースサービスは、初期トークンを提供するためにセキュリティアサーションマークアップ言語（ＳＡＭＬ）標準またはＪＳＯＮウェブトークン（ＪＷＴ）標準を使用する。ＳＡＭＬおよびＪＷＴは例示であって、他の適切な標準および／またはプロトコルを使用することができる。初期トークンは、ユーザＩＤ、コンテキスト情報、デジタル証明書、秘密キーまたは公開キー、認証プロトコル情報またはパラメータなどの情報を有する。一実施形態では、リソースサービスは、ノンスおよび／またはタイムスタンプを初期トークンに追加してもよい。いくつかの実施形態では、初期トークンは、一度のみの使用を許可する方法で署名されてもよい。一実施形態では、リソースサービスは、受信したアクセス要求が、識別された認証プロトコルに含まれる認証スキームに必要な認証資格情報を有するか否か、および／またはリソースサービスがユーザの認証資格情報を検証することができるか否かを判断してもよい。例えば、アクセス要求には、１つ以上のアサーション（タイムスタンプなど）、ユーザ名、パスワードなどを有する認証トークンが含まれるが、これらに限定されない。識別された認証プロトコルに含まれる認証スキームに必要な認証資格情報が検証された場合、初期トークンは、リソースサービスがアクセス要求に含まれる認証資格情報を検証したことを示すアサーションをさらに有する。

【００７０】

認証チャレンジを受信すると、受信機は、認証チャレンジに含まれる認証パラメータを検出し、初期トークンを有する認証要求を４１２で生成し、認証チャレンジで示されたパラメータに従って、当該認証チャレンジ内で識別された少なくとも１つの認証サービスに認証要求を送信する。例えば、受信機は、認証チャレンジで指定された順序で認証要求を認証サービスに送信する。認証サービスに送信される認証要求には、認証サービスによって実行される認証スキームのためのパラメータと適切な認証要件も含まれる。一実施形態では、受信機は、認証要求内に認証サービスによって実行される認証スキームのための応答または資格情報をさらに有する。一実施形態では、受信機は、自身のアサーションを初期トークンに追加してもよい。例えば、識別された認証プロトコルに含まれる１つ以上の認証スキームがすでに実行済みであると受信機が判断した場合、受信機はそのような実行済みの認証スキームのステータスに対応するアサーションを含める。

【００７１】

次に、少なくとも１つの認証サービスは、受信機から認証要求を受信すると、（認証プロトコルに従って）必要な認証スキームをインスタンス化し、実施し、動作し、または４１４で実行する。一実施形態では、認証サービスは、ユーザ（または、１つ以上の認証スキームの一部を構成するユーザもしくはサードパーティサービスプロバイダに関連付けられたハードウェアもしくはソフトウェアなどの他のシステム）へチャレンジを送信するプロ

セス、および／または当該ユーザから応答を受信するプロセスのうち１つ以上のプロセスを引き受ける。例えば、知識ベースの認証サービスは、ユーザに回答させるための一連の質問を発行し、ユーザの応答を格納された正解および認証プロトコル要件（例えば、認証プロトコルは、認証を成功させるために５つのうち４つの正解が必要である。）と比較することによってユーザを認証する。認証スキームの実行後、認証サービスは、初期トークンに、当該認証サービスによって実行された認証スキームのステータス（例えば、成功、合格、失敗、再試行、ロックアウト、パスワード変更など）を示す独自のアサーションを含めることで更新されたトークンを４１６で生成し、当該更新されたトークンを受信機に送信する。例えば、アサーションには、認証サービスによって作成された１つ以上のステートメントが含まれる（例えば、サブジェクトは特定の時間に特定の手段で認証され、サブジェクトは特定の属性と認証のステータス（例えば、成功、合格、失敗、再試行、ロックアウト、パスワード変更など）に関連付けられる。）。別の実施形態では、認証プロトコルに従って、ユーザ応答が格納された正しい情報と一致し、認証が成功したことを示す場合にのみ、認証サービスは初期トークンにアサーションを含める。したがって、認証サービスからアサーションなしで返される初期トークンは、認証が失敗したことを（受信機、認証サービスおよび／またはリソースサービス、または別の仲介者に対して）示している。

【００７２】

少なくとも１つの認証サービスからトークンを受信すると、受信機は、認証パラメータをレビューして、受信された認証チャレンジ内のすべての認証スキームが認証パラメータに従って実行されたか否かを４１８で判断する。

【００７３】

４１８で、受信機が、認証チャレンジ内のすべての認証スキームが実行されたと判断した場合（４１８：ＹＥＳ）、受信機は、アクセスを要求するために、様々な認証サービスから受信したアサーション付きのトークンをリソースサービスに４２０で送信する。一方、４１８で、受信機が、認証チャレンジ内のすべての認証スキームが実行されていないと判断した場合（４１８：ＮＯ）、受信機は、更新されたトークン（以前のアサーションを含む。）を有する新たな認証要求を４２２で生成し、認証チャレンジで指定されたパラメータに基づいて、認証チャレンジ内で識別された少なくとも１つの認証サービスに当該更新されたトークンを送信し、ステップ４１４～４１８が繰り返されるようにする。

【００７４】

言い換えれば、受信機からリソースサービスへのトークンの送信は、識別された認証プロトコルの結果を示している。次に、リソースサービスは、トークンに含まれるアサーションをレビューして、受信したトークンに含まれる（または含まれていない。）アサーションが、識別された認証プロトコルを満たすか否か、すなわち、識別された認証プロトコルのステータス（例えば、成功、合格、失敗、再試行、ロックアウト、詳細情報が必要など）を４２４で判断する。ユーザ認証が成功したと判断された場合（４２４：ＹＥＳ）、リソースサービスは、要求されたリソースへのアクセスを４２６で許可する。ユーザ認証が成功しなかったと判断された場合（４２４：ＮＯ）、リソースサービスは、要求されたリソースへのアクセスを４２８で拒否する。

【００７５】

一実施形態では、リソースサービスは、追加のセキュリティのため、識別された認証プロトコルの完了時にトークンを破棄する。別の実施形態では、リソースサービスは、追加のセキュリティのため、識別された認証プロトコルの完了時に初期アサーションを破棄して、トークンを再利用できないようにする。さらに別の実施形態では、認証サービスおよび／またはリソースサービスは、４２４で、トークンのタイムスタンプを調べて、タイムスタンプが規定の制限時間内にあるか否かを判断することで、アクセスを許可するか否かを判断することで、セキュリティを強化させる。

【００７６】

代替方法として、および／または、追加の方法として、受信機は、受信した認証チャレン

ジ内のすべての認証スキームが実行されたか否かを判断する前に、認証サービスから受信した応答ステータスをレビューして、リソースサービスから受信した認証パラメータに基づいて次のステップを決定してもよい。例えば、認証プロトコルを完了させるために、認証パラメータによってすべての認証スキームの成功が求められる場合において、認証スキームが失敗したことを認証サービスが示したとき、受信機は認証プロセスを中止する。別の例では、受信機は、以前の認証スキームのステータスと認証パラメータにおいて定義されたルールとに基づいて、次の認証スキームおよび／またはモジュールを選択する。

【００７７】

なお、４０２で受信されたアクセス要求は、１つ以上のアサーションを含む認証トークンを有してもよい。リソースサービスは、次の１つ以上の処理を実行するために当該トークンを検証する：トークンに含まれるアサーションが識別された認証プロトコルを満たす場合、アクセスを許可し；トークンに含まれるアサーションが識別された認証プロトコルのすべての要件を満たさない場合、さらなる認証を要請し；および／または、トークンに含まれるアサーションが識別された認証プロトコルの認証要件（上述）を満たさない場合、完全な認証を要請する。

【００７８】

ここで図５を参照すると、例示的なメッセージフロー図のステップは、本明細書に記載の方法を用いてアクセス認証情報（例えば、パスワード）を変更するセルフサービスパスワードリセット（ＳＳＰＲ）サービスへのアクセスを要求するユーザを認証する方法を説明している。なお、図５は、第２要素認証スキームおよび知識ベース認証スキームを用いてＳＳＰＲサービスへのアクセスを提供する前にユーザを認証する方法を示しているが、本明細書で説明する教示はそれほど限定的ではなく、他の認証プロトコル（上述）を用いてクラウドコンピューティング環境内の他のリソースにアクセスするためのユーザ認証についても同様の原理が用いられる。

【００７９】

メッセージフローは５０２で始まり、リモートコンピューティングデバイスによって提供される受信機は、アカウント（例えば、パスワード）のアクセス認証情報をリセットする要求を外部クラウドのＳＳＰＲサービスに送信する。一実施形態では、アクセス認証情報は、ユーザなどの認証情報の所有者を識別および／または認証するために用いられる任意の情報を含む。例えば、認証情報として、ユーザＩＤ（例えば、ユーザ番号、ユーザ名など）および／またはパスワード、個人識別番号（ＰＩＮ）、スマートカードＩＤ、セキュリティ証明書（例：公開鍵証明書）、ユーザの特徴（例えば、指紋リーダー、虹彩スキャン、音声認識、または他の生体認証などのセンサーによってキャプチャされたもの）、または特定の内部／外部リソースにアクセスするための認証に用いられる任意のデータが挙げられるが、これらに限定されない。

【００８０】

アクセス認証情報のリセット要求を受信すると、図４に関して上述したように、ＳＳＰＲサービスは、要求に対応するコンテキスト情報を決定し、識別し、および／または読み出し、当該コンテキスト情報を用いて適切な認証プロトコルを識別する。図５に示すメッセージフロー図の例において、識別された認証プロトコルは２つの認証スキーム（第２要素認証スキームと知識ベース認証スキーム）を有している（なお、本明細書で説明する方法はそれほど限定的ではなく、追加および／または代替の認証スキームまたはプロトコルを用いてもよい。）。次に、ＳＳＰＲサービスは、識別された認証プロトコルに対応する認証パラメータと初期アサーションを含む初期トークン（Ｔ（ｓｓｐｒ））とを有する認証チャレンジを５０４で生成し、保存する。例えば、認証チャレンジには、識別された認証プロトコルに含まれる認証スキーム（すなわち、第２要素認証サービスおよび知識ベース認証サービス）を実行する様々な認証サービスの位置および／またはＩＤが含まれる（ａｕｔｈ位置）。初期アサーションには、要求されたアクション／リソース（例えば、本実施形態ではパスワードリセットサービス）とタイムスタンプが含まれる。ＳＳＰＲサービスは、５０６でチャレンジを受信機に送信する。

【００８１】
次に、受信機は、認証チャレンジに含まれる認証パラメータを検出する。例えば、図５に示すように、認証要求は、識別された認証プロトコルに含まれる認証スキームを実行する際に用いられる認証サービス（第２要素認証サービスおよび知識ベース認証サービス）を識別する認証パラメータを有する。受信機は、５０８で、初期トークンＴ（ｓｓｐｒ）および適切な認証パラメータとともに第１の認証要求を第２要素認証サービスに送信する。上述のように、第２要素認証サービスは、受信機から認証要求を受信すると、ユーザに関連付けられたデバイス（例えば、受信機、モバイルデバイス、または他のデバイス）に対してパスコード（または他の認証資格情報）要求を５１０で発行することによって、必要な認証スキーム（すなわち、第２要素認証）を実行し、応答として５１２でパスコードを受信する。５１４で、第２要素認証サービスは、受信したパスコードを格納された正しいパスコードと比較することによってユーザを検証し、受信したパスコードが格納されたパスコードと一致する場合、パスコード認証が成功したことを示すアサーションを初期トークンＴ（ｓｓｐｒ）に追加する。次に、第２要素認証サービスは、そのアサーションを有する更新されたトークンＴ（ｓｓｐｒ、２ｆａ）を受信機に５１６で送信する。
【００８２】
第２要素認証サービスからトークンＴ（ｓｓｐｒ、２ｆａ）を受信すると、受信機は、認証パラメータをレビューして、受信した認証チャレンジの認証スキームが認証パラメータに従って実行されていないと判断する（上述のように、識別された認証プロトコルは２つの認証スキームを有する。）。次いで、受信機は、受信したトークンＴ（ｓｓｐｒ、２ｆａ）を含む第２の認証要求を知識ベース認証サービスに５１８で送信する。次に、知識ベース認証サービスは、ユーザに回答させるための一連の質問を５２０で発行することによって、必要な認証スキーム（すなわち、知識ベース認証）を実行し、ユーザ応答と格納された正解とを比較することによって、ユーザを認証する。一実施形態では、質問を発行して、ユーザ応答を受信するために、知識ベース認証サービスによって受信機または別のユーザデバイスもしくはポータルが使用される。５２２で、知識ベース認証サービスは、ユーザから回答を受信し、受信した回答または応答が格納された応答と一致する場合、ユーザを５２４で認証し、ＫＢＡ認証が成功したことを示すアサーションをＴ（ｓｓｐｒ、２ｆａ）トークンに追加することでＴ（ｓｓｐｒ、２ｆａ、ｋｂａ）トークンを生成する。次いで、知識ベース認証サービスは、そのアサーションを有する更新されたトークンＴ（ｓｓｐｒ、２ｆａ、ｋｂａ）を受信機に５２６で送信する。
【００８３】
知識ベース認証サービスからトークンＴ（ｓｓｐｒ、２ｆａ、ｋｂａ）を受信すると、受信機は、認証パラメータをレビューして、受信した認証チャレンジの認証スキームが認証パラメータに従って実行されたと判断し、トークンＴ（ｓｓｐｒ、２ｆａ、ｋｂａ）をＳＳＰＲサービスに５２８で送信する。ＳＳＰＲサービスは、トークンＴ（ｓｓｐｒ、２ｆａ、ｋｂａ）を受信すると、アクセス認証情報の変更を許可し、トークンの１回限りの使用を保証するために、受信したトークンを５３０で破棄する。一実施形態では、ＳＳＰＲサービスは、保存されたチャレンジの初期アサーションおよび／またはトークンのタイムスタンプを調べて、経過時間に基づいて許可を付与するか否かを決定することで、セキュリティを強化させる。ＳＳＰＲサービスはまた、アクセス認証情報の変更を許可すると、格納された初期アサーションを削除して、トークンの１回限りの使用を保証することによって、セキュリティを強化させる。
【００８４】
代替方法として、および／または、追加の方法として、５１８で、受信機は、Ｔ（ｓｓｐｒ）のみを知識ベース認証サービスに送信してもよい。次いで、知識ベース認証サービスは、ユーザに回答させるための一連の質問を５２０で発行することによって、必要な認証スキーム（すなわち、知識ベース認証）を実行し、ユーザ応答と格納された正解とを比較することによって、ユーザを認証する。一実施形態では、質問を発行し、ユーザ応答を受信するために、知識ベース認証サービスによって受信機または別のユーザデバイスもしく

はポータルが使用される。５２２で、知識ベース認証サービスは、ユーザから回答を受信し、受信した回答または応答が格納された応答と一致する場合、ユーザを５２４で認証し、ＫＢＡ認証が成功したことを示すアサーションをＴ（ｓｓｐｒ）トークンに追加することでＴ（ｓｓｐｒ、ｋｂａ）トークンを生成する。次いで、知識ベース認証サービスは、そのアサーションを有する更新されたトークンＴ（ｓｓｐｒ、ｋｂａ）を受信機に５２６で送信する。受信機は、Ｔ（ｓｓｐｒ、２ｆａ）とＴ（ｓｓｐｒ、ｋｂａ）とを組み合わせてＴ（ｓｓｐｒ、２ｆａ、ｋｂａ）を作成し、Ｔ（ｓｓｐｒ、２ｆａ、ｋｂａ）をＳＳＰＲサービスに５２８で送信する。

【００８５】

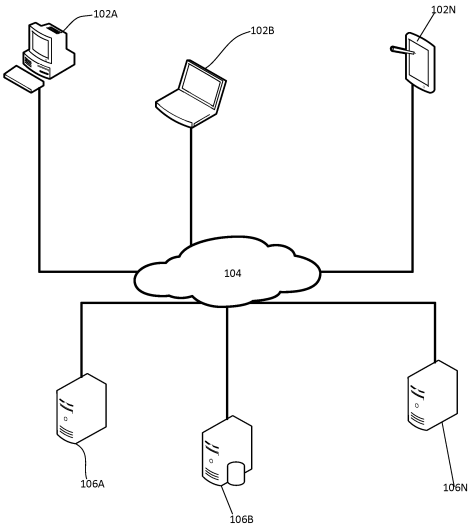
代替方法として、および／または、追加の方法として、受信機は、５２８で、Ｔ（ｓｓｐｒ、２ｆａ）およびＴ（ｓｓｐｒ、ｋｂａ）を、それらを結合することなく、ＳＳＰＲサービスに送信してもよい。

【００８６】

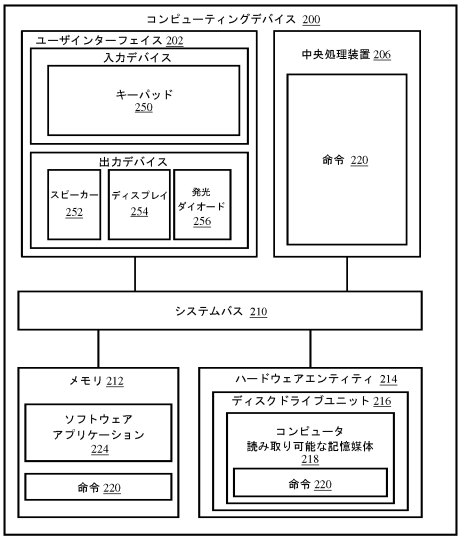
本発明を１つ以上の実施に関して図示および説明したが、本明細書および添付図面を読んで理解すると、同等の変更および変形例が当業者に想到されるであろう。さらに、本発明の特定の特徴は、いくつかの実施のうちの１つのみに関して開示されている可能性があるが、そのような特徴は、任意のまたは特定の用途にとって望ましく有利であるように他の実施の１つ以上の他の特徴と組み合わせることができる。したがって、本発明の広さおよび範囲は、上記の実施形態のいずれによっても限定されるべきではない。むしろ、本発明の範囲は、添付の特許請求の範囲およびそれらの均等物に従って定義されるべきである。

【図面】

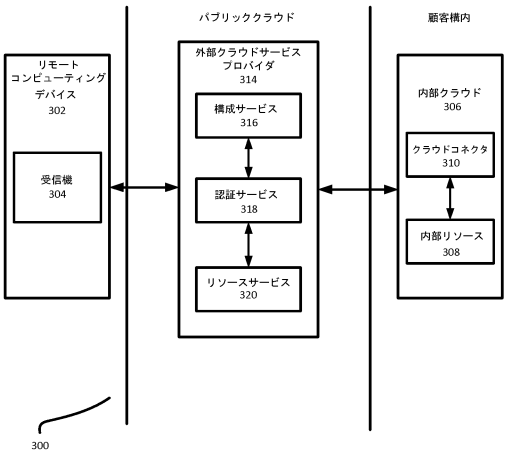
【図１】


102A
102B
102N
104
106A
106B
106N

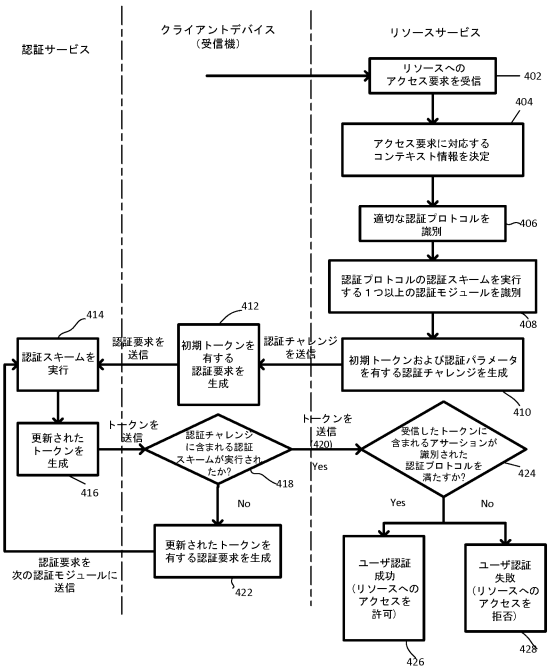
【図２】


コンピューティングデバイス 200
ユーザインターフェイス 202
入力デバイス
キーパッド 250
出力デバイス
スピーカー 252
ディスプレイ 254
発光ダイオード 256
中央処理装置 206
命令 220
システムバス 210
メモリ 212
ソフトウェアアプリケーション 224
命令 220
ハードウェアエンティティ 214
ディスクドライブユニット 216
コンピュータ読み取り可能な記憶媒体 218
命令 220

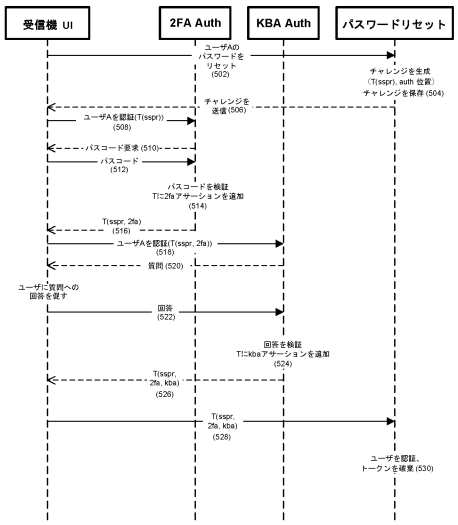
【図３】


パブリッククラウド
顧客構内
リモートコンピューティングデバイス 302
受信機 304
外部クラウドサービスプロバイダ 314
構成サービス 316
認証サービス 318
リソースサービス 320
内部クラウド 306
クラウドコネクタ 310
内部リソース 308
300

【図４】


認証サービス
クライアントデバイス（受信機）
リソースサービス
リソースへのアクセス要求を受信 402
アクセス要求に対応するコンテキスト情報を決定 404
適切な認証プロトコルを識別 406
認証プロトコルの認証スキームを実行する１つ以上の認証モジュールを識別 408
初期トークンおよび認証パラメータを有する認証チャレンジを生成 410
認証チャレンジを送信
初期トークンを有する認証要求を生成 412
認証要求を送信
認証スキームを実行 414
トークンを送信
更新されたトークンを生成 416
認証チャレンジに含まれる認証スキームが実行されたか? 418
No
更新されたトークンを有する認証要求を生成 422
認証要求を次の認証モジュールに送信
Yes
トークンを送信 420
受信したトークンに含まれるアサーションが識別された認証プロトコルを満たすか? 424
Yes
No
ユーザ認証成功（リソースへのアクセスを許可） 426
ユーザ認証失敗（リソースへのアクセスを拒否） 428

【図５】


受信機 UI
2FA Auth
KBA Auth
パスワードリセット
ユーザAの
パスワードを
リセット
(502)
チャレンジを生成
(T(sspr), auth 位置)
チャレンジを保存 (504)
チャレンジを
送信 (506)
ユーザAを認証(T(sspr))
(508)
パスコード要求 (510)
パスコード
(512)
パスコードを検証
Tに2faアサーションを追加
(514)
T(sspr, 2fa)
(516)
ユーザAを認証(T(sspr, 2fa))
(518)
質問 (520)
ユーザに質問への
回答を促す
回答
(522)
回答を検証
Tにkbaアサーションを追加
(524)
T(sspr,
2fa, kba)
(526)
T(sspr,
2fa, kba)
(528)
ユーザを認証、
トークンを発行 (530)

フロントページの続き

ケンブリッジ サイエンス パーク １０１

審査官　平井 誠

(56)参考文献　特表２０１０－５２５４４８（ＪＰ，Ａ）
特開２００３－１９６５６６（ＪＰ，Ａ）
米国特許出願公開第２０１６／００９４５３１（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－８８