(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7523469号
(P7523469)

(45)発行日　令和6年7月26日(2024.7.26)

(24)登録日　令和6年7月18日(2024.7.18)

(51)国際特許分類

Ｇ０６Ｆ　21/33　(2013.01)		Ｇ０６Ｆ	21/33	
Ｇ０６Ｆ　21/62　(2013.01)		Ｇ０６Ｆ	21/62	３１８

ＦＩ

請求項の数　17　（全25頁）

(21)出願番号　特願2021-565850(P2021-565850)
(86)(22)出願日　令和2年4月6日(2020.4.6)
(65)公表番号　特表2022-531872(P2022-531872A)
(43)公表日　令和4年7月12日(2022.7.12)
(86)国際出願番号　PCT/IB2020/053254
(87)国際公開番号　WO2020/225616
(87)国際公開日　令和2年11月12日(2020.11.12)
審査請求日　令和4年9月22日(2022.9.22)
(31)優先権主張番号　19172926.8
(32)優先日　令和1年5月7日(2019.5.7)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
Ｎｅｗ　Ｏｒｃｈａｒｄ　Ｒｏａｄ，　Ａｒｍｏｎｋ，　Ｎｅｗ　Ｙｏｒｋ　１０５０４，　Ｕｎｉｔｅｄ　Ｓｔａｔｅｓ　ｏｆ　Ａｍｅｒｉｃａ
(74)代理人　100112690
弁理士　太佐 種一

最終頁に続く

(54)【発明の名称】　きめの細かいトークン・ベースのアクセス制御

(57)【特許請求の範囲】

【請求項１】

データ処理環境内のトークン・ベースの許可のためのコンピュータ実装方法であって、前記データ処理環境が少なくともユーザ・システム、アプリケーション、認証サーバ、およびアクセス制御サーバを備え、前記ユーザ・システムがネットワーク接続を介して、前記アプリケーションを実行中のサーバに接続され、前記アプリケーションがオペレーションへのアクセスを与え、少なくとも前記オペレーションがその識別子によって識別可能であり、前記方法が、

ユーザ・システム要求を介して前記アプリケーションにアクセスすることと、

前記認証サーバにアクセス要求をリダイレクトすることと、

前記認証サーバに前記アプリケーションから送信された認証証明によってユーザを認証することであって、前記認証証明が、スコープの標準セマンティックを使用する制限付きエンタイトルメントを求める要求を含み、前記制限付きエンタイトルメントが、リソースについて前記アクセス制御サーバによって管理される定義済みの既存のエンタイトルメントのサブセットを表す、前記認証することと、

前記認証が成功し、前記アプリケーションが前記認証サーバに登録された場合、前記認証サーバから前記アプリケーションにアクセス・トークンをリフレッシュ・トークンと共に送ることであって、前記アクセス・トークンおよび前記リフレッシュ・トークンが前記制限付きエンタイトルメントを含む、前記送ることと、

前記ユーザ・システムによって開始された前記アプリケーションによるオペレーション

の実行を要求することであって、
　前記制限付きエンタイトルメントを含む前記アクセス・トークンを提供する前記アプリケーションによる前記オペレーションを起動すること、
　前記オペレーションによって前記アクセス制御サーバを起動すること、
　前記ユーザ・システムの識別子と、前記既存のエンタイトルメントの前記サブセットを含む前記トークンの前記スコープとを前記アクセス制御サーバに提供すること、
　前記アクセス制御サーバによって前記既存のエンタイトルメントの前記サブセットを使用して、前記オペレーションに対する前記ユーザ・システムのアクセスを決定することを含む、前記要求することと
を含む、方法。

【請求項２】
　前記標準セマンティックがＯＡｕｔｈ２に基づく、請求項１に記載の方法。

【請求項３】
　前記アプリケーションがセキュアでないコンポーネントである、請求項１または２に記載の方法。

【請求項４】
　前記認証証明内に含まれる制限付きエンタイトルメントを求める前記要求が第１の要求であり、前記第１の要求が既存のエンタイトルメントの最大サブセットを求める要求を含む、請求項１ないし３のいずれか一項に記載の方法。

【請求項５】
　リフレッシュ・トークンを求める後続の要求も、別の制限付きエンタイトルメントを求める要求を含む、請求項４に記載の方法。

【請求項６】
　前記オペレーションが、事前定義されたデータへのアクセス、データベース・アクセス、ファイル・アクセス、事前定義されたアプリケーション・プログラミング・インターフェース、およびネットワークの特定のサブネットへのアクセスを含むグループから選択された少なくとも１つを含む、請求項１ないし５のいずれか一項に記載の方法。

【請求項７】
　前記アクセス・トークンが事前定義された有効時間を有する、請求項１ないし６のいずれか一項に記載の方法。

【請求項８】
　前記事前定義された有効時間が特権のあるユーザ・システムによって更新可能である、請求項７に記載の方法。

【請求項９】
　データ処理環境内のトークン・ベースの許可のためのアクセス・システムであって、前記データ処理環境が少なくともユーザ・システム、アプリケーション、認証サーバ、およびアクセス制御サーバを備え、前記ユーザ・システムがネットワーク接続を介して、前記アプリケーションを実行中のサーバに接続され、前記アプリケーションがオペレーションへのアクセスを与え、少なくとも前記オペレーションがその識別子によって識別可能であり、前記アクセス・システムが、
　ユーザ・システム要求を介して前記アプリケーションにアクセスするように適合されたアクセシング・モジュールと、
　前記認証サーバにアクセス要求をリダイレクトするように適合されたリダイレクティング・モジュールと、
　前記認証サーバに前記アプリケーションから送信された認証証明によってユーザを認証するように適合された認証サーバであって、前記認証証明が、スコープの標準セマンティックを使用する制限付きエンタイトルメントを求める要求を含み、前記制限付きエンタイトルメントが、リソースについて前記アクセス制御サーバによって管理される定義済みの既存のエンタイトルメントのサブセットを表す、前記認証サーバと、
　前記認証が成功し、前記アプリケーションが前記認証サーバに登録された場合、前記認

証サーバから前記アプリケーションにアクセス・トークンをリフレッシュ・トークンと共に送るように適合された送信側であって、前記アクセス・トークンおよび前記リフレッシュ・トークンが前記制限付きエンタイトルメントを含む、前記送信側と
を備え、
前記ユーザ・システムが、前記ユーザ・システムによって開始された前記アプリケーションによるオペレーションの実行を要求するように適合され、前記オペレーションの実行を要求することが、
前記制限付きエンタイトルメントを含む前記アクセス・トークンを提供する前記アプリケーションによる前記オペレーションを起動すること、
前記オペレーションによって前記アクセス制御サーバを起動すること、
前記ユーザ・システムの識別子と、前記既存のエンタイトルメントの前記サブセットを含む前記トークンの前記スコープとを前記アクセス制御サーバに提供すること、
前記アクセス制御サーバによって前記既存のエンタイトルメントの前記サブセットを使用して、前記オペレーションに対する前記ユーザ・システムのアクセスを決定することを含む、アクセス・システム。
【請求項１０】
前記標準セマンティックがＯＡｕｔｈ２に基づく、請求項９に記載のアクセス・システム。
【請求項１１】
前記アプリケーションがセキュアでないコンポーネントである、請求項９または１０に記載のアクセス・システム。
【請求項１２】
前記認証証明内に含まれる制限付きエンタイトルメントを求める前記要求が第１の要求であり、前記第１の要求が既存のエンタイトルメントの最大サブセットを求める要求を含む、請求項９ないし１１のいずれか一項に記載のアクセス・システム。
【請求項１３】
リフレッシュ・トークンを求める後続の要求も、別の制限付きエンタイトルメントを求める要求を含む、請求項１２に記載のアクセス・システム。
【請求項１４】
前記オペレーションが、事前定義されたデータへのアクセス、データベース・アクセス、ファイル・アクセス、事前定義されたアプリケーション・プログラミング・インターフェース、およびネットワークの特定のサブネットへのアクセスを含むグループから選択された少なくとも１つを含む、請求項９ないし１３のいずれか一項に記載のアクセス・システム。
【請求項１５】
前記アクセス・トークンが事前定義された有効時間を有する、請求項９ないし１４のいずれか一項に記載のアクセス・システム。
【請求項１６】
前記事前定義された有効時間が特権のあるユーザ・システムによって更新可能である、請求項１５に記載のアクセス・システム。
【請求項１７】
データ処理環境内のトークン・ベースの許可のためのコンピュータ・プログラムであって、１つまたは複数のコンピューティング・システムに、請求項１ないし８のいずれか一項に記載の方法を実行させる、コンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般にはトークン・ベースの許可のための方法に関し、より詳細には、データ処理環境内のトークン・ベースの許可のためのコンピュータ実装方法に関する。本発明はさらに、データ処理環境内のトークン・ベースの認証のための関連するアクセス・シス

テム、および関連するコンピュータ・プログラム製品を対象とする。
【背景技術】
【０００２】
最近の１０年間にわたって、トークン・ベースの認証および許可システムが進化してきた。これらのシステムでは、エンド・ユーザは、許可サーバに対して認証し、そのエンド・ユーザの権限を証明し、任意選択でそのエンド・ユーザの識別も証明する一時トークンを返す。このトークンは、たとえば、バックエンド・サービスを安全に起動するためにウェブ・ベースのユーザ・インターフェース（ＵＩ）によって使用される。証明はそうしたサービスに流れないので、トークン・ベースのシステムにより、同一の許可システムを活用し得る様々なベンダのサービスのためのエコシステムが可能となる。サービス間のより複雑な対話のために、サービスを通じてＵＩから別のダウンストリーム・サービスにトークンを渡すことも可能である。
【０００３】
トークン・データの部分として、ペイロードは通常、「スコープ」と呼ばれる許可のセットを搬送する。スコープは、様々なトークン・ベースのシステムで非常に様々に処理される。標準化の観点から、スコープについてのいくつかのキーワードだけが予約され、他の許可は許可フレームワーク次第である。こうしたフレームワークの多くは、しばしばサービス、コンポーネント、またはアクション、あるいはその組合せを記述するアクション・ベースのモデルまたは役割ベースのモデルあるいはその両方を適合させた。たとえば、「database.query.read」のような関数呼出しが、そのような潜在的スコープとなる。
【発明の概要】
【０００４】
本発明の一態様によれば、トークン・ベースの許可のためのコンピュータ実装方法が、少なくともユーザ・システム、アプリケーション、認証サーバ、およびアクセス制御サーバを含み得る。それによって、ユーザ・システムは、ネットワーク接続を介して、アプリケーションを実行中のサーバに接続され得、アプリケーションはオペレーションへのアクセスを与え得る。少なくともオペレーションはその識別子によって識別可能であり得る。
【０００５】
本方法は、ユーザ・システム要求を介してアプリケーションにアクセスすることと、認証サーバにユーザ・アクセス要求をリダイレクトすることと、認証サーバとアプリケーションとの間で交換された認証証明によってユーザを認証することとを含み得る。それによって、認証証明は、スコープの標準セマンティックを使用する制限付きエンタイトルメント（制限付き資格）を求める要求を含み得、制限付きエンタイトルメントは、リソースについてのアクセス制御サーバによって管理または制御される既存のエンタイトルメント（既存の資格）のサブセットを表し得る。
【０００６】
本方法は、認証が成功し、アプリケーションが認証サーバに登録された場合、認証サーバからアプリケーションにアクセス・トークンをリフレッシュ・トークンと共に送ることをさらに含み得、アクセス・トークンおよびリフレッシュ・トークンは制限付きエンタイトルメントを含む。
【０００７】
ユーザ・システムによって開始されたアプリケーションによるオペレーションの実行を要求することは、制限付きエンタイトルメントを含むアクセス・トークンを提供するアプリケーションによるオペレーションを起動すること、オペレーションによってアクセス制御サーバを起動すること、ユーザ・システムの識別子と、既存のエンタイトルメントのサブセットを含むトークンのスコープとをアクセス制御サーバに提供すること、アクセス制御サーバによって既存のエンタイトルメントをフィルタリングするためにエンタイトルメントのサブセットを使用して、結果としてオペレーションに対するユーザ・システムのアクセスを決定することを含み得る。
【０００８】

本発明の別の態様によれば、データ処理環境内のトークン・ベースの許可のための関連するアクセス・システムが提供され得る。

【０００９】

さらに、実施形態は、コンピュータもしくは任意の命令実行システムによって使用され、またはそれに関連して使用され、またはそれと共に使用されるプログラム・コードを提供するコンピュータ使用可能またはコンピュータ可読媒体からアクセス可能な、関連するコンピュータ・プログラム製品の形態を取り得る。この説明では、コンピュータ使用可能またはコンピュータ可読媒体は、命令実行システム、装置、またはデバイスによって使用され、またはそれに関連して使用され、またはそれと共に使用されるプログラムを記憶、通信、伝播、または移送するための手段を含み得る任意の装置であり得る。

【００１０】

本発明の実施形態が様々な主題を参照しながら説明されることに留意されたい。具体的には、いくつかの実施形態は、方法型クレームを参照しながら説明されるのに対して、他の実施形態は装置型クレームを参照しながら説明される。しかしながら、上記および以下の説明から、別段の通知がない限り、あるタイプの主題に属する特徴の任意の組合せに加えて、様々な主題に関する特徴の間の、具体的には方法型クレームの特徴と装置型クレームの特徴の間の任意の組合せも本文書内で開示されると見なされることを当業者は知ることになる。

【００１１】

上記で定義される態様、および本発明の別の態様は、以下で説明される実施形態の例から明らかであり、実施形態の例を参照しながら説明されるが、本発明は実施形態の例に限定されない。

【００１２】

単に例として、以下の図面を参照しながら、本発明の好ましい実施形態が説明される。

【図面の簡単な説明】

【００１３】

【図１】データ処理環境内のトークン・ベースの許可のための本発明のコンピュータ実装方法の一実施形態のブロック図である。

【図２】ここで提案される概念の基礎となる対話モデルのブロック図である。

【図３】代替の開始対話の一実施形態のブロック図である。

【図４】図３に関する説明的な通信ダイアグラムである。

【図５】クライアントが限定エンタイトルメントを有するリソース所有者についてのアクセス・トークンまたはリフレッシュ・トークンあるいはその両方を取り出す、代替の対話のブロック図である。

【図６】クライアント２０４がそれによってセキュアでないコンポーネント２０８に対するオペレーションを起動する、第２のタイプの対話６００のブロック図である。

【図７】図６に関する説明的な通信ダイアグラムである。

【図８】信頼できないコンポーネントがリソース・サーバ１およびリソース・サーバ２と対話する、第３のタイプの対話のブロック図である。

【図９】図８に関する説明的な通信ダイアグラムである。

【図１０】リソース・サーバ１およびリソース・サーバ２がアクセス制御サーバと対話する、第４のタイプの対話のブロック図である。

【図１１】図１０に関する説明的な通信ダイアグラムである。

【図１２】従来のアクセス制御サーバ決定エンジンの例示的擬似コード・セグメントを示す図である。

【図１３】ここで提案されるアクセス制御サーバ決定エンジンの例示的擬似コード・セグメントを示す図である。

【図１４】データ処理環境内のトークン・ベースの許可のためのアクセス・システムのブロック図である。

【図１５】ここで説明されるコンポーネントのためのプログラム・コードを実行するのに

適したコンピューティング・システムの一実施形態を示す図である。
【発明を実施するための形態】
【００１４】
この説明の文脈では、以下の規約、用語、または表現、あるいはその組合せが使用され得る。
【００１５】
「トークン・ベースの許可」という用語は、ユーザがそれに対してユーザの認証を証明した認証サーバから、トークンとして示される一時データ構造をユーザがそれによって受信し得る機構を示し得る。そのようなトークンは、たとえば他のサーバ・システム上の、事前定義されたシステム、アプリケーション、またはサービス、あるいはその組合せにアクセスすることをユーザに許可し得る。
【００１６】
「ユーザ・システム」という用語は、ここでは通常、エンド・ユーザによって操作されるパーソナル・コンピュータ、モバイル・デバイス、または任意の他のコンピュータ化されたシステムのような、ユーザが操作するデバイスを示し得る。
【００１７】
「アプリケーション」という用語は、ユーザ・システムからアクティベートされた後に１つまたは複数のサービスおよび機能を配信する実行可能なソフトウェア・コードを示し得る。通常、アプリケーションは、サーバ・システム、たとえばデータ・センタ内で、またはクラウド・コンピューティング・パラダイム下で、あるいはその両方で動作するサーバ・システム上で管理および実行され得る。したがって、サーバ・システムは通常、ユーザ・システムからリモートで動作し得る。
【００１８】
「認証サーバ」という用語は、（たとえば、ウェブ・ブラウザを使用することによって）ユーザ・システムを操作するエンド・ユーザが、事前定義されたアプリケーションおよびサービスにアクセスすることを許可されるようにエンド・ユーザ自身をそれに対して認証し得る、（通常はユーザ・システムおよびサーバ・システムに対する第３者によって操作される）信頼できるコンピューティング環境を示し得る。
【００１９】
「アクセス制御サーバ」という用語は、アプリケーションまたはアプリケーションを使用するユーザ・システムに対して特定のサービスへのアクセスを許可または拒否するように動作可能なハードウェアまたはソフトウェア・システムを示し得る。
【００２０】
「オペレーション」という用語は、アプリケーションの単一の機能、あるいは１つまたは複数のアプリケーションの複数の機能またはサービスあるいはその両方を示し得る。オペレーションのタイプは、アクセスのスコープによって定義され、または制限され、あるいは定義および制限され得る。オペレーションの例は、データベース読取り、データの指定のサブセットを読み取ること、こうしたデータを操作すること、データを組み合わせること、コンテンツ管理システムで検索を実行すること、および指定のネットワーク・アドレスにアクセスすること、ならびにさらに多くのソフトウェアまたはハードウェアあるいはその両方でサポートされるサービスまたは機能あるいはその両方であり得る。
【００２１】
「認証証明」という用語は、事前定義された機能およびサービスにアクセスすることをエンド・ユーザに許可するためにエンド・ユーザ（または関連するシステム）によって使用されるデータのセットを示し得る。
【００２２】
「制限付きエンタイトルメント」という用語は、ユーザ・システムまたは関連するエンド・ユーザあるいはその両方が、エンティティを提供するアプリケーションまたはサービスのすべての利用可能な機能と比較した場合に限定される機能にアクセスでき得るだけであり、または機能を使用し得るだけであり、あるいはその両方であることを指すことがあ

る。したがって、エンド・ユーザは、機能またはサービスの全セットを使用する資格がなく、制限付きのサブセットだけを使用する資格があることがあり、たとえばデータを読み取るが、データを変更せず、アプリケーションもこれを実行するよう構成され得る。

【００２３】

「スコープ」という用語は、ユーザ・システムまたは関連するエンド・ユーザ、あるいは一般にはシステム・ユーザがアクセスでき得るサービスまたは機能あるいはその両方の定義済みのセットを示し得る。スコープは、リソースから利用可能なサービスおよび機能の完全なセットであり得、またはサブセットのみに限定され得る。

【００２４】

「標準セマンティック」という用語は、ここでは、たとえばバージョン２のＯＡｕｔｈのような標準化許可システムの、コマンドおよび機能の定義済みのセットを示し得る。しかしながら、他のバージョンもサポートされ得る。

【００２５】

「ＯＡｕｔｈ２」という用語は、インターネット・ユーザがウェブサイトまたはアプリケーションあるいはその両方に、パスワードを与えることなく他のウェブサイト上のインターネット・ユーザの情報にアクセスすることを許可するための方式として一般に使用される、アクセス委任(access delegation)についての既知のオープン・スタンダードを示し得る。この機構は、ユーザのアカウントについての情報を第３者アプリケーションまたはウェブサイトと共有することをユーザに許可するために公共のインターネット・サイトによって広く使用されている。一般に、標準のバージョン２を示すＯＡｕｔｈ２は、リソース所有者に代わって、リソースへの「セキュア委任アクセス」をクライアントに提供し得る。ＯＡｕｔｈ２は、リソース所有者が、リソース所有者の証明（すなわち、認証証明）を共有することなく、リソース所有者のリソース、すなわちサービスおよび機能への第３者アクセスを許可するためのプロセスを指定し得る。通常、許可サーバによってユーザ・システムに発行されたアクセス・トークンは、リソース所有者の承認を確認するために使用される。第３者、すなわち第３者の関連するユーザ・システムを伴うエンド・ユーザは、アクセス・トークンを使用して、サーバによってホストされる、保護されたリソースにアクセスし得る。

【００２６】

さらに、ＯＡｕｔｈ２の好ましいトークン・ベースの実装環境のいくつかの用語（具体的には役割）もここで定義され得る。

【００２７】

基本的には、使用される役割は、ＯＡｕｔｈ２仕様ＲＦＣ　６７４９で説明されており、https://tools.ietf.org/html/rfc6749と比較されたい。

【００２８】

リソース所有者（たとえば、エンド・ユーザ、システム・ユーザ）は、保護されたリソースへのアクセスを許可することのできるエンティティであり得る。リソース所有者が人であるとき、リソース所有者はエンド・ユーザと呼ばれる。

【００２９】

リソース・サーバ（すなわち、サービス）は、アクセス・トークンを使用する、保護されたリソース要求を受け入れ、応答することのできる、保護されたリソースをホストするサーバであり得る。ここで提案される概念では、リソース・サーバは、渡されたトークンに基づくオペレーションが許可されるか、それとも拒否されるかを判定するのを助け得るアクセス制御サーバに接続され得る。

【００３０】

クライアントは、リソース所有者の代わりに、リソース所有者の許可と共に、保護されたリソース要求を行うアプリケーションであり得る。「クライアント」という用語は、何らかの実装特徴を示唆するわけではなく、すなわち、これはウェブ・ベースのアプリケーション、デスクトップ・アプリケーション、または異なるデバイス上で動作中のアプリケーションであり得る。

【００３１】
許可サーバは、首尾よくリソース所有者（エンド・ユーザ）を認証し、許可を得た後に、クライアントにアクセス・トークンを発行するサーバであり得る。許可サーバは、リソース・サーバと同一のサーバ、または別々のエンティティであり得る。単一の許可サーバが、複数のリソース・サーバによって受け入れられるアクセス・トークンを発行し得る。
【００３２】
信頼できないコンポーネントは、（ここで説明される概念では、ＯＡｕｔｈ２で定義される役割に加えて）リソース所有者の代わりにスクリプトを実行し得る。このために、信頼できないコンポーネントは、リソース所有者のアクセス・トークンを受け取り、１つまたは複数のリソース・サーバを呼び出すためにそれを使用する。
【００３３】
アクセス制御サーバは（ＯＡｕｔｈ２で定義される役割に加えて）、渡されたトークンからのプロパティを以前に作成されたポリシーと比較することによって、アクセス要求を評価する際にリソース・サーバをサポートすることを意味し得る。
【００３４】
さらに、ＯＡｕｔｈ２による単一の許可サーバの機能が、よりきめの細かい許可およびアクセス制御のために、ここで提案される概念の文脈では、認証サーバおよびアクセス制御サーバに分割されていることに留意することができる。
【００３５】
データ処理環境内のトークン・ベースの認証のための提案されるコンピュータ実装方法は、複数の利点および技術的効果を提供し得る。
【００３６】
提案される概念は、リソース管理ポリシーに対するきめの細かいアクセス制御を可能にするトークン・ベースの許可モデルを使用する識別とアクセス管理（Identity and Access Management, IAM)システムにシームレスに統合され得る。そのようなモデルによれば、トークンは、実施されるオペレーションのアクタ（すなわち、エンド・ユーザ）を識別し得るだけであるが、起動されたサービスに任意のアクセス制御を委任し得る。トークン自体は、許可プロパティの最小セットを含み得るだけであり、たとえばサービスまたは機能あるいはその両方を起動するためにトークンが使用され得るか否かを示し得るだけである。
【００３７】
さらに、いくつかのシナリオでは、トークンは、オペレーションを実行するために潜在的に信頼できないコンポーネントにハンドオーバされ得る。コンポーネントの異常動作の潜在的な影響を限定するために、提案される概念は、トークンの許可を限定するための洗練された方式を開示し、その結果、そのようなトークンを受け取るサービスは、特定のサービス・タイプ、サービス・インスタンス、リソース・タイプ、またはリソース・インスタンス、あるいはその組合せのリスト上のオペレーションを許可するだけとなる。そのようなリストはこれらの異なるタイプを混合し得る。ターゲット・サービスおよびその許可コンポーネントは、こうした限定を効果的に尊重するように「内部で」修正される。許可の関連する制限は、そのトークンのみによってスコーピングされ得、他のトークンは、そのユーザの許可の全セットに基づいて実行オペレーションを引き続き許可する。
【００３８】
ここで使用されるトークンは、時間依存常時区切りされる(time-dependent all-time-delimited)有効性を有し得ることにも留意されたい。したがって、アクセス・トークンまたは認証トークンあるいはその両方と同じオペレーション原理の下にあり得るリフレッシュ・トークンも使用され得る。
【００３９】
したがって、提案される概念の一般的概念は、トークン・スコープの特定のセマンティックを定義し、トークン・セマンティック・スコープを適用することによって既存のエンタイトルメントを変更することなくアクセス制御を修正することにより、リソース所有者

の既存のエンタイトルメントのサブセットへのトークンのアクセスを、サービス・インスタンスまたはリソース・インスタンスあるいはその両方に制限することである。したがって、定義済みの既存のエンタイトルメントは、そのまま存在し続け得、より区切られた機能またはサービスあるいはその両方の追加のサブセットを定義する必要があり得るだけである。

【００４０】

したがって、サービス名によって識別される、サービスへのアクセスのみを限定し得るＯＡｕｔｈ２に関する現在利用可能なアクセス制御が、以下のような、現時点では利用可能でなくＯＡｕｔｈ２の標準外にある複数の追加のアクセス限定に向上し得る。

・サービス内のリソース・タイプへの限定されたアクセス

＜サービス名＞．＜リソース・タイプ＞、たとえばkubernetes.pods、

・サービス・インスタンス内のリソース・タイプへの限定されたアクセス

＜サービス名＞：＜サービス・インスタンス＞．＜リソース・タイプ＞、たとえばkubernetes:6271293102982712.pods

・サービス内のリソースへの限定されたアクセス

＜サービス名＞．＜リソース・タイプ＞：＜リソース＞、たとえばkubernetes.pods:mypod、

・サービス・インスタンス内のリソースへの限定されたアクセス

＜サービス名＞：＜サービス・インスタンス＞．＜リソース・タイプ＞：＜リソース＞、たとえばkubernetes:6271293102982712.pods:mypod、

従来のＯＡｕｔｈ２手法では以下のアクセス制限だけが利用可能である。

・＜サービス名＞のみのサービス、たとえばｋｕｂｅｒｎｅｔｅｓへの限定されたアクセス、

・＜サービス名＞．＜アクション＞のみのサービスのアクション、たとえばdatabase.readへの限定されたアクセス。

【００４１】

さらに、トークンが限定エンタイトルメントのみと共に作成され得、したがって、潜在的に盗まれたトークンはより短いブラスト半径を有する。たとえば、トークンを処理するモバイル・アプリケーションは、同じモバイル・デバイス上の悪意のあるａｐｐによってデバッグまたはハッキングされ得る。エンタイトルメントの限定されたセットを有することは、その盗まれたトークンの潜在的なブラスト半径を削減する助けとなり得る。

【００４２】

推奨されないとしても、いくつかのウェブ・アプリケーションは、クライアント側に、すなわちブラウザのＪａｖａスクリプト・クライアント内にトークンを保つ。ここでも、限定エンタイトルメントを有するトークンは、クロスサイト・スクリプティング攻撃のケースにおいて、より小さい潜在的な破壊的半径を有する。

【００４３】

方法の好ましい実施形態によれば、標準セマンティックはＯＡｕｔｈ２に基づく。したがって、ここで提案される概念について使用される基礎が、サービスおよび機能へのアクセスのよりきめの細かい制御を可能にするアクセス制御機構を実装するために、既により粗いアクセス制御機構を改良または改善することによって、プロトコルおよび機能の既に明確なセット内に統合され得る。したがって、（現在はバージョン２で利用可能な）広く使用されているＯＡｕｔｈセキュリティ機能が向上し、改善される。ここで提案される向上は、ＯＡｕｔｈの後のバージョンでも使用され得ることが予想され得る。

【００４４】

方法の１つの有利な実施形態によれば、アプリケーションは、セキュアでないコンポーネント、たとえばＪｕｐｙｔｅｒ　Ｎｏｔｅｂｏｏｋまたは類似したものであり得る。Ｊｕｐｙｔｅｒ　ＮｏｔｅｂｏｏｋまたはＪｕｐｙｔｅｒ文書は、コンピュータ・コードと、パラグラフ、式、図、リンクなどを伴うリッチ・テキスト要素の両方を含み得る、周知のＪｕｐｙｔｅｒ　Ｎｏｔｅｂｏｏｋ　Ａｐｐによって作られた文書を示し得る。それによ

って、Ｊｕｐｙｔｅｒ　Ｎｏｔｅｂｏｏｋ　Ａｐｐは、たとえばウェブ・ブラウザを介してサーバ・システム上でノートブック文書を編集および実行することを可能にし得るサーバ－クライアント・アプリケーションであり得る。

【００４５】

方法の１つの有用な実施形態によれば、制限付きエンタイトルメントを求める要求は、認証証明内に第１の要求を含み得、第１の要求は既存のエンタイトルメントの最大サブセットを含み得る。したがって、初期許可は、サービスおよび機能の完全なセットにアクセスすることを許可し得、サブセットまたは制限付きエンタイトルメントに制限されないことがある。そのような制限は、限定を伴うリフレッシュ・トークンを要求することによって後で定義または要求され得る。

【００４６】

方法の別の有用な実施形態によれば、リフレッシュ・トークン（および関連するアクセス・トークン）を求める後続の要求（すなわち、初期要求の後でアプリケーションまたは機能もしくはサービスあるいはその両方にアクセスすること）は、別の制限付きエンタイトルメントを求める要求をも含み得る。このようにして、第１のアクセスと後続のアクセスとの間の区別が洗練された方式で管理され得る。

【００４７】

方法の寛容な実施形態によれば、オペレーションは、事前定義されたデータへのアクセス、データベース・アクセス、ファイル・アクセス、事前定義されたアプリケーション・プログラミング・インターフェース（たとえば、何らかの特定の解析または機械学習機能）、またはネットワークの特定のサブネットへのアクセス、あるいはその組合せを含むグループから選択された少なくとも１つを含み得る。一般には、オペレーションは、コンピューティング環境内で利用可能な任意の利用可能な低レベル機能、サービス、またはリソースに関係付けられ得る。

【００４８】

方法の１つの有利な実施形態によれば、アクセス・トークンは、事前定義された有効時間を有し得る。したがって、アクセスが引き続き許可される場合、たとえば関連するリフレッシュ・トークンによって、許可をリフレッシュしなければならない。有効時間は、デフォルト・トークン存続時間よりも著しく短くされ得る。

【００４９】

方法の別の有利な実施形態によれば、事前定義された有効時間は、特権のあるユーザ・システムによって更新可能であり得る。したがって、コンピューティング環境内のリソース、機能、またはサービスあるいはその組合せのグループに対する任意の他のアクセス制御と同様に、きめの細かいアクセス制御が管理可能であり得る。既存のＩＡＭシステムが、このタスクのために使用され得る。

【００５０】

以下では、図の詳細な説明が与えられる。図中のすべての命令は概略的なものである。最初に、データ処理環境内のトークン・ベースの許可のための本発明のコンピュータ実装方法の一実施形態のブロック図が与えられる。その後で、別の実施形態、ならびにデータ処理環境内のトークン・ベースの許可のためのアクセス・システムの実施形態が説明される。

【００５１】

図１は、データ処理環境内のトークン・ベースの許可のためのコンピュータ実装方法１００の一実施形態のブロック図を示す。データ処理環境は、少なくともユーザ・システム、アプリケーション、認証サーバ、およびアクセス制御サーバを備える。ユーザ・システムは、ネットワーク接続を介して、アプリケーションを実行中のサーバに接続される。アプリケーションは、オペレーションへのアクセス（たとえば、データベース・アクセス）を提供し、少なくともオペレーションがその識別子によって識別可能である。

【００５２】

本方法は、ユーザ・システム要求を介して（たとえば、ウェブ・ブラウザを介して）ア

プリケーションにアクセスすること（１０２）、認証サーバにユーザ・アクセス要求をリダイレクトすること（１０４）、および認証サーバとアプリケーションとの間で交換された認証証明によってユーザを認証すること（１０６）を含む。それによって、認証証明は、（ＯＡｕｔｈ２．０用語（terminology）による）スコープの標準セマンティック（具体的には、ＯＡｕｔｈ２）を使用する制限付きエンタイトルメントを求める要求を含み、制限付きエンタイトルメントは、リソースについてアクセス制御サーバによって管理される既存のエンタイトルメントのサブセットを表す。制限付きエンタイトルメントのために必要とされるデータは、標準セマンティック、すなわち使用される標準プロトコル（すなわち、ＯＡｕｔｈ２）に埋め込まれ、または標準セマンティックの部分であり得る。

【００５３】

方法１００は、認証が成功し、アプリケーションが認証サーバに登録された場合、認証サーバからアプリケーションにアクセス・トークンをリフレッシュ・トークンと共に送ること（１０８）をさらに含み、アクセス・トークンおよびリフレッシュ・トークンは制限付きエンタイトルメントを含む。

【００５４】

さらに、本方法は、ユーザ・システムによって開始されたアプリケーションによるオペレーションの実行を要求すること（１１０）を含み、要求することは、制限付きエンタイトルメントを含むアクセス・トークンを提供するアプリケーションによるオペレーションを起動すること（１１２）、オペレーションによってアクセス制御サーバを起動すること（１１４）、ユーザ・システムの識別子と、既存のエンタイトルメントのサブセットを含むトークンのスコープとをアクセス制御サーバに提供すること（１１６）、およびアクセス制御サーバによって既存のエンタイトルメントをフィルタリングするためにエンタイトルメントのサブセットを使用して、結果としてオペレーションに対するユーザ・システムのアクセスを決定すること（１１８）を含む。

【００５５】

図の説明を続ける前に、限定エンタイトルメントのここで説明される構文およびセマンティックが説明されるべきである。好ましい実装での限定エンタイトルメントのセマンティックおよび構文を理解するために、たとえばＩＢＭ Ｃｌｏｕｄ（ＴＭ）およびそのＩｄｅｎｔｉｔｙ ａｎｄ Ａｃｃｅｓｓ Ｍａｎａｇｅｍｅｎｔ（ＩＡＭ）システム内で使用されるときのＣｌｏｕｄ Ｒｅｓｏｕｒｃｅ Ｎａｍｅｓ （ＣＲＮ）の理解が有用である。

【００５６】

エンタイトルメント、ＣＲＮ、およびＩＡＭは今日、以下のように特徴付けられ得る。たとえばクラウド環境内の任意のサービスおよびリソースが、ＣＲＮを介して一意に識別可能である。ＣＲＮの基本正準フォーマットは以下の通りである。

crn:〈version〉:〈cname〉:〈ctype〉:〈service-name〉:〈location〉:〈scope〉:〈service-instance〉:〈resource-type〉:〈resource〉

パラメータは表１に記載されている。

【００５７】

【表１】

表 1:

フィールド	内容
<version>	現在は v1 のみがサポートされる
<cname>	クラウド・パブリックでは: bluemix
<ctype>	クラウド・パブリックでは: public
<service-name>	サービス・タイプについての固有の識別名
<location>	リソースの位置。多くの値が可能であり、グローバル・リソースでは global
<scope>	通常、a/<account id>というフォーマットのアカウント・スコープ
<service-instance>	利用可能な場合、サービス・インスタンスについての識別子。ブランクであり得る。
<resource-type>	このサービス内の任意選択のリソース・タイプ。ブランクであり得る。
<resource>	任意選択のリソース識別子。ブランクであり得る。

【００５８】
Ｃｌｏｕｄ　ＩＡＭのアクセス制御コンポーネントはポリシー内に許可を記憶する。ポリシーは、個々のユーザが、クラウド・コンピューティング環境内のサービスまたはリソースにアクセスすることを可能にする。サンプル・ポリシーは以下のようになる。
Identity: IBMid-2700XYZ
Role: Administrator
Target:crn:v1:bluemix:public:kubernetes::a/1234::::
【００５９】
このポリシーは、識別「IBMid-2700XYZ」を有するユーザが、アカウント「１２３４」内のサービス・タイプ「ｋｕｂｅｒｎｅｔｅｓ」に属する任意のサービスまたはリソースに関して役割「ａｄｍｉｎｉｓｔｒａｔｏｒ」がカバーする任意のアクションを行うことを可能にする。
【００６０】
あるアクションが許可されるかどうかをサービスが判断したいとき、サービスは以下の情報をアクセス制御サーバに提供する：識別／アカウント／必要なアクション／ターゲット・リソース／スコープ。
【００６１】
今日、スコープがキーワード「ｉｂｍ」を含む場合、またはスコープがターゲット・リソース内部で使用されるサービス名を含む場合、第１のチェックが完了する。そうでない場合、ポリシー・チェックは「ｄｅｎｙ」を返す。次に、すべての潜在的な適用ポリシーが、アカウントおよび識別に基づいて評価される。合致するポリシーが見つかった場合、

ポリシー・チェックは「ＰＥＲＭＩＴ」を返す。

【００６２】

特定の識別子は例に過ぎないことを明確にすべきである。ここで提案される概念の範囲から離れることなく、任意の他の識別子または変数あるいはその両方が使用され得る。

【００６３】

図２は、ここで提案される概念の基礎となる対話モデル２００のブロック図を示す。リソース所有者２０２（通常はウェブ・ブラウザの正面に座るエンド・ユーザ）がクライアント２０４（通常はエンド・ユーザにサービスを提供しているウェブ・アプリケーション）と対話している。対話型のログイン体験のために、リソース所有者２０２は、クライアントのアクセス要求の認証および許可のために認証サーバ２０６にリダイレクトされる。クライアント２０４（通常はウェブ・アプリケーション）は認証サーバ２０６と対話して、アクセス・トークンを取り出し、またはリフレッシュする。さらに、ここで提案される概念の部分として、クライアント２０４は、信頼できないコンポーネント２０８とも対話して、オペレーションを実行する。

【００６４】

信頼できないまたはセキュアでないコンポーネント２０８は、リソース・サーバ１、２１０およびリソース・サーバ２、２１２と対話して、そのオペレーションを実行する。リソース・サーバ１、２１０およびリソース・サーバ２、２１２は、アクセス制御サーバ２１４と対話して、要求されたオペレーションが許可されるか、それとも拒否されるかを判定する。

【００６５】

以下の好ましい実装では、例示的な２つのリソース・サーバ２１０、２１２（さらに多くが使用され得る）が、表２に従って、例示的な以下のサービス・タイプ、サービス・インスタンス、リソース・タイプ、およびリソース・インスタンスを使用している。

【００６６】

【表２】

表 2:

リソース・サーバ 1、210		リソース・サーバ 2、212	
サービス・タイプ:	COS	サービス・タイプ:	COS
サービス・インスタンス:	1	サービス・インスタンス:	2
リソース・タイプ:	バケット	リソース・タイプ:	バケット
リソース・インスタンス:	123	リソース・インスタンス:	456

【００６７】

ここで提案される概念での対話を実行するために、以下のステップが必要とされ得る。

１．クライアント２０４が、限定エンタイトルメントを有する（ＯＡｕｔｈ２規格によってカバーされる）リソース所有者２０２についてのアクセス・トークンおよびリフレッシュ・トークンを取り出す（新規な概念の部分）。

２．クライアント２０４が、信頼できないコンポーネントに対するオペレーションを起動する（ウェブ環境内の通常の挙動）。

３．信頼できないコンポーネント２１０がリソース・サーバ１、２１０および２、２１２と対話する（ウェブ環境内の通常の挙動）。

４．リソース・サーバ１、２１０およびリソース・サーバ２、２１２がアクセス制御サーバ２１４と対話して、要求されたオペレーションが許可されるべきか否かを判断する（

新規な概念の部分）。

【００６８】

前提条件が挙げられ得るとき：リソース・サーバ１、２１０とリソース・サーバ２、２１２の両方の上のリソースにリソース所有者２０２がアクセスすることを可能にするアクセス制御サーバ２１４に関するポリシーが、リソース所有者２０２に割り当てられた。これらのポリシーは、以下の対話、すなわちここで新しく提案される概念の部分の間に変更されない。

【００６９】

図３は、代替の開始対話の一実施形態のブロック図３００を示し、クライアント２０４が、限定エンタイトルメントを有するリソース所有者２０２についてのアクセス・トークンまたはリフレッシュ・トークンあるいはその両方を取り出す。クライアント２０４は、ＯＡｕｔｈ２規格に記載の許可タイプのうちの１つによって、リソース所有者２０２についてのアクセス・トークンまたはリフレッシュ・トークンあるいはその両方を取り出す。さらに、新規な概念の部分として、クライアント２０４は、生成されるアクセス・トークンの潜在的アクセスを限定するために、許可サーバ２０６にエンタイトルメントのリストを既に渡している。トークン作成中にスコープのリストを指定することは、ＯＡｕｔｈ２規格の部分であるが、スコープのセマンティック、および後の対話での使用は、ここで新しく提案される概念の部分である。このサンプル対話では、制限付きエンタイトルメントのリストは、ただ１つの要素「COS:1.bucket:123」であると仮定され得る。

【００７０】

図４は、クライアント２０４、認証サーバ２０６、およびリソース所有者２０２をそれぞれのメッセージ・フローと共に示す、関連する説明的な通信ダイアグラム４００を示す。

【００７１】

図５は、クライアント２０４が限定エンタイトルメントを有するリソース所有者２０２についてのアクセス・トークンまたはリフレッシュ・トークンあるいはその両方を取り出す、代替の対話５００のブロック図を示す。クライアント２０４は、ＯＡｕｔｈ２規格に記載の許可タイプのうちの１つによって、リソース所有者２０２についてのアクセス・トークンまたはリフレッシュ・トークンあるいはその両方を取り出す。後続のステップでは、クライアント２０４は、refresh_token許可タイプを使用してアクセス・トークンまたはリフレッシュ・トークンあるいはその両方をリフレッシュし、生成されるアクセス・トークンおよびリフレッシュ・トークンの潜在的アクセスを限定するために、許可サーバ２０６に制限付きエンタイトルメントのリストを渡す。トークン・リフレッシュ中にスコープのリストを指定することは、ＯＡｕｔｈ２規格の部分であるが、スコープのセマンティック、および後の対話での使用は、ここで新しく提案される概念の部分である。このサンプル対話では、制限付きエンタイトルメントのリストは、ただ１つの要素「COS:1.bucket:123」であると仮定され得る。

【００７２】

図６は、クライアント２０４がそれによってセキュアでないコンポーネント２０８に対するオペレーションを起動する、第２のタイプの対話６００のブロック図である。図３、４、５による対話の後、限定エンタイトルメントのセットを搬送するアクセス・トークンがある。この説明では、アクセス・トークンがリソース・サーバ２、２１２にアクセスするためのエンタイトルメントを含むが、リソース・サーバ１、２１０にアクセスするためのエンタイトルメントを含まないと仮定され得る。

【００７３】

クライアント２０４は、セキュアでない、または信頼できないコンポーネント２０８に対するオペレーションを起動する。信頼できないコンポーネント２０８は、たとえば、他者によって開発され、信頼できると検討または検証されていないスクリプトである。信頼できないコンポーネント２０８の呼出しは、ここで提案される概念の部分である、限定エンタイトルメントを有するアクセス・トークンを含む。

【００７４】

図７は、クライアント２０４およびセキュアでないコンポーネント２０８をそれぞれのメッセージ・フローおよび処理と共に示す、関連する説明的な通信ダイアグラム７００を示す。

【００７５】

図８は、信頼できないコンポーネント２０８がリソース・サーバ１、２１０およびリソース・サーバ２、２１２と対話する、第３のタイプの対話のブロック図８００を示す。信頼できないコンポーネント２０８の実行の部分として、スクリプトが、リソース・サーバ１、２１０に対するオペレーションを開始し、限定エンタイトルメントを有するアクセス・トークンを提供する。通常処理の部分として、リソース・サーバ１、２１０は、アクセス制御サーバ２１４と対話して、アクセス・トークンによって表されるリソース所有者がオペレーションを実行し得るかどうかを判定する。リソース・サーバ１、２１０は、ここで提案される概念の明示的コンポーネントであるオペレーションを実行するために、アクセス・トークン内部の識別、アクセス・トークン(COS:1.bucket:123)のエンタイトルメント（スコープ）、およびターゲット・リソース（たとえば、crn:v1:bluemix:public:COS::a/1234:1:bucket:123）を提供している。

【００７６】

アクセス・トークン内部のエンタイトルメントおよび既存のポリシーに基づいて、アクセス制御サーバ２１４はオペレーションを許可すると判定する。アクセス・トークンの(COS:1.bucket:123)エンタイトルメント（スコープ）がターゲット・リソース(crn:v1:bluemix:public:COS::a/1234:2:bucket:456)に合致しないので、リソース・サーバ２、２１２との類似の対話は「ＤＥＮＹ」を返す。

【００７７】

図９は、信頼できないコンポーネント２０８、リソース・サーバ１、２１０、およびリソース・サーバ２、２１２をそれぞれのメッセージ・フローおよび処理と共に示す、関連する説明的な通信ダイアグラム９００を示す。

【００７８】

図１０は、リソース・サーバ１、２１０およびリソース・サーバ２、２１２がアクセス制御サーバ２１４と対話する、第４のタイプの対話１０００のブロック図を示す。信頼できないコンポーネント２０８はリソース・サーバ１、２１０に対するオペレーション、次いでリソース・サーバ２、２１２に対するオペレーションを開始し、限定エンタイトルメントを有するアクセス・トークンを提供する。この場合も、通常のＯＡｕｔｈ２処理の部分として、リソース・サーバ２１０、２１２はアクセス制御サーバ２１４と対話して、オペレーションの実行が許可されるかどうかを判定する。リソース・サーバ２１０、２１２は、オペレーションを実効するために、アクセス・トークンのエンタイトルメント（スコープ）内部の識別、およびターゲット・リソースを提供している。

【００７９】

トークン内部の制限付きエンタイトルメントがリソース・サーバ２、２１２のサービス・インスタンスを含まないので、アクセス制御サーバ２１４は、アクセス・トークン内部の識別のポリシーがシステム内の合致するポリシーを有するとしても、やはりここで新しく提案される概念の明示的部分である、リソース・サーバ２、２１２のオペレーションを拒否すると判断する。

【００８０】

図１１は、リソース・サーバ１、２１０、リソース・サーバ２、２１２、およびアクセス制御サーバ２１４をそれぞれのメッセージ・フローおよび処理と共に示す、関連する説明的な通信ダイアグラム１１００を示す。

【００８１】

次の２つの図１２、１３は、ここで提案される概念（図１３）について必要とされるものと比較した、従来のアクセス制御サーバ決定エンジン（図１２）の擬似コード・セグメントの比較を示す。容易に理解できるように、制限付きエンタイトルメントについての正しいきめの細かいアクセス制御のための、より複雑な判定が必要とされる。しかしながら

、標準のＯＡｕｔｈ２アクセス制御と比べた場合、これによって、より柔軟でセキュアなリソース管理が保証される。

【００８２】

完全性のために、図１４は、データ処理環境内のトークン・ベースの認証のためのアクセス・システム１４００のブロック図を示す。データ処理環境は、少なくともユーザ・システム、アプリケーション、認証サーバ、およびアクセス制御サーバ（すべて図示せず）を備える。それによって、ユーザ・システムは、ネットワーク接続を介して、アプリケーションを実行中のサーバに接続され、アプリケーションはオペレーションへのアクセスを提供する。少なくともオペレーションがその識別子によって識別可能である。ここで論じるすべてのコンポーネントが、コンポーネントを接続するネットワークに接続されることにも留意することができる。

【００８３】

アクセス・システム１４００は、ユーザ・システム要求を介してアプリケーションにアクセスするように適合されたアクセス・モジュール１４０２と、認証サーバ２０６にユーザ・アクセス要求をリダイレクトするように適合されたリダイレクティング・モジュール１４０４とを備える。認証サーバ２０６は、認証サーバとアプリケーションとの間で交換された認証証明によってユーザを認証するように適合され、認証証明は、スコープの標準セマンティックを使用する制限付きエンタイトルメントを求める要求を含み、制限付きエンタイトルメントは、リソースについてアクセス制御サーバによって管理される既存のエンタイトルメントのサブセットを表す。

【００８４】

アクセス・システム１４００は、認証が成功し、アプリケーションが認証サーバ２０６に登録された場合、認証サーバ２０６からアプリケーションにアクセス・トークンをリフレッシュ・トークンと共に送るように適合された送信側をさらに備え、アクセス・トークンおよびリフレッシュ・トークンは制限付きエンタイトルメントを含む。

【００８５】

それによって、ユーザ・システムは、ユーザ・システムによって開始されたアプリケーションによるオペレーションの実行を要求するように適合され、オペレーションの実行を要求することは、制限付きエンタイトルメントを含むアクセス・トークンを提供するアプリケーションによるオペレーションを起動すること、オペレーションによってアクセス制御サーバを起動すること、ユーザ・システムの識別子と、既存のエンタイトルメントのサブセットを含むトークンのスコープとをアクセス制御サーバ２１４に提供すること、アクセス制御サーバ２１４によって既存のエンタイトルメントをフィルタリングするためにエンタイトルメントのサブセットを使用して、結果としてオペレーションに対するユーザ・システムのアクセスを決定することを含む。

【００８６】

本発明の実施形態は、プログラム・コードを記憶または実行あるいはその両方を行うのに適したプラットフォームの如何に関わらず、ほぼ任意のタイプのコンピュータと共に実装され得る。図１５は、一例として、提案される方法に関するプログラム・コードを実行するのに適したコンピューティング・システム１５００を示す。処理環境のほぼ任意のコンポーネントが、図１５によるコンピューティング・システムによって表され得る。

【００８７】

コンピューティング・システム１５００は、適切なコンピュータ・システムの一例に過ぎず、コンピュータ・システム１５００が上記で述べられた機能のいずれかを実装または実施あるいはその両方を行うことができるかどうかの如何に関わらず、本明細書で説明される本発明の実施形態の使用または機能の範囲に関する何らかの限定を示唆するものではない。コンピュータ・システム１５００では、多数の他の汎用または専用コンピューティング・システム環境または構成と共に動作可能なコンポーネントがある。コンピュータ・システム／サーバ１５００と共に使用するのに適していることがある周知のコンピューティング・システム、環境、または構成、あるいはその組合せの例には、限定はしないが、

パーソナル・コンピュータ・システム、サーバ・コンピュータ・システム、シン・クライアント、シック・クライアント、ハンドヘルドまたはラップトップ・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・ベースのシステム、セット・トップ・ボックス、プログラム可能コンシューマ・エレクトロニクス、ネットワークＰＣ、ミニコンピュータ・システム、メインフレーム・コンピュータ・システム、および上記のシステムまたはデバイスのいずれかを含む分散型クラウド・コンピューティング環境が含まれる。コンピュータ・システム／サーバ１５００は、コンピュータ・システム１５００によって実行される、プログラム・モジュールなどのコンピュータ・システム実行可能命令の一般的文脈で説明され得る。一般に、プログラム・モジュールは、特定のタスクを実施し、または特定の抽象データ・タイプを実装するルーチン、プログラム、オブジェクト、コンポーネント、ロジック、データ構造などを含み得る。コンピュータ・システム／サーバ１５００は、通信ネットワークを通じてリンクされるリモート処理デバイスによってタスクが実施される、分散型クラウド・コンピューティング環境で実施され得る。分散型クラウド・コンピューティング環境では、プログラム・モジュールは、メモリ記憶デバイスを含む、ローカル・コンピュータ・システム記憶媒体とリモート・コンピュータ・システム記憶媒体の両方に配置され得る。

【００８８】

図に示されるように、コンピュータ・システム／サーバ１５００が汎用コンピューティング・デバイスの形態で示されている。コンピュータ・システム／サーバ１５００のコンポーネントには、限定はしないが、１つまたは複数のプロセッサまたは処理装置１５０２、システム・メモリ１５０４、システム・メモリ１５０４を含む様々なシステム・コンポーネントをプロセッサ１５０２に結合するバス１５０６が含まれ得る。バス１５０６は、メモリ・バスまたはメモリ・コントローラ、周辺バス、アクセラレーテッド・グラフィックス・ポート、および様々なバス・アーキテクチャのいずれかを使用するプロセッサまたはローカル・バスを含むいくつかのタイプのバス構造のいずれかの１つまたは複数を表す。限定ではなく例として、そのようなアーキテクチャには、Industry Standard Architecture (ISA)バス、Micro Channel Architecture (MCA)バス、Enhanced ISA (EISA)バス、Video Electronics Standards Association (VESA)ローカル・バス、およびPeripheral Component Interconnects (PCI)バスが含まれる。コンピュータ・システム／サーバ１５００は通常、様々なコンピュータ・システム可読媒体を含む。そのような媒体は、コンピュータ・システム／サーバ１５００によってアクセス可能である任意の入手可能な媒体であり得、そのような媒体には、揮発性媒体と不揮発性媒体、取外し可能媒体と取外し不能媒体の両方が含まれる。

【００８９】

システム・メモリ１５０４は、ランダム・アクセス・メモリ（ＲＡＭ）１５０８またはキャッシュ・メモリ１５１０あるいはその両方などの、揮発性メモリの形態のコンピュータ・システム可読媒体を含み得る。コンピュータ・システム／サーバ１５００は、他の取外し可能／取外し不能な揮発性／不揮発性コンピュータ・システム記憶媒体をさらに含み得る。単に例として、取外し不能な不揮発性磁気媒体（図示しておらず、通常は「ハード・ドライブ」と呼ばれる）から読み取り、それに書き込むための記憶システム１５１２が設けられ得る。図示していないが、取外し可能な不揮発性磁気ディスク（たとえば、「フロッピィ・ディスク」）から読み取り、それに書き込むための磁気ディスク・ドライブ、およびＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、または他の光媒体などの取外し可能な不揮発性光ディスクから読み取り、それに書き込むための光ディスク・ドライブが設けられ得る。そのような場合、それぞれは、１つまたは複数のデータ媒体インターフェースによってバス１５０６に接続され得る。以下でさらに図示され、説明されるように、メモリ１５０４は、本発明の実施形態の機能を実施するように構成されるプログラム・モジュールのセット（たとえば、少なくとも１つ）を有する少なくとも１つのプログラム製品を含み得る。

【００９０】

限定ではなく例として、プログラム・モジュール１５１６のセット（少なくとも１つ）

を有するプログラム／ユーティリティ、ならびにオペレーティング・システム、１つまたは複数のアプリケーション・プログラム、他のプログラム・モジュール、およびプログラム・データが、メモリ１５０４内に格納され得る。オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、他のプログラム・モジュール、およびプログラム・データのそれぞれ、またはそれらの何らかの組合せは、ネットワーキング環境の実装を含み得る。プログラム・モジュール１５１６は一般に、本明細書で説明される、本発明の実施形態の機能または方法あるいはその両方を実施する。

【００９１】

コンピュータ・システム／サーバ１５００はまた、キーボード、ポインティング・デバイスなどの１つまたは複数の外部デバイス１５１８、ディスプレイ１５２０など、ユーザがコンピュータ・システム／サーバ１５００と対話することを可能にする１つまたは複数のデバイス、またはコンピュータ・システム／サーバ１５００が１つまたは複数の他のコンピューティング・デバイスと通信することを可能にする任意のデバイス（たとえば、ネットワーク・カード、モデムなど）、あるいはその組合せと通信し得る。そのような通信は、入力／出力（Ｉ／Ｏ）インターフェース１５１４を介して行われ得る。さらに、コンピュータ・システム／サーバ１５００は、ネットワーク・アダプタ１５２２を介して、ローカル・エリア・ネットワーク（ＬＡＮ）、一般の広域ネットワーク（ＷＡＮ）、または公衆ネットワーク（たとえば、インターネット）、あるいはその組合せなどの１つまたは複数のネットワークと通信し得る。図示されるように、ネットワーク・アダプタ１５２２は、バス１５０６を介してコンピュータ・システム／サーバ１５００の他のコンポーネントと通信し得る。図示していないが、他のハードウェア・コンポーネントまたはソフトウェア・コンポーネントあるいはその両方が、コンピュータ・システム／サーバ１５００と共に使用され得ることを理解されたい。限定はしないが、例には、マイクロコード、デバイス・ドライバ、冗長処理装置、外部ディスク・ドライブ・アレイ、ＲＡＩＤシステム、テープ・ドライブ、データ・アーカイブ記憶システムなどが含まれる。

【００９２】

例示のために本発明の様々な実施形態の説明が提示されたが、説明は網羅的なものではなく、開示される実施形態に限定されないものとする。説明された実施形態の範囲および思想から逸脱することなく、多くの修正形態および変形形態が当業者には明らかとなるであろう。本明細書で使用される用語は、実施形態の原理、市場で見出される技術に勝る実際の応用もしくは技術的改良を最良に説明するように、または本明細書で開示される実施形態を当業者が理解することを可能にするように選ばれたものである。

【００９３】

本発明は、システム、方法、またはコンピュータ・プログラム製品、あるいはその組合せとして実施され得る。コンピュータ・プログラム製品は、プロセッサに本発明の態様を実施させるためのコンピュータ可読プログラム命令を有する１つまたは複数のコンピュータ可読記憶媒体を含み得る。

【００９４】

媒体は、伝播媒体用の電子的、磁気的、光学的、電磁的、赤外線式、または半導体システムであり得る。コンピュータ可読媒体の例には、半導体またはソリッド・ステート・メモリ、磁気テープ、取外し可能コンピュータ・ディスケット、ランダム・アクセス・メモリ（ＲＡＭ）、読取り専用メモリ（ＲＯＭ）、硬質磁気ディスク、および光ディスクが含まれ得る。光ディスクの現在の例には、コンパクト・ディスク読取り専用メモリ（ＣＤ－ＲＯＭ）、コンパクト・ディスク読取り／書込み（ＣＤ－Ｒ／Ｗ）、ＤＶＤ、およびＢｌｕ－Ｒａｙ－Ｄｉｓｋが含まれる。

【００９５】

コンピュータ可読記憶媒体は、命令実行デバイスによって使用される命令を保持および記憶し得る有形デバイスであり得る。コンピュータ可読記憶媒体は、たとえば、限定はしないが、電子記憶デバイス、磁気記憶デバイス、光記憶デバイス、電磁記憶デバイス、半導体記憶デバイス、または上記の任意の適切な組合せであり得る。コンピュータ可読記憶

媒体のより具体的な例の非網羅的リストは、以下を含む：ポータブル・コンピュータ・ディスケット、ハード・ディスク、ランダム・アクセス・メモリ（ＲＡＭ）、読取り専用メモリ（ＲＯＭ）、消去可能プログラマブル読取り専用メモリ（ＥＰＲＯＭまたはフラッシュ・メモリ）、静的ランダム・アクセス・メモリ（ＳＲＡＭ）、ポータブル・コンパクト・ディスク読取り専用メモリ（ＣＤ－ＲＯＭ）、デジタル・バーサタイル・ディスク（ＤＶＤ）、メモリ・スティック、フロッピィ・ディスク、パンチ・カード、または命令が記録された溝の中の隆起構造などの機械的符号化されたデバイス、および上記の任意の適切な組合せ。本明細書では、コンピュータ可読記憶媒体は、電波または他の自由に伝播する電磁波、導波路または他の伝送媒体を通じて伝播する電磁波（たとえば、光ファイバ・ケーブルを通る光パルス）、またはワイヤを通じて伝送される電気信号など、本質的に一時的信号であると解釈されるべきではない。

【００９６】

本明細書で説明されるコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体からそれぞれのコンピューティング／処理デバイスに、あるいはネットワーク、たとえばインターネット、ローカル・エリア・ネットワーク、広域ネットワーク、もしくはワイヤレス・ネットワーク、またはその組合せを介して外部コンピュータまたは外部記憶デバイスにダウンロードされ得る。ネットワークは、銅伝送ケーブル、光伝送ファイバ、ワイヤレス伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータ、またはエッジ・サーバ、あるいはその組合せを含み得る。各コンピューティング／処理デバイス内のネットワーク・アダプタ・カードまたはネットワーク・インターフェースは、ネットワークからコンピュータ可読プログラム命令を受信し、それぞれのコンピューティング／処理デバイス内のコンピュータ可読記憶媒体内に記憶するためにコンピュータ可読プログラム命令を転送する。

【００９７】

本発明のオペレーションを実施するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セット・アーキテクチャ（ＩＳＡ）命令、機械語命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、あるいはＳｍａｌｌｔａｌｋ（Ｒ）、Ｃ＋＋などのオブジェクト指向プログラミング言語と、「Ｃ」プログラミング言語または類似のプログラミング言語などの従来の手続型プログラミング言語とを含む１つまたは複数のプログラミング言語の任意の組合せで書かれたソース・コードまたはオブジェクト・コードのどちらかであり得る。コンピュータ可読プログラム命令は、完全にユーザのコンピュータ上で、スタンド・アロン・ソフトウェア・パッケージとして部分的にユーザのコンピュータ上で、部分的にユーザのコンピュータ上、かつ部分的にリモート・コンピュータ上で、または完全にリモート・コンピュータまたはサーバ上で実行され得る。後者のシナリオでは、リモート・コンピュータは、ローカル・エリア・ネットワーク（ＬＡＮ）または広域ネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを通じてユーザのコンピュータに接続され得、あるいは（たとえば、インターネット・サービス・プロバイダを使用して、インターネットを通じて）外部コンピュータに接続が行われ得る。いくつかの実施形態では、たとえば、プログラマブル論理回路、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、またはプログラマブル論理アレイ（ＰＬＡ）を含む電子回路が、本発明の態様を実施するために、コンピュータ可読プログラム命令の状態情報を利用することによってコンピュータ可読プログラム命令を実行して、電子回路を個別設定し得る。

【００９８】

本発明の態様が、本発明の実施形態による方法、装置（システム）、およびコンピュータ・プログラム製品のフローチャート図またはブロック図あるいはその両方を参照しながら本明細書で説明される。フローチャート図またはブロック図あるいはその両方の各ブロック、およびフローチャート図またはブロック図あるいはその両方のブロックの組合せが、コンピュータ可読プログラム命令によって実装され得ることを理解されよう。

【００９９】

これらのコンピュータ可読プログラム命令は、コンピュータまたは他のプログラム可能データ処理装置のプロセッサを介して実行される命令により、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックで指定される機能／動作を実装するための手段を生み出すように、汎用コンピュータ、専用コンピュータ、または他のプログラム可能データ処理装置のプロセッサに与えられ、マシンが作り出され得る。これらのコンピュータ可読プログラム命令はまた、命令を記憶するコンピュータ可読記憶媒体がフローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックで指定される機能／動作の態様を実装する命令を含む製造品を含むように、コンピュータ、プログラム可能データ処理装置、または他のデバイス、あるいはその組合せに特定の方式で機能するように指示し得るコンピュータ可読記憶媒体内に記憶され得る。

【０１００】

コンピュータ可読プログラム命令はまた、コンピュータ、他のプログラム可能装置、または別のデバイス上で実行される命令が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックで指定される機能／動作を実装するように、コンピュータ、他のプログラム可能データ処理装置、または別のデバイス上にロードされ、コンピュータ、他のプログラム可能装置、または他のデバイス上で一連の動作ステップを実施させて、コンピュータ実装プロセスが生成され得る。

【０１０１】

図中のフローチャートまたはブロック図あるいはその両方は、本発明の様々な実施形態によるシステム、方法、およびコンピュータ・プログラム製品の可能な実装のアーキテクチャ、機能、およびオペレーションを示す。この点で、フローチャートまたはブロック図の各ブロックは、指定の論理的機能を実装するための１つまたは複数の実行可能命令を含む命令のモジュール、セグメント、または部分を表し得る。いくつかの代替の実装では、ブロック内に記載の機能は、図に記載されている以外の順序で行われ得る。たとえば、連続して示される２つのブロックは、実際にはほぼ同時に実行され得、またはブロックは、関係する機能に応じて、時には逆の順序で実行され得る。ブロック図またはフローチャート図あるいはその両方の各ブロック、およびブロック図またはフローチャート図あるいはその両方のブロックの組合せが、指定の機能または動作を実施し、あるいは専用ハードウェアおよびコンピュータ命令の組合せを実施する専用ハードウェア・ベースのシステムによって実装され得ることにも留意されよう。

【０１０２】

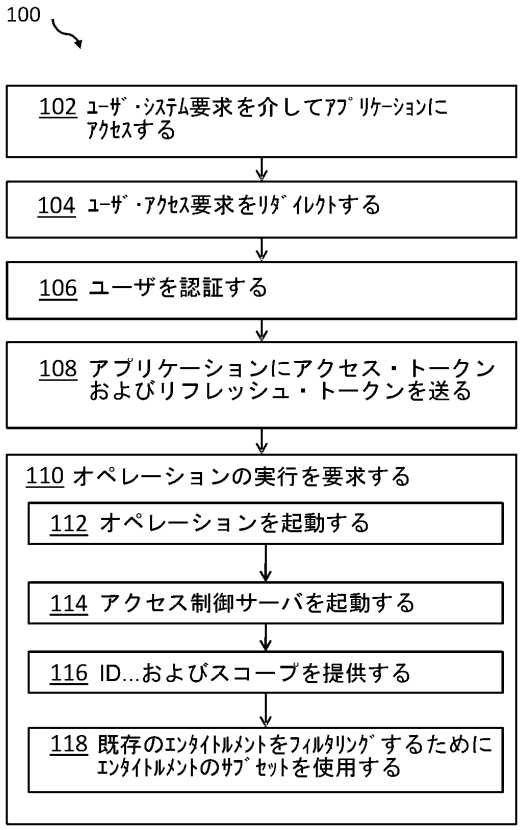
本明細書で使用される用語は、特定の実施形態を説明するためのものに過ぎず、本発明を限定するものではない。本明細書では、単数形「ａ」、「ａｎ」、および「ｔｈｅ」は、文脈が別段に明確に示すのでない限り、複数形も含むものとする。本明細書では、「備える（ｃｏｍｐｒｉｓｅｓ）」または「備えている（ｃｏｍｐｒｉｓｉｎｇ）」あるいはその両方という用語は、明記された特徴、完全体、ステップ、オペレーション、要素、またはコンポーネント、あるいはその組合せの存在を指定するが、１つまたは複数の他の特徴、完全体、ステップ、オペレーション、要素、コンポーネント、またはそのグループ、あるいはその組合せの存在または追加を除外しないことをさらに理解されよう。

【０１０３】

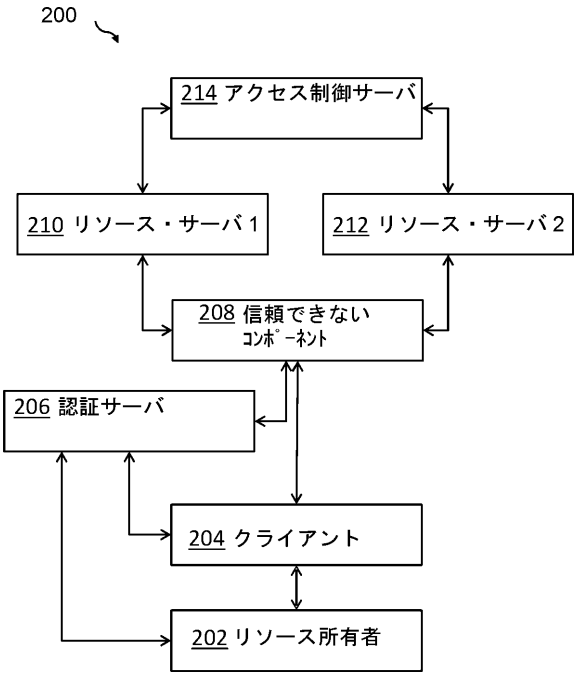
以下の特許請求の範囲のすべての手段またはステップおよび機能要素の対応する構造、材料、動作、および均等物は、具体的に特許請求されるように、他の特許請求される要素と組み合わせて機能を実施するための任意の構造、材料、または動作を含むものとする。本発明の説明は、例示および説明のために提示されたものであり、網羅的なものではなく、開示された形態の発明に限定されるものではないものとする。本発明の範囲および思想から逸脱することなく、多くの修正形態および変形形態が当業者には明らかとなるであろう。実施形態は、本発明の原理および実際の応用を最良に説明するため、および企図される特定の用途に適するような、様々な修正を伴う様々な実施形態について本発明を当業者が理解することを可能にするために選ばれ、説明される。

【図面】

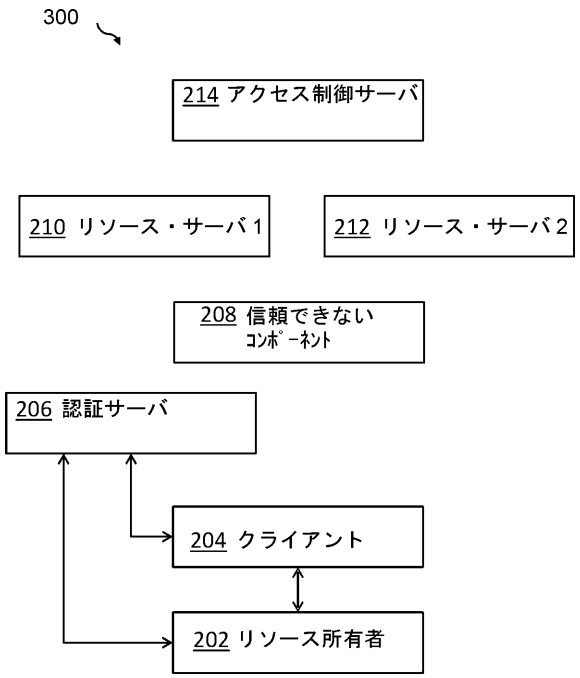
【図１】


100
102 ユーザ・システム要求を介してアプリケーションにアクセスする
104 ユーザ・アクセス要求をリダイレクトする
106 ユーザを認証する
108 アプリケーションにアクセス・トークンおよびリフレッシュ・トークンを送る
110 オペレーションの実行を要求する
112 オペレーションを起動する
114 アクセス制御サーバを起動する
116 ID...およびスコープを提供する
118 既存のエンタイトルメントをフィルタリングするためにエンタイトルメントのサブセットを使用する

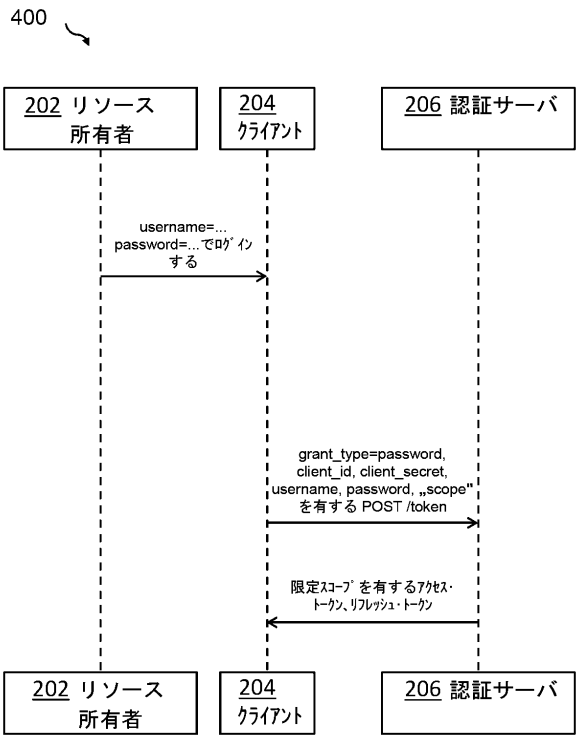
【図２】


200
214 アクセス制御サーバ
210 リソース・サーバ 1
212 リソース・サーバ 2
208 信頼できないコンポーネント
206 認証サーバ
204 クライアント
202 リソース所有者

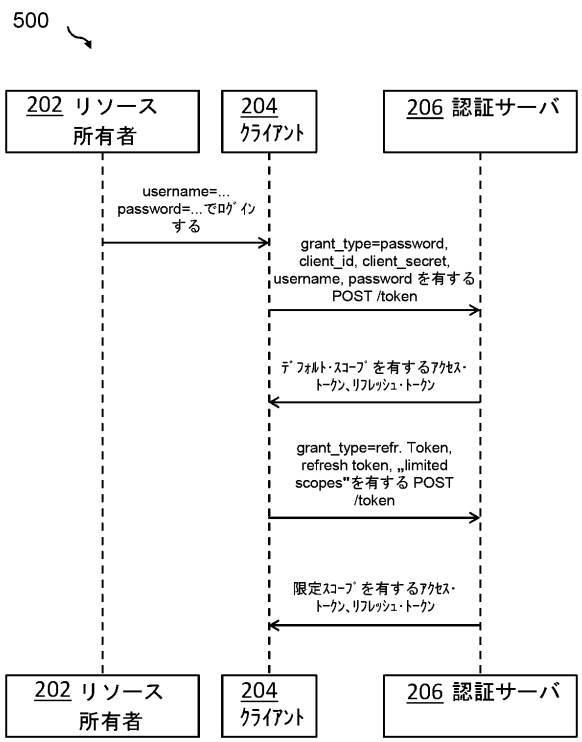
【図３】


300
214 アクセス制御サーバ
210 リソース・サーバ 1
212 リソース・サーバ 2
208 信頼できないコンポーネント
206 認証サーバ
204 クライアント
202 リソース所有者

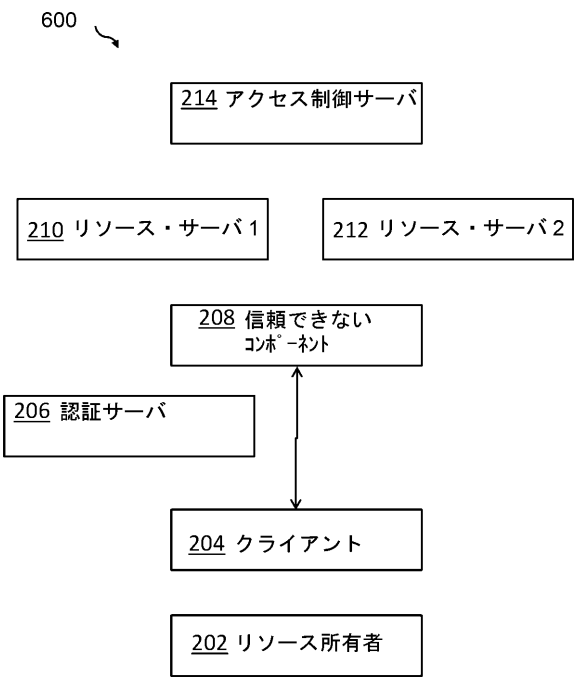
【図４】


400
202 リソース所有者
204 クライアント
206 認証サーバ
username=... password=...でログインする
grant_type=password, client_id, client_secret, username, password, „scope" を有する POST /token
限定スコープを有するアクセス・トークン、リフレッシュ・トークン
202 リソース所有者
204 クライアント
206 認証サーバ

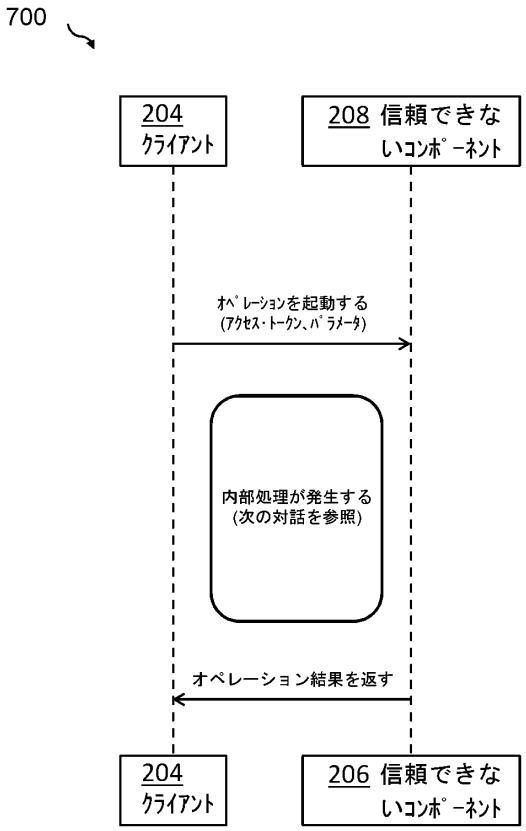
【図５】


500
202 リソース所有者
204 ｸﾗｲｱﾝﾄ
206 認証サーバ
username=... password=...でﾛｸﾞｲﾝする
grant_type=password, client_id, client_secret, username, password を有する POST /token
ﾃﾞﾌｫﾙﾄ･ｽｺｰﾌﾟを有するｱｸｾｽ･ﾄｰｸﾝ、ﾘﾌﾚｯｼｭ･ﾄｰｸﾝ
grant_type=refr. Token, refresh token, „limited scopes"を有する POST /token
限定ｽｺｰﾌﾟを有するｱｸｾｽ･ﾄｰｸﾝ、ﾘﾌﾚｯｼｭ･ﾄｰｸﾝ
202 リソース所有者
204 ｸﾗｲｱﾝﾄ
206 認証サーバ

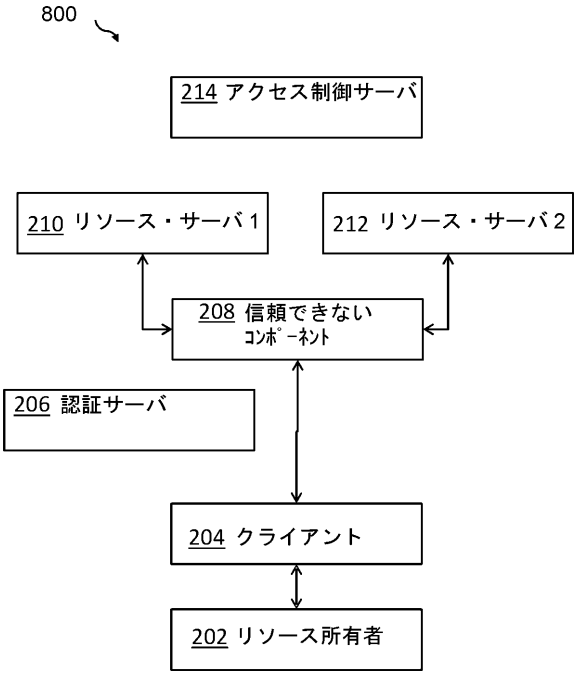
【図６】


600
214 アクセス制御サーバ
210 リソース・サーバ 1
212 リソース・サーバ 2
208 信頼できないｺﾝﾎﾟｰﾈﾝﾄ
206 認証サーバ
204 クライアント
202 リソース所有者

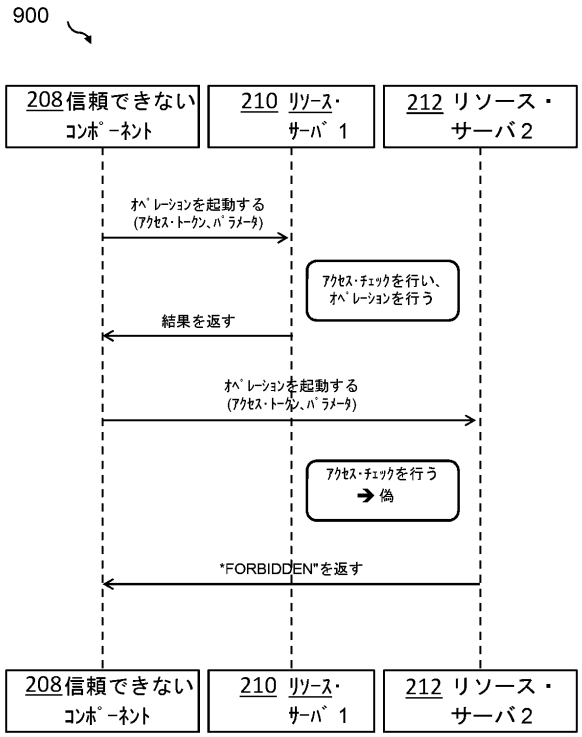
【図７】


700
204 ｸﾗｲｱﾝﾄ
208 信頼できないｺﾝﾎﾟｰﾈﾝﾄ
ｵﾍﾟﾚｰｼｮﾝを起動する (ｱｸｾｽ･ﾄｰｸﾝ、ﾊﾟﾗﾒｰﾀ)
内部処理が発生する (次の対話を参照)
オペレーション結果を返す
204 ｸﾗｲｱﾝﾄ
206 信頼できないｺﾝﾎﾟｰﾈﾝﾄ

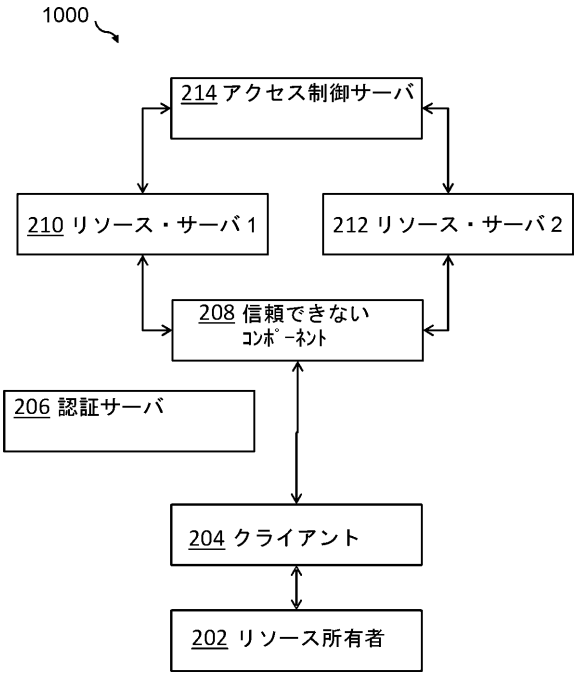
【図８】


800
214 アクセス制御サーバ
210 リソース・サーバ 1
212 リソース・サーバ 2
208 信頼できないｺﾝﾎﾟｰﾈﾝﾄ
206 認証サーバ
204 クライアント
202 リソース所有者

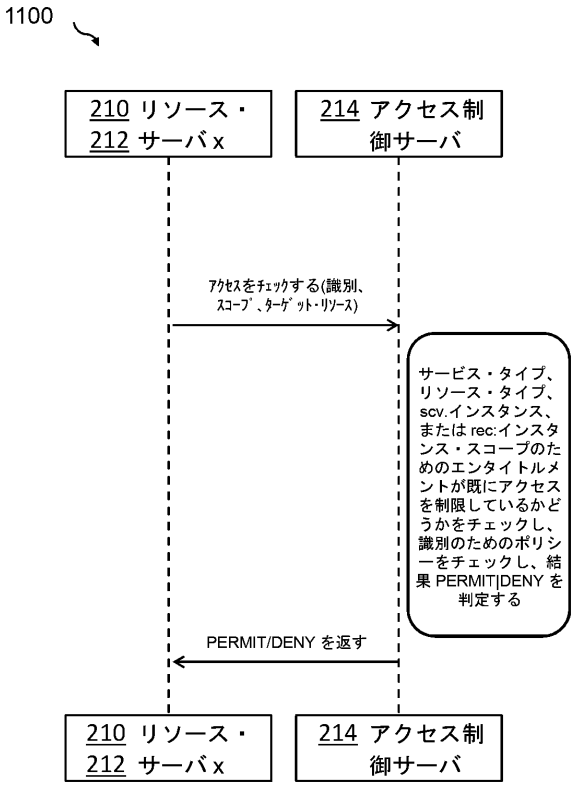
【図９】



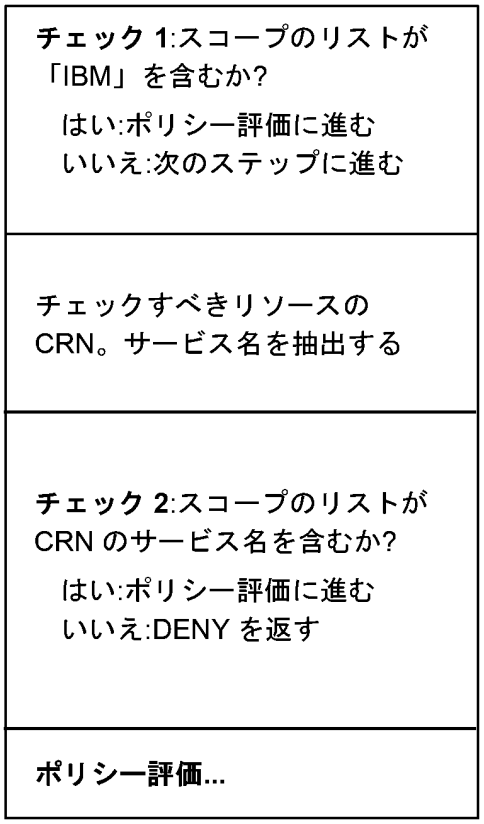
【図１０】



【図１１】



【図１２】



【図１３】

チェック 1:スコープのリストが ibm を含むか?
はい:ポリシー評価に進む
いいえ:次のステップに進む

ﾁｪｯｸすべきﾘｿｰｽの CRN を構文解析する。CRN 構文についての詳細は、ｾｸｼｮﾝ「限定ｴﾝﾀｲﾄﾙﾒﾝﾄの構文およびｾﾏﾝﾃｨｯｸ」で見い出すことができる。
利用可能な場合、**crn-service-name**, **crn-service-instance**, **crn-resource-type**, **crn-resource** を抽出する

チェック 2:スコープのリスト内の各スコープについて以下を行う:
スコープ構文についての詳細は、セクション*「限定エンタイトルメントの構文およびセマンティック」*で見い出すことができる。スコープを **scope-service-name**, **scope-service-instance**, **scope-resource-type**, **scope-resource** に分割する;個々の部分は空であり得る。

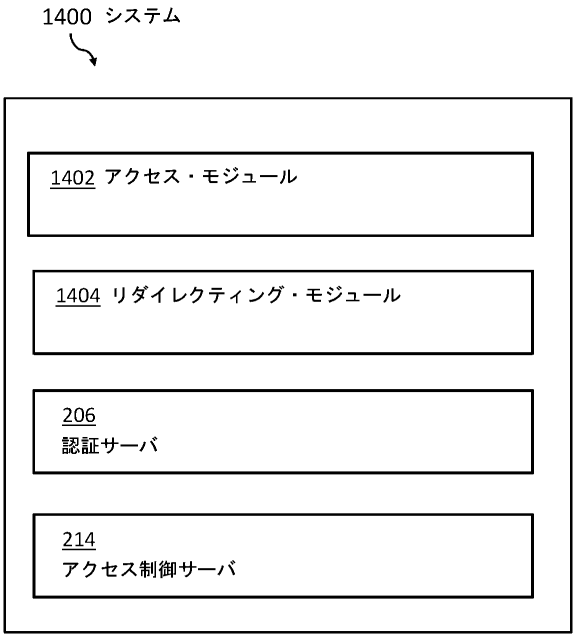
以下をチェックする
(**crn-service-name** が **scope-service-name** に合致)
かつ
((**crn-service-instance** が利用不能かつ **scope-service-name** が利用不能)または
(**crn-service-instance** が利用可能かつ **scope-service-name** が利用不能)または
(**crn-service-instance** が利用可能かつ **scope-service-name** に合致))
かつ
((**crn-resource-type** が利用不能かつ **scope-resource-type** が利用不能)または
(**crn-resource-type** が利用可能かつ **scope-resource-type** が利用不能)または
(**crn-resource-type** が利用可能かつ **scope-resource-type** に合致))
かつ
((**crn-resource** が利用不能かつ **scope-resource** が利用不能)または
(**crn-resource** が利用可能かつ **scope-resource** が利用不能)または
(**crn-resource** が利用可能かつ **scope-resource** に合致))

実際のスコープがこのチェックに合致するか?
はい:ポリシー評価に進む
いいえ:次のスコープに進む

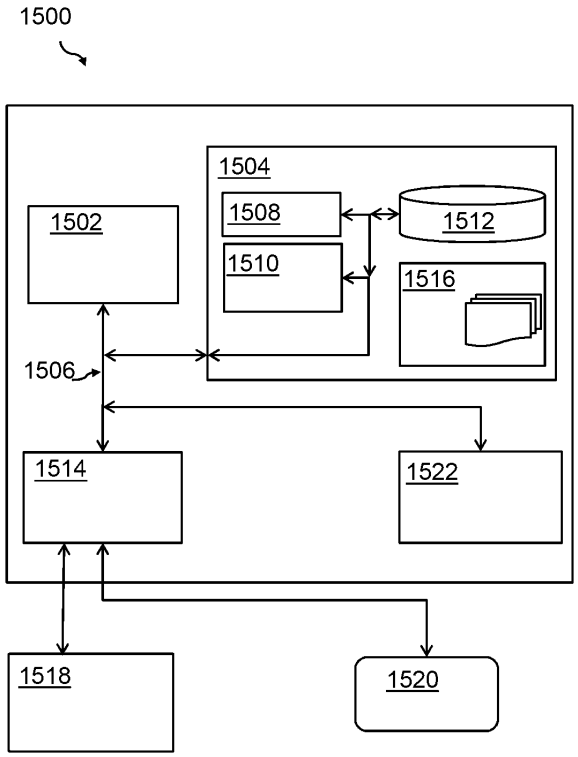
合致するスコープが見つからない?DENY を返す

ポリシー評価...

【図１４】



【図１５】



フロントページの続き

(72)発明者　スモルニー、マーティン
ドイツ７１０３２ ベーブリンゲン シェーナイヒャー・シュトラーセ ２２０
(72)発明者　デュエル、トーマス
ドイツ７１０３２ ベーブリンゲン シェーナイヒャー・シュトラーセ ２２０
(72)発明者　ベック、ミカエル
ドイツ７１０３２ ベーブリンゲン シェーナイヒャー・シュトラーセ ２２０
(72)発明者　シェック、ユルゲン
ドイツ７１０３２ ベーブリンゲン シェーナイヒャー・シュトラーセ ２２０

審査官　小林 秀和
(56)参考文献　米国特許出願公開第２０１７／００３４１７２（ＵＳ，Ａ１）
特開２００３－１２３３８９（ＪＰ，Ａ）
特開２０１８－１６３６１６（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３３
Ｇ０６Ｆ　２１／６２