(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7281483号
(P7281483)

(45)発行日　令和5年5月25日(2023.5.25)

(24)登録日　令和5年5月17日(2023.5.17)

(51)国際特許分類
Ｇ０６Ｆ　21/33　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/33

請求項の数　10　（全63頁）

(21)出願番号　特願2020-560921(P2020-560921)
(86)(22)出願日　令和1年6月21日(2019.6.21)
(65)公表番号　特表2021-528722(P2021-528722A)
(43)公表日　令和3年10月21日(2021.10.21)
(86)国際出願番号　PCT/US2019/038432
(87)国際公開番号　WO2020/005752
(87)国際公開日　令和2年1月2日(2020.1.2)
審査請求日　令和4年4月6日(2022.4.6)
(31)優先権主張番号　62/689,369
(32)優先日　平成30年6月25日(2018.6.25)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　16/404,796
(32)優先日　令和1年5月7日(2019.5.7)
最終頁に続く

(73)特許権者　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国カリフォルニア州９４０６５レッドウッド・シティー，オラクル・パークウェイ５００
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　バンサル，アジート
アメリカ合衆国、９４４０４ カリフォルニア州、フォスター・シティー、エッジウォーター・ブールバード、７２２、アパートメント・２０６
(72)発明者　バート，シバラム
アメリカ合衆国、９４０８７ カリフォ
最終頁に続く

(54)【発明の名称】　マルチテナントアイデンティティクラウドサービスのための宣言型第三者アイデンティティプロバイダの統合

(57)【特許請求の範囲】
【請求項１】
マルチテナントアイデンティティクラウドサービスのための第三者アイデンティティプロバイダを用いてユーザにログインを与える方法であって、前記方法は、
前記第三者アイデンティティプロバイダに対応するトークンエンドポイントのアイデンティティと、対応するパラメータ値とを含む、宣言型メタデータを受信するステップと、
前記宣言型メタデータをデータベースに格納するステップと、
前記第三者アイデンティティプロバイダを用いたログインの要求を受信するステップと、
前記宣言型メタデータを取り出し、認可要求を構築するステップと、
前記認可要求を前記第三者アイデンティティプロバイダに送信し、それに応じた認可コードを受信するステップと、
前記宣言型メタデータを取り出し、前記認可コードを用いてトークン要求を構築するステップと、
前記トークン要求を前記第三者アイデンティティプロバイダに送信し、それに応じたアクセストークンを受信するステップとを含む、方法。
【請求項２】
前記宣言型メタデータを取り出し、前記アクセストークンを用いてユーザ情報要求を構築するステップと、
前記ユーザ情報要求に基づいたユーザ情報を受信するとともに、ユーザセッションの作成要求を受信するステップと、

前記マルチテナントアイデンティティクラウドサービスへの前記ユーザのログインを正常に実現するステップとをさらに含む、請求項１に記載の方法。
【請求項３】
前記アクセストークンはＯＡｕｔｈトークンを含む、請求項１または２に記載の方法。
【請求項４】
前記宣言型メタデータは前記トークン要求の範囲をさらに含む、請求項１～３のいずれかに記載の方法。
【請求項５】
前記宣言型メタデータは、前記第三者アイデンティティプロバイダのユーザプロファイル属性の、前記マルチテナントアイデンティティクラウドサービスのユーザプロファイル属性に対するマッピングをさらに含む、請求項１～４のいずれかに記載の方法。
【請求項６】
前記宣言型メタデータを取り出すことは、クロスドメインアイデンティティ管理用システム（ＳＣＩＭ）レプレゼンテーショナル・ステート・トランスファー（ＲＥＳＴ）エンドポイントをエクスポーズすることを含む、請求項１～５のいずれかに記載の方法。
【請求項７】
前記宣言型メタデータはＪａｖａＳｃｒｉｐｔオブジェクト表記法（ＪＳＯＮ）フォーマットである、請求項１～６のいずれかに記載の方法。
【請求項８】
前記宣言型メタデータは、前記マルチテナントアイデンティティクラウドサービスの前記ユーザによって生成される、請求項１～７のいずれかに記載の方法。
【請求項９】
請求項１～８のいずれかに記載の方法をプロセッサに実行させるためのコンピュータプログラム。
【請求項１０】
請求項９に記載のコンピュータプログラムを格納したメモリと、
前記コンピュータプログラムを実行するためのプロセッサとを備える、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
本願は、２０１８年６月２５日出願の米国仮特許出願第６２／６８９，３６９号に基づく優先権を主張し、その開示を本明細書に引用により援用する。
【０００２】
分野
一実施形態は、概してアイデンティティ管理に関し、特にクラウドシステムにおけるアイデンティティ管理に関する。
【背景技術】
【０００３】
背景情報
一般的に、多様なデバイス（たとえばデスクトップおよびモバイルデバイス）および多様なユーザ（たとえば被雇用者、パートナー、顧客など）からアクセスされる、クラウドベースのアプリケーション（たとえば企業パブリッククラウドアプリケーション、第三者クラウドアプリケーションなど）の使用が、急激に増加している。クラウドベースのアプリケーションは、その多様性およびアクセシビリティが高いので、アイデンティティの管理およびアクセスのセキュリティが中心的な関心事になっている。クラウド環境における典型的なセキュリティの問題は、不正アクセス、アカウントのハイジャック、悪意のあるインサイダーなどである。したがって、クラウドベースのアプリケーションであっても、どこに存在するアプリケーションであっても、アプリケーションにアクセスするデバイスの種類またはユーザの種類にかかわらず、安全なアクセスが必要とされている。

【発明の概要】
【課題を解決するための手段】
【０００４】
概要
実施形態は、マルチテナントアイデンティティクラウドサービスのための第三者アイデンティティプロバイダを用いてユーザにログイン機能を与える。実施形態は、第三者アイデンティティプロバイダに対応するトークンエンドポイントのアイデンティティと、対応するパラメータ値とを含む、宣言型メタデータを受信する。実施形態は、宣言型メタデータをデータベースに格納し、第三者アイデンティティプロバイダを用いたログインの要求を受信する。実施形態は、メタデータを取り出し、認可要求を構築し、認可要求を第三者アイデンティティプロバイダに送信し、それに応じた認可コードを受信する。実施形態は、メタデータを取り出し、認可コードを用いてトークン要求を構築し、トークン要求を第三者アイデンティティプロバイダに送信し、それに応じたアクセストークンを受信する。
【図面の簡単な説明】
【０００５】
【図１】クラウドベースのアイデンティティ管理を提供する実施形態の一例のブロック図である。
【図２】クラウドベースのアイデンティティ管理を提供する実施形態の一例のブロック図である。
【図３】クラウドベースのアイデンティティ管理を提供する実施形態の一例のブロック図である。
【図４】クラウドベースのアイデンティティ管理を提供する実施形態の一例のブロック図である。
【図５】クラウドベースのアイデンティティ管理を提供する実施形態の一例のブロック図である。
【図６】ある実施形態のシステムビューを提供するブロック図である。
【図６Ａ】ある実施形態の機能ビューを提供するブロック図である。
【図７】クラウドゲートを実現するある実施形態のブロック図である。
【図８】一実施形態における複数のテナンシーを実現するシステムの一例を示す図である。
【図９】ある実施形態のネットワークビューのブロック図である。
【図１０】一実施形態におけるシングルサインオン（「ＳＳＯ」）機能のシステムアーキテクチャビューのブロック図である。
【図１１】一実施形態におけるＳＳＯ機能のメッセージシーケンスフローの図である。
【図１２】一実施形態における分散型データグリッドの一例を示す図である。
【図１３】本発明の実施形態に係るシーケンス図を示す。
【発明を実施するための形態】
【０００６】
詳細な説明
実施形態は、マルチテナントアイデンティティクラウドサービスのための第三者アイデンティティプロバイダをプロビジョニングしログイン機構として使用できるようメタデータを定義することを可能にする、宣言型フレームワークを提供する。メタデータは、特別の権限を有するユーザにより生成されることが可能であり、新たな第三者アイデンティティプロバイダの追加が所望されるときにソフトウェアコーディングの要求が生成および格納されないようにする。
【０００７】
実施形態が提供するアイデンティティクラウドサービスは、マイクロサービスベースのアーキテクチャを実現するとともに、マルチテナントアイデンティティおよびデータセキュリティの管理ならびにクラウドベースのアプリケーションへの安全なアクセスを提供する。実施形態は、ハイブリッドクラウドのデプロイメント（すなわちパブリッククラウドとプライベートクラウドとを組み合わせたものを含むクラウドのデプロイメント）につい

て安全なアクセスをサポートする。実施形態は、クラウド内およびオンプレミス双方におけるアプリケーションおよびデータを保護する。実施形態は、ウェブ、モバイル機器、およびアプリケーションプログラミングインターフェイス（application programming interface）（「ＡＰＩ」）を介したマルチチャネルアクセスをサポートする。実施形態は、顧客、パートナー、および被雇用者など、さまざまなユーザのアクセスを管理する。実施形態は、クラウドを通じたアクセスおよびオンプレミスのアクセス双方を管理、制御、および監査する。実施形態は、新たなおよび既存のアプリケーションおよびアイデンティと統合される。実施形態は横方向にスケーラブルである。

【０００８】

一実施形態は、ステートレスな中間層環境において多数のマイクロサービスを実現することによりクラウドベースのマルチテナントアイデンティティおよびアクセス管理サービスを提供するシステムである。一実施形態において、要求された各アイデンティティ管理サービスは、リアルタイムタスクとニア・リアルタイムタスクとに分割される。リアルタイムタスクは中間層のマイクロサービスによって処理されるのに対し、ニア・リアルタイムタスクはメッセージキューにオフロードされる。実施形態は、ルーティング層および中間層によって消費されるアクセストークンを実現することにより、マイクロサービスにアクセスするためのセキュリティモデルを強化する。したがって、実施形態は、マルチテナントのマイクロサービスアーキテクチャに基づいてクラウドスケールのアイデンティティおよびアクセス管理（Identity and Access Management）（「ＩＡＭ」）プラットフォームを提供する。

【０００９】

一実施形態は、組織が、その新たなビジネス構想のために高速で信頼性が高くかつ安全なサービスを迅速に開発できるようにするアイデンティティクラウドサービスを提供する。一実施形態において、アイデンティティクラウドサービスは多数のコアサービスを提供する。各コアサービスは、多くの企業が直面する固有の課題を解決する。一実施形態において、アイデンティティクラウドサービスは、たとえば、最初にユーザのオンボード／インポートを行うとき、ユーザメンバとともにグループをインポートするとき、ユーザを作成／更新／ディスエーブル／イネーブル／削除するとき、ユーザをグループに割り当てる／グループへのユーザ割当を解除するとき、グループを作成／更新／削除するとき、パスワードをリセットするとき、ポリシーを管理するとき、アクティベーションを送信するときなどの、アドミニストレータをサポートする。

【００１０】

<u>統一されたアクセスセキュリティ</u>

一実施形態は、クラウド環境およびオンプレミス環境双方におけるアプリケーションおよびデータを保護する。本実施形態は、どのデバイスからの誰によるどのアプリケーションへのアクセスも安全にする。本実施形態は、これらの環境双方にわたる保護を提供する。なぜなら、これら２つの環境の間でセキュリティに矛盾があればリスクが高くなる可能性があるからである。たとえば、このような矛盾があった場合、販売員は、離反して競合他社に移った後であっても、その顧客関係管理（Customer Relationship Management）（「ＣＲＭ」）アカウントへのアクセス権を有し続ける場合がある。したがって、実施形態は、オンプレミス環境においてプロビジョニングされたセキュリティ制御をクラウド環境に拡張する。たとえば、ある人物が会社を辞めた場合、実施形態は、そのアカウントがオンプレミスおよびクラウド双方においてディスエーブルされることを保証する。

【００１１】

一般的に、ユーザは、ウェブブラウザ、デスクトップ、携帯電話、タブレット、スマートウォッチ、その他のウェアラブル機器などの多種多様なチャネルを通してアプリケーションおよび／またはデータにアクセスし得る。したがって、一実施形態は、これらすべてのチャネルについて、これらを通るアクセスを安全なものにする。たとえば、ユーザは、その携帯電話を用いて、自身のデスクトップ上で開始したトランザクションを完了させることができる。

【００１２】
一実施形態はさらに、顧客、パートナー、被雇用者など、さまざまなユーザのアクセスを管理する。一般的に、アプリケーションおよび／またはデータは、被雇用者だけでなく、顧客または第三者によってもアクセスされる場合がある。既知の多くのシステムは、被雇用者のオンボード時に安全対策を講じるが、この安全対策は通常、顧客、第三者、パートナーなどにアクセス権を付与するときの安全対策と同じレベルではないので、結果として、適切に管理されていない者によってセキュリティが破られる可能性がある。しかしながら、実施形態は、被雇用者だけでなく各タイプのユーザのアクセスについて十分な安全対策が提供されることを保証する。
【００１３】
アイデンティティクラウドサービス
実施形態は、マルチテナントでクラウドスケールのＩＡＭプラットフォームであるアイデンティティクラウドサービス（Identity Cloud Service）（「ＩＤＣＳ」）を提供する。ＩＤＣＳは、認証、認可、監査、および連携（federation）を提供する。ＩＤＣＳは、パブリッククラウドおよびオンプレミスシステム上で実行されているカスタムアプリケーションおよびサービスへのアクセスを管理する。これに代わるまたはこれに加えられる実施形態において、ＩＤＣＳは、パブリッククラウドサービスへのアクセスも管理し得る。たとえば、ＩＤＣＳを用いて、このような多様なサービス／アプリケーション／システムにまたがるシングルサインオン（Single Sign On）（「ＳＳＯ」）機能を提供することができる。
【００１４】
実施形態は、クラウドスケールのソフトウェアサービスを設計、構築、および配信するためのマルチテナントマイクロサービスアーキテクチャに基づく。マルチテナンシーとは、あるサービスを物理的に実現したものがありこのサービスが当該サービスを購入した複数の顧客を安全にサポートするサービスであることを言う。サービスは、異なるクライアントが異なる目的のために再使用できるソフトウェア機能またはソフトウェア機能のセット（指定された情報を取り出すことまたは一組の動作を実行することなど）に、（たとえばサービスを要求しているクライアントのアイデンティティに基づく）その使用を管理するポリシーを合わせたものである。一実施形態において、サービスは、１つ以上の機能へのアクセスを可能にするメカニズムであり、このアクセスは、所定のインターフェイスを用いて提供され、サービスの記述によって明記された制約およびポリシーに従って実行される。
【００１５】
一実施形態において、マイクロサービスは独立してデプロイ可能なサービスである。一実施形態において、マイクロサービスという用語は、言語に依存しないＡＰＩを用いて相互に通信する小さな独立したプロセスから複雑なアプリケーションが構成されている、ソフトウェアアーキテクチャ設計パターンを意図している。一実施形態において、マイクロサービスは、細かく分離された小さなサービスであり、各サービスは、小さなタスクの実行に集中し得る。一実施形態において、マイクロサービスアーキテクチャスタイルは、単一のアプリケーションを小さなサービス一式として開発する手法であり、各サービスは、自身のプロセスにおいて実行され、軽量のメカニズム（たとえばハイパーテキスト・トランスファー・プロトコル（Hypertext Transfer Protocol）（「ＨＴＴＰ」）リソースＡＰＩ）と通信する。一実施形態において、マイクロサービスは、同一機能すべてをまたは同一機能のうちの多くを実行するモノリシックサービスと比較すると、交換がより簡単である。加えて、マイクロサービスは各々、その他のマイクロサービスに悪影響を与えることなく更新し得る。これに対し、モノリシックサービスの一部を更新すると、当該モノリシックサービスの他の部分に望ましくないまたは意図せぬ悪影響が及ぶ可能性がある。一実施形態において、マイクロサービスはその機能を中心として有益に編成し得る。一実施形態において、マイクロサービスのコレクションのうち各マイクロサービスのスタートアップ時間は、これらのマイクロサービスのうちのすべてのサービスをまとめて実行する

単一のアプリケーションのスタートアップ時間よりも遥かに短い。いくつかの実施形態において、このようなマイクロサービス各々のスタートアップ時間は約１秒以下であるのに対し、このような単一のアプリケーションのスタートアップ時間は約１分、数分、またはそれよりも長い場合がある。

【００１６】

一実施形態において、マイクロサービスアーキテクチャとは、フレキシブルで、独立してデプロイ可能なソフトウェアシステムを構築するための、サービス指向アーキテクチャ（service oriented architecture（「ＳＯＡ」））の専門化（すなわちシステム内におけるタスクの分離）および実現の手法のことである。マイクロサービスアーキテクチャにおけるサービスは、目的を達成するためにネットワークを通して相互に通信するプロセスである。一実施形態において、これらのサービスは、技術に依存しないプロトコルを使用する。一実施形態において、サービスは、細分性が小さく軽量であるプロトコルを使用する。一実施形態において、サービスは独立してデプロイ可能である。システムの機能を異なる小さなサービスに分散させることにより、システムの結束性は向上し、システムのカップリングは減少する。それにより、システム変更が容易になり、任意の時点でシステムに機能および品質を追加することが容易になる。また、それによって、個々のサービスのアーキテクチャが、絶え間ないリファクタリングを通して出現することが可能になり、したがって、大規模な事前の設計の必要性は低下しソフトウェアを早期に連続してリリースすることが可能になる。

【００１７】

一実施形態において、マイクロサービスアーキテクチャでは、アプリケーションがサービスのコレクションとして開発され、各サービスはそれぞれのプロセスを実行し軽量のプロトコルを用いて通信する（たとえばマイクロサービスごとの固有ＡＰＩ）。マイクロサービスアーキテクチャにおいて、１つのソフトウェアを個々のサービス／機能に分解することは、提供するサービスに応じて異なるレベルの粒度で行うことができる。サービスはランタイムコンポーネント／プロセスである。各マイクロサービスは、他のモジュール／マイクロサービスに対してトークすることができる内蔵モジュールである。各マイクロサービスは、他からコンタクトできる無名ユニバーサルポートを有する。一実施形態において、マイクロサービスの無名ユニバーサルポートは、従来マイクロサービスがエクスポーズする（たとえば従来のＨＴＴＰポートとしての）標準通信チャネルであり、同一サービス内の他のモジュール／マイクロサービスがそれに対してトークできるようにする標準通信チャネルである。マイクロサービスまたはその他の内蔵機能モジュールを包括的に「サービス」と呼ぶことができる。

【００１８】

実施形態は、マルチテナントアイデンティティ管理サービスを提供する。実施形態は、さまざまなアプリケーションとの容易な統合を保証するオープン標準に基づいており、標準ベースのサービスを通してＩＡＭ機能を提供する。

【００１９】

実施形態は、アイデンティティがアクセスできる対象、このようなアクセスを付与できる者、このようなアクセスを管理できる者などを判断し施行することを伴うユーザアイデンティティのライフサイクルを管理する。実施形態は、クラウド内でアイデンティティ管理ワークロードを実行し、このクラウド内に存在するとは限らないアプリケーションのセキュリティ機能をサポートする。これらの実施形態が提供するアイデンティティ管理サービスはクラウドから購入されてもよい。たとえば、企業は、このようなサービスをクラウドから購入してその被雇用者の当該企業のアプリケーションに対するアクセスを管理してもよい。

【００２０】

実施形態は、システムセキュリティ、大規模なスケーラビリティ、エンドユーザのユーザビリティ、およびアプリケーションのインターオペラビリティを提供する。実施形態は、クラウドの成長と、顧客によるアイデンティティサービスの使用とを扱っている。マイ

クロサービスに基づく基礎は、横方向のスケーラビリティ条件を扱うのに対し、サービスの綿密な調整は機能条件を扱う。これらの目標双方を達成するには、ビジネスロジックを（可能な限り）分解することにより、最終的には一貫性のあるステートレスを達成する一方で、リアルタイム処理を受けない動作論理のほとんどが、配信と処理が保証されたスケーラビリティが高い非同期イベント管理システムに、オフロードされることにより、ニア・リアルタイムにシフトする。実施形態は、コスト効率を実現しシステム管理を容易にするために、ウェブ層からデータまで完全にマルチテナントである。

【００２１】

実施形態は、さまざまなアプリケーションと統合し易くするために、業界の標準（たとえば、ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ、ＯＡｕｔｈ２、セキュリティ・アサーション・マークアップ言語（Security Assertion Markup Language）２（「ＳＡＭＬ２」)、クロスドメインアイデンティティ管理用システム（System for Cross-domain Identity Management）（「ＳＣＩＭ」）、レプレゼンテーショナル・ステート・トランスファー(Representational State Transfer）（「ＲＥＳＴ」)など）に従う。一実施形態は、クラウドスケールＡＰＩプラットフォームを提供し、エラスティックスケーラビリティのために横方向にスケーラブルなマイクロサービスを実現する。本実施形態は、クラウド原理を強化し、テナントごとにデータを分離したマルチテナントアーキテクチャを提供する。本実施形態はさらに、テナントセルフサービスを介してテナントごとのカスタマイズを提供する。本実施形態は、他のアイデンティサービスとのオンデマンドの統合の際にはＡＰＩを介して利用することができ、連続したフィーチャーリリースを提供する。

【００２２】

一実施形態は、インターオペラビリティを提供し、クラウドおよびオンプレミスにおけるアイデンティティ管理（identity management）（「ＩＤＭ」）機能への投資を強化する。本実施形態は、オンプレミスの軽量ディレクトリアクセスプロトコル（Lightweight Directory Access Protocol）（「ＬＤＡＰ」）データからクラウドデータへの、およびその逆の、自動化されたアイデンティティ同期化を提供する。本実施形態は、クラウドと企業との間にＳＣＩＭアイデンティティバスを提供し、ハイブリッドクラウドのデプロイの各種オプションを可能にする（たとえば、アイデンティティ連携および／または同期化、ＳＳＯエージェント、ユーザプロビジョニングコネクタなど）。

【００２３】

したがって、一実施形態は、ステートレスな中間層において多数のマイクロサービスを実現することによりクラウドベースのマルチテナントアイデンティティおよびアクセス管理サービスを提供するシステムである。一実施形態において、要求された各アイデンティティ管理サービスは、リアルタイムタスクとニア・リアルタイムタスクとに分割される。リアルタイムタスクは中間層のマイクロサービスによって処理されるのに対し、ニア・リアルタイムタスクはメッセージキューにオフロードされる。実施形態は、ルーティング層によって消費されて、マイクロサービスにアクセスするためのセキュリティモデルを実施するトークンを実現する。したがって、実施形態は、マルチテナントのマイクロサービスアーキテクチャに基づくクラウドスケールのＩＡＭプラットフォームを提供する。

【００２４】

一般的に、周知のシステムは、たとえば、企業クラウドアプリケーション、パートナークラウドアプリケーション、第三者クラウドアプリケーション、および顧客アプリケーションなど、各種環境によって提供されるアプリケーションに対するサイロ化されたアクセスを提供する。このようなサイロ化されたアクセスは、複数のパスワード、異なるパスワードポリシー、異なるアカウントプロビジョニングおよびデプロビジョニング手法、異種の監査などを必要とする場合がある。しかしながら、一実施形態は、ＩＤＣＳを実現することにより、このようなアプリケーションに対し統一されたＩＡＭ機能を提供する。図１は、ユーザおよびアプリケーションをオンボードするための統一されたアイデンティティプラットフォーム１２６を提供する、ＩＤＣＳ１１８を用いる実施形態の一例のブロック図１００である。本実施形態は、企業クラウドアプリケーション１０２、パートナークラ

ウドアプリケーション１０４、第三者クラウドアプリケーション１１０、および顧客アプリケーション１１２などのさまざまなアプリケーションにまたがるシームレスなユーザ体験を提供する。アプリケーション１０２、１０４、１１０、１１２は、異なるチャネルを通してアクセスされてもよく、たとえば、携帯電話ユーザ１０８が携帯電話１０６を介して、デスクトップコンピュータのユーザ１１６がブラウザ１１４を介して、アクセスしてもよい。ウェブブラウザ（一般的にブラウザと呼ばれる）は、ワールドワイドウェブ上で情報リソースを取得、提示、およびトラバースするためのソフトウェアアプリケーションである。ウェブブラウザの例としては、Mozilla（登録商標） Firefox（登録商標）、Google Chrome（登録商標）、Microsoft（登録商標） Internet Explorer（登録商標）、およびApple（登録商標） Safari（登録商標）が挙げられる。

【００２５】

ＩＤＣＳ１１８は、ユーザのアプリケーションの統一されたビュー１２４、（アイデンティティプラットフォーム１２６を介する）デバイスおよびアプリケーションにまたがる統一された安全なクレデンシャル、および（管理コンソール１２２を介する）統一された管理方法を、提供する。ＩＤＣＳサービスは、ＩＤＣＳ ＡＰＩ１４２にコールすることによって取得されてもよい。このようなサービスは、たとえば、ログイン／ＳＳＯサービス１２８（たとえばＯｐｅｎＩＤ Ｃｏｎｎｅｃｔ）、連携サービス１３０（たとえばＳＡＭＬ）、トークンサービス１３２（たとえばＯＡｕｔｈ）、ディレクトリサービス１３４（たとえばＳＣＩＭ）、プロビジョニングサービス１３６（たとえばＳＣＩＭまたはAny Transport over Multiprotocol（「ＡＴｏＭ」））、イベントサービス１３８（たとえばＲＥＳＴ）、およびロールベースアクセス制御（role-based access control）（「ＲＢＡＣ」）サービス１４０（たとえばＳＣＩＭ）を含み得る。ＩＤＣＳ１１８はさらに、提供されるサービスに関するレポートおよびダッシュボード１２０を提供し得る。

【００２６】

<u>統合ツール</u>

通常、大企業では、そのオンプレミスのアプリケーションへの安全なアクセスのために、ＩＡＭシステムを適所に設けるのが一般的である。ビジネス手法は通常オラクル社の「Oracle IAM Suite」などのインハウスＩＡＭシステムを中心として成熟し標準化される。小～中規模組織でも、通常は、そのビジネスプロセスを、Microsoft Active Directory（「ＡＤ」）などの単純なディレクトリソリューションを通してユーザアクセスを管理することを中心として設計されている。オンプレミス統合を可能にするために、実施形態は、顧客がそのアプリケーションをＩＤＣＳと統合できるようにするツールを提供する。

【００２７】

図２は、オンプレミス２０６のＡＤ２０４との統合を提供する、クラウド環境２０８内のＩＤＣＳ２０２を用いる実施形態の一例のブロック図２００である。本実施形態は、たとえば、クラウドサービス２１０、クラウドアプリケーション２１２、パートナーアプリケーション２１４、および顧客アプリケーション２１６などのクラウド２０８内のさまざまなアプリケーション／サービスならびにオンプレミスアプリケーション２１８などのオンプレミスアプリケーションおよび第三者アプリケーションを含むすべてのアプリケーションにまたがる、シームレスなユーザ体験を提供する。クラウドアプリケーション２１２は、たとえば、ヒューマン・キャピタル・マネージメント（Human Capital Management）（「ＨＣＭ」）、ＣＲＭ、タレント取得（たとえばオラクル社のOracle Taleoクラウドサービス）、構成、価格設定、および見積もり（Configure Price and Quote「ＣＰＱ」）などを含み得る。クラウドサービス２１０は、たとえば、サービスとしてのプラットフォーム（Platform as a Service）（「ＰａａＳ」）、Ｊａｖａ（登録商標）、データベース、ビジネスインテリジェンス（business intelligence）（「ＢＩ」）、文書などを含み得る。

【００２８】

アプリケーション２１０、２１２、２１４、２１６、２１８は、異なるチャネルを通してアクセスされてもよく、たとえば、携帯電話ユーザ２２０が携帯電話２２２を介して、

デスクトップコンピュータのユーザ２２４がブラウザ２２６を介して、アクセスしてもよい。本実施形態は、クラウド２０８と企業２０６との間のＳＣＩＭアイデンティティバス２３４を介して、オンプレミスのＡＤデータからクラウドデータに、アイデンティティの同期化を自動的に行う。本実施形態はさらに、クラウド２０８からオンプレミスＡＤ２０４への、（たとえばパスワード２３２を用いて）認証を連携させるためのＳＡＭＬバス２２８を提供する。

【００２９】

一般的に、アイデンティティバスは、アイデンティティ関連サービスのためのサービスバスである。サービスバスは、メッセージをあるシステムから別のシステムに伝えるためのプラットフォームを提供する。これは、たとえばサービス指向アーキテクチャ（service oriented architecture）（「ＳＯＡ」）において、信頼されているシステム間で情報を交換するための制御されたメカニズムである。アイデンティティバスは、ウェブサービス、ウェブサーバプロキシなどの標準的なＨＴＴＰベースのメカニズムに従って構築された論理バスである。アイデンティティバスにおける通信は、各プロトコル（たとえばＳＣＩＭ、ＳＡＭＬ、ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔなど）に従って実行されてもよい。たとえば、ＳＡＭＬバスは、ＳＡＭＬサービスに関するメッセージを伝えるための、２つのシステム間のＨＴＴＰベースの接続である。同様に、ＳＣＩＭバスを用い、ＳＣＩＭプロトコルに従って、ＳＣＩＭメッセージを伝える。

【００３０】

図２の実施形態は、顧客のＡＤ２０４とともにオンプレミス２０６でダウンロードおよびインストールすることができる小バイナリ（たとえば大きさが１ＭＢ）のアイデンティティ（「ＩＤ」）ブリッジ２３０を実現する。ＩＤブリッジ２３０は、顧客によって選択された組織ユニット（organizational unit）（「ＯＵ」）のユーザおよびグループ（たとえばユーザのグループ）をリッスンし、これらのユーザをクラウド２０８に対して同期させる。一実施形態において、ユーザのパスワード２３２はクラウド２０８に対して同期されていない。顧客は、ＩＤＣＳユーザのグループを、ＩＤＣＳ２０８において管理されているクラウドアプリケーションにマッピングすることにより、ユーザのアプリケーションアクセスを管理することができる。ユーザのグループメンバーシップがオンプレミス２０６で変更されるたびに、対応するクラウドアプリケーションアクセスは自動的に変更される。

【００３１】

たとえば、技術部門から販売部門に異動した被雇用者は、販売クラウドへのアクセスをほぼ瞬間的に取得することができ、開発者クラウドへのアクセスは失う。この変化がオンプレミスＡＤ２０４に反映されると、クラウドアプリケーションのアクセスの変更がニア・リアルタイムで実現される。同様に、ＩＤＣＳ２０８で管理されているクラウドアプリケーションへの、この企業から去るユーザのアクセスは、取消される。完全自動化のために、顧客は、たとえばＡＤ連携サービス（「ＡＤ／ＦＳ」またはＳＡＭＬ連携を実現するその他の何らかのメカニズム）を通して、オンプレミスＡＤ２０４とＩＤＣＳ２０８との間のＳＳＯをセットアップして、エンドユーザが、単一の企業パスワード３３２を用いて、クラウドアプリケーション２１０、２１２、２１４、２１６およびオンプレミスアプリケーション２１８にアクセスできるようにしてもよい。

【００３２】

図３は、図２と同一のコンポーネント２０２、２０６、２０８、２１０、２１２、２１４、２１６、２１８、２２０、２２２、２２４、２２６、２２８、２３４を含む実施形態の一例のブロック図３００である。しかしながら、図３の実施形態において、ＩＤＣＳ２０２は、オラクルＩＤＭのようなオンプレミスＩＤＭ３０４との統合を提供する。オラクルＩＤＭ３０４は、ＩＡＭ機能を提供するための、オラクル社のソフトウェアスイートである。本実施形態は、オンプレミスアプリケーションおよび第三者アプリケーションを含むすべてのアプリケーションにまたがるシームレスなユーザ体験を提供する。本実施形態は、クラウド２０２と企業２０６との間のＳＣＩＭアイデンティティバス２３４を介した

オンプレミスＩＤＭ３０４からＩＤＣＳ２０８へのユーザアイデンティティをプロビジョニングする。本実施形態はさらに、クラウド２０８からオンプレミス２０６への認証の連携のためのＳＡＭＬバス２２８（またはＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔバス）を提供する。

【００３３】

図３の実施形態において、オラクル社のオラクルアイデンティティマネージャ（Oracle Identity Manager）（「ＯＩＭ」）コネクタ３０２およびオラクル社のオラクルアクセスマネージャ（Oracle Access Manager）（「ＯＡＭ」）連携モジュール３０６は、オラクルＩＤＭ３０４の拡張モジュールとして実現される。コネクタは、システムに話しかける方法について物理的な認識があるモジュールである。ＯＩＭは、ユーザアイデンティティを管理するように構成されたアプリケーションである（たとえば、ユーザがアクセス権を持つべき対象とアクセス権を持つべきでない対象に基づいて異なるシステムのユーザアカウントを管理する）。ＯＡＭは、ウェブＳＳＯ、アイデンティコンテキスト、認証および認可、ポリシー管理、テスト、ロギング、監査などのアクセス管理機能を提供するセキュリティアプリケーションである。ＯＡＭはＳＡＭＬに対するビルトイン（built-in）サポートを有する。ユーザがＩＤＣＳ２０２のアカウントを有する場合、ＯＩＭコネクタ３０２およびＯＡＭ連携３０６をオラクルＩＤＭ３０４とともに使用することにより、このアカウントを作成／削除し、このアカントからのアクセスを管理することができる。

【００３４】

図４は、図２および図３と同一のコンポーネント２０２、２０６、２０８、２１０、２１２、２１４、２１６、２１８、２２０、２２２、２２４、２２６、２３４を含む実施形態の一例のブロック図４００である。しかしながら、図４の実施形態において、ＩＤＣＳ２０２は、クラウドアイデンティをオンプレミスアプリケーション２１８に拡張するための機能を提供する。本実施形態は、オンプレミスアプリケーションおよび第三者アプリケーションを含むすべてのアプリケーションにまたがるアイデンティティのシームレスなビューを提供する。図４の実施形態において、ＳＣＩＭアイデンティティバス２３４を用いることにより、ＩＤＣＳ２０２のデータを「クラウドキャッシュ」４０２と呼ばれるオンプレミスＬＤＡＰデータと同期させる。クラウドキャッシュ４０２は以下でより詳細に開示される。

【００３５】

一般的に、ＬＤＡＰに基づいて通信するように構成されたアプリケーションは、ＬＤＡＰ接続を必要とする。このようなアプリケーションはＬＤＡＰ接続をＵＲＬを用いて構築しないかもしれない（たとえばGoogle（登録商標）に接続する「www.google.com」とは違って）。なぜなら、ＬＤＡＰはローカルネットワーク上になければならないからである。図４の実施形態において、ＬＤＡＰベースのアプリケーション２１８は、クラウドキャッシュ４０２に接続し、クラウドキャッシュ４０２は、ＩＤＣＳ２０２に接続してから、要求されているデータをＩＤＣＳ２０２から引出す。ＩＤＣＳ２０２とクラウドキャッシュ４０２との間の通信は、ＳＣＩＭプロトコルに従って実現されてもよい。たとえば、クラウドキャッシュ４０２はＳＣＩＭバス２３４を用いてＳＣＩＭ要求をＩＤＣＳ２０２に送信し、それに対応するデータを受信してもよい。

【００３６】

一般的に、あるアプリケーションの完全な実現は、コンシューマポータルを構築することと、外部ユーザ集団に対してマーケティングキャンペーンを実行することと、ウェブおよびモバイルチャネルをサポートすることと、ユーザ認証、セッション、ユーザプロファイル、ユーザグループ、アプリケーションロール、パスワードポリシー、セルフサービス／登録、社会的統合、アイデンティ連携などを処理することとを含む。一般的に、アプリケーションの開発者はアイデンティティ／セキュリティの専門家ではない。このため、オンデマンドのアイデンティティ管理サービスが望ましいのである。

【００３７】

図５は、図２～図４と同一のコンポーネント２０２、２２０、２２２、２２４、２２６、２３４、４０２を含む実施形態の一例のブロック図５００である。しかしながら、図５

の実施形態において、ＩＤＣＳ２０２は、オンデマンドで安全なアイデンティティ管理を提供する。本実施形態は、オンデマンドの、ＩＤＣＳ２０２のアイデンティサービスとの統合を提供する（たとえばＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ、ＯＡｕｔｈ２、ＳＡＭＬ２、またはＳＣＩＭなどの標準に基づいて）。（オンプレミスであってもパブリッククラウド内またはプライベートクラウド内にあってもよい）アプリケーション５０５は、ＩＤＣＳ２０２のアイデンティティサービスＡＰＩ５０４をコールしてもよい。ＩＤＣＳ２０２が提供するサービスは、たとえば、セルフサービス登録５０６、パスワード管理５０８、ユーザプロファイル管理５１０、ユーザ認証５１２、トークン管理５１４、社会的統合５１６などを含み得る。

【００３８】

本実施形態において、ＳＣＩＭアイデンティティバス２３４を用いることにより、ＩＤＣＳ２０２内のデータを、オンプレミスのＬＤＡＰクラウドキャッシュ４０２内のデータと同期させる。さらに、ウェブサーバ／プロキシ（たとえばＮＧＩＮＸ、Apacheなど）上で実行している「クラウドゲート」５０２を、アプリケーション５０５が用いて、ＩＤＣＳ２０２からユーザウェブＳＳＯおよびＲＥＳＴ　ＡＰＩセキュリティを取得してもよい。クラウドゲート５０２は、クライアントアプリケーションが有効なアクセストークンを提供すること、および／またはユーザがＳＳＯセッション構築のために正常に認証することを保証することによって、マルチテナントＩＤＣＳマイクロサービスへのアクセスを安全なものするコンポーネントである。クラウドゲート５０２は以下でさらに開示される。クラウドゲート５０２（webgate／webagentと同様の実施ポイント）は、サポートされているウェブサーバの背後で実行されているアプリケーションがＳＳＯに参加することを可能にする。

【００３９】

一実施形態は、ＳＳＯおよびクラウドＳＳＯ機能を提供する。多くの組織において、オンプレミスＩＡＭおよびＩＤＣＳいずれにおいても一般的なエントリポイントはＳＳＯである。クラウドＳＳＯは、ユーザが、１回のユーザサイン・インで複数のクラウドリソースにアクセスできるようにする。組織はそのオンプレミスアイデンティティの連携を希望することが多い。したがって、実施形態は、オープン標準を利用することで、既存のＳＳＯとの統合を実現することにより、投資の節約と拡大を可能にする（たとえば、アイデンティティクラウドサービス手法への最終的な完全移行まで）。

【００４０】

一実施形態は以下の機能を提供し得る。

・アイデンティティストアを維持することにより、既に認可されているユーザアカウント、所有権、アクセス、および許可を追跡する。
・ワークフローとの統合により、アプリケーションのアクセスに必要なさまざまな承認（たとえば管理、ＩＴ、人的資源、法律、およびコンプライアンス）を簡単にする。
・選択的装置（たとえばモバイルおよびパーソナルコンピュータ（「ＰＣ」））に対するＳａａＳユーザアカウントをプロビジョニングする。ユーザポータルへのアクセスは、多数のプライベートおよびパブリッククラウドリソースを含む。
・規則および現在の職責へのコンプライアンスのための定期的な管理立証を容易にする。

【００４１】

これらの機能に加えて、実施形態はさらに、

・クラウドアプリケーションにおけるアカウントライフサイクルの管理のためのクラウドアカウントのプロビジョニング、
・よりロバストなマルチファクタ認証（multifactor authentication）（「ＭＦＡ」）の統合、
・拡張モバイルセキュリティ機能、および
・動的認証オプション

を提供し得る。

【００４２】

一実施形態は、適応認証およびＭＦＡを提供する。一般的に、パスワードおよび確認のための質問は、不十分でありフィッシングなどのよくある攻撃に晒され易いとみなされてきた。現代の大半の企業体は、リスクを下げるために何らかの形態のＭＦＡに注目している。しかしながら、ソリューションが首尾よくデプロイされるためには、ソリューションをエンドユーザが簡単にプロビジョニング、維持、および理解する必要がある。なぜなら、エンドユーザは通常、そのデジタル体験を妨害するものに対し、それが何であろうと抵抗するからである。企業は、ＭＦＡを、シームレスなユーザアクセス体験のほぼトランスペアレントなコンポーネントにしつつ、私物の業務利用（bring your own device）（「ＢＹＯＤ」）、社会的アイデンティティ、遠隔ユーザ、顧客、および契約者を安全に組込む方法を探している。ＭＦＡのデプロイにおいて、ＯＡｕｔｈおよびＯｐｅｎＩＤ Ｃｏｎｎｅｃｔなどの産業標準は、既存のマルチファクタソリューションの統合と、より新しい適応認証技術の導入とを保証するのに不可欠である。したがって、実施形態は、動的（または適応）認証を、利用できる情報（すなわちＩＰアドレス、場所、時刻、およびバイオメトリクス）の評価として定義することにより、ユーザセッション開始後のアイデンティを証明する。適切な標準（たとえばオープン認証（open authentication）（「ＯＡＴＨ」）および高速オンライン認証（fast identity online）（「ＦＩＤＯ」）の統合と、拡張可能なアイデンティティ管理フレームワークとを用いて、実施形態は、エンド・ツー・エンドの安全なＩＡＭデプロイの一部としてＩＴ組織内で簡単に採用、アップグレード、および統合できるＭＦＡソリューションを提供する。ＭＦＡおよび適応ポリシーを検討する場合、組織は、ハイブリッドのＩＤＣＳおよびオンプレミスＩＡＭ環境においてシステム間の統合を必要とするオンプレミスリソースおよびクラウドリソースにわたって一貫したポリシーを実現しなければならない。

【００４３】

一実施形態は、ユーザプロビジョニングおよび証明を提供する。一般的に、ＩＡＭソリューションの基本機能は、ユーザプロビジョニングライフサイクル全体を可能にしかつサポートすることである。これは、ユーザに対し、組織内におけるそのアイデンティティおよびロール（role）に適したアプリケーションアクセスを与えること（たとえば、ユーザのロールまたはそのロールの中で使用されるタスクもしくはアプリケーションは時間の経過に伴って変化するので）と、ユーザが組織から脱退するときに必要な、素早いユーザデプロビジョニングとを含む。これは、さまざまなコンプライアンス条件を満たすために重要であるだけでなく、不適切なインサイダーアクセスがセキュリティ侵害および攻撃の主要な原因であるので、重要である。アイデンティティクラウドソリューションにおける、自動化されたユーザプロビジョニング機能は、それ自身の権利において重要になり得るだけでなく、ハイブリッドＩＡＭソリューションの一部としても重要であり、したがって、ＩＤＣＳプロビジョニングは、企業が縮小、拡大、合併する、または既存のシステムをＩａａＳ／ＰａａＳ／ＳａａＳ環境と統合しようとする場合、移行時において、オンプレミスソリューションよりも高い柔軟性を提供し得る。ＩＤＣＳ手法は、一度限りのアップグレードにおいて時間と労力を節約することができ、必要な部門、事業部、およびシステムの適切な統合を保証する。企業ではこの技術をスケーリングする必要性が密かに発生することが多く、企業体系全体にスケーラブルなＩＤＣＳ機能を迅速に提供することは、柔軟性、コスト、および制御の点で利益をもたらし得る。

【００４４】

一般的に、被雇用者は、長年にわたり、職種の変化に応じて追加の権限が付与される（すなわち「権限のクリープ」）。規制が緩やかな企業は一般的に「立証」プロセスが欠落している。このプロセスは、企業の被雇用者の権限（たとえばネットワーク、サーバ、アプリケーション、およびデータへのアクセス権）を定期的に監査して、過剰な権限が付与されたアカウントの原因となる権限のクリープを止めるまたは減速させる管理者を必要とする。したがって、一実施形態は、定期的に実施される（少なくとも１年に一度）立証プロセスを提供し得る。さらに、合併および買収に伴い、これらのツールおよびサービスの必要性は急激に増す。ユーザが、ＳａａＳシステムに存在する、オンプレミス上に存在す

る、異なる部門にまたがっている、および／またはデプロビジョニングされているもしくは再度割り当てられているからである。クラウドへの動きはこの状況をさらに混乱させる可能性があり、事態は、既存の手動管理されることが多い証明方法を超えて急速にエスカレートする可能性がある。したがって、一実施形態は、これらの機能を自動化し、高度な分析を、ユーザプロファイル、アクセス履歴、プロビジョニング／デプロビジョニング、および細分化された権利に適用する。

【００４５】

一実施形態はアイデンティティ分析を提供する。一般的に、アイデンティティ分析を、包括的な証明および立証のためにＩＡＭエンジンと統合する機能は、組織のリスクプロファイルを安全にするためには不可欠となる可能性がある。適切にデプロイされたアイデンティティ分析は、内部ポリシー全体の施行を要求する可能性がある。クラウドおよびオンプレミス全体で統一された単一管理ビューを提供するアイデンティティ分析は、予防的ガバナンス、リスク、およびコンプライアンス（governance, risk, and compliance）（「ＧＲＣ」）企業環境における必要性が高く、リスクを低減しコンプライアンス規則を満たすための閉ループプロセスを提供するのに役立ち得る。したがって、一実施形態はアイデンティティ分析を提供する。アイデンティティ分析は、管理者、幹部職員、および監査役が必要とするレポートおよび分析のために、クライアントが簡単にカスタマイズすることで特定の産業条件および政府規則に適合する。

【００４６】

一実施形態は、セルフサービスおよびアクセス要求機能を提供することにより、エンドユーザの体験および効率を改善するとともに、ヘルプデスクコールに要するコストを低減する。一般的に、多数の企業はその従業員のためにオンプレミスのセルフサービスアクセス要求をデプロイするが、多くは、これらのシステムを正式な企業の壁の外側まで適切に拡張していない。従業員の用途の範囲外の、ポジティブなデジタル顧客体験が、ビジネスの信頼性を高め最終的には収入の増加に貢献し、企業は、顧客ヘルプデスクコールを減じるだけでなく顧客の満足度を高める。したがって、一実施形態は、オープン標準に基づいておりかつ必要に応じて既存のアクセス制御ソフトウェアおよびＭＦＡメカニズムとシームレスに統合される、アイデンティティクラウドサービス環境を提供する。ＳａａＳ配信モデルは、以前はシステムのアップグレードおよびメンテナンスに費やされていた時間と労力を省き、ＩＴ専門スタッフを解放してより中心的なビジネスアプリケーションに集中できるようにする。

【００４７】

一実施形態は、特権アカウント管理（privileged account management）（「ＰＡＭ」）を提供する。一般的に、すべての組織は、ＳａａＳ、ＰａａＳ、ＩａａＳまたはオンプレミスアプリケーションいずれを使用しても、システムアドミニストレータ、幹部職員、人事担当役員、契約者、システムインテグレータなどのスーパーユーザのアクセスクレデンシャルを用いたインサイダーによる特権アカウントの不正使用に弱い。加えて、外部の脅威は一般的に、先ず低レベルユーザアカウントを侵害し、最終的には企業システム内の特権ユーザアクセス制御に到達してこれを利用する。したがって、一実施形態は、ＰＡＭを提供することにより、このような不正なインサイダーによるアカウントの使用を防止する。ＰＡＭソリューションの主要コンポーネントはパスワードボールト（password vault）であり、これはさまざまなやり方で供給し得る。たとえば、企業サーバ上にインストールされるソフトウェアとして、これも企業サーバ上の仮想アプライアンスとして、パッケージングされたハードウェア／ソフトウェアアプライアンスとして、または、クラウドサービスの一部として、さまざまなやり方で供給し得る。ＰＡＭ機能は、エンベロープ内で保持されサインインおよびサイン・アウトのためのマニフェストで定期的に変更されるパスワードを格納するために使用される物理的な安全場所と同様である。一実施形態は、パスワードのチェックアウトだけでなく、タイムリミットの設定、強制的な期間変更、自動的なチェックアウトの追跡、およびすべてのアクティビティに関する報告を、可能にする。一実施形態は、要求されたリソースに、ユーザがパスワードを知らない状態で、直接

接続する方法を提供する。この機能はまた、セッション管理およびその他の機能の方法に道を開く。

【００４８】

一般的に、ほとんどのクラウドサービスは、ＡＰＩおよび管理インターフェイスを利用している。これらは、侵入者がセキュリティを迂回する機会を与える。したがって、一実施形態は、ＰＡＭの実施におけるこれらの欠陥を埋める。クラウドへの移行によってＰＡＭに新たな課題が発生するからである。小規模から中規模の多くのビジネスは現在自身のＳａａＳシステム（たとえばOffice 365）を管理しているが、大企業は自身のＳａａＳおよびＩａａＳサービスの回転数を上げる個々のビジネス単位を持つことが増えている。これらの顧客は、ＰＡＭ機能がアイデンティティクラウドサービスソリューションに含まれるかまたはそのＩａａＳ／ＰａａＳプロバイダから得られるが、この責務を扱った経験がほとんどない。加えて、場合によっては、多くの異なる地理的に分散したビジネス単位が、同じＳａａＳアプリケーションの管理責任を分離しようとする。したがって、一実施形態は、こういった状況にある顧客が、既存のＰＡＭをアイデンティティクラウドサービスの全体的なアイデンティティフレームワークの中にリンクさせ、より高い安全性とコンプライアンスに向けて、ビジネスニーズが要求するクラウドロード条件に合わせて確実に調整することを、可能にする。

【００４９】

ＡＰＩプラットフォーム

実施形態が提供するＡＰＩプラットフォームは、機能のコレクションをサービスとしてエクスポーズする。ＡＰＩはマイクロサービスに集約され、各マイクロサービスは、ＡＰＩのうちの１つ以上をエクスポーズする。すなわち、各マイクロサービスは異なる種類のＡＰＩをエクスポーズし得る。一実施形態において、各マイクロサービスはそのＡＰＩを通してしか通信しない。一実施形態において、各ＡＰＩはマイクロサービスであってもよい。一実施形態において、複数のＡＰＩが１つのサービスに、このサービスが提供するターゲット機能に基づいて集約される（たとえばＯＡｕｔｈ、ＳＡＭＬ、Ａｄｍｉｎなど）。結果として、同様のＡＰＩは別々のランタイムプロセスとしてエクスポーズされない。ＡＰＩは、ＩＤＣＳが提供するサービスを使用するためにサービス消費者が利用できるようにされたものである。

【００５０】

一般的に、ＩＤＣＳのウェブ環境において、ＵＲＬは、３つの部分として、ホストと、マイクロサービスと、リソースとを含む（たとえばホスト／マイクロサービス／リソース）。一実施形態において、マイクロサービスは、特定のＵＲＬプレフィックスを有することを特徴とし（たとえば「host/oauth/v1」）、実際のマイクロサービスは「oauth/v1」である。「oauth/v1」の下で複数のＡＰＩが存在し、たとえば、トークン（token）を要求するためのＡＰＩ：「host/oauth/v1/token」、ユーザを認可する（authorize）ためのＡＰＩ：「host/oauth/v1/authorize」などである。すなわち、ＵＲＬはマイクロサービスを実現し、ＵＲＬのリソース部分はＡＰＩを実現する。したがって、同じマイクロサービスの下で複数のＡＰＩが集約される。一実施形態において、ＵＲＬのホスト部分はテナントを特定する（たとえば、https://tenant3.identity.oraclecloud.com:/oauth/v1/token）。

【００５１】

必要なエンドポイントを有する外部サービスと統合するアプリケーションを構成し当該構成を最新状態に保つことは、一般的に難題である。この難題を克服するために、実施形態は、パブリックディスカバリＡＰＩを周知の場所にエクスポーズし、そこから、アプリケーションは、ＡＤＣＳ　ＡＰＩを消費するために必要なＩＤＣＳに関する情報を発見する（discover）ことができる。一実施形態において、２つのディスカバリ文献がサポートされ、それらは、ＩＤＣＳ構成（たとえば、〈IDCS-URL〉/.well-known/idcs-configurationのＩＤＣＳ、ＳＡＭＬ、ＳＣＩＭ、ＯＡｕｔｈ、およびＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ構成を含む）と、（たとえば〈IDCS-URL〉/.well-known/openid-configuration

の）産業標準ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ構成とである。アプリケーションは、単一のＩＤＣＳ　ＵＲＬで構成されることにより、ディスカバリ文献を取り出すことができる。

【００５２】

図６は、一実施形態におけるＩＤＣＳのシステムビュー６００を提供するブロック部である。図６において、さまざまなアプリケーション／サービス６０２のうちのいずれも、ＩＤＣＳ　ＡＰＩに対してＨＴＴＰコールを行うことにより、ＩＤＣＳサービスを使用することができる。このようなアプリケーション／サービス６０２の例は、ウェブアプリケーション、ネイティブアプリケーション（たとえばWindows（登録商標）アプリケーション、ｉＯＳ（登録商標）アプリケーション、アンドロイド（登録商標）アプリケーションなど、特定のオペレーティングシステム上で走るように構築されたアプリケーション）、ウェブサービス、顧客アプリケーション、パートナーアプリケーション、または、サービスとしてのソフトウェア（Software as a Service）（「ＳａａＳ」）、ＰａａＳ、およびサービスとしてのインフラストラクチャ（Infrastructure as a Service）（「ＩａａＳ」）など、パブリッククラウドによって提供されるサービスである。

【００５３】

一実施形態において、ＩＤＣＳサービスを要求するアプリケーション／サービス６０２のＨＴＴＰ要求は、オラクルパブリッククラウドＢＩＧ－ＩＰアプライアンス６０４およびＩＤＣＳ　ＢＩＧ－ＩＰアプライアンス６０６（またはロードバランサなどの同様の技術、または、適切なセキュリティルールを実現してトラフィックを保護するサービスとしてのクラウドロードバランサ（Cloud Load Balancer as a Service）（「ＬＢａａＳ」）と呼ばれているコンポーネント）を通る。しかしながら、この要求はどのようなやり方で受信されてもよい。ＩＤＣＳ　ＢＩＧ－ＩＰアプライアンス６０６（または、適用できる場合は、ロードバランサまたはクラウドＬＢａａＳなどの同様の技術）において、クラウドプロビジョニングエンジン６０８は、テナントおよびサービスの調整を実行する。一実施形態において、クラウドプロビジョニングエンジン６０８は、クラウドにオンボードされている新たなテナントに対応付けられた内部セキュリティアーティファクト、または、顧客が購入した新たなサービスインスタンスを管理する。

【００５４】

このＨＴＴＰ要求は次にＩＤＣＳウェブルーティング層６１０によって受信される。このルーティング層は、セキュリティゲート（すなわちクラウドゲート）を実現し、サービスルーティングならびにマイクロサービス登録および発見６１２を提供する。要求されるサービスに応じて、ＨＴＴＰ要求は、ＩＤＣＳ中間層６１４のＩＤＣＳマイクロサービスに転送される。ＩＤＣＳマイクロサービスは、外部および内部ＨＴＴＰ要求を処理する。ＩＤＣＳマイクロサービスは、プラットフォームサービスおよびインフラストラクチャサービスを実現する。ＩＤＣＳプラットフォームサービスは、ＩＤＣＳのビジネスを実現する、別々にデプロイされたＪａｖａベースのランタイムサービスである。ＩＤＣＳインフラストラクチャサービスは、ＩＤＣＳに対してインフラストラクチャサポートを提供する、別々にデプロイされたランタイムサービスである。ＩＤＣＳはさらに、ＩＤＣＳサービスによって使用される共有ライブラリとしてパッケージングされた共通コードであるインフラストラクチャライブラリと、共有ライブラリとを含む。インフラストラクチャサービスおよびライブラリは、プラットフォームサービスがその機能を実現するために要求するサポート機能を提供する。

【００５５】

プラットフォームサービス

一実施形態において、ＩＤＣＳは標準認証プロトコルをサポートし、したがって、ＩＤＣＳマイクロサービスは、ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ、ＯＡｕｔｈ、ＳＡＭＬ２、クロスドメインアイデンティティ管理のためのシステム（System for Cross-domain Identity Management++：「ＳＣＩＭ＋＋」）などのプラットフォームサービスを含む。

【００５６】

ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔプラットフォームサービスは、標準ＯｐｅｎＩＤ　Ｃｏｎ

ｎｅｃｔログイン／ログアウトフローを実現する。対話型のウェブベースおよびネイティブアプリケーションは、標準のブラウザベースのＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔフローを推進することによりユーザ認証を要求し、ユーザの認証されたアイデンティティを伝達するＪａｖａＳｃｒｉｐｔ（登録商標）オブジェクト表記法（JavaScript Object Notation（「ＪＳＯＮ」）ウェブトークン（Web Token「ＪＷＴ」）である標準アイデンティティトークンを受信する。内部において、ランタイム認証モデルはステートレスであり、ユーザの認証／セッション状態をホストＨＴＴＰクッキー（ＪＷＴアイデンティティトークンを含む）の形態で維持する。ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔプロトコルを介して開始された認証対話は、ローカルおよび連携ログインのためにユーザのログイン／ログアウトセレモニーを実現する信頼できるＳＳＯサービスに委任される。この機能のさらなる詳細は以下において図１０および図１１を参照しながら開示される。一実施形態において、ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ機能は、たとえばＯｐｅｎＩＤ　Ｆｏｕｎｄａｔｉｏｎ標準に従って実現される。

【００５７】

ＯＡｕｔｈ２プラットフォームサービスは、トークン認可サービスを提供する。これは、ユーザの権利を伝達するアクセストークンを作成し検証してＡＰＩコールを行うためのリッチなＡＰＩインフラストラクチャを提供する。これは、ある範囲の有用なトークン付与タイプをサポートし、顧客がクライアントをそのサービスに安全に接続することを可能にする。これは、標準の２者間および３者間ＯＡｕｔｈ２トークン付与タイプを実現する。ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ（「ＯＩＤＣ」）をサポートすることにより、コンプライアントなアプリケーション（ＯＩＤＣリレーパーティ（「ＲＰ」））が、アイデンティティプロバイダとしてのＩＤＣＳと統合されることを可能にする（ＯＩＤＣ　ＯｐｅｎＩＤプロバイダ（「ＯＰ」）。同様に、ＯＩＤＣ　ＲＰとしてのＩＤＣＳをソーシャルＯＩＤＣ　ＯＰ（たとえばFacebook（登録商標）、Google（登録商標）など）と統合することにより、顧客は、アプリケーションに対する社会的アイデンティのポリシーベースアクセスを可能にする。一実施形態において、ＯＡｕｔｈ機能は、たとえば、インターネットエンジニアリングタスクフォース（Internet Engineering Task Force）（「ＩＥＴＦ」）、コメント要求（Request for Comments）（「ＲＦＣ」）６７４９に従って実現される。

【００５８】

ＳＡＭＬ２プラットフォームサービスは、アイデンティティ連携サービスを提供する。これは、顧客が、ＳＡＭＬアイデンティティプロバイダ（identity provider）（「ＩＤＰ」）およびＳＡＭＬサービスプロバイダ（service provider）（「ＳＰ」）関係モデルに基づいて、そのパートナーとの連携合意を設定することを可能にする。一実施形態において、ＳＡＭＬ２プラットフォームサービスは、標準ＳＡＭＬ２ブラウザポストログインおよびログアウトプロファイルを実現する。一実施形態において、ＳＡＭＬ機能は、たとえばＩＥＴＦ、ＲＦＣ７５２２に従って実現される。

【００５９】

ＳＣＩＭは、ユーザアイデンティ情報を、たとえばＩＥＴＦ、ＲＦＣ　７６４２、７６４３、７６４４によって提供される、アイデンティティドメインまたは情報技術（「ＩＴ」）システム間でのユーザアイデンティティ情報の交換を自動化するためのオープン標準である。ＳＣＩＭ＋＋プラットフォームサービスは、アイデンティティ管理サービスを提供し、顧客がＩＤＣＳのＩＤＰフィーチャー（feature）にアクセスすることを可能にする。管理サービスは、アイデンティティライフサイクル、パスワード管理、グループ管理などをカバーするステートレスなＲＥＳＴインターフェイス（すなわちＡＰＩ）のセットをエクスポーズし、ウェブアクセス可能なリソースのようなアーティファクトをエクスポーズする。

【００６０】

すべてのＩＤＣＳ構成アーティファクトはリソースであり、管理サービスのＡＰＩは、ＩＤＣＳリソース（たとえばユーザ、ロール、パスワードポリシー、アプリケーション、

ＳＡＭＬ／ＯＩＤＣアイデンティティプロバイダ、ＳＡＭＬサービスプロバイダ、キー、証明、通知テンプレートなど）の管理を可能にする。管理サービスは、ＳＣＩＭ標準を強化および拡張することにより、すべてのＩＤＣＳリソースに対する作成（Create）、読み取り（Read）、更新（Update）、削除（Delete）、および問合せ（Query）（「ＣＲＵＤＱ」）動作のためにスキーマベースのＲＥＳＴ　ＡＰＩを実現する。加えて、ＩＤＣＳ自体の管理および構成に使用されるＩＤＣＳのすべての内部リソースは、ＳＣＩＭベースのＲＥＳＴ　ＡＰＩとしてエクスポーズされる。アイデンティティストア６１８へのアクセスはＳＣＩＭ＋＋ＡＰＩに分離される。

【００６１】

一実施形態において、たとえば、ＳＣＩＭ標準は、ＳＣＩＭ規格によって規定されるユーザおよびグループリソースを管理するように実現されるのに対し、ＳＣＩＭ＋＋は、ＳＣＩＭ規格によって規定される言語を用いてさらに他のＩＤＣＳ内部リソース（たとえばパスワードポリシー、ロール、設定など）をサポートするように構成される。

【００６２】

管理サービスは、ＳＣＩＭ２．０標準エンドポイントを、標準ＳＣＩＭ２．０コアスキーマと、必要に応じてスキーマ拡張とを用いてサポートする。加えて、管理サービスは、いくつかのＳＣＩＭ２．０準拠エンドポイント拡張をサポートすることにより、その他のＩＤＣリソースを、たとえばユーザ、グループ、アプリケーション、設定などを、管理する。管理サービスはまた、ＣＲＵＤＱ動作は実行しないがその代わりに機能サービスを、たとえば「UserPasswordGenerator」、「UserPasswordValidator」などを提供する、リモートプロシージャコールスタイル（remote procedure call-style）（「ＲＰＣスタイル」）ＲＥＳＴインターフェイスのセットをサポートする。

【００６３】

ＩＤＣＳ管理ＡＰＩは、ＯＡｕｔｈ２プロトコルを認証および認可に使用する。ＩＤＣＳは、ウェブサーバ、モバイル、およびＪａｖａＳｃｒｉｐｔアプリケーションのためのシナリオといった共通のＯＡｕｔｈ２シナリオをサポートする。ＩＤＣＳ　ＡＰＩへのアクセスはアクセストークンによって保護される。ＩＤＣＳ管理ＡＰＩにアクセスするために、アプリケーションは、ＩＤＣＳ管理コンソールを通してＯＡｕｔｈ２クライアントとしてまたはＩＤＣＳアプリケーションとして（この場合ＯＡｕｔｈ２クライアントは自動的に作成される）登録される必要があり、また、所望のＩＤＣＳ管理ロールを与えられる必要がある。ＩＤＣＳ管理ＡＰＩコールを行うとき、アプリケーションは先ず、ＩＤＣＳＯＡｕｔｈ２サービスにアクセストークンを要求する。このトークンを取得した後に、このアプリケーションはアクセストークンを、そこにＨＴＴＰ認可ヘッダを含めて送信する。アプリケーションは、ＩＤＣＳ管理ＲＥＳＴ　ＡＰＩを直接使用することができる、または、ＩＤＣＳＪａｖａクライアントＡＰＩライブラリを使用することができる。

【００６４】

<u>インフラストラクチャサービス</u>

ＩＤＣＳインフラストラクチャサービスは、ＩＤＣＳプラットフォームサービスの機能をサポートする。これらのランタイムサービスは、（ユーザ通知、アプリケーション申込、およびデータベースに対する監査を非同期的に処理するための）イベント処理サービスと、（ジョブをスケジューリングして実行するため、たとえば、ユーザの介入が不要な長時間実行タスクを直ちに実行するまたは設定時間に実行するための）ジョブスケジューラサービスと、キャッシュ管理サービスと、（パブリッククラウドストレージサービスと統合するための）ストレージ管理サービスと、（レポートおよびダッシュボードを生成するための）レポートサービスと、（内部ユーザ認証およびＳＳＯを管理するための）ＳＳＯサービスと、（異なる種類のユーザインターフェイス（user interface）（「ＵＩ」）クライアントをホストするための）ユーザインターフェイス（「ＵＩ」）サービスと、サービスマネージャサービスとを含む。サービスマネージャは、オラクルパブリッククラウドとＩＤＣＳとの間の内部インターフェイスである。サービスマネージャは、オラクルパブリッククラウドによって発行されたコマンドを管理し、このコマンドはＩＤＣＳによって

実現される必要がある。たとえば、顧客が、何かを購入できる状態になる前にクラウドストア内のアカウントに対してサインアップした場合、クラウドは、テナントを作成することを依頼するための要求をＩＤＣＳに送信する。この場合、サービスマネージャは、ＩＤＣＳがサポートするとクラウドが予測するクラウド固有の動作を実現する。

【００６５】

ＩＤＣＳマイクロサービスは、ネットワークインターフェイスを通して別のＩＤＣＳマイクロサービスをコールしてもよい（すなわちＨＴＴＰ要求）。

【００６６】

一実施形態において、ＩＤＣＳはまた、データベーススキーマを使用できるようにするスキーマサービス（またはパーシステンス（persistence）サービス）を提供し得る。スキーマサービスは、データベーススキーマを管理する責任をＩＤＣＳに委任することを可能にする。したがって、ＩＤＣＳのユーザはデータベースを管理する必要がない。なぜなら、この機能を提供するＩＤＣＳサービスが存在するからである。たとえば、ユーザは、データベースを用いてテナントごとにスキーマをパーシストしてもよく、データベース内にスペースがなくなったときにはスキーマサービスが、ユーザがデータベースを自身で管理しなくてもよいように、別のデータベースを取得し上記空間を拡大するという機能を管理する。

【００６７】

ＩＤＣＳはさらに、ＩＤＣＳが必要とする／生成するデータリポジトリであるデータストアを含む。これは、（ユーザ、グループなどを格納する）アイデンティティストア６１８、（ＩＤＣＳが自身を構成するために使用する構成データを格納する）グローバルデータベース６２０、（テナントごとにスキーマを分離し顧客ごとに顧客データを格納する）オペレーショナルスキーマ６２２、（監査データを格納する）監査スキーマ６２４、（キャッシュされたオブジェクトを格納することにより実施速度を高める）キャッシングクラスタ６２６などを含む。内部および外部のすべてのＩＤＣＳコンシューマは、標準ベースのプロトコルに従ってアイデンティティサービスと統合される。これにより、ドメインネームシステム（domain name system）（「ＤＮＳ」）を用いて、どこに要求をルーティングすべきかを決定することができ、アプリケーションを消費することをアイデンティティサービスの内部実現を理解することから切離す。

【００６８】

<u>リアルタイムおよびニア・リアルタイムタスク</u>

ＩＤＣＳは、要求されたサービスのタスクを、同期リアルタイムタスクと非同期ニア・リアルタイムタスクとに分離する。リアルタイムタスクは、ユーザが進むのに必要なオペレーションのみを含む。一実施形態において、リアルタイムタスクは、最少の遅延で実行されるタスクであり、ニア・リアルタイムタスクは、バックグラウンドにおいて、ユーザが待つことなく実行されるタスクである。一実施形態において、リアルタイムタスクは、実質的に遅延なしでまたはごくわずかな遅延で実行されるタスクであり、ユーザには、ほぼ瞬時に実行されているように見えるタスクである。

【００６９】

リアルタイムタスクは、特定のアイデンティティサービスの主要なビジネス機能を実行する。たとえば、ログインサービスを要求するとき、アプリケーションは、メッセージを送信してユーザのクレデンシャルを認証しそれに対するセッションクッキーを取得する。ユーザが体験するのは、システムへのログインである。しかしながら、ユーザのログインに関しては、ユーザが誰であるかの検証、監査、通知の送信など、その他いくつかのタスクが実行されるであろう。したがって、クレデンシャルの検証は、ユーザがＨＴＴＰクッキーを与えられてセッションを開始するように、リアルタイムで実行されるタスクであるが、通知（たとえば電子メールを送信してアカウント作成を通知すること）、監査（たとえば追跡／記録）などに関連するタスクは、ユーザが最少の遅延で進むことができるよう非同期的で実行することができるニア・リアルタイムタスクである。

【００７０】

マイクロサービスを求めるＨＴＴＰ要求が受信されると、対応するリアルタイムタスクが中間層のマイクロサービスによって実行され、必ずしもリアルタイム処理を受けない演算ロジック／イベントなどの残りのニア・リアルタイムタスクは、メッセージキュー６２８にオフロードされる。メッセージキュー６２８は、配信および処理が保証された状態でスケーラビリティが高い非同期イベント管理システム６３０をサポートする。したがって、特定の挙動は、フロントエンドからバックエンドにプッシュされることにより、ＩＤＣＳが、応答時間のレイテンシを少なくすることにより、ハイレベルサービスを顧客に提供することを、可能にする。たとえば、ログインプロセスは、クレデンシャルの検証、ログレポートの提出、最後のログイン時間の更新などを含み得るが、これらのタスクは、メッセージキューにオフロードして、リアルタイムではなくニア・リアルタイムで実行することができる。

【００７１】

一例において、システムが新たなユーザを登録または作成する必要がある場合がある。システムは、ＩＤＣＳ　ＳＣＩＭ　ＡＰＩをコールしてユーザを作成する。最終結果として、ユーザがアイデンティティストア６１８において作成されたときにこのユーザがそのパスワードをリセットするためのリンクを含む通知電子メールを得る。ＩＤＣＳが、新たなユーザを登録または作成することを求める要求を受けると、対応するマイクロサービスは、オペレーショナルデータベース（図６のグローバルデータベース６２０内に位置する）にある構成データに注目し、「ユーザ作成」という動作が「ユーザ作成」イベントでマーキングされていると判断する。この動作は、構成データにおいて非同期動作であることが識別される。マイクロサービスは、クライアントに戻り、ユーザの作成が正常に行われたことを示すが、通知電子メールの実際の送信は延期されバックエンドにプッシュされる。そうするために、マイクロサービスは、メッセージングＡＰＩ６１６を用いてこのメッセージを、ストアであるキュー６２８に入れる。

【００７２】

キュー６２８から出すために、インフラストラクチャマイクロサービスであるメッセージングマイクロサービスは、バックグラウンドにおいて継続的に実行され、キュー６２８の中にあるイベントを探してキュー６２８をスキャンする。キュー６２８の中にあるイベントは、監査、ユーザ通知、アプリケーション申込、データ解析などのイベントサブスクライバ６３０によって処理される。イベントによって示されるタスクに応じて、イベントサブスクライバ６３０は、たとえば、監査スキーマ６２４、ユーザ通知サービス６３４、アイデンティティイベントサブスクライバ６３２などと通信し得る。たとえば、メッセージングマイクロサービスは、キュー６２８の中に「ユーザ作成」イベントを発見した場合、対応する通知ロジックを実行し対応する電子メールをユーザに送信する。

【００７３】

一実施形態において、キュー６２８は、マイクロサービス６１４によってパブリッシュされたオペレーショナルイベントと、ＩＤＣＳリソースを管理するＡＰＩ６１６によってパブリッシュされたリソースイベントとをキューの中に入れる。

【００７４】

ＩＤＣＳは、リアルタイムキャッシング構造を用いてシステムパフォーマンスおよびユーザ体験を向上させる。キャッシュそのものは、マイクロサービスとしても提供される。ＩＤＣＳは、ＩＤＣＳによってサポートされている顧客の数の増加に伴って増大するエラスティック・キャッシュクラスタ６２６を実現する。キャッシュクラスタ６２６は、以下でより詳細に開示される分散型データグリッドで実現されてもよい。一実施形態において、書込専用リソースがキャッシュをバイパスする。

【００７５】

一実施形態において、ＩＤＣＳランタイムコンポーネントは、ヘルスおよびオペレーショナルメトリクスを、オラクル社のオラクルパブリッククラウドなどのパブリッククラウドのこのようなメトリクスを収集するパブリッククラウドモニタリングモジュール６３６に対してパブリッシュする。

【００７６】
一実施形態において、ＩＤＣＳを用いてユーザを作成してもよい。たとえば、クライアントアプリケーション６０２は、ＲＥＳＴ　ＡＰＩコールを発行してユーザを作成してもよい。管理サービス（６１４のプラットフォームサービス）は、このコールをユーザマネージャ（６１４のインフラストラクチャライブラリ／サービス）に委任する。そうすると、ユーザマネージャは、このユーザを、ＩＤストア６１８内の特定テナント用ＩＤストアストライプにおいて作成する。「ユーザ作成成功（User Create Success）」の場合、ユーザマネージャは、オペレーションを監査することにより監査スキーマ６２４内のテーブルを監査し、メッセージキュー６２８に対して「identity.user.create.success」をパブリッシュする。アイデンティティサブスクライバ６３２は、このイベントをピックアップし、新たに作成されたログイン詳細を含む「ウェルカム」電子メールを、新たに作成されたユーザに送信する。

【００７７】
一実施形態において、ＩＤＣＳを用いてロールをユーザに与えて、その結果ユーザがアクションをプロビジョニングしてもよい。たとえば、クライアントアプリケーション６０２は、ＲＥＳＴ　ＡＰＩコールを発行してユーザにロールを付与してもよい。管理サービス（６１４のプラットフォームサービス）は、このコールをロールマネージャ（６１４のインフラストラクチャライブラリ／サービス）に委任してもよい。このロールマネージャは、ＩＤストア６１８内の特定テナント用ＩＤストアストライプにおけるロールを付与する。「ロール付与成功（Role Grant Success）」の場合、ロールマネージャは、監査スキーマ６２４における監査テーブルに対するオペレーションを監査し、メッセージキュー６２８に対して「identity.user.role.grant.success」をパブリッシュする。アイデンティティサブスクライバ６３２は、このイベントをピックアップしプロビジョニング付与ポリシーを評価する。付与されているロールに対するアクティブなアプリケーション付与があった場合、プロビジョニングサブスクライバは、何らかの検証を実行し、アカウント作成を開始し、ターゲットシステムをコールアウトし、ターゲットシステムにアカウントを作成し、アカウント作成が成功したとマーキングする。これらの機能各々の結果として、「prov.account.create.initiate」、「prov.target.create.initiate」、「prov.target.create.success」または「prov.account.create.success」などの対応するイベントがパブリッシュされることになり得る。これらのイベントは、直近Ｎ日間でターゲットシステムにおいて作成されたアカウントの数を合計する自身のビジネスメトリクスを有し得る。

【００７８】
一実施形態において、ＩＤＣＳはユーザのログインのために使用することができる。たとえば、クライアントアプリケーション６０２は、サポートされている認証フローのうちの１つを用いてユーザのログインを要求してもよい。ＩＤＣＳは、ユーザを認証し、成功すると、監査スキーマ６２４における監査テーブルに対するオペレーションを監査する。失敗すると、ＩＤＣＳは、監査スキーマ６２４における失敗を監査し、メッセージキュー６２８の「login.user.login.failure」イベントをパブリッシュする。ログインサブスクライバは、このイベントをピックアップし、ユーザに対するそのメトリクスを更新し、ユーザのアクセス履歴についての追加分析を実行する必要があるか否かを判断する。

【００７９】
したがって、「制御の反転」機能を実現する（たとえば実行の流れを変更することにより、後の時点におけるオペレーションの実行を、当該オペレーションが別のシステムの支配下になるように、スケジュールする）ことにより、実施形態は、その他のイベントキューおよびサブスクライバを動的に追加して、小さなユーザサンプルに対する新たな特徴を、より広いユーザベースにデプロイする前にテストする、または、特定の内部または外部の顧客のための特定のイベントを処理することができる。

【００８０】
ステートレス機能

ＩＤＣＳマイクロサービスはステートレスである。これは、マイクロサービスそのものはステートを保持しないことを意味する。「ステート」とは、アプリケーションがその機能を果たすために使用するデータのことを言う。ＩＤＣＳは、マルチテナント機能を、すべてのステートを、ＩＤＣＳデータ層内の特定テナント向けリポジトリにパーシストすることによって提供する。中間層（すなわち要求を処理するコード）は、アプリケーションコードと同じ場所に格納されているデータを有しない。したがって、ＩＤＣＳは横方向および縦方向双方においてスケーラビリティが高い。

【００８１】

縦方向のスケーリング（またはスケールアップ／ダウン）は、システム内の１つのノードにリソースを追加する（またはこのノードからリソースを削除する）ことを意味し、１つのコンピュータにＣＰＵまたはメモリを追加することを伴うのが一般的である。縦方向のスケーラビリティによって、アプリケーションはそのハードウェアの限界までスケールアップすることができる。横方向のスケーリング（またはスケールアウト／イン）は、新たなコンピュータを分散型ソフトウェアアプリケーションに追加するといったように、より多くのノードをシステムに追加する（またはシステムからノードを削除する）ことを意味する。横方向のスケーラビリティにより、アプリケーションはほぼ無限にスケーリング可能であり、ネットワークによって提供される帯域幅の量のみの制約を受ける。

【００８２】

ＩＤＣＳの中間層がステートレスであることにより、ＣＰＵをさらに追加するだけで横方向にスケーラブルになり、アプリケーションの仕事を実行するＩＤＣＳコンポーネントは、特定なアプリケーションが走っている指定された物理的インフラストラクチャを持つ必要がない。ＩＤＣＳの中間層がステートレスであることにより、非常に多くの顧客／テナントにアイデンティティサービスを提供しているときであっても、ＩＤＣＳの可用性が高くなる。ＩＤＣＳアプリケーション／サービスを通る各パスは、専らアプリケーショントランザクションを実行するためにＣＰＵ用途に集中するが、データの格納にハードウェアを使用しない。スケーリングは、必要に応じてより多くのコピーを追加できるパーシステンス層にトランザクション用のデータが格納される一方で、アプリケーションが走っているときにより多くのスライスを追加することによって実現される。

【００８３】

ＩＤＣＳウェブ層、中間層、およびデータ層は各々独立してかつ別々にスケーリング可能である。ウェブ層をスケーリングすることにより、より多くのＨＴＴＰ要求を扱うことができる。中間層をスケーリングすることにより、より多くのサービス機能をサポートすることができる。データ層をスケーリングすることにより、より多くのテナントをサポートすることができる。

【００８４】

ＩＤＣＳ機能ビュー

図６Ａは、一実施形態におけるＩＤＣＳの機能ビューのブロック図の一例６００ｂである。ブロック図６００ｂにおいて、ＩＤＣＳ機能スタックは、サービスと、共有ライブラリと、データストアとを含む。サービスは、ＩＤＣＳプラットフォームサービス６４０ｂと、ＩＤＣＳプレミアムサービス６５０ｂと、ＩＤＣＳインフラストラクチャサービス６６２ｂとを含む。一実施形態において、ＩＤＣＳプラットフォームサービス６４０ｂおよびＩＤＣＳプレミアムサービス６５０ｂは、別々にデプロイされたＪａｖａベースのランタイムサービスであり、ＩＤＣＳのビジネスを実現する。ＩＤＣＳインフラストラクチャサービス６６２ｂは、別々にデプロイされたランタイムサービスであり、ＩＤＣＳに対するインフラストラクチャサポートを提供する。共有ライブラリは、ＩＤＣＳサービスによって使用される共有ライブラリとしてパッケージングされた共通コードであるＩＤＣＳインフラストラクチャライブラリ６８０ｂと、共有ライブラリとを含む。データストアは、ＩＤＣＳが必要とする／生成するデータリポジトリであり、アイデンティティストア６９８ｂ、グローバル構成７００ｂ、メッセージストア７０２ｂ、グローバルテナント７０４ｂ、パーソナライゼーション設定７０６ｂ、リソース７０８ｂ、ユーザー時データ７１０

ｂ、システム一時データ７１２ｂ、テナントごとのスキーマ（管理されたＥｘａＤａｔａ）７１４ｂ、オペレーショナルストア（図示せず）、キャッシングストア（図示せず）などを含む。

【００８５】

一実施形態において、ＩＤＣＳプラットフォームサービス６４０ｂは、たとえばＯｐｅｎＩＤ Ｃｏｎｎｅｃｔサービス６４２ｂ、ＯＡｕｔｈ２サービス６４４ｂ、ＳＡＭＬ２サービス６４６ｂ、およびＳＣＩＭ＋＋サービス６４８ｂを含む。一実施形態において、ＩＤＣＳプレミアムサービスは、たとえば、クラウドＳＳＯおよびガバナンス６５２ｂ、企業ガバナンス６５４ｂ、ＡｕｔｈＮブローカー６５６ｂ、連携ブローカー６５８ｂ、およびプライベートアカウント管理６６０ｂを含む。

【００８６】

ＩＤＣＳインフラストラクチャサービス６６２ｂおよびＩＤＣＳインフラストラクチャライブラリ６８０ｂは、ＩＤＣＳプラットフォームサービス６４０ｂがその仕事を実行するのに必要とする機能のサポートを提供する。一実施形態において、ＩＤＣＳインフラストラクチャサービス６６２ｂは、ジョブスケジューラ６６４ｂ、ＵＩ６６６ｂ、ＳＳＯ６６８ｂ、レポート６７０ｂ、キャッシュ６７２ｂ、ストレージ６７４ｂ、サービスマネージャ６７６ｂ（パブリッククラウド制御）、およびイベントプロセッサ６７８ｂ（ユーザ通知、アプリケーション申込、監査、データ解析）を含む。一実施形態において、ＩＤＣＳインフラストラクチャライブラリ６８０ｂは、データマネージャＡＰＩ６８２ｂ、イベントＡＰＩ６８４ｂ、ストレージＡＰＩ６８６ｂ、認証ＡＰＩ６８８ｂ、認可ＡＰＩ６９０ｂ、クッキーＡＰＩ６９２ｂ、キーＡＰＩ６９４ｂ、およびクレデンシャルＡＰＩ６９６ｂを含む。一実施形態において、クラウド計算サービス６０２ｂ（内部Nimbula）は、ＩＤＣＳインフラストラクチャサービス６６２ｂおよびＩＤＣＳインフラストラクチャライブラリ６８０ｂの機能をサポートする。

【００８７】

一実施形態において、ＩＤＣＳは、顧客エンドユーザＵＩ６０４ｂ、顧客管理ＵＩ６０６ｂ、ＤｅｖＯｐｓ管理ＵＩ６０８ｂ、およびログインＵＩ６１０ｂなど、ＩＤＣＳサービスのコンシューマのためのさまざまなＵＩ６０２ｂを提供する。一実施形態において、ＩＤＣＳは、アプリケーション（たとえば顧客アプリケーション６１４ｂ、パートナーアプリケーション６１６ｂ、およびクラウドアプリケーション６１８ｂ）の統合６１２ｂならびにファームウェア統合６２０ｂを可能にする。一実施形態において、さまざまな環境がＩＤＣＳと統合されてそのアクセス制御のニーズをサポートしてもよい。このような統合は、たとえば、アイデンティティブリッジ６２２ｂ（ＡＤ統合、ＷＮＡ、およびＳＣＩＭコネクタを提供）、アパッチエージェント６２４ｂ、またはＭＳＦＴエージェント６２６ｂによって提供される。

【００８８】

一実施形態において、内部および外部のＩＤＣＳコンシューマは、ＯｐｅｎＩＤ Ｃｏｎｎｅｃｔ６３０ｂ、ＯＡｕｔｈ２ ６３２ｂ、ＳＡＭＬ２ ６３４ｂ、ＳＣＩＭ６３６ｂ、およびＲＥＳＴ／ＨＴＴＰ６３８ｂなどの標準ベースのプロトコル６２８ｂに対するＩＤＣＳのアイデンティティサービスと統合される。これにより、ドメインネームシステム（domain name system）（「ＤＮＳ」）を用いて、要求をどこにルーティングするかを判断することができ、アプリケーションの消費を、アイデンティティサービスの内部実現を理解することから切離す。

【００８９】

図６ＡのＩＤＣＳ機能ビューはさらに、ＩＤＣＳが、ユーザ通知（クラウド通知サービス７１８ｂ）、ファイルストレージ（クラウドストレージサービス７１６ｂ）、およびＤｅｖＯＰｓのためのメトリクス／警告（クラウドモニタサービス（ＥＭ）７２２ｂおよびクラウドメトリクスサービス（グラファイト）７２０ｂ）のために依存する共通機能を提供する、パブリッククラウドインフラストラクチャサービスを含む。

【００９０】

クラウドゲート

一実施形態において、ＩＤＣＳはウェブ層において「クラウドゲート」を実現する。クラウドゲートは、ウェブアプリケーションがユーザＳＳＯをアイデンティティ管理システム（たとえばＩＤＣＳ）に外部化することを可能にするウェブサーバプラグインであり、これは、企業ＩＤＭスタックと協力するＷｅｂＧａｔｅまたは Ｗｅｂ Ａｇｅｎｔ技術と同様である。クラウドゲートは、ＩＤＣＳ　ＡＰＩに対するアクセスを安全にするセキュリティゲートキーパの役割を果たす。一実施形態において、クラウドゲートは、ＯＡｕｔｈに基づいてＨＴＴＰリソースを保護するためにウェブポリシー施行点（Policy Enforcement Point）（「ＰＥＰ」）を提供するウェブ／プロキシサーバプラグインによって実現される。

【００９１】

図７は、クラウドゲート７０２を実現する実施形態のブロック図７００である。クラウドゲート７０２は、ウェブサーバ７１２内で実行され、ポリシー施行点（「ＰＥＰ」）の役割を果たす。ポリシー施行点は、オープン標準（たとえばＯＡｕｔｈ２、ＯｐｅｎＩＤ Ｃｏｎｎｅｃｔなど）を用いるＩＤＣＳポリシー決定点（Policy Decision Point）（「ＰＤＰ」）と統合され、一方でウェブブラウザおよびアプリケーションのＲＥＳＴ　ＡＰＩリソース７１４へのアクセスを安全にするように構成されている。いくつかの実施形態において、ＰＤＰは、ＯＡｕｔｈおよび／またはＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔマイクロサービス７０４で実現される。たとえば、ユーザブラウザ７０６がユーザ７１０のログインを求める要求をＩＤＣＳに送信すると、対応するＩＤＣＳ　ＰＤＰは、クレデンシャルを検証した後に、このクレデンシャルが十分であるか否か（たとえば第２のパスワードなどのその他のクレデンシャルを要求するか否か）を判断する。図７の実施形態において、クラウドゲート７０２は、ローカルポリシーを有するので、ＰＥＰとしてもＰＤＰとしてもその役割を果たし得る。

【００９２】

ワンタイム・デプロイメントの一部として、クラウドゲート７０２には、ＯＡｕｔｈ２クライアントとしてのＩＤＣＳが登録され、これが、ＩＤＣＳに対してＯＩＤＣおよびＯＡｕｔｈ２オペレーションを要求することを可能にする。その後、これは、要求マッチングルール（ＵＲＬをたとえばワイルドカード、通常表現などに対して如何にしてマッチングするか）の適用を受ける、アプリケーションの保護されたリソースおよび保護されていないリソースに関する構成情報を保持する。クラウドゲート７０２をデプロイすることにより、異なるセキュリティポリシーを有する異なるアプリケーションを保護することができ、保護されるアプリケーションはマルチテナントであってもよい。

【００９３】

ブラウザベースのユーザアクセス中、クラウドゲート７０２は、ユーザ認証フローを開始するＯＩＤＣ　ＲＰ７１８として機能する。ユーザ７１０が有効なローカルユーザセッションを有していない場合、クラウドゲート７０２は、ユーザをＳＳＯマイクロサービスにリダイレクトし、ＳＳＯマイクロサービスとともにＯＩＤＣ「認証コード」フローに参加する。このフローは、アイデンティティトークンとしてのＪＷＴの配信で終了する。クラウドゲート７０８は、ＪＷＴを検証し（たとえば署名、満了、宛先／オーディエンスなどに注目し）、ユーザ７１０に関するローカルセッションクッキーを発行する。これは、保護されているリソースへのウェブブラウザのアクセスを安全にしかつローカルセッションクッキーを発行、更新、および検証するセッションマネージャ７１６として機能する。これはまた、そのローカルセッションクッキーの削除のためのログアウトＵＲＬを提供する。

【００９４】

クラウドゲート７０２はまた、ＨＴＴＰベーシックＡｕｔｈ認証者の役割を果たし、ＩＤＣＳに対するＨＴＴＰベーシックＡｕｔｈクレデンシャルを検証する。この行動は、セッションレスおよびセッションベースの（ローカルセッションクッキー）モードでサポートされる。この場合、サーバ側ＩＤＣＳセッションは生成されない。

【００９５】
ＲＥＳＴ　ＡＰＩクライアント７０８によるプログラムアクセス中、クラウドゲート７０２は、アプリケーションの保護されているＲＥＳＴ　ＡＰＩ７１４のためのＯＡｕｔｈ２リソースサーバ／フィラー７２０の役割を果たし得る。これは、認証ヘッダおよびアクセストークンに対して要求が存在するか否かを検査する。クライアント７０８（たとえばモバイル、ウェブアプリケーション、ＪａｖａＳｃｒｉｐｔなど）が（ＩＤＣＳによって発行された）アクセストークンを、保護されているＲＥＳＴ　ＡＰＩ７１４とともに使用するために示すと、クラウドゲート７０２は、ＡＰＩへのアクセスを許可する前にアクセストークンを検証する（たとえば署名、満了、オーディエンスなど）。元のアクセストークンは修正なしで送られる。

【００９６】
一般的に、ＯＡｕｔｈを用いてクライアントアイデンティティ伝播トークン（たとえばクライアントが誰であるかを示す）またはユーザアイデンティティ伝播トークン（たとえばユーザが誰であるかを示す）を生成する。本実施形態において、クラウドゲートにおけるＯＡｕｔｈの実現は、たとえばＩＥＴＦ、ＲＦＣ７５１９によって提供されるようなウェブトークンのフォーマットを定めるＪＷＴに基づく。

【００９７】
ユーザがログインすると、ＪＷＴが発行される。ＪＷＴは、ＩＤＣＳによって署名され、ＩＤＣＳにおけるマルチテナント機能をサポートする。クラウドゲートは、ＩＤＣＳが発行したＪＷＴを検証することにより、ＩＤＣＳにおけるマルチテナント機能を可能にする。したがって、ＩＤＣＳは、物理構造においても、セキュリティモデルを支持する論理ビジネスプロセスにおいてもマルチテナンシーを提供する。

【００９８】
テナンシーの種類
ＩＤＣＳは３種類のテナンシーとして、顧客テナンシー、クライアントテナンシー、およびユーザテナンシーを特定する。顧客またはリソーステナンシーは、ＩＤＣＳの顧客が誰であるか（すなわち作業が誰に対して実行されているか）を特定する。クライアントテナンシーは、どのクライアントアプリケーションがデータにアクセスしようとしているか（すなわちどのアプリケーションが作業を実行しているか）を特定する。ユーザテナンシーは、どのユーザがアプリケーションを用いてデータにアクセスしているか（すなわち誰によって作業が実行されているか）を特定する。たとえば、専門サービス企業が大型ディスカウントショップを対象とするシステム統合機能を提供しこの大型ディスカウントショップのシステムのアイデンティティ管理を提供するためにＩＤＣＳを使用するとき、ユーザテナンシーは、この専門サービス企業に相当し、クライアントテナンシーはシステム統合機能を提供するために使用されるアプリケーションに相当し、顧客テナンシーは大型ディスカウントショップである。

【００９９】
これら３つのテナンシーを分離および統合することによってクラウドベースのサービスにおけるマルチテナント機能が可能になる。一般的に、オンプレミスの物理的なマシンにインストールされているオンプレミスソフトウェアの場合、これら３つのテナンシーを特定する必要はない。なぜなら、ユーザはログインするのに物理的にマシン上にいなければならないからである。しかしながら、クラウドベースのサービス構造の場合、実施形態は、トークンを持いて、誰がどのアプリケーションを使用してどのリソースにアクセスするかを判断する。３つのテナンシーは、トークンによってコーディファイ（codify）され、クラウドゲートによって施行され、中間層のビジネスサービスによって使用される。一実施形態において、ＯＡｕｔｈサーバがトークンを生成する。さまざまな実施形態において、このトークンは、ＯＡｕｔｈ以外のセキュリティプロトコルとともに使用されてもよい。

【０１００】
ユーザ、クライアント、およびリソーステナンシーを分離することにより、ＩＤＣＳが提供するサービスのユーザには実質的なビジネス上の利点が与えられる。たとえば、そう

することにより、ビジネス（たとえば健康ビジネス）のニーズおよびそのアイデンティティ管理の問題を理解するサービスプロバイダは、ＩＤＣＳが提供するサービスを購入し、ＩＤＣＳのサービスを消費する自身のバックエンドアプリケーションを開発し、このバックエンドアプリケーションをターゲットビジネスに提供することができる。したがって、サービスプロバイダは、ＩＤＣＳのサービスを拡張してその所望の機能を提供するとともにそれらを特定のターゲットビジネスに対して差出すことができる。サービスプロバイダは、ソフトウェアを構築し実行してアイデンティサービスを提供する必要はないが、その代わりに、ＩＤＣＳのサービスを拡張しカスタマイズしてターゲットビジネスのニーズに合うようにすることができる。

【０１０１】

周知のシステムの中には、顧客テナンシーである単一のテナンシーしか説明しないものがある。しかしながら、そのようなシステムは、顧客ユーザ、顧客のパートナー、顧客のクライアント、クライアント自身、または、アクセスが顧客から委任されたクライアントなどのユーザの組み合わせによるアクセスを処理するときには不十分である。本実施形態において複数のテナンシーを規定し施行することにより、これらの多様なユーザに対して管理機能を特定することが容易になる。

【０１０２】

一実施形態において、ＩＤＣＳの１エンティティは、複数のテナントに同時に属しているのではなく、１つのテナントのみに属し、「テナンシー」はアーティファクトが存在する場所である。一般的に、特定の機能を実現するコンポーネントは複数存在し、これらのコンポーネントは複数のテナントに属することが可能であるまたはインフラストラクチャに属することが可能である。インフラストラクチャは、テナントの代わりに機能する必要があるとき、テナントの代わりにエンティティサービスと対話する。この場合、インフラストラクチャそのものは自身のテナンシーを有し、顧客は自身のテナンシーを有する。要求がサブミットされたとき、この要求に関わる複数のテナンシーが存在する。

【０１０３】

たとえば、「テナント１」に属するクライアントが、「テナント３」におけるユーザを指定する「テナント２」のためのトークンを取得することを求める要求を実行する場合がある。別の例として、「テナント１」に存在するユーザが、「テナント２」が所有するアプリケーションにおけるアクションを実行する必要がある場合がある。よって、ユーザは、「テナント２」のリソースネームスペースに行きそのためのトークンを要求する必要がある。したがって、権限の委任は、「誰が」「何を」「誰」に対して行うことができるかを特定することによって実現される。もう１つの例として、第１の組織（「テナント１」）のために働く第１のユーザが、第２の組織（「テナント２」）のために働く第２のユーザが第３の組織（「テナント３」）がホストする文書にアクセスすることを、許可してもよい。

【０１０４】

一例において、「テナント１」のクライアントは、「テナント３」のアプリケーションにアクセスするために「テナント２」のユーザのためのアクセストークンを要求してもよい。クライアントは、「http://tenant3/oauth/token」に行きこのトークンを求めるＯＡｕｔｈ要求を呼び出すことによって当該トークンを要求してもよい。クライアントは、「クライアントアサーション」を要求に含めることにより、自身が「テナント１」に在住するクライアントであることを明らかにする。このクライアントアサーションは、クライアントＩＤ（たとえば「クライアント１」）とクライアントテナンシー（「テナント１」）とを含む。「テナント１」の「クライアント１」として、クライアントは、「テナント３」に対するトークンを求める要求を呼び出す権利を有し、「テナント２」のユーザのためのトークンを所望する。したがって、「ユーザアサーション」も同じＨＴＴＰ要求の一部として送られる。生成されるアクセストークンは、アプリケーションテナンシー（「テナント３」）であるターゲットテナンシーのコンテキストにおいて発行され、ユーザテナンシー（「テナント２」）を含む。

【０１０５】
一実施形態において、データ層における各テナントは、独立したストライプとして実現される。データ管理の観点からすると、アーティファクトはテナントに存在する。サービスの観点からすると、サービスは、異種のテナントとどのようにして協力するかを知っており、複数のテナンシーは、サービスのビジネス機能における異なるディメンションである。図８は、ある実施形態において複数のテナンシーを実現するシステムの一例８００を示す。システム８００はクライアント８０２を含み、クライアント８０２は、如何にしてデータベース８０６のデータ用いて作業するかを理解しているマイクロサービス８０４が提供するサービスを要求する。このデータベースは複数のテナント８０８を含み、各テナントは対応するテナンシーのアーティファクトを含む。一実施形態において、マイクロサービス８０４は、トークンを得ようとしてhttps://tenant3/oauth/tokenを通して要求されるＯＡｕｔｈマイクロサービスである。ＯＡｕｔｈマイクロサービスの機能が、マイクロサービス８０４において、データベース８０６からのデータを用いて実行されることにより、クライアント８０２の要求が正当であるか否かが検証され、正当である場合は、異なるテナンシー８０８からのデータが使用されてトークンが構成される。したがって、システム８００は、各テナンシーに与えられるサービスをサポートするだけでなく各種テナントに代わって機能し得るサービスをサポートすることによりクロステナント環境において作業できるという点において、マルチテナントである。

【０１０６】
システム８００は好都合である。理由は次の通りである。マイクロサービス８０４はデータベース８０６のデータから物理的に切離されており、クライアントにより近い場所を通ってデータを複製することにより、マイクロサービス８０４をクライアントに対するローカルサービスとして提供することができ、システム８００はサービスのアベイラビリティを管理しそれをグローバルに提供することができる。

【０１０７】
一実施形態において、マイクロサービス８０４はステートレスである。これは、マイクロサービス８０４を走らせるマシンが、特定のテナントに対するサービスを示すマーカを保持していないことを意味する。その代わりに、テナンシーは、たとえば、入ってくる要求のＵＲＬのホスト部分にマーキングされてもよい。このテナンシーはデータベース８０６のテナント８０８のうちの１つを示す。多数のテナント（たとえば何百万ものテナント）をサポートする場合、マイクロサービス８０４は、データベース８０６への同数の接続を有することはできない。マイクロサービス８０４はその代わりに、データベースユーザというコンテキストにおいてデータベース８０６への実際の物理接続を提供する接続プール８１０を使用する。

【０１０８】
一般的に、接続は、基礎をなすドライバまたはプロバイダに接続ストリングを提供することによって構築される。接続ストリングは、特定のデータベースまたはサーバをアドレス指定するために、かつ、インスタンスおよびユーザ認証クレデンシャルを与えるために使用される（たとえば「Server=sql_box;Database=Common;User ID=uid;Pwd=password;」）。接続は、一旦構築されると、開閉が可能であり、プロパティ（たとえばコマンドタイムアウト長さ、または存在するのであればトランザクション）を設定することができる。接続ストリングは、データプロバイダのデータアクセスインターフェイスによって指示されるキーと値とのペアのセットを含む。接続プールは、データベースに対する未来の要求が必要なときに接続を再使用できるように保持されるデータベース接続のキャッシュである。接続プーリングにおいて、接続は、作成後にプールに置かれ、新たな接続を確立しなくてもよいように、再使用される。たとえば、マイクロサービス８０４とデータベース８０８との間に１０の接続が必要な場合、接続プール８１０には、すべてデータベースユーザというコンテキストにおいて（たとえば特定のデータベースユーザに関連して、たとえば、誰がこの接続の所有者か、誰のクレデンシャルが検証中なのか、それはデータベースユーザか、それはシステムクレデンシャルかなどに関連して）開いている１０の

接続があるであろう。

【０１０９】

接続プール８１０内の接続は、何にでもアクセスできるシステムユーザのために作成される。したがって、テナントに代わって要求を処理するマイクロサービス８０４による監査および特権を正しく扱うために、データベース動作は、特定のテナントに割り当てられたスキーマ所有者に関連する「プロキシユーザ」８１２というコンテキストで実行される。このスキーマ所有者は、このスキーマ作成の目的であったテナンシーにのみアクセスでき、このテナンシーの値はこのスキーマ所有者の値である。データベース８０６内のデータを求める要求がなされると、マイクロサービス８０４は、接続プール８１０内の接続を用いてこのデータを提供する。したがって、マルチテナンシーは、リソーステナンシーに対応付けられたデータストアプロキシユーザというコンテキストにおいて（たとえばそれに関連して）作成されたデータ接続のトップにある要求ごとに構築された特定テナント向けデータストアバインディングというコンテキストにおいて（たとえばそれに関連して）入ってくる要求を処理するステートレスでエラスティックな中間層サービスを持つことによって得られ、データベースは、サービスとは無関係にスケーリングできる。

【０１１０】

以下は、プロキシユーザ８１２を実現するための機能の例を提供する。

【０１１１】

【数１】

```
dbOperation = <prepare DB command to execute>
dbConnection = getDBConnectionFromPool()
dbConnection.setProxyUser (resourceTenant)
result = dbConnection.executeOperation (dbOperation)
```

【０１１２】

この機能において、マイクロサービス８０４は、接続プール８１０内のデータベース接続を使用する一方で、接続プール８１０から引出された接続に対する「プロキシユーザ（Proxy User）」設定を、「テナント（Tenant）」にセットし、テナントというコンテキストにおいてデータオペレーションを実行する。

【０１１３】

すべてのテーブルをストライピングすることにより同じデータベースにおいて異なるテナント用に異なるコラムを構成するとき、１つのテーブルは、混合されたすべてのテナントのデータを含み得る。これに対し、一実施形態は、テナント駆動のデータ層を提供する。本実施形態は、異なるテナント用に同一データベースをストライピングするのではなく、テナントごとに異なる物理データベースを提供する。たとえば、マルチテナンシーは、プラガブルデータベース（たとえばオラクル社のOracle Database 12c）を用いて実現されてもよく、この場合、各テナントには別々のパーティションが割り当てられる。データ層では、リソースマネージャが要求を処理し、その後、その要求のデータソースを求める（メタデータとは別）。本実施形態は、要求ごとに各データソース／ストアへのランタイムスイッチを実行する。各テナントのデータをその他のテナントから分離することにより、本実施形態は改善されたデータセキュリティを提供する。

【０１１４】

一実施形態において、互いに異なるトークンは、異なるテナンシーをコーディファイする。ＵＲＬトークンは、サービスを要求するアプリケーションのテナンシーを特定し得る。アイデンティティトークンは、認証すべきユーザのアイデンティティをコーディファイし得る。アクセストークンは複数のテナンシーを特定し得る。たとえば、アクセストークンは、このようなアクセスのターゲットであるテナンシー（たとえばアプリケーションテナンシー）と、アクセス権が付与されたユーザのユーザテナンシーとをコーディファイし

得る。クライアントアサーショントークンは、クライアントＩＤおよびクライアントテナンシーを特定し得る。ユーザアサーショントークンは、ユーザおよびユーザテナンシーを特定し得る。

【０１１５】

一実施形態において、アイデンティティトークンは、少なくとも、ユーザテナント名（すなわちユーザが在住している場所）を示す「クレーム／ステートメント」を含む。認証トークンに関連する「クレーム」（セキュリティ分野の当業者が使用）は、ある主体が自身または別の主体に関して作成するステートメントである。ステートメントは、たとえば名称、アイデンティティ、キー、グループ、権限、または能力に関するものであってもよい。クレームは、プロバイダによって発行され、１つ以上の値が与えられた後に、セキュリティトークンサービス（security token service）（「ＳＴＳ」）として一般的に知られている発行者が発行したセキュリティトークンにパッケージングされる。

【０１１６】

一実施形態において、アクセストークンは、少なくとも、アクセストークンを求める要求がなされた時点のリソーステナント名（たとえば顧客）を示すクレーム／ステートメントと、ユーザテナント名を示すクレームと、要求しているＯＡｕｔｈクライアントの名称を示すクレームと、クライアントテナント名を示すクレームとを含む。一実施形態において、アクセストークンは、以下のＪＳＯＮ機能に従って実現されてもよい。

【０１１７】

【数２】

```
{
   ...
   " tok_type " : "AT",
   "user_id" : "testuser",
   "user_tenantname" : "<value-of-identity-tenant>"
   "tenant" : "<value-of-resource-tenant>"
   "client_id" : "testclient",
   "client_tenantname": "<value-of-client-tenant>"
  ...
}
```

【０１１８】

一実施形態において、クライアントアサーショントークンは、少なくとも、クライアントテナント名を示すクレームと、要求しているＯＡｕｔｈクライアントの名称を示すクレームとを含む。

【０１１９】

本明細書に記載のトークンおよび／または複数のテナンシーは、ＩＤＣＳ以外の任意のマルチテナントクラウドベースサービスによって実現されてもよい。たとえば、本明細書に記載のトークンおよび／または複数のテナンシーは、ＳａａＳまたは企業リソースプランニング（Enterprise Resource Planning）（「ＥＲＰ」）サービスにおいて実現されてもよい。

【０１２０】

図９は、一実施形態におけるＩＤＣＳのネットワークビュー９００のブロック図である。図９は、一実施形態においてアプリケーション「ゾーン」９０４間で行われるネットワーク対話を示す。アプリケーションは、要求される保護レベルと、その他さまざまなシステムへの接続の実現に基づいてゾーンに分割される（たとえばＳＳＬゾーン、ｎｏ　ＳＳＬゾーンなど）。アプリケーションゾーンのうち、いくつかはＩＤＣＳ内部からのアクセスを要するサービスを提供するアプリケーションゾーンであり、いくつかはＩＤＣＳ外部

からのアクセスを要するサービスを提供するアプリケーションゾーンであり、いくつかはオープンアクセスである。したがって、各保護レベルは各ゾーンに対して強化される。

【０１２１】

図９の実施形態において、サービス間の通信は、ＨＴＴＰ要求を用いて行われる。一実施形態において、ＩＤＣＳは、本明細書に記載のアクセストークンを用いて、サービスを提供するだけでなく、ＩＤＣＳへのアクセスおよびＩＤＣＳ自身の内部におけるアクセスを安全なものにする。一実施形態において、ＩＤＣＳマイクロサービスは、ＲＥＳＴｆｕｌインターフェイスを通してエクスポーズされ、本明細書に記載のトークンによって安全なものにされる。

【０１２２】

図９の実施形態において、さまざまなアプリケーション／サービス９０２のうちのいずれか１つが、ＩＤＣＳ　ＡＰＩに対してＨＴＴＰコールすることにより、ＩＤＣＳサービスを使用してもよい。一実施形態において、アプリケーション／サービス９０２のＨＴＴＰ要求は、オラクルパブリッククラウドロードバランシング外部仮想ＩＰアドレス（「ＶＩＰ」）９０６（またはその他同様の技術）、パブリッククラウドウェブルーティング層９０８、およびＩＤＣＳロードバランシング内部ＶＩＰアプライアンス９１０（またはその他同様の技術）を通って、ＩＤＣＳウェブルーティング層９１２により受信されてもよい。ＩＤＣＳウェブルーティング層９１２は、ＩＤＣＳの外部または内部からの要求を受信し、ＩＤＣＳプラットフォームサービス層９１４またはＩＤＣＳインフラストラクチャサービス層９１６を通してルーティングする。ＩＤＣＳプラットフォームサービス層９１４は、ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ、ＯＡｕｔｈ、ＳＡＭＬ，ＳＣＩＭなどのＩＤＣＳの外部から呼び出されたＩＤＣＳマイクロサービスを含む。ＩＤＣＳインフラストラクチャサービス層９１６は、その他のＩＤＣＳマイクロサービスの機能をサポートするためにＩＤＣＳの内部から呼び出されたサポートマイクロサービスを含む。ＩＤＣＳインフラストラクチャマイクロサービスの例は、ＵＩ、ＳＳＯ、レポート、キャッシュ、ジョブスケジューラ、サービスマネージャ、キーを作るための機能などである。ＩＤＣＳキャッシュ層９２６は、ＩＤＣＳプラットフォームサービス層９１４およびＩＤＣＳインフラストラクチャサービス層９１６のためのキャッシング機能をサポートする。

【０１２３】

ＩＤＣＳへの外部アクセスおよびＩＤＣＳ内部アクセス双方のセキュリティを強化することにより、ＩＤＣＳの顧客に、それが実行するアプリケーションのための傑出したセキュリティコンプライアンスを与えることができる。

【０１２４】

図９の実施形態において、構造化照会言語（Structured Query Language）（「ＳＱＬ」）に基づいて通信するデータ層９１８およびＬＤＡＰに基づいて通信するＩＤストア層９２０以外については、ＯＡｕｔｈプロトコルを使用することにより、ＩＤＣＳ内のＩＤＣＳコンポーネント（たとえばマイクロサービス）間の通信を保護し、ＩＤＣＳ外部からのアクセスを安全なものにするために使用される同じトークンをＩＤＣＳ内のセキュリティのためにも使用する。すなわち、ウェブルーティング層９１２は、要求がＩＤＣＳの外部から受けたものであろうとＩＤＣＳの内部から受けたものであろうと、受信した要求を処理するための同じトークンおよびプロトコルを使用する。したがって、ＩＤＣＳは、システム全体を保護するために１つの一貫したセキュリティモデルを提供することにより、傑出したセキュリティコンプライアンスを可能にする。なぜなら、システム内に実現されるセキュリティモデルが少ないほど、システムの安全性は高くなるからである。

【０１２５】

ＩＤＣＳクラウド環境において、アプリケーションは、ネットワークコールを行うことによって通信する。ネットワークコールは、ＨＴＴＰ、伝送制御プロトコル（Transmission Control Protocol）（「ＴＣＰ」）、ユーザデータグラムプロトコル（User Datagram Protocol）（「ＵＤＰ」）などの適用可能なネットワークプロトコルに基づいていればよい。たとえば、アプリケーション「Ｘ」は、アプリケーション「Ｙ」と、ＨＴＴＰに

基づいて、アプリケーション「Ｙ」をＨＴＴＰユニフォーム・リソース・ロケータ（Uniform Resource Locator）（「ＵＲＬ」）としてエクスポーズすることにより、通信し得る。一実施形態において、「Ｙ」は、各々がある機能に対応する多数のリソースをエクスポーズするＩＤＣＳマイクロサービスである。「Ｘ」（たとえば別のＩＤＣＳマイクロサービス）は、「Ｙ」をコールする必要があるとき、「Ｙ」と、呼び出す必要があるリソース／機能とを含むＵＲＬを構成し（たとえばhttps:/host/Y/resource）、ウェブルーティング層９１２を通って「Ｙ」に導かれる対応するＲＥＳＴコールを行う。

【０１２６】

一実施形態において、ＩＤＣＳ外部の呼出元は、「Ｙ」がどこにあるかを知る必要がない場合があるが、ウェブルーティング層９１２はアプリケーション「Ｙ」がどこで走っているかを知る必要がある。一実施形態において、ＩＤＣＳは、発見機能を実現する（ＯＡｕｔｈサービスによって実現される）ことにより、各アプリケーションがどこで走っているかを判断し、スタティックなルーティング情報の可用性が必要ではなくなるようにする。

【０１２７】

一実施形態において、企業マネージャ（enterprise manager）（「ＥＭ」）９２２は、オンプレミスおよびクラウドベース管理をＩＤＣＳに拡張する「一枚のガラス」を提供する。一実施形態において、Chef Software社の構成管理ツールである「シェフ（Chef）」サーバ９２４は、さまざまなＩＤＣＳ層のための構成管理機能を提供する。一実施形態において、サービスデプロイメントインフラストラクチャおよび／または永続格納モジュール９２８は、テナントライフサイクル管理動作、パブリッククラウドライフサイクル管理動作、またはその他の動作のために、ＯＡｕｔｈ２　ＨＴＴＰメッセージをＩＤＣＳウェブルーティング層９１２に送信してもよい。一実施形態において、ＩＤＣＳインフラストラクチャサービス層９１６は、ＩＤ／パスワードＨＴＴＰメッセージを、パブリッククラウド通知サービス９３０またはパブリッククラウドストレージサービス９３２に送信してもよい。

【０１２８】

<u>クラウドアクセス制御‐ＳＳＯ</u>

一実施形態は、クラウドスケールＳＳＯサービスを実現するために軽量クラウド標準をサポートする。軽量クラウド標準の例としては、ＨＴＴＰ、ＲＥＳＴ、および、ブラウザを通してアクセスを提供する標準（ウェブブラウザは軽量であるため）が挙げられる。逆に、ＳＯＡＰは、クライアントを構築するためにより多くの管理、構成、およびツールを必要とする重いクラウド標準の一例である。本実施形態は、アプリケーションのためにＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔセマンティックスを使用することにより、ＩＤＣＳに対してユーザ認証を要求する。本実施形態は、軽量ＨＴＴＰクッキーベースのユーザセッション追跡を用いて、ステートフルなサーバ側セッションサポートなしで、ＩＤＣＳにおけるユーザのアクティブなセッションを追跡する。本実施形態は、使用するアプリケーションに対して、認証されたアイデンティティを自身のローカルセッションに戻すマッピングを行うときに、ＪＷＴベースのアイデンティティトークンを使用する。本実施形態は、連携されているアイデンティティ管理システムとの統合をサポートし、ＩＤＣＳに対してユーザ認証を要求するために企業デプロイメントのＳＡＭＬ　ＩＤＰサポートをエクスポーズする。

【０１２９】

図１０は、一実施形態におけるＩＤＣＳ内のＳＳＯ機能のシステムアーキテクチャビューのブロック図１０００である。本実施形態は、クライアントアプリケーションが標準ベースのウェブプロトコルを推進してユーザ認証フローを開始することを可能にする。クラウドシステムとＳＳＯの統合を要求するアプリケーションは、企業データセンターにあってもよく、遠隔パートナーデータセンターにあってもよく、またはオンプレミスの顧客によって操作されてもよい。一実施形態において、異なるＩＤＣＳプラットフォームサービスが、接続されているネイティブなアプリケーション（すなわちＩＤＣＳと統合するためにＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔを利用するアプリケーション）からのログイン／ログア

ウト要求を処理するためのＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ、接続されているアプリケーションからのブラウザベースのログイン／ログアウト要求を処理するためのＳＡＭＬ　ＩＤＰサービス、外部ＳＡＭＬ　ＩＤＰに対してユーザ認証を調整するためのＳＡＭＬ　ＳＰサービス、および、ローカルなまたは連携されたログインフローを含みＩＤＣＳホストセッションクッキーを管理するためのエンドユーザログインセレモニーを調整するための内部ＩＤＣＳ　ＳＳＯサービスなどの、ＳＳＯのビジネスを実現する。一般的に、ＨＴＴＰは、フォームありでまたはフォームなしで機能する。フォームありで機能するとき、このフォームはブラウザ内で見えるフォームである。フォームなしで機能するとき、これはクライアントからサーバへの通信として機能する。ＯｐｅｎＩＤ　ＣｏｎｎｅｃｔもＳＡＭＬも、フォームをレンダリングする能力を必要とするが、これは、ブラウザの存在によって実現される、または、ブラウザが存在しているかのように機能するアプリケーションによって仮想的に実行される。一実施形態において、ユーザ認証／ＳＳＯをＩＤＣＳを通して実現するアプリケーションクライアントは、ＩＤＣＳにおいて、ＯＡｕｔｈ２クライアントとして登録される必要があり、クライアント識別子およびクレデンシャル（たとえばＩＤ／パスワード、ＩＤ／証明書など）を取得する必要がある。

【０１３０】

図１０の実施形態の例は、２つのプラットフォームマイクロサービスとしてのＯＡｕｔｈ２　１００４およびＳＡＭＬ２　１００６と、１つのインフラストラクチャマイクロサービスとしてのＳＳＯ１００８とを含む、ログイン機能をまとめて提供する３つのコンポーネント／マイクロサービスを含む。図１０の実施形態において、ＩＤＣＳは「アイデンティティメタシステム」を提供する。このメタシステムにおいて、ＳＳＯサービス１００８は、異なる種類のアプリケーションに対して提供される。これらのアプリケーションは、３者間ＯＡｕｔｈフローを必要としＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔリレーパーティ（relaying party）（「ＲＰ」、そのユーザ認証機能をＩＤＰにアウトソーシングするアプリケーション）として機能するブラウザベースのウェブまたはネイティブアプリケーション１０１０、２者間ＯＡｕｔｈフローを必要としＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ　ＲＰとして機能するネイティブアプリケーション１０１１、およびＳＡＭＬ　ＳＰとして機能するウェブアプリケーション１０１２などである。

【０１３１】

一般的に、アイデンティティメタシステムは、デジタルアイデンティティのための相互運用可能なアーキテクチャであり、複数の基礎となる技術、実装、およびプロバイダの集合体を用いることを可能にする。ＬＤＡＰ、ＳＡＭＬ、およびＯＡｕｔｈは、アイデンティティ機能を提供する異なるセキュリティ標準の例であり、アプリケーションを構築するための基礎となることが可能であり、アイデンティティメタシステムは、このようなアプリケーションに対して統一されたセキュリティシステムを提供するように構成されてもよい。ＬＤＡＰセキュリティモデルは、アイデンティティを扱うための特定のメカニズムを指定し、システムを通るすべてのパスは厳密に保護されねばならない。ＳＡＭＬは、一組のアプリケーションが、異なるセキュリティドメインの異なる組織に属する別の一組のアプリケーションとの間で安全に情報を交換できるようにするために開発されたものである。これら２つのアプリケーションの間に信頼はないので、ＳＡＭＬは、一方のアプリケーションが、同じ組織に属していない別のアプリケーションを認証できるように開発された。ＯＡｕｔｈは、ウェブベースの認証を実行するための軽量プロトコルであるＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔを提供する。

【０１３２】

図１０の実施形態において、ＯｐｅｎＩＤアプリケーション１０１０がＩＤＣＳ内のＯｐｅｎＩＤサーバに接続すると、その「チャネル」はＳＳＯサービスを要求する。同様に、ＳＡＭＬアプリケーション１０１２がＩＤＣＳ内のＳＡＭＬサーバに接続すると、その「チャネル」もＳＳＯサービスを要求する。ＩＤＣＳにおいて、各マイクロサービス（たとえばＯｐｅｎＩＤマイクロサービス１００４およびＳＡＭＬマイクロサービス１００６）はアプリケーション各々を処理し、これらのマイクロサービスはＳＳＯマイクロサービ

ス１００８からのＳＳＯ機能を要求する。プロトコルごとにマイクロサービスを追加してからＳＳＯ機能のためにＳＳＯマイクロサービス１００８を用いることにより、このアーキテクチャを拡張して任意の数のその他のセキュリティプロトコルをサポートすることができる。ＳＳＯマイクロサービス１００８は、セッションを発行し（すなわちＳＳＯクッキー１０１４が提供される）、このアーキテクチャにおいてセッションを発行する権限を有する唯一のシステムである。ＩＤＣＳセッションは、ブラウザ１００２がＳＳＯクッキー１０１４を使用することによって実現される。ブラウザ１００２はまた、ローカルセッションクッキー１０１６を用いてそのローカルセッションを管理する。

【０１３３】

一実施形態において、たとえば、ブラウザ内で、ユーザは、ＳＡＭＬに基づいて第１のアプリケーションを使用してログインし、その後、ＯＡｕｔｈなどの異なるプロトコルを用いて構築された第２のアプリケーションを使用してもよい。ユーザには、同じブラウザ内の第２のアプリケーション上のＳＳＯが与えられる。したがって、ブラウザは、ステートまたはユーザエージェントであり、クッキーを管理する。

【０１３４】

一実施形態において、ＳＳＯマイクロサービス１００８は、ログインセレモニー１０１８、ＩＤ／パスワードリカバリ１０２０、第１回ログインフロー１０２２、認証マネージャ１０２４、ＨＴＴＰクッキーマネージャ１０２６、およびイベントマネージャ１０２８を提供する。ログインセレモニー１０１８は、顧客設定および／またはアプリケーションコンテキストに基づいてＳＳＯ機能を実現し、ローカルフォーム（たとえばベーシックＡｕｔｈ）、外部ＳＡＭＬ　ＩＤＰ、外部ＯＩＤＣ　ＩＤＰなどに従って構成されてもよい。ＩＤ／パスワードリカバリ１０２０は、ユーザのＩＤおよび／またはパスワードの回復のために使用される。第１回ログインフロー１０２２は、ユーザが１回目にログインしたときに実現される（すなわちＳＳＯセッションはまだ存在しない）。認証マネージャ１０２４は、認証に成功すると認証トークンを発行する。ＨＴＴＰクッキーマネージャ１０２６は認証トークンをＳＳＯクッキーに保存する。イベントマネージャ１０２８はＳＳＯ機能に関連するイベントをパブリッシュする。

【０１３５】

一実施形態において、ＯＡｕｔｈマイクロサービス１００４とＳＳＯマイクロサービス１００８との間の対話は、ブラウザリダイレクトに基づいており、ＳＳＯマイクロサービス１００８は、ＨＴＭＬフォームを用いてユーザに問いかけ、クレデンシャルを検証し、セッションクッキーを発行する。

【０１３６】

一実施形態において、たとえば、ＯＡｕｔｈマイクロサービス１００４は、ブラウザ１００２から認可要求を受け、３者間ＯＡｕｔｈフローに従ってアプリケーションのユーザを認証する。よって、ＯＡｕｔｈマイクロサービス１００４は、ＯＩＤＣプロバイダ１０３０として機能し、ブラウザ１００２をＳＳＯマイクロサービス１００８にリダイレクトし、アプリケーションコンテキストに沿って進む。ユーザが有効なＳＳＯセッションを有するか否かに応じて、ＳＳＯマイクロサービス１００８は、既存のセッションを検証するかまたはログインセレモニーを実行する。認証または検証に成功すると、ＳＳＯマイクロサービス１００８は、認証コンテキストをＯＡｕｔｈマイクロサービス１００４に返す。そうすると、ＯＡｕｔｈマイクロサービス１００４はブラウザ１００２を認可（「ＡＺ」）コードを有するコールバックＵＲＬにリダイレクトする。ブラウザ１００２は、ＡＺコードをＯＡｕｔｈマイクロサービス１００４に送信し、必要なトークン１０３２を要求する。また、ブラウザ１００２は、ＨＴＴＰ認可ヘッダにおいてそのクライアントクレデンシャル（ＩＤＣＳをＯＡｕｔｈ２クライアントとして登録したときに取得）を含む。これに対し、ＯＡｕｔｈマイクロサービス１００４は、要求されたトークン１０３２をブラウザ１００２に与える。一実施形態において、ブラウザ１００２に与えられるトークン１０３２は、ＪＷアイデンティティと、ＩＤＣＳ　ＯＡｕｔｈ２サーバによって署名されたアクセストークンとを含む。この機能のさらなる詳細は、以下で図１１を参照しながら開示

される。
【０１３７】
一実施形態において、たとえば、ＯＡｕｔｈマイクロサービス１００４は、ネイティブアプリケーション１０１１から認可要求を受け、２者間ＯＡｕｔｈフローに従ってユーザを認証する。この場合、ＯＡｕｔｈマイクロサービス１００４の認証マネージャ１０３４は対応する認証を（たとえばクライアント１０１１から受けたＩＤ／パスワードに基づいて）実行し、トークンマネージャ１０３６は、認証に成功すると、対応するアクセストークンを発行する。
【０１３８】
一実施形態において、たとえば、ＳＡＭＬマイクロサービス１００６は、ブラウザからＳＳＯ　ＰＯＳＴ要求を受け、ＳＡＭＬ　ＳＰとして機能するウェブアプリケーション１０１２のユーザを認証する。ＳＡＭＬマイクロサービス１００６は次に、ＳＡＭＬ　ＩＤＰ１０３８として機能し、ブラウザ１００２をＳＳＯマイクロサービス１００８にリダイレクトし、アプリケーションコンテキストに沿って進む。ユーザが有効なＳＳＯセッションを有しているか否かに応じて、ＳＳＯマイクロサービス１００８は、既存のセッションを検証するか、またはログインセレモニーを実行する。認証または検証に成功すると、ＳＳＯマイクロサービス１００８は、認証コンテキストをＳＡＭＬマイクロサービス１００６に返す。そうすると、ＳＡＭＬマイクロサービスは、必要なトークンでＳＰにリダイレクトする。
【０１３９】
一実施形態において、たとえば、ＳＡＭＬマイクロサービス１００６は、ＳＡＭＬ　ＳＰ１０４０として機能してもよく、遠隔ＳＡＭＬ　ＩＤＰ１０４２（たとえばアクティブディレクトリ連携サービス（active directory federation service）（「ＡＤＦＳ」）に進んでもよい。一実施形態は、標準ＳＡＭＬ／ＡＤフローを実現する。一実施形態において、ＳＡＭＬマイクロサービス１００６とＳＳＯマイクロサービス１００８との間の対話は、ブラウザのリダイレクトに基づいており、ＳＳＯマイクロサービス１００８は、ＨＴＭＬフォームを用いてユーザに問いかけ、クレデンシャルを検証し、セッションクッキーを発行する。
【０１４０】
一実施形態において、ＩＤＣＳ内部のコンポーネント（たとえば１００４、１００６、１００８）と、ＩＤＣＳ外部のコンポーネント（たとえば１００２、１０１１、１０４２）との間の対話は、ファイアウォール１０４４を通して行われる。
【０１４１】
<u>ログイン／ログアウトフロー</u>
図１１は、一実施形態における、ＩＤＣＳによって提供されるＳＳＯ機能のメッセージシーケンスフロー１１００である。ユーザがブラウザ１１０２を用いてクライアント１１０６（たとえばブラウザベースのアプリケーションまたはモバイル／ネイティブアプリケーション）にアクセスするとき、クラウドゲート１１０４は、アプリケーション施行点として機能し、ローカルポリシーテキストファイルに規定されているポリシーを施行する。クラウドゲート１１０４は、ユーザがローカルアプリケーションセッションを有していないことを検出した場合、ユーザの認証を要求する。そうするために、クラウドゲート１１０４は、ブラウザ１１０２をＯＡｕｔｈ２マイクロサービス１１１０にリダイレクトすることにより、ＯＡｕｔｈ２マイクロサービス１１１０に対するＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔログインフローを開始する（３者間ＡＺ　Ｇｒａｎｔフローであり、範囲＝「openid profile」）。
【０１４２】
ブラウザ１１０２の要求は、ＩＤＣＳルーティング層ウェブサービス１１０８およびクラウドゲート１１０４を横断してＯＡｕｔｈ２マイクロサービス１１１０に到達する。ＯＡｕｔｈ２マイクロサービス１１１０は、アプリケーションコンテキスト（すなわちアプリケーションを記述するメタデータ、たとえば接続するアプリケーションのアイデンティ

ティ、クライアントＩＤ、構成、アプリケーションは何ができるかなど）を構成し、ブラウザ１１０２をログインのためにＳＳＯマイクロサービス１１１２にリダイレクトする。

【０１４３】

ユーザが有効なＳＳＯセッションを有する場合、ＳＳＯマイクロサービス１１１２は、ログインセレモニーを開始することなく既存のセッションを検証する。ユーザが有効なＳＳＯセッションを有していない場合（すなわちセッションクッキーが存在しない）、ＳＳＯマイクロサービス１１１２は、顧客のログインプリファレンスに従ってユーザログインセレモニーを開始する（たとえば商標付ログインページを表示する）。そうするために、ＳＳＯマイクロサービス１１１２は、ブラウザ１１０２を、ＪａｖａＳｃｒｉｐｔで実現されるログインアプリケーションサービス１１１４にリダイレクトする。ログインアプリケーションサービス１１１４はブラウザ１１０２にログインページを提供する。ブラウザ１１０２はログインクレデンシャルを含むＲＥＳＴ　ＰＯＳＴをＳＳＯマイクロサービス１１１２に送信する。ＳＳＯマイクロサービス１１１２は、アクセストークンを生成し、ＲＥＳＴ　ＰＯＳＴのクラウドゲート１１０４に送信する。クラウドゲート１１０４は、認証情報を管理ＳＣＩＭマイクロサービス１１１６に送信することによりユーザのパスワードを検証する。管理ＳＣＩＭマイクロサービス１１１６は、認証が成功したと判断し、対応するメッセージをＳＳＯマイクロサービス１１１２に送信する。

【０１４４】

一実施形態において、ログインセレモニー中、ログインページは同意ページを表示しない。「ログイン」オペレーションはさらなる同意を要しないからである。代わりに、アプリケーションに対してエクスポーズされている特定のプロファイル属性についてユーザに知らせるプライバシーポリシーが、ログインページ上に記載される。ログインセレモニー中、ＳＳＯマイクロサービス１１１２は顧客のＩＤＰプリファレンスを尊重し、構成され次第、構成されたＩＤＰに対する認証のためにＩＤＰにリダイレクトする。

【０１４５】

認証または検証が成功すると、ＳＳＯマイクロサービス１１１２は、ブラウザ１１０２を、ユーザの認証トークンを含む、新たに作成／更新されたＳＳＯホストＨＴＴＰクッキー（たとえば「ＨＯＳＴＵＲＬ」が示すホストのコンテキストで作成されたクッキー）を用いて、ＯＡｕｔｈ２マイクロサービス１１１０に戻るようにブラウザ１１０２をリダイレクトする。ＯＡｕｔｈ２マイクロサービス１１１０は、ＡＺコード（たとえばＯＡｕｔｈコンセプト）をブラウザ１１０２に戻しクラウドゲート１１０４にリダイレクトする。ブラウザ１１０２はＡＺコードをクラウドゲート１１０４に送信し、クラウドゲート１１０４はＲＥＳＴ　ＰＯＳＴをＯＡｕｔｈ２マイクロサービス１１１０に送信してアクセストークンおよびアイデンティティトークンを要求する。これらのトークンはどちらも、ＯＡｕｔｈマイクロサービス１１１０にスコーピングされる（オーディエンストークンクレームによって示される）。クラウドゲート１１０４はこれらのトークンをＯＡｕｔｈ２マイクロサービス１１１０から受ける。

【０１４６】

クラウドゲート１１０４は、アイデンティティトークンを用いて、認証されたユーザのアイデンティティをその内部アカウント表現にマッピングし、これは、このマッピングを自身のＨＴＴＰクッキーに保存してもよい。クラウドゲート１１０４は次に、ブラウザ１１０２をクライアント１１０６にリダイレクトする。すると、ブラウザ１１０２は、クライアント１１０６に到達し、対応するレスポンスをクライアント１１０６から受ける。この時点以降、ブラウザ１１０２は、アプリケーションのローカルクッキーが有効である限り、アプリケーション（すなわちクライアント１１０６）にシームレスにアクセスすることができる。ローカルクッキーが無効になると、認証プロセスは繰返される。

【０１４７】

クラウドゲート１１０４はさらに、要求に含められたアクセストークンを用いて、「userinfo」をＯＡｕｔｈ２マイクロサービス１１１０からまたはＳＣＩＭマイクロサービスから取得する。このアクセストークンは、「プロファイル」スコープによって与えられる

属性の「userinfo」リソースにアクセスするには十分である。これは、ＳＣＩＭマイクロサービスを介して「／ｍｅ」リソースにアクセスするのにも十分である。一実施形態において、デフォルトで、含まれているアクセストークンは、「プロファイル」スコープの下で与えられるユーザプロファイル属性に対してのみ十分である。他のプロファイル属性へのアクセスは、クラウドゲート１１０４によって発行されたＡＺグラントログイン要求において提示された追加の（任意の）スコープに基づいて認可される。

【０１４８】

ユーザがＯＡｕｔｈ２が統合された別のアプリケーションにアクセスする場合、同じプロセスが繰返される。

【０１４９】

一実施形態において、ＳＳＯ統合アーキテクチャは、ブラウザベースのユーザログアウトに対し、同様のＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔユーザ認証フローを使用する。一実施形態において、既存のアプリケーションセッションを有するユーザは、クラウドゲート１１０４にアクセスしてログアウトを開始する。その代わりに、ユーザは、ＩＤＣＳ側でログアウトを開始している場合がある。クラウドゲート１１０４は、特定用途向けのユーザセッションを終了し、ＯＡｕｔｈ２マイクロサービス１１１０に対しＯＡｕｔｈ２　ＯｐｅｎＩＤ　プロバイダ（「ＯＰ」）ログアウト要求を開始する。ＯＡｕｔｈ２マイクロサービス１１１０は、ユーザのホストＳＳＯクッキーを削除するＳＳＯマイクロサービス１１１２にリダイレクトする。ＳＳＯマイクロサービス１１１２は、ユーザのＳＳＯクッキーにおいて追跡された既知のログアウトエンドポイントに対し一組のリダイレクト（ＯＡｕｔｈ２　ＯＰおよびＳＡＭＬ　ＩＤＰ）を開始する。

【０１５０】

一実施形態において、クラウドゲート１１０４がＳＡＭＬプロトコルを用いてユーザ認証（たとえばログイン）を要求する場合、同様のプロセスが、ＳＡＭＬマイクロサービスとＳＳＯマイクロサービス１１１２との間で開始される。

【０１５１】

クラウドキャッシュ

一実施形態は、クラウドキャッシュと呼ばれるサービス／機能を提供する。クラウドキャッシュは、ＩＤＣＳに与えられて、ＬＤＡＰベースのアプリケーション（たとえば電子メールサーバ、カレンダーサーバー、何らかのビジネスアプリケーションなど）との通信をサポートする。なぜなら、ＩＤＣＳはＬＤＡＰに従って通信するのではないが、このようなアプリケーションはＬＤＡＰに基づいてのみ通信するように構成されているからである。典型的には、クラウドディレクトリは、ＲＥＳＴ　ＡＰＩを介してエクスポーズされ、ＬＤＡＰプロトコルに従って通信するのではない。一般的に、企業ファイアウォオールを通してＬＤＡＰ接続を管理するには、セットアップおよび管理が難しい特殊な構成が必要である。

【０１５２】

ＬＤＡＰベースのアプリケーションをサポートするために、クラウドキャッシュは、ＬＤＡＰ通信を、クラウドシステムとの通信に適したプロトコルに変換する。一般的に、ＬＤＡＰベースのアプリケーションは、ＬＤＡＰを介してデータベースを使用する。代わりに、アプリケーションは、ＳＱＬのような異なるプロトコルを介してデータベースを使用するように構成されてもよい。しかしながら、ＬＤＡＰはツリー構造のリソースの階層表現を提供するのに対し、ＳＱＬはデータをテーブルとフィールドとして表現する。したがって、ＬＤＡＰは検索機能用であることがより望ましいであろう。一方、ＳＱＬはトランザクション機能用であることがより望ましいであろう。

【０１５３】

一実施形態において、ＩＤＣＳが提供するサービスを、ＬＤＡＰベースのアプリケーションで使用して、たとえば、アプリケーションのユーザを認証する（すなわちアイデンティティサービス）、またはアプリケーションのセキュリティポリシーを施行する（すなわちセキュリティサービス）ことができる。一実施形態において、ＩＤＣＳとのインターフ

ェイスは、ファイアウォールを通り、ＨＴＴＰ（たとえばＲＥＳＴ）に基づく。典型的に、企業ファイアウォールは、内部ＬＤＡＰ通信へのアクセスを、当該通信がセキュア・ソケット・レイヤ（Secure Sockets Layer）（「ＳＳＬ」）を実現する場合であっても許可しない。また、企業ファイアウォールは、ＴＣＰポートがファイアウォールを通してエクスポーズされることを許可しない。しかしながら、クラウドキャッシュは、ＬＤＡＰとＨＴＴＰとの間の変換を行って、ＬＤＡＰベースのアプリケーションが、ＩＤＣＳが提供するサービスに到達できるようにし、ファイアウォールはＨＴＴＰに対してオープンである。

【０１５４】

一般的に、ＬＤＡＰディレクトリは、マーケティングおよび開発などのビジネスライン（line of business）で使用されてもよく、ユーザ、グループ、業務などを規定する。一例において、マーケティングおよび開発ビジネスは、多様な顧客を対象としている場合があり、顧客ごとに、独自のアプリケーション、ユーザ、グループ、業務などを有し得る。ＬＤＡＰキャッシュディレクトリを実行し得るビジネスラインの別の例は、無線サービスプロバイダである。この場合、無線サービスプロバイダのユーザが行う各コールは、ＬＤＡＰディレクトリに対してユーザのデバイスを認証し、ＬＤＡＰディレクトリ内の対応する情報の一部は課金システムと同期させてもよい。これらの例において、ＬＤＡＰは、実行時に探索されるコンテンツを物理的に分離するための機能を提供する。

【０１５５】

一例において、無線サービスプロバイダは、短期マーケティングキャンペーンを支援するＩＤＣＳが提供するサービスを使用する一方で、自身のアイデンティティ管理サービスをそのコアビジネス（たとえば通常のコール）のために扱ってもよい。この場合、クラウドキャッシュは、ＬＤＡＰを、クラウドに対して実行する一組のユーザおよび一組のグループを有する場合は「平坦にする」。一実施形態において、ＩＤＣＳにおいて実現されるクラウドキャッシュの数はいくつであってもよい。

【０１５６】

分散型データグリッド

一実施形態において、ＩＤＣＳにおけるキャッシュクラスタは、たとえばその開示を本明細書に引用により援用する米国特許公開第２０１６／００９２５４０号に開示されている分散型データグリッドに基づいて実現される。分散型データグリッドは、分散環境またはクラスタ環境内で１つ以上のクラスタにおいてコンピュータサーバの集合体が、一緒に作業することにより情報を管理し計算などの関連動作を管理するシステムである。分散型データグリッドを用いることで、サーバ間で共有されるアプリケーションオブジェクトおよびデータを管理することができる。分散型データグリッドは、短いレスポンスタイム、高いスループット、予測可能なスケーラビリティ、継続的なアベイラビリティ、および情報の信頼性を提供する。具体的な例として、たとえばオラクル社のOracle Coherenceのデータグリッドのような分散型データグリッドは、情報をインメモリに格納することによりさらに高いパフォーマンスを達成し、複数のサーバにわたって同期が取られた情報のコピーを保持するにあたって冗長性を用いることにより、サーバ故障イベント時におけるシステムの回復力とデータの継続的なアベイラビリティとを保証する。

【０１５７】

一実施形態において、ＩＤＣＳは、Coherenceなどの分散型データグリッドを実現して、すべてのマイクロサービスがブロックされることなく共有キャッシュオブジェクトへのアクセスを要求できるようにする。Coherenceは、従来のリレーショナルデータベース管理システムと比較して、より高い信頼性、スケーラビリティ、およびパフォーマンスが得られるように設計された、所有権を主張できるＪａｖａベースのインメモリデータグリッドである。Coherenceは、ピアトゥピア（すなわち中央マネージャがない）インメモリ分散型キャッシュを提供する。

【０１５８】

図１２は、データを格納しデータアクセス権をクライアント１２５０に与え本発明の実

施形態を実現する分散型データグリッド１２００の一例を示す。「データグリッドクラスタ」または「分散型データグリッド」は、分散環境またはクラスタ環境内で１つ以上のクラスタ（たとえば１２００ａ、１２００ｂ、１２００ｃ）において一緒に作業することにより情報を格納し関連する計算などの動作を管理する複数のコンピュータサーバ（たとえば１２２０ａ、１２２０ｂ、１２２０ｃ、および１２２０ｄ）を含むシステムである。分散型データグリッド１２００は、クラスタ１２００ａにおいて５つのデータノード１２３０ａ、１２３０ｂ、１２３０ｃ、１２３０ｄ、および１２３０ｅとともに４つのサーバ１２２０ａ、１２２０ｂ、１２２０ｃ、１２２０ｄを含むものとして示されているが、分散型データグリッド１２００は、任意の数のクラスタおよび各クラスタにおける任意の数のサーバおよび／またはノードを含み得る。ある実施形態において、分散型データグリッド１２００は本発明を実現する。

【０１５９】

図１２に示されるように、分散型データグリッドは、一緒に作業する多数のサーバ（たとえば１２２０ａ、１２２０ｂ、１２２０ｃ、および１２２０ｄ）にデータを分散させることによってデータ格納および管理機能を提供する。データグリッドクラスタの各サーバは、たとえば、１つから２つのプロセッサソケットと１プロセッサソケット当たり２つから４つのＣＰＵコアとを有する「コモディティ（commodity）ｘ８６」サーバハードウェアプラットフォームのような、従来のコンピュータシステムであってもよい。各サーバ（たとえば１２２０ａ、１２２０ｂ、１２２０ｃ、および１２２０ｄ）は、１つ以上のＣＰＵと、ネットワークインターフェイスカード（Network Interface Card）（「ＮＩＣ」）と、たとえば最小で４ＧＢのＲＡＭ最大で６４ＧＢ以上のＲＡＭを含むメモリとで構成されている。サーバ１２２０ａは、ＣＰＵ１２２２ａと、メモリ１２２４ａと、ＮＩＣ１２２６ａとを有するものとして示されている（これらの要素は他のサーバ１２２０ｂ、１２２０ｃ、１２２０ｄ上にもあるが図示されていない）。任意で、各サーバにフラッシュメモリ（たとえばＳＳＤ　１２２８ａ）を設けることで過剰な記憶容量を提供してもよい。提供時、ＳＳＤ容量は、好ましくはＲＡＭのサイズの１０倍である。データグリッドクラスタ１２００ａのサーバ（たとえば１２２０ａ、１２２０ｂ、１２２０ｃ、１２２０ｄ）は、高帯域幅のＮＩＣ（たとえばＰＣＩ－ＸまたはＰＣＩｅ）を用いて高性能ネットワークスイッチ１２２０（たとえばギガビット以上のイーサネット（登録商標））に接続されている。

【０１６０】

クラスタ１２００ａは、故障中にデータが失われる可能性を避けるために最小で４つの物理サーバを含むことが好ましいが、典型的な設備はより多くのサーバを有する。各クラスタに存在するサーバが多いほど、フェイルオーバーおよびフェイルバックの効率は高く、サーバの故障がクラスタに与える影響は小さくなる。サーバ間の通信時間を最短にするために、各データグリッドクラスタは、サーバ間の単一ホップ通信を提供する単一のスイッチ１２０２に限定されることが理想的である。このように、クラスタは、スイッチ１２０２上のポートの数によって制限される。したがって、典型的なクラスタは４～９６の物理サーバを含む。

【０１６１】

分散型データグリッド１２００のほとんどの広域ネットワーク（Wide Area Network）（「ＷＡＮ」）構成において、ＷＡＮ内の各データセンターは、独立しているが相互に接続されているデータグリッドクラスタ（たとえば１２００ａ、１２００ｂ、および１２００ｃ）を有する。ＷＡＮは、たとえば図１２に示されるクラスタよりも多くのクラスタを含み得る。加えて、相互接続されているが独立しているクラスタ（たとえば１２００ａ、１２００ｂ、１２００ｃ）を用いることにより、および／または相互接続されているが独立しているクラスタを、互いに離れているデータセンター内に配置することにより、分散型データグリッドは、自然災害、火災、洪水、長期停電などによって生じる、１つのクラスタのすべてのサーバの同時損失を防止すべく、クライアント１２５０に対するデータおよびサービスを保証することができる。

【０１６２】
１つ以上のノード（たとえば１２３０ａ、１２３０ｂ、１２３０ｃ、１２３０ｄおよび１２３０ｅ）は、クラスタ１２００ａの各サーバ（たとえば１２２０ａ、１２２０ｂ、１２２０ｃ、１２２０ｄ）上で動作する。分散型データグリッドにおいて、ノードは、たとえばソフトウェアアプリケーション、仮想マシンなどであってもよく、サーバは、ノードがその上で動作するオペレーティングシステム、ハイパーバイザなど（図示せず）を含み得る。Oracle Coherenceのデータグリッドでは、各ノードはＪａｖａ仮想マシン（Java virtual machine）（「ＪＶＭ」）である。ＣＰＵの処理能力およびサーバ上で利用できるメモリに応じて、各サーバ上に多数のＪＶＭ／ノードを設けてもよい。ＪＶＭ／ノードは、分散型データグリッドの要求に応じて、追加、起動、停止、および削除されてもよい。Oracle Coherenceを実行するＪＶＭは、起動時に自動的に参加しクラスタ化する。クラスタに加わるＪＶＭ／ノードは、クラスタメンバまたはクラスタノードと呼ばれる。
【０１６３】
アーキテクチャ
各クライアントまたはサーバは、情報伝達のためにバスまたはその他の通信機構を含み、情報処理のためにバスに結合されたプロセッサを含む。プロセッサは、どのタイプの汎用または専用プロセッサであってもよい。各クライアントまたはサーバはさらに、プロセッサによって実行される命令および情報を格納するためのメモリを含み得る。メモリは、ランダムアクセスメモリ（「ＲＡＭ」）、読出専用メモリ（「ＲＯＭ」）、磁気もしくは光ディスクなどのスタティックストレージ、またはその他任意の種類のコンピュータ読取可能媒体を組み合わせたもので構成することができる。各クライアントまたはサーバはさらに、ネットワークへのアクセス提供のためにネットワークインターフェイスカードなどの通信デバイスを含み得る。したがって、ユーザは、各クライアントまたはサーバに対して、直接、またはネットワークを通して遠隔から、またはその他任意の手段で、インターフェイスすることができる。
【０１６４】
コンピュータ読取可能な媒体は、プロセッサからアクセスすることが可能な利用可能な媒体であればどのようなものでもよく、揮発性媒体および不揮発性媒体、リムーバブルおよび非リムーバブル媒体、ならびに通信媒体を含む。通信媒体は、コンピュータ読取可能な命令、データ構造、プログラムモジュール、または、たとえば搬送波もしくはその他の搬送機構などの変調されたデータ信号内のその他のデータを含んでいてもよく、任意の情報伝達媒体を含む。
【０１６５】
プロセッサはさらに、液晶ディスプレイ（「ＬＣＤ」）などのディスプレイにバスを介して結合されてもよい。キーボード、およびコンピュータマウスなどのカーソル制御デバイスが、さらにバスに結合されることにより、ユーザが各クライアントまたはサーバに対してインターフェイスできるようにしてもよい。
【０１６６】
一実施形態において、メモリは、プロセッサが実行すると機能を提供するソフトウェアモジュールを格納する。モジュールは、各クライアントまたはサーバにオペレーティングシステム機能を提供するオペレーティングシステムを含む。モジュールはさらに、クラウドアイデンティティ管理機能を提供するためのクラウドアイデンティティ管理モジュールと、本明細書に開示されているその他すべての機能とを含み得る。
【０１６７】
クライアントは、クラウドサービスなどのウェブサービスにアクセスし得る。一実施形態において、ウェブサービスは、オラクル社のWebLogicサーバ上で実現されてもよい。他の実施形態ではウェブサービスの他の実装形態を使用してもよい。ウェブサービスは、クラウドデータを格納しているデータベースにアクセスする。
【０１６８】
ＩＡＭ機能の例

一実施形態において、ＩＡＭ機能は、メモリにまたはその他のコンピュータ読取可能なもしくは有形の媒体に格納されたソフトウェアによって実現され、プロセッサによって実行される。

【０１６９】

アイデンティティ管理サービスの実行の要求を受ける。一実施形態において、この要求は、アイデンティティ管理サービスと当該アイデンティティ管理サービスを実行するように構成されたマイクロサービスとを特定するＡＰＩに対するコールを含む。一実施形態において、マイクロサービスは、他のモジュール／マイクロサービスと通信することが可能な内蔵モジュールであり、各マイクロサービスは、他からコンタクトが可能な無名のユニバーサルポートを有する。たとえば、一実施形態において、図６に示されるように、各種アプリケーション／サービス６０２は、ＩＤＣＳマイクロサービス６１４を使用するためにＩＤＣＳ　ＡＰＩに対してＨＴＴＰコールを行うことができる。一実施形態において、マイクロサービスはランタイムコンポーネント／プロセスである。

【０１７０】

一実施形態において、この要求はＵＲＬを含む。一実施形態において、マイクロサービスはＵＲＬのプレフィックスにおいて特定される。一実施形態において、ＵＲＬのリソース部分はＡＰＩを特定する。一実施形態において、ＵＲＬのホスト部分は要求に関連するリソースのテナンシーを特定する。たとえば、ＩＤＣＳのウェブ環境における「ホスト／マイクロサービス／リソース」のようなＵＲＬにおいて、マイクロサービスは特定のＵＲＬプレフィックスを有することを特徴とし（たとえば「host/oauth/v1」）、実際のマイクロサービスは「oauth/v1」であり、「oauth/v1」の下で複数のＡＰＩが存在し、たとえば、トークン（token）を要求するためのＡＰＩ：「host/oauth/v1/token」、ユーザを認可する（authorize）ためのＡＰＩ：「host/oauth/v1/authorize」などである。すなわち、ＵＲＬはマイクロサービスを実現し、ＵＲＬのリソース部分はＡＰＩを実現する。したがって、同じマイクロサービスの下で複数のＡＰＩが集約される。一実施形態において、ＵＲＬのホスト部分はテナントを特定する（たとえば、https://tenant3.identity.oraclecloud.com:/oauth/v1/token"）。

【０１７１】

次に要求が認証される。一実施形態において、要求は、本明細書においてたとえば図６のウェブルーティング層６１０および／または図７のクラウドゲート７０２を参照しながら説明したクラウドゲートのようなセキュリティゲートによって認証される。

【０１７２】

次に、たとえば本明細書において図６のＩＤＣＳ「ＡＰＩプラットフォーム」およびＩＤＣＳ中間層６１４のマイクロサービスへのアクセスを参照しながら説明したように、マイクロサービスがＡＰＩに基づいてアクセスされる。一実施形態において、マイクロサービスとの通信は、マイクロサービスの無名ユニバーサルポートを通じて構成される。一実施形態において、マイクロサービスの無名ユニバーサルポートは、従来マイクロサービスがエクスポーズする（たとえば従来のＨＴＴＰポートとしての）標準通信チャネルであり、同一サービス内のその他いずれかのモジュール／マイクロサービスがそれに対してトークできるようにする標準通信チャネルである。一実施形態において、マイクロサービスは、１つ以上のＡＰＩをエクスポーズすることによって１つ以上の機能を提供する。一実施形態において、マイクロサービスとの通信は、１つ以上のＡＰＩを通じてのみ実現される。すなわち、マイクロサービスへの接触／コンタクトは、このようなＡＰＩにコールすることによってのみ実現される。一実施形態において、マイクロサービスとの通信は、軽量プロトコルに従って構成される。一実施形態において、軽量プロトコルは、ＨＴＴＰおよびＲＥＳＴを含む。一実施形態において、要求は、ＲＥＳＴｆｕｌ　ＨＴＴＰ　ＡＰＩに対するコールを含む。したがって、一実施形態はディスパッチ機能を提供する。各ＨＴＴＰ要求は、ＵＲＩおよび動詞を含む。本実施形態は、ＵＲＩのエンドポイント（ホスト／サービス／リソース）をパースし、これを、ＨＴＴＰ動詞（たとえば、ＰＯＳＴ、ＰＵＴ、ＰＡＴＣＨ、またはＤｅｌｅｔｅ）と組み合わせることにより、適切なモジュールの適切

な方法をディスパッチする（または呼び出す）。このパターンは、ＲＥＳＴによくあるものであり、さまざまなパッケージ（たとえばJersey）によってサポートされる。

【０１７３】

次に、たとえば本明細書において図６のＩＤＣＳ「ＡＰＩプラットフォーム」およびＩＤＣＳ中間層６１４のマイクロサービスへのアクセスを参照しながら説明したように、アイデンティティ管理サービスがマイクロサービスによって実行される。一実施形態において、マイクロサービスは、ステートレスであり、横方向にスケーラブルであり、独立してデプロイ可能である。一実施形態において、マイクロサービスの各物理的実装は、複数のテナントを安全にサポートするように構成される。一実施形態において、アイデンティティ管理サービスは、ログインサービス、ＳＳＯサービス、フェデレーションサービス、トークンサービス、ディレクトリサービス、プロビジョニングサービス、またはＲＢＡＣサービスを含む。

【０１７４】

マルチテナントアイデンティティクラウドサービスのための宣言型第三者アイデンティティプロバイダの統合

「ソーシャルログイン」または第三者ログインは、ユーザが、Facebook（登録商標）、Twitter（登録商標）またはGoogle（登録商標）のようなソーシャルネットワークサービスまたはその他の第三者サービスを利用してサービス／アプリケーション（たとえばＩＤＣＳ）にログインする、サインイン／ログインの一形態である。Facebookのようなソーシャルログインサービスは、アイデンティティプロバイダ（「ＩＰ」または「ＩｄＰ」）として機能し、ユーザがアクセスを所望するサービスは、サービスプロバイダ（「ＳＰ」）または依拠当事者（relying party）としての役割を果たす。ユーザがそのサービスのアカウントを有していない場合は、サービスプロバイダの実装に応じて、登録を完了するようユーザに依頼してアカウントを作成するか、または、単にユーザの挨拶（salutation）情報を集めてユーザ経験をパーソナライズするために使用することができる。ユーザが既に登録されているのであれば、このユーザを、電子メールアドレスまたはその他の識別子に基づいて既存のユーザにマッピングすることができる。

【０１７５】

具体的には、上で開示されているＩＤＣＳ、およびその他任意のクラウドプロバイダに関連する、アイデンティティアサーションプロバイダとしても知られているアイデンティティプロバイダは、ＩＤＣＳの外部のウェブサイトを用いてＩＤＣＳとの対話を所望するユーザのＩＤを提供する。サービスプロバイダは、アプリケーションをホストするＩＤＣＳのようなウェブサイトである。アドミニストレータは、アイデンティティプロバイダを有効にすることができ、かつ、１つ以上のサービスプロバイダを定義することができる。そうすると、ユーザは、サービスプロバイダがホストするアプリケーションに、アイデンティティプロバイダから直接アクセスすることができる。

【０１７６】

たとえば、ウェブサイトは、ユーザがGoogleクレデンシャルでＩＤＣＳにログインできるようにすることが可能である。Googleはアイデンティティプロバイダとしての役割を果たし、ＩＤＣＳはサービスプロバイダとして機能する。Googleは、このユーザが認可されたユーザであることを確認し、情報（たとえば、電子メールアドレスがユーザ名と異なる場合はこのユーザのユーザ名と電子メールアドレス）をＩＤＣＳに返す。

【０１７７】

ユーザの認証は１度限りでなければならない。この例の場合、ユーザはセキュリティトークンを取得する。次に、このセキュリティトークンは、ユーザがＩＤＣＳにアクセスできるよう、Googleによって検査される。この方法は、ユーザの単一のトークンが複数のＩＴシステムで信頼される、連携シングルサインオン（「ＳＳＯ」）として知られている。同じトークンを用いて、ユーザを、アイデンティティプロバイダとサービスプロバイダ（この例の場合、GoogleとＩＤＣＳ）の双方について認証することができる。

【０１７８】

上で開示されているＩＤＣＳの実施形態は、第三者アイデンティティプロバイダとの統合により、少なくとも以下の機能をサポートする必要がある。（１）ログインユースケース：第三者アイデンティティプロバイダに対する既存のアカウントを用いてＩＤＣＳにログインできるようにすること（すなわちソーシャルログイン）、および（２）プロビジョニングユースケース：第三者アイデンティティドメインにおけるユーザアカウントの自動プロビジョニングであり、このプロビジョニングユースケースにおいて、メタデータは、第三者プロバイダからアクセストークンを取得するプロセスにおいてのみ、使用される。

【０１７９】

これらの第三者アイデンティティプロバイダの多くは、利用できるユーザデータへのアクセスを認可するためにＯＡｕｔｈ標準仕様をサポートするが、通常、各プロバイダのＯＡｕｔｈ実装は互いに相違する。これらの相違は、

・認可要求、アクセストークン要求およびユーザ情報要求に使用されるエンドポイントの名称、

・これらのエンドポイントについてのＨＴＴＰ要求およびＨＴＴＰレスポンスがサポートするパラメータ／属性、

・アクセストークンをＡＰＩコールに含めるためのメカニズム、

・ユーザプロファイルデータのフォーマット、および

・ＯＡｕｔｈプロトコルの一部ではないカスタムパラメータ

を含む。

【０１８０】

これらの相違のため、ＩＤＣＳおよびその他のマルチテナントクラウドプロバイダが使用する、ある周知のソリューションは、Google、Facebook、Microsoft、Linkedin（登録商標）、Twitter、GitHub（登録商標）、Instagram（登録商標）などのような、サポートされる第三者プロバイダの選択ごとに、専用の統合を提供することである。ソーシャルログインでは、ユーザがログインすると、ＩＤＣＳは、同じ電子メールアドレスを有するユーザを探し出す。ユーザが見つからない場合は登録を完了するようユーザに依頼する。周知のソリューションの場合、ソーシャルログインを容易にするために、サービスプロバイダ上で作成されたアプリケーションについてクライアントＩＤおよびクライアントシークレットのみがＩＤＣＳにとって必要となるように、各第三者プロバイダが予め構成されている。

【０１８１】

しかしながら、周知のソーシャルログインソリューションには、

・新規の第三者プロバイダをサポートしようとする場合、コード開発、テスト、およびそのプロバイダとの統合のリリースという、完全なサイクルが必要であること、および

・新規プロバイダのサポートはコーディングを要するので、顧客および第三者インテグレータにとって、新規アイデンティティプロバイダとの統合を開発し実証することは比較的困難であること、

を含む、問題がある。

【０１８２】

ＩＤＣＳはマルチテナントクラウドサービスなので、顧客がカスタム統合のコードを書き込むことおよびそのコードを共有ＩＤＣＳインスタンス上にデプロイすることは、認められない。したがって、顧客には、所望のアイデンティティプロバイダとの顧客自身のカスタム統合を開発するために利用できるセルフサービスオプションはなく、自身が所望するアイデンティティプロバイダに対するサポートを追加するためにはマルチテナントクラウドプロバイダに依拠する以外、オプションはない。

【０１８３】

これに対し、複雑な統合コーティングを必要とする周知のソリューションについて、実施形態は、第三者アイデンティティプロバイダとの統合のために宣言型メカニズムを使用する。これにより、アイデンティティドメインアドミニストレータ、または特別の権限を有するユーザは、アイデンティティプロバイダによってエクスポーズされたサービスエン

ドポイントとやり取りするためのメタデータを指定するだけで、アイデンティティプロバイダに対するサポートを追加することが可能である。次に、このメタデータを、本発明の実施形態における宣言型メカニズムが使用することで、新規の第三者プロバイダが追加される。

【０１８４】

実施形態により、メタデータがプロバイダを定義することでプロバイダを利用できるようにする。この「宣言型」手法は、コーディングを不要にし、新規プロバイダを追加するプロセスを高速にすることができる。実施形態はさらに、（すべてのテナントに対する）グローバルプロバイダのメタデータの定義について、ＳＣＩＭ準拠ＲＥＳＴエンドポイントをエクスポーズする（たとえば、{{idcs-oracle-url}}/admin/v1/SocialIdentityProviderMetadata）。

【０１８５】

実施形態はさらに、顧客に対するカスタムプロバイダを定義する。この手法にはコーディングが不要なので、顧客はプロバイダを追加することができ、クラウドデプロイメントにおける第三者コードに関連する課題を課すことはない。顧客によるメタデータの定義のために、実施形態は、ＳＣＩＭ準拠ＲＥＳＴエンドポイントをエクスポーズする（たとえば、{{tenant-url}}/admin/v1/CustomSocialIdentityProviderMetadata）。

【０１８６】

実施形態におけるメタデータは、新規の第三者アイデンティティプロバイダとの統合を容易にする以下のものを含む。

【０１８７】

・ＯＡｕｔｈエンドポイントならびに対応する要求およびレスポンスヘッダおよびパラメータ。たとえば、以下のパラメータをGitHubのトークンエンドポイントに使用することができる。

【０１８８】

【数３】

```
"tokenPhase": {
        "url": "https://github.com/login/oauth/access_token",
        "method": "post"
},
"tokenPhaseHeaders": [
        {
                "value": "application/json",
                "name": "Accept"
        },
        {
                "value": "Basic $clientCredentials",
                "name": "Authorization"
        }
],
"tokenPhaseParameters": [
        {
                "value": "$socialIdentityProvider.consumerKey",
                "name": "client_id"
        },
        {
                "value": "$socialIdentityProvider.consumerSecret",
                "name": "client_secret"
        },
        {
                "value": "$redirectUri",
                "name": "redirect_uri"
        },
        {
                "value": "$authorizationCode",
                "name": "code"
        },
        {
                "value": "authorization_code",
                "name": "grant_type"
        }
],
```

【０１８９】

・アイデンティティプロバイダが、ソーシャルログインに使用されるのか、またはソーシャルプロバイダプロビジョニングに使用されるのか、またはこれらの双方に使用されるのか。

【０１９０】

・ソーシャルログインおよびプロビジョニングというユースケースそれぞれにおいてアイデンティティプロバイダから要求されるＯＡｕｔｈ範囲とは何か。たとえば、

"user user:email"

は、GitHubに対して定められる範囲の一例である。

【０１９１】
・ユーザプロファイル属性の、ＩＤＣＳユーザプロファイル属性に対するマッピング。GitHubに対して使用されるユーザプロファイル属性マッピングの一例は以下の通りである。
【０１９２】
【数４】

```
"userInfoAttributeMappings": [
                {
                    "idpAttribute": "name",
                    "idcsAttribute": "given_name"
                }
            ]
```

【０１９３】
図１３は、本発明の実施形態に係るシーケンス図を示す。図１３において、要素は、アイデンティティドメインアドミニストレータまたはＩＤＣＳアドミニストレータであってもよいユーザ１３０１を含む。アイデンティティドメインアドミニストレータは、単に特別の権限を有するユーザであってもよい。要素はさらに、ソーシャルアイデンティティプロバイダメタデータサービス１３０２およびＳＳＯ１３０３を含む。メタデータサービス１３０２、ＳＳＯ１３０３およびソーシャルログインサービス１３０４は、ＩＤＣＳ内のマイクロサービスによって実現される。ソーシャルアイデンティティプロバイダ１３０５は、Facebookのような第三者アイデンティティプロバイダによって実現される。一実施形態において、メタデータサービス１３０２は、ＳＣＩＭ準拠ＲＥＳＴエンドポイントである。
【０１９４】
１３１０において、ユーザは、本明細書に開示されている宣言型フレームワークを用いてメタデータを定義する。一実施形態におけるメタデータは、アイデンティティクラウドサービスデータベースに格納される。メタデータは、行われる必要があることを指定するだけでよくそれが如何にして行われるかを指定する必要がないという点において、宣言型である。たとえば、ユーザは、ソーシャルプロバイダ（すなわちソーシャルアイデンティティプロバイダメタデータサービス１３０２）のトークンエンドポイントと、パラメータ（すなわちエンドポイント要求およびレスポンスパラメータ）の所望の値とを指定するだけでよく、トークンエンドポイントへの接続およびトークンの処理の方法について懸念する必要はない。
【０１９５】
１３１１において、ユーザは、ソーシャルアイデンティティプロバイダまたはその他の第三者アイデンティティプロバイダを用いて、要求をＲＥＳＴ　ＡＰＩを介してＳＳＯマイクロサービス１３０３に送信することにより、ログインを開始する。
【０１９６】
１３１２において、ＳＳＯ１３０３は、ソーシャルログインサービス１３０４へのログオンを開始する。次に、ソーシャルログインサービス１３０４は、１３１３において、格納されたメタデータを取り出しこのメタデータを用いて認可要求を構築する。エンドポイント
１３１４～１３１６の認可段階の結果、ユーザ１３０１が認可された後に、ソーシャルログインサービス１３０４において認可コードが得られる。認可コードは、クライアントがアクセストークンと交換することになる一時的なコードである。このコード自体は、ユーザが、クライアントが要求しているのはどのような情報かを知ってその要求を承認または否認する機会を得た場合に、認可サーバから得られる。１３１７～１３１９におけるア

クセストークン段階は、認可コードおよびメタデータを用いてアクセストークン（たとえばＯＡｕｔｈトークン）を取得する。

【０１９７】

１３２０～１３２２のユーザプロファイル段階は、要求をアクセストークンとともにユーザ情報エンドポイント（すなわちメタデータ）に送り、このメタデータを用いて、ユーザ１３０１に関するユーザ情報セキュリティトークンクレームを返す。

【０１９８】

１３２３において、ユーザ情報を用いることにより、ユーザセッション作成を要求し、１３２４において、ログインに成功する。

【０１９９】

認可段階１３１４～１６において、ｉｄｐ１３０５の認可エンドポイントへのリダイレクトのためのＵＲＬがデフォルト実装通りである場合、以下の方法がオーバライドされる必要がある。

【０２００】

【表１】

方法	説明
protected String getDefaultAuthorizationURL()	ｉｄｐ１３０５のデフォルト認可エンドポイントＵＲＬを返す。この値は、テナントアドミンによって構成されたソーシャルｉｄｐプロファイルが認可エンドポイントＵＲＬを指定しない場合に使用される。
protected String getDefaultLoginScopes()	ユーザのソーシャルプロファイルへのアクセス獲得のためにＯＰから要求される範囲のカンマで区切られたリストを返す。オーバライドされなければ、デフォルトは"opened"。プラグインがログイン機能を有する場合にのみ必要。この値は、テナントアドミンによって構成されたソーシャルｉｄｐプロファイルがログイン範囲を指定しない場合に使用される。
protected String getDefaultProvisioningScopes()	プロビジョニング特権の獲得のためにＯＰから要求される範囲のカンマで区切られたリストを返す。オーバライドされなければ、デフォルトは""。プラグインがプロビジョニング機能を有する場合にのみ必要。この値は、テナントアドミンによって構成されたソーシャルｉｄｐプロファイルがプロビジョニング範囲を指定しない場合に使用される。
protected String augmentAuthorizationURL(String authzURL, SocialIdentityProvider config, SocialCapability socialCapability)	この方法を用いることで、認可エンドポイントのリダイレクトｕｒｌに、さらに他のクエリパラメータを追加することができる。

【０２０１】
デフォルト実装によって生成されるＵＲＬは次の通りである。
【０２０２】
【数５】

```
<Authorization Endpoint URL for OP>?
  client_id=<client id>&
  response_type=code&
  scope=<scopes>
  redirect_uri=<tenant base url>/oauth2/v1/social/callback&
  state=<auto generated by idcs>
```

【０２０３】
ＯＰ認可エンドポイントへのリダイレクトのためのＵＲＬが正確にデフォルト実装通りでない場合、実施形態では以下の方法がオーバライドされる必要がある。
【０２０４】
【表２】

方法	説明
protected String getAuthorizationResponse(String state, String returnURL, SocialIdentityProvider config, SocialCapability socialCapability)	ｉｄｐ１３０５の認可エンドポイントにリダイレクトするための完全なＵＲＬを返す。

【０２０５】
アクセストークン段階１３１７～１９において、ｉｄｐ１３０５のトークンエンドポイントとのやり取りがデフォルト実装通りであれば、以下の方法がオーバライドされる必要がある。
【０２０６】
【表３】

方法	説明
public String getDefaultAccesstokenUrl()	ＯＰのトークンエンドポイントのＵＲＬを返す。この値は、テナントアドミンによって構成されたソーシャルｉｄｐプロファイルがトークンエンドポイントＵＲＬを指定しない場合に使用される。

【０２０７】
実施形態におけるデフォルト実装通りのやり取りは、次の通りである。
【０２０８】
【数６】

要求：

POST <OP's Token Endpoint> HTTP/1.1Host: <OP's base url> Content-Type: application/x-www-form-urlencodedcode=<authorization code acquired in authorize phase>& client_id=<client id>& client_secret=<client secret>& redirect_uri=<tenant base url>/oauth2/v1/social/callback& grant_type=authorization_code

レスポンス：

{"access_token":"<accesstoken>","refresh_token":"<refreshtoken>","expires_in":3600}

ログインユースケースではレスポンスでrefresh_tokenは送信されない場合がある。

【０２０９】
ｉｄｐ１３０５のトークンエンドポイントに送信される要求は正確にデフォルト実装通りではないものの、レスポンスがデフォルト実装通りである場合、実施形態は以下の方法をオーバライドする。
【０２１０】
【表４】

方法	説明
public String getAccessTokenResponse(SocialIdentityProvider config, String returnURL, String code, Map<String, String> state) throws SocialLoginException	トークンエンドポイント呼出からのＪＳＯＮレスポンスをストリングとして返す。

【０２１１】
ｉｄｐ１３０５のトークンエンドポイントについての要求もレスポンスもデフォルト通りでない場合、実施形態は以下の方法をオーバライドする。
【０２１２】

【表５】

方法	説明
public SocialBaseResponse getAccessToken(SocialBaseRequest request, Map<String, String> state, String returnURL, SocialIdentityProvider config) throws SocialLoginException	トークンエンドポイント呼出からのレスポンスをSocialBaseResponse オブジェクトとして返す。

【０２１３】
ユーザプロファイルアクセストークン段階１３２０～２２において、ｉｄｐ１３０５のユーザ情報エンドポイントとのやり取りがデフォルト実装通りである場合、実施形態は以下の方法を用いてオーバライドする。

【０２１４】
【表６】

方法	説明
public String getDefaultUserInfoUrl()	ＯＰのユーザ情報エンドポイントのＵＲＬを返す。この値は、テナントアドミンによって構成されたソーシャルｉｄｐプロファイルがユーザ情報エンドポイントＵＲＬを指定しない場合に使用される。

【０２１５】
【数７】

デフォルト実装通りのやり取りのサンプル

要求

https://www.googleapis.com/oauth2/v3/userinfo?access_token=<access-token>

レスポンス

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "sub": "248289761001",
 "name": "Jane Doe",
 "given_name": "Jane",
 "family_name": "Doe",
 "preferred_username": "j.doe",
 "email": "janedoe@example.com",
 "picture": "http://example.com/janedoe/me.jpg"
}
```

【０２１６】
ｉｄｐ１３０５のユーザ情報エンドポイントとのやり取りがデフォルト実装通りでない場合、実施形態はまた以下の方法オーバライドする。
【０２１７】
【表７】

方法	説明
public MapValue getUserProfileResponse(SocialBaseRequest request, Map<String, String> state, SocialLoginResponse accessTokenResponse, SocialIdentityProvider config) throws SocialLoginException	ユーザ情報エンドポイント呼出からのレスポンスを MapValue として返す。以下の標準キーが MapValue に存在すると予測される。 • email : ユーザの電子メールアドレス • given_name: ユーザの名 • family_name: ユーザの姓 したがって、ユーザ情報エンドポイントから返されたレスポンスがこれらの属性について異なるキーを有する場合、キーの名称を変更する必要がある。

【０２１８】
実施形態において、第三者アイデンティティプロバイダメタデータは、以下で開示されるＳＣＩＭ準拠スキーマに従うＪＳＯＮフォーマットである。scratchからＪＳＯＮを生

成する代わりに、以下のサンプルをスターティングポイントとして使用することができる。＄で始まる表現は、一定ではないパラメータ値である。たとえば、
・$socialIdentityProviderは、対応するソーシャルアイデンティティプロバイダリソースを表す。たとえば、$socialIdentityProvider.consumerKeyは、テナント固有のソーシャルアイデンティティプロバイダプロファイルにおいて構成されたクライアントシークレットである。
・${state}は、ソーシャルｉｃｐ１３０５に認可要求１３１４を送信する間にＩＤＣＳランタイムによって生成される状態（state）である。
・${redirectUri}は、ＩＤＣＳランタイムによって生成されるテナント固有のコールバックＵＲＬである。
・${scope}は、
　〇ログインユースケースの場合、「loginScopes」属性の値として指定される範囲ストリングである。
【０２１９】
　〇プロビジョニングユースケースの場合、「provisioningScopes」属性の値として指定される範囲ストリングである。
・${clientCredentials}は、ベーシック認証スキームの認可ヘッダにおいて必要なクライアントＩＤおよびクライアントシークレットの標準ｂａｓｅ６４符号化表現である。
・${authorizationCode}は、ソーシャルｉｄｐからのコールバックとともに受けた認可コードである。
【０２２０】
　以下はログインユースケースのサンプルメタデータである。
【０２２１】

【表８】

```
{
"type": "SampleProviderForLogin",
"status": "enabled",
"idAttribute": "email",
"capabilities": [
"login"
],
"authorizePhase": {
"loginScopes": "<scope string>",
"url": "<Authorization endpoint>"
},
"authorizePhaseParameters": [
{
"value": "${socialIdentityProvider.consumerKey}",
"name": "client_id"
},
{
"value": "code",
"name": "response_type"
},
{
```

```
"value": "${scope}",
"name": "scope"
},
{
"value": "${state}",
"name": "state"
},
{
"value": "${redirectUri}",
"name": "redirect_uri"
}
],
"tokenPhase": {
"url": "<Token endpoint>",
"method": "<HTTP method for Token endpoint - get/post>"
},
"tokenPhaseHeaders": [
{
"value": "application/json",
"name": "Accept"
},
{
"value": "Basic ${clientCredentials}",
"name": "Authorization"
}
],
"tokenPhaseParameters": [
{
"value": "${socialIdentityProvider.consumerKey}",
"name": "client_id"
},
{
```

```
"value": "${socialIdentityProvider.consumerSecret}",
"name": "client_secret"
},
{
"value": "${redirectUri}",
"name": "redirect_uri"
},
{
"value": "${authorizationCode}",
"name": "code"
},
{
"value": "authorization_code",
"name": "grant_type"
}
],
"userInfoPhase": {
"url": "<UserInfo endpoint>",
"method": "<HTTP method for UserInfo endpoint - get/post>"
},
"userInfoPhaseHeaders": [
{
"value": "*/*",
"name": "Accept"
},
{
"value": "token ${accessToken}",
"name": "Authorization"
}
],
"userInfoPhaseParameters": [
{
```

```
"name": "access_token",
"value": "${accessToken}"
}
],
"userInfoAttributeMappings": [
{
"idpAttribute": "firstname",
"idcsAttribute": "given_name"
},
{
"idpAttribute": "lastname",
"idcsAttribute": "family_name"
},
{
"idpAttribute": "email.primary",
"idcsAttribute": "email"
}
],
"iconUrl":"<icon url>",
"schemas": [
"urn:ietf:params:scim:schemas:oracle:idcs:SocialIdentityProviderMetadata"
]
}
```

【０２２２】
以下はプロビジョニングユースケースのサンプルメタデータである。
【０２２３】

【表９】

```
{
"type": "SampleProviderForProvisioning",
"status": "enabled",
"capabilities": [
"provisioning"
],
"authorizePhase": {
"loginScopes": "<scope string>",
"url": "<Authorization endpoint>"
},
"authorizePhaseParameters": [
{
"value": "${socialIdentityProvider.consumerKey}",
"name": "client_id"
},
{
"value": "code",
"name": "response_type"
},
{
"value": "${scope}",
"name": "scope"
},
{
"value": "${state}",
"name": "state"
},
{
```

```
"value": "${redirectUri}",
"name": "redirect_uri"
}
],
"tokenPhase": {
"url": "<Token endpoint>",
"method": "<HTTP method for Token endpoint - get/post>"
},
"tokenPhaseHeaders": [
{
"value": "application/json",
"name": "Accept"
},
{
"value": "Basic ${clientCredentials}",
"name": "Authorization"
}
],
"tokenPhaseParameters": [
{
"value": "${socialIdentityProvider.consumerKey}",
"name": "client_id"
},
{
"value": "${socialIdentityProvider.consumerSecret}",
"name": "client_secret"
},
{
"value": "${redirectUri}",
"name": "redirect_uri"
},
{
```

```
"value": "${authorizationCode}",
"name": "code"
},
{
"value": "authorization_code",
"name": "grant_type"
}
],

"refreshTokenPhaseHeaders": [

{

"value": "application/json",

"name": "Accept"

}

],

"refreshTokenPhaseParameters": [

{

"value": "${socialIdentityProvider.consumerKey}",

"name": "client_id"

},

{

"value": "${socialIdentityProvider.consumerSecret}",

"name": "client_secret"
```

```
},
{
"value": "${refreshToken}",
"name": "refresh_token"
}
{
"value": "refresh_token",
"name": "grant_type"
}
],
"iconUrl":"<icon url>",
"schemas": [
"urn:ietf:params:scim:schemas:oracle:idcs:SocialIdentityProviderMetad
ata"
]
}
```

【０２２４】
周知のソリューションにおいて必要なカスタムコードの作成とは異なり、メタデータの使用は、テクニカルコーダ／プログラマではなく、特別の権限を有するユーザが実現できるものである。さらに、実施形態は、基礎となるソフトウェアに何ら変更を加えることなく、現行のシステムにおいて新規のソーシャルアイデンティティプロバイダに対するサポートを追加する機能を有する。これによりプロセスは大幅に高速化する。コードの開発およびデプロイのプロセスは時間を要するプロセスであるが、宣言型機構を用いると、新規プロバイダに対するサポートを数分で追加することができる。
【０２２５】
さらに、アイデンティティクラウドサービスはマルチテナントサービスなので、セキュリティの観点から、ユーザは、カスタム統合のためのコードを書き込むことおよびこのコードを共有ＩＤＣＳインスタンス上にデプロイすることができない。この問題は、ユーザがメタデータを定義することは認めるがカスタムコードをデプロイすることは認めない本発明の実施形態によって解決される。
【０２２６】
定義されたメタデータは、第三者アイデンティティプロバイダごとに異なっているであ

ろう。しかしながら、メタデータは、その宣言型という性質のおかげで、カスタムコードと比べて、生成するのが実質的に容易である。ユーザは、行われる必要があることを指定するだけでよくそれが如何にして行われるべきかを指定する必要はない。たとえば、ユーザは、ソーシャルプロバイダのトークンエンドポイントと、パラメータの所望の値とを、指定するだけでよく、トークンエンドポイントへの接続およびトークンの処理の方法について懸念する必要はない。

【０２２７】

開示されているように、実施形態は、ユーザが定義し格納する宣言型メタデータを使用することにより、第三者アイデンティティプロバイダがマルチテナントクラウドサービスのためのログイン機能を提供することを容易にする。ログインサービスおよび第三者アイデンティティプロバイダの指示でメタデータを取り出すＳＣＩＭ準拠ＲＥＳＴエンドポイントがエクスポーズされる。

【０２２８】

本明細書ではいくつかの実施形態が具体的に例示および／または記載されている。しかしながら、開示されている実施形態の修正および変形は、本発明の精神および意図する範囲から逸脱することなく、上記教示によってカバーされ以下の請求項の範囲に含まれることが、理解されるであろう。

【図面】

【図１】

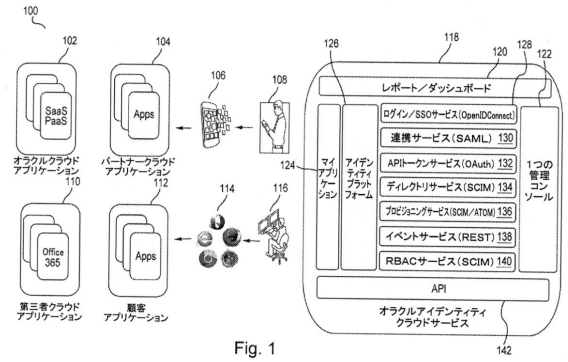

Fig. 1

【図２】

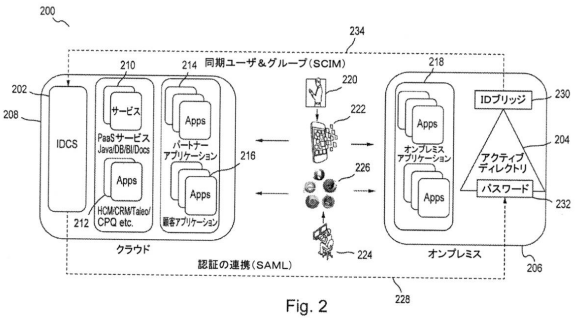

Fig. 2

【図３】

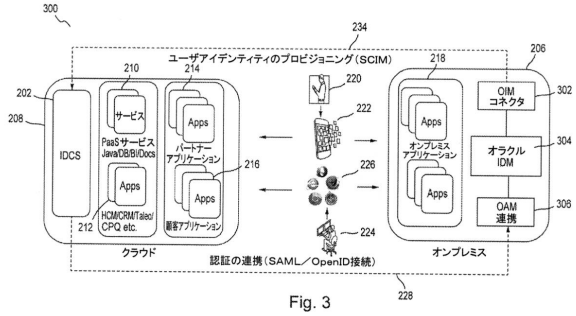

Fig. 3

【図４】

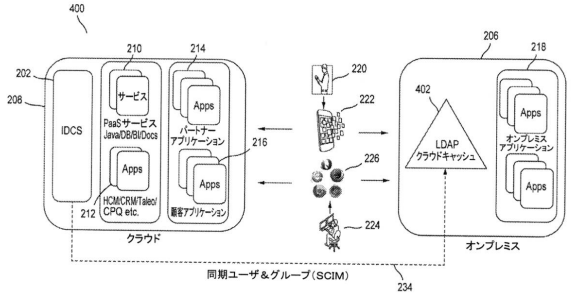

Fig. 4

【図５】

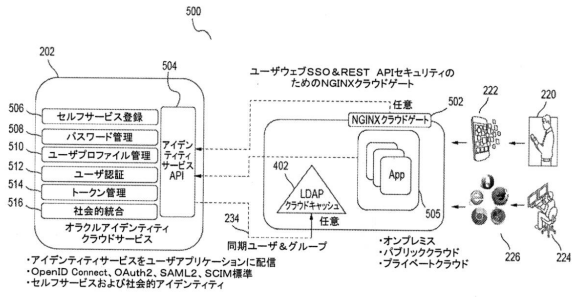

Fig. 5

【図６】

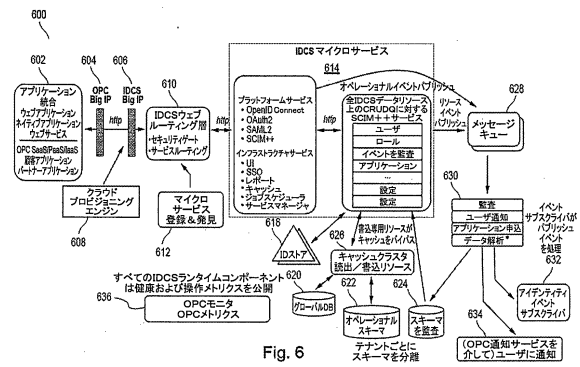

Fig. 6

【図６Ａ】

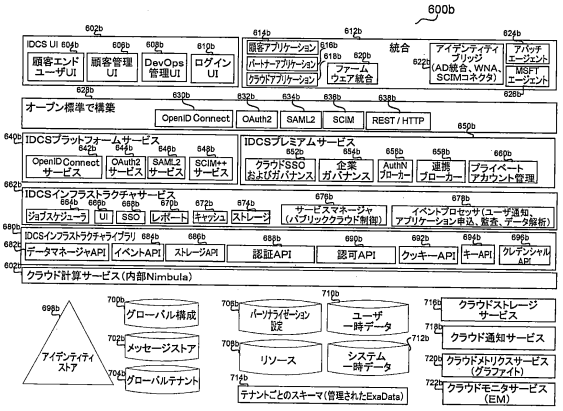

Fig. 6A

【図７】

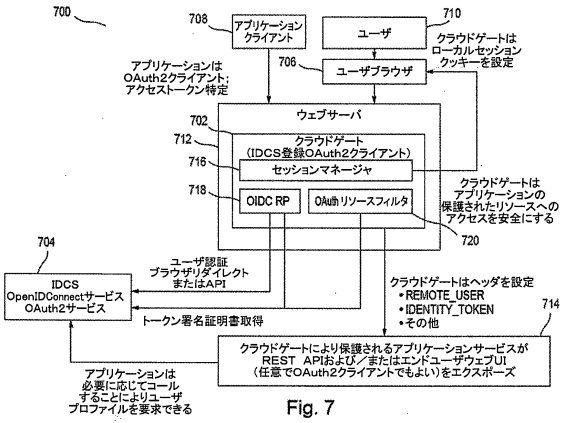

Fig. 7

【図８】

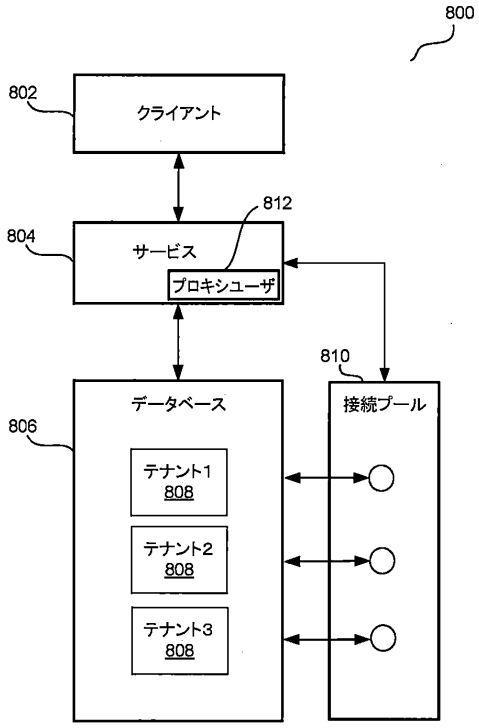

Fig. 8

【図９】

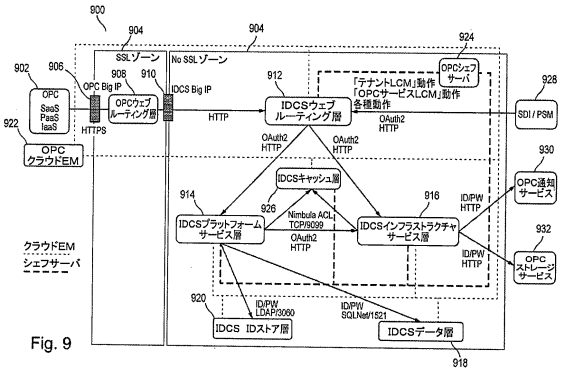

Fig. 9

【図１０】

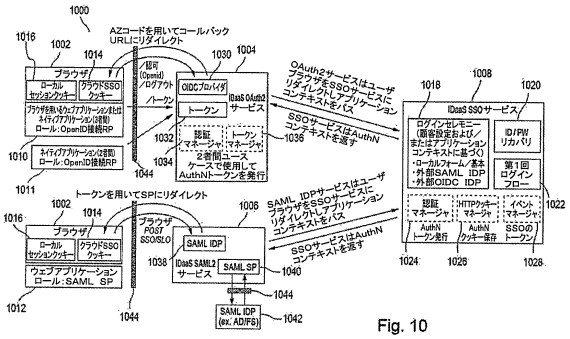

Fig. 10

【図１１】

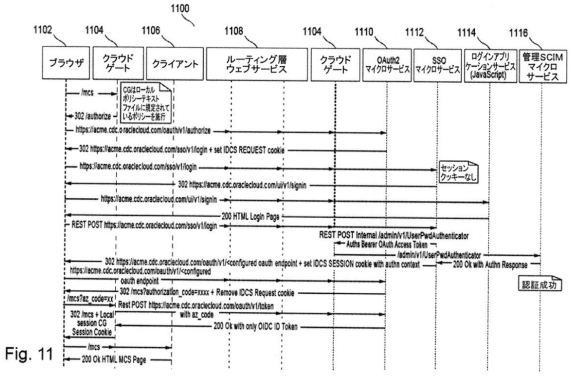

Fig. 11

【図１２】

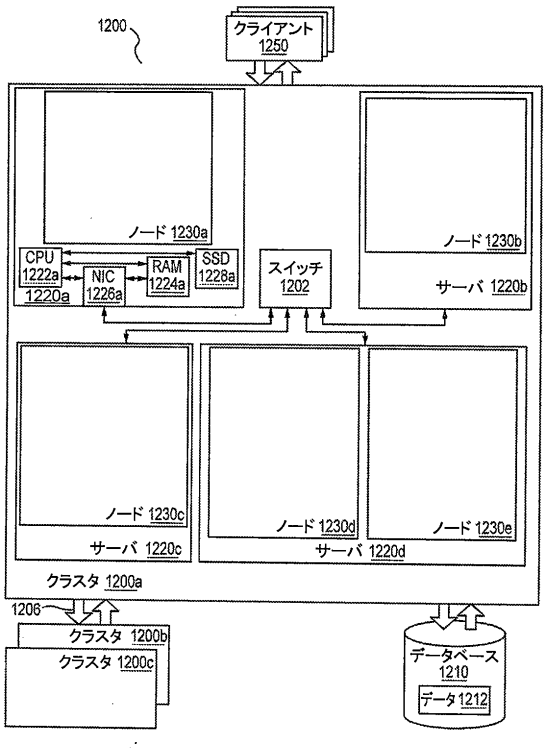

Fig. 12

【図１３】

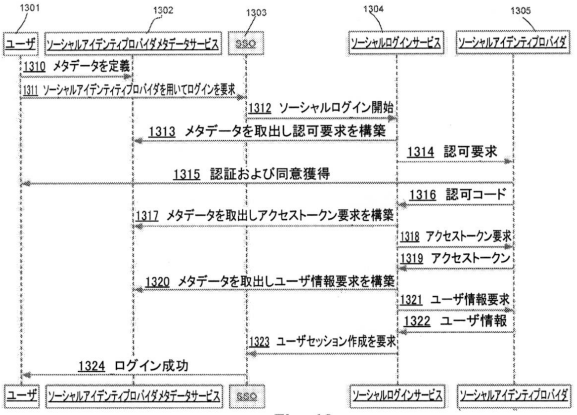

Fig. 13

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
ルニア州、サニーベール、コナマーラ・ウェイ、１２５、ナンバー・２７
審査官　局　成矢
(56)参考文献　米国特許出願公開第２０１６／００６５５４１（ＵＳ，Ａ１）
特開２０１７－００４２８６（ＪＰ，Ａ）
米国特許出願公開第２０１８／００８３９６７（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３３