(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6775013号
(P6775013)
(45)発行日　令和2年10月28日(2020.10.28)　(24)登録日　令和2年10月7日(2020.10.7)

(51)Int.Cl.　　F I
G06F 21/62 (2013.01)　　G06F 21/62 318
G06F 16/182 (2019.01)　　G06F 16/182
　　G06F 21/62 345

請求項の数 14　(全 53 頁)

(21)出願番号　特願2018-520611 (P2018-520611)
(86)(22)出願日　平成28年10月21日 (2016.10.21)
(65)公表番号　特表2019-501438 (P2019-501438A)
(43)公表日　平成31年1月17日 (2019.1.17)
(86)国際出願番号　PCT/US2016/058270
(87)国際公開番号　WO2017/070575
(87)国際公開日　平成29年4月27日 (2017.4.27)
審査請求日　令和1年7月2日 (2019.7.2)
(31)優先権主張番号　62/245,588
(32)優先日　平成27年10月23日 (2015.10.23)
(33)優先権主張国・地域又は機関
米国 (US)
(31)優先権主張番号　62/245,579
(32)優先日　平成27年10月23日 (2015.10.23)
(33)優先権主張国・地域又は機関
米国 (US)

(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
特許業務法人深見特許事務所
(72)発明者　ウー，ジン
アメリカ合衆国、９４４０４　カリフォルニア州、フォスター・シティ、ビスケーン・アベニュ、４１３

最終頁に続く

(54)【発明の名称】データテーブルを共有するためのサポートを有する構成の自己記述

(57)【特許請求の範囲】
【請求項１】
方法であって、
クラウドインフラストラクチャシステムが、前記クラウドインフラストラクチャシステムのクラウドベースのアプリケーションによって使用されるデータモデルにアプリケーションプログラミングインターフェイス（ＡＰＩ）を提供するステップと、
前記クラウドインフラストラクチャシステムが、前記ＡＰＩを介して前記データモデルの構成データに対する要求を受信するステップとを備え、前記要求は、クライアントデバイスと前記クラウドベースのアプリケーションとの間の通信を監視するデータセキュリティプロバイダによって生成され、前記方法はさらに、
前記クラウドインフラストラクチャシステムが、前記構成データを含む応答を生成するステップを備え、前記構成データは、前記データモデルを用いてモデル化されるエンティティの保護可能な属性のセットを含み、前記方法はさらに、
前記クラウドインフラストラクチャシステムが、前記保護可能な属性のセットのうち保護されるべき属性の表示を受信するステップと、
前記クラウドインフラストラクチャシステムが、前記保護可能な属性のセットのうち前記表示された属性を、保護されているものとしてマーキングするステップとを備え、
前記クラウドインフラストラクチャシステムは、前記クラウドベースのアプリケーションによって使用される前記データモデルを用いてモデル化される前記エンティティの前記保護可能な属性のセットを維持する、方法。

【請求項２】
前記構成データは、前記保護可能な属性のセット内の各属性に適用され得る保護のタイプをさらに含む、請求項１に記載の方法。
【請求項３】
前記保護のタイプは、トークン化可能であるか、または暗号化可能である、請求項２に記載の方法。
【請求項４】
前記保護可能な属性のセットのうち保護されるべき前記属性の前記表示は、前記属性に適用される前記保護のタイプの表示をさらに含む、請求項２または３に記載の方法。
【請求項５】
前記保護可能な属性のセットのうち保護されるべき前記属性の前記表示は、（ｉ）前記マーキングされた属性を含むすべてのデータオブジェクトが、データ値がどこで使用されようと当該マーキングされた属性は保護されるとのデータ値を含む、ようなデータレベルにおいて、または、（ｉｉ）前記マーキングされた属性を含む特定のタイプのデータオブジェクトが、データ値がどこで使用されようと当該マーキングされた属性は保護されるとのデータ値を含む、ようなコンポーネントレベルにおいて、新たな属性名を含み、
前記新たな属性名は、前記データセキュリティプロバイダによって認証される、請求項１～４のいずれか１項に記載の方法。
【請求項６】
前記クラウドインフラストラクチャシステムが、前記データモデルを利用するユーザインターフェイスまたはコンポーネントのための識別子と前記新たな属性名との間のマップを生成するステップと、
前記クラウドインフラストラクチャシステムが、前記データモデルを利用するユーザインターフェイスまたはコンポーネントに対する要求を前記クライアントデバイスから受信するステップと、
前記クラウドインフラストラクチャシステムが、前記ユーザインターフェイスまたはコンポーネントと前記マーキングされた属性および前記マップを有するペイロードとを含む応答を生成するステップとをさらに備える、請求項５に記載の方法。
【請求項７】
前記クラウドインフラストラクチャシステムが、前記データモデルを利用する前記ユーザインターフェイスまたはコンポーネントに対する後続の要求を前記クライアントデバイスから受信するステップをさらに備え、前記マーキングされた属性に関連付けられたデータ値は、トークン化されるか、または暗号化される、請求項６に記載の方法。
【請求項８】
方法であって、
クラウドインフラストラクチャシステムが、複数のデータオブジェクトをサポートする複数の列を有するデータベーステーブルの定義を受信するステップと、
前記クラウドインフラストラクチャシステムが、前記複数の列のうちの少なくとも１つの列をエンティティ識別子属性として識別する情報を受信するステップと、
前記クラウドインフラストラクチャシステムが、前記複数の列のうちの前記少なくとも１つの列を前記エンティティ識別子属性として指定するステップとを備え、前記複数のデータオブジェクトのうちの少なくとも１つのデータオブジェクトに対するクエリは、前記少なくとも１つのデータオブジェクトに関連付けられた前記エンティティ識別子属性を有する行セットを返し、前記方法はさらに、
前記クラウドインフラストラクチャシステムが、前記少なくとも１つのデータオブジェクトの複数の属性のうちの少なくとも１つの属性を保護フィールドとして識別する情報を受信するステップと、
前記クラウドインフラストラクチャシステムが、前記少なくとも１つの属性を保護フィールドとして指定するステップとを備え、
前記クラウドインフラストラクチャシステムは、前記少なくとも１つのデータオブジェ

クトの複数の属性のうちの少なくとも１つの属性を保護フィールドとして識別する情報を維持する、方法。
【請求項９】
前記複数の列のうちの前記少なくとも１つの列を前記エンティティ識別子属性として識別する情報を受信するステップは、前記複数の列のうちの前記少なくとも１つの列の選択をエンティティオブジェクトタイプとして受信するステップを備える、請求項８に記載の方法。
【請求項１０】
前記複数の列のうちの前記少なくとも１つの列を前記エンティティ識別子属性として識別する情報を受信するステップは、前記複数の列のうちの前記少なくとも１つの列の選択をインデックスとして受信するステップを備える、請求項８に記載の方法。
【請求項１１】
前記クラウドインフラストラクチャシステムが、前記少なくとも１つの属性を利用するユーザインターフェイスまたはコンポーネントに対する要求をクライアントデバイスから受信するステップと、
前記クラウドインフラストラクチャシステムが、前記ユーザインターフェイスまたはコンポーネントと保護されている少なくとも１つの属性とを含む応答を生成するステップとをさらに備える、請求項８～１０のいずれか１項に記載の方法。
【請求項１２】
前記クラウドインフラストラクチャシステムが、前記少なくとも１つの属性を利用する前記ユーザインターフェイスまたはコンポーネントに対する後続の要求を前記クライアントデバイスから受信するステップをさらに備え、前記少なくとも１つの属性に関連付けられたデータ値は、トークン化されるか、または暗号化される、請求項１１に記載の方法。
【請求項１３】
クラウドインフラストラクチャシステムであって、
プロセッサと、
命令セットを格納するメモリとを備え、前記命令セットは、前記プロセッサによって実行されたときに、前記プロセッサに、
クラウドベースのアプリケーションによって使用されるデータモデルにアプリケーションプログラミングインターフェイス（ＡＰＩ）を提供させ、
前記ＡＰＩを介して前記データモデルの構成データに対する要求を受信させ、前記要求は、クライアントデバイスと前記クラウドベースのアプリケーションとの間の通信を監視するデータセキュリティプロバイダによって生成され、前記命令セットはさらに、前記プロセッサによって実行されたときに、前記プロセッサに、
前記構成データを含む応答を生成させ、前記構成データは、前記データモデルを用いてモデル化されるエンティティの保護可能な属性のセットを含み、前記命令セットはさらに、前記プロセッサによって実行されたときに、前記プロセッサに、
前記保護可能な属性のセットのうち保護されるべき属性の表示を受信させ、
前記保護可能な属性のセットのうち前記表示された属性を、保護されているものとしてマーキングさせ、
前記クラウドインフラストラクチャシステムは、前記データモデルを用いてモデル化されるエンティティの保護可能な属性のセットを維持する、システム。
【請求項１４】
請求項１～１２のいずれか１項に記載の方法をクラウドインフラストラクチャシステムに実行させるためのプログラム。
【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、「構成の自己記述（SELF DESCRIBING CONFIGURATION）」と題される２０１５

年１０月２３日に出願された米国仮出願番号第６２／２４５，５８８号および「暗号化されたテキスト列とクリアテキスト列とで同一のテーブルを共有することのサポート（SUPPORT SHARING THE SAME TABLE FOR ENCRYPTED AND CLEAR TEXT COLUMNS）」と題される２０１５年１０月２３日に出願された米国仮出願番号第６２／２４５，５７９号からの優先権および利益を主張し、それらの内容全体は全ての目的で引用によって本明細書に援用される。

【背景技術】

【０００２】

発明の背景

データプライバシを統治する複雑に絡み合った規定および政策がある。最も頻繁に引用されるのは、医療保険の携行と責任に関する法律（Health Insurance Portability and Accountability Act：ＨＩＰＡＡ）およびペイメントカードインダストリデータセキュリティ基準（Payment Card Industry Data Security Standard：ＰＣＩＤＳＳ）である。欧州データ保護法は往々にしてさらに先を行っており、個人を特定できるいかなる情報もＥＵ外または国境外に移動させることを禁じている。これは、パブリッククラウドの無制限の使用に対していくつかの明らかな制約を課す。また、法執行機関または政府の当局者が会社を完全に飛び越えてクラウドサービスプロバイダから直接データにアクセスするおそれがあることを組織は心配している。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

たとえば、欧州データ保護法は、特定の人物に結び付けることができる個人データを欧州連合（ＥＵ）外またはさらには特定の国境外に移動させることを禁じている。このような法律は、組織がクラウドにデータを格納したりクラウド内のデータを処理したりすることを禁じている場合もある。なぜなら、インフラストラクチャプロバイダは複数の広範囲の場所でデータを格納したり、処理したり、バックアップしたりする可能性があるからである。アメリカでは、医療保険の携行と責任に関する法律（ＨＩＰＡＡ）などの規定は、個人健康情報（personal health information：ＰＨＩ）に関わるセキュリティおよびプライバシーを維持することを命じている。そうすることが複雑であることにより、医療サービス提供者は、医療サービスのコスト上昇を減速させ得るコスト効率のよいパブリッククラウドベースのソリューションを使用することを思いとどまる場合がある。

【０００４】

データセキュリティ、レジデンシおよびプライバシの問題を回避する１つの方法は、クラウドに入るデータを難読化するというものである。２つの一般的な難読化方法は、暗号化およびトークン化である。これらのアプローチのいずれかを用いることにより、組織がクラウドベースのアプリケーションの利益を享受しながら依然として詮索の目がデータを解読できない状態が保証される。暗号化は、アルゴリズムスキームを用いてプレーンテキスト情報を読取不可能な暗号化テキストに変換する。情報を復号化してそれを元のプレーンテキスト形式に戻すためには、鍵（または、アルゴリズム）が必要である。トークン化は、機密データの保護のための人気上昇中のアプローチである。トークン化は、実際の値の代わりにトークン（または、エイリアス）によるデータ置換を使用することを含む。数学的プロセスを用いてデータを変換する暗号化とは異なって、トークン化は、ランダムな文字を用いて実際のデータを置換する。トークンを解読してそれを実際のデータに戻すことができる「鍵」はない。

【０００５】

トークン化のプロセスでは、機密データは、機密データを安全に格納する「ボールト（vault）」と呼ばれる集中型の非常に安全なサーバに送信される。同時に、ランダムな固有の文字セット（トークン）が生成され、返されて、実際のデータの代わりに使用される。ボールトマネージャは、再び必要とされたときにトークン値を実際のデータと交換することを可能にする参照データベースを維持する。一方、詮索の目にとっては何の意味もも

たないトークン値を、実際のデータの信頼できる代用物としてさまざまなクラウドベースのアプリケーションで使用することができる。

【０００６】

商店主は、しばしば、販売が完了した後に、慎重な扱いを要するクレジットカード情報の代わりにトークン化されたデータを使用する。これにより、商店主は、実際のカードデータを危険にさらすことなく顧客の取引に関する販売分析を行うことができる。さらに、ＰＣＩは、支払取引以外のどんなものにも生のカードデータを使用することを禁じている。取引後データをトークン化することによって、商店主はＰＣＩ負担を減少させることができる。なぜなら、バックエンドシステムには機密データは存在しないからである。

【０００７】

同一の方法は、患者記録、顧客口座記録、人材情報などを含む他のタイプの機密データにも適用することができる。実際のデータのトークン化は、データが危険にさらされることから守り、セキュリティ、レジデンシおよびプライバシに対する要求に応える。トークン化されたデータは、紛失または盗難されても実際のデータに戻すことができないので、どこにでも、クラウド内にさえ、格納して使用することができる。

【課題を解決するための手段】

【０００８】

発明の簡単な概要

本開示の以下の部分は、少なくとも主題を基本的に理解できるようにする目的で、本開示に記載されている１つ以上の革新的技術、実施形態および／または実施例の簡単な概要を提供する。この概要は、いずれかの特定の実施形態または実施例の広範囲にわたる概略を提供しようとしているわけではない。また、この概要は、ある実施形態または実施例の重要な／不可欠な要素を識別することを意図したものではなく、または本開示の主題の範囲を図示することを意図したものでもない。したがって、この概要の１つの目的は、簡略化した形で本開示に記載されているいくつかの革新的技術、実施形態および／または実施例を、以下に記載するより詳細な説明に対する前置きとして提供することであり得る。

【０００９】

例示的な実施形態では、コンピューティングデバイスによって実行される方法が提供される。上記方法は、クラウドベースのアプリケーションによって使用されるデータモデルに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）を提供するステップと、上記ＡＰＩを介して上記データモデルの構成データに対する要求を受信するステップとを含む。上記要求は、クライアントデバイスと上記クラウドベースのアプリケーションとの間の通信を監視するデータセキュリティプロバイダによって生成される。上記方法はさらに、上記構成データを含む応答を生成するステップを含む。上記構成データは、上記データモデルを用いてモデル化されるエンティティの保護可能な属性のセットを含む。上記方法はさらに、上記保護可能な属性のセットからの保護されるべき属性の表示を受信するステップと、上記保護可能な属性のセットからの上記表示された属性を、保護されているものとしてマーキングするステップとを含む。

【００１０】

いくつかの実施形態では、上記構成データは、上記保護可能な属性のセット内の各属性に適用され得る保護のタイプをさらに含む。任意に、上記保護のタイプは、トークン化可能であるか、または暗号化可能である。任意に、上記保護可能な属性のセットからの保護されるべき上記属性の上記表示は、上記属性に適用される上記保護のタイプの表示をさらに含む。

【００１１】

いくつかの実施形態では、上記方法は、上記データモデルを利用するユーザインターフェイスまたはコンポーネントに対する要求を上記クライアントデバイスから受信するステップと、上記ユーザインターフェイスまたはコンポーネントと上記保護されているものとしてマーキングされた属性とを含む応答を生成するステップと、上記データモデルを利用する上記ユーザインターフェイスまたはコンポーネントに対する後続の要求を上記クライ

アントデバイスから受信するステップをさらに含み、上記マーキングされた属性に関連付けられたデータ値は、トークン化されるか、または暗号化される。

【００１２】

例示的な実施形態では、命令を格納した非一時的な機械読取可能な記憶媒体が提供され、上記命令は、１つ以上のプロセッサによって実行されたときに、上記１つ以上のプロセッサに方法を実行させる。上記方法は、クラウドベースのアプリケーションによって使用されるデータモデルにアプリケーションプログラミングインターフェイス（ＡＰＩ）を提供するステップと、上記ＡＰＩを介して上記データモデルの構成データに対する要求を受信するステップとを含む。上記要求は、クライアントデバイスと上記クラウドベースのアプリケーションとの間の通信を監視するデータセキュリティプロバイダによって生成される。上記方法はさらに、上記構成データを含む応答を生成するステップを含む。上記構成データは、上記データモデルを用いてモデル化されるエンティティの保護可能な属性のセットを含む。上記方法はさらに、上記保護可能な属性のセットからの保護されるべき属性の表示を受信するステップと、上記保護可能な属性のセットからの上記表示された属性を、保護されているものとしてマーキングするステップとを含む。

【００１３】

いくつかの実施形態では、上記構成データは、上記保護可能な属性のセット内の各属性に適用され得る保護のタイプをさらに含む。任意に、上記保護のタイプは、トークン化可能であるか、または暗号化可能である。任意に、上記保護可能な属性のセットからの保護されるべき上記属性の上記表示は、上記属性に適用される上記保護のタイプの表示をさらに含む。

【００１４】

いくつかの実施形態では、上記方法はさらに、上記データモデルを利用するユーザインターフェイスまたはコンポーネントに対する要求を上記クライアントデバイスから受信するステップと、上記ユーザインターフェイスまたはコンポーネントと上記保護されているものとしてマーキングされた属性とを含む応答を生成するステップと、上記データモデルを利用する上記ユーザインターフェイスまたはコンポーネントに対する後続の要求を上記クライアントデバイスから受信するステップとをさらに含み、上記マーキングされた属性に関連付けられたデータ値は、トークン化されるか、または暗号化される。

【００１５】

例示的な実施形態では、プロセッサと、命令セットを格納するメモリとを含むシステムが提供され、上記命令セットは、上記プロセッサによって実行されたときに、上記プロセッサに方法を実行させる。上記方法は、クラウドベースのアプリケーションによって使用されるデータモデルにアプリケーションプログラミングインターフェイス（ＡＰＩ）を提供するステップと、上記ＡＰＩを介して上記データモデルの構成データに対する要求を受信するステップとを含む。上記要求は、クライアントデバイスと上記クラウドベースのアプリケーションとの間の通信を監視するデータセキュリティプロバイダによって生成される。上記方法はさらに、上記構成データを含む応答を生成するステップを含む。上記構成データは、上記データモデルを用いてモデル化されるエンティティの保護可能な属性のセットを含む。上記方法はさらに、上記保護可能な属性のセットからの保護されるべき属性の表示を受信するステップと、上記保護可能な属性のセットからの上記表示された属性を、保護されているものとしてマーキングするステップとを含む。

【００１６】

いくつかの実施形態では、上記構成データは、上記保護可能な属性のセット内の各属性に適用され得る保護のタイプをさらに含む。任意に、上記保護のタイプは、トークン化可能であるか、または暗号化可能である。任意に、上記保護可能な属性のセットからの保護されるべき上記属性の上記表示は、上記属性に適用される上記保護のタイプの表示をさらに含む。

【００１７】

いくつかの実施形態では、上記方法はさらに、上記データモデルを利用するユーザイン

ターフェイスまたはコンポーネントに対する要求を上記クライアントデバイスから受信するステップと、上記ユーザインターフェイスまたはコンポーネントと上記保護されているものとしてマーキングされた属性とを含む応答を生成するステップと、上記データモデルを利用する上記ユーザインターフェイスまたはコンポーネントに対する後続の要求を上記クライアントデバイスから受信するステップとをさらに含み、上記マーキングされた属性に関連付けられたデータ値は、トークン化されるか、または暗号化される。

【００１８】

例示的な実施形態では、コンピューティングデバイスによって実行される方法が提供される。上記方法は、複数のデータオブジェクトをサポートする複数の列を有するデータベーステーブルの定義を受信するステップと、上記複数の列のうちの少なくとも１つの列をエンティティ識別子属性として識別する情報を受信するステップと、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として指定するステップとを含む。上記複数のデータオブジェクトのうちの少なくとも１つのデータオブジェクトに対するクエリは、上記少なくとも１つのデータオブジェクトに関連付けられた上記エンティティ識別子属性を有する行セットを返す。上記方法はさらに、上記少なくとも１つのデータオブジェクトの複数の属性のうちの少なくとも１つの属性を保護フィールドとして識別する情報を受信するステップと、上記少なくとも属性を保護フィールドとして指定するステップとを含む。

【００１９】

いくつかの実施形態では、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として識別する情報を受信するステップは、上記複数の列のうちの上記少なくとも１つの列の選択をエンティティオブジェクトタイプとして受信するステップを備える。任意に、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として識別する情報を受信するステップは、上記複数の列のうちの上記少なくとも１つの列の選択をインデックスとして受信するステップを備える。任意に、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として指定するステップは、上記少なくとも１つのデータオブジェクトに従って、予め定められた値を設定するステップを備える。

【００２０】

いくつかの実施形態では、上記方法は、上記少なくとも属性を利用するユーザインターフェイスまたはコンポーネントに対する要求をクライアントデバイスから受信するステップと、上記ユーザインターフェイスまたはコンポーネントと上記保護されている少なくとも属性とを含む応答を生成するステップと、上記少なくとも属性を利用する上記ユーザインターフェイスまたはコンポーネントに対する後続の要求を上記クライアントデバイスから受信するステップをさらに含み、上記少なくとも属性に関連付けられたデータ値は、トークン化されるか、または暗号化される。

【００２１】

例示的な実施形態では、命令を格納した非一時的な機械読取可能な記憶媒体が提供され、上記命令は、１つ以上のプロセッサによって実行されたときに、上記１つ以上のプロセッサに方法を実行させる。上記方法は、複数のデータオブジェクトをサポートする複数の列を有するデータベーステーブルの定義を受信するステップと、上記複数の列のうちの少なくとも１つの列をエンティティ識別子属性として識別する情報を受信するステップと、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として指定するステップとを含む。上記複数のデータオブジェクトのうちの少なくとも１つのデータオブジェクトに対するクエリは、上記少なくとも１つのデータオブジェクトに関連付けられた上記エンティティ識別子属性を有する行セットを返す。上記方法はさらに、上記少なくとも１つのデータオブジェクトの複数の属性のうちの少なくとも１つの属性を保護フィールドとして識別する情報を受信するステップと、上記少なくとも属性を保護フィールドとして指定するステップとを含む。

【００２２】

いくつかの実施形態では、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として識別する情報を受信するステップは、上記複数の列のうちの上記少なくとも１つの列の選択をエンティティオブジェクトタイプとして受信するステップを備える。任意に、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として識別する情報を受信するステップは、上記複数の列のうちの上記少なくとも１つの列の選択をインデックスとして受信するステップを備える。任意に、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として指定するステップは、上記少なくとも１つのデータオブジェクトに従って、予め定められた値を設定するステップを備える。

【００２３】

いくつかの実施形態では、上記方法は、上記少なくとも属性を利用するユーザインターフェイスまたはコンポーネントに対する要求をクライアントデバイスから受信するステップと、上記ユーザインターフェイスまたはコンポーネントと上記保護されている少なくとも属性とを含む応答を生成するステップと、上記少なくとも属性を利用する上記ユーザインターフェイスまたはコンポーネントに対する後続の要求を上記クライアントデバイスから受信するステップをさらに含み、上記少なくとも属性に関連付けられたデータ値は、トークン化されるか、または暗号化される。

【００２４】

例示的な実施形態では、プロセッサと、命令セットを格納するメモリとを含むシステムが提供され、上記命令セットは、上記プロセッサによって実行されたときに、上記プロセッサに方法を実行させる。上記方法は、複数のデータオブジェクトをサポートする複数の列を有するデータベーステーブルの定義を受信するステップと、上記複数の列のうちの少なくとも１つの列をエンティティ識別子属性として識別する情報を受信するステップと、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として指定するステップとを含む。上記複数のデータオブジェクトのうちの少なくとも１つのデータオブジェクトに対するクエリは、上記少なくとも１つのデータオブジェクトに関連付けられた上記エンティティ識別子属性を有する行セットを返す。上記方法はさらに、上記少なくとも１つのデータオブジェクトの複数の属性のうちの少なくとも１つの属性を保護フィールドとして識別する情報を受信するステップと、上記少なくとも属性を保護フィールドとして指定するステップとを含む。

【００２５】

いくつかの実施形態では、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として識別する情報を受信するステップは、上記複数の列のうちの上記少なくとも１つの列の選択をエンティティオブジェクトタイプとして受信するステップを備える。任意に、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として識別する情報を受信するステップは、上記複数の列のうちの上記少なくとも１つの列の選択をインデックスとして受信するステップを備える。任意に、上記複数の列のうちの上記少なくとも１つの列を上記エンティティ識別子属性として指定するステップは、上記少なくとも１つのデータオブジェクトに従って、予め定められた値を設定するステップを備える。

【００２６】

いくつかの実施形態では、上記方法は、上記少なくとも属性を利用するユーザインターフェイスまたはコンポーネントに対する要求をクライアントデバイスから受信するステップと、上記ユーザインターフェイスまたはコンポーネントと上記保護されている少なくとも属性とを含む応答を生成するステップと、上記少なくとも属性を利用する上記ユーザインターフェイスまたはコンポーネントに対する後続の要求を上記クライアントデバイスから受信するステップをさらに含み、上記少なくとも属性に関連付けられたデータ値は、トークン化されるか、または暗号化される。

【００２７】

本開示の主題の本質およびその等価物（ならびに、提供されるいかなる固有のまたは明

白な利点および改良点）のさらなる理解は、上記のセクションに加えて、本開示の残りの箇所、添付の図面および特許請求の範囲を参照することによって実現されるべきである。

【００２８】

本開示に記載されている革新的技術、実施形態および／または実施例を合理的に説明し図示するために、１つ以上の添付の図面を参照し得る。１つ以上の添付の図面を説明するために使用されるさらなる詳細または例は、記載されている発明のいずれの範囲に対しても、ここに記載されている実施形態および／または実施例のいずれの範囲に対しても、または本開示に提示されている、現在のところ最良の形態であると理解されている革新的技術のいずれの範囲に対しても、限定として考えられるべきではない。

【図面の簡単な説明】

【００２９】

【図１】本発明に係る一実施形態におけるクラウドベースのアプリケーションを開発するためのシステム環境のブロック図である。

【図２】本発明に係る一実施形態におけるクラウドベースのアプリケーションでプライバシ、レジデンシおよびセキュリティを提供するシステムのブロック図である。

【図３Ａ】本発明に係る一実施形態におけるクライアントデバイスを用いて企業インフラストラクチャシステム内から見たときの、クラウドベースのアプリケーションに関連付けられたユーザインターフェイス（user interface：ＵＩ）ページの図である。

【図３Ｂ】本発明に係る一実施形態におけるクラウドインフラストラクチャシステム内から見たときの、クラウドベースのアプリケーションに関連付けられたＵＩページの図である。

【図４】本発明に係る一実施形態におけるエンティティ間で共有される属性を示すブロック図である。

【図５】本発明に係る一実施形態におけるプライバシ、レジデンシおよびセキュリティサーバの自己記述的な構成を提供するメッセージシーケンス図である。

【図６】本発明に係る一実施形態における自己記述的な構成を利用するためのメッセージシーケンス図である。

【図７】本発明の一実施形態に係る自己記述的な構成を有するクラウドベースのアプリケーションに関して用いられるさまざまな層を示す図である。

【図８】本発明に係る一実施形態における暗号化された列とクリアテキスト列とで同一のテーブルを共有することをサポートするための方法のフローチャートである。

【図９】本発明に係る一実施形態における保護フィールドの自動オペレーション検出方法のフローチャートである。

【図１０】本発明に係る一実施形態における連合検索（federated search）の方法のフローチャートである。

【図１１】実施形態のうちの１つを実現するための分散型システムの簡略図である。

【図１２】本発明のさまざまな実施形態を実現することができる例示的なコンピュータシステムの図である。

【発明を実施するための形態】

【００３０】

発明の詳細な説明

Ⅰ．はじめに

以下の記載では、説明を目的として、本発明の実施形態が完全に理解されるように具体的な詳細が記載されている。しかし、これらの具体的な詳細がなくてもさまざまな実施形態は実施可能であるということが明らかであろう。たとえば、不必要な程に詳細に実施形態を曖昧にすることのないように、回路、システム、ネットワーク、プロセスおよび他のコンポーネントは、ブロック図の形式でコンポーネントとして示されてもよい。他の例では、実施形態を曖昧にすることを回避するために、周知の回路、プロセス、アルゴリズム、構造および技術は、不必要な詳細なしで示されてもよい。図面および説明は、限定的であるように意図されるものではない。むしろ、以下の例示的な実施形態の説明は、例示的

な実施形態を実現するための実施可能な説明を当業者に提供するものである。添付の特許請求の範囲に記載されている本発明の精神および範囲から逸脱することなく、要素の機能および配置をさまざまに変更できることが理解されるべきである。

【００３１】

なお、また、個々の実施形態は、フローチャート、フロー図、データフロー図、構造図またはブロック図として示されるプロセスとして説明してもよい。フローチャートは動作をシーケンシャルなプロセスとして説明し得るが、多くの動作は並列または同時に実行されてもよい。また、動作の順序は並べ替えてもよい。プロセスは、その動作が完了すると終了するが、図に含まれていないさらなるステップを有していてもよい。プロセスは、方法、機能、手順、サブルーチン、サブプログラムなどに対応し得る。プロセスが機能に対応する場合、その終了は、呼出し機能またはメイン機能への機能の戻りに対応し得る。

【００３２】

「機械読取可能な媒体」または「コンピュータ読取可能な媒体」という語は、命令および／またはデータを格納したり、含んでいたり、または伝えたりすることができる携帯型または固定式のストレージデバイス、光学式ストレージデバイス、無線チャネルおよびさまざまな他の媒体を含むが、これらに限定されるものではない。コードセグメントまたは機械実行可能な命令は、手順、機能、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、または、命令、データ構造もしくはプログラム文のいずれかの組み合わせを表わし得る。コードセグメントは、情報、データ、引数、パラメータまたはメモリコンテンツを受け渡すおよび／または受信することによって、別のコードセグメントまたはハードウェア回路に結合されてもよい。情報、引数、パラメータ、データなどは、メモリ共有、メッセージ受け渡し、トークン受け渡し、ネットワーク送信などを含む任意の好適な手段によって受け渡されたり、転送されたり、または送信されたりしてもよい。

【００３３】

さらに、実施形態は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語、またはそれらのいずれかの組み合わせによって実現されてもよい。ソフトウェア、ファームウェア、ミドルウェアまたはマイクロコードで実現される場合、必要なタスクを実行するためのプログラムコードまたはコードセグメントは、機械読取可能またはコンピュータ読取可能な媒体に格納されてもよい。１つ以上のプロセッサが必要なタスクを実行してもよい。

【００３４】

図面のうちのいくつかに示されているシステムは、さまざまな構成で提供されてもよい。いくつかの実施形態では、システムは、システムの１つ以上のコンポーネントがクラウドコンピューティングシステム内の１つ以上のネットワークにわたって分散される分散型システムとして構成されてもよい。さらなる実施形態では、システムは、システムの１つ以上のコンポーネントが単一の構造またはパッケージに統合される単一のシステムとして構成されてもよい。

【００３５】

ＩＩ．クラウドベースのアプリケーションの開発

アプリケーションとは、実行時に特定の所望のタスクを実行するソフトウェアプログラムのことである。一般に、１つ以上のオペレーティングシステム（「ＯＳ」）、（たとえば、Ｊａｖａ（登録商標）プログラミング言語をサポートする）仮想マシン、デバイスドライバなどを含むランタイム環境では、いくつかのアプリケーションが実行される。開発者は、しばしば、所望のアプリケーションを実現／開発するためにアプリケーション開発フレームワーク（Application Development Framework：「ＡＤＦ」）（これ自体がアプリケーションである）を使用する。ＡＤＦは、アプリケーションの開発に直接的／間接的に使用できる予め規定されたコード／データモジュールのセットを提供する。また、ＡＤＦは、統合開発環境（integrated development environment：「ＩＤＥ」）、コード生成プログラム、デバッガなどのツールも提供し得る。一般に、ＡＤＦは、再利用可能なコン

ポーネントを提供することによってアプリケーション開発を簡略化し、当該再利用可能なコンポーネントは、たとえば所望のタスクを実行するようにコンポーネントを選択して、選択されたコンポーネントの外観、挙動および対話を定義することによって、ユーザインターフェイス（「ＵＩ」）およびアプリケーションロジックを定義するようにアプリケーション開発者によって使用され得る。オラクル社からの「オラクルＡＤＦ（Oracle ADF）」などのいくつかのＡＤＦは、疎結合ならびに容易なアプリケーション開発およびメンテナンスを促進するモデル・ビュー・コントローラ（model-view-controller：「ＭＶＣ」）設計パターンに基づく。

【００３６】

図１は、本発明に係る一実施形態におけるクラウドベースのアプリケーションを開発するためのシステム環境１００のブロック図である。示されている実施形態では、システム環境１００は、１つ以上のクライアントコンピューティングデバイス１０４，１０６および１０８にクラウドサービスを提供するクラウドインフラストラクチャシステム１０２を含む。クライアントコンピューティングデバイス１０４，１０６および１０８は、クラウドインフラストラクチャシステム１０２と対話するようにユーザによって使用され得る。クライアントコンピューティングデバイス１０４，１０６および１０８は、ウェブブラウザ、所有権付きクライアントアプリケーション（たとえば、オラクルフォームズ（Oracle Forms））または何らかの他のアプリケーションなどのクライアントアプリケーションを動作させるように構成され得て、当該クライアントアプリケーションは、クラウドインフラストラクチャシステム１０２と対話してクラウドインフラストラクチャシステム１０２によって提供されるサービスを使用するようにクライアントコンピューティングデバイスのユーザによって使用され得る。

【００３７】

クラウドインフラストラクチャシステム１０２は、示されているもの以外のコンポーネントを有していてもよい。さらに、図１に示される実施形態は、本発明の実施形態を組み込むことができるクラウドインフラストラクチャシステムの一例に過ぎない。いくつかの他の実施形態では、クラウドインフラストラクチャシステム１０２は、図１に示されるよりも多くのコンポーネントもしくは少ないコンポーネントを有していてもよく、２つ以上のコンポーネントを組み合わせてもよく、またはコンポーネントの異なる構成もしくは配置を有していてもよい。

【００３８】

クライアントコンピューティングデバイス１０４，１０６および１０８は、携帯可能な手持ち式のデバイス（たとえば、ｉＰｈｏｎｅ（登録商標）、セルラー電話、ｉＰａｄ（登録商標）、コンピューティングタブレット、携帯情報端末（personal digital assistant：「ＰＤＡ」））またはウェアラブルデバイス（たとえば、Ｇｏｏｇｌｅ Ｇｌａｓｓ（登録商標）頭部装着型ディスプレイ）であってもよく、Ｍｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ Ｍｏｂｉｌｅ（登録商標）などのソフトウェア、および／もしくは、ｉＯＳ、Ｗｉｎｄｏｗｓ Ｐｈｏｎｅ、Ａｎｄｒｏｉｄ、ＢｌａｃｋＢｅｒｒｙ １０、Ｐａｌｍ ＯＳなどのさまざまなモバイルＯＳを実行し、インターネット、電子メール、ショートメッセージサービス（short message service：「ＳＭＳ」）、ＢｌａｃｋＢｅｒｒｙ（登録商標）、または使用可能な他の通信プロトコルである。クライアントコンピューティングデバイス１０４，１０６および１０８は、汎用パーソナルコンピュータであってもよく、一例として、Ｍｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ（登録商標）、Ａｐｐｌｅ Ｍａｃｉｎｔｏｓｈ（登録商標）および／またはＬｉｎｕｘ（登録商標）ＯＳのさまざまなバージョンを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを含む。クライアントコンピューティングデバイス１０４，１０６および１０８は、さまざまな市販のＵＮＩＸ（登録商標）またはＵＮＩＸのようなＯＳのうちのいずれかを実行するワークステーションコンピュータであってもよく、当該市販のＵＮＩＸ（登録商標）またはＵＮＩＸのようなＯＳとしては、たとえばＧｏｏｇｌｅ Ｃｈｒｏｍｅ ＯＳなどのさまざまなＧＮＵ／Ｌｉｎｕｘ ＯＳが挙げられるが、これらに限定されるものではない。

代替的に、または加えて、クライアントコンピューティングデバイス１０４，１０６および１０８は、ネットワーク１１０を介して通信することができる、シンクライアントコンピュータ、インターネットにより可能化されるゲームシステム（たとえば、Ｋｉｎｅｃｔ（登録商標）ジェスチャ入力デバイスを有するまたは持たないＭｉｃｒｏｓｏｆｔ　Ｘｂｏｘゲームコンソール）および／または個人メッセージ伝達デバイスなどのその他の電子デバイスであってもよい。

【００３９】

例示的なシステム環境１００は、３つのクライアントコンピューティングデバイスを有するものとして示されているが、いかなる数のクライアントコンピューティングデバイスがサポートされてもよい。センサを有するデバイスなどの他のデバイスがクラウドインフラストラクチャシステム１０２と対話してもよい。

【００４０】

ネットワーク１１０は、クライアント１０４，１０６および１０８とクラウドインフラストラクチャシステム１０２との間のデータの通信および交換を容易にすることができる。ネットワーク１１０は、さまざまな市販のプロトコルのうちのいずれかを用いてデータ通信をサポートすることができる、当業者に馴染のあるいずれかのタイプのネットワークであってもよく、当該市販のプロトコルとしては、伝送制御プロトコル／インターネットプロトコル（transmission control protocol/Internet protocol：「ＴＣＰ／ＩＰ」）、システムネットワークアーキテクチャ（systems network architecture：「ＳＮＡ」）、インターネットパケット交換（Internet packet exchange：「ＩＰＸ」）、ＡｐｐｌｅＴａｌｋなどが挙げられるが、これらに限定されるものではない。一例に過ぎないが、ネットワーク１１０は、イーサネット（登録商標）、トークンリングなどに基づくものなどのローカルエリアネットワーク（local area network：「ＬＡＮ」）であってもよい。ネットワーク１１０は、ワイドエリアネットワークおよびインターネットであってもよい。ネットワーク１１０は、仮想ネットワークを含み得て、当該仮想ネットワークとしては、仮想プライベートネットワーク（virtual private network：「ＶＰＮ」）、イントラネット、エクストラネット、公衆交換電話網（public switched telephone network：「ＰＳＴＮ」）、赤外線ネットワーク、無線ネットワーク（たとえば、米国電気電子学会（Institute of Electrical and Electronics：「ＩＥＥＥ」）８０２．１１プロトコル一式、ブルートゥース（登録商標）および／またはその他の無線プロトコルのうちのいずれかの下で動作するネットワーク）、および／または、これらのいずれかの組み合わせおよび／または他のネットワークが挙げられるが、これらに限定されるものではない。

【００４１】

クラウドインフラストラクチャシステム１０２は、１つ以上のコンピュータおよび／またはサーバを備え得る。これらのコンピュータシステムまたはサーバは、１つ以上の汎用コンピュータ、専用サーバコンピュータ（一例として、パーソナルコンピュータ（personal computer：「ＰＣ」）サーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウント型サーバなどを含む）、サーバファーム、サーバクラスタ、またはその他の適切な配置および／もしくは組み合わせで構成されてもよい。さまざまな実施形態では、クラウドインフラストラクチャシステム１０２に関連付けられた１つ以上のコンピュータシステムまたはサーバは、上記の開示に記載された１つ以上のサービスまたはソフトウェアアプリケーションを実行するように適合され得る。たとえば、クラウドインフラストラクチャシステム１０２に関連付けられた１つ以上のコンピュータシステムまたはサーバは、本開示の実施形態に従って本明細書に記載されている処理を実行するためのサーバに対応してもよい。

【００４２】

クラウドインフラストラクチャシステム１０２に関連付けられた１つ以上のコンピュータシステムまたはサーバは、上記のもののうちのいずれかおよび任意の市販のサーバＯＳを含むＯＳを実行し得る。また、クラウドインフラストラクチャシステム１０２に関連付けられた１つ以上のコンピュータシステムまたはサーバは、さまざまなさらなるサーバア

プリケーションおよび／または中間層アプリケーションのうちのいずれかを実行してもよく、当該さらなるサーバアプリケーションおよび／または中間層アプリケーションは、ハイパーテキスト転送プロトコル（hypertext transport protocol：「ＨＴＴＰ」）サーバ、ファイル転送プロトコル（file transfer protocol：「ＦＴＰ」）サーバ、コモンゲートウェイインターフェイス（common gateway interface：「ＣＧＩ」）サーバ、ＪＡＶＡ（登録商標）サーバ、データベースサーバなどを含む。

【００４３】

特定の実施形態では、クラウドインフラストラクチャシステム１０２によって提供されるサービスは、オンラインデータ格納およびバックアップソリューション、ウェブベースの電子メールサービス、提供されるオフィススイートおよびドキュメントコラボレーションサービス、データベース処理、管理されるテクニカルサポートサービスなどの、クラウドインフラストラクチャシステム１０２のユーザがオンデマンドで利用できる多くのサービスを含み得る。クラウドインフラストラクチャシステム１０２によって提供されるサービスは、そのユーザのニーズを満たすように動的にスケーリングされ得る。クラウドインフラストラクチャシステム１０２によって提供されるサービスの具体的なインスタンス化は、本明細書では「サービスインスタンス」と称される。一般に、インターネットなどの通信ネットワークを介してクラウドサービスプロバイダのシステムからユーザが利用できるいかなるサービスも、「クラウドサービス」と称される。一般に、パブリッククラウド環境では、クラウドサービスプロバイダのシステムを構成するサーバおよびシステムは、顧客自身のオンプレミスサーバおよびシステムとは異なっている。たとえば、クラウドサービスプロバイダのシステムは、アプリケーションを提供してもよく、ユーザは、インターネットなどの通信ネットワークを介してオンデマンドで当該アプリケーションをオーダーして使用してもよい。

【００４４】

いくつかの例では、クラウドインフラストラクチャシステム１０２によってインスタンス化されるサービスインスタンスは、ストレージ、ホスト型データベース、ホスト型ウェブサーバ、ソフトウェアアプリケーション、または、クラウドベンダによってユーザに提供されるかもしくは当該技術分野において公知の他のサービスへの保護されたコンピュータネットワークアクセスを含み得る。たとえば、クラウドインフラストラクチャ１０２によってインスタンス化されるサービスインスタンスは、インターネットを介したクラウド上のリモートストレージへのパスワード保護されたアクセスを含んでもよい。別の例として、クラウドインフラストラクチャ１０２によってインスタンス化されるサービスインスタンスは、ネットワーク化された開発者による私的使用のためのウェブサービスベースのホスト型リレーショナルデータベースおよびスクリプト言語ミドルウェアエンジンを含んでもよい。別の例として、クラウドインフラストラクチャ１０２によってインスタンス化されるサービスインスタンスは、クラウドベンダのウェブサイト上で提供される電子メールソフトウェアアプリケーションへのアクセスを含んでもよい。

【００４５】

特定の実施形態では、クラウドインフラストラクチャシステム１０２は、セルフサービスの、サブスクリプションベースの、弾性的にスケーラブルな、信頼できる、高可用性で安全な態様で顧客に配信されるアプリケーション、ミドルウェア、開発サービスおよびデータベースサービス提供品一式を含み得る。クラウドインフラストラクチャシステム１０２として具体化されるクラウドインフラストラクチャシステムの一例は、オラクル社からの「オラクルパブリッククラウド（Oracle Public Cloud）」である。

【００４６】

クラウドインフラストラクチャシステム１０２は、さまざまなデプロイメントモデルを介してクラウドサービスを提供し得る。たとえば、サービスは、パブリッククラウドモデルの下で提供されてもよく、当該パブリッククラウドモデルでは、クラウドインフラストラクチャシステム１０２は（たとえば、オラクル社によって所有される）クラウドサービスを販売する組織によって所有され、一般大衆またはさまざまな業界企業がサービスを利

用できる。別の例として、サービスは、プライベートクラウドモデルの下で提供されてもよく、当該プライベートクラウドモデルでは、クラウドインフラストラクチャシステム１０２は、単一の組織のためだけに運営され、当該組織内の１つ以上のエンティティに対してサービスを提供し得る。また、クラウドサービスは、コミュニティクラウドモデルの下で提供されてもよく、当該コミュニティクラウドモデルでは、クラウドインフラストラクチャシステム１０２およびクラウドインフラストラクチャシステム１０２によって提供されるサービスは、関連するコミュニティ内のいくつかの組織によって共有される。また、クラウドサービスは、２つ以上の異なるモデルの組み合わせであるハイブリッドクラウドモデルの下で提供されてもよい。

【００４７】

いくつかの実施形態では、クラウドインフラストラクチャシステム１０２によって提供されるサービスは、ソフトウェア・アズ・ア・サービス（software as a service：「ＳａａＳ」）カテゴリ、プラットフォーム・アズ・ア・サービス（platform as a service：「ＰａａＳ」）カテゴリ、インフラストラクチャ・アズ・ア・サービス（infrastructure as a service：「ＩａａＳ」）カテゴリ、ＭＢａａＳカテゴリ、またはハイブリッドサービスを含むサービスの他のカテゴリの下で提供される１つ以上のサービスを含み得る。いくつかの実施形態では、クラウドインフラストラクチャシステム１０２によって提供されるサービスとしては、アプリケーションサービス、プラットフォームサービス、インフラストラクチャサービス、バックエンドサービスなどを挙げることができるが、これらに限定されるものではない。いくつかの例では、アプリケーションサービスは、ＳａａＳプラットフォームを介してクラウドインフラストラクチャシステム１０２によって提供されてもよい。ＳａａＳプラットフォームは、ＳａａＳカテゴリに分類されるクラウドサービスを提供するように構成され得る。たとえば、ＳａａＳプラットフォームは、統合された開発およびデプロイメントプラットフォーム上でオンデマンドアプリケーション一式を構築して配信する機能を提供してもよい。ＳａａＳプラットフォームは、ＳａａＳサービスを提供するための基本的なソフトウェアおよびインフラストラクチャを管理および制御し得る。ＳａａＳプラットフォームによって提供されるサービスを利用することにより、顧客は、クラウドインフラストラクチャシステムで実行されるアプリケーションを利用することができる。顧客は、ライセンスおよびサポートを別途購入する必要なくアプリケーションサービスを取得することができる。さまざまな異なるＳａａＳサービスが提供されてもよい。例としては、販売実績管理、企業統合、大組織のビジネス柔軟性のためのソリューションを提供するサービスが挙げられるが、これに限定されるものではない。

【００４８】

いくつかの実施形態では、プラットフォームサービスは、ＰａａＳプラットフォームを介してクラウドインフラストラクチャシステム１０２によって提供されてもよい。ＰａａＳプラットフォームは、ＰａａＳカテゴリに分類されるクラウドサービスを提供するように構成され得る。プラットフォームサービスの例としては、組織（オラクル社など）が共有の共通のアーキテクチャ上で既存のアプリケーションを整理統合することを可能にするサービス、および、プラットフォームによって提供される共有サービスを活用する新たなアプリケーションを構築する機能を挙げることができるが、これらに限定されるものではない。ＰａａＳプラットフォームは、ＰａａＳサービスを提供するための基本的なソフトウェアおよびインフラストラクチャを管理および制御し得る。顧客は、ライセンスおよびサポートを別途購入する必要なく、クラウドインフラストラクチャシステム１０２によって提供されるＰａａＳサービスを取得することができる。プラットフォームサービスの例としては、オラクル社からの「オラクルＪａｖａクラウドサービス（Oracle Java Cloud Service：「ＪＣＳ」）」、オラクル社からの「オラクルデータベースクラウドサービス（Oracle Database Cloud Service：「ＤＢＣＳ」）」などが挙げられるが、これらに限定されるものではない。

【００４９】

ＰａａＳプラットフォームによって提供されるサービスを利用することにより、顧客は

、クラウドインフラストラクチャシステム１０２によってサポートされるプログラミング言語およびツールを利用することができ、デプロイされたサービスを制御することもできる。いくつかの実施形態では、クラウドインフラストラクチャシステム１０２によって提供されるプラットフォームサービスは、データベースクラウドサービス、ミドルウェアクラウドサービス（たとえば、オラクルフュージョンミドルウェアサービス）およびＪａｖａクラウドサービスを含み得る。一実施形態では、データベースクラウドサービスは、組織がデータベースリソースをプールしてデータベースクラウドの形式でデータベース・アズ・ア・サービスを顧客に提供することを可能にする共有サービスデプロイメントモデルをサポートし得る。ミドルウェアクラウドサービスは、顧客がクラウドインフラストラクチャシステム内でさまざまなビジネスアプリケーションを開発およびデプロイするためのプラットフォームを提供し得て、Ｊａｖａクラウドサービスは、顧客がクラウドインフラストラクチャシステム内でＪａｖａアプリケーションをデプロイするためのプラットフォームを提供し得る。

【００５０】

クラウドインフラストラクチャシステム１０２では、さまざまな異なるインフラストラクチャサービスがＩａａＳプラットフォームによって提供されてもよい。インフラストラクチャサービスは、ストレージ、ネットワークなどの基本的なコンピューティングリソース、ならびに、ＳａａＳプラットフォームおよびＰａａＳプラットフォームによって提供されるサービスを利用する顧客のための他の基礎的なコンピューティングリソースの管理および制御を容易にする。

【００５１】

特定の実施形態では、クラウドインフラストラクチャシステム１０２は、クラウドインフラストラクチャシステム内でのクラウドサービス（たとえば、ＳａａＳサービス、ＰａａＳサービス、ＩａａＳサービスおよびＭＢａａＳサービス）の包括的管理を提供し得る。一実施形態では、クラウド管理機能は、クラウドインフラストラクチャシステム１０２によって受け取られる顧客のサブスクリプションをプロビジョニング、管理および追跡する機能などを含み得る。さまざまな実施形態では、クラウドインフラストラクチャシステム１０２は、クラウドインフラストラクチャシステム１０２によって提供されるサービスに対する顧客のサブスクリプションを自動的にプロビジョニング、管理および追跡するように適合され得る。顧客は、サブスクリプションオーダーを介して、クラウドインフラストラクチャシステム１０２によって提供される１つ以上のサービスをオーダーし得る。そして、クラウドインフラストラクチャシステム１０２は、当該顧客のサブスクリプションオーダーにおけるサービスを提供するように処理を実行する。

【００５２】

一実施形態では、クラウド管理機能は、オーダー管理および監視モジュール１１４などの１つ以上のモジュールによって提供されてもよい。これらのモジュールは、１つ以上のコンピュータおよび／またはサーバを含むかまたは１つ以上のコンピュータおよび／またはサーバを用いて提供され得て、当該１つ以上のコンピュータおよび／またはサーバは、汎用コンピュータ、専用サーバコンピュータ、サーバファーム、サーバクラスタ、またはその他の適切な配置および／もしくは組み合わせであってもよい。

【００５３】

例示的なオペレーションにおいて、顧客は、クライアントコンピューティングデバイス１０４，１０６または１０８を用いて、クラウドインフラストラクチャシステム１０２によって提供される１つ以上のサービスを要求することによってクラウドインフラストラクチャシステム１０２と対話し得る。顧客は、さまざまな手段を用いて、クラウドインフラストラクチャシステム１０２にサービス要求１３０を発行し得る。サービス要求１３０は、クラウドインフラストラクチャシステム１０２によって提供される１つ以上のサービスに対するサブスクリプションをオーダーすること、クラウドインフラストラクチャシステム１０２によって提供される１つ以上のサービスにアクセスすることなどを含み得る。特定の実施形態では、顧客は、クラウドＵＩ１３２，１３４および１３６にアクセスして、

これらのＵＩを介してサブスクリプションオーダーを行い得る。顧客がオーダーを行ったことに応答してクラウドインフラストラクチャシステム１０２によって受け取られるオーダー情報は、顧客を特定する情報、および、顧客が申し込もうとしている、クラウドインフラストラクチャシステム１０２によって提供される１つ以上のサービスを特定する情報を含み得る。顧客によってオーダーがなされた後に、オーダー情報がクラウドＵＩ１３２，１３４および／または１３６を介して受け取られる。

【００５４】

この例では、オーダー管理および監視モジュール１１２は、顧客から受け取った情報を、顧客が行なったオーダーを格納しているオーダーデータベースに送信する。オーダーデータベースは、クラウドインフラストラクチャシステム１０２によって運用され、他のシステム要素と併用して運用されるいくつかのデータベースのうちの１つであってもよい。オーダー管理および監視モジュール１１２は、オーダーデータベースに格納されたオーダー情報の全てまたは一部を含む情報をオーダー管理モジュールに転送し得る。いくつかの例では、オーダー管理モジュールは、オーダーの確認および確認時のオーダーの予約などの、オーダーに関連する請求および課金機能を実行するように構成され得る。

【００５５】

特定の実施形態では、クラウドインフラストラクチャシステム１０２は、アイデンティティ管理モジュール１１４を含み得る。アイデンティティ管理モジュール１１４は、クラウドインフラストラクチャシステム１０２内のアクセス管理および認可サービスなどのアイデンティティサービスを提供するように構成され得る。いくつかの実施形態では、アイデンティティ管理モジュール１１４は、クラウドインフラストラクチャシステム１０２によって提供されるサービスを利用したい顧客についての情報を制御し得る。このような情報としては、このような顧客のアイデンティティを認証する情報、および、それらの顧客がさまざまなシステムリソース（たとえば、ファイル、ディレクトリ、アプリケーション、通信ポート、メモリセグメントなど）に対してどのアクションを実行する権限を与えられているかを説明する情報を挙げることができる。アイデンティティ管理モジュール１１４は、各顧客についての記述的情報、ならびに、当該記述的情報にどのようにして誰がアクセスして変更できるかについての記述的情報の管理も含み得る。

【００５６】

特定の実施形態では、クラウドインフラストラクチャシステム１０２は、さまざまなサービスをクラウドインフラストラクチャシステム１０２の顧客に提供するのに用いられるリソースを提供するためのインフラストラクチャリソース１１６も含み得る。一実施形態では、インフラストラクチャリソース１１６は、ＰａａＳプラットフォームおよびＳａａＳプラットフォームによって提供されるサービスを実行するための、サーバなどのハードウェアとストレージとネットワーキングリソースとの予め統合された、最適化された組み合わせを含み得る。

【００５７】

いくつかの実施形態では、クラウドインフラストラクチャシステム１０２内のリソースは、複数のユーザによって共有され、要求当たり動的に再割り当てされ得る。また、リソースは、さまざまなタイムゾーン内のユーザに割り当てられてもよい。たとえば、クラウドインフラストラクチャシステム１０２は、第１のタイムゾーン内のユーザの第１の組が所定の時間にわたってクラウドインフラストラクチャシステムのリソースを利用することを可能にし、次いで、同一のリソースを異なるタイムゾーンに位置するユーザの別の組に対して再割り当てすることを可能にすることによって、リソースの利用を最大化してもよい。

【００５８】

特定の実施形態では、クラウドインフラストラクチャシステム１０２のさまざまなコンポーネントまたはモジュールによって共有され、かつ、クラウドインフラストラクチャシステム１０２によって提供されるサービスによって共有される複数の内部共有サービス１１８が提供され得る。これらの内部共有サービス１１８としては、セキュリティおよびア

イデンティティサービス、インテグレーションサービス、エンタープライズリポジトリサービス、エンタープライズマネージャサービス、ウイルススキャンおよびホワイトリストサービス、高可用性バックアップおよび回復サービス、クラウドサポートを可能にするためのサービス、電子メールサービス、通知サービス、ファイル転送サービスなどを挙げることができるが、これらに限定されるものではない。

【００５９】

特定の実施形態では、クラウドインフラストラクチャシステム１０２のさまざまなコンポーネントまたはモジュールによって共有され、かつ、クラウドインフラストラクチャシステム１０２によって提供されるサービスによって共有される複数の外部共有サービス１２０が提供され得る。これらの外部共有サービス１２０としては、セキュリティおよびアイデンティティサービス、インテグレーションサービス、エンタープライズリポジトリサービス、エンタープライズマネージャサービス、ウイルススキャンおよびホワイトリストサービス、高可用性バックアップおよび回復サービス、クラウドサポートを可能にするためのサービス、電子メールサービス、通知サービス、ファイル転送サービスなどを挙げることができるが、これらに限定されるものではない。

【００６０】

さまざまな実施形態では、外部共有サービス１２０は、企業コンピュータシステム１２６にアクセス、データ変換、自動化などを提供する１つ以上のコンポーネントを含み得る。企業コンピュータシステム１２６へのアクセスは、クラウドインフラストラクチャシステム１０２のさまざまなコンポーネントまたはモジュールによって共有され、クラウドインフラストラクチャシステム１０２によって提供されるサービスによって共有され得る。いくつかの実施形態では、企業コンピュータシステム１２６へのアクセスは、１つ以上の加入者に限定される、クラウドインフラストラクチャシステム１０２によって提供されるサービスインスタンスによって共有され得る。

【００６１】

さらなる実施形態では、外部共有サービス１２０は、クラウドインフラストラクチャシステム１０２のさまざまなコンポーネントまたはモジュールによって共有され、かつ、クラウドインフラストラクチャシステム１０２によって提供されるサービスによって共有される外部アプリケーションプログラミングインターフェイス（「ＡＰＩ」）サービス１２８を含み得る。これらの外部ＡＰＩサービス１２８としては、他の第三者サービスまたはエンティティによって提供されるＡＰＩを挙げることができるが、これらに限定されるものではない。

【００６２】

さまざまな異なるモバイルクラウドサービスがクラウドインフラストラクチャシステム１０２内のＭＣＳ１２２によって提供され得る。ＭＣＳ１２２は、本発明のいくつかの実施形態に従ってモバイルコンピューティングデバイスと企業コンピュータシステム（たとえば、企業コンピュータシステム１２４および１２６）との間の通信を容易にする。ＭＣＳ１２２は、企業データおよび認証情報を格納するのに用いられる１つ以上のメモリストレージデバイス（「ローカルストレージ」）を含み得る。企業データは、企業コンピュータシステム１２６またはクライアントコンピューティングデバイス１０４，１０６または１０８から受信されてもよく、またはクラウドインフラストラクチャシステム１０２によって変換された企業データを含んでもよく、またはそれらの組み合わせであってもよい。認証情報は、アイデンティティ管理システム１１４から受信されてもよく、および／または、クラウドインフラストラクチャシステム１０２によって生成されてもよい。いくつかの実施形態では、認証情報は、サービス要求に関するユーザのセキュリティ認証を示す情報を含み得る。

【００６３】

企業コンピュータシステム１２６などの企業コンピュータシステムは、クラウドインフラストラクチャシステム１０２のファイアウォールを越えて、クラウドインフラストラクチャシステム１０２とは異なる地理的位置（たとえば、遠隔の地理的位置）に物理的に位

置してもよい。いくつかの実施形態では、企業コンピュータシステム１２６は、１つ以上の異なるコンピュータまたはサーバを含み得る。いくつかの実施形態では、企業コンピュータシステム１２６は、単一のコンピュータシステムの一部であってもよい。

【００６４】

特定の実施形態では、企業コンピュータシステム１２６は、１つ以上の異なるプロトコルを用いてクラウドインフラストラクチャシステム１０２と通信し得る。企業コンピュータシステム１２６の各々は、さまざまな通信プロトコルを用いてクラウドインフラストラクチャシステム１０２と通信し得る。企業コンピュータシステム１２６は、同一のセキュリティプロトコルをサポートしてもよく、または異なるセキュリティプロトコルをサポートしてもよい。いくつかの実施形態では、ＭＣＳ１２２は、企業コンピュータシステム１２６との通信を処理するためのエージェントシステムを含み得る。

【００６５】

プロトコルは、ＳＰｅｅＤＹ（「ＳＰＤＹ」）などの通信プロトコルを含み得る。プロトコルは、ＨＴＴＰベースのプロトコルなどのアプリケーションプロトコルを含み得る。いくつかの実施形態では、企業コンピュータシステム１２６は、ＲＥＳＴまたはシンプル・オブジェクト・アクセス・プロトコル（Simple Object Access Protocol：「ＳＯＡＰ」）などの通信プロトコルを用いてクラウドインフラストラクチャシステム１０２と通信し得る。たとえば、ＲＥＳＴプロトコルは、統一資源識別子（uniform resource identifier：「ＵＲＩ」）または統一資源位置指定子（uniform resource locator：「ＵＲＬ」）を含むフォーマットをサポートしてもよい。ＲＥＳＴプロトコルを用いた通信用にフォーマットされた企業データは、ＪａｖａＳｃｒｉｐｔ（登録商標）オブジェクト表記法（JavaScript Object Notation：「ＪＳＯＮ」）、カンマ区切り値（comma-separated value：「ＣＳＶ」）およびリアリ・シンプル・シンジケーション（really simple syndication：「ＲＳＳ」）などのデータフォーマットに容易に変換できる。企業コンピュータシステム１２６およびクラウドインフラストラクチャシステム１０２は、リモートプロシージャコール（remote procedure call：「ＲＰＣ」）（たとえば、拡張マークアップ言語（extended markup language：「ＸＭＬ」）ＲＰＣ）などの他のプロトコルを用いて通信してもよい。

【００６６】

いくつかの実施形態では、ＭＣＳ１２２は、一部が異なる通信プロトコルまたは技術をサポートし得るクラウドインフラストラクチャシステム１０２によって提供される１つ以上のサービスとの通信をサポートするように構成されたアダプタインターフェイスを含み得る。いくつかの実施形態では、ＭＣＳ１２２は、一部が異なる通信プロトコルまたは技術をサポートし得る企業コンピュータシステム１２６との通信をサポートするように構成されたアダプタインターフェイスを含み得る。ＭＣＳ１２２は、各々が通信プロトコル、企業コンピュータシステムのタイプ、アプリケーションのタイプ、サービスのタイプ、またはそれらの組み合わせに従って通信するように構成され得る１つ以上のアダプタを含み得る。アダプタによってサポートされる通信プロトコルは、サービスまたは企業コンピュータシステム１２６のうちの１つ以上に特有であってもよい。

【００６７】

特定の実施形態では、クライアントコンピューティングデバイス１０４，１０６および１０８の各々は、ＭＣＳ１２２と通信するための特定のＵＩを提供することができるアプリケーションを実行し得る。特定のＵＩは、特定の通信プロトコルを用いて通信するように構成され得る。いくつかの実施形態では、特定のＵＩは、ＭＣＳ１２２と通信するために呼び出され得る呼び出し可能なインターフェイス、機能、ルーチン、方法および／またはオペレーションを含み得る。特定のＵＩは、企業データおよび／またはサービスの要求のためにクラウドインフラストラクチャシステム１０２によって提供されるサービスまたは企業コンピュータシステム１２６と通信するための入力パラメータとして受け入れられてもよい。いくつかの実施形態では、ＭＣＳ１２２を介した通信は、カスタム通信プロトコルを用いた通信用に変換され得る。いくつかの実施形態では、特定のＵＩは、アプリケ

ーションにおけるカスタムクライアントに対応し得る。

【００６８】

ＭＣＳ１２２は、１つ以上の呼出し可能なインターフェイス、たとえばＡＰＩを含み得る。ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェースは、モバイルコンピューティングデバイス上のアプリケーションが要求をＭＣＳ１２２に通信することを可能にし得る。ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスは、一般的または標準的なインターフェイスをサポートし得て、標準化されたプロトコル、アーキテクチャスタイルおよび／またはフォーマット（たとえば、ＲＥＳＴプロトコル）に従って、パラメータを含む要求をアプリから受信することを可能にし得る。ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスは、コンピューティングデバイス１０４，１０６または１０８のうちのいずれか１つのユーザによって構成可能であり得る。ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスは、通信プロトコルに従ってサービスに対する要求を受信し得る。デバイスアプリケーション開発者は、カスタムアプリケーションのためにＭＣＳ１２２に接続することができる。いくつかの実施形態では、ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスは、カスタムアプリケーションを実行してＭＣＳ１２２と通信することができるように、アプリを開発する人物と同一の人物によって構成されてもよい。

【００６９】

ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスはさらに、標準化されたプロトコルまたはフォーマットに従って企業コンピュータシステム１２６がＭＣＳ１２２と通信することを可能にし得る。アプリケーション開発者と同様に、企業コンピュータシステムを管理するものは、１つ以上の呼び出し可能なインターフェイスを介してＭＣＳ１２２と通信するように構成されたコード（たとえば、エージェントシステム）を実行し得る。ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスは、コンピューティングデバイスのタイプ、企業コンピュータシステムのタイプ、アプリ、エージェントシステム、サービス、プロトコル、または他の基準に基づいて実現され得る。いくつかの実施形態では、ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスは、認証、圧縮、暗号化、カーソルによるページネーション、クライアントベースのスロットリング、否認防止、ロギングおよびメトリクス収集を含むサービスに対する要求をサポートし得る。いくつかの実施形態では、ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスは、認証、ポリシー施行、応答のキャッシング、ＭＣＳ１２２に対する呼び出しのスロットリング、非同期パターンと同期パターンとの間の変換、基本的なサービスに対する呼び出しのロギング、またはそれらの組み合わせなどのカスタムビジネス関連サービスのために実現され得る。いくつかの実施形態では、ＭＣＳ１２２に関連付けられた呼び出し可能なインターフェイスは、ユーザがクラウドインフラストラクチャシステム１０２によって実行されるようにカスタムコードをロードすることを可能にし得る。カスタムコードは、ＭＣＳ１２２に関連付けられた１つ以上の呼び出し可能なインターフェイスをクラウドインフラストラクチャシステム１０２のために実現し得て、ユーザがカスタムサービスまたは他の企業コンピュータシステムにアクセスすることを可能にすることができる。

【００７０】

ＭＣＳ１２２に関連付けられたプロトコルトランスレータは、メッセージの通信プロトコルを決定するためのメッセージ、および／または、メッセージを送信先の通信プロトコルに変換するためのメッセージを処理し得る。ＭＣＳ１２２に関連付けられたプロトコルトランスレータは、クライアントコンピューティングデバイス１０４，１０６または１０８から受信した要求を変換し得る。当該要求は、クライアントコンピューティングデバイス１０４，１０６または１０８によってサポートされる通信プロトコルのフォーマットから、クラウドインフラストラクチャシステム１０２または企業コンピュータシステム１２６によって提供されるサービスによってサポートされる通信プロトコルのフォーマットに変換され得る。ＭＣＳ１２２に関連付けられたプロトコルトランスレータは、クラウドインフラストラクチャシステム１０２または企業コンピュータシステム１２６によって提供

されるサービスから受信した応答を変換し得る。応答は、クラウドインフラストラクチャシステム１０２または企業コンピュータシステム１２６によって提供されるサービスによってサポートされる通信プロトコルのフォーマットから、クライアントコンピューティングデバイス１０４，１０６または１０８によってサポートされる通信プロトコルのフォーマットに変換され得る。

【００７１】

ＭＣＳ１２２に関連付けられたセキュリティサービスは、クライアントコンピューティングデバイス１０４，１０６または１０８のうちのいずれかから受信した要求のためのセキュリティ認証を管理し得る。ＭＣＳ１２２に関連付けられたセキュリティサービスは、顧客プロセスおよび企業データの完全性を保護し得る。システムまたはデータが損なわれることを防止するために、セキュリティ認証は、クライアントコンピューティングデバイス１０４，１０６または１０８から要求を受信したときに生じ得る。セキュリティ認証は、要求が送られてクラウドインフラストラクチャシステム１０２によって処理される前に実行され得る。ユーザのために決定されたセキュリティ認証は、モバイルコンピューティングデバイスに関連付けられたユーザがＭＣＳ１２２を介してサービスを要求する権限を有することができるようにし得る。セキュリティ認証は、ＭＣＳ１２２を介して要求されるさまざまな要求および／またはサービスに対してユーザが認証を行う労力を減らすことができる。ＭＣＳ１２２に関連付けられたセキュリティサービスは、要求のセキュリティを認証するさまざまなオペレーションを実行するように構成された１つ以上の機能ブロックまたはモジュールとして実現されてもよい。

【００７２】

ＭＣＳ１２２に関連付けられた認証サービスは、クライアントコンピューティングデバイス１０４，１０６または１０８から受信される要求のセキュリティ認証を管理し得る。ＭＣＳ１２２に関連付けられた認証サービスは、要求をＭＣＳ１２２に送信するコンピューティングデバイスに関連付けられたユーザのセキュリティ認証を決定し得る。セキュリティ認証は、期間に基づいて決定され得て、当該期間は、アプリケーションのオペレーション（たとえば、アプリケーションの起動）、要求、コンピューティングデバイス、企業コンピュータシステム、要求に関連する他の基準、またはそれらの組み合わせに結び付けられ得る。セキュリティ認証は、個々の要求、１つ以上の企業コンピュータシステム、特定のサービス、サービスのタイプ、ユーザ、コンピューティングデバイス、セキュリティ認証を決定するための他の基準、またはそれらの組み合わせなどのもののうちのいずれか１つについて確認され、付与され得る。いくつかの実施形態では、クラウドインフラストラクチャシステム１０２は、企業コンピュータシステムまたは企業コンピュータシステムをサポートする認証システムから受信したユーザの認証情報を格納し得る。クラウドインフラストラクチャシステム１０２は、ルックアップ関数を実行して、要求に関連付けられたユーザのアイデンティティがこのような要求の行う権限を有しているか否かを判断することによって、認証を決定し得る。格納される認証情報としては、ユーザがアクセスする権限を与えられ得る要求、機能、企業コンピュータシステム、企業データのタイプなどの情報を挙げることができる。いくつかの実施形態では、インフラストラクチャシステム１０２は、認証を決定するために、要求を行っているコンピューティングデバイスとの通信を開始し得る。

【００７３】

いくつかの実施形態では、セキュリティ認証は、サービスを要求するユーザに関連付けられた役割に基づいて決定され得る。当該役割は、ＭＣＳ１２２へのアクセスを要求するユーザに関連付けられ得る。いくつかの実施形態では、ユーザは、ＭＣＳ１２２によって提供されるリソースおよび／またはサービスへのアクセスを付与され得るＭＣＳ１２２の加入者またはテナントとしてサービスを要求し得る。認証は、ＭＣＳ１２２に対するユーザのサブスクリプションに対応し得て、ユーザは、加入者としてＭＣＳ１２２を介してサービスを要求する権限を与えられ得る。いくつかの実施形態では、サブスクリプションは、ＭＣＳ１２２によって提供される特定のリソースセットに限定され得る。セキュリティ

認証は、ＭＣＳ１２２のユーザにアクセス可能なリソースおよび／またはサービスに基づき得る。いくつかの実施形態では、要求は、「ランタイム環境」と呼ばれる実行中にテンプレートをプロビジョニングされ得る。ランタイム環境は、要求、ユーザまたはデバイスに割り当てられるリソースに関連付けられ得る。

【００７４】

いくつかの実施形態では、ＭＣＳ１２２に関連付けられた認証サービスは、ユーザのセキュリティ認証を決定するようにアイデンティティ管理システムに要求し得る。アイデンティティ管理システムは、クラウドインフラストラクチャシステム１０２によって（たとえば、アイデンティティ管理１１４として）実現されてもよく、またはクラウドインフラストラクチャシステム１０２の外部の別のコンピュータシステムによって実現されてもよい。アイデンティティ管理１１４は、ユーザの役割またはＭＣＳ１２２にアクセスするためのサブスクリプションに基づいて、ユーザのセキュリティ認証を決定し得る。役割またはサブスクリプションは、企業コンピュータシステム、企業コンピュータシステムによって提供されるサービス、企業コンピュータシステムの機能または特徴、企業コンピュータシステムへのアクセスを制御するための他の基準、またはそれらの組み合わせに関して、特権および／または権利を割り当てられ得る。

【００７５】

さまざまな異なるＡＤＦ１２４がクラウドインフラストラクチャシステム１０２内に設けられ得る。ＡＤＦ１２４は、ＳＯＡベースのアジャイルアプリケーションを実行するためのインフラストラクチャコードを提供する。ＡＤＦ１２４はさらに、１つ以上の開発ツール（たとえば、「Oracle JDeveloper 11g」開発ツール）による開発のための視覚的および宣言的なアプローチを提供する。ＡＤＦ１２４によって提供される１つ以上のフレームワークは、ＭＶＣ設計パターンを実現し得る。このようなフレームワークは、オブジェクト／リレーショナルマッピング、データ持続性、再利用可能なコントローラ層、リッチウェブＵＩフレームワーク、ＵＩへのデータ結合、セキュリティおよびカスタマイズなどの領域に対するソリューションを有するＭＶＣアーキテクチャの全ての層をカバーする統合されたソリューションを提供する。中核のウェブベースのＭＶＣアプローチを越えて、このようなフレームワークは、オラクルＳＯＡおよびウェブセンタポータルフレームワークとも統合して、完全複合アプリケーションの作成を簡略化する。

【００７６】

特定の実施形態では、ＡＤＦ１２４は、サービスインターフェイスをクラウドインフラストラクチャシステム１０２によって提供される組み込み型ビジネスサービスに結合することによってデータをサービスとして公開するアジャイルアプリケーションを開発することを容易にする。このビジネスサービス実装詳細の分離は、メタデータを介してＡＤＦ１２４において実行される。このメタデータ駆動アーキテクチャを用いることにより、アプリケーション開発者は、どのようにサービスにアクセスするかについての詳細ではなく、ビジネスロジックおよびユーザエクスペリエンスに焦点を当てることができる。特定の実施形態では、ＡＤＦ１２４は、メタデータ内のサービスの実装詳細をモデル層に格納する。これにより、開発者はＵＩを変更することなくサービスを交換することができ、アプリケーションが非常にアジャイルになる。また、ＵＩを作成する開発者は、ビジネスサービスアクセス詳細を思い悩まなくてもよくなる。その代わりに、開発者は、アプリケーションインターフェイスおよび対話ロジックを開発することに焦点を当てることができる。ユーザエクスペリエンスを作成することは、所望のビジネスサービスをビジュアル・ページ・デザイナ上にドラッグおよびドロップして、どのタイプのコンポーネントが当該データを表示すべきかを示すことと同じぐらい簡単であろう。

【００７７】

さまざまな実施形態では、開発者は、ＡＤＦ１２４と対話して、企業アプリケーションを形成するモジュールを作成する。企業アプリケーションは、クラウドインフラストラクチャシステム１０２の文脈内で実行することができる。さまざまな実施形態では、開発者は、ＡＤＦ１２４と対話して、モバイルアプリケーションを形成するモジュールを作成す

る。モバイルアプリケーションは、クラウドインフラストラクチャシステム１０２の文脈内で実行することができる。以下で説明する本発明の特徴は、本明細書に提供されている開示を読むことによって当業者に明らかになるプログラミング言語とアプリケーション開発フレームワークとをいずれかの所望の組み合わせを用いて実現することができる。

【００７８】

ＡＤＦ１２４によって提供される１つ以上のフレームワークは、一例ではオラクルＡＤＦとして実施されてもよい。したがって、ＡＤＦ１２４におけるフレームワークは、ＭＶＣ設計パターンに基づき得る。ＭＶＣアプリケーションは、１）データソースとの対話を処理し、ビジネスロジックを実行するモデル層、２）アプリケーションＵＩを処理するビュー層、および３）アプリケーションフローを管理し、モデル層とビュー層との間のインターフェイスの役割を果たすコントローラ、に分離される。アプリケーションをこれら３つの層に分離することにより、アプリケーション全体にわたるコンポーネントのメンテナンスおよび再利用が簡略化される。各層を他の層から独立させることにより、疎結合ＳＯＡがもたらされる。

【００７９】

さまざまな実施形態では、ＡＤＦ１２４は、開発者が複数の層の形態でアプリケーションを作成することを可能にするツールおよびリソースを提供し、各層は、予め規定された仕様に従って所望のロジックを実行するコードモジュール／ファイルを含む。したがって、一実施形態では、ＡＤＦ１２４は、アプリケーションを４つの層として開発することを可能にし、当該４つの層とは、アプリケーションのＵＩを提供するコードモジュール／ファイルを含むビュー層、アプリケーションのフローを制御するコードモジュールを含むコントローラ層、基本的なデータに対して抽象化層を提供するデータ／コードモジュールを含むモデル層、およびさまざまなソースからデータへのアクセスを提供してビジネスロジックを処理するコードモジュールを含むビジネスサービス層である。

【００８０】

特定の実施形態では、ＡＤＦ１２４は、各層を実現する際に使用したい技術を開発者に選択させる。エンタープライズＪａｖａビーン（Enterprise JavaBean：「ＥＪＢ」）、ウェブサービス、Ｊａｖａビーン（JavaBean）、JPA/EclipseLink/TopLinkオブジェクト、その他多数は全て、ＡＤＦ１２４のためのビジネスサービスとして使用することができる。ビュー層は、Ｊａｖａサーバフェイス（Java Server Faces：「ＪＳＦ」）、デスクトップスイングアプリケーションおよびマイクロソフトオフィスフロントエンドで実現されるウェブベースのインターフェイス、ならびにモバイルデバイスのためのインターフェイスを含み得る。

【００８１】

一局面では、ビュー層は、開発中のアプリケーションのＵＩを表示する。ビュー層は、デスクトップ、モバイルおよびブラウザベースのビューを含み得て、それらのビューの各々は、ＵＩの全てまたは一部を提供し、ビュータイプに対応するさまざまな方法でアクセス可能である。たとえば、ウェブページは、対応するＵＲＬを含むクライアント要求を受信したことに応答してアプリケーションによって送信されてもよい。次いで、ウェブページは、要求を行っているクライアントシステムに関連付けられたディスプレイユニット（図示せず）上にブラウザによって表示されてもよく、それによって、要求を行っているクライアントシステムのユーザが企業アプリケーションと対話することを可能にする。ＡＤＦ１２４は、ビジネスサービスへのマルチチャネルアクセスをサポートし、ビジネスサービスの再利用、および、ウェブクライアント、クライアントーサーバスイングデスクトップベースアプリケーション、マイクロソフトエクセルスプレッドシート、スマートフォンなどのモバイルデバイスなどからのアクセスを可能にする。

【００８２】

ビュー層（ウェブページなど）を形成するコードファイル／モジュールは、ハイパーテキストマークアップ言語（hypertext markup language：「ＨＴＭＬ」）、Ｊａｖａサーバページ（Java server page：「ＪＳＰ」）およびＪＳＦのうちの１つ以上を用いて実現

されてもよい。代替的に、ＵＩは、スイングおよび／またはＸＭＬなどのＪａｖａコンポーネントを用いて実現されてもよい。さらに記載されるように、ＵＩは、ユーザエクスペリエンス、ならびに、マイクロソフト社によるワードおよびエクセルなどのデスクトップアプリケーションへの精通を活用してもよい。

【００８３】

上記のように、関連するユーザ開発コード／データモジュールが各層に設けられる。しかし、各層は一般に、ＡＤＦ１２４によって提供される他の予め規定されたコード／データモジュールを含む。予め規定されたモジュールのうちのいくつかは、開発中に、たとえばウェブページを開発するためのテンプレート、開発されたコードに所望の機能を含めるためのテンプレートなどとして使用されてもよい。他の予め規定されたモジュール（ＵＲＬ書換モジュールなど）は、開発されたアプリケーションとともにデプロイされてもよく、企業アプリケーションの実行中にユーザにさらなる機能（要求されたＵＲＬの、内部名へのマッピング）を提供してもよい。

【００８４】

コントローラ層は、アプリケーションのフローを制御するコードモジュール／ファイルを含む。各コントローラオブジェクトは、ビュー層において情報を表示する所望の方法に従って実現されるソフトウェア命令および／またはデータを含む。当該所望の方法としては、別のウェブページにおけるリンクがユーザによってクリック／選択されると特定のウェブページを表示すること、実行中にエラーが生じると、特定のデータを格納／検索取得することを示すページを表示することなどを挙げることができる。

【００８５】

一局面では、コントローラ層は、アプリケーションフローを管理し、ユーザ入力を処理する。たとえば、検索ボタンがページ上でクリックされると、コントローラは、どのアクションを実行すべきであるか（検索を行う）およびどこにナビゲートすべきであるか（結果ページ）を判断する。JDeveloperにおけるウェブベースのアプリケーションでは、標準的なＪＳＦコントローラまたはＪＳＦコントローラ機能を拡張したＡＤＦコントローラの２つのコントローラオプションがある。どちらのコントローラを使用するとしても、アプリケーションフローは一般に、ダイアグラム上にページおよびナビゲーションルールをレイアウトすることによって設計される。アプリケーションのフローは、さらに小さな再利用可能なタスクフローに分けることができ、当該タスクフローは、フロー内のメソッド呼び出しおよび決定点などの非視覚的コンポーネントを含み、単一のページの領域内で実行される「ページフラグメント」フローを作成する。

【００８６】

コントローラ層を形成するコードモジュール／ファイルは、しばしば、クライアント要求を受信して所望のウェブページを対応する応答として送信するＪａｖａサーブレットとして実現される。また、コントローラオブジェクトは、たとえばアパッチ・ジャカルタ・ストラット（Apache Jakarta Struts）コントローラとして、またはＪＳＦ規格に従って、実現されてもよい。

【００８７】

モデル層は、さまざまなビジネスサービスを、上記のコントローラオブジェクトなどの、当該ビジネスサービスを他の層で使用するオブジェクトに接続する、またはデスクトップアプリケーションに直接接続するデータ／コードモジュールを含む。モデル層の各抽象化データオブジェクトは、基本的なビジネスサービス層で実行されるいずれかのタイプのビジネスサービスへのアクセスに使用できる対応するインターフェイスを提供する。データオブジェクトは、クライアントからのサービスのビジネスサービス実装詳細を抽象化し、および／または、データ制御方法／属性をビューコンポーネントに公開し得て、それによって、ビュー層およびデータ層の分離を提供する。

【００８８】

一局面では、モデル層は、メタデータファイルを利用してインターフェイスを定義するデータ制御およびデータ結合の２つのコンポーネントで構成される。データ制御は、クラ

イアントからのビジネスサービス実装詳細を抽象化する。データ結合は、データ制御方法および属性をＵＩコンポーネントに公開して、ビューおよびモデルのクリーンな分離を提供する。モデル層のメタデータアーキテクチャにより、開発者は、いずれのタイプのビジネスサービス層実装をビュー層およびコントローラ層に結合しても同一の開発経験を得ることになる。

【００８９】

特定の実施形態では、ＡＤＦ１２４は、ユーザが実装詳細に踏み込む必要なしにアプリケーション作成のロジックに集中することができるように、開発プロセス全体を通して宣言型プログラミングパラダイムを用いることを重視する。高いレベルにおいて、フュージョンウェブアプリケーションの開発プロセスは、通常、アプリケーション作業領域を作成することを含む。ウィザードを用いて、開発者によって選択された技術に必要とされるライブラリおよび構成が自動的に追加され、アプリケーションは、パッケージおよびディレクトリを有するプロジェクトに構造化される。

【００９０】

データベースオブジェクトをモデル化することによって、いかなるデータベースのオンラインデータベースまたはオフラインレプリカも作成することができ、定義を編集することができ、スキーマを更新することができる。次いで、統一モデリング言語（unified modeling language：「ＵＭＬ」）モデラを用いて、アプリケーションについてユースケースを作成することができる。アプリケーション制御およびナビゲーションも設計することができる。ダイアグラマを用いて、アプリケーション制御およびナビゲーションのフローを視覚的に決定することができる。次いで、フローを記述する基本的なＸＭＬファイルを自動的に作成することができる。リソースライブラリを用いて、開発者は、インポートされたライブラリを単にアプリケーションにドラッグおよびドロップすることによって、インポートされたライブラリを見て使用することができるようになる。ウィザードまたはダイアログを用いて、データベーステーブルからエンティティオブジェクトを作成することができる。それらのエンティティオブジェクトからビューオブジェクトが作成され、アプリケーションにおけるページによって使用される。検証ルールおよび他のタイプのビジネスロジックが実装されてもよい。

【００９１】

この例では、ビジネスサービス層は、データ持続層との対話を管理する。ビジネスサービス層は、データ持続性、オブジェクト／リレーショナルマッピング、トランザクション管理およびビジネスロジック実行などのサービスを提供する。ビジネスサービス層は、単純なＪａｖａクラス、ＥＪＢ、ウェブサービス、ＪＰＡオブジェクトおよびオラクルＡＤＦビジネスコンポーネントのうちのいずれかで実現されてもよい。また、データはファイル（ＸＭＬまたはＣＳＶ）およびＲＥＳＴから直接消費され得る。したがって、各ビジネスサービスは、対応するデータ持続層との対話を管理し、オブジェクト／リレーショナルマッピング、トランザクション管理、ビジネスロジック実行などのサービスも提供する。ビジネスサービス層は、単純なＪａｖａクラス、エンタープライズＪａｖａビーン、ウェブサービスなどのうちの１つ以上を用いて実現されてもよい。

【００９２】

ビジネスコンポーネントは、たとえばオラクル社からの「オラクルＡＤＦビジネスコンポーネント」を用いて実現されるビジネスサービスを表示して、データバース、ウェブサービス、レガシーシステム、アプリケーションサーバなどとの対話を提供する。一実施形態では、ビジネスサービス層のビジネスコンポーネントは、協働してビジネスサービス実装を提供するアプリケーションモジュールとビュー／クエリオブジェクトとエンティティオブジェクトとの混合物を含む。アプリケーションモジュールは、ＵＩクライアントがアプリケーション／トランザクションデータと連携するために通信するトランザクションコンポーネント／コードモジュールであってもよい。アプリケーションモジュールは、更新可能なデータモデルを提供し得て、ユーザトランザクションに関連する手順／機能（一般にサービス方法と称される）も提供し得る。

【００９３】
エンティティオブジェクトは、データベーステーブル内の対応する行を表示し得て、当該対応する行に格納されたデータの操作（更新、削除など）を簡略化する。エンティティオブジェクトは、しばしば、対応する行のためのビジネスロジックを封入して、所望のビジネスルールが一貫して実施されることを保証する。また、エンティティオブジェクトは、基本的なデータベースに格納された行間に存在する関係を反映するように他のエンティティオブジェクトに関連付けられ得る。
【００９４】
ＩＩＩ．プライバシ、レジデンシおよびセキュリティ
プライバシ、レジデンシおよびセキュリティ（Privacy, Residency and Security：ＰＲＳ）は、クラウドに入るデータを難読化する問題に対処することに関連する。２つの一般的な難読化方法は、暗号化およびトークン化である。これらのアプローチのいずれかを用いることにより、組織がクラウドインフラストラクチャシステム１０２によって提供されるクラウドベースのアプリケーションの利益を享受しながら依然として詮索の目がデータを解読できない状態が保証される。
【００９５】
図２は、本開示のいくつかの実施形態に係るクラウドベースのアプリケーションでプライバシ、レジデンシおよびセキュリティを提供するシステム２００のブロック図である。図２に示される実施形態では、システム２００は、１つ以上のクライアントコンピューティングデバイス２０５，２１０および２１５を含み、当該１つ以上のクライアントコンピューティングデバイス２０５，２１０および２１５は、難読化される場合もあれば難読化されない場合もあるデータへのアクセスを提供するためのサービスを含むクラウドサービスを提供するクラウドインフラストラクチャシステム２２０（たとえば、図１に関連して説明したクラウドインフラストラクチャシステム１０２）と対話するようにユーザによって使用され得る。システム２００は、示されているコンポーネント以外のコンポーネントを有していてもよいということが理解されるべきである。さらに、図２に示される実施形態は、いくつかの実施形態を組み込むことができる、クラウドベースのアプリケーションでプライバシ、レジデンシおよびセキュリティを提供するためのシステムの一例に過ぎない。いくつかの他の実施形態では、システム２００は、図に示されるよりも多くのコンポーネントもしくは少ないコンポーネントを有していてもよく、２つ以上のコンポーネントを組み合わせてもよく、またはコンポーネントの異なる構成もしくは配置を有していてもよい。
【００９６】
この例では、システム２００は、企業インフラストラクチャシステム２２５と、ＰＲＳシステム２３０と、クラウドインフラストラクチャシステム２２０とを含む。企業インフラストラクチャシステム２２５は、１つ以上のクライアントデバイス、サーバ、ネットワーキングデバイス、ルータ、プロキシ、ゲートウェイなどを含み得る。示されているように、企業インフラストラクチャシステム２２５は、ＰＲＳシステム２３０およびクラウドインフラストラクチャシステム２２０と通信する１つ以上のクライアントコンピューティングデバイス２０５，２１０および２１５を含む。示されているように、ＰＲＳシステム２３０は、ＰＲＳサーバ２３５とプライベートデータベース２４０とを含み、クラウドインフラストラクチャシステム２２０は、クラウドベースのアプリケーション２４５とクラウドデータベース２５０とを含む。
【００９７】
クライアントコンピューティングデバイス２０５，２１０および２１５は、図１に示される上記のデバイス１０４，１０６および１０８と同様のデバイスであってもよい。クライアントコンピューティングデバイス２０５，２１０および２１５は、ウェブブラウザ、所有権付きクライアントアプリケーション（たとえば、オラクルフォームズ）または何らかの他のアプリケーションなどのクライアントアプリケーションを動作させるように構成され得て、当該クライアントアプリケーションは、クラウドインフラストラクチャシステ

ム２２０と対話してクラウドインフラストラクチャシステム２２０によって提供されるサービスを使用するようにクライアントコンピューティングデバイスのユーザによって使用され得る。例示的なシステム環境２００は、３つのクライアントコンピューティングデバイスを有するものとして示されているが、いかなる数のクライアントコンピューティングデバイスがサポートされてもよい。センサを有するデバイスなどの他のデバイスがクラウドインフラストラクチャシステム２２０と対話してもよい。

【００９８】

クライアントコンピューティングデバイス２０５，２１０および２１５は、携帯可能な手持ち式のデバイス（たとえば、ｉＰｈｏｎｅ（登録商標）、セルラー電話、ｉＰａｄ（登録商標）、コンピューティングタブレット、携帯情報端末（「ＰＤＡ」））またはウェアラブルデバイス（たとえば、Ｇｏｏｇｌｅ　Ｇｌａｓｓ（登録商標）頭部装着型ディスプレイ）であってもよく、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ　Ｍｏｂｉｌｅ（登録商標）などのソフトウェア、および／もしくは、ｉＯＳ、Ｗｉｎｄｏｗｓ　Ｐｈｏｎｅ、Ａｎｄｒｏｉｄ、ＢｌａｃｋＢｅｒｒｙ　１０、Ｐａｌｍ　ＯＳなどのさまざまなモバイルＯＳを実行し、インターネット、電子メール、ショートメッセージサービス（「ＳＭＳ」）、ＢｌａｃｋＢｅｒｒｙ（登録商標）、または使用可能な他の通信プロトコルである。クライアントコンピューティングデバイス２０５，２１０および２１５は、汎用パーソナルコンピュータであってもよく、一例として、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）、Ａｐｐｌｅ　Ｍａｃｉｎｔｏｓｈ（登録商標）および／またはＬｉｎｕｘ（登録商標）ＯＳのさまざまなバージョンを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを含む。クライアントコンピューティングデバイス２０５，２１０および２１５は、さまざまな市販のＵＮＩＸ（登録商標）またはＵＮＩＸのようなＯＳのうちのいずれかを実行するワークステーションコンピュータであってもよく、当該市販のＵＮＩＸ（登録商標）またはＵＮＩＸのようなＯＳとしては、たとえばＧｏｏｇｌｅ　Ｃｈｒｏｍｅ　ＯＳなどのさまざまなＧＮＵ／Ｌｉｎｕｘ　ＯＳが挙げられるが、これらに限定されるものではない。代替的に、または加えて、クライアントコンピューティングデバイス２０５，２１０および２１５は、１つ以上のネットワークを介して通信することができる、シンクライアントコンピュータ、インターネットにより可能化されるゲームシステム（たとえば、Ｋｉｎｅｃｔ（登録商標）ジェスチャ入力デバイスを有するまたは持たないＭｉｃｒｏｓｏｆｔ　Ｘｂｏｘゲームコンソール）および／または個人メッセージ伝達デバイスなどのその他の電子デバイスであってもよい。

【００９９】

ＰＲＳサーバ２３５は、１つ以上のコンピュータおよび／またはサーバを備え得る。これらのコンピュータシステムまたはサーバは、１つ以上の汎用コンピュータ、専用サーバコンピュータ（一例として、パーソナルコンピュータ（「ＰＣ」）サーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウント型サーバなどを含む）、サーバファーム、サーバクラスタ、またはその他の適切な配置および／もしくは組み合わせで構成され得る。ＰＲＳサーバ２３５に関連付けられた１つ以上のコンピュータシステムまたはサーバは、上記のもののうちのいずれかを含むＯＳおよびいずれかの市販のサーバＯＳを実行してもよい。また、ＰＲＳサーバ２３５に関連付けられた１つ以上のコンピュータシステムまたはサーバは、ハイパーテキスト転送プロトコル（「ＨＴＴＰ」）サーバ、ファイル転送プロトコル（「ＦＴＰ」）サーバ、コモンゲートウェイインターフェイス（「ＣＧＩ」）サーバ、ＪＡＶＡ（登録商標）サーバ、データベースサーバ、電子メールサーバ、リバースプロキシなどを含むさまざまなさらなるサーバアプリケーションおよび／または中間層アプリケーションのうちのいずれかを実行してもよい。

【０１００】

特定の実施形態では、ＰＲＳサーバ２３５によって提供されるサービスは、データプライバシ、レジデンシおよびセキュリティなどの多数のサービスを含み得る。ＰＲＳサーバ２３５は、グラフィカルにインストールされ、アプリケーションに特有のアダプタを用い

てクラウドアプリケーションに特有の要件をサポートするように構成され得る。いくつかの例では、ＰＲＳサーバ２３５は、たとえば暗号化またはトークン化を用いて企業インフラストラクチャシステム２２５から出て行くデータを保護することによってデータプライバシを提供し得る。ＰＲＳサーバ２３５は、クライアントコンピューティングデバイス２０５，２１０および２１５とクラウドベースのアプリケーション２４５との間のデータ伝送をシームレスに傍受し、機密データを置換データ、たとえばトークンまたは暗号化されたデータと置換し得る。組織によって定義されるように、企業インフラストラクチャシステム２２５を出て行くことができないまたは出て行くべきでない機密データは、プライベートデータベース２４０内に、たとえばＰＲＳシステム２３０のファイアウォールの後ろにとどまるが、クライアントコンピューティングデバイス２０５，２１０および２１５のユーザは、当該機密データがあるか否かにかかわらず、クラウドベースのアプリケーション２４５の実質的に全ての機能を経験する。ＰＲＳサーバ２３５は、「オンザフライ暗号化」を実行することができ、「オンザフライ暗号化」では、機密データをローカルに格納して管理する代わりに、機密データは、クラウドベースのアプリケーション２４５に送信される前に暗号化またはトークン化され、戻ってきたときに復号化されるかまたは機密データと置き換えられる。クラウドベースのアプリケーション２４５によって受信され、任意にクラウドデータベース２５０自体に格納された機密データは、ＰＲＳシステム２３０なしに直接アクセスされた場合、値またはトークンの暗号化されたリストのようにしか見えないであろう。

【０１０１】

ＰＲＳサーバ２３５は、特定の条件を満たすデータ、たとえば機密データが企業インフラストラクチャシステム２２５から出て行くことを防止することによってデータレジデンシを提供し得る。ＰＲＳサーバ２３５は、条件を満たすデータ伝送から特定のデータを識別し、当該特定のデータをプライベートデータベース２４０に保存し、識別された特定のデータの実際の値に対する置換値（たとえば、暗号化値またはトークン）を生成し、生成された置換値をクラウドベースのアプリケーション２４５に送信し得る。識別された特定のデータの実際の値は、ローカルにプライベートデータベース２４０内にあるままであり、ローカルな規則によって統治され、企業方針の下で運用され得る。したがって、クラウドベースのアプリケーション２４５は、クラウドデータベース２５０に格納することができる置換データで動作する。ＰＲＳサーバ２３５は、トークン、分類可能なトークン、暗号化された値およびクリアテキストなどのカテゴリを用いてクラウドアプリケーションデータを分類し得る。いくつかの実施形態では、データは、本明細書で詳細に説明する難読化ストラテジを用いてフィールドごとに保護されてもよい。

【０１０２】

ＰＲＳサーバ２３５は、プライベートデータベース２４０に格納されたデータへのアクセスを管理することによってデータプライバシ、レジデンシおよびセキュリティを提供し得る。ＰＲＳサーバ２３５は、クラウドベースのアプリケーション２４５への認可されたアクセスのみが組織から生じることを保証することができる。ＰＲＳサーバ２３５は、企業インフラストラクチャシステム２２５とクラウドインフラストラクチャシステム２２０との間のセキュリティ保護された認証リンクを作成し得る。一実施形態では、ＰＲＳサーバ２３５は、アルゴリズム暗号化スキームを利用して、ネットワーク伝送において検出されたプレーンテキスト情報を読取不可能な暗号化テキストに変換するように構成される。ＰＲＳサーバ２３５は、ＰＲＳサーバ２３５がネットワーク伝送内のデータを暗号化および復号化することを可能にする鍵管理を提供し得る。鍵管理は、必要に応じて暗号鍵を生成、配布、格納、回転および無効化／破壊して、関連付けられた機密データを保護する機能を含み得る。他の実施形態では、ＰＲＳサーバ２３５は、トークン化を利用して機密データを保護するように構成される。ＰＲＳサーバ２３５は、実際の値の代わりにトークン（または、エイリアス）によるデータ置換を使用し得る。トークン化のプロセスでは、ＰＲＳサーバ２３５は、機密データを傍受して、当該データを安全に格納するプライベートデータベース２３５に当該データを送信する。同時に、ＰＲＳサーバ２３５は、ランダム

な固有の文字セット（トークン）を生成し、トークンを返して、実際のデータの代わりに使用し得る。ＰＲＳサーバ２３５（または、プライベートデータベース２４０）は、再び必要とされたときにトークン値を実際のデータと交換することを可能にする参照データベースを維持し得る。

【０１０３】

したがって、ＰＲＳサーバ２３５は、詮索の目にとっては何の意味ももたない暗号化された値またはトークン値を、実際のデータの信頼できる代用物としてクラウドベースのアプリケーション２４５などのさまざまなクラウドベースのアプリケーションで使用することを可能にし得る。クラウドベースのアプリケーション２４５は、図１に関連して説明したＡＤＦ１２４を用いて開発される１つ以上の企業アプリケーションを表わし得る。企業アプリケーションは、クラウドインフラストラクチャシステム２２０の文脈内で実行することができる。クラウドベースのアプリケーション２４５は、ＭＶＣアプリケーションを含み得て、当該ＭＶＣアプリケーションは、１）クラウドデータベース２５０との対話を処理し、ビジネスロジックを実行するモデル層、２）クライアントデバイス２０５，２１０および２１５のうちの１つ以上に配信されるアプリケーションＵＩを処理するビュー層、および３）アプリケーションフローを管理し、モデル層とビュー層との間のインターフェイスの役割を果たすコントローラ、に分離される。

【０１０４】

一局面では、ビュー層は、開発中のアプリケーションのＵＩを表示する。ビュー層は、デスクトップ、モバイルおよびブラウザベースのビューを含み得て、それらのビューの各々は、ＵＩの全てまたは一部を提供し、ビュータイプに対応するさまざまな方法でアクセス可能である。たとえば、ウェブページは、対応するＵＲＬを含むクライアント要求をクライアントデバイス２０５，２１０および２１５のうちの１つ以上から受信したことに応答してクラウドベースのアプリケーション２４５によって送信されてもよい。次いで、ウェブページは、クライアントデバイス２０５，２１０および２１５のうちの１つ以上に関連付けられたディスプレイユニット（図示せず）上にブラウザによって表示されてもよく、それによって、１つ以上のクライアントデバイス２０５，２１０および２１５のユーザがクラウドベースのアプリケーション２４５と対話することを可能にする。ビュー層（ウェブページなど）を形成するコードファイル／モジュールは、ハイパーテキストマークアップ言語（「ＨＴＭＬ」）、Ｊａｖａサーバページ（「ＪＳＰ」）およびＪＳＦのうちの１つ以上を用いて実現されてもよい。代替的に、ＵＩは、スイングおよび／またはＸＭＬなどのＪａｖａコンポーネントを用いて実現されてもよい。さらに記載されるように、ＵＩは、ユーザエクスペリエンス、ならびに、マイクロソフト社によるワードおよびエクセルなどのデスクトップアプリケーションへの精通を活用してもよい。

【０１０５】

上記のように、ＰＲＳサーバ２３５は、ネットワークトラフィックを監視（たとえば、傍受）して、プライバシ、レジデンシおよびセキュリティポリシーを実施し得る。１つ以上のクライアントデバイス２０５，２１０および２１５とクラウドベースのアプリケーション２４５との間の通信に関して、ＰＲＳサーバ２３５は、１つ以上のクライアントデバイス２０５，２１０および２１５から生じる伝送を傍受して、プライバシ、レジデンシおよびセキュリティポリシーを実施し得る。示されている例では、１つ以上のクライアントデバイス２０５，２１０および２１５は、住所＝「１２３メイン」および連絡先＝「ジョン」という情報を含むネットワーク伝送をクラウドインフラストラクチャシステム２２０に送信し得る。ＰＲＳサーバ２３５は、当該ネットワーク伝送を傍受し、その内容を検査して、情報のうちのいずれかがプライバシ、レジデンシおよびセキュリティポリシーの対象であるか否かを判断し得る。たとえば、ＰＲＳサーバ２３５は、「連絡先」情報がプライバシ、レジデンシおよびセキュリティポリシーの対象の機密データであり、クラウドインフラストラクチャシステム２２０に送信されるべきでないと判断してもよい。ＰＲＳサーバ２３５は、ネットワーク伝送を変更して、以下のように情報を暗号化またはトークン化し得る。すなわち、「連絡先」情報が機密またはプライベートデータとして指定されて

、住所＝「１２３メイン」［パブリックデータ］および連絡先＝「ＪＩＤＬ４５」［プライベートデータ］となる。ＰＲＳサーバ２３５は、トークンマップとともに暗号鍵および／または元のデータをプライベートデータベース２４０に格納し得る。次いで、ＰＲＳサーバ２３５は、置換値（たとえば、暗号化値またはトークン）を有する変更されたネットワーク伝送をクラウドベースのアプリケーション２４５に転送し得る。

【０１０６】

１つ以上のクライアントデバイス２０５，２１０および２１５とクラウドベースのアプリケーション２４５との間の通信に関して、ＰＲＳサーバ２３５は、逆のプロセスで１つ以上のクライアントデバイス２０５，２１０および２１５に向かう伝送を傍受して、プライバシ、レジデンシおよびセキュリティポリシーを実施し得る。示されている例では、ＰＲＳサーバ２３５は、「連絡先」情報が暗号化またはトークン化されていると判断し得て、ＰＲＳサーバ２３５は、ネットワーク伝送を変更して、プライベートデータベース２４０から検索取得されたトークンマップとともに暗号鍵および／または元のデータを用いて情報を復号化またはトークン化解除し得る。次いで、ＰＲＳサーバ２３５は、変更されたネットワーク伝送を１つ以上のクライアントデバイス２０５，２１０および２１５に転送し得る。

【０１０７】

図３Ａは、１つ以上のクライアントデバイス２０５，２１０および２１５を用いて企業インフラストラクチャシステム２２５内から見たときの、クラウドベースのアプリケーション２４５に関連付けられたＵＩ３００の図である。示されているように、「連絡先」ページ３０５は、１枚以上の連絡先カード３１０で表示される。各連絡先の名前３１５は、写真および住所を含む他のデータフィールドなどの他のＵＩ要素とともに見ることができる。ＰＲＳサーバ２３５の管理者は、本明細書で詳細に説明するように、ＵＩページ３００の名前フィールドを保護データとして指定し得る。図３Ｂは、クラウドインフラストラクチャシステム２２０内から見たときの、またはコンピューティングデバイスを用いて企業インフラストラクチャシステム２２５の外側の位置からクラウドベースのアプリケーション２４５にアクセスするときの、クラウドベースのアプリケーション２４５に関連付けられたＵＩ３００の図である。示されているように、「連絡先」ページ３０５′は、同一の連絡先カード３１０′で表示されるが、各連絡先の名前３１５′は、トークン化されたデータで暗号化または置換されており、写真および住所を含む他のデータフィールドなどの他のＵＩ要素は、実際の値のままである。

【０１０８】

ＩＶ．構成の自己記述

いくつかの実施形態では、クラウドベースのアプリケーション２４５に関連付けられたモデル層は、さまざまなビジネスサービスを、上記のコントローラオブジェクトなどの、当該ビジネスサービスを他の層で使用するオブジェクトに接続する、またはデスクトップアプリケーションに直接接続するデータ／コードモジュールを含む。モデル層の各抽象化データオブジェクトは、基本的なビジネスサービス層で実行されるいずれかのタイプのビジネスサービスへのアクセスに使用できる対応するインターフェイスを提供する。データオブジェクトは、クライアントからのサービスのビジネスサービス実装詳細を抽象化し、および／または、データ制御方法／属性をビューコンポーネントに公開し得て、それによって、ビュー層およびデータ層の分離を提供する。

【０１０９】

一局面では、モデル層は、メタデータファイルを利用してＵＩを定義するデータ制御およびデータ結合の２つのコンポーネントで構成される。データ制御は、クライアントからのビジネスサービス実装詳細を抽象化する。データ結合は、データ制御方法および属性をＵＩコンポーネントに公開して、ビューおよびモデルのクリーンな分離を提供する。データベースオブジェクトをモデル化することによって、クラウドデータベース２５０を作成してクラウドベースのアプリケーション２４５とともに使用することができる。ウィザードまたはダイアログを用いて、データベーステーブルからエンティティオブジェクトを作

成することができる。それらのエンティティオブジェクトからビューオブジェクトが作成され、アプリケーションにおけるページによって使用される。検証ルールおよび他のタイプのビジネスロジックが実装されてもよい。

【０１１０】

エンティティオブジェクトは、データベーステーブル内の対応する行を表示し得て、当該対応する行に格納されたデータの操作（更新、削除など）を簡略化する。エンティティオブジェクトは、しばしば、対応する行のためのビジネスロジックを封入して、所望のビジネスルールが一貫して実施されることを保証する。また、エンティティオブジェクトは、基本的なデータベースに格納された行間に存在する関係を反映するように他のエンティティオブジェクトに関連付けられ得る。

【０１１１】

したがって、エンティティオブジェクトは、クラウドデータベース２５０内の行を表示し、その関連付けられた属性の変更を簡略化するＡＤＦビジネスコンポーネントであり得る。エンティティオブジェクトは、行を表示することになるクラウドデータベース２５０内のデータベーステーブルを特定することによって定義することができる。次いで、エンティティオブジェクト間の関係を反映するように関連付けが作成され得る。実行時、エンティティ行は、関連するエンティティ定義オブジェクトによって管理され、各エンティティ行は、関連する行鍵によって識別される。エンティティ行は、データベーストランザクションをクラウドデータベース２５０に提供するクラウドベースのアプリケーション２４５に関連付けられたアプリケーションモジュールの文脈内で検索取得されて変更される。

【０１１２】

図４は、本発明に係る一実施形態におけるエンティティ間で共有される属性を示すブロック図である。図４は、エンティティオブジェクト、たとえばアカウントオブジェクト４０５、連絡先オブジェクト４１０、連絡先オブジェクト４１５および従業員オブジェクト４２０を示す。図４はさらに、データベーステーブル、たとえば住所テーブル４２５、電話／電子メールテーブル４３０および人物テーブル４３５を示し、各々は、エンティティ間で共有されるさまざまな属性４４０，４４５および４５０を含む。示されているように、アカウントオブジェクト４０５および連絡先オブジェクト４１０の住所属性４４０は、同一のデータベーステーブル、たとえば住所テーブル４２５に格納され得る。各行は、関連する行鍵によって識別されて、当該行がアカウントオブジェクト４０５および／または連絡先オブジェクト４１０の住所属性４４０の値を保持しているか否かを特定し得る。同様に、アカウントオブジェクト４０５および連絡先オブジェクト４１０の電話／電子メール属性４４５は、同一のデータベーステーブル、たとえば電話／電子メールテーブル４３０に格納され得る。さらに示されているように、連絡先オブジェクト４１５および従業員オブジェクト４２０は、人物テーブル４３５に格納された属性４５０を有する人物オブジェクトのサブタイプであり得る。各行は、行鍵によって識別されて、当該行が保持する人物オブジェクトのタイプ、たとえば連絡担当者であるか従業員人物であるか、を特定し得る。

【０１１３】

ＰＲＳサーバの一般的アプローチは、通信量を探ったり監視したりして保護フィールド上でデータ暗号化またはトークン化を実行するというものであるので、この機能を、図４に示されるさまざまなエンティティオブジェクトを共有するコンポーネントを利用するクラウドベースのアプリケーションと統合することは困難であろう。従来、ユーザは、保護したい機密フィールドをマーキングするように各クラウドベースのアプリケーションの各ＵＩページを構成しなければならなかった。たとえば、ユーザは、たとえ同一の基本的なデータベーステーブルまたは属性を共有していても、連絡先オブジェクト４１５のためにＵＩページを構成し、従業員オブジェクト４２０のためにＵＩページを構成する必要があるかもしれない。これは、大きくかつ複雑なアプリケーションでは非常に難しくなる。たとえ正規表現を用いて管理者が行う作業の量を減らしても、ユーザは考えられる全てのＵＩページを検討して各ＵＩページを１つずつ構成しなければならないかもしれない。また

、クラウドベースのアプリケーションは、共有および再利用されるコンポーネントを有し得るので、フィールドの同一の識別子が、必ずしもフィールドの実際の「意味」を反映していなくても、複数のＵＩ上で使用される場合がある。正規表現を用いることは、非常に手間がかかるだけでなく、機密データの漏えいまたは非機密情報の保護に関する不必要な性能オーバーヘッドが生じることにもつながり得る。

【０１１４】

これらの問題を克服するために、いくつかの実施形態では、クラウドインフラストラクチャシステム２２０は、ＰＲＳサーバ２３５に対してクラウドベースのアプリケーション２４５のエンティティオブジェクト、ＵＩページなどの構成を自己記述するための１つ以上のサービスを提供することができる。クラウドインフラストラクチャシステム２２０は、ＰＲＳサーバ２３５の管理者が（たとえば、企業インフラストラクチャシステム２２５に関連付けられた組織の要求により）クラウドベースのアプリケーション２４５のデータまたはコンポーネントレベルで機密データを識別することを可能にするＡＰＩを提供することができる。たとえば、管理者は、機密データが企業インフラストラクチャシステム２２５外のどこで使用されても、社会保障番号属性４５０を含むありとあらゆる連絡先および従業員オブジェクト４１５，４２０のデータが保護されるように、エンティティオブジェクトの社会保障番号属性４５０をデータレベルでマーキングしてもよい。別の例では、管理者は、名前属性４５０を含む所与のコンポーネントによって使用されるエンティティオブジェクトのみが、企業インフラストラクチャシステム２２５外で所与のコンポーネントによって使用されたときに保護されるように、特定のタイプのエンティティオブジェクト（たとえば、従業員オブジェクト４２０）のみの名前属性４５０をコンポーネントレベルでマーキングしてもよい。次いで、クラウドインフラストラクチャシステム２２０は、ＰＲＳサーバ２３５によって認識されるＵＩ要素とマーキングされたフィールドとの間にマップを動的に生成し得る。このように、クラウドインフラストラクチャシステム２２０は、どこで使用されようと、およびどの値が識別子に関連付けられようと、共有されるコンポーネントを保護することができる。これにより、ＰＲＳサーバ２３５によって複数の入力を維持させる必要性が低くなる。

【０１１５】

ＰＲＳサーバ２３５を用いて機密データオブジェクトが識別されると、一実施形態では、管理者は、（１）コンポーネントの基本的なデータ層にヒントを追加し、（２）コンポーネントに保護鍵属性を追加し得る。保護されたエンティティオブジェクトを用いてクラウドベースのアプリケーション２４５がＵＩページを生成すると、それらの保護されたコンポーネントを含むいかなるデータも、識別子とＰＲＳサーバ２３５によって認識可能なフィールドとの間のマップとともに、ネットワーク伝送のペイロードで送信され、必要なデータ暗号化／トークン化が実行される。したがって、コンポーネントを構成する際に、コンポーネントの値が保護されるべきか否かを制御する、保護鍵という名前の新たな属性を編集可能値コンポーネントに追加することができる。属性の値は、ＰＲＳサーバ２３５が認識するコンポーネントの名前であってもよい。ＰＲＳサーバ２３５によって認識される値を含む保護ヒントを抽出するためにクラウドベースのアプリケーション２４５のデータ結合層においてロジックが追加され得る。コンポーネントレベルで保護鍵が存在しなければ、クラウドベースのアプリケーション２４５は、データ結合層から保護鍵属性を検索取得し得る。要求がクラウドベースのアプリケーション２４５に送信されると、関連する保護データがあれば、保護鍵マップへの構築ｉｄがネットワーク伝送のペイロードに挿入され得る。このように、ＰＲＳサーバ２３５によって認識可能なオブジェクト／フィールドにコンポーネントクライアント識別子を直接マッピングする代わりに、静的な構成に基づいて実行中にマップを生成することができる。

【０１１６】

図５は、いくつかの実施形態におけるＰＲＳサーバ２３５の自己記述的な構成を提供するメッセージシーケンス図を示す。ブロック５０２において、クラウドインフラストラクチャシステム２２０は、クラウドベースのアプリケーション２４５によって使用されるデ

ータモデルにＡＰＩを提供し、当該ＡＰＩからＰＲＳサーバ２３５は構成にアクセスすることができる。ＡＰＩを提供することは、アプリケーションまたは設計者が要求（一般に、ＨＴＴＰ要求、ＳＯＡＰ要求、ＸＭＬメッセージなど）に行き当たる可能性があるサーバ側エンドポイントを提供することを含み得る。サーバ側エンドポイントは、明確に定義されたＵＲＬスキーム（たとえば、www.enterpirse.com/contacts）を有するＨＴＴＰエンドポイントを用いて実現されてもよい。ブロック５０４において、ＰＲＳサーバ２３５は、提供されたＡＰＩを用いてクラウドインフラストラクチャシステム２２０にデータモデルの構成データを要求する。構成データは、データモデルを用いてモデル化されるエンティティの保護可能な属性／コンポーネントのセット（たとえば、プライバシ、レジデンシおよびセキュリティポリシーの対象であるように構成され得る属性／コンポーネントに関する情報）を含み得る。要求５０６は、ＨＴＴＰ要求、ＳＯＡＰ要求、ＸＭＬメッセージなどを含み得る。ブロック５０８において、クラウドインフラストラクチャシステム２２０は、データモデルを用いてモデル化されるエンティティの保護可能な属性／コンポーネントのセットを含む構成データを提供する。いくつかの実施形態では、構成データは、保護可能な属性のセット内の各属性に適用され得る保護のタイプ（たとえば、トークン化可能または暗号化可能）をさらに含む。

【０１１７】

一実施形態では、クラウドインフラストラクチャシステム２２０は、クラウドベースのアプリケーション２４５によって使用される保護可能な属性／コンポーネントのリストを維持する。また、クラウドインフラストラクチャシステム２２０は、保護フィールドについてのタイプ情報などのヒントを、保護可能な属性／コンポーネントのリストとともにＰＲＳサーバ２３５に送信してもよい。当該ヒントは、保護可能なデータのパラメータに関する情報を提供し得る。クラウドインフラストラクチャシステム２２０は、以下のフォーマットを有する応答５１０を返す。

【０１１８】

【数１】

```
<objects>
 <object name="emp" type="object">
  <field name="fname" protectable="protectable" tokenizable="tokenizable"
type="short_text"
  maxLength="255"/>
   <description>Employee's first name</description>
  </field>
  <field name="lname" protectable="protectable" tokenizable="tokenizable"
type="short_text"
  maxLength="255"/>
   <description>Employee's last name</description>
  </field>
  <field name="email" protectable="protectable" encryptable="encryptable"
type="short_text"
  maxLength="255"/>
   <description>Employee's email address</description>
  </field>
 </object>
</objects>
```

【０１１９】
ブロック５１２において、ＰＲＳサーバ２３５は、クラウドインフラストラクチャシステム２２０から受信した保護可能な属性／コンポーネントに関する情報を用いてユーザインターフェイスを生成する。当該ユーザインターフェイスは、ＰＲＳサーバ２３５の管理者が、モデル化されたエンティティの１つ以上の保護可能な属性／コンポーネントを、保護された属性／コンポーネントとして構成することを可能にする。ブロック５１４において、ＰＲＳサーバ２３５の管理者は、（たとえば、企業インフラストラクチャシステム２２５に関連付けられた組織の要求により）モデル化されたエンティティの１つ以上の保護可能な属性／コンポーネント、たとえばオブジェクト「ｅｍｐ」におけるフィールド「ｆｎａｍｅ」を、保護された属性／コンポーネントとしてマーキングされるようにユーザインターフェイスにおいて構成する。いくつかの実施形態では、属性／コンポーネントを保護されているものとしてマーキングすることは、属性／コンポーネントに適用される保護のタイプ（たとえば、トークン化または暗号化）に関する表示をさらに含み得る。ブロック５１６において、ＰＲＳサーバ２３５は、ユーザインターフェイスを用いて生成された保護された属性／コンポーネントの情報をクラウドインフラストラクチャシステム２２０に送信することによって、保護された属性／コンポーネントをクラウドインフラストラクチャシステム２２０に通知する。一実施形態では、ＰＲＳサーバ２３５は、以下のフォーマットを有するメッセージ５１８を送信する。

【０１２０】
【数２】

```
<objects>
 <object name=“emp” type=“object”>
  <field name=“fname” protect=“protect” tokenize=“tokenize"/>
  <field name=“lname” protect=“protect” tokenize=“tokenize"/>
 </object>
</objects>
```

【０１２１】
ブロック５２０において、クラウドインフラストラクチャシステム２２０は、指定されたコンポーネントまたはエンティティオブジェクト属性を、保護されているものとしてマーキングする。ブロック５２２において、クラウドインフラストラクチャシステム２２０は、保護フィールドの確認情報をＰＲＳサーバ２３５に送信し得る。クラウドインフラストラクチャシステム２２０は、以下のフォーマットを有する応答５２４を返し得る。

【０１２２】
【数３】

```
<objects>
 <object name=“emp” type=“object”>
  <field name=“fname” protect=“protect” tokenize=“tokenize" type=“short_text”
  maxLength=“255”/>
  <field name=“lname” protect=“protect” tokenize=“tokenize" type=“short_text”
  maxLength=“255”/>
 </object>
</objects>
```

【０１２３】
図６は、本発明に係る一実施形態における自己記述的な構成を利用するためのメッセージシーケンス図を示す。ブロック６０２において、クライアントデバイス２０５，２１０および２１５のうちの１つ以上は、クラウドインフラストラクチャシステム２２０にＵＩ

ページまたはクライアントコンポーネントを要求する。要求６０４は、ＨＴＴＰ要求、ＳＯＡＰ要求、ＸＭＬメッセージなどを含み得る。ブロック６０８において、クラウドインフラストラクチャシステム２２０は、各々の保護された属性の識別子を決定する。一実施形態では、クラウドベースのアプリケーション２４５（たとえば、オラクルＡＤＦフェイスレンダリング）に関連付けられたＵＩまたはコンポーネントランタイムは、データモデルレベルに各々の保護フィールドのトークン化識別子を尋ねる。ブロック６１０において、クラウドインフラストラクチャシステム２２０は、ＵＩまたはクライアントコンポーネントを生成し、保護フィールドをマーキングする。クラウドインフラストラクチャシステム２２０は、応答６１２の際に、マーキングされた保護フィールドを有する生成されたＵＩまたはクライアントコンポーネントを返し得る。ブロック６１０において生成されるマーキングされた保護フィールドは、応答６１２のペイロードに含まれる。たとえば、保護フィールドをマーキングすることは、以下のフォーマットを有し得る。

【０１２４】

【数４】

```
<label class="af_inputText_label-text" for="it3::content">Ename</label></td><td
valign="top" nowrap class="xve"><input id="it3::content" name="it3" style="width:auto"
class="x25" size="10" maxlength="10" type="text" value="testname"
protetionKey="EMP_OBJ/Ename_FLD"></td>
```

【０１２５】

生成されたＵＩまたはクライアントコンポーネントは、以下のフォーマットを有し得る。

【０１２６】

【数５】

```
AdfPage.PAGE.addComponents(newAdfRichInputText('it3',{'columns':10,'maximumLength'
:10,'protectionKey':'EMP_OBJ/Ename_FLD'))
```

【０１２７】

応答６１２の後続のペイロードは、以下のフォーマットを有するマップ情報を含み得る。

【０１２８】

【数６】

```
oracle.adf.view.rich.TOKENIZED={'it3':{'EMP_OBJ/Ename_FLD'}'}
```

【０１２９】

ブロック６１４において、ＰＲＳサーバ２３５は、応答６１２を傍受し、応答６１２のペイロードに含まれるマップを用いて、ＵＩまたはクライアントコンポーネントにプライベートデータベース２４０からのいずれかの保護されたデータを投入する。たとえば、ＰＲＳサーバ２３５は、マップを用いて、<field name="fname" protect="protect" tokenize="tokenize"/>で用いられるランダムなトークン化された値を、同一の保護フィールド：<field name="fname" protect="protect" tokenize="tokenize"/>についてのプライベートデータベース２４０に格納された機密データ値と置換する。次いで、ＰＲＳサーバ２３５は、変更された応答６１６を１つ以上のクライアントデバイス２０５，２１０および２１５に転送する。ブロック６１８において、１つ以上のクライアントデバイス２０５，２１０および２１５は、保護フィールド内のプライベートデータベース２４０からのいずれかの保護されたデータを含む生成されたＵＩまたはクライアントコンポーネントを表示する。

【０１３０】

ブロック６２０において、１つ以上のクライアントデバイス２０５，２１０および２１

５は、クラウドインフラストラクチャシステム２２０にデータを掲載し得る。掲載されたデータは、ＵＩまたはクライアントコンポーネント内の保護フィールドの機密データに対する変更または更新を含み得る。一実施形態では、クライアントランタイム（たとえば、ＡＤＦフェイスクライアント）は、ＵＩまたはクライアントコンポーネントのトークン化情報を用いて、ＰＲＳサーバ２３５へのマッピングを周知のフィールド（たとえば、保護鍵）を使用して手取り足取り教える。たとえば、ＰＲＳサーバ２３５は、当該周知のフィールドを用いて、その構成を調べて対応するアクション（たとえば、暗号化またはトークン化）を見つけ出してもよい。ブロック６２２において、１つ以上のクライアントデバイス２０５，２１０および２１５は、マッピングを要求６２４（たとえば、oracle.adf.view.rich.TOKENIZED={'rl:0:foo:itl':{'object':'emp','field':'fname'}}などのgenerate ID->protectionKey Map）に挿入する。１つ以上のクライアントデバイス２０５，２１０および２１５は、ブロック６２２からのマッピングを含むように、要求６２４を以下の通り生成し得る。

【０１３１】

【数７】

r1:0:foo:it1=SecretFirstName

r1:0:foo:it5=PublicLastName

r2:1:bar:it1=publicemail@oracle.com

javax.faces.ViewState=!-12t5t4tf7q

org.apache.myfaces.trinidad.faces.FORM=f1

Adf-Page-Id=0

event=b5

event.b5=<m xmlns="http://oracle.com/richClient/comm"><k

v="type"><s>action</s></k></m>

oracle.adf.view.rich.PROCESS=f1,b5

oracle.adf.view.rich.TOKENIZED={'r1:0:foo:it1':{‘object’:’emp', ‘field’:’fname'}}

【０１３２】

ブロック６２６において、ＰＲＳサーバ２３５は、要求６２４を傍受し、マップ（たとえば、ID->protectionKey Map）を用いて、いずれかの保護されたデータを暗号化またはトークン化された値と置換し、保護されたデータをプライベートデータベース２２５に格納する。次いで、ＰＲＳサーバ２３５は、変更された要求６２８をクラウドインフラストラクチャシステム２２０に転送する。

【０１３３】

したがって、ＰＲＳサーバ２３５の管理者は、データモデル／コンポーネントレベルで機密データを識別して、それらを自己記述的な態様でマーキングすることができる。クラウドベースのアプリケーションに関連付けられたいかなる生成されたＵＩ要素も、ＰＲＳサーバ２３５によって認識されるオブジェクト／フィールドトークンに動的にマッピングすることができる。このように、共有されるコンポーネントは、それがどこで使用されようと、およびそれがどのｉｄ値を有していようと、常に保護されることになる。さらに、複数の入力をＰＲＳサーバ２３５に追加する必要はない。

【０１３４】

Ｖ．保護されたデータ列と保護されていないデータ列とで同一のテーブルを共有することのサポート

クラウドデータベース２５０は、機密データの暗号化またはトークン化されたバージョンを含み得る。上記で示唆されるように、エンティティオブジェクトは、同一の構造を共有し、同一のデータベーステーブルを共有する可能性がある。いくつかのエンティティオ

ブジェクトは保護することができるが、他のエンティティオブジェクトは保護されない。従来より、異なる保護構成を提供するには異なるデータベーステーブルが必要であり、その結果、データベーステーブルが重複する。

【０１３５】

これらの問題を克服するために、いくつかの実施形態では、ＰＲＳサーバ２３５の管理者がデータオブジェクト層においてコンポーネントまたはデータオブジェクトの保護ルールを構成する際に、特定の行がどのコンポーネントまたはデータオブジェクトに属しているかを識別するために識別フラグを定義することができる。したがって、異なる保護ルールを有しながら同一の構造を共有している全てのコンポーネントまたはデータオブジェクトは、依然として同一のデータベーステーブルを共有することができる。これにより、複数の同様のデータベーステーブルを維持するという管理者の作業が簡略化されるが、いかなるセキュリティ問題も発生させることなく、構造的に同様にコンポーネントまたはデータオブジェクト上で動作する共通のロジックを再利用することも可能になる。

【０１３６】

図７は、本発明の一実施形態に係るクラウドベースのアプリケーション２４５に関して用いられるさまざまな層を示す図である。層７１０は、クラウドデータベース２５０に格納される、クラウドベースのアプリケーション２４５によって使用されるデータテーブルを表わす。示されているデータベーステーブルは、コンポーネントまたはデータオブジェクトの識別フラグとして指定される少なくとも１つの列、たとえばエンティティ識別子属性「ＴＹＰＥ」を含む。示されているデータベーステーブルは、クラウドベースのアプリケーション２４５によって使用される複数のコンポーネントまたはデータオブジェクト間で共有される属性の上位セットをサポートするように構成され得る。識別フラグを用いて、特定の行が属しているコンポーネントまたはデータオブジェクト、たとえば従業員オブジェクトおよび連絡先オブジェクトを識別することができる。理解されるべきであるように、複数のコンポーネントまたはデータオブジェクトは、異なる保護ルール、たとえばトークン化、暗号化または無保護、を有しながら同一のデータベーステーブルを共有することができる。

【０１３７】

セキュリティ構成（すなわち、コンポーネントまたはデータオブジェクトの保護ルール）は、データベーステーブルの上側の層、たとえばデータモデル層７２０に配置され得る。各データモデルの属性、たとえばＴＹＰＥは、明示的に定義される場合もあれば、示唆される場合もある。識別フラグがデータオブジェクトに組み込まれるので、データオブジェクトがたとえばさまざまなＵＩコンポーネントに結合されているようにクラウドベースのアプリケーション２４５で使用される際に、データオブジェクトに属している行のみがピックアップされるべきである。たとえば、「Ｅｍｐ」オブジェクトでは、「Ａ」属性は、保護されているため、保護状態と保護鍵との２つのヒントをデータモデル層内に有する。これらは、「Ｃｏｎｔａｃｔ」オブジェクト内の「Ａ」属性には存在しない。さらに、「Ｃｏｎｔａｃｔ」オブジェクトでは、「Ｂ」属性は、保護されているため、保護状態と保護鍵との２つのヒントをデータモデル層内に有する。これらは、「Ｅｍｐ」オブジェクト内の「Ｂ」属性には存在しない。したがって、データ保護はデータオブジェクトレベルで構成され、そのため、データオブジェクトに属している行のみが暗号化／トークン化の対象になる。

【０１３８】

データオブジェクトは、ＵＩ層７３０内の１つ以上のＵＩコンポーネントに結合され得る。一般に、データオブジェクトは、データオブジェクトの１つ以上の属性をレンダリングするためのＵＩコンポーネントに結合される。たとえば、データモデル層７２０からのデータオブジェクトは、<af:inputText id="FIELD1" value="#{EMPbinding.A.inputValue}"/>などの標準的な式言語を介してＵＩ層７３０に公開されてもよい。ドキュメントオブジェクトモデル層７４０では、レンダリングされたＵＩコンポーネントは、特定のドキュメントオブジェクトモデル（document object model：ＤＯＭ）要素が保護フィールドで

あることを示す識別子を含み得る。上記のように、当該識別子は、ＰＲＳサーバ２３５によって生成されるトークン識別子を含み得る。

【０１３９】

図８は、本発明に係る一実施形態における保護されたデータ列と保護されていないデータ列とで同一のテーブルを共有することをサポートするための方法８００のフローチャートである。図８に示される方法８００の実現または図８に示される方法８００における処理は、コンピュータシステムまたは情報処理装置などのロジックマシンの中央処理装置（ＣＰＵまたはプロセッサ）によって実行されたときにソフトウェア（たとえば、命令またはコードモジュール）によって行われてもよく、電子デバイスまたは特定用途向け集積回路のハードウェアコンポーネントによって行われてもよく、またはソフトウェア要素とハードウェア要素との組み合わせによって行われてもよい。図８に示される方法８００は、ステップ８１０から開始する。

【０１４０】

ステップ８１０において、複数のデータオブジェクトをサポートするデータベーステーブル定義を受信する。データベーステーブルは、複数のデータオブジェクトをサポートするように定義することができる。たとえば、人物テーブルは、複数のデータオブジェクト間で共有される属性の上位セットに対応する列を含み得る。ステップ８２０において、少なくとも１つの列をデータオブジェクトの識別フラグとして指定する。いくつかの実施形態では、データベーステーブルの予め定められた列が用いられてもよく、または識別フラグのために新たな列が作成されてもよい。

【０１４１】

ステップ８３０において、少なくともデータベーステーブルによってサポートされるデータオブジェクトの属性を保護フィールドとして指定する。自己記述的な構成の提供に関連して上記したように、ＰＲＳサーバ２３５の管理者は、クラウドベースのアプリケーション２４５によって使用されるデータオブジェクトのリストを要求し得る。管理者は、どのデータオブジェクト（および／または、それらの個々の属性）がセキュリティポリシーの対象であるかを選択し、当該情報をクラウドベースのアプリケーション２４５に送信し得る。次いで、クラウドベースのアプリケーション２４５は、保護される必要があるいかなるデータベーステーブル、データモデルおよびコンポーネントも構成し得る。

【０１４２】

ステップ８４０において、保護されたデータと保護されていないデータとが混在するデータベーステーブルにデータを格納する。したがって、ＰＲＳサーバ２３５の管理者がデータオブジェクト層においてコンポーネントまたはデータオブジェクトの保護ルールを構成する際に、特定の行がどのコンポーネントまたはデータオブジェクトに属しているかを識別するために識別フラグを定義することができる。したがって、異なる保護ルールを有しながら同一の構造を共有している全てのコンポーネントまたはデータオブジェクトは、依然として同一のデータベーステーブルを共有することができる。これにより、複数の同様のデータベーステーブルを維持するという管理者の作業が簡略化されるが、いかなるセキュリティ問題も発生させることなく、構造的に同様にコンポーネントまたはデータオブジェクト上で動作する共通のロジックを再利用することも可能になる。

【０１４３】

ＶＩ．保護フィールド上での自動オペレーション検出

データオブジェクトが異なれば保護フィールドも異なり得るので、クラウドベースのアプリケーション２４５によって実行される特定のオペレーションは、オペレーションが保護フィールド対して実行されると無効になる場合がある。いくつかの実施形態では、クラウドベースのアプリケーション２４５は、ユーザの混乱を回避するために、サポートされていない可能性のあるオペレーションを自動的に判断することができる。たとえば、クラウドベースのアプリケーション２４５は、保護されたデータに関する全ての可能な演算子を調べ、それらをイネーブル／ディスエーブルにすることに関して賢明な決定を行ってもよい。これにより、保護されたデータに対して実行される特定のオペレーションに関して

発生する誤った結果を回避するのに必要な作業の量を大幅に減少させることができる。この場合、自己記述的な構成は有用である。なぜなら、特定のフィールドの保護状態に対して変更がなされたときに、クラウドベースのアプリケーション２４５は、当該変更に気付いて、いかなる関連する演算子も自動的にイネーブル／ディスエーブルにすることができるからである。イネーブル／ディスエーブルにすることができるオペレーションのいくつかの例としては、保護されたデータに関するサーバ側の確認、保護されたデータに関する自動提案挙動、保護されたデータに対する完全一致検索の可能化、保護されたデータに対するソートなどが挙げられる。

【０１４４】

図９は、本発明に係る一実施形態における保護フィールドの自動オペレーション検出のための方法９００のフローチャートである。図９に示される方法９００の実現または図９に示される方法９００における処理は、コンピュータシステムまたは情報処理装置などのロジックマシンの中央処理装置（ＣＰＵまたはプロセッサ）によって実行されたときにソフトウェア（たとえば、命令またはコードモジュール）によって行われてもよく、電子デバイスまたは特定用途向け集積回路のハードウェアコンポーネントによって行われてもよく、またはソフトウェア要素とハードウェア要素との組み合わせによって行われてもよい。図９に示される方法９００は、ステップ９１０から開始する。

【０１４５】

ステップ９１０において、データモデル層においてデータモデル層構成を生成し、当該データモデル層構成をＰＲＳサーバ２３５で受信する。たとえば、ＰＲＳサーバ２３５は、クラウドインフラストラクチャシステム２２０のＡＰＩを利用して、セキュリティポリシーの対象となるデータモデル属性を取得してもよい。データモデル層構成は、以下のフォーマットを有し得る。

【０１４６】

【数８】

```
<EMP_OBJAttribute
  Name="Ename"
  AttrName="FName">
  <Properties>
   <CustomProperties>
    <Property
     Name="protectionState"
     Value="TOKENIZED"/>
    <Property
     Name="protectionKey"
     Value="EMP_OBJ/Fname_FLD"/>
   </CustomProperties>
  </Properties>
 </EMP_OBJAttribute>
```

【０１４７】

ステップ９２０において、１つ以上の保護フィールドを決定する。自己記述的な構成の提供に関連して上記したように、ＰＲＳサーバ２３５の管理者は、クラウドベースのアプリケーション２４５によって使用されるデータオブジェクトのリストを要求し得る。管理者は、どのデータオブジェクト（および／または、それらの個々の属性）がセキュリティ

ポリシーの対象であるかを選択し、当該情報をクラウドベースのアプリケーション２４５に送信し得る。次いで、クラウドベースのアプリケーション２４５は、どのフィールドが保護されるかを判断し得る。

【０１４８】

ステップ９３０において、保護フィールドを用いて実行可能なオペレーションを決定する。これは、保護フィールドが検索可能であるか否か、オートコンプリートで使用されるか否かなどを判断することを含み得る。ステップ９４０において、保護フィールド上で実行可能な決定されたオペレーションに基づいてクラウドベースのアプリケーション２４５を構成する。一実施形態では、クラウドベースのアプリケーション２４５は、保護されたデータに関する検証ツールを処理する際に、必要なチェックのみを処理してその他の検証ツールをスキップするように構成されてもよい。クラウドベースのアプリケーション２４５は、保護されたデータに関する自動提案挙動を制御するためのロジックを追加するように構成されてもよい。クラウドベースのアプリケーション２４５は、クエリページをレンダリングする際に、完全一致検索演算子のみを可能にするように構成されてもよい。クラウドベースのアプリケーション２４５は、テーブルをレンダリングする際に、保護されたデータオブジェクトからの列に関するソートをディスエーブルにするように構成されてもよい。

【０１４９】

ＶＩＩ．連合検索

保護フィールドに対して運用された場合に無効になる可能性がある、クラウドベースのアプリケーション２４５によって実行可能な１つのオペレーションは、検索である。特定のフィールドが保護される場合、検索が問題になる。従来より、完全一致をサポートするためだけに検索機能に支障を来すか、ＰＲＳサーバ２３５が１つ１つの検索可能な行の完全なコピーを有していなければならず、クラウドデータベース２５０とプライベートデータベース２４０との間にはデータ重複セットアップがあるか、のいずれかである。次いで、ＰＲＳサーバ２３５は、機密データの検索も、最終結果をレンダリングするためのロジックのレンダリングも実行する必要がある。

【０１５０】

いくつかの実施形態では、１つ以上のクライアントデバイス２０５，２１０および２１５は、プライベートデータベース２４０およびクラウドデータベース２５０を検索することにより生成された検索結果を連合または集中化し得る。クラウドベースのアプリケーション２４５に関連付けられたページのレンダリングは、非常に複雑である可能性がある。たとえば、ＰＲＳサーバ２３５がクラウドベースのアプリケーション２４５をレンダリングしなければならない場合にクラウドベースのアプリケーション２４５をＰＲＳサーバ２３５と統合することは、ユーザにとって大仕事である可能性がある。クライアント側での連合検索を用いることによって、統合作業の量を減少させることができ、クラウドベースのアプリケーション２４５は、最終結果ページを完全にレンダリングすることができるため、全てのページは同一のルック・アンド・フィールを有することになり、一貫したものになる。したがって、連合検索は、エンドユーザに透過的な、保護フィールドおよび無保護フィールドに対する検索を行う。また、機密データに対する検索性に支障を来すことはない。

【０１５１】

さまざまな実施形態では、１つ以上のクライアントデバイス２０５，２１０および２１５は、元の検索を２つの検索に分割する。１つ以上のクライアントデバイス２０５，２１０および２１５は、図６のブロック６１０に見られるようなマーキングされた保護フィールドに基づいて元の検索を分割する。なぜなら、１つ以上のクライアントデバイス２０５，２１０および２１５の各々は、どのフィールドが保護されており、どのフィールドが保護されていないかを知っているからである。第１の検索は、プライベートデータベース２４０を用いて保護フィールドに対して実行され（たとえば、検索要求ペイロードは、ＰＲＳサーバ２３５が保護フィールドに対してのみクライアント側検索を実行するための情報

を有し）、第２の検索は、クラウドデータベース２５０を用いて無保護フィールドを含む全ての他のフィールドに対して実行される（たとえば、ＰＲＳサーバ２３５は、その後、クラウドベースのアプリケーション２４５が保護トークンにより新たな検索語を理解するようにペイロード情報を変更してもよい）。保護フィールドに対する第１の検索は、ＰＲＳサーバ２３５を用いて実行され、結果セットは、（元の検索に加えて）クラウドベースのアプリケーション２４５に渡される。クラウドベースのアプリケーション２４５は、第１および第２の検索から最終結果セットを組み立てて、連合された検索結果ページをレンダリングすることができる。

【０１５２】

たとえば、ユーザが「FirstName startwith 'B'」を検索する際、「Ｅｍｐ」オブジェクトの「firstName」属性は、保護鍵EMP_OBJ/Ename_FLDで保護されてもよく、元の検索要求は、必要な全ての情報を含む。ＰＲＳサーバ２３５は、要求を傍受し、プライベートデータベース２４０においてFirstNameを検索し、要求のペイロードを全ての一致したFirstNameのトークン化された値で更新し、要求をクラウドベースのアプリケーション２４５に渡す。次いで、クラウドベースのアプリケーション２４５は、ＰＲＳサーバ２３５からのトークン化された値を用いてクラウドデータベース２５０を検索し、最終ページレンダリングで用いられる最終結果データセットを生成する。レンダリングされたページは、１つ以上のクライアントデバイス２０５，２１０および２１５に戻される。ＰＲＳサーバ２３５は、応答を傍受し、１つ以上のクライアントデバイス２０５，２１０および２１５に送信する前に、トークン化された値を実際のテキストに変換する。ＰＲＳサーバ２３５からの保護フィールドの検索結果と、クラウドベースのアプリケーション２４５において直接なされた無保護フィールド検索結果とは、組み合わせられて最終データセットになる。

【０１５３】

さまざまな実施形態では、ユーザが検索を開始すると、検索基準のうちのいずれかが保護フィールドに対するものであれば、ＰＲＳサーバ２３５は、プライベートデータベース２４０に対して検索を適用し得る。ＰＲＳサーバ２３５は、行鍵によって識別される適格な行のセットとして結果セットを生成し得る。次いで、行鍵のセットは、クラウドベースのアプリケーション２４５に対する検索要求に送信される。クラウドベースのアプリケーション２４５が当該検索要求を処理する際に、適格な行鍵のセットを用いて最終検索結果をフィルタリングする。たとえば、行鍵を用いて、検索基準に一致するトークン化または暗号化されたデータを識別し、トークン化または暗号化されたデータは、クラウドデータベース２５０内の保護されていないデータに対して検索基準を実行することにより得られる検索結果に追加される。最終検索結果は、レンダリングされ、１つ以上のクライアントデバイス２０５，２１０および２１５に戻されて、元の検索要求に対する応答として表示される。

【０１５４】

図１０は、本発明に係る一実施形態における連合検索の方法１０００のフローチャートである。図１０に示される方法１０００の実現または図１０に示される方法１０００における処理は、コンピュータシステムまたは情報処理装置などのロジックマシンの中央処理装置（ＣＰＵまたはプロセッサ）によって実行されたときにソフトウェア（たとえば、命令またはコードモジュール）によって行われてもよく、電子デバイスまたは特定用途向け集積回路のハードウェアコンポーネントによって行われてもよく、またはソフトウェア要素とハードウェア要素との組み合わせによって行われてもよい。図１０に示される方法１０００は、ステップ１０１０から開始する。

【０１５５】

ステップ１０１０において、クエリを受信する。たとえば、１つ以上のクライアントデバイス２０５，２１０および２１５は、ユーザによって提供される情報からクエリを構築してもよく、クラウドベースのアプリケーション２４５は、１つ以上のクライアントデバイス２０５，２１０および２１５から当該クエリを受信してもよい。クエリは、保護フィールドおよび無保護フィールドに適用可能な検索基準、たとえば人物のファーストネーム

およびラストネームの検索を含み得て、ファーストネームは保護されていないデータであり、ラストネームは保護されたデータである。ステップ１０２０において、保護フィールドに関連する検索基準をＰＲＳサーバ２３５などのデータセキュリティプロバイダに送信する。一実施形態では、１つ以上のクライアントデバイス２０５，２１０および２１５は、クエリ全体をＰＲＳサーバ２３５に送信して、保護フィールド上で処理する。次いで、ＰＲＳサーバ２３５は、検索結果を元のクエリとともにクラウドベースのアプリケーション２３０に送信し得る。たとえば、ステップ１０３０において、保護フィールド検索の結果とともに、パブリックフィールドに関連する検索基準をクラウドベースのアプリケーションに送信する。いくつかの実施形態では、各々のプライベートデータベース２２５の検索基準とクラウドデータベース２３５の検索基準とは、独立して送信されてもよい。

【０１５６】

ステップ１０４０において、保護フィールド結果およびクラウド検索結果を用いていずれの検索最終結果もレンダリングする。一実施形態では、ユーザが検索を開始すると、検索基準のうちのいずれかが保護フィールドに対するものであれば、ＰＲＳサーバ２３５は、プライベートデータベース２４０に対して検索を適用し得る。ＰＲＳサーバは、行鍵によって識別される適格な行のセットとして結果セットを生成し得る。次いで、行鍵のセットは、クラウドベースのアプリケーション２４５に対する検索要求に送信される。クラウドベースのアプリケーション２４５が当該要求を処理する際に、適格な行鍵のセットを用いて最終検索結果をフィルタリングする。最終検索結果のみが、レンダリングされ、クライアントデバイス２１５に返されて、表示される。

【０１５７】

最終検索結果は、プライベートデータベース２４０に対する検索基準を満たしたクラウドデータとトークン化／暗号化されたデータとの組み合わせを含む。トークン化／暗号化されたデータは、１つ以上のクライアントデバイス２０５，２１０および２１５によって表示される前に、プライベートデータベース２４０からのデータと置換することができる。したがって、プライベートデータベース２４０およびクラウドデータベース２５０の両方のデータベースからの検索結果を連合して、よりシームレスな検索経験をユーザに提供することができる。

【０１５８】

ＶＩＩＩ．ハードウェア環境

以下の記載では、説明を目的として、本発明の実施形態が完全に理解されるように具体的な詳細が記載されている。しかし、これらの具体的な詳細がなくてもさまざまな実施形態は実施可能であるということが明らかであろう。図面および説明は、限定的であるように意図されるものではない。

【０１５９】

図面のうちのいくつかに示されているシステムは、さまざまな構成で提供されてもよい。いくつかの実施形態では、システムは、システムの１つ以上のコンポーネントがクラウドコンピューティングシステム内の１つ以上のネットワークにわたって分散される分散型システムとして構成されてもよい。

【０１６０】

図１１は、実施形態のうちの１つを実現するための分散型システム１１００の簡略図を示す。示されている実施形態では、分散型システム１１００は、１つ以上のクライアントコンピューティングデバイス１１０２，１１０４，１１０６および１１０８を含み、それらは、１つ以上のネットワーク１１１０を介してウェブブラウザ、所有権付きクライアント（たとえばオラクルフォームズ）などのクライアントアプリケーションを実行および動作させるように構成される。サーバ１１１２は、リモートクライアントコンピューティングデバイス１１０２，１１０４，１１０６および１１０８とネットワーク１１１０を介して通信可能に結合されてもよい。

【０１６１】

さまざまな実施形態では、サーバ１１１２は、システムのコンポーネントのうちの１つ

以上によって提供される１つ以上のサービスまたはソフトウェアアプリケーションを実行するように適合されてもよい。いくつかの実施形態では、これらのサービスは、ウェブベースのサービスもしくはクラウドサービスとして、またはソフトウェア・アズ・ア・サービス（ＳａａＳ）モデルの下で、クライアントコンピューティングデバイス１１０２，１１０４，１１０６および／または１１０８のユーザに対して提供されてもよい。クライアントコンピューティングデバイス１１０２，１１０４，１１０６および／または１１０８を動作させるユーザは、次いで、１つ以上のクライアントアプリケーションを利用してサーバ１１１２と対話して、これらのコンポーネントによって提供されるサービスを利用してもよい。

【０１６２】

図に示される構成では、システム１１００のソフトウェアコンポーネント１１１８，１１２０および１１２２は、サーバ１１１２上で実現されるものとして示されている。他の実施形態では、システム１１００のコンポーネントのうちの１つ以上および／またはこれらのコンポーネントによって提供されるサービスは、クライアントコンピューティングデバイス１１０２，１１０４，１１０６および／または１１０８のうちの１つ以上によって実現されてもよい。クライアントコンピューティングデバイスを動作させるユーザは、次いで、１つ以上のクライアントアプリケーションを利用して、これらのコンポーネントによって提供されるサービスを用いてもよい。これらのコンポーネントは、ハードウェア、ファームウェア、ソフトウェア、またはそれらの組み合わせで実現されてもよい。分散型システム１１００とは異なってもよいさまざまな異なるシステム構成が可能であることが理解されるべきである。図に示される実施形態は、したがって、実施形態のシステムを実現するための分散型システムの一例であり、限定的であるよう意図されるものではない。

【０１６３】

クライアントコンピューティングデバイス１１０２，１１０４，１１０６および／または１１０８は、携帯可能な手持ち式のデバイス（たとえば、ｉＰｈｏｎｅ（登録商標）、セルラー電話、ｉＰａｄ（登録商標）、コンピューティングタブレット、携帯情報端末（ＰＤＡ））またはウェアラブルデバイス（たとえば、Ｇｏｏｇｌｅ　Ｇｌａｓｓ（登録商標）頭部装着型ディスプレイ）であってもよく、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ　Ｍｏｂｉｌｅ（登録商標）などのソフトウェア、および／もしくは、ｉＯＳ、Ｗｉｎｄｏｗｓ　Ｐｈｏｎｅ、Ａｎｄｒｏｉｄ、ＢｌａｃｋＢｅｒｒｙ　１０、Ｐａｌｍ　ＯＳなどのさまざまなモバイルオペレーティングシステムを実行し、インターネット、電子メール、ショートメッセージサービス（ＳＭＳ）、ＢｌａｃｋＢｅｒｒｙ（登録商標）、または他のイネーブルにされた通信プロトコルである。クライアントコンピューティングデバイスは、汎用パーソナルコンピュータであってもよく、一例として、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）、Ａｐｐｌｅ　Ｍａｃｉｎｔｏｓｈ（登録商標）および／またはＬｉｎｕｘ（登録商標）オペレーティングシステムのさまざまなバージョンを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを含む。クライアントコンピューティングデバイスは、さまざまな市販のＵＮＩＸ（登録商標）またはＵＮＩＸのようなオペレーティングシステムのうちのいずれかを実行するワークステーションコンピュータであってもよく、当該ＵＮＩＸ（登録商標）またはＵＮＩＸのようなオペレーティングシステムとしては、たとえばＧｏｏｇｌｅ　Ｃｈｒｏｍｅ　ＯＳなどのさまざまなＧＮＵ／Ｌｉｎｕｘオペレーティングシステムが挙げられるが、これらに限定されるものではない。代替的に、または加えて、クライアントコンピューティングデバイス１１０２，１１０４，１１０６および１１０８は、ネットワーク１１１０を介して通信することができる、シンクライアントコンピュータ、インターネットにより可能化されるゲームシステム（たとえば、Ｋｉｎｅｃｔ（登録商標）ジェスチャ入力デバイスを有するまたは持たないＭｉｃｒｏｓｏｆｔ　Ｘｂｏｘゲームコンソール）および／または個人メッセージ伝達デバイスなどのその他の電子デバイスであってもよい。

【０１６４】

例示的な分散型システム１１００は４つのクライアントコンピューティングデバイスと

ともに示されているが、任意の数のクライアントコンピューティングデバイスがサポートされてもよい。センサを有するデバイスなど、他のデバイスがサーバ１１１２と対話してもよい。

【０１６５】

分散型システム１１００におけるネットワーク１１１０は、ＴＣＰ／ＩＰ（伝送制御プロトコル／インターネットプロトコル）、ＳＮＡ（システムネットワークアーキテクチャ）、ＩＰＸ（インターネットパケット交換）、ＡｐｐｌｅＴａｌｋなどを限定を伴うことなく含む、さまざまな市販のプロトコルのうちのいずれかを用いてデータ通信をサポートすることができる、当業者が精通している任意のタイプのネットワークであってもよい。単に一例として、ネットワーク１１１０は、イーサネット（登録商標）、トークンリングなどに基づくものなどのローカルエリアネットワーク（ＬＡＮ）であってもよい。ネットワーク１１１０は、ワイドエリアネットワークおよびインターネットであってもよい。ネットワーク１１１０は、仮想ネットワークを含み得て、当該仮想ネットワークとしては、仮想プライベートネットワーク（virtual private network：ＶＰＮ）、イントラネット、エクストラネット、公衆交換電話網（public switched telephone network：ＰＳＴＮ）、赤外線ネットワーク、無線ネットワーク（たとえば、米国電気電子学会（ＩＥＥＥ）８０２．１１のプロトコル一式、ブルートゥース（登録商標）、および／もしくはその他の無線プロトコルのうちのいずれかの下で動作するネットワーク）、ならびに／またはこれらのいずれかの組み合わせおよび／もしくは他のネットワークが挙げられるが、これらに限定されるものではない。

【０１６６】

サーバ１１１２は、１つ以上の汎用コンピュータ、専用サーバコンピュータ（一例として、ＰＣ（パーソナルコンピュータ）サーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウント型サーバなどを含む）、サーバファーム、サーバクラスタ、またはその他の適切な配置および／もしくは組み合わせで構成されてもよい。さまざまな実施形態では、サーバ１１１２は、前述の開示に記載される１つ以上のサービスまたはソフトウェアアプリケーションを実行するように適合されてもよい。たとえば、サーバ１１１２は、本開示の実施形態に従って上記の処理を実行するためのサーバに対応してもよい。

【０１６７】

サーバ１１１２は、上記のもののうちのいずれかを含むオペレーティングシステム、および任意の市販のサーバオペレーティングシステムを実行してもよい。サーバ１１１２は、ＨＴＴＰ（ハイパーテキスト転送プロトコル）サーバ、ＦＴＰ（ファイル転送プロトコル）サーバ、ＣＧＩ（コモンゲートウェイインターフェイス）サーバ、ＪＡＶＡ（登録商標）サーバ、データベースサーバなどを含むさまざまなさらに他のサーバアプリケーションおよび／または中間層アプリケーションのうちのいずれかも実行してもよい。例示的なデータベースサーバとしては、オラクル、マイクロソフト、サイベース、ＩＢＭ（インターナショナルビジネスマシンズ）などから市販されているものが挙げられるが、これらに限定されるものではない。

【０１６８】

いくつかの実現例では、サーバ１１１２は、クライアントコンピューティングデバイス１１０２，１１０４，１１０６および１１０８のユーザから受信されるデータフィードおよび／またはイベント更新情報を解析および整理統合するための１つ以上のアプリケーションを含んでもよい。一例として、データフィードおよび／またはイベント更新情報としては、センサデータアプリケーション、金融株式相場表示板、ネットワーク性能測定ツール（たとえば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム解析ツール、自動車交通監視などに関連するリアルタイムのイベントを含んでもよい、１つ以上の第三者情報源および連続データストリームから受信される、Ｔｗｉｔｔｅｒ（登録商標）フィード、Ｆａｃｅｂｏｏｋ（登録商標）更新情報またはリアルタイムの更新情報を挙げることができるが、これらに限定されるものではない。サーバ１１１

２は、データフィードおよび／またはリアルタイムのイベントをクライアントコンピューティングデバイス１１０２，１１０４，１１０６および１１０８の１つ以上の表示デバイスを介して表示するための１つ以上のアプリケーションも含んでもよい。

【０１６９】

分散型システム１１００は、１つ以上のデータベース１１１４および１１１６も含んでもよい。データベース１１１４および１１１６は、さまざまな位置にあってもよい。一例として、データベース１１１４および１１１６のうちの１つ以上は、サーバ１１１２に局在する（および／またはサーバ１１１２に常駐する）非一時的な記憶媒体にあってもよい。代替的に、データベース１１１４および１１１６は、サーバ１１１２から遠隔にあり、ネットワークベースまたは専用の接続を介してサーバ１１１２と通信してもよい。一組の実施形態では、データベース１１１４および１１１６は、記憶域ネットワーク（storage-area network：ＳＡＮ）にあってもよい。同様に、サーバ１１１２に帰する機能を実行するための任意の必要なファイルが、適宜、サーバ１１１２上においてローカルに、および／または遠隔で格納されてもよい。一組の実施形態では、データベース１１１４および１１１６は、ＳＱＬフォーマットされたコマンドに応答してデータを格納、更新および検索取得するように適合される、オラクルによって提供されるデータベースなどのリレーショナルデータベースを含んでもよい。

【０１７０】

図１２は、本発明のさまざまな実施形態を実現することができる例示的なコンピュータシステム１２００を示す。システム１２００は、上記のコンピュータシステムのうちのいずれかを実現するよう用いられてもよい。図に示されるように、コンピュータシステム１２００は、多数の周辺サブシステムとバスサブシステム１２０２を介して通信する処理ユニット１２０４を含む。これらの周辺サブシステムは、処理加速ユニット１２０６、Ｉ／Ｏサブシステム１２０８、ストレージサブシステム１２１８および通信サブシステム１２２４を含んでもよい。ストレージサブシステム１２１８は、有形のコンピュータ読取可能な記憶媒体１２２２およびシステムメモリ１２１０を含む。

【０１７１】

バスサブシステム１２０２は、コンピュータシステム１２００のさまざまなコンポーネントおよびサブシステムに想定通りに互いに通信させるための機構を提供する。バスサブシステム１２０２は単一のバスとして概略的に示されているが、バスサブシステムの代替的実施例は、複数のバスを利用してもよい。バスサブシステム１２０２は、さまざまなバスアーキテクチャのうちのいずれかを用いるメモリバスまたはメモリコントローラ、周辺バスおよびローカルバスを含むいくつかのタイプのバス構造のうちのいずれかであってもよい。たとえば、このようなアーキテクチャは、業界標準アーキテクチャ（Industry Standard Architecture：ＩＳＡ）バス、マイクロチャネルアーキテクチャ（Micro Channel Architecture：ＭＣＡ）バス、エンハンストＩＳＡ（Enhanced ISA：ＥＩＳＡ）バス、ビデオ・エレクトロニクス・スタンダーズ・アソシエーション（Video Electronics Standards Association：ＶＥＳＡ）ローカルバス、およびＩＥＥＥ　Ｐ１３８６．１規格に従って製造される中二階バスとして実現され得る周辺コンポーネントインターコネクト（Peripheral Component Interconnect：ＰＣＩ）バスを含んでもよい。

【０１７２】

１つ以上の集積回路（たとえば、従来のマイクロプロセッサまたはマイクロコントローラ）として実現可能な処理ユニット１２０４は、コンピュータシステム１２００の動作を制御する。１つ以上のプロセッサが処理ユニット１２０４に含まれてもよい。これらのプロセッサは、シングルコアプロセッサを含んでもよく、またはマルチコアプロセッサを含んでもよい。特定の実施形態では、処理ユニット１２０４は、シングルコアまたはマルチコアプロセッサが各処理ユニットに含まれる１つ以上の独立した処理ユニット１２３２および／または１２３４として実現されてもよい。他の実施形態では、処理ユニット１２０４は、２つのデュアルコアプロセッサを単一のチップに統合することによって形成されるクアッドコア処理ユニットとして実現されてもよい。

【０１７３】
さまざまな実施形態では、処理ユニット１２０４は、プログラムコードに応答してさまざまなプログラムを実行することができ、複数の同時に実行されるプログラムまたはプロセスを維持することができる。任意の所与の時点で、実行されるべきプログラムコードの一部または全ては、プロセッサ１２０４、および／または、ストレージサブシステム１２１８に常駐することができる。好適なプログラミングを介して、プロセッサ１２０４は、上記のさまざまな機能を提供することができる。コンピュータシステム１２００は、デジタル信号プロセッサ（digital signal processor：ＤＳＰ）、特殊目的プロセッサなどを含み得る処理加速ユニット１２０６をさらに含んでもよい。
【０１７４】
Ｉ／Ｏサブシステム１２０８は、ユーザインターフェイス入力デバイスおよびユーザインターフェイス出力デバイスを含んでもよい。ユーザインターフェイス入力デバイスは、キーボード、マウスまたはトラックボールなどのポインティングデバイス、ディスプレイに組み込まれたタッチパッドまたはタッチスクリーン、スクロールホイール、クリックホイール、ダイアル、ボタン、スイッチ、キーパッド、音声コマンド認識システムを有する音声入力デバイス、マイクロフォン、および他のタイプの入力デバイスを含んでもよい。ユーザインターフェイス入力デバイスは、たとえば、ジェスチャおよび話し言葉コマンドを用いて、ナチュラルユーザインターフェイスを介して、Ｍｉｃｒｏｓｏｆｔ Ｘｂｏｘ（登録商標）３６０ゲームコントローラなどの入力デバイスをユーザが制御して対話することを可能にするＭｉｃｒｏｓｏｆｔ Ｋｉｎｅｃｔ（登録商標）モーションセンサなどのモーション感知および／またはジェスチャ認識デバイスを含んでもよい。ユーザインターフェイス入力デバイスは、ユーザから目の動き（たとえば、写真を撮っている間および／またはメニュー選択を行なっている間の「まばたき」）を検出し、アイジェスチャを入力デバイス（たとえば、Ｇｏｏｇｌｅ Ｇｌａｓｓ（登録商標））への入力として変換するＧｏｏｇｌｅ Ｇｌａｓｓ（登録商標）瞬き検出器などのアイジェスチャ認識デバイスも含んでもよい。また、ユーザインターフェイス入力デバイスは、ユーザが音声コマンドを介して音声認識システム（たとえば、Ｓｉｒｉ（登録商標）ナビゲータ）と対話することを可能にする音声認識感知デバイスを含んでもよい。
【０１７５】
ユーザインターフェイス入力デバイスは、三次元（３Ｄ）マウス、ジョイスティックまたはポインティングスティック、ゲームパッドおよびグラフィックタブレット、ならびにスピーカ、デジタルカメラ、デジタルカムコーダ、ポータブルメディアプレーヤ、ウェブカム、画像スキャナ、指紋スキャナ、バーコードリーダ３Ｄスキャナ、３Ｄプリンタ、レーザレンジファインダ、および視線追跡デバイスなどの聴覚／視覚デバイスも含んでもよいが、それらに限定されるものではない。また、ユーザインターフェイス入力デバイスは、たとえば、コンピュータ断層撮影、磁気共鳴撮像、ポジションエミッショントモグラフィー、医療用超音波検査デバイスなどの医療用画像化入力デバイスを含んでもよい。ユーザインターフェイス入力デバイスは、たとえば、ＭＩＤＩキーボード、デジタル楽器などの音声入力デバイスも含んでもよい。
【０１７６】
ユーザインターフェイス出力デバイスは、ディスプレイサブシステム、インジケータライト、または音声出力デバイスなどの非ビジュアルディスプレイなどを含んでもよい。ディスプレイサブシステムは、陰極線管（cathode ray tube：ＣＲＴ）、液晶ディスプレイ（liquid crystal display：ＬＣＤ）またはプラズマディスプレイを使うものなどのフラットパネルデバイス、投影デバイス、タッチスクリーンなどであってもよい。一般に、「出力デバイス」という語の使用は、コンピュータシステム１２００からユーザまたは他のコンピュータに情報を出力するための全ての考えられ得るタイプのデバイスおよび機構を含むよう意図される。たとえば、ユーザインターフェイス出力デバイスは、モニタ、プリンタ、スピーカ、ヘッドフォン、自動車ナビゲーションシステム、プロッタ、音声出力デバイスおよびモデムなどの、テキスト、グラフィックスおよび音声／映像情報を視覚的に

伝えるさまざまな表示デバイスを含んでもよいが、それらに限定されるものではない。
【０１７７】
コンピュータシステム１２００は、現在のところシステムメモリ１２１０内に位置しているものとして示されているソフトウェア要素を備えるストレージサブシステム１２１８を備えてもよい。システムメモリ１２１０は、処理ユニット１２０４上でロード可能および実行可能なプログラム命令と、これらのプログラムの実行中に生成されるデータとを格納してもよい。
【０１７８】
コンピュータシステム１２００の構成およびタイプによって、システムメモリ１２１０は、揮発性であってもよく（ランダムアクセスメモリ（ＲＡＭ）など）、および／または、不揮発性であってもよい（リードオンリメモリ（ＲＯＭ）、フラッシュメモリなど）。ＲＡＭは、一般に、処理ユニット１２０４にすぐにアクセス可能であり、および／または、処理ユニット１２０４によって現在動作および実行されているデータおよび／またはプログラムモジュールを含む。いくつかの実現例では、システムメモリ１２１０は、スタティックランダムアクセスメモリ（ＳＲＡＭ）またはダイナミックランダムアクセスメモリ（ＤＲＡＭ）などの複数の異なるタイプのメモリを含んでもよい。いくつかの実現例では、起動中などにコンピュータシステム１２００内の要素間における情報の転送を助ける基本的なルーティンを含むベーシックインプット／アウトプットシステム（basic input/output system：ＢＩＯＳ）は、一般に、ＲＯＭに格納されてもよい。一例として、限定を伴うことなく、システムメモリ１２１０は、クライアントアプリケーション、ウェブブラウザ、中間層アプリケーション、リレーショナルデータベース管理システム（relational database management system：ＲＤＢＭＳ）などを含んでもよいアプリケーションプログラム１２１２、プログラムデータ１２１４およびオペレーティングシステム１２１６も示す。一例として、オペレーティングシステム１２１６は、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）、Ａｐｐｌｅ　Ｍａｃｉｎｔｏｓｈ（登録商標）および／もしくはＬｉｎｕｘオペレーティングシステム、さまざまな市販のＵＮＩＸ（登録商標）またはＵＮＩＸのようなオペレーティングシステム（さまざまなＧＮＵ／Ｌｉｎｕｘオペレーティングシステム、Ｇｏｏｇｌｅ　Ｃｈｒｏｍｅ（登録商標）ＯＳなどを含むがこれらに限定されない）、ならびに／または、ｉＯＳ、Ｗｉｎｄｏｗｓ（登録商標）　Ｐｈｏｎｅ、Ａｎｄｒｏｉｄ（登録商標）　ＯＳ、ＢｌａｃｋＢｅｒｒｙ（登録商標）　１２　ＯＳ、およびＰａｌｍ（登録商標）　ＯＳオペレーティングシステムなどのモバイルオペレーティングシステムのさまざまなバージョンを含んでもよい。
【０１７９】
ストレージサブシステム１２１８は、いくつかの実施形態の機能を提供する基本的なプログラミングおよびデータ構造を格納するための有形のコンピュータ読取可能な記憶媒体も提供してもよい。プロセッサによって実行されたときに上記の機能を提供するソフトウェア（プログラム、コードモジュール、命令）は、ストレージサブシステム１２１８に格納されてもよい。これらのソフトウェアモジュールまたは命令は、処理ユニット１２０４によって実行されてもよい。ストレージサブシステム１２１８は、本発明に従って使用されるデータを格納するためのリポジトリも提供してもよい。
【０１８０】
ストレージサブシステム１２１８は、コンピュータ読取可能な記憶媒体１２２２にさらに接続可能なコンピュータ読取可能記憶媒体リーダ１２２０も含んでもよい。システムメモリ１２１０とともに、およびオプションとしてシステムメモリ１２１０との組み合わせで、コンピュータ読取可能な記憶媒体１２２２は、コンピュータ読取可能な情報を一時的および／またはより永久的に収容、格納、伝送および検索取得するための、遠隔の、ローカルな、固定された、および／またはリムーバブルなストレージデバイスに記憶媒体を加えたものを包括的に表わしてもよい。
【０１８１】
コードまたはコードの一部を含むコンピュータ読取可能な記憶媒体１２２２は、記憶媒

体および通信媒体を含む、当該技術分野において公知であるまたは使用されるいずれかの適切な媒体も含んでもよく、当該媒体は、情報の格納および／または伝送のための任意の方法または技術において実現される揮発性および不揮発性の、リムーバブルおよび非リムーバブルな媒体などであるが、これらに限定されるものではない。これは、ＲＡＭ、ＲＯＭ、電気的に消去可能なプログラム可能ＲＯＭ（electronically erasable programmable ROM：ＥＥＰＲＯＭ）、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）、または他の光学式ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または他の有形のコンピュータ読取可能な媒体などの有形のコンピュータ読取可能な記憶媒体を含んでもよい。これは、データ信号、データ伝送、または所望の情報を伝送するために使用可能でありコンピューティングシステム１２００によってアクセス可能であるその他の媒体などの無形のコンピュータ読取可能な媒体も含んでもよい。

【０１８２】

一例として、コンピュータ読取可能な記憶媒体１２２２は、非リムーバブル不揮発性磁気媒体に対して読み書きするハードディスクドライブ、リムーバブル不揮発性磁気ディスクに対して読み書きする磁気ディスクドライブ、ＣＤ　ＲＯＭ、ＤＶＤおよびブルーレイ（登録商標）ディスクなどの、リムーバブル不揮発性光ディスクに対して読み書きする光ディスクドライブ、または他の光学式媒体を含んでもよい。コンピュータ読取可能な記憶媒体１２２２は、Ｚｉｐ（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス（universal serial bus：ＵＳＢ）フラッシュドライブ、セキュアデジタル（secure digital：ＳＤ）カード、ＤＶＤディスク、デジタルビデオテープなどを含んでもよいが、これらに限定されるものではない。コンピュータ読取可能な記憶媒体１２２２は、フラッシュメモリベースのＳＳＤ、エンタープライズフラッシュドライブ、ソリッドステートＲＯＭなどの不揮発性メモリに基づくソリッドステートドライブ（solid-state drive：ＳＳＤ）、ソリッドステートＲＡＭ、ダイナミックＲＡＭ、スタティックＲＡＭなどの揮発性メモリに基づくＳＳＤ、ＤＲＡＭベースのＳＳＤ、磁気抵抗ＲＡＭ（magnetoresistive RAM：ＭＲＡＭ）ＳＳＤ、およびＤＲＡＭとフラッシュメモリベースのＳＳＤとの組み合わせを使用するハイブリッドＳＳＤも含んでもよい。ディスクドライブおよびそれらの関連付けられたコンピュータ読取可能な媒体は、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および他のデータの不揮発性ストレージをコンピュータシステム１２００に提供してもよい。

【０１８３】

通信サブシステム１２２４は、他のコンピュータシステムおよびネットワークに対するインターフェイスを提供する。通信サブシステム１２２４は、他のシステムとコンピュータシステム１２００との間のデータの送受のためのインターフェイスとして働く。たとえば、通信サブシステム１２２４は、コンピュータシステム１２００がインターネットを介して１つ以上のデバイスに接続することを可能にしてもよい。いくつかの実施形態では、通信サブシステム１２２４は、（たとえば、セルラー電話技術、３Ｇ、４ＧもしくはＥＤＧＥ（グローバル進化のための高速データレート）などの先進データネットワーク技術、ＷｉＦｉ（ＩＥＥＥ８０２．１１ファミリー規格、もしくは他のモバイル通信技術、またはそれらのいずれかの組み合わせを用いて）無線音声および／またはデータネットワークにアクセスするための無線周波数（radio frequency：ＲＦ）送受信機コンポーネント、グローバルポジショニングシステム（global positioning system：ＧＰＳ）受信機コンポーネント、ならびに／または、他のコンポーネントを含んでもよい。いくつかの実施形態では、通信サブシステム１２２４は、無線インターフェイスに加えて、またはその代わりに、有線ネットワーク接続（たとえば、イーサネット）を提供することができる。

【０１８４】

また、いくつかの実施形態では、通信サブシステム１２２４は、コンピュータシステム１２００を使用し得る１人以上のユーザの代わりに、構造化されたおよび／または構造化されていないデータフィード１２２６、イベントストリーム１２２８、イベント更新情報

１２３０などの形式で入力通信を受信してもよい。
【０１８５】
一例として、通信サブシステム１２２４は、ソーシャルネットワーク、および／または、Ｔｗｉｔｔｅｒ（登録商標）フィード、Ｆａｃｅｂｏｏｋ（登録商標）更新情報、Ｒｉｃｈ Ｓｉｔｅ Ｓｕｍｍａｒｙ（ＲＳＳ）フィードなどのウェブフィード、および／もしくは１つ以上の第三者情報源からのリアルタイム更新情報などの他の通信サービスのユーザからリアルタイムでデータフィード１２２６を受信するように構成されてもよい。
【０１８６】
さらに、また、通信サブシステム１２２４は、連続データストリームの形式でデータを受信するように構成されてもよく、当該連続データストリームは、明確な終端を持たない、本来は連続的または無限であり得るリアルタイムイベントのイベントストリーム１２２８および／またはイベント更新情報１２３０を含んでもよい。連続データを生成するアプリケーションの例としては、たとえば、センサデータアプリケーション、金融株式相場表示板、ネットワーク性能測定ツール（たとえば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム解析ツール、自動車交通監視などを挙げることができる。
【０１８７】
また、通信サブシステム１２２４は、構造化されたおよび／または構造化されていないデータフィード１２２６、イベントストリーム１２２８、イベント更新情報１２３０などを、コンピュータシステム１２００に結合される１つ以上のストリーミングデータソースコンピュータと通信し得る１つ以上のデータベースに出力するよう構成されてもよい。
【０１８８】
コンピュータシステム１２００は、手持ち式の携帯デバイス（たとえば、ｉＰｈｏｎｅ（登録商標）携帯電話、ｉＰａｄ（登録商標）コンピューティングタブレット、ＰＤＡ）、ウェアラブルデバイス（たとえば、Ｇｏｏｇｌｅ Ｇｌａｓｓ（登録商標）頭部装着型ディスプレイ）、ＰＣ、ワークステーション、メインフレーム、キオスク、サーバラック、またはその他のデータ処理システムを含む、さまざまなタイプのもののうちの１つであり得る。
【０１８９】
常に変化するコンピュータおよびネットワークの性質のため、図に示されるコンピュータシステム１２００の記載は、単に具体的な例として意図される。図に示されるシステムよりも多くのコンポーネントまたは少ないコンポーネントを有する多くの他の構成が可能である。たとえば、カスタマイズされたハードウェアも使用されてもよく、および／または、特定の要素が、ハードウェア、ファームウェア、ソフトウェア（アプレットを含む）、または組み合わせで実現されてもよい。さらに、ネットワーク入力／出力デバイスなどの他のコンピューティングデバイスへの接続が利用されてもよい。本明細書における開示および教示に基づいて、当業者は、さまざまな実施形態を実現するための他の態様および／または方法を理解するであろう。
【０１９０】
上記の明細書では、本発明の局面についてその具体的な実施形態を参照して説明しているが、本発明はそれに限定されるものではないということを当業者は認識するであろう。上記の発明のさまざまな特徴および局面は、個々にまたは一緒に用いられてもよい。さらに、実施形態は、明細書のさらに広い精神および範囲から逸脱することなく、本明細書に記載されているものを超えて、さまざまな環境およびアプリケーションで利用することができる。したがって、明細書および図面は、限定的ではなく例示的であると見なされるべきである。

【図１】

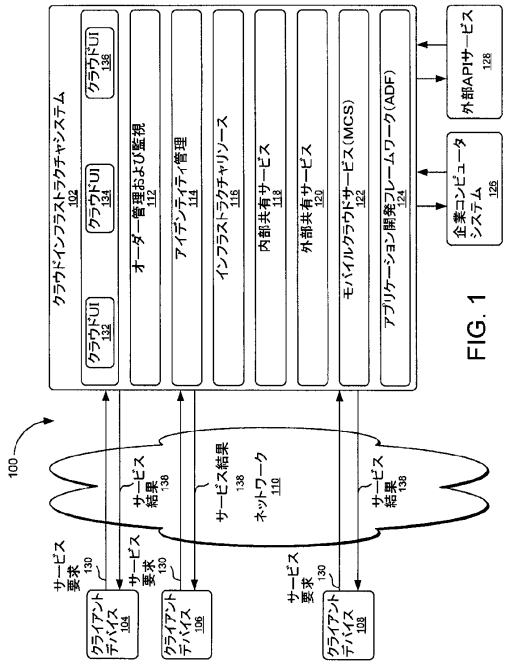


FIG. 1

【図２】

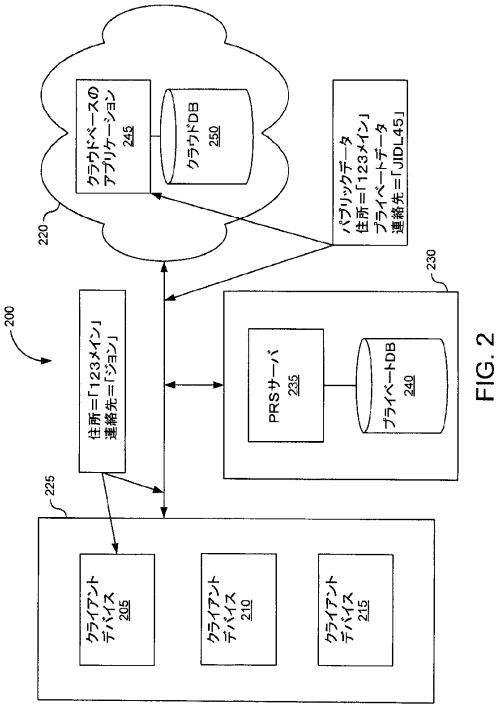


FIG. 2

【図３Ａ】

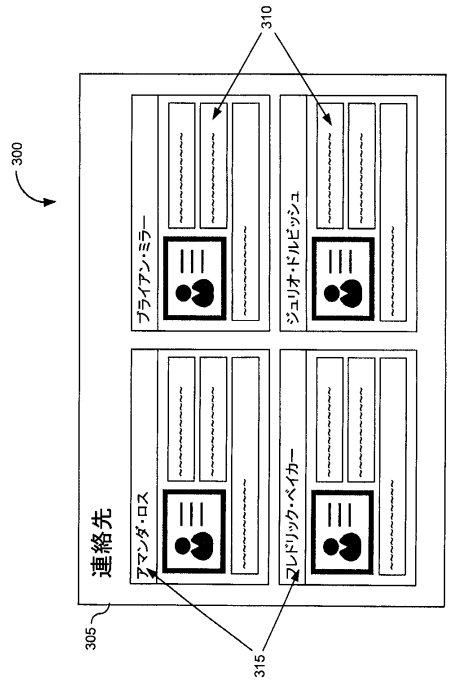


FIG. 3A

【図３Ｂ】

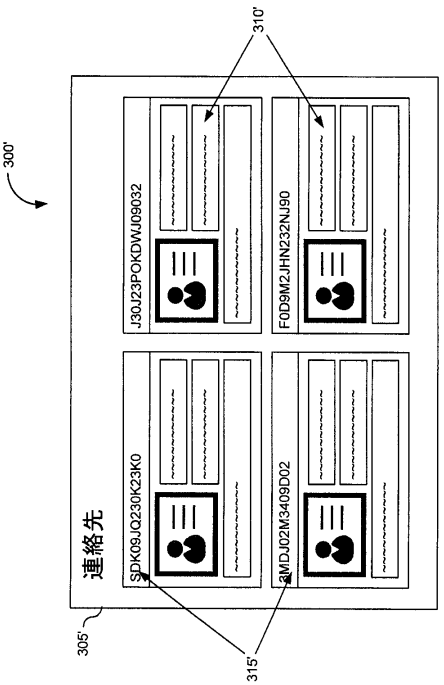


FIG. 3B

【図４】

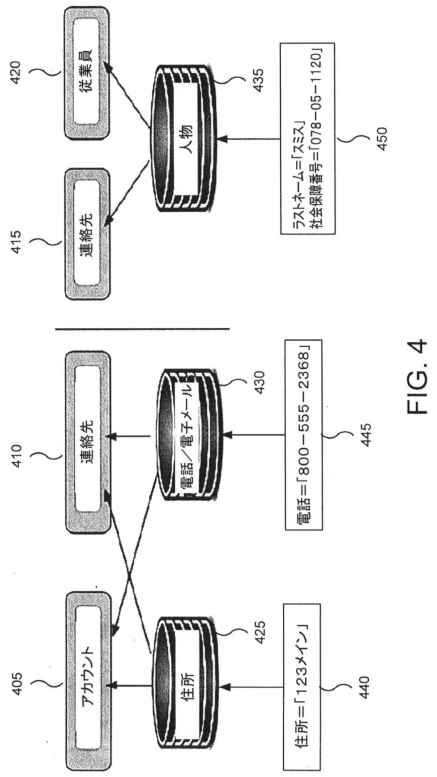


FIG. 4

【図５】

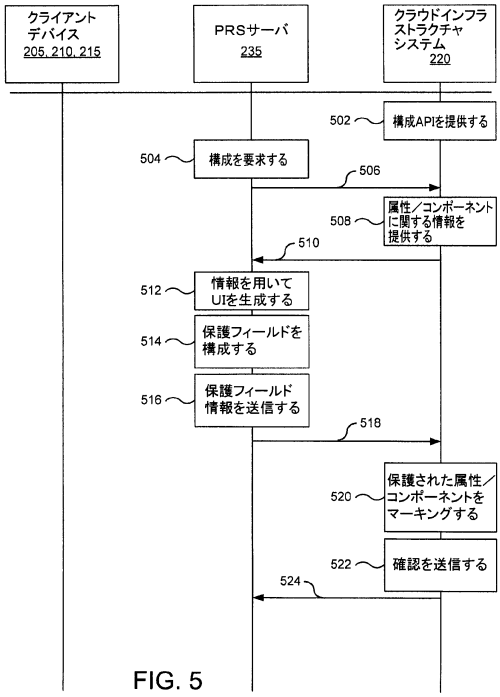


FIG. 5

【図６】

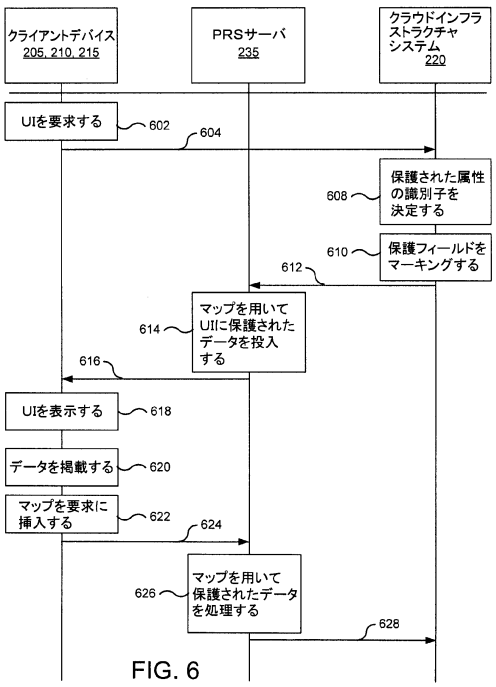
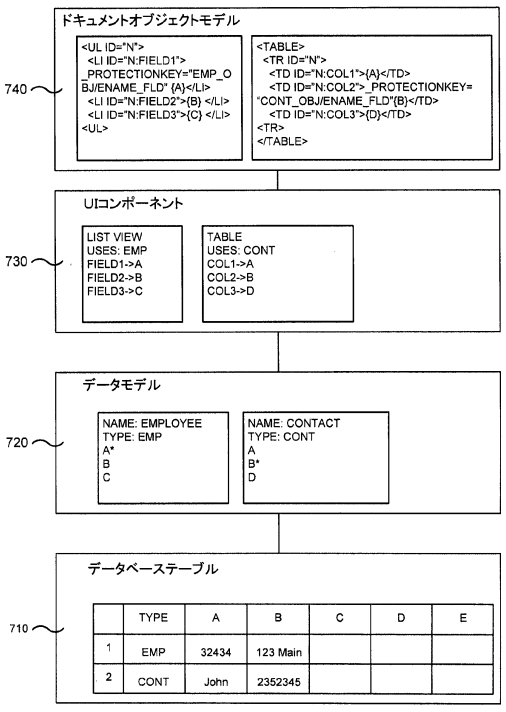


FIG. 6

【図７】



	TYPE	A	B	C	D	E
1	EMP	32434	123 Main			
2	CONT	John	2352345			

FIG. 7

【図８】

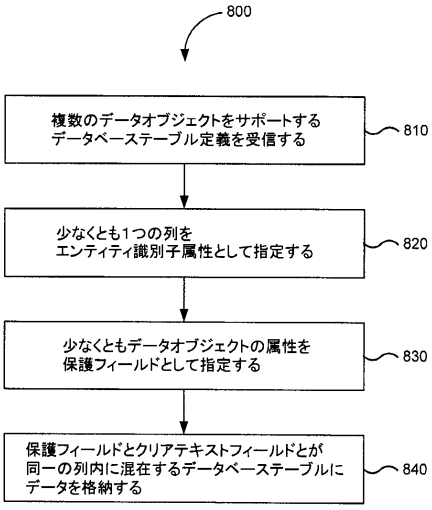


FIG. 8

【図９】

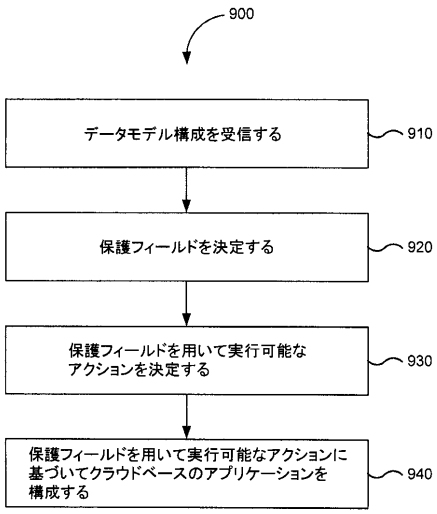


FIG. 9

【図１０】

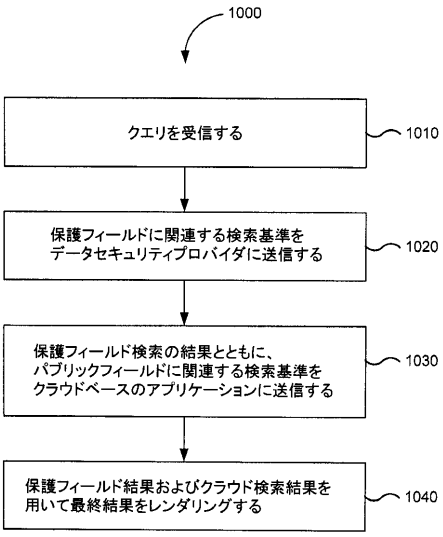


FIG. 10

【図１１】

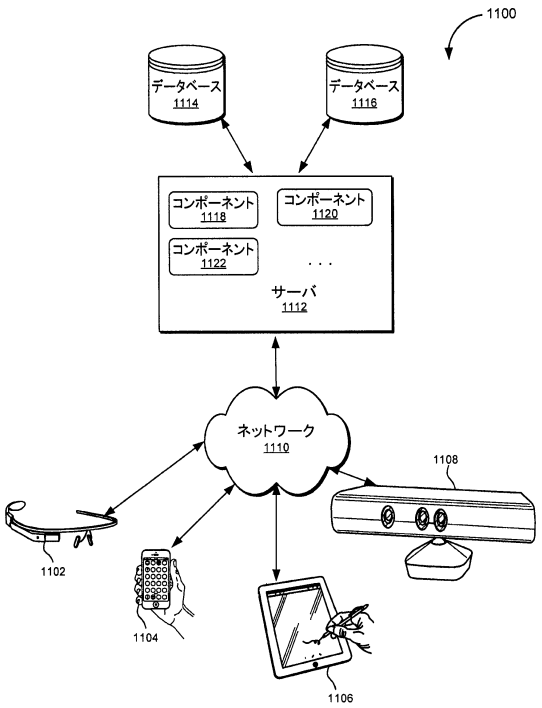


FIG. 11

【図１２】

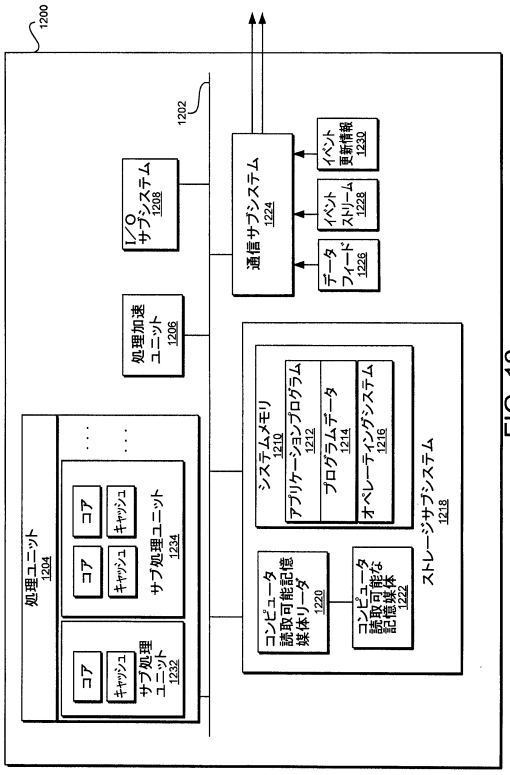

1200
1202
処理ユニット
1204
コア
キャッシュ
サブ処理ユニット
1232
サブ処理ユニット
1234
処理加速ユニット
1206
I/Oサブシステム
1208
通信サブシステム
1224
データフィード
1226
イベントストリーム
1228
イベント更新情報
1230
システムメモリ
1210
アプリケーションプログラム
1212
プログラムデータ
1214
オペレーティングシステム
1216
コンピュータ読取可能記憶媒体リーダ
1220
コンピュータ読取可能な記憶媒体
1222
ストレージサブシステム
1218

FIG. 12

フロントページの続き

(72)発明者　スリバン，ブレイク
アメリカ合衆国、９４０６２　カリフォルニア州、レッドウッド・シティ、ウィップル・アベニュ、１７２９
(72)発明者　マグラス，マイケル・ウィリアム
アメリカ合衆国、９４５８２　カリフォルニア州、サン・ラモン、アセンズ・ドライブ、５０６５
(72)発明者　ルー，ミン
アメリカ合衆国、９４５３９　カリフォルニア州、フリーモント、メント・ドライブ、２０４５

審査官　岸野　徹

(56)参考文献　特開２０１４－２３８６４２（ＪＰ，Ａ）
特開２０１４－１９４６６２（ＪＰ，Ａ）
特開２０１３－１２５０３９（ＪＰ，Ａ）
特開２０１１－１４５８０２（ＪＰ，Ａ）
米国特許出願公開第２０１１／０１７０６７４（ＵＳ，Ａ１）
特表２０１５－５２７６３７（ＪＰ，Ａ）
国際公開第２０１５／１１９６５８（ＷＯ，Ａ１）
中国特許出願公開第１０４２３９８１１（ＣＮ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　１６／１８２