

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6633913号
(P6633913)

(45) 発行日 令和2年1月22日 (2020.1.22)

(24) 登録日 令和1年12月20日 (2019.12.20)

(51) Int. Cl.

F I

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62 3 1 8

請求項の数 5 (全 24 頁)

(21) 出願番号	特願2015-525498 (P2015-525498)	(73) 特許権者	314015767
(86) (22) 出願日	平成25年7月30日 (2013.7.30)		マイクロソフト テクノロジー ライセン
(65) 公表番号	特表2015-524592 (P2015-524592A)		シング, エルエルシー
(43) 公表日	平成27年8月24日 (2015.8.24)		アメリカ合衆国 ワシントン州 9805
(86) 国際出願番号	PCT/US2013/052601		2 レッドモンド ワン マイクロソフト
(87) 国際公開番号	W02014/022323		ウェイ
(87) 国際公開日	平成26年2月6日 (2014.2.6)	(74) 代理人	100079108
審査請求日	平成28年6月23日 (2016.6.23)		弁理士 稲葉 良幸
審判番号	不服2018-6987 (P2018-6987/J1)	(74) 代理人	100109346
審判請求日	平成30年5月22日 (2018.5.22)		弁理士 大貫 敏史
(31) 優先権主張番号	13/561, 113	(74) 代理人	100117189
(32) 優先日	平成24年7月30日 (2012.7.30)		弁理士 江口 昭彦
(33) 優先権主張国・地域又は機関	米国 (US)	(74) 代理人	100134120
			弁理士 内藤 和彦

最終頁に続く

(54) 【発明の名称】 企業データシステム内のテナントのためのセキュリティおよびデータの隔離

(57) 【特許請求の範囲】

【請求項 1】

各テナントが複数のユーザを有する組織であるマルチテナントデータストアにおけるデータ操作要求を処理するコンピュータ実装方法であって、

所与のテナント以外の少なくとも1つの他のテナントを有する企業データアプリケーションにおいて前記所与のテナントを生成するためのユーザ入力を受け取るユーザ入力機構を有するテナント生成管理者表示を表示することと、

前記所与のテナントにおいてクライアントを前記所与のテナントに関連するユーザのためのセキュリティ規則を識別するセキュリティ管理者として識別するユーザ入力を受け取るユーザ入力機構を有するセキュリティ管理者指定表示を表示することと、

前記セキュリティ管理者から前記セキュリティ規則を受け取ることと、

要求元のクライアントを前記所与のテナントのものであると識別するテナント識別データを含む前記要求元のクライアントからのデータ操作要求を前記企業データアプリケーションで受信することと、

前記所与のテナントに関連する第1のデータと、前記少なくとも1つの他のテナントに関連する第2のデータを記憶する前記マルチテナントデータストアからコンピュータプロセッサを用いて前記データ操作要求を処理することであって、

前記少なくとも1つの他のテナントによる前記第1のデータに対するアクセスを制限するために、前記所与のテナントのための前記第1のデータが、関連性に基づいて、前記マルチテナントデータストア内で他のテナントのための前記第2のデータと区分けされ、前記

10

20

データ操作要求が、前記テナント識別データに基づいて前記データ操作要求を前記所与のテナントに関連して記憶されたデータに制限することによって処理される、処理することを含み、

前記データ操作要求を受信することが、データを前記マルチテナントデータストアに記憶する要求を受信することを含み、

前記データ操作要求を処理することが、

前記要求の前記データを前記マルチテナントデータストアに記憶することと、

前記データが前記所与のテナントに属することを示す区分識別子で、前記マルチテナントデータストアに記憶される前記データをマークすることとを含み、

前記セキュリティ管理者から前記セキュリティ規則を受け取ることが、

前記ユーザ入力機構を有するセキュリティ規則表示を表示することと、

前記セキュリティ規則表示の前記ユーザ入力機構を通じて前記所与のテナントのために実施されるべきセキュリティ規則を受け取ることとを含み、

前記データ操作要求を処理することが、

前記データ操作要求の前記テナント識別データに基づいて前記所与のテナントのための前記セキュリティ規則にアクセスすることと、

前記データ操作要求を処理する間に、前記所与のテナントのための前記セキュリティ規則を実施することを含む方法。

【請求項 2】

前記データ操作要求が、アクセスされるべき前記マルチテナントデータストアのデータを識別し、識別されるデータが、前記他のテナントのうちの 1 つまたは複数からのデータを含むように定義される請求項 1 に記載のコンピュータ実装方法。

【請求項 3】

前記データ操作要求を処理することが、

前記所与のテナントに属するデータのみを定義する修正されたデータ操作要求を得るよう前記データ操作要求を修正することと、

前記修正されたデータ操作要求を処理することを含む請求項 2 に記載のコンピュータ実装方法。

【請求項 4】

前記データ操作要求を受信することが、

前記他のテナントのうちの 1 つまたは複数からのデータを包含するデータの問い合わせを受信することを含み、前記データ操作要求を修正することが、

前記区分識別子によって前記所与のテナントに属すると識別されたデータのみを返すよう前記問い合わせを修正することを含む請求項 3 に記載のコンピュータ実装方法。

【請求項 5】

前記データ操作要求を処理することが、

キャッシュメモリ内で各テナントについてキャッシュされたデータの別個のコピーを維持することを含み、前記データ操作要求が、データを要求する問い合わせを含み、前記キャッシュされたデータの別個のコピーを維持することが、

要求されたデータを、前記所与のテナントのためのキャッシュされたデータのみを記憶するキャッシュメモリに記憶することを含む請求項 1 に記載のコンピュータ実装方法。

【発明の詳細な説明】

【技術分野】

【0001】

企業データシステム内のテナントのためのセキュリティおよびデータの隔離に関する。

【背景技術】

【0002】

[0001] 企業組織は、多くの異なる種類の企業コンピュータプログラムまたはアプリケーションを使用することが多い。一部のそのようなプログラムは、企業資源計画（ERP）シ

10

20

30

40

50

システム、顧客資源管理（CRM: customer resource management）システム、基幹業務（LOB: line of business）アプリケーション、および多くの他の企業に関連するプログラムを含む。

【0002】 さらに、多くの組織は、それらの組織の企業プログラムにおいて役割（role）に基づくセキュリティを実施する。すなわち、ユーザは、会社において特定の役割を果たす可能性があり、その役割を負うユーザは、特定のデータにアクセスすることができるが、他のデータにはアクセスすることができない可能性がある。例えば、人材管理の役割を負っているユーザは、さまざまな従業員の給与および個人ファイルにアクセスすることができる可能性があるが、販売データまたは他の種類の通常の企業情報にはアクセスすることができない可能性がある。対照的に、営業部長の役割を負っているユーザは、さまざまな製品ラインにわたって会社の複数のレベルの販売データにアクセスすることができる可能性があるが、他の従業員のための個人ファイルおよび給与情報にはアクセスすることができない可能性がある。

10

【0003】

【0003】 加えて、多くの会社は、それらの会社の企業に関連するデータの多くが極秘または企業独自のもの（proprietary）であるとみなす。例えば、多くの会社は、販売記録、セールスリード、個人ファイル情報、および他の企業情報のホスト（host）全体が極秘であり、その会社の企業独自のものであるとみなす。会社は、競合他社などの他の会社または関連会社さえもそのデータにアクセスすることができることを望まない。

【0004】

20

【0004】 この状況では、会社が特定の方法で互いに関連するようになることができるが、それらの会社が互いに情報を共有することをやはり望まない場合が生じる可能性がある。例えば、会社が、独立した企業（または子会社）を買収することによって大きくなる持ち株会社である可能性がある。子会社は、それらの子会社自体の管理および運営の大部分を握っており、それぞれの子会社のためのデータおよびプロセスは、他の子会社との間で共有されるべきでない。

【0005】

【0005】 一部の現在の解決策は、子会社のそれぞれがその子会社自体の企業データを記憶するためのその子会社自体の別個のデータベースを持つことを必要とする。他の現在の解決策においては、それぞれの別個の子会社に、その子会社自体の別個のデータベース製品が与えられる。子会社のそれぞれのために与えられた企業データプログラムのまったく別々の設備が、存在する。例えば、それぞれの子会社は、ERPシステムをその子会社自体で別々に設置される可能性がある。

30

【発明の概要】

【発明が解決しようとする課題】

【0006】

【0006】 しかし、子会社が、それらの子会社の情報技術（IT）リソースをプールし、単一の企業ソフトウェアアプリケーションを利用することを望むこともあり得る。すなわち、子会社（または子会社のサブセット）は、単一の企業アプリケーションのインストールのコストを分担したいと望む可能性があるが、それでもなお、自身の企業データを、同じ企業アプリケーションを共有している他の子会社から完全に分け、隔離したままにしておきたいと望む。同様に、子会社のそれぞれは、その子会社自体の役割に基づくセキュリティ規則または他のセキュリティ規則を実施したいと望む可能性がある。

40

【0007】

【0007】 以上の考察は、全般的な背景情報に関して与えられたものに過ぎず、特許請求の範囲の決定を幫助するものとして使用されることを意図したものではない。

【課題を解決するための手段】

【0008】

【0008】 マルチテナントホスティングシステムが、テナントから企業データおよびテナント識別データを受信する。複数の異なるテナントからのデータが、単一のデータベースに

50

記憶されるが、各テナントに対応するデータは、データベース内で、区分識別子でデータをマークすることによって区分けされる。したがって、ホスティングシステムは、個々のテナントがそれら自体のデータにアクセスできることのみ可能にする。

【 0 0 0 9 】

[0009] この「課題を解決するための手段」は、「発明を実施するための形態」において以下でさらに説明される概念の選択を簡略化された形態で導入するために与えられる。この「課題を解決するための手段」は、特許請求の対象の重要な特徴または必須の特徴を識別するように意図されておらず、特許請求の範囲の決定を幫助するものとして使用されることを意図したものでもない。特許請求の対象は、「背景技術」で述べられたいずれかのまたはすべての欠点を解決する実装に限定されない。

10

【図面の簡単な説明】

【 0 0 1 0 】

【図 1】[0010]企業データシステムの一実施形態のブロック図である。

【図 2】[0011]テナントを設定する際の図 1 に示されたシステムの全体的な動作の一実施形態を示す流れ図である。

【図 2 A】[0012]例示的なユーザインターフェース表示を示す図である。

【図 2 B】例示的なユーザインターフェース表示を示す図である。

【図 2 C】例示的なユーザインターフェース表示を示す図である。

【図 2 D】例示的なユーザインターフェース表示を示す図である。

【図 2 E】例示的なユーザインターフェース表示を示す図である。

20

【図 3】[0013]区分けされたデータのためのデータ構造の一実施形態を示す図である。

【図 3 A】[0014]区分けされたデータをテーブルで示す例示的なユーザインターフェース表示を示す図である。

【図 3 B】区分けされたデータをテーブルで示す例示的なユーザインターフェース表示を示す図である。

【図 3 C】区分けされたデータをテーブルで示す例示的なユーザインターフェース表示を示す図である。

【図 4】[0015]企業データへのマルチテナントアクセスをホストする際の図 1 に示されたシステムの全体的な動作の一実施形態を示す流れ図である。

【図 5】[0016]データアクセスおよびキャッシュ動作を行う際の図 1 に示されたシステムの動作の一実施形態を示す流れ図である。

30

【図 5 A】[0017]テナントのサブセットがデータを共有するようにデータストアが区分けされるアーキテクチャを示す図である。

【図 6】[0018]さまざまなアーキテクチャにおける図 1 のシステムの一実施形態を示すブロック図である。

【図 7】[0019]モバイルデバイスのさまざまな実施形態を示す図である。

【図 8】モバイルデバイスのさまざまな実施形態を示す図である。

【図 9】モバイルデバイスのさまざまな実施形態を示す図である。

【図 1 0】モバイルデバイスのさまざまな実施形態を示す図である。

【図 1 1】[0020]1つの例示的なコンピューティング環境のブロック図である。

40

【発明を実施するための形態】

【 0 0 1 1 】

[0021] 図 1 は、企業データシステム 1 0 0 の一実施形態のブロック図を示す。企業データシステム 1 0 0 は、テナント 1 0 2 および 1 0 4 を示し、テナント 1 0 2 および 1 0 4 のそれぞれは、複数のクライアント（またはユーザ）1 0 6、1 0 8 および 1 1 0、1 1 2 をそれぞれ有する。テナント 1 0 2 および 1 0 4 は、サーバレイヤ 1 1 4 にアクセスすることができ、サーバレイヤ 1 1 4 自体は、複数のサーバ 1 1 6、1 1 8、および 1 2 0 を有する。図 1 に示されるように、テナント 1 0 2 および 1 0 4 は、ネットワーク 1 2 2 を通じてか、または矢印 1 2 4 および 1 2 6 にそれぞれ示されるように直接かのどちらかでサーバレイヤ 1 1 4 にアクセスすることができる。サーバレイヤ 1 1 4 は、データスト

50

ア 1 2 8 に記憶されたデータにアクセスする（テナント 1 0 2 および 1 0 4 からの）要求を処理する。さらに、サーバレイヤ 1 1 4 は、キャッシュ 1 3 0 を用いてキャッシュを実装する。

【 0 0 1 2 】

[0022] 一実施形態において、システム 1 0 0 は、企業データシステム 1 0 0 で新しいテナントを設定するために管理者によって使用され得る管理者構成要素 1 3 2 も含む。新しいテナントのそれぞれは、（同じ E R P もしくは C R M のインストールまたは他の企業アプリケーションのインストールなどの）同じシステムを使用する。加えて、一実施形態においては、サーバレイヤ 1 1 4 が、テナント 1 0 2 および 1 0 4 のそれぞれのためのセキュリティ規則にアクセスすることができる。セキュリティ規則は、ブロック 1 3 4 によって示される。したがって、サーバレイヤ 1 1 4 は、それぞれのテナント 1 0 2 および 1 0 4 についてセキュリティを実施することができる。一実施形態において、セキュリティ規則は、クライアントがテナント 1 0 2 または 1 0 4 にログインするときの認証手順を定義し、さらに、テナント毎の役割に基づくセキュリティを定義する。言うまでもなく、他の種類のセキュリティ規則またはセキュリティ手順も、実施され得る。

10

【 0 0 1 3 】

[0023] 図 1 は、少なくともそれぞれのテナント 1 0 2 および 1 0 4 がプロセッサ 1 3 6 および 1 3 8 を有することを示す。当然ながら、各クライアントがそのクライアント自体のプロセッサをやはり有する可能性があり、簡単にするために各テナントについて 1 つのプロセッサが示されていることに留意されたい。図 1 は、各サーバ 1 1 6、1 1 8、および 1 2 0 がそのサーバ自体のプロセッサ 1 4 0、1 4 2、および 1 4 4 を有する可能性があることも示す。サーバレイヤ 1 1 4 がサーバのそれぞれによってアクセスされる単一のプロセッサを有する可能性があるが、各サーバのための個々のプロセッサが例示のために示されることに留意されたい。一実施形態において、プロセッサのそれぞれは、メモリおよびタイミング回路（図示せず）に関連するコンピュータプロセッサを含む。プロセッサは、システム 1 0 0 の機能部分を形成し、システム 1 0 0 の他の構成要素によって作動され、システム 1 0 0 の他の構成要素の機能を助ける。

20

【 0 0 1 4 】

[0024] データストア 1 2 8 は、単一のデータストアとして示されているが、複数の異なるデータストアとして実装することもでき、それらのデータストアはサーバレイヤ 1 1 4 に対してローカルに位置するか、またはサーバレイヤ 1 1 4 の遠隔に位置することができることも、留意されたい。データストア 1 2 8 は、例示的に、システム 1 0 0 のすべてのテナントによって使用される単一のデータベースインストールのためのストレージである。同様に、キャッシュ 1 3 0 は、単一のメモリ内キャッシュとして示されているが、複数の異なるメモリ内に実装されるなど、他の方法で実装される可能性もある。

30

【 0 0 1 5 】

[0025] さらに、図 1 は、一実施形態において、各クライアント 1 0 6 ~ 1 1 2 がそのクライアント自体の構成データ 1 4 6、1 4 8、1 5 0、および 1 5 2 をそれぞれ有することを示す。構成データは、例示的に、各クライアントの役割と、さらに、各クライアントが属する特定のテナントとを識別する。テナントはそのテナントの複数のクライアントのための構成データの共通の組を有する可能性もあるが、単に例として、各クライアントについて別々の構成データ（または構成ファイル）が示されていることに留意されたい。

40

【 0 0 1 6 】

[0026] システム 1 0 0 の動作の詳細な説明が残りの図に関連して以下で与えられるが、残りの説明の理解を深めるために、ここで、概要が与えられる。システム 1 0 0 は、テナント 1 0 2 および 1 0 4 が、単一の E R P アプリケーション（または他の企業に関連するアプリケーション）を使用し、共通データベース 1 2 8 にそれらのテナントのデータのすべてを記憶することによって情報技術リソースをプールしたいが、それでもなお、それらのテナント自体の個人データが他のテナントによって閲覧またはアクセスされ得ないようにそれらの個人データの区分けを維持し続けたいと望むシナリオを例示的に示す。例えば

50

、一例において、テナント１０２および１０４は、両方とも、（親持ち株会社の子会社などの）所有者が同じ企業である。その場合、各テナント１０２および１０４は、例示的に、そのテナント自体の管理および運営を握っており、そのテナントのデータを他のテナントから安全に区分けしておきたいと望む。その場合、クライアント１０６～１０８は、テナント１０２によって使用される（例えば、ＥＲＰアプリケーションなどの）企業に関連するアプリケーションのユーザに対応し、クライアント１１０および１１２は、テナント１０４によって使用される同じアプリケーションのユーザに対応する。テナント１０２および１０４は、両方とも、企業に関連するアプリケーションの同じインストールを使用する。

【００１７】

[0027] 新しい組織が持ち株会社に追加されるとき（すなわち、新しいテナントがシステム１００に追加されるとき）、管理者１３３は、例示的に、管理者構成要素１３２を通じてサーバレイヤ１１４にアクセスする。構成要素１３２は、例示的に、管理者１３３に提供されるユーザインターフェース表示１３５を生成するユーザインターフェース構成要素を有する。ユーザインターフェース表示１３５は、例示的に、サーバレイヤ１１４によって実装され、システムのさまざまなテナントのさまざまなクライアントによって使用される企業に関連するアプリケーションを操作するためのユーザ入力を管理者１３３が与えることを可能にするユーザ入力機構を含む。ユーザ入力機構は、（マウスまたはトラックボールなどの）ポイントアンドクリックデバイス、キーボード（仮想またはハードウェア）、ディスプレイスクリーンがタッチ感知式スクリーンである場合のタッチジェスチャ、音声入力などからのユーザ入力を受け取ることができる。図２Ａは、管理者が新しいテナントを設定することを可能にするユーザインターフェース表示１７９の一実施形態を示す。管理者は、ユーザ入力機構１８１および１８３を使用して新しいテナントを識別し、設定（または生成）する。

【００１８】

[0028] 新しいテナントを設定するために、管理者１３３は、例示的に、新しいテナントのクライアントのうちの１つをセキュリティ管理者として識別する。例えば、テナント１０２が追加されるべき新しいテナントであると仮定する。管理者１３３は、クライアント１０６を、テナント１０２のセキュリティ管理者であるものとして識別する可能性がある。

【００１９】

[0029] 図２Ｂは、ユーザインターフェース表示１２５の別の実施形態を示す。表示１２５は、新しいテナントを生成するために管理者に対して表示され得る。表示１２５は、区分キー列１２７および名前列１２９を含む１組の列を含む。ユーザは、区分キー列１２７のセルを選択し、区分キーを入力し、列１２９の隣接するセルに対応する区分名を入力することができる。このようにして、管理者は、さまざまなクライアントのためのデータを区分けするためにデータストア１２８およびキャッシュ１３０で使用され得るテナント（すなわち、区分）を設定することができる。区分キー列１２７が３つの区分キー、「初期」、「Ｐ１」、および「Ｐ２」を含むことが、図２Ｂで見られ得る。対応する名前は、それぞれ、「初期パーティション」、「Ｐ１」、および「Ｐ２」である。

【００２０】

[0030] 図２Ｃは、管理者１３３が新しいテナントのクライアントをセキュリティ管理者として指定することを可能にするユーザインターフェース表示１８５の一実施形態である。管理者は、ユーザ入力機構１８７を用いてこれを行うことができる。

【００２１】

[0031] これは、クライアント１０６がログインし、テナント１０２を用いてデータストア１２８の情報にアクセスする（クライアント１０８などの）他のユーザを設定することができるようにクライアント１０６にセキュリティ構成要素を配信する。セキュリティ管理者（ここではクライアント１０６）は、セキュリティ規則と、テナント１０２の各ユーザの役割とを識別することもできる。図２Ｄは、セキュリティ管理者（例えば、ここでは

10

20

30

40

50

クライアント 106) がこれを行うことを可能にするユーザインターフェース表示 189 の一実施形態を示す。テナントのユーザまたはクライアントは、ユーザ入力機構 191 を用いて設定される可能性があり、セキュリティ規則は、入力機構 193 を用いて設定される可能性がある。セキュリティ規則の役割およびユーザが、図 1 の 134 で示された各テナントのためのセキュリティ規則として記憶される。クライアント 108 に対応する役割情報と、クライアント 108 がテナント 102 に属するという事実とが、そのクライアント 108 に対応する構成ファイル (または構成データ) 148 に記憶される。構成ファイルは、クライアントに自動的に配信されるか、またはセキュリティ管理者が図 2 D の機構 195 などのユーザ入力機構を作動させるときに送信される可能性がある。

【0022】

[0032] 図 2 E は、管理者が所与のテナントでユーザを設定するために使用することができるユーザインターフェース表示 131 の別の実施形態を示す。管理者が 1 組のテキストボックスおよびチェックボックスにユーザについてのさまざまな情報を入力することを可能にするユーザタブ 133 を管理者が選択したことが、見られ得る。例えば、管理者は、テキストボックス 135 にユーザ ID を入力し、ボックス 137 にユーザ名を入力し、ボックス 139 にネットワークドメインを入力し、ボックス 141 に別名 (alias) を入力することができる。ユーザは、例示的に、ドロップダウンメニュー 143 を用いてアカウントの種類を定義し、別のドロップダウンメニュー 145 を用いてデフォルトの会社を選択することもできる。そのとき、管理者は、チェックボックス 147 にチェックをすることによってこのユーザを有効にすることができ、ユーザは、ボックス 149 にチェックをすることによってこのユーザをデフォルトの区分に割り振ることができる。

【0023】

[0033] 管理者は、例示的に、ボックス 151 に情報を入力することによってこのユーザのためのプロフィールを確立することができる。管理者は、ボタン 153 を作動させることによってこのユーザに 1 つまたは複数の役割を割り振ることもできる。これは、例示的に、管理者によってこのユーザに対して選択され得るかまたは他の方法で割り振られ得る 1 組の役割 155 を提示する。同様に、ドロップダウンボックス 157 を作動させることによって、管理者は、選択された役割の権限を見直すことができ、ドロップダウンボックス 159 を作動させることによって、管理者は、選択された役割に割り振られた他のユーザを見直すことができる。当然ながら、図 2 E に示されたユーザインターフェース表示 131 は、例示的であるに過ぎず、ユーザを識別し、役割を割り振る他の方法も、使用され得る。

【0024】

[0034] クライアント 108 は、データストア 128 の情報にアクセスするか、データストア 128 に情報を記憶したいと望むとき、まず、テナント 102 にログインする。構成データ 148 は、サーバレイヤ 114 に、クライアント 108 の役割と、クライアント 108 がどのテナントに属するかを示す。したがって、例えば、クライアント 108 がデータストア 128 に記憶されるべき情報を提供するとき、サーバレイヤ 114 は、そのデータをテナントデータ 154 としてデータストア 128 に記憶する。さらに、サーバレイヤ 114 は、例示的に、テナントデータ 154 をテナント 102 から来たものとして識別する。したがって、サーバレイヤ 114 は、テナントデータ 154、156、および 158 のすべてを所与のテナントに固有であるものとして識別する。クライアントがその後ログインし、データストア 128 のデータにアクセスすることを求めるとき、サーバレイヤ 114 は、その特定のクライアントのアクセスを、クライアントがログインで使ったテナント 102 または 104 に対応するデータ 154、156、または 158 だけに制限する。例えば、クライアント 110 が後でクライアント 104 を通じてログインする場合、サーバレイヤ 114 は、構成データ 150 によって、クライアント 110 が所与の役割を有し、テナント 104 を通じてログインしたことを識別する。したがって、サーバレイヤ 114 は、テナント 104 におけるクライアント 110 の役割を考慮して、クライアント 110 のアクセスを、テナント 104 に対応するデータだけに制限する。

【 0 0 2 5 】

[0035] 言うまでもなく、システム 1 0 0 が、それぞれの個々のテナント 1 0 2 ~ 1 0 4 がそのテナント自体の別個のテナントデータ 1 5 4 ~ 1 5 6 を有することを示すことにも留意されたい。しかし、テナント 1 0 2 ~ 1 0 4 のサブセットは、テナント 1 0 2 ~ 1 0 4 の別のサブセットとは区分されたそのサブセットのデータを欲する可能性があることがあり得る。その場合、それぞれのサブセットは、そのサブセットのデータをサーバレイヤ 1 1 4 によって区分けされており、したがって、そのデータは、そのサブセットの任意のテナントによってアクセスされ得る。しかし、そのデータは、そのサブセット外のいかなるテナントによってもアクセスされ得ない。データは、例示のみを目的として、図 1 においては (サブセット毎ではなく) テナント毎に区分けされているところが表示されている。

10

【 0 0 2 6 】

[0036] サーバレイヤ 1 1 4 がデータストア 1 2 8 と複数回やりとりをすることは望ましくない可能性があるので、サーバレイヤ 1 1 4 は、キャッシュ 1 3 0 を実装する。メモリ内キャッシュ 1 3 0 においてさえもデータの隔離を維持するために、サーバレイヤ 1 1 4 は、システム 1 0 0 の各テナントについてキャッシュされたデータの別個のコピーを設ける。したがって、例として、キャッシュされたテナントデータ 1 6 0 は、テナント 1 0 2 のためのキャッシュされたメモリのコピーである。キャッシュされたテナントデータ 1 6 2 は、テナント 1 0 4 のためのキャッシュされたデータのコピーであり、キャッシュされたテナントデータ 1 6 4 は、システム 1 0 0 の別のテナントのためのキャッシュされたデータのコピーである。サーバレイヤ 1 1 4 は、システム 1 0 0 のそれぞれの個々のテナント 1 0 2 ~ 1 0 4 に対応するキャッシュされたデータ 1 6 2 ~ 1 6 4 の別個のコピーを保有する。

20

【 0 0 2 7 】

[0037] 一部の共有されたデータ 1 6 6 は、テナント 1 0 2 ~ 1 0 4 のすべてに共通である可能性があることがあり得る。例えば、共有されたデータ 1 6 6 は、テナントのそれぞれの親持ち株会社についての全般的な情報を含む可能性がある。その場合、サーバレイヤ 1 1 4 は、共有されたデータ 1 6 6 を記憶し、したがって、その共有されたデータは、任意のテナント (またはテナントの任意のサブセット) によってアクセスされ得る。共有されたデータ 1 6 6 は任意選択であるので破線で示されており、別の実施形態においては、いかなるデータもテナントの間で共有されない。

30

【 0 0 2 8 】

[0038] システム 1 0 0 の動作のより詳細な考察が、以降で与えられる。図 2 ~ 1 1 が参照される。

【 0 0 2 9 】

[0039] 図 2 は、管理者 1 3 3 に新しいテナントを設定させる際のシステム 1 0 0 の動作の一実施形態を示す流れ図である。図 2 は、管理者 1 3 3 が、まずシステムにログインし、管理者構成要素 1 3 2 が、管理者 1 3 3 が新しいテナントまたは区分を生成することを可能にするユーザ入力機構 1 8 1、1 8 3、1 2 7、および 1 2 9 を有する (図 2 A の表示 1 7 9 または図 2 B の表示 1 2 5 などの) ユーザインターフェース表示を生成する。これは、図 2 のブロック 1 7 0 によって示される。そのとき、管理者構成要素 1 3 2 は、新しいテナントを生成する管理者 1 3 3 から入力を受け取る。

40

【 0 0 3 0 】

[0040] 新しいテナントが生成されると、管理者構成要素 1 3 2 は、新しいテナントのための (例えば、テナント 1 0 2 のための) セキュリティ管理者として (クライアント 1 0 6 などの) 別のユーザを割り振る管理者 1 3 3 からの入力を受け取るユーザ入力機構 1 8 7 を有する (図 2 C の表示 1 8 5 などの) ユーザインターフェース表示を表示する。クライアント 1 0 6 をテナント 1 0 2 のためのセキュリティ管理者として割り振ることは、図 2 のブロック 1 7 4 によって示される。これは、サーバレイヤ 1 1 4 に、クライアント 1 0 6 が (E R P アプリケーションなどの) 企業データシステムにログインし、新しいテナント 1 0 2 のユーザを (例えば、図 2 D に示された表示 1 8 9 または図 2 E の表示 1 3 1

50

を用いて)設定することを可能にさせる。これは、図2のブロック176によって示される。例えば、これは、セキュリティ管理者(例えば、クライアント106)がテナント102のユーザのそれぞれについて構成ファイル146~148をロードすることを可能にする。構成ファイルをロードすることは、図2のブロック178によって示される。次いで、セキュリティ管理者は、テナント102のクライアントのそれぞれに役割を割り振ることもできる。これは、ブロック180によって示される。したがって、セキュリティ管理者は、さまざまな役割に基づくセキュリティ規則、認証規則、または他の種類のセキュリティ規則を企業データシステムに入力することができ、それらの規則は、サーバレイヤ114によって134でアクセスされ得る。当然ながら、セキュリティ管理者は、他のタスクも実行する可能性があり、これは、図2のブロック182によって示される。

10

【0031】

[0041] 新しいテナント102が企業データシステムで設定されると、テナント102は、データストア128に企業データを記憶したいと望む可能性がある。それが行われる場合、データ転送を開始する特定のクライアント106~108の構成データ146~148も、データストア128にデータを記憶する要求に含められる。

【0032】

[0042] 次いで、サーバレイヤ114は、新しいテナント102のデータをテナント102に属するテナントデータ154として識別することによってデータストア128に実装されたデータベースのそのデータを区分けする。このようにしてデータを区分けすることは、図2のブロック184によって示される。サーバレイヤ114は、さまざまな異なる方法でこれを行う可能性がある。例えば、サーバレイヤ114は、テナントデータ154の各テーブルを特定のテナントに属するものとして識別する区分識別子をそのテーブルに設ける可能性がある。テーブル毎にデータを区分けすることは、図2のブロック186によって示される。加えて、サーバレイヤ114は、各テーブルのそれぞれの個々の行のデータを区分けする可能性がある。すなわち、サーバレイヤは、テナント102に属するテーブルにおいて、テナント102に属するデータのあらゆる行を、その行のデータがテナント102に属することを区分識別子が示すようにしてストライピング(stripe)する可能性がある。行毎の区分けは、ブロック188によって示される。サーバレイヤ114は、他の方法で区分けする可能性もある。例えば、サーバレイヤ114は、テナント102によってのみアクセスされ得るスキーマに応じてテナントデータ154のテーブルのデータを構成する可能性がある。スキーマに基づく方法でデータを区分けすることは、ブロック190によって示される。サーバレイヤ114は、他の方法でデータを区分けする可能性もあり、これは、ブロック192によって示される。

20

30

【0033】

[0043] 図3は、テナントデータ154および156がテナント102および104のためにデータベース128にどのように記憶されるかの例示的な例である1組のテーブル194および196の一実施形態を示す。図3の実施形態において、テーブル194は、テーブルレベル、行レベルである可能性がある区分識別子を有するか、またはスキーマに基づく可能性がある。区分識別子198は、データ200をテナント102に属するものと識別する。同様に、テーブル196は、データ204をテナント104に属するものと識別する区分識別子202を有する。データを区分けする他の方法も、本明細書においてやはり想定される。

40

【0034】

[0044] 図3A~3Cは、例として、テーブル内の区分けされたデータを示すユーザインターフェース表示を示す。図3Aは、顧客テーブルに関して、属性タブ213が選択されるときに属性を表示するユーザインターフェース表示211を示す。さまざまな属性が表示されており、四角215で縁取られた属性は、区分識別子に基づくのみでなく、会社毎でもデータが区分けされることを示す。したがって、データにアクセスするテナントは、関連する区分にのみ属すればよいのではなく、関連する会社にも属しなければならない。

【0035】

50

[0045] 図3Bは、異なるテーブルのための属性を示すユーザインターフェース表示217を示す。ここで、四角215は、データが区分識別子のみに基づいて区分けされることを示す。すなわち、関連する区分に割り振られた任意のテナントが、示されたテーブルにアクセスし得る。したがって、（例えば）会社のサブセットが、同じデータにアクセスする可能性がある。

【0036】

[0046] 図3Cは、さらに別のテーブルのための属性を示すユーザインターフェース表示219を示す。ユーザインターフェース表示219において四角221内に示されたテーブルの属性は、テーブルがシステムデータを含むことを示す。テーブルが会社毎でも、区分毎でも区分けされないことを示し、テーブルがフレームワークテーブルグループ（table group）に属することを示すことによって、四角223内の属性は、テーブルがシステムで共有される共有されたデータを含むことを示す。

【0037】

[0047] 図4は、テナント102がデータストア128に対するデータ操作要求を実行することを可能にする際のシステム100の動作の一実施形態を示す。一実施形態において、クライアント108は、テナント102にログインする。これは、図4のブロック210によって示される。クライアント108は、テナント102のセキュリティ管理者がクライアント108を設定するとき確立された認証手順を経ることによってこれを行う。認証は、図4のブロック212によって示される。そのとき、サーバレイヤ114は、クライアント108が属する特定のテナントを決定する。これは、多種多様な異なる方法で行われ得る。例えば、サーバレイヤ114は、クライアント108が属するテナントを確認することをクライアント108に求めるユーザインターフェース表示を提供する可能性がある。同様に、サーバレイヤ114は、クライアント108が属する特定のテナントを識別するためにクライアント108が書き込むアプリケーションプログラミングインターフェースを表示する可能性がある。これは、図4のブロック214によって示される。言うまでもなく、クライアント108は、さらに、サーバレイヤ114に構成データ148を自動的に提供する可能性があり、構成データは、例示的に、テナント102のためのクライアント108の役割のみでなく、クライアント108がシステムへのログインに使ったテナント102の識別情報も含む。これは、図4のブロック216によって示される。サーバレイヤ114は、クライアント108が属する特定のテナント102を識別する他の方法を使用する可能性もあり、これは、図4のブロック218によって示される。

【0038】

[0048] テナントを通じてログインすると、クライアント108は、データ操作要求を送り、構成データ148が、その要求と一緒に送信される。これは、図4のブロック220によって示される。データ操作要求は、データベース128のデータを操作するか、またはデータベース128にデータを追加する任意の種類の要求である可能性がある。例えば、データ操作要求は、図4のブロック222によって示されるように、データベース128に記憶されるべき新しいデータを生成する可能性がある。要求は、ブロック224によって示されるように、データストア128からデータを削除する要求である可能性がある。要求は、データストア128のデータを更新するデータ修正要求である可能性がある。これは、ブロック226によって示される。要求は、ブロック228によって示されるように、単純に、データストア128のデータを取り出し、読み取る要求である可能性もある。もちろん、データ操作要求は、任意の他の種類の要求である可能性もあり、これは、ブロック230によって示される。

【0039】

[0049] 次いで、サーバレイヤ114は、要求とともに送られた構成データを読み取って、クライアント108が属する特定のテナント102を判定し、さらに、（例えば）テナント102でクライアント108が担う役割を判定する。次いで、サーバレイヤ114は、クライアント108のストア128のデータへのアクセスを、構成データ148で識別される特定のテナント102のためのデータに制限することによって、データ操作要求を

処理する。また、サーバレイヤ 114 は、例示的に、テナント 102 のためのセキュリティ規則 134 にアクセスしてクライアント 108 の役割を識別し、それらの規則にしたがってセキュリティを実施する。対応するテナントデータのみを用いて要求を処理し、そのテナントのためのセキュリティを実施することは、図 4 のブロック 232 によって示される。

【0040】

[0050] システム 100 の動作をより詳細に示すために、図 5 は、データストア 128 からデータを取得するためにクライアント 108 によって送られる特定のデータアクセス要求を示す流れ図である。やはり、クライアント 108 は、例示的に、認証または他の所望のログイン手順を用いてテナント 102 にログインする。これは、図 5 のブロック 240 によって示される。次いで、クライアント 108 は、データストア 128 のテナントデータのクエリを送る。これは、図 5 のブロック 242 によって示される。クエリは、制限されない場合、ストア 128 の他のテナントのためのテナントデータを包含する可能性がある。例えば、クエリは、11月に生成されたすべてのセールスリードを探している場合、データベース 128 のすべてのテナントのためのテナントデータを包含する。クライアント 108 は、サーバレイヤ 114 にクエリと一緒に構成データ 148 を送信する。これは、図 5 のブロック 244 によって示される。サーバレイヤ 114 は、ブロック 246 によって示されるように、クエリおよび対応する構成データを受信する。サーバレイヤ 114 は、構成データ 148 を調べ、クエリがどのテナントから生じたか、およびテナントでクライアント 108 が担う役割を判定する。次いで、サーバレイヤ 114 は、テナント 102 に属し、テナント 102 のための役割に基づくセキュリティ（またはセキュリティ規則 134 によって定義された他のセキュリティ）を実施するデータのみを要求するために、構成データに基づいてクエリを修正する。これは、図 5 のブロック 148 によって示される。サーバレイヤ 114 は、クライアント 108 が属するテナント（この場合、クライアント 102）に属するデータのみを包含するようにデータ要求を効果的に制限する。

【0041】

[0051] 一実施形態において、サーバレイヤ 114 は、そのサーバレイヤ 114 がキャッシュ 130 によりデータ要求を処理することができるかどうかを判定する。そのようにする際に、サーバレイヤ 114 は、まず、この特定のテナント 102 のためのキャッシュされたテナントデータ 160 のコピーが実際に存在するかどうかを判定する。これは、図 5 のブロック 250 によって示される。存在しない場合、サーバレイヤ 114 は、ブロック 252 によって示されるように、テナント 102 のためのキャッシュのコピーを生成し、次いで、データストア 128 にアクセスして要求されたデータを取得する。これは、ブロック 254 によって示される。

【0042】

[0052] しかし、サーバレイヤ 114 は、ブロック 250 において、テナント 102 のためのキャッシュのコピーが存在すると判定する場合、要求されたデータに関してそのキャッシュされたテナントデータを調べる。これは、図 5 のブロック 256 によって示される。サーバレイヤ 114 は、キャッシュ 130 により要求を処理することができる場合、そのように処理する。しかし、サーバレイヤ 114 は、キャッシュ 130 により要求を処理することができない場合、データベース 128 のデータにやはりアクセスしなくてはならない。要求がキャッシュ 130 によって処理され得るかどうかを判定することは、図 5 のブロック 258 によって示される。

【0043】

[0053] どちらの場合も、サーバレイヤ 114 がキャッシュ 130 からデータを取得したか、またはデータストア 128 からデータを取得したかに関わらず、クエリに回答するデータが、テナント 102 のクライアント 108 に返される。これは、図 5 のブロック 260 によって示される。次いで、サーバレイヤ 114 は、任意の他の所望のキャッシュ動作を行う。例えば、（テナントのキャッシュのコピーにない）新しいデータがデータストア 128 から取り出された場合、サーバレイヤ 114 は、テナント 102 のためのキャッシ

ユされたテナントデータにそのデータを追加する。言うまでもなく、サーバレイヤ 114 は、他の方法でテナントのキャッシュのコピーを更新する可能性もあり、キャッシュ 130 を維持するためのキャッシュ動作を行うことは、図 5 のブロック 262 によって示される。したがって、サーバレイヤ 114 は、そのサーバ 114 が（安全で区分された方法で）複数のテナントのためのデータを記憶することができるようにデータベース 128 を区分するだけでなく、そのサーバレイヤ 114 が同じことを行うことができるようにキャッシュ 130 を制御する。キャッシュされたデータのそれぞれのコピーは、所与のテナントに属するものとしてマークされ、他のテナントは、キャッシュされたデータのそのコピーにアクセスすることができない。キャッシュされたデータのそれぞれのコピーは、他のテナントのキャッシュされたデータとは別々に維持され、区分けされる。

10

【0044】

[0054] 図 5 A は、テナントのサブセットが、まとめて、しかし他のテナントとは別に区分けされる別の実施形態を示す。図 5 A は、図 1 に示されたシステム 100 と同様であるシステム 100 を示し、同様の項目は、同様に番号を振られている。しかし、図 5 A のシステム 100 は、テナント 102 および 104 が、例示的に、サブセット 161 としてグループにまとめられる 2 つの企業であることを示す。したがって、サブセット 161 のテナントは、互いのデータにアクセスすることができることを望むが、テナント 105 などのさらなるテナントのためのデータからそのデータを分け、隔離したいと望む。したがって、管理者は、両方のテナント 102 および 104 を同じ区分に割り振る。そのようにして、サーバレイヤ 114 は、両方のテナント 102 および 104 がデータ 163 のすべてにアクセスすることができるようにテナント 102 および 104 のために区分けされるそのデータ 163 を記憶する。しかし、データ 163 は、テナント 105 のための区分に割り振られるデータ 165 とは別々に区分けされる。したがって、テナント 105 は、データ 163 にアクセスすることができず、テナント 102 および 104 のサブセット 161 は、データ 165 にアクセスすることができない。

20

【0045】

[0055] 一実施形態において、キャッシュ 130 は、データストア 128 と同じようにしてやはり別々に区分けされることに留意されたい。したがって、キャッシュ 130 は、テナント 102 および 104 のサブセット 161 のためのキャッシュされたデータの別個のコピーと、テナント 105 のためのキャッシュされたデータの別々に区分けされたコピーとを含む。したがって、キャッシュ 130 は、データストア 128 と同じようにして区分けされ、その結果、キャッシュ 130 に要求される任意のデータも、同じようにして区分けされる。

30

【0046】

[0056] 本明細書において考察される企業データは、顧客の記録、注文、供給業者、リード、提案 (proposal)、見積もり (quote)、販売データ、製品データ、位置データ、会社の財務およびマーケティングデータおよび戦略、個人データ、賃金または他の人材管理情報などの多種多様な企業データを含み得ることに留意されたい。他の企業データまたは企業の記録も、使用され得る。

【0047】

40

[0057] 図 6 は、システム 100 がクラウドコンピューティングアーキテクチャ 500 内に配置される点を除いて図 1 に示されたシステム 100 のブロック図である。クラウドコンピューティングは、サービスを提供するシステムの物理的な位置または構成をエンドユーザが知っていることを必要としない計算、ソフトウェア、データアクセス、およびストレージサービスを提供する。さまざまな実施形態において、クラウドコンピューティングは、適切なプロトコルを用いてインターネットなどの広域ネットワーク上でサービスを提供する。例えば、クラウドコンピューティングプロバイダは、広域ネットワーク上でアプリケーションを提供し、それらのアプリケーションは、ウェブブラウザまたは任意の他のコンピューティング構成要素を通じてアクセスされ得る。システム 100 のソフトウェアまたは構成要素および対応するデータは、遠隔の位置にあるサーバに記憶される可能性が

50

ある。クラウドコンピューティング環境の計算リソースは、遠隔のデータセンターの位置に集約される可能性があり、または分散される可能性がある。クラウドコンピューティングインフラストラクチャは、ユーザのための単一のアクセスポイント (point of access) に見えとしても、共有されたデータセンターを通じてサービスを提供する可能性がある。したがって、本明細書において説明される構成要素および機能は、クラウドコンピューティングアーキテクチャを用いて遠隔の位置のサービスプロバイダから提供される可能性がある。代替的に、それらの構成要素および機能は、通常のサーバから提供される可能性があり、またはクライアントデバイスに直接もしくは他の方法でインストールされる可能性がある。

【 0 0 4 8 】

10

[0058] 説明は、パブリッククラウドコンピューティングとプライベートクラウドコンピューティングとの両方を含むように意図される。(パブリックとプライベートとの両方の)クラウドコンピューティングは、リソースの実質的にシームレスなプールを行い、基礎を成すハードウェアインフラストラクチャを管理し、構成する必要性を減らす。

【 0 0 4 9 】

[0059] パブリッククラウドは、供給業者によって管理され、典型的には、同じインフラストラクチャを用いて複数の消費者をサポートする。また、パブリッククラウドは、プライベートクラウドとは対照的に、エンドユーザをハードウェアの管理から解放することができる。プライベートクラウドは、組織自体によって管理される可能性があり、インフラストラクチャは、典型的には、他の組織と共有されない。組織は、インストールおよび修理など、ハードウェアを引き続きある程度維持する。

20

【 0 0 5 0 】

[0060] 図 6 に示された実施形態において、一部の項目は、図 1 に示された項目と同様であり、同様に番号を振られている。図 6 は、特に、サーバレイヤ 1 1 4、データストア 1 2 8、キャッシュ 1 3 0、およびセキュリティ規則 1 3 4 が(パブリック、プライベート、または一部がパブリックである一方、他がプライベートである組合せである可能性がある)クラウド 5 0 2 内に位置することを示す。したがって、テナント 1 0 2 のクライアント 1 0 8 (またはユーザ 1 0 3)は、ユーザデバイス 5 0 4 を用いてクラウド 5 0 2 を通じてそれらのシステムにアクセスする。

【 0 0 5 1 】

30

[0061] さらに、図 6 は、クラウドアーキテクチャの別の実施形態を示す。図 6 は、システム 1 0 0 の一部の要素がクラウド 5 0 2 に配置される一方、他の要素はクラウド 5 0 2 に配置されないことも想定されることを示す。例として、データストア 1 2 8 は、クラウド 5 0 2 の外に配置され、クラウド 5 0 2 を通じてアクセスされ得る。別の実施形態においては、セキュリティ規則 1 3 4 も、クラウド 5 0 2 の外にある。それらの要素は、どこに位置するかに関わりなく、ネットワーク(広域ネットワークもしくはローカルエリアネットワークのどちらか)を通じてデバイス 5 0 4 によって直接アクセスされ得るか、サービスによって遠隔の場所でホストされ得るか、またはクラウドを通じてサービスとして提供されるかもしくはクラウドにある接続サービスによってアクセスされ得る。これらのアーキテクチャのすべては、本明細書において想定される。

40

【 0 0 5 2 】

[0062] システム 1 0 0 またはその一部は多種多様な異なるデバイスに配置することができることに留意されたい。それらのデバイスの一部は、サーバ、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、またはパームトップコンピュータ、セル電話、スマートフォン、マルチメディアプレーヤー、携帯情報端末などの他のモバイルデバイスを含む。

【 0 0 5 3 】

[0063] 図 7 は、本システム(またはその一部)が展開され得る、ユーザまたはクライアントのハンドヘルドデバイス 1 6 として使用され得るハンドヘルドまたはモバイルコンピューティングデバイスの 1 つの例示的な実施形態の簡略化されたブロック図である。図 8

50

～ 10 は、ハンドヘルドまたはモバイルデバイスの例である。

【0054】

[0064] 図7は、(テナントもしくはクライアントもしくは他の構成要素などの)システム100の構成要素を実行することができ、またはシステム100とインタラクションし、またはその両方を行うクライアントデバイス16の構成要素の全体的なブロック図を与える。デバイス16においては、ハンドヘルドデバイスが他のコンピューティングデバイスと通信することを可能にし、一部の実施形態では、スキャンングすることによるなどして自動的に情報を受信するためのチャネルを提供する通信リンク13が、設けられる。通信リンク13の例は、赤外線ポートと、シリアル/USBポートと、イーサネット(登録商標)ポートなどのケーブルネットワークポートと、ネットワークへのセルラアクセスを提供するために使用される無線サービスである汎用パケット無線サービス(GPRS)、LTE、HSPA、HSPA+、および他の3Gおよび4G無線プロトコル、1Xrtt、およびショートメッセージサービス、ならびにネットワークへのローカル無線接続を提供する802.11および802.11b(Wi-Fi)プロトコル、およびBluetooth(登録商標)プロトコルを含む1つまたは複数の通信プロトコルによる通信を可能にする無線ネットワークポートとを含む。

10

【0055】

[0065] 他の実施形態では、(システム100のERPアプリケーションのような)アプリケーションまたはシステムは、セキュアデジタル(SD)カードインターフェース15に接続される取り外し可能なSDカードに収容される。SDカードインターフェース15および通信リンク13は、メモリ21、および入力/出力(I/O)構成要素23、ならびにクロック25、およびロケーションシステム27にも接続されるバス19を通じて(図1のプロセッサ136または138をやはり具現化する可能性がある)プロセッサ17と通信する。

20

【0056】

[0066] I/O構成要素23は、一実施形態において、入力および出力動作を容易にするために設けられる。デバイス16のさまざまな実施形態のためのI/O構成要素23は、ボタン、タッチセンサ、マルチタッチセンサ、光学または映像センサ、音声センサ、タッチスクリーン、近接センサ、マイクロホン、チルトセンサ、および重力スイッチ(gravity switch)などの入力構成要素と、ディスプレイデバイス、スピーカ、および/またはプリンタポートなどの出力構成要素とを含み得る。他のI/O構成要素23も、使用され得る。

30

【0057】

[0067] クロック25は、例示的に、時間および日にちを出力するリアルタイムクロック構成要素を含む。さらに、クロック25は、例示的に、プロセッサ17のためのタイミング機能を提供する可能性がある。

【0058】

[0068] ロケーションシステム27は、例示的に、デバイス16の現在の地理的位置を出力する構成要素を含む。これは、例えば、全地球測位システム(GPS)受信機、LORANシステム、推測航法(dead reckoning)システム、セルラ三角測量システム、または他の測位システムを含み得る。さらに、ロケーションシステム27は、例えば、所望の地図、ナビゲーション経路、および他の地理的機能を生成するマッピングソフトウェアまたはナビゲーションソフトウェアを含み得る。

40

【0059】

[0069] メモリ21は、オペレーティングシステム29、ネットワーク設定31、アプリケーション33、アプリケーション構成設定35、データストア37、通信ドライバ39、および通信構成設定41を記憶する。メモリ21は、すべての種類の有形の揮発性および不揮発性コンピュータ可読メモリデバイスを含み得る。メモリ21は、(以下で説明される)コンピュータストレージ媒体も含み得る。メモリ21は、プロセッサ17によって実行されるときに、プロセッサに、コンピュータによって実装される工程または機能を命

50

令にしたがって実行させるコンピュータ可読命令を記憶する。システム 100、またはデータストア 128 もしくはキャッシュ 130 の項目は、例えば、メモリ 21 に存在する可能性がある。同様に、デバイス 16 は、さまざまな企業アプリケーションを実行するか、または企業システム 100 の一部もしくはすべてを具現化することができるクライアント企業システム 24 を有する可能性がある。プロセッサ 17 は、他の構成要素の機能を助けるために他の構成要素によって作動される可能性もある。

【0060】

[0070] ネットワーク設定 31 の例は、プロキシ情報、インターネット接続情報、およびマッピングなどの事柄を含む。アプリケーション構成設定 35 は、アプリケーションを特定の企業またはユーザのために適合させる設定を含む。通信構成設定 41 は、他のコンピュータとの通信のためのパラメータを与え、GPRS パラメータ、SMS パラメータ、接続ユーザ名、およびパスワードなどの項目を含む。

10

【0061】

[0071] アプリケーション 33 は、オペレーティングシステム 29 の一部であるか、またはデバイス 16 の外部からホストされる可能性もあるが、デバイス 16 に既に記憶されたアプリケーションであるか、または使用中にインストールされるアプリケーションである可能性がある。

【0062】

[0072] 図 8 は、デバイス 16 がタブレットコンピュータ 600 である一実施形態を示す。図 8 においては、ディスプレイスクリーン 602 に表示される（新しいテナントを生成するために使用される）ユーザインターフェース表示 179 を有するコンピュータ 600 が、示される。スクリーン 602 は、タッチスクリーンである可能性があり（したがって、ユーザの指 604 のタッチジェスチャがアプリケーションとインタラクションするために使用される可能性があり）、またはペンもしくはスタイラスから入力を受け取るペン対応インターフェースである可能性がある。スクリーン 602 は、オンスクリーン仮想キーボードを使用する可能性もある。言うまでもなく、スクリーン 602 は、例えば、無線リンクまたは USB ポートなどの好適な取り付け機構によってキーボードまたは他のユーザ入力デバイスに取り付けられる可能性もある。コンピュータ 600 は、例示的に、音声入力も受け取る可能性がある。

20

【0063】

[0073] 図 9 および 10 は、使用され得るデバイス 16 のさらなる例を与えるが、他のデバイス 16 も使用され得る。図 9 においては、スマートフォンまたはモバイル電話 45 が、デバイス 16 として与えられる。電話 45 は、電話番号をダイヤルするための 1 組のキーパッド 47、アプリケーションの画像を含む画像、アイコン、ウェブページ、写真、および映像を表示することができるディスプレイ 49、ならびにディスプレイ上に示される項目を選択するための制御ボタン 51 を含む。電話は、汎用パケット無線サービス（GPRS）および 1Xrtt などのセルラ電話信号と、ショートメッセージサービス（SMS）信号とを受信するためのアンテナ 53 を含む。一部の実施形態において、電話 45 は、セキュアデジタル（SD）カード 57 を受ける SD カードスロット 55 も含む。

30

【0064】

[0074] 図 10 のモバイルデバイスは、携帯情報端末（PDA）59 または（以降、PDA 59 と呼ばれる）マルチメディアプレーヤーもしくはタブレットコンピューティングデバイスなどである。PDA 59 は、スタイラスがスクリーン上に位置づけられるときにスタイラス 63（またはユーザの指などの他のポインタ）の位置を感知する電磁誘導式スクリーン 61 を含む。これは、ユーザがスクリーン上の項目を選択し、強調表示し、移動させ、描画し、書くことを可能にする。PDA 59 は、ディスプレイ 61 に触れることなく、ユーザがディスプレイ 61 に表示されるメニューオプションまたは他の表示オプションをスクロールすることを可能にし、ユーザがアプリケーションを変更するかまたはユーザ入力機能を選択することを可能にするいくつかのユーザ入力キーまたは（ボタン 65 などの）ボタンも含む。図示されていないが、PDA 59 は、他のコンピュータとの無線通信を

40

50

可能にする内蔵アンテナおよび赤外線送信機／受信機と、他のコンピューティングデバイスとのハードウェア接続を可能にする接続ポートとを含み得る。そのようなハードウェア接続は、概して、シリアルまたはUSBポートを通じて他のコンピュータに接続するクレードルによってなされる。したがって、これらの接続は、非ネットワーク接続である。一実施形態において、モバイルデバイス59は、SDカード69を受けるSDカードスロット67も含む。

【0065】

[0075] デバイス16の他の形態があり得ることに留意されたい。

【0066】

[0076] 図11は、(例えば)システム100が展開され得るコンピューティング環境の一実施形態である。図11を参照すると、一部の実施形態を実装するための例示的なシステムは、コンピュータ810の形態の多目的コンピューティングデバイスを含む。コンピュータ810の構成要素は、(サーバまたはテナントのためのプロセッサを含み得る)処理ユニット820、システムメモリ830、およびシステムメモリを含むさまざまなシステム構成要素を処理ユニット820に接続するシステムバス821を含み得るがこれらに限定されない。システムバス821は、各種のバスアーキテクチャのいずれかを使用した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数種のバス構造のいずれである可能性がある。限定ではなく例として、そのようなアーキテクチャは、業界標準アーキテクチャ(ISA)バス、マイクロチャネルアーキテクチャ(MCA)バス、拡張ISA(EISA)バス、ビデオ電子装置規格化協会(VESA: Video Electronics Standards Association)ローカルバス、およびMezzanineバスとしても知られる周辺装置相互接続(PCI: Peripheral Component Interconnect)バスを含む。図1に関連して説明されたメモリおよびプログラムは、図11の対応する部分に展開される可能性がある。

【0067】

[0077] 通常、コンピュータ810は、さまざまなコンピュータ可読媒体を含む。コンピュータ可読媒体は、コンピュータ810によってアクセスされる可能性があり、揮発性の媒体と不揮発性の媒体との両方、取り外し可能な媒体および取り外し不可能な媒体を含む任意の利用可能な媒体である可能性がある。限定でなく例として、コンピュータ可読媒体は、コンピュータストレージ媒体および通信媒体を含む可能性がある。コンピュータストレージ媒体は、変調されたデータ信号または搬送波とは異なり、変調されたデータ信号または搬送波を含まない。コンピュータストレージ媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの情報を記憶するための任意の方法または技術で実現された揮発性と不揮発性との両方の取り外し可能な媒体および取り外し不可能な媒体を含むハードウェアストレージ媒体を含む。コンピュータストレージ媒体は、RAM、ROM、EEPROM、フラッシュメモリ、もしくは他のメモリ技術、CD-ROM、デジタルバーサタイルディスク(DVD)、もしくは他の光ディスクストレージ、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、または所望の情報を記憶するために使用される可能性があり、コンピュータ810によってアクセスされる可能性がある任意の他の媒体を含むがこれらに限定されない。通常、通信媒体は、搬送機構でコンピュータ可読命令、データ構造、プログラムモジュール、または他のデータを具現化し、任意の情報配信媒体を含む。用語「変調されたデータ信号」は、その信号の特徴のうちの1つまたは複数を、信号中に情報を符号化するような方法で設定または変更した信号を意味する。限定ではなく例として、通信媒体は、有線ネットワークまたは直接有線接続などの有線媒体、ならびに音響、RF、赤外線、および他の無線媒体などの無線媒体を含む。上記の媒体のうちの任意のものの組合せも、コンピュータ可読媒体の範囲に含まれるべきである。

【0068】

[0078] システムメモリ830は、読み出し専用メモリ(ROM)831およびランダムアクセスメモリ(RAM)832などの揮発性および/または不揮発性メモリの形態のコンピ

10

20

30

40

50

ユータストレージ媒体を含む。起動中などにコンピュータ 810 内の要素間で情報を転送することに役立つ基礎的なルーチンを含む基本入出力システム 833 (BIOS) は、概して ROM 831 に記憶される。通常、RAM 832 は、処理ユニット 820 によって直ちにアクセスすることができる、および/または処理ユニット 820 によって現在動作させら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。限定ではなく例として、図 11 は、オペレーティングシステム 834、アプリケーションプログラム 835、他のプログラムモジュール 836、およびプログラムデータ 837 を示す。

【0069】

[0079] コンピュータ 810 は、他の取り外し可能な/取り外し不可能な揮発性/不揮発性コンピュータストレージ媒体をやはり含む可能性がある。単なる例として、図 11 は、取り外し不可能な不揮発性磁気媒体からの読み出し、または当該媒体に対する書き込みを行うハードディスクドライブ 841 と、取り外し可能な不揮発性磁気ディスク 852 からの読み出し、または当該磁気ディスクに対する書き込みを行う磁気ディスクドライブ 851 と、CD ROM または他の光媒体などの取り外し可能な不揮発性光ディスク 856 からの読み出し、または当該光ディスクに対する書き込みを行う光ディスクドライブ 855 とを示す。例示的な動作環境で使用され得る他の取り外し可能な/取り外し不可能な揮発性/不揮発性コンピュータストレージ媒体は、磁気テープカセット、フラッシュメモ리카ード、デジタルバーサタイルディスク、デジタルビデオテープ、固体 RAM、固体 ROM などを含むがこれらに限定されない。ハードディスクドライブ 841 は、概してインターフェース 840 などの取り外し不可能なメモリアンターフェースを介してシステムバス 821 に接続され、磁気ディスクドライブ 851 および光ディスクドライブ 855 は、概してインターフェース 850 などの取り外し可能なメモリアンターフェースによってシステムバス 821 に接続される。

【0070】

[0080] 上記で考察され、図 11 に示されたドライブおよびそれらのドライブに関連するコンピュータストレージ媒体は、コンピュータ 810 のためのコンピュータ可読命令、データ構造、プログラムモジュール、および他のデータの記憶を行う。例えば、図 11 において、ハードディスクドライブ 841 は、オペレーティングシステム 844、アプリケーションプログラム 845、他のプログラムモジュール 846、およびプログラムデータ 847 を記憶するものとして示されている。これらの構成要素は、オペレーティングシステム 834、アプリケーションプログラム 835、他のプログラムモジュール 836、およびプログラムデータ 837 と同じであるかまたは異なるかのどちらかである可能性があることに留意されたい。オペレーティングシステム 844、アプリケーションプログラム 845、他のプログラムモジュール 846、およびプログラムデータ 847 は、少なくともそれらが異なるコピーであることを示すために、ここでは異なる番号を与えられる。

【0071】

[0081] ユーザは、キーボード 862、マイクロホン 863、およびマウス、トラックボール、またはタッチパッドなどのポインティングデバイス 861 などの入力デバイスを通じてコンピュータ 810 に命令および情報を入力することができる。他の入力デバイス(図示せず)は、ジョイスティック、ゲームパッド、衛星パラボラアンテナ、スキャナなどを含む可能性がある。これらのおよび他の入力デバイスは、システムバスに結合されたユーザ入力インターフェース 860 を介して処理ユニット 820 に接続されることが多いが、パラレルポート、ゲームポート、またはユニバーサルシリアルバス(USB)などの他のインターフェースおよびバス構造によって接続される可能性がある。視覚ディスプレイ 891 または他の種類のディスプレイデバイスも、ビデオインターフェース 890 などのインターフェースを介してシステムバス 821 に接続される。モニタに加えて、コンピュータは、出力周辺機器インターフェース 895 を介して接続され得るスピーカ 897 およびプリンタ 896 などの他の周辺出力デバイスを含む可能性もある。

【0072】

[0082] コンピュータ 810 は、遠隔のコンピュータ 880 などの 1 つまたは複数の遠隔

10

20

30

40

50

のコンピュータへの論理接続を使用したネットワーク化された環境で動作させられる。遠隔のコンピュータ 880 は、パーソナルコンピュータ、ハンドヘルドデバイス、サーバ、ルータ、ネットワーク PC、ピアデバイス、または他のよくあるネットワークノードである可能性があり、概してコンピュータ 810 に関連して上で説明された要素の多くまたはすべてを含む。図 8 に示された論理接続は、ローカルエリアネットワーク (LAN) 871 および広域ネットワーク (WAN) 873 を含むが、他のネットワークを含む可能性もある。そのようなネットワーキング環境は、オフィス、企業規模のコンピュータネットワーク、イントラネット、およびインターネットにおいて一般的である。

【0073】

[0083] LAN ネットワーキング環境において使用される場合、コンピュータ 810 は、ネットワークインターフェースまたはアダプタ 870 を介して LAN 871 に接続される。WAN ネットワーキング環境において使用される場合、概して、コンピュータ 810 は、モデム 872、またはインターネットなどの WAN 873 を介して通信を確立するための他の手段を含む。内蔵または外付けである可能性があるモデム 872 は、ユーザ入力インターフェース 860 または他の適切な機構を介してシステムバス 821 に接続され得る。ネットワーク化された環境において、コンピュータ 810 に関連して示されたプログラムモジュール、またはそれらのモジュールの一部は、遠隔のメモリストレージデバイスに記憶され得る。限定ではなく例として、図 11 は、遠隔のコンピュータ 880 に存在するものとして遠隔のアプリケーションプログラム 885 を示す。図示されたネットワーク接続は例示的であり、コンピュータ間で通信リンクを確立する他の手段が使用され得ることが理解されるであろう。

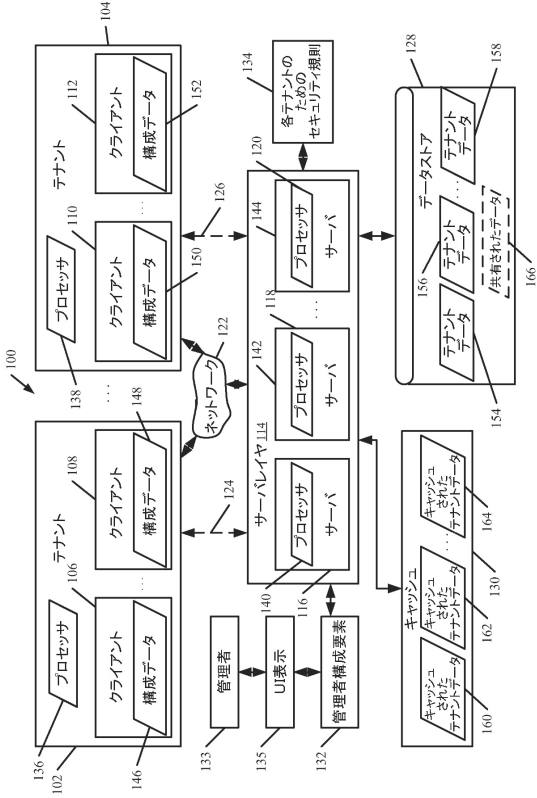
【0074】

[0084] 対象が構造的特徴および/または方法の動作に特有の言葉で説明されたが、添付の特許請求の範囲で定義された対象は上記で説明された特定の特徴または動作に必ずしも限定されないことを理解されたい。むしろ、上述の特定の特徴および動作は特許請求の範囲を実施する例示的な形態として開示される。

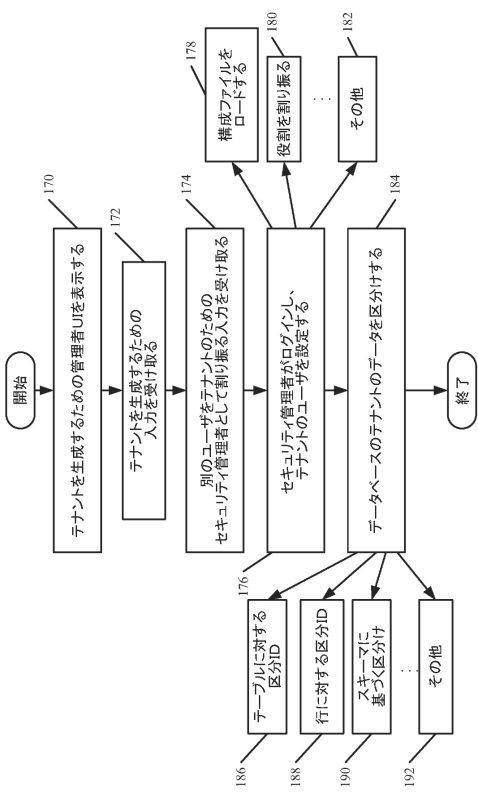
10

20

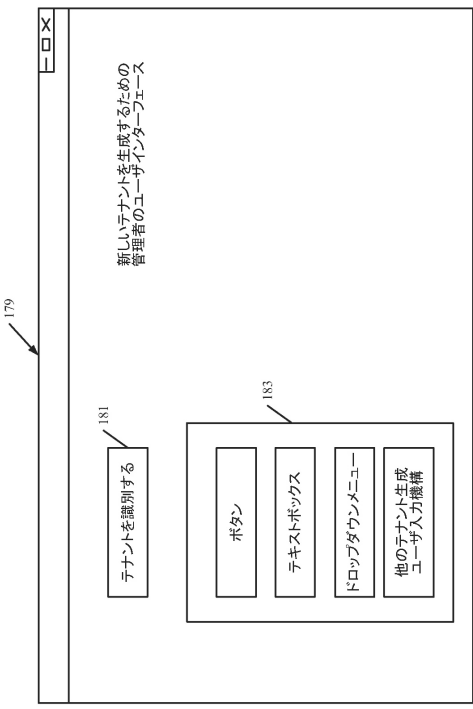
【図 1】



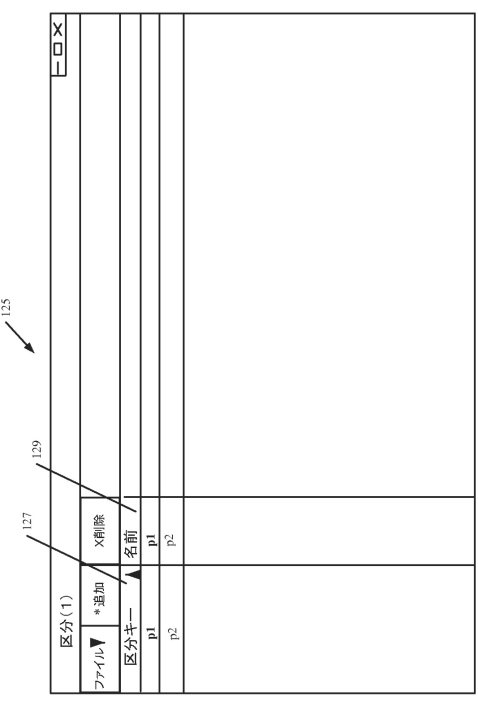
【図 2】



【図 2 A】



【図 2 B】



【 図 2 C 】

セキュリティ管理者を指定する

ポタン

テキストボックス

ドロップダウンメニュー

他のユーザ入力機構

185

187

【 図 2 D 】

189

ユーザ／クライアントを設定する

ユーザ名	入力機構
パスワード	入力機構
役割	入力機構
その他	入力機構

このテナントのクライアントおよびセキュリティ規則をセキュリティ管理者のユーザ／クライアントエージェントに設定するための

191

ユーザ／クライアントを設定する

役割に基づく規則	入力機構
他の規則	入力機構

193

構成ファイルを読み込む

195

【 図 2 E 】

<input type="checkbox"/> ユーザ(1) - 新しいコード <input type="checkbox"/> ユーザ <input type="checkbox"/> ファイル		<input type="checkbox"/> 編集 <input type="checkbox"/> 削除 <input type="checkbox"/> ユーザ <input type="checkbox"/> インポート <input type="checkbox"/> オプション <input type="checkbox"/> 関係 <input type="checkbox"/> 設定 <input type="checkbox"/> ログ <input type="checkbox"/> オンライン時間 <input type="checkbox"/> 送付 <input type="checkbox"/> 送付		<input type="checkbox"/> 133 <input type="checkbox"/> 131	
一般 * ユーザID <input type="text"/> ユーザ名 <input type="text"/> ネットワークドメイン <input type="text"/> 有効 現在の区分がデフォルトの区分である。 139 141 135 137		アカウントの種類 デフォルトの会社 有価 143 アクティブ化/リユース DAT 145 147 149 159		最終更新: 11:56:16 am このグリッドは空です 151 選択された役割の権限 選択された役割のユーザ 157 159	
ユーザの役割 <input type="checkbox"/> 役割を割り振る <input type="checkbox"/> 組織を割り振る <input type="checkbox"/> 削除 <input type="checkbox"/> 役割を編集する <input type="checkbox"/> 役割 155		153 312			

【 図 3 】

Figure 1 illustrates an example of a table structure. It shows two identical table structures side-by-side, separated by an ellipsis (...). Each table consists of three rows. The first row is labeled 'テーブル' (Table) and is pointed to by reference numeral 194. The second row is labeled '区分ID(テーブルレベル/行レベル/スキーマ)' (Distinction ID (Table level/Row level/Schema)) and is pointed to by reference numeral 198. The third row is labeled 'データ' (Data) and is pointed to by reference numeral 200. The rightmost table's rows are also pointed to by reference numerals 196, 202, and 204 respectively.

【図 3 A】

213

211

215

テーブル: CustTable	
属性	カテゴリ
ID	77
Name	CustTable
Label	Customers
FormRel	
ListPageRel	
ReportRel	
PreviewFormRel	
SearchLinkRelType	Url
SearchLinkRelName	EPCustTableInfo
TitleField1	AccountNum
TitleField2	Party
TableType	Regular
TableContents	Not specified
SystemTable	No
ConfigurationKey	LedgerBasic
SecurityKey	CustTables
Visible	Yes
AOSAuthorization	None
CacheLookup	Found
CreateRecIdIndex	Yes
SaveDataPerCompany	Yes
SaveDataPerPartition	Yes
TableGroup	Main
PrimaryIndex	AccountIdx
ClusterIndex	AccountIdx

会社毎のテーブル

【図 3 B】

217

213

215

テーブル: DirPartyEcoResCategory	
属性	カテゴリ
ID	4871
Name	DirPartyEcoResCategory
Label	Set up categories
FormRel	
ListPageRel	
ReportRel	
PreviewFormRel	
SearchLinkRelType	Url
SearchLinkRelName	
TitleField1	Party
TitleField2	relationType
TableType	Regular
TableContents	Not specified
SystemTable	No
ConfigurationKey	LogisticsBasic
SecurityKey	DirAddressService
Visible	Yes
AOSAuthorization	None
CacheLookup	Found
CreateRecIdIndex	Yes
SaveDataPerCompany	No
SaveDataPerPartition	Yes
TableGroup	Main
PrimaryIndex	SynopgateKey
ClusterIndex	ValidCategory_AK

区分毎のテーブル

【図 3 C】

217

213

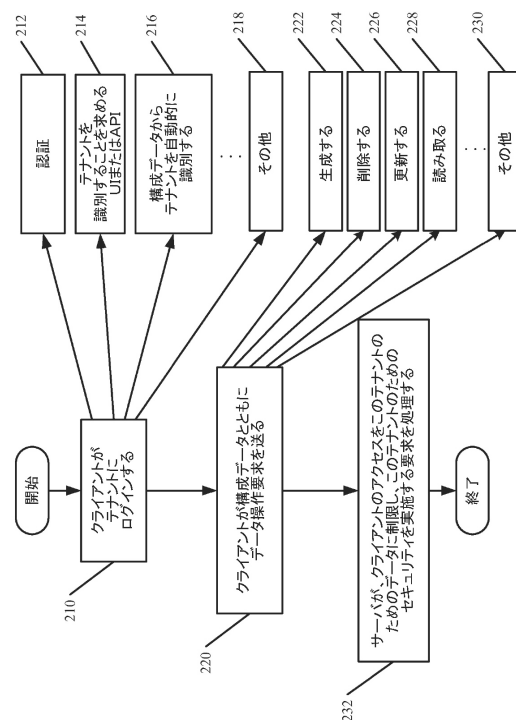
221

223

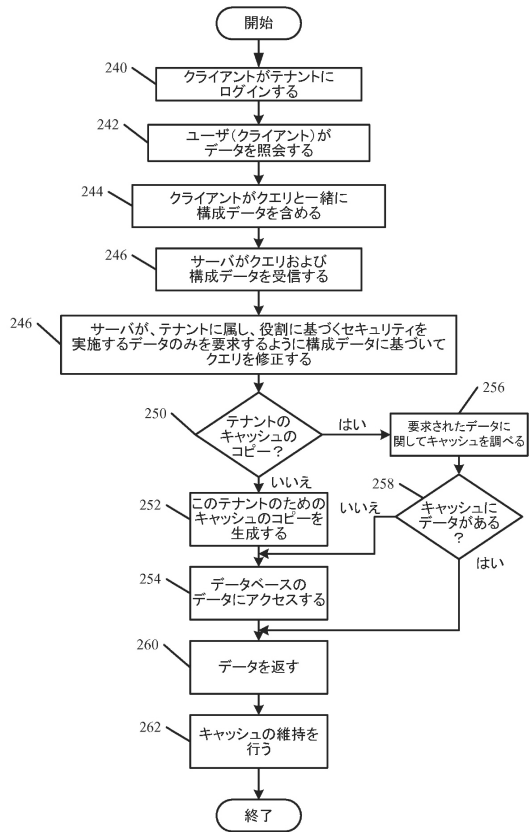
テーブル: xRefTableRelation	
属性	カテゴリ
ID	66
Name	xRefTableRelation
Label	Table relations
FormRel	
ListPageRel	
ReportRel	
PreviewFormRel	
SearchLinkRelType	Url
SearchLinkRelName	
TitleField1	TableName
TitleField2	RelationName
TableType	Regular
TableContents	Not specified
SystemTable	Yes
ConfigurationKey	
SecurityKey	SysDevelopmentTables
Visible	Yes
AOSAuthorization	CreateReadUpdateDelete
CacheLookup	None
CreateRecIdIndex	No
SaveDataPerCompany	No
SaveDataPerPartition	No
TableGroup	Framework
PrimaryIndex	RecIdIdx
ClusterIndex	Table

共有されるテーブル(システムのみ)

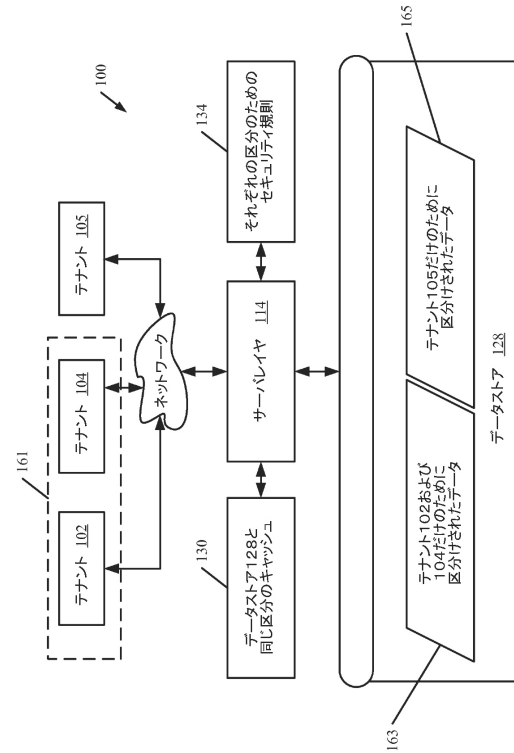
【図 4】



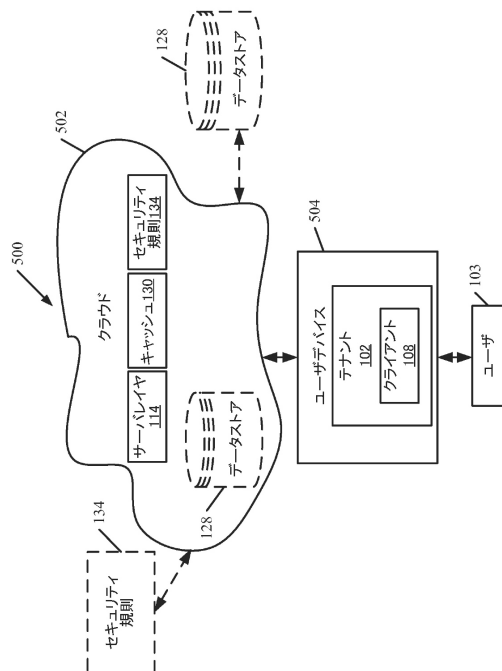
【図 5】



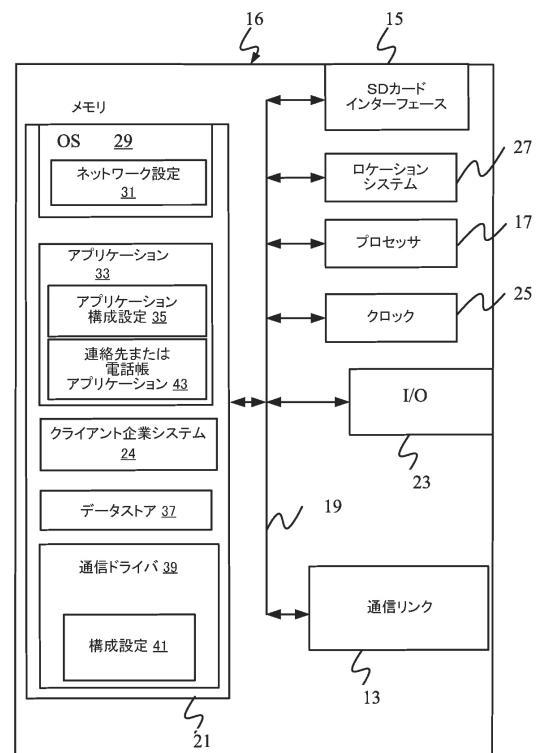
【図 5 A】



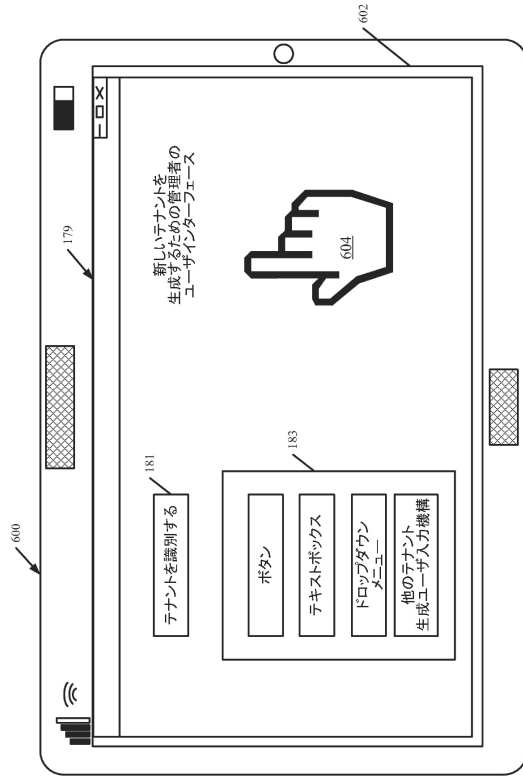
【図 6】



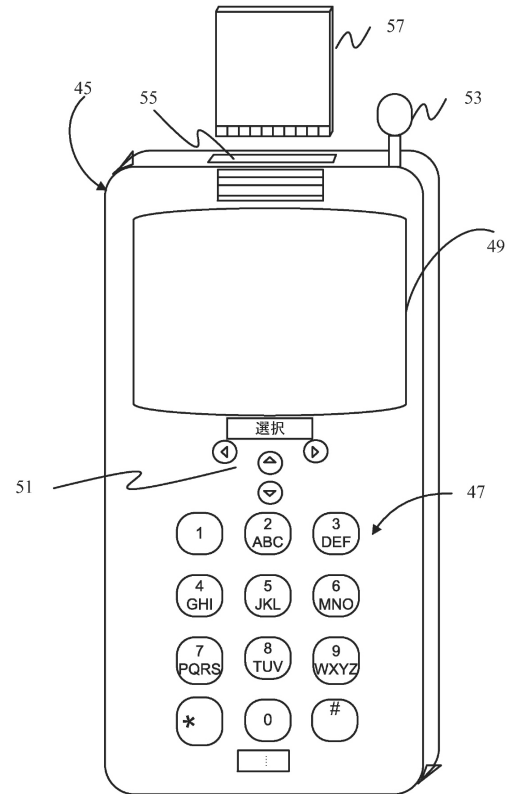
【図 7】



【図 8】



【図 9】



【図 10】

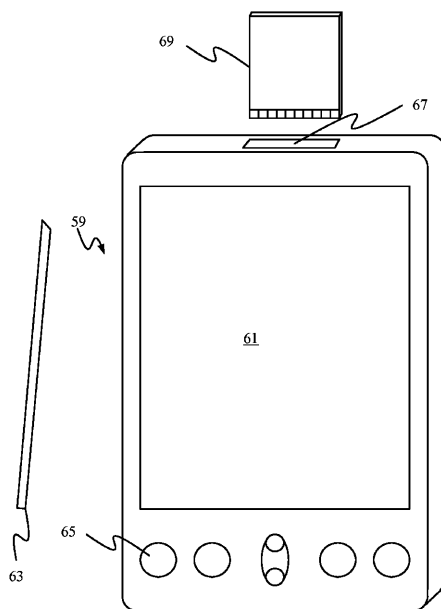
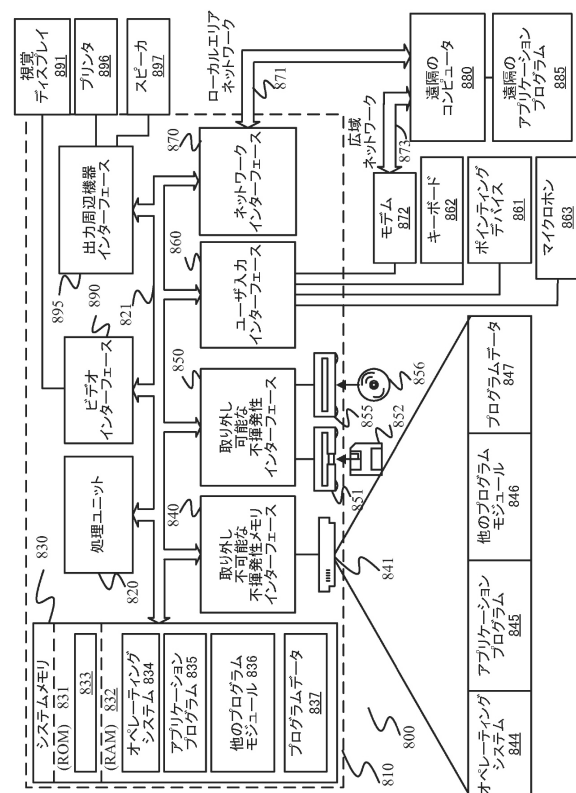


FIG. 10

【図 11】



フロントページの続き

(74)代理人 100108213

弁理士 阿部 豊隆

(72)発明者 ジョリー, ビジェータ

アメリカ合衆国, ワシントン州 98052-6399, レッドモンド, ワン マイクロソフト
ウェイ, マイクロソフト コーポレーション内, エルシーエー - インターナショナル パテン
ツ

(72)発明者 ナラ, アマール

アメリカ合衆国, ワシントン州 98052-6399, レッドモンド, ワン マイクロソフト
ウェイ, マイクロソフト コーポレーション内, エルシーエー - インターナショナル パテン
ツ

(72)発明者 ナトゥ, マダン ジー.

アメリカ合衆国, ワシントン州 98052-6399, レッドモンド, ワン マイクロソフト
ウェイ, マイクロソフト コーポレーション内, エルシーエー - インターナショナル パテン
ツ

合議体

審判長 仲間 晃

審判官 辻本 泰隆

審判官 須田 勝巳

(56)参考文献 特表2007-531941(JP, A)

米国特許出願公開第2011/0106802(US, A1)

特表2010-524083(JP, A)

国際公開第2011/111532(WO, A1)

特開2011-019129(JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F21/62

G06F12/00