(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2025-518495
(P2025-518495A)
(43)公表日　令和7年6月17日(2025.6.17)

(51)国際特許分類　FI
G06F 21/62 (2013.01)　G06F 21/62 318
H04L 67/562 (2022.01)　H04L 67/562

審査請求　未請求　予備審査請求　未請求　（全42頁）

(21)出願番号　特願2024-566592(P2024-566592)
(86)(22)出願日　令和5年5月2日(2023.5.2)
(85)翻訳文提出日　令和6年12月12日(2024.12.12)
(86)国際出願番号　PCT/US2023/020663
(87)国際公開番号　WO2023/219829
(87)国際公開日　令和5年11月16日(2023.11.16)
(31)優先権主張番号　17/742,472
(32)優先日　令和4年5月12日(2022.5.12)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,CV,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV
最終頁に続く

(71)出願人　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 ９４０６５ カリフォルニア州 レッドウッド ショアーズ，メール ストップ ５オーピー７ オラクル パークウェイ ５００
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　カレイ，ハルシット・クマール
アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・ショアーズ、メール・ストップ・５・オー・ピー・７、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレ
最終頁に続く

(54)【発明の名称】　インタークラウドサービスゲートウェイ

(57)【要約】
本明細書では、ソースクラウド環境にデプロイされたリソースに対して、ターゲットクラウド環境で提供されるサービスへのアクセスを容易にするフレームワークについて考察する。ソースクラウド環境は、ターゲットクラウド環境に対して異なり、独立している。ソースクラウド環境で実行されるコンピュートインスタンスが、ターゲットクラウド環境で提供されるサービスを使用する要求を生成する。要求は、ソースクラウド環境からインタークラウドサービスゲートウェイを介してターゲットクラウド環境に送信される。サービスは、コンピュートインスタンスに関連付けられたアクセスロールに基づき、ターゲットクラウド環境で実行される。

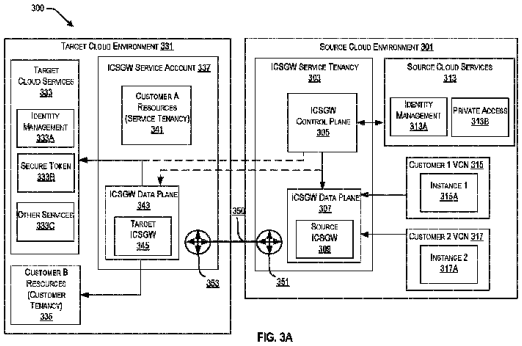


FIG. 3A

【特許請求の範囲】
【請求項１】
方法であって、
ソースクラウド環境で実行されるコンピュートインスタンスが、ターゲットクラウド環境で提供されるサービスを使用するための要求を生成することを含み、
前記ソースクラウド環境は、前記ターゲットクラウド環境とは異なり、
前記方法は、
前記要求を前記ソースクラウド環境からインタークラウドサービスゲートウェイを介して前記ターゲットクラウド環境に送信することと、
前記コンピュートインスタンスに関連付けられたアクセスロールに基づいて、前記ターゲットクラウド環境において前記サービスを実行することとをさらに含む、方法。
【請求項２】
前記方法は、前記コンピュートインスタンスが、前記ソースクラウド環境に配置されたソースインタークラウドサービスゲートウェイに前記要求を送信することをさらに含み、
前記要求は、前記コンピュートインスタンスに関連付けられたアイデンティティプリンシパルを含み、
前記方法は、前記ソースインタークラウドサービスゲートウェイが、前記コンピュートインスタンスの前記アイデンティティプリンシパルを検証することをさらに含む、請求項１に記載の方法。
【請求項３】
前記アイデンティティプリンシパルを検証することは、前記コンピュートインスタンスが前記ターゲットクラウド環境における前記サービスにアクセスすることが許可されているか否かを検証することを含む、請求項２に記載の方法。
【請求項４】
前記アイデンティティプリンシパルが成功裏に検証されたことに応答して、前記ソースインタークラウドサービスゲートウェイが、前記ソースクラウド環境に格納された予め構成された情報から、前記コンピュートインスタンスに関連付けられた前記アクセスロールを取得することをさらに含む、請求項２に記載の方法。
【請求項５】
前記方法は、前記アイデンティティプリンシパルが成功裏に検証されたことに応答して、前記ソースインタークラウドサービスゲートウェイが、前記要求を変更して変更された要求を生成することをさらに含み、
前記変更することは、前記要求のメタデータに含まれる前記アイデンティティプリンシパルを除去することと、前記コンピュートインスタンスに関連付けられた前記アクセスロールを前記メタデータに組み込むこととを含み、
前記方法は、前記ソースインタークラウドサービスゲートウェイが、前記変更された要求を、前記ターゲットクラウド環境に配置されたターゲットインタークラウドサービスゲートウェイに送信することをさらに含む、請求項４に記載の方法。
【請求項６】
前記ソースインタークラウドサービスゲートウェイは、前記ソースクラウド環境の第１のデータプレーンに配置され、前記ターゲットインタークラウドサービスゲートウェイは、前記ターゲットクラウド環境の第２のデータプレーンに配置され、前記ソースインタークラウドサービスゲートウェイは、信頼できる通信チャネルを介して前記ターゲットインタークラウドサービスゲートウェイに通信可能に連結される、請求項５に記載の方法。
【請求項７】
前記ターゲットインタークラウドサービスゲートウェイが、前記変更された要求から前記コンピュートインスタンスに関連付けられた前記アクセスロールを抽出することと、
前記ターゲットインタークラウドサービスゲートウェイが、前記ターゲットクラウド環境に含まれる管理サービスから、前記アクセスロールに関連付けられたトークンを取得することとをさらに含む、請求項５に記載の方法。

【請求項８】
前記ターゲットインタークラウドサービスゲートウェイが、前記変更された要求に、前記アクセスロールに関連付けられた前記トークンで署名して、署名付きの変更された要求を形成することと、
前記署名付きの変更された要求を、前記コンピュートインスタンスが使用することを望む前記サービスに転送することとをさらに含む、請求項７に記載の方法。
【請求項９】
前記サービスが、前記トークンに基づいて前記署名付きの変更された要求を検証することと、
成功裏に検証されたことに応答して、前記サービスが前記要求を実行することとをさらに含む、請求項８に記載の方法。
【請求項１０】
特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体であって、前記コンピュータ実行可能命令は、プロセッサによって実行されると、コンピュータシステムに、少なくとも、
ソースクラウド環境で実行されるコンピュートインスタンスによって、ターゲットクラウド環境で提供されるサービスを使用する要求を生成することを実行させ、
前記ソースクラウド環境は、前記ターゲットクラウド環境とは異なり、
前記コンピュータ実行可能命令は、前記コンピュータシステムに、少なくとも、
前記要求を前記ソースクラウド環境からインタークラウドサービスゲートウェイを介して前記ターゲットクラウド環境に送信することと、
前記コンピュートインスタンスに関連付けられたアクセスロールに基づいて、前記ターゲットクラウド環境において前記サービスを実行することとをさらに実行させる、コンピュータ可読媒体。
【請求項１１】
前記コンピュータシステムは、前記コンピュートインスタンスによって、前記ソースクラウド環境に配置されたソースインタークラウドサービスゲートウェイに前記要求を送信するようにさらに構成されており、
前記要求は、前記コンピュートインスタンスに関連付けられたアイデンティティプリンシパルを含み、
前記コンピュータシステムは、前記ソースインタークラウドサービスゲートウェイによって、前記コンピュートインスタンスの前記アイデンティティプリンシパルを検証するようにさらに構成されている、請求項１０に記載の特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体。
【請求項１２】
前記アイデンティティプリンシパルを検証することは、前記コンピュートインスタンスが前記ターゲットクラウド環境における前記サービスにアクセスすることが許可されているか否かを検証することを含む、請求項１１に記載の特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体。
【請求項１３】
前記コンピュータシステムは、前記アイデンティティプリンシパルが成功裏に検証されたことに応答して、前記ソースインタークラウドサービスゲートウェイによって、前記ソースクラウド環境に格納された予め構成された情報から、前記コンピュートインスタンスに関連付けられた前記アクセスロールを取得するようにさらに構成されている、請求項１１に記載の特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体。
【請求項１４】
前記コンピュータシステムは、前記アイデンティティプリンシパルが成功裏に検証されたことに応答して、前記ソースインタークラウドサービスゲートウェイによって前記要求を変更して変更された要求を生成するようにさらに構成され、
前記変更することは、前記要求のメタデータに含まれる前記アイデンティティプリンシ

パルを除去し、前記コンピュートインスタンスに関連付けられた前記アクセスロールを前記メタデータに組み込むことを含み、
前記コンピュータシステムは、前記ソースインタークラウドサービスゲートウェイによって、前記変更された要求を、前記ターゲットクラウド環境に配置されたターゲットインタークラウドサービスゲートウェイに送信するようにさらに構成されている、請求項１３に記載の特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体。
【請求項１５】
前記ソースインタークラウドサービスゲートウェイは、前記ソースクラウド環境の第１のデータプレーンに配置され、前記ターゲットインタークラウドサービスゲートウェイは、前記ターゲットクラウド環境の第２のデータプレーンに配置され、前記ソースインタークラウドサービスゲートウェイは、信頼できる通信チャネルを介して前記ターゲットインタークラウドサービスゲートウェイに通信可能に連結される、請求項１４に記載の特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体。
【請求項１６】
前記コンピュータシステムは、
前記ターゲットインタークラウドサービスゲートウェイによって、前記変更された要求から前記コンピュートインスタンスに関連付けられた前記アクセスロールを抽出し、
前記ターゲットインタークラウドサービスゲートウェイによって、前記ターゲットクラウド環境に含まれる管理サービスから、前記アクセスロールに関連付けられたトークンを取得するようにさらに構成されている、請求項１４に記載の特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体。
【請求項１７】
前記コンピュータシステムは、
前記ターゲットインタークラウドサービスゲートウェイによって、前記変更された要求に、前記アクセスロールに関連付けられた前記トークンで署名して、署名付きの変更された要求を形成し、
前記署名付きの変更された要求を、前記コンピュートインスタンスが使用することを望む前記サービスに転送するようにさらに構成されている、請求項１６に記載の特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体。
【請求項１８】
システムであって、
プロセッサと、
命令を含むメモリとを備え、
前記命令は、前記プロセッサで実行されると、前記システムに、少なくとも、
ソースクラウド環境で実行されるコンピュートインスタンスによって、ターゲットクラウド環境で提供されるサービスを使用する要求を生成することを実行させ、
前記ソースクラウド環境は、前記ターゲットクラウド環境とは異なり、
前記命令は、前記システムに、少なくとも、
前記要求を前記ソースクラウド環境からインタークラウドサービスゲートウェイを介して前記ターゲットクラウド環境に送信することと、
前記コンピュートインスタンスに関連付けられたアクセスロールに基づいて、前記ターゲットクラウド環境において前記サービスを実行することとをさらに実行させる、システム。
【請求項１９】
前記システムは、前記コンピュートインスタンスによって、前記ソースクラウド環境に配置されたソースインタークラウドサービスゲートウェイに前記要求を送信するようにさらに構成され、
前記要求は、前記コンピュートインスタンスに関連付けられたアイデンティティプリンシパルを含み、
前記システムは、前記ソースインタークラウドサービスゲートウェイによって、前記コ

ンピュートインスタンスの前記アイデンティティプリンシパルを検証するようにさらに構成されている、請求項１８に記載のシステム。
【請求項２０】
前記コンピュートインスタンスが前記ターゲットクラウド環境における前記サービスにアクセスすることが許可されているか否かを検証することによって、前記アイデンティティプリンシパルを検証するように構成されている、請求項１９に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、２０２２年5月１２日に出願された米国特許出願第１７／７４２，４７２号の出願日の利益を主張するものであり、その出願の内容は、あらゆる目的のために参照によりその全体が本明細書に組み込まれる。
【０００２】
分野
本開示は、第２のクラウド環境（例えば、第２のパブリッククラウド）にデプロイされたリソースに対して、第１のクラウド環境（例えば、第１のパブリッククラウド）で提供されるサービスへのアクセスを容易にするフレームワークを提供するインタークラウドサービスゲートウェイに関する。サービスへのアクセスは、２つのクラウド環境間でリソースに関連付けられたアイデンティティプリンシパル（例えば、証明書またはクレデンシャル）を交換することも共有することもなく提供される。
【背景技術】
【０００３】
背景
パブリッククラウドのユーザまたは顧客は、さまざまなクラウドサービスプロバイダから最高級のサービスにアクセスしたいと望む。クラウド環境では、このようなサービス設計の現行のパラダイムは、クラウド環境によって提供されるローカルサービスの上に構築することを奨励している。クロスクラウドまたはインタークラウドのサービスアクセスは、容易には利用可能ではない。そのため、ユーザは、第１のクラウド環境から、第１のクラウド環境とは異なる独立した第２のクラウド環境で提供されるサービスにアクセスするために、独自の特注のソリューションを設計する。別のクラウドサービスプロバイダによって提供されるサービスにアクセスすることができるように設計された典型的なソリューションは、時間がかかり、エラーが発生しやすく、費用がかかる。さらに、典型的なアクセスソリューションの主な欠点のうちの１つは、クレデンシャル管理にある。具体的には、第２のクラウド環境にデプロイされたリソースから、第１のクラウド環境で提供されるサービスにアクセスするには、２つのクラウド環境間のネットワーク接続をセットアップする必要がある。このようなフレームワークでは、第１のクラウド環境のサービスにアクセスするには、ユーザは、クラウドインフラストラクチャにわたって自身のクレデンシャルを配布する必要がある。このようなソリューションは本質的に安全ではなく、不都合である。
【０００４】
本明細書に記載する実施形態は、異なるクラウド環境間でのアプリケーションの移行に関連するこれらおよび他の問題に対処する。
【発明の概要】
【課題を解決するための手段】
【０００５】
概要
本開示は、概して、第２のクラウド環境（例えば、第２のパブリッククラウド）にデプロイされたリソースに対して、第１のクラウド環境（例えば、第１のパブリッククラウド）で提供されるサービスへのアクセスを容易にするフレームワークを提供するインターク

ラウドサービスゲートウェイに関する。サービスへのアクセスは、２つのクラウド環境間でリソースに関連付けられたアイデンティティプリンシパル（例えば、証明書またはクレデンシャル）を交換または共有することなく提供される。本明細書では、方法、システム、１つまたは複数のプロセッサによって実行可能なプログラム、コード、または命令を格納する非一時的コンピュータ可読記憶媒体などを含む、さまざまな実施形態について説明する。これらの例示的な実施形態は、本開示を限定または定義するためではなく、本開示の理解を助ける例を提供するために言及する。追加の実施形態については、詳細な説明のセクションで考察し、そこでは、さらなる説明を提供する。

【０００６】

本開示の一態様は、方法であって、ソースクラウド環境で実行されるコンピュートインスタンスが、ターゲットクラウド環境で提供されるサービスを使用する要求を生成することを含み、ソースクラウド環境は、ターゲットクラウド環境とは異なり、方法は、要求をソースクラウド環境からインタークラウドサービスゲートウェイを介してターゲットクラウド環境に送信することと、コンピュートインスタンスに関連付けられたアクセスロールに基づいて、ターゲットクラウド環境においてサービスを実行することと、をさらに含む、方法を提供する。

【０００７】

本開示の別の態様は、プロセッサによって実行されると、コンピュータシステムに、少なくとも、ソースクラウド環境で実行されるコンピュートインスタンスによって、ターゲットクラウド環境で提供されるサービスを使用する要求を生成することをさせ、ソースクラウド環境は、ターゲットクラウド環境とは異なり、要求をソースクラウド環境からインタークラウドサービスゲートウェイを介してターゲットクラウド環境に送信することと、コンピュートインスタンスに関連付けられたアクセスロールに基づいて、ターゲットクラウド環境においてサービスを実行することと、をさせる特定のコンピュータ実行可能命令を格納するコンピュータ可読媒体を提供する。

【０００８】

本開示の１つの態様は、システムであって、プロセッサと、プロセッサで実行されると、システムに、少なくとも、ソースクラウド環境で実行されるコンピュートインスタンスによって、ターゲットクラウド環境で提供されるサービスを使用する要求を生成することをさせ、ソースクラウド環境は、ターゲットクラウド環境とは異なり、要求をソースクラウド環境からインタークラウドサービスゲートウェイを介してターゲットクラウド環境に送信することと、コンピュートインスタンスに関連付けられたアクセスロールに基づいて、ターゲットクラウド環境においてサービスを実行することと、をさせる命令を含むメモリとを備える、システムを提供する。

【０００９】

上述したことは、他の特徴および実施形態とともに、以下の明細書、特許請求の範囲、および添付図面を参照することにより、より明らかとなろう。

【図面の簡単な説明】

【００１０】

【図１】さまざまな実施形態による、インタークラウドサービスゲートウェイ（ＩＣＳＧＷ：intercloud service gateway）の例示的な高レベルアーキテクチャを示す図である。

【図２】さまざまな実施形態による、インタークラウドサービスゲートウェイ（ＩＣＳＧＷ）によって実行されるプロセスを示すフロー図である。

【図３Ａ】さまざまな実施形態による、インタークラウドサービスゲートウェイ（ＩＣＳＧＷ）の詳細なアーキテクチャを示す図である。

【図３Ｂ】いくつかの実施形態による、ソースインタークラウドサービスゲートウェイによって実行されるプロセスを示すフロー図である。

【図３Ｃ】いくつかの実施形態による、ターゲットインタークラウドサービスゲートウェイによって実行されるプロセスを示すフロー図である。

【図４Ａ】いくつかの実施形態による、ターゲットクラウド環境で提供されるサービスを利用してソースクラウド環境で実行されるコンピュートインスタンスの例示的なプロセスを示す図である。
【図４Ｂ】いくつかの実施形態による、ターゲットクラウド環境で提供されるサービスを利用してソースクラウド環境で実行されるコンピュートインスタンスの別の例示的なプロセスを示す図である。
【図５】少なくとも１つの実施形態による、サービスとしてのクラウドインフラストラクチャシステムを実装するための１つのパターンを示すブロック図である。
【図６】少なくとも１つの実施形態による、サービスとしてのクラウドインフラストラクチャシステムを実装するための別のパターンを示すブロック図である。
【図７】少なくとも１つの実施形態による、サービスとしてのクラウドインフラストラクチャシステムを実装するための別のパターンを示すブロック図である。
【図８】少なくとも１つの実施形態による、サービスとしてのクラウドインフラストラクチャシステムを実装するための別のパターンを示すブロック図である。
【図９】少なくとも１つの実施形態による、コンピュータシステム例を示すブロック図である。
【発明を実施するための形態】
【００１１】
詳細な説明
以下の説明では、さまざまな実施形態について説明する。説明の目的で、実施形態が完全に理解されるために、具体的な構成および詳細について示す。しかしながら、具体的な詳細なしにそれらの実施形態を実施することができることも当業者には明らかとなろう。さらに、説明している実施形態を不明瞭にしないために、周知の特徴は簡略化することがある。
【００１２】
クラウドコンピューティングにおいて、クラウドとは、クラウドの顧客が通信ネットワーク、例えばインターネットを介してアクセスするサーバの集合体である。顧客に対して種々のサービスを提供するクラウドサービスプロバイダ（ＣＳＰ）がクラウドのインフラストラクチャを管理する。対照的に、一般的なマルチクラウド環境は、いくつかのクラウドインフラストラクチャの使用に関連し、インフラストラクチャの各々は、一意のＣＳＰによって管理されている。マルチクラウドデプロイメントには多くの用途がある。マルチクラウドデプロイメントでは、複数のサービスとしてのインフラストラクチャ（ＩａａＳ：Infrastructure-as-a-Service）ベンダーを活用することができ、または、ＩａａＳサービス、サービスとしてのプラットフォーム（ＰａａＳ：Platform-as-a-Service）サービス、およびサービスとしてのソフトウェア（ＳａａＳ：Software-as-a-Service）サービスに異なるベンダーを使用することができる。マルチクラウドは、単に冗長性およびシステムバックアップを目的とすることができ、または、マルチクラウドデプロイメントは、異なるサービスに対して異なるクラウドベンダーを組み込むことができる。
【００１３】
今日まで、大部分のマルチクラウドソリューションは、主にネットワークアクセスを簡略化することに焦点を当ててきた。異なるＣＳＰにアカウントを有するユーザまたは顧客は、アイデンティティフェデレーション、すなわちユーザのアイデンティティフェデレーションに基づいて、異なるクラウド内のリソースにアクセスすることができる。具体的には、アイデンティティフェデレーションは、ユーザを認証し、ユーザによるリソースへのアクセスを許可するために必要な情報を伝達する目的で、２者間の信頼を確立するシステムである。しかしながら、このようなフレームワークは、必然的に、リソース（すなわち、コンピュートインスタンス、ＶＭ、関数などの非ユーザアクター）間で信頼を確立することにまで拡張しない。
【００１４】
さらに、可能な限り、顧客は、コンピュートワークロード（すなわち、ＶＭ、コンテナ

、関数）からクラウドサービスへの自身のトラフィックをプライベートに保つことを好み、これらのコンピュートワークロードへの自身の長期間のクレデンシャルの配布を避けることを好む。顧客は、このタイプの通信を実現することができるが、ただし、それは、それぞれのクラウドが提供する環境内、すなわち、単一のクラウド環境内でのみである。目下、インタークラウド環境において同様の通信モードを実現するメカニズムはない。本開示の実施形態は、顧客が、あるクラウド環境（例えば、第１のＣＳＰによって管理されるクラウド環境）における自身のコンピュートワークロードまたはコンピュートインスタンスを、より安全な方法で異なるクラウド環境（すなわち、第２のＣＳＰによって管理されるクラウド環境）のサービスにアクセスするように構成するために使用することができる、フレームワークを提供することを目的とする、インタークラウドサービスゲートウェイ（ＩＣＳＧＷ）を提供する。

【００１５】

図１は、さまざまな実施形態によるインタークラウドサービスゲートウェイ（ＩＣＳＧＷ）の例示的な高レベルアーキテクチャを示す。図１に示す高レベルアーキテクチャ１００は、ソースクラウド環境１０１とターゲットクラウド環境１０７との間にシームレスに配置されたマルチテナンシサービスである、インタークラウドサービスゲートウェイ１０５を含む。具体的には、ＩＣＳＧＷ１０５は、ソースクラウド環境１０１およびターゲットクラウド環境１０７の両方にフットプリントを有する。

【００１６】

ソースクラウド環境１０１は、１つまたは複数のコンピュートインスタンス１０２（例えば、仮想マシン（ＶＭ）、コンテナ、関数）をホストする１つまたは複数の顧客仮想クラウドネットワーク（例えば、顧客ＶＣＮ１０３）を含む。このようなコンピュートインスタンス１０２は、ＩＣＳＧＷ１０５を介して、ターゲットクラウド環境１０７によって提供されるサービス１０９を利用することができる。ターゲットクラウド環境１０７によって提供されるサービス１０９は、ターゲットクラウド環境１０７にテナンシ（すなわち、ターゲットクラウド環境１０７における顧客アカウント）を有する顧客だけでなく、ターゲットクラウド環境１０７に顧客テナンシを有していない顧客によっても利用することができることが理解される。

【００１７】

いくつかの実施形態によれば、コンピュートワークロード（例えば、ソースクラウド環境１０１におけるコンピュートインスタンス１０２）が、ソースクラウド環境１０１においてローカルに利用可能なアイデンティティプリンシパル（すなわち、リソースのアイデンティティに対応するリソースプリンシパル）を用いて、ターゲットクラウド環境におけるターゲットサービス１０９にアクセスするとき、ＩＣＳＧＷ１０５サービスは、アクションのセットを実行する。１つの実施態様では、アクションのセットは、少なくとも、（ｉ）コンピュートワークロードとターゲットサービスとの間の要求／応答をインターセプトすることと、（ｉｉ）コンピュートインスタンスに関連付けられたアイデンティティプリンシパルを検証することと、（ｉｉｉ）アイデンティティプリンシパルをターゲットクラウド環境におけるコンピュートインスタンスのアクセスロールに変換することと、（ｉｖ）要求をターゲットクラウド環境における最終宛先（例えば、所望のサービス）に転送することとを含む。言い換えれば、ソースクラウド環境におけるコンピュートインスタンス１０２は、ターゲットクラウド環境におけるサービス１０９にアクセスする要求を生成する。要求は、ソースクラウド環境１０１からセキュア通信チャネルを介してターゲットクラウド環境１０７にさらに通信される。サービスは、ソースクラウド環境１０１におけるコンピュートインスタンスに関連付けられたアクセスロール（すなわち、１つまたは複数の権限）に基づいて、ターゲットクラウド環境１０７において実行される。さらに、ＩＣＳＧＷ１０５のアーキテクチャに関する詳細と、ソースクラウド環境におけるコンピュートインスタンスによって使用される（ターゲットクラウド環境における）サービスを開始するプロセスについては、図３Ａ～図３Ｃを参照して後に詳細に説明する。

【００１８】

図２は、さまざまな実施形態によるインタークラウドサービスゲートウェイ（ＩＣＳＧＷ）によって実行されるプロセスを示す高レベルフロー図を示す。具体的には、図２は、ソースクラウド環境で実行されるコンピュートインスタンス（例えば、仮想マシン、コンテナ、関数）が、ＩＣＳＧＷを介して、ターゲットクラウド環境で提供されるサービスにアクセスするためにプロビジョニングするステップを例示するプロセスを示す。図２に示す処理は、それぞれのシステム、ハードウェア、またはそれらの組み合わせの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）で実装することができる。ソフトウェアは、非一時的記憶媒体に（例えば、メモリデバイスに）格納することができる。図２に提示し、以下に説明する方法は、例示的であり非限定的であるように意図されている。図２は、さまざまな処理ステップが特定のシーケンスまたは順序で発生するように示すが、これは限定的であるように意図されていない。いくつかの代替実施形態では、ステップを何らかの異なる順序で実行してもよく、または、いくつかのステップを並行して実行してもよい。

【００１９】

プロセスはステップ２０１で開始し、そこでは、ソースクラウド環境で実行されるコンピュートインスタンス（例えば、ソースクラウド環境における顧客ＶＣＮで実行されるコンピュートインスタンス）が、ターゲットクラウド環境で提供されるサービスを使用する要求を生成する。ターゲットクラウド環境は、ソースクラウド環境とは異なり、独立していることが留意される。

【００２０】

ステップ２０３において、コンピュートインスタンスによって生成された要求は、ソースクラウド環境からインタークラウドサービスゲートウェイを介してターゲットクラウド環境に通信される。具体的には、図３Ａを参照して後述するように、要求は、信頼できる通信チャネル（例えば、Ｆａｓｔｃｏｎｎｅｃｔ通信チャネル）を介して通信可能に連結されている、（ソースクラウド環境にデプロイされている）ソースインタークラウドサービスゲートウェイから（ターゲットクラウド環境にデプロイされている）ターゲットインタークラウドサービスゲートウェイに通信される。要求がターゲットクラウド環境に送信されると、ステップ２０５において、コンピュートインスタンスに関連付けられたアクセスロールに基づいて、ターゲットクラウド環境においてサービスが実行される。

【００２１】

ここで図３Ａを参照すると、さまざまな実施形態によるインタークラウドサービスゲートウェイ（ＩＣＳＧＷ）の詳細なアーキテクチャが図示されている。ＩＣＳＧＷは、第２のパブリッククラウド（すなわち、本明細書ではソースクラウド環境と称する）にデプロイされたリソースに対して、第１のパブリッククラウド（すなわち、本明細書ではターゲットクラウド環境と称する）で提供されるサービスへのアクセスを、それら２つのクラウド環境にわたってアイデンティティプリンシパルを共有することなく容易にするサービスのフレームワークを提供する。

【００２２】

ＩＣＳＧＷのアーキテクチャ３００は、ソースクラウド環境３０１およびターゲットクラウド環境３３１を含む。ソースクラウド環境３０１は、ＩＣＳＧＷサービステナンシ３０３と、ソースクラウドサービス３１３と、１つまたは複数の顧客仮想クラウドネットワーク（ＶＣＮ）（例えば、顧客１ＶＣＮ３１５、顧客２ＶＣＮ３１７）とを含む。ＩＣＳＧＷサービステナンシ３０３は、コントロールプレーンコンポーネント（すなわち、ＩＣＳＧＷコントロールプレーン３０５）と、データプレーンコンポーネント（すなわち、ＩＣＳＧＷデータプレーン３０７）とを含む。ＩＣＳＧＷデータプレーン３０７において、ソースＩＣＳＧＷ３０９がホストされる。ソースクラウドサービス３１３は、アイデンティティおよび管理サービス３１３Ａ、およびプライベートアクセスサービス３１３Ｂを含む、複数のサービスを含む。顧客ＶＣＮの各々は、そこで実行されるコンピュートインスタンスを含む（例えば、顧客１ＶＣＮ３１５はコンピュートインスタンス３１５Ａを含み、顧客２ＶＣＮ３１７は別のコンピュートインスタンス３１７Ａを含む）。

【００２３】
ターゲットクラウド環境３３１は、ＩＣＳＧＷサービスアカウント（またはサービステナンシ）３３７およびターゲットクラウドサービス３３３を含む。ＩＣＳＧＷサービスアカウント３３７は、ターゲットＩＣＳＧＷ３４５をホストするデータプレーンコンポーネント（すなわち、ＩＣＳＧＷデータプレーン３４３）を含む。ターゲットクラウドサービスは、アイデンティティ管理３３３Ａ、セキュアトークンサービス３３３Ｂ、および他のサービス３３３Ｃ（例えば、キューサービス、ストレージサービス）などのサービスを含むことができる。ソースクラウド環境３０１は、信頼できる、高帯域幅で低レイテンシの通信リンク３５０（例えば、ＦａｓｔＣｏｎｎｅｃｔ通信リンク）を介して、ターゲットクラウド環境３３１に通信可能に連結されている。具体的には、１つの実施形態によって、信頼できる通信リンク３５０は、（ソースクラウド環境３０１のデータプレーン３０７に配置されている）ソースＩＣＳＧＷ３０９を、一対のルータ（例えば、高速接続対応ダイナミックルーティングゲートウェイ（ＤＲＧ：dynamic routing gateway））を介して（ターゲットクラウド環境３３１のデータプレーン３４３に配置されている）ターゲットＩＣＳＧＷ３４５に接続することによって確立される。例えば、図３Ａに示すように、ソースクラウド環境３０１におけるＩＣＳＧＷサービステナンシ３０３は、ターゲットクラウド環境３３１のＩＣＳＧＷサービステナンシ３３７に含まれる第２の高速接続対応ＤＲＧ３５３に通信可能に連結される、第１の高速接続対応ＤＲＧ３５１を含む。

【００２４】
ソースＩＣＳＧＷ３０９は、ターゲットＩＣＳＧＷ３４５と連携して、ソースクラウド環境３０１において実行されるコンピュートインスタンス（例えば、コンピュートインスタンス３１５Ａおよび３１７Ａ）がターゲットクラウド環境３３１において提供されるサービス（例えば、他のサービス３３３Ｃ）にアクセスするのを容易にするフレームワークを提供する。ターゲットクラウド環境３３１で提供されるサービスは、ターゲットクラウド環境３３１にテナンシ（またはアカウント）（例えば、顧客Ｂのテナンシ３３５）を有するソースクラウド環境３０１の顧客だけでなく、ターゲットクラウド環境にテナンシを有していないソースクラウド環境３０１の顧客にとっても利用可能であることが理解される。ターゲットクラウド環境３３１においてテナンシを有していない顧客に対して、ソースクラウド環境３０１のＩＣＳＧＷコントロールプレーン３０５は、ターゲットクラウド環境のＩＣＳＧＷサービスアカウント３３７において顧客のためのリソースグループ（例えば、顧客Ａリソースグループ）をインスタンス化するように構成されていることが留意される。リソースグループは、キュー、ストレージバケット、アクセスロールなどのリソースを含む。図３Ａの上述した実施形態は、決して本開示の範囲を限定するものではないことが理解される。むしろ、インタークラウドサービスゲートウェイ（ＩＣＳＧＷ）のアーキテクチャに対する変更は、本開示の範囲内に十分に含まれる。例えば、いくつかの実施形態によれば、（ソースクラウド環境３０１における）ＩＣＳＧＷデータプレーン３０７は、ソースＩＣＳＧＷのプールを含んでもよく、（ターゲットクラウド環境３３１における）ＩＣＳＧＷデータプレーン３４３は、ターゲットＩＣＳＧＷのプールを含んでもよい。このような設定では、要求をソースクラウド環境３０１からターゲットクラウド環境３３１に送信するために、ソースＩＣＳＧＷのプールからの１つのソースＩＣＳＧＷとともに、ターゲットＩＣＳＧＷのプールからの１つのターゲットＩＣＳＧＷを、いくつかの条件（例えば、システムにおける現在のトラフィック負荷）に基づいて動的に選択することができる。

【００２５】
以下では、ソースクラウド環境で実行されるリソース（例えば、コンピュートインスタンス３１５Ａ）がターゲットクラウド環境３３１におけるサービスにアクセスする方法に関する詳細な説明を提供する。動作時、ターゲットクラウド環境３３１におけるサービスおよびソースクラウド環境３０１におけるリソースへのアクセスを容易にするプロセスは、動作の２つのフェーズ、すなわち、セットアップフェーズおよび実行フェーズを含む。セットアップフェーズでは、ソースクラウド環境において動的グループが作成される。動

的グループは、ユーザをユーザグループにグループ化するのと同様の方法で、プリンシパルアクターとしてコンピュートインスタンスのグループ化を提供する。セットアップフェーズでは、動的グループ内のコンピュートインスタンスがターゲットクラウド環境からサービスを取得するためのＡＰＩ呼び出しを発行することを許可するポリシーが作成される。動的グループ内のメンバーシップは、マッチングルールと称する基準のセットによって決定することができる。マッチングルールを満たすクラウドインフラストラクチャリソース（例えば、コンピュートインスタンス）は、動的グループのメンバーとして含まれる。

【００２６】

さらに、セットアップフェーズでは、各動的グループには、その動的グループのメンバーがターゲットクラウド環境において想定することができる権限のセットに対応するロール（本明細書ではアクセスロールと称する）が割り当てられる。さらに、セットアップフェーズでは、顧客は、顧客がターゲットクラウド環境においてテナンシ（すなわち、アカウント）を有するか否かに関する情報を提供することができる。このような情報としては、ターゲットクラウド環境の識別子、ターゲットクラウド環境のリージョン、ターゲットクラウド環境における顧客のテナンシのアカウントＩＤなどを挙げることができる。顧客がターゲットクラウド環境においてテナンシを有していない場合、（ソースクラウド環境３０１に含まれる）ＩＣＳＧＷコントロールプレーン３０５は、セットアップフェーズにおいて、顧客のためのリソースグループ（例えば、顧客Ａリソースグループ３４１）を確立することができることが理解される。リソースグループは、ターゲットクラウド環境３３１のＩＣＳＧＷサービスアカウント３３７に作成されることが留意される。

【００２７】

いくつかの実施形態によれば、セットアップフェーズでは、ソースクラウド環境３０１のＩＣＳＧＷコントロールプレーン３０５は、プライベートアクセスサービス３１３Ｂを利用して、ソースクラウド環境の顧客テナンシにおける顧客ＶＣＮ（例えば、顧客１ＶＣＮ３１５、顧客２ＶＣＮ３１７）とＩＣＳＧＷデータプレーン３０７との間のプライベート接続を提供する。さらに、ＩＣＳＧＷコントロールプレーン３０５は、ＶＣＮ／ＤＮＳインフラストラクチャサービスを利用して、顧客ＶＣＮにおいて、ターゲットクラウド環境におけるサービス宛ての顧客トラフィックをＩＣＳＧＷデータプレーン３０７に再ルーティングするようにドメインネームシステム（ＤＮＳ）リゾルバをプログラムすることができる。

【００２８】

実行フェーズでは、顧客ＶＣＮにおいて実行されるコンピュートインスタンス（例えば、コンピュートインスタンス３１５Ａ）は、ターゲットクラウド環境３３１において提供されるサービスの使用を要求する要求を送信する。このような要求は、ソースＩＣＳＧＷ３０９によってインターセプトされる。１つの実施態様では、要求は、コンピュートインスタンスに関連付けられたアイデンティティプリンシパル（例えば、証明書またはクレデンシャル）を含む。ソースＩＣＳＧＷは、要求からアイデンティティプリンシパルを抽出し、コンピュートインスタンスに関連付けられた許可の検証を実行する。例えば、ソースＩＣＳＧＷ３０９は、ソースクラウド環境３０１のアイデンティティ管理サービス３１３Ａと通信して、特定のコンピュートインスタンスが、ターゲットクラウド環境によって提供されるサービスを要求する要求を発行することが許可されているか否かを検証する。

【００２９】

成功裏に検証されると、ソースＩＣＳＧＷ３０９は、（すなわち、セットアップフェーズにおいて）コンピュートインスタンスに対して予め構成されたアクセスロールを取得する。次いで、ソースＩＣＳＧＷ３０９は、コンピュートインスタンスから受信した要求を変更し、この変更された要求を、ターゲットクラウド環境に含まれるターゲットＩＣＳＧＷ３４５に転送する。変更された要求は、セットアップフェーズで確立された信頼できる通信チャネル（例えば、通信チャネル３５０）を介して、ソースクラウド環境３０１からターゲットクラウド環境に通信されることに留意されたい。１つの実施態様では、ソースＩＣＳＧＷ３０９は、要求からアイデンティティプリンシパルを取り除き（すなわち、除

去し）、要求にアクセスロールを組み込んで変更された要求を形成することによって、要求を変更する。このように、ソースクラウド環境３０１のリソースに関連付けられたアイデンティティプリンシパルがターゲットクラウド環境３３１に送信されないことが確実になる。

【００３０】

ターゲットＩＣＳＧＷ３４５は、ソースＩＣＳＧＷ３０９によって送信された変更された要求を受信すると、変更された要求に含まれる（コンピュートインスタンスに関連付けられた）アクセスロールを抽出する。１つの実施形態では、ターゲットＩＣＳＧＷ３４５は、管理サービス（例えば、ターゲットクラウド環境３３１に含まれるアイデンティティ管理サービス３３３Ａまたはセキュアトークンサービス３３３Ｂ）と通信して、コンピュートインスタンスのアクセスロールに関連付けられたクレデンシャル（例えば、トークン）を取得する。ターゲットＩＣＳＧＷ３４５は、変更された要求に、取得されたクレデンシャルで署名し、署名付き要求を、コンピュートインスタンスが使用することを望むサービス（例えば、サービス３３３Ｃ）に転送する。１つの実施形態では、望まれるサービスは、ターゲットクラウド環境３３１の管理サービス（例えば、アイデンティティ管理サービス３３３Ａ）と通信して、要求に署名するために使用されたクレデンシャルが、要求されたアクションを実行するのに十分な権限を有しているか否かを判定することができる。成功裏に検証されると、サービスは、ターゲットクラウド環境３３１に含まれる顧客のテナンシで実行される。すなわち、要求は、（顧客がターゲットクラウド環境にテナンシを有している場合）顧客Ｂテナンシ３３５で実行され、または、要求は、（顧客がターゲットクラウド環境に独自のテナンシを有していない場合）顧客Ａリソースグループ３４１で実行される。

【００３１】

図３Ｂは、いくつかの実施形態によるソースインタークラウドサービスゲートウェイ（ＩＣＳＧＷ）によって実行されるプロセスを示すフロー図を示す。図３Ｂに示す処理は、それぞれのシステム、ハードウェア、またはそれらの組み合わせの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）で実装することができる。ソフトウェアは、非一時的記憶媒体に（例えば、メモリデバイスに）格納することができる。図３Ｂに提示し、以下に説明する方法は、例示的であり非限定的であるように意図されている。図３Ｂは、さまざまな処理ステップが特定のシーケンスまたは順序で発生するように示すが、これは限定的であるようには意図されていない。いくつかの代替実施形態では、ステップを異なる順序で実行してもよく、または、いくつかのステップを並行して実行してもよい。

【００３２】

プロセスはステップ３６１で開始し、そこで、ソースＩＣＳＧＷは、ソースクラウド環境で実行されるコンピュートインスタンスから要求を受信する。要求は、ターゲットクラウド環境によって提供されるサービスの使用を要求するコンピュートインスタンスに対応する。１つの実施態様では、要求は、コンピュートインスタンスに関連付けられたアイデンティティプリンシパル（例えば、証明書またはクレデンシャル）を含む。ステップ３６３において、ソースＩＣＳＧＷは、要求からアイデンティティプリンシパルを抽出し、コンピュートインスタンスに関連付けられた許可の検証を実行する。例えば、ソースＩＣＳＧＷは、特定のコンピュートインスタンスが、ターゲットクラウド環境によって提供されるサービスを要求する要求を発行することが許可されているか否かを検証する。

【００３３】

ステップ３６５において、ソースＩＣＳＧＷは、コンピュートインスタンスに関連付けられたアイデンティティプリンシパルに関連付けられた許可の検証が成功するか否かを判定するために、クエリを実行する。クエリに対する応答が肯定である（すなわち、コンピュートインスタンスが、ターゲットクラウド環境によって提供されるサービスを要求することが許可されている）場合、プロセスはステップ３６７に移る。しかしながら、ステップ３６５におけるクエリに対する応答が否定である（すなわち、コンピュートインスタン

スが、ターゲットクラウド環境によって提供されるサービスを要求することが許可されていない）場合、プロセスはステップ３６６に移る。ソースＩＣＳＧＷは、ソースクラウド環境の管理サービス（例えば、アイデンティティアクセス管理サービス）に従って、コンピュートインスタンスに関連付けられたアイデンティティプリンシパルを検証することができることが理解される。

【００３４】

ステップ３６６において（すなわち、ステップ３６５のクエリに対する応答が否定であると判定すると）、ソースＩＣＳＧＷは、コンピュートインスタンスによって送信された要求に対する応答を提供する。例えば、ソースＩＣＳＧＷは、コンピュートインスタンスのアイデンティティプリンシパルが成功裏に検証されなかったため、ターゲットクラウド環境の要求されたサービスをコンピュートインスタンスに提供することができないこと（すなわち、サービスアクセスの失敗）を示す応答メッセージを、コンピュートインスタンスに送信する。ステップ３６６で応答メッセージを送信すると、図３Ａのプロセスは終了する。

【００３５】

ステップ３６５のクエリに対する応答が肯定であると判定すると、プロセスはステップ３７６に移る。このステップにおいて、ソースＩＣＳＧＷは、予め構成された情報（例えば、セットアップフェーズに関連付けられた情報）から、要求されたサービスに対してコンピュートインスタンスに関連付けられたアクセスロールを取得する。アクセスロールは、ターゲットクラウド環境のコンピュートインスタンスに関連付けられた権限（例えば、読み取り書き込みの権限、読み取りのみの権限）を示す。

【００３６】

次いで、プロセスはステップ３６９に進み、そこで、ソースＩＣＳＧＷは、コンピュートインスタンスから取得された要求を変更して、変更された要求を生成する。１つの実施態様では、ソースＩＣＳＧＷは、コンピュートインスタンスに関連付けられたアイデンティティプリンシパルを要求から除去し、コンピュートインスタンスに関連付けられた（ステップ３６７で取得された）アクセスロールを要求に含めて、変更された要求を生成する。その後、ソースＩＣＳＧＷは、変更された要求をターゲットＩＣＳＧＷに送信する。図３Ａを参照すると、変更された要求は、ソースクラウド環境とターゲットクラウド環境との間に確立される信頼できる通信チャネル３５０を介して、ソースＩＣＳＧＷからターゲットＩＣＳＧＷに送信されることが理解される。

【００３７】

図３Ｃは、いくつかの実施形態によるターゲットインタークラウドサービスゲートウェイ（ＩＣＳＧＷ）によって実行されるプロセスを示すフロー図を示す。図３Ｃに示す処理は、それぞれのシステム、ハードウェア、またはそれらの組み合わせの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）で実行することができる。ソフトウェアは、非一時的記憶媒体に（例えば、メモリデバイスに）格納することができる。図３Ｃに提示し、以下に説明する方法は、例示的であり非限定的であるように意図されている。図３Ｃは、さまざまな処理ステップが特定のシーケンスまたは順序で発生するように示すが、これは限定的であるようには意図されていない。いくつかの代替実施形態では、ステップを何らかの異なる順序で実行してもよく、または、いくつかのステップを並行して実行してもよい。

【００３８】

プロセスはステップ３７１で開始し、そこで、ターゲットＩＣＳＧＷは、ソースＩＣＳＧＷによって送信された変更された要求（すなわち、図３Ｂのステップ３７０においてソースＩＣＳＧＷによって送信された要求）を受信する。ステップ３７３において、ターゲットＩＣＳＧＷは、変更された要求に含まれるアクセスロールを抽出する。次いで、プロセスはステップ３７５に移り、そこで、ターゲットＩＣＳＧＷは、ターゲットクラウド環境に含まれる管理サービス（例えば、図３Ｂのセキュアトークンサービス３３３Ｂ）と通信する。具体的には、ターゲットＩＣＳＧＷは、管理サービスと通信して、コンピュート

インスタンスのアクセスロールに関連付けられたクレデンシャル（例えば、トークン）を取得する。

【００３９】

ステップ３７７において、ターゲットＩＣＳＧＷは、変更された要求に、ステップ３７５で取得されたクレデンシャルで署名し、ステップ３７９において、署名付き要求を、コンピュートインスタンスが使用することを望むサービスに転送する。次いで、プロセスはステップ３８１に移り、そこでは、クレデンシャルの有効性を判定するためにクエリが実行される。例えば、１つの実施態様では、望まれるサービスは、ターゲットクラウド環境の管理サービス（例えば、アイデンティティ管理サービス）と通信して、要求に署名するために使用されたクレデンシャルが、要求されたアクションを実行するのに十分な権限を有しているか否かを判定することができる。ステップ３８１におけるクエリに対する応答が肯定である（すなわち、クレデンシャルがアクションを実行するのに十分な権限を有している）場合、プロセスはステップ３８３に移る。しかしながら、ステップ３８１のクエリに対する応答が否定である場合、プロセスはステップ３８５に移る。

【００４０】

ステップ３８５において、サービスは、サービスが実行する要求されたアクション（例えば、読み取り、書き込み、更新）に対するアクセスの失敗を示すメッセージで応答する。言い換えれば、サービスは、要求されたアクションが、権限が不十分であるために実行することができなかったことを、ターゲットＩＣＳＧＷに通知する。いくつかの実施態様では、ターゲットＩＣＳＧＷは、信頼できる通信チャネルを介して、取得された応答をソースクラウド環境にデプロイされたコンピュートインスタンスに転送することができる。しかしながら、ステップ３８１においてクレデンシャルの成功裏な検証に応答して、プロセスは、ステップ３８３において引き続き、望まれたサービスによる要求を実行する。その後、図３Ｂに示すプロセスは終了する。

【００４１】

ここで図４Ａおよび図４Ｂを参照すると、いくつかの実施形態による、ターゲットクラウド環境で提供されるサービスを利用してソースクラウド環境で実行されるコンピュートインスタンスの例示的なプロセスが図示されている。図４Ａを参照すると、ソースクラウド環境４０１およびターゲットクラウド環境４５１が図示されている。ソースクラウド環境４０１は、２つのアプリケーション（すなわち、アプリケーション１　４０５Ａおよびアプリケーション２　４０５Ｂ）をホストする顧客仮想クラウドネットワーク（すなわち、顧客ＶＣＮ４０３）を含む。さらに、ソースクラウド環境４０１は、ターゲットクラウド環境４５１に含まれるターゲットＩＣＳＧＷ４５９と通信可能に連結されているソースＩＣＳＧＷ４０７を含む。

【００４２】

ターゲットクラウド環境４５１は、ターゲットクラウドサービス４６１、顧客テナンシまたはアカウント４６３、および他のターゲットクラウドサービス４５３を含む。他のターゲットクラウドサービス４５３は、アイデンティティ管理サービス４５３Ａ、セキュアトークンサービス４５３Ｂなどの追加サービスを含むことができる。説明のために、コンピュートインスタンス（すなわち、ソースクラウド環境４０１におけるアプリケーション１　４０５Ａおよびアプリケーション２　４０５Ｂ）が利用することを望む、ターゲットクラウド環境４５１におけるターゲットクラウドサービス４６１は、Ｓ３サービスおよびＳＱＳサービスとして図示されている。Ｓ３サービス（すなわち、シンプルストレージサービス）は、データをオブジェクトとしてバケットに格納するオブジェクトストレージサービスである。オブジェクトは、ファイルと、そのファイルを記述する任意のメタデータとである。バケットは、オブジェクトのためのコンテナである。ＳＱＳ（すなわち、シンプルキューサービス）は、さまざまなサイズの複数のメッセージを非同期で送信、格納、および取得するために使用される、管理されたメッセージキューイングサービスである。

【００４３】

いくつかの実施形態によれば、セットアップフェーズにおいて、ソースクラウド環境に

おいて動的グループが作成される。動的グループは、ユーザをユーザグループにグループ化するのと同様の方法で、プリンシパルアクターとしてのコンピュートインスタンスのグループ化を提供する。セットアップフェーズにおいて、動的グループ内のコンピュートインスタンスがサービスを取得するためのＡＰＩ呼び出しを発行することを許可するポリシーを作成することができる。動的グループ内のメンバーシップは、マッチングルールと称する基準のセットによって決定することができることが理解される。マッチングルールを満たすクラウドインフラストラクチャリソースは、動的グループのメンバーとして含まれる。例えば、図４Ａに示すように、アプリケーション１　４０５Ａは第１の動的グループ（ＤＧ１）に含まれ、アプリケーション２　４０５Ｂは第２の動的グループ（ＤＧ２）に含まれる。

【００４４】

さらに、セットアップフェーズにおいて、各動的グループに、その動的グループのメンバーがターゲットクラウド環境で想定することができる権限のセットに対応するロール（本明細書ではアクセスロールとも称する）を割り当てることができる。例えば、図４Ａに示すように、動的グループ１（ＤＧ１）に属するアプリケーション１　４０５Ａには（ＩＡＭロール１と表記する）第１のロールが割り当てられ、動的グループ２（ＤＧ２）に属するアプリケーション２　４０５Ｂには（ＩＡＭロール２と表記する）第２のロールが割り当てられている。簡単のために、第１のロールに関連付けられた権限は読み取りおよび書き込みの権限に対応し、第２のロールに関連付けられた権限は読み取りのみの権限に対応する。このように構築された動的グループのセットは、図４Ａにおいて点線のボックス４０９に図示されている。図４Ａに示すように、異なる動的グループに割り当てられたロールも、セットアップフェーズにおいて、ターゲットクラウド環境における顧客アカウント４６３にインスタンス化されることが理解される。具体的には、セットアップフェーズにおいて、顧客は、顧客がターゲットクラウド環境において顧客テナンシを有するか否かを指定する。顧客がターゲットクラウド環境における顧客テナンシ（例えば、ターゲットクラウド環境４５１における顧客アカウント４６３）を有している場合、セットアップフェーズにおいて、ターゲットクラウド環境、ターゲットクラウド環境における顧客テナンシ、顧客ＶＣＮの動的グループに割り当てられた異なるロールなどを特定する情報が指定される。

【００４５】

さらに、いくつかの実施形態によって、各動的グループにおけるコンピュートインスタンスは、ターゲットクラウド環境で提供されるサービスに対する要求を、動的グループに関連付けられたエンドポイントに送信するようにプログラムすることができる。エンドポイントは、そうした要求をソースＩＣＳＧＷに転送し、ソースＩＣＳＧＷは、さらに、セキュア通信チャネルを介して要求をターゲットＩＣＳＧＷに転送する。例えば、図４Ａに示すように、ＤＧ１に含まれるアプリケーション１　４０５Ａは、アプリケーションによって発行された要求（すなわち、ターゲットクラウド環境で提供されるサービスを要求する要求）をＩＣＳＧＷ１エンドポイント４０６Ａに転送し、ＤＧ２に含まれるアプリケーション２　４０５Ｂは、アプリケーションによって発行された要求をＩＣＳＧＷ２エンドポイント４０６Ｂに転送する。

【００４６】

以下では、図４Ａを参照して、顧客ＶＣＮ４０３に含まれるコンピュートインスタンスによって発行される、（ターゲットクラウド環境によって提供されるサービスに対する）４つの異なる要求に関連するフローについて詳細に説明する。具体的には、（１．１～１．５と表記するステップを有する）フロー１は、アプリケーション１　４０５Ａが、ファイルをアップロードするためにターゲットクラウド環境におけるＳ３バケットにアクセスする要求を発行するというシナリオに対応する。（２．１～２．５と表記するステップを有する）フロー２は、アプリケーション１　４０５Ａが、メッセージを送信するためにＳＱＳサービスを呼び出す要求を発行するというシナリオに対応する。（３．１～３．５と表記するステップを有する）フロー３は、アプリケーション２　４０５ＢがＳＱＳキュー

をポーリングしてメッセージの存在を判定するというシナリオに対応し、（４．１～４．５と表記するステップを有する）フロー４は、アプリケーション２　４０５Ｂがファイルを読み取る要求を発行するというシナリオに対応する。

【００４７】

フロー１を参照すると、ステップ１．１において、アプリケーション１　４０５Ａは、ファイルをアップロードする要求を発行する。この要求は、ＩＣＳＧＷ１エンドポイント４０６Ａを介してソースＩＣＳＧＷ４０７に転送される。ソースＩＣＳＧＷ４０７は、要求を終了し、検証確認を実行して、アプリケーション１　４０５Ａに関連付けられたアイデンティティプリンシパルがそのような要求を行うことを許可されているか否かを判定する。成功裏に検証されると、ソースＩＣＳＧＷ４０７は、アプリケーション１　４０５Ａに関連付けられたアクセスロール（例えば、ＩＡＭロール１）を要求に含めるように要求を変更する。ソースＩＣＳＧＷ４０７は、ステップ１．２において、変更された要求をターゲットＩＣＳＧＷ４５９に転送する。変更された要求は、ソースクラウド環境４０１とターゲットクラウド環境４５１との間に確立されたセキュア通信チャネル（例えば、ＦａｓｔＣｏｎｎｅｃｔ）を介して転送されることに留意されたい。ステップ１．３において、ターゲットＩＣＳＧＷ４５９は、ソースＩＣＳＧＷ４０７から受信した変更された要求から対応するアクセスロールを抽出する。ターゲットＩＣＳＧＷ４５９は、管理サービス（例えば、ターゲットクラウドサービス４５３に含まれるセキュアトークンサービス４５３Ｂ）と通信して、アクセスロールに関連付けられたクレデンシャルを取得する。ステップ１．４において、ターゲットＩＣＳＧＷ４５９は、変更された要求に（ステップ１．３の）取得されたクレデンシャルで署名し、署名付き要求をサービス（例えば、アプリケーション１　４０５Ａが使用することを望むサービス４６１）に転送する。ステップ１．５において、ターゲットサービス４６１は、（ターゲットＩＣＳＧＷ４５９から取得された）クレデンシャルが、要求されたアクションを実行する（すなわち、ファイルをアップロードする）のに十分な権限に関連付けられているか否かを判定するための確認を実行することができる。さらに、アプリケーション１　４０５Ａは、読み取りおよび書き込みの権限を有するアクセスロールに関連付けられているため、ステップ１．５において、ファイルは、顧客のテナンシ４６３におけるＳ３バケットにアップロードされる。

【００４８】

ここでフロー２を参照すると、ステップ２．１において、アプリケーション１　４０５Ａは、ターゲットクラウド環境におけるＳＱＳサービスを呼び出して（例えば、ＳＱＳキューに）メッセージを送信する要求を発行する。この要求は、ＩＣＳＧＷ１エンドポイント４０６Ａを介してソースＩＣＳＧＷ４０７に転送される。ソースＩＣＳＧＷ４０７は、要求を終了し、検証確認を実行して、アプリケーション１　４０５Ａに関連付けられたアイデンティティプリンシパルがそのような要求を行うことが許可されているか否かを判定する。成功裏に検証されると、ソースＩＣＳＧＷ４０７は、アプリケーション１　４０５Ａに関連付けられたアクセスロール（例えば、ＩＡＭロール１）を要求に含めるように要求を変更する。ソースＩＣＳＧＷ４０７は、ステップ２．２において、変更された要求をターゲットＩＣＳＧＷ４５９に転送する。ステップ２．３において、ターゲットＩＣＳＧＷ４５９は、ソースＩＣＳＧＷ４０７から受信した変更された要求から対応するアクセスロールを抽出する。ターゲットＩＣＳＧＷ４５９は、管理サービス（例えば、ターゲットクラウドサービス４５３に含まれるセキュアトークンサービス４５３Ｂ）と通信して、アクセスロールに関連付けられたクレデンシャルを取得する。ステップ２．４において、ターゲットＩＣＳＧＷ４５９は、変更された要求に（ステップ１．３の）取得されたクレデンシャルで署名し、署名付き要求をサービス（例えば、アプリケーション１　４０５Ａが使用することを望むＳＱＳサービス４６１）に転送する。ステップ２．５において、ターゲットサービス４６１は、（ターゲットＩＣＳＧＷ４５９から取得された）クレデンシャルが、要求されたアクションを実行する（すなわち、ＳＱＳキューにメッセージを送信する）のに十分な権限に関連付けられているか否かを判定するための確認を実行することができる。さらに、アプリケーション１　４０５Ａは、読み取りおよび書き込みの権限を有

するアクセスロールに関連付けられているため、ステップ２．５において、メッセージは、顧客のテナンシ４６３におけるＳＱＳキューに追加される。

【００４９】

ここで、アプリケーション２　４０５ＢがＳＱＳキューをポーリングしてメッセージの存在を判定する（すなわち、ＳＱＳキューからメッセージを読み出す）というシナリオに対応するフロー３を参照する。ステップ３．１において、アプリケーション２　４０５Ｂは、ＳＱＳキューからメッセージをフェッチする要求を発行する。この要求は、ＩＣＳＧＷ２エンドポイント４０６Ｂを介してソースＩＣＳＧＷ４０７に転送される。ソースＩＣＳＧＷ４０７は、要求を終了し、上述したように検証確認を実行する。成功裏に検証されると、ソースＩＣＳＧＷ４０７は、アプリケーション２　４０５Ｂに関連付けられたアクセスロール（例えば、ＩＡＭロール２）を要求に含めるように要求を変更する。ソースＩＣＳＧＷ４０７は、ステップ３．２において、変更された要求をターゲットＩＣＳＧＷ４５９に転送する。ステップ３．３において、ターゲットＩＣＳＧＷ４５９は、ソースＩＣＳＧＷ４０７から受信した変更された要求から対応するアクセスロールを抽出する。ターゲットＩＣＳＧＷ４５９は、管理サービスと通信して、アクセスロールに関連付けられたクレデンシャルを取得する。ステップ３．４において、ターゲットＩＣＳＧＷ４５９は、変更された要求に（ステップ３．３の）取得されたクレデンシャルで署名し、署名付き要求をサービス（例えば、アプリケーション２　４０５Ｂが使用することを望むＳＱＳサービス４６１）に転送する。ステップ３．５において、ターゲットサービス４６１は、（ターゲットＩＣＳＧＷ４５９から取得された）クレデンシャルが、要求されたアクションを実行する（すなわち、ＳＱＳキューからメッセージをフェッチする）のに十分な権限に関連付けられているか否かを判定するための確認を実行することができる。さらに、アプリケーション２　４０５Ｂは、読み取りの権限を有するアクセスロールに関連付けられているため、ステップ３．５において、メッセージは、顧客のテナンシ４６３におけるＳＱＳキューからフェッチされる。

【００５０】

ここで、アプリケーション２　４０５Ｂが、Ｓ３バケットからオブジェクトをフェッチするためにＳ３サービスに対する呼び出しを呼び出すというシナリオに対応するフロー４を参照する。ステップ４．１において、アプリケーション２　４０５Ｂは、Ｓ３バケットからオブジェクトをフェッチする要求を発行する。この要求は、ＩＣＳＧＷ２エンドポイント４０６Ｂを介してソースＩＣＳＧＷ４０７に転送される。ソースＩＣＳＧＷ４０７は、要求を終了し、上述したように検証を実行する。成功裏に検証されると、ソースＩＣＳＧＷ４０７は、アプリケーション２　４０５Ｂに関連付けられたアクセスロール（例えば、ＩＡＭロール２）を要求に含めるように要求を変更する。ソースＩＣＳＧＷ４０７は、ステップ４．２において、変更された要求をターゲットＩＣＳＧＷ４５９に転送する。ステップ４．３において、ターゲットＩＣＳＧＷ４５９は、ソースＩＣＳＧＷ４０７から受信した変更された要求から対応するアクセスロールを抽出する。ターゲットＩＣＳＧＷ４５９は、管理サービスと通信して、アクセスロールに関連付けられたクレデンシャルを取得する。ステップ４．４において、ターゲットＩＣＳＧＷ４５９は、変更された要求に（ステップ４．３の）取得されたクレデンシャルで署名し、署名付き要求をサービス（例えば、アプリケーション２　４０５Ｂが使用することを望むＳ３サービス４６１）に転送する。ステップ４．５において、ターゲットサービス４６１は、（ターゲットＩＣＳＧＷ４５９から取得された）クレデンシャルが、要求されたアクションを実行する（すなわち、Ｓ３バケットからオブジェクトをフェッチする）のに十分な権限に関連付けられているか否かを判定するための確認を実行することができる。さらに、アプリケーション２　４０５Ｂは、読み取りの権限を有するアクセスロールに関連付けられているため、ステップ４．５において、オブジェクトは、顧客のテナンシ４６３におけるＳ３バケットからフェッチされる。

【００５１】

ここで図４Ｂを参照すると、顧客ＶＣＮ４０３に含まれるコンピュートインスタンスに

よって発行される、（ターゲットクラウド環境によって提供されるサービスに対する）４つの異なる要求に関するフローが詳細に記載されている。具体的には、（５．１～５．４と表記するステップを有する）フロー５は、アプリケーション２　４０５Ｂが、Ｓ３バケットにファイルをアップロードする要求を発行するというシナリオに対応する。（６．１～６．４と表記するステップを有する）フロー６は、アプリケーション２　４０５Ｂが、ＳＱＳキューからメッセージを削除する要求を発行するというシナリオに対応する。（７．１～７．５と表記するステップを有する）フロー７は、アプリケーション１　４０５Ａが、ＳＱＳキューからメッセージを削除する要求を発行するというシナリオに対応し、（８．１～８．５と表記するステップを有する）フロー８は、アプリケーション１　４０５Ａが、Ｓ３バケットからファイルを削除する要求を発行するというシナリオに対応する。

【００５２】

ここで、アプリケーション２　４０５ＢがＳ３バケットにファイルをアップロードする要求を発行するというシナリオに対応するフロー５を参照する。ステップ５．１において、アプリケーション２　４０５Ｂは、Ｓ３バケットにファイルをアップロードする要求を発行する。この要求は、ＩＣＳＧＷ２エンドポイント４０６Ｂを介してソースＩＣＳＧＷ４０７に転送される。ソースＩＣＳＧＷ４０７は、要求を終了し、上述したように検証確認を実行する。成功裏に検証されると、ソースＩＣＳＧＷ４０７は、アプリケーション２　４０５Ｂに関連付けられたアクセスロール（例えば、ＩＡＭロール２）を要求に含めるように要求を変更する。ソースＩＣＳＧＷ４０７は、ステップ５．２において、変更された要求をターゲットＩＣＳＧＷ４５９に転送する。ステップ５．３において、ターゲットＩＣＳＧＷ４５９は、ソースＩＣＳＧＷ４０７から受信した変更された要求から対応するアクセスロールを抽出する。ターゲットＩＣＳＧＷ４５９は、管理サービスと通信して、アクセスロールに関連付けられたクレデンシャルを取得する。ステップ５．４において、ターゲットＩＣＳＧＷ４５９は、変更された要求に（ステップ５．３の）取得されたクレデンシャルで署名し、署名付き要求をサービス（例えば、アプリケーション２　４０５Ｂが使用することを望むＳ３サービス４６１）に転送する。ターゲットサービス４６１は、（ターゲットＩＣＳＧＷ４５９から取得された）クレデンシャルが、要求されたアクションを実行する（すなわち、Ｓ３バケットにファイルをアップロードする）のに十分な権限に関連付けられているか否かを判定するための確認を実行する。アプリケーション２　４０５Ｂは、読み取りのみの権限を有するアクセスロールに関連付けられているため、ターゲットクラウド環境におけるＳ３サービスは、Ｓ３バケットにファイルをアップロードする要求を拒否する（ステップ５．４）。したがって、この要求は、顧客のアカウント４６３におけるサービス４６１によって実行されない。

【００５３】

ここで、アプリケーション２　４０５ＢがＳＱＳキューからメッセージを削除する要求を発行するというシナリオに対応するフロー６を参照する。ステップ６．１において、アプリケーション２　４０５Ｂは、ＳＱＳキューからメッセージを削除する要求を発行する。この要求は、ＩＣＳＧＷ２エンドポイント４０６Ｂを介してソースＩＣＳＧＷ４０７に転送される。ソースＩＣＳＧＷ４０７は、要求を終了し、上述したように検証確認を実行する。成功裏に検証されると、ソースＩＣＳＧＷ４０７は、アプリケーション２　４０５Ｂに関連付けられたアクセスロール（例えば、ＩＡＭロール２）を要求に含めるように要求を変更する。ソースＩＣＳＧＷ４０７は、ステップ６．２において、変更された要求をターゲットＩＣＳＧＷ４５９に転送する。ステップ６．３において、ターゲットＩＣＳＧＷ４５９は、ソースＩＣＳＧＷ４０７から受信した変更された要求から対応するアクセスロールを抽出する。ターゲットＩＣＳＧＷ４５９は、管理サービスと通信して、アクセスロールに関連付けられたクレデンシャルを取得する。ステップ６．４において、ターゲットＩＣＳＧＷ４５９は、変更された要求に（ステップ６．３の）取得されたクレデンシャルで署名し、署名付き要求をサービス（例えば、アプリケーション２　４０５Ｂが使用することを望むＳＱＳサービス４６１）に転送する。ターゲットサービス４６１は、（ターゲットＩＣＳＧＷ４５９から取得された）クレデンシャルが、要求されたアクションを実

行する（すなわち、ＳＱＳキューからメッセージを削除する）のに十分な権限に関連付けられているか否かを判定するための確認を実行する。アプリケーション２　４０５Ｂは、読み取りのみの権限を有するアクセスロールに関連付けられているため、ターゲットクラウド環境におけるＳＱＳサービスは、メッセージを削除する要求を拒否する（ステップ６．４）。したがって、この要求は、顧客のアカウント４６３におけるサービス４６１によって実行されない。

【００５４】

ここでフロー７を参照すると、ステップ７．１において、アプリケーション１　４０５Ａは、ＳＱＳキューからメッセージを削除する要求を発行する。この要求は、ＩＣＳＧＷ１エンドポイント４０６Ａを介してソースＩＣＳＧＷ４０７に転送される。ソースＩＣＳＧＷ４０７は、要求を終了し、検証確認を実行して、アプリケーション１　４０５Ａに関連付けられたアイデンティティプリンシパルがそのような要求を行うことを許可されているか否かを判定する。成功裏に検証されると、ソースＩＣＳＧＷ４０７は、アプリケーション１　４０５Ａに関連付けられたアクセスロール（例えば、ＩＡＭロール１）を要求に含めるように要求を変更する。ソースＩＣＳＧＷ４０７は、ステップ７．２において、変更された要求をターゲットＩＣＳＧＷ４５９に転送する。ステップ７．３において、ターゲットＩＣＳＧＷ４５９は、ソースＩＣＳＧＷ４０７から受信した変更された要求から対応するアクセスロールを抽出する。ターゲットＩＣＳＧＷ４５９は、ターゲットクラウド環境の管理サービス（例えば、ターゲットクラウドサービス４５３に含まれるセキュアトークンサービス４５３Ｂ）と通信して、アクセスロールに関連付けられたクレデンシャルを取得する。ステップ７．４において、ターゲットＩＣＳＧＷ４５９は、変更された要求に（ステップ７．３の）取得されたクレデンシャルで署名し、署名付き要求をサービス（例えば、アプリケーション１　４０５Ａが使用することを望むＳＱＳサービス４６１）に転送する。ステップ７．５において、ターゲットサービス４６１は、（ターゲットＩＣＳＧＷ４５９から取得された）クレデンシャルが、要求されたアクションを実行する（すなわち、メッセージを削除する）のに十分な権限に関連付けられているか否かを判定するための確認を実行することができる。さらに、アプリケーション１　４０５Ａは、読み取りおよび書き込みの権限を有するアクセスロールに関連付けられているため、ステップ７．５において、メッセージは、顧客のテナンシ４６３におけるＳＱＳキューから削除される。

【００５５】

（８．１～８．５と表記するステップを有する）フロー８は、アプリケーション１　４０５ＡがＳ３バケットからファイルを削除する要求を発行するというシナリオに対応する。ステップ８．１において、アプリケーション１　４０５Ａは、Ｓ３バケットからファイルを削除する要求を発行する。この要求は、ＩＣＳＧＷ１エンドポイント４０６Ａを介してソースＩＣＳＧＷ４０７に転送される。ソースＩＣＳＧＷ４０７は、要求を終了し、検証確認を実行して、アプリケーション１　４０５Ａに関連付けられたアイデンティティプリンシパルがそのような要求を行うことが許可されているか否かを判定する。成功裏に検証されると、ソースＩＣＳＧＷ４０７は、アプリケーション１　４０５Ａに関連付けられたアクセスロール（例えば、ＩＡＭロール１）を要求に含めるように要求を変更する。ソースＩＣＳＧＷ４０７は、ステップ８．２において、変更された要求をターゲットＩＣＳＧＷ４５９に転送する。ステップ８．３において、ターゲットＩＣＳＧＷ４５９は、ソースＩＣＳＧＷ４０７から受信した変更された要求から対応するアクセスロールを抽出する。ターゲットＩＣＳＧＷ４５９は、ターゲットクラウド環境の管理サービス（例えば、ターゲットクラウドサービス４５３に含まれるセキュアトークンサービス４５３Ｂ）と通信して、アクセスロールに関連付けられたクレデンシャルを取得する。ステップ８．４において、ターゲットＩＣＳＧＷ４５９は、変更された要求に（ステップ８．３の）取得されたクレデンシャルで署名し、署名付き要求をサービス（例えば、アプリケーション１　４０５Ａが使用することを望むＳ３サービス４６１）に転送する。ステップ８．５において、ターゲットサービス４６１は、（ターゲットＩＣＳＧＷ４５９から取得された）クレデ

ンシャルが、要求されたアクションを実行する（すなわち、Ｓ３バケットからファイルを削除する）のに十分な権限に関連付けられているか否かを判定するための確認を実行する。さらに、アプリケーション１　４０５Ａは、読み取りおよび書き込みの権限を有するアクセスロールに関連付けられているため、ステップ８．５において、メッセージは、顧客のテナンシ４６３におけるＳ３バケットから削除される。

【００５６】

図４Ａおよび図４Ｂに図示する例示的なシナリオは、顧客がターゲットクラウド環境におけるテナンシ、すなわち顧客アカウント（例えば、図３Ａの顧客Ｂテナンシ３３５）を有する場合に対応することに留意されたい。この場合、ＩＣＳＧＷサービスアカウント３３７は、ソースクラウド環境で実行されるコンピュートインスタンスに代わって（ターゲットクラウド環境における）サービスを管理するように構成される。顧客がターゲットクラウド環境においてテナンシを有していない場合にも、同様のシナリオのセットを実装することができることが理解される。そのような場合、ＩＣＳＧＷコントロールプレーン（図３Ａの３０５）は、ターゲットクラウド環境のＩＣＳＧＷサービスアカウント３３７内で顧客リソースグループ（例えば、顧客Ａリソースグループ３４１）をセットアップするように構成することができる。

【００５７】

クラウドインフラストラクチャ例

図５は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャのパターン例を示すブロック図５００である。サービスオペレータ５０２は、仮想クラウドネットワーク（ＶＣＮ）５０６およびセキュアホストサブネット５０８を含むことができるセキュアホストテナンシ５０４に通信可能に連結することができる。いくつかの例では、サービスオペレータ５０２は、１つまたは複数のクライアントコンピューティングデバイスを使用している場合があり、１つまたは複数のクライアントコンピューティングデバイスは、Microsoft Windows Mobile（登録商標）などのソフトウェア、および／またはｉＯＳ、Windows Phone、Ａｎｄｒｏｉｄ、ＢｌａｃｋＢｅｒｒｙ　８、Ｐａｌｍ　ＯＳなどの種々の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）または他の通信プロトコルに対応している、ポータブルハンドヘルドデバイス（例えば、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、携帯情報端末（ＰＤＡ））、またはウェアラブルデバイス（Google Glass（登録商標）ヘッドマウントディスプレイ）であってもよい。代替的に、クライアントコンピューティングデバイスは、例として、Microsoft Windows（登録商標）オペレーティングシステム、Apple Macintosh（登録商標）オペレーティングシステム、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してい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、汎用パーソナルコンピュータであってもよい。クライアントコンピューティングデバイスは、限定なしに、例えばGoogle Chrome OSなど、種々のＧＮＵ／Ｌｉｎｕｘオペレーティングシステムを含む、種々の市販のＵＮＩＸ（登録商標）またはＵＮＩＸ系オペレーティングシステムのうちのいずれかを実行している、ワークステーションコンピュータとすることができる。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は、ＶＣＮ５０６および／またはインターネットにアクセスすることができる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、インターネット対応ゲーミングシステム（例えば、Kinect（登録商標）ジェスチャ入力デバイスを有するかまたは有していないMicrosoft Xboxゲーム機）、および／またはパーソナルメッセージングデバイスなどの他の任意の電子デバイスであってもよい。

【００５８】

ＶＣＮ５０６は、ローカルピアリングゲートウェイ（ＬＰＧ）５１０を含むことができ、ＬＰＧ５１０は、セキュアシェル（ＳＳＨ）ＶＣＮ５１２に、ＳＳＨ　ＶＣＮ５１２に含まれるＬＰＧ５１０を介して通信可能に連結することができる。ＳＳＨ　ＶＣＮ５１２

は、ＳＳＨサブネット５１４を含むことができ、ＳＳＨ　ＶＣＮ５１２は、コントロールプレーンＶＣＮ５１６に、コントロールプレーンＶＣＮ５１６に含まれるＬＰＧ５１０を介して通信可能に連結することができる。また、ＳＳＨ　ＶＣＮ５１２は、ＬＰＧ５１０を介して、データプレーンＶＣＮ５１８に通信可能に連結することができる。コントロールプレーンＶＣＮ５１６およびデータプレーンＶＣＮ５１８は、ＩａａＳプロバイダによって所有および／または運営することができるサービステナンシ５１９に含めることができる。

【００５９】

コントロールプレーンＶＣＮ５１６は、境界ネットワーク（例えば、企業イントラネットと外部ネットワークとの間の企業ネットワークの部分）として作用するコントロールプレーン非武装地帯（ＤＭＺ：demilitarized zone）層５２０を含むことができる。ＤＭＺベースのサーバは、制限された責任を有し、セキュリティ侵害を抑制するのに役立つことができる。さらに、ＤＭＺ層５２０は、１つまたは複数のロードバランサ（ＬＢ）サブネット５２２と、アプリサブネット５２６を含むことができるコントロールプレーンアプリ層５２４と、データベース（ＤＢ）サブネット５３０（例えば、フロントエンドＤＢサブネットおよび／またはバックエンドＤＢサブネット）を含むことができるコントロールプレーンデータ層５２８とを含むことができる。コントロールプレーンＤＭＺ層５２０に含まれるＬＢサブネット５２２は、コントロールプレーンアプリ層５２４に含まれるアプリサブネット５２６と、コントロールプレーンＶＣＮ５１６に含めることができるインターネットゲートウェイ５３４とに通信可能に連結することができ、アプリサブネット５２６は、コントロールプレーンデータ層５２８に含まれるＤＢサブネット５３０と、サービスゲートウェイ５３６と、ネットワークアドレス変換（ＮＡＴ）ゲートウェイ５３８とに通信可能に連結することができる。コントロールプレーンＶＣＮ５１６は、サービスゲートウェイ５３６およびＮＡＴゲートウェイ５３８を含むことができる。

【００６０】

コントロールプレーンＶＣＮ５１６は、アプリサブネット５２６を含むことができるデータプレーンミラーアプリ層５４０を含むことができる。データプレーンミラーアプリ層５４０に含まれるアプリサブネット５２６は、コンピュートインスタンス５４４を実行することができる仮想ネットワークインターフェースコントローラ（ＶＮＩＣ）５４２を含むことができる。コンピュートインスタンス５４４は、データプレーンミラーアプリ層５４０のアプリサブネット５２６を、データプレーンアプリ層５４６に含めることができるアプリサブネット５２６に通信可能に連結することができる。

【００６１】

データプレーンＶＣＮ５１８は、データプレーンアプリ層５４６と、データプレーンＤＭＺ層５４８と、データプレーンデータ層５５０とを含むことができる。データプレーンＤＭＺ層５４８は、データプレーンアプリ層５４６のアプリサブネット５２６およびデータプレーンＶＣＮ５１８のインターネットゲートウェイ５３４に通信可能に連結することができるＬＢサブネット５２２を含むことができる。アプリサブネット５２６は、データプレーンＶＣＮ５１８のサービスゲートウェイ５３６およびデータプレーンＶＣＮ５１８のＮＡＴゲートウェイ５３８に通信可能に連結することができる。データプレーンデータ層５５０は、データプレーンアプリ層５４６のアプリサブネット５２６に通信可能に連結することができるＤＢサブネット５３０も含むことができる。

【００６２】

コントロールプレーンＶＣＮ５１６のインターネットゲートウェイ５３４およびデータプレーンＶＣＮ５１８のインターネットゲートウェイ５３４は、パブリックインターネット５５４に通信可能に連結することができるメタデータ管理サービス５５２に通信可能に連結することができる。パブリックインターネット５５４は、コントロールプレーンＶＣＮ５１６のＮＡＴゲートウェイ５３８およびデータプレーンＶＣＮ５１８のＮＡＴゲートウェイ５３８に通信可能に連結することができる。コントロールプレーンＶＣＮ５１６のサービスゲートウェイ５３６およびデータプレーンＶＣＮ５１８のサービスゲートウェイ

５３６は、クラウドサービス５５６に通信可能に連結することができる。

【００６３】

いくつかの例では、コントロールプレーンＶＣＮ５１６またはデータプレーンＶＣＮ５１８のサービスゲートウェイ５３６は、パブリックインターネット５５４を経由することなく、クラウドサービス５５６へのアプリケーションプログラミングインターフェース（ＡＰＩ）呼び出しを行うことができる。サービスゲートウェイ５３６からのクラウドサービス５５６へのＡＰＩ呼び出しは、一方向であり得る。すなわち、サービスゲートウェイ５３６は、クラウドサービス５５６へのＡＰＩ呼び出しを行うことができ、クラウドサービス５５６は、要求されたデータをサービスゲートウェイ５３６に送信することができる。しかしながら、クラウドサービス５５６は、サービスゲートウェイ５３６へのＡＰＩ呼び出しを開始することができない。

【００６４】

いくつかの例では、セキュアホストテナンシ５０４は、さもなければ隔離される可能性があるサービステナンシ５１９に直接接続することができる。セキュアホストサブネット５０８は、さもなければ隔離されていたシステムでの双方向通信を可能にすることができるＬＰＧ５１０を介して、ＳＳＨサブネット５１４と通信することができる。セキュアホストサブネット５０８をＳＳＨサブネット５１４に接続することによって、セキュアホストサブネット５０８は、サービステナンシ５１９内の他のエンティティにアクセスすることができる。

【００６５】

コントロールプレーンＶＣＮ５１６は、サービステナンシ５１９のユーザが所望のリソースをセットアップするかまたは他の方法でプロビジョニングすることを可能にすることができる。コントロールプレーンＶＣＮ５１６においてプロビジョニングされた所望のリソースは、データプレーンＶＣＮ５１８においてデプロイするかまたは他の方法で使用することができる。いくつかの例では、コントロールプレーンＶＣＮ５１６は、データプレーンＶＣＮ５１８から隔離することができ、コントロールプレーンＶＣＮ５１６のデータプレーンミラーアプリ層５４０は、データプレーンミラーアプリ層５４０およびデータプレーンアプリ層５４６に含めることができるＶＮＩＣ５４２を介して、データプレーンＶＣＮ５１８のデータプレーンアプリ層５４６と通信することができる。

【００６６】

いくつかの例では、システムのユーザまたは顧客は、パブリックインターネット５５４を介して、要求、例えば、作成、読み取り、更新、または削除（ＣＲＵＤ）操作の要求を行うことができ、パブリックインターネット５５４は、そうした要求をメタデータ管理サービス５５２に通信することができる。メタデータ管理サービス５５２は、インターネットゲートウェイ５３４を介して、要求をコントロールプレーンＶＣＮ５１６に通信することができる。要求は、コントロールプレーンＤＭＺ層５２０に含まれるＬＢサブネット５２２によって受信することができる。ＬＢサブネット５２２は、要求が有効であると判定する場合があり、この判定に応答して、ＬＢサブネット５２２は、要求をコントロールプレーンアプリ層５２４に含まれるアプリサブネット５２６に送信することができる。要求が検証され、パブリックインターネット５５４への呼び出しを必要とする場合、パブリックインターネット５５４への呼び出しを、パブリックインターネット５５４への呼び出しを行うことができるＮＡＴゲートウェイ５３８に送信することができる。要求によって格納することが望まれる可能性があるメモリは、ＤＢサブネット５３０に格納することができる。

【００６７】

いくつかの例では、データプレーンミラーアプリ層５４０は、コントロールプレーンＶＣＮ５１６とデータプレーンＶＣＮ５１８との間の直接通信を容易にすることができる。例えば、データプレーンＶＣＮ５１８に含まれるリソースに対して、構成に対する変更、更新、または他の好適な修正が適用されることが望まれる場合がある。コントロールプレーンＶＣＮ５１６は、ＶＮＩＣ５４２を介して、データプレーンＶＣＮ５１８に含まれる

リソースと直接通信することができ、それによって、リソースに対する構成に対する変更、更新、または他の適切な修正を実行することができる。

【００６８】

いくつかの実施形態では、コントロールプレーンＶＣＮ５１６およびデータプレーンＶＣＮ５１８は、サービステナンシ５１９に含めることができる。この場合、システムのユーザまたは顧客は、コントロールプレーンＶＣＮ５１６およびデータプレーンＶＣＮ５１８のいずれも所有および操作しなくてもよい。代わりに、ＩａａＳプロバイダが、コントロールプレーンＶＣＮ５１６およびデータプレーンＶＣＮ５１８を所有または操作することができ、これらの両方は、サービステナンシ５１９に含めることができる。この実施形態により、ネットワークの隔離を可能にすることができ、それにより、ユーザまたは顧客が、他のユーザのリソースまたは他の顧客のリソースとインタラクトすることを防止することができる。また、この実施形態により、システムのユーザまたは顧客が、格納するのに所望のレベルのセキュリティレベルを有していない可能性のあるパブリックインターネット６５４に依存する必要なく、データベースをプライベートに格納することができるようにすることができる。

【００６９】

他の実施形態では、コントロールプレーンＶＣＮ５１６に含まれるＬＢサブネット５２２は、サービスゲートウェイ５３６から信号を受信するように構成することができる。この実施形態では、コントロールプレーンＶＣＮ５１６およびデータプレーンＶＣＮ５１８は、パブリックインターネット５５４を呼び出すことなく、ＩａａＳプロバイダの顧客によって呼び出されるように構成することができる。顧客が使用するデータベースは、ＩａａＳプロバイダによって制御することができ、パブリックインターネット５５４から隔離することができるサービステナンシ５１９に格納することができるため、ＩａａＳプロバイダの顧客は、この実施形態を望む可能性がある。

【００７０】

図６は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別のパターン例を示すブロック図６００である。サービスオペレータ６０２（例えば、図５のサービスオペレータ５０２）は、仮想クラウドネットワーク（ＶＣＮ）６０６（例えば、図５のＶＣＮ５０６）およびセキュアホストサブネット６０８（例えば、図５のセキュアホストサブネット５０８）を含むことができるセキュアホストテナンシ６０４（例えば、図５のセキュアホストテナンシ５０４）に通信可能に連結することができる。ＶＣＮ６０６は、ローカルピアリングゲートウェイ（ＬＰＧ）６１０（例えば、図５のＬＰＧ５１０）を含むことができ、ＬＰＧ６１０は、セキュアシェル（ＳＳＨ）ＶＣＮ６１２（例えば、図５のＳＳＨ　ＶＣＮ５１２）に、ＳＳＨ　ＶＣＮ６１２に含まれるＬＰＧ５１０を介して通信可能に連結することができる。ＳＳＨ　ＶＣＮ６１２は、ＳＳＨサブネット６１４（例えば、図５のＳＳＨサブネット５１４）を含むことができ、ＳＳＨ　ＶＣＮ６１２は、コントロールプレーンＶＣＮ６１６（例えば、図５のコントロールプレーンＶＣＮ５１６）に、コントロールプレーンＶＣＮ６１６に含まれるＬＰＧ６１０を介して通信可能に連結することができる。コントロールプレーンＶＣＮ６１６は、サービステナンシ６１９（例えば、図５のサービステナンシ５１９）に含めることができ、データプレーンＶＣＮ６１８（例えば、図５のデータプレーンＶＣＮ５１８）は、システムのユーザまたは顧客が所有または運営する可能性がある顧客テナンシ６２１に含めることができる。

【００７１】

コントロールプレーンＶＣＮ６１６は、ＬＢサブネット６２２（例えば、図５のＬＢサブネット５２２）を含むことができるコントロールプレーンＤＭＺ層６２０（例えば、図５のコントロールプレーンＤＭＺ層５２０）と、アプリサブネット６２６（例えば、図５のアプリサブネット５２６）を含むことができるコントロールプレーンアプリ層６２４（例えば、図５のコントロールプレーンアプリ層５２４）と、（例えば、図５のＤＢサブネット５３０と同様の）データベース（ＤＢ）サブネット６３０を含むことができるコントロールプレーンデータ層６２８（例えば、図５のコントロールプレーンデータ層５２８）

とを含むことができる。コントロールプレーンＤＭＺ層６２０に含まれるＬＢサブネット６２２は、コントロールプレーンアプリ層６２４に含まれるアプリサブネット６２６と、コントロールプレーンＶＣＮ６１６に含めることができるインターネットゲートウェイ６３４（例えば、図５のインターネットゲートウェイ５３４）とに通信可能に連結することができ、アプリサブネット６２６は、コントロールプレーンデータ層６２８に含まれるＤＢサブネット６３０と、サービスゲートウェイ６３６（例えば、図５のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ６３８（例えば、図５のＮＡＴゲートウェイ５３８）とに通信可能に連結することができる。コントロールプレーンＶＣＮ６１６は、サービスゲートウェイ６３６およびＮＡＴゲートウェイ６３８を含むことができる。

【００７２】

コントロールプレーンＶＣＮ６１６は、アプリサブネット６２６を含むことができるデータプレーンミラーアプリ層６４０（例えば、図５のデータプレーンミラーアプリ層５４０）を含むことができる。データプレーンミラーアプリ層６４０に含まれるアプリサブネット６２６は、（例えば、図５のコンピュートインスタンス５４４と同様の）コンピュートインスタンス６４４を実行することができる仮想ネットワークインターフェースコントローラ（ＶＮＩＣ）６４２（例えば、ＶＮＩＣ５４２）を含むことができる。コンピュートインスタンス６４４は、データプレーンミラーアプリ層６４０に含まれるＶＮＩＣ６４２およびデータプレーンアプリ層６４６に含まれるＶＮＩＣ６４２を介して、データプレーンミラーアプリ層６４０のアプリサブネット６２６と、データプレーンアプリ層６４６（例えば、図５のデータプレーンアプリ層５４６）に含めることができるアプリサブネット６２６との間の通信を促進することができる。

【００７３】

コントロールプレーンＶＣＮ６１６に含まれるインターネットゲートウェイ６３４は、パブリックインターネット６５４（例えば、図５のパブリックインターネット５５４）に通信可能に連結することができるメタデータ管理サービス６５２（例えば、図５のメタデータ管理サービス５５２）に通信可能に連結することができる。パブリックインターネット６５４は、コントロールプレーンＶＣＮ６１６に含まれるＮＡＴゲートウェイ６３８に通信可能に連結することができる。コントロールプレーンＶＣＮ６１６に含まれるサービスゲートウェイ６３６は、クラウドサービス６５６（例えば、図５のクラウドサービス５５６）に通信可能に連結することができる。

【００７４】

いくつかの例では、データプレーンＶＣＮ６１８は、顧客テナンシ６２１に含めることができる。この場合、ＩａａＳプロバイダは、各顧客に対してコントロールプレーンＶＣＮ６１６を提供することができ、ＩａａＳプロバイダは、各顧客に対して、サービステナンシ６１９に含まれる一意のコンピュートインスタンス６４４をセットアップすることができる。各コンピュートインスタンス６４４は、サービステナンシ６１９に含まれるコントロールプレーンＶＣＮ６１６と、顧客テナンシ６２１に含まれるデータプレーンＶＣＮ６１８との間の通信を可能にすることができる。コンピュートインスタンス６４４は、サービステナンシ６１９に含まれるコントロールプレーンＶＣＮ６１６においてプロビジョニングされるリソースが、顧客テナンシ６２１に含まれるデータプレーンＶＣＮ６１８にデプロイされるかまたは他の方法で使用されるのを可能にすることができる。

【００７５】

他の例では、ＩａａＳプロバイダの顧客は、顧客テナンシ６２１に存在するデータベースを有することができる。この例では、コントロールプレーンＶＣＮ６１６は、アプリサブネット６２６を含むことができるデータプレーンミラーアプリ層６４０を含むことができる。データプレーンミラーアプリ層６４０は、データプレーンＶＣＮ６１８に常駐することができるが、データプレーンミラーアプリ層６４０は、データプレーンＶＣＮ６１８に存在しない場合もある。すなわち、データプレーンミラーアプリ層６４０は、顧客テナンシ６２１にアクセスすることができるが、データプレーンミラーアプリ層６４０は、デ

ータプレーンＶＣＮ６１８に存在しなくてもよく、またはＩａａＳプロバイダの顧客が所有および運営しなくてもよい。データプレーンミラーアプリ層６４０は、データプレーンＶＣＮ６１８への呼び出しを行うように構成してもよいが、コントロールプレーンＶＣＮ６１６に含まれる任意のエンティティへの呼び出しを行うようには構成しなくてもよい。顧客は、コントロールプレーンＶＣＮ６１６にプロビジョニングされている、データプレーンＶＣＮ６１８内のリソースをデプロイするかまたは他の方法で使用することを望む場合があり、データプレーンミラーアプリ層６４０は、顧客のリソースの所望のデプロイメントまたは他の使用を促進することができる。

【００７６】

いくつかの実施形態では、ＩａａＳプロバイダの顧客は、データプレーンＶＣＮ６１８にフィルタを適用することができる。この実施形態では、顧客は、データプレーンＶＣＮ６１８がアクセスできるものを決定することができ、顧客は、データプレーンＶＣＮ６１８からのパブリックインターネット６５４へのアクセスを制限することができる。ＩａａＳプロバイダは、データプレーンＶＣＮ６１８から任意の外部ネットワークまたはデータベースへのアクセスにフィルタを適用するかまたは他の方法でそうしたアクセスを制御することができない場合がある。顧客が顧客テナンシ６２１に含まれるデータプレーンＶＣＮ６１８にフィルタおよび制御を適用することは、データプレーンＶＣＮ６１８を他の顧客から、およびパブリックインターネット６５４から隔離するのに役立つことができる。

【００７７】

いくつかの実施形態では、サービスゲートウェイ６３６が、パブリックインターネット６５４上に、コントロールプレーンＶＣＮ６１６上に、またはデータプレーンＶＣＮ６１８上に存在していない可能性があるサービスにアクセスするために、クラウドサービス６５６を呼び出すことができる。クラウドサービス６５６とコントロールプレーンＶＣＮ６１６またはデータプレーンＶＣＮ６１８との間の接続は、ライブでも連続的でなくてもよい。クラウドサービス６５６は、ＩａａＳプロバイダによって所有または運営されている異なるネットワーク上に存在してもよい。クラウドサービス６５６は、サービスゲートウェイ６３６から呼び出しを受信するように構成してもよく、パブリックインターネット６５４から呼び出しを受信しないように構成してもよい。いくつかのクラウドサービス６５６は、他のクラウドサービス６５６から隔離されている場合があり、コントロールプレーンＶＣＮ６１６は、コントロールプレーンＶＣＮ６１６と同じリージョンにない可能性があるクラウドサービス６５６から隔離されている場合がある。例えば、コントロールプレーンＶＣＮ６１６は、「リージョン１」に位置する場合があり、クラウドサービス「デプロイメント６」は、リージョン１および「リージョン２」に位置する場合がある。デプロイメント６への呼び出しが、リージョン１に位置するコントロールプレーンＶＣＮ６１６に含まれるサービスゲートウェイ６３６によって行われる場合、この呼び出しは、リージョン１内のデプロイメント６に送信することができる。この例では、コントロールプレーンＶＣＮ６１６またはリージョン１のデプロイメント６は、リージョン２のデプロイメント６と通信可能に連結されないか、または他の方法で通信していない可能性がある。

【００７８】

図７は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別のパターン例を示すブロック図７００である。サービスオペレータ７０２（例えば、図５のサービスオペレータ５０２）は、仮想クラウドネットワーク（ＶＣＮ）７０６（例えば、図５のＶＣＮ５０６）およびセキュアホストサブネット７０８（例えば、図５のセキュアホストサブネット５０８）を含むことができるセキュアホストテナンシ７０４（例えば、図５のセキュアホストテナンシ５０４）に通信可能に連結することができる。ＶＣＮ７０６は、ＬＰＧ７１０（例えば、図５のＬＰＧ５１０）を含むことができ、ＬＰＧ７１０は、ＳＳＨ　ＶＣＮ７１２（例えば、図５のＳＳＨ　ＶＣＮ５１２）に、ＳＳＨ　ＶＣＮ７１２に含まれるＬＰＧ７１０を介して通信可能に連結することができる。ＳＳＨ　ＶＣＮ７１２は、ＳＳＨサブネット７１４（例えば、図５のＳＳＨサブネット５１４）を含むことができ、ＳＳＨ　ＶＣＮ７１２は、コントロールプレーンＶＣＮ７１６（例えば、図５のコントロ

ールプレーンＶＣＮ５１６）に、コントロールプレーンＶＣＮ７１６に含まれるＬＰＧ７１０を介して、およびデータプレーンＶＣＮ７１８（例えば、図５のデータプレーン５１８）に、データプレーンＶＣＮ７１８に含まれるＬＰＧ７１０を介して、通信可能に連結することができる。コントロールプレーンＶＣＮ７１６およびデータプレーンＶＣＮ７１８は、サービステナンシ７１９（例えば、図５のサービステナンシ５１９）に含めることができる。

【００７９】

コントロールプレーンＶＣＮ７１６は、ロードバランサ（ＬＢ）サブネット７２２（例えば、図５のＬＢサブネット５２２）を含むことができるコントロールプレーンＤＭＺ層７２０（例えば、図５のコントロールプレーンＤＭＺ層５２０）と、（例えば、図５のアプリサブネット５２６と同様の）アプリサブネット７２６を含むことができるコントロールプレーンアプリ層７２４（例えば、図５のコントロールプレーンアプリ層５２４）と、ＤＢサブネット７３０を含むことができるコントロールプレーンデータ層７２８（例えば、図５のコントロールプレーンデータ層５２８）とを含むことができる。コントロールプレーンＤＭＺ層７２０に含まれるＬＢサブネット７２２は、コントロールプレーンアプリ層７２４に含まれるアプリサブネット７２６と、コントロールプレーンＶＣＮ７１６に含めることができるインターネットゲートウェイ７３４（例えば、図５のインターネットゲートウェイ５３４）とに通信可能に連結することができ、アプリサブネット７２６は、コントロールプレーンデータ層７２８に含まれるＤＢサブネット７３０と、サービスゲートウェイ７３６（例えば、図５のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ７３８（例えば、図５のＮＡＴゲートウェイ５３８）とに通信可能に連結することができる。コントロールプレーンＶＣＮ７１６は、サービスゲートウェイ７３６およびＮＡＴゲートウェイ７３８を含むことができる。

【００８０】

データプレーンＶＣＮ７１８は、データプレーンアプリ層７４６（例えば、図５のデータプレーンアプリ層５４６）と、データプレーンＤＭＺ層７４８（例えば、図５のデータプレーンＤＭＺ層５４８）と、データプレーンデータ層７５０（例えば、図５のデータプレーンデータ層５５０）とを含むことができる。データプレーンＤＭＺ層７４８は、データプレーンＶＣＮ７１８に含まれる、データプレーンアプリ層７４６の信頼できるアプリサブネット７６０および信頼できないアプリサブネット７６２、ならびにインターネットゲートウェイ７３４に、通信可能に連結することができる、ＬＢサブネット７２２を含むことができる。信頼できるアプリサブネット７６０は、データプレーンＶＣＮ７１８に含まれるサービスゲートウェイ７３６、データプレーンＶＣＮ７１８に含まれるＮＡＴゲートウェイ７３８、およびデータプレーンデータ層７５０に含まれるＤＢサブネット７３０に、通信可能に連結することができる。信頼できないアプリサブネット７６２は、データプレーンＶＣＮ７１８に含まれるサービスゲートウェイ７３６、およびデータプレーンデータ層７５０に含まれるＤＢサブネット７３０に通信可能に連結することができる。データプレーンデータ層７５０は、データプレーンＶＣＮ７１８に含まれるサービスゲートウェイ７３６に通信可能に連結することができるＤＢサブネット７３０を含むことができる。

【００８１】

信頼できないアプリサブネット７６２は、テナント仮想マシン（ＶＭ）７６６（１）～（Ｎ）に通信可能に連結することができる、１つまたは複数のプライマリＶＮＩＣ７６４（１）～（Ｎ）を含むことができる。各テナントＶＭ７６６（１）～（Ｎ）は、それぞれの顧客テナンシ７７０（１）～（Ｎ）に含めることができるそれぞれのコンテナエグレスＶＣＮ７６８（１）～（Ｎ）に含めることができるそれぞれのアプリサブネット７６７（１）～（Ｎ）に、通信可能に連結することができる。それぞれのセカンダリＶＮＩＣ７７２（１）～（Ｎ）が、データプレーンＶＣＮ７１８に含まれる信頼できないアプリサブネット７６２と、コンテナエグレスＶＣＮ７６８（１）～（Ｎ）に含まれるアプリサブネットとの間の通信を促進することができる。各コンテナエグレスＶＣＮ７６８（１）～（Ｎ

）は、パブリックインターネット７５４（例えば、図５のパブリックインターネット５５４）に通信可能に連結することができる、ＮＡＴゲートウェイ７３８を含むことができる。

【００８２】

コントロールプレーンＶＣＮ７１６に含まれるインターネットゲートウェイ７３４およびデータプレーンＶＣＮ７１８に含まれるインターネットゲートウェイ７３４は、パブリックインターネット７５４に通信可能に連結することができるメタデータ管理サービス７５２（例えば、図５のメタデータ管理システム５５２）に、通信可能に連結することができる。パブリックインターネット７５４は、コントロールプレーンＶＣＮ７１６に含まれるＮＡＴゲートウェイ７３８およびデータプレーンＶＣＮ７１８に含まれるＮＡＴゲートウェイ７３８に、通信可能に連結することができる。コントロールプレーンＶＣＮ７１６に含まれるサービスゲートウェイ７３６およびデータプレーンＶＣＮ７１８に含まれるサービスゲートウェイ７３６は、クラウドサービス７５６に通信可能に連結することができる。

【００８３】

いくつかの実施形態では、データプレーンＶＣＮ７１８は、顧客テナンシ７７０と統合することができる。この統合は、コードを実行するときにサポートを望む可能性がある場合などのいくつかの場合において、ＩａａＳプロバイダの顧客にとって有用または望ましい可能性がある。顧客は、破壊的であり得る、他の顧客リソースと通信する可能性がある、または、その他の点で望ましくない影響を引き起こす可能性があるコードを、実行するように提供する場合がある。これに応じて、ＩａａＳプロバイダは、顧客がＩａａＳプロバイダに与えたコードを実行するか否かを判定することができる。

【００８４】

いくつかの例では、ＩａａＳプロバイダの顧客は、一時的なネットワークアクセスをＩａａＳプロバイダに許可し、データプレーン層アプリ７４６にアタッチすべき機能を要求することができる。機能を実行するコードは、ＶＭ７６６（１）～（Ｎ）で実行することができ、データプレーンＶＣＮ７１８上の他のいかなる場所でも実行されるように構成しなくてもよい。各ＶＭ７６６（１）～（Ｎ）は、１つの顧客テナンシ７７０に接続することができる。ＶＭ７６６（１）～（Ｎ）に含まれるそれぞれのコンテナ７７１（１）～（Ｎ）は、コードを実行するように構成することができる。この場合、二重の隔離があり得る（例えば、コンテナ７７１（１）～（Ｎ）がコードを実行し、コンテナ７７１（１）～（Ｎ）は、少なくとも、信頼できないアプリサブネット７６２に含まれるＶＭ７６６（１）～（Ｎ）に含めることができる）。これは、間違ったまたは他の意味で望ましくないコードが、ＩａａＳプロバイダのネットワークに損害を与えること、または異なる顧客のネットワークに損害を与えることを防止するのに役立つことができる。コンテナ７７１（１）～（Ｎ）は、顧客テナンシ７７０に通信可能に連結することができ、顧客テナンシ７７０からデータを送信または受信するように構成することができる。コンテナ７７１（１）～（Ｎ）は、データプレーンＶＣＮ７１８内の他の任意のエンティティからデータを送信または受信するように構成しなくてもよい。コードの実行が完了したとき、ＩａａＳプロバイダは、コンテナ７７１（Ｉ）～（Ｎ）を強制停止するまたは他の方法で廃棄することができる。

【００８５】

いくつかの実施形態では、信頼できるアプリサブネット７６０は、ＩａａＳプロバイダが所有または操作することができるコードを実行することができる。この実施形態では、信頼できるアプリサブネット７６０は、ＤＢサブネット７３０に通信可能に連結し、ＤＢサブネット７３０においてＣＲＵＤ操作を実行するように構成することができる。信頼できないアプリサブネット７６２は、ＤＢサブネット７３０に通信可能に連結することができるが、この実施形態では、信頼できないアプリサブネットは、ＤＢサブネット７３０内で読み取り操作を実行するように構成することができる。各顧客のＶＭ７６６（１）～（Ｎ）に含めることができ、顧客からのコードを実行することができるコンテナ７７１（１

）～（Ｎ）は、ＤＢサブネット７３０と通信可能に連結しなくてもよい。

【００８６】

他の実施形態では、コントロールプレーンＶＣＮ７１６およびデータプレーンＶＣＮ７１８は、直接通信可能に連結しなくてもよい。この実施形態では、コントロールプレーンＶＣＮ７１６とデータプレーンＶＣＮ７１８との間に直接の通信はなくてもよい。しかしながら、通信は、少なくとも１つの方法により、間接的に起こり得る。ＩａａＳプロバイダによって、コントロールプレーンＶＣＮ７１６とデータプレーンＶＣＮ７１８との間の通信を容易にすることができるＬＰＧ７１０を確立してもよい。別の例では、コントロールプレーンＶＣＮ７１６またはデータプレーンＶＣＮ７１８は、サービスゲートウェイ７３６を介してクラウドサービス７５６への呼び出しを行うことができる。例えば、コントロールプレーンＶＣＮ７１６からクラウドサービス７５６への呼び出しは、データプレーンＶＣＮ７１８と通信することができるサービスに対する要求を含むことができる。

【００８７】

図８は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別のパターン例を示すブロック図８００である。サービスオペレータ８０２（例えば、図５のサービスオペレータ５０２）は、仮想クラウドネットワーク（ＶＣＮ）８０６（例えば、図５のＶＣＮ５０６）およびセキュアホストサブネット８０８（例えば、図５のセキュアホストサブネット５０８）を含むことができるセキュアホストテナンシ８０４（例えば、図５のセキュアホストテナンシ５０４）に通信可能に連結することができる。ＶＣＮ８０６は、ＳＳＨ　ＶＣＮ８１２（例えば、図５のＳＳＨ　ＶＣＮ５１２）に、ＳＳＨ　ＶＣＮ８１２に含まれるＬＰＧ８１０を介して通信可能に連結することができる、ＬＰＧ８１０（例えば、図５のＬＰＧ５１０）を含むことができる。ＳＳＨ　ＶＣＮ８１２は、ＳＳＨサブネット８１４（例えば、図５のＳＳＨサブネット５１４）を含むことができ、ＳＳＨ　ＶＣＮ８１２は、コントロールプレーンＶＣＮ８１６（例えば、図５のコントロールプレーンＶＣＮ５１６）に、コントロールプレーンＶＣＮ８１６に含まれるＬＰＧ８１０を介して、およびデータプレーンＶＣＮ８１８（例えば、図５のデータプレーン５１８）に、データプレーンＶＣＮ８１８に含まれるＬＰＧ８１０を介して、通信可能に連結することができる。コントロールプレーンＶＣＮ８１６およびデータプレーンＶＣＮ８１８は、サービステナンシ８１９（例えば、図５のサービステナンシ５１９）に含めることができる。

【００８８】

コントロールプレーンＶＣＮ８１６は、ＬＢサブネット８２２（例えば、図５のＬＢサブネット５２２）を含むことができるコントロールプレーンＤＭＺ層８２０（例えば、図５のコントロールプレーンＤＭＺ層５２０）と、アプリサブネット８２６（例えば、図５のアプリサブネット５２６）を含むことができるコントロールプレーンアプリ層８２４（例えば、図５のコントロールプレーンアプリ層５２４）と、ＤＢサブネット８３０（例えば、図７のＤＢサブネット７３０）を含むことができるコントロールプレーンデータ層８２８（例えば、図５のコントロールプレーンデータ層５２８）とを含むことができる。コントロールプレーンＤＭＺ層８２０に含まれるＬＢサブネット８２２は、コントロールプレーンアプリ層８２４に含まれるアプリサブネット８２６と、コントロールプレーンＶＣＮ８１６に含めることができるインターネットゲートウェイ８３４（例えば、図５のインターネットゲートウェイ５３４）とに通信可能に連結することができ、アプリサブネット８２６は、コントロールプレーンデータ層８２８に含まれるＤＢサブネット８３０と、サービスゲートウェイ８３６（例えば、図５のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ８３８（例えば、図５のＮＡＴゲートウェイ５３８）とに通信可能に連結することができる。コントロールプレーンＶＣＮ８１６は、サービスゲートウェイ８３６およびＮＡＴゲートウェイ８３８を含むことができる。

【００８９】

データプレーンＶＣＮ８１８は、データプレーンアプリ層８４６（例えば、図５のデータプレーンアプリ層５４６）と、データプレーンＤＭＺ層８４８（例えば、図５のデータプレーンＤＭＺ層５４８）と、データプレーンデータ層８５０（例えば、図５のデータプ

レーンデータ層５５０）とを含むことができる。データプレーンＤＭＺ層８４８は、データプレーンＶＣＮ８１８に含まれる、データプレーンアプリ層８４６の信頼できるアプリサブネット８６０（例えば、図７の信頼できるアプリサブネット７６０）および信頼できないアプリサブネット８６２（例えば、図７の信頼できないアプリサブネット７６２）、ならびにインターネットゲートウェイ８３４に、通信可能に連結することができる、ＬＢサブネット８２２を含むことができる。信頼できるアプリサブネット８６０は、データプレーンＶＣＮ８１８に含まれるサービスゲートウェイ８３６、データプレーンＶＣＮ８１８に含まれるＮＡＴゲートウェイ８３８、およびデータプレーンデータ層８５０に含まれるＤＢサブネット８３０に、通信可能に連結することができる。信頼できないアプリサブネット８６２は、データプレーンＶＣＮ８１８に含まれるサービスゲートウェイ８３６、およびデータプレーンデータ層８５０に含まれるＤＢサブネット８３０に通信可能に連結することができる。データプレーンデータ層８５０は、データプレーンＶＣＮ８１８に含まれるサービスゲートウェイ８３６に通信可能に連結することができるＤＢサブネット８３０を含むことができる。

【００９０】

信頼できないアプリサブネット８６２は、信頼できないアプリサブネット８６２内に常駐するテナント仮想マシン（ＶＭ）８６６（１）～（Ｎ）に通信可能に連結することができる、プライマリＶＮＩＣ８６４（１）～（Ｎ）を含むことができる。各テナントＶＭ８６６（１）～（Ｎ）は、それぞれのコンテナ８６７（１）～（Ｎ）においてコードを実行することができ、コンテナエグレスＶＣＮ８６８に含めることができるデータプレーンアプリ層８４６に含めることができるアプリサブネット８２６に、通信可能に連結することができる。それぞれのセカンダリＶＮＩＣ８７２（１）～（Ｎ）が、データプレーンＶＣＮ８１８に含まれる信頼できないアプリサブネット８６２と、コンテナエグレスＶＣＮ８６８に含まれるアプリサブネットとの間の通信を促進することができる。コンテナエグレスＶＣＮ８６８は、パブリックインターネット８５４（例えば、図５のパブリックインターネット５５４）に通信可能に連結することができる、ＮＡＴゲートウェイ８３８を含むことができる。

【００９１】

コントロールプレーンＶＣＮ８１６に含まれるインターネットゲートウェイ８３４およびデータプレーンＶＣＮ８１８に含まれるインターネットゲートウェイ８３４は、パブリックインターネット８５４に通信可能に連結することができるメタデータ管理サービス８５２（例えば、図５のメタデータ管理システム５５２）に、通信可能に連結することができる。パブリックインターネット８５４は、コントロールプレーンＶＣＮ８１６に含まれるＮＡＴゲートウェイ８３８およびデータプレーンＶＣＮ８１８に含まれるＮＡＴゲートウェイ８３８に、通信可能に連結することができる。コントロールプレーンＶＣＮ８１６に含まれるサービスゲートウェイ８３６およびデータプレーンＶＣＮ８１８に含まれるサービスゲートウェイ８３６は、クラウドサービス８５６に通信可能に連結することができる。

【００９２】

いくつかの例では、図８のブロック図８００のアーキテクチャによって示すパターンは、図６のブロック図６００のアーキテクチャによって示すパターンの例外とみなしてもよく、ＩａａＳプロバイダが顧客と直接通信することができない場合（例えば、非接続リージョン）、ＩａａＳプロバイダの顧客にとって望ましい場合がある。顧客は、各顧客のＶＭ８６６（１）～（Ｎ）に含まれるそれぞれのコンテナ８６７（１）～（Ｎ）に、リアルタイムでアクセスすることができる。コンテナ８６７（１）～（Ｎ）は、コンテナエグレスＶＣＮ８６８に含めることができるデータプレーンアプリ層８４６のアプリサブネット８２６に含まれるそれぞれのセカンダリＶＮＩＣ８７２（１）～（Ｎ）を呼び出すように構成することができる。セカンダリＶＮＩＣ８７２（１）～（Ｎ）は、パブリックインターネット８５４に呼び出しを送信することができるＮＡＴゲートウェイ８３８に呼び出しを送信することができる。この例では、顧客がリアルタイムでアクセスすることができる

コンテナ８６７（１）～（Ｎ）は、コントロールプレーンＶＣＮ８１６から隔離することができ、データプレーンＶＣＮ８１８に含まれる他のエンティティから隔離することができる。コンテナ８６７（１）～（Ｎ）は、他の顧客のリソースから隔離することもできる。

【００９３】

他の例では、顧客は、コンテナ８６７（１）～（Ｎ）を使用して、クラウドサービス８５６を呼び出すことができる。この例では、顧客は、コンテナ８６７（１）～（Ｎ）において、クラウドサービス８５６にサービスを要求するコードを実行することができる。コンテナ８６７（１）～（Ｎ）は、この要求をセカンダリＶＮＩＣ８７２（１）～（Ｎ）に送信することができ、セカンダリＶＮＩＣ８７２（１）～（Ｎ）は、要求をパブリックインターネット８５４に送信することができるＮＡＴゲートウェイに要求を送信することができる。パブリックインターネット８５４は、インターネットゲートウェイ８３４を介して、コントロールプレーンＶＣＮ８１６に含まれるＬＢサブネット８２２にこの要求を送信することができる。要求が有効であると判定することに応答して、ＬＢサブネットは、この要求をアプリサブネット８２６に送信することができ、アプリサブネット８２６は、サービスゲートウェイ８３６を介して、この要求をクラウドサービス８５６に要求を送信することができる。

【００９４】

図に示すＩａａＳアーキテクチャ５００、６００、７００、８００は、図示するもの以外のコンポーネントを含んでもよいことが理解されるべきである。さらに、図に示す実施形態は、本開示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部の例に過ぎない。他のいくつかの実施形態では、ＩａａＳシステムは、図に示すものよりも多いかまたは少ないコンポーネントを有してもよく、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または配置を有してもよい。

【００９５】

いくつかの実施形態では、本明細書に記載するＩａａＳシステムは、セルフサービスの、サブスクリプションベースの、弾力的にスケーラブルであり、信頼性が高く、高可用性であり、セキュアな方法で顧客に提供される、アプリケーション、ミドルウェア、およびデータベースサービス提供品の一式を含むことができる。このようなＩａａＳシステムの一例は、本譲受人によって提供されるOracle Cloud Infrastructure（ＯＣＩ）である。

【００９６】

図９は、さまざまな実施形態を実行することができる、コンピュータシステム例９００を示す。システム９００は、上述したコンピュータシステムのうちの任意のものを実行するために使用することができる。図に示すように、コンピュータシステム９００は、バスサブシステム９０２を介して複数の周辺サブシステムと通信する処理ユニット９０４を含む。これらの周辺サブシステムは、処理加速ユニット９０６、Ｉ／ＯサブシステムＩ／Ｏサブシステム９０８、ストレージサブシステム９１８、および通信サブシステム９２４を含むことができる。ストレージサブシステム９１８は、有形のコンピュータ可読記憶媒体９２２とシステムメモリ９１０とを含む。

【００９７】

バスサブシステム９０２は、コンピュータシステム９００のさまざまなコンポーネントおよびサブシステムに、意図されたよう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９０２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実施形態は、複数のバスを利用してもよい。バスサブシステム９０２は、種々のバスアーキテクチャのうちの任意のものを使用する、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任意のものであってもよい。例えば、そのようなアーキテクチャとしては、業界標準アーキテクチャ（ＩＳＡ：Industry Standard Architecture）バス、マイクロチャネルアーキテク

チャ（ＭＣＡ：Micro Channel Architecture）バス、拡張ＩＳＡ（ＥＩＳＡ：Enhanced ISA）バス、ビデオエレクトロニクス規格協会（ＶＥＳＡ：Video Electronics Standards Association）ローカルバス、およびＩＥＥＥ　Ｐ１３８６．１規格に準拠して製造されたメザニン（Mezzanine）バスとして実装することができるペリフェラルコンポーネントインターコネクト（ＰＣＩ：Peripheral Component Interconnect）バスを挙げることができる。

【００９８】

１つまたは複数の集積回路（例えば、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）として実装することができる処理ユニット９０４は、コンピュータシステム９００の動作を制御する。処理ユニット９０４に、１つまたは複数のプロセッサを含めることができる。これらのプロセッサは、シングルコアプロセッサまたはマルチコアプロセッサを含むことができる。いくつかの実施形態では、処理ユニット９０４は、各処理ユニットに含まれるシングルコアまたはマルチコアプロセッサを有する１つまたは複数の独立した処理ユニット９３２および／または９３４として実装することができる。他の実施形態では、処理ユニット９０４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装してもよい。

【００９９】

さまざまな実施形態において、処理ユニット９０４は、プログラムコードに応じて種々のプログラムを実行することができ、複数の同時に実行してい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、実行すべきプログラムコードの一部またはすべてが、プロセッサ９０４におよび／またはストレージサブシステム９１８に存在することができる。好適なプログラミングを通して、プロセッサ９０４は、上述した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９００は、さらに、処理加速ユニット９０６を含むことができ、この処理加速ユニット９０６は、デジタル信号プロセッサ（ＤＳＰ）、専用プロセッサなどを含むことができる。

【０１００】

Ｉ／Ｏサブシステム９０８は、ユーザインターフェース入力デバイスおよびユーザインターフェース出力デバイスを含むことができる。ユーザインターフェース入力デバイスは、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、ダイヤル、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むことができる。ユーザインターフェース入力デバイスは、例えば、ジェスチャおよび発話コマンドを使用するナチュラルユーザインターフェースを通して、ユーザが、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制御し、それとインタラクトするのを可能にする、Microsoft Kinect（登録商標）モーションセンサなどのモーションセンシングおよび／またはジェスチャ認識デバイスを含むことができる。ユーザインターフェース入力デバイスは、ユーザから目の活動（例えば、写真撮影中および／またはメニュー選択中の「まばたき」）を検出し、目のジェスチャを入力デバイス（例えば、Google Glass（登録商標））への入力として変換する、Google Glass（登録商標）まばたき検出器などのアイジェスチャ認識デバイスも含むことができる。さらに、ユーザインターフェース入力デバイスは、ユーザが音声コマンドを介して音声認識システム（例えば、Ｓｉｒｉ（登録商標）ナビゲータ）と対話するのを可能にする音声認識センシングデバイスを含んでもよい。

【０１０１】

ユーザインターフェース入力デバイスはまた、限定されないが、３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、デジタルビデオカメラ、ポータブルメディアプレーヤ、ウェブカメラなどのオーディオ／ビジュアルデバイス、イメージスキャナ、指紋スキャナ、バーコードリーダ３Ｄスキャナ、３Ｄプリンタ、レーザ測距装置、な

らびに視線追跡デバイスを含んでもよい。さらに、ユーザインターフェース入力デバイスは、例えば、コンピュータ断層撮影装置、磁気共鳴画像装置、陽電子断層撮影装置、医療用超音波検査装置などの医療用画像入力装置を含んでもよい。ユーザインターフェース入力デバイスはまた、例えば、ＭＩＤＩキーボード、デジタル楽器などの音声入力装置を含んでもよい。

【０１０２】

ユーザインターフェース出力デバイスは、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視覚的ディスプレイなどを含むことができる。ディスプレイサブシステムは、陰極線管（ＣＲＴ）、液晶ディスプレイ（ＬＣＤ）またはプラズマディスプレイを使用するようなフラットパネル装置、投影装置、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」という用語の使用は、コンピュータシステム９００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すべてのあり得るタイプのデバイスおよび機構を含むように意図されている。例えば、ユーザインターフェース出力デバイスは、限定されないが、モニタ、プリンタ、スピーカ、ヘッドフォン、自動車用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、テキスト、グラフィック、およびオーディオ／ビデオ情報を視覚的に伝える種々の表示デバイスを含むことができる。

【０１０３】

コンピュータシステム９００は、現在システムメモリ９１０内に位置しているように示されているソフトウェア要素を含む、ストレージサブシステム９１８を含むことができる。システムメモリ９１０は、処理ユニット９０４にロード可能であり処理ユニット９０４で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することができる。

【０１０４】

コンピュータシステム９００の構成およびタイプに応じて、システムメモリ９１０は、揮発性（ランダムアクセスメモリ（ＲＡＭ）など）および／または不揮発性（リードオンリメモリ（ＲＯＭ）、フラッシュメモリなど）であってもよい。ＲＡＭは、典型的には、処理ユニット９０４が即座にアクセス可能であるおよび／または現在操作し実行している、データおよび／またはプログラムモジュールを含む。いくつかの実施態様では、システムメモリ９１０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むことができる。いくつかの実施態様では、ＲＯＭには、典型的には、起動中などでコンピュータシステム９００内の要素間で情報を転送するのに役立つ基本ルーチンを含む基本入出力システム（ＢＩＯＳ）を格納することができる。限定ではなく例として、システムメモリ９１０はまた、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（ＲＤＢＭＳ）などを含むことができるアプリケーションプログラム９１２と、プログラムデータ９１４と、オペレーティングシステム９１６とを示す。例として、オペレーティングシステム９１６は、さまざまなバージョンのMicrosoft Windows（登録商標）、Apple Macintosh（登録商標）、および／またはＬｉｎｕｘオペレーティングシステム、種々の市販のＵＮＩＸ（登録商標）またはＵＮＩＸ系オペレーティングシステム（限定されないが、種々の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）、および／またはｉＯＳ、Windows（登録商標）Phone、Ａｎｄｒｏｉｄ（登録商標）ＯＳ、ＢｌａｃｋＢｅｒｒｙ（登録商標）１０　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を含むことができる。

【０１０５】

ストレージサブシステム９１８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可読記憶媒体も提供することができる。ストレージサブシステム９１８には、プロセッサによって実行されると上述した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）を格納

することができる。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９０４が実行することができる。ストレージサブシステム９１８は、本開示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することができる。

【０１０６】

ストレージサブシステム９００は、コンピュータ可読記憶媒体９２２にさらに接続することができるコンピュータ可読記憶媒体リーダ９２０も含むことができる。システムメモリ９１０とともに、任意選択的に組み合わせて、コンピュータ可読記憶媒体９２２は、コンピュータ可読情報を一時的におよび／またはより恒久的に収容し、格納し、伝送し、取得するための、リモート、ローカル、固定、および／またはリムーバブル記憶デバイスに記憶媒体を加えて、包括的に表すことができる。

【０１０７】

コード、またはコードの一部を含むコンピュータ可読記憶媒体９２２は、限定されないが、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で実装される、揮発性および不揮発性、リムーバルおよび非リムーバブル媒体などの記憶媒体および通信媒体を含む、本技術分野において既知であるかまたは使用されている任意の適切な媒体も含むことができる。これは、ＲＡＭ、ＲＯＭ、電子的に消去可能なプログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）、もしくは他の光学記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置もしくは他の磁気記憶デバイス、または他の有形のコンピュータ可読媒体などの有形のコンピュータ可読記憶媒体を含むことができる。これは、所望の情報を伝送するために使用することができ、コンピューティングシステム９００がアクセスすることができる、データ信号、データ伝送、または他の任意の媒体などの、非有形のコンピュータ可読媒体も含むことができる。

【０１０８】

例として、コンピュータ可読記憶媒体９２２は、非リムーバブル不揮発性磁気媒体から読み出すかまたは非リムーバブル不揮発性磁気媒体に書き込む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から読み出すかまたはリムーバブル不揮発性磁気ディスクに書き込む磁気ディスクドライブ、および、ＣＤ　ＲＯＭ、ＤＶＤ、およびＢｌｕ－Ｒａｙ（登録商標）ディスク、または他の光学媒体などのリムーバブル不揮発性光ディスクから読み出すかまたはリムーバブル不揮発性光ディスクに書き込む光ディスクドライブを含むことができる。コンピュータ可読記憶媒体９２２としては、限定されないが、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（ＵＳＢ）フラッシュドライブ、セキュアデジタル（ＳＤ）カード、ＤＶＤディスク、デジタルビデオテープなどを挙げることができる。コンピュータ可読記憶媒体９２２としては、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（ＳＳＤ）、ソリッドステートＲＡＭ、ダイナミックＲＡＭ、スタティックＲＡＭ、ＤＲＡＭベースのＳＳＤ、磁気抵抗ＲＡＭ（ＭＲＡＭ）ＳＳＤなどの揮発性メモリに基づく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も挙げることができる。ディスクドライブおよびそれらの関連するコンピュータ可読媒体は、コンピュータシステム９００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不揮発性ストレージを提供することができる。

【０１０９】

通信サブシステム９２４は、他のコンピュータシステムおよびネットワークへのインターフェースを提供する。通信サブシステム９２４は、コンピュータシステム９００からデータを受信し、コンピュータシステム９００から他のシステムにデータを送信するためのインターフェースとして機能する。例えば、通信サブシステム９２４は、コンピュータシステム１０００がインターネットを介して１つまたは複数のデバイスに接続するのを可能にすることができる。いくつかの実施形態では、通信サブシステム９２４は、（例えば、携帯電話技術、３Ｇ、４Ｇもしくは ＥＤＧＥ（enhanced data rates for global ev

olution）などの高度データネットワーク技術、Ｗｉ－Ｆｉ（ＩＥＥＥ　８０２．１１ファミリ規格、または他のモバイル通信技術、またはそれらの任意の組み合わせを使用する）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（ＲＦ）トランシーバコンポーネント、全地球測位システム（ＧＰＳ）受信機コンポーネント、および／または他のコンポーネントを含むことができる。いくつかの実施形態では、通信サブシステム９２４は、無線インターフェースに加えてまたはその代わりに、有線ネットワーク接続性（例えば、Ｅｔｈｅｒｎｅｔ（登録商標））を提供することができる。

【０１１０】

いくつかの実施形態では、通信サブシステム９２４は、コンピュータシステム９００を使用することができる１人または複数のユーザに代わって、構造化および／または非構造化データフィード９２６、イベントストリーム９２８、イベントアップデート９３０などの形態の入力通信を受け取ることもできる。

【０１１１】

例として、通信サブシステム９２４は、Ｔｗｉｔｔｅｒ（登録商標）フィード、Ｆａｃｅｂｏｏｋ（登録商標）アップデート、リッチサイトサマリー（ＲＳＳ：Rich Site Summary）フィードなどのウェブフィード、および／または１つもしくは複数のサードパーティ情報源からのリアルタイムアップデートなど、ソーシャルネットワークおよび／または他の通信サービスのユーザからデータフィード９２６をリアルタイムで受信するように構成してもよい。

【０１１２】

さらに、通信サブシステム９２４は、明確な終わりがない本質的に連続的なまたは無限である可能性がある、リアルタイムイベントのイベントストリーム９２８および／またはイベントアップデート９３０を含むことができる、連続データストリームの形態のデータを受信するように構成することもできる。連続データを生成するアプリケーションの例としては、例えば、センサデータアプリケーション、金融ティッカー、ネットワークパフォーマンス測定ツール（例えば、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分析ツール、自動車交通監視などを挙げることができる。

【０１１３】

通信サブシステム９２４は、構造化および／または非構造化データフィード９２６、イベントストリーム９２８、イベントアップデート９３０などを、コンピュータシステム９００に連結された１つまたは複数のストリーミングデータソースコンピュータと通信することができる１つまたは複数のデータベースに出力するように構成することもできる。

【０１１４】

コンピュータシステム９００は、ハンドヘルドポータブルデバイス（例えば、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（例えば、Google Glass（登録商標）ヘッドマウントディスプレイ）、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、または他の任意のデータ処理システムを含む、さまざまなタイプのうちの１つとすることができる。

【０１１５】

コンピュータおよびネットワークの性質は常に変化するため、図に示すコンピュータシステム９００の説明は、単に具体的な一例として意図されている。図に示すシステムよりも多いかまたは少ないコンポーネントを有する他の多くの構成が可能である。例えば、カスタマイズされたハードウェアを使用してもよく、および／または、特定の要素を、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装してもよい。さらに、ネットワーク入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を採用してもよい。本明細書で提供する開示および教示に基づいて、当業者であれば、さまざまな実施形態を実装するための他の様式および／または方法を理解するであろう。

【０１１６】

具体的な実施形態について説明してきたが、さまざまな変更形態、改変形態、代替構造、および均等物も、本開示の範囲内に包含される。実施形態は、ある具体的なデータ処理環境内で動作するようには限定されず、複数のデータ処理環境内で自由に動作することができる。さらに、実施形態について、特定の一連のトランザクションおよびステップを用いて説明してきたが、本開示の範囲が記載した一連のトランザクションおよびステップに限定されないことは、当業者には明らかなはずである。上述した実施形態のさまざまな特徴および態様は、個別に使用しても共同で使用してもよい。

【０１１７】

さらに、実施形態について、ハードウェアおよびソフトウェアの特定の組み合わせを用いて説明してきたが、ハードウェアおよびソフトウェアの他の組み合わせも本開示の範囲内にあることが認識されるべきである。実施形態は、ハードウェアのみで実行しても、またはソフトウェアのみで実行しても、またはそれらの組み合わせを用いて実行してもよい。本明細書に記載するさまざまなプロセスは、同じプロセッサで実行することも、任意の組み合わせの異なるプロセッサで実行することもできる。したがって、コンポーネントまたはモジュールについて、いくつかの動作を実行するように構成されているものとして説明している場合、そのような構成は、例えば、その動作を実行するように電子回路を設計することによって、その動作を実行するようにプログラム可能な電子回路（マイクロプロセッサなど）をプログラムすることによって、またはそれらの任意の組み合わせによって、実現することができる。プロセスは、限定されないが、プロセス間通信を行う従来の技術を含む種々の技術を用いて、通信することができ、プロセスの異なる対は、異なる技術を使用することができ、または、プロセスの同じ対は、異なる時点で異なる技術を使用することができる。

【０１１８】

したがって、明細書および図面は、制限的な意味ではなく例示的な意味で考慮されるべきである。しかしながら、特許請求の範囲に示すようなより広義の趣旨および範囲から逸脱することなく、追加、削減、削除、および他の改変および変更を行ってもよいことは、明らかとなろう。したがって、具体的な開示の実施形態について説明してきたが、これらは、限定的であるようには意図されていない。さまざまな変更形態および均等物は、続く特許請求の範囲内にある。

【０１１９】

開示する実施形態について説明する文脈において（特に続く特許請求の範囲の文脈において）「１つの、ある（ａ、ａｎ）」、および「その（ｔｈｅ）」という用語および同様の指示対象の使用は、本明細書において別段の指示がなく、文脈上明らかに矛盾しない限り、単数および複数の両方を包含するように解釈されるべきである。「備える（comprising）」、「有する（having）」、「含む（including）」、および「含む（containing）」という用語は、特に断りのない限り、非限定的な（open-ended）用語（すなわち、「を含むが、限定されない」を意味する）として解釈されるべきである。「接続され」という用語は、介在するものがあっても、部分的にまたは全体として、その内部に含まれている、それに取り付けられている、または互いに接合されているとして解釈されるべきである。本明細書における値の範囲の列挙は、本明細書において別段の指示のない限り、単に、その範囲内にある各個別の値を個々に言及する略記方法としての役割を果たすように意図されているに過ぎず、各個別の値は、本明細書に個々に列挙されているかのように、本明細書に組み込まれる。本明細書において別段の指示がなく、または文脈上明らかに矛盾しない限り、本明細書に記載するすべての方法は、任意の好適な順序で行うことができる。本明細書に提供するありとあらゆる例、または例示的な文言（例えば、「など」）の使用は、単に実施形態をより明瞭にするように意図されるものであり、別段の請求のない限り、本開示の範囲を限定するものではない。本明細書中のいかなる文言も、請求されていないいかなる要素も本開示の実施に不可欠であるものとして示すものとしても解釈されるべきではない。

【０１２０】

「Ｘ、Ｙ、またはＺのうちの少なくとも１つ」という句など、選言的な文言は、具体的に別段の定めのない限り、項目、用語などがＸ、Ｙ、もしくはＺのいずれか、またはそれらの任意の組み合わせ（例えば、Ｘ、Ｙ、および／またはＺ）であってもよいことを示すために一般的に用いられるものとして文脈内で理解されるように意図されている。したがって、このような選言的な文言は、一般に、いくつかの実施形態が、Ｘのうちの少なくとも１つ、Ｙのうちの少なくとも１つ、またはＺのうちの少なくとも１つが各々存在することを必要とすることを、意味するようには意図されておらず、意味するべきではない。

【０１２１】

本明細書では、本開示を実施するために知られている最良の形態を含む、本開示の好ましい実施形態について説明している。当業者には、前述の説明を読むことにより、これらの好ましい実施形態の変形形態が明らかとなろう。当業者であれば、このような変形形態を適宜採用することができるはずであり、本開示は、本明細書に具体的に説明したもの以外の方法で実施してもよい。したがって、本開示は、適用法によって許容される、本明細書に添付の特許請求の範囲に記載する主題のすべての変更形態および均等物を含む。さらに、本明細書において別段の指示のない限り、そのすべてのあり得る変形における上述した要素の任意の組み合わせは、本開示に包含される。

【０１２２】

本明細書に引用した刊行物、特許出願、および特許を含むすべての参考文献は、各文献が参照により組み込まれることが個々に具体的に示され、その全体が本明細書に記載された場合と同じ程度に、参照により組み込まれる。

【０１２３】

前述の明細書では、本開示の態様をその具体的な実施形態に関して説明したが、当業者であれば、本開示はそれらに限定されないことを認識するであろう。上述した開示のさまざまな特徴および態様は、個々にまたは共同で使用することができる。さらに、実施形態は、本明細書のより広い趣旨および範囲から逸脱することなく、本明細書に記載したものを越える任意の数の環境および用途において利用することができる。したがって、本明細書および図面は、制限的ではなく例示的なものとみなされるべきである。

【図面】

【図１】

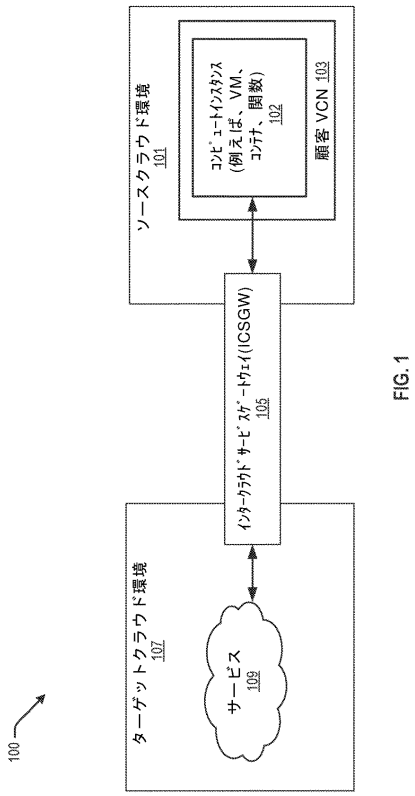


FIG. 1

【図２】

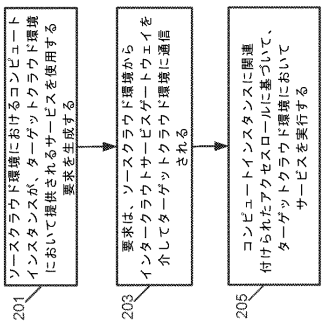


FIG. 2

【図３Ａ】

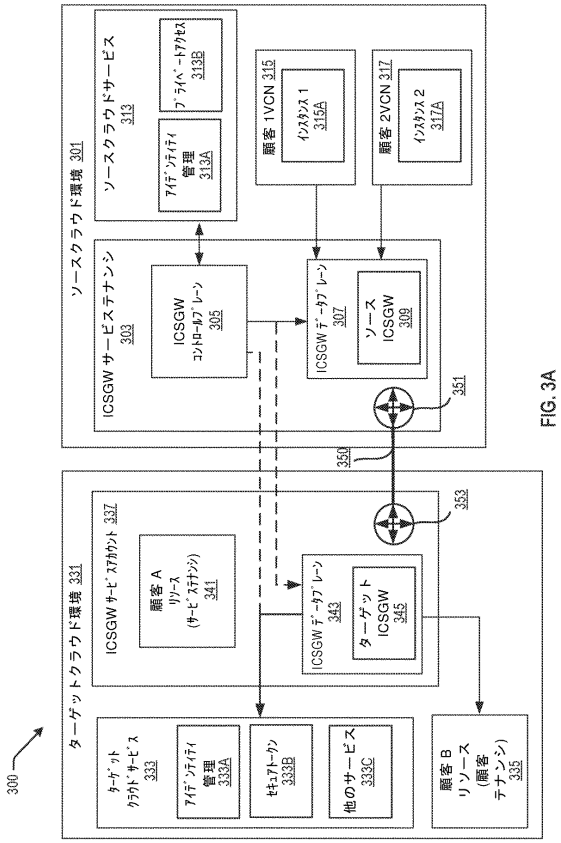


FIG. 3A

【図３Ｂ】

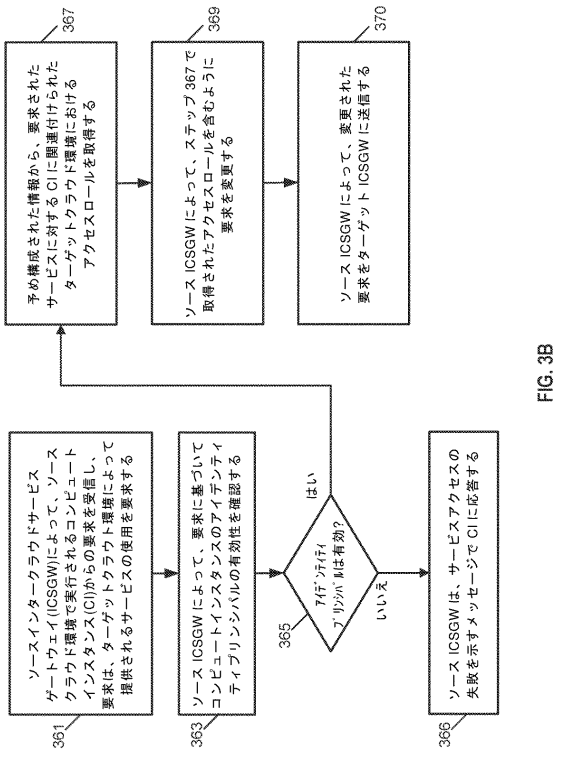


FIG. 3B

【図３Ｃ】

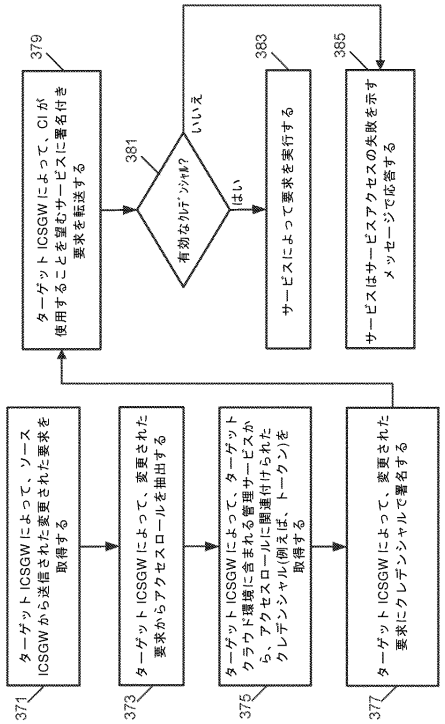


FIG. 3C

【図４Ａ】

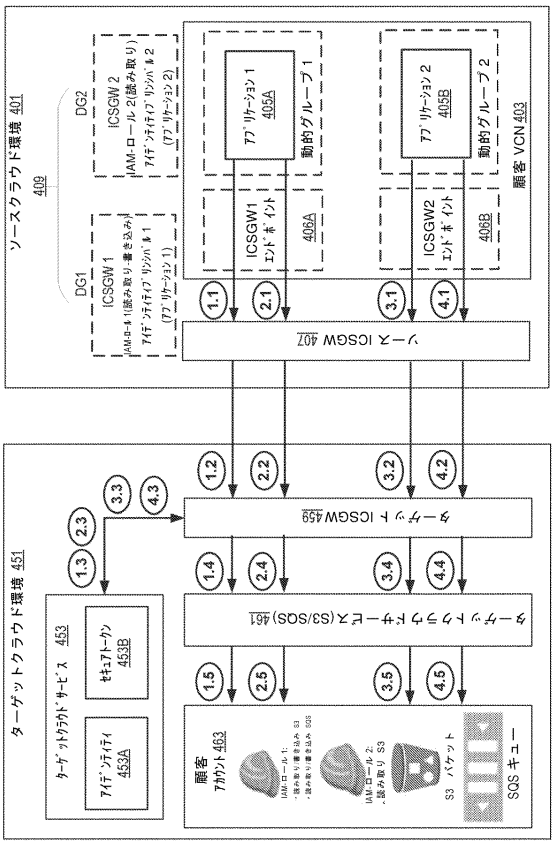


FIG. 4A

【図４Ｂ】

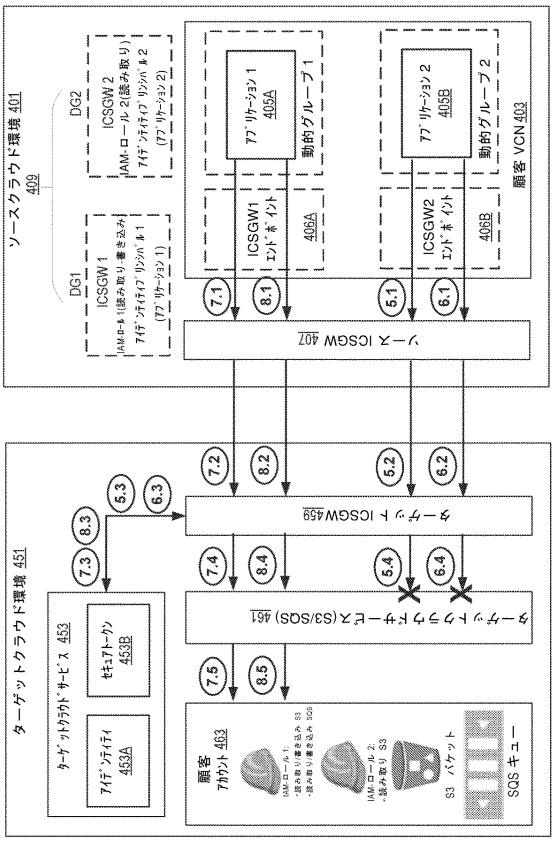


FIG. 4B

【図５】

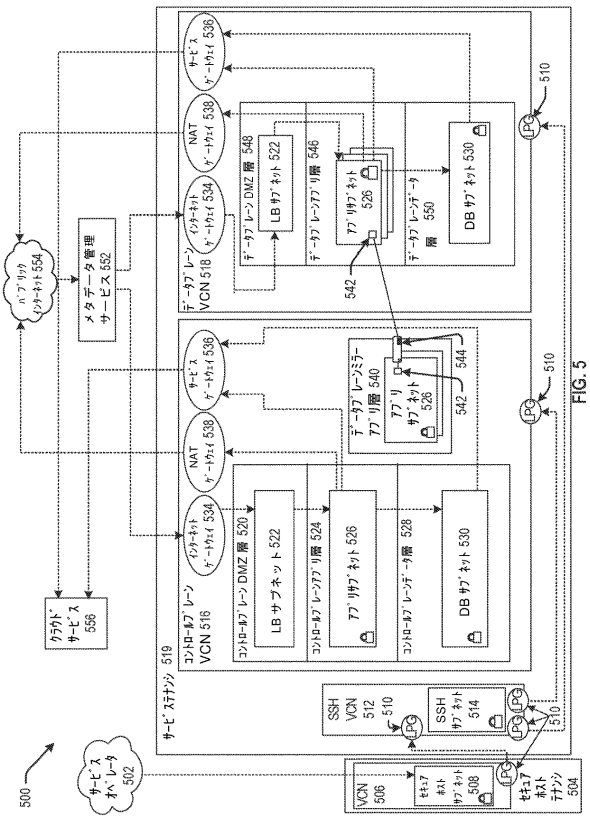


FIG. 5

【図６】

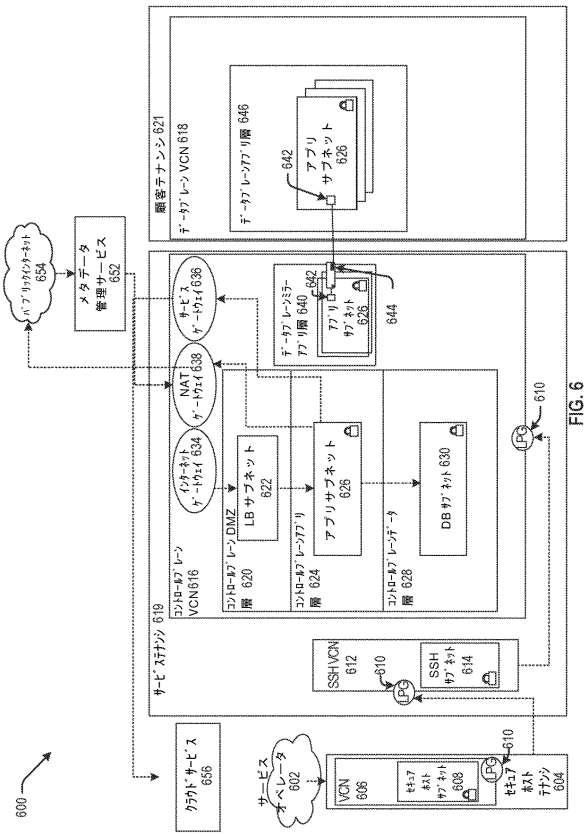


FIG. 6

【図７】

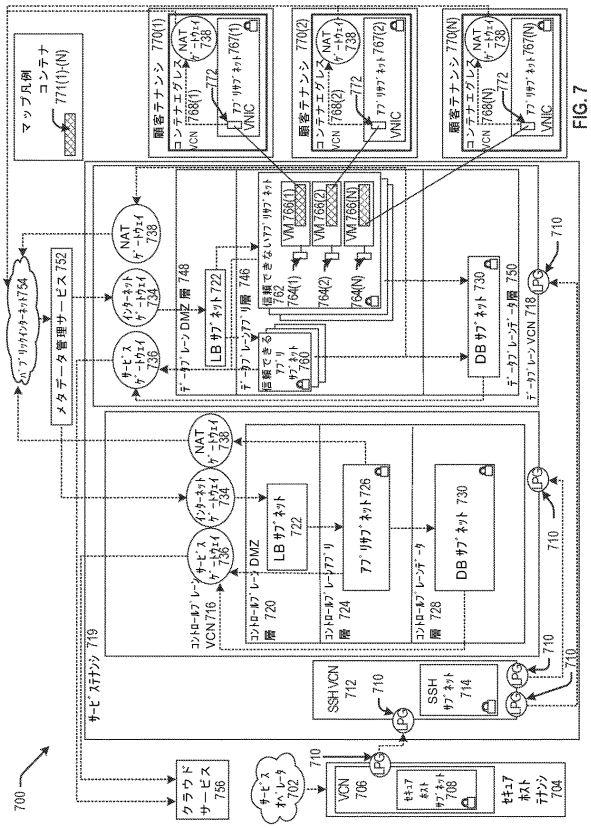


FIG. 7

【図８】

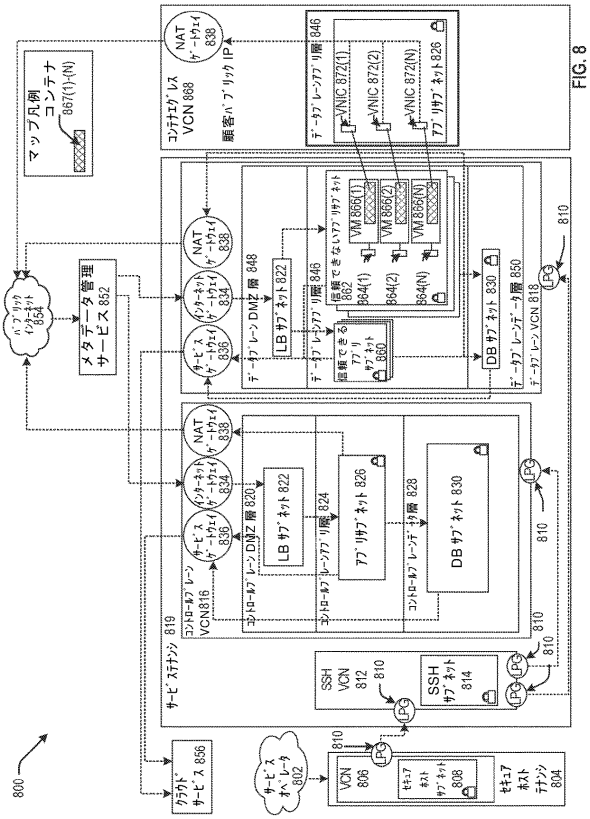


FIG. 8

【図９】

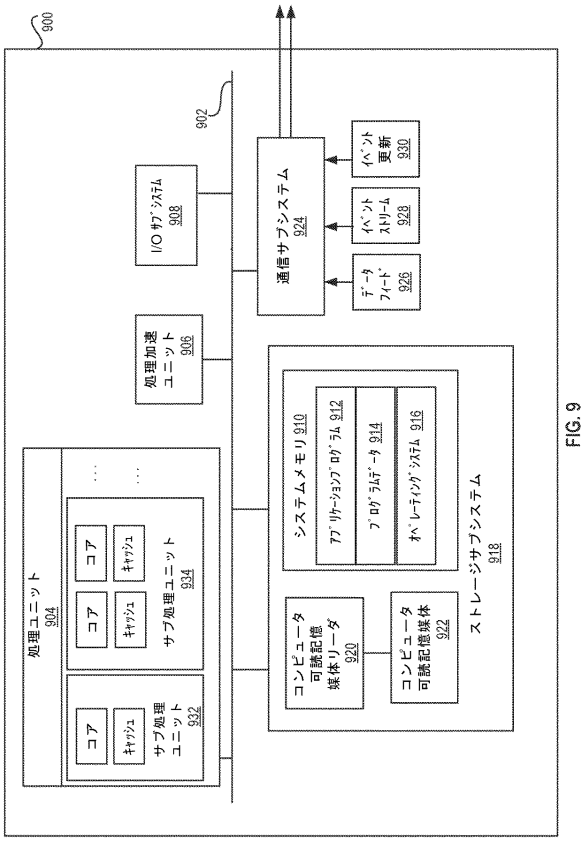


FIG. 9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2023/020663

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/62 H04L9/40
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105 049 408 A (CITY CLOUD DATA CT CO LTD) 11 November 2015 (2015-11-11) page 2, line 39 - page 3, line 35 page 8, line 38 - page 11, line 16	1-20
A	CN 110 990 858 A (UNIV SUN YAT SEN) 10 April 2020 (2020-04-10) paragraph [0029] - paragraph [0050]	1-20
A	US 2017/006119 A1 (POGREBINSKY VLADIMIR [US] ET AL) 5 January 2017 (2017-01-05) paragraph [0028] - paragraph [0066]	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 August 2023	25/08/2023

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Cartrysse, Kathy

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2023/020663

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN 105049408 A	11-11-2015	NONE	
CN 110990858 A	10-04-2020	NONE	
US 2017006119 A1	05-01-2017	US 2017006119 A1	05-01-2017
		US 2019045018 A1	07-02-2019
		US 2020213404 A1	02-07-2020

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

,MC,ME,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MU,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．ＷＩＮＤＯＷＳ　ＰＨＯＮＥ
２．ｉＯＳ

イション内
(72)発明者　バビラパッリ，スリカンス
アメリカ合衆国、９４０６５　カリフォルニア州、レッドウッド・ショアーズ、メール・ストップ・５・オー・ピー・７、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション内