

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号

特表2024-538626

(P2024-538626A)

(43)公表日 令和6年10月23日(2024.10.23)

(51)国際特許分類

F I

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62 3 1 8

G 0 6 F 21/64 (2013.01)

G 0 6 F 21/64

審査請求 未請求 予備審査請求 未請求 (全56頁)

(21)出願番号 特願2024-519653(P2024-519653)
(86)(22)出願日 令和4年9月27日(2022.9.27)
(85)翻訳文提出日 令和6年4月11日(2024.4.11)
(86)国際出願番号 PCT/US2022/044894
(87)国際公開番号 WO2023/055734
(87)国際公開日 令和5年4月6日(2023.4.6)
(31)優先権主張番号 63/250,980
(32)優先日 令和3年9月30日(2021.9.30)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 63/250,992
(32)優先日 令和3年9月30日(2021.9.30)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 17/953,175

最終頁に続く

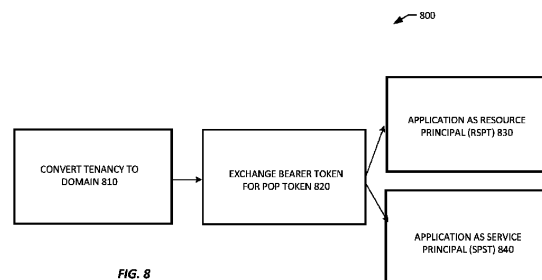
(71)出願人 502303739
オラクル・インターナショナル・コーポ
レイション
アメリカ合衆国 9 4 0 6 5 カリフォル
ニア州 レッドウッド ショアーズ、メー
ル ストップ 5 オーピー 7 オラクル パ
ークウェイ 5 0 0
(74)代理人 110001195
弁理士法人深見特許事務所
(72)発明者 ウィルソン、グレッグ・アラン
アメリカ合衆国、9 4 0 6 5 カリフォ
ルニア州、レッドウッド・シティ、オ
ラクル・パークウェイ、5 0 0
(72)発明者 エルメンシャウィ、アイマン・モハメド
・アリー・ハッサン

最終頁に続く

(54)【発明の名称】 リソースプリンシパルまたはサービスプリンシパルとしてのアプリケーション

(57)【要約】

第1のタイプのアイデンティティトークンを用いる、第1のタイプのアイデンティティシステムのアプリケーションが、第2のタイプのアイデンティティトークンを用いる、第2のタイプのアイデンティティシステムにアクセスすることを認める技術が提供される。アプリケーションはトークン交換システムへの要求を行うことができる。要求はアプリケーションのベアラートークンおよび公開鍵を含むことができる。トークン交換システムは、検証ステップを遂行した後に、ベアラートークンを所持証明トークンと交換することができる。トークン交換システムは、第2のアイデンティティシステムにアクセスするためのクレデンシャルの入力を必要とすることなく、第1のアイデンティティシステムのための第1のトークン（例えば、ベアラートークン）を第2のアイデンティティシステムのための第2のトークン（例えば、所持証明トークン）と交換することができる。



【特許請求の範囲】**【請求項 1】**

方法であって、

クラウドサービスの統合アイデンティティ管理システムのトークン交換システムにより、エンティティが第 1 のアイデンティティシステムにアクセスすることを認可されると決定することを含み、前記エンティティはアプリケーションであり、前記方法は、

前記トークン交換システムにより、前記エンティティが第 2 のアイデンティティシステムにアクセスするための第 1 の要求を生成することをさらに含み、前記第 1 の要求は、前記エンティティに関連付けられたベアラートークンおよび第 1 の公開鍵を含み、前記方法は、

前記トークン交換システムにより、前記ベアラートークンが有効なベアラートークンであることを検証することと、

前記トークン交換システムにより、前記エンティティのロールが、前記第 2 のアイデンティティシステムにアクセスすることを認可されたロールであるかどうかを検証することと、

前記トークン交換システムにより、前記第 1 の要求において受信された前記ベアラートークンおよび前記第 1 の公開鍵に基づいて第 2 のトークンを生成することと、

前記トークン交換システムにより、前記第 2 のトークンを前記エンティティへ送信することとをさらに含み、

前記第 2 のトークンは前記第 2 のアイデンティティシステムに関連付けられており、前記第 2 のトークンは前記エンティティの前記第 1 の公開鍵を含む、方法。

【請求項 2】

前記トークン交換システムにより、前記エンティティが前記第 2 のアイデンティティシステムにアクセスするための第 2 の要求を生成することをさらに含み、前記第 2 の要求は前記第 2 のトークンを含み、前記第 2 の要求は前記エンティティのプライベート鍵によって署名され、前記方法は、

前記トークン交換システムにより、前記エンティティが、前記第 2 のアイデンティティシステムにアクセスすることを認可されたアイデンティティを有することを検証することと、

前記トークン交換システムにより、前記エンティティが前記第 2 のアイデンティティシステムにアクセスすることを認可することとをさらに含む、請求項 1 に記載の方法。

【請求項 3】

前記エンティティが、前記第 2 のアイデンティティシステムにアクセスすることを認可された前記アイデンティティを有することを検証することは、

前記トークン交換システムにより、前記エンティティが、前記第 2 の要求に署名した前記エンティティであることを検証すること、および

前記トークン交換システムにより、前記第 2 のトークンが、前記第 2 のアイデンティティシステムにアクセスすることを認可されていることを検証することを含む、請求項 2 に記載の方法。

【請求項 4】

前記第 2 のトークンは所持証明（P o P）トークンである、請求項 1 に記載の方法。

【請求項 5】

前記エンティティが前記第 2 のアイデンティティシステムにアクセスすることを認可することは、前記エンティティにリソースプリンシパルの特権を与えることを含む、請求項 1 に記載の方法。

【請求項 6】

前記エンティティが前記第 2 のアイデンティティシステムにアクセスすることを認可することは、前記エンティティにサービスプリンシパルの特権を与えることを含む、請求項 1 に記載の方法。

【請求項 7】

前記リソースプリンシプルは、前記第 2 のアイデンティティシステムのリソースにアクセスすることを認可される、請求項 5 に記載の方法。

【請求項 8】

サービスプリンシプルは、前記第 2 のアイデンティティシステムのサービスにアクセスすることを認可される、請求項 4 に記載の方法。

【請求項 9】

前記エンティティは、前記第 2 のアイデンティティシステムにおけるエンティティクレデンシャルの入力を必要とすることなく前記第 2 のトークンを用いて前記第 2 のアイデンティティシステム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）にアクセスすることを認可される、請求項 1 に記載の方法。

10

【請求項 10】

前記エンティティは、前記第 1 のアイデンティティシステムのための前記エンティティのクレデンシャルに基づいて前記第 1 のアイデンティティシステムにアクセスすることを認可されると決定される、請求項 2 に記載の方法。

【請求項 11】

前記第 1 のアイデンティティシステムは第 1 のシステムモデルを有し、前記第 2 のアイデンティティシステムは、前記第 1 のシステムモデルとは異なる仕様を有する第 2 のシステムモデルを有する、請求項 1 に記載の方法。

【請求項 12】

前記エンティティは統合クラウドサービスアプリケーションである、請求項 1 に記載の方法。

20

【請求項 13】

前記統合クラウドサービスアプリケーションは、SaaS アプリケーション、PaaS アプリケーション、または融合アプリケーションである、請求項 12 に記載の方法。

【請求項 14】

1 つまたは複数の非一時的機械可読媒体内に有形に組み込まれたコンピュータプログラム製品であって、前記コンピュータプログラム製品は、1 つまたは複数のデータプロセッサに、方法を遂行させるように構成された命令を含み、前記方法は、

クラウドサービスの統合アイデンティティ管理システムのトークン交換システムにより、エンティティが第 1 のアイデンティティシステムにアクセスすることを認可されると決定することを含み、前記エンティティはアプリケーションであり、前記方法は、

30

前記トークン交換システムにより、前記エンティティが第 2 のアイデンティティシステムにアクセスするための第 1 の要求を生成することをさらに含み、前記第 1 の要求は、前記エンティティに関連付けられたベアラートークンおよび第 1 の公開鍵を含み、前記方法は、

前記トークン交換システムにより、前記ベアラートークンが有効なベアラートークンであることを検証することと、

前記トークン交換システムにより、前記エンティティのロールが、前記第 2 のアイデンティティシステムにアクセスすることを認可されたロールであるかどうかを検証することと、

40

前記トークン交換システムにより、前記第 1 の要求において受信された前記ベアラートークンおよび前記第 1 の公開鍵に基づいて第 2 のトークンを生成することと、

前記トークン交換システムにより、前記第 2 のトークンを前記エンティティへ送信することとをさらに含み、前記第 2 のトークンは前記第 2 のアイデンティティシステムに関連付けられており、前記第 2 のトークンは前記エンティティの前記第 1 の公開鍵を含む、コンピュータプログラム製品。

【請求項 15】

前記方法は、前記トークン交換システムにより、前記エンティティが前記第 2 のアイデンティティシステムにアクセスするための第 2 の要求を生成することをさらに含み、前記第 2 の要求は前記第 2 のトークンを含み、前記第 2 の要求は前記エンティティのプライベ

50

ート鍵によって署名され、前記方法は、

前記トークン交換システムにより、前記エンティティが、前記第2のアイデンティティシステムにアクセスすることを認可されたアイデンティティを有することを検証することと、

前記トークン交換システムにより、前記エンティティが前記第2のアイデンティティシステムにアクセスすることを認可することとをさらに含む、請求項14に記載のコンピュータプログラム製品。

【請求項16】

前記エンティティが、前記第2のアイデンティティシステムにアクセスすることを認可された前記アイデンティティを有することを検証することは、

前記トークン交換システムにより、前記エンティティが、前記第2の要求に署名した前記エンティティであることを検証すること、および

前記トークン交換システムにより、前記第2のトークンが、前記第2のアイデンティティシステムにアクセスすることを認可されていることを検証することを含む、請求項15に記載のコンピュータプログラム製品。

【請求項17】

システムであって、

1つまたは複数のデータプロセッサと、

前記1つまたは複数のデータプロセッサによって実行されると、前記1つまたは複数のデータプロセッサに方法を遂行させる命令を記憶する1つまたは複数の非一時的コンピュ

ータ可読媒体とをさらに備え、前記方法は、
クラウドサービスの統合アイデンティティ管理システムのトークン交換システムにより、エンティティが第1のアイデンティティシステムにアクセスすることを認可されると決定することを含み、前記エンティティはアプリケーションであり、前記方法は、

前記トークン交換システムにより、前記エンティティが第2のアイデンティティシステムにアクセスするための第1の要求を生成することをさらに含み、前記第1の要求は、前記エンティティに関連付けられたベアラートークンおよび第1の公開鍵を含み、前記方法は、

前記トークン交換システムにより、前記ベアラートークンが有効なベアラートークンであることを検証することと、

前記トークン交換システムにより、前記エンティティのロールが、前記第2のアイデンティティシステムにアクセスすることを認可されたロールであるかどうかを検証することと、

前記トークン交換システムにより、前記第1の要求において受信された前記ベアラートークンおよび前記第1の公開鍵に基づいて第2のトークンを生成することと、

前記トークン交換システムにより、前記第2のトークンを前記エンティティへ送信することとをさらに含み、前記第2のトークンは前記第2のアイデンティティシステムに関連付けられており、前記第2のトークンは前記エンティティの前記第1の公開鍵を含む、システム。

【請求項18】

前記方法は、前記トークン交換システムにより、前記エンティティが前記第2のアイデンティティシステムにアクセスするための第2の要求を生成することをさらに含み、前記第2の要求は前記第2のトークンを含み、前記第2の要求は前記エンティティのプライベート鍵によって署名され、前記方法は、

前記トークン交換システムにより、前記エンティティが、前記第2のアイデンティティシステムにアクセスすることを認可されたアイデンティティを有することを検証することと、

前記トークン交換システムにより、前記エンティティが前記第2のアイデンティティシステムにアクセスすることを認可することとをさらに含む、請求項17に記載のシステム

。

【請求項 19】

前記エンティティが、前記第2のアイデンティティシステムにアクセスすることを認可された前記アイデンティティを有することを検証することは、

前記トークン交換システムにより、前記エンティティが、前記第2の要求に署名した前記エンティティであることを検証すること、および

前記トークン交換システムにより、前記第2のトークンが、前記第2のアイデンティティシステムにアクセスすることを認可されていることを検証することを含む、請求項18に記載のシステム。

【発明の詳細な説明】

【背景技術】

10

【0001】

関連出願の相互参照

本出願は、「APPLICATIONS AS RESOURCE PRINCIPALS OR SERVICE PRINCIPALS」と題する2022年9月26日に出願された、非仮特許出願第17/953,175号に対する優先権を主張する。同出願は、米国特許法第119条(e)の下で、「TOKEN EXCHANGE BETWEEN BEARER AND POP TOKENS」と題する2021年9月30日に出願された、米国仮特許出願第63/250,992号、および「APPLICATIONS AS RESOURCE PRINCIPALS OR SERVICE PRINCIPALS」と題する2021年9月30日に出願された、米国仮特許出願第63/250,980号の利益および優先権を主張する。これらの出願の内容全体は全ての目的のために本明細書において参照により組み込まれる。

20

【0002】

背景

インフラストラクチャアイデンティティおよびアクセス管理(IAM: Identity and Access Management)システムならびにアイデンティティクラウドサービス(IDCS: Identity Cloud Service)システムなどの、アイデンティティ管理システムと対話するには、アクセストークンが必要とされる。例えば、IAMシステムの場合、トークンは所持証明(POP: Proof of Possession)トークンを含むことができ、アイデンティティクラウドサービス(IDCS)システムの場合、トークンはベアラートークンを含むことができる。ユーザが異なるアイデンティティアクセス管理システムのサービスまたはリソースにアクセスすることを欲する場合、ユーザは、各タイプのアイデンティティアクセス管理システムにアクセスするために別個のアクセストークンを必要とするであろう。

30

【0003】

しかし、異なるアイデンティティ管理システムのための異なるトークンを管理することはユーザへの負担となる。さらに、所与のセッションにおいて、ユーザは異なるアイデンティティ管理システムの間で対話し得、これにより、異なるアイデンティティ管理システムのフィーチャにアクセスするための異なるアクセストークンを必要とする。異なるアクセストークンを取得すること、および提供することをユーザに要請することは、ワークフローを中断し、タスクの遂行における非効率性をもたらす。

40

【0004】

さらに、ユーザは、各タイプのアイデンティティ管理システムのためのサービスを管理するためにクレデンシャルのセットを維持しなければならないであろう。ユーザは各アイデンティティ管理システムに別個にログインし、各アイデンティティ管理システムと通信するための別個のアクセストークンを取得しなければならないであろう。さらに、各タイプのアイデンティティ管理システムのためのアクセストークンはアイデンティティシステムごとに別個に記憶されるであろう。

【0005】

さらに、ベアラートークンを有する、アプリケーションなどの、一部のエンティティはそれらのベアラートークンをPOPトークンと交換することができないことがある。具体

50

的には、一部のエンティティは、それらがベアラートークンを P o P トークンと交換することを可能にする特権を有しないことがある。これは、エンティティがアプリケーションであり、アプリケーションが、I A M アイデンティティシステム内のリソースおよびサービスなどの、P o P トークンを必要とするリソースまたはサービスにアクセスすることを欲する場合に、さらなる困難をもたらす。

【0006】

本開示の例示的な実施形態はこれらおよび他の問題に、個々に、および共同して対処する。

【発明の概要】

【0007】

概要

例示的な実施形態は、異なるアイデンティティ管理システム間のトークン交換に関する。詳細には、例示的な実施形態は、第1のタイプのアイデンティティ管理システムのベアラートークンを第2のタイプのアイデンティティ管理システムの所持証明 (P o P) タイプのトークンと交換すること、およびその逆に関する。

【0008】

例示的な実施形態はまた、アプリケーションなどのエンティティのための、所持証明トークンとのベアラートークンの交換に関する。アプリケーションなどのエンティティは、追加の特権を提供するアイデンティティを提供される。アプリケーションは、追加の特権を取得するためにベアラートークンを所持証明トークンと交換することができる。

【0009】

異なるアイデンティティ管理システムは異なる仕様に従う。したがって、異なるアイデンティティ管理システムにアクセスするには、各アイデンティティシステムに固有のアクセストークンが必要とされる。例示的な実施形態は、異なるアイデンティティ管理システム内で用いられるべきトークンの途切れのない交換を可能にする。したがって、エンティティは両方のアイデンティティ管理システムのフィーチャにアクセスすることができる。

【0010】

例えば、第1のアイデンティティ管理システム (例えば、アイデンティティクラウドサービス (I D C S)) にアクセスするために用いられる第1のタイプのトークン (例えば、ベアラートークン、O A u t h アクセストークン) は、第2のアイデンティティ管理システム (例えば、インフラストラクチャアイデンティティおよびアクセス管理 (I A M)) にアクセスするために用いられる第2のタイプのトークン (例えば、所持証明 (P o P) トークン) と交換され得、その逆もしかりである。インフラストラクチャアイデンティティおよびアクセス管理 (I A M) はアイデンティティおよびアクセス管理 (I A M) と称され得る。アイデンティティクラウドサービス (I D C S) ならびにインフラストラクチャアイデンティティおよびアクセス管理 (I A M) は総称的にアイデンティティシステムと称され得る。

【0011】

第2のアイデンティティシステムのための別個のトークンが取得される間、エンティティは第1のアイデンティティシステムのためのトークンを管理し続ける。したがって、エンティティは、エンティティがアクセスすることを欲する第2のアイデンティティシステムとの前方互換性を有することになり、その一方で、エンティティは、エンティティがアクセストークンを有する第1のアイデンティティシステムとの後方互換性を有し続ける。

【0012】

例示的な実施形態では、第1のアイデンティティシステムは I D C S システムであり、第2のアイデンティティシステムは I A M システムである。しかし、これは単に説明を容易にするためのものにすぎない。第1のアイデンティティシステムは、第2のアイデンティティシステムとは異なり、異なる仕様に従う任意のアイデンティティシステムであることができる。仕様は、第1または第2のアイデンティティシステムを動作させるために必要とされるルールを指すことができる。仕様は、アイデンティティシステムが正しく動作

10

20

30

40

50

することができること、およびコンポーネント間の対話が正しく機能することになることを確実にする。

【0013】

例示的な実施形態は、各システムと通信するために必要とされるトークンを維持しつつ、IAMシステムと互換性のあるIDCSシステムのためのトークンを交換することができる、その逆もしかりである。したがって、エンティティはもはやクレデンシャルの2つのセットを維持しなくてもよく、ユーザは2つの別個のシステムにログインする必要がない。エンティティが有する現在のトークンは、アクセスされるアイデンティティシステムと互換性を有するために、統合アイデンティティ管理システム（IDMS：integrated identity management system）によって自動的に交換され得る。統合アイデンティティ管理システム（IDMS）は統合管理システムとも称され得る。

10

【0014】

エンティティは、第1のアイデンティティシステムおよび第2のアイデンティティシステムのリソースにアクセスする任意のエンティティを含むことができる。エンティティは第1のアイデンティティシステムおよび第2のアイデンティティシステムのユーザまたは顧客とも称され得る。

【0015】

例示的な実施形態は、各アイデンティティ管理システムに別個にログインすることをユーザに要請せず、アイデンティティ管理システムごとのログインクレデンシャルを維持することをユーザに要請しない。その代わりに、ユーザは1つのアイデンティティシステムにログインし得、ユーザがログインしたアイデンティティシステムのために生成されたアクセストークンが、ユーザが交換に気付くことなく、異なるアイデンティティシステムのためのアクセストークンと交換され得る。統合アイデンティティ管理システム（IDMS）のトークン交換システムは、各アイデンティティシステムにアクセスするために必要とされるトークンを管理、記憶、および維持することができる。

20

【0016】

したがって、ユーザは、別個にログインすることを必要とすることなく、および別個のクレデンシャルおよびアクセストークンを維持する必要なく、異なるアイデンティティシステムと対話することができる。エンティティは、異なるタイプのトークンを用いるアイデンティティ管理システムの間で途切れなく作業することができる。これはプロダクトワークフローの中断を減少させる。

30

【0017】

例えば、IAMシステム内の、とあるリソースおよびサービスにアクセスするために、エンティティはアイデンティティを必要とするであろう。しかし、一部のエンティティは、現在、アイデンティティを割り当てられていないことがある。例えば、IDCSシステム内のアプリケーションはベアラートークンを用い、アイデンティティを割り当てられない。IAMは、エンティティがアイデンティティを有することを必要とするため、このようなエンティティはIAM内のリソースまたはサービスにアクセスすることが不可能であろう。

【0018】

したがって、例示的な実施形態は、現在、アイデンティティを有しない、アプリケーションなどの、エンティティのためのアイデンティティを提供する。このようなエンティティは、その後、それらのベアラートークンを所持証明トークンと交換することが可能になり、それゆえ、アイデンティティを必要とするリソースおよびサービス、IAM内のこのようなリソースおよびサービスと通信することができる。

40

【0019】

例示的な実施形態は、方法であって、クラウドサービスの統合アイデンティティ管理システムのトークン交換システムにより、エンティティが第1のアイデンティティシステムにアクセスすることを認可されると決定することを含み、エンティティは第1のトークンを有し、方法は、トークン交換システムにより、第1のアイデンティティシステムのエン

50

ティティから、第2のアイデンティティシステムにアクセスするための要求を受信することと、トークン交換システムにより、第1のトークンを検証することと、トークン交換システムにより、第1のアイデンティティシステムのための第1のトークンに基づいて第2のアイデンティティシステムのための第2のトークンを生成することと、トークン交換システムにより、第2のトークンに基づいてエンティティが第2のアイデンティティシステムにアクセスすることを認証することと、トークン交換システムにより、第2のトークンを用いてエンティティが第2のアイデンティティシステム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：application programming interface）にアクセスすることを認可することと、をさらに含む、方法を含むことができる。

【0020】

10

例示的な実施形態は、方法であって、クラウドサービスの統合アイデンティティ管理システムのトークン交換システムにより、エンティティが第1のアイデンティティシステムにアクセスすることを認可されると決定することを含み、エンティティはアプリケーションであり、方法は、トークン交換システムにより、エンティティが第2のアイデンティティシステムにアクセスするための第1の要求を生成することをさらに含み、第1の要求は、エンティティに関連付けられたベアラートークンおよび第1の公開鍵を含み、方法は、トークン交換システムにより、ベアラートークンが有効なベアラートークンであることを検証することと、トークン交換システムにより、エンティティのロールが、第2のアイデンティティシステムにアクセスすることを認可されたロールであるかどうかを検証することと、トークン交換システムにより、第1の要求において受信されたベアラートークンおよび第1の公開鍵に基づいて第2のトークンを生成することと、をさらに含み、方法は、トークン交換システムにより、第2のトークンをエンティティへ送信することをさらに含み、第2のトークンは第2のアイデンティティシステムに関連付けられており、第2のトークンはエンティティの第1の公開鍵を含む、方法を含むことができる。

20

【0021】

例示的な実施形態はまた、1つまたは複数のプロセッサに、上述された方法を遂行させるための、1つまたは複数のプロセッサによって実行可能な複数の命令を記憶する非一時的コンピュータ可読記憶媒体を含むことができる。

【0022】

例示的な実施形態はまた、メモリと、メモリに結合されており、上述された方法を遂行するように構成された1つまたは複数のプロセッサと、を含むコンピューティングシステムを含むことができる。

30

【0023】

他の実施形態は、本明細書において説明される方法に関連付けられたシステム、デバイス、およびコンピュータ可読媒体に関する。

【0024】

以下の詳細な説明および添付の図面を参照することで、例示的な実施形態の本質および利点のより深い理解を得ることができる。

【0025】

本開示は、添付の図面と併せて以下の詳細な説明によって容易に理解されるであろう。図面において、同様の参照符号は同様の要素を指示する。

40

【図面の簡単な説明】

【0026】

【図1】一部の例示的な実施形態に係る、トークンを交換するための方法の大まかな概略を示す図である。

【図2】一部の例示的な実施形態に係る、トークンを交換するためのトークン交換システムのブロック図である。

【図3】一部の例示的な実施形態に係る、トークンを交換するための統合コンソールのブロック図である。

【図4】アクセストークンを取得するためのシーケンス図である。

50

【図 5】一部の例示的な実施形態に係る、所持証明トークンをベアラートークンと交換するためのシーケンス図である。

【図 6】一部の例示的な実施形態に係る、ベアラートークンを所持証明トークンと交換するためのシーケンス図である。

【図 7】一部の例示的な実施形態に係る、トークンを交換するための方法を示す図である。

【図 8】一部の例示的な実施形態に係る、アプリケーションをリソースプリンシパルまたはサービスプリンシパルに変換するためのシーケンス図である。

【図 9】一部の例示的な実施形態に係る、IDCS のための相互通信のためのブロック図である。

【図 10】一部の例示的な実施形態に係る、IDCS 内のアプリケーションをIAM 内のリソースまたはサービスに変換するためのブロック図である。

【図 11】一部の例示的な実施形態に係る、アプリケーションがベアラートークンをPOP トークンと交換する方法を示す図である。

【図 12】一部の例示的な実施形態に係る、アプリケーションがIAM API への要求を行う方法を示す図である。

【図 13】一部の例示的な実施形態に係る、アプリケーションがトークンを交換する方法の概略を示す図である。

【図 14】一部の例示的な実施形態に係る、アプリケーションのためのトークンを交換するためのトークン交換システムのブロック図である。

【図 15】一部の例示的な実施形態に係る、クラウド・インフラストラクチャ・アズ・ア・サービス・システムを実施するための 1 つのパターンを示すブロック図である。

【図 16】一部の例示的な実施形態に係る、クラウド・インフラストラクチャ・アズ・ア・サービス・システムを実施するための別のパターンを示すブロック図である。

【図 17】一部の例示的な実施形態に係る、クラウド・インフラストラクチャ・アズ・ア・サービス・システムを実施するための別のパターンを示すブロック図である。

【図 18】一部の例示的な実施形態に係る、クラウド・インフラストラクチャ・アズ・ア・サービス・システムを実施するための別のパターンを示すブロック図である。

【図 19】一部の例示的な実施形態に係る、例示的なコンピュータシステムを示すブロック図である。

【発明を実施するための形態】

【0027】

詳細な説明

以下の説明では、説明の目的上、例示的な実施形態の完全な理解を与えるために、具体的詳細が説明される。しかし、様々な実施形態はこれらの具体的詳細を有せず実施され得ることは明らかであろう。例えば、システム、アルゴリズム、構造、技術、ネットワーク、プロセス、および他のコンポーネントは、実施形態を不必要な詳細で不明瞭にしないように、ブロック図の形のコンポーネントとして示され得る。図および説明は限定であることを意図されていない。

【0028】

クラウドサービスプロバイダ (CSP) は複数のクラウドサービスを加入顧客に提供し得る。これらのサービスは、ソフトウェア・アズ・ア・サービス (SaaS)、プラットフォーム・アズ・ア・サービス (PaaS)、インフラストラクチャ・アズ・ア・サービス (IaaS) モデル、および他のものを含む異なるモデルの下で提供され得る。

【0029】

クラウド環境内では、概して、クラウドサービスによって提供される、または用いられるリソースへのユーザアクセスを制御するためのアイデンティティ管理システムがクラウドサービスプロバイダによって提供される。アイデンティティ管理システムによって提供される典型的なサービスまたは機能は、限定するものではないが、ユーザのためのシングルサインオン能力、認証および認可サービス、ならびに他のアイデンティティベースのサ

10

20

30

40

50

ービスを含む。

【0030】

アイデンティティ管理システムによって保護されるリソースは、計算インスタンス、ブロックストレージボリューム、仮想クラウドネットワーク（VCN：virtual cloud network）、サブネット、ルート表、様々な呼び出し可能なAPI、内部もしくはレガシーアプリケーション、および同様のものなどの、異なる種類のものであることができる。これらのリソースは、クラウドおよび／または顧客オンプレミスリソース内に記憶されたリソースを含む。各リソースは、通例、リソースが作成された際にリソースに割り当てられる一意識別子（例えば、ID）によって識別される。

【0031】

CSPは、それらのクラウド提供のための2つ以上の別個の独立したアイデンティティ管理システムを提供し得る。これは、例えば、CSPによって提供されるIaaSアプリケーションおよびサービスのためのクラウドリソースへのアクセスを制御するために、第1のアイデンティティ管理システムまたはプラットフォーム（例えば、インフラストラクチャアイデンティティおよびアクセス管理（IAM：Infrastructure Identity and Access Management））が提供され得る場合に行われ得る。別個に、CSPによって提供されるSaaSおよびPaaSサービスのためのセキュリティおよびアイデンティティ管理のために、第2のアイデンティティ管理システムまたはプラットフォーム（例えば、アイデンティティクラウドサービス（IDCS：Identity Cloud Service））が提供され得る。

【0032】

このような2つの別個のプラットフォームを提供する結果、CSPの顧客が、CSPによって提供されるSaaSもしくはPaaSサービスおよびIaaSサービスの両方に加入している場合、顧客は、概して、2つの別個のアカウント——IaaS加入のためのIAMを有する1つのアカウント、およびPaaS／SaaS加入のためのIDCSを有する別個のアカウント——を有する。各アカウントは、ユーザログイン、パスワード等の、それ自体のクレデンシャルを有することになる。それゆえ、同じ顧客が2つのアカウントのための2つの別個のクレデンシャルセットを有する。これは不満足な顧客体験をもたらす。加えて、2つの別個のアイデンティティ管理システムを有することは、SaaS／PaaSとIaaSサービスとの間の相互作用についての障害をも生み出す。

【0033】

さらに、これらの異なるプラットフォームの各々は異なる仕様またはルールに適合する。これらのプラットフォームの各々のための仕様は容易に変更され得ない。一部のユーザは一方のプラットフォームとのみ対話し得、他のユーザは両方のプラットフォームと対話し得る。したがって、一部のユーザは両方のプラットフォームと通信することを必要としなくてもよく、一部のユーザは両方のプラットフォームと通信することを必要とし得る。しかし、ユーザが両方のプラットフォームと対話している場合には、例示的な実施形態は、異なるプラットフォームの間で途切れなく対話するためのソリューションを提供する。したがって、例示的な実施形態は、エンティティが異なるアイデンティティシステムにアクセスすることを可能にしつつ、アイデンティティシステムの各々のための規格と適合する。

【0034】

本出願の目的のために、および一例として、2つのプラットフォームはアイデンティティおよびアクセス管理システム（IAM）ならびにアイデンティティクラウドサービス（IDCS）と称される。しかし、これらの名称および用語はいかなる様態でも限定であることを意図されない。本開示の教示は、2つの（またはそれを超える）異なるアイデンティティ管理システムが統合されるべき任意の状況に適用される。統合されるべきアイデンティティ管理システムまたはプラットフォームは1つまたは複数のCSPによって提供され得る。

【0035】

10

20

30

40

50

一部の実施形態では、2つの別個の（例えば、IAMおよびIDCS）プラットフォームによって提供される様々な特徴および機能性を保持し、提供しつつ、複数のアイデンティティ管理プラットフォーム（例えば、IAMおよびIDCSプラットフォーム）を、クラウドサービスのユーザまたは顧客に透明である仕方で統合する、統合アイデンティティ管理プラットフォーム（統合アイデンティティ管理システム（IDMS）と称される）が提供される。それゆえ、統合は、より途切れのない向上したユーザ体験を提供する。

【0036】

しかし、この統合はいくつかの理由のために技術的に非常に困難である。2つのプラットフォームは、アイデンティティ関連機能を実施するための異なる手続きおよびプロトコルを用い得る。IAMは、例えば、多くの異なる属性を評価することができる複雑なブールルールセットを表現するポリシーの使用を通じてアクセス権がユーザに認められるアクセス制御パラダイムを規定する、ポリシーベースアクセス制御システムとしても知られる、属性ベースアクセス制御（ABAC）システムであり得る。ABACの目的は、無認可のユーザおよびアクション — 組織のセキュリティポリシーによって規定されたとおりの「承認された」特性を有しないもの — から、データ、ネットワークデバイス、およびITリソースなどのオブジェクトを保護することである。他方で、IDCSは、ロールおよび特権の周辺で規定されたポリシー中立的なアクセス制御機構であるロールベースアクセス制御（RBAC）システムであり得る。ロール許可、ユーザーロールおよびロール—ロール関係などのRBACの構成要素は、ユーザ割り当ての遂行を簡単にする。さらに別の理由として、2つのプラットフォームによって用いられる認証および認可フレームワークまたはワークフロー（例えば、用いられるトークンの種類、OAuthなどの異なる認証フレームワーク等）は異なり得る。これは、統合されたソリューションを提供することが技術的に非常に困難である理由のほんの小さな例にすぎない。

【0037】

I. 方法の概略 — トークンの交換

図1は、一部の例示的な実施形態に係る、トークンを交換するための方法100の大きな概略を示す。図1に示される方法100は統合アイデンティティ管理システム（IDMS）のトークン交換システムによって遂行され得る。トークン交換は、ベアラートークンを所持証明（PoP）トークンと交換するため、またはPoPトークンをベアラートークンと交換するために遂行され得る。例示的な実施形態では、第1のアイデンティティシステムのためのトークンが、第2のアイデンティティシステムのための異なるタイプのトークンを取得するために交換され得る。

【0038】

ステップ110において、第1のアイデンティティシステムの第1のエンティティから、第2のアイデンティティシステムのリソースにアクセスするための要求を受信する。第1のアイデンティティシステム内の第1のエンティティは第1のアイデンティティシステムのためのアクセストークンを有する。しかし、第2のアイデンティティシステムは第2のアイデンティティシステムのための異なるアクセストークンを必要とする。エンティティはユーザまたはクライアントとも称され得る。エンティティは、IAMシステムまたはIDCSシステムのフィーチャにアクセスすることを欲する任意のコンポーネント、アプリケーション、またはサービスを含むことができる。

【0039】

例えば、第1のアイデンティティシステム（例えば、IDCS）上のSaaSまたはPaaSサービスが第2のアイデンティティシステム（例えば、IAM）上のストレージサービスにアクセスすることを欲する。別の例として、第2のアイデンティティシステム（例えば、IAM）上のストレージサービスが第1のアイデンティティシステム（例えば、IDCS）のSaaSまたはPaaSの機能と通信することを欲し得る。別の例として、IAMシステム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）鍵がIDCSシステムのトークンを取得することを欲し得る。代替的に、IDCSトークンを有するIDCSサービスが、IAMシステムと通信し、プロダクトのためのIAMリソースを

取得することを欲し得る。

【0040】

エンティティが第2のアイデンティティシステムのためのアクセストークンを取得するために、エンティティは第2のアイデンティティシステムにログインし、第2のアイデンティティシステムのためのクレデンシャルを確立することができるであろう。第2のアイデンティティシステムのためのクレデンシャルを確立した後に、エンティティは、第2のアイデンティティシステムにアクセスするためのアクセストークンを提供される。しかし、第2のアイデンティティシステムのためのクレデンシャルを確立することをエンティティに要請することは、これは負担となり、非効率的である。具体的には、エンティティがアクセスするアイデンティティシステムごとにクレデンシャルを確立することをエンティティに要請することは負担となる。アイデンティティシステムごとにクレデンシャルを取得することをエンティティに要請することはまた、ワークフローを中断する。両方のアイデンティティシステムにアクセスする多数のユーザを前提とすると、これは累積的に負担となる。

10

【0041】

したがって、例示的な実施形態によれば、ステップ120において、統合アイデンティティ管理システム（IDMS）のトークン交換システムは第1のアイデンティティシステムのアクセストークンを第2のアイデンティティシステムのためのアクセストークンに交換することができる。エンティティは、その後、アイデンティティシステムごとのクレデンシャルを入力することを必要とすることなく、第1のアイデンティティシステムおよび第2のアイデンティティシステムの両方内のリソースにアクセスすることができる。

20

【0042】

ステップ130において、統合アイデンティティ管理システム（IDMS）のトークン交換システムは、第1のアイデンティティシステムおよび第2のアイデンティティシステムとのエンティティのセッション全体を通して、第1のアイデンティティシステムおよび第2のアイデンティティシステムのためのアクセストークンを管理し続ける。セッションは、ユーザが第1または第2のアイデンティティシステムにアクセスしている期間を指すことができる。ユーザはブラウザ上のサインオンセッションを介して第1または第2のアイデンティティシステムにログインすることができる。アクセストークンはブラウザセッションの存在に基づいて用いられ続けられ得る。例えば、ブラウザセッションは12時間であることができるであろう。しかし、これは単なる一例にすぎない。

30

【0043】

したがって、例示的な実施形態は、セッション中における第1のアイデンティティシステムおよび第2のアイデンティティシステムのフィーチャにアクセスするための途切れない相互運用を可能にする。

【0044】

トークンはセッションベースのものであることができる。すなわち、ユーザがセッション中に認証されている間、トークンは用いられ続け得る。トークンはまた、ブラウザベースのものであることもできる。ユーザがサインオンセッションを用いてブラウザにログインしている場合、トークンが用いられ続け得る長さはブラウザセッションに基づくことができる。

40

【0045】

II. トークン交換システム

図2は、一部の例示的な実施形態に係る、トークンを交換するためのトークン交換システム200のブロック図を示す。

【0046】

トークン交換システム200は統合アイデンティティ管理システム（IDMS）の部分であることができる。トークン交換システム200は第1のアイデンティティシステム210および第2のアイデンティティシステム220とインターフェースを取る。トークン交換システムは、1つまたは複数のプロセッサ、およびトークン情報などのデータを記憶

50

するための1つまたは複数のメモリを含む。

【0047】

第1のアイデンティティシステムはIDCSに対応することができ、第2のアイデンティティシステムはIAMに対応することができる。第1のアイデンティティシステム210は、サービス211、第1のアイデンティティシステムモデル212、およびトークンストレージ213を含むことができる。サービス211は、例えば、SaaSおよびPaaSサービスを含むことができる。第2のアイデンティティシステム220は、サービス221、第2のアイデンティティシステムモデル222、およびトークンストレージ223を含むことができる。サービス221は、例えば、IaaS、ストレージサービス、およびデータサービスを含むことができる。

10

【0048】

第1のアイデンティティシステム210はIDCSシステムを指す。IDCSシステムに関連付けられたトークンはベアラートークンである。ベアラートークンは、OAuthトークン、OAuthアクセストークン、またはアクセストークンとも称され得る。ベアラートークンはOAuth仕様に従うことができる。IDCSアクセストークンはJSONウェブトークン(JWT: JSON Web Token)であることができる。IDCSシステムに関連付けられたトークンはアプリケーションプリンシパルまたはクレデンシャルと称され得る。エンドユーザは、IDCSシステムにアクセスしている認可ユーザを含むことができる。

【0049】

第2のアイデンティティシステム220はIAMシステムを指すことができる。IAMシステムはトークンを含むことができる。本明細書では、第2のアイデンティティシステムはIAMシステムを指す。IAMシステムに関連付けられたトークンは所持証明(POP)トークンである。所持証明(POP)トークンはインターネットエンジニアタスクフォース(IETF: Internet Engineer Task Force)仕様に従うことができる。

20

【0050】

IAMシステムに関連付けられたトークンはセキュリティプリンシパルまたはインスタンスプリンシパルと称され得る。例示的なセキュリティプリンシパルはサービスプリンシパルセッショントークン(SPST: service principal session token)を含むことができる。SPSTトークンはJSONウェブトークン(JWT)であることができる。トークンはユーザベースのものまたはリソースベースのものであることができる。ユーザベースのトークンは、IAMシステムのユーザ、エンドユーザ、または顧客に関連付けられ得る。エンドユーザは、IAMシステムにアクセスしている認可ユーザを含むことができる。

30

【0051】

第1のアイデンティティシステムモデル212は第1のアイデンティティシステムのためのモデル情報を含むことができる。第2のアイデンティティシステムモデル222は第2のアイデンティティシステムのためのモデル情報を含むことができる。IDCSシステムのためのトークンまたはプリンシパルは異なり、IAMシステムのためのトークンまたはプリンシパルとは異なる規格およびモデルに従う。さらに、IDCSシステムからのトークンはIDCSシステムのための目的を果たし、それに対して、IAMトークンはIAMシステムに固有の目的を果たす。したがって、各アイデンティティシステムは、アイデンティティシステムが正しく動作するために必要とされる仕様を識別するモデルを記憶する。

40

【0052】

トークンストレージ213およびトークンストレージ223は、アイデンティティシステムに関連付けられたアクセストークンを記憶することができる。アクセストークンは、APIにアクセスするためにアプリケーションによって用いられ得るクレデンシャルであることができる。アクセストークンは、不透明文字列、JSONウェブトークン(JWT)、または非JWTトークンであることができる。アクセストークンは、トークンの所持

50

者がAPIへの委任アクセスを認められ、アクションの所定のセットを要求していることをAPI 231などのAPIに知らせるために用いられ得る。要求されるアクションは、トークンの所持者のスコープ内にあるアクションである。

【0053】

トークンストレージ213は、例えば、ベアラートークンを記憶することができる。ベアラートークンは、所有権に基づいて用いられ得るトークンである。すなわち、ベアラートークンを所持するエンティティがそれを用いることができる。ベアラートークンを所持するエンティティは、鍵などの、追加の情報を必要とすることなく、ベアラートークンを直接用いることができる。ベアラートークンは、中間者攻撃を防止するためにHTTPSを通信のために用いる。さらに、ベアラートークンは、応答を送信するために、正確な指定されたアドレスを用いる。特有アドレスの使用は、悪意のあるリダイレクトなどの、URL内の追加パラメータによって引き起こされ得る不正行為を回避する。

【0054】

トークンストレージ213および223はまた、IDトークンを記憶することができる。IDトークンは、認証が成功したことを証明するアーティファクトである。IDトークンは、ユーザプロファイル属性を包含するJWTであることができる。ユーザプロファイル属性はクレームの形で表現され得る。IDトークンはアプリケーションによって消費され、ユーザ名および電子メールなどのユーザ情報を取得するために用いられ得る。ユーザ情報はユーザインターフェース(UI: user interface)の表示の目的のために用いられ得る。

【0055】

トークンストレージ223は、例えば、所持証明(POP)トークンを記憶することができる。POPは、セキュリティトークンが攻撃者によって盗まれ、用いられるリスクを軽減する暗号メカニズムを指すことができる。POPトークンは、POPトークンを取得するために攻撃者によってそう簡単には用いられ得ない。POPトークンを用いるには、トークン自体、およびトークンに関連付けられた鍵へのアクセスの両方が必要とされる。鍵は、エンティティに関連付けられたプライベート鍵であることができる。POPトークンはHolder of Key(HoK)トークンとも称され得る。IAM内のセキュリティトークンは、APIにセキュリティアクセスすることへの手段をアプリケーションに提供するためのJSONウェブ鍵(JWK: JSON Web Key)としての公開POP鍵を包含するJWTである。

【0056】

トークン交換システム200はまた、統合コンソール230およびトークンマネージャ240を含む。統合コンソール230はアプリケーションプログラミングインターフェース231を含むことができる。統合コンソール230のAPI 231は、トークン交換を要求し、異なるアイデンティティシステム間のトークン交換を遂行するために用いられ得る。

【0057】

トークン交換システム200のトークンマネージャ240は、エンティティのために交換されたトークンを管理する。トークンマネージャ240は、エンティティが第1のアイデンティティシステムおよび第2のアイデンティティシステムと通信することを可能にするトークンを管理する。第1のアイデンティティシステムおよび第2のアイデンティティシステムと通信するためのトークンが維持されるため、前方および後方互換性が維持される。すなわち、エンティティは第2のアイデンティティシステムのフィーチャにアクセスすることができ、その一方で、引き続き第1のアイデンティティシステムのフィーチャにアクセスすることができる。IAMエンティティは、IDCSに加えてIAMのためのアイデンティティを有し続けることになり、その逆もしかりである。

【0058】

A. 統合コンソールおよびトークンマネージャ

図3は、一部の例示的な実施形態に係る、トークンを交換するための統合コンソール3

10

20

30

40

50

00のブロック図を示す。統合コンソール300は、図2に示される統合コンソール230に対応することができる。統合コンソールは交換およびストレージサービスの役割を果たすことができる。

【0059】

統合コンソール300は、第1のアイデンティティシステムと第2のアイデンティティシステムとの間のトークンの交換を遂行するために用いられる。統合コンソール300は、API331、第1のアイデンティティシステムコンソール320、および第2のアイデンティティシステムコンソール330を含むことができる。

【0060】

エンティティは、例えば、第1のアイデンティティシステムのトークンを第2のアイデンティティシステムのトークンと交換するために、統合コンソール300上の第1のアイデンティティシステムコンソール320にアクセスすることができる。

10

【0061】

例えば、ユーザは、統合アイデンティティ管理システムにアクセスするために第1のアイデンティティシステムコンソール320にログインすることができる。統合コンソール300はクラウドサービスコンソールであり、ユーザがクラウドサービスにアクセスすることを可能にする。統合コンソールは種々のAPIをサービス提供として提供する。ユーザは、クラウドサービスを開始するためにAPIサービス提供を用いることができる。

【0062】

バックエンドにおいて、トークン交換のためのコードが存在することができる。コードは、トークンを、システムのための適切なトークンに変換するために統合コンソール300によって用いられ得る。統合コンソール300はトークン交換を遂行する。論理は、統合コンソール300が適切なトークン交換を呼び出すことができるように書かれ得る。統合コンソールはまた、ストレージサービスの役割を果たすこともできる。

20

【0063】

さらに、エンティティは、例えば、第2のアイデンティティシステムのトークンを第1のアイデンティティシステムのトークンと交換するために、統合コンソール300上の第2のアイデンティティシステムコンソール330にアクセスすることができる。

【0064】

第2のアイデンティティシステムコンソール(IAM)330は、IAMによって生成されたトークンを有し得る。しかし、提供されるAPIのうちの一部はIDCSに関係付けられ得る。したがって、第2のアイデンティティシステムコンソール(IAM)330は第1のアイデンティティシステムコンソール(IDCS)320とのトークン交換を遂行することができる。統合コンソール300は、顧客が、統合された仕方でIDCSシステムおよびIAMシステムとインターフェースを取るためのポータル役の役割を果たす。コンソールはアイデンティティ管理システムの異なるサービスとインターフェースを取ることができる。

30

【0065】

統合コンソールは、顧客が、IDCSシステムおよびIAMシステムによって提供される様々なサービスの間の異なるタイプの統合を発展させることを助ける。

40

【0066】

III. トークンを取得するための方法

図4は、アクセストークンを取得するためのシーケンス図400を示す。図4に示される例では、IDCSシステムのクライアントがIDCSシステムのためのアクセストークンを要求している。

【0067】

図4に示される図は、クライアント410、IDCS OAuthサービス420、およびリソースアプリケーションプログラミングインターフェース(API)430の間の対話を示す。図4に示される例では、IDCSシステムのクライアント410はIDCSアクセストークンを取得する。

50

【0068】

ステップ411において、クライアント410がIDCS OAuthサービス420へのトークン要求を行う。クライアントはアプリケーションであることができ、アプリケーションは、IDCSシステムのフィーチャにアクセスするためにアクセストークンを必要とする。アプリケーションはそれ自体のクレデンシャルを有し、それは何らかの要求を行うことになる。例えば、それは、アクセストークンを求める要求を行うことになる。要求を行う際、アプリケーションはペイロードを送信し、その結果、それはトークン（例えば、アクセストークン）を受信することになる。

【0069】

ステップ412において、OAuthサービス420がクライアントのためのIDCSシステムへのアクセストークンを生成し、アクセストークンをクライアントへ返す。IDCSでは、アクセストークンはベアラートークンであることができる。

10

【0070】

ステップ413において、今やアクセストークンを有するクライアントが、アクセストークンを用いてリソースAPIを起動することができる。したがって、クライアントは、今や、IDCSシステムのリソースと対話するためのクレデンシャルを有する。クライアントは、それらは今やアクセストークンを有するため、リソースAPIにアクセスすることができる。

【0071】

アクセストークンを取得するための方法は仕様に基づいて異なり得る。図4に示される例では、アクセストークンを取得するための方法は様々なOAuth仕様またはOAuth規格に基づく。さらに、アクセストークンを取得するための方法はオープンIDコネクト（OIDC：Open ID Connect）仕様に基づくことができる。

20

【0072】

これは、単に、アクセストークンを取得するための例にすぎず、様々な方法を、アクセストークンを取得するために用いることができる。図示の例は、IDCSトークンを取得するためのものである。しかし、ユーザはIAMトークンを取得することもできる。

【0073】

ユーザが、ユーザがアクセスすることを欲するシステムごとにアクセストークンを取得することは不便である。ユーザは、それらが作業しているプロダクトがIDCSシステムおよびIAMシステムのフィーチャにアクセスすることを欲する際に、IDCSトークンおよび別個のIAMトークンを取得することを必要とすることを欲しない。さらに、クライアントは、異なるアイデンティティシステムのために別個のアクセストークンを取得し、それらのアクセストークンを管理するプロセスを経ることを欲しない。

30

【0074】

したがって、ユーザが一方のタイプのアイデンティティシステム（例えば、第1のアイデンティティシステム）のためのアクセストークンをすでに有する場合には、第1のアイデンティティシステムのためのアクセストークンを異なるアイデンティティシステム（例えば、第2のアイデンティティシステム）のためのトークンと交換することができる。

【0075】

40

IV．ベアラートークンとのPOPトークンの交換

ユーザがIAMアプリケーションにログインし、ユーザがPOPトークンを有し、同じ顧客が、IDCSシステムによって制御されるアプリケーションにアクセスすることを試みる場合には、別個のログインを再度行うことを必要とする代わりに、例示的な実施形態は、顧客が既存のPOPトークンに基づいてベアラートークンを取得することを可能にする。また、その逆もしかりである。例示的な実施形態は、エンティティが、交換が行われていることに気付くことなく、エンティティが異なるアイデンティティシステムのためのトークンを取得することを可能にする。ユーザは異なるアイデンティティシステムのフィーチャに途切れなくアクセスすることができる。さらに、例示的な実施形態は異なるアイデンティティシステムのための相互運用性を向上させる。

50

【0076】

図5は、一部の例示的な実施形態に係る、所持証明（PoP）トークンをベアラートークンと交換するためのシーケンス図500を示す。

【0077】

PoPトークンを有するエンティティはIAMシステムのリソースにアクセスすることができる。しかし、IDCSシステムのリソースにアクセスするために、エンティティはベアラートークンを必要とすることになる。図5は、エンティティのためのPoPトークンがどのようにIDCSのためのベアラートークンと交換されるのかを示す。

【0078】

図5は、クラウドインフラストラクチャサービス501、OAuth保護API502、IDCS503、およびIDDP（identity data plane（アイデンティティデータプレーン））504の間の対話を示す。IDDP504は、メモリ内に全てのアイデンティティデータを包含することができるトークン交換エンドポイントであることができ、メモリ内のデータは共有されない。クラウドインフラストラクチャサービス510はクラウドインフラストラクチャ基板またはオーバーレイ505上に配置され得る。OAuth保護API502はクラウドインフラストラクチャオーバーレイ506上に配置され得る。IDCS503はクラウドインフラストラクチャオーバーレイ507上に配置され得る。IDDP504はクラウドインフラストラクチャ基板508上に配置され得る。

【0079】

図5に示される例では、エンティティはIAM所持証明（PoP）トークンを有し、これらのPoPトークンがIDCSシステムのためのベアラートークンと交換される。例えば、ユーザは、認証されたPoPトークンを有し得、ユーザはIAMシステム内で動作を遂行している。ユーザは認証され、それらはIAMシステムにログインしている。同じセッション内で、ユーザはIDCSシステムのためのトークンを取得することができる。ユーザは、IDCSシステムのフィーチャにアクセスすることを欲するプロダクト、アプリケーション、またはアプリケーションのサービスを指すことができる。プロダクトまたはアプリケーションは、IAMまたはIDCSシステムと対話するプロダクトまたはアプリケーションを含むことができる。アプリケーションはまた、ウェブアプリケーションを含むこともできる。

【0080】

図5に示される例では、IaaSなどの、IAMサービスが、PaaSなどの、IDCSサービスにアクセスすることを試みている。IAMサービスはIAMトークンを有する。しかし、IDCSシステムのPaaSサービスにアクセスするために、IDCSトークンを必要とすることになる。したがって、IAMサービスはIDCSトークン（例えば、IDCSのためのベアラートークン）を要求することになる。

【0081】

サービスがIAMトークンを有する場合には、PaaSサービス（IDCS）にアクセスするために、サービスはIDCSトークンを要求することができる。サービスは要求をIDCSへ送信することができる。要求はIAM PoP / API鍵を用いて署名される。IDCSは、その後、要求を検証することができる。要求が有効である場合には、IDCSは、クラウドインフラストラクチャ（CI：cloud infrastructure）サービスがIDCS内で用いるためのベアラートークンを生成することができる。IDCSは、IDCSのプライベート鍵を用いて、生成されたベアラートークンに署名する。IDCSによって署名された、検証されたベアラートークンは、IDCS APIへのコールを行うために用いられ得る。

【0082】

図5に示されるステップは、ユーザが統合コンソール300上のIAMコンソール330にアクセスする際に開始され得る。

【0083】

ステップ510において、トークンをポストまたは要求するための要求がIAMサービ

10

20

30

40

50

ス（クラウドインフラストラクチャサービス501）からIDCS503へ行われる。

【0084】

ステップ520において、基板またはオーバーレイのいずれかの内部のクラウド統合（CI）サービス501が、署名されたトークン交換／トークン要求をオーバーレイ内のIDCSへ発行する。

【0085】

ステップ530において、IDCS OAuthサービス（IDCS503）が要求署名を検証する。各アプリケーションは、ユーザ名および／またはパスワードなどの、初期鍵を割り当てられ得る。要求はIAM所持証明（PoP）およびAPI鍵を用いて署名される。要求の署名はIDCSによって検証され、IDCSは要求の有効性を検証することができる。

10

【0086】

ステップ540において、コンピューティングシステムは、署名内に含まれる鍵の種類に基づいてアクセストークンを生成する。図示の例では、ベアラートークンが生成される。IDCSはIDCS適合トークンを生成する。

【0087】

ステップ550において、IDCS503はIDCSのプライベート鍵を用いてトークンに署名する。

【0088】

ステップ560において、署名されたベアラートークンをクラウドインフラストラクチャ（CI）サービスへ送信する。署名されたベアラートークンは呼び出し元サービスへ返される。

20

【0089】

ステップ570において、CIサービス501が、リソースを得ることを要求する。CIサービスはアクセストークンを用いて要求をOAuth保護APIへ発行することになる。CIサービスは、生成されたトークンを用いてAPIを呼び出すことができる。

【0090】

ステップ580において、OAuth保護API502がベアラートークンを用いて要求を認可することができる。

【0091】

30

ステップ590において、その結果、リソースエンティティを取得することができる。

IAM PoPトークンを有するIAMアイデンティティシステムのサービスはそのIAM PoPトークンをIDCSトークン（例えば、ベアラートークン）と交換することができ、IAMサービスはIDCSシステムのサービスにアクセスすることができる。

【0092】

したがって、サービスが任意の他のCI APIと通信することを試みる際、要求はユーザのプライベート鍵を用いて署名され得、トークンがアタッチされる。他のサービスは、エンティティが実際にトークンに署名したことを検証するために、IDDP（アイデンティティデータプレーン）に働きかけ、公開鍵を要求することができる。

【0093】

40

IV. PoPトークンとのベアラートークンの交換

特定のテナンシーまたは論理コンテナ内のリソースは、時として、他のリソースが保護された、テナンシー／論理コンテナ内の別のリソースへのアクセスを要求し得る。人間のユーザのように、インスタンスは、それらに割り当てられた識別子を有することができる。クラウドプラットフォームの部分として提供されるアイデンティティおよびアクセス管理（IAM）サービス内において、このようなエンティティは、時として、プリンシパルと称される。プリンシパルは、プリンシパルのアイデンティティに基づいて、クラウドコンピューティング環境内の他のリソースと対話すること（例えば、読み出し、書き込み、またはサービス関連動作を遂行すること）を許可され得るエンティティである。

【0094】

50

図 6 は、一部の例示的な実施形態に係る、ベアラートークンを所持証明 (P o P) トークンと交換するためのシーケンス図 6 0 0 を示す。

【0095】

図 6 は、管理クラウドサービス (M C S : management cloud service) 6 0 1、I D D P (アイデンティティデータプレーン) 6 0 2、およびドメイン共有キャッシュ 6 0 3 の間の対話を示す。管理クラウドサービス 6 0 1 はクラウドインフラストラクチャ S a a S / P a a S サービス 6 0 4 上に配置され得る。I D D P 6 0 2 およびドメイン共有キャッシュ 6 0 3 はクラウドインフラストラクチャ基板 6 0 5 上に配置され得る。I D D P 6 0 2 はトークン交換エンドポイントであることができる。

【0096】

図 6 に示される例では、I D C S トークン (例えば、ベアラートークン) を有する、S a a S および P a a S などの、I D C S サービスが I A M システムのサービスにアクセスすることを欲する。ユーザは認証され、それらは I D C S システムにログインし、I D C S トークンを取得している。同じセッション内で、ユーザは I A M システムのためのトークンを取得することができる。ユーザは、I A M システムのフィーチャにアクセスすることを欲するプロダクト、アプリケーション、またはアプリケーションのサービスを指すことができる。I A M システムのサービスは I A M データサービスおよびストレージサービスを含むことができる。I D C S の P a a S および S a a S サービスは、I A M によって生成されたトークンを用いて I A M の任意のデータサービスを確保することができる。

【0097】

ステップ 6 1 0 において、トークンを I D D P 6 0 2 へポストするための要求が S a a S / P a a S サービスから行われる。要求はベアラートークンおよび公開鍵を含む。セッション中にエンティティによって行われる全てのアクセスのために、1 つのベアラートークンを用いることができる。

【0098】

ステップ 6 2 0 において、ベアラートークンおよび公開鍵を識別する。

ステップ 6 3 0 において、ベアラートークンからドメイン I D を取り出す。

【0099】

ステップ 6 4 0 において、ドメイン共有キャッシュからドメインの公開鍵を取得する。

ステップ 6 5 0 において、ベアラートークンの署名の有効性を検証する。

【0100】

ステップ 6 6 0 において、タグを取り出し、リソースタイプを識別する。

ステップ 6 7 0 において、応答を I D D P 6 0 2 に提供する。

【0101】

ステップ 6 8 0 において、リソースプリンシパルセッショントークン (R P S T : resource principal session token) を生成する。例は、リソースプリンシパルセッショントークンを取得することに関して示されているが、さらなる実施形態は、サービスプリンシパルセッショントークン (S P S T) を取得することに関し得る。

【0102】

ステップ 6 9 0 において、要求は、続行することを認可されるかどうかを決定する。

上述された例はサービスに関するものであるが、アプリケーションはまた、交換を遂行するためにも用いられ得る。

【0103】

したがって、例示的な実施形態は、ユーザが、異なるアイデンティティシステムの諸側面にアクセスする際に、途切れのない統一された体験を有することになるよう、異なるメカニズムを統合する。エンドユーザおよび顧客は I A M および I D C S システムのユーザを含むことができる。トークン交換が行われる間にシステムのエンドユーザの動作は影響を受けない。それゆえ、ユーザは、生成されたトークンを用いて I A M と I D C S システムとの間で途切れなく動作することができる。

【0104】

10

20

30

40

50

例示的な実施形態は、異なるアイデンティティ管理システムなどの、異なるシステムのコンポーネントにアクセスする際に、ユーザによって直面される問題に対処する。ユーザは2つの異なるアイデンティティ管理システムの間で行き来することができる。それらは各システムに別個にログインしなくてもよい、ユーザ体験は向上し、途切れがない。

【0105】

V. トークンを交換するための方法

図7は、一部の例示的な実施形態に係る、トークンを交換するための方法700を示す。

【0106】

ステップ710において、トークン交換システムは、エンティティが第1のアイデンティティシステムにアクセスすることを認可されると決定することができる。エンティティはアプリケーションであることができる。

【0107】

ステップ720において、トークン交換システムは、第2のアイデンティティシステムにアクセスするためのエンティティによる第1の要求を受信することができる。第1の要求はベアラートークンおよび公開鍵を含むことができる。

【0108】

ステップ730において、トークン交換システムは、トークンは有効であることを検証することができる。要求上の署名が有効である場合に、トークンは有効であると決定され得る。

【0109】

ステップ740において、トークン交換システムは第1のアイデンティティシステムのための第1のトークンに基づいて第2のアイデンティティシステムのための第2のトークンを生成することができる。

【0110】

ステップ750において、トークン交換システムはエンティティのプライベート鍵を用いて第2のトークンに署名し、第2の署名付きトークンを生成することができる。

【0111】

ステップ760において、コンピューティングシステムが、第2の署名付きトークンに基づいてエンティティが第2のアイデンティティシステムにアクセスすることを認証する。トークン交換システムは、公開鍵に基づいて、エンティティは、ベアラートークンに署名したエンティティであることを検証することができる。

【0112】

ステップ770において、トークン交換システムは、第2のトークンを用いてエンティティが第2のアイデンティティシステムのアプリケーションプログラミングインターフェースにアクセスすることを認可することができる。

【0113】

上述の例はトークン交換を一般的に説明している。しかし、トークン交換は、アプリケーションなどの、特定のエンティティによって遂行され得る。

【0114】

VI. リソースプリンシパルまたはサービスプリンシパルとしてのアプリケーション
アプリケーションは、アプリケーションがアイデンティティを有しないため、他のリソースと対話することができないことがある。アプリケーションは、ベアラートークンを用いるOAuth認証モデルに従い得る。アプリケーションはドメインの部分であり、したがって、それはドメイン内の要素と対話することができる。しかし、アプリケーションはそのドメインの外部の要素と対話する能力を有し得ない。

【0115】

IAMアプリケーションプログラミングインターフェース(API)はリソースまたはサービスからの接続を受け入れるのみであり得る。エンティティがリソースまたはサービスでない場合には、このとき、エンティティはIAM APIと通信することができない

10

20

30

40

50

。I A M A P I は、要求がプライベート鍵によって署名され、要求元のみがプライベート鍵を有する、署名付き要求を得ることに依存する。

【0116】

例示的な実施形態は、SaaSアプリケーション、PaaSアプリケーション、または融合アプリケーション（FA：fusion application）などの、アプリケーションによって所持されるベアラートークンアイデンティティを変換し、トークン交換システムは、ベアラートークンアイデンティティを、IAM内のAPIによって受け入れられる、リソースプリンシパルセッショントークン（RSP T）アイデンティティと交換することができる。RSP TアイデンティティはPOPトークンを用いる。アプリケーションのベアラートークンは、アプリケーションがリソースプリンシパルまたはサービスプリンシパルの役割を果たすことを可能にする、POPトークンに変換される。

10

【0117】

過去においては、1つのドメイン内のアプリケーションはそのドメイン内のリソースにアクセスすることができるのみである。しかし、今や、アプリケーションはリソースプリンシパルアイデンティティまたはサービスプリンシパルアイデンティティを与えられ得る。アプリケーションがプリンシパルアイデンティティに更新された場合には、それはドメイン内の全てのユーザのデータを管理することができる。

【0118】

アプリケーションがリソースプリンシパルセッショントークンアイデンティティを有すると、エンティティは動的グループの部分になることができる。エンティティは様々な特権を割り当てられ得、エンティティはリソースプリンシパルとして扱われ得る。上述の例は、リソースプリンシパルのためのアイデンティティを有するアプリケーションを用いたものであるが、アプリケーションはまた、サービスプリンシパルのアイデンティティも与えられ得るであろう。リソースおよび／またはサービスプリンシパルとして、アプリケーションはより多くのスコープおよびより多くの特権を有することになり、動的グループの部分になることができる。

20

【0119】

ベアラートークンを有するアプリケーションは、その後、プリンシパル（すなわち、リソースまたはサービスにアクセスすることができるエンティティ）の役割を果たす能力を有する。アプリケーションは、IAMにアクセスする前に認証／認可される。

30

【0120】

例示的な実施形態では、SaaS、PaaS、または融合アプリケーション（FA）が有するベアラートークンはリソースプリンシパルセッショントークンアイデンティティと交換され得る。アプリケーションがリソースプリンシパルセッショントークンアイデンティティを有すると、アプリケーションは動的グループの部分になることができ、任意の特権を割り当てられ得、サービスとして扱われ得る。

【0121】

アプリケーションは、単なるリソースではなく、サービスプリンシパルとして扱われ得る。アプリケーションはより多くのスコープおよびより多くの特権を有する。

【0122】

40

A. シーケンス図 — アプリケーションをプリンシパルへ

IDCSにおいて、アプリケーションはストライプを有することができる。ストライプはテナンシーまたはアカウントとしても知られ得る。このストライプ内において、ユーザは、アプリケーションを管理するためのルールを有する。テナンシー内では、異なるルールが存在し得る。例えば、財務アプリを管理するためのとあるルールを有する1つのストライプ内に、財務アプリケーションが存在し得る。さらに、別のストライプ内の別のグループは人事（HR：Human Resources）アプリケーションを有し得、HRアプリケーションを管理するためのルールを有し得る。さらに、データベースアプリケーションが存在し得、データベースにアクセスするためのルールが存在する。しかし、会社などの企業が1つを超えるストライプを有する場合には、ストライプ内のアプリケーションは互いに

50

通信することができない。すなわち、テナンシー間またはストライプ間通信が存在しない。これらのシステムはベアラートークンを用いる。

【0123】

図8は、一部の例示的な実施形態に係る、アプリケーションをリソースプリンシパルまたはサービスプリンシパルに変換するためのシーケンス図800を示す。

【0124】

図8に示されるように、ステップ810において、アプリケーションテナンシーをドメインに変換する。単一のテナンシーが示されているが、いくつかのテナンシーをいくつかのドメインに変換することができる。

【0125】

ステップ810において、アプリケーションのベアラートークンをPOPトークンと交換する。アプリケーションは今やPOPトークンを用いるため、アプリケーションは、ステップ830に示されるように、リソースプリンシパルの役割、またはステップ840に示されるように、サービスプリンシパルの役割を果たすことを可能にされる。

【0126】

アプリケーションがリソースプリンシパルの役割を果たすとき、それはIAM内のリソースの役割を果たす能力を有する。アプリケーションがサービスプリンシパルの役割を果たすとき、それはIAM内のサービスの役割を果たす能力を有する。

【0127】

B. IDC S内の相互通信

図9は、一部の例示的な実施形態に係る、IDC S内の相互通信のためのブロック図900を示す。

【0128】

図9に示されるように、アプリケーションはIDC S内のテナンシー910内にあることができる。テナンシーはストライプまたはアカウントとしても知られ得る。図9に示されるように、人事、財務、および会計などの、会社内の各部門はそれら自体のテナンシー（人事911、財務912、および会計913）を各々有することができる。テナンシーはベアラートークンを用いて動作することができる。図9に示されるテナンシーは例示を目的とするものであり、様々な他のテナンシーが存在することができる。人事テナンシー911はベアラートークンストア914を含むことができ、財務テナンシー912はベアラートークンストア915を含むことができ、会計テナンシー913はベアラートークンストア916を含むことができる。

【0129】

図9に示されるように、各テナンシーは他のテナンシーとは独立して動作する。すなわち、人事テナンシー911内のユーザは人事テナンシー911内の情報にアクセスすることのみでき、財務テナンシー912内のユーザは財務テナンシー912内の情報にアクセスすることのみでき、会計テナンシー913内のユーザは会計テナンシー913内の情報にアクセスすることのみできる。

【0130】

テナンシーが他のテナンシー内の情報にアクセスすること（例えば、相互通信）を可能にするために、テナンシーはドメインに変換される。IDC Sテナンシー910はIDC Sドメイン920に変換される。ドメインを用いることで、異なる部門は情報にアクセスし、他の部門内の情報と通信することができる。したがって、人事ドメイン921、財務ドメイン922、および会計ドメイン923は互いに通信し、他のドメインからの情報にアクセスすることができる。さらに、ドメインの各々が他のドメインにアクセスすることができる範囲は、各部門に関連付けられた権限および特権に基づくことができる。図9に示されるように、人事ドメイン921はベアラートークンストア924を含み、財務ドメイン922はベアラートークンストア925を含み、会計ドメイン923はベアラートークンストア926を含む。

【0131】

10

20

30

40

50

いくつかのユーザおよびグループを含むHRテナンシーの代わりに、全てがHRドメイン内に配置されるようになる。さらに、ドメイン内のユーザは一意である。

【0132】

アプリケーションが属するドメインは、ドメイン内のアプリケーションに割り当てられるアイデンティティ (identity) 特権に対して用いられ得、決定され得る。図9に示されるように、アプリケーションは、ドメインに関連付けられた特権を有し、ドメインの外部の特権を有しない。

【0133】

C. 第1のアイデンティティシステムおよび第2のアイデンティティシステムとのエンティティ通信

図10は、一部の例示的な実施形態に係る、IDCS内のアプリケーションをIAM内のリソースまたはサービスに変換するためのブロック図1000を示す。IDCS内のアプリケーションは、それがそのベアラートークンをPOPトークンと交換するため、サービスプリンシパルまたはリソースプリンシパルの役割を果たすことができる。

【0134】

図10は、人事アプリケーション1020、財務アプリケーション1030、および会計アプリケーション1040を示す。人事アプリケーション1020は、ベアラートークンストア1021内に記憶されたとおりのベアラートークンを用いる。財務アプリケーション1030は、ベアラートークンストア1031内に記憶されたとおりのベアラートークンを用いる。会計アプリケーション1040は、ベアラートークンストア1041内に記憶されたとおりのベアラートークンを用いる。

【0135】

図10に示されるように、IDCSドメイン1010内のアプリケーションはそれらのベアラートークンをPOPトークンと換える。IAMドメイン1050内に示されるように、アプリケーションは、IAMドメイン内にあるとき、それらのPOPトークンを用いることができる。IAMドメイン1050内において、人事アプリケーション1060、財務アプリケーション1070、および会計アプリケーション1080は、それらは今やPOPトークンを有するため、今や、リソースプリンシパルまたはサービスプリンシパルの役割を果たすことができる。アプリケーションのためのPOPトークンは、POPトークンストア1061、POPトークンストア1071、およびPOPトークンストア1081内に記憶され得る。

【0136】

図10に示されるように、IDCSドメイン1010内のアプリケーションはそれらのベアラートークンをPOPトークンと交換し、したがって、IDCSドメイン1050内のリソースプリンシパルまたはサービスプリンシパルの役割を果たす能力を有する。

【0137】

したがって、例示的な実施形態は、異なるストライプ内にあったアプリケーションが所持証明 (POP) トークンの使用を通じて互いに通信することを可能にする。

【0138】

ドメインは、IDCSアカウントエンティティを、それがアイデンティティ自体内の部分エンティティまたは部分アイデンティティになるときに記述するために使用される。したがって、IDCS内のストライプはアイデンティティ/IAM内のドメインに対応付けられ得る。企業内の部門ごとにドメインが存在することができ、各ドメインはそれ自体のリソースを有することになる。したがって、ストライプおよびテナンシーの代わりに、ドメインが作成された。

【0139】

D. アプリケーションがトークンを交換する

1. 方法 — アプリケーションがベアラートークンをPOPトークンと交換する

図11は、一部の例示的な実施形態に係る、アプリケーションがベアラートークンをPOPトークンと交換する方法1100を示す。

【0140】

エンティティは、セッション鍵ペアを生成することによってクラウドインフラストラクチャAPIへの要求を行うことができる。公開鍵は、IAMの他のクラウドインフラストラクチャサービスが検証することができるアイデンティティトークン内に記憶され、エンティティはプライベート鍵を所有する。要求はエンティティのプライベート鍵を用いて署名され得る。公開鍵を含むトークンが要求にアタッチされ、これにより、IAMサービスのクラウドインフラストラクチャはエンティティを検証することができる。ベアラートークンアイデンティティは要求の部分としてIAMへ送信される。他のサービスは、エンティティがトークンに署名したことを検証するために、エンティティに働きかけ、エンティティの公開鍵を要求することができる。したがって、エンティティは今やIAMリソースおよびサービスと通信することができる。

10

【0141】

図11において開示されるように、アプリケーションのためのベアラートークンはPOPトークンと交換される。例えば、アプリケーションは、POPトークンのみを受け入れることになるIAMのためのAPIとの通信を欲し得る。したがって、アプリケーションは、それらのベアラートークンをPOPトークンと交換するためのプロセスを開始することができる。

【0142】

ステップ1110において、トークン交換システムは、エンティティが第1のアイデンティティシステムのために認可されると決定する。エンティティは、それが、第1のアイデンティティシステムにアクセスするためのクレデンシャルを有する場合に、第1のアイデンティティシステムのために認可される。エンティティのクレデンシャルは第1のアイデンティティシステムに入力され、クレデンシャルが正しい場合には、このとき、エンティティは、第1のアイデンティティシステムにアクセスすることを認可される。

20

【0143】

ステップ1120において、トークン交換システムは、IAMトークンを求めるアプリケーションからの要求を受信することができる。アプリケーションは鍵ペア（例えば、公開およびプライベート鍵ペア）を生成することになり、アプリケーションは公開鍵をペイロード内に提供することになる。したがって、要求はアプリケーションのベアラートークンおよび公開鍵を含む。要求はアプリケーションのプライベート鍵を用いて署名される。アプリケーションはそのプライベート鍵を送信せず、そのプライベート鍵を用いて要求に署名する。

30

【0144】

公開鍵は、他のIAMサービスが、有効性を検証し、アプリケーションがプライベート鍵を所有することを検証するためにアクセスすることができるアイデンティティトークンストア内に保存されるか、または記憶されることができる。

【0145】

ステップ1130において、トークン交換システムは、アプリケーションが有効なベアラートークンを有するかどうかを決定することができる。IAMと通信する際に、ベアラートークンアイデンティティを要求の部分としてIAMへ送信することができる。アイデンティティがIAMエンティティによってIDCSアイデンティティのために要求されている際に、ベアラートークンアイデンティティは、IDCSへの要求に署名するために用いられるが、ベアラートークンアイデンティティは要求と共に送信されない。

40

【0146】

ステップ1140において、トークン交換システムはアプリケーションのロールを決定し、アプリケーションのロールはリソースのための要件に適合するかどうかを決定することができる。アプリケーションのロールはアプリケーション内で指定され得る。ロールは、アプリケーションがアクセスすることができるデータを識別することができる。アプリケーションは、リソースに変換され得る正しいロールを有することが検証される。

【0147】

50

トークン交換システムは、アプリケーションのロールが、リソースプリンシパルの役割を果たすために十分であるかどうかを決定する。上述の例では、アプリケーションのロールは、リソースプリンシパルの役割を果たすために十分であるかどうかを決定する。しかし、アプリケーションがサービスプリンシパルの役割を果たすことを欲する場合には、このとき、トークン交換システムは、アプリケーションのロールが、サービスプリンシパルの役割を果たすために十分であるかどうかを決定することになる。

【0148】

ステップ1150において、トークン交換システムは、アプリケーションの公開鍵を含むトークンを生成することができる。トークンはIAMシステムによって署名され、アプリケーションの公開鍵を含む。IAMシステムによって署名されたトークンは、図13に示されるとおりのトークン生成器1360によって生成され得る。

10

【0149】

ステップ1160において、トークン交換システムはアプリケーションへ、IAMによって署名されたトークンを送信することができる。トークンは、IAMへの将来のAPIコールを行うためにアプリケーションによって用いられ得る。トークンはまた、鍵としても知られ得る。鍵をアプリケーションに割り当てることによって、鍵は、アプリケーションはそれが自称しているものであることを確実にするために用いられ得る。

【0150】

アプリケーションはアイデンティティを提供され、したがって、統合された環境内のリソースと通信し、要求を行うことができる。アプリケーションは、後方互換性のために、それら自体のベアラートークンアイデンティティを用いるか、またはそれに依存する、それら自体のドメイン内の全てのエンティティと協働し続けることになる。

20

【0151】

アプリケーションは、アプリケーションの公開鍵を有するIAMによって署名されたトークンを有する。アプリケーションが他のIAM APIと通信する際、要求はプライベート鍵を用いて署名され、トークンがアタッチされる。

【0152】

2. 方法 — アプリケーションがIAM APIへのコールを行う

図12は、一部の例示的な実施形態に係る、アプリケーションがIAM APIへの要求を行う方法1200を示す。

30

【0153】

ステップ1210において、トークン交換システムは、第2のアイデンティティシステム内のリソースにアクセスするための要求を受信することができる。要求は、ベアラートークン、およびアプリケーションの公開鍵を含む、IAMから受信されたトークンを含むことができる。要求はアプリケーションのプライベート鍵によって署名され得る。コールを行っているアプリケーションは公開鍵を提供し、それを、返されるセッショントークンに関連付けることができる。

【0154】

アプリケーションが将来のAPIコールを行う場合、トークン交換システムはIAMへのAPIコールのための要求を受信することができる。要求は、IAMによって署名された公開トークンを含む。要求はアプリケーションのプライベート鍵を用いて署名される。

40

【0155】

アプリケーションは、IAMから受信されたトークンを任意の要求内にアタッチすることができ、アプリケーションはまた、アプリケーションのプライベート鍵を用いて要求に署名することができる。アプリケーションは、プライベート鍵、およびIAMからの有効なトークンを所持することを証明することができる。したがって、アプリケーションがアクセスすることを試みているリソースはアプリケーションのアイデンティティを検証することができる。アプリケーションは、アプリケーションのプライベート鍵を用いて要求に署名し、IAMによって署名されたトークンをアタッチすることによって、IAM APIへの将来の参照を行うことができる。

50

【0156】

ステップ1220において、トークン交換システムは、公開鍵に基づいて、アプリケーションが、ベアラートークンに署名したエンティティであることを検証することができる。トークン交換システムは、要求がアプリケーションのプライベート鍵を用いて署名されていることを検証することができる。トークン交換システムは、アプリケーションの受信された公開鍵を、アプリケーションのために記憶された公開鍵と比較することができる。その後、アプリケーションは有効性を検証され得る。公開トークンはIAMによって署名されたと決定され、プライベート鍵がアプリケーションのプライベート鍵であること、およびアプリケーションが要求に署名したことが検証される。

【0157】

ステップ1230において、トークン交換システムは、エンティティが第2のアイデンティティシステムにアクセスすることを認可することができる。アプリケーションは、指定された秘密情報を所持することを実証する能力を有するため、それは、他のリソースにアクセスすることができるように特権を認められ得る。

【0158】

アプリケーションはこのトークンを所持し、このアプリケーションのみがこのトークンを所持する。したがって、アプリケーションは、他のリソースと通信することを可能にされる。他のリソースは、ベアラートークンを用いずに、アプリケーションはそれが自称しているものであることを確かめることができる。

【0159】

トークンは署名され、公開鍵がトークンストア内に記憶されている場合には、これは、有効な公開鍵が存在することを指示する。要求はプライベート鍵を用いて署名され、プライベート鍵は、エンティティに属するものとして検証され得る。さらに、POPトークンを用いることによって、ベアラートークンに付随し得る問題が回避される。具体的には、他のエンティティは、要求を行っているアプリケーションに成り済ますこと、またはそれであることを装うことができない。

【0160】

3. 方法 — メッセージング

インスタンスはインスタンスの作成時にアイデンティティを割り当てられる。インスタンスはリソースプリンシパルセッショントークンアイデンティティを割り当てられ得るため、それらは動的グループの部分になることができる。一部のエンティティ（例えば、アプリケーション）はリソースプリンシパルセッショントークン（RPST）アイデンティティまたはPOPトークンを有しない。IDCS内のアプリケーション（例えば、SaaSアプリケーション、PaaSアプリケーション、融合アプリケーション等）はリソースプリンシパルセッショントークンアイデンティティを与えられておらず、したがって、アプリケーションはIAM内の動的グループの部分になることができなかった。

【0161】

図13は、一部の例示的な実施形態に係る、アプリケーションがトークンを交換する方法1300の概略を示す。

【0162】

ステップ1310において、アプリケーションはそのIDCSアクセストークン（例えば、ベアラートークン）をIDDP（アイデンティティデータプレーン）へポストする。要求のペイロードはアプリケーションの公開鍵を含む。要求は、署名、またはベアラートークン、または秘密クライアントIDのいずれかを用いて認証され得る。

【0163】

ステップ1320において、アプリケーションのインスタンスは、ペイロードを用いて署名付きRPSTを用いて別のコールを行う。これは、ペイロードアクセストークンのためのトークンの代わりである。ペイロードは、コールのための、呼び出し元からアプリケーションインスタンスおよびターゲットサービスへのIDCSアクセストークンを含む。要求が、認可ベアラートークンまたは秘密クライアントID、ならびに公開鍵を含み、ペ

10

20

30

40

50

イロードアクセストークンが存在しない場合には、このとき、返される R P S T はトークン内に公開鍵を含むことができる。要求がペイロードアクセストークンを用いて署名される場合には、このとき、トークン内に公開鍵を含まないトークンが返され得る。

【0164】

ステップ1330において、アプリケーションインスタンスは、認可ヘッダ内で R P S T を指定することによって I A M サービスへのコールを行う。それはトークンヘッダ内に任意選択的なトークンを含むことができる。要求はステップ1310からの R P S T プライベート鍵を用いて署名される。

【0165】

I A M にアクセスするために、要求は、アプリケーションのみがこのプライベート鍵を有することを示すプライベート鍵によって署名されることを必要とする。したがって、アプリケーションが要求に署名したことが検証され得る。

【0166】

アプリケーションの公開鍵を含むトークンは I A M システムによって署名されるため、公開鍵は、有効な公開鍵であると決定される。さらに、アプリケーションは P o P トークンを用いて動作しているため、トランザクションはより安全である。

【0167】

4. アプリケーショントークン交換システム

図14は、一部の例示的な実施形態に係る、アプリケーションのためのトークンを交換するためのトークン交換システム1400のブロック図を示す。図14に示されるトークン交換システムは図2のトークン交換システムと類似している。したがって、類似した要素の説明は繰り返されない。

【0168】

トークン交換システム1400は統合アイデンティティ管理システム (I D M S) の部分であることができる。トークン交換システム1400は第1のアイデンティティシステム1410および第2のアイデンティティシステム1420とインターフェースを取る。第1のアイデンティティシステムは I D C S に対応することができる、第2のアイデンティティシステムは I A M に対応することができる。第1のアイデンティティシステム1410は、サービス1411、第1のアイデンティティシステムモデル1412、およびトークンストレージ1413を含むことができる。サービス1411は、例えば、 S a a S および P a a S サービスを含むことができる。第2のアイデンティティシステム1420は、サービス1421、第2のアイデンティティシステムモデル1422、およびトークンストレージ1423を含むことができる。サービス1421は、例えば、 I a a S 、 ストレージサービス、およびデータサービスを含むことができる。

【0169】

第1のアイデンティティシステムモデル1412は第1のアイデンティティシステムのためのモデル情報を含むことができる。第2のアイデンティティシステムモデル1422は第2のアイデンティティシステムのためのモデル情報を含むことができる。

【0170】

トークンストレージ1413およびトークンストレージ1423は、アイデンティティシステムに関連付けられたアクセストークンを記憶することができる。トークンストレージ1413は、例えば、ベアラートークンを記憶することができる。トークンストレージ1413および1423はまた、 I D トークンを記憶することができる。トークンストレージ1423は、例えば、所持証明 (P o P) トークンを記憶することができる。

【0171】

トークン交換システム1400はまた、統合コンソール1430およびトークンマネージャ1440を含む。統合コンソール1430はアプリケーションプログラミングインターフェース1421を含むことができる。統合コンソール1430の A P I 1431は、トークン交換を要求し、異なるアイデンティティシステム間のトークン交換を遂行するために用いられ得る。

10

20

30

40

50

【0172】

トークン交換システム1400のトークンマネージャ1440は、エンティティのために交換されたトークンを管理する。トークンマネージャ1440は、エンティティが第1のアイデンティティシステムおよび第2のアイデンティティシステムと通信することを可能にするトークンを管理する。

【0173】

さらに、トークン交換システム1400の第1のアイデンティティシステム1410はまた、テナンシー変換器1414を含むことができる。テナンシー変換器1414はテナンシーをドメインに変換することができる。ドメイン内のエンティティはPOPトークンを取得することができる。

10

【0174】

トークン交換システム1400はまた、ロール識別器1450およびトークン生成器1460を含むことができる。ロール識別器1450は、ベアラートークンから取得されたロールを決定するためにトークン交換システムによって用いられ得、ロールがリソースまたはサービスにアクセスするために必要とされる要件に適合するかどうかを決定することができる。

【0175】

トークン生成器1460は、IAM APIにアクセスするための要求を行うエンティティ（例えば、アプリケーション）の公開鍵を含むことができるトークンを生成するためにトークン交換システム1400によって用いられ得る。トークンはまた、鍵としても知られ得る。生成されたトークンはエンティティに提供され得、エンティティは、IAM APIにアクセスする際にトークンを要求内に含めることができる。

20

【0176】

例示的な実施形態によれば、アプリケーションは今やリソースとして扱われ得、動的グループの部分になることができる。アプリケーションは、動的グループに提供され、かくして、アプリケーションが対話し、他のリソースにアクセスすることを可能にする、特権を取得することができる。

【0177】

例示的な実施形態によれば、アプリケーションは、リソースプリンシパルまたはサービスプリンシパルの役割を果たすことができるよう、アイデンティティを割り当てられ得る。例えば、IDCS内のアプリケーションはIAM内のリソースプリンシパルまたはサービスプリンシパルにされ得る。

30

【0178】

アプリケーションは、他のリソースまたはサービスに与えられるものなどの、それ自体のアイデンティティを与えられる。アプリケーションは統合され得、リソースとして、または動的グループの参加者として扱われ得る。したがって、アプリケーションがIDCSシステムにログインさせられている場合には、アプリケーションはリソースの役割を果たし、IAMシステムの諸側面にアクセスすることができる。

【0179】

アプリケーションは、IDCSまたはIAMシステムのクライアントによって用いられるアプリケーションを含むことができる。クライアントによって用いられるアプリケーションはクライアントアプリケーションとしても知られ得る。例えば、アプリケーションはSaaSアプリケーション、PaaSアプリケーション、融合アプリケーション（FA）アプリケーション、またはIaaSアプリケーションを含むことができる。しかし、それらは単なる例にすぎず、IDCSおよびIAM内で用いられる様々なタイプのアプリケーションはクライアントアプリケーションであることができる。具体的には、IDCSまたはIAMシステムのリソースにアクセスすることを欲するアプリケーションは、アイデンティティを有するアプリケーションであることができ、アクセストークンを取得することができる。

40

【0180】

50

異なるシステムは、トークンの処理、およびシングルサインオン管理の異なる方法を有する。IDCSはIAMとは異なるサービスであるため、それらはトークンを異なって処理する。しかし、第1のアイデンティティシステムにアクセスするための第1のトークンを作成して管理し、第2のアイデンティティシステムにアクセスするための第2のトークンを作成して管理しなければならないことは、ユーザにとって不便である。

【0181】

例示的な実施形態は、クラウドサービス内の異なるアイデンティティシステムの間の前方および後方互換性をもたらすシングルアイデンティティソリューションを提供する。例示的な実施形態は、異なるアイデンティティシステムを用いて遂行されている動作を中断することなく、途切れのない仕方でこのようなソリューションを提供する。統合は、エンドユーザまたは顧客が、行われている交換に気付かないよう、舞台裏で遂行され得る。

【0182】

例示的な実施形態は、異なるアイデンティティ管理システムなどの、異なるシステムのコンポーネントにアクセスする際に、ユーザによって直面される問題に対処する。ユーザは2つの異なるアイデンティティ管理システムの間で行き来することができる。それらは各システムに別個にログインしなくてもよいため、ユーザ体験は向上し、途切れがない。

【0183】

例示的な実施形態は、異なるアイデンティティシステムのための両方のトークンを依然として維持しつつ、トークンを交換することを可能にする。トークンは、両方のシステムと通信することが可能になるために交換される。したがって、トークンは前方および後方互換性をもつことになる。エンティティは第1のアイデンティティシステムのそのトークンを第2のアイデンティティシステムのトークンと交換することができる。しかし、エンティティが第1のアイデンティティシステムに戻ってアクセスすることを必要とする場合には、エンティティは第1のアイデンティティシステムのためのトークンを維持する。したがって、エンティティは、異なるアクセストークンを必要とし、異なる規格に適合するアイデンティティシステムの間で継続的に対話することができる。

【0184】

コンピュータシステム

上述されたように、インフラストラクチャ・アズ・ア・サービス（IaaS）は1つの特定の種類のクラウドコンピューティングである。IaaSは、公衆ネットワーク（例えば、インターネット）を通じて、仮想化されたコンピューティングリソースを提供するように構成され得る。IaaSモデルでは、クラウドコンピューティングプロバイダは、インフラストラクチャコンポーネント（例えば、サーバ、記憶デバイス、ネットワークノード（例えば、ハードウェア）、デプロイメントソフトウェア、プラットフォーム仮想化（例えば、ハイパーバイザ層）、または同様のもの）をホストすることができる。場合によっては、IaaSプロバイダはまた、それらのインフラストラクチャコンポーネントに付随する種々のサービス（例えば、課金、監視、ロギング、ロードバランシング、およびクラスタ化等）も供給し得る。それゆえ、これらのサービスはポリシー駆動型であり得るため、IaaSのユーザは、アプリケーションの可用性および性能を維持するべくロードバランシングを駆動するためのポリシーを実施することが可能であり得る。

【0185】

場合によっては、IaaSの顧客は、インターネットなどの、ワイドエリアネットワーク（WAN：wide area network）を通じてリソースおよびサービスにアクセスし得、クラウドプロバイダのサービスを用いてアプリケーションスタックの残りの要素をインストールすることができる。例えば、ユーザはIaaSプラットフォームにログインし、仮想機械（VM：virtual machine）を作成し、オペレーティングシステム（OS：operating system）を各VM上にインストールし、データベースなどのミドルウェアをデプロイし、作業負荷およびバックアップのためのストレージバケットを作成し、さらに、企業ソフトウェアをVM内にインストールすることができる。次に、顧客は、プロバイダのサービスを用いて、ネットワークトラフィックのバランスを取ることを、アプリケーション

10

20

30

40

50

ョンの問題のトラブルシューティングを行うこと、パフォーマンスを監視すること、障害回復を管理すること等を含む、様々な機能を遂行することができる。

【0186】

大抵の場合、クラウドコンピューティングモデルはクラウドプロバイダの関与を必要とすることになる。クラウドプロバイダは、IaaSを供給すること（例えば、提供すること、貸与すること、販売すること）を専門にするサードパーティサービスであり得るが、そうである必要はない。エンティティはまた、プライベートクラウドをデプロイし、インフラストラクチャサービスの独自のプロバイダになることも選択し得るであろう。

【0187】

例によっては、IaaSのデプロイメントは、新たなアプリケーション、またはアプリケーションの新たなバージョンを、準備されたアプリケーションサーバまたは同様のものに入れるプロセスである。それはまた、サーバを準備する（例えば、ライブラリ、デーモン等をインストールする）プロセスを含み得る。これは、多くの場合、クラウドプロバイダによって、ハイパーバイザ層より下で（例えば、サーバ、ストレージ、ネットワークハードウェア、および仮想化）管理される。それゆえ、顧客は、（例えば、（例えば、オンデマンドでスピンアップされ得る）セルフサービス仮想機械などの上の、（OS）、ミドルウェア、および／またはアプリケーションデプロイメントの取り扱いの責任を負い得る。

10

【0188】

例によっては、IaaSのプロビジョニングは、コンピュータまたは仮想ホストを使用のために獲得すること、ならびにさらに、必要なライブラリまたはサービスをそれらにインストールすることを指し得る。大抵の場合、デプロイメントはプロビジョニングを含まず、プロビジョニングは、最初に遂行されることを必要とし得る。

20

【0189】

場合によっては、IaaSのプロビジョニングにとって2つの異なる問題が存在する。第1に、インフラストラクチャの初期セットを、いずれかが実行する前にプロビジョニングするという、初期の課題が存在する。第2に、全てのものがプロビジョニングされた後に、既存のインフラストラクチャを発展させる（例えば、新たなサービスを追加する、サービスを変更する、サービスを除去する等）という課題が存在する。場合によっては、これらの2つの課題は、インフラストラクチャの構成が宣言的に規定されることを可能にすることによって対処され得る。換言すれば、インフラストラクチャ（例えば、どのようなコンポーネントが必要とされるのか、およびそれらはどのように相互作用するのか）は、1つまたは複数の構成ファイルによって規定され得る。それゆえ、インフラストラクチャの全体的トポロジ（例えば、どのリソースがどれに依存するのか、およびそれらは各々、どのように協働するのか）は宣言的に記述され得る。場合によっては、トポロジが規定されると、構成ファイル内で記述される異なるコンポーネントを作成および／または管理するワークフローが生成され得る。

30

【0190】

例によっては、インフラストラクチャは、多くの相互接続された要素を有し得る。例えば、コアネットワークとしても知られる、1つまたは複数の仮想プライベートクラウド（VPC: virtual private cloud）（例えば、構成可能な、および／または共有されたコンピューティングリソースの、オンデマンドになる可能性のあるプール）が存在し得る。例によっては、ネットワークのインバウンドおよび／またはアウトバウンドトラフィックがどのようにセットアップされることになるのかを規定するためにプロビジョニングされる1つまたは複数のインバウンド／アウトバウンドトラフィックグループルール、および1つまたは複数の仮想機械（VM）も存在し得る。ロードバランサ、データベース、または同様のものなどの、他のインフラストラクチャ要素もプロビジョニングされ得る。所望され、および／または追加されるインフラストラクチャ要素が増えるにつれて、インフラストラクチャは徐々に発展し得る。

40

【0191】

50

場合によっては、様々な仮想コンピューティング環境にわたるインフラストラクチャコードのデプロイメントを可能にするために、継続的デプロイメント技術が採用され得る。加えて、上述の技術はこれらの環境内のインフラストラクチャ管理を可能にすることができる。例によっては、サービスチームが、（例えば、時として世界中に及ぶ、様々な異なる地理的場所にわたる）1つまたは複数の、しかし、多くの場合、多数の、異なる生産環境にデプロイされることを所望されるコードを書くことができる。しかし、例によっては、コードがデプロイされることになるインフラストラクチャがまずセットアップされなければならない。場合によっては、プロビジョニングは手動で行われ得、プロビジョニングツールが、リソースをプロビジョニングするために利用され得、および／またはインフラストラクチャがプロビジョニングされると、デプロイメントツールが、コードをデプロイするために利用され得る。

10

【0192】

図15は、少なくとも1つの実施形態に係る、クラウド・インフラストラクチャ・アズ・ア・サービス・システムを実施するための1つのパターンを示すブロック図である。

【0193】

図15は、少なくとも1つの実施形態に係る、IaaSアーキテクチャの例示的なパターンを示すブロック図1500である。サービスオペレータ1502は、仮想クラウドネットワーク（VCN）1506およびセキュアホストサブネット1508を含むことができるセキュアホストテナンシー1504に通信可能に結合され得る。例によっては、サービスオペレータ1502は、Microsoft Windows Mobile（登録商標）などのソフトウェア、ならびに／あるいはiOS、Windows Phone、Android、BlackBerry 8、Palm OS、および同様のもの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：short message service）、Blackberry（登録商標）、または他の通信プロトコルが使用可能である、ポータブルハンドヘルドデバイス（例えば、iPhone（登録商標）、セルラ電話、iPad（登録商標）、コンピューティングタブレット、パーソナルデジタルアシスタント（PDA：personal digital assistant））、あるいは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）であり得る、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用い得る。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）、Apple Macintosh（登録商標）、および／またはLinux（登録商標）オペレーティングシステムの様々なバージョンを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを含む汎用パーソナルコンピュータであることができる。クライアントコンピューティングデバイスは、限定するものではないが、例えば、Google Chrome OSなどの、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任意のものを実行するワークステーションコンピュータであることができる。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、VCN1506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通じて通信する能力を有する、シンクライアントコンピュータ、インターネット接続可能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、もしくは有しない、Microsoft Xboxゲーミングコンソール）、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、任意の他の電子デバイスであり得る。

20

30

40

【0194】

VCN1506は、SSH VCN1512内に包含されるLPG1510を介してセキュアシェル（SSH：secure shell）VCN1512に通信可能に結合され得るローカルピアリングゲートウェイ（LPG：local peering gateway）1510を含むことができる。SSH VCN1512はSSHサブネット1514を含むことができ、SSH VCN1512は、制御プレーンVCN1516内に包含されるLPG1510を介して制御プレーンVCN1516に通信可能に結合され得る。また、SSH VCN1

50

512はLPG1510を介してデータプレーンVCN1518に通信可能に結合され得る。制御プレーンVCN1516およびデータプレーンVCN1518は、IaaSプロバイダによって所有され、および／または操作され得るサービステナンスー1519内に包含され得る。

【0195】

制御プレーンVCN1516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）の役割を果たす制御プレーン非武装地帯（DMZ：demilitarized zone）層1520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、侵害をせき止めておくのを助け得る。加えて、DMZ層1520は、1つまたは複数のロードバランサ（LB：load balancer）サブネット1522、アプリサブネット1526を含むことができる制御プレーンアプリ層1524、データベース（DB：database）サブネット1530（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制御プレーンデータ層1528を含むことができる。制御プレーンDMZ層1520内に包含されるLBサブネット1522は、制御プレーンアプリ層1524内に包含されるアプリサブネット1526、および制御プレーンVCN1516内に包含され得るインターネットゲートウェイ1534に通信可能に結合され得、アプリサブネット1526は、制御プレーンデータ層1528内に包含されるDBサブネット1530、ならびにサービスゲートウェイ1536、およびネットワークアドレス変換（NAT：network address translation）ゲートウェイ1538に通信可能に結合され得る。制御プレーンVCN1516はサービスゲートウェイ1536およびNATゲートウェイ1538を含むことができる。

10

20

【0196】

制御プレーンVCN1516は、アプリサブネット1526を含むことができるデータプレーンミラーアプリ層1540を含むことができる。データプレーンミラーアプリ層1540内に包含されるアプリサブネット1526は、計算インスタンス1544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：virtual network interface controller）1542を含むことができる。計算インスタンス1544はデータプレーンミラーアプリ層1540のアプリサブネット1526を、データプレーンアプリ層1546内に包含され得るアプリサブネット1526に通信可能に結合することができる。

30

【0197】

データプレーンVCN1518は、データプレーンアプリ層1546、データプレーンDMZ層1548、およびデータプレーンデータ層1550を含むことができる。データプレーンDMZ層1548は、データプレーンアプリ層1546のアプリサブネット1526およびデータプレーンVCN1518のインターネットゲートウェイ1534に通信可能に結合され得るLBサブネット1522を含むことができる。アプリサブネット1526はデータプレーンVCN1518のサービスゲートウェイ1536およびデータプレーンVCN1518のNATゲートウェイ1538に通信可能に結合され得る。データプレーンデータ層1550もまた、データプレーンアプリ層1546のアプリサブネット1526に通信可能に結合され得るDBサブネット1530を含むことができる。

40

【0198】

制御プレーンVCN1516の、およびデータプレーンVCN1518のインターネットゲートウェイ1534は、公衆インターネット1554に通信可能に結合され得るメタデータ管理サービス1552に通信可能に結合され得る。公衆インターネット1554は、制御プレーンVCN1516の、およびデータプレーンVCN1518のNATゲートウェイ1538に通信可能に結合され得る。制御プレーンVCN1516の、およびデータプレーンVCN1518のサービスゲートウェイ1536はクラウドサービス1556に通信可能に結合することができる。

【0199】

例によっては、制御プレーンVCN1516の、またはデータプレーンVCN1518

50

のサービスゲートウェイ1536は公衆インターネット1554を経由することなくクラウドサービス1556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：application programming interface）コールを行うことができる。サービスゲートウェイ1536からクラウドサービス1556へのAPIコールは片方向であることができ、サービスゲートウェイ1536はクラウドサービス1556へのAPIコールを行うことができ、クラウドサービス1556は、要求されたデータをサービスゲートウェイ1536へ送信することができる。しかし、クラウドサービス1556はサービスゲートウェイ1536へのAPIコールを開始し得ない。

【0200】

例によっては、セキュアホストテナンシー1504は、さもなければ隔離され得る、サービステナンシー1519に直接接続され得る。セキュアホストサブネット1508は、さもなければ隔離されたシステムを通じた双方向通信を可能にし得るLPG1510を介してSSHサブネット1514と通信することができる。セキュアホストサブネット1508をSSHサブネット1514に接続することは、セキュアホストサブネット1508にサービステナンシー1519内の他のエンティティへのアクセスを与え得る。

【0201】

制御プレーンVCN1516は、サービステナンシー1519のユーザが所望のリソースをセットアップすること、または他の仕方ではプロビジョニングすることを可能にし得る。制御プレーンVCN1516内で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VCN1518内でデプロイされるか、または他の仕方では使用され得る。例によっては、制御プレーンVCN1516はデータプレーンVCN1518から隔離され得、制御プレーンVCN1516のデータプレーンミラーアプリ層1540は、データプレーンミラーアプリ層1540およびデータプレーンアプリ層1546内に包含され得るVNIC1542を介してデータプレーンVCN1518のデータプレーンアプリ層1546と通信することができる。

【0202】

例によっては、システムのユーザ、または顧客は、要求をメタデータ管理サービス1552へ通信することができる公衆インターネット1554を通じて、要求、例えば、作成（create）、読み出し（read）、更新（update）、または削除（delete）（CRUD）操作を行うことができる。メタデータ管理サービス1552はインターネットゲートウェイ1534を通じて要求を制御プレーンVCN1516へ通信することができる。要求は、制御プレーンDMZ層1520内に包含されるLBサブネット1522によって受信され得る。LBサブネット1522は、要求は有効であると決定し得、この決定に応じて、LBサブネット1522は要求を、制御プレーンアプリ層1524内に包含されるアプリサブネット1526へ伝送することができる。要求の有効性が検証され、公衆インターネット1554へのコールを必要とする場合には、公衆インターネット1554へのコールは、公衆インターネット1554へのコールを行うことができるNATゲートウェイ1538へ伝送され得る。要求によって記憶されることを所望され得るメモリはDBサブネット1530内に記憶され得る。

【0203】

例によっては、データプレーンミラーアプリ層1540は制御プレーンVCN1516とデータプレーンVCN1518との間の直接通信を促進することができる。例えば、構成の改変、更新、または他の好適な変更が、データプレーンVCN1518内に包含されるリソースに適用されることを所望され得る。VNIC1542を介して、制御プレーンVCN1516は、データプレーンVCN1518内に包含されるリソースと直接通信することができる。これにより、それらに対する構成の改変、更新、または他の好適な変更を実行することができる。

【0204】

実施形態によっては、制御プレーンVCN1516およびデータプレーンVCN1518はサービステナンシー1519内に包含され得る。この場合には、システムのユーザ、

10

20

30

40

50

または顧客は制御プレーンVCN1516またはデータプレーンVCN1518のどちらも所有または操作し得ない。その代わりに、IaaSプロバイダが、どちらもサービステナンシー1519内に包含され得る、制御プレーンVCN1516およびデータプレーンVCN1518を所有または操作し得る。本実施形態は、ユーザまたは顧客が、他のユーザの、または他の顧客のリソースと対話することを防止し得るネットワークの隔離を可能にすることができる。また、本実施形態は、システムのユーザまたは顧客が、記憶のために、所望の脅威防御レベルを有しないことがある、公衆インターネット1554に頼ることを必要とすることなく、データベースをプライベートに記憶することを可能にし得る。

【0205】

他の実施形態では、制御プレーンVCN1516内に包含されるLBサブネット1522は、サービスゲートウェイ1536からの信号を受信するように構成され得る。本実施形態では、制御プレーンVCN1516およびデータプレーンVCN1518は、公衆インターネット1554をコールすることなくIaaSプロバイダの顧客によってコールされるように構成され得る。顧客が使用するデータベースがIaaSプロバイダによって制御され得、公衆インターネット1554から隔離され得る、サービステナンシー1519上に記憶され得るので、IaaSプロバイダの顧客は本実施形態を所望し得る。

【0206】

図16は、少なくとも1つの実施形態に係る、クラウド・インフラストラクチャ・アズ・ア・サービス・システムを実施するための別のパターンを示すブロック図である。

【0207】

図16は、少なくとも1つの実施形態に係る、IaaSアーキテクチャの別の例示的なパターンを示すブロック図1600である。サービスオペレータ1602（例えば、図15の、サービスオペレータ1502）は、仮想クラウドネットワーク（VCN）1606（例えば、図15のVCN1506）およびセキュアホストサブネット1608（例えば、図15のセキュアホストサブネット1508）を含むことができるセキュアホストテナンシー1604（例えば、図15のセキュアホストテナンシー1504）に通信可能に結合され得る。VCN1606は、SSH VCN1612内に包含されるLPG1510を介してセキュアシェル（SSH）VCN1612（例えば、図15のSSH VCN1512）に通信可能に結合され得るローカルピアリングゲートウェイ（LPG）1610（例えば、図15のLPG1510）を含むことができる。SSH VCN1612はSSHサブネット1614（例えば、図15のSSHサブネット1514）を含むことができ、SSH VCN1612は、制御プレーンVCN1616内に包含されるLPG1610を介して制御プレーンVCN1616（例えば、図15の制御プレーンVCN1516）に通信可能に結合され得る。制御プレーンVCN1616はサービステナンシー1619（例えば、図15のサービステナンシー1519）内に包含され得、データプレーンVCN1618（例えば、図15のデータプレーンVCN1518）は、システムのユーザ、または顧客によって所有または操作され得る顧客テナンシー1621内に包含され得る。

【0208】

制御プレーンVCN1616は、LBサブネット1622（例えば、図15のLBサブネット1522）を含むことができる制御プレーンDMZ層1620（例えば、図15の制御プレーンDMZ層1520）、アプリサブネット1626（例えば、図15のアプリサブネット1526）を含むことができる制御プレーンアプリ層1624（例えば、図15の制御プレーンアプリ層1524）、データベース（DB）サブネット1630（例えば、図15のDBサブネット1530と同様のもの）を含むことができる制御プレーンデータ層1628（例えば、図15の制御プレーンデータ層1528）を含むことができる。制御プレーンDMZ層1620内に包含されるLBサブネット1622は、制御プレーンアプリ層1624内に包含されるアプリサブネット1626、および制御プレーンVCN1616内に包含され得るインターネットゲートウェイ1634（例えば、図15のインターネットゲートウェイ1534）に通信可能に結合され得、アプリサブネット162

6 は、制御プレーンデータ層 1 6 2 8 内に包含される DB サブネット 1 6 3 0、ならびにサービスゲートウェイ 1 6 3 6（例えば、図 1 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 1 6 3 8（例えば、図 1 5 の NAT ゲートウェイ 1 5 3 8）に通信可能に結合され得る。制御プレーン VCN 1 6 1 6 はサービスゲートウェイ 1 6 3 6 および NAT ゲートウェイ 1 6 3 8 を含むことができる。

【0209】

制御プレーン VCN 1 6 1 6 は、アプリサブネット 1 6 2 6 を含むことができるデータプレーンミラーアプリ層 1 6 4 0（例えば、図 1 5 のデータプレーンミラーアプリ層 1 5 4 0）を含むことができる。データプレーンミラーアプリ層 1 6 4 0 内に包含されるアプリサブネット 1 6 2 6 は、計算インスタンス 1 6 4 4（例えば、図 1 5 の計算インスタンス 1 5 4 4 と同様のもの）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）1 6 4 2（例えば、1 5 4 2 の VNIC）を含むことができる。計算インスタンス 1 6 4 4 は、データプレーンミラーアプリ層 1 6 4 0 内に包含される VNIC 1 6 4 2 およびデータプレーンアプリ層 1 6 4 6 内に包含される VNIC 1 6 4 2 を介して、データプレーンミラーアプリ層 1 6 4 0 のアプリサブネット 1 6 2 6 と、データプレーンアプリ層 1 6 4 6（例えば、図 1 5 のデータプレーンアプリ層 1 5 4 6）内に包含され得るアプリサブネット 1 6 2 6 との間の通信を促進することができる。

10

【0210】

制御プレーン VCN 1 6 1 6 内に包含されるインターネットゲートウェイ 1 6 3 4 は、公衆インターネット 1 6 5 4（例えば、図 1 5 の公衆インターネット 1 5 5 4）に通信可能に結合され得るメタデータ管理サービス 1 6 5 2（例えば、図 1 5 のメタデータ管理サービス 1 5 5 2）に通信可能に結合され得る。公衆インターネット 1 6 5 4 は、制御プレーン VCN 1 6 1 6 内に包含される NAT ゲートウェイ 1 6 3 8 に通信可能に結合され得る。制御プレーン VCN 1 6 1 6 内に包含されるサービスゲートウェイ 1 6 3 6 は、クラウドサービス 1 6 5 6（例えば、図 1 5 のクラウドサービス 1 5 5 6）に通信可能に結合することができる。

20

【0211】

例によっては、データプレーン VCN 1 6 1 8 は顧客テナンシー 1 6 2 1 内に包含され得る。この場合には、IaaS プロバイダは制御プレーン VCN 1 6 1 6 を顧客ごとに提供し得、IaaS プロバイダは、顧客ごとに、サービステナンシー 1 6 1 9 内に包含される固有の計算インスタンス 1 6 4 4 をセットアップし得る。各計算インスタンス 1 6 4 4 は、サービステナンシー 1 6 1 9 内に包含される、制御プレーン VCN 1 6 1 6 と、顧客テナンシー 1 6 2 1 内に包含されるデータプレーン VCN 1 6 1 8 との間の通信を可能にし得る。計算インスタンス 1 6 4 4 は、サービステナンシー 1 6 1 9 内に包含される制御プレーン VCN 1 6 1 6 内でプロビジョニングされた、リソースが、顧客テナンシー 1 6 2 1 内に包含されるデータプレーン VCN 5 1 8 内でデプロイされるか、または他の仕方で使用されることを可能にし得る。

30

【0212】

他の例では、IaaS プロバイダの顧客は、顧客テナンシー 1 6 2 1 内を本拠とするデータベースを有し得る。本例では、制御プレーン VCN 1 6 1 6 は、アプリサブネット 1 6 2 6 を含むことができるデータプレーンミラーアプリ層 1 6 4 0 を含むことができる。データプレーンミラーアプリ層 1 6 4 0 はデータプレーン VCN 1 6 1 8 内に駐在することができるが、データプレーンミラーアプリ層 1 6 4 0 はデータプレーン VCN 1 6 1 8 内を本拠とし得ない。すなわち、データプレーンミラーアプリ層 1 6 4 0 は顧客テナンシー 1 6 2 1 へのアクセスを有し得るが、データプレーンミラーアプリ層 1 6 4 0 はデータプレーン VCN 1 6 1 8 内に存在するか、または IaaS プロバイダの顧客によって所有もしくは操作され得ない。データプレーンミラーアプリ層 1 6 4 0 は、データプレーン VCN 1 6 1 8 へのコールを行うように構成され得るが、制御プレーン VCN 1 6 1 6 内に包含されるいかなるエンティティへのコールも行うように構成され得ない。顧客は、制御プレーン VCN 1 6 1 6 内でプロビジョニングされたデータプレーン VCN 1 6 1 8 内の

40

50

リソースをデプロイするか、または他の仕方を使用することを所望し得、データプレーンミラーアプリ層 1640 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。

【0213】

実施形態によっては、IaaSプロバイダの顧客はフィルタをデータプレーンVCN1618に適用することができる。本実施形態では、顧客は、データプレーンVCN1618が何にアクセスすることができるかを決定することができ、顧客はデータプレーンVCN1618から公衆インターネット1654へのアクセスを制限し得る。IaaSプロバイダは、フィルタを適用するか、または他の仕方ですべての外部ネットワークまたはデータベースへのデータプレーンVCN1618のアクセスを制御することが不可能であり得る。顧客テナンシー1621内に包含される、データプレーンVCN1618に対して顧客によってフィルタおよび制御を適用することは、データプレーンVCN1618を他の顧客から、および公衆インターネット1654から隔離することを助けることができる。

【0214】

実施形態によっては、クラウドサービス1656は、公衆インターネット1654上、制御プレーンVCN1616上、またはデータプレーンVCN1618上に存在し得ないサービスにアクセスするためにサービスゲートウェイ1636によってコールされ得る。クラウドサービス1656と制御プレーンVCN1616またはデータプレーンVCN1618との間の接続はライブまたは継続的でなくてもよい。クラウドサービス1656は、IaaSプロバイダによって所有または操作される異なるネットワーク上に存在し得る。クラウドサービス1656は、サービスゲートウェイ1636からのコールを受信するように構成され得、公衆インターネット1654からのコールを受信しないように構成され得る。一部のクラウドサービス1656は他のクラウドサービス1656から隔離され得、制御プレーンVCN1616は、制御プレーンVCN1616と同じリージョン内にないことがあるクラウドサービス1656から隔離され得る。例えば、制御プレーンVCN1616は「リージョン1」内に配置され得、クラウドサービス「デプロイメント5」はリージョン1内および「リージョン2」内に配置され得る。リージョン1内に配置された制御プレーンVCN1616内に包含されるサービスゲートウェイ1636によってデプロイメント5へのコールが行われた場合には、コールはリージョン1内のデプロイメント5へ伝送され得る。本例では、制御プレーンVCN1616、またはリージョン1内のデプロイメント5は、リージョン2内のデプロイメント5と通信可能に結合されるか、または他の仕方ですべてと通信し得ない。

【0215】

図17は、少なくとも1つの実施形態に係る、クラウド・インフラストラクチャ・アズ・ア・サービス・システムを実施するための別のパターンを示すブロック図である。

【0216】

図17は、少なくとも1つの実施形態に係る、IaaSアーキテクチャの別の例示的なパターンを示すブロック図1700である。サービスオペレータ1702（例えば、図15の、サービスオペレータ1502）は、仮想クラウドネットワーク（VCN）1706（例えば、図15のVCN1506）およびセキュアホストサブネット1708（例えば、図15のセキュアホストサブネット1508）を含むことができるセキュアホストテナンシー1704（例えば、図15のセキュアホストテナンシー1504）に通信可能に結合され得る。VCN1706は、SSH VCN1712内に包含されるLPG1710を介してSSH VCN1712（例えば、図15のSSH VCN1512）に通信可能に結合され得るLPG1710（例えば、図15のLPG1510）を含むことができる。SSH VCN1712はSSHサブネット1714（例えば、図15のSSHサブネット1514）を含むことができ、SSH VCN1712は、制御プレーンVCN1716内に包含されるLPG1710を介して制御プレーンVCN1716（例えば、図15の制御プレーンVCN1516）に、およびデータプレーンVCN1718内に包含されるLPG1710を介してデータプレーンVCN1718（例えば、図15のデータ

プレーン 1 5 1 8) に通信可能に結合され得る。制御プレーン V C N 1 7 1 6 およびデータプレーン V C N 1 7 1 8 はサービステナンシー 1 7 1 9 (例えば、図 1 5 のサービステナンシー 1 5 1 9) 内に包含され得る。

【0 2 1 7】

制御プレーン V C N 1 7 1 6 は、ロードバランサ (L B) サブネット 1 7 2 2 (例えば、図 1 5 の L B サブネット 1 5 2 2) を含むことができる制御プレーン D M Z 層 1 7 2 0 (例えば、図 1 5 の制御プレーン D M Z 層 1 5 2 0)、アプリサブネット 1 7 2 6 (例えば、図 1 5 のアプリサブネット 1 5 2 6 と同様のもの) を含むことができる制御プレーン アプリ層 1 7 2 4 (例えば、図 1 5 の制御プレーン アプリ層 1 5 2 4)、D B サブネット 1 7 3 0 を含むことができる制御プレーン データ層 1 7 2 8 (例えば、図 1 5 の制御プレーン データ層 1 5 2 8) を含むことができる。制御プレーン D M Z 層 1 7 2 0 内に包含される L B サブネット 1 7 2 2 は、制御プレーン アプリ層 1 7 2 4 内に包含されるアプリサブネット 1 7 2 6 に、および制御プレーン V C N 1 7 1 6 内に包含され得るインターネットゲートウェイ 1 7 3 4 (例えば、図 1 5 のインターネットゲートウェイ 1 5 3 4) に通信可能に結合され得、アプリサブネット 1 7 2 6 は、制御プレーン データ層 1 7 2 8 内に包含される D B サブネット 1 7 3 0 に、ならびにサービスゲートウェイ 1 7 3 6 (例えば、図 1 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 (N A T) ゲートウェイ 1 7 3 8 (例えば、図 1 5 の N A T ゲートウェイ 1 5 3 8) に通信可能に結合され得る。制御プレーン V C N 1 7 1 6 はサービスゲートウェイ 1 7 3 6 および N A T ゲートウェイ 1 7 3 8 を含むことができる。

10

20

【0 2 1 8】

データプレーン V C N 1 7 1 8 は、データプレーン アプリ層 1 7 4 6 (例えば、図 1 5 のデータプレーン アプリ層 1 5 4 6)、データプレーン D M Z 層 1 7 4 8 (例えば、図 1 5 のデータプレーン D M Z 層 1 5 4 8)、およびデータプレーン データ層 1 7 5 0 (例えば、図 1 5 のデータプレーン データ層 1 5 5 0) を含むことができる。データプレーン D M Z 層 1 7 4 8 は、データプレーン アプリ層 1 7 4 6 の信頼できるアプリサブネット 1 7 6 0 および信頼できないアプリサブネット 1 7 6 2、ならびにデータプレーン V C N 1 7 1 8 内に包含されるインターネットゲートウェイ 1 7 3 4 に通信可能に結合され得る L B サブネット 1 7 2 2 を含むことができる。信頼できるアプリサブネット 1 7 6 0 は、データプレーン V C N 1 7 1 8 内に包含されるサービスゲートウェイ 1 7 3 6、データプレーン V C N 1 7 1 8 内に包含される N A T ゲートウェイ 1 7 3 8、およびデータプレーン データ層 1 7 5 0 内に包含される D B サブネット 1 7 3 0 に通信可能に結合され得る。信頼できないアプリサブネット 1 7 6 2 は、データプレーン V C N 1 7 1 8 内に包含されるサービスゲートウェイ 1 7 3 6、およびデータプレーン データ層 1 7 5 0 内に包含される D B サブネット 1 7 3 0 に通信可能に結合され得る。データプレーン データ層 1 7 5 0 は、データプレーン V C N 1 7 1 8 内に包含されるサービスゲートウェイ 1 7 3 6 に通信可能に結合され得る D B サブネット 1 7 3 0 を含むことができる。

30

【0 2 1 9】

信頼できないアプリサブネット 1 7 6 2 は、テナント仮想機械 (V M) 1 7 6 6 (1) ~ (N) に通信可能に結合され得る 1 つまたは複数のプライマリ V N I C 1 7 6 4 (1) ~ (N) を含むことができる。各テナント V M 1 7 6 6 (1) ~ (N) は、それぞれの顧客テナンシー 1 7 7 0 (1) ~ (N) 内に包含され得るそれぞれのコンテナエグレス V C N 1 7 6 8 (1) ~ (N) 内に包含され得るそれぞれのアプリサブネット 1 7 6 7 (1) ~ (N) に通信可能に結合され得る。それぞれのセカンダリ V N I C 1 7 7 2 (1) ~ (N) は、データプレーン V C N 1 7 1 8 内に包含される信頼できないアプリサブネット 1 7 6 2 とコンテナエグレス V C N 1 7 6 8 (1) ~ (N) 内に包含さ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 V C N 1 7 6 8 (1) ~ (N) は、公衆インターネット 1 7 5 4 (例えば、図 1 5 の公衆インターネット 1 5 5 4) に通信可能に結合され得る N A T ゲートウェイ 1 7 3 8 を含むことができる。

40

【0 2 2 0】

50

制御プレーンVCN1716内に包含される、およびデータプレーンVCN1718内に包含されるインターネットゲートウェイ1734は、公衆インターネット1754に通信可能に結合され得るメタデータ管理サービス1752（例えば、図15のメタデータ管理システム1552）に通信可能に結合され得る。公衆インターネット1754は、制御プレーンVCN1716内に包含される、およびデータプレーンVCN1718内に包含されるNATゲートウェイ1738に通信可能に結合され得る。制御プレーンVCN1716内に包含される、およびデータプレーンVCN1718内に包含されるサービスゲートウェイ1736はクラウドサービス1756に通信可能に結合することができる。

【0221】

実施形態によっては、データプレーンVCN1718は顧客テナンシー1770と統合され得る。この統合は、コードを実行する際のサポートを所望し得る場合などの一部の場合に、IaaSプロバイダの顧客のために有用になる、または望ましくなり得る。顧客は、破壊性を有し得るコードを実行のために提供し得るか、他の顧客リソースと通信し得るか、または他の仕方では望ましくない影響を引き起こし得る。これに応じて、IaaSプロバイダは、顧客によってIaaSプロバイダに与えられたコードを実行するべきかどうかを決定し得る。

【0222】

例によっては、IaaSプロバイダの顧客はIaaSプロバイダへの一時的なネットワークアクセスを許可し、機能がデータプレーン層アプリ1746にアタッチされることを要求し得る。機能を実行するべきコードはVM1766（1）～（N）内で実行され得、コードは、データプレーンVCN1718上の他のどの場所でも実行するようには構成され得ない。各VM1766（1）～（N）は1つの顧客テナンシー1770に接続され得る。VM1766（1）～（N）内に包含されるそれぞれのコンテナ1771（1）～（N）は、コードを実行するようには構成され得る。この場合には、誤った、または他の状態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を助け得る、二重隔離が存在し得る（例えば、コンテナ1771（1）～（N）がコードを実行し、コンテナ1771（1）～（N）は、少なくとも、信頼できないアプリサブネット1762内に包含されるVM1766（1）～（N）内に包含され得る）。コンテナ1771（1）～（N）は顧客テナンシー1770に通信可能に結合され得、顧客テナンシー1770に対してデータを伝送または受信するようには構成され得る。コンテナ1771（1）～（N）は、データプレーンVCN1718内のいずれの他のエンティティに対してもデータを伝送または受信するようには構成され得ない。コードの実行を完了すると、IaaSプロバイダはコンテナ1771（1）～（N）をキルするか、または他の仕方では処分し得る。

【0223】

実施形態によっては、信頼できるアプリサブネット1760は、IaaSプロバイダによって所有または操作され得るコードを実行し得る。本実施形態では、信頼できるアプリサブネット1760はDBサブネット1730に通信可能に結合され、DBサブネット1730内のCRUD操作を実行するようには構成され得る。信頼できないアプリサブネット1762はDBサブネット1730に通信可能に結合され得るが、本実施形態では、信頼できないアプリサブネットは、DBサブネット1730内の読み出し操作を実行するようには構成され得る。各顧客のVM1766（1）～（N）内に包含され得、顧客からのコードを実行し得るコンテナ1771（1）～（N）はDBサブネット1730と通信可能に結合され得ない。

【0224】

他の実施形態では、制御プレーンVCN1716およびデータプレーンVCN1718は直接通信可能に結合され得ない。本実施形態では、制御プレーンVCN1716とデータプレーンVCN1718との間の直接通信が存在し得ない。しかし、通信は少なくとも1つの方法を通じて間接的に行われ得る。制御プレーンVCN1716とデータプレーンVCN1718との間の通信を促進することができるLPG1710がIaaSプロバイ

10

20

30

40

50

ダによって確立され得る。別の例では、制御プレーンVCN1716またはデータプレーンVCN1718はサービスゲートウェイ1736を介してクラウドサービス1756へのコールを行うことができる。例えば、制御プレーンVCN1716からクラウドサービス1756へのコールは、データプレーンVCN1718と通信することができるサービスのための要求を含むことができる。

【0225】

図18は、少なくとも1つの実施形態に係る、クラウド・インフラストラクチャ・アズ・ア・サービス・システムを実施するための別のパターンを示すブロック図である。

【0226】

図18は、少なくとも1つの実施形態に係る、IaaSアーキテクチャの別の例示的なパターンを示すブロック図1800である。サービスオペレータ1802（例えば、図15の、サービスオペレータ1502）は、仮想クラウドネットワーク（VCN）1806（例えば、図15のVCN1506）およびセキュアホストサブネット1808（例えば、図15のセキュアホストサブネット1508）を含むことができるセキュアホストテナンシー1804（例えば、図15のセキュアホストテナンシー1504）に通信可能に結合され得る。VCN1806は、SSH VCN1812内に包含されるLPG1810を介してSSH VCN1812（例えば、図15のSSH VCN1512）に通信可能に結合され得るLPG1810（例えば、図15のLPG1510）を含むことができる。SSH VCN1812はSSHサブネット1814（例えば、図15のSSHサブネット1514）を含むことができ、SSH VCN1812は、制御プレーンVCN1816内に包含されるLPG1810を介して制御プレーンVCN1816（例えば、図15の制御プレーンVCN1516）に、およびデータプレーンVCN1818内に包含されるLPG1810を介してデータプレーンVCN1818（例えば、図15のデータプレーン1518）に通信可能に結合され得る。制御プレーンVCN1816およびデータプレーンVCN1818はサービステナンシー1819（例えば、図15のサービステナンシー1519）内に包含され得る。

【0227】

制御プレーンVCN1816は、LBサブネット1822（例えば、図15のLBサブネット1522）を含むことができる制御プレーンDMZ層1820（例えば、図15の制御プレーンDMZ層1520）、アプリサブネット1826（例えば、図15のアプリサブネット1526）を含むことができる制御プレーンアプリ層1824（例えば、図15の制御プレーンアプリ層1524）、DBサブネット1830（例えば、図17のDBサブネット1730）を含むことができる制御プレーンデータ層1828（例えば、図15の制御プレーンデータ層1528）を含むことができる。制御プレーンDMZ層1820内に包含されるLBサブネット1822は、制御プレーンアプリ層1824内に包含されるアプリサブネット1826に、および制御プレーンVCN1816内に包含され得るインターネットゲートウェイ1834（例えば、図15のインターネットゲートウェイ1534）に通信可能に結合され得、アプリサブネット1826は、制御プレーンデータ層1828内に包含されるDBサブネット1830に、ならびにサービスゲートウェイ1836（例えば、図15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1838（例えば、図15のNATゲートウェイ1538）に通信可能に結合され得る。制御プレーンVCN1816はサービスゲートウェイ1836およびNATゲートウェイ1838を含むことができる。

【0228】

データプレーンVCN1818は、データプレーンアプリ層1846（例えば、図15のデータプレーンアプリ層1546）、データプレーンDMZ層1848（例えば、図15のデータプレーンDMZ層1548）、およびデータプレーンデータ層1850（例えば、図15のデータプレーンデータ層1550）を含むことができる。データプレーンDMZ層1848は、データプレーンアプリ層1846の信頼できるアプリサブネット1860（例えば、図17の信頼できるアプリサブネット1760）および信頼できないアプ

10

20

30

40

50

リサブネット 1862（例えば、図 17 の信頼できないアプリサブネット 1762）、ならびにデータプレーン VCN 1818 内に包含されるインターネットゲートウェイ 1834 に通信可能に結合され得る LB サブネット 1822 を含むことができる。信頼できるアプリサブネット 1860 は、データプレーン VCN 1818 内に包含されるサービスゲートウェイ 1836、データプレーン VCN 1818 内に包含される NAT ゲートウェイ 1838、およびデータプレーンデータ層 1850 内に包含される DB サブネット 1830 に通信可能に結合され得る。信頼できないアプリサブネット 1862 は、データプレーン VCN 1818 内に包含されるサービスゲートウェイ 1836、およびデータプレーンデータ層 1850 内に包含される DB サブネット 1830 に通信可能に結合され得る。データプレーンデータ層 1850 は、データプレーン VCN 1818 内に包含されるサービスゲートウェイ 1836 に通信可能に結合され得る DB サブネット 1830 を含むことができる。

10

【0229】

信頼できないアプリサブネット 1862 は、信頼できないアプリサブネット 1862 内に常駐するテナント仮想機械（VM）1866（1）～（N）に通信可能に結合され得るプライマリ VNIC 1864（1）～（N）を含むことができる。各テナント VM 1866（1）～（N）はそれぞれのコンテナ 1867（1）～（N）内でコードを実行し、コンテナエグレス VCN 1868 内に包含され得るデータプレーンアプリ層 1846 内に包含され得るアプリサブネット 1826 に通信可能に結合され得る。それぞれのセカンダリ VNIC 1872（1）～（N）は、データプレーン VCN 1818 内に包含される信頼できないアプリサブネット 1862 とコンテナエグレス VCN 1868 内に包含さ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 VCN は、公衆インターネット 1854（例えば、図 15 の公衆インターネット 1554）に通信可能に結合され得る NAT ゲートウェイ 1838 を含むことができる。

20

【0230】

制御プレーン VCN 1816 内に包含される、およびデータプレーン VCN 1818 内に包含されるインターネットゲートウェイ 1834 は、公衆インターネット 1854 に通信可能に結合され得るメタデータ管理サービス 1852（例えば、図 15 のメタデータ管理システム 1552）に通信可能に結合され得る。公衆インターネット 1854 は、制御プレーン VCN 1816 内に包含される、およびデータプレーン VCN 1818 内に包含される NAT ゲートウェイ 1838 に通信可能に結合され得る。制御プレーン VCN 1816 内に包含される、およびデータプレーン VCN 1818 内に包含されるサービスゲートウェイ 1836 はクラウドサービス 1856 に通信可能に結合することができる。

30

【0231】

例によっては、図 18 のブロック図 1800 のアーキテクチャによって示されるパターンは、図 17 のブロック図 1700 のアーキテクチャによって示されるパターンに対する例外と考えられ得、IaaS プロバイダが顧客（例えば、切断されたリージョン）と直接通信することができない場合に、IaaS プロバイダの顧客のために望ましくなり得る。顧客ごとの VM 1866（1）～（N）内に包含されるそれぞれのコンテナ 1867（1）～（N）は顧客によってリアルタイムにアクセスされ得る。コンテナ 1867（1）～（N）は、コンテナエグレス VCN 1868 内に包含され得るデータプレーンアプリ層 1846 のアプリサブネット 1826 内に包含されるそれぞれのセカンダリ VNIC 1872（1）～（N）へのコールを行うように構成され得る。セカンダリ VNIC 1872（1）～（N）はコールを NAT ゲートウェイ 1838 へ伝送することができ、NAT ゲートウェイ 1838 はコールを公衆インターネット 1854 へ伝送し得る。本例では、顧客によってリアルタイムにアクセスされ得るコンテナ 1867（1）～（N）は、制御プレーン VCN 1816 から隔離され得、データプレーン VCN 1818 内に包含される他のエンティティから隔離され得る。コンテナ 1867（1）～（N）はまた、他の顧客からのリソースからも隔離され得る。

40

【0232】

50

他の例では、顧客はコンテナ 1867 (1) ~ (N) を用いてクラウドサービス 1856 をコールすることができる。本例では、顧客はコンテナ 1867 (1) ~ (N) 内で、クラウドサービス 1856 からのサービスを要求するコードを実行し得る。コンテナ 1867 (1) ~ (N) はこの要求をセカンダリ VNIC 1872 (1) ~ (N) へ伝送することができ、セカンダリ VNIC 1872 (1) ~ (N) は要求を NAT ゲートウェイへ伝送することができ、NAT ゲートウェイは要求を公衆インターネット 1854 へ伝送することができる。公衆インターネット 1854 はインターネットゲートウェイ 1834 を介して要求を、制御プレーン VCN 1816 内に包含される LB サブネット 1822 へ伝送することができる。要求は有効であると決定したことに応じて、LB サブネットは要求をアプリサブネット 1826 へ伝送することができ、アプリサブネット 1826 はサービスゲートウェイ 1836 を介して要求をクラウドサービス 1856 へ伝送することができる。

10

【0233】

図に示される IaaS アーキテクチャ 1500、1600、1700、1800 は、示されたもの以外のコンポーネントを有し得ることを理解されたい。さらに、図に示される実施形態は、単に、本開示の一実施形態を組み込み得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すぎない。他の実施形態によっては、IaaS システムは、図に示されるのよりも多数または少数のコンポーネントを有し得るか、2 つ以上のコンポーネントを組み合わせ得るか、あるいはコンポーネントの異なる構成または配置を有し得る。

20

【0234】

一部の実施形態では、本明細書において説明される IaaS システムは、セルフサービスの、加入ベースの、弾力的にスケラブルな、信頼できる、高度に利用可能な、および安全な仕方で顧客へ配布される、アプリケーションのスイート、ミドルウェア、およびデータベースサービス提供を含み得る。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。

【0235】

図 19 は、少なくとも 1 つの実施形態に係る、例示的なコンピュータシステムを示すブロック図である。

【0236】

図 19 は、本開示の様々な実施形態が実施され得る、例示的なコンピュータシステム 1900 を示す。システム 1900 は、上述されたコンピュータシステムのうちの任意のものを実施するために用いられ得る。図に示されるように、コンピュータシステム 1900 は、バスサブシステム 1902 を介して多数の周辺サブシステムと通信する処理ユニット 1904 を含む。これらの周辺サブシステムは、処理加速ユニット 1906、I/O サブシステム 1908、ストレージサブシステム 1918、および通信サブシステム 1924 を含み得る。ストレージサブシステム 1918 は有形のコンピュータ可読記憶媒体 1922 およびシステムメモリ 1910 を含む。

30

【0237】

バスサブシステム 1902 は、コンピュータシステム 1900 の様々なコンポーネントおよびサブシステムに、意図されたとおりに互いに通信させるための機構を提供する。バスサブシステム 1902 は単一のバスとして概略的に示されているが、バスサブシステムの代替的实施形態は複数のバスを利用し得る。バスサブシステム 1902 は、メモリバスもしくはメモリコントローラ、周辺バス、および種々のバスアーキテクチャのうちの任意のものをを用いたローカルバスを含むいくつかの種類のバス構造のうちの任意のものであり得る。例えば、こ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 規格に合わせて製造されるメザンバスとして実施され得る、周辺装置相互接続 (PCI: Peripheral Co

40

50

Component Interconnect) バスが挙げられ得る。

【0238】

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）として実施され得る、処理ユニット1904がコンピュータシステム1900の動作を制御する。1つまたは複数のプロセッサが処理ユニット1904内に含まれ得る。これらのプロセッサはシングルコアまたはマルチコアプロセッサを含み得る。一部の実施形態では、処理ユニット1904は、シングルまたはマルチコアプロセッサが各処理ユニット内に含まれる1つまたは複数の独立した処理ユニット1932および／または1934として実施され得る。他の実施形態では、処理ユニット1904はまた、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たクアッドコア処理ユニットとして実施され得る。

10

【0239】

様々な実施形態では、処理ユニット1904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、複数の同時に実行するプログラムまたはプロセスを維持することができる。いかなる時でも、実行されるべきプログラムコードのうちの一部または全てはプロセッサ1904内および／またはストレージサブシステム1918内に常駐していることができる。好適なプログラミングを通じて、プロセッサ1904は、上述された様々な機能性を提供することができる。コンピュータシステム1900は、デジタル信号プロセッサ（DSP：digital signal processor）、専用プロセッサ、および／または同様のものを含むことができる、処理加速ユニット1906を追加的に含み得る。

20

【0240】

I/Oサブシステム1908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み得る。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、ディスプレイ内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、マイクロフォンを用いたオーディオ入力デバイス、ならびに他の種類の入力デバイスを含み得る。ユーザインターフェース入力デバイスは、例えば、ユーザが、ジェスチャおよび発話コマンドを用いたナチュラルユーザインターフェースを通じて、Microsoft Xbox（登録商標）360ゲームコントローラなどの、入力デバイスを制御し、それと対話することを可能にする、Microsoft Kinect（登録商標）動きセンサなどの動作検知および／またはジェスチャ認識デバイスを含み得る。ユーザインターフェース入力デバイスはまた、ユーザから眼の活動（例えば、写真を撮影している、および／またはメニューの選択を行っている間に「瞬きすること」）を検出し、アイジェスチャを入力デバイス（例えば、Google Glass（登録商標））内への入力として変換する、Google Glass（登録商標）瞬き検出器などのアイジェスチャ認識デバイスを含み得る。加えて、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通じて音声認識システム（例えば、Siri（登録商標）ナビゲータ）と対話することを可能にする音声認識感知デバイスを含み得る。

30

【0241】

ユーザインターフェース入力デバイスはまた、限定するものではないが、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、デジタルカムコーダ、ポータブルメディアプレーヤ、ウェブカメラ、イメージスキャナ、指紋スキャナ、バーコードリーダー3Dスキャナ、3Dプリンタ、レーザー測距器、および視線追跡デバイスなどの聴覚／視覚デバイスを含み得る。加えて、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、磁気共鳴映像、位置（position）放射断層撮影、医療超音波検査デバイスなどの医療撮像入力デバイスを含み得る。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、および同様のものなどのオーディオ入力デバイスを含み得る。

40

【0242】

50

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、またはオーディオ出力デバイス等の非視覚的ディスプレイを含み得る。ディスプレイサブシステムは、陰極線管（CRT：cathode ray tube）、液晶ディスプレイ（LCD：liquid crystal display）またはプラズマディスプレイを用いるものなどの、フラットパネルデバイス、投影デバイス、タッチスクリーン、ならびに同様のものであり得る。概して、用語「出力デバイス」の使用は、情報をコンピュータシステム1900からユーザまたは他のコンピュータへ出力するための全ての可能な種類のデバイスおよび機構を含むことを意図される。例えば、ユーザインターフェース出力デバイスは、限定するものではないが、モニタ、プリンタ、スピーカ、ヘッドフォン、自動車ナビゲーションシステム、プロッタ、音声出力デバイス、およびモデムなどの、テキスト、グラフィックス、および音声／映像情報を視覚的に伝える種々の表示デバイスを含み得る。

10

【0243】

コンピュータシステム1900は、本開示において説明される実施形態の機能性を提供するソフトウェアおよびデータ構造を記憶するための有形の非一時的コンピュータ可読記憶媒体を提供するストレージサブシステム1918を備え得る。ソフトウェアは、処理ユニット1904の1つまたは複数のコアまたはプロセッサによって実行されると、上述された機能性を提供する、プログラム、コードシステム、命令、スクリプト等を含むことができる。ストレージサブシステム1918はまた、本開示に従って用いられるデータを記憶するためのリポジトリを提供し得る。

【0244】

図19における例に示されるように、ストレージサブシステム1918は、システムメモリ1910、コンピュータ可読記憶媒体1922、およびコンピュータ可読記憶媒体リーダー1920を含む様々なコンポーネントを含むことができる。システムメモリ1910は、処理ユニット1904によってロード可能で、実行可能であるプログラム命令を記憶し得る。システムメモリ1910はまた、命令の実行中に用いられるデータ、および／またはプログラム命令の実行中に生成されたデータを記憶し得る。限定するものではないが、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：relational database management system）、仮想機械、コンテナ等を含む、様々な異なる種類のプログラムがシステムメモリ1910内にロードされ得る。

20

30

【0245】

システムメモリ1910はまた、オペレーティングシステム1916を記憶し得る。オペレーティングシステム1916の例としては、様々なバージョンの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）もしくはUNIX系オペレーティングシステム（限定するものではないが、種々のGNU/Linuxオペレーティングシステム、Google Chrome（登録商標）OS、および同様のものを含む）、ならびに／あるいはiOS、Windows（登録商標）Phone、Android（登録商標）OS、BlackBerry（登録商標）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挙げることができる。コンピュータシステム1900が1つまたは複数の仮想機械を実行する一部の実装形態では、仮想機械はそれらのゲストオペレーティングシステム（GOS：guest operating system）と共にシステムメモリ1910内にロードされ、処理ユニット1904の1つまたは複数のプロセッサまたはコアによって実行され得る。

40

【0246】

システムメモリ1910は、コンピュータシステム1900の種類に応じて異なる構成のものであることができる。例えば、システムメモリ1910は、揮発性メモリ（ランダムアクセスメモリ（RAM：random access memory）など）、および／または不揮発性メモリ（リードオンリーメモリ（ROM：read-only memory）、フラッシュメモリ等）であり得る。スタティックランダムアクセスメモリ（SRAM：static random

50

access memory)、ダイナミックランダムアクセスメモリ(DRAM:dynamic random access memory)、および他のものを含む、異なる種類のRAM構成が提供され得る。実装形態によっては、システムメモリ1910は、起動の最中などに、コンピュータシステム1900内の要素間で情報を転送するのを助けるための基本ルーチンを包含する、基本入出力システム(BIOS:basic input/output system)を含み得る。

【0247】

コンピュータ可読記憶媒体1922は、コンピュータシステム1900の処理ユニット1904によって実行可能な命令を含むコンピュータシステム1900による使用のためのコンピュータ可読情報を、一時的に、および／またはより永久的に包含し、記憶するための、リモート、ローカル、固定式、および／または着脱式記憶デバイス・プラス・記憶媒体を表現し得る。

10

【0248】

コンピュータ可読記憶媒体1922はまた、限定するものではないが、情報の記憶および／または伝送のための任意の方法または技術において実施される揮発性および不揮発性、着脱式および非着脱式媒体などの、記憶媒体および通信媒体を含む、当技術分野において知られた、または用いられる、任意の適切な媒体を含むことができる。これは、RAM、ROM、電氣的削除可能プログラマブルROM(EEPROM:electronically erasable programmable ROM)、フラッシュメモリ、または他のメモリ技術、CD-ROM、デジタルバーサタイルディスク(DVD:digital versatile disk)、または他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージ、または他の磁気記憶デバイス、あるい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。

20

【0249】

例として、コンピュータ可読記憶媒体1922は、非着脱式不揮発性磁気媒体から読み出す、またはそれに書き込むハードディスクドライブ、着脱式不揮発性磁気ディスクから読み出す、またはそれに書き込む磁気ディスクドライブ、ならびにCD-ROM、DVD、およびBlu-Ray(登録商標)ディスク、または他の光媒体などの、着脱式不揮発性光ディスクから読み出す、またはそれに書き込む光ディスクドライブを含み得る。コンピュータ可読記憶媒体1922は、限定するものではないが、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:universal serial bus)フラッシュドライブ、セキュアデジタル(SD:secure digital)カード、DVDディスク、デジタルビデオテープ、および同様のものを含み得る。コンピュータ可読記憶媒体1922はまた、フラッシュメモリベースのSSD、企業フラッシュドライブ、ソリッドステートROM、および同様のものなどの、不揮発性メモリに基づくソリッドステートドライブ(SSD:solid-state drive)、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:magnetoresistive RAM)SSDなどの、揮発性メモリに基づくSSD、ならびにDRAMおよびフラッシュメモリベースのSSDの組み合わせを用いるハイブリッドSSDを含み得る。ディスクドライブおよびそれらの関連コンピュータ可読媒体は、コンピュータ可読命令、データ構造、プログラムシステム、およびコンピュータシステム1900のための他のデータの非揮発性記憶をもたらし得る。

30

40

【0250】

処理ユニット1904の1つまたは複数のプロセッサまたはコアによって実行可能な機械可読命令は非一時的コンピュータ可読記憶媒体上に記憶され得る。非一時的コンピュータ可読記憶媒体は、揮発性メモリ記憶デバイスおよび／または不揮発性記憶デバイスを含む物理的に有形のメモリまたは記憶デバイスを含むことができる。非一時的コンピュータ可読記憶媒体の例としては、磁気記憶媒体(例えば、ディスクまたはテープ)、光記憶媒体(例えば、DVD、CD)、様々な種類のRAM、ROM、またはフラッシュメモリ、ハードドライブ、フロッピー(登録商標)ドライブ、着脱式メモリドライブ(例えば、USBドライブ)、あるいは他の種類の記憶デバイスが挙げられる。

50

【0251】

通信サブシステム1924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1924は、他のシステムからデータを受信し、コンピュータシステム1900から他のシステムへデータを伝送するためのインターフェースの役割を果たす。例えば、通信サブシステム1924は、コンピュータシステム1900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ことを可能にし得る。実施形態によっては、通信サブシステム1924は、（例えば、セルラ電話技術、3G、4G、もしくはEDGE（enhanced data rates for global evolution（エンハンスドデータレート・フォー・グローバルエボリューション））などの、先進データネットワーク技術、Wi-Fi（IEEE 802.11ファミリー規格、または他のモバイル通信技術、あるいはこれらの任意の組み合わせ）を用いて）無線音声および／またはデータネットワークにアクセスするための無線周波数（RF：radio frequency）トランシーバコンポーネント、全地球測位システム（GPS：global positioning system）受信器コンポーネント、ならびに／あるいは他のコンポーネントを含むことができる。実施形態によっては、通信サブシステム1924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）を提供することができる。

10

【0252】

実施形態によっては、通信サブシステム1924はまた、コンピュータシステム1900を使用し得る1人または複数のユーザのために、構造化された、および／または構造化されていないデータフィード1926、イベントストリーム1928、イベント更新1930、ならびに同様のものの形態の入力通信を受信し得る。

20

【0253】

例として、通信サブシステム1924は、Twitter（登録商標）フィード、Facebook（登録商標）更新、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つまたは複数のサードパーティ情報源からのリアルタイム更新など、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1926をリアルタイムに受信するように構成され得る。

【0254】

加えて、通信サブシステム1924はまた、明確な終端を本質的に有しない、連続的な、または境界のないものであり得る、リアルタイムイベントのイベントストリーム1928、および／またはイベント更新1930を含み得る、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され得る。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、金融株式相場表示板、ネットワーク性能測定ツール（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、自動車トラフィック監視、ならびに同様のものが挙げられ得る。

30

【0255】

通信サブシステム1924はまた、構造化された、および／または構造化されていないデータフィード1926、イベントストリーム1928、イベント更新1930、ならびに同様のものを、コンピュータシステム1900に結合された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し得る1つまたは複数のデータベースへ出力するように構成され得る。

40

【0256】

コンピュータシステム1900は、ハンドヘルドポータブルデバイス（例えば、iPhone（登録商標）セルラ電話、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、または任意の他のデータ処理システムを含む、様々な種類のうちの1つであることができる。

【0257】

50

コンピュータおよびネットワークの絶え間なく変化し続ける性質のゆえに、図に示されるコンピュータシステム1900の説明は単なる具体例として意図されているにすぎない。図に示されるシステムよりも多数または少数のコンポーネントを有する多くの他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も用いられ得、ならびに／あるいは特定の要素は、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）、または組み合わせの形で実施され得るであろう。さらに、ネットワーク入力／出力デバイスなどの、他のコンピューティングデバイスへの接続が採用され得る。本明細書において提供される開示および教示に基づいて、当業者は、様々な実施形態を実施するための他の仕方および／または方法を理解するであろう。

【0258】

本開示の特定の実施形態が説明されたが、様々な変更、改変、代替的構造、および同等物も本開示の範囲内に包含される。本開示の実施形態は一部の特定のデータ処理環境内の動作に限定されず、複数のデータ処理環境内で自由に動作できる。加えて、本開示の実施形態は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されたが、当業者には、本開示の範囲は、説明され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が明らかであるはずである。上述の実施形態の様々な特徴および態様は、個々に、または合同で用いられ得る。

【0259】

さらに、本開示の実施形態は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されたが、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であることが認識されるべきである。本開示の実施形態は、ハードウェアの形でのみ、またはソフトウェアの形でのみ、あるいはこれらの組み合わせを用いて実施され得る。本明細書において説明される様々なプロセスは同じプロセッサまたは異なるプロセッサ上で任意の組み合わせで実施され得る。したがって、コンポーネントまたはシステムが、とある動作を遂行するように構成されているように説明されている場合、このような構成は、例えば、電子回路を、動作を遂行するように設計することによって、プログラム可能な電子回路（マイクロプロセッサなど）を、動作を遂行するようにプログラムすること、またはこれらの任意の組み合わせによって達成され得る。プロセスは、限定するものではないが、プロセス間通信のための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、異なる対のプロセスは異なる技術を用い得、または同じ対のプロセスは異なる時点で異なる技術を用い得る。

【0260】

したがって、明細書および図面は、限定でなく、例示的な意味で捉えられるべきである。しかし、請求項において記載されるとおりのより広い趣旨および範囲から逸脱することなく、追加、削減、削除、ならびに他の変更および改変がそれらに対して行われ得ることは明らかであろう。それゆえ、具体的な開示の実施形態が説明されたが、これらは限定であることを意図されていない。様々な変更および等価物が添付の請求項の範囲に含まれる。

【0261】

本開示の実施形態を説明する文脈における（特に、添付の請求項の文脈における）用語「a」、および「an」、および「the」ならびに同様の指示対象の使用は、本明細書において別途記載がないか、または文脈によって明確に否定されない限り、単数形および複数形の両方を包括すると解釈されるべきである。用語「備える（comprising）」、「有する（having）」、「含む（including）」、および「包含する（containing）」は、特に断りのない限り、オープンエンドな用語（すなわち、「限定するものではないが、～を含む（including, but not limited to）」を意味する）として解釈されるべきである。用語「接続される（connected）」は、たとえ、何らかの介在物が存在する場合でも、～内に部分的もしくは完全に包含される（partly or wholly contained within）、～に取り付けられる（attached to）、または相互に連結される（joined together）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記載は、本明細書にお

10

20

30

40

50

いて別途記載のない限り、単に、範囲に含まれる各々の別個の値に個々に言及する簡略的方法の役割を果たすことを意図されているにすぎず、各々の別個の値は、あたかもそれが本明細書において個々に記載されているかのように明細書に組み込まれる。本明細書において説明される全ての方法は、本明細書において別途記載がないか、または文脈によって別途明確に否定されない限り、任意の好適な順序で遂行され得る。本明細書において与えられるありとあらゆる例、または例示的な文言（例えば、「～など（such as）」）の使用は、単に、本開示の実施形態の理解をより容易にすることを意図されているにすぎず、別途断りのない限り、本開示の範囲に限定を課すものではない。明細書中のいかなる文言も、非クレーム要素を本開示の実施に不可欠のものとして指示していると解釈されてはならない。

10

【0262】

語句「X、Y、またはZのうちの少なくとも1つ」などの、離接的な文言は、別途特に断りのない限り、概して、項目、用語等は、X、Y、またはZのいずれか、あるいはこれらの任意の組み合わせ（例えば、X、Y、および／またはZ）であり得ることを示すために使用されると文脈内で理解されることを意図されている。それゆえ、このような離接的な文言は、概して、一部の実施形態は、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暗示することを意図されておらず、暗示するべきでない。

【0263】

本明細書では、本開示を実施するための発明者に知られた最良の形態を含む、本開示の好ましい実施形態が説明されている。それらの好ましい実施形態の変形例は、上述の説明を読むことで当業者に明らかになり得る。発明者は、当業者に、必要に応じてこのような変形例を採用することを期待しており、発明者は、本開示は、本明細書において具体的に説明されたもの以外の仕方を実施されることを意図している。したがって、本開示は、適用法によって許されるとおりの本明細書に添付された請求項に記載される主題の全ての変更例および同等物を含む。さらに、本明細書において別途記載がないか、または文脈によって別途明確に否定されない限り、それらの全ての可能な変形例における上述の要素の任意の組み合わせが本開示によって包含される。

20

【0264】

本明細書において挙げられた、公報、特許出願、および特許を含む、全ての参考文献は、あたかも、各参考文献が、参照により組み込まれるよう個々に具体的に指示され、その全体が本明細書において記載されているのと同じ程度に、本明細書において参照により組み込まれる。

30

【0265】

上述の明細書において、本開示の態様はその特定の実施形態を参照して説明されているが、当業者は、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。上述の開示の様々な特徴および態様は、個々に、または合同で用いられ得る。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、本明細書において説明されるものを超える任意の数の環境および適用において利用され得る。したがって、明細書および図面は、限定でなく、例示として捉えられるべきである。

40

【図面】
【図 1】

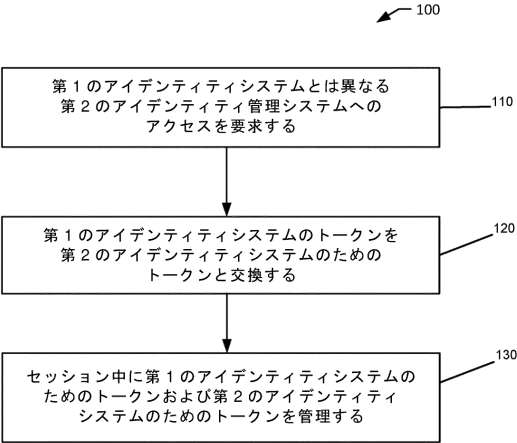


FIG. 1

【図 2】

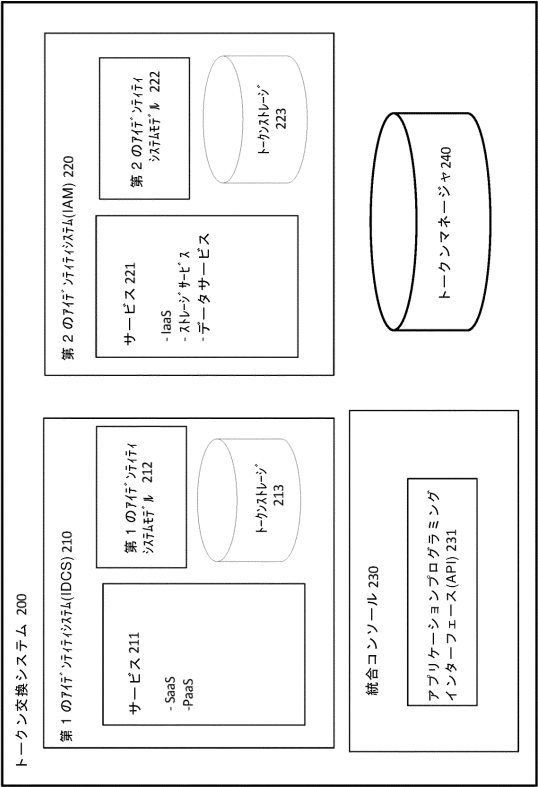


FIG. 2

【図 3】

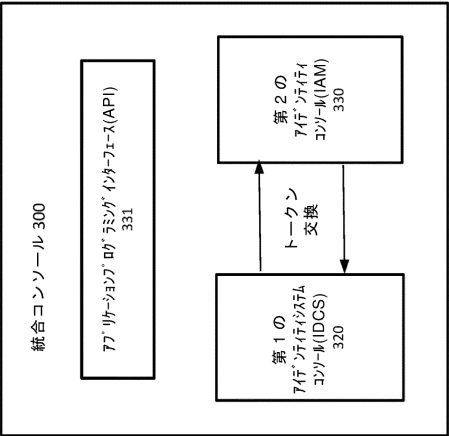


FIG. 3

【図 4】

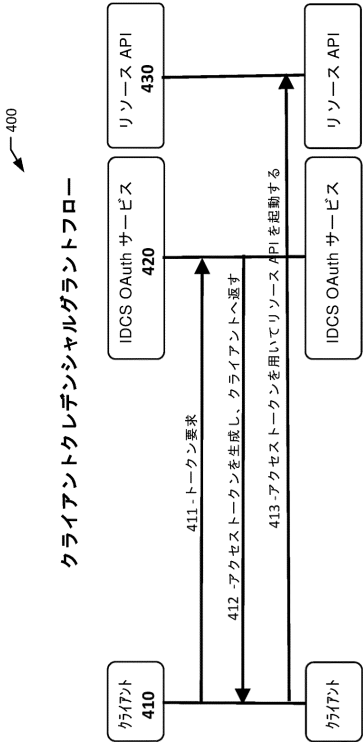


FIG. 4

10

20

30

40

50

【図 9】

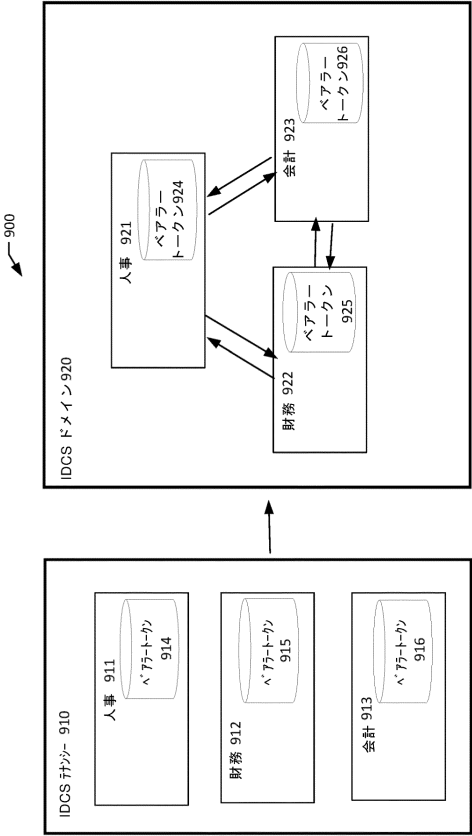


FIG. 9

【図 10】

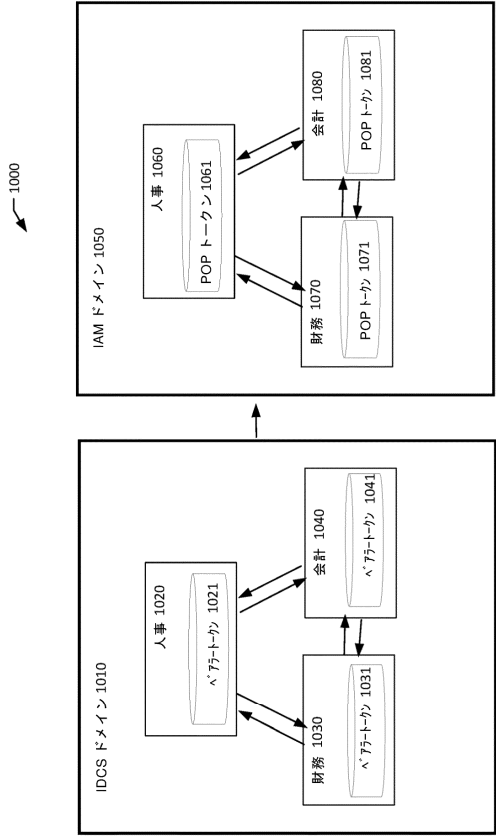


FIG. 10

【図 11】

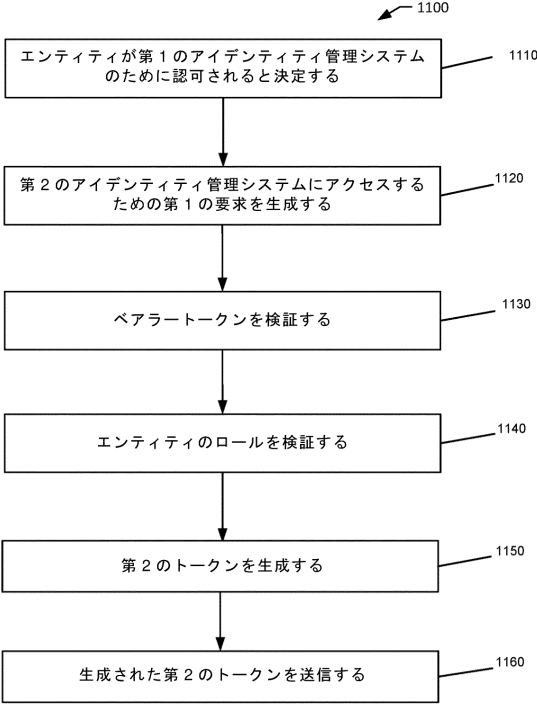


FIG. 11

【図 12】

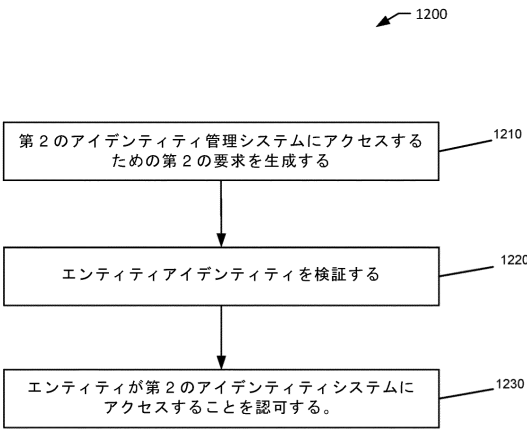


FIG. 12

10

20

30

40

50

【図 13】

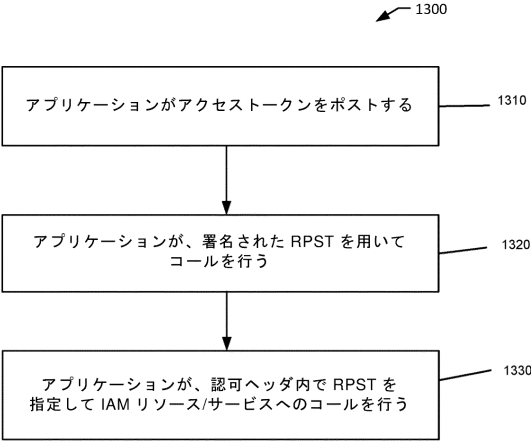


FIG. 13

【図 14】

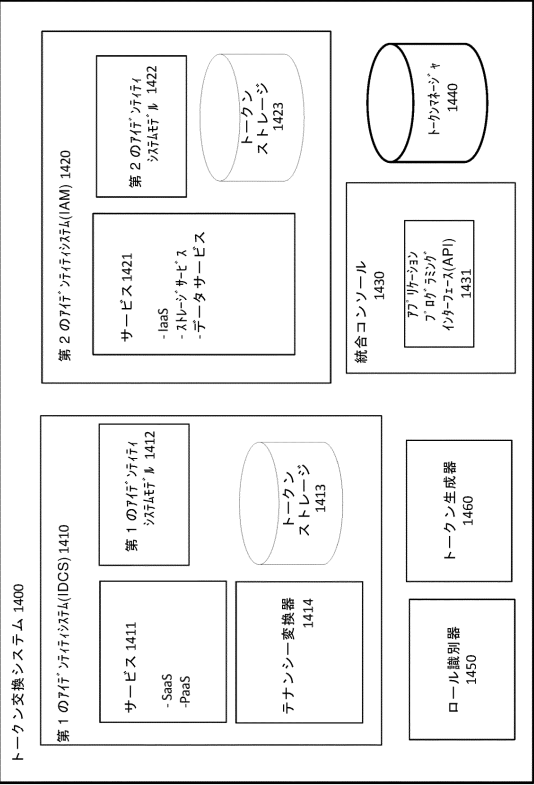


FIG. 14

【図 15】

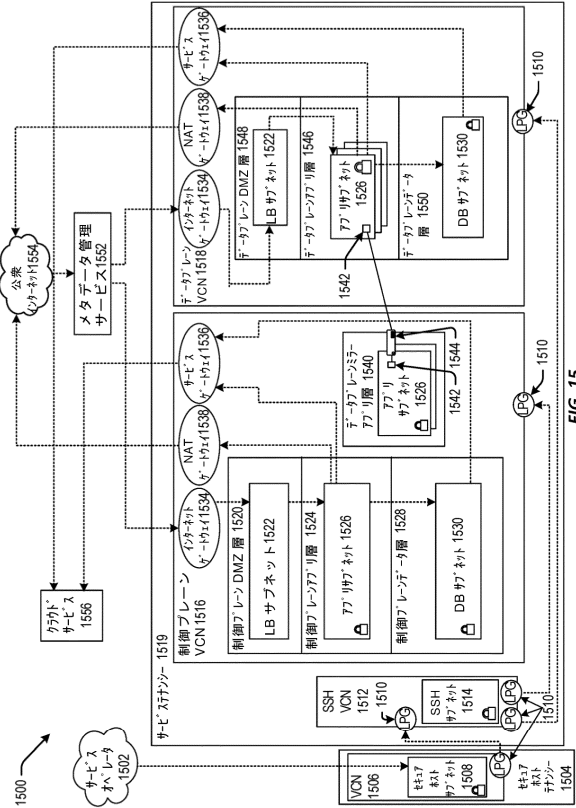


FIG. 15

【図 16】

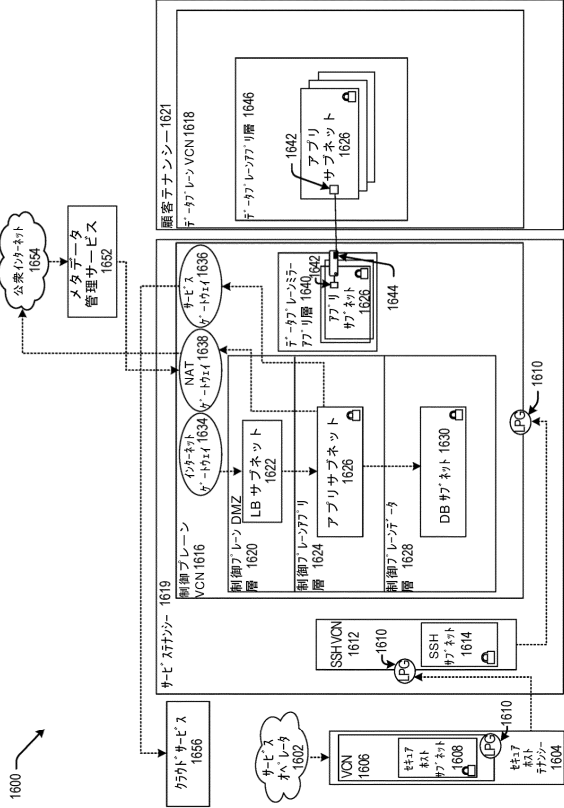


FIG. 16

【図 17】

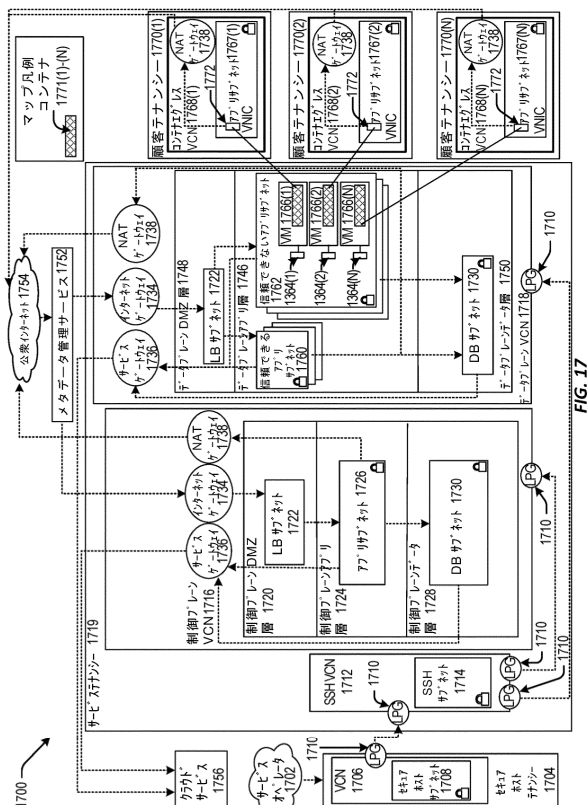


FIG. 17

【図 18】

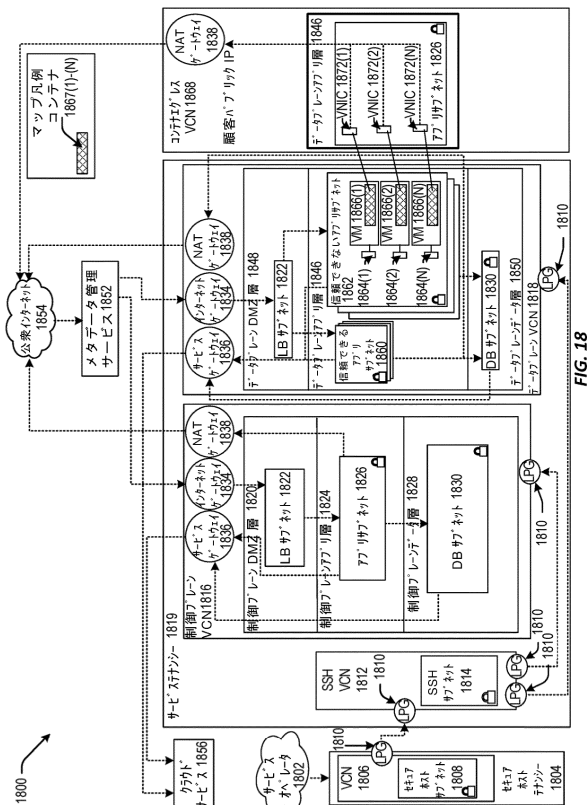


FIG. 18

【図 19】

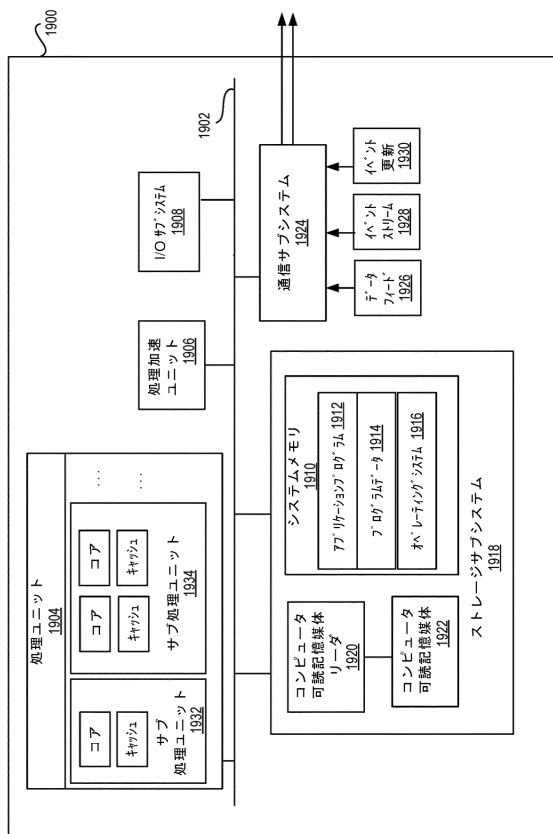


FIG. 19

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/044894

A. CLASSIFICATION OF SUBJECT MATTER
INV. 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 H04W

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of the Mission Critical (MC) service; (Release 17)", 3GPP STANDARD; TECHNICAL SPECIFICATION; 3GPP TS 33.180, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG3, no. V17.4.0 23 September 2021 (2021-09-23), pages 1-204, XP052056666, Retrieved from the Internet: URL:https://ftp.3gpp.org/Specs/archive/33_ series/33.180/33180-h40.zip 33180-h40.doc [retrieved on 2021-09-23] section 5.1.4; annexes B.4, B.7, C.1, C.2 -/-	1-19

☒ 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

11 January 2023

Date of mailing of the international search report

19/01/2023

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

Authorized officer

Murgan, Tudor A.

1

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

page 1 of 2

10

20

30

40

50

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/044894

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	----- US 2020/259652 A1 (SCHMALTZ III DOUGLAS BRENT [US] ET AL) 13 August 2020 (2020-08-13) abstract; par. 54-100	1-19
A	----- EP 2 761 522 B1 (ORACLE INT CORP [US]) 22 June 2016 (2016-06-22) abstract; par. 276; Fig. 3-5 and corresponding passages	1-19
A	----- HUNT P ET AL: "OAuth 2.0 Proof-of-Possession (PoP) Security Architecture; draft-ietf-oauth-pop-architecture-06.txt", OAUTH 2.0 PROOF-OF-POSSESSION (POP) SECURITY ARCHITECTURE; DRAFT-IETF-OAUTH-POP-ARCHITECTURE-06.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, 24 November 2015 (2015-11-24), pages 1-23, XP015109986, [retrieved on 2015-11-24] abstract -----	1-19

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/044894

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020259652 A1	13-08-2020	EP 3921991 A1	15-12-2021
		US 2020259652 A1	13-08-2020
		WO 2020163083 A1	13-08-2020

EP 2761522 B1	22-06-2016	CN 104255007 A	31-12-2014
		EP 2761522 A2	06-08-2014
		JP 6018210 B2	02-11-2016
		JP 2015501021 A	08-01-2015
		US 2013086645 A1	04-04-2013
		US 2013086657 A1	04-04-2013
		WO 2013049461 A2	04-04-2013

フロントページの続き

(32)優先日 令和4年9月26日(2022.9.26)

(33)優先権主張国・地域又は機関
米国(US)

(81)指定国・地域 AP(BW,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,MC,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,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,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. i O S

2. E T H E R N E T

アメリカ合衆国、9 4 0 6 5 カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、5 0 0

(72)発明者 ナガラジャ，ギリシュ

アメリカ合衆国、9 4 0 6 5 カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、5 0 0

(72)発明者 タマナ，ベンカタ・ラマ・プラサド

アメリカ合衆国、9 4 0 6 5 カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、5 0 0

(72)発明者 コール，ゲイリー・フィリップ

アメリカ合衆国、9 4 0 6 5 カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、5 0 0