(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-546424
(P2024-546424A)
(43)公表日　令和6年12月24日(2024.12.24)

(51)国際特許分類　ＦＩ
Ｇ０６Ｆ　21/57　(2013.01)　Ｇ０６Ｆ　21/57　３５０

審査請求　未請求　予備審査請求　未請求　（全36頁）

(21)出願番号　特願2024-527433(P2024-527433)
(86)(22)出願日　令和4年10月5日(2022.10.5)
(85)翻訳文提出日　令和6年7月2日(2024.7.2)
(86)国際出願番号　PCT/US2022/077605
(87)国際公開番号　WO2023/086712
(87)国際公開日　令和5年5月19日(2023.5.19)
(31)優先権主張番号　17/523,789
(32)優先日　令和3年11月10日(2021.11.10)
(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,
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　ペイン，ブライアン・スペンサー
アメリカ合衆国、９４０６５ 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、５００、オラクル・インターナショナル・コーポレイション内

(54)【発明の名称】　クラウドインフラストラクチャシステム内のコンピューティングノードの認可のためのエッジアテステーション

(57)【要約】
本実施形態は、クラウドインフラストラクチャ環境にアクセスするためのホストノードのエッジアテステーションに関する。認証データのセットは、ホストノードの認可のためにコンソールから取得され得る。認証データのセットは、第１の保証キー、およびホストノードの特徴を識別する認証ポリシを含み得る。ホストノードは、クラウドインフラストラクチャ環境に接続するためにネットワークアドレスの要求を送信し得る。ホストノードは、第２の保証キー、およびコンソールから受信される認証データのセットに対応するものとして検証され得る認証データを生成し得る。第２の保証キーおよび受信したホストノード認証データを検証することに応答して、ネットワークアドレスは、ネットワークアドレスを使用してクラウドインフラストラクチャ環境に接続するために使用され得るホストノードに提供され得る。

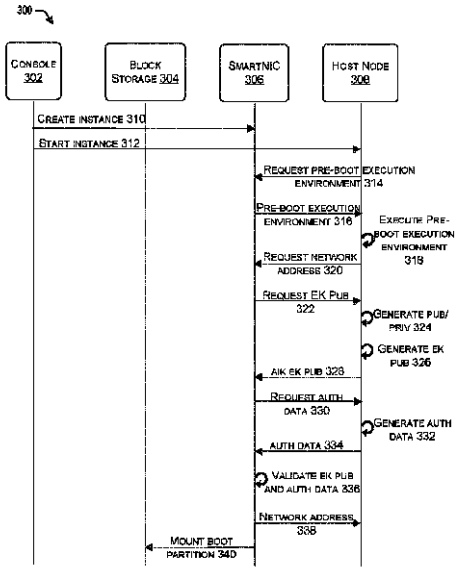


FIG. 3

【特許請求の範囲】
【請求項１】
クラウドインフラストラクチャ環境にアクセスするためのホストノードのアテステーションのための方法であって、
前記ホストノードの認可のためにコンソールから認証データのセットを取得することを含み、前記認証データのセットは、第１の保証キー、および前記ホストノードの特徴を識別する認証ポリシを含み、前記認証ポリシは、第１のプラットフォーム構成レジスタ値を含み、
前記方法は、
前記ホストノードから、前記クラウドインフラストラクチャ環境に接続するためにネットワークアドレスの要求を取得することと、
前記ホストノードから第２の保証キーを受信することと、
前記第２の保証キーを検証するために、前記認証データのセット内で受信した前記第１の保証キーと前記第２の保証キーとを比較することと、
前記ホストノードからホストノード認証データのセットを受信することとをさらに含み、前記ホストノード認証データのセットは、前記ホストノードのブートプロシージャ中にハッシュ化レジスタ値を含む第２のプラットフォーム構成レジスタ値を含み、
前記方法は、
前記第１のプラットフォーム構成レジスタ値が前記第２のプラットフォーム構成レジスタ値に一致するかどうかを決定することによって、前記受信したホストノード認証データのセットを検証するために、前記認証データのセット内で受信した前記認証ポリシと前記受信したホストノード認証データのセットとを比較することと、
前記第２の保証キーおよび前記受信したホストノード認証データのセットを検証することに応答して、前記ホストノードに前記ネットワークアドレスを提供することとをさらに含み、前記ホストノードは、前記ネットワークアドレスを使用して前記クラウドインフラストラクチャ環境に接続するように構成される、方法。
【請求項２】
前記第１の保証キーおよび前記第２の保証キーは、公開アテステーションアイデンティティキーである、請求項１に記載の方法。
【請求項３】
前記クラウドインフラストラクチャノードは、データセンタに配置されるエッジノードである、請求項１または請求項２に記載の方法。
【請求項４】
前記第２の保証キーを検証するために、前記認証データのセット内で受信した前記第１の保証キーと前記第２の保証キーとを比較することは、前記第２の保証キー内の少なくとも１つの値が前記第１の保証キー内の対応する値に一致することを決定することをさらに含む、先行する請求項のいずれかに記載の方法。
【請求項５】
前記方法は、
前記ホストノードからプリブート実行環境クライアントの要求を受信することと、
前記ホストノードにプリブート実行環境クライアントを提供することとをさらに含み、前記ホストノードは、前記プリブート実行環境クライアントを使用してブートプロシージャを実行するように構成される、先行する請求項のいずれかに記載の方法。
【請求項６】
前記方法は、
前記ホストノードに前記ネットワークアドレスを提供することに応答して、ストレージモジュールにブートパーティションをマウントすることをさらに含み、前記ブートパーティションは、前記ホストノードおよび前記ネットワークアドレスを指定する、先行する請求項のいずれかに記載の方法。
【請求項７】

前記ネットワークアドレスの前記要求は、前記クラウドインフラストラクチャ環境を実装する１つまたは複数のコンピューティングデバイスを備えるデータセンタ環境に接続する前記ホストノードに応答して、前記ホストノードから取得される、先行する請求項のいずれかに記載の方法。

【請求項８】

クラウドインフラストラクチャノードであって、

プロセッサと、

命令を含む非一時的なコンピュータ可読媒体とを備え、前記命令は、前記プロセッサによって実行されると、前記プロセッサに、

ホストノードの認可のためにコンソールから認証データのセットを取得することを行わせ、前記認証データのセットは、第１の保証キー、および前記ホストノードの特徴を識別する認証ポリシを含み、

前記ホストノードから、前記クラウドインフラストラクチャ環境に接続するためにネットワークアドレスの要求を取得することと、

第２の保証キーの要求を前記ホストノードに伝送することと、

前記ホストノードから前記第２の保証キーを受信することと、

前記第２の保証キーを検証するために、前記認証データのセット内で受信した前記第１の保証キーと前記第２の保証キーとを比較することと、

ホストノード認証データの要求を前記ホストノードに伝送することと、

前記ホストノードから前記ホストノード認証データを受信することと、

前記受信したホストノード認証データを検証するために、前記受信したホストノード認証データと前記認証データのセット内で受信した前記認証ポリシとを比較することと、

前記第２の保証キーおよび前記受信したホストノード認証データを検証することに応答して、前記ホストノードに前記ネットワークアドレスを提供することと、をさらに行わせ、前記ホストノードは、前記ネットワークアドレスを使用して前記クラウドインフラストラクチャ環境に接続するように構成される、クラウドインフラストラクチャノード。

【請求項９】

前記第２の保証キーは、公開アテステーションアイデンティティキーである、請求項８に記載のクラウドインフラストラクチャノード。

【請求項１０】

前記第２の保証キーを検証するために、前記認証データのセット内で受信した前記第１の保証キーと前記第２の保証キーとを比較することは、前記第２の保証キー内の少なくとも１つの値が前記第１の保証キー内の対応する値に一致することを決定することをさらに含む、請求項８または請求項９に記載のクラウドインフラストラクチャノード。

【請求項１１】

前記非一時的なコンピュータ可読媒体は、前記プロセッサに、

前記ホストノードからプリブート実行環境クライアントの要求を受信することと、

前記ホストノードにプリブート実行環境クライアントを提供することをさらに行わせる命令を含み、前記ホストノードは、前記プリブート実行環境クライアントを使用してブートプロシージャを実行するように構成される、請求項８～請求項１０のいずれかに記載のクラウドインフラストラクチャノード。

【請求項１２】

前記受信した認証データを検証するために、前記認証データのセット内で受信した前記認証ポリシと前記受信したホストノード認証データとを比較することは、

前記認証ポリシ内に含まれる第１のプラットフォーム構成レジスタ値および前記受信したホストノード認証データ内に提供される第２のプラットフォーム構成レジスタ値を識別することをさらに含み、前記第２のプラットフォーム構成レジスタ値は、前記ブートプロシージャ後の前記ホストノードの状態を示す前記ホストノードのブートプロシージャ中のハッシュ化レジスタ値を含み、

前記第１のプラットフォーム構成レジスタ値が前記第２のプラットフォーム構成レジス

タ値に一致するかどうかを決定することをさらに含み、前記受信したホストノード認証データは、前記第１のプラットフォーム構成レジスタ値が前記第２のプラットフォーム構成レジスタ値に一致することを決定することに応答して検証される、請求項８～請求項１１のいずれかに記載のクラウドインフラストラクチャノード。

【請求項１３】

前記非一時的なコンピュータ可読媒体は、前記プロセッサに、

前記ホストノードに前記ネットワークアドレスを提供することに応答して、ストレージモジュールにブートパーティションをマウントすることをさらに行わせる命令を含み、前記ブートパーティションは、前記ホストノードおよび前記ネットワークアドレスを指定する、請求項８～請求項１２のいずれかに記載のクラウドインフラストラクチャノード。

【請求項１４】

前記ネットワークアドレスの前記要求は、前記クラウドインフラストラクチャ環境を実装する１つまたは複数のコンピューティングデバイスを備えるデータセンタ環境に接続する前記ホストノードに応答して、前記ホストノードから取得される、請求項８～請求項１３のいずれかに記載のクラウドインフラストラクチャノード。

【請求項１５】

プロセッサによって実行されると、前記プロセッサにプロセスを実行させる命令のシーケンスが格納されている非一時的なコンピュータ可読媒体であって、前記プロセスは、

前記ホストノードの認可のためにコンソールから認証データのセットを取得することを含み、前記認証データのセットは、第１の保証キー、および前記ホストノードの特徴を識別する認証ポリシを含み、

前記ホストノードから、クラウドインフラストラクチャ環境に接続するためにネットワークアドレスの要求を取得することと、

前記ホストノードからプリブート実行環境クライアントの要求を受信することと、

前記ホストノードにプリブート実行環境クライアントを提供することをさらに含み、前記ホストノードは、前記プリブート実行環境クライアントを使用してブートプロシージャを実行するように構成され、

前記ホストノードから第２の保証キーを受信することと、

前記第２の保証キーを検証するために、前記認証データのセット内で受信した前記第１の保証キーと前記第２の保証キーとを比較することと、

前記プリブート実行環境クライアントを使用して前記ブートプロシージャ中に導出される前記ホストノードからのホストノード認証データのセットを受信することと、

前記受信したホストノード認証データのセットを検証するために、前記認証データのセット内で受信した前記認証ポリシと前記受信したホストノード認証データのセットとを比較することと、

前記第２の保証キーおよび前記受信したホストノード認証データのセットを検証することに応答して、前記ホストノードに前記ネットワークアドレスを提供することとをさらに含み、前記ホストノードは、前記ネットワークアドレスを使用して前記クラウドインフラストラクチャ環境に接続するように構成される、非一時的なコンピュータ可読媒体。

【請求項１６】

前記第２の保証キーは、公開アテステーションアイデンティティキーである、請求項１５に記載の非一時的なコンピュータ可読媒体。

【請求項１７】

前記第２の保証キーを検証するために、前記認証データのセット内で受信した前記第１の保証キーと前記第２の保証キーとを比較することは、前記第２の保証キー内の少なくとも１つの値が前記第１の保証キー内の対応する値に一致することを決定することをさらに含む、請求項１５または請求項１６に記載の非一時的なコンピュータ可読媒体。

【請求項１８】

前記受信した認証データを検証するために、前記認証データのセット内で受信した前記認証ポリシと前記受信したホストノード認証データのセットとを比較することは、

前記認証ポリシ内に含まれる第１のプラットフォーム構成レジスタ値および前記受信したホストノード認証データのセット内に提供される第２のプラットフォーム構成レジスタ値を識別することをさらに含み、前記第２のプラットフォーム構成レジスタ値は、前記ブートプロシージャ後の前記ホストノードの状態を示す前記ホストノードの前記ブートプロシージャ中のハッシュ化レジスタ値を含み、

前記第１のプラットフォーム構成レジスタ値が前記第２のプラットフォーム構成レジスタ値に一致するかどうかを決定することをさらに含み、前記受信したホストノード認証データのセットは、前記第１のプラットフォーム構成レジスタ値が前記第２のプラットフォーム構成レジスタ値に一致することを決定することに応答して検証される、請求項１５～請求項１７のいずれかに記載の非一時的なコンピュータ可読媒体。

【請求項１９】

前記プロセスは、

前記ホストノードに前記ネットワークアドレスを提供することに応答して、ストレージモジュールにブートパーティションをマウントすることをさらに含み、前記ブートパーティションは、前記ホストノードおよび前記ネットワークアドレスを指定する、請求項１５～請求項１８のいずれかに記載の非一時的なコンピュータ可読媒体。

【請求項２０】

前記ネットワークアドレスの前記要求は、前記クラウドインフラストラクチャ環境を実装する１つまたは複数のコンピューティングデバイスを備えるデータセンタ環境に接続する前記ホストノードに応答して、前記ホストノードから取得される、請求項１５～請求項１９のいずれかに記載の非一時的なコンピュータ可読媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願への相互参照

本出願は、「Ｅｄｇｅ Ａｔｔｅｓｔａｔｉｏｎ ｆｏｒ Ａｕｔｈｏｒｉｚａｔｉｏｎ ｏｆ ａ Ｃｏｍｐｕｔｉｎｇ Ｎｏｄｅ ｉｎ ａ Ｃｌｏｕｄ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ Ｓｙｓｔｅｍ」という表題の２０２１年１１月１０日に出願された米国特許出願第１７／５２３，７８９号に対する優先権を主張するものであり、その開示は、あらゆる目的のためにその全体が参照により本明細書に組み込まれる。

【０００２】

分野

開示した技術は、クラウドコンピューティング認証に関する。より詳細には、開示した技術は、例えば、新規ホストノードへのネットワークアクセスを付与する前に、クラウドコンピューティング環境にとって新規であるホストノードの認証のためにクラウドコンピューティング環境のエッジコンポーネントを利用することに関する。

【背景技術】

【０００３】

背景

データセンタ環境において、新規コンポーネント（例えば、サーバ）は、新規ホストデバイスとして追加され得る。新規コンポーネントは、クラウド環境内のコンピューティングリソースを増加させるため、またはクラウド環境内のコンポーネント上で実行するアプリケーション／サービスに追加の機能性を提供するために、クラウドコンピューティング環境に追加され得る。新規コンポーネントは、クラウドコンピューティング環境を実装する複数のデバイスを接続するデータセンタ環境内の他のデバイスに物理的に接続され得る。例えば、コロケーションセンタは、クラウドコンピューティング環境を実装するコンポーネントを収容するデータセンタ環境を提供し得る。

【０００４】

しかしながら、多くの場合において、データセンタ環境（例えば、コロケーションセンタ）は、他のエンティティのためのコンピューティングデバイス／データセンタを収容し

得る。そのような場合、別のエンティティは、クラウドコンピューティング環境を実装するコンポーネントを収容するデータセンタ環境の近くのエリアへのアクセスを有し得る。例えば、別のエンティティは、悪意を持って認可なしにデータセンタ環境にデバイスを接続し得る。いかなる検証プロセスもなしに、接続されたデバイスは、クラウドコンピューティング環境内でプライベートに管理されるデータおよび／またはサービスへのアクセスを入手し得る。

【発明の概要】

【課題を解決するための手段】

【０００５】

概要

本実施形態は、クラウドインフラストラクチャ環境にアクセスするためのホストノードのエッジアテステーションに関する。第１の例示的な実施形態は、クラウドインフラストラクチャ環境にアクセスするためのホストノードのアテステーションのための方法を提供する。本方法は、ホストノードの認可のためにコンソールから認証データのセットを取得することを含み得る。認証データのセットは、第１の保証キー、およびホストノードの特徴を識別する認証ポリシを含み得る。認証ポリシは、第１のプラットフォーム構成レジスタ（ＰＣＲ）値を含み得る。

【０００６】

本方法はまた、ホストノードから、クラウドインフラストラクチャ環境に接続するためにネットワークアドレスの要求を取得することを含み得る。本方法はまた、ホストノードから第２の保証キーを受信することを含み得る。本方法はまた、第２の保証キーを検証するために、認証データのセット内で受信した第１の保証キーと第２の保証キーとを比較することを含み得る。

【０００７】

本方法はまた、ホストノードからホストノード認証データのセットを受信することを含み得る。ホストノード認証データのセットは、ホストノードのブートプロシージャ中のハッシュ化レジスタ値を含む第２のＰＣＲ値を含み得る。本方法はまた、第１のＰＣＲ値が第２のＰＣＲ値に一致するかどうかを決定することによって、受信したホストノード認証データを検証するために、認証データのセット内で受信した認証ポリシと受信したホストノード認証データとを比較することを含み得る。本方法はまた、第２の保証キーおよび受信したホストノード認証データを検証することに応答して、ホストノードにネットワークアドレスを提供することを含み得る。ホストノードは、ネットワークアドレスを使用してクラウドインフラストラクチャ環境に接続するように構成され得る。

【０００８】

第２の例示的な実施形態は、クラウドインフラストラクチャノードに関する。クラウドインフラストラクチャノードは、プロセッサおよび非一時的なコンピュータ可読媒体を含み得る。非一時的なコンピュータ可読媒体は、プロセッサによって実行されると、プロセッサに、ホストノードの認可のためにコンソールから認証データのセットを取得することを行わせる命令を含み得る。認証データのセットは、第１の保証キー、およびホストノードの特徴を識別する認証ポリシを含み得る。命令は、プロセッサに、ホストノードから、クラウドインフラストラクチャ環境に接続するためにネットワークアドレスの要求を取得することをさらに行わせ得る。

【０００９】

命令は、プロセッサに、第２の保証キーの要求をホストノードに伝送することをさらに行わせ得る。命令は、プロセッサに、ホストノードから第２の保証キーを受信することをさらに行わせ得る。命令は、プロセッサに、第２の保証キーを検証するために、認証データのセット内で受信した第１の保証キーと第２の保証キーとを比較することをさらに行わせ得る。命令は、プロセッサに、ホストノード認証データの要求をホストノードに伝送することをさらに行わせ得る。命令は、プロセッサに、ホストノードからホストノード認証データを受信することをさらに行わせ得る。

【００１０】
命令は、プロセッサに、受信したホストノード認証データを検証するために、認証データのセット内で受信した認証ポリシと受信したホストノード認証データとを比較することをさらに行わせ得る。命令は、プロセッサに、第２の保証キーおよび受信したホストノード認証データを検証することに応答して、ホストノードにネットワークアドレスを提供することをさらに行わせ得る。ホストノードは、ネットワークアドレスを使用してクラウドインフラストラクチャ環境に接続するように構成され得る。
【００１１】
第３の例示的な実施形態は、非一時的なコンピュータ可読媒体に関する。非一時的なコンピュータ可読媒体は、プロセッサによって実行されると、プロセッサにプロセスを実行させる、格納された命令のシーケンスを含み得る。本プロセスは、ホストノードの認可のためにコンソールから認証データのセットを取得することを含み得る。認証データのセットは、第１の保証キー、およびホストノードの特徴を識別する認証ポリシを含み得る。本プロセスはまた、ホストノードから、クラウドインフラストラクチャ環境に接続するためにネットワークアドレスの要求を取得することを含み得る。
【００１２】
本プロセスはまた、ホストノードからプリブート実行環境クライアントの要求を受信することを含み得る。本プロセスはまた、ホストノードにプリブート実行環境クライアントを提供することをさらに含み得、ホストノードは、プリブート実行環境クライアントを使用してブートプロシージャを実行するように構成される。
【００１３】
本プロセスはまた、ホストノードから第２の保証キーを受信することを含み得る。本プロセスはまた、第２の保証キーを検証するために、認証データのセット内で受信した第１の保証キーと第２の保証キーとを比較することを含み得る。本プロセスはまた、プリブート実行環境クライアントを使用してブートプロシージャ中に導出されるホストノードからのホストノード認証データのセットを受信することを含み得る。
【００１４】
本プロセスはまた、受信したホストノード認証データを検証するために、認証データのセット内で受信した認証ポリシと受信したホストノード認証データとを比較することをさらに含み得る。本プロセスはまた、第２の保証キーおよび受信したホストノード認証データを検証することに応答して、ホストノードにネットワークアドレスを提供することを含み得る。ホストノードは、ネットワークアドレスを使用してクラウドインフラストラクチャ環境に接続するように構成され得る。
【図面の簡単な説明】
【００１５】
【図１】少なくとも１つの実施形態による、例となるネットワーク環境のブロック図である。
【図２】少なくとも１つの実施形態による、例となるクラウドインフラストラクチャシステムのブロック図である。
【図３】少なくとも１つの実施形態による、例となるエッジアテステーションプロセスを例証するシグナリングプロセスである。
【図４】少なくとも１つの実施形態による、エッジアテステーションプロセスを実施するためのＳｍａｒｔＮＩＣによって実施される例となる方法を例証するブロック図である。
【図５】少なくとも１つの実施形態による、エッジアテステーションプロセスを使用して検証されるべきホストノードによって実施される例となる方法を例証するブロック図である。
【図６】少なくとも１つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための１つのパターンを例証するブロック図である。
【図７】少なくとも１つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための別のパターンを例証するブロック図である。

【図８】少なくとも１つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための別のパターンを例証するブロック図である。
【図９】少なくとも１つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための別のパターンを例証するブロック図である。
【図１０】少なくとも１つの実施形態による、例となるコンピュータシステムを例証するブロック図である。
【発明を実施するための形態】
【００１６】
詳細な説明
多くの場合において、複数のコンピューティングデバイス（例えば、サーバ）および複数のコンピューティングデバイス上で実行するアプリケーション／サービスは、クラウドコンピューティングインフラストラクチャを実装することができる。さらに、新規ホストノードが、クラウドインフラストラクチャのためのコンピューティングリソースまたは機能性を増加させるために複数のコンピューティングデバイスに追加され得る。そのような場合、新規ホストノードは、新規コンピューティングデバイスのアイデンティティおよびセキュリティ特徴を検証することによって管理され得る。そのような検証は、遠隔アテステーションによって実施され得、遠隔アテステーションは、各コンピューティングデバイスのアイデンティティおよび構成を検証するために暗号によって検証可能な情報を提供するコンピューティングデバイスを含み得る。遠隔アテステーションプロシージャは、例えば、ネットワーク内のデバイスのセキュリティを管理し、コンピューティングデバイスの状態を識別するために使用され得る。
【００１７】
クラウドインフラストラクチャ内で遠隔アテステーションを集中的に実装するために集中サービスを実装するのではなく、検証サービスは、ホストノード近くのクラウドインフラストラクチャ環境内のエッジノードによって実施され得る。アテステーション検証サービスは、クラウドインフラストラクチャ内のｂｕｍｐ－ｉｎ－ｔｈｅ－ｗｉｒｅノード（例えば、スマートネットワークインターフェースコントローラ（ＳｍａｒｔＮＩＣ））の一部として含まれ得る。ＳｍａｒｔＮＩＣにおいてアテステーション検証サービスを実装することは、クラウドインフラストラクチャの中央コンポーネントから処理タスクをオフロードし得、以て、クラウドインフラストラクチャのデータ処理効率を増加させる。さらに、アテステーション検証サービス内に不具合があった場合、アテステーション検証サービスがクラウドインフラストラクチャのエッジ上のＳｍａｒｔＮＩＣで実行されて、少数のデバイス／アプリケーションにだけ影響を及ぼし得る。
【００１８】
本実施形態は、ネットワーク環境内のホストノードの認証および認可のためのエッジアテステーションサービスに関連する。新規ホストノードがネットワークへのアクセスを許可される前に、認証プロセスが実施され得る。例えば、コンソールが、クラウドインフラストラクチャ内のエッジコンポーネント（例えば、ｓｍａｒｔＮＩＣ）とインタラクトして、新規ホストノードの検証のために認証データのセット（例えば、公開保証キー、テナンシ認証データ）を取得し得る。
【００１９】
いくつかの場合において、ＳｍａｒｔＮＩＣは、ＯＳがホストノードに先にインストールされていることを必要とせずに、ホストノードがブートプロシージャを実行するために、ホストノードにプリブート実行環境（例えば、ｉＰＸＥ）を提供し得る。例えば、ｉＰＸＥクライアントが、ホストノードに提供されて、ホストノード上で実行するｉＰＸＥクライアントとＳｍａｒｔＮＩＣ上で実行するｉＰＸＥ環境との通信を可能にし得る。
【００２０】
ＳｍａｒｔＮＩＣは、保証キーの要求をホストノードに伝送し得、それに応答して、ホストノードは、（例えば、生成された公開／プライベートキーペアに基づいて）保証キーを生成し得る。ＳｍａｒｔＮＩＣは、保証キーを取得し、それを認証データのセット内で

受信した公開保証キーと比較し、ホストノードから取得した保証キーが認証データのセット内で受信した公開保証キーと対応する（例えば、一致する）ことを検証し得る。受信した保証キーを検証することは、ホストノードのアイデンティティを検証し得る。

【００２１】

ＳｍａｒｔＮＩＣは、認証データの要求をホストノードに伝送し得る。認証データは、ファームウェア構成、デバイス構成、プラットフォーム構成レジスタ（ＰＣＲ）値など、ホストノードを認証するデータを含み得る。ホストノードは、認証データを生成し得、また生成した認証データをＳｍａｒｔＮＩＣに提供し得る。受信した認証データは、受信した認証データを検証するために（例えば、ホストノードによって生成されるＰＣＲ値を認証データのセット内で提供される対応するＰＣＲ値と一致させることによって）、認証データのセット内で受信した認証ポリシと比較され得る。

【００２２】

ＳｍａｒｔＮＩＣは、受信した保証キーおよびホストノードから受信される認証データを検証することに応答してネットワークアドレスをホストノードに提供し得る。ネットワークアドレス（例えば、インターネットプロトコル（ＩＰ）アドレス）をホストノードに提供することにより、ホストノードがクラウドインフラストラクチャ内のコンポーネント／アプリケーション／サービスにアクセスすることを可能にし得る。これは、クラウドインフラストラクチャへのアクセスを提供することにおける増大したセキュリティを可能にし得る。

【００２３】

Ａ．システム概要

図１は、例となるネットワーク環境１００のブロック図である。ネットワーク環境１００は、１つまたは複数のネットワーク（例えば、インターネット）を使用して環境内のデバイス同士のデータ通信を可能にし得る。図１に示されるように、ネットワーク環境１００は、コンソール１０２、クラウドインフラストラクチャ（ＣＩ）システム１０４（および対応するコンピューティングデバイス１０６ａ－ｃ）、およびホストノード１０８のいずれかを含み得る。

【００２４】

コンソール１０２は、ＣＩシステム１０４と通信することが可能なコンピューティングデバイス（例えば、ラップトップコンピュータ）を含み得る。例えば、コンソール１０２は、ホストノード１０８のためのインスタンス（例えば、認証データのセットを含む）を作成するための命令をＣＩシステム１０４に提供し得る。別の例として、コンソール１０２は、ＣＩシステム１０４からプリブート実行環境クライアント（例えば、ｉＰＸＥ）をフェッチするように、またはホストノード１０８とＳｍａｒｔＮＩＣ１１０との間のセッションを開始するように、ホストノード１０８に命令し得る。

【００２５】

本明細書に説明されるようなＣＩシステム１０４は、１つまたは複数のクラウドアプリケーションまたはサービスを実装する１つまたは複数の相互接続されたコンピューティングデバイスを含み得る。例えば、ＣＩシステム１０４は、データベースデータを格納し、そこへのアクセスを（例えば、データベースのクエリを介して）提供し得る。ＣＩシステム１０４に含まれるコンピューティングデバイス（例えば、１０６ａ－ｃ）は、１つまたは複数のデータセンタ環境（例えば、コロケーションセンタ）内に位置し得る。

【００２６】

図１に示されるように、コンピューティングデバイス１０６ｃは、ＳｍａｒｔＮＩＣ１１０を実装し得る。ＳｍａｒｔＮＩＣ１１０は、ＣＩシステム１０４内のエッジコンポーネント（例えば、コンピューティングデバイス１０６ｃ）上に位置し得る。例えば、ＳｍａｒｔＮＩＣ１１０は、ＣＩシステム１０４へのエッジアクセスポイントとして作用するデータセンタ内に配置されるサーバに常駐し得る。ＳｍａｒｔＮＩＣ１１０は、本明細書に説明されるような遠隔アテステーションサービスを実施し得る。

【００２７】

ホストノード１０８は、コンピューティングデバイス（例えば、サーバ）、またはＣＩシステム１０４に導入されている一連のコンピューティングデバイスを含み得る。例えば、ホストノードは、データセンタ環境（例えば、コロケーションセンタ）においてＣＩシステム１０４に接続され、ＣＩシステム１０４にアクセスすることを要求しているサーバを含み得る。ホストノード１０８は、様々な処理タスクを実施するように、または１つもしくは複数のアプリケーション／サービスを実装するように構成され得る。本明細書に説明されるように、ホストノード１０８は、ＣＩシステム１０４にアクセスするためのネットワークアドレスを要求し、ＳｍａｒｔＮＩＣ１１０がコンソール１０２およびホストノード１０８によってそれぞれ提供される保証キーおよび認証データを検証することに応答して、ネットワークアドレスを受信し得る。

【００２８】

図２は、例となるクラウドインフラストラクチャシステム１０４のブロック図である。上に説明されるように、ＣＩシステム１０４は、様々なアプリケーション／サービスを実装する１つまたは複数の相互接続されたコンピューティングデバイスを含み得る。ＣＩシステム１０４は、ＣＩシステム１０４のコア機能を実装する１つまたは複数の中央コンピューティングデバイス、およびＳｍａｒｔＮＩＣ１１０を維持するエッジデバイスを含み得る。ＳｍａｒｔＮＩＣ１１０は、本明細書に説明されるように認証データを取得して認証データを検証するために、ホストノード（例えば、１０８）とインタラクトし得る。

【００２９】

ＣＩシステム１０４は、プリブート実行環境２０４を含み得る。プリブート実行環境２０４は、クライアントをホストノードに提供するように構成される環境（例えば、ｉＰＸＥ）を含み得、ホストノード上のインストールされたオペレーティングシステム（ＯＳ）なしにホストノードがプリブート実行環境を実行することを可能にする。例えば、ホストノードは、ＳｍａｒｔＮＩＣからｉＰＸＥクライアントを取得し、ＣＩシステム１０４内で実行するプリブート実行環境２０４とインタラクトすることによってｉＰＸＥクライアントを実行し得る。

【００３０】

ＣＩシステム１０４は、ストレージモジュール２０６を含み得る。ストレージモジュール２０６は、ＣＩシステム１０４内のデバイスにわたって様々なデータタイプ（例えば、検証されたホストノードのためのマウントされたブートパーティション）を格納し得る。

【００３１】

ＣＩシステム１０４は、コンソール認証データ２０８を含み得る。コンソール認証データ２０８は、新規ホストノードのエッジアテステーションのためにコンソールから認証データのセット内で取得されるデータを含み得る。コンソール認証データ２０８は、第１の保証キー（ＥＫ）２１０ａおよびテナンシ認可ポリシ２１２を含み得る。いくつかの場合において、コンソール認証データ２０８は、ＣＩシステム１０４に導入される複数のホストノードのための取得した認証データを格納し得る。

【００３２】

第１のＥＫ２１０ａは、ホストノードを識別するコンソールによって提供されるキー（例えば、トラステッドプラットフォームモジュール（ＴＰＭ）ＲＳＡキー）を含み得る。テナンシ認可ポリシ２１２は、ファームウェアバージョン、構成設定、ＰＣＲ値など、ホストノードの特徴を含み得る。

【００３３】

ＣＩシステム１０４はまた、ホスト認証データ２１４を含み得る。ホスト認証データ２１４は、第２のＥＫ２１０ｂおよび認証データ（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｄａｔａ）（または「認証データ（ａｕｔｈ　ｄａｔａ）」）２１６など、ホストノードから取得される情報を含み得る。ホスト認証データ２１４内のデータは、本明細書に説明されるようにホストノードの識別および検証のためにコンソール認証データ２０８と比較され得る。

【００３４】

ＣＩシステム１０４は、認証データ取得モジュール２１８を含み得る。認証データ取得モジュール２１８は、本明細書に説明されるように、認証データ（例えば、コンソール認証データ２０８）を取得し、ホストノードからホスト認証データ（例えば、２１４）を受信し得る。いくつかの場合において、認証データ取得モジュール２１８は、ホストノードにプリブート実行環境クライアントを提供すること、および／またはホストノードからネットワークアドレスの要求を受信することに応答して、ホスト認証データ（例えば、２１４）を要求し得る。

【００３５】

ＣＩシステム１０４は、キー検証モジュール２２０を含み得る。キー検証モジュール２２０は、ホストノードからキーを取得し、そのキーを、コンソール１０２によって提供されるキーを使用して検証し得る。キーを検証することは、受信したキーがコンソールによって提供されるキーに一致する／対応する（例えば、いくつかの類似性を含む）かどうかを決定することを含み得る。

【００３６】

ＣＩシステム１０４は、認証データ検証モジュール２２２を含み得る。認証データ検証モジュール２２２は、認証データを取得／識別し、受信した認証データをコンソールから受信される認証ポリシと比較し得る。例えば、認証データは、ファームウェアバージョン、ホストノード構成、ＰＣＲ値（例えば、ブートプロシージャ中に識別／作動されるコンポーネントに応答して追加される値のハッシュ化シリーズ）などを指定し得る。この例では、認証データは、ホストノードに特有の値、ファームウェアバージョン、データタイプなどに一致するためにテナンシ認証ポリシと比較され得る。キーおよび認証データが検証されることに応答して、ホストノードは、検証され、（例えば、ホストノードにネットワークアドレスを提供することによって）クラウドインフラストラクチャへのアクセスを許可され得る。

【００３７】

Ｂ．エッジアテステーションプロシージャを実施するための例となる方法

図３は、例となるエッジアテステーションプロセスを例証するシグナリングプロセス３００である。図３に示されるように、コンソール３０２およびホストノード３０８は、ＳｍａｒｔＮＩＣ３０６（例えば、ＣＩシステム内のエッジコンピューティングデバイス上で実行される）とインタラクトし得る。

【００３８】

３１０において、コンソール３０２は、新規ホストインスタンスを作成する要求をＳｍａｒｔＮＩＣ３０６に送信し得る。新規ホストインスタンスを作成する要求は、新規ホストノードを識別し得、またホストノードの検証のために第１の保証キーおよびテナンシ認証ポリシを含み得る。

【００３９】

３１２において、コンソール３０２は、ホストノードインスタンスを開始する要求をホストノード３０８に送信し得る。ホストノード３０８によって受信される要求は、ＳｍａｒｔＮＩＣ３０６に接続してブートプロシージャを開始する命令を含み得る。

【００４０】

３１４において、ホストノード３０８は、プリブート実行環境（例えば、ｉＰＸＥクライアント）の要求をＳｍａｒｔＮＩＣ３０６に送信し得る。この要求は、ＳｍａｒｔＮＩＣ３０６からのｉＰＸＥクライアントの要求を含み得る。本明細書に説明されるように、ｉＰＸＥクライアントは、オペレーティングシステムがホストノード３０８にロードされることなしに、ブートプロシージャがホストノード３０８によって実行されることを可能にし得る。

【００４１】

３１６において、ＳｍａｒｔＮＩＣ３０６は、プリブート実行環境（例えば、ｉＰＸＥクライアント）をホストノードに提供し得る。３１８において、ホストノード３０８は、プリブート実行環境を実行し得る（例えば、ｉＰＸＥクライアントが、エッジデバイス上

で実行するＳｍａｒｔＮＩＣ３０６と関連付けられたｉＰＸＥインスタンスとインタラクトすることによって。プリブート実行環境を実行することは、ブートプロシージャを実行すること、サービス／アプリケーションおよびコンポーネントを開始すること、などを含むブートプロシージャを実行し得る。

【００４２】

いくつかの場合において、ブートプロシージャ中、ＰＣＲ値が計算され得る。ＰＣＲ値は、ホストノード３０８によって各々開始したコンポーネント／サービスを示す値のハッシュ化シリーズを含み得る。ＰＣＲ値は、ブートプロシージャ後のホストノード３０８の状態を示すものであり得る。

【００４３】

３２０において、ホストノード３０８は、ＳｍａｒｔＮＩＣ３０６からのネットワークアドレスを要求し得る。ネットワークアドレス（例えば、ＩＰアドレス）は、ＣＩシステムへの接続を可能にし得る。ＳｍａｒｔＮＩＣ３０６は、本明細書に説明されるようにホストノードを検証することに応答してネットワークアドレスを付与するだけであってもよい。

【００４４】

３２２において、ＳｍａｒｔＮＩＣ３０６は、ホストノード３０８からの公開保証キー（ＥＫ）を要求し得る。３２４において、ホストノード３０８は、公開／プライベートキーペアを生成し得る。３２６において、ホストノード３０８は、キーペアから公開保証キーを生成し得る。３２８において、ホストノード３０８は、公開保証キーをＳｍａｒｔＮＩＣ３０６に送信し得る。公開保証キーは、コンソールによって提供されるインスタンス（例えば、３１０において）を作成するために要求中に提供されるキーと比較され得る。

【００４５】

３３０において、ＳｍａｒｔＮＩＣ３０６は、ホストノード３０８からの認証データのセットを要求し得る。３３２において、ホストノード３０８は、認証データのセットの要求において指定されるように、要求された認証データのセット（例えば、ホストノード、ファームウェアバージョン、構成設定、ＰＣＲ値に関する詳細）を生成し得る。３３４において、ホストノード３０８は、認証データの検証のために認証データのセットをＳｍａｒｔＮＩＣ３０６に送信し得る。

【００４６】

３３６において、ＳｍａｒｔＮＩＣは、受信した公開保証キーおよび認証データのセットを検証し得る。これは、ホストノード３０８から受信されるデータを、インスタンスを作成する要求内で（例えば、３１０において）コンソール３０２から取得されるデータと比較することを含み得る。

【００４７】

受信したデータを検証することに応答して、３３８において、ＳｍａｒｔＮＩＣ３０６は、ネットワークアドレスをホストノード３０８に送信し得る。ネットワークアドレスは、ホストノード３０８とＣＩシステムとの間の接続およびデータ通信を可能にし得る。３４０において、ＳｍａｒｔＮＩＣ３０６は、ブロックストレージ３０４においてホストノードに特有のブートパーティションをマウントし得る。

【００４８】

図４は、エッジアテステーションプロセスを実施するためのＳｍａｒｔＮＩＣによって実施される例となる方法を例証するブロック図４００である。４０２において、ＳｍａｒｔＮＩＣは、ホストノードの認可のためにコンソールから認証データのセットを取得し得る。認証データのセットは、第１の保証キー、およびホストノードの特徴を識別する認証ポリシを含み得る。

【００４９】

４０４において、ＳｍａｒｔＮＩＣは、プリブート実行環境（例えば、ｉＰＸＥクライアント）を提供する。ＳｍａｒｔＮＩＣは、ホストノードからプリブート実行環境クライアントの要求を受信し得る。ＳｍａｒｔＮＩＣは、プリブート実行環境クライアントをホ

ストノードに提供し得る。ホストノードは、プリブート実行環境クライアントを使用してブートプロシージャを実行するように構成され得る。

【００５０】

４０６において、ＳｍａｒｔＮＩＣは、ホストノードから、クラウドインフラストラクチャ環境に接続するためにネットワークアドレスの要求を取得し得る。いくつかの場合において、ネットワークアドレスの要求は、クラウドインフラストラクチャ環境を実装する１つまたは複数のコンピューティングデバイスを備えるデータセンタ環境に接続するホストノードに応答して、ホストノードから取得される。

【００５１】

４０８において、ＳｍａｒｔＮＩＣは、第２の保証キーの要求をホストノードに伝送し得る。４１０において、ＳｍａｒｔＮＩＣは、ホストノードから第２の保証キーを受信し得る。第２の保証キーは、公開アテステーションアイデンティティキー（ＡＩＫ）を含み得る。

【００５２】

４１２において、ＳｍａｒｔＮＩＣは、第２の保証キーを検証するために、認証データのセット内で受信した第１の保証キーと第２の保証キーを比較し得る。これは、第２の保証キー内の少なくとも１つの値が第１の保証キー内の対応する値に一致することを決定することを含み得る。

【００５３】

４１４において、ＳｍａｒｔＮＩＣは、ホストノード認証データの要求をホストノードに伝送し得る。４１６において、ＳｍａｒｔＮＩＣは、ホストノードからホストノード認証データを受信し得る。

【００５４】

４１８において、ＳｍａｒｔＮＩＣは、受信したホストノード認証データを検証するために、認証データのセット内で受信した認証ポリシと受信したホストノード認証データを比較し得る。これは、認証ポリシに含まれる第１のプラットフォーム構成レジスタ（ＰＣＲ）値、および受信したホストノード認証データ（例えば、ブートプロシージャ中に生成される）内に提供される第２のＰＣＲ値を識別することを含み得る。第２のＰＣＲ値は、ブートプロシージャ後のホストノードの状態を示すホストノードのブートプロシージャ中のハッシュ化レジスタ値を含み得る。これはまた、第１のＰＣＲ値が第２のＰＣＲ値に一致するかどうかを決定することを含み得る。受信したホストノード認証データは、第１のＰＣＲ値が第２のＰＣＲ値に一致することを決定することに応答して検証され得る。

【００５５】

４２０において、ＳｍａｒｔＮＩＣは、ホストノードにネットワークアドレスを提供し得る。ホストノードは、ネットワークアドレスを使用してクラウドインフラストラクチャ環境に接続するように構成され得る。これは、第２の保証キーおよび受信したホストノード認証データを検証することに応答して実施され得る。

【００５６】

図５は、エッジアテステーションプロセスを使用して検証されるべきホストノードによって実施される例となる方法を例証するブロック図５００である。５０２において、ホストノードは、コンソールからインスタンスを開始する要求を受信し得る。インスタンスを開始する要求は、ＳｍａｒｔＮＩＣと通信せよという命令およびブートプロシージャを実施せよという命令を含み得る。

【００５７】

５０４において、ホストノードは、ＳｍａｒｔＮＩＣからのプリブート実行環境を要求し得る。５０６において、ホストノードは、ＳｍａｒｔＮＩＣからプリブート実行環境を受信し得る。５０８において、ホストノードは、プリブート実行環境を実行し得る。プリブート実行環境は、ＳｍａｒｔＮＩＣにおいてｉＰＸＥインスタンスとインタラクトすることによってホストノード上のオペレーティングシステムの使用なしにブートプロシージャを実施することが可能なｉＰＸＥクライアントを含み得る。

【００５８】
５１０において、ホストノードは、ＳｍａｒｔＮＩＣからのネットワークアドレス（例えば、ＩＰアドレス）の要求を伝送し得る。５１２において、ホストノードは、ＳｍａｒｔＮＩＣから公開保証キー（ＥＫ　ｐｕｂ）の要求を受信し得る。５１４において、ホストノードは、ＥＫ　ｐｕｂを生成し得る。ＥＫ　ｐｕｂは、ホストノードによって生成される公開／プライベートキーペアから生成され得る。５１６において、ホストノードは、生成したＥＫ　ｐｕｂをＳｍａｒｔＮＩＣに伝送し得る。ＳｍａｒｔＮＩＣは、受信したＥＫ　ｐｕｂをコンソールによって受信されるキーと比較することによって、受信したＥＫ　ｐｕｂ（例えば、または第２の保証キー）を検証し得る。
【００５９】
５１８において、ホストノードは、認証データ（例えば、ホストノード認証データ）の要求を受信し得る。５２０において、ホストノードは、認証データ（例えば、ブートプロシージャに基づいた第２のＰＣＲ値）を生成し得る。５２２において、ホストノードは、生成した認証データをＳｍａｒｔＮＩＣに伝送し得る。ＳｍａｒｔＮＩＣは、受信した認証データを認証ポリシと比較することによって、認証データを検証し得る。
【００６０】
５２４において、ホストノードは、ＳｍａｒｔＮＩＣからネットワークアドレスを受信し得る。ネットワークアドレスは、ネットワークアドレスを使用したクラウドインフラストラクチャへの接続／データ伝送を可能にし得る。ネットワークアドレスは、ＳｍａｒｔＮＩＣが認証データを検証することに応答して受信され得る。
【００６１】
Ｃ．ＩａａＳ概要
上に記されるように、Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ　ａｓ　ａ　Ｓｅｒｖｉｃｅ（ＩａａＳ）は、クラウドコンピューティングの１つの特定のタイプである。ＩａａＳは、公開ネットワーク（例えば、インターネット）を通じて仮想化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モデルにおいて、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、ストレージデバイス、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）をホストし得る。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様々なサービス（例えば、料金請求、モニタリング、ロギング、負荷バランシング、およびクラスタリングなど）を供給し得る。故に、これらのサービスがポリシ駆動であり得るため、ＩａａＳユーザは、アプリケーション可用性および性能を維持するために負荷バランシングを駆動するためにポリシを実装することができてもよい。
【００６２】
いくつかの場合において、ＩａａＳ顧客は、インターネットなどの広域ネットワーク（ＷＡＮ）を通じてリソースおよびサービスにアクセスし得、またクラウドプロバイダのサービスを使用して、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し得る。例えば、ユーザは、ＩａａＳプラットフォームにログインして、仮想マシン（ＶＭ）を作成し、オペレーティングシステム（ＯＳ）を各ＶＭ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にストレージバケットを作成し、さらには企業ソフトウェアをそのＶＭにインストールし得る。顧客は、次いで、プロバイダのサービスを使用して、ネットワークトラフィックのバランスを取ること、アプリケーション問題をトラブルシューティングすること、性能をモニタリングすること、障害復旧を管理することなどを含む、様々な機能を実施し得る。
【００６３】
大半の場合、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参加を必要とする。しかしながら、クラウドプロバイダは、ＩａａＳを提供（例えば、用意、賃借、販売）することに特化したサードパーティサービスである必要がない場合がある。エンティティはまた、プライベートクラウドをデプロイすることを選んでもよく、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。

【００６４】

いくつかの例において、ＩａａＳデプロイメントは、新規アプリケーション、またはアプリケーションの新規バージョンを、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置くプロセスである。それはまた、サーバを準備する（例えば、ライブラリ、デーモンなど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、ハイパーバイザ層（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）の下で、クラウドプロバイダによって管理される。故に、顧客は、ハンドリング（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（例えば、セルフサービス仮想マシン（例えば、オンデマンドでスピンアップされ得る）または同様のものに対して責任を負い得る。

【００６５】

いくつかの例において、ＩａａＳプロビジョニングは、使用のためにコンピュータまたは仮想ホストを取得すること、さらには、必要とされる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。大半の場合、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、最初に実施される必要があり得る。

【００６６】

いくつかの場合において、ＩａａＳプロビジョニングには２つの異なる課題が存在する。第１に、何かを実行する前にインフラストラクチャの初期セットをプロビジョニングするという最初の課題が存在する。第２に、すべて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進化させる（例えば、新規サービスを追加する、サービスを変更する、サービスを削除するなど）という課題が存在する。いくつかの場合において、これら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解決され得る。言い換えると、インフラストラクチャ（例えば、どのコンポーネントが必要とされるか、それらがどのようにインタラクトするか）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。故に、インフラストラクチャの全体的なトポロジ（例えば、どのリソースがどれに依存するか、およびそれらが各々どのように協働するか）は、宣言的に説明され得る。いくつかの場合において、一旦トポロジが規定されると、構成ファイル内に説明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。

【００６７】

いくつかの例において、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）（例えば、おそらくは、構成可能なおよび／または共有のコンピューティングリソースのオンデマンドプール）が存在し得る。いくつかの例において、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かを規定するよう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、ならびに１つまたは複数の仮想マシン（ＶＭ）も存在し得る。負荷バランサ、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。より多くのインフラストラクチャ要素が所望および／または追加されるほど、インフラストラクチャは、徐々に進化し得る。

【００６８】

いくつかの場合において、連続デプロイメント技術が、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採用され得る。追加的に、説明された技術は、これらの環境内でインフラストラクチャ管理を可能にし得る。いくつかの例において、サービスチームは、１つまたは複数の、しかしながら多くの場合、多くの、異なる生産環境に（例えば、様々な異なる地理的場所にわたって、時として世界全体に及んで）デプロイされることが所望されるコードを書くことができる。しかしながら、いくつかの例において、コードがデプロイされ得るインフラストラクチャがまずセットアップされる必要があり得る。いくつかの場合において、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、デプロイメントツールが、インフラストラクチャがプロビジョニングされた後にコードをデプロイするために利用され得る。

【００６９】

図６は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの例となるパターンを例証するブロック図６００である。サービスオペレータ６０２は、仮想クラウドネットワーク（ＶＣＮ）６０６およびセキュアホストサブネット６０８を含み得るセキュアホストテナンシ６０４に通信可能に結合され得る。いくつかの例において、サービスオペレータ６０２は、携帯型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、パーソナルデジタルアシスタント（ＰＤＡ））、また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）、Ｍｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ Ｍｏｂｉｌｅ（登録商標）などの実行ソフトウェア、ならびに／またはｉＯＳ、Ｗｉｎｄｏｗｓ Ｐｈｏｎｅ、Ａｎｄｒｏｉｄ、ＢｌａｃｋＢｅｒｒｙ８、Ｐａｌｍ ＯＳ、および同様のものなどの様々なモバイルオペレーティングシステムであり得る、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使用すること、さらにはインターネット、Ｅ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が有効にされていてもよい。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）、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り得る。クライアントコンピューティングデバイスは、限定することなく、例えば、Ｇｏｏｇｌｅ Ｃｈｒｏｍｅ ＯＳなど、様々なＧＮＵ／Ｌｉｎｕｘオペレーティングシステムを含む、様々な市販のＵＮＩＸ（登録商標）またはＵＮＩＸ様のオペレーティングシステムのいずれかを実行するワークステーションコンピュータであり得る。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、ＶＣＮ６０６および／またはインターネットにアクセスし得るネットワークを通じて通信することが可能な、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ムシステム（例えば、Ｋｉｎｅｃｔ（登録商標）ジェスチャ入力デバイスありまたはなしのＭｉｃｒｏｓｏｆｔ Ｘｂｏｘゲームコンソール）、および／またはパーソナルメッセージングデバイスなど、任意の他の電子デバイスであり得る。

【００７０】

ＶＣＮ６０６は、セキュアシェル（ＳＳＨ）ＶＣＮ６１２に含まれるＬＰＧ６１０を介してＳＳＨ ＶＣＮ６１２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）６１０を含み得る。ＳＳＨ ＶＣＮ６１２は、ＳＳＨサブネット６１４を含み得、ＳＳＨ ＶＣＮ６１２は、制御プレーンＶＣＮ６１６に含まれるＬＰＧ６１０を介して制御プレーンＶＣＮ６１６に通信可能に結合され得る。また、ＳＳＨ ＶＣＮ６１２は、ＬＰＧ６１０を介してデータプレーンＶＣＮ６１８に通信可能に結合され得る。制御プレーンＶＣＮ６１６およびデータプレーンＶＣＮ６１８は、ＩａａＳプロバイダによって所有および／または動作され得るサービステナンシ６１９に含まれ得る。

【００７１】

制御プレーンＶＣＮ６１６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）として作用する制御プレーン非武装化地帯（ＤＭＺ）階層６２０を含み得る。ＤＭＺベースのサーバは、制限された責任を有し、違反が阻止され続けるのを助け得る。追加的に、ＤＭＺ階層６２０は、１つもしくは複数の負荷バランサ（ＬＢ）サブネット６２２、アプリサブネット６２６を含み得る制御プレーンアプリ階層６２４、データベース（ＤＢ）サブネット６３０（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）を含み得る制御プレーンデータ階層６２８を含み得る。制御プレーンＤＭＺ階層６２０に含まれるＬＢサブネット

６２２は、制御プレーンアプリ階層６２４に含まれるアプリサブネット６２６および制御プレーンＶＣＮ６１６に含まれ得るインターネットゲートウェイ６３４に通信可能に結合され得、アプリサブネット６２６は、制御プレーンデータ階層６２８に含まれるＤＢサブネット６３０、およびサービスゲートウェイ６３６、およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ６３８に通信可能に結合され得る。制御プレーンＶＣＮ６１６は、サービスゲートウェイ６３６およびＮＡＴゲートウェイ６３８を含み得る。

【００７２】

制御プレーンＶＣＮ６１６は、アプリサブネット６２６を含み得るデータプレーンミラーアプリ階層６４０を含み得る。データプレーンミラーアプリ階層６４０に含まれるアプリサブネット６２６は、コンピュートインスタンス６４４を実行し得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を含み得る。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階層６４０のアプリサブネット６２６を、データプレーンアプリ階層６４６に含まれ得るアプリサブネット６２６に通信可能に結合し得る。

【００７３】

データプレーンＶＣＮ６１８は、データプレーンアプリ階層６４６、データプレーンＤＭＺ階層６４８、およびデータプレーンデータ階層６５０を含み得る。データプレーンＤＭＺ階層６４８は、データプレーンアプリ階層６４６のアプリサブネット６２６およびデータプレーンＶＣＮ６１８のインターネットゲートウェイ６３４に通信可能に結合され得るＬＢサブネット６２２を含み得る。アプリサブネット６２６は、データプレーンＶＣＮ６１８のサービスゲートウェイ６３６およびデータプレーンＶＣＮ６１８のＮＡＴゲートウェイ６３８に通信可能に結合され得る。データプレーンデータ階層６５０はまた、データプレーンアプリ階層６４６のアプリサブネット６２６に通信可能に結合され得るＤＢサブネット６３０を含み得る。

【００７４】

制御プレーンＶＣＮ６１６のインターネットゲートウェイ６３４、およびデータプレーンＶＣＮ６１８のインターネットゲートウェイ６３４は、公開インターネット６５４に通信可能に結合され得るメタデータ管理サービス６５２に通信可能に結合され得る。公開インターネット６５４は、制御プレーンＶＣＮ６１６のＮＡＴゲートウェイ６３８、およびデータプレーンＶＣＮ６１８のＮＡＴゲートウェイ６３８に通信可能に結合され得る。制御プレーンＶＣＮ６１６のサービスゲートウェイ６３６、およびデータプレーンＶＣＮ６１８のサービスゲートウェイ６３６は、クラウドサービス６５６に通信可能に結合され得る。

【００７５】

いくつかの例において、制御プレーンＶＣＮ６１６のサービスゲートウェイ６３６、またはデータプレーンＶＣＮ６１８のサービスゲートウェイ６３６は、公開インターネット６５４を通さずにクラウドサービス６５６に対するアプリケーションプログラミングインターフェース（ＡＰＩ）呼び出しを行い得る。サービスゲートウェイ６３６からのクラウドサービス６５６に対するＡＰＩ呼び出しは、一方向であり得、サービスゲートウェイ６３６は、クラウドサービス６５６に対するＡＰＩ呼び出しを行うことができ、クラウドサービス６５６は、要求されたデータをサービスゲートウェイ６３６に送信し得る。しかしながら、クラウドサービス６５６は、サービスゲートウェイ６３６に対するＡＰＩ呼び出しを開始しなくてもよい。

【００７６】

いくつかの例において、セキュアホストテナンシ６０４は、サービステナンシ６１９に直接接続され得、サービステナンシ６１９はさもなければ隔離され得る。セキュアホストサブネット６０８は、さもなければ隔離されたシステムを通じて双方向通信を可能にし得るＬＰＧ６１０を通じてＳＳＨサブネット６１４と通信し得る。セキュアホストサブネット６０８をＳＳＨサブネット６１４に接続することは、セキュアホストサブネット６０８にサービステナンシ６１９内の他のエンティティへのアクセスを付与し得る。

【００７７】
制御プレーンＶＣＮ６１６は、サービステナンシ６１９のユーザが所望のリソースをセットアップすること、または別途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ＶＣＮ６１６内でプロビジョニングされる所望のリソースは、データプレーンＶＣＮ６１８内でデプロイされ得るか、または別途使用され得る。いくつかの例において、制御プレーンＶＣＮ６１６は、データプレーンＶＣＮ６１８から隔離され得、制御プレーンＶＣＮ６１６のデータプレーンミラーアプリ階層６４０は、データプレーンミラーアプリ階層６４０およびデータプレーンアプリ階層６４６に含まれ得るＶＮＩＣ６４２を介して、データプレーンＶＣＮ６１８のデータプレーンアプリ階層６４６と通信し得る。

【００７８】
いくつかの例において、システムのユーザ、または顧客は、メタデータ管理サービス６５２に要求を通信することができる公開インターネット６５４を通じて、要求を出すこと、例えば、動作を作成すること、読み出すこと、更新すること、または削除すること（ＣＲＵＤ）ができる。メタデータ管理サービス６５２は、インターネットゲートウェイ６３４を通じて制御プレーンＶＣＮ６１６に要求を通信することができる。要求は、制御プレーンＤＭＺ階層６２０に含まれるＬＢサブネット６２２によって受信され得る。ＬＢサブネット６２２は、要求が有効であることを決定し得、この決定に応答して、ＬＢサブネット６２２は、制御プレーンアプリ階層６２４に含まれるアプリサブネット６２６に要求を伝送し得る。要求が検証され、公開インターネット６５４に対する呼び出しを必要とする場合、公開インターネット６５４に対する呼び出しは、ＮＡＴゲートウェイ６３８に伝送され得、ＮＡＴゲートウェイ６３８が、公開インターネット６５４に対する呼び出しを行い得る。要求によって格納されることが所望され得るメモリは、ＤＢサブネット６３０に格納され得る。

【００７９】
いくつかの例において、データプレーンミラーアプリ階層６４０は、制御プレーンＶＣＮ６１６とデータプレーンＶＣＮ６１８との間の直接通信を促進し得る。例えば、構成に対する変更、更新、または他の好適な修正が、データプレーンＶＣＮ６１８に含まれるリソースに適用されることが所望され得る。ＶＮＩＣ６４２を介して、制御プレーンＶＣＮ６１６は、データプレーンＶＣＮ６１８に含まれるリソースと直接通信することができ、以て、それに対する構成への変更、更新、または他の好適な修正を実行し得る。

【００８０】
いくつかの実施形態において、制御プレーンＶＣＮ６１６およびデータプレーンＶＣＮ６１８は、サービステナンシ６１９に含まれ得る。この場合、システムのユーザまたは顧客は、制御プレーンＶＣＮ６１６またはデータプレーンＶＣＮ６１８のいずれかを所有または動作しなくてもよい。代わりに、ＩａａＳプロバイダが、制御プレーンＶＣＮ６１６およびデータプレーンＶＣＮ６１８を所有または動作し得、それらの両方は、サービステナンシ６１９内に含まれ得る。この実施形態は、ユーザまたは顧客が他のユーザ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ぎ得るネットワークの隔離を可能にし得る。また、この実施形態は、システムのユーザまたは顧客が、格納のため、所望のレベルの脅威防止を有さない場合のある公開インターネット６５４に依拠する必要なしに、データベースをプライベートに格納することを可能にし得る。

【００８１】
他の実施形態において、制御プレーンＶＣＮ６１６に含まれるＬＢサブネット６２２は、サービスゲートウェイ６３６から信号を受信するように構成され得る。この実施形態において、制御プレーンＶＣＮ６１６およびデータプレーンＶＣＮ６１８は、公開インターネット６５４を呼び出すことなしに、ＩａａＳプロバイダの顧客によって呼び出されるように構成され得る。ＩａａＳプロバイダの顧客は、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、公開インターネット６５４から隔離され得るサービステナンシ６１９に格納され得ることから、この実施形態を所望し得る。

【００８２】

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例となるパターンを例証するブロック図７００である。サービスオペレータ７０２（例えば、図６のサービスオペレータ６０２）は、仮想クラウドネットワーク（ＶＣＮ）７０６（例えば、図６のＶＣＮ６０６）およびセキュアホストサブネット７０８（例えば、図６のセキュアホストサブネット６０８）を含み得るセキュアホストテナンシ７０４（例えば、図６のセキュアホストテナンシ６０４）に通信可能に結合され得る。ＶＣＮ７０６は、セキュアシェル（ＳＳＨ）ＶＣＮ７１２に含まれるＬＰＧ６１０を介してＳＳＨ　ＶＣＮ７１２（例えば、図６のＳＳＨ　ＶＣＮ６１２）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）７１０（例えば、図６のＬＰＧ６１０）を含み得る。ＳＳＨ　ＶＣＮ７１２は、ＳＳＨサブネット７１４（例えば、図６のＳＳＨサブネット６１４）を含み得、ＳＳＨ　ＶＣＮ７１２は、制御プレーンＶＣＮ７１６に含まれるＬＰＧ７１０を介して制御プレーンＶＣＮ７１６（例えば、図６の制御プレーンＶＣＮ６１６）に通信可能に結合され得る。制御プレーンＶＣＮ７１６は、サービステナンシ７１９（例えば、図６のサービステナンシ６１９）に含まれ得、データプレーンＶＣＮ７１８（例えば、図６のデータプレーンＶＣＮ６１８）は、システムのユーザまたは顧客によって所有または動作され得る顧客テナンシ７２１に含まれ得る。

【００８３】

制御プレーンＶＣＮ７１６は、ＬＢサブネット７２２（例えば、図６のＬＢサブネット６２２）を含み得る制御プレーンＤＭＺ階層７２０（例えば、図６の制御プレーンＤＭＺ階層６２０）、アプリサブネット７２６（例えば、図６のアプリサブネット６２６）を含み得る制御プレーンアプリ階層７２４（例えば、図６の制御プレーンアプリ階層６２４）、データベース（ＤＢ）サブネット７３０（例えば、図６のＤＢサブネット６３０と同様）を含み得る制御プレーンデータ階層７２８（例えば、図６の制御プレーンデータ階層６２８）を含み得る。制御プレーンＤＭＺ階層７２０に含まれるＬＢサブネット７２２は、制御プレーンアプリ階層７２４に含まれるアプリサブネット７２６、および制御プレーンＶＣＮ７１６に含まれ得るインターネットゲートウェイ７３４（例えば、図６のインターネットゲートウェイ６３４）に通信可能に結合され得、アプリサブネット７２６は、制御プレーンデータ階層７２８に含まれるＤＢサブネット７３０、およびサービスゲートウェイ７３６（例えば、図６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６のＮＡＴゲートウェイ６３８）に通信可能に結合され得る。制御プレーンＶＣＮ７１６は、サービスゲートウェイ７３６およびＮＡＴゲートウェイ７３８を含み得る。

【００８４】

制御プレーンＶＣＮ７１６は、アプリサブネット７２６を含み得るデータプレーンミラーアプリ階層７４０（例えば、図６のデータプレーンミラーアプリ階層６４０）を含み得る。データプレーンミラーアプリ階層７４０に含まれるアプリサブネット７２６は、コンピュートインスタンス７４４（例えば、図６のコンピュートインスタンス６４４と同様）を実行し得る仮想ネットワークインターフェースコントローラ（ＶＮＩＣ）７４２（例えば、６４２のＶＮＩＣ）を含み得る。コンピュートインスタンス７４４は、データプレーンミラーアプリ階層７４０に含まれるＶＮＩＣ７４２およびデータプレーンアプリ階層７４６に含まれるＶＮＩＣ７４２を介して、データプレーンミラーアプリ階層７４０のアプリサブネット７２６と、データプレーンアプリ階層７４６（例えば、図６のデータプレーンアプリ階層６４６）に含まれ得るアプリサブネット７２６との間の通信を促進し得る。

【００８５】

制御プレーンＶＣＮ７１６に含まれるインターネットゲートウェイ７３４は、公開インターネット７５４（例えば、図６の公開インターネット６５４）に通信可能に結合され得るメタデータ管理サービス７５２（例えば、図６のメタデータ管理サービス６５２）に通信可能に結合され得る。公開インターネット７５４は、制御プレーンＶＣＮ７１６に含まれるＮＡＴゲートウェイ７３８に通信可能に結合され得る。制御プレーンＶＣＮ７１６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（例えば、図６のクラ

ウドサービス６５６）に通信可能に結合され得る。

【００８６】

いくつかの例において、データプレーンＶＣＮ７１８は、顧客テナンシ７２１に含まれ得る。この場合、ＩａａＳプロバイダは、顧客ごとに制御プレーンＶＣＮ７１６を提供し得、ＩａａＳプロバイダは、顧客ごとに、サービステナンシ７１９に含まれる固有のコンピュートインスタンス７４４をセットアップし得る。各コンピュートインスタンス７４４は、サービステナンシ７１９に含まれる制御プレーンＶＣＮ７１６と顧客テナンシ７２１に含まれるデータプレーンＶＣＮ７１８との間の通信を可能にし得る。コンピュートインスタンス７４４は、サービステナンシ７１９に含まれる制御プレーンＶＣＮ７１６内でプロビジョニングされるリソースが、顧客テナンシ７２１に含まれるデータプレーンＶＣＮ７１８内でデプロイされるか、または別途使用されることを可能にし得る。

【００８７】

他の例において、ＩａａＳプロバイダの顧客は、顧客テナンシ７２１内に存在するデータベースを有し得る。この例では、制御プレーンＶＣＮ７１６は、アプリサブネット７２６を含み得るデータプレーンミラーアプリ階層７４０を含み得る。データプレーンミラーアプリ階層７４０は、データプレーンＶＣＮ７１８に常駐し得るが、データプレーンミラーアプリ階層７４０は、データプレーンＶＣＮ７１８内に存在しなくてもよい。すなわち、データプレーンミラーアプリ階層７４０は、顧客テナンシ７２１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階層７４０は、データプレーンＶＣＮ７１８内に存在しなくてもよく、またはＩａａＳプロバイダの顧客によって所有もしくは動作されなくてもよい。データプレーンミラーアプリ階層７４０は、データプレーンＶＣＮ７１８に対する呼び出しを行うように構成され得るが、制御プレーンＶＣＮ７１６に含まれる任意のエンティティに対する呼び出しを行うように構成されなくてもよい。顧客は、制御プレーンＶＣＮ７１６内でプロビジョニングされるデータプレーンＶＣＮ７１８内のリソースをデプロイすること、または別途使用することを所望し得、データプレーンミラーアプリ階層７４０は、顧客の、所望のデプロイメントまたはリソースの他の使用を促進し得る。

【００８８】

いくつかの実施形態において、ＩａａＳプロバイダの顧客は、データプレーンＶＣＮ７１８にフィルタを適用し得る。この実施形態において、顧客は、どのデータプレーンＶＣＮ７１８がアクセスすることができるかを決定し得、顧客は、データプレーンＶＣＮ７１８からの公開インターネット７５４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こと、またはデータプレーンＶＣＮ７１８のアクセスを任意の外側のネットワークもしくはデータベースへと別途制御することができなくてもよい。顧客テナンシ７２１に含まれるデータプレーンＶＣＮ７１８に対して顧客によりフィルタおよび制御を適用することは、データプレーンＶＣＮ７１８を他の顧客から、および公開インターネット７５４から隔離するのを助け得る。

【００８９】

いくつかの実施形態において、クラウドサービス７５６は、公開インターネット７５４上、制御プレーンＶＣＮ７１６上、またはデータプレーンＶＣＮ７１８上に存在しない場合のあるサービスにアクセスするためにサービスゲートウェイ７３６によって呼び出され得る。クラウドサービス７５６と制御プレーンＶＣＮ７１６またはデータプレーンＶＣＮ７１８との間の接続は、ライブまたは連続的でなくてもよい。クラウドサービス７５６は、ＩａａＳプロバイダによって所有または動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７５６は、サービスゲートウェイ７３６からの呼び出しを受信するように構成され得、また公開インターネット７５４からの呼び出し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７５６は、他のクラウドサービス７５６から隔離され得、制御プレーンＶＣＮ７１６は、制御プレーンＶＣＮ７１６と同じ領域内にない場合のあるクラウドサービス７５６から隔離され得る。例えば、制御プレーンＶＣＮ７１６は、「領域１」に位置し得、クラウドサービス「デプロイメント６」は、領域１および「領域２」に位置し得る。デプロイメント６に対する呼び出しが、領域１に位置する制御プレー

ンＶＣＮ７１６に含まれるサービスゲートウェイ７３６によって行われる場合、呼び出しは、領域１内のデプロイメント６へ伝送され得る。この例では、制御プレーンＶＣＮ７１６、または領域１内のデプロイメント６は、領域２内のデプロイメント６に通信可能に結合されなくてもよく、またはこれと別途通信状態になくてもよい。

【００９０】

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例となるパターンを例証するブロック図８００である。サービスオペレータ８０２（例えば、図６のサービスオペレータ６０２）は、仮想クラウドネットワーク（ＶＣＮ）８０６（例えば、図６のＶＣＮ６０６）およびセキュアホストサブネット８０８（例えば、図６のセキュアホストサブネット６０８）を含み得るセキュアホストテナンシ８０４（例えば、図６のセキュアホストテナンシ６０４）に通信可能に結合され得る。ＶＣＮ８０６は、ＳＳＨ　ＶＣＮ８１２に含まれるＬＰＧ８１０を介してＳＳＨ　ＶＣＮ８１２（例えば、図６のＳＳＨ　ＶＣＮ６１２）に通信可能に結合され得るＬＰＧ８１０（例えば、図６のＬＰＧ６１０）を含み得る。ＳＳＨ　ＶＣＮ８１２は、ＳＳＨサブネット８１４（例えば、図６のＳＳＨサブネット６１４）を含み得、ＳＳＨ　ＶＣＮ８１２は、制御プレーンＶＣＮ８１６に含まれるＬＰＧ８１０を介して制御プレーンＶＣＮ８１６（例えば、図６の制御プレーンＶＣＮ６１６）に、およびデータプレーンＶＣＮ８１８に含まれるＬＰＧ８１０を介してデータプレーンＶＣＮ８１８（例えば、図６のデータプレーン６１８）に通信可能に結合され得る。制御プレーン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６のサービステナンシ６１９）に含まれ得る。

【００９１】

制御プレーンＶＣＮ８１６は、負荷バランサ（ＬＢ）サブネット８２２（例えば、図６のＬＢサブネット６２２）を含み得る制御プレーンＤＭＺ階層８２０（例えば、図６の制御プレーンＤＭＺ階層６２０）、アプリサブネット８２６（例えば、図６のアプリサブネット６２６と同様）を含み得る制御プレーンアプリ階層８２４（例えば、図６の制御プレーンアプリ階層６２４）、ＤＢサブネット８３０を含み得る制御プレーンデータ階層８２８（例えば、図６の制御プレーンデータ階層６２８）を含み得る。制御プレーンＤＭＺ階層８２０に含まれるＬＢサブネット８２２は、制御プレーンアプリ階層８２４に含まれるアプリサブネット８２６に、および制御プレーンＶＣＮ８１６に含まれ得るインターネットゲートウェイ８３４（例えば、図６のインターネットゲートウェイ６３４）に通信可能に結合され得、アプリサブネット８２６は、制御プレーンデータ階層８２８に含まれるＤＢサブネット８３０に、ならびにサービスゲートウェイ８３６（例えば、図６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６のＮＡＴゲートウェイ６３８）に通信可能に結合され得る。制御プレーンＶＣＮ８１６は、サービスゲートウェイ８３６およびＮＡＴゲートウェイ８３８を含み得る。

【００９２】

データプレーンＶＣＮ８１８は、データプレーンアプリ階層８４６（例えば、図６のデータプレーンアプリ階層６４６）、データプレーンＤＭＺ階層８４８（例えば、図６のデータプレーンＤＭＺ階層６４８）、およびデータプレーンデータ階層８５０（例えば、図６のデータプレーンデータ階層６５０）を含み得る。データプレーンＤＭＺ階層８４８は、データプレーンアプリ階層８４６の信頼できるアプリサブネット８６０および信頼できないサブネット８６２、ならびにデータプレーンＶＣＮ８１８に含まれるインターネットゲートウェイ８３４に通信可能に結合され得るＬＢサブネット８２２を含み得る。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階層８５０に含まれるＤＢサブネット８３０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階層８５０に含まれるＤＢサブネット８３０に通信可能に結合され得る。データプレーンデータ階層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に通信可能に結合され得る

ＤＢサブネット８３０を含み得る。
【００９３】
信頼できないアプリサブネット８６２は、テナント仮想マシン（ＶＭ）８６６（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ＶＮＩＣ８６４（１）－（Ｎ）を含み得る。各テナントＶＭ８６６（１）－（Ｎ）は、それぞれの顧客テナンシ８７０（１）－（Ｎ）に含まれ得るそれぞれのコンテナイグレスＶＣＮ８６８（１）－（Ｎ）に含まれ得るそれぞれのアプリサブネット８６７（１）－（Ｎ）に通信可能に結合され得る。それぞれのセカンダリＶＮＩＣ８７２（１）－（Ｎ）は、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とコンテナイグレスＶＣＮ８６８（１）－（Ｎ）に含まれるアプリサブネットとの間の通信を促進し得る。各コンテナイグレスＶＣＮ８６８（１）－（Ｎ）は、公開インターネット８５４（例えば、図６の公開インターネット６５４）に通信可能に結合され得るＮＡＴゲートウェイ８３８を含み得る。
【００９４】
制御プレーン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、公開インターネット８５４に通信可能に結合され得るメタデータ管理サービス８５２（例えば、図６のメタデータ管理システム６５２）に通信可能に結合され得る。公開インターネット８５４は、制御プレーン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に通信可能に結合され得る。制御プレーン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に通信可能に結合され得る。
【００９５】
いくつかの実施形態において、データプレーンＶＣＮ８１８は、顧客テナンシ８７０と統合され得る。この統合は、コードを実行するときにサポートを所望し得る場合など、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ものであり得る。顧客は、破壊的であり得る実行すべきコードを提供し得、他の顧客リソースと通信し得、または望ましくない影響を別途引き起こし得る。これに応答して、ＩａａＳプロバイダは、顧客によってＩａａＳプロバイダに与えられるコードを実行するべきかどうかを決定し得る。
【００９６】
いくつかの例において、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プロバイダに付与し、データプレーン階層アプリ８４６に付随する関数を要求し得る。関数を実行するためのコードは、ＶＭ８６６（１）－（Ｎ）内で実行され得、コードは、データプレーンＶＣＮ８１８の他の場所で実行するようには構成されなくてもよい。各ＶＭ８６６（１）－（Ｎ）は、１つの顧客テナンシ８７０に接続され得る。ＶＭ８６６（１）－（Ｎ）に含まれるそれぞれのコンテナ８７１（１）－（Ｎ）は、コードを実行するように構成され得る。この場合、二重隔離（例えば、コードを実行するコンテナ８７１（１）－（Ｎ）、この場合、コンテナ８７１（１）－（Ｎ）は、信頼できないアプリサブネット８６２に含まれる少なくともＶＭ８６６（１）－（Ｎ）に含まれ得る）が存在し得、これは、正しくない、または別途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傷を及ぼすこと、または異なる顧客のネットワークに損傷を及ぼすことを防ぐのを助け得る。コンテナ８７１（１）－（Ｎ）は、顧客テナンシ８７０に通信可能に結合され得、データを顧客テナンシ８７０から伝送または受信するように構成され得る。コンテナ８７１（１）－（Ｎ）は、データプレーンＶＣＮ８１８内の任意の他のエンティティからデータを伝送または受信するように構成されなくてもよい。コードを実行することを完了すると、ＩａａＳプロバイダは、コンテナ８７１（１）－（Ｎ）を抹消または別途処分し得る。
【００９７】
いくつかの実施形態において、信頼できるアプリサブネット８６０は、ＩａａＳプロバ

イダによって所有または動作され得るコードを実行し得る。この実施形態において、信頼できるアプリサブネット８６０は、ＤＢサブネット８３０に通信可能に結合され得、ＤＢサブネット８３０内でＣＲＵＤ動作を実行するように構成され得る。信頼できないアプリサブネット８６２は、ＤＢサブネット８３０に通信可能に結合され得るが、この実施形態において、信頼できないアプリサブネットは、ＤＢサブネット８３０内で読み出し動作を実行するように構成され得る。各顧客のＶＭ８６６（１）－（Ｎ）に含まれ得、顧客からのコードを実行し得るコンテナ８７１（１）－（Ｎ）は、ＤＢサブネット８３０と通信可能に結合されなくてもよい。

【００９８】

他の実施形態において、制御プレーンＶＣＮ８１６およびデータプレーンＶＣＮ８１８は、直接的に通信可能に結合されなくてもよい。この実施形態において、制御プレーンＶＣＮ８１６とデータプレーンＶＣＮ８１８との間に直接通信は存在しなくてもよい。しかしながら、通信は、少なくとも１つの方法を通じて間接的に発生し得る。ＬＰＧ８１０は、制御プレーンＶＣＮ８１６とデータプレーンＶＣＮ８１８との間の通信を促進し得るＩａａＳプロバイダによって確立され得る。別の例において、制御プレーンＶＣＮ８１６またはデータプレーンＶＣＮ８１８は、サービスゲートウェイ８３６を介してクラウドサービス８５６に対する呼び出しを行い得る。例えば、制御プレーンＶＣＮ８１６からのクラウドサービス８５６に対する呼び出しは、データプレーンＶＣＮ８１８と通信し得るサービスの要求を含み得る。

【００９９】

図９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例となるパターンを例証するブロック図９００である。サービスオペレータ９０２（例えば、図６のサービスオペレータ６０２）は、仮想クラウドネットワーク（ＶＣＮ）９０６（例えば、図６のＶＣＮ６０６）およびセキュアホストサブネット９０８（例えば、図６のセキュアホストサブネット６０８）を含み得るセキュアホストテナンシ９０４（例えば、図６のセキュアホストテナンシ６０４）に通信可能に結合され得る。ＶＣＮ９０６は、ＳＳＨ　ＶＣＮ９１２に含まれるＬＰＧ９１０を介してＳＳＨ　ＶＣＮ９１２（例えば、図６のＳＳＨ　ＶＣＮ６１２）に通信可能に結合され得るＬＰＧ９１０（例えば、図６のＬＰＧ６１０）を含み得る。ＳＳＨ　ＶＣＮ９１２は、ＳＳＨサブネット９１４（例えば、図６のＳＳＨサブネット６１４）を含み得、ＳＳＨ　ＶＣＮ９１２は、制御プレーンＶＣＮ９１６に含まれるＬＰＧ９１０を介して制御プレーンＶＣＮ９１６（例えば、図６の制御プレーンＶＣＮ６１６）に、およびデータプレーンＶＣＮ９１８に含まれるＬＰＧ９１０を介してデータプレーンＶＣＮ９１８（例えば、図６のデータプレーン６１８）に通信可能に結合され得る。制御プレーンＶＣＮ９１６およびデータプレーンＶＣＮ９１８は、サービステナンシ９１９（例えば、図６のサービステナンシ６１９）に含まれ得る。

【０１００】

制御プレーンＶＣＮ９１６は、ＬＢサブネット９２２（例えば、図６のＬＢサブネット６２２）を含み得る制御プレーンＤＭＺ階層９２０（例えば、図６の制御プレーンＤＭＺ階層６２０）、アプリサブネット９２６（例えば、図６のアプリサブネット６２６）を含み得る制御プレーンアプリ階層９２４（例えば、図６の制御プレーンアプリ階層６２４）、ＤＢサブネット９３０（例えば、図８のＤＢサブネット８３０）を含み得る制御プレーンデータ階層９２８（例えば、図６の制御プレーンデータ階層６２８）を含み得る。制御プレーンＤＭＺ階層９２０に含まれるＬＢサブネット９２２は、制御プレーンアプリ階層９２４に含まれるアプリサブネット９２６に、および制御プレーンＶＣＮ９１６に含まれ得るインターネットゲートウェイ９３４（例えば、図６のインターネットゲートウェイ６３４）に通信可能に結合され得、アプリサブネット９２６は、制御プレーンデータ階層９２８に含まれるＤＢサブネット９３０に、ならびにサービスゲートウェイ９３６（例えば、図６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９３８（例えば、図６のＮＡＴゲートウェイ６３８）に通信可能に結合され得る。制御プレーンＶＣＮ９１６は、サービスゲートウェイ９３６およびＮＡＴゲートウェイ９３

８を含み得る。
【０１０１】
データプレーンＶＣＮ９１８は、データプレーンアプリ階層９４６（例えば、図６のデータプレーンアプリ階層６４６）、データプレーンＤＭＺ階層９４８（例えば、図６のデータプレーンＤＭＺ階層６４８）、およびデータプレーンデータ階層９５０（例えば、図６のデータプレーンデータ階層６５０）を含み得る。データプレーンＤＭＺ階層９４８は、データプレーンアプリ階層９４６の信頼できるアプリサブネット９６０（例えば、図８の信頼できるアプリサブネット８６０）および信頼できないアプリサブネット９６２（例えば、図８の信頼できないアプリサブネット８６２）、ならびににデータプレーンＶＣＮ９１８に含まれるインターネットゲートウェイ９３４に通信可能に結合され得るＬＢサブネット９２２を含み得る。信頼できるアプリサブネット９６０は、データプレーンＶＣＮ９１８に含まれるサービスゲートウェイ９３６、データプレーンＶＣＮ９１８に含まれるＮＡＴゲートウェイ９３８、およびデータプレーンデータ階層９５０に含まれるＤＢサブネット９３０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９６２は、データプレーンＶＣＮ９１８に含まれるサービスゲートウェイ９３６およびデータプレーンデータ階層９５０に含まれるＤＢサブネット９３０に通信可能に結合され得る。データプレーンデータ階層９５０は、データプレーンＶＣＮ９１８に含まれるサービスゲートウェイ９３６に通信可能に結合され得るＤＢサブネット９３０を含み得る。
【０１０２】
信頼できないアプリサブネット９６２は、信頼できないアプリサブネット９６２に常駐するテナント仮想マシン（ＶＭ）９６６（１）－（Ｎ）に通信可能に結合され得るプライマリＶＮＩＣ９６４（１）－（Ｎ）を含み得る。各テナントＶＭ９６６（１）－（Ｎ）は、それぞれのコンテナ９６７（１）－（Ｎ）内でコードを実行し得、コンテナイグレスＶＣＮ９６８に含まれ得るデータプレーンアプリ階層９４６に含まれ得るアプリサブネット９２６に通信可能に結合され得る。それぞれのセカンダリＶＮＩＣ９７２（１）－（Ｎ）は、データプレーンＶＣＮ９１８に含まれる信頼できないアプリサブネット９６２とコンテナイグレスＶＣＮ９６８に含まれるアプリサブネットとの間の通信を促進し得る。コンテナイグレスＶＣＮは、公開インターネット９５４（例えば、図６の公開インターネット６５４）に通信可能に結合され得るＮＡＴゲートウェイ９３８を含み得る。
【０１０３】
制御プレーンＶＣＮ９１６に含まれるインターネットゲートウェイ９３４、およびデータプレーンＶＣＮ９１８に含まれるインターネットゲートウェイ８３４は、公開インターネット９５４に通信可能に結合され得るメタデータ管理サービス９５２（例えば、図６のメタデータ管理システム６５２）に通信可能に結合され得る。公開インターネット９５４は、制御プレーンＶＣＮ９１６に含まれるＮＡＴゲートウェイ９３８、およびデータプレーンＶＣＮ９１８に含まれるＮＡＴゲートウェイ９３８に通信可能に結合され得る。制御プレーンＶＣＮ９１６に含まれるサービスゲートウェイ９３６、およびデータプレーンＶＣＮ９１８に含まれるサービスゲートウェイ９３６は、クラウドサービス９５６に通信可能に結合され得る。
【０１０４】
いくつかの例において、図９のブロック図９００のアーキテクチャによって例証されるパターンは、図８のブロック図８００のアーキテクチャによって例証されるパターンの例外と見なされ得、ＩａａＳプロバイダが顧客と直接的に通信することができない場合（例えば、切断された領域）、ＩａａＳプロバイダの顧客にとって望ましい場合がある。各顧客のためのＶＭ９６６（１）－（Ｎ）に含まれるそれぞれのコンテナ９６７（１）－（Ｎ）は、顧客によりリアルタイムでアクセスされ得る。コンテナ９６７（１）－（Ｎ）は、コンテナイグレスＶＣＮ９６８に含まれ得るデータプレーンアプリ階層９４６のアプリサブネット９２６に含まれるそれぞれのセカンダリＶＮＩＣ９７２（１）－（Ｎ）に対する呼び出しを行うように構成され得る。セカンダリＶＮＩＣ９７２（１）－（Ｎ）は、公開インターネット９５４に対する呼び出しを伝送し得るＮＡＴゲートウェイ９３８に対する

呼び出しを伝送し得る。この例では、顧客によりリアルタイムでアクセスされ得るコンテナ９６７（１）－（Ｎ）は、制御プレーンＶＣＮ９１６から隔離され得、データプレーンＶＣＮ９１８に含まれる他のエンティティから隔離され得る。コンテナ９６７（１）－（Ｎ）はまた、他の顧客からのリソースから隔離され得る。

【０１０５】

他の例では、顧客は、クラウドサービス９５６を呼び出すためにコンテナ９６７（１）－（Ｎ）を使用し得る。この例では、顧客は、クラウドサービス９５６からサービスを要求するコンテナ９６７（１）－（Ｎ）内でコードを実行し得る。コンテナ９６７（１）－（Ｎ）は、この要求をセカンダリＶＮＩＣ９７２（１）－（Ｎ）に伝送し得、このセカンダリＶＮＩＣ９７２（１）－（Ｎ）がＮＡＴゲートウェイに要求を伝送し得、このＮＡＴゲートウェイが公開インターネット９５４に要求を伝送し得る。公開インターネット９５４は、インターネットゲートウェイ９３４を介して制御プレーンＶＣＮ９１６に含まれるＬＢサブネット９２２に要求を伝送し得る。要求が有効であることを決定することに応答して、ＬＢサブネットは、アプリサブネット９２６に要求を伝送し得、このアプリサブネット９２６が、サービスゲートウェイ９３６を介してクラウドサービス９５６に要求を伝送し得る。

【０１０６】

図に描写されるＩａａＳアーキテクチャ６００、７００、８００、９００は、描写されるもの以外のコンポーネントを有し得るということを理解されたい。さらに、図に示される実施形態は、本開示の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いくつかの例にすぎない。いくつかの他の実施形態において、ＩａａＳシステムは、図に示されるよりも多くのもしくは少ないコンポーネントを有し得、２つ以上のコンポーネントを組み合わせ得、または異なる構成もしくは配置のコンポーネントを有し得る。

【０１０７】

特定の実施形態において、本明細書に説明されるＩａａＳシステムは、セルフサービス、購読ベース、弾力的に拡張可能な、信頼性のある、高可用性の、およびセキュアな様式で顧客に配信される一連のアプリケーション、ミドルウェア、およびデータベースサービスを含み得る。そのようなＩａａＳシステムの例は、特許譲受人によって提供されるオラクルクラウドインフラストラクチャ（ＯＣＩ）である。

【０１０８】

図１０は、様々な実施形態が実装され得る例となるコンピュータシステム１０００を例証する。システム１０００は、上に説明されるコンピュータシステムのいずれかを実装するために使用され得る。図に示されるように、コンピュータシステム１０００は、バスサブシステム１００２を介していくつかの周辺サブシステムと通信する処理装置１００４を含む。これらの周辺サブシステムは、処理加速装置１００６、Ｉ／Ｏサブシステム１００８、ストレージサブシステム１０１８、および通信サブシステム１０２４を含み得る。ストレージサブシステム１０１８は、有形コンピュータ可読記憶媒体１０２２およびシステムメモリ１０１０を含む。

【０１０９】

バスサブシステム１００２は、コンピュータシステム１０００の様々なコンポーネントおよびサブシステムに意図したように互いと通信させるための機構を提供する。バスサブシステム１００２は、単一のバスとして概略的に示されるが、バスサブシステムの代替の実施形態は、複数のバスを利用し得る。バスサブシステム１００２は、様々なバスアーキテクチャのいずれかを使用する、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体のいずれかであり得る。例えば、そのようなアーキテクチャは、ＩＥＥＥ　Ｐ１３８６．１規格に合わせて製造されるＭｅｚｚａｎｉｎｅバスとして実装され得る、業界標準アーキテクチャ（ＩＳＡ）バス、マイクロチャネルアーキテクチャ（ＭＣＡ）バス、拡張ＩＳＡ（ＥＩＳＡ）バス、ＶｉｄｅｏＥｌｅｃｔｒｏｎｉｃｓ　Ｓｔａｎｄａｒｄｓ　Ａｓｓｏｃｉａｔｉｏｎ（ＶＥＳＡ）ローカルバス、および周辺コンポーネント相互接続（ＰＣＩ）バスを含み得る。

【０１１０】
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）として実装され得る処理装置１００４は、コンピュータシステム１０００の動作を制御する。１つまたは複数のプロセッサは、処理装置１００４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。特定の実施形態において、処理装置１００４は、各処理装置に含まれるシングルまたはマルチコアプロセッサを伴う１つまたは複数の独立した処理装置１０３２および／または１０３４として実装され得る。他の実施形態において、処理装置１００４はまた、２つのデュアルコアプロセッサをシングルチップへと統合することによって形成されるクアッドコア処理装置として実装され得る。

【０１１１】
様々な実施形態において、処理装置１００４は、プログラムコードに応答して様々なプログラムを実行し得、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し得る。任意の所与の時間において、実行されるべきプログラムコードのいくつかまたはすべては、プロセッサ１００４および／またはストレージサブシステム１０１８に常駐し得る。好適なプログラミングを通じて、プロセッサ１００４は、上に説明される様々な機能性を提供し得る。コンピュータシステム１０００は、追加的に、デジタル信号プロセッサ（ＤＳＰ）、特殊目的プロセッサ、および／または同様のものを含み得る処理加速装置１００６を含み得る。

【０１１２】
Ｉ／Ｏサブシステム１００８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、ディスプレイに組み込まれるタッチパッドまたはタッチスクリーン、スクロールホイール、クリックホイール、ダイアル、ボタン、スイッチ、キーパッド、音声コマンド認識システムを有する音声入力デバイス、マイク、および他のタイプ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使用した自然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、これとインタラクトすることを可能にする、Ｍｉｃｒｏｓｏｆｔ　Ｋｉｎｅｃｔ（登録商標）動作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、ユーザから目の活動（例えば、写真を撮っているおよび／またはメニュー選択を行っている間の「瞬き」）を検出し、アイジェスチャを入力デバイス（例えば、ＧｏｏｇｌｅＧｌａｓｓ（登録商標））への入力として変換するＧｏｏｇｌｅ　Ｇｌａｓｓ（登録商標）瞬き検出器などのアイジェスチャ認識デバイスを含み得る。追加的に、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）とインタラクトすることを可能にする音声認識検知デバイスを含み得る。

【０１１３】
ユーザインターフェース入力デバイスはまた、限定なしに、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イヤ、ウェブカム、画像スキャナ、指紋スキャナ、バーコードリーダ３Ｄスキャナ、３Ｄプリンタ、レーザ距離計、および視線追跡デバイスなどの音声／視覚デバイスを含み得る。追加的に、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、磁気共鳴撮像、位置エミッション断層撮影、医用超音波診断デバイスなどの医用画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音声入力デバイスを含み得る。

【０１１４】
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、インジケータ光

、または音声出力デバイスなどの非視覚ディスプレイを含み得る。ディスプレイサブシステムは、ブラウン管（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ものなどのフラットパネルデバイス、投射デバイス、タッチスクリーン、および同様のものであり得る。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１０００からの情報をユーザまたは他のコンピュータに出力するためのすべての可能なタイプのデバイスおよび機構を含むことが意図される。例えば、ユーザインターフェース出力デバイスは、限定なしに、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、テキスト、図形、および音声／ビデオ情報を視覚的に伝達する様々なディスプレイデバイスを含み得る。

【０１１５】

コンピュータシステム１０００は、現在システムメモリ１０１０内に位置するものとして示される、ソフトウェア要素を備えるストレージサブシステム１０１８を備え得る。システムメモリ１０１０は、処理装置１００４上でロード可能および実行可能であるプログラム命令、ならびにこれらのプログラムの実行中に生成されるデータを格納し得る。

【０１１６】

コンピュータシステム１０００の構成およびタイプに応じて、システムメモリ１０１０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）であり得る。ＲＡＭは、典型的には、処理装置１００４に直ちにアクセス可能であり、ならびに／または処理装置１００４によって現在動作および実行されているデータおよび／またはプログラムモジュールを含む。いくつかの実装形態において、システムメモリ１０１０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み得る。いくつかの実装形態において、スタートアップ中など、コンピュータシステム１０００内の要素間で情報を転送するのを助ける基本ルーチンを含む基本入力／出力システム（ＢＩＯＳ）は、典型的には、ＲＯＭに格納され得る。例として、および限定ではなく、システムメモリ１０１０はまた、クライアントアプリケーション、ウェブブラウザ、中間階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）などを含み得るアプリケーションプログラム１０１２、プログラムデータ１０１４、およびオペレーティングシステム１０１６を例証する。例として、オペレーティングシステム１０１６は、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の様々なバージョン、様々な市販のＵＮＩＸ（登録商標）またはＵＮＩＸ様のオペレーティングシステム（限定なしに、様々な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／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み得る。

【０１１７】

ストレージサブシステム１０１８はまた、いくつかの実施形態の機能性を提供する基本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コンピュータ可読記憶媒体を提供し得る。プロセッサによって実行されると、上に説明される機能性を提供するソフトウェア（プログラム、コードモジュール、命令）は、ストレージサブシステム１０１８に格納され得る。これらのソフトウェアモジュールまたは命令は、処理装置１００４によって実行され得る。ストレージサブシステム１０１８はまた、本開示に従って使用されるデータを格納するためのレポジトリを提供し得る。

【０１１８】

ストレージサブシステム１０００はまた、コンピュータ可読記憶媒体１０２２にさらに接続され得るコンピュータ可読記憶媒体リーダ１０２０を含み得る。一緒に、および任意

選択的に、システムメモリ１０１０と組み合わせて、コンピュータ可読記憶媒体１０２２は、遠隔、ローカル、固定、および／または除去可能ストレージデバイスに加えて、一時的に、および／またはより恒久的に、コンピュータ可読情報を含む、格納する、伝送する、および取得するための記憶媒体を包括的に表し得る。

【０１１９】

コードまたはコードの部分を含むコンピュータ可読記憶媒体１０２２はまた、限定されるものではないが、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、除去可能および除去不可能な媒体など、記憶媒体および通信媒体を含む、当該技術分野において知られている、または使用される任意の適切な媒体を含み得る。これは、ＲＡＭ、ＲＯＭ、電気的に消去可能なプログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）、もしくは他の光学ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または他の有形コンピュータ可読媒体など、有形コンピュータ可読記憶媒体を含み得る。これはまた、所望の情報を伝送するために使用され得、コンピューティングシステム１０００によってアクセスされ得る、データ信号、データ伝送、または任意の他の媒体など、非有形コンピュータ可読媒体を含み得る。

【０１２０】

例として、コンピュータ可読記憶媒体１０２２は、除去不可能な不揮発性磁気媒体から読み出す、またはこれに書き込むハードディスクドライブ、除去可能な不揮発性磁気ディスクから読み出す、またはこ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、または他の光学媒体など、除去可能な不揮発性の光学ディスクから読み出す、またはこれに書き込む光学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１０２２は、Ｚｉｐ（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス（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、および同様のものを含み得るが、これらに限定されない。コンピュータ可読記憶媒体１０２２はまた、不揮発性メモリに基づいたソリッドステートドライブ（ＳＳＤ）、例えば、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、揮発性メモリに基づいたＳＳＤ、例えば、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、ならびにＤＲＡＭおよびフラッシュメモリベースのＳＳＤの組合せを使用するハイブリッド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、プログラムモジュール、およびコンピュータシステム１０００のための他のデータの不揮発性ストレージを提供し得る。

【０１２１】

通信サブシステム１０２４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１０２４は、他のシステムからデータを受信し、またコンピュータシステム１０００から他のシステムにデータを伝送するためのインターフェースとしての役割を果たす。例えば、通信サブシステム１０２４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ことを可能にし得る。いくつかの実施形態において、通信サブシステム１０２４は、（例えば、携帯電話技術、３Ｇ、４Ｇ、またはＥＤＧＥ（Ｅｎｈａｎｃｅｄ　Ｄａｔａ　ｒａｔｅｓ　ｆｏｒ　Ｇｌｏｂａｌ　Ｅｖｏｌｕｔｉｏｎ）などの高度なデータネットワーク技術、ＷｉＦｉ（ＩＥＥＥ８０２．１１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合せを使用して）ワイヤレス音声および／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）送受信機コンポーネント、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み得る。いくつかの実施形態において、通信サブシステム１０２４は、ワイヤレス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（例えば、イーサネット（登録商標）

）を提供し得る。
【０１２２】
いくつかの実施形態において、通信サブシステム１０２４は、コンピュータシステム１０００を使用し得る１つ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１０２６、イベントストリーム１０２８、イベント更新１０３０、ならびに同様のものの形態で入力通信を受信し得る。
【０１２３】
例として、通信サブシステム１０２４は、Ｔｗｉｔｔｅｒ（登録商標）フィード、Ｆａｃｅｂｏｏｋ（登録商標）更新、Ｒｉｃｈ　Ｓｉｔｅ　Ｓｕｍｍａｒｙ（ＲＳＳ）フィードなどのウェブフィード、ならびに／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リアルタイムでデータフィード１０２６を受信するように構成され得る。
【０１２４】
追加的に、通信サブシステム１０２４はまた、明白な終わりなしに事実上連続的または無限であり得る、リアルタイムイベントのイベントストリーム１０２８、および／またはイベント更新１０３０を含み得る、連続的なデータストリームの形態でデータを受信するように構成され得る。連続的な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、ネットワーク性能測定ツール（例えば、ネットワークモニタリング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モニタリング、および同様のものを挙げることができる。
【０１２５】
通信サブシステム１０２４はまた、構造化および／または非構造化データフィード１０２６、イベントストリーム１０２８、イベント更新１０３０、ならびに同様のものを、コンピュータシステム１０００に結合される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状態にあり得る１つまたは複数のデータベースに出力するように構成され得る。
【０１２６】
コンピュータシステム１０００は、ハンドヘルド携帯デバイス（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、または任意の他のデータ処理システムを含む様々なタイプのうちの１つであり得る。
【０１２７】
コンピュータおよびネットワークの絶え間なく変化する性質に起因して、図に描写されるコンピュータシステム１０００の説明は、特定の例として意図されるにすぎない。図に描写されるシステムよりも多くのまたは少ないコンポーネントを有する多くの他の構成が可能である。例えば、カスタマイズされたハードウェアもまた使用され得、および／または、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）、もしくは組合せにおいて実装され得る。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手段および／または方法を理解するものとする。
【０１２８】
特定の実施形態が説明されているが、様々な修正、変更、代替構造、および等価物もまた、本開示の範囲内に包含される。実施形態は、ある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する。追加的に、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使用して説明されているが、本開示の範囲は、説明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とって明らかであるものとする。上述した実施形態の様々な特徴および態様は、個別にまたは共同で

使用され得る。

【０１２９】

さらに、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合せを使用して説明されているが、ハードウェアおよびソフトウェアの他の組合せも本開示の範囲内であることを理解されたい。実施形態は、ハードウェアのみ、ソフトウェアのみ、またはそれらの組合せを使用して、実施され得る。本明細書に説明される様々なプロセスは、同じプロセッサ上で、または任意の組合せで異なるプロセッサ上で実施され得る。したがって、コンポーネントまたはモジュールが、ある動作を実施するように構成されるものとして説明される場合、そのような構成は、例えば、その動作を実施するように電子回路を設計することによって、その動作を実施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）をプログラミングすることによって、またはそれらの任意の組合せによって達成され得る。プロセスは、プロセス間通信のための従来の技術を含むがこれに限定されない様々な技術を使用して通信することができ、異なる対のプロセスは、異なる技術を使用し得、または同じ対のプロセスは、異なる時間に異なる技術を使用し得る。

【０１３０】

したがって、明細書および図面は、限定的な意味ではなく例証的な意味で捉えられるべきである。しかしながら、追加、減算、削除、ならびに他の修正および変更が、クレームに明記されるような広範な趣旨および範囲から逸脱することなく、行われ得ることは明白である。故に、特定の開示実施形態が説明されているが、これらは限定することは意図されない。様々な修正および等価物は、以下のクレームの範囲内である。

【０１３１】

開示した実施形態を説明する文脈における（特に、以下のクレームの文脈における）用語「１つの（ａ）」および「１つの（ａｎ）」および「その（ｔｈｅ）」ならびに同様の指示対象の使用は、本明細書に別途示されるか、文脈上明白に矛盾しない限り、単数形および複数形の両方を網羅するように解釈されるものとする。用語「含む（ｃｏｍｐｒｉｓｉｎｇ）」、「有する（ｈａｖｉｎｇ）」、「含む（ｉｎｃｌｕｄｉｎｇ）」、および「含有する（ｃｏｎｔａｉｎｉｎｇ）」は、別途記載のない限り、無制限の用語（すなわち、「含むがこれに限定されない」を意味する）と解釈されるものとする。用語「接続される」は、介在するものが存在するとしても、部分的または全体的に、中に含まれる、取り付けられる、または一緒に接合されると解釈されるものとする。本明細書内の値の範囲の列挙は、本明細書に別途示されない限り、その範囲内に入る各々別個の値を個別に言及する手短な方法としての役割を果たすことが意図されるにすぎず、各々別個の値は、それが本明細書に個々に列挙されるかのように、本明細書に組み込まれる。本明細書に説明されるすべての方法は、本明細書に別途示されない限り、または別途明白に文脈上矛盾のない限り、任意の好適な順序で実施され得る。任意およびすべての例の使用、または本明細書に提供される例示的な言語（例えば、「など」）は、実施形態をより明瞭にすることが意図されるにすぎず、別途特許請求されない限り、本開示の範囲を制限するものではない。本明細書内の言語は、本開示の実践に不可欠な任意の非特許請求要素を示すものと解釈されるべきではない。

【０１３２】

「Ｘ、Ｙ、またはＺのうちの少なくとも１つ」という表現などの離接語は、別途具体的に記載のない限り、ある項目、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合せ（例えば、Ｘ、Ｙ、および／またはＺ）であり得ることを提示するために一般的に使用されるものとして文脈内で理解されることが意図される。故に、そのような離接語は、ある実施形態が、Ｘの少なくとも１つ、Ｙの少なくとも１つ、またはＺ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示唆することは概して意図せず、またこれを示唆するべきではない。

【０１３３】

本開示を実行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が本明細書に説明される。それらの好ましい実施形態の変異形は、先述の説明を読む際に当

業者に明らかになり得る。当業者は、適宜、そのような変異形を採用することができるものとし、本開示は、本明細書に具体的に説明されるものとは別途に実践され得る。したがって、本開示は、適用法によって許可される場合、本明細書に添付されるクレームに列挙される主題のすべての修正形態および等価物を含む。さらには、そのすべての可能な変異形における上述の要素の任意の組合せは、本明細書に別途示されない限り、本開示によって包含される。

【０１３４】

本明細書に引用される刊行物、特許出願、および特許を含むすべての参考文献は、各参考文献が、参照により組み込まれるように個々および具体的に示され、その全体が本明細書に明記された場合と同じ程度に、本明細書に参照により組み込まれる。

【０１３５】

先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るが、当業者は、本開示がそれに限定されないことを認識するものとする。上述した開示の様々な特徴および態様は、個別にまたは共同で使用され得る。さらに、実施形態は、本明細書の広範な趣旨および範囲から逸脱することなく、本明細書に説明されるものを超える任意の数の環境およびアプリケーションにおいて利用され得る。したがって、明細書および図面は、限定的ではなく例証的であると捉えられるべきである。

【０１３６】

追加的に、実施形態は、プロセッサによって実行されると、プロセッサに、本明細書内の本開示に説明される方法／技術のいずれかを実施させるコンピュータプログラム／命令を含むコンピュータプログラム製品を使用することによって実施され得る。

【図面】

【図１】

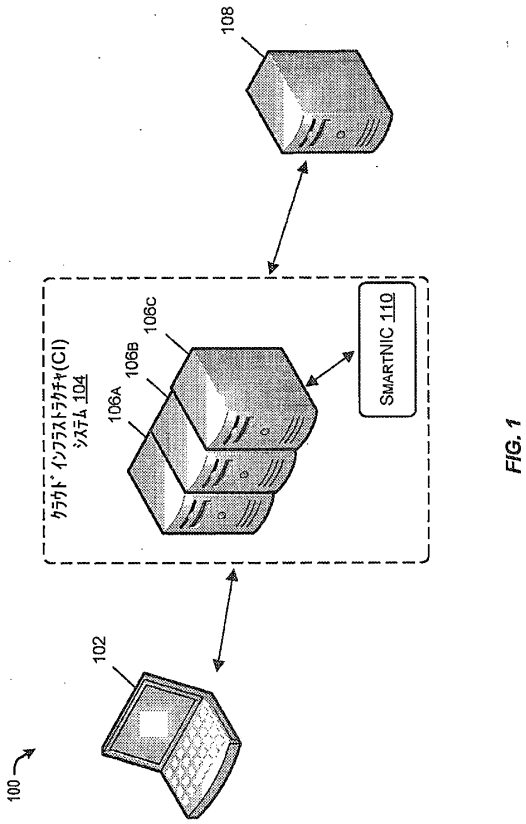


FIG. 1

【図２】

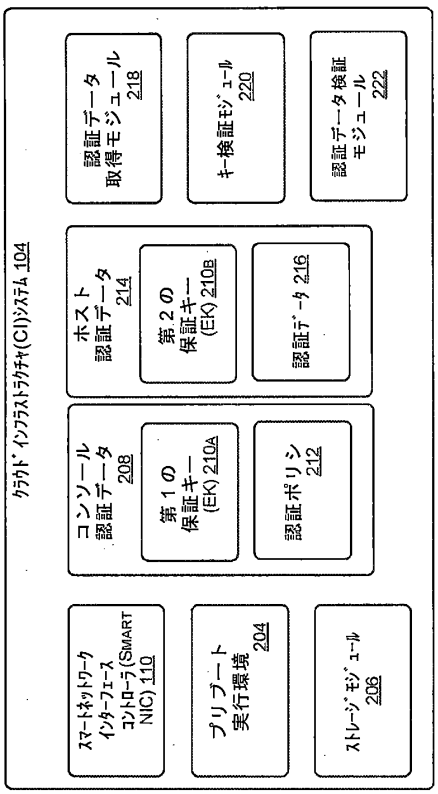


FIG. 2

【図３】

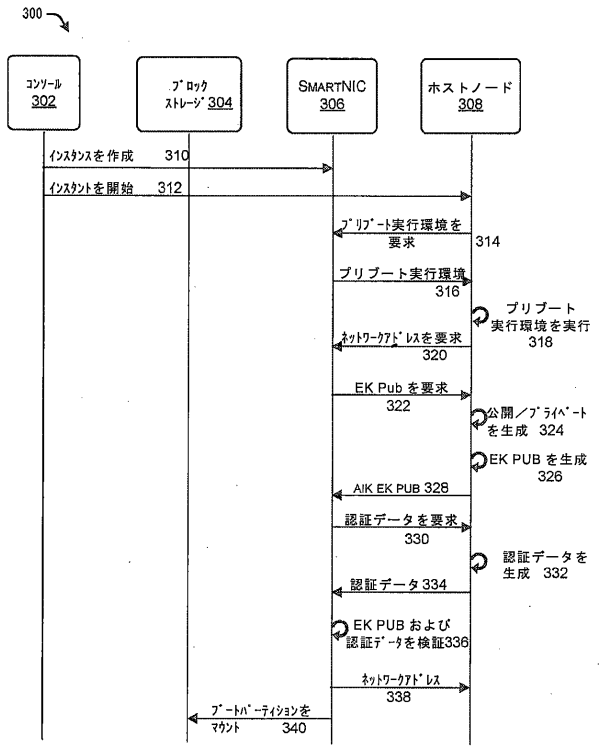


FIG. 3

【図４】

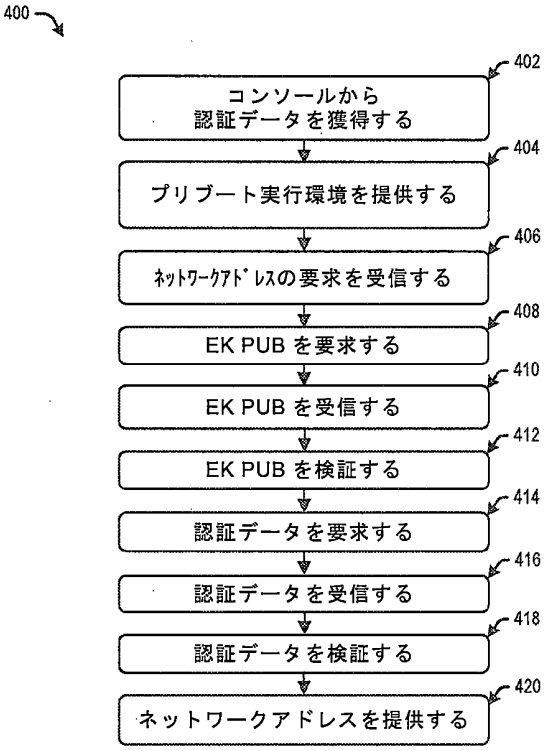


FIG. 4

【図５】

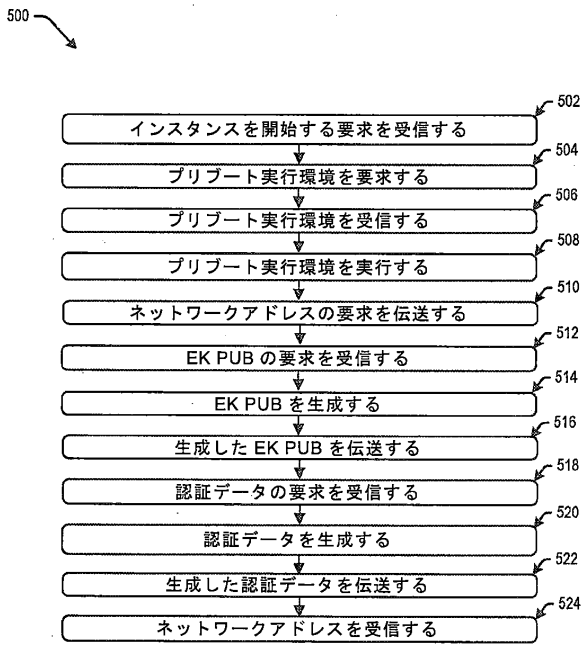


FIG. 5

【図６】

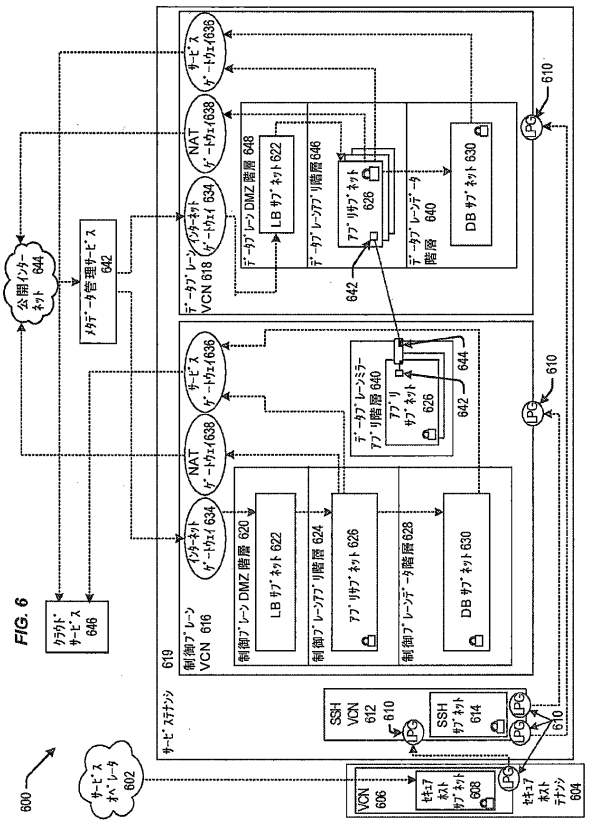
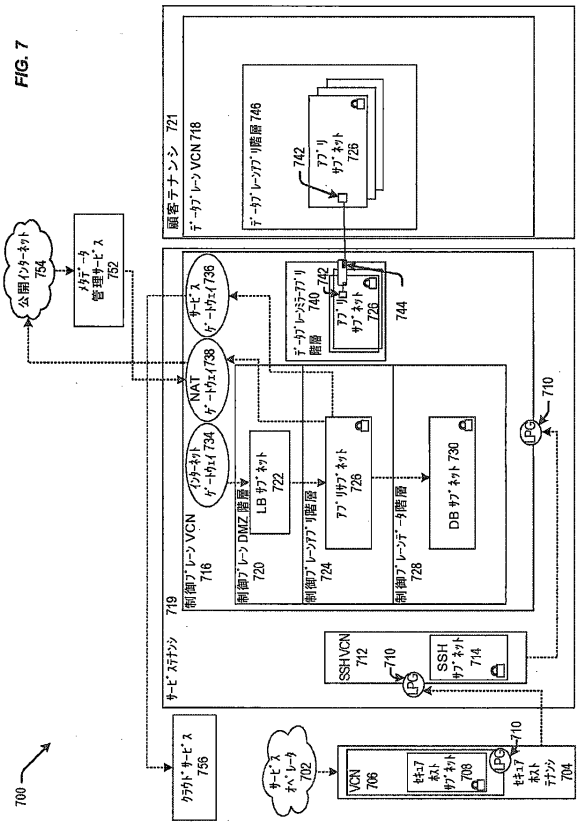
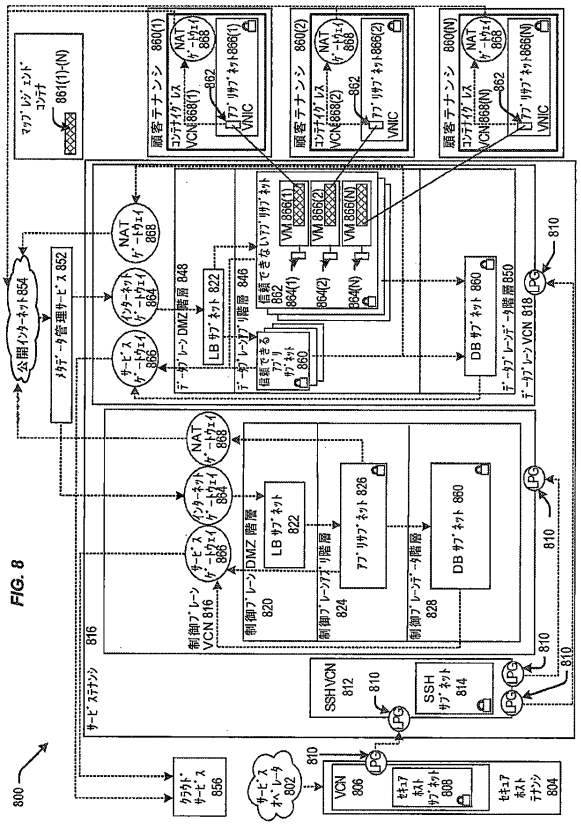


FIG. 6

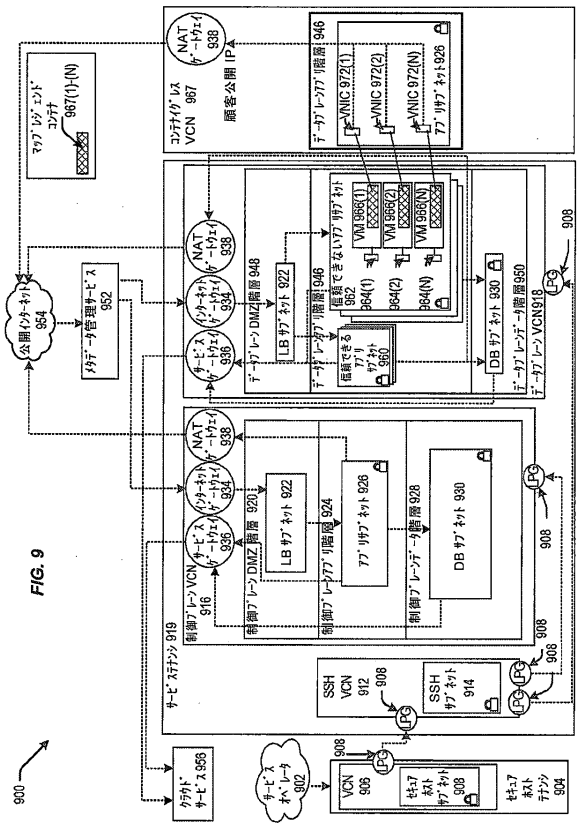
【図７】


FIG. 7
700
公開インターネット 754
メタデータ管理サービス 752
顧客テナンシ 721
データレーンVCN 718
データレーンアプリ層 746
742
アプリサブネット 726
サービステナンシ 719
制御プレーンVCN 716
制御プレーンDMZ層 720
LBサブネット 722
インターネットゲートウェイ 734
NATゲートウェイ 738
サービスゲートウェイ 736
制御プレーンアプリ層 724
アプリサブネット 726
データレーンデータ層 740
744
制御プレーンデータ層 728
DBサブネット 730
710
SSH VCN 712
SSHサブネット 714
クラウドサービス 756
サービスオペレータ 702
VCN 706
セキュアホストサブネット 708
セキュアホストテナンシ 704

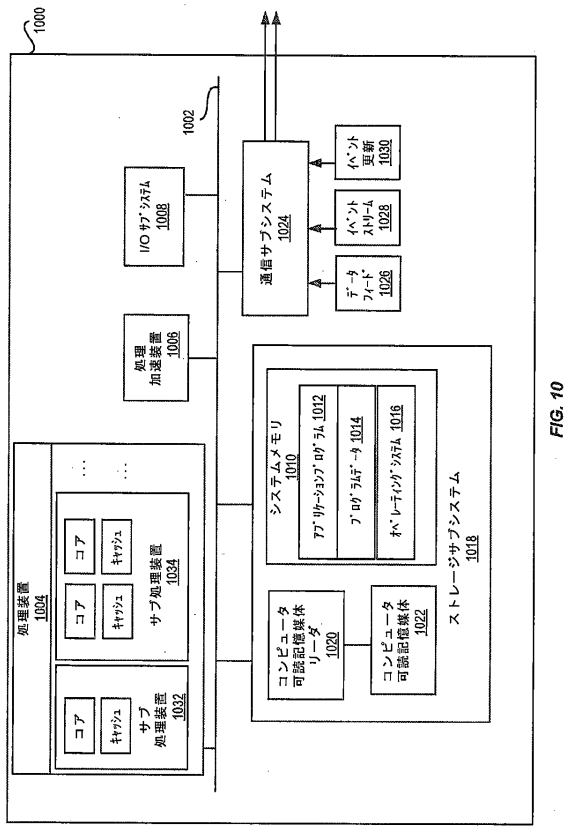
【図８】


FIG. 8
800
マップレジェンド 861(1)-(N)
顧客テナンシ 860(1)
コンテナインスタンスVCN(868(1) 862
アプリサブネット868(1) VNIC
顧客テナンシ 860(2)
コンテナインスタンスVCN(868(2) 862
アプリサブネット868(2) VNIC
顧客テナンシ 860(N)
コンテナインスタンスVCN(868(N) 862
アプリサブネット868(N) VNIC
NATゲートウェイ 868
公開インターネット 854
メタデータ管理サービス 852
サービスゲートウェイ 866
インターネットゲートウェイ 864
データレーンDMZ層 848
LBサブネット 822
データレーンアプリ層 846
信頼できるアプリサブネット 860
VM 866(1)
VM 866(2)
VM 866(N)
信頼できないアプリサブネット 862
864(1)
864(2)
864(N)
データレーンVCN 818
データレーンデータ層 850
DBサブネット 860
810
制御プレーンVCN 816
制御プレーンDMZ層 820
制御プレーンアプリ層 824
制御プレーンデータ層 828
SSH VCN 812
SSHサブネット 814
サービステナンシ 816
クラウドサービス 856
サービスオペレータ 802
VCN 806
セキュアホストサブネット 808
セキュアホストテナンシ 804

【図９】


FIG. 9
900
マップレジェンド 987(1)-(N)
コンテナインスタンスVCN 967
顧客公開IP
NATゲートウェイ 938
公開インターネット 954
メタデータ管理サービス 952
データレーンアプリ層 946
VNIC 972(1)
VNIC 972(2)
VNIC 972(N)
アプリサブネット 926
インターネットゲートウェイ 934
サービスゲートウェイ 936
データレーンDMZ層 948
LBサブネット 922
信頼できるアプリサブネット 960
信頼できないアプリサブネット 962
VM 966(1)
VM 966(2)
VM 966(N)
964(1)
964(2)
964(N)
DBサブネット 930
データレーンデータ層 950
データレーンVCN 916
908
制御プレーンVCN 916
制御プレーンDMZ層 920
制御プレーンアプリ層 924
制御プレーンデータ層 928
サービステナンシ 919
SSH VCN 912
SSHサブネット 914
クラウドサービス 955
サービスオペレータ 902
VCN 906
セキュアホストサブネット 908
セキュアホストテナンシ 904

【図１０】


FIG. 10
1000
1002
処理装置 1004
コア
キャッシュ
サブ処理装置 1032
サブ処理装置 1034
処理加速装置 1006
I/Oサブシステム 1008
通信サブシステム 1024
イベント更新 1030
イベントストリーム 1028
データフィード 1026
システムメモリ 1010
アプリケーションプログラム 1012
プログラムデータ 1014
オペレーティングシステム 1016
ストレージサブシステム 1018
コンピュータ可読記憶媒体リーダ 1020
コンピュータ可読記憶媒体 1022

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/077605

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/40 H04L9/08 H04L9/32 G06F9/4401 G06F21/57
G06F21/64
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, 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 Y	US 2004/039946 A1 (SMITH NED MCARTHUR [US] ET AL) 26 February 2004 (2004-02-26) paragraphs [0015], [0018] - [0027] -----	1,2,4, 8-10,12 3,5-7, 11,13-20
Y	US 2020/184078 A1 (HINRICHS SUSAN [US] ET AL) 11 June 2020 (2020-06-11) paragraphs [0039], [0050] -----	3,5,11, 15-20
Y	US 2021/334123 A1 (LENT ARTHUR [US] ET AL) 28 October 2021 (2021-10-28) paragraphs [0046] - [0053] -----	6,7,13, 14,19,20

☐ 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
16 January 2023	23/01/2023

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	Herzog, Till-Henning

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/077605

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004039946 A1	26-02-2004	NONE	
US 2020184078 A1	11-06-2020	NONE	
US 2021334123 A1	28-10-2021	NONE	

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

フロントページの続き

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．ｉＯＳ