(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6496404号
(P6496404)
(45)発行日　平成31年4月3日(2019.4.3)　(24)登録日　平成31年3月15日(2019.3.15)

(51)Int.Cl.　F I
H04L 12/66 (2006.01)　H04L 12/66 B
H04L 12/721 (2013.01)　H04L 12/721 Z

請求項の数 15　(全 40 頁)

(21)出願番号　特願2017-514693(P2017-514693)
(86)(22)出願日　平成27年4月27日(2015.4.27)
(65)公表番号　特表2017-529793(P2017-529793A)
(43)公表日　平成29年10月5日(2017.10.5)
(86)国際出願番号　PCT/US2015/027757
(87)国際公開番号　WO2016/048418
(87)国際公開日　平成28年3月31日(2016.3.31)
審査請求日　平成29年11月2日(2017.11.2)
(31)優先権主張番号　62/054,613
(32)優先日　平成26年9月24日(2014.9.24)
(33)優先権主張国　米国(US)
(31)優先権主張番号　14/696,186
(32)優先日　平成27年4月24日(2015.4.24)
(33)優先権主張国　米国(US)

(73)特許権者　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国カリフォルニア州９４０６５レッドウッド・シティー，オラクル・パークウェイ５００
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　ハンダ，ニティン
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、オラクル・パークウェイ、５００、エム／エス・５・オゥ・ピィ・７

最終頁に続く

(54)【発明の名称】コンピュータサブネットワーク内のプロキシサーバ

(57)【特許請求の範囲】
【請求項１】
コンピュータネットワーク間で送信されるメッセージを処理する方法であって、前記方法は、
内部コンピュータネットワークのサブネットワーク内のプロキシサーバで第１のメッセージを受信するステップを含み、前記プロキシサーバは、前記内部コンピュータネットワークの一組のウェブアプリケーションまたはサービスを外部コンピュータネットワークに公開し、前記方法はさらに、
前記第１のメッセージのための意図された宛先を判断するステップと、
前記第１のメッセージのための前記意図された宛先に基づいて、前記プロキシサーバがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかを判断するステップと、
前記プロキシサーバ内の前記第１のメッセージのための予め定められた処理フローにおける現在点を判断するステップと、
前記プロキシサーバ内でメッセージを処理するための複数のポリシーから、前記第１のメッセージを処理するためのポリシーを選択するステップとを含み、選択は、前記予め定められた処理フローにおける前記現在点、または、前記プロキシサーバがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかの判断、のうちの少なくとも１つに基づいており、前記方法はさらに、
選択された前記ポリシーに従って前記第１のメッセージを処理するステップと、

前記第１のメッセージを処理した後で、前記第１のメッセージを前記意図された宛先に送信するステップとを含む、方法。

【請求項２】

前記プロキシサーバはセキュリティプロキシを含み、選択された前記ポリシーは、１つ以上のウェブサービスセキュリティポリシーを呼び出すマシン実行可能コードを含む、請求項１に記載の方法。

【請求項３】

前記プロキシサーバは、前記内部コンピュータネットワークの物理的サブネットワーク内で動作するコンピュータシステムを含む、請求項１または２に記載の方法。

【請求項４】

前記プロキシサーバは、前記内部コンピュータネットワークの論理的サブネットワーク内で実行されるプロキシサーバアプリケーションを含む、請求項１または２に記載の方法。

【請求項５】

前記第１のメッセージを処理するための前記ポリシーを選択するステップは、

前記第１のメッセージのための前記処理フロー中にエラーが起こったと判断するステップと、

前記エラーが起こったという判断に基づいて前記ポリシーを選択するステップとを含む、請求項１～４のいずれか１項に記載の方法。

【請求項６】

前記第１のメッセージを処理するための前記ポリシーを選択するステップは、

前記第１のメッセージのための着信メッセージフォーマットを判断するステップと、

前記第１のメッセージは、前記着信メッセージフォーマットとは異なる、必要とされる発信メッセージフォーマットに変換されるべきであると判断するステップと、

前記第１のメッセージは変換されるべきであるという判断に基づいて前記ポリシーを選択するステップとを含む、請求項１～４のいずれか１項に記載の方法。

【請求項７】

前記第１のメッセージのための前記処理フローにおける前記現在点を判断するステップは、

前記第１のメッセージは、前記外部コンピュータネットワークにおけるクライアント装置からの要求に対応していると判断するステップ、または

前記プロキシサーバは、前記内部コンピュータネットワークにおけるウェブアプリケーションまたはウェブサービスに前記要求を送信すべきであると判断するステップ、

のうちの少なくとも１つを含む、請求項１～６のいずれか１項に記載の方法。

【請求項８】

前記第１のメッセージのための前記処理フローにおける前記現在点を判断するステップは、

前記第１のメッセージは、前記プロキシサーバによって送信された以前のメッセージに対する、前記内部コンピュータネットワークにおけるウェブアプリケーションまたはウェブサービスからの応答に対応していると判断するステップ、または

前記プロキシサーバは、前記外部コンピュータネットワークにおけるクライアント装置に前記応答を送信すべきであると判断するステップ、

のうちの少なくとも１つを含む、請求項１～６のいずれか１項に記載の方法。

【請求項９】

前記第１のメッセージは、前記内部コンピュータネットワークの簡易オブジェクトアクセスプロトコル（ＳＯＡＰ）仮想サービス内の１つ以上のＳＯＡＰ動作を呼び出すためのメッセージである、または当該１つ以上のＳＯＡＰ動作からのメッセージの一部であると判断するステップと、

判断された前記ＳＯＡＰ動作および前記ＳＯＡＰ仮想サービスに基づいて、前記第１のメッセージを処理するための前記ポリシーを選択するステップと、

選択された前記ポリシーに従って前記第１のメッセージを処理した後で、前記第１のメッセージ内のデータを使用して、判断された前記１つ以上のＳＯＡＰ動作を呼び出すステップとをさらに含む、請求項１～８のいずれか１項に記載の方法。

【請求項１０】

前記第１のメッセージは、前記内部コンピュータネットワークのレプリゼンテーショナル・ステート・トランスファー（ＲＥＳＴ）仮想サービスまたは仮想ウェブアプリケーションに関連付けられた１つ以上のハイパーテキスト転送プロトコル（ＨＴＴＰ）方法に対応していると判断するステップと、

判断された前記ＨＴＴＰ方法および前記ＲＥＳＴ仮想サービスまたは仮想ウェブアプリケーションに基づいて、前記第１のメッセージを処理するための前記ポリシーを選択するステップと、

選択された前記ポリシーに従って前記第１のメッセージを処理した後で、前記第１のメッセージ内のデータを使用して、判断された前記１つ以上のＨＴＴＰ方法を呼び出すステップとをさらに含む、請求項１～８のいずれか１項に記載の方法。

【請求項１１】

前記第１のメッセージに関連付けられた１つ以上のユーザクレデンシャルを受信するステップをさらに含み、前記第１のメッセージは、前記外部コンピュータネットワークにおけるクライアント装置からの、前記内部コンピュータネットワークの第１のウェブサービスにアクセスしたいという要求に対応しており、前記方法はさらに、

前記ユーザクレデンシャルを使用して、前記要求に関連付けられた第１のユーザを認証するステップを含む、請求項１～１０のいずれか１項に記載の方法。

【請求項１２】

前記第１のウェブサービスにアクセスするために、第１のトークンタイプの認証トークンが必要とされると判断するステップと、

前記内部コンピュータネットワークのウェブサービスから第１の認証トークンを検索するステップとをさらに含み、前記第１の認証トークンは前記第１のトークンタイプのもので、前記第１のユーザに関連付けられており、前記方法はさらに、

前記要求に従って前記第１のウェブサービスにアクセスするために前記第１の認証トークンを使用するステップを含む、請求項１１に記載の方法。

【請求項１３】

前記予め定められた処理フローにおける判断された前記現在点に基づいて、OnRequest()、OnInvoke()、OnResponse()、またはonError()方法を実行するステップをさらに含む、請求項１～１２のいずれか１項に記載の方法。

【請求項１４】

システムであって、

１つ以上のプロセッサを含む処理部と、

前記処理部と結合され、前記処理部によって読取可能であるメモリとを含み、前記メモリは、前記処理部によって実行されると前記処理部に以下のステップを行なわせる一組の命令を格納しており、前記以下のステップは、

第１のメッセージを受信するステップを含み、前記システムは、内部コンピュータネットワークのサブネットワーク内で動作するように構成され、前記システムは、前記内部コンピュータネットワークの一組のウェブアプリケーションまたはサービスを外部コンピュータネットワークに公開し、前記以下のステップはさらに、

前記第１のメッセージのための意図された宛先を判断するステップと、

前記第１のメッセージのための前記意図された宛先に基づいて、前記システムがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかを判断するステップと、

前記第１のメッセージのための予め定められた処理フローにおける現在点を判断するステップと、

メッセージを処理するための複数のポリシーから、前記第１のメッセージを処理するた

めのポリシーを選択するステップとを含み、選択は、前記予め定められた処理フローにおける前記現在点、または、前記システムがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかの判断、のうちの少なくとも１つに基づいており、前記以下のステップはさらに、

選択された前記ポリシーに従って前記第１のメッセージを処理するステップと、

前記第１のメッセージを処理した後で、前記第１のメッセージを前記意図された宛先に送信するステップとを含む、システム。

【請求項１５】

請求項１から１３のいずれか１項に記載の方法をプロセッサに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願

本願は、２０１５年４月２４日に出願された、「コンピュータサブネットワーク内のプロキシサーバ」（PROXY SERVERS WITHIN COMPUTER SUBNETWORKS）と題された米国非仮出願第１４／６９６，１８６号の利益および優先権を主張し、当該非仮出願は、２０１４年９月２４日に出願された、「モバイルセキュリティアクセスサーバ（MOBILE SECURITY ACCESS SERVER：ＭＳＡＳ）」と題された米国仮特許出願第６２／０５４，６１３号の利益および優先権を主張する。上述の特許出願の内容全体は、あらゆる目的のために、ここに引用により援用される。

【背景技術】

【０００２】

背景

この開示は一般に、セキュリティサービスを提供するためのシステム、方法、およびマシン読取可能媒体に関する。より特定的には、この開示は、とりわけ、認証、認可、監査、シングルサインオン、セキュリティポリシー実施、キー管理および分散、安全な通信、安全なデータ格納、および安全なデータ共有を含む、モバイル装置と企業アプリケーションとの接続のためのセキュリティサービスを提供するためのシステム、方法、およびマシン読取可能媒体に関する。

【発明の概要】

【課題を解決するための手段】

【０００３】

簡単な概要

ここに説明される局面は、コンピュータネットワーク間で送信されるメッセージを処理するためのさまざまな手法を提供する。いくつかの実施形態では、さまざまなタイプのウェブサービス、アプリケーション、および他のウェブコンテンツに対する要求および応答といったメッセージが、複数のコンピュータネットワーク間で送信されてもよい。物理的または論理的サブネットワーク内に実装されたプロキシサーバといった、１つ以上の中間装置またはアプリケーションが、通信エンドポイント間でメッセージを受信し、処理し、送信してもよい。たとえば、プロキシサーバは、内部コンピュータネットワークのサブネットワーク内で動作するように構成されてもよく、内部コンピュータネットワークのさまざまなウェブアプリケーションおよび／またはサービスを外部コンピュータネットワークに公開する。

【０００４】

ある実施形態では、プロキシサーバは、内部ネットワークにおけるエンドポイントから外部システムにおけるエンドポイントに送信されたメッセージを受信してもよく、または、その逆も同様である。メッセージは、メッセージの意図された宛先を判断するために、および／または、メッセージを処理する際にプロキシサーバがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかを判断するために、分析されてもよい

。加えて、プロキシサーバは、特定のメッセージを処理するためのエンドツーエンドポリシーモデルといった予め定められた処理フローにおける現在点（カレントポイント：current point）を判断してもよい。メッセージの分析および予め定められた処理フローにおける現在点に基づいて、プロキシサーバは、メッセージに適用されるべき１つ以上のポリシーを選択してもよい。そのようなポリシーは、たとえば、メッセージを認証する、セキュリティトークン仲介およびキー管理を提供する、プロトコルおよびペイロード仲介を行なう、装置ベースのセキュリティを行なう、非武装ゾーン（demilitarized zone：ＤＭＺ）脅威保護をサポートする、などのためのセキュリティポリシーおよび他の通信管理ポリシーを含んでいてもよい。メッセージに適用されるべき特定のポリシーを選択した後で、プロキシサーバは、ポリシーに従ってメッセージを処理し、メッセージをその意図された宛先に発送してもよい。

【０００５】

また、ここに説明される例が示すように、さまざまな実施形態は、異なるセキュリティポリシーおよび他の通信管理ポリシーが、ＤＭＺもしくは他の論理的または物理的サブネットワーク内で、メッセージのエンドツーエンド処理フロー全体にわたるさまざまな異なる処理点で適用され得る、動的ポリシーモデルをサポートしてもよい。そのような動的ポリシーモデルフレームワークは、通信エンドポイント内では可能ではなかったかもしれない、または好ましくなかったかもしれない、さまざまなタイプのコンピュータネットワークおよびシステムセキュリティおよび他の通信ポリシーを構築し実現するために使用されてもよい。

【図面の簡単な説明】

【０００６】

【図１】この発明のさまざまな実施形態が実現され得る例示的な分散型システムのコンポーネントを示すブロック図である。

【図２】この発明の実施形態によって提供されるサービスをクラウドサービスとして提供し得るシステム環境のコンポーネントを示すブロック図である。

【図３】この発明の実施形態が実現され得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。

【図４】この発明の１つ以上の実施形態に従った、コンピューティング装置および／またはシステム間でメッセージを処理して送信するためのプロキシサーバを含むコンピューティング環境を、高レベルで示すブロック図である。

【図５】この発明の１つ以上の実施形態に従った、選択されたメッセージ処理ポリシーを使用してメッセージを受信して処理するためのプロセスを示すフローチャートである。

【図６Ａ】この発明の１つ以上の実施形態に従った、予め定められたメッセージ処理フローの例を示すマークアップ言語文書を示す図である。

【図６Ｂ】この発明の１つ以上の実施形態に従った、予め定められたメッセージ処理フローの例を示すマークアップ言語文書を示す図である。

【図７Ａ】この発明の１つ以上の実施形態に従った、１つ以上のメッセージ処理フロー内の異なる点に対応するメッセージ処理ポリシーの例示的なテンプレートを示すマークアップ言語文書を示す図である。

【図７Ｂ】この発明の１つ以上の実施形態に従った、１つ以上のメッセージ処理フロー内の異なる点に対応するメッセージ処理ポリシーの例示的なテンプレートを示すマークアップ言語文書を示す図である。

【図７Ｃ】この発明の１つ以上の実施形態に従った、１つ以上のメッセージ処理フロー内の異なる点に対応するメッセージ処理ポリシーの例示的なテンプレートを示すマークアップ言語文書を示す図である。

【図７Ｄ】この発明の１つ以上の実施形態に従った、１つ以上のメッセージ処理フロー内の異なる点に対応するメッセージ処理ポリシーの例示的なテンプレートを示すマークアップ言語文書を示す図である。

【図８】この発明の１つ以上の実施形態に従った、外部クライアント装置から内部ウェブ

サービスに送信されたウェブサービス要求のエンドツーエンド処理フローを示すフロー図である。
【図９】この発明の１つ以上の実施形態に従った、内部クライアント装置から外部ウェブサービスまたはアプリケーションに送信されたウェブサービスまたはアプリケーション要求のエンドツーエンド処理フローを示すフロー図である。
【発明を実施するための形態】
【０００７】
詳細な説明
以下の記載では、説明の目的のため、多くの特定の詳細が、この発明のさまざまな実施形態の完全な理解を提供するために述べられる。しかしながら、これらの特定の詳細のうちのいくつかがなくてもこの発明の実施形態は実践され得る、ということは、当業者には明らかであろう。他の例では、周知の構造および装置は、ブロック図の形で示される。
【０００８】
以下の記載は例示的な実施形態のみを提供しており、この開示の範囲、利用可能性、または構成を限定するよう意図されてはいない。むしろ、例示的な実施形態の以下の記載は、例示的な実施形態を実現するための実施可能な説明を当業者に提供するであろう。添付された請求項で述べられるようなこの発明の精神および範囲から逸脱することなく、要素の機能および配置においてさまざまな変更が行なわれてもよい、ということが理解されるべきである。
【０００９】
以下の記載では、実施形態の完全な理解を提供するために、特定の詳細が与えられる。しかしながら、これらの特定の詳細がなくても実施形態は実践され得る、ということは、当業者には理解されるであろう。たとえば、実施形態を必要以上に詳細に記して不明瞭にすることがないように、回路、システム、ネットワーク、プロセス、および他のコンポーネントは、ブロック図の形のコンポーネントとして示されてもよい。他の例では、実施形態を不明瞭にしないように、周知の回路、プロセス、アルゴリズム、構造、および手法は、不要な詳細なしで示されてもよい。
【００１０】
また、個々の実施形態は、フローチャート、フロー図、データフロー図、構造図、またはブロック図として示されるプロセスとして説明され得ることに留意されたい。フローチャートは動作を順次プロセスとして説明し得るものの、動作の多くは並行してまたは同時に行なうことが可能である。加えて、動作の順序は並べ替えられてもよい。プロセスは、その動作が完了すると終了するが、図に含まれない追加のステップを有していてもよい。プロセスは、方法、機能、手順、サブルーチン、サブプログラムなどに対応していてもよい。プロセスがある機能に対応している場合、その終了は、その機能が呼出し元の機能または主機能に戻ることに対応可能である。
【００１１】
「コンピュータ読取可能媒体」という用語は、命令および／またはデータを格納し、含み、または担持することができる、携帯型または固定式記憶装置、光学記憶装置、ならびにさまざまな他の媒体といった非一時的媒体を含むものの、それらに限定されない。コードセグメントまたはコンピュータ実行可能命令が、手順、機能、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、もしくは、命令、データ構造またはプログラム文の任意の組合せを表わしてもよい。コードセグメントは、情報、データ、引数、パラメータ、またはメモリ内容を渡し、および／または受信することによって、別のコードセグメントまたはハードウェア回路に結合されてもよい。情報、引数、パラメータ、データなどは、メモリ共有、メッセージパッシング、トークンパッシング、ネットワーク送信などを含む任意の好適な手段を介して渡され、発送され、または送信されてもよい。
【００１２】
さらに、実施形態は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、

マイクロコード、ハードウェア記述言語、またはそれらの任意の組合せによって実現されてもよい。ソフトウェア、ファームウェア、ミドルウェアまたはマイクロコードで実現される場合、必要なタスクを行なうためのプログラムコードまたはコードセグメントが、マシン読取可能媒体に格納されてもよい。プロセッサが、必要なタスクを行なってもよい。

【００１３】

コンピュータネットワーク間で送信されるメッセージを処理するために、さまざまな手法（たとえば、方法、システム、１つ以上のプロセッサによって実行可能な複数の命令を格納する非一時的なコンピュータ読取可能記憶メモリ、など）がここに説明される。いくつかの実施形態では、さまざまなタイプのウェブサービス、アプリケーション、および他のウェブコンテンツに対する要求および応答といったメッセージが、複数のコンピュータネットワーク間で送信されてもよい。物理的または論理的サブネットワーク内に実装されたプロキシサーバといった、１つ以上の中間装置またはアプリケーションが、通信エンドポイント間でメッセージを受信し、処理し、送信してもよい。たとえば、プロキシサーバは、内部コンピュータネットワークのサブネットワーク内で動作するように構成されてもよく、内部コンピュータネットワークのさまざまなウェブアプリケーションおよび／またはサービスを外部コンピュータネットワークに公開する。

【００１４】

いくつかの実施形態では、プロキシサーバは、内部ネットワークにおけるエンドポイントから外部システムにおけるエンドポイントに送信されたメッセージを受信してもよく、または、その逆も同様である。メッセージは、メッセージの意図された宛先を判断するために、および／または、メッセージを処理する際にプロキシサーバがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかを判断するために、分析されてもよい。加えて、プロキシサーバは、特定のメッセージを処理するためのエンドツーエンドポリシーモデルといった予め定められた処理フローにおける現在点を判断してもよい。メッセージの分析および予め定められた処理フローにおける現在点に基づいて、プロキシサーバは、メッセージに適用されるべき１つ以上のポリシーを選択してもよい。そのようなポリシーは、たとえば、メッセージを認証する、セキュリティトークン仲介およびキー管理を提供する、プロトコルおよびペイロード仲介を行なう、装置ベースのセキュリティを行なう、非武装ゾーン（ＤＭＺ）脅威保護をサポートする、などのためのセキュリティポリシーおよび他の通信管理ポリシーを含んでいてもよい。メッセージに適用されるべき特定のポリシーを選択した後で、プロキシサーバは、ポリシーに従ってメッセージを処理し、メッセージをその意図された宛先に発送してもよい。この発明の実施形態のさまざまな追加の詳細を、図を参照して以下に説明する。

【００１５】

図１は、この発明のさまざまな実施形態が実現され得る例示的な分散型システムのコンポーネントを示すブロック図である。図示された実施形態では、分散型システム１００は１つ以上のクライアントコンピューティング装置１０２、１０４、１０６、および１０８を含み、それらは、１つ以上のネットワーク１１０を通して、ウェブブラウザ、専用クライアント（たとえば、オラクル・フォームズ（Oracle Forms））などのクライアントアプリケーションを実行し、動作させるように構成される。サーバ１１２は、ネットワーク１１０を介して、リモートクライアントコンピューティング装置１０２、１０４、１０６、および１０８と通信可能に結合されてもよい。

【００１６】

さまざまな実施形態では、サーバ１１２は、システムのコンポーネントのうちの１つ以上によって提供される１つ以上のサービスまたはソフトウェアアプリケーションを実行するように適合されてもよい。いくつかの実施形態では、これらのサービスは、ウェブベースのサービスまたはクラウドサービスとして、もしくはソフトウェア・アズ・ア・サービス（Software as a Service：ＳａａＳ）モデルの下で、クライアントコンピューティング装置１０２、１０４、１０６、および／または１０８のユーザに提供されてもよい。クライアントコンピューティング装置１０２、１０４、１０６、および／または１０８を動

作させるユーザは次に、これらのコンポーネントによって提供されるサービスを利用するためにサーバ１１２とやりとりするために、１つ以上のクライアントアプリケーションを利用してもよい。

【００１７】

図に示す構成では、システム１００のソフトウェアコンポーネント１１８、１２０および１２２は、サーバ１１２上で実現されるとして図示されている。他の実施形態では、システム１００のコンポーネントおよび／またはこれらのコンポーネントによって提供されるサービスのうちの１つ以上も、クライアントコンピューティング装置１０２、１０４、１０６、および／または１０８のうちの１つ以上によって実現されてもよい。クライアントコンピューティング装置を動作させるユーザは次に、これらのコンポーネントによって提供されるサービスを使用するために、１つ以上のクライアントアプリケーションを利用してもよい。これらのコンポーネントは、ハードウェア、ファームウェア、ソフトウェア、またはそれらの組合せで実現されてもよい。分散型システム１００とは異なり得るさまざまな異なるシステム構成が可能であることが理解されるべきである。図に示す実施形態はこのため、実施形態システムを実現するための分散型システムの一例であり、限定的であるよう意図されてはいない。

【００１８】

クライアントコンピューティング装置１０２、１０４、１０６、および／または１０８は、携帯型ハンドヘルド装置（たとえば、ｉＰｈｏｎｅ（登録商標）、携帯電話、ｉＰａｄ（登録商標）、コンピューティングタブレット、携帯情報端末（ＰＤＡ））、またはウェアラブル装置（たとえば、グーグル・グラス（Google Glass）（登録商標）頭部装着型ディスプレイ）であってもよく、マイクロソフト・ウィンドウズ・モバイル（Microsoft Windows Mobile）（登録商標）などのソフトウェア、および／または、ｉＯＳ、ウィンドウズ（登録商標）フォン、アンドロイド（登録商標）、ブラックベリー（登録商標）１０、パームＯＳなどのさまざまなモバイルオペレーティングシステムを実行し、インターネット、電子メール、ショートメッセージサービス（short message service：ＳＭＳ）、ブラックベリー（登録商標）、または他の通信プロトコルに対応している。クライアントコンピューティング装置は、マイクロソフト・ウィンドウズ（登録商標）、アップル・マッキントッシュ（登録商標）、および／またはＬｉｎｕｘ（登録商標）オペレーティングシステムのさまざまなバージョンを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを例として含む、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装置は、たとえばグーグル・クロームＯＳなどのさまざまなＧＮＵ／Ｌｉｎｕｘオペレーティングシステムを何ら限定されることなく含む、商業的に入手可能なさまざまなＵＮＩＸ（登録商標）またはＵＮＩＸ様オペレーティングシステムのうちのいずれかを実行するワークステーションコンピュータであり得る。それに代えて、またはそれに加えて、クライアントコンピューティング装置１０２、１０４、１０６、および１０８は、ネットワーク１１０を通して通信可能である、シンクライアントコンピュータ、インターネット対応ゲーミングシステム（たとえば、Ｋｉｎｅｃｔ（登録商標）ジェスチャー入力装置を有する、または有さない、マイクロソフト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装置といった、任意の他の電子装置であってもよい。

【００１９】

例示的な分散型システム１００は４つのクライアントコンピューティング装置を有して図示されているが、任意の数のクライアントコンピューティング装置がサポートされてもよい。センサを有する装置などの他の装置が、サーバ１１２とやりとりしてもよい。

【００２０】

分散型システム１００におけるネットワーク１１０は、ＴＣＰ／ＩＰ（transmission control protocol/Internet protocol：伝送制御プロトコル／インターネットプロトコル）、ＳＮＡ（systems network architecture：システムネットワークアーキテクチャ）、ＩＰＸ（Internet packet exchange：インターネットパケット交換）、アップル・トーク

（Apple Talk）などを何ら限定されることなく含む、商業的に入手可能なさまざまなプロトコルのうちのいずれかを使用してデータ通信をサポートできる、当業者にはよく知られた任意のタイプのネットワークであってもよい。単なる例として、ネットワーク１１０は、イーサネット（登録商標）、トークンリング（Token-Ring）などに基づくものといった、ローカルエリアネットワーク（local area network：ＬＡＮ）であり得る。ネットワーク１１０は、ワイドエリアネットワークおよびインターネットであり得る。それは、仮想プライベートネットワーク（virtual private network：ＶＰＮ）を何ら限定されることなく含む仮想ネットワーク、イントラネット、エクストラネット、公衆交換電話網（public switched telephone network：ＰＳＴＮ）、赤外線ネットワーク、無線ネットワーク（たとえば、電気電子技術者協会（the Institute of Electrical and Electronics：ＩＥＥＥ）８０２．１１プロトコルスイート、Bluetooth（登録商標）、および／または任意の他の無線プロトコルのうちのいずれかの下で動作するネットワーク）、ならびに／もしくは、これらのおよび／または他のネットワークの任意の組合せを含み得る。

【００２１】

サーバ１１２は、１つ以上の汎用コンピュータ、専用サーバコンピュータ（ＰＣ（パーソナルコンピュータ）サーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウントサーバなどを例として含む）、サーバファーム、サーバクラスタ、もしくは任意の他の適切な構成および／または組合せで構成されてもよい。さまざまな実施形態では、サーバ１１２は、前述の開示で説明された１つ以上のサービスまたはソフトウェアアプリケーションを実行するように適合されてもよい。たとえば、サーバ１１２は、この開示の一実施形態に従った上述の処理を行なうためのサーバに対応していてもよい。

【００２２】

サーバ１１２は、上述のもののうちのいずれかを含むオペレーティングシステム、および商業的に入手可能な任意のサーバオペレーティングシステムを実行してもよい。サーバ１１２はまた、さまざまな追加のサーバアプリケーションおよび／または中間層アプリケーションのうちのいずれかを実行してもよく、ＨＴＴＰ（hypertext transport protocol：ハイパーテキスト伝送プロトコル）サーバ、ＦＴＰ（file transfer protocol：ファイル転送プロトコル）サーバ、ＣＧＩ（common gateway interface：コモンゲートウェイインターフェイス）サーバ、ＪＡＶＡ（登録商標）サーバ、データベースサーバなどを含む。例示的なデータベースサーバは、オラクル、マイクロソフト、サイベース（Sybase）、ＩＢＭ（International Business Machines：インターナショナル・ビジネス・マシーンズ）などから商業的に入手可能なものを何ら限定されることなく含む。

【００２３】

いくつかの実現化例では、サーバ１１２は、クライアントコンピューティング装置１０２、１０４、１０６、および１０８のユーザから受信されたデータフィードおよび／またはイベント更新を分析して統合するための１つ以上のアプリケーションを含んでいてもよい。一例として、データフィードおよび／またはイベント更新は、センサデータアプリケーション、金融ティッカー、ネットワーク性能測定ツール（たとえば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム分析ツール、自動車交通監視などに関連するリアルタイムイベントを含み得る、１つ以上の第三者情報源および連続データストリームから受信されたツイッター（登録商標）フィード、フェースブック（登録商標）更新またはリアルタイム更新を含んでいてもよいが、それらに限定されない。サーバ１１２はまた、クライアントコンピューティング装置１０２、１０４、１０６、および１０８の１つ以上の表示装置を介してデータフィードおよび／またはリアルタイムイベントを表示するための１つ以上のアプリケーションを含んでいてもよい。

【００２４】

分散型システム１００はまた、１つ以上のデータベース１１４および１１６を含んでいてもよい。データベース１１４および１１６は、さまざまな位置に存在していてもよい。例として、データベース１１４および１１６のうちの１つ以上は、サーバ１１２に対して

ローカルな（および／または、サーバ１１２内にある）非一時的記憶媒体上に存在していてもよい。それに代えて、データベース１１４および１１６は、サーバ１１２からリモートであってもよく、ネットワークベースの接続または専用接続を介してサーバ１１２と通信してもよい。一組の実施形態では、データベース１１４および１１６は、ストレージエリアネットワーク（storage-area network：ＳＡＮ）に存在していてもよい。同様に、サーバ１１２に帰する機能を行なうための任意の必要なファイルが適宜、サーバ１１２上にローカルに格納されてもよく、および／またはリモートに格納されてもよい。一組の実施形態では、データベース１１４および１１６は、ＳＱＬフォーマットのコマンドに応答してデータを格納し、更新し、検索するように適合された、オラクルによって提供されるデータベースなどのリレーショナルデータベースを含んでいてもよい。

【００２５】

図２は、この発明の実施形態によって提供されるサービスをクラウドサービスとして提供し得るシステム環境のコンポーネントを示すブロック図である。図示された実施形態では、システム環境２００は、クラウドサービスを提供するクラウドインフラストラクチャシステム２０２とやりとりするためにユーザによって使用され得る１つ以上のクライアントコンピューティング装置２０４、２０６、および２０８を含む。クライアントコンピューティング装置は、クラウドインフラストラクチャシステム２０２によって提供されるサービスを使用するためにクラウドインフラストラクチャシステム２０２とやりとりするためにクライアントコンピューティング装置のユーザによって使用され得る、ウェブブラウザ、専用クライアントアプリケーション（たとえば、オラクル・フォームズ）、または何らかの他のアプリケーションといったクライアントアプリケーションを動作させるように構成されてもよい。

【００２６】

図に示すクラウドインフラストラクチャシステム２０２は、図示されたもの以外のコンポーネントを有していてもよい、ということが理解されるべきである。また、図に示す実施形態は、この発明の一実施形態を取入れ得るクラウドインフラストラクチャシステムの単なる一例である。いくつかの他の実施形態では、クラウドインフラストラクチャシステム２０２は、図に示すものよりも多い、または少ないコンポーネントを有していてもよく、２つ以上のコンポーネントを組合せてもよく、もしくは、異なる構成または配置のコンポーネントを有していてもよい。

【００２７】

クライアントコンピューティング装置２０４、２０６、および２０８は、１０２、１０４、１０６、および１０８について上述したものと同様の装置であってもよい。

【００２８】

例示的なシステム環境２００は３つのクライアントコンピューティング装置を有して図示されているが、任意の数のクライアントコンピューティング装置がサポートされてもよい。センサを有する装置などの他の装置が、クラウドインフラストラクチャシステム２０２とやりとりしてもよい。

【００２９】

ネットワーク２１０は、クライアント２０４、２０６、および２０８とクラウドインフラストラクチャシステム２０２との間のデータの通信および交換を容易にしてもよい。各ネットワークは、ネットワーク１１０について上述したものを含む、商業的に入手可能なさまざまなプロトコルのうちのいずれかを使用してデータ通信をサポートできる、当業者にはよく知られた任意のタイプのネットワークであってもよい。

【００３０】

クラウドインフラストラクチャシステム２０２は、サーバ１１２について上述したものを含み得る１つ以上のコンピュータおよび／またはサーバを含んでいてもよい。

【００３１】

ある実施形態では、クラウドインフラストラクチャシステムによって提供されるサービスは、オンラインデータストレージおよびバックアップソリューション、ウェブベースの

電子メールサービス、ホスト型オフィススイートおよび文書コラボレーションサービス、データベース処理、管理された技術サポートサービスといった、クラウドインフラストラクチャシステムのユーザにとってオンデマンドで利用可能にされる多数のサービスを含んでいてもよい。クラウドインフラストラクチャシステムによって提供されるサービスは、そのユーザの必要性を満たすために動的にスケール変更され得る。クラウドインフラストラクチャシステムによって提供されるサービスの特定のインスタンス化は、ここに「サービスインスタンス」と呼ばれる。一般に、クラウドサービスプロバイダのシステムから、インターネットなどの通信ネットワークを介してユーザに利用可能とされる任意のサービスは、「クラウドサービス」と呼ばれる。典型的には、パブリッククラウド環境では、クラウドサービスプロバイダのシステムを作り上げるサーバおよびシステムは、顧客自身の業務用サーバおよびシステムとは異なっている。たとえば、クラウドサービスプロバイダのシステムは、アプリケーションをホストしてもよく、ユーザは、インターネットなどの通信ネットワークを介してオンデマンドでアプリケーションをオーダーし、使用してもよい。

【００３２】

いくつかの例では、コンピュータネットワーククラウドインフラストラクチャにおけるサービスは、クラウドベンダーによってユーザに提供されるかまたは当該技術分野において他の態様で公知であるようなストレージ、ホスト型データベース、ホスト型ウェブサーバ、ソフトウェアアプリケーション、もしくは他のサービスへの、保護されたコンピュータネットワークアクセスを含んでいてもよい。たとえば、サービスは、インターネットを通した、クラウド上のリモートストレージへの、パスワードで保護されたアクセスを含み得る。別の例として、サービスは、ネットワーク化された開発者による私的使用のための、ウェブサービスベースのホスト型リレーショナルデータベースおよびスクリプト言語ミドルウェアエンジンを含み得る。別の例として、サービスは、クラウドベンダーのウェブサイト上でホストされる電子メールソフトウェアアプリケーションへのアクセスを含み得る。

【００３３】

ある実施形態では、クラウドインフラストラクチャシステム２０２は、セルフサービスで、サブスクリプションベースで、弾力的にスケーラブルで、信頼でき、高可用性で、かつ安全な態様で顧客に配信される、アプリケーション、ミドルウェアおよびデータベースサービス提供物一式を含んでいてもよい。そのようなクラウドインフラストラクチャシステムの一例は、本譲受人によって提供されるオラクル・パブリック・クラウド（Oracle Public Cloud）である。

【００３４】

さまざまな実施形態では、クラウドインフラストラクチャシステム２０２は、クラウドインフラストラクチャシステム２０２によって提供されるサービスに顧客のサブスクリプションを自動的にプロビジョニングし、管理し、追跡するように適合されてもよい。クラウドインフラストラクチャシステム２０２は、異なるデプロイメントモデルを介してクラウドサービスを提供してもよい。たとえば、サービスは、クラウドインフラストラクチャシステム２０２がクラウドサービスを販売する組織によって所有され（たとえば、オラクルによって所有され）、サービスが一般大衆または異なる産業企業にとって利用可能とされる、パブリッククラウドモデルの下で提供されてもよい。別の例として、サービスは、クラウドインフラストラクチャシステム２０２が単一の組織のためにのみ動作され、その組織内の１つ以上のエンティティのためのサービスを提供し得る、プライベートクラウドモデルの下で提供されてもよい。クラウドサービスはまた、クラウドインフラストラクチャシステム２０２、およびクラウドインフラストラクチャシステム２０２によって提供されるサービスが、関連するコミュニティにおけるいくつかの組織によって共有される、コミュニティクラウドモデルの下で提供されてもよい。クラウドサービスはまた、２つ以上の異なるモデルの組合せであるハイブリッドクラウドモデルの下で提供されてもよい。

【００３５】

いくつかの実施形態では、クラウドインフラストラクチャシステム２０２によって提供されるサービスは、ソフトウェア・アズ・ア・サービス（ＳａａＳ）カテゴリー、プラットフォーム・アズ・ア・サービス（Platform as a Service：ＰａａＳ）カテゴリー、インフラストラクチャ・アズ・ア・サービス（Infrastructure as a Service：ＩａａＳ）カテゴリー、または、ハイブリッドサービスを含むサービスの他のカテゴリーの下で提供される、１つ以上のサービスを含んでいてもよい。顧客は、クラウドインフラストラクチャシステム２０２によって提供される１つ以上のサービスを、サブスクリプションオーダーを介してオーダーしてもよい。クラウドインフラストラクチャシステム２０２は次に、顧客のサブスクリプションオーダーにおけるサービスを提供するために処理を行なう。

【００３６】

いくつかの実施形態では、クラウドインフラストラクチャシステム２０２によって提供されるサービスは、アプリケーションサービス、プラットフォームサービス、およびインフラストラクチャサービスを、何ら限定されることなく含んでいてもよい。いくつかの例では、アプリケーションサービスは、ＳａａＳプラットフォームを介して、クラウドインフラストラクチャシステムによって提供されてもよい。ＳａａＳプラットフォームは、ＳａａＳカテゴリーに該当するクラウドサービスを提供するように構成されてもよい。たとえば、ＳａａＳプラットフォームは、統合された開発およびデプロイメントプラットフォーム上にオンデマンドアプリケーション一式を構築し、配信するための能力を提供してもよい。ＳａａＳプラットフォームは、ＳａａＳサービスを提供するための基本ソフトウェアおよびインフラストラクチャを管理し、制御してもよい。ＳａａＳプラットフォームによって提供されるサービスを利用することにより、顧客は、クラウドインフラストラクチャシステム上で実行されるアプリケーションを利用できる。顧客は、顧客が別々のライセンスおよびサポートを購入する必要なく、アプリケーションサービスを取得できる。さまざまな異なるＳａａＳサービスが提供されてもよい。例は、大型組織のための販売実績管理、企業統合、およびビジネス柔軟性についてのソリューションを提供するサービスを、何ら限定されることなく含む。

【００３７】

いくつかの実施形態では、プラットフォームサービスは、ＰａａＳプラットフォームを介して、クラウドインフラストラクチャシステムによって提供されてもよい。ＰａａＳプラットフォームは、ＰａａＳカテゴリーに該当するクラウドサービスを提供するように構成されてもよい。プラットフォームサービスの例は、（オラクルなどの）組織が共有の共通アーキテクチャ上で既存のアプリケーションを統合できるようにするサービスと、プラットフォームによって提供される共有のサービスを活用する新しいアプリケーションを構築するための能力とを、何ら限定されることなく含んでいてもよい。ＰａａＳプラットフォームは、ＰａａＳサービスを提供するための基本ソフトウェアおよびインフラストラクチャを管理し、制御してもよい。顧客は、顧客が別々のライセンスおよびサポートを購入する必要なく、クラウドインフラストラクチャシステムによって提供されるＰａａＳサービスを取得できる。プラットフォームサービスの例は、オラクルＪａｖａ（登録商標）クラウドサービス（Java Cloud Service：ＪＣＳ）、オラクル・データベース・クラウド・サービス（Database Cloud Service：ＤＢＣＳ）などを、何ら限定されることなく含む。

【００３８】

ＰａａＳプラットフォームによって提供されるサービスを利用することにより、顧客は、クラウドインフラストラクチャシステムによってサポートされるプログラミング言語およびツールを採用するとともに、デプロイメントされたサービスを制御することができる。いくつかの実施形態では、クラウドインフラストラクチャシステムによって提供されるプラットフォームサービスは、データベースクラウドサービス、ミドルウェアクラウドサービス（たとえば、オラクル・フュージョン・ミドルウェア（Oracle Fusion Middleware）サービス）、およびＪａｖａクラウドサービスを含んでいてもよい。一実施形態では、データベースクラウドサービスは、組織がデータベースリソースをプールし、データベースクラウドの形をしたデータベース・アズ・ア・サービスを顧客に提供することを可能に

する共有のサービスデプロイメントモデルをサポートしてもよい。ミドルウェアクラウドサービスは、顧客がさまざまなビジネスアプリケーションを開発してデプロイメントするためのプラットフォームを提供してもよく、Ｊａｖａクラウドサービスは、顧客がクラウドインフラストラクチャシステムにおいてＪａｖａアプリケーションをデプロイメントするためのプラットフォームを提供してもよい。

【００３９】

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

【００４０】

ある実施形態では、クラウドインフラストラクチャシステム２０２はまた、クラウドインフラストラクチャシステムの顧客にさまざまなサービスを提供するために使用されるリソースを提供するためのインフラストラクチャリソース２３０を含んでいてもよい。一実施形態では、インフラストラクチャリソース２３０は、ＰａａＳプラットフォームおよびＳａａＳプラットフォームによって提供されるサービスを実行するために、サーバ、ストレージ、およびネットワーキングリソースなどのハードウェアの予め統合され最適化された組合せを含んでいてもよい。

【００４１】

いくつかの実施形態では、クラウドインフラストラクチャシステム２０２におけるリソースは、複数のユーザによって共有され、要望ごとに動的に再割当てされてもよい。加えて、リソースは、異なる時間帯におけるユーザに割当てられてもよい。たとえば、クラウドインフラストラクチャシステム２３０は、第１の時間帯における第１の一組のユーザが、特定数の時間、クラウドインフラストラクチャシステムのリソースを利用することを可能にし、次に、異なる時間帯に位置する別の一組のユーザへの同じリソースの再割当てを可能にして、それによりリソースの利用を最大化してもよい。

【００４２】

ある実施形態では、クラウドインフラストラクチャシステム２０２の異なるコンポーネントまたはモジュールによって、およびクラウドインフラストラクチャシステム２０２によって提供されるサービスによって共有される、多くの内部共有サービス２３２が提供されてもよい。これらの内部共有サービスは、セキュリティおよびアイデンティティサービス、統合サービス、企業リポジトリサービス、企業マネージャサービス、ウィルススキャニングおよびホワイトリストサービス、高可用性、バックアップおよび復元サービス、クラウドサポートを可能にするためのサービス、電子メールサービス、通知サービス、ファイル転送サービスなどを、何ら限定されることなく含んでいてもよい。

【００４３】

ある実施形態では、クラウドインフラストラクチャシステム２０２は、クラウドインフラストラクチャシステムにおけるクラウドサービス（たとえば、ＳａａＳ、ＰａａＳ、およびＩａａＳサービス）の包括的管理を提供してもよい。一実施形態では、クラウド管理機能性は、クラウドインフラストラクチャシステム２０２によって受信された顧客のサブスクリプションをプロビジョニングし、管理し、追跡するための能力などを含んでいてもよい。

【００４４】

一実施形態では、図に示すように、クラウド管理機能性は、オーダー管理モジュール２２０、オーダーオーケストレーションモジュール２２２、オーダープロビジョニングモジュール２２４、オーダー管理および監視モジュール２２６、ならびにアイデンティティ管理モジュール２２８などの１つ以上のモジュールによって提供されてもよい。これらのモジュールは、汎用コンピュータ、専用サーバコンピュータ、サーバファーム、サーバクラ

スタ、もしくは任意の他の適切な構成および／または組合せであり得る、１つ以上のコンピュータおよび／またはサーバを含んでいてもよく、もしくはそれらを使用して提供されてもよい。

【００４５】

例示的な動作２３４では、クライアント装置２０４、２０６または２０８などのクライアント装置を使用する顧客は、クラウドインフラストラクチャシステム２０２によって提供される１つ以上のサービスを要求し、クラウドインフラストラクチャシステム２０２によって提供される１つ以上のサービスについてサブスクリプションオーダーを出すことにより、クラウドインフラストラクチャシステム２０２とやりとりしてもよい。ある実施形態では、顧客は、クラウドユーザインターフェイス（User Interface：ＵＩ）であるクラウドＵＩ２１２、クラウドＵＩ２１４および／またはクラウドＵＩ２１６にアクセスし、これらのＵＩを介してサブスクリプションオーダーを出してもよい。顧客がオーダーを出したことに応答してクラウドインフラストラクチャシステム２０２が受信したオーダー情報は、顧客と、顧客が申し込むつもりである、クラウドインフラストラクチャシステム２０２によって提供される１つ以上のサービスとを識別する情報を含んでいてもよい。

【００４６】

顧客によってオーダーが出された後で、オーダー情報がクラウドＵＩ２１２、２１４および／または２１６を介して受信される。

【００４７】

動作２３６で、オーダーがオーダーデータベース２１８に格納される。オーダーデータベース２１８は、クラウドインフラストラクチャシステム２０２によって動作され、他のシステム要素とともに動作される、いくつかのデータベースのうちの１つであり得る。

【００４８】

動作２３８で、オーダー情報はオーダー管理モジュール２２０に発送される。場合によっては、オーダー管理モジュール２２０は、オーダーを検証し、検証後にオーダーを予約するといった、オーダーに関連する請求および課金機能を行なうように構成されてもよい。

【００４９】

動作２４０で、オーダーに関する情報がオーダーオーケストレーションモジュール２２２に通信される。オーダーオーケストレーションモジュール２２２は、顧客によって出されたオーダーのためのサービスおよびリソースのプロビジョニングをオーケストレーションするために、オーダー情報を利用してもよい。場合によっては、オーダーオーケストレーションモジュール２２２は、オーダープロビジョニングモジュール２２４のサービスを使用して、申し込まれたサービスをサポートするようにリソースのプロビジョニングをオーケストレーションしてもよい。

【００５０】

ある実施形態では、オーダーオーケストレーションモジュール２２２は、各オーダーに関連付けられたビジネスプロセスの管理を可能にし、オーダーがプロビジョニングに進むべきか否かを判断するためにビジネス論理を適用する。動作２４２で、新規サブスクリプションのオーダーを受信すると、オーダーオーケストレーションモジュール２２２は、リソースを割当ててサブスクリプションオーダーを遂行するために必要とされるリソースを構成するようにという要求を、オーダープロビジョニングモジュール２２４に送信する。オーダープロビジョニングモジュール２２４は、顧客によってオーダーされたサービスのためのリソースの割当てを可能にする。オーダープロビジョニングモジュール２２４は、クラウドインフラストラクチャシステム２０２によって提供されるクラウドサービスと、要求されたサービスを提供するためのリソースをプロビジョニングするために使用される物理的実装層との間の抽象化のレベルを提供する。オーダーオーケストレーションモジュール２２２はこのため、サービスおよびリソースが実際にオンザフライでプロビジョニングされるか否か、または予めプロビジョニングされて要求時にのみ割当てられるか否かといった実装詳細から切り離されてもよい。

【００５１】
動作２４４で、サービスおよびリソースが一旦プロビジョニングされると、提供されるサービスの通知が、クラウドインフラストラクチャシステム２０２のオーダープロビジョニングモジュール２２４によって、クライアント装置２０４、２０６および／または２０８上の顧客に送信されてもよい。
【００５２】
動作２４６で、顧客のサブスクリプションオーダーが、オーダー管理および監視モジュール２２６によって管理され、追跡されてもよい。場合によっては、オーダー管理および監視モジュール２２６は、使用されるストレージの量、転送されるデータの量、ユーザの数、システムアップタイムおよびシステムダウンタイムの量といった、サブスクリプションオーダーにおけるサービスについての使用統計を収集するように構成されてもよい。
【００５３】
ある実施形態では、クラウドインフラストラクチャシステム２０２は、アイデンティティ管理モジュール２２８を含んでいてもよい。アイデンティティ管理モジュール２２８は、クラウドインフラストラクチャシステム２０２においてアクセス管理および認証サービスなどのアイデンティティサービスを提供するように構成されてもよい。いくつかの実施形態では、アイデンティティ管理モジュール２２８は、クラウドインフラストラクチャシステム２０２によって提供されるサービスを利用したい顧客についての情報を制御してもよい。そのような情報は、そのような顧客のアイデンティティを認証する情報と、さまざまなシステムリソース（たとえば、ファイル、ディレクトリ、アプリケーション、通信ポート、メモリセグメントなど）に対してそれらの顧客がどのアクションを行なうことが認可されているかを記述する情報とを含み得る。アイデンティティ管理モジュール２２８はまた、各顧客についての記述的情報と、その記述的情報が誰によってどのようにアクセスされ、修正され得るかについての記述的情報との管理を含んでいてもよい。
【００５４】
図３は、この発明の実施形態が実現され得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。システム３００は、上述のコンピュータシステムのうちのいずれかを実現するために使用されてもよい。図に示すように、コンピュータシステム３００は、バスサブシステム３０２を介して多くの周辺サブシステムと通信する処理部３０４を含む。これらの周辺サブシステムは、処理加速部３０６と、Ｉ／Ｏサブシステム３０８と、記憶サブシステム３１８と、通信サブシステム３２４とを含んでいてもよい。記憶サブシステム３１８は、有形のコンピュータ読取可能記憶媒体３２２と、システムメモリ３１０とを含む。
【００５５】
バスサブシステム３０２は、コンピュータシステム３００のさまざまなコンポーネントおよびサブシステムを意図されるように互いに通信させるためのメカニズムを提供する。バスサブシステム３０２は単一のバスとして概略的に図示されているが、バスサブシステムの代替的な実施形態は複数のバスを利用してもよい。バスサブシステム３０２は、さまざまなバスアーキテクチャのうち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のうちのいずれかであってもよい。たとえば、そのようなアーキテクチャは、ＩＥＥＥ　Ｐ１３８６．１規格で製造されるメザニンバスとして実現可能な、産業標準アーキテクチャ（Industry Standard Architecture：ＩＳＡ）バス、マイクロチャネルアーキテクチャ（Micro Channel Architecture：ＭＣＡ）バス、強化ＩＳＡ（ＥＩＳＡ）バス、ビデオエレクトロニクス標準組織（Video Electronics 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（Peripheral Component Interconnect：ＰＣＩ）バスを含んでいてもよい。
【００５６】
１つ以上の集積回路（たとえば、従来のマイクロプロセッサまたはマイクロコントローラ）として実現され得る処理部３０４は、コンピュータシステム３００の動作を制御する

。処理部３０４には、１つ以上のプロセッサが含まれていてもよい。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んでいてもよい。ある実施形態では、処理部３０４は、各処理部にシングルまたはマルチコアプロセッサが含まれた、１つ以上の独立した処理部３３２および／または３３４として実現されてもよい。他の実施形態では、処理部３０４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集積することによって形成されるクアッドコア処理部として実現されてもよい。

【００５７】

さまざまな実施形態では、処理部３０４は、プログラムコードに応答してさまざまなプログラムを実行でき、同時に実行される複数のプログラムまたはプロセスを維持できる。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うちのいくつかまたはすべては、プロセッサ３０４に、および／または記憶サブシステム３１８にあり得る。好適なプログラミングを通して、プロセッサ３０４は、上述のさまざまな機能性を提供できる。コンピュータシステム３００は加えて処理加速部３０６を含んでいてもよく、それは、デジタル信号プロセッサ（digital signal processor：ＤＳＰ）、専用プロセッサなどを含み得る。

【００５８】

Ｉ／Ｏサブシステム３０８は、ユーザインターフェイス入力装置と、ユーザインターフェイス出力装置とを含んでいてもよい。ユーザインターフェイス入力装置は、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装置、ディスプレイに組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付き音声入力装置、マイクロホン、および他のタイプの入力装置を含んでいてもよい。ユーザインターフェイス入力装置は、たとえば、ジェスチャーおよび口頭コマンドを使用したナチュラルユーザインターフェイスを通して、マイクロソフトＸｂｏｘ（登録商標）３６０ゲームコントローラなどの入力装置をユーザが制御し、それとやりとりすることを可能にする、マイクロソフトＫｉｎｅｃｔ（登録商標）運動センサなどの運動感知および／またはジェスチャー認識装置を含んでいてもよい。ユーザインターフェイス入力装置はまた、ユーザから目の活動（たとえば、写真撮影中および／またはメニュー選択中の「まばたき」）を検出し、アイジェスチャーを入力装置（たとえば、グーグル・グラス（登録商標））への入力として変換する、グーグル・グラス（登録商標）まばたき検出器などのアイジェスチャー認識装置を含んでいてもよい。加えて、ユーザインターフェイス入力装置は、ユーザが音声コマンドを通して音声認識システム（たとえば、Ｓｉｒｉ（登録商標）ナビゲータ）とやりとりできるようにする音声認識感知装置を含んでいてもよい。

【００５９】

ユーザインターフェイス入力装置はまた、３次元（３Ｄ）マウス、ジョイスティックまたはポインティングスティック、ゲームパッドおよびグラフィックタブレット、ならびに、スピーカ、デジタルカメラ、デジタルビデオカメラ、携帯型メディアプレイヤー、ウェブカメラ、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、レーザー測距器、および視線追跡装置などの音声／視覚装置を、何ら限定されることなく含んでいてもよい。加えて、ユーザインターフェイス入力装置は、たとえば、コンピュータ断層撮影装置、磁気共鳴撮像装置、ポジトロン放出断層撮影装置、医療用超音波検査装置などの医療用撮像入力装置を含んでいてもよい。ユーザインターフェイス入力装置はまた、たとえば、ＭＩＤＩキーボード、デジタル楽器などの音声入力装置を含んでいてもよい。

【００６０】

ユーザインターフェイス出力装置は、表示サブシステム、表示灯、または、音声出力装置などの非視覚的ディスプレイを含んでいてもよい。表示サブシステムは、陰極線管（cathode ray tube：ＣＲＴ）、液晶ディスプレイ（liquid crystal display：ＬＣＤ）またはプラズマディスプレイを使用するものなどのフラットパネル装置、投影装置、タッチスクリーンなどであってもよい。一般に、「出力装置」という用語の使用は、コンピュータ

システム３００からユーザまたは他のコンピュータに情報を出力するためのあらゆる可能なタイプの装置およびメカニズムを含むよう意図されている。たとえば、ユーザインターフェイス出力装置は、モニタ、プリンタ、スピーカ、ヘッドホン、自動車ナビゲーションシステム、プロッタ、音声出力装置、およびモデムといった、テキスト、グラフィックスおよび音声／映像情報を視覚的に伝えるさまざまな表示装置を、何ら限定されることなく含んでいてもよい。

【００６１】

コンピュータシステム３００は、現在システムメモリ３１０内に位置するとして図示されたソフトウェア要素を含む記憶サブシステム３１８を含んでいてもよい。システムメモリ３１０は、処理部３０４上でロード可能および実行可能なプログラム命令と、これらのプログラムの実行中に生成されたデータとを格納してもよい。

【００６２】

コンピュータシステム３００の構成およびタイプに依存して、システムメモリ３１０は揮発性（ランダムアクセスメモリ（random access memory：ＲＡＭ）など）であってもよく、および／または不揮発性（読出専用メモリ（read-only memory：ＲＯＭ）、フラッシュメモリなど）であってもよい。ＲＡＭは典型的には、処理部３０４に直ちにアクセス可能であり、および／または処理部３０４によって現在動作および実行中のデータおよび／またはプログラムモジュールを含む。いくつかの実現化例では、システムメモリ３１０は、スタティックランダムアクセスメモリ（static random access memory：ＳＲＡＭ）またはダイナミックランダムアクセスメモリ（dynamic random access memory：ＤＲＡＭ）などの複数の異なるタイプのメモリを含んでいてもよい。いくつかの実現化例では、起動中などにコンピュータシステム３００内の要素間で情報を転送するのに役立つ基本ルーチンを含む基本入力／出力システム（basic input/output system：ＢＩＯＳ）が、典型的にはＲＯＭに格納されていてもよい。限定のためではなく例として、システムメモリ３１０はまた、クライアントアプリケーション、ウェブブラウザ、中央層アプリケーション、リレーショナルデータベース管理システム（relational database management system：ＲＤＢＭＳ）などを含み得るアプリケーションプログラム３１２と、プログラムデータ３１４と、オペレーティングシステム３１６とを示す。例として、オペレーティングシステム３１６は、マイクロソフト・ウィンドウズ（登録商標）、アップル・マッキントッシュ（登録商標）、および／またはＬｉｎｕｘオペレーティングシステムのさまざまなバージョン、商業的に入手可能なさまざまなＵＮＩＸ（登録商標）またはＵＮＩＸ様オペレーティングシステム（さまざまなＧＮＵ／Ｌｉｎｕｘオペレーティングシステム、グーグル・クローム（登録商標）ＯＳなどを何ら限定されることなく含む）、および／または、ｉＯＳ、ウィンドウズ（登録商標）フォン、アンドロイド（登録商標）ＯＳ、ブラックベリー（登録商標）１０ＯＳ、パーム（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んでいてもよい。

【００６３】

記憶サブシステム３１８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のコンピュータ読取可能記憶媒体を提供してもよい。プロセッサによって実行されると上述の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）が、記憶サブシステム３１８に格納されてもよい。これらのソフトウェアモジュールまたは命令は、処理部３０４によって実行されてもよい。記憶サブシステム３１８はまた、この発明に従って使用されるデータを格納するためのリポジトリを提供してもよい。

【００６４】

記憶サブシステム３００はまた、コンピュータ読取可能記憶媒体３２２にさらに接続され得るコンピュータ読取可能記憶媒体リーダ３２０を含んでいてもよい。システムメモリ３１０とともに、およびオプションでシステムメモリ３１０と組合わされて、コンピュータ読取可能記憶媒体３２２は、リモート、ローカル、固定および／またはリムーバブルの記憶装置に加えて、コンピュータ読取可能情報を一時的におよび／またはより永続的に含

み、格納し、送信し、検索するための記憶媒体を包括的に表わしてもよい。

【００６５】

コードまたはコードの一部を含むコンピュータ読取可能記憶媒体３２２はまた、情報の格納および／または送信のためのあらゆる方法または技術で実現される揮発性および不揮発性でリムーバブルおよび非リムーバブルの媒体を含むがそれらに限定されない記憶媒体および通信媒体を含む、当該技術分野において公知であるかまたは使用されるあらゆる適切な媒体を含み得る。これは、ＲＡＭ、ＲＯＭ、電子的消去可能プログラマブルＲＯＭ（electronically erasable programmable ROM：ＥＥＰＲＯＭ）、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（digital versatile disk：ＤＶＤ）また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または他の磁気記憶装置、もしくは他の有形のコンピュータ読取可能媒体といった、非一時的で有形のコンピュータ読取可能記憶媒体を含み得る。これは、所望の情報を送信するために使用可能であり、コンピューティングシステム３００によってアクセスされ得るデータ信号、データ送信、または任意の他の媒体といった、非有形のコンピュータ読取可能媒体も含み得る。

【００６６】

例として、コンピュータ読取可能記憶媒体３２２は、非リムーバブルで不揮発性の磁気媒体から読出し、またはそれに書込むハードディスクドライブ、リムーバブルで不揮発性の磁気ディスクから読出し、またはそれに書込む磁気ディスクドライブ、ならびに、ＣＤＲＯＭ、ＤＶＤ、およびＢｌｕ－Ｒａｙ（登録商標）ディスク、または他の光学媒体といった、リムーバブルで不揮発性の光ディスクから読出し、またはそれに書込む光ディスクドライブを含んでいてもよい。コンピュータ読取可能記憶媒体３２２は、Ｚｉｐ（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス（universal serial bus：ＵＳＢ）フラッシュドライブ、セキュアデジタル（secure digitalＳＤ）カード、ＤＶＤディスク、デジタルビデオテープなどを含んでいてもよいが、それらに限定されない。コンピュータ読取可能記憶媒体３２２はまた、フラッシュメモリベースのソリッドステートドライブ（solid-state drive：ＳＳＤ）、企業フラッシュドライブ、ソリッドステートＲＯＭといった、不揮発性メモリに基づいたＳＳＤ、ソリッドステートＲＡＭ、ダイナミックＲＡＭ、スタティックＲＡＭ、ＤＲＡＭベースのＳＳＤ、磁気抵抗ＲＡＭ（ＭＲＡＭ）ＳＳＤといった、揮発性メモリに基づいたＳＳＤ、および、ＤＲＡＭベースのＳＳＤとフラッシュメモリベースのＳＳＤとの組合せを使用するハイブリッドＳＳＤを含んでいてもよい。ディスクドライブおよびそれらの関連付けられたコンピュータ読取可能媒体は、コンピュータ読取可能命令、データ構造、プログラムモジュールおよび他のデータの不揮発性ストレージをコンピュータシステム３００に提供してもよい。

【００６７】

通信サブシステム３２４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イスを提供する。通信サブシステム３２４は、コンピュータシステム３００とは別のシステムからデータを受信し、別のシステムにデータを送信するためのインターフェイスとして機能する。たとえば、通信サブシステム３２４は、コンピュータシステム３００がインターネットを介して１つ以上の装置に接続できるようにしてもよい。いくつかの実施形態では、通信サブシステム３２４は、（たとえば、３Ｇ、４Ｇ、またはＥＤＧＥ（enhanced data rates for global evolution：エンハンスト・データレート・フォー・グローバル・エボリューション）、ＷｉＦｉ（ＩＥＥＥ８０２．１１ファミリー規格）、または他の移動通信技術、またはそれらの任意の組合せといった携帯電話技術、高度なデータネットワーク技術を使用した）無線音声および／またはデータネットワークにアクセスするための無線周波数（radio frequency：ＲＦ）トランシーバコンポーネント、全地球測位システム（global positioning system：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では、通信サブシステム３２４は、無線インターフェイスに加えて、またはその代わりに、有線ネットワーク接続（たとえば、イーサネット）を提供できる。

【００６８】
いくつかの実施形態では、通信サブシステム３２４はまた、コンピュータシステム３００を使用し得る１人以上のユーザのために、構造化および／または非構造化データフィード３２６、イベントストリーム３２８、イベント更新３３０などのフォームを有した入力通信を受信してもよい。
【００６９】
例として、通信サブシステム３２４は、ツイッター（登録商標）フィード、フェースブック（登録商標）更新、リッチ・サイト・サマリー（Rich Site Summary：ＲＳＳ）フィードなどのウェブフィード、および／または１つ以上の第三者情報源からのリアルタイム更新といった、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のデータフィード３２６をリアルタイムで受信するように構成されてもよい。
【００７０】
加えて、通信サブシステム３２４はまた、リアルタイムイベントのイベントストリーム３２８および／またはイベント更新３３０を含み得る、明確な終わりがなく本質的に連続的または無限であり得る連続データストリームの形をしたデータを受信するように構成されてもよい。連続データを生成するアプリケーションの例は、たとえば、センサデータアプリケーション、金融ティッカー、ネットワーク性能測定ツール（たとえば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム分析ツール、自動車交通監視などを含んでいてもよい。
【００７１】
通信サブシステム３２４はまた、構造化および／または非構造化データフィード３２６、イベントストリーム３２８、イベント更新３３０などを、コンピュータシステム３００に結合された１つ以上のストリーミングデータソースコンピュータと通信し得る１つ以上のデータベースに出力するように構成されてもよい。
【００７２】
コンピュータシステム３００は、ハンドヘルド携帯装置（たとえば、ｉＰｈｏｎｅ（登録商標）携帯電話、ｉＰａｄ（登録商標）コンピューティングタブレット、ＰＤＡ）、ウェアラブル装置（たとえば、グーグル・グラス（登録商標）頭部装着型ディスプレイ）、ＰＣ、ワークステーション、メインフレーム、キオスク、サーバラック、または任意の他のデータ処理システムを含む、さまざまなタイプのうちの１つであり得る。
【００７３】
コンピュータおよびネットワークの絶えず変化する性質により、図に示すコンピュータシステム３００の説明は、単に特定の一例として意図される。図に示すシステムよりも多い、または少ないコンポーネントを有する多くの他の構成が可能である。たとえば、カスタマイズされたハードウェアも使用されてもよく、および／または、特定の要素が、ハードウェア、ファームウェア、ソフトウェア（アプレットを含む）、または組合せで実現されてもよい。また、ネットワーク入力／出力装置などの他のコンピューティング装置への接続が採用されてもよい。ここに提供される開示および教示に基づいて、当業者であれば、さまざまな実施形態を実現するための他のやり方および／または方法を理解するであろう。
【００７４】
上に紹介されたように、この発明の実施形態は、コンピュータネットワーク間で送信されるメッセージを処理するための手法を提供する。より特定的には、ある実施形態は、さまざまなタイプのウェブサービス、アプリケーション、および他のウェブコンテンツに対する要求および応答といったメッセージを、複数のコンピュータネットワーク間で送信するための手法を提供する。物理的または論理的サブネットワーク内に実装されたプロキシサーバといった、１つ以上の中間装置またはアプリケーションが、通信エンドポイント間でメッセージを受信し、処理し、送信してもよい。いくつかの実施形態では、プロキシサーバは、内部ネットワークにおけるエンドポイントから外部システムにおけるエンドポイントに送信されたメッセージを受信してもよく、または、その逆も同様である。メッセー

ジは、メッセージの意図された宛先を判断するために、および／または、メッセージを処理する際にプロキシサーバがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかを判断するために、分析されてもよい。プロキシサーバはまた、特定のメッセージを処理するために使用されるエンドツーエンドポリシーモデルといった、メッセージのための予め定められた処理フローにおける現在点を判断してもよい。メッセージの分析および予め定められた処理フローにおける現在点に基づいて、プロキシサーバは、メッセージに適用されるべき１つ以上のポリシーを選択してもよい。そのようなポリシーは、たとえば、メッセージを認証する、セキュリティトークン仲介およびキー管理を提供する、プロトコルおよびペイロード仲介を行なう、装置ベースのセキュリティを行なう、非武装ゾーン（ＤＭＺ）脅威保護をサポートする、などのためのセキュリティポリシーおよび他の通信管理ポリシーを含んでいてもよい。メッセージに適用されるべき特定のポリシーを選択した後で、プロキシサーバは、ポリシーに従ってメッセージを処理し、メッセージをそれらの意図された宛先に発送してもよい。

【００７５】

図４は、さまざまなコンピュータネットワークにおけるコンピューティング装置および／またはシステム間でメッセージを処理して送信するためのプロキシサーバ４２０を含むコンピューティング環境４００のコンポーネントを示すブロック図である。この例に示すコンピューティング環境４００は、ウェブアプリケーションおよびウェブサービスといったコンピューティングリソースへのアクセスをさまざまなクライアント装置に提供するように設計された高レベルコンピュータアーキテクチャに対応していてもよい。さまざまな実施形態では、コンピューティング環境４００は、小さく単純なコンピューティングシステムから、大きく非常に複雑なシステムに及ぶ場合があり、当該システムは、さまざまな組織のコンピューティング需要をサポートするために他のそのようなシステムと統合するように設計されたハードウェア、ソフトウェア、およびネットワークコンポーネントを含む。コンピューティング環境４００は、多層コンピュータアーキテクチャとして実現されてもよく、それはウェブベースの、および／またはクラウドベースの実装を含んでいてもよく、そこでは、さまざまなエンドポイント装置（たとえば、ユーザ装置４１０、ウェブアプリケーションまたはウェブサービスプロバイダ４３０など）が、１つ以上の中間層システムを介してやりとりする。加えて、コンピューティング環境４００に示す各コンポーネントは、ハードウェア、ソフトウェア、および／またはネットワークコンポーネントのさまざまな組合せを含む、個々のコンピュータシステムとして実装されてもよい。他の場合、コンピューティング環境４００に示す複数のコンポーネントは、組合わせたコンピュータシステムで動作する論理的サブコンポーネント（たとえば、コンピュータ読取可能媒体上で具現化されたソフトウェアアプリケーションなど）として実装されてもよい。

【００７６】

図４に示すように、コンピューティング環境４００は、クライアント装置４１０が、さまざまな通信ネットワーク４１５、ファイアウォール４３５、プロキシサーバ４２０、および／または他の中間装置を介して、１つ以上のバックエンドウェブアプリケーションまたはウェブサービス４３０に要求を送信し得る、クライアント－サーバシステムに対応していてもよい。ウェブアプリケーションまたはサービス４３０は、簡易オブジェクトアクセスプロトコル（Simple Object Access protocol：ＳＯＡＰ）ウェブサービスまたはＡＰＩ、レプリゼンテーショナル・ステート・トランスファー（ＲＥＳＴ）ウェブサービスまたはＡＰＩ、および／または、ハイパーテキスト転送プロトコル（ＨＴＴＰ）またはＨＴＴＰセキュアプロトコルを介して公開されたウェブコンテンツを何ら限定されることなく含む、さまざまなシステム４３０によって公開された任意のアプリケーションプログラムインターフェイス（application programming interface：ＡＰＩ）、サービス、アプリケーション、および任意の他の情報資産を含んでいてもよい。そのような場合、プロキシサーバ４２０は、クライアント装置４１０とバックエンドサービス／アプリケーション４３０との間にセキュリティ層を提供するリバースプロキシサーバとして作用してもよい。リバースプロキシとして作用する場合、プロキシサーバ４２０は、バックエンドサービ

ス／アプリケーション４３０のための中央アクセスポイントを、バックエンドサービス／アプリケーション４３０に関連付けられたさまざまなセキュリティおよび管理ポリシーのサービス仮想化および実施とともに提供してもよい。リバースプロキシとして作用する場合、プロキシサーバ４２０は、これらのバックエンドサービス／アプリケーション４３０を仮想化して不明瞭にしながら、バックエンドサービス／アプリケーション４３０を公開してもよい。たとえば、プロキシサーバ４２０は、信頼できないネットワーク上のクライアント装置４１０が基盤のバックエンドサービス／アプリケーション４３０を読み取らないように、またはバックエンドサービス／アプリケーション４３０についての知識を持たないように、仮想ユニフォームリソースロケータ（uniform resource locator：ＵＲＬ）のみを公開してもよい。

【００７７】

それに加えて、またはそれに代えて、コンピューティング環境４００は、逆方向に送信された要求－応答のためのクライアント－サーバシステムに対応していてもよい。たとえば、ウェブサービス／アプリケーション４３０と同じ内部コンピュータネットワーク４６０内で動作するクライアント装置４４０が、プロキシサーバ４２０およびファイアウォール４３５を超えて、さまざまな外部コンピュータシステムおよびネットワーク上で動作するウェブサービスまたはアプリケーション４５０に要求を送信してもよい。そのような場合、プロキシサーバ４２０は、内部ネットワーク４６０内のクライアント装置４４０と外部ネットワーク上のバックエンドサービス／アプリケーション４５０との間にセキュリティ層を提供するフォワードプロキシサーバとしても作用してもよい。リバースプロキシ動作と同様に、フォワードプロキシ動作における通信は、ＳＯＡＰウェブサービス、ＲＥＳＴウェブサービス、ＨＴＴＰ／ＨＴＴＰＳウェブコンテンツなどへの要求、およびそれらからの応答を含んでいてもよい。プロキシサーバ４２０がフォワードプロキシサーバとして動作している場合、内部ネットワーク内のクライアント装置４４０は、バックエンドサービス／アプリケーション４５０について知っているかもしれず、それらのサービス／アプリケーション４５０は、クライアント側に構成されたプロキシサーバ４２０から直接送信を受信するかもしれない。そのような場合、プロキシサーバ４２０は、任意のセキュリティまたは通信管理ポリシーを使用して、フォワードプロキシユニフォームリソース識別子（uniform resource identifier：ＵＲＩ）エンドポイントのためのセキュリティを提供してもよい。

【００７８】

フォワードプロキシモードまたはリバースプロキシモードのいずれであっても、プロキシサーバ４２０は、Kerberos Kinitベースの認証、Kerberos Pkinitベースの認証、オープン・スタンダード・フォー・オーソライゼーション・プロトコル・バージョン２．０（open standard for authorization protocol version 2.0：ＯＡｕｔｈ２）ベースの認証、ＴＬＰベースの認証といったさまざまなセキュリティおよび認証特徴をサポートし、単純で保護されたＧＳＳＡＰＩネゴシエーションメカニズム（Simple and Protected GSSAPI Negotiation Mechanism：ＳＰＮＥＧＯ）トークン、ＷＩＮＤＯＷＳ（登録商標）ＮＴＬＡＮマネージャ（WINDOWS NT LAN Manager：ＮＴＬＭ）トークン、セキュリティアサーションマークアップ言語（Security Assertion Markup Language：ＳＡＭＬ）トークンなどを使用してバックエンドサービスのセッショントークンおよび／またはチャレンジベースの認証を作成する。

【００７９】

クライアント装置４１０および４４０は、図１～３の例示的なコンピューティングシステムにおける上述のハードウェア、ソフトウェア、およびネットワーキングコンポーネントのうちのいくつかまたはすべてを含む、デスクトップまたはラップトップコンピュータ、モバイル装置、および他のさまざまなコンピューティング装置／システムを含んでいてもよい。いくつかの実施形態では、クライアント装置４１０および４４０は、バックエンドウェブサービス／アプリケーション４３０および４５０からデータを要求して受信するように構成された１つ以上のクライアントソフトウェアアプリケーション（たとえばウェ

ブブラウザ）を含んでいてもよい。クライアント装置４１０および４４０はまた、ネットワークインターフェイス、セキュリティおよび認証能力、ならびに、ライブコンテンツを受信してそれをユーザにリアルタイムで（またはほぼリアルタイムで）提供するコンテンツキャッシング能力を確立するために、必要なハードウェアおよびソフトウェアコンポーネントを含んでいてもよい。

【００８０】

通信ネットワーク４１５は、ここに説明されるコンピュータネットワークおよび他の通信ネットワークの任意の組合せを含んでいてもよい。たとえば、ネットワーク４１５は、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（wide area network：ＷＡＮ）（たとえばインターネット）、およびさまざまな無線通信ネットワークといった、ＴＣＰ／ＩＰ（伝送制御プロトコル／インターネットプロトコル）ネットワークを含んでいてもよい。加えて、通信ネットワーク４１５は、バックエンドアプリケーション／サービス４３０からクライアント装置４１０を分離する多くの異なる物理的および論理的ネットワークの組合せを表わしてもよい、ということが理解されるべきである。１つ以上のファイアウォール４３５に加えて、ウェブサーバ、認証サーバなどのさまざまなサーバ、および／または、ファイアウォール、ルータ、ゲートウェイ、ロードバランサなどの特殊なネットワーキングコンポーネントが、クライアント装置４１０とバックエンドアプリケーション／サービス４３０との通信を容易にしてもよい。

【００８１】

以下に説明されるように、プロキシサーバ４２０は、隔てられたコンピュータシステム（たとえばプロキシコンピュータサーバ）として、または、特殊なハードウェア、ソフトウェア、およびネットワークコンポーネントを含む、コンピュータが複数のコンピューティングシステムの組合せとして実装されてもよい。それに代えて、またはそれに加えて、プロキシサーバ４２０は、信頼できるネットワーク４６０内のネットワーク装置（たとえば、ウェブサーバまたはファイアウォール）またはコンピュータサーバ内で実行されるプロキシサーバソフトウェアアプリケーションであってもよい。このため、プロキシサーバ４２０は、内部コンピュータネットワーク４６０の物理的サブネットワークまたは論理的サブネットワーク４６５に存在していてもよく、いずれの場合も、信頼できる内部ネットワーク上のクライアント／サーバと、信頼できない外部ネットワーク上のクライアント／サーバとの間の仲介主体として作用してもよい。加えて、プロキシサーバ４２０内のコンポーネント４２１～４２８の各々は、プロキシサーバ４２０と通信するように構成された別個のコンピューティングシステムとして実装されてもよく、または、プロキシサーバ４２０と同じコンピュータサーバ内に統合された論理的サブコンポーネントとして動作してもよい。いずれの場合も、各コンポーネント４２１～４２８は、ここに説明される手法を行なうために、特殊なハードウェア、ソフトウェア、ネットワーク、およびメモリサブシステムを使用して実装されてもよい。

【００８２】

この例では、プロキシサーバ４２０は、外部クライアント装置４１０から通信ネットワーク４１５および／またはファイアウォール４３５を介してメッセージを受信するように構成されたロードバランサ４２２を含む。いくつかの実施形態では、ロードバランサ４２２は、任意の外部ネットワークからバックエンドサービス／アプリケーション４３０へのすべてのＴＣＰ、ＵＤＰ、ＨＴＴＰ、およびＨＴＴＰＳトラフィックのためのエントリポイントであってもよい。ロードバランサ４２２はまた、バックエンドサーバと通信するように、および応答をクライアント装置４１０に送信するように構成されてもよい。メッセージを受信して構文解析した後で、ロードバランサ４２２は、（たとえば、Ｊａｖａネーティブインターフェイス（Java Native Interface：ＪＮＩ）または．ＮＥＴプログラミングフレームワークなどを介して）メッセージを適切なウェブサービスフレームワークに送信してもよい。たとえば、クライアント装置からプロキシサーバ４２０で受信されたＳＯＡＰ要求は、ＳＯＡＰウェブサービスフレームワーク４２１に送信され、ＲＥＳＴ要求は、ＲＥＳＴウェブサービスフレームワーク４２３に送信されてもよい。ウェブコンテン

ツ要求は、要求を構文解析し、ＵＲＬ仮想化コンポーネントまたはサービスといったさまざまなコンポーネントに送信することによって同様に扱われてもよい。これらのウェブサービスおよびコンポーネントはまた、ＳＯＡＰからＲＥＳＴへの、およびＲＥＳＴからＳＯＡＰへの、ならびに、JavaScript（登録商標）オブジェクト表記法（JavaScript Object Notation：ＪＳＯＮ）からＸＭＬへの、またはＪＳＯＮからＳＯＡＰへの、およびその逆のメッセージ変換といったプロトコル変換を行なうように構成されてもよい。

【００８３】

メッセージスロットリングシステム（またはメッセージスロットリングサブコンポーネント）４２４は、クライアント装置４１０および／またはバックエンドサービス／アプリケーション４３０から受信されたネットワークトラフィックを監視するように構成されてもよい。メッセージスロットリングシステム４２４は、特定のクライアント装置４１０および／または特定のウェブサービスまたはアプリケーション４３０のための設定可能なメッセージレート制限を有していてもよい。メッセージスロットリングシステム４２４は、特定されたクライアント４１０への／からの、または特定されたウェブサービス／アプリケーション４３０への／からのある数のメッセージを可能にする既存のポリシーを使用してもよい。メッセージの数がメッセージレート制限を超える場合、メッセージスロットリングシステム４２４は、警告送信、ロギング、または今後のメッセージ送信の中断といったアクションを行なうように構成されてもよい。

【００８４】

プロキシサーバ４２０はまた、プロキシサーバ４２０内にさまざまなセキュリティポリシーを実装するように構成されたさまざまなセキュリティシステムまたはコンポーネントを含んでいてもよい。この例では、プロキシサーバ４２０は、キー管理システム４２５と、トークン仲介システム４２６と、認証および認可システム４２７とを含む。プロキシサーバ４２０内のこれらのシステムおよびセキュリティコンポーネントは、クライアント装置４１０からのメッセージを認証する、セキュリティトークン仲介を提供する、ＡＰＩキー管理を行なう、きめの細かい認可および／またはデータ改訂を行なう、機密性および完全性をサポートする、リスクベースの認証を行なう、モバイルクライアント装置４１０のための装置ベースのセキュリティを行なう、非武装ゾーン（ＤＭＺ）脅威保護をサポートする、プロトコルおよびペイロード仲介を行なう、などといったことをしてもよい。たとえば、ロードバランサ４２２および／または認証／認可システム４２７は、サービス妨害（Denial of Service：ＤｏＳ）攻撃を防止し、不正な形式のメッセージを検出してフィルタリングし、ＳＱＬ、ＪａｖａＳｃｒｉｐｔ、および／またはＸＰａｔｈ／ＸＱｕｅｒｙインジェクション攻撃を検出して防止し、悪意のあるコンテンツから保護するためにメッセージ確認を行なう（たとえば、メッセージ添付物内のウィルスを検出する、ＸＭＬおよびＪＳＯＮデータ構造を確認する、形状およびクエリパラメータを確認するなど）ためのサブシステムを含んでいてもよい。トークン仲介システム４２６は、特定されたクライアント装置４１０とバックエンドウェブサービス／アプリケーション４３０との間で認証トークンを変換するように構成されてもよい。セキュリティシステム４２４～４２７はまた、たとえば、複数のバックエンドＡＰＩまたはサービスを集め、自動仲介または合成を行なうことによって、動作のオーケストレーションおよび除去をサポートしてもよい。

【００８５】

加えて、この例では、プロキシサーバ４２０は、メッセージ処理ポリシー４２８のデータストアを含む。メッセージ処理ポリシーは、ＸＭＬ、JavaScript、または他のタイプの実行可能ソフトウェアコンポーネントといったさまざまな形のコンピュータ読取可能媒体に格納されてもよい。以下により詳細に説明されるように、メッセージ処理ポリシー４２８は、プロキシサーバ４２０内でセキュリティポリシーおよび他の通信管理ポリシーを実施するために使用されてもよい。データストア４２８は、個々のメッセージのためのエンドツーエンド処理フロー中のさまざまな段階で検索され、個々のメッセージに適用され得る、個々のメッセージ処理ポリシーを含んでいてもよい。メッセージ処理ポリシーデータストア４２８は、この例に示すようにプロキシサーバ４２０に存在していてもよく、もし

くは、信頼できる内部コンピュータネットワークのバックエンドサーバ、または安全な第三者サーバなどの内部に存在していてもよい。

【００８６】

図４に示すように、プロキシサーバ４２０は、２つ以上のコンピュータネットワーク間、たとえば、ウェブアプリケーション／サービス４３０を提供する第１の信頼できる内部ネットワークと、信頼できないさまざまなクライアント装置４１０が内部ウェブアプリケーション／サービス４３０にアクセスし得る第２の信頼できない外部ネットワーク４１５（たとえばインターネット）との間の、中間ネットワーク装置内に実装されてもよい。いくつかの実施形態では、プロキシサーバ４２０は、内部コンピュータネットワークのためのセキュリティおよび通信管理の初期層を提供するために、内部コンピュータネットワークのサブネットワーク内で動作してもよい。たとえば、安全な内部ネットワーク４６０は、複数のウェブサービス／アプリケーション４３０を、さまざまな他のサーバおよびクライアント装置４４０とともに含んでいてもよい。プロキシサーバ４２０および／または追加の装置は、同じ内部ネットワーク４６０の一部であってもよいが、ファイアウォール４３５ｂによって内部コンピュータネットワークから分離された、内部コンピュータネットワークの物理的サブネットワーク４６５内で動作してもよい。いくつかの例では、プロキシサーバ４２０は、内部コンピュータネットワーク４６０の（物理的サブネットワークではなく）論理的サブネットワーク４６５内で実行されるプロキシサーバアプリケーションとして実装されてもよい。このため、プロキシサーバ４２０は、ファイアウォール４３５ｂおよび／またはバックエンドウェブサービス／アプリケーション４３０のうちの１つ以上と同じコンピューティングシステム上に存在していてもよい。

【００８７】

加えて、いくつかの実施形態では、プロキシサーバ４２０は、信頼できる内部ネットワーク４６０と信頼できない外部ネットワークとの間の非武装ゾーン（ＤＭＺ）ネットワーク内で動作してもよい。ＤＭＺは、クライアント装置４１０および４４０、ならびにバックエンドウェブサービス／アプリケーション４３０および４５０で提供されるエンドポイントセキュリティとは別の、セキュリティおよび通信管理の第１の層を提供する、物理的サブネットワーク４６５として実装されてもよい。図４に示すように、ＤＭＺは、２つのファイアウォール４３５ａと４３５ｂとの間に実装されてもよい。他の実施形態では、ＤＭＺは、単一のファイアウォールを使用して、または、信頼できる内部ネットワーク４６０および信頼できない外部ネットワーク双方からサブネットワーク４６５を物理的にまたは論理的に分離するネットワーク装置の他のさまざまな構成を使用して、実装されてもよい。プロキシサーバ４２０など、ＤＭＺ内のすべてのコンピュータサーバおよび他の装置は、内部ネットワーク４６０内の装置のある特定の部分集合（たとえば、ウェブアプリケーション／サーバ４３０）への限定された接続性を有していてもよい。そのような接続性は、特定のホスト、ポート、プロトコルなどに基づいて限定されてもよい。同様に、信頼できない任意の外部ネットワーク（たとえば、ネットワーク４１５および装置４１０）と通信する際、限定された接続性のポリシーがＤＭＺ内の装置に対して実施されてもよい。ＤＭＺ内でプロキシサーバ４２０を動作させることに加えて、ある実施形態では、ＤＭＺ内でバックエンドウェブサーバ／アプリケーション４３０のうちの１つ以上が動作してもよい。たとえば、外部システムからの攻撃をより受けやすいあるサーバ（たとえば、ウェブサーバ、電子メールサーバ、ドメイン名システム（Domain Name System：ＤＮＳ）サーバなど）を、プロキシサーバ４２０とともにＤＭＺ内に移動させてもよい。

【００８８】

ここで図５を参照して、選択されたメッセージ処理ポリシーを使用してメッセージを受信して処理するためのプロセスを示すフローチャートが示される。以下に説明されるように、このプロセスにおけるステップは、コンピューティング環境４００における１つ以上のコンポーネント、たとえば、プロキシサーバ４２０、およびそこに実装されたさまざまなサブシステム／サブコンポーネントによって行なわれてもよい。加えて、いくつかの実施形態では、このプロセスにおけるあるステップは、クライアント装置４１０、バックエ

ンドウェブサービス／アプリケーション４３０内で、および／または他のさまざまな中間装置によって行なわれてもよい。メッセージを受信して分析すること、メッセージ処理ポリシーを選択すること、およびメッセージを処理することを含む、ここに説明される手法は、上述の特定のシステムおよびハードウェア実装に限定されなくてもよく、ハードウェア、ソフトウェア、およびネットワークコンポーネントの他の組合せを含む他のハードウェアおよびシステム環境内で行なわれてもよい、ということがさらに理解されるべきである。

【００８９】

ステップ５０１で、ネットワークメッセージが、プロキシサーバ４２０といった中間コンピューティングシステムまたはアプリケーションによって受信されてもよい。上述のように、プロキシサーバ４２０は、信頼できる内部ネットワーク４６０と１つ以上の信頼できない外部ネットワークとの間の中間サーバ装置および／またはアプリケーションとして実装されてもよい。したがって、ステップ５０１で受信されたネットワークメッセージは、プロキシサーバ４２０に向けられていないかもしれない。代わりに、プロキシサーバ４２０は、第１のエンドポイント装置（たとえば、クライアント装置４１０）によって送信され、第２のエンドポイント装置（たとえば、バックエンドウェブサービスおよび／またはアプリケーション４３０をホストするコンピュータサーバ）に向けられた、またはその逆のメッセージを遮ってもよい。

【００９０】

いくつかの実施形態では、内部ネットワーク４６０に出入りするすべてのネットワークトラフィックは、プロキシサーバ４２０を通してルーティングされてもよい。他の場合、プロキシサーバ４２０は、特定のタイプまたはプロトコルのネットワークメッセージ、たとえば、クライアント装置４１０および４４０からのＳＯＡＰ、ＲＥＳＴ、またはＵＲＬリソースに対するＨＴＴＰ要求、ならびに、ＳＯＡＰ、ＲＥＳＴ、またはＵＲＬウェブサービス／アプリケーション４３０および４５０からクライアント装置に戻るＨＴＴＰ応答を遮るように構成されてもよい。したがって、ステップ５０１で受信されたネットワークメッセージは、たとえば、および何ら限定されることなく、ＴＣＰメッセージ、ＨＴＴＰまたはＨＴＴＰＳメッセージ、簡易メール転送プロトコル（Simple Mail Transport Protocol：ＳＭＴＰ）、ユーザデータグラムプロトコル（User Datagram Protocol：ＵＤＰ）メッセージ、および／またはＪａｖａメッセージサービス（Java Message Service：ＪＭＳ）メッセージであってもよい。場合によっては、ネットワークメッセージは、クライアント装置４１０からウェブサービス／アプリケーション４３０をホストするバックエンドコンピュータサーバへのＳＯＡＰ、ＲＥＳＴ、またはウェブコンテンツ要求に対応していてもよく、もしくは、クライアント装置４１０からのＳＯＡＰ、ＲＥＳＴ、またはウェブコンテンツ要求に対するバックエンドウェブサービスまたはアプリケーション４３０による応答に対応していてもよい。加えて、ネットワークメッセージは、内部コンピュータネットワーク４６０内で動作するクライアント装置４４０から外部コンピュータネットワーク上で動作するウェブサービス／アプリケーションを提供するコンピュータサーバ４５０へのＳＯＡＰ、ＲＥＳＴ、またはウェブコンテンツ要求に対応していてもよく、もしくは、内部クライアント装置４４０からのＳＯＡＰ、ＲＥＳＴ、またはウェブコンテンツ要求に対する外部ウェブサービスまたはアプリケーション４５０からの応答に対応していてもよい。

【００９１】

ステップ５０２で、プロキシサーバ４２０は、ステップ５０１で受信されたネットワークメッセージを分析して、メッセージの意図された宛先を判断し、また、ネットワークメッセージを処理する際にプロキシサーバ４２０がフォワードプロキシとして作用すべきか（すなわちフォワードプロキシモード）、リバースプロキシとして作用すべきか（すなわちリバースプロキシモード）を判断してもよい。ここに使用されるように、ネットワークメッセージの「意図された宛先」とは、送信装置または送信装置のユーザによって指定されたメッセージの宛先を指してもよい。メッセージの意図された宛先は、メッセージヘッ

ダおよび／またはメッセージ本文の一部を構文解析し、分析することによって判断されてもよい。たとえば、メッセージのユニフォームリソース識別子（ＵＲＩ）、もしくは、ウェブサービスまたはアプリケーションの識別子、および／またはメッセージ本文内の動作識別子が、内部ネットワーク４６０によって提供されるウェブサービス／アプリケーションまたはウェブコンテンツに対応していてもよい。この例では、プロキシサーバ４２０は、メッセージヘッダおよびコンテンツに基づいて、メッセージは内部ネットワーク４６０内の特定のサーバに向けられていると判断してもよい。別の例では、メッセージＵＲＩが信頼できないネットワーク上のリモートサーバに対応している場合、プロキシサーバ４２０は、メッセージの意図された宛先は、内部ネットワーク４６０内の装置ではなく、リモートサーバであると判断してもよい。ソースＩＰアドレスまたはホスト名識別子といった、メッセージの送信元を識別するメッセージ内の情報も、メッセージの意図された宛先を判断するために使用されてもよい。

【００９２】

メッセージの意図された宛先を判断することに加えて、プロキシサーバ４２０は、メッセージを処理する際にプロキシサーバ４２０がフォワードプロキシモードで動作すべきかリバースプロキシモードで動作すべきかを判断するために、メッセージは、クライアント装置４１０または４４０からの要求の一部か、もしくはウェブサービス／アプリケーションサーバ装置４３０または４５０からの応答の一部かを判断してもよい。たとえば、受信されたメッセージがクライアント装置４１０からウェブサービスまたはアプリケーション４３０への要求である場合、意図された宛先は信頼できる内部ネットワーク４６０内にあり、プロキシサーバ４２０はリバースプロキシモードで動作すべきである。対照的に、受信されたメッセージが内部クライアント装置４４０から外部ウェブサービス４５０、ウェブアプリケーション４５０、またはＵＲＬ４５０への要求である場合、意図された宛先は信頼できる内部ネットワークの外部にあり、プロキシサーバ４２０はフォワードプロキシモードで動作すべきである。

【００９３】

他の場合、ステップ５０１で受信されたメッセージは、クライアント装置４１０または４４０からの要求ではないかもしれず、代わりに、以前の要求に対するウェブサーバ４３０または４５０からの応答であるかもしれない。たとえば、受信されたメッセージが、クライアント装置４１０からの要求に対する、信頼できる内部ネットワーク４６０内のウェブサービス／アプリケーション４３０または他のサーバからの応答である場合、元の要求の意図された宛先は信頼できる内部ネットワーク４６０内にあり、プロキシサーバ４２０はリバースプロキシモードで動作すべきである。対照的に、受信されたメッセージが、クライアント装置４４０からの要求に対する、内部ネットワーク４６０の外部のウェブサービス／アプリケーション４５０または他のサーバからの応答である場合、元の要求の意図された宛先は内部ネットワーク４６０の外部にあり、プロキシサーバ４２０はフォワードプロキシモードで動作すべきである。

【００９４】

ステップ５０３で、プロキシサーバ４２０は、ステップ５０１で受信されたメッセージのための予め定められた処理フローにおける現在点を判断してもよい。メッセージ処理フローとは、プロキシサーバ４２０によるクライアント装置４１０または４４０からのメッセージの受信で始まり、プロキシサーバ４２０によるクライアント装置４１０または４４０への応答の送信で終わる、プロキシサーバ４２０によって実行されるべきエンドツーエンドメッセージ処理フローを指してもよい。以下に説明されるように、メッセージのための予め定められた処理フローにおける現在点を判断することは、メッセージに関連付けられたポリシーモデルを識別し、処理モデル内の現在の処理位置を判断することを含んでいてもよい。

【００９５】

いくつかの実施形態では、メッセージのための予め定められたメッセージ処理フローは、ポリシーモデルによって定義されてもよい。ポリシーモデルは、メッセージのエンドツ

ーエンドメッセージ処理フロー中のさまざまな点でメッセージを処理するためにプロキシサーバ４２０によって適用され得る一組のポリシー（たとえば、セキュリティポリシー、通信管理ポリシーなど）を定義するデータを含んでいてもよい。メッセージのエンドツーエンド処理フローを定義するポリシーモデル、および個々のメッセージ処理ポリシーは双方とも、ＸＭＬ、JavaScript、または他のタイプの実行可能ソフトウェアコンポーネントといったさまざまな形のコンピュータ読取可能媒体であってもよい。ポリシーモデルおよび／またはメッセージ処理ポリシーは、プロキシサーバ４２０内に、たとえばデータストア４２８に、または内部ネットワーク４６０内の他のところに格納されてもよい。

【００９６】

上述のように、ポリシーモデルは、プロキシサーバ４２０がメッセージのエンドツーエンド処理フローにおけるさまざまな点でメッセージに適用し得る一組のメッセージ処理ポリシーを定義してもよい。いくつかの実施形態では、ステップ５０３で、プロキシサーバ４２０は、ステップ５０１で受信されたメッセージの特性に依存して、異なるポリシーモデルを適用してもよい。たとえば、プロキシサーバ４２０によって検索され適用される特定のポリシーモデルは、ステップ５０２で行なわれたメッセージの意図された宛先、およびフォワードまたはリバースプロキシモードの判断に依存していてもよい。加えて、プロキシサーバ４２０によって検索され適用されるポリシーモデルは、メッセージを送信するために使用されるネットワークプロトコル、および／または、メッセージの要求タイプまたはクライアントタイプに依存していてもよい。たとえば、ＲＥＳＴ要求、ＳＯＡＰ要求、ウェブコンテンツ（ＵＲＬ）要求などのために、異なるポリシーモデルが使用されてもよい。

【００９７】

図６Ａおよび図６Ｂを簡潔に参照して、ポリシーモデルの２つの例が示されており、それらは双方ともＸＭＬで実現されている。図６Ａは、仮想アプリケーションのための例示的なポリシーモデルを示す。このため、例示的なポリシーモデル６００ａは、リバースプロキシ使用事例についてのメッセージ処理のために検索され、使用されてもよい。対照的に、図６Ｂは、プロキシアプリケーションのための例示的なポリシーモデルを示し、したがって、例示的なポリシーモデル６００ｂは、フォワードプロキシ使用事例についてのメッセージ処理のために検索され、使用されてもよい。これらの例の各々に示すように、ポリシーモデルは、処理フロー内のさまざまな点（「アサーション」とも呼ばれ得る）のタグまたは識別子、および、処理点／アサーションの各々についての１つ以上のポリシー識別子を含んでいてもよい。たとえば、例示的なポリシーモデル６００ａは、要求が受信されると行なわれるべき２つのポリシー（「on-request」タグ内）、メッセージ変換を行なうポリシー（「message-transformation」タグ内）、および、バックエンドウェブサービスが呼び出されると行なわれるべきポリシー（「invoke」タグ内）を識別する。例示的なポリシーモデル６００ｂは、要求が受信されると行なわれるべきポリシー（「on-request」タグ内）、および、バックエンドウェブサービスが呼び出されると行なわれるべきポリシー（「invoke-proxy」タグ内）を識別する。

【００９８】

いくつかの実施形態では、プロキシサーバ４２０は、プロキシアプリケーションについては（すなわち、フォワードプロキシモードでは）サービスレベル（またはＵＲＬレベル）でポリシーを適用してもよく、一方、仮想アプリケーションについては（すなわち、リバースプロキシモードでは）、プロキシサーバ４２０は、サービスレベルおよび／または動作レベル（または方法レベル）でポリシーを適用してもよい。したがって、信頼できる内部ネットワーク４６０内のバックエンドウェブサービス／アプリケーション４３０を呼び出す場合、プロキシサーバ４２０はまず、動作（ＳＯＡＰについて）または方法（ＲＥＳＴおよびＵＲＬについて）を判断してから、ポリシーモデル内で識別されたポリシーを実施できるようになっていてもよい。

【００９９】

ステップ５０１で受信されたメッセージに関連付けられたポリシーモデル（または処理

フローを定義する他のデータ）を識別した後で、プロキシサーバ４２０は、ポリシーまたは処理フローに従って、メッセージ処理における現在点を判断してもよい。メッセージ処理フローにおける現在点は、メッセージ自体の特性によって、および、メッセージの以前の処理に関する以前に格納されたデータに基づいて判断されてもよい。上述のように、予め定められた処理フローは、クライアント装置４１０または４４０による最初の要求から、クライアント装置４１０または４４０に返送された応答までの、メッセージのためのエンドツーエンド処理を適用してもよい。したがって、ステップ５０１で受信されたメッセージが、クライアント装置からの最初の要求であるか、クライアント装置からの追加データ（たとえば、要求に関する認証クレデンシャルまたは追加データ）の送信であるか、バックエンドウェブサービス／アプリケーションからの応答であるか、もしくは、バックエンドサーバまたは装置からの追加データ（たとえば、シングルサインオンまたはトークン翻訳サービスからのデータ）の送信であるかを判断することは、プロキシサーバ４２０が、エンドツーエンドメッセージ処理フロー内のメッセージ処理の現在点を判断することを可能にし得る。加えて、プロキシサーバ４２０は、プロキシサーバ４２０がメッセージに適用すべき次のメッセージ処理ポリシーを判断するために、以前のメッセージ変換、サービスの呼び出し、遭遇した処理エラーの結果といった、メッセージまたは他の関連するメッセージに対して行なわれた以前の処理に関連するデータを格納してもよい。

【０１００】

以下の段落は、メッセージ処理ポリシーが適用され得る、ポリシーモデルまたは他のメッセージ処理フロー内の可能な点（「アサーション」とも呼ばれ得る）のいくつかの例を含む。これらの例は単なる例示であり、網羅的なリストでなくてもよい、ということが理解されるべきである。また、ここに説明されるアサーション名（たとえば、OnRequest、OnInvoke、OnResponse、OnError、MessageTransformationなど）、ならびに、アサーションおよびポリシーに使用されるＸＭＬ構造およびタグ名は、さまざまな他の実施形態において変更されてもよい。

【０１０１】

ステップ５０３でポリシーモデルまたは他の予め定められたメッセージ処理フロー内の現在点を判断する第１の例は、ステップ５０１で受信されたメッセージが外部コンピュータネットワークにおけるクライアント装置４１０からの要求に対応していると判断することを含んでいてもよい。メッセージのエンドツーエンド処理フローの初めにあるこの点は、「OnRequest」アサーションなどと呼ばれてもよい。以下により詳細に説明されるように、OnRequestアサーションは、仮想サービス、プロキシサービス、および／またはウェブアプリケーションを安全にするために適用され得るポリシーへの参照を含んでいてもよい。たとえば、OnRequestアサーションは、外部クライアント装置４１０から受信された新規のウェブサービス／アプリケーション／コンテンツ要求のためにプロキシサーバ４２０が実施すべきセキュリティポリシーを表わすＵＲＩまたは他の識別子を含んでいてもよい。OnRequestアサーションはまた、他のポリシーを参照してもよく、および／または、他のアサーションを含んでいてもよい。場合によっては、OnRequestアサーションは、リバースプロキシモードでのみ動作してもよく、すなわち、外部クライアント装置４１０からの内部ウェブサービス４３０に対する要求のみを扱ってもよい。そのような場合、内部クライアント装置４４０からの外部ウェブリソース４５０に対する要求は、異なるメッセージ処理ポリシーを適用し得る異なるアサーションによって扱われてもよい。

【０１０２】

ステップ５０３で起こり得る現在のメッセージ処理点の別の判断は、外部クライアント装置４１０から要求を受信した後で、プロキシサーバ４２０は内部コンピュータネットワーク４６０におけるバックエンドウェブアプリケーションまたはウェブサービス４３０に要求を送信すべきであると判断することを含んでいてもよい。メッセージのエンドツーエンド処理フロー内のこの点は、「OnInvoke」アサーションなどと呼ばれてもよい。OnRequestアサーションと同様に、いくつかの実施形態では、OnInvokeアサーションは、内部ネットワーク４６０内のバックエンドウェブサービス／アプリケーション４３０を呼び出す

ために最初の要求が外部クライアント装置４１０から受信されたリバースプロキシ使用事例にのみ当てはまり得る。OnInvokeアサーションは、エンドツーエンド処理フローにおけるこの点でプロキシサーバ４２０が実施すべきポリシーを表わすＵＲＩまたは他の識別子を含んでいてもよい。たとえば、複数のＸＭＬ「ポリシーＵＲＩ」ＸＭＬ要素を使用することによって、複数のポリシー識別子（または参照）がOnInvokeアサーション内に含まれてもよい。加えて、OnInvokeアサーションは、クライアントのリソースパターンを使用することから、クライアント詳細を一意的に識別してもよい。OnInvokeアサーションに使用されるクライアントタイプ（たとえば、ＲＥＳＴクライアント、ＳＯＡＰクライアント、ＵＲＬ／ウェブクライアントなど）は、OnInvokeアサーション内に構成された値に基づいて、実行時間にプロキシサーバ４２０によって判断されてもよい。OnInvokeアサーションはまた、他のポリシーを参照してもよく、および／または、他のアサーションを含んでいてもよい。

【０１０３】

現在のメッセージ処理点を判断する別の例は、外部クライアント装置４１０から要求を受信した後で、およびバックエンドウェブサービス／アプリケーション４３０を呼び出した後で、プロキシサーバ４２０は外部クライアント装置４１０に応答を送信すべきであると判断することを含んでいてもよい。メッセージのエンドツーエンド処理フロー内のこの点は、「OnResponse」アサーションなどと呼ばれてもよい。OnRequestおよびOnInvokeアサーションと同様に、いくつかの実施形態では、OnResponseアサーションは、内部ネットワーク４６０内のバックエンドウェブサービス／アプリケーション４３０を呼び出すために最初の要求が外部クライアント装置４１０から受信されたリバースプロキシ使用事例にのみ当てはまり得る。OnResponseアサーションは、エンドツーエンド処理フローにおけるこの点でプロキシサーバ４２０が実施すべきポリシーを表わすＵＲＩまたは他の識別子を含んでいてもよい。複数のポリシー識別子（または参照）がOnResponse内に含まれてもよく、OnResponseアサーションはまた、他のポリシーを参照してもよく、および／または、他のアサーションを含んでいてもよい。

【０１０４】

ステップ５０３で起こり得る現在のメッセージ処理点の別の判断は、プロキシサーバ４２０は内部クライアント装置４４０から外部ウェブサービスまたはアプリケーション４５０に要求を送信すべきであると判断することを含んでいてもよい。メッセージのエンドツーエンド処理フロー内のこの点は、「OnProxyInvoke」アサーションなどと呼ばれてもよい。上述のOnInvokeアサーションの例とは異なり、OnProxyInvokeアサーションは、信頼できない外部ネットワーク内のバックエンドウェブサービス／アプリケーション４５０を呼び出すために最初の要求が内部クライアント装置４４０から受信されたフォワードプロキシ使用事例にのみ当てはまり得る。OnProxyInvokeアサーションは、エンドツーエンド処理フローにおけるこの点でプロキシサーバ４２０が実施すべきポリシーを表わすＵＲＩまたは他の識別子を含んでいてもよい。たとえば、複数のＸＭＬ「ポリシーＵＲＩ」ＸＭＬ要素を使用することによって、複数のポリシー識別子（または参照）がOnProxyInvokeアサーション内に含まれてもよい。OnProxyInvokeアサーションに使用されるクライアントタイプ（たとえば、ＲＥＳＴクライアント、ＳＯＡＰクライアント、ＵＲＬ／ウェブクライアントなど）は、たとえば実行時間引数に基づいて、実行時間にプロキシサーバ４２０によって判断されてもよい。OnProxyInvokeアサーションはまた、他のポリシーを参照してもよく、および／または、他のアサーションを含んでいてもよい。

【０１０５】

現在のメッセージ処理点を判断する別の例は、エンドツーエンド処理フロー中のいずれかの点で、プロキシサーバ４２０はあるメッセージタイプから別のメッセージタイプにメッセージを変換すべきであると判断することを含んでいてもよい。メッセージのエンドツーエンド処理フロー内のこの点は、「MessageTransformation」アサーションなどと呼ばれてもよい。たとえば、プロキシサーバ４２０は、第１のメッセージタイプ（たとえばＲＥＳＴ要求）を有するメッセージを受信し、メッセージを分析して、メッセージは、第２

のメッセージタイプ（たとえばバックＳＯＡＰサービス）のみを受け入れるバックエンドサービスまたはアプリケーションに向けられていると判断してもよい。そのような判断の後で、プロキシサーバ４２０は、メッセージに対して適切なMessageTransformationアサーションを実行してから、変換されたメッセージを意図された宛先に送信してもよい。プロキシサーバ４２０によってサポートされ得る変換ポリシーの例は、ＸＭＬポリシーからJavaScriptオブジェクト表記法（ＪＳＯＮ）ポリシー、およびＪＳＯＮポリシーからＸＭＬポリシー、ＸＭＬポリシーからＳＯＡＰポリシー、およびＳＯＡＰポリシーからＸＭＬポリシー、ならびに、ＪＳＯＮポリシーからＳＯＡＰポリシー、およびＳＯＡＰポリシーからＪＳＯＮポリシーを、何ら限定されることなく含んでいてもよい。他の周知の媒体タイプ間の変換が、さまざまな実施形態においてサポートされてもよい。プロキシサーバ４２０は、バックエンドサービス仮想化の際に適切な変換ポリシーを自動的に添付してもよく、変換は、プロキシサーバ４２０に、またはコンピューティング環境４００における他のところにインストールされた１つ以上の翻訳フレームワークを使用して行なわれてもよい。いくつかの実施形態では、MessageTransformationアサーションはリバースプロキシモードでのみ動作してもよく、すなわち、外部クライアント装置４１０からの内部ウェブリソース４３０に対する要求およびクライアント装置４１０への応答の変換のためにのみサポートされてもよい。他の実施形態では、MessageTransformationアサーションは、フォワードプロキシおよびリバースプロキシ使用事例双方のためにサポートされてもよい。

【０１０６】

現在のメッセージ処理点を判断する別の例は、メッセージのためのエンドツーエンド処理フロー中のいずれかの点でエラーが起こったと判断することを含んでいてもよい。メッセージのエンドツーエンド処理フロー内のこの点は、「OnError」アサーションなどと呼ばれてもよい。メッセージのためのOnErrorアサーションをトリガしている（たとえば、メッセージに関連付けられたOnErrorアサーションで識別された１つ以上のポリシーの実行をトリガしている）エラーは、プロキシサーバ４２０によって行なわれた処理内で起こったエラー、および／または、バックエンドコンピュータサーバまたは装置からプロキシサーバ４２０によって受信されたエラーであってもよい。たとえば、プロキシサーバ４２０は、認可サービス、トークン翻訳サービス、またはバックエンドウェブサービス／アプリケーション４３０または４５０といったメッセージの処理フロー中に呼び出されたバックエンドコンピュータサーバからエラー表示を受信してもよい。加えて、プロキシサーバ４２０は、メッセージ処理タスクを行ないながらエラーを識別または生成してもよく、OnErrorアサーションでポリシーをトリガするメッセージは、メッセージを構文解析または確認する際のエラー、もしくはメッセージ変換ポリシーを実行する際のエラーといった、プロキシサーバ４２０によって行なわれるメッセージ処理内で起こったエラーであってもよい。このため、特定のメッセージ処理ポリシーが適用され得る処理フロー内の点（「アサーション」とも呼ばれる）の以前の例のうちのいくつかとは異なり、OnErrorアサーションは条件付きであってもよい。すなわち、メッセージのエンドツーエンド処理フロー中、プロキシサーバ４２０は、処理中に起こり得るエラーの数およびタイプに依存して、OnErrorアサーションからポリシーを１回、複数回、適用してもよく、または全く適用しなくてもよい。さまざまな異なる実施形態では、OnErrorアサーションは、フォワードプロキシ使用事例、リバースプロキシ使用事例、または双方に適用されてもよい。

【０１０７】

ステップ５０４で、ステップ５０１で受信されたメッセージを処理するための１つ以上の特定のポリシーが、プロキシサーバ４２０によって選択され、検索されてもよい。上述のように、プロキシサーバ４２０によって選択され、メッセージに適用される特定のポリシーは、セキュリティポリシーおよび任意の他のタイプの通信管理ポリシーを含んでいてもよい。たとえば、および何ら限定されることなく、そのようなポリシーは、とりわけ、認証、認可、監査、シングルサインオン、セキュリティポリシー実施、キー管理および分散、安全な通信、安全なデータ格納、および安全なデータ共有に関連する機能を行なってもよい。

【０１０８】
ステップ５０４で、プロキシサーバ４２０によって、まず、メッセージに関連付けられたエンドツーエンド処理フロー（たとえばポリシーモデル）を検索し、次に、ステップ５０３で判断されたエンドツーエンド処理フロー内の現在点（たとえばアサーション）を使用して、エンドツーエンドフローにおける現在点でメッセージに適用されるであろう特定のポリシーを識別することにより、ポリシーが選択されてもよい。たとえば、ステップ５０１で受信されたメッセージが、外部クライアント装置４１０からのウェブサービス／アプリケーション４３０に対する要求である場合、および、例示的なポリシーモデル６００ａがそのようなメッセージのエンドツーエンド処理を制御するために使用される場合、プロキシサーバ４２０は、ポリシーモデル６００ａの「on-request」タグ内で識別された任意のポリシーを検索してもよい。この場合、ポリシーモデル６００ａの「on-request」タグ内には２つのポリシー識別子が見出され、それらは各々、「PolicyReference URI」タグ内に含まれている。このため、この例では、プロキシサーバ４２０はステップ５０４でこれら２つのポリシーを選択して、ステップ５０５でメッセージを処理するために使用してもよい。

【０１０９】
別の例として、ステップ５０１で受信されたメッセージが、内部クライアント装置４４０からの、外部ウェブサービス／アプリケーション４５０にアクセスしたいという要求である場合、および、例示的なポリシーモデル６００ｂがそのようなメッセージのエンドツーエンド処理を制御するために使用される場合、プロキシサーバ４２０は、ポリシーモデル６００ｂの「on-request」タグ内で識別されたポリシーを検索してもよい。それに代えて、「on-request」ポリシーがすでに適用され、プロキシサーバ４２０が外部ウェブサービス／アプリケーション４５０に要求を送信する準備ができている場合、プロキシサーバ４２０は、ポリシーモデル６００ｂの「invoke-proxy」タグ内で識別されたポリシーを検索してもよい。

【０１１０】
ステップ５０５で、プロキシサーバ４２０は、ステップ５０４で選択されたポリシーを使用してメッセージを処理してもよい。上述のように、プロキシサーバ４２０は、メッセージのための予め定められたエンドツーエンド処理フローからＵＲＩまたは他のポリシー識別子を識別することによって、メッセージに適用されるべき適切なポリシーを判断してもよい。例示的なポリシーモデル６００ａおよび６００ｂでは、適用されるべきポリシーのＵＲＩは、エンドツーエンド処理フローにおける現在点に対応するアサーションの「PolicyReference URI」タグ内に見出されてもよい。そのようなポリシーＵＲＩは、ポリシーの格納位置を参照してもよい。他の例では、ポリシー識別子はＵＲＩとして表わされなくてもよく、ＡＰＩまたはサービス識別子、機能名、方法名、および／または動作名などといった他の識別データを含んでいてもよい。いずれにせよ、ポリシー識別子は、メッセージ処理ポリシーのための格納位置または他のアクセス情報を識別してもよい。ポリシー自体は、ＸＭＬ、JavaScript、または他のタイプの実行可能ソフトウェアコンポーネントといったさまざまな形のコンピュータ読取可能媒体に格納されてもよい。

【０１１１】
メッセージ処理ポリシーは、コンピューティング環境４００内のさまざまな異なるサーバまたは装置に位置する、データベースおよび／またはファイルベースの記憶システムといったデータストアに格納されてもよい。たとえば、比較的不変であるかもしれず、安全なデータを有さない、メッセージ変換ポリシー、メッセージスロットリングポリシー、ロードバランシングポリシー、および他のポリシー、といったあるポリシーは、プロキシサーバ４２０内に（たとえば、メッセージ処理ポリシーデータストア４２８内に）局所的に格納されてもよい。しばしば変わり得る、または安全なデータを含み得る、ユーザ認証／認可ポリシー、および他のポリシー、といった他のポリシーは、信頼できる内部コンピュータネットワーク４６０の安全なサーバまたは記憶システム内に格納されてもよい。他の場合、あるポリシーは、外部ネットワークにおける安全な第三者サーバまたはクライアン

ト装置４１０上に格納されてもよい。プロキシサーバ４２０は、ステップ５０５でこれらのさまざまな位置のいずれかからポリシーを検索し、適用するように構成されてもよい。

【０１１２】

ステップ５０５でさまざまなセキュリティポリシーおよび／または他の通信管理ポリシーを使用してメッセージを処理した後で、ステップ５０６で、プロキシサーバ４２０は、処理されたメッセージをその意図された宛先に送信してもよい。上述のように、意図された宛先は、ステップ５０２でメッセージヘッダおよび／またはメッセージ本文の一部を構文解析し、分析することによって判断されてもよい。ウェブサービス／アプリケーション４３０への要求、もしくは内部クライアント装置４４０への応答または他の送信といったメッセージの意図された宛先は、内部ネットワーク４６０内にあってもよい。それに代えて、外部ウェブサービス／アプリケーション４５０への要求、もしくは外部クライアント装置４１０への応答または他の送信といったメッセージの意図された宛先は、外部ネットワーク内にあってもよい。

【０１１３】

上述のように、プロキシサーバ４２０内でメッセージを処理するための特定のポリシーの選択および適用は、そのメッセージのための予め定められたエンドツーエンド処理フローによって、エンドツーエンドフロー内のメッセージのための現在の処理点の判断とともに判断されてもよい。上に紹介されたポリシーモデルは、プロキシサーバ４２０がメッセージのエンドツーエンド処理フローにおけるさまざまな点でメッセージに適用するであろう一組のメッセージ処理ポリシーを定義してもよい。たとえば、例示的なポリシーモデル６００ａおよび６００ｂは、仮想アプリケーション（すなわち、リバースプロキシ使用事例）およびプロキシアプリケーション（すなわち、フォワードプロキシ使用事例）のためのエンドツーエンド処理フローをそれぞれ定義する。これらのポリシーモデルは、メッセージのエンドツーエンド処理フロー内のさまざまな点（またはアサーション）を識別し、識別された各処理点またはアサーションでメッセージに適用されるべき特定のポリシーを含む。

【０１１４】

いくつかの実施形態では、エンドツーエンド処理フローを定義するためのポリシーモデルおよび他の手法は、一組のポリシーテンプレートを使用して作成されてもよい。たとえば、図７Ａ～７Ｄを簡潔に参照して、４つの異なるアサーションに対応する４つの例示的なポリシーテンプレートが示される。図７Ａは、例示的な「On Request」ポリシーテンプレートを示し、図７Ｂは、例示的な「Invoke」ポリシーテンプレートを示し、図７Ｃは、例示的な「Invoke Proxy」ポリシーテンプレートを示し、図７Ｄは、例示的な「On Response」ポリシーテンプレートを示す。図７Ａ～７Ｄにおけるポリシーテンプレートの各々は「PolicyReference URI」タグを含むが、これらのテンプレートではＵＲＩは空のままである。このため、そのようなテンプレートは、ポリシーモデル６００ａおよび６００ｂといったポリシーモデルエンドツーエンド処理フローを作成するために使用されてもよい。たとえば、図７Ａ～７Ｄのテンプレートのうちの１つ以上がコピーされてもよく、適切なポリシーＵＲＩが各テンプレートコピーに挿入されてもよい。カスタマイズされたテンプレートは次に、エンドツーエンド処理フロー中に実行され得るポリシーを定義するために、適切なポリシーモデルに追加されてもよい。

【０１１５】

エンドツーエンド処理フロー中に実行されるべきアサーションおよびポリシーを定義することに加えて、ポリシーモデル（および予め定められたエンドツーエンド処理フローの他の形）は、あるポリシーが行なわれ得る、または行なわれない条件も定義してもよい。いくつかの実施形態では、ポリシーモデルは、ポリシーモデルで参照されるポリシーの各々を行なうための条件を実現するための一組の論理命令を含んでいてもよい。たとえば、ポリシーモデルは、あるポリシーが、あるメッセージタイプ（たとえば、ＳＯＡＰ、ＲＥＳＴ、またはＵＲＬメッセージ）については実行されるべきであるものの、他のメッセージタイプについては実行されるべきではないことをプロキシサーバ４２０に命令する条件

を含んでいてもよい。加えて、上述のように、ポリシーモデルは、場合によっては、サービス／アプリケーションレベルで、および／または動作／方法レベルでポリシーを選択的に適用してもよく、このため、特定のポリシーの適用は、呼び出されているバックエンドウェブアプリケーション／サービス４３０にだけでなく、アプリケーション／サービス４３０内でコールされている特定の動作または方法にも依存していてもよい。さまざまな追加の実施形態では、いくつかのポリシーモデルは、あるポリシーが、あるユーザについては実行されるべきであるものの、他のユーザについては実行されるべきではないこと、あるクライアント装置タイプについては実行されるべきであるものの、他のクライアント装置タイプについては実行されるべきではないこと、あるバックエンドウェブサービス／アプリケーションについては実行されるべきであるものの、他のバックエンドウェブサービス／アプリケーションについては実行されるべきではないこと、および／またはメッセージに関連する任意の他の特性をプロキシサーバ４２０に命令する条件を含んでいてもよい。

【０１１６】

ここで図８を参照して、外部クライアント装置４１０から内部ＳＯＡＰウェブサービス４３０に送信されたＲＥＳＴ要求のエンドツーエンド処理フローの例示的な図を示す。この例の処理フローの実行は、プロキシサーバ４２０によって、上述のようなコンピューティング環境４００におけるさまざまな他のコンポーネントとともに行なわれてもよい。この例では、最初のメッセージは、クライアント装置４１０から内部コンピュータネットワーク４６０におけるバックエンドウェブサービス４３０に向けられたＲＥＳＴ要求であり、このため、プロキシサーバ４２０はリバースプロキシモードで動作してもよい。

【０１１７】

上述のように、この例のエンドツーエンド処理フロー図８００は、特定の処理点（またはアサーション）と、エンドツーエンド処理フロー中の各処理点でプロキシサーバ４２０によって実行されるべき特定のポリシーとを定義する、予め定められたポリシーモデルによって制御されてもよい。この例では、ステップ８０１で、ＲＥＳＴ要求がクライアント装置４１０から受信される。ステップ８０２で、プロキシサーバ４２０は、この要求の処理を制御するポリシーモデル内で識別された１つ以上の「On Request」ポリシーを実行してもよい。この例では、「On Request」ポリシーは、ステップ８０３で、クライアント装置４１０から受信されたユーザクレデンシャルを認証するために、および／または、要求されたバックエンドウェブサービス４３０にアクセスするためのユーザの認可許可を確認するために、認証／認可サービスにアクセスすることを含む。ステップ８０４で、プロキシサーバ４２０は、要求されたサービスはＳＯＡＰ入力を必要とすると判断し、したがって、ステップ８０５で、ＲＥＳＴ要求をＳＯＡＰ要求に変換するために「Message Transformation」ポリシーを実行する。ステップ８０６で、プロキシサーバ４２０は、さまざまなセキュリティおよび通信管理機能を実現し得る「Invoke Service」ポリシーを実行してから、ステップ８０７で、ＳＯＡＰ要求をバックエンドＳＯＡＰウェブサービス４３０に送信する。ステップ８０８で、バックエンドＳＯＡＰウェブサービス４３０からＳＯＡＰ応答を受信した後で、プロキシサーバ４２０は再度、クライアント４１０への出力はＲＥＳＴ出力であるべきであると判断してもよく、したがって、ステップ８０９で、ＳＯＡＰ応答をＲＥＳＴ応答に変換するために別の「Message Transformation」ポリシーを実行してもよい。ステップ８１０で、プロキシサーバ４２０は、さまざまな追加のセキュリティおよび通信管理機能を実現し得る「On Response」ポリシーを実行してから、ステップ８１１で、ＲＥＳＴ応答をクライアント装置に送信する。

【０１１８】

ここで図９を参照して、内部クライアント装置４４０から外部ウェブサービスまたはアプリケーション４５０に送信されたウェブリソースに対する要求のエンドツーエンド処理フローの別の例示的な図を示す。前述の例と同様に、この例の処理フローの実行は、プロキシサーバ４２０によって、上述のようなコンピューティング環境４００におけるさまざまな他のコンポーネントとともに行なわれてもよい。この例では、最初のメッセージは、

内部コンピュータネットワーク４６０におけるクライアント装置４４０から外部ウェブサービスまたはアプリケーション４５０に向けられた要求であり、このため、プロキシサーバ４２０はフォワードプロキシモードで動作してもよい。

【０１１９】

上述のように、この例のエンドツーエンド処理フロー図９００は、特定の処理点（またはアサーション）と、エンドツーエンド処理フロー中の各処理点でプロキシサーバ４２０によって実行されるべき特定のポリシーとを定義する、予め定められたポリシーモデルによって制御されてもよい。この例では、ステップ９０１で、ウェブ要求がクライアント装置４４０から受信される。ステップ９０２で、プロキシサーバ４２０は、この要求の処理を制御するポリシーモデル内で識別された１つ以上の「On Request」ポリシーを実行してもよい。任意の「On Request」ポリシーを実行した後で、プロキシサーバ４２０は、ステップ９０３で、さまざまなセキュリティおよび通信管理機能を実現するために１つ以上の「On Invoke」ポリシーを実行してから、ステップ９０４で、外部ウェブサービスまたはアプリケーション４５０に要求を送信してもよい。この例では、プロキシサーバ４２０は、外部ウェブサービスまたはアプリケーション４５０から受信されたエラー、またはプロキシサーバ４２０によって行なわれた処理内で起こったエラーといった、エンドツーエンド処理フロー中に起こったエラーを識別する。したがって、ステップ９０５で、プロキシサーバ４２０は、さまざまなセキュリティ機能、分析、およびエラー取扱いを実現するために１つ以上の「On Error」ポリシーを実行してもよい。この場合、「On Error」ポリシーはプロキシサーバ４２０に、追加のメッセージ処理を行なってから外部ウェブサービスまたはアプリケーション４５０に要求を再送信するように命令してもよい。したがって、「On Error」ポリシーが適用された後で、プロキシサーバ４２０はステップ９０６で「On Invoke」ポリシーを再実行し、次に、ステップ９０７で外部ウェブサービスまたはアプリケーション４５０に要求を再送信してもよい。ステップ９０８で、バックエンドウェブサービスまたはアプリケーション４５０から応答を受信した後で、プロキシサーバ４２０は、さまざまな追加のセキュリティおよび通信管理機能を実現し得る「On Response」ポリシーを実行してから、ステップ９０９で、応答を内部クライアント装置４４０に送信する。

【０１２０】

上述の例が示すように、ここに説明されたさまざまな実施形態は、異なるセキュリティポリシーおよび他の通信管理ポリシーが、ＤＭＺもしくは他の論理的または物理的サブネットワーク内で、メッセージのエンドツーエンド処理フロー全体にわたるさまざまな異なる処理点で適用され得る、動的ポリシーモデルをサポートしてもよい。この動的ポリシーモデルフレームワークは、悪意のある外部コンピューティングシステムからの攻撃を防止するための追加のセキュリティを構築し実現するために使用されてもよく、ラストマイルセキュリティインフラストラクチャ内（たとえば、バックエンドウェブサービス／アプリケーション４３０内）では可能ではなかったかもしれない、または好ましくなかったかもしれない、追加のタイプのセキュリティポリシーを実現してもよい。加えて、ここに説明された動的ポリシーモデルを使用して、トークン翻訳および／またはシングルサインオンアクセス制御システムといった、頑強な認証および認可システムが実現されてもよい。たとえば、クライアント装置４１０は、ユーザ名／パスワードまたは他のユーザクレデンシャルを介して認証してもよく、予め定められたエンドツーエンド処理フローは、異なるタイプのさまざまな異なるアクセストークン（たとえば、Kerberosトークン、ＳＰＮＥＧＯトークン、ユーザ名トークン、ＮＴＬＭトークン、ＳＡＭＬトークンなど）を検索または生成するために、内部ネットワーク４６０内の信頼できる認証／認可サービスからのトークン検索および確認を行なうプロキシサーバ４２０内で実行されてもよい。したがって、ユーザが一組の有効なクレデンシャルを提供し、順調に認証および認可された後で、プロキシサーバ４２０内のさまざまなポリシーモデルを使用して、ユーザが次にアクセスするさまざまな異なるバックエンドウェブサービス／アプリケーション４３０のための対応するトークンタイプを検索または生成することによって、シングルサインオンアクセス制御

システムを実現してもよい。

【０１２１】

本願の一実施形態によれば、処理部と通信部とを含むシステムが提供される。そのようなシステムは、この発明の原理を実行するために、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアとの組合わせによって実現されてもよい。処理部および通信部は、図３に示すコンポーネントといった上述のコンポーネントによって実現されてもよい、ということが当業者には理解される。一方、処理部および通信部は、上述されたようなこの発明の原理を実現するために、組合わされてもよく、またはサブユニットへと分離されてもよい、ということが当業者には理解される。したがって、ここでの説明は、ここに説明された機能部の任意の可能な組合せまたは分離またはさらなる定義をサポートしてもよい。

【０１２２】

上述の実施形態の例では、処理部および通信部は、以下の動作を行なうために協働することができ、動作は、第１のメッセージを受信する動作を含み、システムは、内部コンピュータネットワークのサブネットワーク内で動作するように構成され、システムは、内部コンピュータネットワークの一組のウェブアプリケーションまたはサービスを外部コンピュータネットワークに公開し、動作はさらに、第１のメッセージのための意図された宛先を判断する動作と、第１のメッセージのための意図された宛先に基づいて、システムがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかを判断する動作と、第１のメッセージのための予め定められた処理フローにおける現在点を判断する動作と、メッセージを処理するための複数のポリシーから、第１のメッセージを処理するためのポリシーを選択する動作とを含み、選択は、予め定められた処理フローにおける現在点、または、システムがフォワードプロキシとして作用すべきかリバースプロキシとして作用すべきかの判断、のうちの少なくとも１つに基づいており、動作はさらに、選択されたポリシーに従って第１のメッセージを処理する動作と、第１のメッセージを処理した後で、第１のメッセージを意図された宛先に送信する動作とを含む。

【０１２３】

別の例では、処理部および通信部は、以下の動作をさらに行なうように協働することができ、動作は、第１のメッセージは、内部コンピュータネットワークの簡易オブジェクトアクセスプロトコル（ＳＯＡＰ）仮想サービス内の１つ以上のＳＯＡＰ動作を呼び出すかまたは当該動作の一部であると判断する動作と、判断されたＳＯＡＰ動作およびＳＯＡＰ仮想サービスに基づいて、第１のメッセージを処理するためのポリシーを選択する動作と、選択されたポリシーに従って第１のメッセージを処理した後で、第１のメッセージ内のデータを使用して、判断された１つ以上のＳＯＡＰ動作を呼び出す動作とを含む。

【０１２４】

さらに別の例では、処理部および通信部は、以下の動作をさらに行なうように協働することができ、動作は、第１のメッセージは、内部コンピュータネットワークのレプリゼンテーショナル・ステート・トランスファー（ＲＥＳＴ）仮想サービスまたは仮想ウェブアプリケーションに関連付けられた１つ以上のハイパーテキスト転送プロトコル（ＨＴＴＰ）方法に対応していると判断する動作と、判断されたＨＴＴＰ方法およびＲＥＳＴ仮想サービスまたは仮想ウェブアプリケーションに基づいて、第１のメッセージを処理するためのポリシーを選択する動作と、選択されたポリシーに従って第１のメッセージを処理した後で、第１のメッセージ内のデータを使用して、判断された１つ以上のＨＴＴＰ方法を呼び出す動作とを含む。

【０１２５】

前述の説明では、例示のために、方法は特定の順序で説明された。代替的な実施形態では、方法は、説明されたものとは異なる順序で行なわれてもよい、ということが理解されるべきである。上述の方法はハードウェアコンポーネントによって行なわれてもよく、もしくは、汎用または専用プロセッサ、もしくは命令でプログラミングされた論理回路といったマシンに方法を行なわせるために使用され得るマシン実行可能命令のシーケンスで具

現化されてもよい、ということも理解されるべきである。これらのマシン実行可能命令は、１つ以上のマシン読取可能媒体またはメモリ装置、たとえば、ＣＤ－ＲＯＭまたは他のタイプの光ディスク、フロッピーディスケット、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気カードまたは光カード、フラッシュメモリ、もしくは、電子命令を格納するのに好適である他のタイプのマシン読取可能媒体またはメモリ装置上に格納されてもよい。それに代えて、方法は、ハードウェアとソフトウェアとの組合わせによって行なわれてもよい。

【０１２６】

この発明の例示的で現在好ましい実施形態がここに詳細に説明されてきたが、発明の概念は他のやり方でさまざまに具現化され採用されてもよいこと、および、添付された請求項は、先行技術によって限定される場合を除き、そのような変更を含むと解釈されるよう意図されていることが理解されるべきである。

【図１】

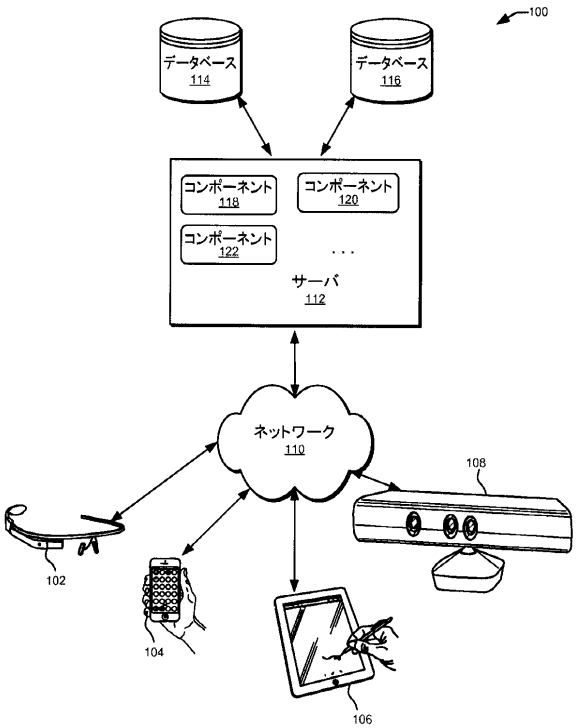

FIG. 1

【図２】

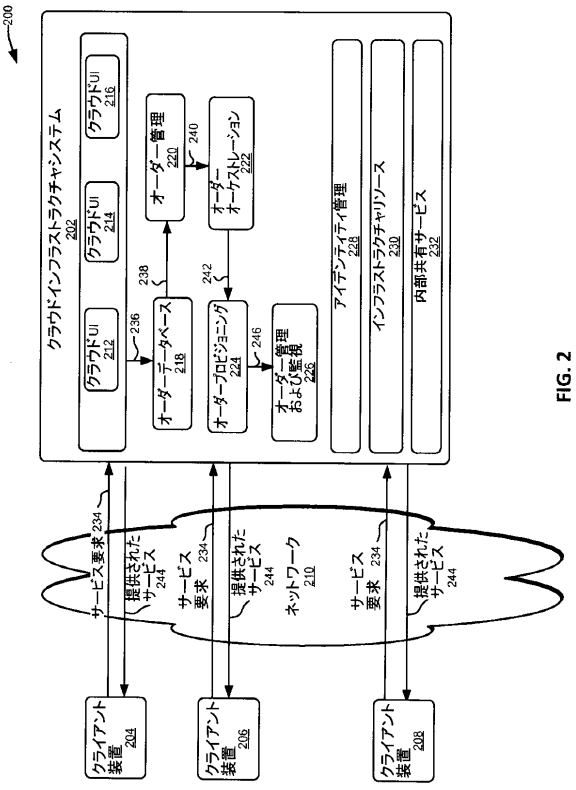

FIG. 2

【図３】

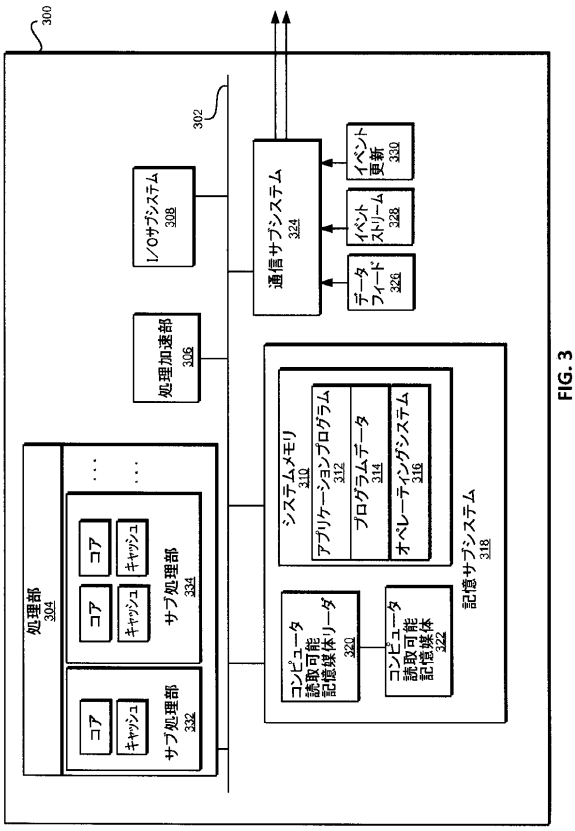

FIG. 3

【図４】

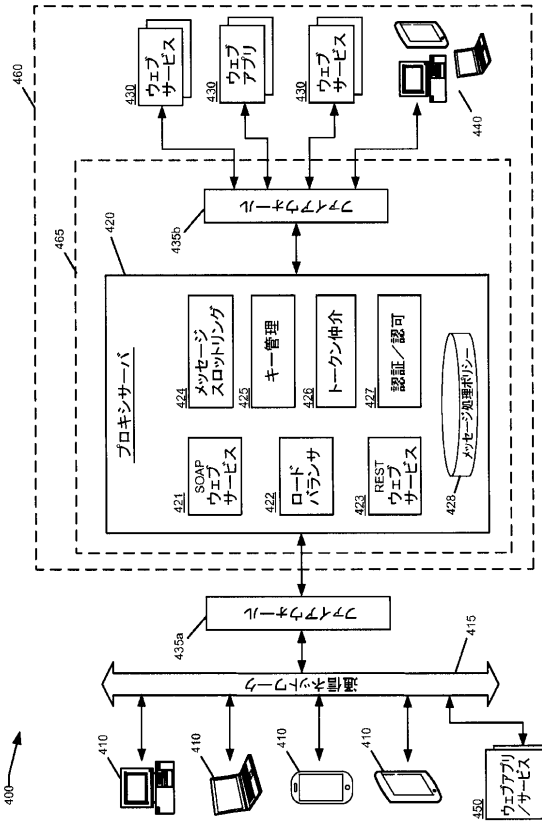

FIG. 4

【図５】

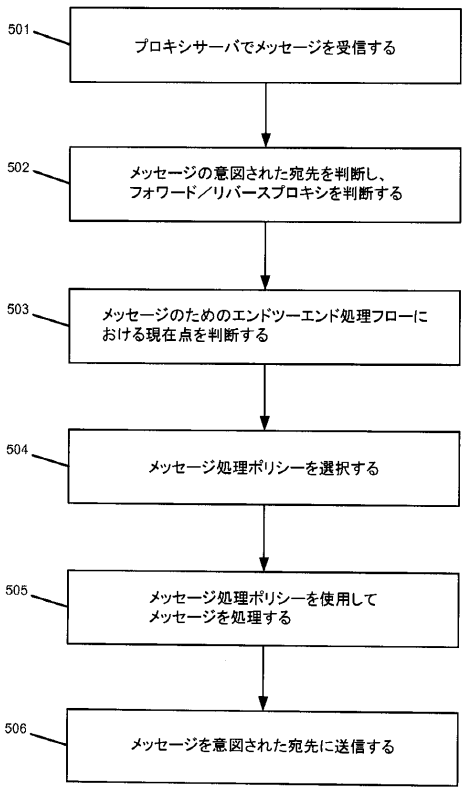

FIG. 5

【図６Ａ】

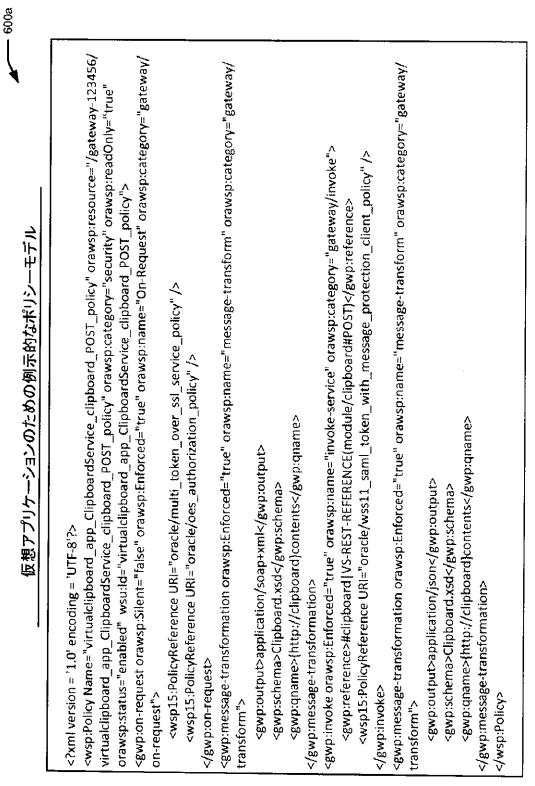

FIG. 6A

【図７Ｂ】

例示的な「INVOKE」メッセージ処理ポリシーテンプレート

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<orawsp:Template
orawsp:Id="invoke_template"
orawsp:description="i18n:oracle.idm.gateway.common.resources.artifactsdescription.GatewayArtifactsDescriptio
nBundle_oracle/invoke_template_ATDescKey"
orawsp:displayName="i18n:oracle.idm.gateway.common.resources.artifactsdescription.GatewayArtifactsDescripti
onBundle_oracle/invoke_template_ATDispNameKey"
        orawsp:readOnly="true"
        orawsp:attachTo="generic"
        xmlns:orawsp="http://schemas.oracle.com/ws/2006/01/policy"
        orawsp:name="oracle/invoke_template"
        orawsp:category="gateway"
        xmlns:gwp="http://schemas.oracle.com/gw-policy">
  <gwp:invoke orawsp:name="Invoke" orawsp:Silent="true" orawsp:Enforced="true"
              orawsp:category="gateway/invoke"/>
        <wsp15:PolicyReference URI="" />
</orawsp:Template>
```

FIG. 7B

【図６Ｂ】

600b

プロキシアプリケーションのための例示的なポリシーモデル

```
<wsp:Policy Name="justthename_rest_policy" orawsp:attachTo="generic" orawsp:category="security"
orawsp:name="justthename_rest_policy" orawsp:resource="/gateway-123456/firstproxy" orawsp:status="enabled"
wsu:Id="justthename_rest_policy">
  <gwp:on-request orawsp:Enforced="true" orawsp:category="gateway/on-request" orawsp:name="On-Request">
    <wsp15:PolicyReference URI="oracle/wss_http_token_service_policy" orawsp:effective="true"
orawsp:provides=""/>
  </gwp:on-request>
  <gwp:invoke-proxy orawsp:Enforced="true" orawsp:category="gateway/invoke" orawsp:name="Invoke">
    <wsp15:PolicyReference URI="oracle/http_saml20_token_bearer_client_policy" orawsp:effective="true"
orawsp:provides=""/>
    <gwp:proxy-server>
      <gwp:host>www-proxy.us.oracle.com</gwp:host>
      <gwp:port>80</gwp:port>
    </gwp:proxy-server>
  </gwp:invoke-proxy>
</wsp:Policy>
```

FIG. 6B

【図７Ｃ】

例示的な「INVOKE PROXY」メッセージ処理ポリシーテンプレート

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<orawsp:Template
orawsp:Id="invoke_proxy_template"
orawsp:description="i18n:oracle.idm.gateway.common.resources.artifactsdescription.GatewayArtifactsDescriptio
nBundle_oracle/invoke_proxy_template_ATDescKey"
orawsp:displayName="i18n:oracle.idm.gateway.common.resources.artifactsdescription.GatewayArtifactsDescripti
onBundle_oracle/invoke_proxy_template_ATDispNameKey"
        orawsp:readOnly="true"
        orawsp:attachTo="generic"
        xmlns:orawsp="http://schemas.oracle.com/ws/2006/01/policy"
        orawsp:name="oracle/invoke_proxy_template"
        orawsp:category="gateway"
        xmlns:gwp="http://schemas.oracle.com/gw-policy">
      <gwp:invoke-proxy orawsp:name="Invoke-Proxy" orawsp:Silent="true" orawsp:Enforced="true"
                        orawsp:category="gateway/invoke"/>
        <wsp15:PolicyReference URI="" />
</orawsp:Template>
```

FIG. 7C

【図７Ａ】

例示的な「ON REQUEST」メッセージ処理ポリシーテンプレート

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<orawsp:Template
orawsp:Id="on_request_template"
orawsp:description="i18n:oracle.idm.gateway.common.resources.artifactsdescription.GatewayArtifactsDescriptio
nBundle_oracle/on_request_template_ATDescKey"
orawsp:displayName="i18n:oracle.idm.gateway.common.resources.artifactsdescription.GatewayArtifactsDescripti
onBundle_oracle/on_request_template_ATDispNameKey"
orawsp:readOnly="true"
orawsp:attachTo="generic"
xmlns:orawsp="http://schemas.oracle.com/ws/2006/01/policy"
orawsp:name="oracle/on_request_template"
orawsp:category="gateway"
xmlns:gwp="http://schemas.oracle.com/gw-policy">
        <gwp:on-request orawsp:name="On-Request" orawsp:Silent="true" orawsp:Enforced="true"
            orawsp:category="gateway/on-request"/>
        <wsp15:PolicyReference URI="" />
</orawsp:Template>
```

FIG. 7A

【図７Ｄ】

例示的な「ON RESPONSE」メッセージ処理ポリシーテンプレート

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<orawsp:Template
orawsp:id="on_response_template"
orawsp:description="i18n:oracle.idm.gateway.common.resources.artifactsdescription.GatewayArtifactsDescriptio
nBundle_oracle/on_response_template_ATDescKey"
orawsp:displayName="i18n:oracle.idm.gateway.common.resources.artifactsdescription.GatewayArtifactsDescripti
onBundle_oracle/on_response_template_ATDispNameKey"
orawsp:readOnly="true"
orawsp:attachTo="generic"
xmlns:orawsp="http://schemas.oracle.com/ws/2006/01/policy"
orawsp:name="oracle/on_response_template"
orawsp:category="gateway"
xmlns:gwp="http://schemas.oracle.com/gw-policy">
    <gwp:on-response orawsp:name="On-Response" orawsp:Silent="true" orawsp:Enforced="true"
        orawsp:category="gateway/on-response"/>
        <wsp15:PolicyReference URI="" />
</orawsp:Template>
```

FIG. 7D

【図８】

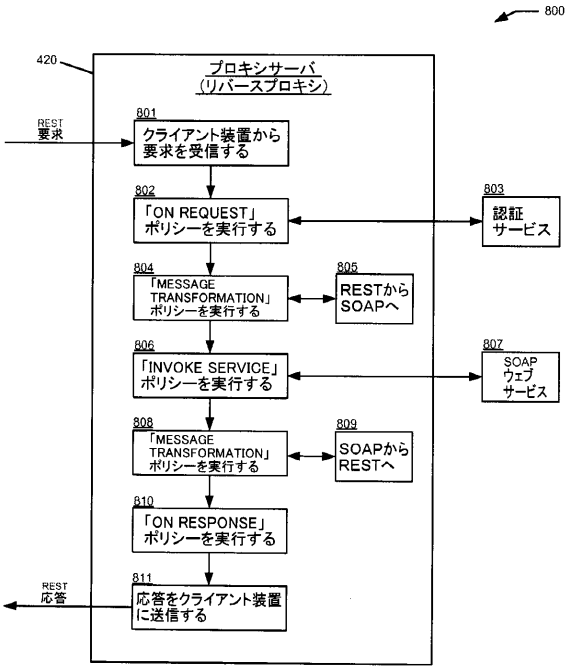

FIG. 8

【図９】

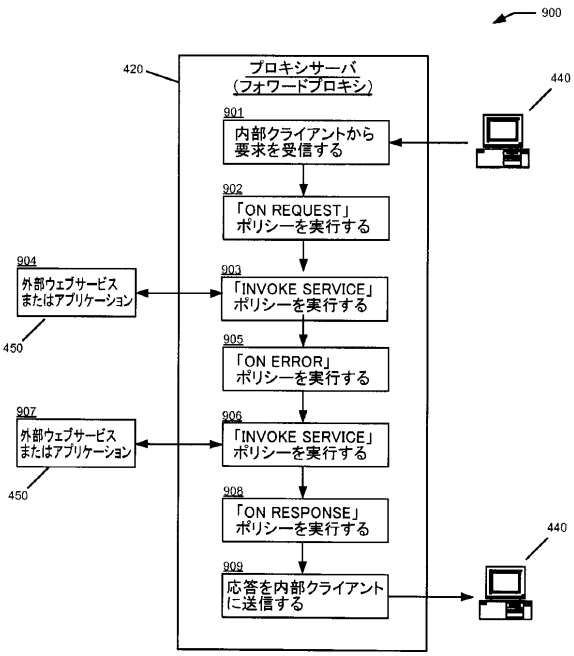

FIG. 9

フロントページの続き

(72)発明者　カバンザス，ニコラス
アメリカ合衆国、９４０６５　カリフォルニア州、レッドウッド・ショアーズ、オラクル・パークウェイ、５００、エム／エス・５・オゥ・ピィ・７
(72)発明者　スリバスタバ，ロイット
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、オラクル・パークウェイ、５００、エム／エス・５・オゥ・ピィ・７

審査官　玉木　宏治

(56)参考文献　特開２０１２－０４４２８３（ＪＰ，Ａ）
米国特許出願公開第２０１３／０２２７２９１（ＵＳ，Ａ１）
特開２００６－１１５０５９（ＪＰ，Ａ）
特開２００５－２１７８２８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／００－９５５