

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7617859号
(P7617859)

(45)発行日 令和7年1月20日(2025.1.20)

(24)登録日 令和7年1月9日(2025.1.9)

(51)国際特許分類	F I	
H 0 4 L 65/1108(2022.01)	H 0 4 L	65/1108
H 0 4 M 3/00 (2024.01)	H 0 4 M	3/00 B
H 0 4 L 67/02 (2022.01)	H 0 4 L	67/02
H 0 4 L 67/141 (2022.01)	H 0 4 L	67/141
H 0 4 L 65/1104(2022.01)	H 0 4 L	65/1104

請求項の数 7 (全17頁)

(21)出願番号	特願2021-569541(P2021-569541)	(73)特許権者	502303739
(86)(22)出願日	令和2年5月28日(2020.5.28)		オラクル・インターナショナル・コーポ レイション
(65)公表番号	特表2022-538736(P2022-538736 A)		アメリカ合衆国 9 4 0 6 5 カリフォル ニア州 レッドウッド ショアーズ、メー ル ストップ 5 オーピー7 オラクル パ ークウェイ 5 0 0
(43)公表日	令和4年9月6日(2022.9.6)	(74)代理人	110001195
(86)国際出願番号	PCT/US2020/035002		弁理士法人深見特許事務所
(87)国際公開番号	WO2020/263492	(72)発明者	ジャン、シューチュエン
(87)国際公開日	令和2年12月30日(2020.12.30)		中華人民共和国、1 0 0 1 9 3 ペイジ ン、チョングアンツン・ソフトウェア・ パーク、ビルディング・ナンバー・2 4
審査請求日	令和5年5月17日(2023.5.17)	(72)発明者	ジー、ウェイガン
(31)優先権主張番号	16/453,952		中華人民共和国、1 0 0 0 2 8 ペイジ
(32)優先日	令和1年6月26日(2019.6.26)		最終頁に続く
(33)優先権主張国・地域又は機関	米国(US)		

(54)【発明の名称】 公衆交換電話網 (P S T N) エンドポイントとウェブリアルタイム通信 (W E B R T C) エンドポイントと間の通信セッションを確立するための方法、システム、およびコンピュー

(57)【特許請求の範囲】

【請求項1】

方法であって、

公衆交換電話網 (P S T N) マイクロサービス (M S) によって、 P S T N エンドポイントからセッション開始プロトコル (S I P) ベースのシグナリングメッセージを受信するステップと、

前記 P S T N M S によって、前記 S I P ベースのシグナリングメッセージからエンドポイントコンテキスト属性情報を取得するステップとを含み、

前記エンドポイントコンテキスト属性情報は、前記 S I P ベースのシグナリングメッセージの指定受信者であるアソシエイトエンドポイント (A E) に対応するアクセス番号情報を含み、

前記エンドポイントコンテキスト属性情報を取得するステップは、前記エンドポイントコンテキスト属性情報を生成するために用いられる、発信元および/または宛先情報を取得するために、前記 S I P ベースのシグナリングメッセージのヘッダ部を解析するステップを含み、前記方法は、さらに、

前記 P S T N M S によって、アソシエイトマイクロサービス (M S) に、前記エンドポイントコンテキスト属性情報を提供するステップを含み、前記アソシエイト M S は、前記エンドポイントコンテキスト属性情報の受信にตอบสนองして、ルーティングルールに基づいて前記 A E に対応するアドレス識別子を特定し、前記アドレス識別子を P S T N M S に提供し、前記方法は、さらに、

前記 P S T N M S によって、前記エンドポイントコンテキスト属性情報に関連付けられた前記 A E の前記アドレス識別子を含むウェブリアルタイム通信 (W e b R T C) ベースのシグナリングメッセージを生成するステップと、

前記 P S T N M S によって、前記 P S T N エンドポイントと前記 A E との間のコールセッションを開始するために、前記 W e b R T C ベースのシグナリングメッセージを前記 A E に送信するステップとを含む、方法。

【請求項 2】

前記 A E の前記アドレス識別子は、前記エンドポイントコンテキスト属性情報を、前記 A E に関連付けられた前記アソシエイト M S に、 R E S T (R e p r e s e n t a t i o n S t a t e T r a n s f e r) アプリケーションプログラミングインターフェース (A P I) を介してプッシュすることに対応して、取得される、請求項 1 に記載の方法。

10

【請求項 3】

前記 P S T N M S は、前記エンドポイントコンテキスト属性情報が前記 R E S T A P I を介してプッシュされることに対応して、前記 A E にジョインキュー要求を送信する、請求項 2 に記載の方法。

【請求項 4】

前記 P S T N M S は、前記 S I P ベースのシグナリングメッセージを、前記 A E によって認識される J S O N (J a v a S c r i p t (登録商標) O b j e c t N o t a t i o n) プロトコルシグナリングメッセージに変換する、請求項 1 ~ 3 のいずれか 1 項に記載の方法。

20

【請求項 5】

前記 J S O N プロトコルシグナリングメッセージは、前記 A E との前記コールセッションを開始する会話開始要求メッセージである、請求項 4 に記載の方法。

【請求項 6】

少なくとも 1 つのプロセッサおよびメモリを備えるクラウド通信環境 (C C E) と、公衆交換電話網 (P S T N) マイクロサービス (M S) とを備え、

前記 P S T N M S は、前記メモリに格納され、かつ、前記少なくとも 1 つのプロセッサによって実行されたときに、

P S T N エンドポイントからセッション開始プロトコル (S I P) ベースのシグナリングメッセージを受信し、

30

前記 S I P ベースのシグナリングメッセージからエンドポイントコンテキスト属性情報を取得し、

前記エンドポイントコンテキスト属性情報は、前記 S I P ベースのシグナリングメッセージの指定受信者であるアソシエイトエンドポイント (A E) に対応するアクセス番号情報を含み、

前記 P S T N M S は、

前記エンドポイントコンテキスト属性情報を生成するために用いられる、発信元および/または宛先情報を取得するために、前記 S I P ベースのシグナリングメッセージのヘッダ部を解析することによって、前記エンドポイントコンテキスト属性情報を取得し、アソシエイトマイクロサービス (M S) に、前記エンドポイントコンテキスト属性情報を提供し、

40

前記アソシエイト M S は、前記エンドポイントコンテキスト属性情報の受信に対応して、ルーティングルールに基づいて前記 A E に対応するアドレス識別子を特定し、前記アドレス識別子を P S T N M S に提供し、

前記 P S T N M S は、

前記エンドポイントコンテキスト属性情報に関連付けられた前記 A E の前記アドレス識別子を含むウェブリアルタイム通信 (W e b R T C) ベースのシグナリングメッセージを生成し、

前記 P S T N エンドポイントと前記 A E との間のコールセッションを開始するために、前記 W e b R T C ベースのシグナリングメッセージを前記 A E に送信するように構成さ

50

れる、システム。

【請求項 7】

請求項 1 ~ 5 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コンピュータ可読プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

優先権の主張

本願は、2019年6月26日に出願された米国特許出願連続番号第16/453,952号の優先権の利益を主張し、その開示の全体を本明細書に引用により援用する。

10

【0002】

技術分野

本明細書に記載される主題は、公衆交換電話網(PSTN)ユーザとウェブリアルタイム通信(WebRTC)ユーザとの間のリアルタイム通信を可能にすることに関する。特に、本明細書に記載される主題は、PSTNエンドポイントとWebRTCエンドポイントとの間で通信セッションを確立するための方法、システム、およびコンピュータ可読媒体に関する。

【背景技術】

【0003】

背景

現在、インターネット上でメディアおよびメッセージを通信するために、ウェブベースのアプリケーションやインスタントメッセージングクライアントが頻繁に使用されている。同様に、PSTN電話ベースの通信は、音声ベースのコールセッションを確立するために一般的に採用されている。特に、これらの異なるネットワークシステムの各々は、通常、サポートされるすべてのエンドポイントが、共通のプロトコル、共通のソフトウェアクライアントなどを使用して、コールセンターまたはサーバとの接続を確立することを必要とする。WebRTCエンドポイントとPSTNベースのエンドポイントとの間の通信が望まれる場合、互換性のないシグナリングプロトコルおよび/または異なる端末装置がエンドポイント情報を確実に共有できないことによって問題が生じる可能性がある。特に、WebRTCアプリケーションにとって、アプリケーションが通信しているエンドポイントのいくつかの特定の詳細情報を知っていることが重要である。さらに、WebRTCベースのシステムは、PSTNのエンドポイントやシステムによって使用されていない、セキュアリアルタイムプロトコル(SRTP)を用いたリアルタイムメディアの通信が主に可能であるため、WebRTCエンドポイントがPSTNエンドポイントとの連携を試みる場合、さらに技術的課題が発生する可能性がある。

20

【0004】

したがって、PSTNエンドポイントとWebRTCエンドポイントとの間で通信セッションを確立するための方法、システム、およびコンピュータ可読媒体が必要である。

【発明の概要】

【課題を解決するための手段】

30

40

【0005】

概要

本明細書に記載の主題は、PSTNエンドポイントとWebRTCエンドポイントとの間で通信セッションを確立するための方法、システム、およびコンピュータ可読媒体を含む。ある方法は、PSTNマイクロサービス(MS)によって、PSTNエンドポイントからセッション開始プロトコル(SIP)ベースのシグナリングメッセージを受信するステップと、PSTN MSによって、SIPベースのシグナリングメッセージからエンドポイントコンテキスト属性情報を取得するステップとを含む。本方法は、PSTN MSによって、コンテキスト属性情報に関連付けられたアソシエートエンドポイント(AE)のアドレス識別子を含むWebRTCベースのシグナリングメッセージを生成するステッ

50

プと、PSTN MSによって、PSTNエンドポイントとAEとの間のコールセッションを開始するために、WebRTCベースのシグナリングメッセージをAEに送信するステップとをさらに含む。

【0006】

本方法の一例では、PSTN MSは、SIPベースのシグナリングメッセージの受信に回答して、シグナリングエンジン(SE)とのWebSocket接続を開始する。

【0007】

一例では、本方法によるエンドポイントコンテキスト属性情報を取得するステップは、エンドポイントコンテキスト属性情報を生成するために用いられる、発信元および/または宛先情報とコール種別情報とを取得するために、SIPベースのシグナリングメッセージのヘッダ部を解析するステップを含む。

10

【0008】

本方法の一例では、AEのアドレス識別子は、エンドポイントコンテキスト属性情報を、AEに関連付けられたアソシエイトマイクロサービスに、REST (Representation State Transfer) アプリケーションプログラミングインターフェース(API)を介してプッシュすることに対応して、取得される。

【0009】

本方法の一例では、PSTN MSは、エンドポイントコンテキスト属性情報がREST APIを介してプッシュされることに対応して、AEにジョインキュー(join queue)要求を送信する。

20

【0010】

本方法の一例では、PSTN MSは、SIPシグナリングメッセージを、AEによって認識されるJSON (JavaScript (登録商標) Object Notation) プロトコルシグナリングメッセージに変換する。

【0011】

本方法の一例では、JSONプロトコルシグナリングメッセージは、AEとのコールセッションを開始する会話開始要求メッセージである。

【0012】

PSTNエンドポイントとWebRTCエンドポイントとの間で通信セッションを確立するためのシステムは、少なくとも1つのプロセッサおよびメモリを備えるクラウド通信環境(CCE)を含む。

30

【0013】

システムは、メモリに格納されたPSTN MSをさらに含み、少なくとも1つのプロセッサによって実行されたときに、PSTNエンドポイントからSIPベースのシグナリングメッセージを受信し、SIPベースのシグナリングメッセージからエンドポイントコンテキスト属性情報を取得し、コンテキスト属性情報に関連付けられたAEのアドレス識別子を含むWebRTCベースのシグナリングメッセージを生成し、PSTNエンドポイントとAEとの間のコールセッションを開始するために、WebRTCベースのシグナリングメッセージをAEに送信するように構成される。

【0014】

本システムの一例では、PSTN MSは、SIPベースのシグナリングメッセージの受信に回答して、シグナリングエンジン(SE)とのWebSocket接続を開始する。

40

【0015】

本システムの一例では、PSTN MSは、エンドポイントコンテキスト属性情報を生成するために用いられる、発信元および/または宛先情報とコール種別情報とを取得するために、SIPベースのシグナリングメッセージのヘッダ部を解析するようにさらに構成される。

【0016】

本システムの一例では、AEのアドレス識別子は、エンドポイントコンテキスト属性情報を、AEに関連付けられたアソシエイトマイクロサービスに、REST APIを介し

50

てプッシュすることに対応して、取得される。

【0017】

システムの一例では、PSTN MSは、エンドポイントコンテキスト属性情報がREST APIを介してプッシュされることに対応して、AEにジョインキュー要求を送信する。

【0018】

本システムの一例では、PSTN MSは、SIPシグナリングメッセージを、AEによって認識されるJSON (JavaScript Object Notation) プロトコルシグナリングメッセージに変換する。

【0019】

本システムの一例では、JSONプロトコルシグナリングメッセージは、AEとのコールセッションを開始する会話開始要求メッセージである。

【0020】

本明細書に記載されている主題は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組み合わせで実装されてもよい。そのため、本明細書で使用されている「機能」、「ノード」または「エンジン」という用語は、説明されている機能を実装するための、ソフトウェアおよび/またはファームウェアコンポーネントも含み得るハードウェアを指す。1つの例示的な実装において、本明細書に記載された主題は、コンピュータのプロセッサによって実行されたとき、ステップを実行するためにコンピュータを制御するコンピュータ実行可能命令を格納した非一時的コンピュータ可読媒体を用いて実装されてもよい。本明細書に記載の主題を実装するのに適した例示的なコンピュータ可読媒体は、ディスクメモリデバイス、チップメモリデバイス、プログラマブルロジックデバイス、および特定用途向け集積回路などの非一時的コンピュータ可読媒体を含む。さらに、本明細書に記載されている主題を実装するコンピュータ可読媒体は、単一のデバイスまたはコンピューティングプラットフォーム上に配置されてもよいし、複数のデバイスまたはコンピューティングプラットフォームに分散されてもよい。

【図面の簡単な説明】

【0021】

【図1】本明細書に記載されている主題の一実施形態に係る、PSTNエンドポイントとWebRTCエンドポイントとの間で通信セッションを確立するための例示的なネットワークを示すブロック図である。

【図2】本明細書に記載されている主題の一実施形態に係る、PSTNエンドポイントとWebRTCエンドポイントとの間で通信セッションを確立するための例示的なコールフローを示すシグナリング図である。

【図3】本明細書に記載されている主題の一実施形態に係る、PSTNエンドポイントとWebRTCエンドポイントとの間で通信セッションを確立するための例示的なプロセスを示すフローチャートである。

【発明を実施するための形態】

【0022】

詳細な説明

公衆交換電話網 (PSTN) エンドポイントとウェブリアルタイム通信 (WebRTC) エンドポイントとの間で通信セッションを確立するための方法、システム、およびコンピュータ可読媒体が開示される。いくつかの実施形態では、開示された主題は、ウェブベースのアソシエートエンドポイント (AE) と通信することが許可されている外部PSTNエンドポイントを含む。このような例では、コールまたは通信セッションを開始および確立するために、プロトコル変換が必要である。クラウド通信環境 (CCE) などのホストシステムは、複数のマイクロサービス (例えば、仮想マシンおよび/またはソフトウェアアプリケーション) を利用している。これら複数のマイクロサービスは、CCEの外部からインバウンドセッション開始プロトコル (SIP) INVITEメッセージを受信し、その後、JSON (JavaScript Object Notation) RTCプロトコルに基づいてS

10

20

30

40

50

IP INVITEメッセージをシグナリングメッセージに変換するようにまとめて構成されている。このようにすることで、受信側のAEは、即座に着信を受け付けることができる(たとえば、別のAEから着信があったかのように機能する)。CCEシステムは、また、コールシグナリングメッセージがPSTNシステムでサポートされているエンドポイントから発信されていることを宛先AEに通知するために、送信側のPSTNエンドポイントに関連するコンテキスト属性情報をプッシュするように構成される(例えば、「callType:PSTN」)。

【0023】

図1は、本明細書に記載された主題の一実施形態に係る、PSTNエンドポイントとWebRTCエンドポイントとの間で通信セッションを確立するための例示的なネットワークを示すブロック図である。例えば、図1は、PSTNエンドポイント102、PSTN SIPトランク104、ファイアウォール106、ロードバランサ108、および、少なくとも1つの外部ホストドメイン110と少なくとも1つの内部ホストドメイン112とを備えるCCEシステムを含むネットワーク100を示している。

10

【0024】

いくつかの実施形態では、PSTNエンドポイント102は、PSTNネットワーク(例えば、PSTN SIPトランク104)を介して通信可能なモバイルデバイス、ユーザ機器、VoIP(Voice over IP)電話などを備える。特に、エンドポイント102は、SIPおよびセッション記述プロトコル(SDP)シグナリングメッセージを用いて通信し、セッションを確立するように構成される。特に、PSTNエンドポイント102は、外部ホストドメイン110に向けてSIP INVITEメッセージを指示することによって、AE114などのWebRTCエンドポイントとのコールセッションの確立を試みてもよい。いくつかの実施形態では、AE114は、デスクトップデバイス、ラップトップデバイス、モバイルデバイス(例えば、iOS、Androidなど)などの、任意のWebRTCエンドポイントを備えてもよい。

20

【0025】

PSTNエンドポイント102によって送信されたSIP INVITEメッセージは、PSTN SIPトランク104を介してファイアウォール106によって最初に受信される。特に、ファイアウォール106は、外部ホストドメイン110のデバイスおよび/またはマイクロサービスが接続されているプライベートネットワーク(例えば、10.0.x.x)に対して、パブリック側のインターネットプロトコル(IP)ネットワーク(例えば、129.146.x.x)のネットワークアドレス変換(NAT)サービスを提供できる。いくつかの実施形態では、ファイアウォール106は、BaaS(bare metal as a service)ファイアウォールである。

30

【0026】

ファイアウォール106を(例えば、特定のポートを介して)正常に通過した後、SIP INVITEメッセージは、ロードバランサ108によって受信される。いくつかの実施形態では、ロードバランサ108は、バックエンドサーバおよび/または仮想マシンのセットとして構成され得る、外部ホストドメイン110のホストデバイスおよび/またはマイクロサービスに、1つまたは複数のPSTNコールを分散させるように構成される。例えば、ロードバランサ108は、任意の着信SIP INVITEメッセージを処理するために、CCEシステムの外部ホストドメイン110においてホストされている複数のエンタープライズセッションボーダーコントローラ(ESBC)マイクロサービス(例えば、ESBC MS116)の1つを選択するように適合される。いくつかの実施形態では、ロードバランサ108のIPアドレスは、PSTN SIPトランク104にプロビジョニングされている。例えば、PSTNシグナリングおよびメディアトラフィックを伝送するために、既存の10.0.x.xプライベートネットワークアドレスが使用され得る。ESBC MS116はファイアウォール106の後ろに配置されているため、ESBC MS116は、SIPおよびメディアのネゴシエーションがファイアウォール106の公開側IPアドレスを反映するようにNATトラバーサル用に構成される。より具

40

50

体的には、SIPとメディアとのネゴシエーションの間、PSTNエンドポイント102は、外部ホストドメイン110内のESBC MS116に到達するために、BMAASのパブリック側のIPアドレスが提示される。

【0027】

いくつかの実施形態では、外部ホストドメイン110は、ESBC MS116、TURN MS128、およびOHS MS124をサポートおよび実行するように構成された1つまたは複数のハードウェアデバイスを備える。例えば、外部ホストドメイン110は、ハードウェアおよび/またはファームウェアと組み合わせたソフトウェアで実装可能であってもよい。特に、本明細書に記載されている主題は、プロセッサによって実行されるソフトウェアで実装可能である。1つの例示的な実装では、外部ホストドメイン110は、中央処理装置（例えば、単一のコアまたは複数の処理コア）、マイクロプロセッサ、マイクロコントローラ、ネットワークプロセッサ、特定用途向け集積回路（ASIC）などの、1つまたは複数のプロセッサを含んでもよい。また、外部ホストドメイン110は、メモリを含んでもよい。メモリは、ランダムアクセスメモリ（RAM）、フラッシュメモリ、磁気ディスク記憶ドライブなどで構成されてもよい。いくつかの実施形態では、メモリは、1つまたは複数のマイクロサービスを格納するように構成されてもよい。いくつかの実施形態では、プロセッサ（複数可）およびメモリは、外部ホストドメイン110においてサポートされている前述のマイクロサービス116、124、128をサポートする仮想マシン（複数可）（VMs）をサポートするための基礎的なハードウェアとして動作するように、ハイパーバイザによって管理されてもよい。

10

20

【0028】

図1に示すように、ESBC MS116は、ファイアウォール106およびロードバランサ108を介してPSTN SIPトランク104からシグナリング通信を受信するように構成される。例えば、ESBC MSのポート「5061」は、TLS接続においてSIPを受け入れるために、公開されて適合され得る。ESBC MS116は、コールセッションのPSTN側を終了し、その後、SIP INVITEメッセージを複数のバックエンドPSTNマイクロサービス（例えば、PSTN MS118）に負荷分散するように構成される。いくつかの実施形態では、ESBC MS116は、ラウンドロビン負荷分散方式を利用するように構成される。別の実施形態では、ESBC MS116は、必要に応じてAEに向けられたシグナリングメッセージを負荷分散するための他のタイプのアルゴリズムまたは方法をサポートし得る。適切なPSTNマイクロサービスを選択した後、ESBC MS116は、トランスポート層セキュリティ（TLS）、セキュアソケットレイヤー（SSL）、伝送制御プロトコル（TCP）/IPなどを用いて、PSTN MS118との安全な接続を確立し得る。

30

【0029】

いくつかの実施形態では、ESBC MS116は、CCEによって受信されるPSTNトラフィックに必要なセキュリティを提供するように構成される。例えば、ESBC MS116は、（例えば、PSTN SIPトランク104を介して）PSTNサービスプロバイダと通信するときに、SIP over TLS通信を要求することによって、SIPシグナリングプレーンを保護してもよい。同様に、ESBC MS116は、セキュアリアルタイムトランスポートプロトコル（SRTP）を用いてすべてのメディアトラフィックの暗号化を要求することによって、メディアプレーンを保護するように構成し得る。SRTPの利用に加えて、ESBC MS116は、サービス拒否（DoS）攻撃、分散型サービス拒否（DDoS）攻撃、および中間者攻撃（man-in-the-middle attack）に対して、公開されたメディアポートの保護を提供し得る。いくつかの実施形態では、ESBC MS116は、OHS MS124およびTURN MS128とは異なり、CCEの外部ホストドメイン内のカーネルベースの仮想マシン（KVM）インスタンスとして実行し得る。

40

【0030】

いくつかの実施形態では、ESBC MS116は、CCEを介してPSTNコールを

50

確立するために必要な SIP シグナリングとメディアシグナリングとをネゴシエートするように構成されたパブリック側のサービスとして使用され得る。上述のように、ESBC MS 116 は、外部ホストドメイン 110 内の 1 つまたは複数のデバイス / サーバ上の KVM インスタンスとしてプロビジョニングし得る。外部ホストドメイン (複数可) は、B Ma a s ファイアウォール 106 およびロードバランサ 108 の後ろに配置されている。ファイアウォール 106 は、外部ホストドメイン 110 において外部ホストが接続されているプライベートネットワーク (10.0.x.x) に対するパブリック側の IP ネットワーク (129.146.x.x) に、ネットワークアドレス変換 (NAT) サービスを提供する。いくつかの実施形態では、外部ホストドメイン 110 は、PSTN サービスプロバイダの SIP ポート (および一連のメディアポート) から発信される着信パケットトラフィックを許可し、そのトラフィックを ESBC MS 116 の 10.0.x.x プライベートインターフェースに転送する、少なくとも 1 つのファイアウォールルールがプロビジョニングされる。さらに、PSTN サービスプロバイダは、通信を CCE に向けるために、B Ma a s ロードバランサの IP アドレスで構成され得る。例えば、B Ma a s ロードバランサ 108 は、外部ホストドメイン 110 の 1 つまたは複数のバックエンドサーバ (および / またはマイクロサービス) に着信コールを分散し得る。B Ma a s ロードバランサ 108 の既存の IP アドレスは、CCE サービスに到達するために PSTN SIP トランク 104 にプロビジョニングされ得る。既存の 10.0.x.x プライベートネットワークは、PSTN のシグナリングおよびメディアトラフィックを伝送するために用いられる。

10

20

【0031】

ESBC MS 116 は、B Ma a s ファイアウォール 106 の背後にあるため、ESBC MS 116 は、SIP およびメディアのネゴシエーションが B Ma a s ファイアウォール 106 のパブリック側の IP アドレスを反映するように、NAT トラバーサル用に構成される。具体的には、SIP とメディアとのネゴシエーションの間、PSTN のエンドポイント (例えば、エンドポイント 102) は、ESBC MS 116 とのコンタクトを確立するために使用し得る B Ma a s のパブリック側の IP アドレスが提示される。

【0032】

SIP シグナリングトラフィックについては、ESBC MS 116 は、内部ホストドメイン 112 内の複数の PSTN マイクロサービス (例えば、PSTN MS 118) の間で負荷を分散するように構成され得る。メディアトラフィックについては、ESBC MS 116 は、パケットトラフィックをバックエンドのメディアエンジン (ME) サーバ (例えば、ME マイクロサービス 120) に転送し得る。この ME サーバは、アソシエイトエンドポイント (例えば、AE 114) への配送のために、メディアトラフィックに次の中継先 (例えば、TURN サーバおよび / またはマイクロサービス 128) を指示する。既存の ME マイクロサービスは、MCU セッションと SFU セッションとの混在をサポートし得ることが理解される。

30

【0033】

いくつかの実施形態では、ESBC MS 116 は、SIP トランキングの終結、TLS および SRTP のサポート、高度な DOS および過負荷保護、NAT サポート (例えば、ESBC MS がファイアウォールの後ろに配置されている場合)、KVM サポート、および、バックエンドのサーバ群への SIP メッセージのルーティングを実行するように構成される。ESBC MS 116 は、さらに、1:1 の任意の高可用性 (HA) サポートを行うように構成されており、関連するすべての PSTN および ME 関連のコーデックをサポートし、12000 のシグナリングセッション、6000 の SRTP セッション、および 2500 のトランスコードセッション (G.721 <-> G.729) をサポート可能である。

40

【0034】

いくつかの実施形態では、ESBC MS は、負荷分散された SIP INVITE メッセージを、CCE の内部ホストドメイン 112 に配置されている選択 / 指定された PST

50

N MS 118 に転送する。いくつかの実施形態では、内部ホストドメイン 112 は、テナント (tenant) MS 105、アソシエイト (associate) MS 107、PSTN MS 118、ME MS 120、および SE MS 122 をサポートおよび実行するように構成された 1 つまたは複数のハードウェアデバイスを備えてもよい。例えば、内部ホストドメイン 112 は、ハードウェアおよび/またはファームウェアと組み合わせたソフトウェアで実装されてもよい。特に、本明細書に記載の主題は、プロセッサによって実行されるソフトウェアで実装され得る。ある例示的な実装では、内部ホストドメイン 112 は、中央処理装置 (例えば、単一のコアまたは複数の処理コア)、マイクロプロセッサ、マイクロコントローラ、ネットワークプロセッサ、特定用途向け集積回路 (ASIC) などの、1 つまたは複数のプロセッサを含んでもよい。また、内部ホストドメイン 112 は、メモリも含んでよい。メモリは、ランダムアクセスメモリ (RAM)、フラッシュメモリ、磁気ディスク記憶ドライブなどで構成されてもよい。いくつかの実施形態では、メモリは、1 つまたは複数のマイクロサービスを格納するように構成されてもよい。いくつかの実施形態では、プロセッサ (複数可) およびメモリは、前述のマイクロサービス 105 ~ 107 および 118 ~ 122 をサポートする仮想マシン (複数可) (VM) をサポートするための基礎的なハードウェアとして動作するように、ハイパーバイザによって管理されてもよい。

10

【0035】

いくつかの実施形態では、PSTN MS 118 は、(ESBC MS 116 を介して) CCE の外部から受信した SIP 要求を処理するように構成される。一例として、PSTN MS 118 は、SIP 関連のコール設定方法と、SIP INVITE、UPDATE、ACK、BYE、および CANCEL メッセージなどのシグナリングメッセージとをサポートし得る。いくつかの実施形態では、PSTN MS 118 は、また、SIP INVITE 要求を処理するために SipServlet を実装するように構成され得る。

20

【0036】

最初の SIP INVITE メッセージを受信した後、PSTN MS 118 は、i) ターゲット電話番号 (すなわち、コールされた相手の電話番号) に基づいてテナントキーおよび/またはクライアント識別子を取得し、ii) JWT トークンを生成し、iii) WebSocket を介して SE MS 122 への接続を確立し、iiii) 受信した SIP INVITE の「from」および「to」ヘッダを解析し、エンドポイントコンテキスト属性情報を生成し、iv) エンドポイントコンテキスト属性データを REST API を介してアソシエイト MS 107 にプッシュするように構成される。いくつかの実施形態では、アソシエイト MS 107 は、PSTN MS 118 を介して PSTN エンドポイントとターゲット AE との間の接続を確立するために使用され得る複数のルーティングルールを含む。特に、PSTN コールを正しいアソシエイトまたは正しいチーム (例えば、AE 114) にルーティングするために、ルーティングルールは、TOB UI 103 上でテナント管理者によって最初に構成される必要がある。プロビジョニングされたルーティングルールは、ターゲット PSTN 番号に基づくことができ、例えば、「+01234」に向けられたコールは、「mceAgent@example.com」にルーティングされる。あるいは、ルーティングルールは、PSTN エンドポイント 102 の発信番号に基づくこともできる (例えば、「+64xxx」からのコールは、「NZ サポートチーム」にルーティングされてもよい)。アソシエイト MS 107 によって PSTN MS 118 に返されたアソシエイト名に基づいて、PSTN MS 118 は、アソシエイト名に関連付けられたターゲット (例えば、AE) との通信セッションを開始するために、SIP INVITE メッセージを転送または変換することができる。そのため、この要求は、正しいアソシエイトまたは AE に送信される。例えば、PSTN MS 118 は、v) コンテキスト属性情報がアソシエイト MS 107 に正常にプッシュされた後に、ジョインキュー REST 要求メッセージを送信し、vi) 会話照会要求を生成し、メッセージを SE MS 122 に送信するようにさらに構成されてもよい。照会/応答の取得後、関連する AE 情報を含む会話開始/要求メッセージを生成する。開始/応答メッセージの取得後、PSTN MS 11

30

40

50

8は、PSTNエンドポイント102によって送信された最初のSIP INVITE要求に対するSIP 200応答メッセージを生成する。より具体的には、AEがアンサーSDPで応答すると、PSTN MS 118は、PSTNエンドポイント102によって送信されたオリジナル/初期のSIP INVITE要求に対するアンサーSDPを含むSIP 200メッセージを生成してもよい。

【0037】

いくつかの実施形態では、PSTN MS 118は、コールが回答される前にSIP CANCELメッセージを受信し、キャンセル「joinQueue (ジョインキュー) 要求」をアソシエイトMS 107に送信するように構成され、また、SE MS 122とのWebSocketを閉じるようにしてもよい。その後、PSTN MS 118は、AE 114が回答した後にSIP CANCELメッセージを受信する。しかしながら、SIP 200メッセージは、PSTNクライアント(例えば、PSTNエンドポイント102)に配送されない。このような場合、PSTN MS 118は、SE MS 122にシャットダウンメッセージを送信し、WebSocketを閉じる。

10

【0038】

いくつかの実施形態では、AE 114は、ホストされたブラウザ上でリアルタイム通信を可能にするプロトコルである(IETFおよびW3C標準で定義されている)WebRTCを使用して、PSTN MS 118を介して通信するように構成されている。上述したように、WebRTCで通信するように構成されたエンドポイントは、PSTNエンドポイントとの通信が望まれる場合に、いくつかの技術的課題が発生する。例えば、WebRTCは、SRTPを使用してリアルタイムメディアの安全な通信が可能である。しかしながら、このプロトコルは、PSTNネットワークによって、あまり認識かつ/または利用されていない。この技術的な問題に対処するために、開示された主題は、プッシュコンテキストAPI、JavaScript Conversation SDK、およびJSON RTCプロトコルを提供する方法について説明している。これにより、開示された主題は、PSTNユーザおよびWebRTCユーザの両者に対してインターワーキングサービスを提供するアプリケーションを、開発者が容易に構築可能にする。

20

【0039】

いくつかの実施形態では、ESBC MS 116は、(シグナリングセッションが開始された後に)PSTN SIPトランク104を介してPSTNサービスとメディアセッションをネゴシエートするように構成されている。特に、ESBC MS 116によって一連のESBCメディアポートが公開され得る。このように、公開されたESBCメディアポートに到達したメディアトラフィックは、ファイアウォール106によって、外部ホストドメイン110のプライベートIPアドレスへのネットワークアドレス変換(NAT)が受けられる。いくつかの実施形態では、外部ホストドメイン110は、メディアポートの範囲をESBC MS 116にポート転送するためにプロビジョニングされたファイアウォールルールを有する。ESBC MS 116がPSTNメディアトラフィックを受信すると、ESBC MS 116は、AE 114に配送するために、メディアトラフィックをME MS 120に転送する。PSTN SIPトランク104とESBC MS 116との間に存在するメディアパスは、通信されたメディアトラフィックの機密性、メッセージ認証、およびリプレイ保護を提供するために、SRTPを使用してもよい。ESBC MS 116は、SRTPに加えて、公開されたESBCメディアポートに対して、DOS攻撃、DDOS攻撃、および中間者攻撃に対するセキュリティおよび保護を提供し得る。しかしながら、ESBC MS 116は、いかなるトランスコーディング機能も提供しない。むしろ、ME MS 120は、PSTNエンドポイント102とAE 114との間で確立された通話に関連するメディアトラフィックに必要とされる可能性のあるトランスコーディングを担当する。

30

40

【0040】

いくつかの実施形態では、開示された主題は、多数のセキュリティ対策を実施するように構成され得る。いくつかの実施形態では、PSTN MS 118は、一連のまたは複数

50

のメディアポートがCCEシステムのパブリック側に公開されることが必要である。特に、MESは、公開されたメディアポートに対するDOS/DDOSまたは中間者のいかなる保護も提供しない。そのため、CCEサービスでは、これらのメディアポートを外部からの攻撃から保護することが重要である。このため、前述のESBC MS116は、SIPメッセージがCCEに入ると、PSTNのSIPトランクを終了するように構成される。ESBC MS116は、パブリックPSTN側でセキュリティを提供するバックユーザエージェント(b2bua)として、かつ、CCEの内部ホストドメイン112に配置されているPSTN MS118へのインターフェースとして機能する。いくつかの実施形態では、ESBCのセキュリティは、DOS/DDOSおよび中間者攻撃から保護することと同様に、SIPシグナリングにTLSをサポートしかつメディアパスにSRTPをサポートすることによって実現される。例えば、ESBC MS116は、エンドポイントからの接続数を制限することによって、および、SIPインターフェースへの同時TCP/TLS接続数を制限することによって、TCP/TLSメッセージフラッディングの可能性からの保護を提供する。例えば、ESBC MS116は、PSTNサービスプロバイダからCCEシステムへの単一のTLS接続が確立されることを意味する、PSTN SIPトランク104への「Static TLS」接続を利用可能である。特に、すべてのコールのシグナリングは、その単一のTLS接続を利用するように指定される。コールが確立されると、CCE側(例えば、AE)からSIPシグナリングイベントが開始された場合、CCEシステムは、PSTNサービスプロバイダによってサポートされるPSTNエンドポイントに戻る、新しいTLS接続を開始する必要がある可能性がある。例えば、最初のSIP INVITEメッセージのContactヘッダにおいてPSTNサービスプロバイダから送信されたIP:ポートに接続可能である。したがって、ESBC MS116によって、アクセス側のSIPインターフェースを介したTLS接続のソフト制限を実施するポリシーが実施されてもよい。

【0041】

さらに、ESBC MS116は、シグナリングメッセージにセキュリティ対策を施すように構成され得る。例えば、SIPシグナリングメッセージの受信に対応するために、ファイアウォール106およびESBC MS116において単一のポートが開放され得る。例えば、SIP over TLS通信のために新しいポート(例えば、5061)が開放され得る。同様に、メディアトラフィックの収容を容易にするために、ファイアウォール106とESBC MS116とで複数のポートを開放することができる。例えば、外部のPSTN電話機(例えば、エンドポイント102)がAE114と通信できるように、ESBC MS116は外部ホストドメイン110に設置可能であり、外部ホストドメイン110において(ファイアウォール106およびESBC MS116の両方で)メディアトラフィック用に一連のポート(例えば、UDPポート49152-60152)が開放され得る。いくつかの実施形態では、PSTNのSIPトランク104とESBC MS116との間で確立されるメディア接続は、通信されるメディアトラフィックに機密性、メッセージ認証、およびリプレイ保護を提供するためにSRTPを使用することが要求される。

【0042】

いくつかの実施形態では、ESBC MS116は、シグナリングおよびメディアの暗号化を提供するように構成される。例えば、PSTNサービスプロバイダへのESBCアクセス側インターフェース(例えば、PSTN SIPトランク104)は、SIPシグナリング層の機密性を確保するためにTLSを使用する。同様に、ESBCアクセス側のメディア層は、メディアパスに対する機密性、メッセージ認証、およびリプレイ保護を提供するためにSRTPを使用する。TLSおよびSRTPに加えて、PSTNサービスプロバイダは、CCEシステムに対応するBmaasのパブリックIPからのコールのみを受け入れるためにプロビジョニングされている。他のCCEではないIPからPSTNのSIPトランク104に接続しようとしても、PSTNサービスプロバイダによって拒否される。同様に、CCEは、CCEサービスのためだけにプロビジョニングされている特

10

20

30

40

50

定の P S T N サービスプロバイダのパブリック IP からのシグナリングおよびメディアポートへの外部アクセスのみを許可するセキュリティリストをプロビジョニングしている。P S T N サービスプロバイダの IP アドレス以外のソースからのシグナリング/メディアポートへのアクセスは、E S B C M S 1 1 6 によって拒否される。

【 0 0 4 3 】

いくつかの実施形態では、E S B C M S 1 1 6 は、構成された「セッションエージェント」からの接続のみを許可することによって、C C E ネットワーク内で内部的にさらなる保護を提供する。E S B C 用語における「セッションエージェント」は、E S B C M S 1 1 6 が通信する S I P ホップであるため、C C E はアクセス側（すなわち、外部ホストドメイン IP アドレス）に 1 つ、およびサポートされる P S T N M S ごとに 1 つ、セッションエージェントを持つ。E S B C M S 1 1 6 は、これらの構成されたセッションエージェントからの S I P ダイアログのみを許可し、他のすべての IP からの試みを拒否する。

10

【 0 0 4 4 】

図 1 に示すように、ネットワーク 1 0 0 は、テナントオンボーディング (T O B) 管理者ユーザインタフェース (U I) 1 0 3 をさらに含む。このインターフェースを使用して、テナント管理者ユーザは、複数のテナントおよび/またはアソシエイトエンティティ（すなわち、システム加入者）のそれぞれについて、P S T N ルールをプロビジョニングおよび構成し得る。例えば、テナント管理者は、テナント構成テーブルにコンテキスト属性データを追加するために、T O B U I 1 0 3（これは、ユーザコンピューティングデバイスによってホストされかつ実行されるブラウザアプリケーションとして実現されてもよい）を利用し得る。テナント管理者は、その後、T O B U I 1 0 3 上で、1 つまたは複数のテナントまたはアソシエイトに対して、新たに定義されたコンテキスト属性を用いて P S T N ルールを構成し得る。特に、P S T N プロバイダ/ベンダが、C C E システムによってサポートされる A E に P S T N コールをルーティングできるように構成するために、T O B U I 1 0 3 を使用してプロビジョニングされたコンテキスト属性データが使用され得る。例えば、ルーティングルールの条件テーブルに発信元の P S T N 番号を指定し、かつ、事前に定義されたコールの宛先（例えば、対象の電話番号）として A E を指定するために、T O B U I 1 0 3 が使用し得る。このように、特定の P S T N エンドポイントまたは P S T N ベンダから発信されるすべてのコールシグナリングメッセージは、特定の A E（例えば、「チーム」）に明確にルーティングされ得る。

20

30

【 0 0 4 5 】

いくつかの実施形態では、テナント管理者によって構成されたセキュリティ情報は、管理データベースに保存される前に暗号化される。いくつかの実施形態では、プライベートデータを暗号化するために D K K e y が使用される。さらに、P S T N ベンダの認証情報は、プライベートな情報とみなされるが、テナントが契約した電話番号は、パブリックな情報として指定され得る。さらに、クロスマイクロサービスアクセスのために、A u t h M S の秘密鍵が P S T N M S ドメイン（例えば、内部ホストドメイン 1 1 2）に複製され、秘密鍵は、特定の T e n a n t K e y（テナントキー）/ C l i e n t I d（クライアント ID）のための J W T トークンを生成するために使用される。特に、J W T トークンは、アソシエイト M S 1 0 7 および S E M S 1 2 2 にアクセスするために、P S T N M S 1 1 8 によって使用される。J W T トークンの使用は、内部アクセスのために指定され、パブリック A P I はエクスポートされない。

40

【 0 0 4 6 】

いくつかの実施形態では、ルーティングルールは、R E S T フル (R E S T f u l) な構成データとして、対応する 1 つまたは複数のテナントマイクロサービス (T M S) 1 0 5 にルールをオンボードすることによって、1 つまたは複数のテナントにプロビジョニングされ得る。構成データを受信した後、T M S 1 0 5 は、1 つまたは複数の関連するアソシエイトマイクロサービス (A M S) 1 0 7 に同期メッセージを送信し得る。A M S 1 0 7 は、その後、加入したアソシエイト M S またはテナント M S に関連する P S T N エンド

50

ポイントのための特定のルーティングルールを指定するために、構成データを使用し得る。

【 0 0 4 7 】

図 2 は、本明細書に記載の主題の一実施形態に係る、P S T N エンドポイントと W e b R T C エンドポイントとの間で通信セッションを確立するための例示的なコールフローを示すシグナリング図である。図 2 に示すように、テナント管理者 (T A) 2 2 2 は、1 つまたは複数のテナントエンティティ (例えば、メッセージ 1 を参照) のそれぞれに対して P S T N 構成を割り当てるために、テナントオンボーディング (T O B) ユーザインタフェース 2 1 6 を利用する。いくつかの実施形態では、テナント管理者 2 2 2 は、C C E システムに加入してサポートするテナントの管理に対して責任を負うシステムユーザまたはオペレータである。特に、テナント管理者 2 2 2 は、C C E システムによってサービスを受けるテナントエンティティの構成データを更新し得る。

10

【 0 0 4 8 】

テナント管理者 2 2 2 による入力に応答して、T O B U I 2 1 6 は、R E S T フル (R E S T f u l l) 構成データ (テナントエンティティ用) を含むシグナリングメッセージをテナントマイクロサービス (T M S) 2 1 0 に送信するように構成される (例えば、メッセージ 2 を参照) 。テナント M S 2 1 0 は、その後、同期 (synchronization) の目的で、受信した構成 (configuration) 情報をアソシエイト M S (A M S) 2 0 8 に提供する (例えば、メッセージ 3 を参照) 。したがって、アソシエイト M S 2 0 8 は、このようにして、T O B U I 2 1 6 を用いてテナント管理者 2 2 2 によって元々指定された P S T N 構成情報でプロビジョニングされる。

20

【 0 0 4 9 】

図 2 に示すように、P S T N エンドポイント 2 0 2 は、(例えば、ユーザによって) A E 2 1 8 に対応するおよび / または A E 2 1 8 にマッピングされ得るアクセス番号をダイヤルするために利用される (例えば、メッセージ 4 を参照) 。ダイヤルされた番号情報は、P S T N ベンダ (vendor) 2 0 4 によって (例えば、P S T N S I P トランクを介して) 受信され、次に、P S T N ベンダ 2 0 4 は、外部ホストドメインおよび / または A E 2 1 8 に向けられた S I P I N V I T E メッセージ (例えば、メッセージ 5 を参照) を生成する。ファイアウォール、ロードバランサ、および指定された E B S C M S (上記説明および図 1 を参照) を通過した後、S I P I N V I T E メッセージ (例えば、メッセージ 6 を参照) は、外部ホストネットワークおよび / または E B S C M S によって選択された P S T N M S (例えば、P S T N M S 2 0 6) によって受信される。特に、P S T N M S 2 0 6 は、受信した S I P I N V I T E メッセージからエンドポイントコンテキスト属性情報を抽出し、このデータをプッシュコンテキストメッセージを介してアソシエイト M S 2 0 8 に提供する。

30

【 0 0 5 0 】

いくつかの実施形態では、アソシエイト M S 2 0 8 は、テナント管理者 2 2 2 によって最初に生成されたエージェントアプリケーションであって、P S T N エンドポイントからのコールに回答する責務を負う。いくつかの実施形態では、P S T N M S 2 0 6 は、R E S T A P I を介して送信されるプッシュコンテキストメッセージ (例えば、p u s h C o n t e x t (プッシュコンテキスト) / g e t A g e n t U r i (ゲットエージェント U r i) メッセージ) を用いて、エンドポイントコンテキスト属性情報をアソシエイト M S 2 0 8 に提供する (例えば、メッセージ 6 を参照) 。特に、エンドポイントコンテキスト属性情報は、受信した S I P I N V I T E メッセージのヘッダから抽出された情報を用いて、P S T N M S 2 0 6 によって生成され得る。例えば、エンドポイントコンテキスト属性情報は、S I P I N V I T E メッセージのヘッダに含まれる「 F r o m 」または「 T o 」情報を含み得る。

40

【 0 0 5 1 】

いくつかの実施形態では、アソシエイト M S 2 0 8 は、P S T N エンドポイント 2 0 2 からのコール要求に回答するために、どの A E が選択されるべきかを決定する責務を負う。プッシュコンテキストメッセージ (例えば、メッセージ 6 を参照) を受信すると、アソ

50

シエイトMS208は、ターゲットとして指定されるべきAEを示すローカルルーティンググループにアクセスするように構成されてもよい。上述したように、ルーティンググループは、PSTN MS206によって提供されたエンドポイントコンテキスト属性情報に含まれるデータに基づいて、ターゲットAEを指定し得る。いくつかの実施形態では、アソシエイトMS208は、エンドポイントコンテキスト属性情報を、AEアドレス識別子と各種コンテキスト属性に対応するデータとのマッピングを含むエントリを有するローカルルーティンググループデータベースのエントリと相互参照してもよい。

【0052】

アソシエイトMS208は、その後、コールをAE218などの選択された宛先AEにルーティングする（例えば、メッセージ7を参照）。コールを受信した後、AE218は、着信アラートを表示するように構成され得る（例えば、メッセージ8を参照）。そのような着信アラートは、コールを受信し、最終的にメディアセッション接続を確立するために、アソシエイトユーザ220（例えば、AE218のユーザ）に回答ボタン（例えば、メッセージ9を参照）を選択するよう促す視覚的表示および/または可聴信号とすることができる。アソシエイトユーザ220によって回答ボタンがインターフェースされ/アクティベートされた後、AE218は、アソシエイトユーザ220のアドレス識別子を含む「associateUserURI（アソシエイトユーザURI）」メッセージ（例えば、メッセージ10参照）などの応答メッセージをアソシエイトMS208に送信する。いくつかの実施形態では、アドレス識別子は、AE218および/またはアソシエイトユーザ220に対応するURI（uniform resource identifier）アドレスであり得る。

【0053】

したがって、アソシエイトMS208は、アソシエイトユーザURI情報を含むメッセージをPSTN MS206に転送し、PSTN MS206は、シグナリングエンジン（SE）MS212とのWebSocket接続の確立を開始する。例えば、PSTN MS206は、WebSocket接続を確立するために、JSON RTC接続要求メッセージなどのWeb RTCメッセージを生成し、SE212に送信する。SE212からの応答を受信した後、PSTN MS206は、JSON RTC開始要求メッセージをSE212に送信する。

【0054】

開始要求メッセージを受信した後、SE212はSDP要求メッセージ（AE218用）をME MS214に送信する。ME MS214は、メディアチャネルのパラメータ、例えば、メディアを送信するためのコーデックをネゴシエートするために、エンドポイントによって使用されるSDPメッセージで応答する。SDPメッセージは、また、JSON RTC開始要求メッセージをAE218に送信するようにSE212を促す。AE218は、JSON RTC応答メッセージで応答する。これに応答して、SE MS212は、次に、ME MS214にSDPメッセージを送信する。ME MS214からSDPメッセージを受信した後、SE212は、最初のJSON開始要求メッセージに対する応答として、JSON RTC開始応答メッセージをPSTN MS206に送り返す。これに応答して、PSTN MS206は、200 SIP INVITE確認（acknowledge）メッセージを（PSTN SIPトランクを介して）PSTNベンダ204に伝達するためのトリガとなる。PSTNベンダ204は、その後、エンドポイント202とAE218との間のメディア接続を完成するために、PSTN MS206に確認（acknowledge）メッセージを送信する。

【0055】

図3は、本明細書に記載された主題の一実施形態に係る、PSTNエンドポイントとWeb RTCエンドポイントとの間で通信セッションを確立するための例示的なプロセスまたは方法300を示すフローチャートである。いくつかの実施形態では、図3に示される方法300は、ハードウェアプロセッサによって実行されたときに、ブロック302~308のうちの1つまたは複数を実行する、メモリに格納されたアルゴリズムである。

【0056】

10

20

30

40

50

ブロック302において、公衆交換電話網（PSTN）マイクロサービス（MS）によって、PSTNエンドポイントからSIPベースのシグナリングメッセージが受信される。いくつかの実施形態では、PSTNは、PSTNエンドポイントデバイスからSIP INVITEメッセージを受信する。特に、SIP INVITEメッセージは、（CCEシステムの内部ホストドメインにある）PSTN MSに到達する前に、ファイアウォール、ロードバランサ、および（CCEの外部ホストドメインにある）ESBC MSを通過してもよい。

【0057】

ブロック304において、PSTN MSによって、SIPベースのシグナリングメッセージからエンドポイントコンテキスト属性情報が取得される。いくつかの実施形態では、PSTN MSは、シグナリングメッセージから「to」および「from」データを抽出するために、受信したSIP INVITEメッセージのヘッダを解析する。PSTN MSは、ルーティングルールでプロビジョニングされているアソシエイトMSに、エンドポイントコンテキスト属性情報をプッシュする。エンドポイントコンテキスト属性情報の受信に回答して、アソシエイトMSは、ローカルルーティングルールデータベースにアクセスし、ターゲットAEに対応するアドレス識別子を特定し、その識別子をPSTN MSに提供する。アドレス識別子は、ターゲットAEに対応するURIであってもよい。

【0058】

ブロック306において、PSTN MSによって、エンドポイントコンテキスト属性情報に関連付けられたアソシエイトエンドポイント（AE）のアドレス識別子を含むウェブリアルタイム通信（WebRTC）ベースのシグナリングメッセージが生成される。いくつかの実施形態では、PSTN MSは、アドレス識別子に対応するターゲットAEとの通信セッションを要求するJSON RTCメッセージなどのWeb RTCメッセージを生成する。

【0059】

ブロック308において、PSTNエンドポイントとAEとの間のコールセッションを開始するために、WebRTCベースのシグナリングメッセージがPSTN MSによってAEに送信される。いくつかの実施形態では、PSTN MSは、AEと送信するPSTNエンドポイントとの間のコールセッションを確立するために、JSON RTCメッセージをAEの宛先に向ける。

【0060】

本開示の主題のさまざまな詳細が本開示の主題の範囲から逸脱することなく変更され得ることが理解されるであろう。さらに、上述の説明は、例示のみを目的としたものであって、限定を目的としたものではない。

10

20

30

40

50

【図面】
【図 1】

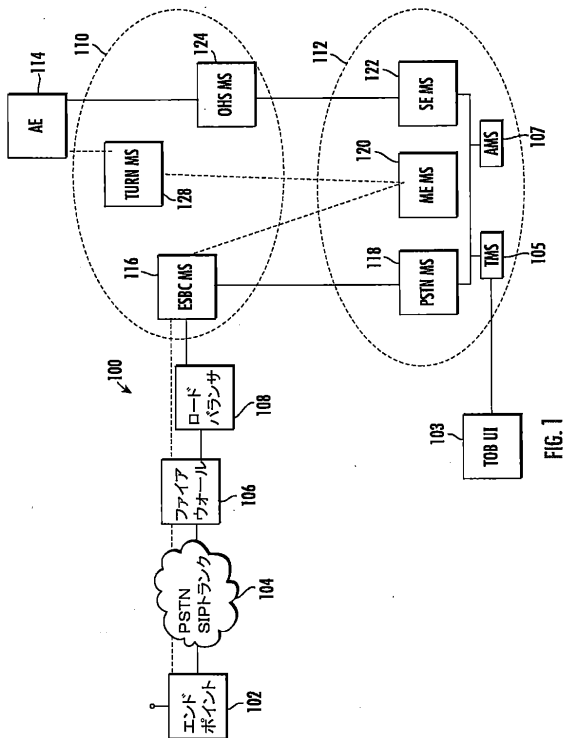


FIG. 1

【図 2】

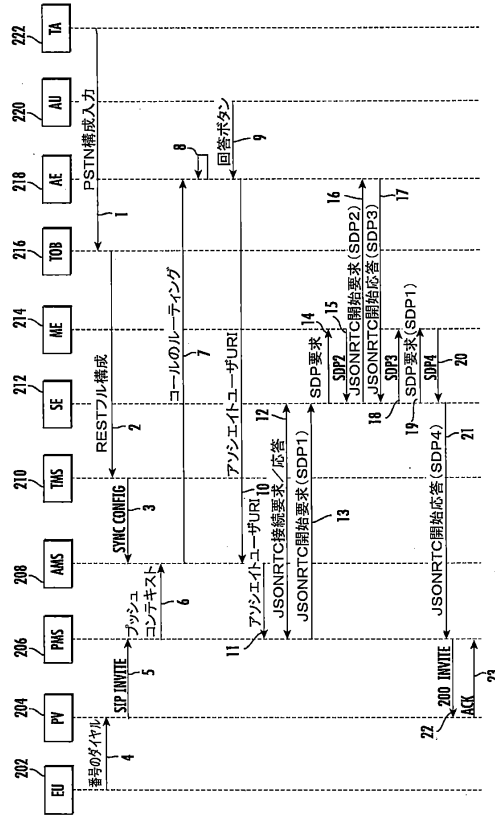


FIG. 2

【図 3】

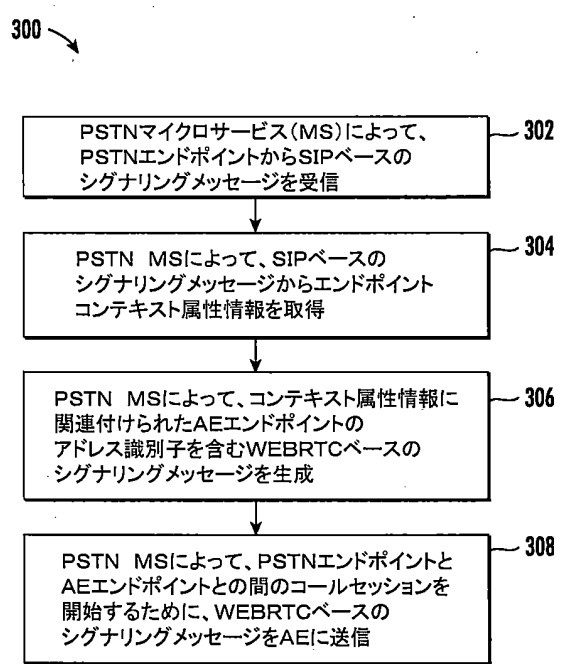


FIG. 3

10

20

30

40

50

フロントページの続き

(54)【発明の名称】 タ可読媒体

ン、チャオヤン・ディストリクト、ズーバーホーベイリー、ナンバー・26

(72)発明者 メロ, マイケル・デイビッド

アメリカ合衆国、01701 マサチューセッツ州、フレーミングハム、バーチ・ロード、24

(72)発明者 ココ, フランク

アメリカ合衆国、03079 ニュー・ハンプシャー州、セーレム、ザイオン・ヒル・ロード、6

審査官 中川 幸洋

(56)参考文献 米国特許出願公開第2014/0126714 (US, A1)

音声・ビデオ通話が変わる! WebRTCのインパクト Part 3 企業コミュニケーションでの活用法, テレコミュニケーション, 第31巻第6号, 2014年06月, pp.21-25

(58)調査した分野 (Int.Cl., DB名)

H04L 65/1108

H04M 3/00

H04L 67/02

H04L 67/141

H04L 65/1104