(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5330540号
(P5330540)

(45)発行日　平成25年10月30日(2013.10.30)　(24)登録日　平成25年8月2日(2013.8.2)

(51)Int.Cl.		F I		
H04L 12/70	(2013.01)	H04L	12/70	A
H04M 3/00	(2006.01)	H04M	3/00	B
H04W 12/08	(2009.01)	H04W	12/08	
H04W 80/10	(2009.01)	H04W	80/10	

請求項の数 7　(全 25 頁)

(21)出願番号　特願2011-542902 (P2011-542902)
(86)(22)出願日　平成20年12月26日 (2008.12.26)
(65)公表番号　特表2012-514364 (P2012-514364A)
(43)公表日　平成24年6月21日 (2012.6.21)
(86)国際出願番号　PCT/IB2008/003630
(87)国際公開番号　WO2010/073061
(87)国際公開日　平成22年7月1日 (2010.7.1)
審査請求日　平成23年11月25日 (2011.11.25)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン（パブル）
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】企業ネットワークアクセスポイントの判定のための方法およびシステム

(57)【特許請求の範囲】
【請求項１】
在圏ネットワークから企業ネットワークへ通信をルーティングする方法であって、
前記在圏ネットワークから、宛先ユーザアドレスを含むクエリメッセージを送信するステップと、
前記在圏ネットワークにおいて、前記宛先ユーザアドレスに関連する内部メッセージルーティング情報とアクセスポイント識別情報とを含む応答メッセージを受信するステップと、
前記在圏ネットワークにおいて、前記アクセスポイント識別情報をメッセージに組み込むステップと、
前記在圏ネットワークが、前記内部メッセージルーティング情報に基づいて、前記メッセージを前記アクセスポイント識別情報に関連するアクセスポイントへ送信するステップと、
を備え、
前記在圏ネットワークと前記企業ネットワークとの間の相互接続は、加入相互接続であり、
前記在圏ネットワークが、前記内部メッセージルーティング情報に基づいて、前記メッセージを前記アクセスポイント識別情報に関連するアクセスポイントへ送信する前記ステップは、
前記内部メッセージルーティング情報に基づいて、前記メッセージを、仮想プライベ

ートネットワーク・ルーティング機能（ＶＰＮ－ＲＦ）からインテロゲーティング呼セッション制御機能（Ｉ－ＣＳＣＦ）へ送信するステップと、
前記宛先ユーザアドレスに関連するアクセスポイント識別情報を含むクエリメッセージを前記Ｉ－ＣＳＣＦから送信するステップと、
前記宛先ユーザアドレスに関連する前記アクセスポイント識別情報を用いてルックアップを実行するステップであって、当該ルックアップに基づいてサービング呼セッション制御機能（Ｓ－ＣＳＣＦ）が特定される、ステップと、
前記メッセージを前記特定されたＳ－ＣＳＣＦへ送信するステップと、
前記メッセージを前記Ｓ－ＣＳＣＦからプロキシ呼セッション制御機能（Ｐ－ＣＳＣＦ）へ転送するステップと、
前記Ｐ－ＣＳＣＦが、前記宛先ユーザアドレスに関連する前記アクセスポイント識別情報を削除するステップと、
前記メッセージを前記アクセスポイントへ転送するステップと、
を更に含む
ことを特徴とする方法。
【請求項２】
在圏ネットワークから企業ネットワークへ通信をルーティングする方法であって、
前記在圏ネットワークから、宛先ユーザアドレスを含むクエリメッセージを送信するステップと、
前記在圏ネットワークにおいて、前記宛先ユーザアドレスに関連する内部メッセージルーティング情報とアクセスポイント識別情報とを含む応答メッセージを受信するステップと、
前記在圏ネットワークにおいて、前記アクセスポイント識別情報をメッセージに組み込むステップと、
前記在圏ネットワークが、前記内部メッセージルーティング情報に基づいて、前記メッセージを前記アクセスポイント識別情報に関連するアクセスポイントへ送信するステップと、
を備え、
前記在圏ネットワークと前記企業ネットワークとの間の相互接続は、ピアリング相互接続であり、
前記在圏ネットワークが、前記内部メッセージルーティング情報に基づいて、前記メッセージを前記アクセスポイント識別情報に関連するアクセスポイントへ送信する前記ステップは、
前記内部メッセージルーティング情報に基づいて、前記メッセージを、仮想プライベートネットワーク・ルーティング機能（ＶＰＮ－ＲＦ）から相互接続境界制御機能（ＩＢＣＦ）へ送信するステップと、
前記ＩＢＣＦが、前記宛先ユーザアドレスに関連する前記アクセスポイント識別情報を削除するステップと、
前記メッセージを前記アクセスポイントへ転送するステップと、
を更に含む
ことを特徴とする方法。
【請求項３】
前記メッセージは、セッション開始プロトコル（ＳＩＰ）メッセージである
ことを特徴とする請求項１又は２に記載の方法。
【請求項４】
前記アクセスポイント識別情報は、前記メッセージ中のＰ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダに組み込まれる
ことを特徴とする請求項１に記載の方法。
【請求項５】
前記アクセスポイント識別情報は、前記メッセージ中のＰ－Ｓｅｒｖｅｄ－Ｕｓｅｒへ

ッダに組み込まれる
ことを特徴とする請求項２に記載の方法。
【請求項６】
前記内部メッセージルーティング情報は、使用すべき前記Ｉ－ＣＳＣＦを識別し、セッション開始プロトコル（ＳＩＰ）ルートヘッダに組み込まれる
ことを特徴とする請求項１に記載の方法。
【請求項７】
前記内部メッセージルーティング情報は、使用すべき前記ＩＢＣＦを識別し、ＳＩＰルートヘッダに組み込まれる
ことを特徴とする請求項２に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本書の例示的実施形態は、一般にシステムとデバイスとソフトウェアと方法とに関し、より詳細には、相互接続ネットワークを通って企業内のユーザにメッセージをルーティングするためのメカニズムおよび技法に関する。
【背景技術】
【０００２】
技術的能力が拡大を続けるのにつれて、通信の選択肢は多様化してきた。例えば、この３０年余りの間に通信業界では個人間の通信が進化し、以前は家庭にダイヤル式電話が１台しかなかったのに、今では家庭には電話とケーブルと、および／または、音声とデータとの両方に対応する光ファイバ回線とが複数ある。さらに、携帯電話およびＷｉ－Ｆｉによって、通信に移動要素が加わった。同様に娯楽業界では、３０年前にはテレビ用のフォーマットは１つしかなく、このフォーマットが電波で送信され、家庭にあるアンテナを介して受信された。これが進化して、例えばＳＤＴＶ（ｓｔａｎｄａｒｄ ｄｅｆｉｎｉｔｉｏｎ ｔｅｌｅｖｉｓｉｏｎ：標準画質テレビ）、ＥＤＴＶ（ｅｎｈａｎｃｅｄ ｄｅｆｉｎｉｔｉｏｎ ＴＶ）、およびＨＤＴＶ（ｈｉｇｈ ｄｅｆｉｎｉｔｉｏｎ ＴＶ：高精細度テレビジョン）のように画質の標準が多様化しただけでなく、ケーブルや衛星というように、これらの多様なテレビジョン表示フォーマットを配信するためのシステムも多様化した。さらに、これらの２つの業界の間で各種のサービスが成長してオーバラップするようになってきた。これらのシステムが両方の業界において進化し続けるにつれて、サービス提供は融合し続けるであろうし、消費者は新たなサービスの利用可能性を期待できよう。また、これらのサービスの一部は、より多くの情報を処理して出力するための技術的能力に基づくことが予想される。
【０００３】
通信業界と娯楽業界との両方に影響を与えるもう１つの関連技術は、相互接続ネットワークである。また、これらの通信ネットワークと関連の通信ストリームとの物理的構造の進化によって、より多量のデータフローを処理できるようになってきた。サーバは、かつてないほど多量のメモリを有し、これまで以上の高い帯域幅を有する通信リンクが存在し、プロセッサは以前より高速かつ高性能であり、そして、これらの要素を活用するプロトコルが存在する。これらの通信ネットワークは、ユーザと企業とを結びつけるものであれば、いかなるネットワークであってもよい。消費者によるこれらのネットワークの利用が増加すれば、この増加は、サービス提供のための、相互接続されうるより多くのネットワークの創造を促す可能性がある。これらのサービスには、例えば、ＩＰＴＶ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｔｅｌｅｖｉｓｉｏｎ：ＩＰデータパケットを用いるネットワーク経由でテレビ番組を配信するシステムまたはサービスのことを言う）と、インターネットラジオと、ビデオ・オン・デマンド（ＶｏＤ）と、ライブイベントと、ＶｏＩＰ（Ｖｏｉｃｅ ｏｖｅｒ ＩＰ：ＩＰ電話）と、その他の単独で受信されるかまたはバンドルで一緒に受信されるウェブ関連サービスとが含まれてもよい。また、技術革新とサービス拡大とに伴って、新たなネットワークと通信プロトコル、例えば、ＩＭＳ（Ｉｎｔｅｒ

ｎｅｔ Ｐｒｏｔｏｃｏｌ Ｍｕｌｔｉｍｅｄｉａ Ｓｕｂｓｙｓｔｅｍ：ＩＰマルチメディア・サブシステム）ネットワークおよびＳＩＰ（ｓｅｓｓｉｏｎ ｉｎｉｔｉａｔｉｏｎ ｐｒｏｔｏｃｏｌ：セッション開始プロトコル）が開発されて、これらの多様なサービスを改良し、それらの利用を進めた。

【０００４】

通信ネットワークの１つの特徴は、そのようなネットワークが多数存在し（それぞれがネットワークオペレータによって運用され）、そして、これらのネットワークが相互接続されていることである。この相互接続は、２つのネットワーク間で直接的であってもよいし、１つ以上の相互接続ネットワークまたは中継ネットワークを介して間接的であってもよい。これらのネットワークオペレータ各社は、その相互接続パートナ各社と業務上のＳＬＡ（サービス品質保証契約）を締結しているであろうし、１）宛先ユーザアドレスと、２）業務上のＳＬＡと、に基づいてルーティングの決定を行う装置を有するであろう。宛先ユーザアドレスは或るユーザを識別し、このユーザは或るネットワークオペレータによってサービス提供される。宛先ユーザアドレスは、電話番号であってもよいし、何らかの電子メールのような形式のＵＲＩ（ｕｎｉｆｏｒｍ ｒｅｓｏｕｒｃｅ ｉｄｅｎｔｉｆｉｅｒ：ユニフォーム・リソース・アイデンティファイア）であってもよい。後者の場合、宛先ユーザアドレスは、例えばｊｏｈｎ@ｂａｎｋ．ｃｏｍ、ｊｏｈｎ@ｂａｌｄｗｉｎ．ｏｒｇのように、在圏ネットワークオペレータを即座に識別しないことがある。これは、要求をどうルーティングするかを発信側ネットワークオペレータが知ることの難しさを示す。

【０００５】

従って、多様な相互接続ネットワーク経由の通信を改良するためのデバイス、システム、および方法を提供することが望ましいであろう。

【発明の概要】

【０００６】

例示的実施形態によるシステムおよび方法が、多様な相互接続ネットワーク経由の通信フローを改良するためのシステムと方法とを提供することによって、このニーズなどに対応する。

【０００７】

例示的な一実施形態によれば、在圏ネットワークから企業ネットワークへ通信をルーティングする方法は、前記在圏ネットワークから、宛先ユーザアドレスを含むクエリメッセージを送信するステップと、前記在圏ネットワークにおいて、前記宛先ユーザアドレスに関連する内部メッセージルーティング情報とアクセスポイント識別情報とを含む応答メッセージを受信するステップと、前記在圏ネットワークにおいて、前記アクセスポイント識別情報をメッセージに組み込むステップと、前記在圏ネットワークが、前記内部メッセージルーティング情報に基づいて、前記メッセージを前記アクセスポイント識別情報に関連するアクセスポイントへ送信するステップと、を備える。

【０００８】

別の例示的実施形態によれば、通信ノードにおける、通信をルーティングするための方法は、複数の宛先ユーザアドレスを記憶するステップであって、各宛先ユーザアドレスがアクセスポイントおよび内部メッセージルーティング情報に関連付けられる、ステップと、宛先ユーザアドレスを含むクエリメッセージを受信するステップと、前記宛先ユーザアドレスを用いてルックアップを実行して対応するアクセスポイントおよび内部メッセージルーティング情報を判定するステップと、前記ルックアップにより特定された、前記対応するアクセスポイントおよび内部メッセージルーティング情報に基づく情報を含む応答メッセージを送信するステップと、を備える。

【０００９】

更に別の例示的実施形態によれば、通信ノードは、宛先ユーザアドレス、アクセスポイント識別情報、および内部メッセージルーティング情報を記憶するメモリと、前記宛先ユーザアドレス、前記アクセスポイント識別情報、および前記内部メッセージルーティング

情報に関連するメッセージを送受信する通信インタフェースと、前記宛先ユーザアドレスを含むクエリが受信された場合に、前記アクセスポイント識別情報および前記内部メッセージルーティング情報を結果として返すルックアップを実行するプロセッサと、を備え、前記通信インタフェースは、前記アクセスポイント識別情報および前記内部メッセージルーティング情報を含む応答メッセージを送信する。

【００１０】

添付の図面は、本明細書に組み込まれて本明細書の一部を構成するものであって、１つ以上の実施形態を図解し、記述と共にこれらの実施形態を説明する。

【図面の簡単な説明】

【００１１】

【図１】例示的実施形態による、相互接続ネットワーク経由で中継される通信を示す図である。

【図２】ＩＭＳ（インターネットプロトコル・マルチメディア・サブシステム）ネットワークの相互接続を図解する図である。

【図３（ａ）】加入相互接続のためのＥＴＳＩ（Ｅｕｒｏｐｅａｎ　Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｓｔａｎｄａｒｄｓ　Ｉｎｓｔｉｔｕｔｉｏｎ）　ＴＳ　１８２　０２５のアーキテクチャを示す図である。

【図３（ｂ）】ピアリング相互接続のためのＥＴＳＩ　ＴＳ　１８２　０２５のアーキテクチャを示す図である。

【図４】例示的実施形態による、相互接続されたプライベートネットワークを描いた図である。

【図５】例示的実施形態による、メッセージトラヒックをルーティングするためのシグナリング図である。

【図６】例示的実施形態による、１つの企業が２つの在圏オペレータネットワークに関連する場合の通信アーキテクチャを示す図である。

【図７】例示的実施形態による、メッセージトラヒックをルーティングするための複数の在圏オペレータの選択肢を伴う応答を含むシグナリング図である。

【図８】例示的実施形態による、ＩＭＳネットワークの要素を示す図である。

【図９】例示的実施形態による、アクセスポイントテーブルの使用を図解する図である。

【図１０】例示的実施形態による、相互接続タイプに基づくメッセージトラヒックの配信を描く図である。

【図１１（ａ）】、

【図１１（ｂ）】例示的実施形態による、メッセージトラヒックを在圏ネットワークから企業にいるユーザに配信するためのシグナリング図である。

【図１２】例示的実施形態による通信ノードの図である。

【図１３】例示的実施形態による、在圏ネットワークからの通信をルーティングするための方法のフローチャートである。

【図１４】例示的実施形態による、通信ノードで通信をルーティングするための別の方法のフローチャートである。

【発明を実施するための形態】

【００１２】

例示的実施形態についての下記の記述は、添付の図面を参照する。別の図面における同じ参照番号は、同じかまたは類似の要素を示す。下記の詳細記述は、本発明を限定するものではない。そうではなく、本発明の範囲は、添付の請求項によって定義される。下記の実施形態は、話を簡単にするために、以下に記述する通信ネットワークの用語および構造に関して論じている。しかし、次に論じることになる実施形態は、これらのシステムに限定されるのではなく、他の既存の通信システムに適用されうる。

【００１３】

本明細書を通じて、「一実施形態」または「ある実施形態」または「例示的実施形態」への言及は、ある実施形態に関連して述べた特定の特徴、構造、または特性が、本発明の

少なくとも１つの実施形態に含まれることを意味する。従って、本明細書の全体を通じていろいろな箇所で「一実施形態では」または「ある実施形態では」または「例示的実施形態では」という表現があっても、必ずしもそれらすべてが同じ実施形態に言及しているとは限らない。また、特定の特徴、構造または特性が、１つ以上の実施形態においていずれかの適切なやり方で組み合わされてもよい。

【００１４】

上記のように、各種の相互接続ネットワーク経由の通信を改良するためのデバイス、システム、および方法を提供することが望ましい。以下の例示的実施形態は、メッセージ、例えばＳＩＰ（セッション開始プロトコル）メッセージを、多様な相互接続ネットワーク経由で、例えば、ＩＭＳ（インターネットプロトコル・マルチメディア・サブシステム）を用いるネットワーク経由で、ルーティングすることについて記述する。この議論について何らかの文脈を提供するために、図１に例示的な通信の枠組みを示す。

【００１５】

例示的実施形態によれば、図１は、複数の相互接続ネットワーク経由で中継される通信を使って、或るユーザが別のユーザ（または、企業内のリソース、例えば会社内のデバイスまたは人物）と通信することを示す。詳細には、例示的な通信の枠組み１００は、ユーザ１　１０２が、例えばＳＩＰメッセージを送信することができるデバイス、例えば移動電話およびコンピュータを使って企業／ユーザ２　１１０と通信することを示す。これらのＳＩＰメッセージは、最初に発信側ネットワーク１０４を通って、次いで１つ以上の中継ネットワーク１０６を通って、次いで在圏ネットワーク１０８を通って送信される。しかし、これらの多様なネットワーク、例えば各種のパブリック通信ネットワークおよび相互接続ネットワークにおいてそのようなメッセージをアドレス指定するのに用いられるＤＮＳ（ｄｏｍａｉｎ　ｎａｍｅ　ｓｙｓｔｅｍ：ドメイン・ネーム・システム）の規則に関して多様な提案が存在し、それが、今度は、これらのＳＩＰメッセージの正確かつ効率的な配信についての課題となる。また本書では、「発信側ネットワーク」、「発信側オペレータネットワーク」および「発信側ネットワークオペレータ」とは、呼を開始するデバイスが接続している発信側ネットワークのことを言う。また本書では、「在圏ネットワーク」、「在圏オペレータネットワーク」および「在圏ネットワークオペレータ」とは、エンドユーザにサービス提供し、呼を宅内ユーザまたは企業内ユーザに配信するネットワークのことを言う。

【００１６】

ＩＭＳネットワークを相互接続するための１つのありうる枠組みが、図２に示すようにＧＳＭＡ（Ｇｌｏｂａｌ　Ｓｙｓｔｅｍ　ｆｏｒ　Ｍｏｂｉｌｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ａｓｓｏｃｉａｔｉｏｎ）によって提案されている。このグローバルなサービスプロバイダ間のＩＰバックボーンは、典型的にはＩＰＸ（Ｉｎｔｅｒｎｅｔｗｏｒｋ　Ｐａｃｋｅｔ　Ｅｘｃｈａｎｇｅ）と呼ばれ、ＧＳＭＡ　ＩＲ．３４の中に記述されている。この枠組みの中には、オペレータＡ　２０２とオペレータＢ　２０４とが含まれ、それらはいずれもＩＰＸプロバイダＸ　２０８に接続しており、さらにオペレータＣ　２１４も含まれるが、こちらはＩＰＸプロバイダＹ　２１０に接続している。ＩＰＸプロバイダＸ　２０８およびＩＰＸプロバイダＹ　２１０は、ＩＰＸ２０６の一部であり、ＥＮＵＭ（Ｅｌｅｃｔｒｏｎｉｃ　Ｎｕｍｂｅｒ　Ｍａｐｐｉｎｇ　Ｓｙｓｔｅｍ）を備えたＤＮＳ（ｄｏｍａｉｎ　ｎａｍｅ　ｓｙｓｔｅｍ）ルートデータベース２１２と通信する。ＩＰＸ２０６の１つの目的は、合意された共同利用できるサービス定義および業務契約、例えばＳＬＡ（サービス品質保証契約）に従ってサービスプロバイダ間の相互接続を円滑化することである。これを円滑化するために、ＩＰＸ２０６は、この通信の枠組みに複数の利害関係者を導入することによって、ＧＰＲＳ（ｇｅｎｅｒａｌ　ｐａｃｋｅｔ　ｒａｄｉｏ　ｓｅｒｖｉｃｅ）のアーキテクチャの上にＧＲＸ（ｒｏａｍｉｎｇ　ｅｘｃｈａｎｇｅ）を構築してＧＰＲＳのアーキテクチャを拡張する。これらの利害関係者には、固定ネットワークオペレータ、インターネットサービスプロバイダ、およびアプリケーションサービスプロバイダが含まれうる。ＩＰＸ２０６は、メッセージトラヒックをルーティ

ングする目的で、自分自身のＤＮＳインフラストラクチャを有すると想定され、その関連情報はＤＮＳルートデータベース２１２の中に記憶されうる。ＩＰＸに接続するオペレータのためのＧＳＭＡが定義したＤＮＳ命名規則は、ＭＮＣ（ｍｏｂｉｌｅ ｎｅｔｗｏｒｋ ｃｏｄｅ）とＭＣＣ（ｍｏｂｉｌｅ ｃｏｕｎｔｒｙ ｃｏｄｅ）とを利用することに基づいている。ＧＳＭＡ提案に基づくＳＩＰメッセージのための一意の識別情報の一例をあげると、以下のようであろう。

ｓｉｐ：＋４４７７０３１２３４５６@ｍｎｃ００１．ｍｃｃ２３４．３ｇｐｐｎｅｔｗｏｒｋｓ．ｏｒｇ

【００１７】

ネットワークの相互接続のためのもう１つの提案が、ＥＴＳＩ（Ｅｕｒｏｐｅａｎ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｔａｎｄａｒｄｓ Ｉｎｓｔｉｔｕｔｉｏｎ）ＴＩＳＰＡＮ（Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ ａｎｄ Ｉｎｔｅｒｎｅｔ Ｓｅｒｖｉｃｅｓ ａｎｄ Ｐｒｏｔｏｃｏｌｓ ｆｏｒ Ａｄｖａｎｃｅｄ Ｎｅｔｗｏｒｋｓ）ＮＧＮ（ｎｅｘｔ ｇｅｎｅｒａｔｉｏｎ ｎｅｔｗｏｒｋ：次世代ネットワーク）リリース２によって行われた。より詳細には、図３（ａ）に示すように、ＥＴＳＩ ＴＳ １８２ ０２５は、ビジネス・トランキング(business trunking)ＮＧＣＮ（ｎｅｘｔ ｇｅｎｅｒａｔｉｏｎ ｃｏｒｐｏｒａｔｅ ｎｅｔｗｏｒｋ：次世代企業ネットワーク）３０４が、加入に基づいて在圏オペレータのＩＭＳネットワーク３０２にどのようにして接続されうるかについてのアーキテクチャ３００を提供する。Ｇｍ参照ポイント３０６は、在圏オペレータのＩＭＳネットワーク３０２と企業ネットワークとの境界を示す。加入相互接続の場合、ＮＧＣＮ３０４は、ＩＭＳの文脈の中の単一ユーザとして実現され、ＮＧＣＮ３０４は、在圏オペレータのＩＭＳネットワーク３０２にユーザ登録を行うと想定される。次いで、在圏オペレータのＩＭＳネットワーク３０２は、ＣＳＣＦ（呼セッション制御機能）、例えばＳ－ＣＳＣＦ（サービングＣＳＣＦ）３１０およびＰ－ＣＳＣＦ（プロキシＣＳＣＦ）３０８、並びにＡＳ（アプリケーションサーバ）３１２を通してユーザにサービスを提供することができる。

【００１８】

ＥＴＳＩ ＴＳ １８２ ０２５は、その他のビジネスシナリオについて図３（ａ）に示すアーキテクチャの変形を可能にし、そしてそれを特定する。一例では、図３（ｂ）に示すように、ビジネス・トランキングＮＧＣＮが、加入協定の代わりにピアリング協定によって在圏オペレータのＩＭＳネットワーク３０２に接続する。ピアリング相互接続の場合、在圏オペレータのＩＭＳネットワーク３０２の中には、ＮＧＣＮ３０４についてのユーザがいない。代わりに、ＮＧＣＮ３０４は、在圏オペレータのＩＭＳネットワーク３０２の中で、ＩＢＣＦ（Ｉｎｔｅｒｃｏｎｎｅｃｔ Ｂｏｒｄｅｒ Ｃｏｎｔｒｏｌ Ｆｕｎｃｔｉｏｎ：相互接続境界制御機能）３１４を通してルーティングされるセッション情報と共にＩＢＣＦ３１４によって示される。

【００１９】

Ｈｏｓｔｅｄ Ｅｎｔｅｒｐｒｉｓｅ Ｓｅｒｖｉｃｅ（ホストされた企業サービス）ＮＧＣＮと呼ばれる別のケースでは、ＮＧＣＮ３０４の中の各ユーザが、在圏オペレータのＩＭＳネットワーク３０２の中の１人のユーザとして実現され、従って、ＮＧＣＮ３０４の中の各ユーザが、在圏オペレータのＩＭＳネットワーク３０２にユーザ登録し、ＣＳＣＦを通してサービスをルーティングしてもらうと想定される。また、大企業のネットワーク（または複数のネットワーク）については、ＮＧＣＮ３０４のサイトと在圏オペレータネットワーク（または各種の在圏オペレータネットワーク）との間のこれらの接続に複数の事例がある可能性があり、この場合、これらの接続の事例は、上記の３つのケースが混じり合ったものでありうる。

【００２０】

上述したこれらのケースの各々において、ＴＩＳＰＡＮアーキテクチャを用いてＳＩＰメッセージを通信することができ、それによってユーザは、ＲＦＣ（ｒｅｑｕｅｓｔ ｆｏｒ ｃｏｍｍｅｎｔｓ）３２６１の中で記述されたようにｓｉｐ：ｕｓｅｒ@ｄｏｍａ

ｉｎという形式のＵＲＩ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｉｄｅｎｔｉｆｉｅｒ）によってアドレス指定されることができる。企業、例えば会社の場合には、ＵＲＩは、電子メールアドレスから導出することができ、例えば、ｓｉｐ：ｊｏｈｎ@ｅｎｔｅｒｐｒｉｓｅ．ｃｏｍのように表されてもよいだろうし、あるいは、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）－ＰＢＸ（Ｐｒｉｖａｔｅ Ｂｒａｎｃｈ ｅＸｃｈａｎｇｅ）から導出することができ、例えばｓｉｐ：８５０１２３４@ｅｎｔｅｒｐｒｉｓｅ．ｃｏｍ；ｕｓｅｒ＝ｐｈｏｎｅのように表されてもよいだろう。その他の許容される選択肢には、宅内ユーザ、例えばｓｉｐ：ｊｏｈｎ@ｂａｌｄｗｉｎ．ｏｒｇまたは、ユーザフレンドリーなオペレータ名、例えば、ｓｉｐ：ｊｏｈｎ@ｔｅｌｉａ．ｓｅ等がある。

【００２１】

ＧＳＭＡおよびＴＩＳＰＡＮによって定義された、提案のネットワークアーキテクチャの文脈では、既存の標準および解決策は、ＲＦＣ３２６１に基づいて上記で示した形式のＳＩＰ ＵＲＩにアドレス指定されたセッションを発信側オペレータがどのようにルーティングできるかに関して、決定的とはいえない。この分野では、諸標準は、ＳＩＰ ＵＲＩにアドレス指定されたセッションをルーティングするため、ＤＮＳの使用を一般的に言及するが、それは、いろいろな理由で大規模な展開には不十分である。例えば、複数のネットワークが関与する場合、各ネットワークは、ＩＰＸ用に提案されたもののような共有ＤＮＳに接続するだけでなく、内部的なＤＮＳを有することがある。しかし、各種の標準は、これらの多様なＤＮＳがどのようにして設定され使用されることになるのかを記述していない。事態を一層複雑にするのだが、完全修飾ドメイン名（ｆｕｌｌｙ ｑｕａｌｉｆｉｅｄ ｄｏｍａｉｎ ｎａｍｅｓ：ＦＱＤＮ）がパブリックインターネット上に数千万も存在することを考えると、一意のアドレスの全体量は相互接続ネットワークでも同様となりうるだろうと想定されることから、スケーラビリティが問題である。これは、トラヒック、例えばＳＩＰトラヒックを複数の相互接続ネットワーク経由でルーティングするための課題となりうる。

【００２２】

加えて、オペレータ各社は、他のパブリックネットワークへの自社の相互接続の知識だけでなく、これらのネットワークオペレータ各社に対する相互接続合意に基づいてルーティングの決定をしたいと望むことが多い。この情報は、彼らのローカルなＤＮＳサーバや関連のインフラストラクチャによって完全に供給されるとは限らない。在圏ネットワークオペレータがＵＲＩから容易に導出できないＳＩＰ ＵＲＩも多い。例えば、ｓｉｐ：ｊｏｈｎ@ｅｎｔｅｒｐｒｉｓｅ．ｃｏｍまたはｓｉｐ：ｊｏｈｎ@ｂａｌｄｗｉｎ．ｏｒｇまたはｊｏｈｎ@ｂｒａｎｄ＿ｎａｍｅ．ｃｏｍのようなＳＩＰ ＵＲＩには、在圏ネットワークオペレータが示されない。従って、特定のオペレータにメッセージをルーティングするのに複数のやり方がある場合、発信側オペレータがどの相互接続選択肢を用いるかという決定は、典型的には、企業ユーザまたは宅内ユーザにサービス提供しているオペレータの知識に基づいて行われうるだけである。また、電話セッションについての既存の課金モデルは、一部は発呼ユーザと被呼ユーザの地理的位置に基づき、そして多くの場合、一部は発呼ユーザと被呼ユーザにサービス提供するオペレータにも基づく。言い換えれば、オペレータ各社は、典型的には、着信側オペレータについての情報に基づいて課金の決定を行うことを望むのだが、それはｓｉｐ：ｊｏｈｎ@ｅｎｔｅｒｐｒｉｓｅ．ｃｏｍまたはｓｉｐ：ｊｏｈｎ@ｂａｌｄｗｉｎ．ｏｒｇのようなＳＩＰ ＵＲＩには示されない。従って、以下の例示的実施形態は、ＳＩＰ ＵＲＩにアドレス指定されたセッションが、複数のネットワークを通って正確な宛先までルーティングされることを可能にする、アドレス指定メカニズムとルーティングメカニズムとを提供する。

【００２３】

上記のように、これらの例示的実施形態についての一般的な文脈には、各種の通信ネットワークと在圏ネットワークとを含むオペレータネットワーク上の電話が含まれる。しかし、理解されるであろうが、本発明は、電話に限らず、いかなるタイプのメッセージをルーティングするのにも使用されうる。これらのネットワークは典型的には、多様な通信経

路と、各種のネットワークを分離するＩＢＣＦと、に関する可能性を有するであろう。加えて、メッセージトラヒックが所望のエンドポイントに到達することができるように、これらの各種のネットワーク間で通信を転送するための必要な詳細を詳述するＳＬＡ（サービス品質保証契約）が作成されるであろうと予想される。一部の詳細には、サービス品質要件やコストを含んでもよいし、さらに、例えばネットワークを識別するためにネットワークによって用いられることになる合意済み形式のようなアドレス指定の規則が含まれてもよい。

【００２４】

例示的実施形態によれば、要求またはメッセージの所望のルーティング経路を（例えば発信側ネットワークが）判定するための解決策には、発信側ネットワークがデータベースにクエリを行って、メッセージのルーティングを判定するのに用いられる応答を受信することが含まれる。例えば、発信側ネットワークが、宛先ユーザアドレス、例えばｓｉｐ：ｊｏｈｎ@ｂａｎｋ．ｃｏｍというＳＩＰ　ＵＲＩを含むＳＩＰメッセージをユーザから受信すると仮定しよう。この発信側ネットワークは発信側ネットワークとして動作しているため、どの在圏ネットワークがサービスをｂａｎｋ．ｃｏｍに提供するのか分からず、従って、どこにメッセージを送信するのか分からない。次いで、発信側ネットワークが、何らかのタイプの宛先識別情報、例えばｓｉｐ：ｊｏｈｎ@ｂａｎｋ．ｃｏｍ、またはｂａｎｋ．ｃｏｍ、または、宛先ユーザアドレスに関連するいずれかの他のタイプの宛先識別情報を使って、（マスタＤＮＳデータベースを含みうるであろう）在圏オペレータデータベースにクエリを行って、そして、在圏ネットワークを識別する情報、例えば在圏ネットワークのＦＱＤＮまたはその他の合意された識別情報を含む応答を受信する。

【００２５】

例示的実施形態によれば、この在圏オペレータデータベースは、典型的なネットワークレベルＤＮＳサーバより相当多くの情報を含むことが可能であり、例えば、在圏オペレータデータベースは、すべてのＦＱＤＮについての情報と、相互接続されている各種ネットワークについての情報とを含んでもよいだろう。それに比べて、ネットワークレベルＤＮＳは典型的には、共有の相互接続からのネットワークオペレータの入口ポイント(ingress points)についてのレコードを保持するだけであり、各種のオペレータまたはＩＰＸのようなグループによって運用される。従って、本書で議論されるネットワークレベルＤＮＳが、典型的にはネットワーク毎に用いられて、単一のオペレータネットワークについてドメイン名とＩＰアドレスとの間の翻訳を行うのに対し、本書で議論される在圏オペレータデータベースは、特に、特定のメッセージに関連する在圏ネットワークを識別するのに用いられる。その後、在圏オペレータデータベースからデータを受信した時点で、発信側ネットワークは、例えば、各種のネットワーク間の適切なＳＬＡと、コストと、トラヒック管理の検討材料とのうちのいずれか、または一部、または全部に基づいて、ルーティング経路を判定する。次いで、発信側ネットワークは、メッセージを在圏ネットワークに向けて送信し、そして、宛先ユーザアドレスと在圏オペレータを識別するための情報とを両方含める。このように宛先ユーザアドレスと在圏オペレータを識別するための情報とを両方共用いることは、２層のアドレス指定の一例である。

【００２６】

例示的実施形態によって、一企業（または複数の企業）および個人ユーザに通信をルーティングすることができる各種の相互接続ネットワークを図４に示す。この例示的通信の枠組みは、２つのオペレータネットワークであるＴｅｌｅ２　４０２およびＴｅｌｉａ４０４と、ＩＰＸ４０６と、企業ネットワークであるＢａｎｋ４０８とを含む。ＳＢＧ（セッション境界ゲートウェイ）は典型的にはアクセスポイントであるが、同時に、各種のオペレータネットワークおよびＩＰＸ４０６に出入りする通信のためのファイアウォールとしても動作することができる。加えて、オペレータネットワークであるＴｅｌｅ２　４０２およびＴｅｌｉａ４０４はそれぞれ、少なくともローカルに格納されたドメイン情報を有する、自分自身のネットワークレベルＤＮＳサーバ４２２および４２４（またはその同等物）を有する。在圏オペレータデータベース４１０は、ＩＰＸ４０６に関連するすべて

のネットワークについてのＤＮＳ情報を含む。この例ではＩＰＸ４０６の中に位置しているが、在圏オペレータデータベース４１０は、オペレータネットワークに接続されていてそれらにアクセス可能ならばどこに存在してもよく、例えば、第三者の所在地に存在してもよい。在圏オペレータデータベース４１０に記憶されたＤＮＳ情報は、例を挙げれば、例えばＴｅｌｅ２　４０２およびＴｅｌｉａ４０４のようなネットワークによって在圏オペレータデータベース４１０に報告された、各ネットワークによってサービス提供される住居や企業について記述する情報を含んでもよい。

【００２７】

企業ネットワークＢａｎｋ４０８は、各種のリソースおよび個人をアドレス可能な場所を表すＢａｎｋ　Ｃｅｎｔｒｅｘ４１２と2つのＢａｎｋ　ＰＢＸ４１４および４１６とを含む。ユーザ１　４１８は、Ｔｅｌｅ２によってサービスを提供されるユーザを表し、ユーザ２　４２０は、Ｂａｎｋ　ＰＢＸ４１４に関連することが知られているＢａｎｋ４０８のために働いているユーザを表す。本書ではＢａｎｋ　Ｃｅｎｔｒｅｘ４１２は、バーチャルＰＢＸであると考えられている。バーチャルＰＢＸは、典型的には小規模なリモートの企業拠点に関連付けられる。本書で記述する例示的実施形態において、在圏ネットワークは、通常のＰＢＸとバーチャルＰＢＸとをいずれも呼とメッセージとをエンドユーザに配信することについては同様に取り扱い、すなわち、本書で記述する例示的実施形態は、通常のＰＢＸとバーチャルなＰＢＸとのうちのいずれを利用するのかによって制約されない。

【００２８】

上記の例示的実施形態によれば、在圏オペレータデータベース４１０は、ユーザに関連する宛先識別情報と、それらの個別の在圏オペレータネットワークについての情報との両方に関連する情報を含む。在圏オペレータデータベース４１０は、この情報を用いてこれらの情報の集合間のマッピングを行うことができる。加えて、この情報は、さまざまなかたちで存在しうる。例えば、各種のネットワークおよびユーザを識別するのに、一般的なドメイン名、例えばｅｒｉｃｓｓｏｎ．ｃｏｍ、ｔｅｌｉａ．ｓｅ、ｂａｌｄｗｉｎ．ｏｒｇが用いられてもよいし、構造化された通信名、例えばｍｎｃ００１、ｍｃｃ２３４が用いられてもよい。また、在圏オペレータデータベース４１０は、一般的なドメイン名と、ｍｎｃやｍｃｃを用いる構造化された識別情報との間のマッピングを行ってもよい。

【００２９】

次に、図５に示すシグナリング図に関して、例示的実施形態によって、例えば図４に示す通信ネットワーク経由で呼をルーティングするメッセージについて記述しよう。最初に、ユーザ１　４１８が、メッセージＩＮＶＩＴＥ　ｓｉｐ：ｇｅｒｔ@ｂａｎｋ．ｃｏｍ　５０２を、発信側オペレータネットワークとして動作するＴｅｌｅ２　４０２に送信する。Ｔｅｌｅ２　４０２は、どのネットワークがサービスをｂａｎｋ．ｃｏｍに提供するのか分からず、従って、「ｂａｎｋ．ｃｏｍ」（またはその翻訳バージョン）を含むクエリメッセージ５０４を在圏オペレータデータベース４１０に送信する。在圏オペレータデータベース４１０は、ルックアップを行って、「ｂａｎｋ．ｃｏｍ」がＴｅｌｉａ４０４によってサービス提供されることを見つけ、応答メッセージ５０６の一部として「ｖｐｎｓｅｒｖｉｃｅ@ｔｅｌｉａ．ｓｅ」を送信する。Ｔｅｌｅ２　４０２は、この情報を用いて、Ｔｅｌｅ２　４０２とＴｅｌｉａ４０４との間の相互接続および契約、例えばＳＬＡに基づいてルーティング経路を判定する。

【００３０】

図４に示すように、Ｔｅｌｅ２　４０２は、直接接続とＩＰＸ４０６経由との両方を通してＴｅｌｉａ４０４に接続している。この事例では、Ｔｅｌｅ２　４０２は、「ＩＮＶＩＴＥ　ｖｐｎｓｅｒｖｉｃｅ@ｔｅｌｉａ．ｓｅ　Ｔａｒｇｅｔ　ｓｉｐ：ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」を含むメッセージ５０８で示すようにＩＰＸ４０６を通してトラヒックをルーティングすることを選ぶ。ＩＰＸ４０６は受信したメッセージ５０８の中の「ｔｅｌｉａ．ｓｅ」を見て、メッセージ５１０をＴｅｌｉａ４０４へルーティングする。次いでＴｅｌｉａ４０４は、「ＩＮＶＩＴＥ　ｓｉｐ：ｇｅｒｔ@ｂａｎｋ．ｃｏｍを含む

メッセージ５１２をユーザ２　４２０に送信する。

【００３１】

上記のように、上述したルーティング情報は、宛先アドレスと、例えばユーザまたは企業のような宛先にサービスを提供するネットワークについて記述する情報とを両方含む。後者の情報は、在圏オペレータデータベース４１０への発信側ネットワークのクエリへの応答を介して発信側ネットワークが利用できるようにされる。例示的実施形態によれば、ルーティング情報は、さまざまなやり方でＳＩＰメッセージに組み込むことができる。当業者であれば理解するであろうが、ＳＩＰメッセージは、Ｒｅｑｕｅｓｔ　ＵＲＩとＴａｒｇｅｔ　ＵＲＩヘッダとを両方含むことができる。例示的な一実施形態によれば、在圏オペレータＩＤ、例えばｔｅｌｉａ．ｓｅをＲｅｑｕｅｓｔ　ＵＲＩに入れることができ、そして、宛先の元のＳＩＰ　ＵＲＩ、例えばｇｅｒｔ@ｂａｎｋ．ｃｏｍを、ＳＩＰメッセージのＴａｒｇｅｔ　ＵＲＩヘッダに入れることができる。呼が在圏オペレータネットワークに到着すると、在圏オペレータは、Ｔａｒｇｅｔ　ＵＲＩをＲｅｑｕｅｓｔ　ＵＲＩに戻すように促し、呼をＮＧＣＮ３０４へとさらに配信させる。

【００３２】

別の例示的実施形態によれば、在圏オペレータＩＤを、Ｒｅｑｕｅｓｔ　ＵＲＩに添付することができる（例えば、ｓｉｐ：ｊｏｈｎ@ｅｎｔｅｒｐｒｉｓｅ．ｃｏｍ．ｍａｒｋｅｒ．ｍｎｃ１２３．ｍｃｃ２３４．３ｇｐｐｎｅｔｗｏｒｋｓ．ｏｒｇのように）。あるいは、新たなパラメータをＳＩＰ　Ｒｅｑｕｅｓｔ　ＵＲＩに入れることができる。例えば、在圏オペレータをパラメータとしてＳＩＰ　Ｒｅｑｕｅｓｔ　ＵＲＩに追加し、ｓｉｐ：ｊｏｈｎ@ｅｎｔｅｒｐｒｉｘｅ．ｃｏｍ；ｓｏ＝ｍｎｃ１２３．ｍｃｃ２３４．３ｇｐｐｎｅｔｏｗｏｒｋｓ．ｏｒｇのようにすることができる。別の例示的実施形態によれば、情報をＲｅｑｕｅｓｔ　ＵＲＩに添付するために上記で述べたのと同様のやり方でＲＮ（ルーティング番号）またはＴＲＧＰ（トランクグループパラメータ）のような他の既存のパラメータを拡張することによって、必要な在圏オペレータ情報を搬送することができる。

【００３３】

上記の例示的実施形態によれば、ＳＩＰメッセージの中で最初のＳＩＰ　ＵＲＩと在圏オペレータＩＤとを両方搬送することによって、発信側ネットワークと中継／相互接続ネットワークとが、中枢の在圏オペレータデータベース４１０によって取得された在圏オペレータ識別情報に基づいてメッセージをルーティングすることが可能になる。従って、在圏オペレータネットワークルーティング情報は、中継／相互接続ネットワークが知っていて読み取ることができるＳＩＰメッセージについての通常のルーティング情報の一部として提供されるのだから、中継／相互接続ネットワークは、典型的には、企業または住宅用ＦＱＤＮについての情報を知る必要はないし、在圏オペレータデータベース４１０にクエリを行う必要もない。

【００３４】

例示的な一実施形態によれば、メッセージがその中を移動できる各種のネットワークはそれぞれ、典型的には、内部では別個のローカルＩＰアドレスを用いる。従って、ＩＰアドレスとＩＰアドレスを用いたルーティングとを求める従来のＤＮＳクエリは、典型的には、発信側オペレータネットワークから在圏ネットワークおよび宛先までルーティングするためには用いられない。加えて、ＩＰアドレスによるルーティングは、発信側ネットワークによって制御されない状態で使用ルートの選択を行う自動ルーティングであると考え得ることから、典型的には望まれない。これでは、発信側オペレータネットワークが経路を制御することができず、ＳＬＡに関する問題や、収入が最適にならないことにつながりうるであろう。

【００３５】

一企業について複数の在圏オペレータの事例

上記の例示的実施形態は、企業が単一の在圏オペレータネットワークによってサービス提供される場合にメッセージトラヒックをルーティングするためのシステムおよび方法を

記述する。しかし、大企業については、ＮＧＣＮサイトと在圏オペレータネットワークとの間に複数の接続事例がありうる。例えば、大規模な企業ネットワークについては、企業は、企業の各部門が地理的に広域に位置していることや、ビジネス上の競合の理由等から、複数の在圏オペレータを望むことがある。例示的実施形態によって、企業が２つの異なる在圏オペレータネットワークを用いる通信の枠組みについて、図６に関して以下に述べる。

【００３６】

図６は、例示的な通信の枠組みを示すが、ここにはＩＰＸ４０６が含まれ、それが各種のオペレータネットワーク、例えばＴｅｌｉａ４０４、Ｔｅｌｅ２　４０２、Ｊｅｒｓｅｙ　Ｔｅｌ６０４、Ｇａｍｍａ　Ｔｅｌ６０８に接続する。また、この例では、ＩＰＸ４０６は、一次ＤＮＳデータベース４１０を含むが、これは宛先のＦＱＤＮを、その宛先にサービスを提供する在圏ネットワークにマッピングするための情報を含む。企業Ｂａｎｋが、Ｔｅｌｉａ４０４によってサービス提供されるＢａｎｋ　ＰＢＸ４１４と、Ｊｅｒｓｅｙ　Ｔｅｌ６０４によってサービス提供されるＢａｎｋ　ＰＢＸ６０２とで示すように、２つの異なる在圏オペレータネットワークによってサービス提供され、Ｂａｎｋ　ＰＢＸ４１４とＢａｎｋ　ＰＢＸ６０２とはＶＰＮ６０６によって接続される。さらに、ユーザ１　４１８とユーザ２　４２０とを示す。

【００３７】

次に、例示的実施形態によって、一企業について複数の在圏オペレータネットワークを有するケースについて図６に示すアーキテクチャを用いる、図７に示すようなシグナリングフローについて記述しよう。最初に、ユーザ１　４１８が、「ＩＮＶＩＴＥ　ｓｉｐ：ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」を含むメッセージ７０２を、発信側ネットワークとして動作するＴｅｌｅ２　４０２に送信する。次いでＴｅｌｅ２　４０２は、例えば「ｂａｎｋ．ｃｏｍ」や「ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」のような宛先ユーザアドレスに関連する宛先識別情報を含むクエリメッセージ７０４を在圏オペレータデータベース４１０に送信する。在圏オペレータデータベース４１０は、ルックアップを行って、２つの在圏オペレータネットワーク、例えばｖｐｎｓｅｒｖｉｃｅ@ｔｅｌｉａ．ｓｅやｖｐｎｓｅｒｖｉｃｅ@ｊｅｒｓｅｙ．ｕｋについての識別情報を含む応答メッセージ７０６を送信する。次いでＴｅｌｅ２　４０２は、どの在圏オペレータネットワークに要求を送信し、要求をどのようにルーティングするかを決定する。これらの決定は、既知の相互接続、ＳＬＡ、地理的位置、コスト、その他の関連情報に基づいて行われてもよい。これらの決定に基づいて、Ｔｅｌｅ２　４０２は、「ＩＮＶＩＴＥ　ｖｐｎｓｅｒｖｉｃｅ@ｔｅｌｉａ．ｓｅおよびＴａｒｇｅｔ　ｓｉｐ：ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」を含むメッセージ７０８をＩＰＸ４０６に送信する。ＩＰＸ４０６は、自分が必要とするルーティング情報、例えばｔｅｌｉａ．ｓｅが分かり、そして、メッセージ７１０に示すように、メッセージをＴｅｌｉａ４０４に転送する。ついでＴｅｌｉａ４０４は、メッセージの内容をよく調査して、それらを、ｇｅｒｔ@ｂａｎｋ．ｃｏｍであることが分かっているユーザ２　４２０に転送する。

【００３８】

上記のように、企業は、その企業の異なる部門について各種の在圏オペレータネットワークを有することがある。例示的実施形態によれば、すべての在圏オペレータネットワークが、対応する識別情報またはルーティング情報を在圏オペレータデータベース４１０の中に記憶しておく必要はない。加えて、クエリメッセージ７０４に応じて、在圏オペレータデータベース４１０の中に記憶された１つの、または少数の、またはすべての在圏オペレータネットワークが、応答メッセージ７０６の中で返信されてもよい。応答メッセージ７０６の中で用いられる在圏オペレータネットワークは、在圏オペレータネットワークと企業との間で事前に定められ、それに従って一次ＤＮＳデータベース４１０に記憶されてもよい。

【００３９】

例示的実施形態によれば、不適切な在圏オペレータネットワークがメッセージを受信し

た場合、すなわち、在圏オペレータネットワークがそのメッセージについてはその宛先にサービス提供しないと判定する場合、システムと方法とを用いてメッセージを別の在圏オペレータネットワークにさらにルーティングすることができる。ある場合には、例えば、宅内ユーザが企業に電話をかけることによって、呼がパブリックネットワークにおいて開始される。発信側オペレータネットワークが、（そのクエリによって受信された）複数の在圏オペレータのうちの１つを選択し、呼をその在圏オペレータに配信した。しかし、これは実際には、当該ユーザにとっては不適切な在圏オペレータであった。在圏オペレータネットワークは、企業にクエリを行うことができ、例えば企業内のデータベースにルーティングについての指示を求めるクエリを行って、次いで、上記の２層のアドレス指定スキームを用いて呼を正しい在圏オペレータネットワークにルーティングすることができる。

【００４０】

別の例示的実施形態によれば、呼は、企業内で、例えば企業ユーザが別の企業ユーザに対して開始することができる。宛先企業ユーザは、発信企業ユーザとは別の在圏ネットワークオペレータによってサービス提供される企業ネットワークの一部である。この場合、これはオンネット・コールとして知られるものだが、呼は、各種の相互接続ネットワークを経て正しい在圏オペレータネットワークにルーティングされる必要がある。また、上記の２層のアドレス指定スキームを用いてこの呼を正しい在圏オペレータに転送することもできる。

【００４１】

ドメイン名ポータビリティ

例示的実施形態によれば、上記のシステムおよび方法の実装によって、ドメイン名ポータビリティが可能になる。本書ではドメイン名ポータビリティとは、ユーザまたは企業のドメインを、１つの在圏オペレータから別の在圏オペレータに最小限のオーバーヘッドまたは作業で移動させることを言う。例えば、上記のように、これらの例示的実施形態で用いられる在圏オペレータデータベース４１０は、各ネットワークで用いられる典型的なネットワークレベルのＤＮＳデータベース４２２、４２４とは別である。この在圏オペレータデータベース４１０は、在圏オペレータデータベース４１０のプロバイダと各ネットワークオペレータとによって定められたように各ネットワークによって更新されるが、更新は変更が行われる時にタイムリーに行われることが望ましく、それによってドメイン名ポータビリティが円滑化される。

【００４２】

例えば、企業Ｂａｎｋ４０８が、Ｔｅｌｉａ４０４を自社のサービスプロバイダとして用いていると仮定する。次いで、企業Ｂａｎｋ４０８は、自社のサービスプロバイダとしてＴｅｌｅ２　４０２に変更することを決め、すなわち、Ｂａｎｋ４０８から在圏ネットワークへの接続ポイントが、新たな在圏ネットワークに変更されるが、Ｂａｎｋ４０８の中の内部アドレス指定は典型的には変更されず、例えば個別のＳＩＰ　ＵＲＩ、内線番号、直通電話番号（ｄｉｒｅｃｔ　ｄｉａｌｉｎｇ　ｉｎｗａｒｄｓ：ＤＤＩ）は以前と同じであろう。次いで、この変更が行われた後、Ｔｅｌｅ２　４０２は、その変更について、在圏オペレータデータベース４１０を更新する。典型的には、２つのネットワークがこの変更によって直接影響を受ける場合を除き、ＤＮＳインフラストラクチャの低い方のレベルでは変更が行われる必要はない。また、Ｂａｎｋ４０８のネットワーク構造の範囲内での内部変更は、大部分は、修正される必要はないだろう。また、このプロセスは、住宅用についても当てはまるであろう。例えば、ユーザがｇｅｒｔ@ｂａｌｄｗｉｎ．ｏｒｇというドメイン名を有していて、在圏オペレータネットワークを変更した場合、ドメイン名は、新たな在圏オペレータネットワークへ持ち運ぶことができるであろうし、依然としてｇｅｒｔ@ｂａｌｄｗｉｎ．ｃｏｍへのシームレスな移行により使用することができるであろう。

【００４３】

企業ネットワークアクセスポイントの判定

上記の一部の例示的実施形態は、メッセージトラヒックを発信側ネットワークから相互

接続ネットワークを経由して在圏ネットワークへとルーティングするためのシステムと方法とを含む。以下の例示的実施形態は、在圏オペレータネットワークから企業内のエンティティへとメッセージを配信するための各種のシステムと方法とを含む。しかし、これらの例示的実施形態について論じる前に、まず、在圏ネットワークから企業へのセッションのルーティングに関する文脈についてさらに論じよう。

【００４４】

ＥＴＳＩ　ＴＳ　１８２　０２５によって定義された、提案するネットワークアーキテクチャの文脈では、既存の標準および解決策は、例えば企業ネットワークにサービス提供する在圏ネットワークが、どうすればセッションを企業ネットワーク内のエンドユーザへの正しい場所へとルーティングすることができるかについて記述していない。例えば、ｊｏｈｎ@ｂａｎｋ．ｃｏｍやｓｉｐ：８５０１２３４@ｂａｎｋ．ｃｏｍ；ｕｓｅｒ＝ｐｈｏｎｅのようなＳＩＰ　ＵＲＩは、在圏ネットワークがそのエンティティ、例えば銀行という企業内の例えばＪｏｈｎに配信するためのアドレス指定されたユーザの地理的位置に関する十分な情報を提供しない。加えて、そのようなＳＩＰ　ＵＲＩは、企業は呼が企業のネットワークにどのように到達してほしいかについて記述しない。例えば、企業は、すべての外部呼（またはメッセージ）が１つのロケーションに到達するかまたは、外部呼が、アドレス指定されたユーザが通常存在するロケーションに配信されることを必要とすることを望むことがある。加えて、一旦在圏ネットワークが適切な企業ネットワークアクセスポイントを決めると、在圏ネットワークは典型的には、自分のＩＭＳネットワークを経て呼をルーティングする必要がある。呼は、加入に基づく相互接続を用いるＨｏｓｔｅｄ　Ｅｎｔｅｒｐｒｉｓｅユーザおよびビジネス・トランキングＰＢＸの場合は正しいＳ－ＣＳＣＦ３１０とＡＳ３１２とを通過し、または、ピアリングに基づく相互接続については正しいＩＢＣＦを通過する必要がある。下記の例示的実施形態は、ピアリング相互接続と加入相互接続との両方について、在圏オペレータネットワークから企業ネットワークへのこれらのルーティング問題の解決策を提供する。

【００４５】

例示的実施形態によれば、システムと方法とが、アドレス指定メカニズムおよびルーティングメカニズムを提供し、それらによって、セッション、例えばＳＩＰセッションが在圏ＮＧＮと企業ネットワークとの間の正しい相互接続ポイントへ、さらに正しい宛先ユーザアドレスへとルーティングされることが可能になる。加えて、これらの例示的実施形態を用いて、多様な相互接続ポイントの後方に位置する企業ユーザ間で呼を配信することができる。在圏ＮＧＮと企業ネットワークとの間のこれらの相互接続ポイントを、本書では企業ネットワークアクセスポイントと呼ぶ。下記のこれらの例示的実施形態は、典型的には、加入に基づく相互接続およびピアリングに基づく相互接続の両方について、ビジネス・トランキングＮＧＣＮの一部である企業内ユーザに適用される。

【００４６】

例示的実施形態によれば、これらの方法およびシステムによって、あるユーザについてそのユーザについての関連の企業ネットワークアクセスポイントと必要に応じてルーティングを円滑化する追加の関連情報とを（上述したように、例えばＳＩＰ　ＵＲＩのユーザパートによって）定義する情報へのアクセスを、企業が在圏ネットワークに提供することが可能になる。これをサポートするため、例示する方法およびシステムは、企業がこの情報を更新し、ポリシーを記憶し、ポリシーを通信することを可能にし、そして加入者（ユーザ）は在圏ＮＧＮに移動／変更する。加えて、これらの方法およびシステムによって、在圏ネットワークは呼をこの情報に基づいて所望のやり方で、または企業と在圏ネットワークによって合意されたやり方で、ルーティングすることができる。

【００４７】

前述したように、在圏ネットワークは典型的にはＩＭＳネットワークであるが、これは必要というわけではない。図３（ａ）および３（ｂ）は、ピアリング相互接続および加入相互接続の両方について、ＮＧＣＮ３０４およびＡＳ３１２と通信するＩＭＳネットワーク３０２の各部を示す図である。例示的実施形態によって、ＩＭＳネットワーク３０２を

経てサービスを企業ネットワークにルーティングする際に用いられうるＩＭＳネットワーク３０２のさらなる構成要素を図８に示す。ＩＭＳネットワーク３０２のこれらのノードには、Ｐ－ＣＳＣＦ３０８とＳ－ＣＳＣＦ３１０とＩ－ＣＳＣＦ（インテロゲーティングＣＳＣＦ）８０４とが含まれる。Ｐ－ＣＳＣＦ３０８は、典型的には、ＩＭＳネットワーク３０２のコア部分におけるユーザの最初のコンタクトポイントであり、メッセージや要求を所望のＳ－ＣＳＣＦ３１０に転送する。Ｓ－ＣＳＣＦ３１０は、セッション制御サービスを行い、セッション状態情報を必要に応じて維持する。Ｉ－ＣＳＣＦ８０４は、中継ルーティング機能を行ってもよく、ユーザ宛ての接続についての在圏オペレータネットワークの範囲内でコンタクトポイントとして動作することができる。

【００４８】

ＨＳＳ（ホーム加入者サーバ）８０２は、典型的には、ＩＭＳネットワークへの登録のような動作のために他のネットワークエンティティが用いる、ユーザ（および必要に応じて企業）についての加入に関連する情報を含む。加えて、ＨＳＳ８０２は、Ｓ－ＣＳＣＦ３１０およびＩ－ＣＳＣＦ８０４と通信する。図８に示す３つのＣＳＣＦはすべて、境界制御機能を提供するＩＢＣＦ３１４と通信することができる。ＶＰＮ－ＲＦ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ　Ｒｏｕｔｉｎｇ　Ｆｕｎｃｔｉｏｎ：仮想プライベートネットワーク・ルーティング機能）８０６は、在圏オペレータネットワークの一部であって、例えばＩＭＳアプリケーションサーバであってもよく、企業ネットワークアクセスポイントレポジトリ（以下に記す）にアクセスし、かつ、本書に記述する各種の例示的実施形態を実装することができる。加えて、ＶＰＮ－ＲＦ８０６は、着信セッションを受信し、セッションを在圏オペレータネットワークを経て在圏オペレータネットワークの正しい出口ポイント(egress point)、例えばＩＢＣＦ３１４にルーティングすることができる。図８に示すもの以外のノードがＩＭＳネットワーク３０２の範囲内で用いられてもよく、ＩＭＳネットワークに関するさらなる情報は、一般に３ＧＰＰ　ＴＳ　２３．００２　バージョン８．３．０リリース８および３ＧＰＰ　ＴＳ　２３．２２８バージョン８．６．０リリース８のいずれにも記載されている。また、本書で記述する例示的実施形態において、以下の例えば、ピアリング相互接続および加入相互接続の実施形態の場合のように、図８に示すノードが、もっと重い度合いでまたはもっと軽い度合いで用いられてもよい。

【００４９】

例示的実施形態によれば、企業ネットワークは複数の企業ネットワークアクセスポイントを有することができる。企業内の多様なユーザを、企業の希望に従って多様な企業ネットワークアクセスポイントに関連付けることができる。企業内の多様なユーザと彼らの企業ネットワークアクセスポイントへの関連とについての情報が、データベースにかまたは他の所望の記憶位置に記憶されることにより、情報が企業と在圏ネットワークとの両方から検索でき、アクセスされうる。どのようにして企業とそのユーザとが在圏オペレータネットワークに接続するかに関する多様なシナリオについては、多様な方法を用いてこの情報を利用できるようにすることができる。例えば、このユーザコンタクト情報を記憶しているそれらの各々のセキュアな記憶位置の間で特定のレベルのアクセスを許可することによって、在圏ネットワークと企業との両方がこの情報にアクセスすることができる。

【００５０】

例示的実施形態によれば、ビジネス・トランキングＮＧＣＮの場合、企業はデータベース、例えば企業ネットワークアクセスポイントレポジトリに、各ユーザについての企業ネットワークアクセスポイント情報を使ってデータ投入することができる。この企業ネットワークアクセスポイントレポジトリは、在圏ネットワークがアクセスする企業ネットワークの一部かまたは企業がアクセスする在圏ネットワークの一部かのいずれか一方であってもよいだろう。しかし、例えばｃｅｎｔｒｅｘのようなホストされた企業ＮＧＣＮを用いるユーザの場合、情報は典型的には在圏ネットワークのＨＳＳ８０２の中の各ユーザのエントリの中に提供されるであろうから、すなわち、各企業ユーザについてＩＭＳユーザが存在するであろうから、企業は、典型的には、そのような情報を使って追加のデータベー

スにデータ投入する必要はないであろう。いずれにしても、図９に関して以下に詳述するであろうが、企業はどの企業ネットワークアクセスポイントに自分が自分のユーザを関連させているかを知っているため、必要に応じてデータベースにデータ投入することができる。

【００５１】

例示的実施形態によれば、図９は、企業Ｂａｎｋのネットワーク４０８と通信する在圏オペレータネットワーク、例えばＴｅｌｉａ４０４と、複数の企業ネットワークアクセスポイント９０８、９１０、および９１２と、どの企業ネットワークアクセスポイントを用いて通信をＢａｎｋ４０８の範囲内の各種のユーザに転送すべきかを判定するための企業ネットワークアクセスポイントレポジトリ９０４とを示す図である。図９で分かるように、Ｔｅｌｉａ４０４は、Ｂａｎｋ４０８との３つの企業ネットワークアクセスポイント９０８、９１０および９１２を有する。企業ネットワークアクセスポイント９０８は、Ｂａｎｋ　ＰＢＸ４１４とＢａｎｋ　ＰＢＸ４１６とにいるユーザ、例えば、それぞれ、ｇｅｒｔ@ｂａｎｋ．ｃｏｍとｐｅｒ@ｂａｎｋ．ｃｏｍとに向かうトラヒックに利用される。企業ネットワークアクセスポイント９１０は、Ｂａｎｋ　ＰＢＸ９０２にいるユーザ、例えばｊｏｈｎ@ｂａｎｋ．ｃｏｍに向かうトラヒックに利用され、そして、企業ネットワークアクセスポイント９１２は、Ｂａｎｋ　Ｃｅｎｔｒｅｘ４１２に向かうトラヒックに利用される。

【００５２】

この例示的通信アーキテクチャを用いて、所望の企業ネットワークアクセスポイントを識別するためのプロセスを、下記のステップを通じて行うことができる。最初に、企業の管理者がポリシーとユーザ位置とを設定する。次いで、企業の管理者は、企業ネットワークアクセスポイントレポジトリ９０４を更新して、この情報に在圏ネットワークがアクセスできるようにする。着信呼が在圏オペレータネットワークに到着し、例えば、図８のＶＰＮ　ＲＦ８０６で示すように、ＩＭＳのＰＳＩ（ｐｕｂｌｉｃ　ｓｅｒｖｉｃｅ　ｉｄｅｎｔｉｔｙ：パブリックサービスＩＤ）を利用したＶＰＮサービスであると識別される。在圏オペレータネットワークは、受信した呼から元のＳＩＰ　ＵＲＩを取得し、それを使って企業ネットワークアクセスポイントレポジトリにクエリを行う。企業ネットワークアクセスポイントレポジトリ９０４からの応答には、使用されることになる企業ネットワークアクセスポイントのＩＤが含まれる。

【００５３】

次に、この例示的アーキテクチャと企業ネットワークアクセスポイントを識別するプロセスとを用いて、図９に基づく例示的実施形態による例示的な利用のケースについて記述しよう。最初に、ＳＩＰメッセージが、ＩＰＸ４０６を通過し、次いでＳＢＧ９０６を通過してＴｅｌｉａ４０４に達する。Ｔｅｌｉａ４０４は、（上記の例示的実施形態によるＳＩＰメッセージに組み込まれているように）「ＩＮＶＩＴＥ　ｓｉｐ：ｂａｎｋｖｐｎ@ｔｅｌｉａ．ｓｅ」と「Ｔａｒｇｅｔ　ｓｉｐ：ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」とが含まれるメッセージを読み取り、「ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」を用いて企業ネットワークアクセスポイントレポジトリ９０４にクエリを行う。企業ネットワークアクセスポイントレポジトリ９０４は、図９の企業ネットワークアクセスポイント９０８であるアクセスポイント１とｇｅｒｔとの関連を含む応答を使って返信する。次いで、ＳＩＰメッセージが、企業ネットワークアクセスポイント９１０を介してｇｅｒｔ@ｂａｎｋ．ｃｏｍへ転送される。

【００５４】

例示的実施形態によれば、一旦企業ネットワークアクセスポイントが識別されると、呼は在圏ＩＭＳネットワーク３０２を横切って、企業ネットワークとの識別された相互接続ポイントにルーティングされる。また、在圏オペレータネットワークは典型的には、各企業ネットワークアクセスポイントについて、そのアクセスポイントが加入相互接続かピアリング相互接続かを識別する設定データを有する。ＩＭＳネットワーク３０２の範囲内の多様なノードは、典型的には相互接続タイプに依存して配信プロセスにおいて利用される

ため、この情報は有益である。

【００５５】

例示的実施形態によれば、企業ネットワークがピアリング相互接続を用いる場合には、企業ネットワークアクセスポイントレポジトリ９０４の中の関連情報は、用いられることになるＩＢＣＦ３１４を識別するであろう。次に、図１０に示す例示的ネットワークノードを用いて、ピアリング相互接続に関するルーティングの一例について記述しよう。最初に、ＶＰＮ－ＲＦ８０６が、ＳＩＰメッセージの中に「ＶＰＮｓｅｒｖｉｃｅ@ｔｅｌｉａ．ｃｏｍ」と「Ｔａｒｇｅｔ＝ｊｏｈｎ@ｂａｎｋ．ｃｏｍ」とを含むメッセージ１０１２を受信する。次いでＶＰＮ－ＲＦ８０６は、「ｊｏｈｎ@ｂａｎｋ．ｃｏｍ」を使って企業ネットワークアクセスポイントレポジトリ９０４にクエリを行い、ｊｏｈｎに関連する企業ネットワークアクセスポイント、例えば、「ａｃｃｅｓｓｐｏｉｎｔＸ@ｂａｎｋ．ｃｏｍ」と、このピアリング相互接続を扱う在圏ネットワークの端点のＩＢＣＦ３１４のＩＤとを含む応答を受信する。次いで、ＶＰＮ－ＲＦ８０６は、企業ネットワークアクセスポイント情報をＰ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダに挿入し、ＩＢＣＦ３１４のＩＤを、ルーティングされることになるメッセージのＳＩＰルートヘッダに挿入する。当業者には理解されるであろうが、Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダは、Ｓ－ＣＳＣＦ３１０からＡＳ３１２へ、またはＡＳ３１２からＳ－ＣＳＣＦ３１０へとルーティングされる最初の要求に追加することができるヘッダフィールドであって、典型的には、Ｓ－ＣＳＣＦ３１０によってサービス提供されるユーザのＩＭＳパブリック・ユーザ・アイデンティティを含み、そして、そのユーザに代わってアプリケーションが呼び出されるようなヘッダフィールドである。Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダは、セッションケースパラメータを含むことができ、それを用いて、最初の要求が在圏ユーザによって発信されたかまたは在圏ユーザに宛てられたかが伝達されてもよい。また、Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダは、最初の要求が登録済ユーザについてかまたは未登録ユーザについてかをＡＳ３１２に示すためにＳ－ＣＳＣＦ３１０が用いうる登録状態パラメータを含むこともできる。ＤＮＳおよびＳＩＰルートヘッダに基づく通常のＩＭＳルーティング手順を用いて、呼を正しいＩＢＣＦ３１４に配信することができる。

【００５６】

例えば、メッセージがＩＭＳネットワーク３０２を通してＩＢＣＦ３１４まで転送され、メッセージには「ｊｏｈｎ@ｂａｎｋ．ｃｏｍ」と、ＳＩＰルートヘッダの中にＩＢＣＦ３１４を識別する情報と、Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダの中に「ｒｏｕｔｅ＝ａｃｃｅｓｓｐｏｉｎｔＸ@ｂａｎｋ．ｃｏｍ」とが含まれる。次いで、ＩＢＣＦ３１４は、このメッセージがどの企業ネットワークアクセスポイントに配信されることになるのかを判定するために、Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダ情報を分析するであろう。メッセージを転送する前に、ＩＢＣＦ３１４は、Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダを削除するであろう。加えて、ＩＢＣＦ３１４は、いずれかの所定のポリシー決定を要望どおり適用することができる。この例では、メッセージは、識別された企業ネットワークアクセスポイントを通してＢａｎｋ　ＰＢＸ９０２に転送される。

【００５７】

例示的実施形態によれば、企業ネットワークが加入相互接続を用いる場合には、データベース内の企業ネットワークアクセスポイントデータは、ＮＧＣＮの企業ネットワークアクセスポイントを表すＩＭＳユーザを識別するであろう。次に、図１０の例示的ネットワークノードを用いて、加入相互接続を用いた呼のルーティングの一例について記述しよう。最初に、ＶＰＮ－ＲＦ８０６が、ＳＩＰメッセージの中に「ＶＰＮｓｅｒｖｉｃｅ@ｔｅｌｉａ．ｃｏｍ」と「Ｔａｒｇｅｔ＝ｊｏｈｎ@ｂａｎｋ．ｃｏｍ」とを含むメッセージ１０１２を受信する。次いでＶＰＮ－ＲＦ８０６は、「ｊｏｈｎ@ｂａｎｋ．ｃｏｍ」を使って企業ネットワークアクセスポイントレポジトリ９０４にクエリを行い、企業ネットワークアクセスポイント、例えば、ａｃｃｅｓｓｐｏｉｎｔＸ@ｂａｎｋ．ｃｏｍと、用いられることになるＩ－ＣＳＣＦ８０４のＩＤとを含む応答を受信する。次いで、ＶＰＮ－ＲＦ８０６は、企業ネットワークアクセスポイント情報をＰ－Ｓｅｒｖｅｄ－Ｕｓｅ

ｒヘッダに挿入することができる。次いでＶＰＮ－ＲＦ８０６は、呼をＩ－ＣＳＣＦ８０４に配信し、Ｉ－ＣＳＣＦ８０４がＰ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダをクエリキーとして用いてＨＳＳ８０２にクエリを行い、ＨＳＳ８０２は登録済ユーザに関連するＳ－ＣＳＣＦ３１０を使って応答する。この例では、「ａｃｃｅｓｓｐｏｉｎｔＸ@ｂａｎｋ．ｃｏｍ」は、ＨＳＳ８０２の中で提供されるＩＭＳユーザであり、他方、「ｊｏｈｎ@ｂａｎｋ．ｃｏｍ」は、企業ユーザである。企業ネットワークアクセスポイントレポジトリ９０４に記憶されたＩＭＳユーザと企業ユーザ（およびそれらの関係）との両方の知識があれば、複数の企業ユーザが「ａｃｃｅｓｓｐｏｉｎｔＸ@ｂａｎｋ．ｃｏｍ」の後方に位置してもよい。

【００５８】

例えば、「ａｃｃｅｓｓｐｏｉｎｔＸ@ｂａｎｋ．ｃｏｍ」がＰ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダの中にあって、Ｉ－ＣＳＣＦ８０４によってＨＳＳ８０２にクエリを行うために用いられ、ＨＳＳ８０２が、「ａｃｃｅｓｓｐｏｉｎｔＸ@ｂａｎｋ．ｃｏｍ」と関連しているとしてＳ－ＣＳＣＦ３１０を識別する情報を送信すると仮定しよう。次いで、Ｉ－ＣＳＣＦ８０４は、呼を適切なＳ－ＣＳＣＦ３１０に転送することができる。その後、Ｓ－ＣＳＣＦ３１０は、それ以降Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダを要望どおりに用いることができる。また、その後の呼については、通常の着信ＩＭＳ手順を用いて、呼をＡＳ３１２およびＰ－ＣＳＣＦ３０８に配信することができる。次いで、この例を完了させるには、Ｓ－ＣＳＣＦ３１０は呼をＰ－ＣＳＣＦ３０８に転送し、Ｐ－ＣＳＣＦ３０８は、Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダ情報を分析し、Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダ情報を削除し、その後、呼をアクセスポイントＸに送信して企業内で配信し、例えば、Ｂａｎｋ　ＰＢＸ９０２に関連するユーザｊｏｈｎがメッセージを受信する。

【００５９】

また、図１０には、Ｓ－ＣＳＣＦ１００４と、Ｐ－ＳＣＳＦ１００８と、ＡＳ１００６と、Ｂａｎｋ　Ｃｅｎｔｒｅｘ４１２とを示す。これらのノードは、バーチャルＰＢＸ、例えばＢａｎｋ　Ｃｅｎｔｒｅｘ４１２に終端する加入相互接続を表す。本書で記述する例示的実施形態において、在圏ネットワークは正しく呼とメッセージとを配信するのに必要な情報を有するのだから、典型的なＰＢＸとバーチャルＰＢＸとのいずれについてのこれらの例示的実施形態の実装も、当業者にとって認識できる違いはない。

【００６０】

次に、図１０に示す例示的アーキテクチャを用いて、例示的実施形態による加入相互接続のシグナリング図について、図１１（ａ）に関して記述しよう。最初に、ＶＰＮ－ＲＦ８０６が、「ｖｐｎｓｅｒｖｉｃｅ@ｔｅｌｉａ．ｓｅ」と「Ｔａｒｇｅｔ　ｓｉｐ：ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」とを含むＳＩＰ　ＩＮＶＩＴＥメッセージ１１０２を受信する。次いで、ＶＰＮ－ＲＦ８０６が、宛先情報ｇｅｒｔ@ｂａｎｋ．ｃｏｍを含むクエリメッセージ１１０４を企業ネットワークアクセスポイントレポジトリ９０４に送信する。企業ネットワークアクセスポイントレポジトリ９０４は、ルックアップを行って、クエリメッセージ１１０４の中の宛先ユーザアドレスに関連する企業ネットワークアクセスポイントと、Ｉ－ＣＳＣＦ８０４とを判定する。この企業ネットワークアクセスポイント情報は、応答メッセージ１１０６の中でＶＰＮ－ＲＦ８０６に返信される。次いでＶＰＮ－ＲＦ８０６は、企業ネットワークアクセスポイント情報を、受信したＳＩＰ　ＩＮＶＩＴＥメッセージのＰ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダの中に組み込んで、メッセージ１１０８をＩ－ＣＳＣＦ８０４に転送する。

【００６１】

Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダ情報を用いて、Ｉ－ＣＳＣＦ８０４は、ボックス１１１０で示すように、その企業ネットワークアクセスポイントに関連するＳ－ＣＳＣＦ３１０についてＨＳＳ８０２にクエリを行う。次いで、Ｉ－ＣＳＣＦ８０４は、ＳＩＰ　ＩＮＶＩＴＥメッセージ１１１２を適切なＳ－ＣＳＣＦ３１０およびＰ－ＣＳＣＦ３０８に転送する。Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダの中の情報を用いて、Ｐ－ＣＳＣＦは、ＳＩＰメッセージからＰ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダを削除した後、指定の企業ネット

ワークアクセスポイントを通ってＢａｎｋ　ＰＢＸ９０２によって表される正しいユーザにメッセージ１１１６を転送する。

【００６２】

次に、図１０に示す例示的アーキテクチャを用いて、例示的実施形態によるピアリング相互接続のシグナリング図について、図１１（ｂ）に関して記述しよう。最初に、ＶＰＮ－ＲＦ８０６が、「ｖｐｎｓｅｒｖｉｃｅ@ｔｅｌｉａ．ｓｅ」と「Ｔａｒｇｅｔ　ｓｉｐ：ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」とを含むＳＩＰ　ＩＮＶＩＴＥメッセージ１１１８を受信する。次いで、ＶＰＮ－ＲＦ８０６は、宛先ユーザアドレス「ｇｅｒｔ@ｂａｎｋ．ｃｏｍ」を含むクエリメッセージ１１２０を企業ネットワークアクセスポイントレポジトリ９０４に送信する。企業ネットワークアクセスポイントレポジトリは、ルックアップを行って、クエリメッセージ１１２０の中のユーザ（または宛先）に関連する企業ネットワークアクセスポイントと、ＩＢＣＦ３１４とを判定する。この企業ネットワークアクセスポイント情報は、応答メッセージ１１２２の中でＶＰＮ－ＲＦ８０６に返信される。次いでＶＰＮ－ＲＦ８０６は、企業ネットワークアクセスポイント情報を、受信したＳＩＰ　ＩＮＶＩＴＥメッセージのＰ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダの中に組み込んで、メッセージ１１２４をＩＢＣＦ３１４に転送する。ＩＢＣＦ３１４は、メッセージ１１２４を読み取って、指定のユーザについて用いる企業ネットワークアクセスポイントを判定する。次いでＩＢＣＦ３１４は、Ｐ－Ｓｅｒｖｅｄ－Ｕｓｅｒヘッダ１１２６を削除して、ＳＩＰ　ＩＮＶＩＴＥをメッセージ１１２８として、Ｂａｎｋ　ＰＢＸ９０２を介してｇｅｒｔ@ｂａｎｋ．ｃｏｍへ転送する。

【００６３】

上記の例示的実施形態は、企業ネットワークアクセスポイントレポジトリ９０４を用いてエンドユーザに適合する企業ネットワークアクセスポイント情報を記憶するための方法およびシステムについて記述する。次に、企業ネットワークアクセスポイントレポジトリ９０４として動作しうる例示的通信ノード１２００について、図１２に関して記述しよう。通信ノード１２００は、プロセッサ１２０２（または複数のプロセッサコア）と、メモリ１２０４と、１つ以上の二次ストレージデバイス１２０６と、通信を円滑化する通信インタフェース１２０８とを含んでもよい。メモリ１２０４（または二次ストレージデバイス１２０６）は、アクセスポイントテーブル９０４で用いられる情報のストレージ用として用いてもよい。従って、例示的実施形態による通信ノード１２００は、クエリを受信して、宛先ユーザアドレスに関連する企業ネットワークアクセスポイントを返信することができる。加えて、通信ノード１２００は、上記の各種の通信ネットワークにおけるその他のノード、例えばＶＰＮ－ＲＦ８０６およびＨＳＳ８０２の機能を実行することができる。

【００６４】

例示的実施形態によって上記の例示的システムを利用して、メッセージトラヒックをルーティングするための方法を、図１３のフローチャートに示す。最初に、在圏ネットワークから企業ネットワークへメッセージトラヒックをルーティングするための方法は、ステップ１３０２で宛先ユーザアドレスを含むクエリメッセージを在圏ネットワークから送信することと、ステップ１３０４で宛先ユーザアドレスに関連する内部メッセージルーティング情報とアクセスポイント識別情報とを含む応答メッセージを在圏ネットワークで受信することと、ステップ１３０６で在圏ネットワークにおいてアクセスポイント情報をメッセージに組み込むことと、ステップ１３０８で在圏ネットワークが内部メッセージルーティング情報に基づいてメッセージをアクセスポイント識別情報に関連するアクセスポイントに向けて送信することとを含む。

【００６５】

例示的実施形態によって上記の例示的システムを利用して、メッセージトラヒックをルーティングするための別法を、図１４のフローチャートに示す。最初に、通信ノードにおいてメッセージトラヒックをルーティングするための方法は、ステップ１４０２で複数の宛先ユーザアドレスを記憶し、ここでは各宛先ユーザアドレスがアクセスポイントおよび

内部ルーティング情報に関連付けられることと、ステップ１４０４で宛先ユーザアドレスを含むクエリメッセージを受信することと、ステップ１４０６で宛先ユーザアドレスを使ってルックアップを行って、対応するアクセスポイントと内部メッセージルーティング情報とを判定することと、ステップ１４０８でルックアップで識別された対応するアクセスポイントと内部メッセージルーティング情報とに基づく情報を含む応答メッセージを送信することとを含む。

【００６６】

上記で開示した例示的実施形態は、相互接続ネットワークを経てメッセージトラヒックをルーティングすることに関連するシステムおよび方法について記述する。理解されるべきだが、この記述は、本発明を限定することを意図していない。そうではなく、例示的実施形態は、代替形態、修正形態、均等形態をカバーすることが意図されており、それらは添付の請求項によって定義されるように本発明の精神と範囲に含まれる。さらに、例示的実施形態の詳細記述において、請求された本発明の完全な理解を提供することを目的として多数の個別の詳細が記述されている。しかし、当業者であれば、そのような個別の詳細がなくても各種の実施形態が実施されうることを理解するであろう。

【００６７】

本書の例示的実施形態の特徴および要素は、特定の組み合わせにおける実施形態として記述されているけれども、それぞれの特徴または要素は、実施形態のその他の特徴および要素なしに単独で用いられてもよいし、本書で開示した他の特徴および要素と共にかまたはそれらなしに各種の組み合わせで用いられてもよい。本願で提供した方法またはフローチャートは、汎用コンピュータまたはプロセッサによって実行するための、コンピュータ可読記録媒体に収録されるコンピュータプログラム、ソフトウェア、またはファームウェアとして実装されてもよい。

【図１】

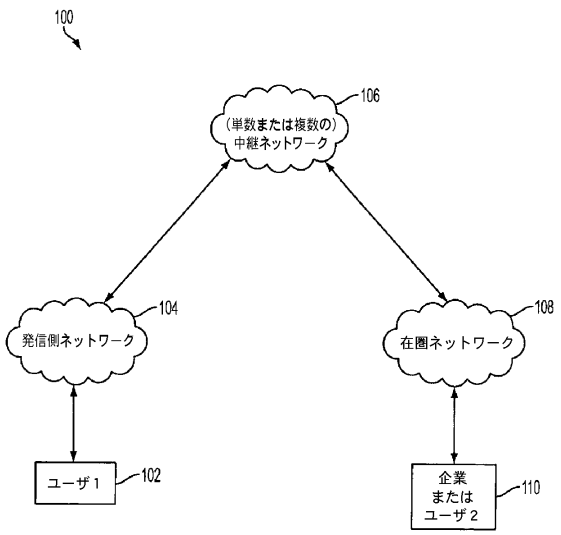

FIG. 1

【図２】

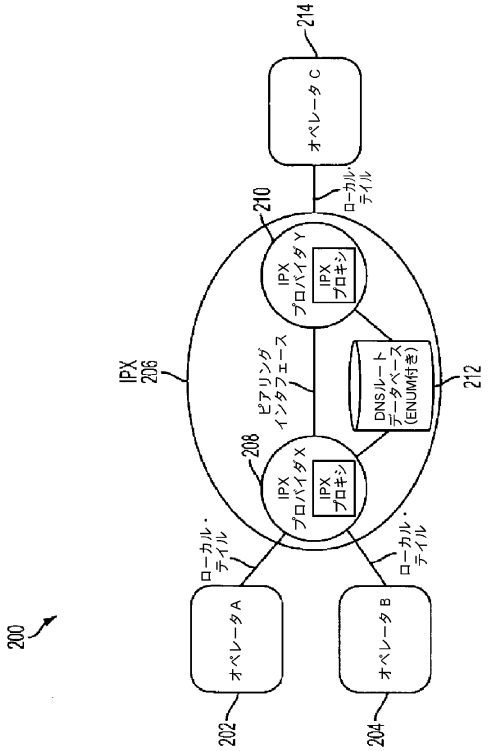

FIG. 2
先行技術

【図３（ａ）】

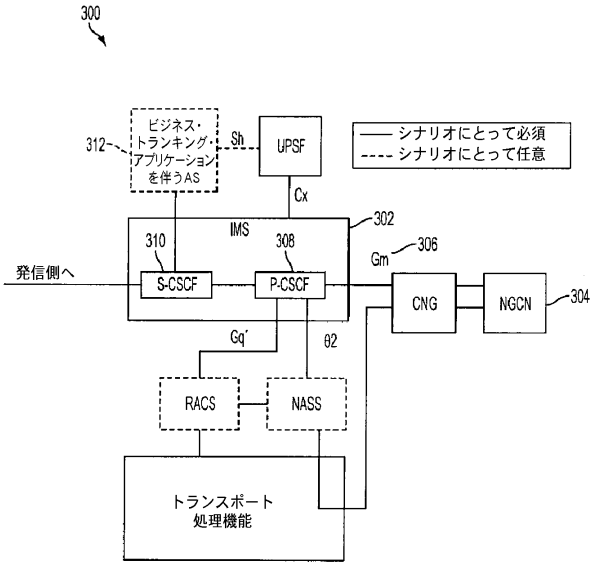

FIG. 3A
先行技術

【図３（ｂ）】

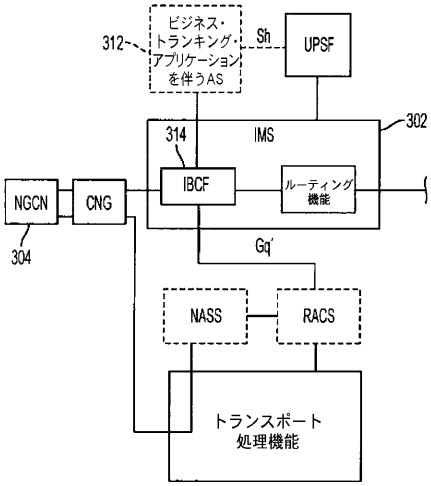

FIG. 3B
先行技術

【図４】

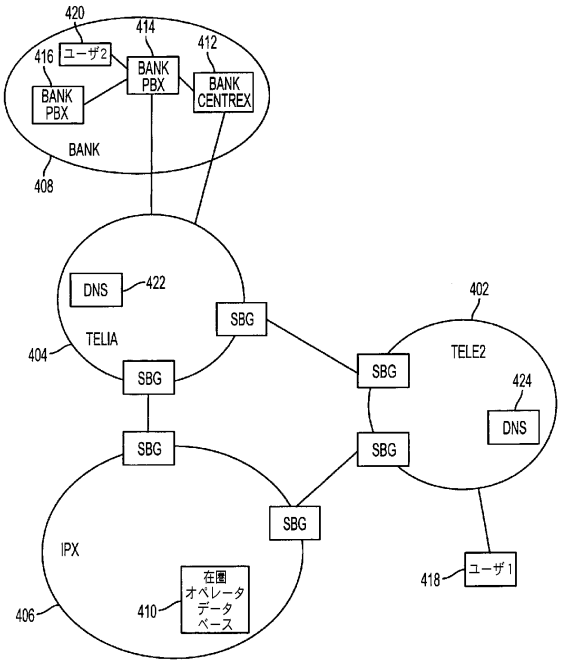

FIG. 4

【図５】

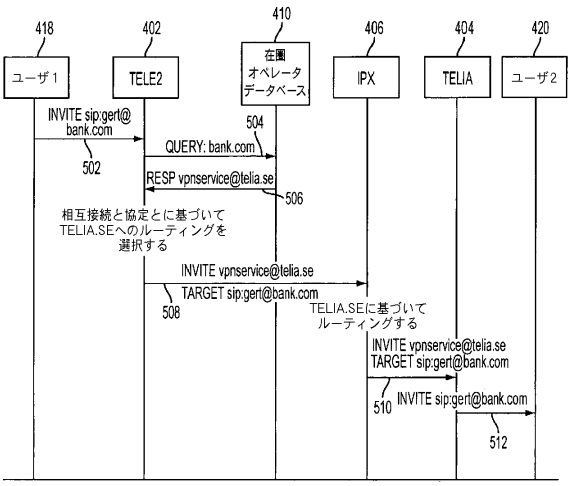

FIG. 5

【図６】

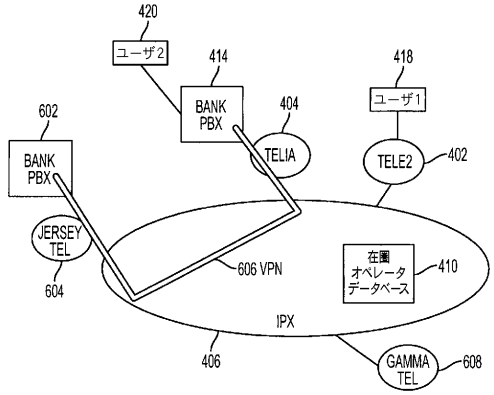

FIG. 6

【図７】

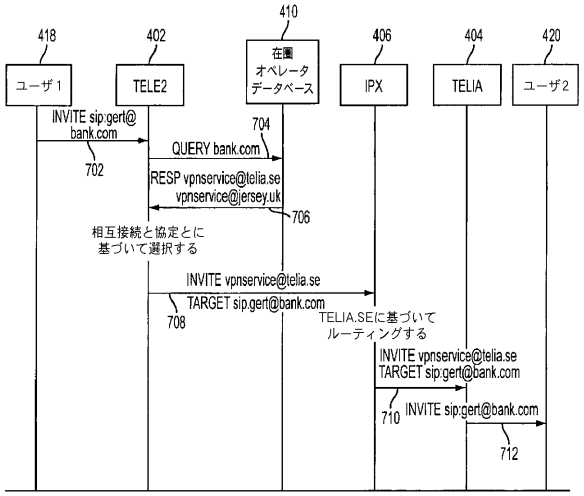

FIG. 7

【図８】

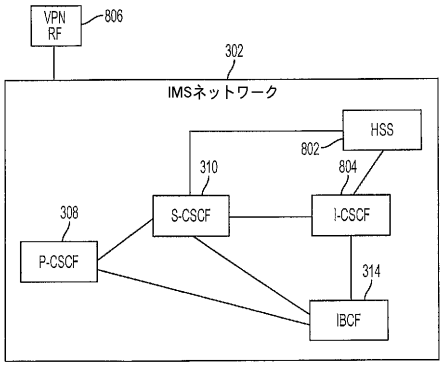

FIG. 8

【図９】

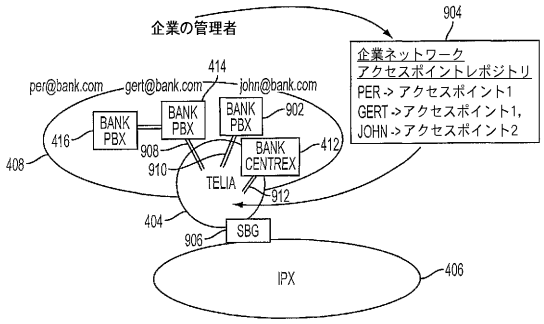

FIG. 9

【図１０】

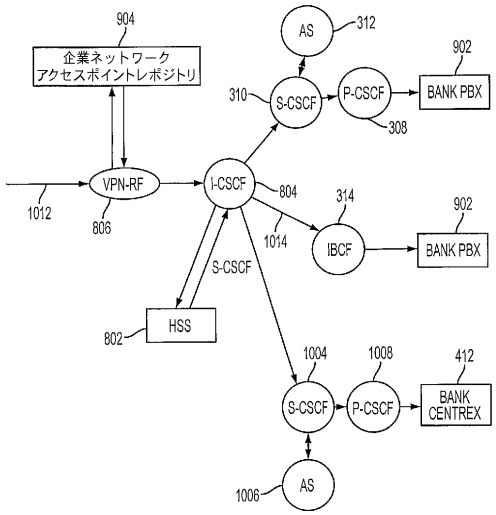

FIG. 10

【図１１（ａ）】

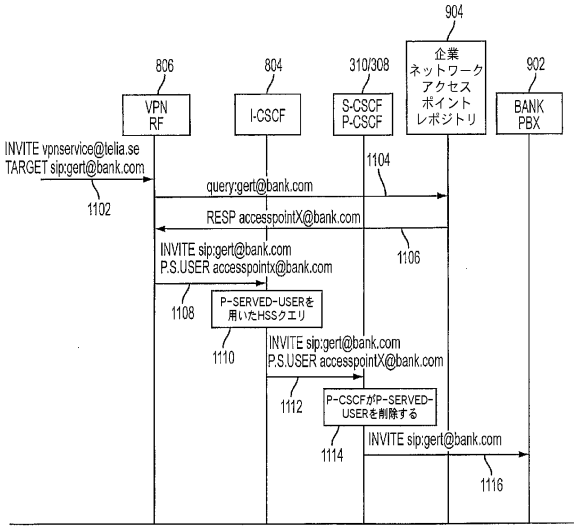

FIG. 11A

【図１１（ｂ）】

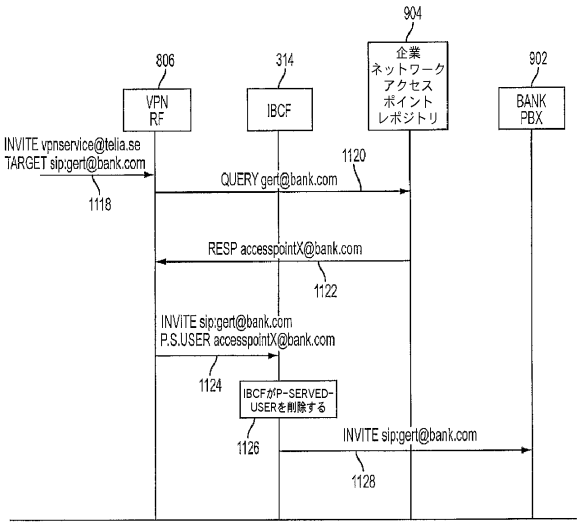

FIG. 11B

【図１２】

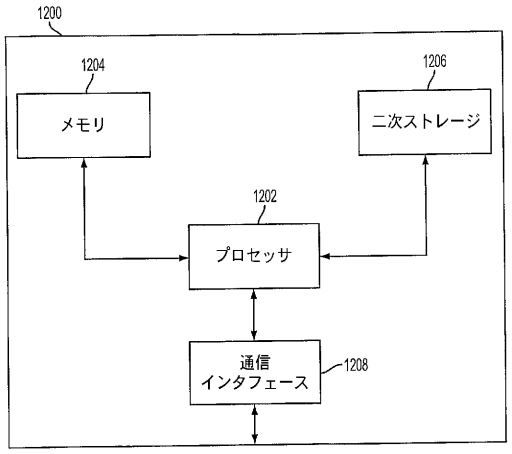

FIG. 12

【図１３】

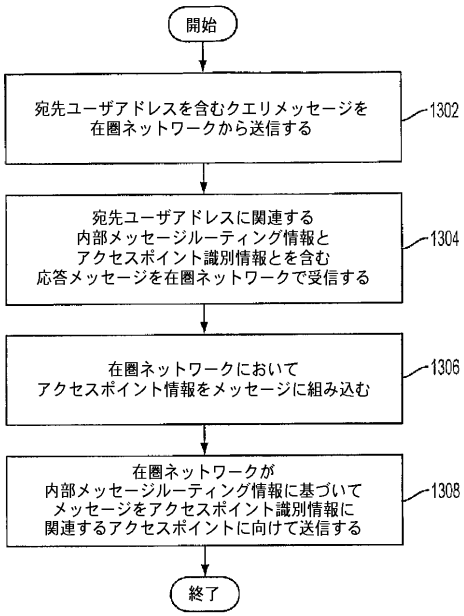

FIG. 13

【図１４】

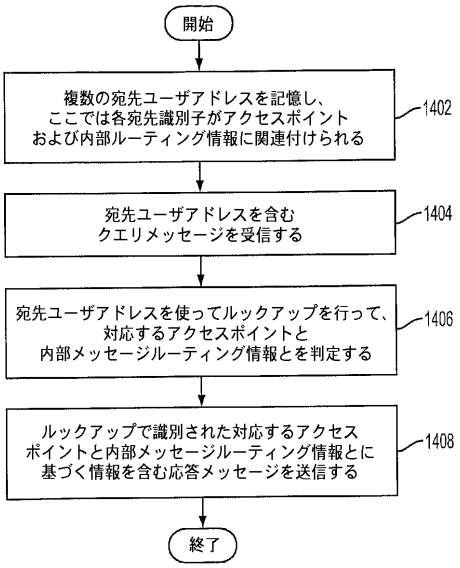
開始
複数の宛先ユーザアドレスを記憶し、
ここでは各宛先識別子がアクセスポイント
および内部ルーティング情報に関連付けられる
1402
宛先ユーザアドレスを含む
クエリメッセージを受信する
1404
宛先ユーザアドレスを使ってルックアップを行って、
対応するアクセスポイントと
内部メッセージルーティング情報とを判定する
1406
ルックアップで識別された対応するアクセス
ポイントと内部メッセージルーティング情報とに
基づく情報を含む応答メッセージを送信する
1408
終了

FIG. 14

フロントページの続き

(74)代理人 100134474
弁理士 坂田 恭弘
(72)発明者 エステル, イェルト
スウェーデン国 イェルフェッラ エス－１７５ ４８, タンブリングレンド ８
(72)発明者 ボールドウィン, ジョン
イギリス国 コヴェントリー シーブイ３ ２エックスエー, ビンレー, スキップワース ロード ７
(72)発明者 ヴァン エルベリ, ヨハネス
オランダ国 オーステルハウト エヌエル－４９０７ ディーエム, ハゲビームド ５

審査官 衣鳩 文彦

(56)参考文献 特開２００４－３４３５３７（ＪＰ, Ａ）
国際公開第２００８／１０１８３８（WO, Ａ２）
特表２００３－５１８８８５（ＪＰ, Ａ）
特表２０１２－５１４３６３（ＪＰ, Ａ）
特表２０１０－５３２５９１（ＪＰ, Ａ）
特表２０１０－５１９８３７（ＪＰ, Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ １２／００～１２／９５５
Ｈ０４Ｍ ３／００
Ｈ０４Ｗ ４／００～９９／００