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

特許第4738060号
(P4738060)

(45)発行日　平成23年8月3日(2011.8.3)　(24)登録日　平成23年5月13日(2011.5.13)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
G09C 1/00	(2006.01)	G09C	1/00	640E
H04L 9/32	(2006.01)	H04L	9/00	675D
H04L 12/56	(2006.01)	H04L	12/56	100C
H04M 3/00	(2006.01)	H04M	3/00	B

請求項の数 5　(全 15 頁)

(21)出願番号　特願2005-155900 (P2005-155900)
(22)出願日　平成17年5月27日 (2005.5.27)
(65)公開番号　特開2005-348402 (P2005-348402A)
(43)公開日　平成17年12月15日 (2005.12.15)
審査請求日　平成20年5月23日 (2008.5.23)
(31)優先権主張番号　10/856,259
(32)優先日　平成16年5月27日 (2004.5.27)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ジェレミー　ブーフ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】データ通信網のセキュアな連合

(57)【特許請求の範囲】
【請求項１】
ネットワークを連合させるための方法であって、エッジプロキシサーバが、
該エッジプロキシサーバあてのフェデレーションモードの指示を受け取るステップであって、該フェデレーションモードが、指定されたエンティティのセットとメッセージを交換するように該エッジプロキシサーバが構成される直接フェデレーションモード、及び、有効な証明書を有するエンティティからのすべての着信メッセージを該エッジプロキシサーバが受け入れることができる自動フェデレーションモードを含んでいる、ステップ、
指示されたフェデレーションモードが前記直接フェデレーションモードである場合に、管理者によって指定された許可されるべきエンティティを含むリストである、認可されたエンティティの指示を受け取るステップ、
メッセージを受信するステップ、
該メッセージが認証されたエンティティによって送信されたことを、前記指示されたフェデレーションモードに基づいて確認するステップ、並びに、
該エンティティが認証されているかどうか及び前記指示されたフェデレーションモードに基づいて、前記メッセージを扱うステップ
を実行し、
該扱うステップが、
許可され且つ認証されたエンティティによって前記メッセージが送信されたことを確認した後に、該メッセージに関する次のホップを特定するステップ、

該メッセージを該次のホップに転送するステップ、
前記指示されたフェデレーションモードが前記自動フェデレーションモードである場合に、前記メッセージのヘッダフィールドに示された証明書が、取り消された証明書のリスト中に現れるかどうかを判定するステップ、
前記メッセージが着信メッセージである場合に、該メッセージの送信者に関して示されるユニフォームリソースアイデンティファイアが該メッセージの送信元のドメインとマッチすることを確認するステップ、並びに、
前記メッセージが送信メッセージである場合に、ドメインネームサービスにクエリを行うステップ
を含むことを特徴とする方法。

【請求項２】
請求項１に記載の方法において、
前記フェデレーションモードがクリアリングハウスフェデレーションモードをさらに含み、前記エッジプロキシサーバがさらに、
前記クリアリングハウスフェデレーションモードが指示された場合に、メッセージを受信するステップと、
該受信されたメッセージを該メッセージ中で指定された受信者に転送するステップと、
前記受信されたメッセージの送信者と前記受信されたメッセージの受信者の間で直接にセッションを確立するステップと
を実行することを特徴とする方法。

【請求項３】
ネットワークを連合させるためのエッジプロキシサーバシステムであって、
エッジプロキシサーバあてのフェデレーションモードの指示を受け取る手段であって、該フェデレーションモードが、指定されたエンティティのセットとメッセージを交換するように該エッジプロキシサーバが構成される直接フェデレーションモード、及び、有効な証明書を有するエンティティからのすべての着信メッセージを該エッジプロキシサーバが受け入れることができる自動フェデレーションモードを含んでいる、手段、
メッセージを受信する手段、
該メッセージが認証されたエンティティによって送信されたことを、前記指示されたフェデレーションモードに基づいて確認する手段、
該エンティティが認証されているかどうか及び前記指示されたフェデレーションモードに基づいて、前記メッセージを扱う手段、
前記直接フェデレーションモードが前記指示されたフェデレーションモードである場合に、前記直接フェデレーションモードを試みて、管理者によって指定された許可されるべきエンティティを含むリストである、認可されたエンティティの指示を受け取る手段、並びに、
該受信されたメッセージが認証されたエンティティによって送信されたことを確認する手段
を備え、
前記扱う手段が、許可され且つ認証されたエンティティによって前記メッセージが送信されたことを確認した後に、該メッセージに関する次のホップを特定し、及び、該メッセージを該次のホップに転送し、さらに、
前記受信されたメッセージのヘッダフィールドに示された証明書が取り消された証明書のリスト中に現れない場合に前記自動フェデレーションモードを試みて、前記受信されたメッセージが着信メッセージである場合に、該メッセージの送信者に関して示されるユニフォームリソースアイデンティファイアが、該メッセージの送信元のドメインとマッチすることを確認し、及び、前記受信されたメッセージが送信メッセージである場合に、ドメインネームサービスにクエリを行う手段
を備えることを特徴とするエッジプロキシサーバシステム。

【請求項４】

請求項３に記載のエッジプロキシサーバシステムにおいて、
前記フェデレーションモードはクリアリングハウスフェデレーションモードをさらに含み、
前記クリアリングハウスフェデレーションモードが選択されたときに、メッセージを受信する手段と、
該受信されたメッセージを該メッセージ中で指定された受信者に転送する手段と、
前記受信されたメッセージの送信者と前記受信されたメッセージの受信者の間で直接にセッションを確立する手段と
をさらに備えることを特徴とするエッジプロキシサーバシステム。
【請求項５】
コンピュータが実行可能な命令をコンピュータにより読み取り可能に記憶した記憶媒体において、
前記命令が前記コンピュータに請求項１または２に記載の方法を実行させることを特徴とする記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
ここで説明する技術は、全体としてはデータ通信網に関する。より詳細には、データ通信網のセキュアな連合（secure federation）に関する。
【背景技術】
【０００２】
アプリケーションは、ときとして、コンピューティングデバイス間でセッションを確立し、管理する必要がある。セッションは、ある期間にわたって行われるコンピューティングデバイス間の対話のセットである。一例として、ＭＩＣＲＯＳＯＦＴ　ＭＥＳＳＥＮＧＥＲ（登録商標）または「ボイスオーバーインターネットプロトコル」であるＶｏＩＰなどのリアルタイム通信アプリケーションは、ユーザのために通信デバイス間でセッションを確立する。これらのアプリケーションは、「セッション開始プロトコル」である「ＳＩＰ」などの様々な機構を使用して、セッションを確立することができる。ＳＩＰは、デバイスが、互いを検出し、デバイス間でセッションを確立し、変更し、終了するのに使用することができるアプリケーションレイヤ制御プロトコルである。ＳＩＰは、インターネット提案標準（internet proposed standard）である。ＳＩＰの仕様である「ＲＦＣ３２６１」は、非特許文献１より入手可能である。イベント通知に関連するＳＩＰの拡張に関する仕様である「ＲＦＣ３２６５」は、非特許文献２より入手可能である。ＳＩＰサーバを探し出すことに関する仕様である「ＲＦＣ３２６３」は、非特許文献３より入手可能である。以上の仕様の３つすべては、参照により全体が本明細書に組み込まれている。
【０００３】
アプリケーションは、ＳＩＰを別のプロトコルとともに使用して、情報を送受信することができる。一例として、アプリケーションは、セッション中にリアルタイムデータを転送するために「リアルタイムトランスポートプロトコル」であるＲＴＰとともにＳＩＰを使用することができる。他のプロトコルとともにＳＩＰを使用することにより、アプリケーションは、セッションを作成し、管理し、セッション中に情報を交換することができる。情報を交換するためにＳＩＰとともに使用されるプロトコルは、情報をメッセージにセグメント化することがある。一例として、ＶｏＩＰアプリケーションは、長いナレーション（narration）をより短いメッセージにセグメント化することができる。セッション中にメッセージを交換することは「ダイアログ」と呼ばれる。ＳＩＰは、一般に使用されるトランスポートレイヤプロトコルおよびネットワークレイヤプロトコルであるＴＣＰ／ＩＰ（伝送制御プロトコル／インターネットプロトコル）などの、より低レベルの通信レイヤを使用して、ダイアログのメッセージを転送することができる。
【０００４】
ＳＩＰネットワークは、クライアントとして、サーバとして、または両方としてダイア

ログに参加することができるエンティティを含む。ＳＩＰは、次の４つのタイプのエンティティ、すなわち、ユーザエージェント、プロキシサーバ、リダイレクト（redirect）サーバ、およびレジストラ（registrar）をサポートする。ユーザエージェントは、他のＳＩＰエンティティとメッセージを交換することにより、セッションの開始および終了を行う。ユーザエージェントは、一般に、ＳＩＰ要求（例えば、セッションを開始する）を開始するデバイスであるユーザエージェントクライアント、または、一般に、ＳＩＰ要求を受信し、そのような要求に応答するデバイスであるユーザエージェントサーバとすることができる。一例として、「ＩＰ電話」、パーソナルデジタルアシスタント、および他の任意のタイプのコンピューティングデバイスは、ユーザエージェントとすることができる。デバイスは、あるダイアログではユーザエージェントクライアントとし、別のダイアログではユーザエージェントサーバとすることができ、あるいはダイアログ中で役割を変更することができる。プロキシサーバは、クライアント(複数)に対しサーバとして動作し、サーバ(複数)に対してはクライアントとして動作するエンティティである。このように動作する際、プロキシサーバは、クライアントとサーバ間でメッセージの代行受信、解釈または転送を行う。プロキシサーバは、例えば、メッセージの送信者および受信者を検証することにより、ネットワークセキュリティに貢献する。リダイレクトサーバは、ＳＩＰ要求を受け入れ、ＳＩＰ応答を生成して、要求を送信したクライアントに代替のネットワークリソースと接触するように指示する。一例として、リダイレクトサーバは、幾つかのデバイスのいずれにおいて特定のユーザが現在、応対可能かを示すことができる。レジストラは、ＳＩＰクライアント(複数)から登録情報を受け入れ、ロケーションサービス、またはその他のエンティティに受け取られた登録情報を知らせるサーバである。

【０００５】

ＳＩＰは次の２つのメッセージタイプをサポートする。クライアントからサーバに送信される要求、および、一般に、要求に応答する際にサーバからクライアントに送信される応答である。ＳＩＰメッセージは３つの部分を含む。ＳＩＰメッセージの第１の部分は、メッセージタイプを示すフィールド、およびプロトコルバージョンを示すフィールドを含む「開始行」である。ＳＩＰメッセージの第２の部分は、値が名前－値のペアとして表されるヘッダフィールド(複数)を含む。ＳＩＰメッセージの第３の部分は、開始されるべきセッションを記述する、またはセッションに関連するデータを含むのに使用されるメッセージの本文である。メッセージ本文は、要求中または応答中に現れることができる。

【０００６】

ＳＩＰメッセージは、ＳＩＰメッセージのヘッダフィールド(複数)の内容に基づいてルーティングされる。適正には、ＳＩＰ要求は少なくとも次の６つのヘッダフィールドを含まなければならない。すなわち、Ｔｏフィールド、Ｆｒｏｍフィールド、ＣＳｅｑフィールド、Ｃａｌｌ－ＩＤフィールド、Ｍａｘ－Ｆｏｒｗａｒｄｓフィールド、Ｖｉａフィールドである。Ｔｏヘッダフィールドは要求の受信者の論理的ＩＤを示す。Ｆｒｏｍヘッダフィールドは要求の開始者の論理的ＩＤを示す。Ｍａｘ－Ｆｏｒｗａｒｄｓヘッダフィールドは、要求の宛先に着信するまでに要求が行うことができるホップの回数を示す。一例として、デバイスＡからのメッセージが宛先デバイスＣに着信する前にデバイスＢを通過する場合、そのメッセージは２回のホップ（例えば、デバイスＢおよびＣ）を行ったという言い方をされる。Ｖｉａヘッダフィールドは、それまでに要求が辿ってきたパス（例えば、要求が通過してきたデバイスのネットワークアドレスのシーケンス）を示し、応答をルーティングする際に辿るべきパスを示す。ヘッダは、将来の要求および応答が示されたデバイス経由でルーティングされるべきことを示すのに使用されるＲｅｃｏｒｄ－Ｒｏｕｔｅフィールド(複数)も含むことができる。ネットワークデバイス(複数)は、ダイアログの中の後続のメッセージが指定されたデバイスを介してルーティングされるように強制しようとして、ＳＩＰメッセージを転送する際にデバイス(複数)を指定するＲｅｃｏｒｄ－Ｒｏｕｔｅヘッダフィールド(複数)を挿入することができる。Ｒｅｃｏｒｄ－Ｒｏｕｔｅヘッダフィールドは、デバイスおよびパラメータに関する識別子（例えば、ネットワークアドレス）を含むことができる。以上、およびその他のヘッダフィールド(複数)は、前述

したＳＩＰ仕様書中で説明されている。
【０００７】
幾つかの組織(organizations)がそれぞれ、ＳＩＰサーバ(複数)をネットワークリソースとして提供することができる。それらの組織は、それらの組織のネットワークの外部から、例えば、インターネットから、または他の組織からのＳＩＰクライアント(複数)およびＳＩＰサーバ(複数)が、それらの組織のＳＩＰサーバ(複数)に接続して、メッセージを交換できるようにすることができる。組織は、組織のＳＩＰサーバに関する証明書を信頼されるエンティティから獲得して、組織のＳＩＰサーバが送信するメッセージを他の組織が認証できるようにすることができる。ＳＩＰサーバは、「ＴＬＳ」（トランスポートレイヤセキュリティ）などのプロトコルを使用して、その証明書の指示をＳＩＰサーバが送信するメッセージに追加することができる。
【０００８】
組織は、組織のＳＩＰサーバ(複数)またはＳＩＰネットワーク(複数)を連合させる（federate）ことを所望することがある。組織のＳＩＰサーバ(複数)またはＳＩＰネットワーク(複数)を連合させることにより、組織は、組織のネットワーク(複数)の参加者が、その連合（federation）内の他の信頼される組織のＳＩＰサーバ(複数)と通信できるようにする。一例として、組織は、アプリケーションレベル「ＶＰＮ」（仮想プライベートネットワーク）をセットアップして、組織によって実行されているアプリケーション(複数)が、別の組織のネットワークに位置しているであろうＳＩＰサーバ(複数)とセキュアに通信できるようにすることを所望することがある。ＳＩＰサーバ(複数)の管理者らが、管理者らのＳＩＰサーバ(複数)をセキュアに連合させることができるようにする有効なアプローチは、重要な有用性を有する。
【０００９】
【非特許文献１】ＲＦＣ３２６１，<http://www.ietf.org/rfc/rfc3261.txt>
【非特許文献２】ＲＦＣ３２６５，<http://www.ietf.org/rfc/rfc3265.txt>
【非特許文献３】ＲＦＣ３２６３，<http://www.ietf.org/rfc/rfc3263.txt>
【発明の開示】
【発明が解決しようとする課題】
【００１０】
従来、データ通信網のセキュアな連合のための技術が必要とされている。
【課題を解決するための手段】
【００１１】
データ通信網のセキュアな連合のための技術を提供する。この技術は、エッジプロキシサーバを使用して、フェデレーションモードに依存してメッセージをルーティングする。直接フェデレーションモード（Direct federation mode）では、ネットワークのエッジプロキシサーバは、メッセージを、他のネットワーク(複数)、サーバ(複数)、デバイス(複数)、またはユーザ(複数)などの指定されたエンティティのセットと交換するように構成される。自動フェデレーションモード（Automatic federation mode）では、エッジプロキシサーバは、有効な証明書を有するエンティティからのすべての着信メッセージを受け入れることができる。クリアリングハウスフェデレーションモード（Clearinghouse federation mode）では、エッジプロキシサーバは、すべての送信メッセージを、指定された信頼されるクリアリングハウスサーバに転送する。
【発明を実施するための最良の形態】
【００１２】
一実施形態では、データ通信網のセキュアな連合のための技術が提供される。この技術は、エッジプロキシサーバを使用して、フェデレーションモードに依存してメッセージをルーティングする。エッジプロキシサーバは、エッジプロキシサーバのネットワーク「外部の」コンピューティングデバイスが、エッジプロキシサーバを介してエッジプロキシサーバのネットワーク「内部の」コンピューティングデバイスと通信するように、また同様にその逆を行うように、２つのネットワーク（例えば、イントラネットとインターネット

、または２つのイントラネット）間にまたがるネットワークリソースである。エッジプロキシサーバは、エッジプロキシサーバのネットワークの両側のコンピューティングデバイス間における仲介役として動作する。そのように動作する際、エッジプロキシサーバは、クライアントやサーバなどのエンティティ間で、メッセージの代行受信、解釈、または転送を行う。管理者は、ダイレクトモード、オートモード、またはクリアリングハウスモードを含む幾つかのフェデレーションモードの１つまたは複数において、エッジプロキシサーバを有するデータ通信網を連合させることを選択することができる。管理者は、エッジプロキシサーバのネットワーク外部のコンピューティングデバイスのユーザによるエッジプロキシサーバのネットワーク内部のコンピューティングデバイスへのアクセスを許す、または拒否することを選択することもできる。

【００１３】

直接フェデレーションモードでは、ネットワークのエッジプロキシサーバは、メッセージを、他のネットワーク(複数)、サーバ(複数)、デバイス(複数)、またはユーザ(複数)などの指定されたエンティティのセットと交換するように構成される。ネットワーク管理者は、エッジプロキシサーバがメッセージを交換することが許可される相手である、サーバまたはドメインなどの許可されたエンティティを指定することができる。管理者は、「ＵＲＩ」（ユニフォームリソースアイデンティファイア）を使用して、それらのエンティティを指定することができる。一例として、管理者は、管理者のエッジプロキシサーバ「ｅｄｇｅ．ｐａｒｔｎｅｒａ．ｃｏｍ」を介するダイレクトフェデエレーションに関してパートナー（「ＰａｒｔｎｅｒＡ」）を許可するように示し、ＰａｒｔｎｅｒＡにドメイン「ｐａｒｔｎｅｒａ．ｃｏｍ」に関してだけ責任および許可を与えることができる。この構成は、「ｅｄｇｅ．ｐａｒｔｎｅｒａ．ｃｏｍ」が、接続し、「＜任意のユーザ＞@ｐａｒｔｎｅｒａ．ｃｏｍ」のパターンとマッチするＵＲＩを有する任意のユーザに関するメッセージを送信、または受信することを許可する。エッジプロキシサーバは、例えば、証明書、共有鍵、秘密で交換される公開鍵／秘密鍵ペア、Ｋｅｒｂｅｒｏｓ、またはその他の資格証明書ベースの認証を含む、様々な認証モデルを使用して、エッジプロキシサーバのネットワーク外部のコンピューティングデバイス(複数)を認証することもできる。エッジプロキシサーバによって使用される認証モデルを選択する管理者は、「ＤＮＳ」（ドメインネームサービス）以外の認証が使用されてはならないことを示すこともできる。この認証は、接続が確立された際に受け取られた、または着信メッセージのヘッダフィールドの中で現れる証明書が、取り消された証明書のリスト中に現れるかどうかを判定することを含むことができる。証明書が使用される場合、取り消された証明書のこのリストは、ときどき、自動的に、または手動で更新されることができる。許可されたエンティティを認証することは、許可されたエンティティが有効な（例えば、認証済みの）接続上でメッセージを送信したかどうかを判定することも含むことができる。認証検査および許可検査が完了すると、エッジプロキシサーバは、認証されていない、または許可されていないエンティティからの、またはそのようなエンティティへのすべてのメッセージを無視することができる。メッセージが許可されたエンティティ（認証済みであることも可能な）から着信すると、エッジプロキシサーバは、そのメッセージを送信したエンティティ、またはそのメッセージの受信者であるエンティティが、「拒否リスト」の中に現れるかどうかを検査することができる。一例として、「Ｘ．ＣＯＭ」は、許可されたエンティティであるが、「ＪＯＥ@Ｘ．ＣＯＭ」は拒否リストの中にある可能性がある。そのようなケースでは、「ＳＡＬＬＹ@Ｘ．ＣＯＭ」からのメッセージは受け入れられるが、「ＪＯＥ@Ｘ．ＣＯＭ」からのメッセージは無視される。次に、エッジプロキシサーバは、無視されなかったメッセージを適切な「次のホップ（next hop）」に転送することができる。次のホップは、そのメッセージが次にルーティングされるコンピューティングデバイスである。エッジプロキシサーバは、メッセージのヘッダフィールド(複数)の内容に基づいて、次のホップの管理者構成により、またはそのメッセージの受信に関連する登録サーバなどの別のサーバにクエリを行うことにより、そのメッセージに関する次のホップを特定する。このため、直接フェデレーションモードでは、メッセージは管理者によって許可されるように

指示されたエンティティとだけ交換されることがあり、認証されることができる。

【００１４】

自動フェデレーションモードでは、エッジプロキシサーバは、エッジプロキシサーバの管理者によって容認できると示された形で自らを認証することができるエンティティからのすべての着信メッセージを受け入れることができる。エッジプロキシサーバは、例えば、証明書、共有鍵、秘密で交換される公開鍵／秘密鍵ペア、Ｋｅｒｂｅｒｏｓ、またはその他の資格証明書ベースの認証を含む、様々な認証モデルを使用して、エッジプロキシサーバのネットワーク外部のコンピューティングデバイス(複数)を認証することができる。一例として、エンティティは、メッセージをエッジプロキシサーバに送信する際、すべてのメッセージに証明書を追加すること、または接続に関連する証明書を提供することにより、自らをエッジプロキシサーバに対して認証することができる。認証済みの接続上でメッセージを受信すると、エッジプロキシサーバは、その証明書に基づいてメッセージを受け入れることを選択することができる。これとは別に、メッセージは、認証されていない接続上のメッセージを認証する証明書を含むこともできる。認証は、例えば、メッセージの中で示された証明書が、取り消された証明書のリストの中で現れるかどうかを判定することによって証明書を検証することを含むことができ、これは、メッセージまたは接続を無効にする指示とすることができる。この取り消された証明書のリストは、ときどき、自動的に、または手動で更新される。エッジプロキシサーバは、メッセージの送信者に関して示されたＵＲＩが、メッセージを実際に送信したドメイン（送信側エンティティを認証するのに使用される証明書で識別される）とマッチすることを検証することができる。エッジプロキシサーバは、エッジプロキシサーバのネットワーク内部のコンピューティングデバイスから送信メッセージを受信すると、ＤＮＳのクエリサービスである「ＳＲＶ」を使用して、宛先サーバがどのようなサービスを提供するかを知ることができる。この機構は、合わせて「ＤＮＳ－ＳＲＶ」と呼ばれる。次に、エッジプロキシサーバは、宛先サーバが相互認証トランスポートレイヤセキュリティ（Mutually authenticated Transport Layer Security）である「ＭＴＬＳ」を提供する場合、ＭＴＬＳを使用して、宛先サーバに対してセキュリアなセッションを要求することができる。自動フェデレーションモードは、そこからのメッセージが拒否される、またはそこにメッセージが送信されないことが可能なエンティティを含む拒否リストも有することができる。このため、自動フェデレーションモードでは、エッジプロキシサーバは、メッセージが実際に受信されるか、または送信されるまで、その連合（federation）の他のネットワーク(複数)またはサーバ(複数)について知る必要がない。

【００１５】

クリアリングハウスフェデレーションモードでは、エッジプロキシサーバは、すべての送信メッセージを、指定された信頼されるクリアリングハウスサーバに転送する。クリアリングハウスサーバは、クリアリングハウスサーバが受信するメッセージを、メッセージの中で指定された受信者に転送することができる。一実施形態では、クリアリングハウスサーバは、セッションの中で接続されたコンピューティングデバイス間でメッセージをルーティングすることを続ける。一実施形態では、メッセージの受信者は、セッションの中の後続のメッセージに関してクリアリングハウスを迂回して、送信者に対して直接にセッションを確立することができる。クリアリングハウスを使用することにより、エッジプロキシサーバは、その連合（federation）の他のネットワーク(複数)またはサーバ(複数)について知る必要がなく、信頼されるクリアリングハウスサーバについてだけ知っていればよい。ある連合のネットワーク(複数)またはサーバ(複数)は、クリアリングハウスによってメッセージが転送されたすべてのエンティティを黙示的に信頼することができる。ただし、自動フェデレーションモードおよび直接フェデレーションモードと同様に、クリアリングハウスフェデレーションモードは、そこからのメッセージが拒否されるエンティティを含む拒否リストも有することができる。クリアリングハウスフェデレーションモードでは、エッジプロキシサーバは、そのメッセージ交換を円滑にする管理されたクリアリングハウスの使用を介して、最小限の構成で多数のネットワークとメッセージを交換するよう

に容易に構成することができる。

【００１６】

クリアリングハウスフェデレーションモードの代替の実施形態では、クリアリングハウスサーバは、いずれのドメインにクリアリングハウスサーバがメッセージを転送することができるかを示すことができる。この指示（indication）により、クリアリングハウスサーバのサブセットが管理者のエッジプロキシサーバ(複数)にメッセージを転送するのを管理者が許可することができるようになる。

【００１７】

複数のフェデレーションモードを、様々な「ハイブリッド」フェデレーションモードにおいて同時に使用することもできる。一例として、幾つかの直接フェデレーションモードのパートナーが構成されている場合でも、オートフェデエレーションを使用することができる。エッジプロキシサーバは、エッジプロキシサーバが対話する相手のエンティティを、管理者が後に改良してエントリを追加する、または削除することができる許可リストに動的に追加することにより、追加のエンティティを自動的に許可することもできる。クリアリングハウスフェデレーションモードを直接フェデレーションモードと一緒に使用することもできる。この構成では、エッジプロキシサーバは、許可されたエンティティと直接にメッセージを交換することができ、クリアリングハウスサーバを使用して他のエンティティを認証することができる。既知のエンティティを指定し、より大きいセットのエンティティとのメッセージ交換も可能にすることにより、システムは、管理者側の相当な手作業を要求することなしに、大きいセットのエンティティとの通信が可能になる。

【００１８】

次に図を参照すると、図１は、データ通信網をセキュアに連合させる（federating data communications networks securely）ためのシステムの実施形態を示すブロック図である。このシステムは、１つまたは複数のクライアント１０２、１つまたは複数のネットワーク１０４、並びにインターネットなどのクライアント(複数)およびネットワーク(複数)１１４を接続するネットワークを有することができる。クライアント(複数)は、ネットワーク接続１０８を介してインターネットに接続することができる。ネットワーク(複数)１０４は、様々な形態のデータ通信リンク１１０を使用してインターネットに接続することができる。クライアント(複数)は、例えば、コンピュータ(複数)、携帯電話(複数)、またはインターネットに接続された他のデバイス(複数)であって良い。ネットワーク(複数)は、例えば、イントラネット(複数)とすることができる。クライアント(複数)は、専用データ通信リンク１１２を使用してネットワーク(複数)に直接に接続することもできる。同様に、ネットワーク(複数)も、専用データ通信リンク１１２を使用して他のネットワーク(複数)に直接に接続することができる。システムは、データ通信リンク１１８を介してインターネットに接続されたクリアリングハウス１１６も有することができる。インターネットは、他の様々なコンピューティングデバイス（図示せず）にも接続することができる。本明細書で説明する接続は、物理的とすることが可能であり、ワイアレスとすることが可能であり、実際、任意の形態のデータ通信網接続とすることができる。

【００１９】

図２は、図１のネットワークの実施形態を示すブロック図である。ネットワーク２００は、１つまたは複数のクライアント２０２、サーバ２０４、ディレクトリサーバ２０６、ダイレクタ（director）２０８、ＤＮＳ２１０、およびエッジプロキシサーバ２１２を含む。ネットワークは、その他のデバイス(複数)（図示せず）も含むことができる。ネットワークの図示したデバイス(複数)（および図示していないデバイス(複数)）は、ネットワーク２００に関連するデータ通信網を介して互いに接続することができる。クライアント(複数)２０２およびサーバ２０４は、ＳＩＰメッセージを交換することを含め、様々な活動を実行することができる。ディレクトリサービス２０６は、デバイス(複数)、ユーザ(複数)、およびその他のネットワークリソース(複数)に関するロケーションサービスを提供することができる。一例として、ディレクトリサービスは、ＡＣＴＩＶＥ　ＤＩＲＥＣＴＯＲＹサービスとすることができる。ダイレクタ２０８は、例えば、クライアント(複

数)をクライアント(複数)が関連するサーバに、またはサーバのプールにリダイレクトすること、ネットワークトラフィックのログをとること、およびネットワークの一部ではないコンピューティングデバイスからネットワークに接続するユーザ(複数)を認証することを含め、様々なサーバ関連機能を実行する。ＤＮＳは、ネットワークリソース名（例えば、デバイス名）をネットワークロケーション（例えば、ＩＰアドレス）にマップするデータベースを有する。ネットワークのデバイス(複数)は、ＤＮＳを使用して、「フレンドリな」デバイス名を、そのデバイスがメッセージをルーティングするのに使用することができるネットワークアドレスに帰着（resolve）することができる。エッジプロキシサーバ２１２は、ネットワーク２００（「内部」ネットワーク）と「外部」ネットワーク、例えば、インターネット（図示せず）の両方に接続される。クライアントがサーバに対するセッションを開くことを所望する場合、エッジプロキシサーバは、例えば、セッションが開かれるべきかどうか、およびいずれの通信リンクが使用されるべきかを判定することができる。

【００２０】

図３は、図２のエッジプロキシサーバに関連するコンポーネント(複数)の実施形態を示すブロック図である。コンポーネント(複数)は、トランスポートコンポーネント３０２、ＤＮＳ－ＳＲＶコンポーネント３０４、ルーティングコンポーネント３０６、およびリストコンポーネント３０８を含む。エッジプロキシサーバは、着信メッセージ（すなわち、「外部」ネットワークから着信するメッセージ）を受信し、送信メッセージ（すなわち、「外部」ネットワークに向かうメッセージ）を転送する。エッジプロキシサーバは、メッセージに関連する様々な操作を実行した後、着信メッセージまたは送信メッセージを次のホップ（すなわち、メッセージが次にルーティングされるデバイス）に転送する。これらの操作には、メッセージが、メッセージヘッダフィールド中に示されたサーバから受信されたかどうかを確認すること、メッセージの送信者が、エッジプロキシサーバのネットワークにメッセージを送信することを許可されているかどうかを判定すること、いずれのデバイスにメッセージが次にルーティングされるべきかを判定することが含まれ得る。これらの操作は、トランスポートコンポーネント３０２、ルーティングコンポーネント３０６、ドメインネームサービスクエリサービスコンポーネント３０４、リストコンポーネント３０８などの、ネットワークの様々なコンポーネント、およびエッジプロキシサーバによって、またはそれらを使用して実行される。

【００２１】

トランスポートコンポーネント３０２は、エッジプロキシサーバがメッセージを交換する相手のコンピューティングデバイス(複数)に対してセッションを確立する。一例として、トランスポートコンポーネントは、メッセージをネットワークに送り込むコンピューティングデバイスに対してＭＴＬＳ接続を確立することができる。トランスポートコンポーネントは、例えば、エッジプロキシサーバが指定された機能を実行するのを妨げようとする、悪意のあるユーザまたはデバイスによる試みである「ＤｏＳ攻撃」から、エッジプロキシサーバを保護しようと努めて、トランスポートコンポーネントが他のコンピューティングデバイス(複数)に対して確立するセッション数、または接続数を制御することもできる。トランスポートコンポーネントは、ネットワーク外部のデバイスからのメッセージ中に現れる、またはネットワーク外部のデバイスに対して接続を確立する際に受け取られた証明書が、無効な証明書のリストに現れないことを確認することもできる。トランスポートコンポーネントは、システムがネットワーク外部のデバイス(複数)に転送する、またはそのようなデバイス(複数)に対して接続を確立するメッセージに独自の証明書を追加することもできる。

【００２２】

ルーティングコンポーネント３０６は、着信メッセージおよび送信メッセージが、メッセージのヘッダフィールド(複数)の内容に基づいて転送されるべきかどうかを判定する。ルーティングコンポーネントは、メッセージの送信者のＵＲＩが、メッセージのヘッダに含まれる認証情報、およびその他の情報とマッチするかどうかを判定することにより、着

信メッセージを検証する。エッジプロキシサーバが直接フェデレーションモードで動作しているか、自動フェデレーションモードで動作しているか、またはハイブリッドフェデレーションモードで動作しているかに関わらず、ルーティングコンポーネントは、送信者または受信者のエンティティ（またはエンティティのドメイン）が、許可されたエンティティまたはドメインのリストに現れるかどうかを判定する。エッジプロキシサーバが自動フェデレーションモード（または自動フェデレーションモードを含むハイブリッドフェデレーションモード）で動作している場合、ルーティングコンポーネントは、ＵＲＩのドメインがメッセージのヘッダに含まれる他の情報とマッチするかどうかも判定する。

【００２３】

ルーティングコンポーネントは、メッセージのヘッダフィールド(複数)の内容に基づき、送信メッセージの検証も行う。直接フェデレーションモードで動作している場合、ルーティング機構は、送信メッセージに関して示されたドメインが許可されているかどうかを判定する。そのドメインが許可されていない場合、ルーティングコンポーネントは、そのメッセージを無視するか、またはそのドメインが許可されていないことを示す応答メッセージを戻す。自動フェデレーションモードで動作している場合、ルーティングコンポーネントは、メッセージの中で示された宛先エンティティのドメインが許可されているかどうかをまず確認する。そのドメインが許可されていない場合、メッセージは、ＤＮＳ－ＳＲＶコンポーネントに転送され、そのメッセージを転送することができるかどうか判定することができる。メッセージは、ＤＮＳ－ＳＲＶコンポーネントが、そのメッセージを受信する適切なエンティティを探し出すことができない場合は転送されないことができる。

【００２４】

「ＤＮＳ－ＳＲＶ」（ドメインネームサービスクエリサービスコンポーネント）３０４は、メッセージに関する宛先サーバ(複数)を特定する。このコンポーネントを送信メッセージに関して使用して、メッセージをどのようにルーティングするかを特定することができる。ＤＮＳ－ＳＲＶコンポーネントは、いずれのサーバにメッセージをルーティングするかをコンポーネントが特定することができない場合、メッセージを無視するか、または失敗を示す応答メッセージを戻すことができる。メッセージがルーティングされるべき適切なサーバを探し出すことができないことは、メッセージが、許可されていないサーバを宛先としていることを示す可能性がある。ＤＮＳ－ＳＲＶコンポーネントは、ＤＮＳサーバにクエリを行うことにより、そのメッセージをルーティングすることができるサーバのセットを獲得する。ＤＮＳ－ＳＲＶコンポーネントは、トランスポートコンポーネントによって要求された場合、このクエリを実行して、例えば、ＵＲＩに基づいてメッセージに関するサーバを示す。すると、トランスポートコンポーネントが、示されたサーバにメッセージを送信しようと試みる。トランスポートコンポーネントは、示されたサーバと接触することができない場合、代替のサーバを提供するようにＤＮＳ－ＳＲＶコンポーネントに要求することができる。このプロセスは、トランスポートコンポーネントが接触することができるサーバをＤＮＳ－ＳＲＶコンポーネントが明らかにするまで繰り返される。これとは別に、ＤＮＳ－ＳＲＶコンポーネントは、サーバのリストをトランスポートコンポーネントに提供し、トランスポートコンポーネントは、トランスポートコンポーネントが接触することができるサーバを探し出すまで、独立にリストを反復処理する（iterate）。ＤＮＳ－ＳＲＶコンポーネントは、エッジプロキシサーバが直接フェデレーションモードで動作している場合は、以上のステップを実行しなくてもよいことがある。というのは、サーバアドレスが明示的に示されることができるからである。

【００２５】

リストコンポーネント３０８は、エッジプロキシがメッセージを交換する相手のエンティティの関連リスト（「受け入れリスト」）、およびエッジプロキシがメッセージを交換しない相手のエンティティの関連リスト（「拒否リスト」）を有することができる。リストは、ハードディスクドライブ、ランダムアクセスメモリ、または接続されたファイルサーバ（図示せず）などの、エッジプロキシサーバに関連する、または接続された記憶装置に格納できる。一実施形態では、システムは、受け入れリスト（すなわち、許可済みのエ

ンティティを含む）を調べてから、拒否リスト（すなわち、許可されていないエンティティを含む）を調べることができる。代替の実施形態では、システムは逆の順序でリストを調べることができる。いずれのリストが先に調べられるかは、あるエンティティが両方のリストに現れる場合、異なる結果をもたらす可能性がある。一例として、あるエンティティが両方のリストに現れ、拒否リストが先に調べられる場合、そのエンティティからのメッセージは、そのエンティティが受け入れリストに後で追加された場合でも、受け入れられない可能性がある。

【００２６】

リストは、探索をサポートする様々なスキームを使用して指定されたエンティティを含むことができる。一例として、管理者が、完全修飾ドメイン名、ＩＰアドレス、ＤＮＲ－ＳＲＶクエリ、並びにサーバまたはドメインを示す他の一般に使用される手段を使用して、エンティティを指定することができる。リスト中の情報は、式（expression）を使用して示される。一例として、管理者は、「ＭＩＣＲＯＳＯＦＴ（登録商標）．ＣＯＭ」で終わるすべてのドメインが許可されることを示すことができる。リストコンポーネントが、パターン探索機構を使用して、リストの中でエンティティを探索することができる。このようなパターンは、ワイルドカードを含むことができる。一例として、「＊．ＭＩＣＲＯＳＯＦＴ（登録商標）．ＣＯＭ」を、「ＭＩＣＲＯＳＯＦＴ（登録商標）．ＣＯＭ」で終わるドメインへの、またはそのようなドメインからのすべてのメッセージが許可される指示（indication）とすることができる。

【００２７】

許可されたエンティティと許可されていないエンティティの組み合わせを使用して、ドメイン内の特定のエンティティが、メッセージを送信する、または受信することができるようにすることができる。一例として、「＊．ｘ．ｃｏｍ」は、「ｘ．ｃｏｍ」で終わるすべてのドメインが許可されていないが、「ｃｅｏ．ｘ．ｃｏｍ」は許されることができることを示すことができる。このようなケースでは、ドメイン「ｘ．ｃｏｍ」を有するいずれのエンティティへの、またはそのようないずれのエンティティからのメッセージも、「ｃｅｏ．ｘ．ｃｏｍ」への、または「ｃｅｏ．ｘ．ｃｏｍ」からのメッセージを除き、すべて無視される。

【００２８】

システムは、以上のコンポーネントを使用して、送信メッセージを様々な形でルーティングするかどうか、またはどのようにルーティングするかを判定することができる。システムは、メッセージを受信するエンティティが許可されたドメイン内にあるかどうかをまず判定することができる。エンティティが許可されていないドメイン内にある場合、システムは、そのエンティティが許可されたエンティティのリストに現れるかどうかを判定することができる。一例として、「Ｘ．ＣＯＭ」ドメインは、許可されていないが、「ＣＥＯ．Ｘ．ＣＯＭ」エンティティは、許可されていることができる。ドメインが許可されていないわけではなく（明示的に許可されていない）場合、システムは、ＤＮＳと接触して、そのメッセージをどのようにルーティングするかを判定することができる。受信者に関するＤＮＳエントリが存在しない場合、システムは、そのメッセージをルーティングするようにクリアリングハウスと接触することができる。これとは別に、システムは、メッセージをどのようにルーティングするか（例えば、「既定の」経路）を独立に知っていることが可能な信頼されるパーティにメッセージを送信することができる。

【００２９】

エッジプロキシサーバは、メッセージをルーティングするための企業のビジネスモデルに関連する許可論理を実施することもできる。一例として、エッジプロキシサーバは、一部のユーザおよびデバイスがＳＩＰメッセージを交換できるようにするが、他のユーザおよびデバイスがそうできるようにはしないように構成することができる。この許可論理は、あらゆるフェデレーションモードを使用して、メッセージを許可し、ルーティングすることができる。別の例として、エッジプロキシサーバは、ダイレクトフェデレーションルーティングをまず試みることができる。それが失敗した場合、エッジプロキシサーバは、

次にオートフェデレーションルーティングを試みることができる。これらのフェデレーションルーティング機構のいずれも、メッセージが転送されることを可能にしなかった場合、エッジプロキシサーバは、クリアリングハウスが「既定の」経路として示されるクリアリングハウスフェデレーションモデルを使用することができる。

【００３０】

図４は、別の連合させられたネットワーク上のデバイス(複数)と交換されるメッセージを扱うためにエッジプロキシサーバによって実行されるルーチンの実施形態を示す流れ図である。一例として、ルーチンは、異なるネットワークにそれぞれが結合された２つのデバイス間でセッションに関連するメッセージの許可、認証、および転送を行うことができる。ルーチンはブロック５０２で始まり、メッセージをパラメータとして受け取る。ブロック５０４で、メッセージが内部サーバから受信されたかどうかを判定する。メッセージが内部サーバから受信されている場合はブロック５０６に進み、そうでない場合はブロック５１４に進む。ブロック５０６で、メッセージが要求であるか、応答であるかを判定する。メッセージが要求である場合はブロック５０８に進み、要求ではない場合はブロック５１２に進む。ブロック５０８で、ルーチンは、送信者または受信者が許可されているかどうかを判定する。許可されている場合、ルーチンは、メッセージからのＲｏｕｔｅヘッダフィールド(複数)を検証し、Ｒｅｃｏｒｄ－ＲｏｕｔｅヘッダフィールドおよびＶｉａヘッダフィールドに署名し、要求を転送する。Ｒｅｃｏｒｄ－ＲｏｕｔｅヘッダフィールドおよびＶｉａヘッダフィールドには、ルーティングのためにＲｏｕｔｅヘッダおよびＶｉａヘッダを使用するデバイス(複数)が、デバイス(複数)が受信する将来のメッセージの中のメッセージヘッダ(複数)を信頼することができるように署名が行われる。

【００３１】

ブロック５１２で、応答の中で示された送信者または受信者が許可されているかどうかを判定する。許可されている場合、応答の署名済みのＶｉａヘッダフィールド(複数)に基づいて応答をルーティングする。

【００３２】

ブロック５１４で、メッセージが要求であるか、応答であるかを判定する。メッセージが要求であった場合はブロック５１６に進み、要求ではなかった場合はブロック５１８に進む。ブロック５１６で、要求が転送されるべきサーバを認証する。サーバが認証された場合、ＦｒｏｍヘッダフィールドおよびＵＲＩヘッダフィールドを検証する。これらのヘッダフィールド(複数)が有効であった場合、メッセージを次のホップに転送する。

【００３３】

ブロック５１８で、メッセージのＶｉａヘッダフィールド(複数)を検証する。これらのフィールドが有効であった場合、応答をサーバに転送する。

【００３４】

ルーチンは、ブロック５１０でルーチンの呼び出し元に戻る。

【００３５】

本明細書で説明した特定の実施例はＳＩＰを使用することに関し述べているが、代替の実施形態では、他の均等なプロトコルまたは類似のプロトコルを使用することもできる。

【００３６】

データ通信網のセキュアな連合のためのシステムが実施されるコンピューティングデバイスは、中央処理装置、メモリ、入力デバイス(複数)（例えば、キーボードおよびポインティングデバイス）、出力デバイス(複数)（例えば、ディスプレイデバイス(複数)）、および記憶装置(複数)（例えば、ディスクドライブ(複数)）を含むことができる。メモリおよび記憶装置(複数)は、本システムを実施する命令を含むことが可能なコンピュータ可読媒体である。さらに、データ構造およびメッセージ構造は、通信リンク上の信号などのデータ伝送媒体を介して格納または伝送することができる。インターネット、ローカルエリアネットワーク、ワイドエリアネットワーク、またはポイントツーポイントダイヤルアップ接続などの様々な通信リンクを使用することができる。

【００３７】

図１は、データ通信網のセキュアな連合のためのシステムを実施することができる適切な動作環境の実施例を示す。この動作環境は、適切な動作環境の一例に過ぎず、本システムの用法または機能の範囲について何ら限定するものではない。使用に適する可能性がある他の周知のコンピューティングシステム、コンピューティング環境、およびコンピューティング構成には、パーソナルコンピュータ、サーバコンピュータ、「スマート」携帯電話を含むハンドヘルドデバイスまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、プログラム可能な家庭用電化製品、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、以上のシステムまたはデバイスのいずれかを含む分散コンピューティング環境などが含まれる。

【００３８】

データ通信網のセキュアな連合のためのシステムは、１つまたは複数のコンピュータまたは他のデバイスによって実行される、プログラムモジュール(複数)などの、コンピュータ実行可能命令の一般的な文脈で説明することができる。一般に、プログラムモジュール(複数)には、特定のタスクを実行する、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などが含まれる。通常、プログラムモジュール(複数)の機能は、様々な実施形態において所望に応じて組み合わせること、または分散させることができる。

【００３９】

以上から、本発明の特定の実施形態を例示の目的で本明細書で説明してきたが、本発明の趣旨および範囲を逸脱することなく、様々な変更形態を実施できることが認められよう。したがって、本発明は、添付の特許請求の範囲による他、限定されるものでない。

【図面の簡単な説明】

【００４０】

【図１】データ通信網のセキュアな連合のためのシステムの一実施形態を示すブロック図である。

【図２】図１のネットワークの実施形態を示すブロック図である。

【図３】図２のエッジプロキシサーバの実施形態を示すブロック図である。

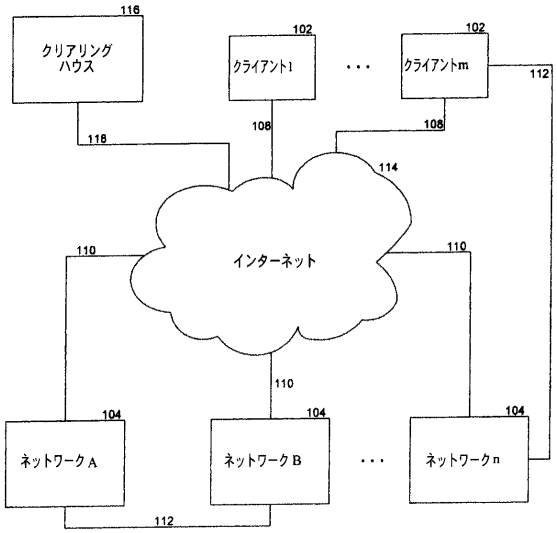
【図４】別の連合させられたネットワーク上のデバイス(複数)と交換されるメッセージを扱うためにエッジプロキシサーバによって実行されるルーチンの実施形態を示す流れ図である。

【符号の説明】

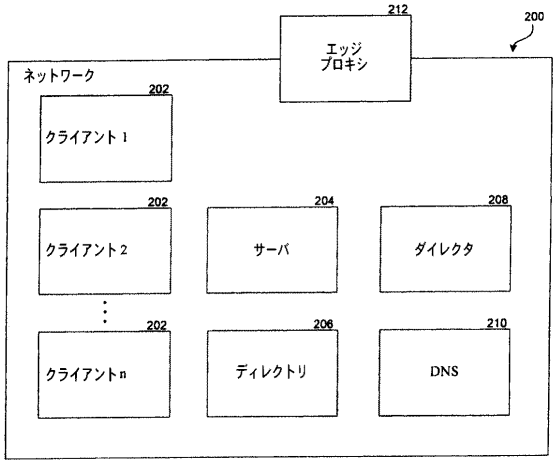
【００４１】

１０２，２０２　クライアント
１０４，２００　ネットワーク
１１４　インターネット
１１６　クリアリングハウス
２０４　サーバ
２０６　ディレクトリ
２０８　ダイレクタ
２１０　ＤＮＳ
２１２，３００　エッジプロキシ
３０２　トランスポートコンポーネント
３０４　ＤＮＳ－ＳＲＶコンポーネント
３０６　ルーティングコンポーネント
３０８　リストコンポーネント

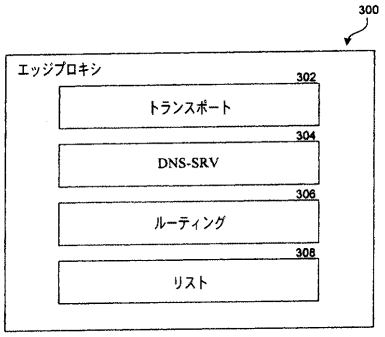
【図１】


116
クリアリング
ハウス
102
クライアント1
102
クライアントm
112
118
108
108
114
インターネット
110
110
110
104
104
104
ネットワークA
ネットワークB
ネットワークn
112

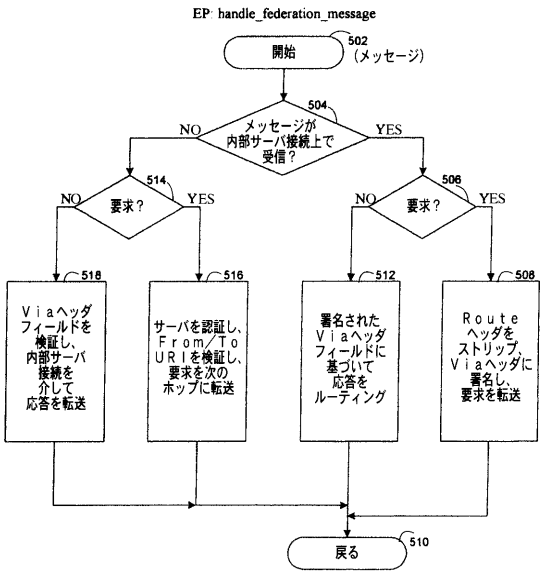
【図２】


212
エッジ
プロキシ
200
ネットワーク
202
クライアント1
202
クライアント2
204
サーバ
208
ダイレクタ
202
クライアントn
206
ディレクトリ
210
DNS

【図３】


300
エッジプロキシ
302
トランスポート
304
DNS-SRV
306
ルーティング
308
リスト

【図４】


EP: handle_federation_message
開始
502
(メッセージ)
504
メッセージが
内部サーバ接続上で
受信?
NO
YES
514
要求?
NO
YES
506
要求?
NO
YES
518
Viaヘッダ
フィールドを
検証し、
内部サーバ
接続を
介して
応答を転送
516
サーバを認証し、
From/To
URIを検証し、
要求を次の
ホップに転送
512
署名された
Viaヘッダ
フィールドに
基づいて
応答を
ルーティング
508
Route
ヘッダを
ストリップ、
Viaヘッダに
署名し、
要求を転送
戻る
510

フロントページの続き

(72)発明者　グル　キムチ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　スリカンス　ショロフ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

審査官　倉山　徹男

(56)参考文献　特開２００３－１３２０２０（ＪＰ，Ａ）
特開２００２－１５２２７９（ＪＰ，Ａ）
特開２００３－３２４５２４（ＪＰ，Ａ）
特開平１０－２４７９４６（ＪＰ，Ａ）
石川　大法，ＲＳＩＰサーバにおけるポート番号によるパケットフィルタリングの提案とその性能検証，情報処理学会論文誌，社団法人情報処理学会，２００４年　2月１５日，第45巻　第2号，pp.586～596

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／６６
Ｇ０９Ｃ　１／００
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　１２／５６
Ｈ０４Ｍ　３／００