(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-100301
(P2012-100301A)
(43)公開日　平成24年5月24日(2012.5.24)

(51)Int.Cl.		F I		テーマコード（参考）
H04M 3/00	(2006.01)	H04M 3/00	B	5K201
H04M 11/00	(2006.01)	H04M 11/00	302	

審査請求 有　請求項の数 15　ＯＬ　（全 15 頁）

(21)出願番号　特願2011-274188 (P2011-274188)
(22)出願日　平成23年12月15日 (2011.12.15)
(62)分割の表示　特願2006-295700 (P2006-295700)の分割
原出願日　平成18年10月31日 (2006.10.31)
(31)優先権主張番号　11/514580
(32)優先日　平成18年9月1日 (2006.9.1)
(33)優先権主張国　米国 (US)

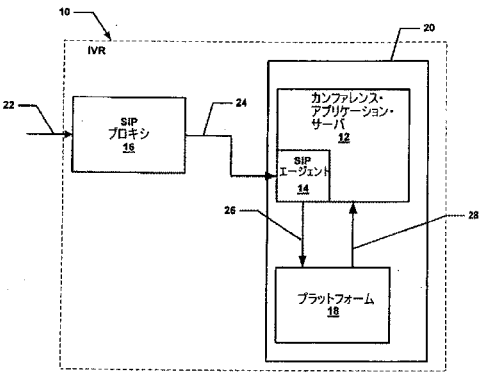
（特許庁注：以下のものは登録商標）
１．フロッピー

(71)出願人　506079711
アバイア　テクノロジー　エルエルシー
アメリカ合衆国　０７９２０－２３３２
ニュージャーシィ，バスキング　リッジ，
マウント　エアリー　ロード　２１１
(74)代理人　100094112
弁理士　岡部　讓
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100128657
弁理士　三山　勝巳
(72)発明者　ロバート　エリック　ブラウデス
アメリカ合衆国　０１８２６　マサシューセッツ，ドラクト，ミドウ　クリーク　ドライヴ　１０９

最終頁に続く

(54)【発明の名称】拡張プロトコル・ヘッダを含む通信の提供

(57)【要約】
【課題】拡張プロトコル・ヘッダを含む通信を提供するための方法、装置およびコンピュータ・プログラム製品を提供すること。
【解決手段】ヘッダを有するメッセージは通信プロトコルの中で提供される。このヘッダは、さらなる情報を含む拡張子を有する。さらなる情報を含む拡張子がヘッダの中に含まれる。メッセージは受信者に送信され、受信者はヘッダの拡張子に含まれるさらなる情報を、さらなる機能を提供するために利用することができる。
【選択図】図１



【特許請求の範囲】
【請求項１】
拡張プロトコル・ヘッダを含む通信を提供する方法であって、
メッセージを通信プロトコルの中で提供するステップであって、前記メッセージがヘッダを有するステップ、
拡張子を前記ヘッダの中に含ませるステップであって、前記拡張子がさらなる情報を含み、前記ヘッダ内の拡張子が該ヘッダへの追加フィールドの付加部からなり、前記さらなる情報が認証情報を含み、受信者が最初のユーザ認証を実行し、次いで前記メッセージに埋め込まれた前記認証情報とともに最初のリクエスタを第２の情報サービスに送り、該第２のサービスは、開始側のユーザからの信用証明を再要求することを必要とせずに、前記メッセージの前記認証情報によって前記ユーザを認証する、ステップ、及び
前記メッセージを前記受信者に送信するステップであって、前記受信者が前記ヘッダの前記拡張子に含まれる前記さらなる情報を、さらなる機能を提供するために利用することができるステップ
を備える方法。
【請求項２】
前記さらなる情報は変更された受信者アドレスを含み、前記受信者は前記メッセージを受信して変更された受信者アドレスに前記メッセージを送る請求項１に記載の方法。
【請求項３】
前記さらなる情報はサービス識別子を含み、前記受信者は前記メッセージを受信して前記サービス識別子によって識別される特定のサービスを選択する請求項１に記載の方法。
【請求項４】
前記認証情報はセキュリティ符号を含む請求項１に記載の方法。
【請求項５】
前記プロトコルはセッション開始プロトコル（ＳＩＰ）を含み、拡張子を含む前記ヘッダは拡張ＳＩＰヘッダを含む請求項１に記載の方法。
【請求項６】
請求項１記載の方法において、外部ネットワークに公表されることなく隠された受信者にプロトコルメッセージがルーティングされるようにすることによって、前記さらなる情報がさらなるセキュリティを与える、方法。
【請求項７】
拡張プロトコル・ヘッダを含む通信を提供するための、コンピュータ可読符号を有するコンピュータ可読記憶媒体であって、
メッセージを通信プロトコルの中で提供する命令であって、前記メッセージがヘッダを有する、命令、
拡張子を前記ヘッダの中に含ませる命令であって、前記拡張子がさらなる情報を含み、前記ヘッダ内の拡張子が該ヘッダへの追加フィールドの付加部からなり、前記さらなる情報が認証情報を含み、受信者が最初のユーザ認証を実行し、次いで前記メッセージに埋め込まれた前記認証情報とともに最初のリクエスタを第２の情報サービスに送り、該第２のサービスは、開始側のユーザからの信用証明を再要求することを必要とせずに、前記メッセージの前記認証情報によって前記ユーザを認証するように構成された命令、及び
前記メッセージを前記受信者に送信する命令であって、前記受信者が前記ヘッダの前記拡張子に含まれる前記さらなる情報を、さらなる機能を提供するために利用することができる、命令
を備えるコンピュータ可読記憶媒体。
【請求項８】
拡張子を前記ヘッダの中に含ませる前記命令であって、前記拡張子がさらなる情報を含む前記命令は、前記さらなる情報が変更された受信者アドレスを含み、前記受信者が前記メッセージを受信して前記変更された受信者アドレスに前記メッセージを送るための命令を含む請求項７に記載のコンピュータ可読記憶媒体。

【請求項９】
拡張子を前記ヘッダの中に含ませる前記命令であって、前記拡張子がさらなる情報を含む前記命令は、前記さらなる情報がサービス識別子を含み、前記受信者が前記メッセージを受信して前記サービス識別子によって識別される特定のサービスを選択するための命令を含む請求項７に記載のコンピュータ可読記憶媒体。
【請求項１０】
拡張子を前記ヘッダの中に含ませる前記命令であって、前記拡張子が認証情報を含む前記命令は、セキュリティ符号を含む請求項７に記載のコンピュータ可読記憶媒体。
【請求項１１】
前記プロトコルはセッション開始プロトコル（ＳＩＰ）を含み、拡張子を含む前記ヘッダは拡張ＳＩＰヘッダを含む請求項７に記載のコンピュータ可読記憶媒体。
【請求項１２】
請求項７記載のコンピュータ可読記憶媒体において、外部ネットワークに公表されることなく隠された受信者にプロトコルメッセージがルーティングされるようにすることによって、前記さらなる情報がさらなるセキュリティを与えるものである、コンピュータ可読記憶媒体。
【請求項１３】
メモリ、
プロセッサ、
通信インタフェース、及び
メモリとプロセッサと通信インタフェースとを接続する相互接続機構
を備え、
前記メモリは、プロセッサ上で実行されたときに、
メッセージを通信プロトコルの中で受信するステップであって、前記メッセージがヘッダを有し、ヘッダが前記ヘッダの中に拡張子を含み、前記ヘッダ内の拡張子が該ヘッダへの追加フィールドの付加部からなり、前記拡張子がさらなる情報を含み、前記ヘッダ内の拡張子が該ヘッダへの追加フィールドの付加部からなり、前記さらなる情報が認証情報を含み、受信者が最初のユーザ認証を実行し、次いで前記メッセージに埋め込まれた前記認証情報とともに最初のリクエスタを第２の情報サービスに送り、該第２のサービスは、開始側のユーザからの信用証明を再要求することを必要とせずに、前記メッセージの前記認証情報によって前記ユーザを認証する、ステップ、及び
前記メッセージを前記受信者に送信するステップであって、前記受信者が前記ヘッダの前記拡張子に含まれる前記さらなる情報を、さらなる機能を提供するために利用することができるステップ
の操作をコンピュータ・システムが実行できるようにする、プロセシング情報のためのプロセスを提供するアプリケーションによって符号化されるコンピュータ・システム。
【請求項１４】
前記さらなる情報は変更された受信者アドレスを含み、前記受信者は前記メッセージを受信して変更された受信者アドレスに前記メッセージを送る請求項１３に記載のコンピュータ・システム。
【請求項１５】
前記さらなる情報はサービス識別子を含み、前記受信者は前記メッセージを受信して前記サービス識別子によって識別される特定のサービスを選択する請求項１３に記載のコンピュータ・システム。
【請求項１６】
前記認証情報はセキュリティ符号を含む請求項１３に記載のコンピュータ・システム。
【請求項１７】
前記プロトコルはセッション開始プロトコル（ＳＩＰ）を含み、拡張子を含む前記ヘッダは拡張ＳＩＰヘッダを含む請求項１３に記載のコンピュータ・システム。
【請求項１８】

請求項１３記載のコンピュータ・システムにおいて、外部ネットワークに公表されることなく隠された受信者にプロトコルメッセージがルーティングされるようにすることによって、前記さらなる情報がさらなるセキュリティを与えるものである、コンピュータ・システム。

【発明の詳細な説明】

【技術分野】

【０００１】

拡張プロトコル・ヘッダを含む通信を提供する。

【背景技術】

【０００２】

参加者の組織間でのデータの交換とみなされるセッションの生成および管理を必要とするインターネットのアプリケーションは数多く存在する。これらのアプリケーションの実施は、参加者が実行することで複雑になる。すなわち、ユーザはエンドポイント間を移動する場合もあるし、複数の名前によってアドレス可能である場合もあるし、複数の異なるメディアと、時には同時に通信する場合もある。音声、ビデオまたはテキスト・メッセージなどの様々な形態のリアルタイム・マルチメディアのセッション・データを運搬するプロトコルが複数作り出されてきた。セッション開始プロトコル（ＳＩＰ）は、インターネットのエンドポイント（ユーザ・エージェントと呼ばれる）がお互いを見つけ出し、共有しようとするセッションの特徴付けに同意できるようにすることによって、これらのプロトコルと一緒に機能する。予想されるセッションの参加者の位置を見つけ出すため、およびその他の機能のため、ＳＩＰはユーザ・エージェントが登録、セッションへの招待およびその他の要求を送信することができるネットワーク・ホスト（プロキシ・サーバと呼ばれる）の基盤作成を可能にする。セッションの生成に使用されるＳＩＰ招待は、参加者が互換性のあるメディア型のセットに同意できるようにするセッション記述を運搬する。ＳＩＰはユーザの現在位置への要求の発送、サービスのためのユーザの認証および許可、プロバイダのコール・ルーティング・ポリシーの実施、およびユーザへの機能の提供を促進するために、プロキシ・サーバと呼ばれる要素を使用する。ＳＩＰはまた、プロキシ・サーバによる使用のために、ユーザが自らの現在位置をアップロードできるようにする登録機能も提供する。ＳＩＰは複数の異なる輸送プロトコルの先頭で動作する。ＳＩＰはインターネット電話方式の呼び出しなどのマルチメディア・セッション（カンファレンス）を確立、変更および終端することができる、アプリケーション層の制御プロトコルである。ＳＩＰはまた、マルチキャスト・カンファレンスのような既存のセッションへ参加者を招待することもできる。

【０００３】

従来のシステムでは複数のＳＩＰの受信者アドレスが利用されており、これらのアドレスが変わるか、または異なるアプリケーション・サーバへマップされる必要がある場合、ＳＩＰプロキシは再設定される。パスコード・システムのために、予め設定された受信者アドレスがサービスを識別するのに使用され、サービスに対して１対１の基準で、さらなるアドレスの供給が必要となる。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

上で述べたような従来の機構には様々な欠点がある。そのような欠点の１つは、現在の解決策が標準的なプロトコル（例えばＳＩＰ）のヘッダで公表されるために、最終的な受信者アドレス必要とすることである。現在の解決策はまた、これらのアドレスが変わる場合に、プロキシ設定の再設定も必要とする。さらに、現在の機構はプロトコル・ヘッダ中のアドレスと受信システム上の最終的な受信者との間で１対１のマッピングを必要とする。認証のために、開始側のユーザは通常２回目に自らの信用証明を入力することを要求される。

【０００５】

拡張プロトコル・ヘッダを含む通信を提供する本発明の方法および装置は、従来のシステムに関連する複数の問題を解決する。拡張プロトコル・ヘッダを含む通信を提供する本発明の方法および装置は、プロトコルのメッセージが標準的な方法で外部ネットワークに公表されることなく、隠された受信者に発送されるようにすることによって、さらなるセキュリティを可能にする。さらに、拡張プロトコル・ヘッダを含む通信を提供する本発明の方法および装置により、ルーティング情報がネットワーク中のプロキシ・サーバの変更を必要とせずに、ネットワークで変えられることが可能になる。さらにまた、拡張プロトコル・ヘッダを含む通信を提供する本発明の方法および装置により、メッセージの送信者は複数の受信者に対して単一のプロトコルのアドレスを利用することができる。その上さらに、拡張プロトコル・ヘッダを含む通信を提供する本発明の方法および装置により、送信者は所望のサービスのための識別子およびパスワード／パスコードを埋め込むことが可能であり、受信者はこの情報に対する入力促進を必要とすることなく、送信者を認証することができる。

【０００６】

本発明の実施形態はこのような欠点を大いに克服し、拡張プロトコル・ヘッダを含む通信を提供する機構および技術を提供する。このことは、サービスの認証情報を伝えるために同一の機構を使用し、単一の受信者アドレスを複数の情報サービスにマップするために、ルーティング基盤に何らかの変更がある場合、ネットワークのルーティング設定を最小限に変更する能力を提供する。このことは、プロトコル・ヘッダ中の信用証明を符号化するために拡張プロトコル・ヘッダの情報を使用し、さらなるセキュリティのために「隠された」アドレスを使用し、通常はルーティング情報に基づくサービス選択がルーティング基盤を迂回できるようにし、単一のプロトコル・アドレスが第２レベルのアドレッシング機構を使用することにより多重送信されるようにすることによって達成される。

【課題を解決するための手段】

【０００７】

拡張プロトコル・ヘッダを含む通信方法の特定の実施形態で、方法はヘッダを有するメッセージを通信プロトコルの中で提供するステップを含む。さらに本方法は、さらなる情報を含む拡張子をヘッダの中に含ませるステップを含む。その上さらに、本方法は受信者にメッセージを送信するステップであって、受信者がヘッダの拡張子に含まれるさらなる情報を、さらなる機能を提供するために利用することができるステップを含む。

【０００８】

その他の実施形態は、拡張プロトコル・ヘッダを含む通信を提供するために、コンピュータ可読符号を有するコンピュータ可読媒体を含む。媒体は、通信プロトコルの中でヘッダを有するメッセージを提供するステップのための命令を含む。コンピュータ可読媒体はさらなる情報を含む拡張子をヘッダの中に含ませるステップのための命令と、受信者にメッセージを送信するステップであって、受信者がヘッダの拡張子に含まれるさらなる情報を、さらなる機能を提供するために利用することができるステップのための命令とをさらに含む。

【０００９】

さらに別の実施形態は、本発明の実施形態として本明細書で開示される本方法の動作のすべてを処理するために構成された、コンピュータ化デバイスを含む。このような実施形態で、コンピュータ化デバイスはメモリ・システム、プロセッサ、通信インタフェースを、これらの構成要素を接続する相互接続機構の中で含む。メモリ・システムはプロセッサ上で実行される（ｐｅｒｆｏｒｍｅｄ）場合（例えば執行（ｅｘｅｃｕｔｉｎｇ）の場合）、本明細書で説明される拡張プロトコル・ヘッダを含む通信を提供し、本発明の実施形態として本明細書で説明される、本方法の実施形態および動作のすべてを実行するために、本明細書で説明されるようにコンピュータ処理デバイス内で動作するプロセスによって符号化される。したがって、本明細書で説明される処理を実行するか、または実行するようにプログラムされた、いかなるコンピュータ処理デバイスも本発明の実施形態である。

【００１０】

本明細書で開示される本発明の実施形態のその他の配置は、上で要約され、以下で詳細が開示される本方法の実施形態のステップおよび動作を実行するためのソフトウェア・プログラムを含む。より詳細には、コンピュータ・プログラム製品は、コンピュータ処理デバイスで実行された場合、本明細書で説明されるような拡張プロトコル・ヘッダを含む通信を提供する関連の動作を提供する、論理符号化されたコンピュータ・プログラムを含むコンピュータ可読媒体を有する１つの実施形態である。コンピュータ・プログラム論理は、コンピューティング・システムによって少なくとも１つのプロセッサ上で実行される場合、本発明の実施形態として本明細書で明らかにされる動作（例えば方法）をプロセッサに実行させる。本発明のこのような配置は、典型的にはソフトウェア、符号、および／または光媒体（例えばＣＤ－ＲＯＭ）、フロッピーもしくはハード・ディスク、または１つまたは複数のＲＯＭもしくはＲＡＭもしくはＰＲＯＭチップのファームウェアまたはマイクロコード、または特定用途向け集積回路（ＡＳＩＣ）、または１つまたは複数のモジュール、共用ライブラリ等でダウンロード可能なソフトウェア・イメージのようなその他の媒体などの、コンピュータ可読媒体上で配置または符号化されるその他のデータ構造として提供される。ソフトウェアまたはファームウェアまたはその他のこのような構成は、１つまたは複数のプロセッサに本発明の実施形態として本明細書で説明される技術をコンピュータ処理デバイスで実行させるために、コンピュータ処理デバイスにインストールされることが可能である。データ通信デバイスまたはその他エンティティのグループの中など、コンピュータ処理デバイスの集合の中で動作するソフトウェア・プロセスもまた、本発明のシステムを提供することができる。本発明のシステムは、複数のデータ通信デバイス上の多くのソフトウェア・プロセスの間で分散させることができるか、またはすべてのプロセスは専用コンピュータの小規模なセットか、もしくは単独のコンピュータ上で動作することができる。

【００１１】

本発明の実施形態は、データ通信デバイスの中などで、ソフトウェア・プログラムとして、ソフトウェアおよびハードウェアとして、またはハードウェアおよび／または回路単独として厳密に実現されることが可能なことを理解されたい。本明細書で説明されるような本発明の機能は、データ通信デバイスおよび／またはＮｅｗ　Ｊｅｒｓｅｙ、ＬｉｎｃｒｏｆｔのＡｖａｙａ社製品などの、そうしたデバイスのためのソフトウェア・システムで用いられてもよい。

【００１２】

異なる図を通して同じ参照符号が同じ部分を指す添付の図面に示されるように、前述のものは以下の本発明の好ましい実施形態のより詳細な説明から明らかとなろう。図面は必ずしも一定の縮尺であるというわけではなく、それよりも本発明の原理を例示するものとして添えることを強調する。

【図面の簡単な説明】

【００１３】

【図１】本発明の実施形態による拡張プロトコル・ヘッダを含む通信を利用するシステム環境の構成図である。

【図２Ａ】本発明の実施形態による拡張プロトコル・ヘッダを含む通信を提供する特定の方法の流れ図である。

【図２Ｂ】本発明の実施形態による拡張プロトコル・ヘッダを含む通信を提供する特定の方法の流れ図である。

【図３】本発明の実施形態による拡張プロトコル・ヘッダを含む通信を提供するステップを実行するコンピュータ・システムのためのコンピュータ・システム構造例を示す図である。

【発明を実施するための形態】

【００１４】

ここに開示される、拡張プロトコル・ヘッダを含む通信を提供するため方法および装置は、特定の実施形態で、メッセージの受信者にさらなる情報を与えるために拡張ヘッダ（

例えばＲＦＣ３２６１に支援されるＳＩＰヘッダ拡張子）を含有することを含む。さらなる情報は変更された受信者アドレス、サービス識別子、認証情報および個人識別番号（ＰＩＮ）のうちの１つまたは複数を含むことができるが、これらに限定されるわけではない。

【００１５】

拡張ヘッダで提供される情報が変更された受信者アドレスを含む場合、この情報によって受信者は変更されたアドレスに呼び出しを送ることが可能となり、基礎となっているＳＩＰネットワークの再設定を必要とすることなく、新たなアドレスを受信システムに迅速に追加することができる。メッセージを元々の、公表されているアドレスに送信すると、次いで受信者は所望の受信者への内部ルーティングのために、拡張ヘッダの中に含まれる変更された受信者アドレスを利用する。

【００１６】

拡張ヘッダで提供される情報がサービス識別子を含む場合、サービス識別子は所望の受信者による特定のサービスの選択のために使用される。

拡張ヘッダで提供される情報が認証情報を含む場合、送信者がエンド・ユーザを認証するのに必要とされる利用可能な情報を持っている場合に、認証情報はサイレント認証（ｓｉｌｅｎｔ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を可能にする。これによりメッセージは、最初のユーザ認証を実行し、次いでメッセージに埋め込まれた認証情報とともに第２の情報サービスに最初のリクエスタ（ｒｅｑｕｅｓｔｏｒ）を送るために、ポータル・エントリ・サービスなどの最初のサービスによって受信される。これによって２番目のサービスは、開始側のユーザからの信用証明を再要求することを必要とせずに認証を行う。これはパスワードまたはパスコードを含み、選択的にＰＩＮを含む。

【００１７】

図１を参照すると、特定の実施例で、フロント・エンドの対話型音声応答（ＩＶＲ）システム１０が示されている。ＩＶＲシステム１０はユーザを認証し、次いで一連の情報サービスのうちの１つに呼び出しを伝えるために使用される。これらのサービスのうちの１つはカンファレンシング・システム（ＣＳ）２０である。カンファレンシング・システム２０はカンファレンス・アプリケーション・サーバ１２、ＳＩＰエージェント１４およびプラットフォーム１８を含む。認証のために最初にＩＶＲ（ＳＩＰプロキシ１６）を通過していない、システム上のカンファレンスの部分集合に入ることを許されるべきではないＣＳ２０では、セキュリティが必要とされる。さらに、この実施例では（オーディオ、ビデオ、データ等の）共同カンファレンスである特定の情報サービスの識別は、さらなるセキュリティのためにエンド・ユーザには隠されていてもよいが、ＩＶＲ１０およびＣＳ２０には知られる。

【００１８】

ＩＶＲ１０はユーザを認証する場合、ユーザから直接入手するか、または情報の記憶場所にアクセスすることによって、共同カンファレンスへのエントリを得るために必要とされる信用証明を入手する。次いで、これらの信用証明は以下のメッセージ２４のような拡張ＳＩＰヘッダを使用してＣＳ２０に伝えられる。

ｓｉｐ：＜ＤＮＩＳ＞；@ｂｒｉｄｇｅＤｏｍａｉｎ．ｃｏｍ；ｃｏｎｆ＝＜ＩｎｔｅｎａｌＤＮＩＳ，ｃｏｎｆＣｏｄｅ＞

【００１９】

ここで＜ＩｎｔｅｒｎａｌＤＮＩＳ＞は拡張プロトコル・ヘッダであり、かつ通常は安全なカンファレンスのためだけに使用されるコール・ブランディング表（Ｃａｌｌ　Ｂｒａｎｄｉｎｇ　ｔａｂｌｅ）のカンファレンス・ブリッジで設定される新たなＤＮＩＳである。これが変更された受信者アドレスである。「ｃｏｎｆ＝」は所望の情報サービスを識別するために使用される。何らかのさらなる信用証明が必要とされる場合、角括弧の間にこれらが加えられる。例えばＰＩＮが必要とされる場合、ＳＩＰの列の形式は、

ｓｉｐ：＜ＤＮＩＳ＞，ｃｏｎｆ＝＜ＩｎｔｅｒｎａｌＤＮＩＳ，ｃｏｎｆＣｏｄｅ，ＰＩＮ＞

となる。

【００２０】

ＳＩＰメッセージ２６を受信すると、ＣＳ２０は共同カンファレンスの存在を検証するためにＩｎｔｅｎａｌＤＮＩＳを使用し、次いで信用証明（この実施例では「ｃｏｎｆＣｏｄｅ」）を検査する。信用証明が検証を合格する場合、次いでユーザはカンファレンスに配置される。プラットフォーム１８からカンファレンス・アプリケーション・サーバ１２へのメッセージ２８は、カンファレンス・アプリケーション・サーバ１２には、あたかもｉｎｔｅｒｎａｌ　ＤＮＩＳがダイヤルされたかのようにみえる。さらなるセキュリティのために、ＳＩＰメッセージは例えば伝送レベル・セキュリティ（ＴＬＳ）を使用して、暗号化された回線を介して運ばれることもできる。この場合、「ｓｉｐ：」は「ｓｉｐｓ：」で置き換えられる。

【００２１】

類似の実施例で、ヘッダが同じＤＮＩＳを含むＳＩＰ　Ｔｏは、外部の発信者によって使用される。コール・ブランディング表は、パスコードの入力を促されることを避けるために固有の＜ＨｉｄｄｅｎＤＮＩＳ＞を利用することができるが、ＳＩＰプロキシは新たなエントリを必要としない。

【００２２】

詳細は以下の通りである。

ＳＩＰ　Ｔｏ：ヘッダは以下の形式で宛先（Ｔｏ）アドレスを含む。

ｓｉｐ：＜ＤＮＩＳ＞；ｃｏｎｆ＝＜ＨｉｄｄｅｎＤＮＩＳ，ｃｏｎｆＣｏｄｅ＞

ここで＜ＨｉｄｄｅｎＤＮＩＳ＞はコール・ブランディング表のオン・ザ・カンファレンス・ブリッジで（ｉｎ　ｔｈｅ　ｏｎ　ｔｈｅ　Ｃｏｎｆｅｒｅｎｃｅ　Ｂｒｉｄｇｅ）構成された新たなＤＮＩＳである。ＳＩＰヘッダは解析され、「＜ＨｉｄｄｅｎＤＮＩＳ＞、＜ｃｏｎｆＣｏｄｅ＞」はカンファレンシング・アプリケーションに渡される。表は、発信者がパスコードの入力を促されることのないダイレクト・コールとしてエントリを指定する、「＜ＨｉｄｄｅｎＤＮＩＳ＞」に合致するエントリで構成される。カンファレンシング・アプリケーションは、合致するエントリで指定された入力促進を行う。カンファレンシング・アプリケーションはパスコードの入力促進を回避し、発信者はダイレクト・コールのために今日使用されているのと同様の方法で、パスコードの入力を促されることなく、カンファレンスに配置される。＜ｃｏｎｆＣｏｄｅ＞の領域が有効な議長パスコードを含んでいる場合、発信者は議長として適切なカンファレンスに配置される。＜ｃｏｎｆＣｏｄｅ＞の領域が有効な参加者パスコードを含んでいる場合、発信者は参加者として適切なカンファレンスに配置される。＜ｃｏｎｆＣｏｄｅ＞が供給されたパスコードに合致しない場合、呼び出しは中断される。

【００２３】

拡張プロトコル・ヘッダを含む通信を提供する本方法および装置に関する利点は複数ある。ワークフローの観点から、拡張プロトコル・ヘッダを含む通信を提供する本方法および装置により、ネットワーク管理者は第２のレベルでルーティング情報を変えることが可能であり、新たなエントリの作成が必要な場合に、最初のネットワークのルーティング基盤を変更する必要がなくなる。このことは操作コストを削減する。この機能は、信用証明を合格させるための新たな方法を可能にすることによって、強化されたセキュリティを提供する。さらに、拡張プロトコル・ヘッダを含む通信を提供する本方法および装置は、１回のみのログオンのための新たな機構を提供する。

【００２４】

類似の統合システムの別の実施形態で、通常ユーザは１回のみのログオンの機構を使用することではなく、自らの信用証明を複数回入力することが要求される。また、ＳＩＰプロキシのルーティング表は、新たなアドレスがネットワークに加えられる度に更新される必要がある。

【００２５】

上述の説明および実施例ではプロトコルとしてＳＩＰを使用したが、これは説明の目的

でなされたものであり、拡張プロトコル・ヘッダを含む通信を提供する本方法および装置は、ＳＩＰプロトコルまたはコール・カンファレンスの実施形態に限定されることが意図されるわけではないことを理解されたい。さらに、変更された受信者アドレス、サービス識別子および認証情報が拡張ヘッダで与えられるさらなる情報の例として論じられているが、拡張ヘッダは異なる機能またはさらなる機能をメッセージの受信者に提供するために、その他の情報を含むことができるということを理解されたい。

【００２６】

図２Ａおよび２Ｂには、ここで開示される方法のフロー・チャートが示される。長方形の要素はここでは「処理ブロック」を意味し、コンピュータ・ソフトウェアの命令または命令群を表す。代替として、処理ブロックはデジタル信号プロセッサ回路または特定用途向け集積回路（ＡＳＩＣ）などの機能的に等価な回路によって実行されるステップを表す。流れ図には、いかなる特定のプログラミング言語の構文も記載していない。むしろ流れ図は、当業者が回路を製造するか、またはコンピュータ・ウェアを作成して、本発明により求められる処理を実行するために必要とする機能上の情報を示す。ループおよび変数の初期化、ならびに一時変数の使用などの多くのルーチンのプログラム要素は示していないことに留意されたい。本明細書に特に明記しない限り、説明される特定の順序のステップは例示的であるに過ぎず、本発明の精神から逸脱することなく変更が可能であることを当業者には理解されたい。したがって特に言及しない限り、以下で説明するステップは、可能であれば、任意の都合のよい順番または望ましい順番で実行されることができるということを意味し、順不同である。

【００２７】

ここで図２Ａおよび２Ｂを参照すると、拡張プロトコル・ヘッダを含む通信を提供する方法１００が示されている。方法は、通信プロトコルの中でヘッダを有するメッセージを提供することを開示する、処理ブロック１０２で始まる。

【００２８】

処理ブロック１０４は、ヘッダの中にさらなる情報を含む拡張子を含むことを述べる。処理ブロック１０６に示すように、これは変更された受信者アドレスと、サービス識別子と、認証情報とから構成されるグループのうちの少なくとも１つを含むことができる。処理ブロック１０８でさらなる情報は変更された受信者アドレスを含み、受信者はメッセージを受信し、変更された受信者アドレスへメッセージを送る。処理ブロック１１０でさらなる情報はサービス識別子を含み、受信者はメッセージを受信し、サービス識別子によって識別される特定のサービスを選択する。処理ブロック１１２でさらなる情報は認証情報を含み、受信者は最初のユーザ認証を実行し、次いでメッセージに埋め込まれた認証情報とともに最初のリクエスタを第２の情報サービスに送り、第２のサービスは、開始側のユーザからの信用証明を再要求することを必要とせずに、メッセージの認証情報によってユーザを認証する。処理ブロック１１４で示すように、認証情報はセキュリティ符号を含む。

【００２９】

受信者へのメッセージの送信を述べる処理ブロック１１６で処理は続き、受信者はさらなる機能を提供するために、ヘッダの拡張子に含まれるさらなる情報を利用することができる。

【００３０】

処理ブロック１１８は、プロトコルがセッション開始プロトコル（Ｓｅｓｓｉｏｎ Ｉｎｉｔｉａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）（ＳＩＰ）を含み、拡張子を含むヘッダが拡張ＳＩＰヘッダを含むことを述べる。

【００３１】

拡張プロトコル・ヘッダを含む通信を提供するための上述の方法は、プロトコルのメッセージが標準的な方法で外部ネットワークに公表されることなく、隠された受信者に発送されるようにすることによって、さらなるセキュリティを可能にする。さらに本方法により、ネットワークでのプロキシ・サーバの変更を必要とせずに、ルーティング情報がネッ

トワークで変えられることが可能になる。さらにまた本方法により、メッセージの送信者は複数の受信者に対して単一のプロトコルのアドレスを利用することができる。その上さらに本方法より、送信者は所望のサービスのための識別子およびパスワード／パスコードを埋め込むことが可能であり、受信者はこの情報に対する入力促進を必要とすることなく、送信者を認証することができる。

【００３２】

図３はホスト・コンピュータ・システム２４０として設定された、コンピュータ・システム構造の実施例を示す。コンピュータ・システム２４０はパーソナル・コンピュータ、ワークステーション、携帯型コンピューティング・デバイス、メーンフレーム、サーバおよびその他等の任意の種類のコンピュータ化システムであってよい。この実施例で、システムはメモリ・システム２１２とプロセッサ２１３と通信インタフェース２１４とを接続する相互接続機構２１１を含む。通信インタフェース２１４によって、コンピュータ・システム２４０は外部のデバイスまたはシステムと通信することができる。

【００３３】

メモリ・システム２１２は、上述の本発明の実施形態の処理機能を実施する、（例えばメモリ内か、またはディスクなどのその他のコンピュータ可読媒体上に格納される）データおよび／または論理命令などのソフトウェア符号を示すアプリケーション２５５－Ａによって符号化される任意の種類のコンピュータ可読媒体であってよい。プロセッサ２１３は、対応するプロセス２５５－Ｂを生成するために、ホストのためのアプリケーション２５５－Ａの論理命令を開始、操作、執行、解釈またはその他の仕方で実行するため、相互接続機構２１１を介してメモリ・システム２１２にアクセスすることができる。つまりプロセス２５５－Ｂは、コンピュータ・システムのプロセッサ２１３内か、またはその上で機能するアプリケーション２５５－Ａの１つまたは複数の部分を示す。

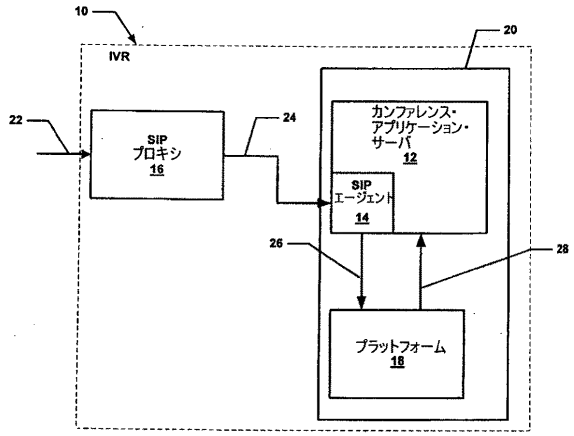
【００３４】

本発明の実施形態はフロッピー・ディスク、ハード・ディスクもしくは光学媒体などのコンピュータ可読媒体の中で、またはファームウェア、読み出し専用メモリ（ＲＯＭ）の中などのメモリ型システムの中で符号化されるか、またはこの実施形態の中でのようにメモリ・システム２１２内（例えばランダム・アクセス・メモリすなわちＲＡＭ内）で実行可能符号として符号化されるアプリケーション（すなわち未実行か、または非実行の論理命令および／またはデータ）を含むことを理解されたい。本発明のその他の実施形態は、プロセッサ２１３内でプロセスとして動作するアプリケーションを提供できることもまた理解されたい。この実施例では示されていないが、コンピュータ・システムは、本発明の説明を簡略化するためにこの例示では省かれているオペレーティング・システムなどの、その他のプロセスおよび／またはソフトウェアおよびハードウェア部品を含んでもよいことを当業者であれば理解されよう。

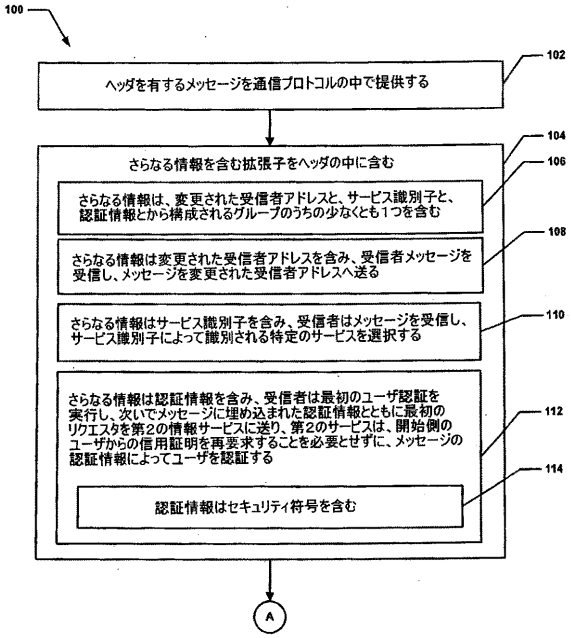
【００３５】

本発明の好ましい実施形態を説明してきたことで、これらの概念を組み込んだその他の実施形態が使用されてもよいことが、ここで当業者には明らかとなろう。さらに、本発明の一部として含まれるソフトウェアは、コンピュータによる使用が可能な媒体を含むコンピュータ・プログラム製品の中で実施されてもよい。例えば、そうしたコンピュータによる使用が可能な媒体はコンピュータ可読のプログラム符号区分が格納されたハード・ドライブ・デバイス、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、またはコンピュータ・ディスケットなどの読み出し可能メモリ・デバイスを含むことができる。コンピュータ可読媒体はまた、デジタルまたはアナログ信号として運搬されるプログラム符号区分を有する、光、有線または無線の通信リンクを含むこともできる。したがって、本発明は説明されている実施形態に限定されるべきではなく、むしろ添付の特許請求項の精神および範囲によってのみ限定されるべきである。

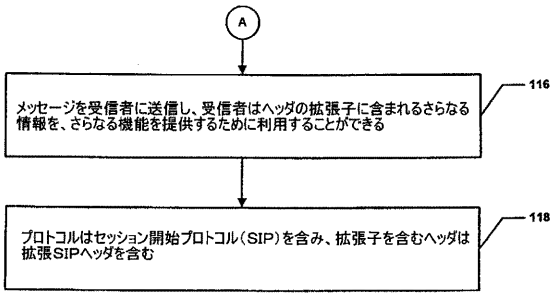
【図１】


10
IVR
20
22
SIP
プロキシ
16
24
カンファレンス・
アプリケーション・
サーバ
12
SIP
エージェント
14
26
28
プラットフォーム
18

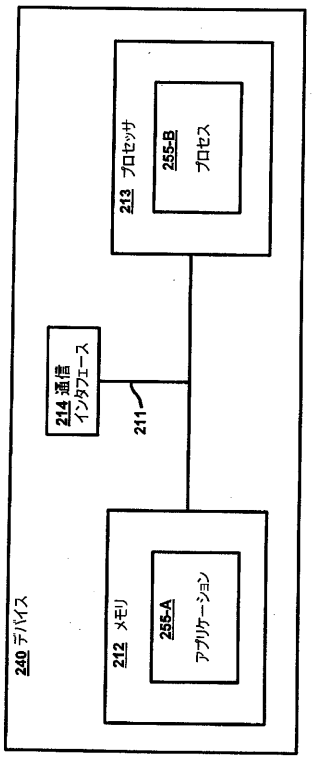
【図２Ａ】


100
ヘッダを有するメッセージを通信プロトコルの中で提供する
102
さらなる情報を含む拡張子をヘッダの中に含む
104
さらなる情報は、変更された受信者アドレスと、サービス識別子と、
認証情報とから構成されるグループのうちの少なくとも１つを含む
106
さらなる情報は変更された受信者アドレスを含み、受信者メッセージを
受信し、メッセージを変更された受信者アドレスへ送る
108
さらなる情報はサービス識別子を含み、受信者はメッセージを受信し、
サービス識別子によって識別される特定のサービスを選択する
110
さらなる情報は認証情報を含み、受信者は最初のユーザ認証を
実行し、次いでメッセージに埋め込まれた認証情報とともに最初の
リクエスタを第２の情報サービスに送り、第２のサービスは、開始側の
ユーザからの信用証明を再要求することを必要とせずに、メッセージの
認証情報によってユーザを認証する
112
認証情報はセキュリティ符号を含む
114
A

【図２Ｂ】


A
メッセージを受信者に送信し、受信者はヘッダの拡張子に含まれるさらなる
情報を、さらなる機能を提供するために利用することができる
116
プロトコルはセッション開始プロトコル（SIP）を含み、拡張子を含むヘッダは
拡張SIPヘッダを含む
118

【図３】


213 プロセッサ
255-B プロセス
214 通信
インタフェース
211
212 メモリ
255-A アプリケーション
240 デバイス

【手続補正書】
【提出日】平成24年1月13日(2012.1.13)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
拡張プロトコル・ヘッダを含む通信を提供する方法であって、
メッセージを通信プロトコルの中で提供するステップであって、前記メッセージがヘッダを有するステップ、
拡張子を前記ヘッダの中に含ませるステップであって、前記拡張子がさらなる情報を含み、前記ヘッダ内の拡張子が該ヘッダへの追加フィールドの付加部からなり、前記さらなる情報が認証情報を含み、受信者が最初のユーザ認証を実行し、次いで前記メッセージに埋め込まれた前記認証情報とともに最初のリクエスタを第２の情報サービスに送り、該第２のサービスは、開始側のユーザからの信用証明を再要求することを必要とせずに、前記メッセージの前記認証情報によって前記ユーザを認証する、ステップ、及び
前記メッセージを前記受信者に送信するステップであって、前記受信者が前記ヘッダの前記拡張子に含まれる前記さらなる情報を、さらなる機能を提供するために利用することができるステップ
を備え、
外部ネットワークに公表されることなく隠された受信者にプロトコルメッセージがルーティングされるようにすることによって、前記さらなる情報がさらなるセキュリティを与える、方法。
【請求項２】
前記さらなる情報は変更された受信者アドレスを含み、前記受信者は前記メッセージを受信して変更された受信者アドレスに前記メッセージを送る請求項１に記載の方法。
【請求項３】
前記さらなる情報はサービス識別子を含み、前記受信者は前記メッセージを受信して前記サービス識別子によって識別される特定のサービスを選択する請求項１に記載の方法。
【請求項４】
前記認証情報はセキュリティ符号を含む請求項１に記載の方法。
【請求項５】
前記プロトコルはセッション開始プロトコル（ＳＩＰ）を含み、拡張子を含む前記ヘッダは拡張ＳＩＰヘッダを含む請求項１に記載の方法。
【請求項６】
拡張プロトコル・ヘッダを含む通信を提供するための、コンピュータ可読符号を有するコンピュータ可読記憶媒体であって、
メッセージを通信プロトコルの中で提供する命令であって、前記メッセージがヘッダを有する、命令、
拡張子を前記ヘッダの中に含ませる命令であって、前記拡張子がさらなる情報を含み、前記ヘッダ内の拡張子が該ヘッダへの追加フィールドの付加部からなり、前記さらなる情報が認証情報を含み、受信者が最初のユーザ認証を実行し、次いで前記メッセージに埋め込まれた前記認証情報とともに最初のリクエスタを第２の情報サービスに送り、該第２のサービスは、開始側のユーザからの信用証明を再要求することを必要とせずに、前記メッセージの前記認証情報によって前記ユーザを認証するように構成された命令、及び
前記メッセージを前記受信者に送信する命令であって、前記受信者が前記ヘッダの前記拡張子に含まれる前記さらなる情報を、さらなる機能を提供するために利用することができる、命令

を備え、
外部ネットワークに公表されることなく隠された受信者にプロトコルメッセージがルーティングされるようにすることによって、前記さらなる情報がさらなるセキュリティを与えるものである、コンピュータ可読記憶媒体。
【請求項７】
拡張子を前記ヘッダの中に含ませる前記命令であって、前記拡張子がさらなる情報を含む前記命令は、前記さらなる情報が変更された受信者アドレスを含み、前記受信者が前記メッセージを受信して前記変更された受信者アドレスに前記メッセージを送るための命令を含む請求項６に記載のコンピュータ可読記憶媒体。
【請求項８】
拡張子を前記ヘッダの中に含ませる前記命令であって、前記拡張子がさらなる情報を含む前記命令は、前記さらなる情報がサービス識別子を含み、前記受信者が前記メッセージを受信して前記サービス識別子によって識別される特定のサービスを選択するための命令を含む請求項６に記載のコンピュータ可読記憶媒体。
【請求項９】
拡張子を前記ヘッダの中に含ませる前記命令であって、前記拡張子が認証情報を含む前記命令は、セキュリティ符号を含む請求項６に記載のコンピュータ可読記憶媒体。
【請求項１０】
前記プロトコルはセッション開始プロトコル（ＳＩＰ）を含み、拡張子を含む前記ヘッダは拡張ＳＩＰヘッダを含む請求項６に記載のコンピュータ可読記憶媒体。
【請求項１１】
メモリ、
プロセッサ、
通信インタフェース、及び
メモリとプロセッサと通信インタフェースとを接続する相互接続機構
を備え、
前記メモリは、プロセッサ上で実行されたときに、
メッセージを通信プロトコルの中で受信するステップであって、前記メッセージがヘッダを有し、ヘッダが前記ヘッダの中に拡張子を含み、前記ヘッダ内の拡張子が該ヘッダへの追加フィールドの付加部からなり、前記拡張子がさらなる情報を含み、前記ヘッダ内の拡張子が該ヘッダへの追加フィールドの付加部からなり、前記さらなる情報が認証情報を含み、受信者が最初のユーザ認証を実行し、次いで前記メッセージに埋め込まれた前記認証情報とともに最初のリクエスタを第２の情報サービスに送り、該第２のサービスは、開始側のユーザからの信用証明を再要求することを必要とせずに、前記メッセージの前記認証情報によって前記ユーザを認証する、ステップ、及び
前記メッセージを前記受信者に送信するステップであって、前記受信者が前記ヘッダの前記拡張子に含まれる前記さらなる情報を、さらなる機能を提供するために利用することができるステップ
の操作をコンピュータ・システムが実行できるようにする、プロセシング情報のためのプロセスを提供するアプリケーションによって符号化され、
外部ネットワークに公表されることなく隠された受信者にプロトコルメッセージがルーティングされるようにすることによって、前記さらなる情報がさらなるセキュリティを与えるものである、コンピュータ・システム。
【請求項１２】
前記さらなる情報は変更された受信者アドレスを含み、前記受信者は前記メッセージを受信して変更された受信者アドレスに前記メッセージを送る請求項１１に記載のコンピュータ・システム。
【請求項１３】
前記さらなる情報はサービス識別子を含み、前記受信者は前記メッセージを受信して前記サービス識別子によって識別される特定のサービスを選択する請求項１１に記載のコン

ピュータ・システム。
【請求項１４】
前記認証情報はセキュリティ符号を含む請求項１１に記載のコンピュータ・システム。
【請求項１５】
前記プロトコルはセッション開始プロトコル（ＳＩＰ）を含み、拡張子を含む前記ヘッダは拡張ＳＩＰヘッダを含む請求項１１に記載のコンピュータ・システム。

フロントページの続き

(72)発明者　ロバート　エス．ホーン
アメリカ合衆国　０１４６０　マサシューセッツ，リットルトンブルース　ストリート　７４
(72)発明者　イグナシオ　ミランダ
スペイン　２８７００　マドリッド，マクシミリアノ　プエロ　デル　テル　（２シー）　２１
(72)発明者　ブルース　ワルシュ
アメリカ合衆国　０３０５３　ニュー　ハンプシャー，ロンドンデリー，ハゼルナット　レーン　１８

Ｆターム(参考) 5K201 AA09 BB09 CB06 CD09 DA10