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

特許第4800651号
(P4800651)

(45)発行日　平成23年10月26日(2011.10.26)　(24)登録日　平成23年8月12日(2011.8.12)

(51)Int.Cl.		F I		
H04L 9/36	(2006.01)	H04L	9/00	685
H04L 29/06	(2006.01)	H04L	13/00	305A
H04L 9/32	(2006.01)	H04L	9/00	675B

請求項の数 27　外国語出願　(全 36 頁)

(21)出願番号	特願2005-92424(P2005-92424)
(22)出願日	平成17年3月28日(2005.3.28)
(65)公開番号	特開2005-312026(P2005-312026A)
(43)公開日	平成17年11月4日(2005.11.4)
審査請求日	平成20年2月29日(2008.2.29)
(31)優先権主張番号	10/815,232
(32)優先日	平成16年3月31日(2004.3.31)
(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　トーマス　バック
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】セッション開始プロトコルルーティングヘッダに対して署名および検証を行う方法

(57)【特許請求の範囲】

【請求項１】

ＳＩＰ（セッション開始プロトコル）メッセージを処理する方法であって、

ＳＩＰノードにおいてＳＩＰ要求を受信するステップであって、前記ＳＩＰ要求は、ネットワークルーティングロケーションを示すデータを含むメッセージヘッダを含む、ステップと、

前記ＳＩＰ要求を受信する前記ＳＩＰノードのネットワークロケーションを示すさらなるデータを前記メッセージヘッダに付加するステップと、

該付加されたデータを含む少なくとも前記メッセージヘッダの一部分に基づいて署名を生成するステップと、

ＳＩＰノードヘッダエントリを生成するステップと、

前記ＳＩＰノードヘッダエントリに前記署名を挿入するステップと

を備えることを特徴とする方法。

【請求項２】

前記ＳＩＰノードヘッダエントリは、エコーされるヘッダであることを特徴とする請求項１に記載の方法。

【請求項３】

前記ＳＩＰ要求に対する返信として、前記ＳＩＰノードにおいてＳＩＰ応答を受信するステップであって、前記ＳＩＰ応答は、前記ＳＩＰノードヘッダエントリからエコーされたヘッダに基づいて生成された応答ヘッダを含み、前記応答ヘッダは、前記署名を含む、

ステップと、
前記応答ヘッダから、前記署名を除くステップと、
前記署名を除いた応答ヘッダの少なくとも一部分に基づいて検証署名を生成するステップと、
前記検証署名を前記署名と比較するステップと、
該比較の結果、前記検証署名と前記署名とが合致した場合に、次のＳＩＰノードに前記ＳＩＰ応答を転送するステップと
をさらに備えることを特徴とする請求項１に記載の方法。
【請求項４】
前記ＳＩＰノードヘッダエントリは、ＶＩＡヘッダであることを特徴とする請求項３に記載の方法。
【請求項５】
前記ＳＩＰ応答を受信するステップは、前記ＳＩＰ要求に対する返信として、前記ＳＩＰノードに関する前記ＶＩＡヘッダを含むＳＩＰ応答を受信するステップであって、前記ＳＩＰノードに関する前記ＶＩＡヘッダは、前記署名を含む、ステップを含むことを特徴とする請求項４に記載の方法。
【請求項６】
前記検証署名を生成するステップは、前記ＳＩＰ応答の少なくとも１つのＶＩＡヘッダに基づいて前記検証署名を生成するステップを含むことを特徴とする請求項５に記載の方法。
【請求項７】
前記ＳＩＰ要求を受信する次のＳＩＰノードへの次のリンクを特定するステップと、
前記次のＳＩＰノードへの前記次のリンクが信頼されないリンクであるかどうかを判定するステップとをさらに備え、
前記署名は、前記次のリンクが信頼されないリンクである場合に生成されることを特徴とする請求項５に記載の方法。
【請求項８】
前記署名を生成するステップは、前記メッセージヘッダの少なくとも１つのＶＩＡヘッダに基づいて前記署名を生成するステップを含むことを特徴とする請求項１に記載の方法。
【請求項９】
前記署名を生成するステップは、前記メッセージヘッダの少なくとも１つのＶＩＡヘッダと、ピアＦＱＤＮ、前記メッセージが次のホップ上で送信される前記接続の接続識別子、前記メッセージヘッダのＦＲＯＭヘッダの少なくとも一部分、前記メッセージヘッダのＴＯヘッダの少なくとも一部分、前記メッセージヘッダのＣＡＬＬ－ＩＤヘッダの少なくとも一部分、および前記メッセージヘッダのＣＳｅｑヘッダの前記少なくとも一部分の少なくとも１つとに基づくことを特徴とする請求項８に記載の方法。
【請求項１０】
前記メッセージヘッダは、複数のＶＩＡヘッダを含み、
前記署名を生成するステップは、前記ＳＩＰノードの前記ＶＩＡヘッダを除く、前記複数のＶＩＡヘッダに基づいて前記署名を生成するステップを含むことを特徴とする請求項８に記載の方法。
【請求項１１】
前記署名を生成するステップは、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの少なくとも一部分、および前記メッセージヘッダのＣＯＮＴＡＣＴヘッダの少なくとも一部分に基づいて第２の署名を生成するステップを含むことを特徴とする請求項１に記載の方法。
【請求項１２】
前記署名を挿入するステップは、前記第２の署名をＵＲＩパラメータとして、前記ＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入するステップを含むことを特徴とする請求項１１に記載の方法。

【請求項１３】
前記第２の署名を生成するステップは、前記ＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを除く、前記メッセージヘッダ内の各ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのＵＲＩ部分、および前記メッセージヘッダ内の前記ＣＯＮＴＡＣＴヘッダのＵＲＩ部分に基づいて第２の署名を生成するステップを含むことを特徴とする請求項１１に記載の方法。
【請求項１４】
前記応答ヘッダのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダおよびＣＯＮＴＡＣＴヘッダに基づいて第３の署名を生成するステップと、
前記応答の前記ＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダに前記第３の署名を挿入するステップと
をさらに備えることを特徴とする請求項３に記載の方法。
【請求項１５】
前記第３の署名を生成する前に、前記ＳＩＰノードヘッダエントリから既存の署名を削除するステップをさらに備えることを特徴とする請求項１４に記載の方法。
【請求項１６】
前記第３の署名を挿入するステップは、前記第３の署名をＵＲＩパラメータとして、前記ＳＩＰノードの前記ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入するステップを含むことを特徴とする請求項１４に記載の方法。
【請求項１７】
前記第３の署名を生成するステップは、前記ＳＩＰノードの前記ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを除く、前記応答の各ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの前記ＵＲＩ部分、および前記ＣＯＮＴＡＣＴヘッダのＵＲＩ部分に基づいて前記第３の署名を生成するステップを含むことを特徴とする請求項１４に記載の方法。
【請求項１８】
前記ＳＩＰ要求を受信する次のＳＩＰノードへの次のリンクを特定するステップと、
前記次のＳＩＰノードへの前記次のリンクが信頼されないリンクであるかどうかを判定するステップとをさらに備え、
前記第３の署名を生成するステップは、前記次のリンクが信頼されないリンクである場合にだけ前記第３の署名を生成するステップを含むことを特徴とする請求項１４に記載の方法。
【請求項１９】
前記ＳＩＰノードは、サーバのプール内にあり、前記方法は、暗号化されたセッションキーを前記ＳＩＰノードの前記ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入するステップをさらに備えることを特徴とする請求項１８に記載の方法。
【請求項２０】
前記ＳＩＰ要求のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを特定するステップをさらに備え、
前記署名を生成するステップは、前記ＳＩＰ要求の前記ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの少なくとも一部分に基づいて第４の署名を生成するステップを含むことを特徴とする請求項３に記載の方法。
【請求項２１】
前記署名を挿入するステップは、前記ＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダに前記第４の署名を挿入するステップを含むことを特徴とする請求項２０に記載の方法。
【請求項２２】
前記第４の署名を挿入するステップは、前記第４の署名を前記ＳＩＰノードの前記ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのヘッダパラメータとして挿入するステップを含むことを特徴とする請求項２１に記載の方法。
【請求項２３】
前記ＳＩＰ応答を受信するステップは、前記ＳＩＰ要求に対する返信として、前記ＳＩＰノードに関する前記ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを含むＳＩＰ応答を受信するステップであって、前記ＳＩＰノードに関する前記ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダは、前記

第４の署名を含む、ステップを含むことを特徴とする請求項２１に記載の方法。
【請求項２４】
前記ＳＩＰ要求を受信する次のＳＩＰノードへの次のリンクを特定するステップと、
前記次のＳＩＰノードへの前記次のリンクが信頼されないリンクであるかどうかを判定するステップとをさらに備え、
前記第４の署名を生成するステップは、前記次のリンクが信頼されないリンクである場合にだけ前記第４の署名を生成するステップを含むことを特徴とする請求項２０に記載の方法。
【請求項２５】
請求項１に記載の方法を実行するためのコンピュータ実行可能命令を格納したことを特徴とするコンピュータ読み取り可能な記録媒体。
【請求項２６】
前記エコーされたヘッダは、ＶＩＡヘッダ、ＦＲＯＭヘッダ、ＴＯヘッダ、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ、ＣＡＬＬ－ＩＤヘッダ、およびＣＳｅｑヘッダから成るグループから選択されるヘッダであることを特徴とする請求項３に記載の方法。
【請求項２７】
前記検証署名を生成するステップは、ＶＩＡヘッダ、ＣＯＮＴＡＣＴヘッダ、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ、ＲＯＵＴＥヘッダ、ＣＡＬＬ－ＩＤヘッダ、およびＣＳｅｑヘッダの少なくとも１つに基づいて前記検証署名を生成するステップを含むことを特徴とする請求項２５に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、コンピュータネットワークを介してデバイス間で通信するための方法およびコンピュータ可読媒体を対象とし、より詳細には、「ＳＩＰ」（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（セッション開始プロトコル））ルーティングヘッダに対する署名および検証（validating）を行って、ＳＩＰメッセージに含まれるルーティングコマンドを認証するための方法およびコンピュータ可読媒体を対象とする。
【背景技術】
【０００２】
「ＳＩＰ」（セッション開始プロトコル）は、インスタントメッセージング、インターネット電話コール、およびインターネットビデオ会議を含む、通信セッションを確立すること、管理すること、および終了させることに関するインターネットシグナルプロトコルである。ＳＩＰは、参照によりそれぞれが本明細書に組み込まれている非特許文献１および非特許文献２において規定されている。ＳＩＰセッションには、１名または複数名の参加者またはクライアント（通常、呼び出し元および呼び出し先と呼ばれる）が関与する。ＳＩＰメッセージは、通常、様々なサーバであるＳＩＰノード群のネットワークを介して、各エンドポイントＳＩＰノード（例えば、呼び出し元と呼び出し先）の間でルーティングされる。
【０００３】
一般に、次の２つのタイプのＳＩＰメッセージが存在する。すなわち、呼び出し元（例えば、エンドポイントＳＩＰノード）から呼び出し先に送信される要求、および要求に応答して呼び出し先から呼び出し元に送信される応答である。一部のケースでは、呼び出し先は、ダイアログセッションが開始された後、呼び出し元に応答を送信することも可能である。各ＳＩＰメッセージは、応答であるか、要求であるかにかかわらず、一般に、次の３つの部分を含む。すなわち、開始行（ｓｔａｒｔ　ｌｉｎｅ）、ヘッダ、および本文である。開始行は、メッセージタイプ（例えば、要求または応答）およびプロトコルバージョンを伝え、メッセージ本文は、メッセージの内容を含み、開始行におけるシグナル情報を超えるセッション記述情報を伝えることができる。ＳＩＰヘッダフィールドは、メッセージの属性を伝え、メッセージの意味を変更する。ヘッダフィールドの中に格納されるメ

ッセージの一部の属性は、メッセージをどのようにルーティングするかについての命令であるとともに、メッセージが伝送される実際の経路の記録も行う。例えば、経路についての要求を管理する各ＳＩＰノードは、完全修飾ドメイン名（fully qualified domain）またはインターネットプロトコルアドレスなどの、ＳＩＰノードを識別する情報を含む「ＶＩＡ」ヘッダを追加する。このようにして、経路におけるループが検出されることが可能であり、応答は、要求からのＶＩＡヘッダを使用して、呼び出し元に戻るように伝送される経路を決める。しかし、メッセージの特定のパスは、時間とともに変わる可能性があり、このため、ホームサーバなどのＳＩＰノードは、電話コールなどのダイアログの第１の要求を受信するが、同一のダイアログにおける後続の要求は受信しない可能性がある。そのダイアログのために「ループに入った」ままであるように、ＳＩＰノードは、「ＵＲＩ」（ユニフォームリソースインジケータ）、または他のサーバまたはエンドポイントがＳＩＰノードに到達することを可能にする他のアドレスなどの、ＳＩＰノードを識別する情報を含むＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを挿入することができる。次に、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの完成されたリストの諸部分が、受信側エンドクライアント（要求に関して呼び出し先、応答に関して呼び出し元）によって一組のＲＯＵＴＥヘッダの中にコピーされる。ＲＯＵＴＥ　ＳＥＴヘッダは、同一のダイアログセッション内のあらゆる将来の要求をどのようにルーティングするかについての命令をＳＩＰノード群に提供するデータを含む。

【０００４】

前述したＳＩＰヘッダフィールドは、メッセージの経路上のサーバ群などの、ＳＩＰノードに、またＳＩＰノードからメッセージをルーティングするのに役立つが、それらのヘッダの多くは、ＳＩＰ標準（ＲＦＣ３２６１）に従って使用される場合、セキュリティで保護されない。例えば、サービス拒否攻撃が、ＳＩＰヘッダ内の偽のルーティング情報を含む、複数の偽造されたＳＩＰメッセージを使用して、サーバに向けられることが可能である。偽のメッセージの真の送信元は、偽造されたヘッダ情報で隠されて、場合により、サービス拒否攻撃が、無実のサーバを送信元としているように見せかけることが可能である。さらに、偽造されたルーティングヘッダは、２つのサーバ間でループメッセージを作成することも可能である。このようにして、偽のメッセージの偽造された「経路」上の各サーバが、偽のメッセージを処理し、転送するのに貴重なリソースを浪費して、それらのリソースを正当なユーザに拒否する可能性がある。

【０００５】

【非特許文献１】International Engineering Task Force Request for Comments 2543

【非特許文献２】International Engineering Task Force Request for Comments 3261

【発明の開示】

【発明が解決しようとする課題】

【０００６】

従来のシステムには上述したような種々の問題があり、さらなる改善が望まれている。

【０００７】

本発明は、このような状況に鑑みてなされたもので、その目的とするところは、ＳＩＰルーティングヘッダに対する署名および検証を行って、ＳＩＰメッセージに含まれるルーティングコマンドを認証するための方法およびコンピュータ読み取り可能な記録媒体を提供することにある。

【課題を解決するための手段】

【０００８】

本発明の諸実施形態は、ＳＩＰメッセージの中に見られるルーティングヘッダを認証するための方法およびコンピュータ可読媒体を対象とする。具体的には、ＳＩＰノードが、メッセージヘッダを含むＳＩＰ要求を受信することが可能である。メッセージヘッダの少なくとも一部分に基づいて署名が生成され、ＳＩＰノードヘッダエントリの中に挿入されることが可能である。本明細書で使用するＳＩＰノードとは、ＳＩＰクライアントまたはサーバとして動作することができるコンピューティングデバイス上で実行されるＳＩＰア

プリケーションを意味する。

【０００９】

例えば、受信された要求ヘッダ内のＶＩＡヘッダの少なくとも一部分に基づいて第１の署名が生成され、ＳＩＰノードに関するＶＩＡヘッダの中に挿入されることが可能である。ＳＩＰ要求に対する応答が生成されると、ＳＩＰノードのＶＩＡヘッダは、ＳＩＰ標準の処理に従って応答ヘッダの中でエコーバック（ｅｃｈｏ　ｂａｃｋ）される。ＳＩＰノードは、応答を受信すると、応答のＳＩＰノードＶＩＡヘッダ内の第１の署名を検証して（verify）、応答が伝送された実際のパスの完全性を認証することができる。

【００１０】

さらに、または代替として、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの少なくとも一部分、およびメッセージヘッダのＣＯＮＴＡＣＴヘッダに基づき、第２の署名が生成されることも可能である。第２の署名は、ＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダに挿入されることが可能である。付加された第２の署名を有するこのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの諸部分は、セッションが開始された後に、呼び出し先システムによって呼び出し元システムに対して生成された要求をルーティングし、検証するためのＲＯＵＴＥヘッダとして使用するために、呼び出し先システムによって保存されることが可能である。

【００１１】

さらに、または代替として、メッセージヘッダのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの少なくとも一部分に基づき、第３の署名が生成されることも可能である。第３の署名は、ＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダに挿入されることが可能である。呼び出し先がＳＩＰ要求に応答すると、ＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダは、応答ヘッダの中でエコーバックされる。将来の要求をどのようにルーティングするかについての命令の完全性を検証するため、ＳＩＰノードが応答を受信すると、第３の署名がＳＩＰノードによって検証されることが可能である。例えば、応答を受信したＳＩＰノードは、要求ヘッダからエコーされたデータを含むＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを識別し、エコーされたヘッダから署名を抽出することができる。ＳＩＰノードは、第３の署名を生成するのに使用されたのと同一のプロセスを使用して、例えば、応答ヘッダ内のヘッダ群の少なくとも一部分に基づいて署名を生成して、検証署名を生成することができる。次に、ＳＩＰノードは、検証署名を抽出された署名と比較することができる。署名が合致した場合、メッセージは、通常の形で処理されることが可能である。

【００１２】

第４の署名が生成され、ＳＩＰ応答ヘッダに挿入されることも可能である。例えば、応答を受信したＳＩＰノードは、応答ヘッダのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの少なくとも一部分、および応答ヘッダのＣＯＮＴＡＣＴヘッダに基づき、第４の署名を生成することができる。第４の署名は、前述した第２の署名に類似するが、第４の署名は、応答の中のＣＯＮＴＡＣＴヘッダに基づいて生成されるので、ＣＯＮＴＡＣＴは、要求の場合のように呼び出し元ではなく、呼び出し先を識別する。次に、第４の署名は、ＳＩＰノードに関するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダに挿入されることが可能である。呼び出し元システムは、応答を受信すると、付加された署名を有するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの諸部分を、後続の要求の中のルーティング命令の使用および検証のためのＲＯＵＴＥ　ＳＥＴヘッダとして保存することができる。

【００１３】

一部のケースでは、ＳＩＰメッセージを処理するＳＩＰノードは、同一のダイアログにおけるメッセージを処理するのに互いに区別なく使用されることが可能な少なくとも第１のサーバと第２のサーバとを有するサーバのプールによって提供されることが可能である。ただし、メッセージが交換される際、ダイアログにおける要求が、第１のサーバによって生成された署名を含むが、処理のために第２のサーバに送信されることが可能である。これは、第２のサーバが、要求の中の署名を検証するのに使用されるセッションキーを有することを要する。要求の中の署名を生成するのに使用されたセッションキーをセキュリティで保護された形で転送するため、署名を生成した第１のサーバは、暗号化され、署名

されたセッションキーをメッセージのヘッダに付加することができる。例えば、このセッションキーは、このキーによって生成された署名を含むのと同一のヘッダに挿入されることが可能である。他のＳＩＰノード群からセッションキーを保護するため、第１のサーバは、サーバのプールがアクセスできる公開キーを使用して、セッションキーを暗号化することができる。次に、第１のサーバは、サーバのプールがアクセスできる秘密キーを使用して、暗号化されたキーに署名することができる。要求を受信した第２のサーバは、暗号化されたキー上の署名を検証した後、セッションキーを解読することができる。解読されたセッションキーを使用して、第２のサーバは、次に、メッセージヘッダの少なくとも一部分に基づいて署名を検証することができる。例えば、公開キー／秘密キーペアを含む非対称キー技術を含め、任意の適切なセキュリティプロセスを使用して、セッションキーを保護することができることを認識されたい。

【００１４】

本発明の以上の態様、および付随する利点の多くは、添付の図面と併せて解釈される、以下の詳細な説明を参照することで本発明がよりよく理解されるにつれ、より容易に認められるようになろう。

【発明を実施するための最良の形態】

【００１５】

以下、図面を参照して本発明を適用できる実施形態を詳細に説明する。サービス拒否攻撃は、通常、Ｗｅｂサーバ群またはファイルサーバ群などの、ネットワークサービスを過負荷状態にする（ｏｖｅｒｌｏａｄ）、または停止させるように攻撃者によって仕掛けられるコンピュータ化された攻撃である。例えば、攻撃は、サーバが、偽のメッセージに応答しようと試みることに余りにも忙しくなり、正当な接続要求を無視することを生じさせる。代替として、正当なメッセージのルーティングが壊れ、ＳＩＰノードが、誤った形で応答を転送するようにさせる可能性がある。一部のケースでは、コンピュータネットワークにわたってメッセージを伝送するのに使用される通信プロトコルが、重大な攻撃点であることが可能である。例えば、前述したとおり、偽造されたＶＩＡヘッダ、偽造されたＲＯＵＴＥヘッダ、および／または偽造されたＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを有する偽のＳＩＰメッセージが送信されて、メッセージが、被害（ｖｉｃｔｉｍ）ＳＩＰノード群に向けられること、および／または攻撃者の身元およびソースが隠されることが可能である。これらのサービス拒否攻撃を減らすため、ＳＩＰヘッダに含まれるルーティング命令、および実際のルーティングパスを検証して、命令およびパスの完全性を確実にすることができる。

【００１６】

図１は、ＳＩＰクライアント１０２のユーザ１００（例えば、アリス）が、インターネット、イントラネット、ワイドエリアネットワーク、ローカルエリアネットワーク、仮想プライベートネットワークなどを含むことが可能な通信ネットワークを介して、別のユーザ４００（ボブ）と通信セッションを開始することを所望する、典型的なセッション開始動作を示す。この目的で、コンピュータシステム１０４上に存在するＳＩＰクライアント１０２が、ボブを目的の受信者として識別するＩＮＶＩＴＥ要求メッセージ５００を送信する。ＳＩＰ標準の下における通信の文脈では、ＩＮＶＩＴＥメッセージ５００を送信してセッションを開始するＳＩＰクライアント１０２は、「呼び出し元」と呼ばれ、ボブのコンピュータシステム４０４上のＳＩＰクライアント４０２は、「呼び出し先」と呼ばれる。ＳＩＰにおける定義では、ＳＩＰクライアント１０２は、新たな要求を作成するので、「ＵＡＣ」（「ユーザエージェントクライアント」）とも呼ばれ、ＳＩＰクライアント４０２は、ＳＩＰ要求５００に対する応答６００を生成するので、「ＵＡＳ」（「ユーザエージェントサーバ」）とも呼ばれる。

【００１７】

図１に示すとおり、アリスからのＩＮＶＩＴＥメッセージ５００は、呼び出し元ＳＩＰクライアントのドメイン用の送信サーバ２００に送信される。その後、ＩＮＶＩＴＥメッセージは、シグナル動作に関与する複数のＳＩＰノードを経由させられてから、ボブのド

メインのＳＩＰプロキシサーバ３００に到達することが可能である。簡潔にするため、５つのＳＩＰノードだけを図１に例示するが、リンクのいずれも、他のサーバ群、ゲートウェイ群、ブリッジ群などを含むことが可能であることを認識されたい。ＳＩＰプロキシ３００は、ＩＮＶＩＴＥメッセージをボブのコンピュータのＳＩＰクライアント４０２（呼び出し先）に転送する。ボブのコンピュータは、自動的に、またはボブからの許可の後、伝送の成功を示す「２００（ＯＫ）」メッセージのような、ＩＮＶＩＴＥに対する応答６００を送信することができる。

【００１８】

前述したとおり、各ＳＩＰメッセージは、一般に、開始行と、メッセージの属性およびルーティングに関する情報を含むヘッダと、メッセージの本文とを含む。例えば、図２は、アリスのＳＩＰクライアント１０２によって送信され、ＳＩＰノード２００によって受信されたＩＮＶＩＴＥ要求５００を図示する。典型的なＩＮＶＩＴＥ５００は、開始行５０２、複数のヘッダ５０４、および本文５０６を含む。開始行５０２は、メッセージタイプ（この場合、ＩＮＶＩＴＥ）、一般に呼び出し先のＳＩＰアドレスである要求ＵＲＩ、およびＳＩＰバージョンを識別する。ヘッダ群５０４は、ＳＩＰ標準の下で許容されるフィールド群である。ＶＩＡヘッダ５０８は、前のホップのプロトコルおよびアドレスを示す情報を含む。ＦＲＯＭヘッダ５１０は、要求の送信元であるユーザ（呼び出し元）を、この場合は、アリスを示す情報を含む。ＴＯヘッダ５１２は、呼び出し元によって指定された呼び出し先を示す情報を含む。Ｃａｌｌ－ＩＤヘッダ５１４は、開始されるセッションのグローバル一意識別子を示す情報を含む。ＣＳｅｑヘッダ５１６は、同一のトランザクションの一環として、同一のＦＲＯＭヘッダ、同一のＴＯヘッダ、および同一のＣａｌｌ－ＩＤヘッダで送信された複数のメッセージを区別する識別子を示す。ＣＯＮＴＡＣＴヘッダ５１８は、後続の要求の宛先を示す情報を含み、将来のメッセージのルーティングが、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ（以下にさらに説明する）内にリストされていないＳＩＰノード群をバイパスすることを可能にする。ＶＩＡヘッダ、ＴＯヘッダ、ＦＲＯＭヘッダ、ＣＯＮＴＡＣＴヘッダ、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ、およびＲＯＵＴＥヘッダはそれぞれ、ＵＲＩ、インターネットプロトコルアドレスなどの、ネットワーク内のルーティングロケーションを示すデータを含む。例えば、ルーティングロケーションを示すデータを含むＲＥＣＯＲＤ－ＲＯＵＴＥヘッダは、「＜　＞」ブラケットの中に囲まれたＵＲＩ部分を含み、その後にヘッダパラメータが続くことが可能である。「＜　＞」ブラケット内のＵＲＩ部分は、ＵＲＩ、およびＵＲＩパラメータを含むことが可能である。一般に、少なくとも１つの空白行が、ヘッダ群５０４の終りと、本文部分５０６の先頭を示す。ＩＮＶＩＴＥ要求のような、図５に示した典型的な応答６００は、開始行６０２、ヘッダ部分６０４、および本文６０６を含む。

【００１９】

ＳＩＰ標準の下では、ＩＮＶＩＴＥ５００がネットワークを伝送される際、ＩＮＶＩＴＥ５００を管理するすべてのＳＩＰノードが、ＶＩＡヘッダをＩＮＶＩＴＥヘッダ５０４に追加する。このようにして、蓄積されたＶＩＡヘッダが、呼び出し先により、要求に返信する応答のルーティングを呼び出し元に向けるのに使用されることが可能である。ＳＩＰノードが、呼び出し元と呼び出し先の間におけるその特定のダイアログに関するメッセージを管理することを続けることを望む場合、ＳＩＰノードは、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをＩＮＶＩＴＥヘッダ５０４に挿入することができる。このようにして、呼び出し先によって生成されることが可能な将来の要求のルーティングを指示するため、ダイアログ開始要求に関するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダおよびＣＯＮＴＡＣＴヘッダの蓄積されたＵＲＩ部分が、受信側の呼び出し先によって、ヘッダ群のＲＯＵＴＥ　ＳＥＴとして、リストされるのと同一の順序で保存されることが可能である。同様に、呼び出し元によって生成される将来の要求に関するルーティング命令を提供するため、ダイアログ開始要求に対する応答の中のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダおよびＣＯＮＴＡＣＴヘッダの蓄積されたＵＲＩ部分が、呼び出し元によって、ＲＯＵＴＥ　ＳＥＴヘッダ群とは逆の順序で保存されることが可能である。

【００２０】
図１は、処理側ＳＩＰノード群によるヘッダの追加に鑑みて、ＩＮＶＩＴＥ要求およびＩＮＶＩＴＥ応答をルーティングすることの具体的な例を示す。簡潔にするため、無関係のヘッダ、およびその他のメッセージ情報は含めていない。図示したＳＩＰノード群の機能および数は、典型的であり、メッセージルーティングおよびメッセージ検証は、特定の目的および／またはネットワークアーキテクチャに合わせて変更することができることを認識されたい。
【００２１】
図１に示すとおり、ＳＩＰノード２００は、ホームサーバであることが可能であり、ＳＩＰクライアント１０２からＩＮＶＩＴＥ要求を受信することができる。メッセージを受信したＳＩＰノード２００は、ＶＩＡヘッダをＩＮＶＩＴＥ要求のヘッダ５０４に挿入する。ＳＩＰノード２００は、ホームサーバとして、ＳＩＰクライアント１０２に対する、またはクライアント１０２からのあらゆるＳＩＰメッセージを管理することを望む可能性がある。したがって、ＳＩＰノード２００は、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをＩＮＶＩＴＥメッセージの中に挿入してから、そのメッセージを次のＳＩＰノードに転送することができる。図１の例示する実施形態では、次のＳＩＰノード２５０は、呼び出し元ＳＩＰクライアント１０２に対するエッジサーバである。ＳＩＰノード２５０は、独自のＶＩＡヘッダおよびＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをメッセージのヘッダ５０４に挿入した後、ＩＮＶＩＴＥメッセージを転送する。最終的に、ＩＮＶＩＴＥメッセージは、図１の例示する実施形態では、呼び出し先ＳＩＰクライアント４０２のエッジプロキシサーバであるＳＩＰノード３００にルーティングされる。エッジプロキシサーバは、ネットワークの端部（ｅｄｇｅ）で実行されるように設計された、例えば、インターネットからローカルネットワークを分離する、プロキシサーバであることが可能である。エッジサーバ２５０と同様に、エッジプロキシサーバ３００は、ＶＩＡヘッダおよびＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをＩＮＶＩＴＥヘッダ５０４に挿入してから、そのメッセージをＳＩＰクライアント４０２に転送する。ＩＮＶＩＴＥ要求５００の中に挿入される、ＳＩＰノード２００のＶＩＡヘッダ５３０、ＳＩＰノード２５０のＶＩＡヘッダ５３２、およびＳＩＰノード３００のＶＩＡヘッダ５３４の例を、図３に示す。ＩＮＶＩＴＥメッセージ５００の中に挿入される、ＳＩＰノード２００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２０、ＳＩＰノード２５０のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２２、およびＳＩＰノード３００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２４の例を、図４に示す。
【００２２】
ボブのＳＩＰノード４０２は、ＩＮＶＩＴＥを受け入れることができ、ＩＮＶＩＴＥ要求に返信してＯＫ応答６００を送信することができる。図５は、ＳＩＰノード４０２からサーバ３００への典型的な応答６００を示す。ＳＩＰ標準の下では、応答６００の、ヘッダフィールドの多く、またはヘッダフィールドの少なくともいくつかの部分は、受信された要求からコピーされるか、またはエコーされる。それらのエコーされるヘッダ群には、例えば、ＳＩＰ標準の下における規定によれば、各ＶＩＡヘッダ、ＦＲＯＭヘッダ、ＴＯヘッダ、各ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ、Ｃａｌｌ－ＩＤヘッダ、およびＣＳｅｑヘッダが含まれることが可能である。このようにして、図５に示した応答６００は、エコーされるヘッダ群を例示する。具体的には、応答６００の中のＶＩＡヘッダ６０８、６３０、６３２、６３４が、呼び出し先ＳＩＰノード４０２によって受信されたＩＮＶＩＴＥ５００の中のＶＩＡヘッダ５０８、５３０、５３２、５３４と同一である。同様に、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２０、６２２、６２４は、ＳＩＰノード群によって生成され、呼び出し先ＳＩＰノード４０２によって受信されたＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２０、５２２、５２４と同一である。このため、応答メッセージは、ＶＩＡヘッダ６０８、６３０、６３２、６３４によって指示されるとおりにネットワークを経由して、呼び出し元ＳＩＰノード１０２にルーティングされる。
【００２３】
応答を処理するＳＩＰノード群、例えば、ＳＩＰノード３００、２５０、２００が、Ｖ

ＩＡヘッダ群の中に含まれるルーティング命令を検証することにより、応答が伝送される実際の経路の完全性を検証することができる。一実施形態では、ＳＩＰノードは、応答ＶＩＡヘッダ６０８、６３０、６３２を検証するのに後にアクセスし、使用するため、ＶＩＡヘッダ５０８、５３０、５３２などのルーティング情報をデータベースの中に格納することができる。代替として、ＳＩＰノードにかかるメモリ負荷およびアクセス負荷を減らすため、ＳＩＰノードは、メッセージの経路におけるネットワークルーティングロケーションを示すデータを含む少なくとも１つのヘッダの少なくとも一部分に基づき、署名を生成することができる。例えば、署名は、ネットワークルーティングロケーションを含むヘッダのすべてに基づくことも、ＵＲＩ、ＵＲＩパラメータ、ピアの「ＦＱＤＮ」（完全修飾ドメイン名）などの、ヘッダの一部分だけに基づくことも可能である。書名は、少なくとも１つのヘッダに加え、メッセージが次のホップ上で送信される接続の接続識別子、エコーされたヘッダ、ＴＯヘッダ、ＦＲＯＭヘッダ、ＣＯＮＴＡＣＴヘッダ、ＣＡＬＬ－ＩＤヘッダ、ＣＳｅｑヘッダ、およびＢｒａｎｃｈ－ＩＤを含め、他の情報にも基づくことが可能である。要求の少なくとも１つのヘッダの少なくとも一部分に基づく署名は、次に、応答に移され、その応答がＳＩＰノードによって処理される際に検証されることが可能である。あるヘッダ部分が署名の中に含められるべきか否かは、そのヘッダ部分が、ＳＩＰプロキシによって検証される前に変化するかどうかに依存することが可能である。例えば、署名の検証のためにアクセスされる前に削除される、または変更される可能性がある情報を含むヘッダ部分は、署名の中に含められるべきではない。ＳＩＰメッセージの経路におけるＳＩＰノードのいずれか、またはすべてが、本明細書で説明した形を含め、任意の適切な形で検証署名を生成し、格納することが可能であることを認識されたい。また、ＳＩＰメッセージのヘッダ群は、信頼されるリンクのリストを保持すること、署名に関するグローバルポリシーを遵守すること、特定のドメインへ／からのメッセージに対して署名／検証を行うことを含め、ネットワークおよびＳＩＰノード群のセキュリティ上の関心事および標準に従って、適宜、検証することができることも認識されたい。例えば、信頼されるリンクのリストを実施するため、各サーバが、信頼されると考えるリンクのリストを保持することができる。このため、信頼されるリンクに送られる／信頼されるリンクから来るメッセージには、署名／検証を行わなくてもよい。したがって、サーバは、リンクが信頼されない、すなわち、信頼されるリンクのリストの中にリストされていないことを確かめるために、信頼されるリンクのリストを調べてから、署名の生成／検証を行う。

【００２４】

一実施形態では、署名は、アクセス可能なセッションキーを使用して、要求メッセージの少なくとも１つのＶＩＡヘッダに基づいて生成されることが可能である。メッセージが伝送される経路を検証するため、ＳＩＰノードは、すべてのＶＩＡヘッダ、または少なくとも、ＳＩＰノードによって受信されたすべてのＶＩＡヘッダに基づいて、ＶＩＡ署名を生成することができる。例えば、図１および図２に示したＩＮＶＩＴＥメッセージ５００の場合、ＳＩＰノード２００は、ＳＩＰノード２００がアクセスできるセッションキーを使用することにより、ＳＩＰクライアント１０２（アリス）を指定する情報を含むＶＩＡヘッダ５０８に基づき、ＶＩＡ署名を提供することができる。生成されたＶＩＡ署名は、メッセージ内に格納され、応答メッセージに転送され、次に、ＳＩＰノード２００を介して、メッセージの帰路で検証されることが可能である。同様に、ＳＩＰノード３００は、受信されたＶＩＡヘッダに基づいてＶＩＡ署名を生成し、後に、応答がＳＩＰノード３００において受信された際に、応答を検証することができる。ＶＩＡヘッダ群に署名するのに、ＳＩＰノード３００は、アクセス可能なセッションキーを使用して、アリスのＶＩＡヘッダ５０８、ＳＩＰノード２００のＶＩＡヘッダ５３０、およびＳＩＰノード２５０のＶＩＡヘッダ５３２に基づき、ＶＩＡ署名を生成することができる。

【００２５】

ＶＩＡヘッダ群とその他のヘッダ情報の任意の適切な組合せに署名して、応答ヘッダ６０４内のルーティング命令を認証することができることを認識されたい。例えば、ＶＩＡ署名は、ＴＯヘッダ、ＦＲＯＭヘッダ、または要求ヘッダ５０４から応答ヘッダ６０４に

エコーされることが可能な他の任意のヘッダに加え、ＶＩＡヘッダの一部分に基づくことも可能である。さらに、要求ヘッダ５０４の中に挿入されるＶＩＡ署名５５０は、生成されたデジタル署名を示す任意のデータまたは信号であることも可能である。例えば、格納された署名５５０は、生成された署名ブラブ（ｂｌｏｂ）の所定の数の上位ビットであることも、デジタル署名全体であることも可能である。

【００２６】

ＩＮＶＩＴＥ要求の処理中に生成されたＶＩＡ署名がＳＩＰノードにおける応答の中に検証のために存在することを確実にするため、生成されたＶＩＡ署名は、ＩＮＶＩＴＥ要求のエコーされたヘッダの中に挿入することができる。例えば、署名は、標準のルーティングロケーション情報の後、ＵＲＩパラメータまたはヘッダパラメータとして挿入することができる。このため、クライアントＳＩＰノード４０２は、ＳＩＰ要求のエコーされるヘッダに基づいて応答ヘッダ群６０４を生成し、生成された署名は、要求から応答に自動的に移される。したがって、応答を受信したＳＩＰノードは、応答ヘッダに移された署名を検証することができる。先立つ合意に基づいてクライアントＳＩＰノードによってエコーされる、任意のエコーされたヘッダまたはカスタムヘッダが、ＳＩＰノードによる検証のために署名を格納するのに適する可能性があることを理解されたい。

【００２７】

図３に示すとおり、ＶＩＡ署名は、その署名を生成するＳＩＰノードのＶＩＡヘッダの中に挿入されることが可能である。例えば、ＳＩＰノード３００は、要求５００の中で受信されたＶＩＡヘッダ５０８、５３０、５３２に基づいてＶＩＡ署名５５０を生成することができる。ＳＩＰノード３００は、ＶＩＡ署名５５０をＳＩＰノード３００のＶＩＡヘッダ５３４の中に挿入することができる。前述したとおり、要求ヘッダ内のＶＩＡヘッダ群は、応答ヘッダ６０４内でエコーバックされる。このため、ＳＩＰノード４０２は、応答６００を形成する際、ＶＩＡヘッダ５３４内に含まれる情報を（図１）ＳＩＰノード３００のＶＩＡヘッダ６３４の中にコピーすることができる。標準のＳＩＰ処理の下では、ＶＩＡヘッダがエコーされる際、標準のＶＩＡ情報がコピーされるとともに、ＶＩＡ署名５５０などの任意の情報が、ヘッダパラメータとして付加される。

【００２８】

受信されたＶＩＡ署名６５０を検証するのに、ＳＩＰノード３００（図１）は、図５に示す受信されたＶＩＡ署名６５０を取り外し（ｓｔｒｉｐ）、保存することができる。ＳＩＰノード３００は、要求の中に挿入されるＶＩＡ署名５５０を生成するのに使用されたのと同一の手続きを使用して、検証ＶＩＡ署名を生成することができる。前述したＶＩＡ署名５５０の生成に従って、ＳＩＰノード３００は、受信された応答６００の中のＶＩＡヘッダ群を識別し、ＳＩＰノード３００のＶＩＡヘッダ５３４の下にリストされたすべてのＶＩＡヘッダに基づき、検証ＶＩＡ署名を生成することができる。このようにして、検証ＶＩＡ署名は、ＳＩＰノード３００が要求メッセージ５００の中のＶＩＡ署名５５０を生成した際にＳＩＰノード３００が知っているＶＩＡヘッダ群に基づくことが可能である。したがって、ＳＩＰノード３００に関する検証ＶＩＡ署名は、ＳＩＰノード２５０に関するＶＩＡヘッダ６３２、ＳＩＰノード２００に関するＶＩＡヘッダ６３０、および呼び出し元ＳＩＰノード１０２に関するＶＩＡヘッダ６０８に基づくことが可能である。ＳＩＰノード３００は、検証ＶＩＡ署名を受信されたＶＩＡ署名６５０と比較することができる。

【００２９】

署名が合致した場合、ＳＩＰノード３００は、ＳＩＰ標準の下で通常の処理を続け、応答ヘッダ群６０４のＶＩＡヘッダ群の中で示される次のＳＩＰノードにその応答を転送することができる。署名が合致しなかった場合、ＳＩＰノード３００は、処理スタックからその応答６００をドロップし、かつ／または、プロトコルによってサポートされている場合、ＳＩＰノード監視サービス（図示せず）または任意の適切な監視エージェントにエラーメッセージを送信することができる。署名の適合（ｃｏｍｐｌｉａｎｃｅ）および／または攻撃の検出に関するメッセージ処理パフォーマンスを測定するのに、ＳＩＰノード３

００は、メッセージが拒否されるたびに、署名失敗パフォーマンスカウンタを増分することができる。署名失敗パフォーマンスカウンタは、ＳＩＰノードがヘッダ署名を検証するのに失敗したことを示す、任意のデータまたは信号であることが可能である。例えば、署名失敗パフォーマンスカウンタは、ある期間内の失敗した署名検証の回数をカウントすることが可能である。次に、署名失敗パフォーマンスカウンタを、およそ１秒間のメッセージ処理時間中に、およそ６回の失敗した署名検証、およそ１０回の失敗した署名検証、またはおよそ２５回の失敗した署名検証などの、その期間に関する失敗した署名検証の所定の閾値と比較することができる。パフォーマンスカウンタが閾値を超えた場合、ＳＩＰノードは、人間のシステム管理者、および／またはコンピュータベースのシステムアドミニストレータに通知する、または警報する（電子メールおよび／またはページを介することを含め）ことができ、人間のシステム管理者および／またはコンピュータベースのシステムアドミニストレータは、例えば、失敗したメッセージをルーティングしているネットワークをドロップすること、ネットワークをロックすること、および／またはメッセージキュー（ｑｕｅｕｅ）をフラッシュする（ｆｌｕｓｈ）ことを含め、パフォーマンスカウンタに基づく所定のアクションを開始することができる。

【００３０】

一部のケースでは、署名は、経路の各ステップにおいて、例えば、要求および／または帰路上の応答を処理する各ＳＩＰノードにおいて生成され、かつ／または検証されることが可能である。ただし、ＳＩＰノードサーバ群にかかる計算上の負担を軽減するため、メッセージは、要求される場合にだけ検証してもよい。

【００３１】

例えば、要求が、１つのＶＩＡヘッダ、例えば、要求５００の中のアリスのＳＩＰノード１０２のＶＩＡヘッダ５０８だけを含む場合、そのノードにおいて署名がまったく生成されなくてもよい。詳細には、アリスのＳＩＰノード１０２は、応答６００の中でまったくルーティング命令を検証しなくてもよい。というのは、この応答は、ＳＩＰノード１０２によって消費される、例えば、さらなる転送が行われないからである。このため、要求が１つのＶＩＡヘッダだけを含む場合、ＶＩＡ署名がまったく生成されなくてもよく、これに対応して、受信された要求が１つだけのＶＩＡヘッダ、例えば、受信側ＳＩＰノードのＶＩＡヘッダだけを含む場合、ＶＩＡ署名は、まったく検証されなくてもよい。

【００３２】

さらなる例では、メッセージが信頼されない接続を介して受信された場合、サービス拒否攻撃の可能性がより高い可能性がある。メッセージのセキュリティを向上させるため、メッセージは、信頼されない接続を介して受信された場合、検証することができる。例えば、信頼されない接続には、あらゆるサーバタイプに関するあらゆるクライアント接続が含まれることが可能である。というのは、他のサーバ群から受信されたメッセージは、他の方法で認証される可能性があるからである。また、信頼されない接続には、エッジプロキシサーバに関する外部サーバ接続も含まれることが可能であり、より詳細には、すべての外部サーバ接続が含まれることが可能である。

【００３３】

図１に示すとおり、ＳＩＰノード２００とＳＩＰノード２５０の間の接続２１０、２１２は、信頼される接続である。というのは、これらの接続は、ホームサーバとエッジサーバの間の内部リンクと考えることができるからである。サーバ群は、サーバ間でメッセージトラフィックを認証する他の方法を有する可能性があるため、ＳＩＰノード２５０とＳＩＰノード３００の間のリンク２６０、２６２は、信頼される接続である可能性がある。しかし、これらのリンクは、一部のケースでは、特に、他のサーバ認証方法が十分であると考えられない場合、信頼されないと考えることができる。クライアントノード４０２とＳＩＰノード３００の間のリンク３１０、３１２は、信頼されない接続である可能性がある。というのは、ＳＩＰメッセージは、クライアントＳＩＰノードに、またはクライアントＳＩＰノードから送信されるからである。したがって、リンク３１２などの、信頼されない接続を介して受信される、あらゆるメッセージトラフィックは、ＳＩＰノードにおい

て検証して、メッセージの完全性および／または真正性を検証することができる。

【００３４】

信頼されたリンクを介して受信された応答が検証されない場合、要求が信頼されたリンクを介して次のＳＩＰノードに転送される際、ＶＩＡ署名は、生成されなくてもよい。例えば、ＳＩＰノード２００および２５０は、信頼されない接続を介して応答６００を受信する必要がなく、したがって、これらのノードは、ＩＮＶＩＴＥ要求のヘッダ群５０４の中にＶＩＡ署名を生成または格納しなくてもよい。というのは、これらのノードは、応答の経路を検証する要件をまったく有さない可能性があるからである。したがって、ＶＩＡ署名を生成する前に、ＳＩＰノードは、対応する応答の検証が要求されるかどうかを判定することができる。応答を検証する必要がない場合、例えば、次のリンクが信頼される接続である場合、ＶＩＡ署名は、まったく生成する必要がなく、ＳＩＰ要求の通常の処理を続けることができる。しかし、対応する応答が、信頼されない接続を介してＳＩＰノードにおいて受信される場合は、前述したとおり、ＶＩＡ署名を生成することができる。同様に、応答を受信した後、ＳＩＰノードはまず、その応答が信頼されない接続から受信されたかどうかを判定することができる。信頼されない接続から受信された場合、ＶＩＡ署名を、この署名が存在する場合、検証することができる。例えば、ＳＩＰノード３００は、応答６００が信頼されない接続を介して受信されたかどうかを判定することができる。図１に示すとおり、リンク３１２は、信頼されない接続である。この結果、ＳＩＰノード３００は、応答のヘッダ６０４内のＳＩＰノード３００のＶＩＡヘッダ６３４を識別することができる。ＳＩＰノード３００は、識別されたＶＩＡヘッダ６３４内に署名が存在するかどうかを判定することができる。ＶＩＡ署名が存在しない場合、ＳＩＰノード３００は、プロトコルによって許される場合、エラーメッセージを送信することができ、処理スタックからメッセージをドロップすることができ、署名失敗パフォーマンスカウンタを増分することができ、かつ／または他の任意の適切なアクションを行うことができる。図５に示すとおり、ＶＩＡ署名６５０が存在する場合、ＳＩＰノード３００は、前述したとおり、その署名を検証することができる。

【００３５】

ＶＩＡヘッダ群に署名することは、前述したとおり、応答ヘッダ６０４内のルーティング命令の完全性を検証するのに役立つ可能性がある。しかし、ＳＩＰノードは、さらに、または代替として、呼び出し先によって生成された要求に関するルーティング命令の検証を望む可能性がある。したがって、ＳＩＰノードは、ダイアログ開始要求のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの少なくとも１つの少なくとも一部分に基づいて署名を生成し、次に、呼び出し先からの後の要求の中でその署名を検証して、ダイアログ内（ｉｎ－ｄｉａｌｏｇ）要求のルーティング命令の完全性を確実にすることができる。

【００３６】

呼び出し先要求が伝送される経路の完全性を確実にするため、ＳＩＰノードは、要求の受信されたヘッダフィールド内に含まれるＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群およびＣＯＮＴＡＣＴヘッダのＵＲＩ部分に基づき、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名を生成することができる。複数のＣＯＮＴＡＣＴヘッダが存在する場合、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群の選択されたＵＲＩ部分、および最初にリストされたＣＯＮＴＡＣＴヘッダのＵＲＩ部分に基づくことが可能である。より詳細には、図１、図２、および図４に示したＩＮＶＩＴＥメッセージ５００の場合、ＳＩＰノード３００は、ＳＩＰノード２５０のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２２のＵＲＩ部分、ＳＩＰノード２００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２０のＵＲＩ部分、および呼び出し元であるアリスのＣＯＮＴＡＣＴヘッダ５１８のＵＲＩ部分に基づき、ＲＯＵＴＥ　ＳＥＴ署名を提供することができる。生成された呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、同一のダイアログに属する呼び出し先ＳＩＰノード４０２によって生成されたあらゆる要求内に格納し、使用するために、メッセージ内に格納され、呼び出し先ＳＩＰノード４０２に転送されることが可能である。ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダと他のヘッダ情報の任意の適切な組合せに署名を行い、呼び出し先ＳＩＰノード４０２によって生成される

あらゆる後続の要求に関するルーティング命令を認証することができることを認識されたい。要求ヘッダ５０４の中に挿入される呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、署名ブラブの所定の数の上位ビット、およびデジタル署名全体を含め、生成された署名を示す任意のデータまたは信号であることが可能である。

【００３７】

要求の処理中に生成された呼び出し先ＲＯＵＴＥ　ＳＥＴ署名が、呼び出し元ＳＩＰノード４０２によって生成された後続の要求の中に検証のために存在することを確実にするため、生成された呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、要求のエコーされるヘッダの中に挿入することができる。このため、クライアントＳＩＰノード４０２が、ＳＩＰダイアログ開始要求のエコーされるヘッダ群に基づいて新たな要求を生成すると、生成された署名は、自動的に転送される。したがって、要求を受信したＳＩＰノードは、要求ヘッダに移された署名を検証することができる。先立つ合意に基づいてクライアントＳＩＰノードによってエコーバックされることが可能な任意のエコーされるヘッダ部分またはカスタムヘッダ部分が、ＳＩＰノードによる検証のために呼び出し先ＲＯＵＴＥ　ＳＥＴ署名を格納するのに適する可能性があることを認識されたい。

【００３８】

図２および図４に示すとおり、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、ＵＲＩパラメータとして、署名を生成したＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入することができる。例えば、ＳＩＰノード３００は、要求５００の中のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２２、５２０、およびＣＯＮＴＡＣＴヘッダ５１８のＵＲＩ部分に基づいて呼び出し先ＲＯＵＴＥ　ＳＥＴ署名５６０を生成することができる。ＳＩＰノード３００は、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名５６０をＵＲＩパラメータとして、ＳＩＰノード３００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２４の中に挿入することができる。前述したとおり、呼び出し元からのダイアログ開始要求のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群およびＣＯＮＴＡＣＴヘッダのＵＲＩ部分が、呼び出し先ＳＩＰノードによってＲＯＵＴヘッダ群の中に格納され、エコーされて、ダイアログ内の呼び出し先によって生成されたあらゆる将来の要求に関するルーティング命令が提供される。このため、図６に示すとおり、ＳＩＰノード４０２は、要求を形成する際、標準のＳＩＰ処理の下で、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２４のＵＲＩ部分をＳＩＰノード３００のＲＯＵＴＥヘッダ７２４の中にコピーすることができる。ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのＵＲＩ部分がエコーされると、標準の経路情報がコピーされるとともに、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名５６０を含むあらゆるＵＲＩパラメータもコピーされる。

【００３９】

図６の受信された呼び出し先ＲＯＵＴＥ　ＳＥＴ署名７６０を検証するため、ＳＩＰノード３００は、受信された呼び出し先ＲＯＵＴＥ　ＳＥＴ署名７６０を取り外し、保存することができる。ＳＩＰノード３００は、この場合、ＩＮＶＩＴＥであるダイアログ作成要求の中に挿入される呼び出し先ＲＯＵＴＥ　ＳＥＴ署名５６０を生成するのに使用されたのと同一の手続きを使用して、検証ＲＯＵＴＥ　ＳＥＴ署名を生成することができる。前述した呼び出し先ＲＯＵＴＥ　ＳＥＴ署名５６０の生成に従って、ＳＩＰノード３００は、受信された要求７００の中でＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを識別し、受信側ＳＩＰノードのＲＯＵＴＥヘッダを除き、要求の中に存在するすべてのＲＯＵＴＥヘッダに基づいて検証ＲＯＵＴＥ　ＳＥＴ署名を生成することができる。このようにして、検証ＲＯＵＴＥ　ＳＥＴ署名は、ＳＩＰノード３００が要求メッセージ５００の中で呼び出し先ＲＯＵＴＥ　ＳＥＴ署名５６０を生成した際に、ＳＩＰノード３００が知っているＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群およびＣＯＮＴＡＣＴヘッダに基づくことが可能である。例えば、図１のセットアップにおいて、ＳＩＰノード３００の検証ＲＯＵＴＥ　ＳＥＴ署名は、ＳＩＰノード２５０のＲＯＵＴＥヘッダ７２２、ＳＩＰノード２００のＲＯＵＴＥヘッダ７２０、ならびに呼び出し元ＳＩＰノード１０２を識別するＣＯＮＴＡＣＴヘッダに基づくＲＯＵＴＥヘッダ７１８に基づくことが可能である。ＳＩＰノード３００は、検証ＲＯＵＴＥ　ＳＥＴ署名を受信された呼び出し先ＲＯＵＴＥ　ＳＥＴ署名７６０と比較する

ことができる。署名が合致しなかった場合、ＳＩＰノード３００は、プロトコルによって許される場合、エラーメッセージを送信し、処理スタックから要求７００を削除し、署名失敗パフォーマンスカウンタを増分し、かつ／または他の任意の適切なアクションを行うことができる。署名が合致した場合、ＳＩＰノード３００は、ＳＩＰ標準の下で通常の処理を続け、要求ヘッダ群７０４のＲＯＵＴＥヘッダ群の中で示される次のＳＩＰノードに要求を転送することができる。

【００４０】

一部のケースでは、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、経路の各ステップにおいて、例えば、要求を処理する各ＳＩＰノードにおいて生成され、かつ／または検証されることが可能である。ただし、ＳＩＰノードサーバ群にかかる計算上の負担を軽減するため、要求は、必須の場合にだけ検証してもよい。

【００４１】

例えば、要求がＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをまったく含まない場合、例えば、現在、処理を行っているＳＩＰノードさえ、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを追加していない場合、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、生成されなくてもよい。より詳細には、要求を処理しているＳＩＰノードが、呼び出し先と呼び出し元の間のさらなる通信のために「ループに入った」ままになることを要求していない場合、ＳＩＰノードは、将来に受信されるメッセージの中のルーティング情報を検証することを望まない可能性がある。

【００４２】

さらなる例では、要求がＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群を含むが、１つのＣＯＮＴＡＣＴヘッダも含まない場合、ＳＩＰノードは、それらのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをエコーするいずれの応答または要求も検証することを望まない可能性がある。これは、一部のタイプのＡＣＫメッセージおよびＣＡＮＣＥＬ　ＳＩＰメッセージを含む、一部のケースで生じる可能性がある。より詳細には、受信された要求が、少なくとも１つのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを含み、ＣＯＮＴＡＣＴヘッダをまったく含まない場合、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、生成されなくてもよく、メッセージの通常の処理が続けられることが可能である。

【００４３】

追加の例では、メッセージは、信頼されない接続を介して受信された場合に検証されることが可能である。というのは、信頼されないリンクからの要求は、サービス拒否攻撃のソースである可能性がより高い可能性があるからである。信頼されるリンクを介して受信された呼び出し先からの要求が検証されない場合、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名５６０は、呼び出し元からのダイアログ開始要求が信頼されるリンクを介して次のＳＩＰノードに転送される際は、生成されなくてもよい。例えば、図１に示すとおり、ＳＩＰノード２００は、信頼される接続を介して要求７００を受信する、つまり、ＳＩＰノードは、信頼されない接続を介して要求７００を受信しない。したがって、このノードは、ＩＮＶＩＴＥ要求のヘッダ群５０４の中で呼び出し先ＲＯＵＴＥ　ＳＥＴ署名を生成または挿入しなくてもよい。というのは、このノードは、呼び出し先からのいずれの要求の経路を検証する要件も有さない可能性があるからである。このため、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名を生成する前に、ＳＩＰノードは、呼び出し先要求の検証が要求されるかどうかを判定することができる。呼び出し先要求が検証されない場合、例えば、現在の要求が、信頼される接続を介して受信される場合、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、まったく生成されなくてもよく、ＳＩＰ要求の通常の処理が続けられることが可能である。しかし、呼び出し先要求が、信頼されない接続を介してＳＩＰノードで受信される場合は、前述したとおり、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名が生成されることが可能である。同様に、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名の検証中、処理を行うＳＩＰノードはまず、呼び出し先から受信された要求が信頼されない接続を介してであるかどうかを判定することができる。信頼されない接続を介してである場合、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名を、この署名が存在する場合、検証することができる。例えば、ＳＩＰノード３００は、要求７００が信頼されない接続を介して受信されたかどうかを判定することができる。図１に示

すとおり、リンク３１２は、信頼されない接続である。この結果、ＳＩＰノード３００は、図６に示した要求７００のヘッダ７０４内で、ＳＩＰノード３００のＲＯＵＴＥヘッダ７２４を識別することができる。ＳＩＰノード３００は、識別されたＲＯＵＴＥヘッダ７２４内に署名が存在するかどうかを判定し、存在する場合、その署名を検証することができる。

【００４４】

ＳＩＰノードは、さらに、または代替として、ダイアログ開始要求の後に呼び出し元によって生成されたダイアログ内要求に関するルーティング命令の検証を望むことも可能である。したがって、ＳＩＰノードは、ダイアログ開始要求に対する応答のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの少なくとも１つの少なくとも一部分に基づいて署名を生成し、次に、呼び出し元からの後続の要求の中でその署名を検証して、要求のルーティング命令の完全性を確実にすることができる。

【００４５】

呼び出し元要求が伝送される経路の完全性を確実にするため、ＳＩＰノードは、受信された応答のヘッダフィールドの中に含まれるＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群およびＣＯＮＴＡＣＴヘッダのＵＲＩ部分に基づき、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名を生成することができる。複数のＣＯＮＴＡＣＴヘッダが存在する場合、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名は、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群の選択されたＵＲＩ部分、および最初にリストされたＣＯＮＴＡＣＴヘッダのＵＲＩ部分に基づくことが可能である。より詳細には、図１および図５に示した応答メッセージ６００の場合、ＳＩＰノード２００は、ＳＩＰノード２５０のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２２のＵＲＩ部分、ＳＩＰノード３００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２４のＵＲＩ部分、および呼び出し先であるボブのＣＯＮＴＡＣＴヘッダ６１８のＵＲＩ部分に基づき、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名を提供することができる。生成された呼び出し元ＲＯＵＴＥ　ＳＥＴ署名は、同一のダイアログの中に属する呼び出し元ＳＩＰノード１０２によって生成されたあらゆる要求内に格納し、使用するために、メッセージの中に格納され、呼び出し元ＳＩＰノード１０２に転送されることが可能である。ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群と他のヘッダ情報の任意の適切な組合せに署名して、呼び出し元ＳＩＰノード１０２によって生成される、あらゆる後続の要求の中のルーティング命令を認証することができることを認識されたい。応答ヘッダ６０４の中に挿入される呼び出し元署名は、署名ブラブの所定の数の上位ビット、およびデジタル署名全体を含め、生成されたデジタル署名を示す任意のデータまたは信号であることが可能である。

【００４６】

応答の処理中に生成された呼び出し元ＲＯＵＴＥ　ＳＥＴ署名が、呼び出し元ＳＩＰノード１０２によって生成された後続の要求の中に検証のために存在することを確実にするため、生成された呼び出し元ＲＯＵＴＥ　ＳＥＴ署名は、ＵＲＩパラメータとして応答のエコーされるヘッダの中に挿入することができる。このため、クライアントＳＩＰノード１０２が、ＳＩＰ応答のエコーされるヘッダ群に基づいて新たな要求を生成すると、生成された署名は、自動的に転送される。したがって、要求を受信したＳＩＰノードは、要求ヘッダに移された署名を検証することができる。先立つ合意に基づいてクライアントＳＩＰノードによってエコーバックされる任意のエコーされるヘッダ部分またはカスタムヘッダが、ＳＩＰノードによる検証のために呼び出し元ＲＯＵＴＥ　ＳＥＴ署名を格納するのに適する可能性があることを認識されたい。

【００４７】

図５に示すとおり、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名が、その署名を生成したＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入されることが可能である。例えば、ＳＩＰノード２００は、応答６００の中のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２２、６２４、およびＣＯＮＴＡＣＴヘッダ６１８のＵＲＩ部分に基づき、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名６６０を生成することができる。ＳＩＰノード２００は、ＳＩＰノード２００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２０の中にＲＯＵＴＥ　ＳＥＴ署名６６０を挿入す

ることができる。前述したとおり、ダイアログ開始要求に対する応答のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群およびＣＯＮＴＡＣＴヘッダのＵＲＩ部分は、呼び出し元ＳＩＰノードによってＲＯＵＴＥヘッダ群の中に格納され、エコーされて、ダイアログ内の呼び出し元によって生成される、将来のあらゆる要求に関するルーティング命令を提供する。このため、図７の典型的な要求８００に示すとおり、ＳＩＰノード１０２は、そのダイアログの中で後続の要求を形成する際、標準のＳＩＰ処理の下でＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２０のＵＲＩ部分をＳＩＰノード２００のＲＯＵＴＥヘッダ８２０の中にコピーすることができる。ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのＵＲＩ部分がエコーされると、標準の経路情報がコピーされるとともに、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名６６０を含むあらゆるＵＲＩパラメータもコピーされる。

【００４８】

図７の受信された呼び出し元ＲＯＵＴＥ　ＳＥＴ署名８６０を検証するため、ＳＩＰノード２００は、図７に示す受信された呼び出し元ＲＯＵＴＥ　ＳＥＴ署名８６０を取り外し、保存することができる。ＳＩＰノード２００は、ダイアログ作成要求の中に挿入される呼び出し元ＲＯＵＴＥ　ＳＥＴ署名６６０を生成するのに使用されたのと同一の手続きを使用して、検証ＲＯＵＴＥ　ＳＥＴ署名を生成することができる。前述した呼び出し元ＲＯＵＴＥ　ＳＥＴ署名６６０の生成に従って、ＳＩＰノード２００は、受信された要求８００の中でＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを識別し、受信側ＳＩＰノードのＲＯＵＴＥヘッダを除き、要求の中に存在するすべてのＲＯＵＴＥヘッダに基づいて検証ＲＯＵＴＥ　ＳＥＴ署名を生成することができる。このようにして、検証ＲＯＵＴＥ　ＳＥＴ署名は、ＳＩＰノード２００が応答メッセージ６００の中で呼び出し元ＲＯＵＴＥ　ＳＥＴ署名６６０を生成した際に、ＳＩＰノード２００が知っているＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群およびＣＯＮＴＡＣＴヘッダに基づくことが可能である。したがって、ＳＩＰノード２００に関する検証ＲＯＵＴＥ　ＳＥＴ署名は、ＳＩＰノード２５０のＲＯＵＴＥヘッダ８２２、ＳＩＰノード３００のＲＯＵＴＥヘッダ８２４、ならびに呼び出し先ＳＩＰノード４０２を識別するＣＯＮＴＡＣＴヘッダに基づくＲＯＵＴＥヘッダ８１８に基づく。ＳＩＰノード２００は、検証ＲＯＵＴＥ　ＳＥＴ署名を受信された呼び出し元ＲＯＵＴＥ　ＳＥＴ署名８６０と比較することができる。署名が合致しなかった場合、ＳＩＰノード２００は、プロトコルによってサポートされる場合、エラーメッセージを送信し、処理スタックから要求８００を削除し、署名失敗パフォーマンスカウンタを増分し、かつ／または他の任意の適切なアクションを行うことができる。署名が合致した場合、ＳＩＰノード２００は、ＳＩＰ標準の下で通常の処理を続け、要求ヘッダ群８０４のＲＯＵＴＥヘッダ群の中で示される次のＳＩＰノードに要求を転送することができる。

【００４９】

一部のケースでは、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名は、経路の各ステップにおいて、例えば、応答および／または要求をそれぞれ処理する各ＳＩＰノードにおいて生成され、かつ／または検証されることが可能である。ただし、要求の中に挿入されるＶＩＡ署名およびＲＯＵＴＥ　ＳＥＴ署名に関連して前述したとおり、ＳＩＰノードサーバ群にかかる計算上の負担は、必須の場合にだけ、要求の中で呼び出し元ＲＯＵＴＥ　ＳＥＴ署名の検証を要求することにより、軽減することができる。

【００５０】

例えば、要求に対する応答がＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをまったく含まない場合、例えば、現在のＳＩＰノードさえ、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを追加していない場合、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名は、生成されなくてもよい。より詳細には、応答を処理しているＳＩＰノードが、呼び出し先と呼び出し元の間のさらなる通信のために「ループに入った」ままになることを要求していない場合、ＳＩＰノードは、将来のメッセージの中のルーティング情報を検証することを望まない可能性がある。

【００５１】

さらなる例では、応答がＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群を含むが、１つのＣＯＮＴＡＣＴヘッダも含まない場合、ＳＩＰノードは、それらのＲＥＣＯＲＤ－ＲＯＵＴＥヘッ

ダをエコーするいずれの応答または要求の検証も望まない可能性がある。より詳細には、受信された応答が少なくとも１つのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを含み、ＣＯＮＴＡＣＴヘッダをまったく含まない場合、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名は、生成されなくてもよく、通常の処理が続けられることが可能である。

【００５２】

追加の例では、呼び出し元要求のＲＯＵＴＥ　ＳＥＴヘッダ群は、信頼されない接続を介して受信された場合にだけ検証されることが可能である。信頼されるリンクを介して受信された要求が検証されない場合、応答が信頼されるリンクを介して次のＳＩＰノードに転送される際、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名６６０が生成される必要はない。同様に、呼び出し元から要求を受信した後、ＲＯＵＴＥ　ＳＥＴ署名は、信頼される接続を介して受信された場合、検証されなくてもよい。

【００５３】

前述したとおり、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群は、ダイアログ開始要求、および対応する応答の中に含まれて、後続の要求をルーティングするのに使用される呼び出し先ＲＯＵＴＥ　ＳＥＴヘッダおよび呼び出し元ＲＯＵＴＥ　ＳＥＴヘッダを生成する。このため、一部のケースでは、ＳＩＰノードは、ダイアログ開始要求に対する応答の中のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを検証して、それらのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの完全性を確実にすることができる。例えば、接続する（ａｔｔａｃｈｉｎｇ）ノードが要求の中のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群を改ざんする可能性があり、その結果、後続のＳＩＰノードが、不正なＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群全体に署名し、有効なＲＯＵＴＥ　ＳＥＴ署名を有するが、不正なルーティング情報に基づくＲＯＵＴＥヘッダを生じさせる可能性がある。したがって、ＳＩＰノードは、要求のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの少なくとも１つの少なくとも一部分に基づいて署名を生成し、次に、呼び出し先からの応答の中でその署名を検証して、メッセージのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群の完全性を確実にすることができる。

【００５４】

ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのセットの完全性を確実にするため、ＳＩＰノードは、受信された要求のヘッダフィールドに含まれるＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群のＵＲＩ部分に基づき、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名を生成することができる。より詳細には、図１、図２、および図４に示したＩＮＶＩＴＥメッセージ５００の場合、ＳＩＰノード３００は、ＳＩＰノード２５０のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２２のＵＲＩ部分、およびＳＩＰノード２００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２０のＵＲＩ部分に基づいてＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０を提供することができる。前述した呼び出し先ＲＯＵＴＥ　ＳＥＴ署名とは異なり、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０は、ＣＯＮＴＡＣＴヘッダを含まない。というのは、呼び出し先は、ＳＩＰ標準の下では、応答の中でＣＯＮＴＡＣＴヘッダ５１８をエコーしないからである。生成されたＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０は、メッセージ内に格納され、応答メッセージに移され、応答がＳＩＰノードを介して処理される際に検証されることが可能である。ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群と他のヘッダ情報の任意の適切な組合せに署名を行い、呼び出し先ＳＩＰノード４０２によって生成された応答の中でルーティング命令を認証することができることを認識されたい。要求ヘッダ５０４の中に挿入されるＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０は、署名ブラブの所定の数の上位ビット、およびデジタル署名全体を含め、生成されたデジタル署名を示す任意のデータまたは信号であることが可能である。

【００５５】

要求の処理中に生成されたＲＥＣＯＲＤ－ＲＯＵＴＥ署名が、呼び出し先ＳＩＰノード４０２によって生成された応答の中に検証のために存在することを確実にするため、生成されたＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０は、ヘッダパラメータまたはＵＲＩパラメータとして、要求のエコーされるヘッダの中に挿入することができる。このため、クライアントＳＩＰノード４０２がＳＩＰ要求からのエコーされるヘッダに基づいて応答を生成すると、生成された署名は、要求から応答に自動的に移される。したがって、応答を受信し

たＳＩＰノードは、応答ヘッダに移された署名を検証することができる。先立つ合意に基づいてクライアントＳＩＰノードによってエコーされる任意のエコーされるヘッダまたはカスタムヘッダが、ＳＩＰノードによる検証のためにＲＥＣＯＲＤ－ＲＯＵＴＥ署名を格納するのに適する可能性があることを認識されたい。

【００５６】

図４に示すとおり、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名は、その署名を生成したＳＩＰノードのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入することができる。例えば、ＳＩＰノード３００は、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０をヘッダパラメータとして、ＳＩＰノード３００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２４の中に挿入することができる。前述したとおり、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群は、応答ヘッダ群６０４の中でエコーバックされる。このため、ＳＩＰノード４０２は、図５に示した応答６００のような応答を形成する際、標準のＳＩＰ処理の下で、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５２４をＳＩＰノード２００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２４にコピーすることができる。ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダがエコーされると、標準の情報とならび、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０を含むあらゆるヘッダパラメータもコピーされる。

【００５７】

図５の受信されたＲＥＣＯＲＤ－ＲＯＵＴＥ署名６７０を検証するのに、ＳＩＰノード３００は、受信されたＲＥＣＯＲＤ－ＲＯＵＴＥ署名６７０を取り外し、保存することができる。ＳＩＰノード３００は、この場合、ＩＮＶＩＴＥである、対応する要求の中に挿入されるＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０を生成するのに使用されたのと同一の手続きを使用して、検証ＲＥＣＯＲＤ－ＲＯＵＴＥ署名を生成することができる。前述したＲＥＣＯＲＤ－ＲＯＵＴＥ署名５７０の生成に従って、ＳＩＰノード３００は、ＳＩＰノード２５０のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２２のＵＲＩ部分、およびＳＩＰノード２００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ６２０のＵＲＩ部分に基づき、検証ＲＥＣＯＲＤ－ＲＯＵＴＥ署名を生成することができる。ＳＩＰノード３００は、検証ＲＥＣＯＲＤ－ＲＯＵＴＥ署名を受信されたＲＥＣＯＲＤ－ＲＯＵＴＥ署名６７０と比較することができる。署名が合致しなかった場合、ＳＩＰノード３００は、プロトコルによってサポートされる場合、エラーメッセージを送信し、処理スタックから応答６００を削除し、かつ／または署名失敗パフォーマンスカウンタを増分することができる。署名が合致した場合、ＳＩＰノード３００は、ＳＩＰ標準の下で通常の処理を続け、応答ヘッダ群６０４のＶＩＡヘッダ群の中で示される次のＳＩＰノードに応答を転送することができる。

【００５８】

一部のケースでは、応答のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群は、経路の各ステップにおいて、例えば、応答を処理する各ＳＩＰノードにおいて検証されることが可能である。ただし、ＳＩＰノード群にかかる計算上の負担を軽減するため、応答は、ＶＩＡ署名６５０に関連して前述したのと同様に、要求される場合にだけ検証することもできる。例えば、要求がＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをまったく含まない場合、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名は、生成されなくてもよい。追加の例では、次のＳＩＰノードへの接続が信頼される接続である場合、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名は、生成されなくてもよい。通信システムにかかる負担を軽減するため、ＳＩＰノードは、検証後、応答を次のＳＩＰノードに転送する前に、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダからＲＥＣＯＲＤ－ＲＯＵＴＥ署名を削除することもできる。

【００５９】

ＳＩＰメッセージの中のヘッダ群の少なくとも一部分に基づいて署名を生成するのに、検証能力および検証能力を要するＳＩＰノードは、中央処理装置上で実行されて、暗号化、解読、署名、および／または検証を含む、いくつかの暗号機能を実行する暗号化プログラムを含むことが可能である。例として、暗号化プログラムは、署名を計算する際にランダムなデータを追加するのに使用される、または暗号化／解読の目的で使用される対称キーなどの、暗号化キーを生成すること、および破壊することができることが可能である。代替として、暗号化プログラムは、非対称（公開／秘密）キーペアにアクセスすることが

できる。通常の非対称キーペアでは、公開キーは、情報を暗号化するのに使用することができ、対応する秘密キーは、情報を解読するのに使用することができる。秘密キーを使用してデジタル署名が生成されることが可能であり、その署名が、公開キーを使用して認証されることが可能である。攻撃に対する強度（ｒｅｓｉｌｉｅｎｃｅ）、相対的な速度、および関連する署名の生成に関する計算上の負担などの、多くの要因に基づき、ＭＤ５、ソルト（ｓａｌｔ）、ＨＭＡＣ、ＳＨＡ１、およびＲＳＡを単独で、または組合せで含む任意の一方向ハッシュ機構が、ＳＩＰヘッダ群に基づいて署名を生成するのに適する可能性があることを認識されたい。また、署名ブラブ全体、署名ブラブの部分、または任意の符号化スキームを使用する署名ブラブの符号化されたバージョンを、ＶＩＡ署名、ＲＥＣＯＲＤ　ＳＥＴ署名、および／またはＲＥＣＯＲＤ－ＲＯＵＴＥ署名として挿入することができることも認識されたい。一例では、署名は、ＳＩＰメッセージヘッダ群の選択された部分と、乱数および／またはセッションキーを含む他の任意の情報との１６バイトの一方向ＭＤ５ハッシュであることが可能である。ＳＩＰヘッダ群に基づく署名は、署名の生成と検証の間で順序に整合性が保たれる限り、妥当なヘッダを任意の特定の順序にして生成することができる。

【００６０】

同一のＳＩＰノードによって処理されるＶＩＡ署名、ＲＯＵＴＥ　ＳＥＴ署名、およびＲＥＣＯＲＤ－ＲＯＵＴＥ署名はそれぞれ、同一のセッションキーで生成されることが可能である。代替として、各署名、または署名の任意の組合せに関して、異なる強度、および異なる速度のキーを使用してもよい。例えば、ＶＩＡ署名および／またはＲＥＣＯＲＤ－ＲＯＵＴＥ署名は、例えば、対応する応答において、通常、かなり迅速に検証されるので、ＶＩＡ署名を生成するのに使用されるＶＩＡキーは、かなり小さい計算上の負担を伴う、かなり軽量のキー／暗号化ソリューションであることが可能である。しかし、ＲＯＵＴＥ　ＳＥＴヘッダは、ダイアログ全体を通じて検証されつづける可能性があるため、ＲＯＵＴＥ　ＳＥＴキーは、軽量のキー／暗号化ソリューションと比べてそれほど攻撃に対して脆弱でない重量のキー／暗号化ソリューションであることが可能である。

【００６１】

署名を生成するためのセッションキー自体、特定のＳＩＰノードによってある時間枠の中で処理されるすべてのダイアログ要求および／または応答に関して生成され、使用されることが可能である。代替として、各ダイアログに、特定のセッションキーが発行されることが可能であり、セッションキーは、そのＳＩＰノードによって使用される他のダイアログセッションキーと同一であることも、異なることも可能であり、他のＳＩＰノードによって使用されるダイアログセッションキーと同一であることも、異なることも可能である。セッションキーは、所定の期間の後、ダイアログの終了時に、および／またはキーおよび／またはヘッダの破損の指示を受け取ると、暗号化プログラムによって破壊されることが可能である。

【００６２】

各ＳＩＰノードは、ＶＩＡ署名を生成するためのＶＩＡキー、ＲＯＵＴＥ　ＳＥＴヘッダを生成するためのＲＯＵＴＥキー、およびＲＥＣＯＲＤ－ＲＯＵＴＥ署名を生成するためのＲＥＣＯＲＤ－ＲＯＵＴＥキーなどの、独自のセッションキーを生成することができる。代替として、セッションキーには、公開キー／秘密キーペアに関する証明書などを介して、ＳＩＰノードのそれぞれがアクセスできて、各タイプのヘッダに同一のキーを使用して署名が行われることも可能である。

【００６３】

署名を生成するのに使用されるセッションキーの脆弱性を小さくするため、キーをときどきリフレッシュすることができる。例えば、セッションキーは、４時間毎にリフレッシュすることができる。ただし、セッションキーがリフレッシュされた後にダイアログが続けられることを可能にすることを確実にするため、ＳＩＰノードの暗号化プログラムは、以前のセッションキーを格納し、保持することができる。格納されたキーは、ＲＥＣＯＲＤ－ＲＯＵＴＥキーおよびＲＯＵＴＥ　ＳＥＴキーの場合、およそ５分間からおよそ２４

時間の範囲内で、ＶＩＡキーの場合、およそ５分間からおよそ３０分間の範囲内でなど、所定の期間にわたって格納されることが可能である。さらに、または代替として、セッションキーは、そのキーを使用して署名されたすべてのメッセージが検証されるまで保存することができる。署名を検証するのに正しいキーにアクセスが行われることを確実にするため、暗号化プログラムは、キー識別子を署名の中に挿入すること、および／またはキー識別子を符号化されたＳＩＰヘッダ内に追加のパラメータとして付加することができる。

【００６４】

一部のケースでは、ＳＩＰメッセージを処理するＳＩＰノードは、サーバのプールによって提供される可能性がある。しかし、署名を検証するのと同一のサーバが、署名を生成したのと同一のサーバであるという保証はまったく存在しない。このため、サーバのプール内のサーバ群は、署名を生成するのに使用されたキーを通信して、それらのキーがメッセージを処理するのに使用される場合、プール内の他のサーバ群がそれらの署名を検証することができるようにする必要がある可能性がある。一例では、サーバ群は、キーを互いに送信すること、あるいは証明書、または他の適切な方法を介して、キーサービスから適切なキーにアクセスすることができる。ただし、サーバのプール内のサーバ群は、一般に、サーバ間の通信を最小限に抑えて汚染（ｃｏｎｔａｍｉｎａｔｉｏｎ）を減らし、キーサービスにアクセスすることは、メッセージ処理時間を増大させる可能性がある。このため、署名を生成するサーバから署名を検証するサーバへセッションキーをセキュリティで保護された形で転送するのに、署名を生成したサーバは、署名を有するメッセージのエコーされるヘッダに暗号化され、署名されたセッションキーを追加することができる。

【００６５】

例えば、ＳＩＰノード３００が、図１に点線で示した第１のサーバ３００Ａおよび第２のサーバ３００Ｂを含むサーバのプールによって提供されることが可能である。一部のケースでは、要求５００は、ＳＩＰノード３００Ａを介してルーティングされることが可能であり、呼び出し先からの後続のダイアログ内要求７００は、ＳＩＰノード３００Ｂを介してルーティングされることが可能である。したがって、ダイアログ内要求の中のＲＯＵＴＥ　ＳＥＴ署名７６０を検証するのに、ＳＩＰノード３００Ｂは、ＲＯＵＴＥ　ＳＥＴ署名５６０を生成するのにＳＩＰノード３００Ａによって使用されたキーを知る必要がある。図４の典型的な要求ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群の中に示すとおり、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ５３４などのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダは、標準のＳＩＰ処理の下における典型的なネットワークロケーション情報、ＳＩＰノード３００Ａによって生成されたＲＯＵＴＥ　ＳＥＴ署名５６０、および署名５６０を生成するのにＳＩＰノード３００Ａによって使用されたＲＯＵＴＥ　ＳＥＴキー５８０を表すデータを含むことが可能である。

【００６６】

ただし、他のＳＩＰノード群がメッセージヘッダ内のＲＯＵＴＥ　ＳＥＴキー５８０へのアクセスを有さないことを確実にするため、ＳＩＰノード３００Ａは、公開キーを使用してＲＯＵＴＥ　ＳＥＴキーを暗号化することができる。これに対応して、その暗号化の完全性を検証するのに、ＳＩＰノードは、秘密キーを使用して、暗号化されたＲＯＵＴＥ　ＳＥＴキーに署名することができる。次に、ＳＩＰノード３００Ａは、暗号化され、署名されたセッションキーをＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのＵＲＩパラメータなどとして、エコーされるヘッダの中に挿入して、セッションキーを暗号化し、セッションキーに署名するのに使用される公開キー／秘密キーペアにアクセスを有するサーバに、セキュリティで保護されたセッションキーを配信することができる。暗号化されたセッションキー、および署名されたセッションキーは、単一のパラメータとして挿入されることも、複数のパラメータとして挿入されることも可能である。

【００６７】

一部のケースでは、２対の公開キー／秘密キーペアを利用して、メッセージヘッダ群の中のセッションキーをセキュリティで保護することが所望される可能性がある。例えば、第１の公開キー／秘密キーペア、および第２の公開キー／秘密キーペアが、インストール

されること、または証明書システムを介してアクセス可能であることが可能である。署名を生成したＳＩＰノードにおいて、第１の公開キー／秘密キーペアの第１の公開キーが、セッションキーを暗号化するのに使用され、第２の公開キー／秘密キーペアの第２の秘密キーが、セッションキーに署名するのに使用されることが可能である。このようにして、両方の公開キー／秘密キーペアにアクセスを有する受信側ＳＩＰノードは、第２の公開キー／秘密キーペアの第２の公開キーを使用して、署名の有効性を検証することができ、第２の公開キー／秘密キーペアの第１の秘密キーを使用して、セッションキーを解読することができる。

【００６８】

公開キー／秘密キーペアによるセッションキーの暗号化および署名は、計算能力を多く使用する（ｃｏｍｐｕｔａｔｉｏｎａｌｌｙ　ｉｎｔｅｎｓｉｖｅ）である可能性がある。このため、ＳＩＰノードにかかる負担を軽減するため、署名済みの暗号化されたセッションキーは、解読されたキー情報、キーの作成の日付／時刻タイムスタンプ、キーの有効期限の日付／時刻、および／または他の任意の情報に関連付けられたキーデータベースの中に格納することができる。このようにして、各伝送に先立って暗号化／署名を計算する必要がなくなる可能性がある。

【００６９】

例えば、図６に示すとおり、ＳＩＰノード３００Ｂは、ＲＯＵＴＥ　ＳＥＴ署名７６０を含むＲＯＵＴＥ　ＳＥＴヘッダ７２４を有する要求７００を受信すると、ＲＯＵＴＥ　ＳＥＴ署名を検査して、その署名５６０を生成するのにいずれのＲＯＵＴＥ　ＳＥＴキーが使用されたかを識別することができる。一部のケースでは、ＳＩＰノード３００Ｂは、格納されたキーのデータベースにアクセスして、データベースの中に識別されたＲＯＵＴＥ　ＳＥＴキー５８０が格納されているかどうかを検証することができる。ＲＯＵＴＥ　ＳＥＴキーが格納されていない場合、ＳＩＰノード３００Ｂは、公開キー／秘密キーペアにアクセスして、ＲＯＵＴＥ　ＳＥＴヘッダからＲＯＵＴＥ　ＳＥＴキーを特定することができる。より詳細には、ＳＩＰノード３００Ｂは、証明書サービスを使用して公開キー／秘密キーペアにアクセスすること、あるいはデータベースから、または任意の適切な方法またはプロセスを介して、公開キー／秘密キーペアを取得することができる。公開キーを使用して、ＳＩＰノード３００Ｂは、セッションキーの署名を認証することができる。ＳＩＰノード３００Ｂは、秘密キーを使用してＲＯＵＴＥ　ＳＥＴキー５８０を解読した後、その解読されたセッションキーを使用して、検証ＲＯＵＴＥ　ＳＥＴ署名を生成することもできる。同様の形で、ＶＩＡヘッダおよびＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを生成するのに使用されたセッションキーを、エコーされるヘッダの中に挿入することができ、より詳細には、そのセッションキーによって生成された署名を含む、エコーされるヘッダの中に挿入することができる。

【００７０】

セッションキーは、単独で暗号化してもよく、公開キーを使用して暗号化する前に、他の情報をセッションキーとともに含めてもよい。同様に、暗号化されたセッションキーには、単独で署名してもよく、代替として、秘密キーを使用して全体に署名を行う前に、暗号化されたセッションキーブラブに、暗号化されても、暗号化されなくてもよい他の情報が追加されてもよい。このようにして、キー識別子、セッションキー有効期限日、または暗号化された／署名されたセッションキーとともに伝送されることが所望される他の任意の情報などの他の情報。追加の情報は、暗号化された／署名されたセッションキーに追加することができ、同一の公開キー／秘密キーペア、または他の適切な暗号化プロセスを使用して暗号化すること、および／または署名することができる。

【００７１】

一部のケースでは、署名され、暗号化されたセッションキーを受信したＳＩＰノードは、セッションキーの有効期限の時刻および／または日付を検証することができる。これに関して、ＳＩＰノード３００Ａは、セッションキーとならび、セッションキーの作成の日付および／または時刻のスタンプも暗号化し、署名することができる。ＳＩＰノード３０

０Ｂは、ダイアログ内要求を受信すると、前述したとおり、セッションキーおよび日付／時刻スタンプの署名を認証し、セッションキーおよび日付／時刻スタンプを解読することができる。さらに、ＳＩＰノード３００Ｂは、セッションキーの日付／時刻スタンプを、そのキーの予期される有効期間（ｌｉｆｅｔｉｍｅ）、または格納された有効期限の日付／時刻と比較することができる。キーが失効している場合、ＳＩＰノード３００Ｂは、サポートされる場合、エラーメッセージを送信することができ、処理スタックからメッセージを削除することができ、かつ／または他の任意の適切なアクションを行うことができる。ドロップ（ｄｒｏｐ）キーがアクティブである場合、ＳＩＰノード３００Ｂは、継続して解読されたキーを使用して、メッセージの中の対応する署名を検証することができる。

【００７２】

図１に示した包括的な例では、ＳＩＰノード３００は、ＶＩＡ署名を生成し、その署名を、要求５００のＶＩＡヘッダのヘッダパラメータなどの、エコーされるヘッダの中に挿入することができる。次に、呼び出し先が、その要求に対する応答６００を送信すると、ＶＩＡ署名が、ＳＩＰノード３００において検証されることが可能である。同様に、要求がダイアログ開始要求であった場合、ＳＩＰノード３００は、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名を生成し、要求５００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのヘッダパラメータなどの、エコーされるヘッダの中にその署名を挿入することができる。次に、呼び出し先が、ダイアログ開始要求に対する応答６００を送信すると、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名が、ＳＩＰノード３００において検証されることが可能である。さらに、要求がダイアログ開始要求であった場合、ＳＩＰノード３００は、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名も生成し、要求５００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのＵＲＩパラメータなどの、エコーされるヘッダの中にその署名を挿入することができる。このＲＯＵＴＥ　ＳＥＴ署名は、そのダイアログにおける呼び出し先によって生成される、あらゆる将来の要求の中でＲＯＵＴＥヘッダのセットとして使用されるように、呼び出し先ＳＩＰノードによって保存されることが可能である。このため、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名は、要求の中で呼び出し先によって使用されるまで検証されない。同様に、ダイアログ開始要求に応答して、ＳＩＰノード２００は、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名を生成し、ＳＩＰノード２００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのＵＲＩパラメータとして、その署名を挿入することができる。呼び出し元ＲＯＵＴＥ　ＳＥＴ署名は、呼び出し元ＳＩＰノードによって生成される、あらゆる要求に関するＲＯＵＴＥヘッダのセットにおいて使用されるように、呼び出し元ＳＩＰノードによって保存されることが可能である。このようにして、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名は、呼び出し元から要求の中で伝送されるまで検証されないことが可能である。

【００７３】

次に、図８～１４を参照して、ＳＩＰノードサーバの典型的なインプリメンテーションを説明する。

【００７４】

図１に示した、呼び出し元ＳＩＰノード１０２、ＳＩＰノード２００、ＳＩＰノード２５０、ＳＩＰノード３００、および／または呼び出し先ＳＩＰノード４０２の任意の組合せが、存在し、ＳＩＰノードプロセッサとして動作する１つまたは複数のコンピュータ上、または１つまたは複数の他のデバイス上で動作していることが可能である。以上のノードのそれぞれは、複数のコンピュータシステム上、または複数の他のデバイス上で完全に、または部分的に提供されること、および／または、有線接続、無線接続などを含む当技術分野で周知の任意の方法を使用して一緒にネットワーク化されて、前述したプロセスを提供することが可能である。

【００７５】

例示した実施形態では、ＳＩＰノード３００は、図８～１４を参照して以下に説明するノードサーバ１３００によって提供される。ＳＩＰノード１０２、ＳＩＰノード２５０、ＳＩＰノード２００、およびＳＩＰノード４０２も、類似するサーバ／コンピュータシステムによって提供されることが可能である。

【００７６】
図８に示すとおり、ノードサーバ１３００は、１つまたは複数のプロセッサ１３０４、内部データー時間クロック１３０６、ならびに、実行されると、ＳＩＰノード３００の動作を実行するようにコンピュータに命令する、命令群を定義する１つまたは複数のコンピュータプログラム１３２２を含むことが可能なストレージ１３０８、１つまたは複数の通信ポート１３０２を含むことが可能である。ストレージには、以下に図９に関連してより詳細に説明するキーデータベース１３１０も含まれることが可能であり、プログラム群１３２２は、図１０～１４に関連して以下にさらに説明する。
【００７７】
図９は、１つまたは複数のレコード１３５２を含む、キーデータベース１３１０に関する典型的なテーブル１３５０を示す。一般に、各レコードは、セッションキー１３５４を、そのキーに関する追加の情報に関連付ける。この例では、各レコード１３５２は、キー識別子１３５３、セッションキー１３５４、公開キーで暗号化された暗号化済みのキー１３５６、作成の日付／時刻１３５８、および有効期限の日付／時刻１３６０を含む。ＳＩＰノード３００は、セッションキー１３５４を生成することができる。ただし、ＳＩＰノードは、メッセージ自体からセッションキーを識別すること、キーサービスから、またはデータに署名するために使用されるセッションキーを生成するのに適した任意の方法を介して、キーを取得することもできる。同様に、残りのデータも、ＳＩＰノード３００、メッセージ自体、または他のシステムがキー情報を提供するにつれ、初期設定され、更新されることが可能である。
【００７８】
キーデータベースは、リレーショナルデータベース、オブジェクト指向データベース、非構造化データベース、メモリ内データベース、またはその他のデータベースを含め、任意の種類のデータベースであることが可能である。データベースは、ＡＣＳＩＩテキスト、バイナリファイル、通信ネットワークを介して伝送されるデータ、または他の任意のファイルシステムなどの、フラットファイルシステムを使用して構築されることが可能である。以上のデータベースのこれらの可能なインプリメンテーションにもかかわらず、本明細書で使用するデータベースという用語は、コンピュータがアクセスできる任意の形で収集され、格納された任意のデータを指す。
【００７９】
次に、図１０～１４を参照して、ＳＩＰノード３００によって実行される様々なオペレーションを説明する。より詳細には、図１０を参照してＶＩＡ署名の生成を説明し、図１１を参照して、ＶＩＡ署名の検証を説明する。図１２を参照して、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名およびＲＯＵＴＥ　ＳＥＴ署名の生成を説明し、図１３を参照して、それらの署名の検証を説明する。図１４は、サーバのプール内のあるサーバから別のサーバにセッションキーをインポートする諸動作を示す。
【００８０】
図１０を参照すると、ＶＩＡ署名を生成する諸動作には、ＳＩＰ要求を受信すること９００が含まれるが、これには限定されない。前述の図は、ＩＮＶＩＴＥ要求に関連して説明するが、ＶＩＡ署名は、システムのセキュリティ要件および処理要件に依存して、すべての要求、または選択された要求に関して生成されることが可能である。ＳＩＰノードは、応答が転送されるリンクが信頼されないリンクであるかどうかを判定すること９０２ができる。リンクが信頼される場合、ＳＩＰノードは、ＳＩＰ標準プロセスの下で要求の標準の処理を続けることができる。転送リンクが信頼されない場合、諸動作には、処理を行うノードのＶＩＡヘッダを除く、すべての受信されたＶＩＡヘッダのＶＩＡヘッダセットを順序どおり構築すること９０４が含まれることが可能である。具体的には、要求が検査されることが可能であり、受信されたメッセージの中に存在するＶＩＡヘッダ群が、サーバ１３００メモリの中に格納されることが可能である。ＶＩＡヘッダセットが空である場合（９０６）、メッセージの標準の処理を続けることができる。複数のＶＩＡヘッダが存在する場合、諸動作には、ＶＩＡキーを識別すること９０８も含まれ、キーは、前述した

とおり、サーバ１３００によって生成されても、メッセージ自体においてアクセスされても（図１４を参照して以下にさらに説明する）、インターネットなどの手段を介するキーサービスから取得されてもよい。次に、ＶＩＡ署名が生成されることが可能であり９１０、暗号化プログラムを呼び出して、メモリの中に格納されたＶＩＡヘッダセットのハッシュを生成することが含まれることが可能である。処理を行うＳＩＰノード３００に関するＶＩＡヘッダが生成されることが可能であり９１２、ＶＩＡ署名が、ヘッダパラメータとして、ＳＩＰノード３００に関するＶＩＡヘッダの中に挿入されることが可能である。サーバ１３００は、図９に関連して前述したキーデータベースの中にＶＩＡセッションを格納すること９１６ができ、キー識別子、キー作成日付／時刻、有効期限の日付／時刻、暗号化されたキー、および／またはその他の情報などのキーパラメータを初期設定する、または更新することができる。

【００８１】

図１１を参照すると、要求の中でＶＩＡ署名を生成した後、ＳＩＰノードは、以前に処理された要求に返信する応答を受信すること９１８ができる。サーバは、応答のＶＩＡヘッダを検査し、複数のＶＩＡヘッダが存在するかどうかを判定すること９２０ができる。１つだけのＶＩＡヘッダが存在する場合、メッセージの標準の処理を続けることができる。複数のＶＩＡヘッダが存在する場合、ＳＩＰノードは、応答が信頼される接続を介して受信されたか、または信頼されない接続を介して受信されたかを判定すること９２２ができる。リンクが信頼される場合、メッセージの標準の処理を続けることができる。リンクが信頼されない場合、ＳＩＰノード３００は、ＳＩＰノード３００に関するＶＩＡヘッダを検査して、署名が存在するかどうかを判定すること９２４ができる。署名が存在しない場合、ＳＩＰノード３００は、処理スタックからメッセージをドロップすることができる。署名が存在する場合、ＳＩＰノード３００は、ヘッダから署名を取り外し、ＶＩＡ署名をメモリに保存し９２６、次に、メッセージから先頭のＶＩＡヘッダ（例えば、ＳＩＰノード３００のＶＩＡヘッダ）を取り外すこと９２８ができる。ＳＩＰノードは、キーデータベース、キーサービス、またはメッセージ自体から適切なＶＩＡセッションキーを取得すること９３０ができる。適切なキーは、署名自体の中で明らかな識別子、メッセージの日付／時刻、署名のタイプ（例えば、ＶＩＡ）、または適切なＶＩＡセッションキーを識別するのに適した他の任意のパラメータに基づいて選択されることが可能である。ＳＩＰノードは、応答の中に存在する残りのＶＩＡヘッダのＶＩＡヘッダセットを生成すること９３２ができる。ＶＩＡ署名が、メッセージの中で与えられる順序のＶＩＡヘッダ群で生成された場合、検証ＶＩＡヘッダも同一の順序で生成されて、署名パラメータの適切な順序を確実にすることが可能である。また、諸動作には、ＶＩＡヘッダセットおよび取得されたセッションキーに基づいてＶＩＡ検証署名を生成すること９３４、および次に、その検証ＶＩＡ署名を格納されたＶＩＡ署名と比較すること９３６も含まれる。ＶＩＡ署名が合致した場合、メッセージの標準の処理を続けることができる。署名が合致しなかった場合は、ＳＩＰノードは、処理スタックからメッセージをドロップすること、または他の任意の適切なアクションをとることができる。

【００８２】

図１２を参照すると、ＲＯＵＴＥ　ＳＥＴ署名およびＲＥＣＯＲＤ－ＲＯＵＴＥ署名を生成する諸動作には、ＳＩＰノードにおいてメッセージを受信すること９３８、およびそのメッセージが少なくとも１つのＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを含むかどうかを判定すること９４０が含まれる。メッセージがＲＥＣＯＲＤ－ＲＯＵＴＥヘッダをまったく含まない場合、メッセージの標準の処理を続けることができる。ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを含む場合、ＳＩＰサーバは、メッセージが信頼されるリンクを介して伝送されるか、信頼されないリンクを介して伝送されるかを判定すること９４４ができる。より詳細には、ＳＩＰサーバは、検証されるべきメッセージが、信頼されるリンクを介して受信されるか、または信頼されないリンクを介して受信されるかを判定することができる。応答リンクが信頼される場合、標準の処理を続けることができる。リンクが信頼されない場合、ＳＩＰサーバは、受信されたメッセージが要求であるかどうか判定すること９４６がで

きる。メッセージが要求ではない場合、ＳＩＰサーバは、応答の中のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群に基づき、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダセットを構築すること９４８ができる。メッセージが要求である場合、ＳＩＰサーバは、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダセットを構築すること９５０ができ、ＲＥＣＯＲＤ－ＲＯＵＴＥセッションキーを識別すること９５１ができ、セッションキーは、前述したとおり、サーバ１３００によって生成されること、メッセージ自体においてアクセスされること（図１４を参照して以下にさらに説明する）、またはインターネットなどの手段を介してキーサービスから取得されることも可能である。次に、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名が生成されること９５２が可能であり、暗号化プログラムを呼び出して、メモリの中に格納されたＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのＵＲＩ部分のハッシュを生成することが含まれることが可能である。ＲＥＣＯＲＤ－ＲＯＵＴＥ署名は、ヘッダパラメータとして、ＳＩＰノード３００に関するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入されること９５４が可能である。サーバ１３００は、ＲＥＣＯＲＤ－ＲＯＵＴＥセッションキーを、図９に関連して前述したキーデータベースの中に格納すること９５６ができ、キー識別子、キー作成日付／時刻、有効期限の日付／時刻、および／または暗号化されたキーなどのキーパラメータを初期設定する、または更新することができる。メッセージが要求であるか否かにかかわらず、ＳＩＰサーバは、受信されたメッセージ内に１つのＣＯＮＴＡＣＴヘッダが存在するかどうかを判定すること９４２ができる。存在しない場合、標準の処理を続けることができ、存在する場合、ＳＩＰノードは、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダセットおよびＣＯＮＴＡＣＴヘッダから、ＲＯＵＴＥヘッダセットを構築すること９５８ができる。次に、ＳＩＰサーバは、ＲＯＵＴＥ　ＳＥＴセッションキーを識別すること９６０ができ、そのキーを使用して、ＲＯＵＴＥ　ＳＥＴ署名を生成すること９６２ができ、ＲＯＵＴＥ　ＳＥＴ署名は、次に、ＵＲＩパラメータとして、ＳＩＰノード３００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入されること９６４が可能である。ＳＩＰノードは、前述したとおり、ＲＯＵＴＥ　ＳＥＴセッションキーおよびキーパラメータをキーデータベースの中に保存すること９６６ができる。次に、ＳＩＰサーバは、メッセージの標準の処理に取りかかることができる。

【００８３】

図１３を参照すると、ＳＩＰノードが応答を受信すると９６８、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名の検証が行われることが可能である。ＳＩＰノードは、メッセージの中にＲＥＣＯＲＤ－ＲＯＵＴＥヘッダが存在するかどうかを判定すること９７０ができる。存在しない場合、メッセージの標準の処理を行うことができる。存在する場合、ＳＩＰノードは、応答が信頼されないリンクを介して受信されたかどうかを判定すること９７２ができる。リンクが信頼される場合、メッセージの標準の処理を続けることができる。リンクが信頼されない場合、ＳＩＰノードは、ＳＩＰノードに関するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダがＲＥＣＯＲＤ－ＲＯＵＴＥ署名を含むかどうかを判定すること９７４ができる。ＲＥＣＯＲＤ－ＲＯＵＴＥ署名を含まない場合、メッセージは、ＳＩＰノード３００の処理スタックからドロップすることができる。ＲＥＣＯＲＤ－ＲＯＵＴＥ署名が存在する場合、ＳＩＰノードサーバは、ＳＩＰノード３００のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ内のすべての署名を取り外し、保存すること９７６ができる。例えば、ＳＩＰノード３００に関するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダは、ＲＥＣＯＲＤ－ＲＯＵＴＥ署名とＲＯＵＴＥ　ＳＥＴ署名の両方を含むことが可能である。署名の配置がダイアログ全体を通じて一貫しており、かつ／または署名が、複数の署名を区別する適切な形で識別される限り、どちらの署名がＲＥＣＯＲＤ－ＲＯＵＴＥ　ＵＲＩパラメータの中で先にリストされてもよい。例えば、複数の署名を有するヘッダの中に挿入された各署名は、ヘッダのタイプを指定する識別子を含むことが可能であり、かつ／または各署名に、挿入された署名のタイプを識別する追加のパラメータが付随することが可能である。ＳＩＰノードは、メッセージのヘッダ群の中のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群のＵＲＩ部分を含むＲＥＣＯＲＤ－ＲＯＵＴＥヘッダセットを構築すること９７８ができる。また、ＳＩＰノードは、図１１の動作９３０に関連して前述した手続きに従って、適切なＲＥＣＯＲＤ－ＲＯＵＴＥセッションキ

ーを取得すること９８０もできる。ＳＩＰノードは、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダセットおよびセッションキーに基づいて検証ＲＥＣＯＲＤ－ＲＯＵＴＥ署名を生成すること９８２ができ、次に、検証ＲＥＣＯＲＤ－ＲＯＵＴＥ署名を格納されたＲＥＣＯＲＤ－ＲＯＵＴＥ署名と比較すること９８４ができる。署名が合致しない場合、ＳＩＰノードは、処理スタックからメッセージをドロップすることができる。署名が合致した場合は、標準の処理を続けることができる。ＲＯＵＴＥ　ＳＥＴ署名が、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダのＵＲＩパラメータとして存在していた場合、ＳＩＰノードサーバは、メッセージおよび／またはメモリからその署名を削除すること９８６ができる。より詳細には、呼び出し先ＲＯＵＴＥ　ＳＥＴ署名が、呼び出し先ＳＩＰノードによって保存されており、このため、現在のメッセージを呼び出し元に向かわせるのにもはや要求されない。呼び出し元に関する新たなＲＯＵＴＥ　ＳＥＴ署名が生成され、呼び出し先に伝送されるべきかどうかを判定するのに、ＳＩＰノードは、次のＳＩＰノードが信頼されないリンクを介してであり、かつ少なくとも１つのＣＯＮＴＡＣＴヘッダが存在するかどうかを判定すること９８７ができる。そうではない場合、メッセージの標準の処理を続けることができる。次のリンクが信頼されない場合、ＳＩＰノードサーバは、ＲＥＣＯＲＤ－ＲＯＵＴＥキーと同一のキーであることが可能なＲＯＵＴＥ　ＳＥＴセッションキーを取得すること９８８により、呼び出し元ＲＯＵＴＥ　ＳＥＴ署名を生成することができる。そのキーを使用して、ＳＩＰノードは、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダセット、および最初にリストされたＣＯＮＴＡＣＴヘッダのＵＲＩ部分に基づき、ＲＯＵＴＥ　ＳＥＴ署名を生成すること９９０ができる。ＲＯＵＴＥ　ＳＥＴ署名は、呼び出し元ＳＩＰノード１０２に転送されるように、ＳＩＰノード３００に関するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入すること９９２ができる。ＳＩＰノードは、前述したとおり、ＲＯＵＴＥ　ＳＥＴセッションキーおよび／またはＲＥＣＯＲＤ－ＲＯＵＴＥセッションキー、およびキーパラメータをキーデータベースの中に保存すること９９４ができる。次に、ＳＩＰサーバは、メッセージの標準の処理に取りかかることができる。後続の要求の中の呼び出し先ＲＯＵＴＥ　ＳＥＴ署名、および／または呼び出し元ＲＯＵＴＥ　ＳＥＴ署名の検証も、前述したのと同様のプロセスに従うことが可能である。

【００８４】

図１４は、サーバのプール内のサーバ群の間でセッションキーを転送するための１つの典型的なインプリメンテーションにおける動作を示す。例えば、前述したとおり、ＳＩＰノード３００は、サーバ３００Ａおよびサーバ３００Ｂによって提供されることが可能である。このようにして、ＳＩＰノード３００Ａが、セッションキーを使用して署名を生成すること可能であり、次に、ＳＩＰノード３００Ｂが、その署名を検証するように要求されることが可能である。以下の例は、ＲＯＵＴＥ　ＳＥＴヘッダ群に関連して説明するが、類似したプロセスを使用して、ＲＥＣＯＲＤ－ＲＯＵＴＥセッションキーおよび／またはＶＩＡセッションキーに対して暗号化、署名、およびアクセスを行うこともできる。

【００８５】

図１４に示すとおり、公開キー／秘密キーペアの共通の証明書が生成されて９９６、サーバプール内の各サーバ（３００Ａ、３００Ｂ）にインストールされること９９８が可能である。前述したとおり、公開キー／秘密キーペアを使用して、そのノードによって処理されるすべてのセッションキーに署名および暗号化を行うことも、各タイプのセッションキー（ＶＩＡ、ＲＥＣＯＲＤ－ＲＯＵＴＥ、および／またはＲＯＵＴＥ　ＳＥＴ）が別個の公開キー／秘密キーペアを有することも可能である。動作の際、ＳＩＰノード３００Ａは、署名される必要がある要求を受信すること１０００が可能である。前述したとおり、ＳＩＰノードサーバは、ＲＯＵＴＥ　ＳＥＴセッションキーを生成すること、ＲＯＵＴＥ　ＳＥＴセッションキーにアクセスすること、またはＲＯＵＴＥ　ＳＥＴセッションキーを取得することにより、ＲＯＵＴＥ　ＳＥＴセッションキーを識別すること１００２ができる。ＳＩＰノードは、証明書が、キー交換に関するルーティング情報向けに構成されていることを検証すること１００４もできる。ＳＩＰサーバは、ＲＯＵＴＥ　ＳＥＴセッションキーの作成の日付／時刻スタンプを特定すること、およびその日付／時刻スタンプを

セッションキーに付加すること１００６ができる。公開キーを使用して、ＳＩＰサーバは、セッションキーおよび日付／時刻スタンプを暗号化すること１００８、およびその結果に秘密キーを使用して署名すること１０１０ができる。暗号化され、署名されたセッションキーの結果は、図９に関連して前述したキーデータベースの中に、日付／時刻スタンプ、セッションキー、セッションキー識別子などのキーパラメータとともに格納すること１０１２ができる。ＲＯＵＴＥ　ＳＥＴセッションキーを使用して、ＳＩＰノードは、図１２に関連して前述したとおり、ＲＯＵＴＥ　ＳＥＴ署名を生成することができ、ＳＩＰノード３００に関するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを生成すること１０１４ができる。ＳＩＰノードサーバは、ＲＯＵＴＥ　ＳＥＴ署名をＳＩＰノードに関するＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入すること１０１８ができ、署名され、暗号化されたＲＯＵＴＥ　ＳＥＴセッションキーをＵＲＩパラメータとして、ＳＩＰノードＲＥＣＯＲＤ－ＲＯＵＴＥヘッダの中に挿入すること１０２０もできる。

【００８６】

呼び出し先は、要求を受信した後、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群およびＣＯＮＴＡＣＴヘッダのＵＲＩ部分をＲＯＵＴＥ　ＳＥＴヘッダのセットの中に保存する。呼び出し先ＳＩＰノードは、後続のダイアログ内要求を生成する際、ＳＩＰノード３００Ａによって生成されたＲＯＵＴＥ　ＳＥＴ署名およびＲＯＵＴＥ　ＳＥＴセッションキーを含む、ＲＥＣＯＲＤ－ＲＯＵＴＥヘッダ群およびＣＯＮＴＡＣＴヘッダをエコーするＲＯＵＴＥ　ＳＥＴヘッダ群を含めることができる。第２のＳＩＰノード３００Ｂは、少なくとも１つのＲＯＵＴＥヘッダを有するダイアログ内要求を受信すること１０２２が可能である。図１２に関連して前述した適切なセッションキーを取得すること９３０に鑑みて、ＳＩＰノードは、署名され、暗号化されたＲＯＵＴＥ　ＳＥＴセッションキーをＲＯＵＴＥヘッダから抽出し１０２４、その署名され、暗号化されたキーをキーデータベース内のエントリと比較して１０２６、サーバノード３００Ｂが、解読されたセッションキーへのアクセスを有するかどうかを判定することができる。合致が存在する場合、ＳＩＰノード３００Ｂは、キーデータベースからのセッションキーを使用して、ＲＯＵＴＥヘッダ内のＲＯＵＴＥ　ＳＥＴ署名を検証することができる。合致が存在しない場合、ＳＩＰノードは、キー署名を抽出すること１０２８ができ、公開キーを使用してキー署名を検証すること１０３０ができる。署名が検証されなかった場合、ＳＩＰノードは、処理スタックからメッセージをドロップすること、または他の任意の適切なアクションを行うことができる。署名が合致した場合、暗号化されたセッションキーを抽出すること１０３２ができる。日付／時刻スタンプは、セッションキーとは別個に解読して１０３４、キーがもはやアクティブではない（例えば、失効している）場合、サーバリソースを最小限に抑えることができる。より詳細には、ＳＩＰノードは、日付／時刻スタンプが、そのタイプのセッションキーに関する構成有効期間内にあることを検証した後、日付／時刻スタンプを検証すること１０３６ができる。日付／時刻スタンプを検証することができない場合、メッセージは、処理スタックからドロップすることができる。日付／時刻スタンプが検証された場合、秘密キーを使用してセッションキーを解読した１０３８後、ＲＯＵＴＥ　ＳＥＴ署名を検証するのに１０４０使用することができる。解読されたセッションキーの結果は、図９に関連して前述したキーデータベースの中に、日付／時刻スタンプ、署名され、暗号化されたセッションキー、セッションキー識別子などのキーパラメータとともに格納すること１０４２ができる。何らかの時点で、セッションキーは、失効することが可能であり、セッションキー、署名され、暗号化されたセッションキーなどを含む、そのセッションキーにかかるデータベースレコードが、ダイアログが完了した時点、そのセッションキーを使用するヘッダがもはや予期されなくなった時点、セッションキーのアクティブな有効期間の終了時、および／またはセッションキーの有効期限日後などに、キーデータベースから削除されること１０４４が可能である。

【００８７】

図１および／または図８のＳＩＰノード群の様々な要素を個々に、または組合せで実装することができるコンピュータシステムは、通常、ユーザに情報を表示する出力デバイス

と、ユーザから入力を受け取る入力デバイスの両方に接続された少なくとも１つのメインユニットを含む。メインユニットは、相互接続機構を介してメモリシステムに接続されたプロセッサを含むことが可能である。また、入力デバイスおよび出力デバイスも、相互接続機構を介してプロセッサおよびメモリシステムに接続される。

【００８８】

図１および／または図８に示したコンピューティングデバイス群は、通常、何らかの形態のコンピュータ可読媒体を含む。コンピュータ可読媒体は、ＳＩＰサーバ内部の他のコンピューティングデバイス群がアクセスすることができる任意の利用可能な媒体であることが可能である。例として、限定としてではなく、コンピュータ可読媒体は、コンピュータ記憶媒体および通信媒体を含むことが可能である。コンピュータ記憶媒体には、コンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータなどの情報を格納するために任意の方法または技術で実装された、揮発性媒体および不揮発性媒体、リムーバブルな媒体およびリムーバブルでない媒体が含まれる。コンピュータ記憶媒体には、ＲＡＭ（random access memory）、ＲＯＭ（read only memory）、ＥＥＰＲＯＭ（Electronically Erasable and Programmable Read Only Memory）、フラッシュメモリまたは他のメモリ技術、ＣＤ（compact disc）－ＲＯＭ、デジタルバーサタイルディスク（ＤＶＤ）または他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージまたは他の磁気記憶装置、あるいは所望の情報を格納するのに使用することができ、ＳＩＰノード内部のコンピュータシステム群がアクセスすることができる他の任意の媒体が含まれるが、以上には限定されない。通信媒体は、通常、搬送波などの変調されたデータ信号、または他のトランスポート機構でコンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータを実体化し、あらゆる情報配信媒体が含まれる。例として、限定としてではなく、通信媒体には、有線ネットワークまたは直接配線接続などの有線媒体、ならびに音響媒体、ＲＦ（radio frequency）媒体、赤外線媒体、およびその他の無線媒体などの無線媒体が含まれる。また、以上の媒体のいずれかの組合せも、コンピュータ可読媒体の範囲に含められるべきである。

【００８９】

１つまたは複数の出力デバイス、および１つまたは複数の入力デバイスが、コンピュータシステムに接続されることが可能である。本発明は、コンピュータシステムと組合せで使用される特定の入力デバイス群、または特定の出力デバイス群、または本明細書で説明するデバイス群に限定されない。

【００９０】

コンピュータシステムは、ＳｍａｌｌＴａｌｋ、Ｃ＋＋、Ｊａｖａ（登録商標）、Ａｄａ、またはＣ＃（Ｃシャープ）、あるいはスクリプト言語やアセンブリ言語などの他の言語などの、コンピュータプログラミング言語を使用してプログラミング可能な、汎用コンピュータシステムであることが可能である。本発明の様々な態様は、プログラミングされない環境（例えば、ブラウザプログラムのウインドウ内に表示されると、グラフィカルユーザインタフェースの諸態様を表示する、または他の諸機能を実行する、ＨＴＭＬ（HyperText Markup Language）、ＸＭＬ（Extensible Markup Language）、またはその他の形式で作成されたドキュメント）において実施することもできる。本発明の様々な態様は、プログラミングされた要素、またはプログラミングされない要素、あるいはプログラミングされた要素とプログラミングされない要素の組合せとして実施することができる。また、コンピュータシステムは、特別にプログラミングされた専用ハードウェア、または特定用途向け集積回路（ＡＳＩＣ）であることも可能である。リーダ（ｒｅａｄｅｒ）システムには、ポケットベル、電話機、パーソナルデジタルアシスタント、またはその他の電子データ通信デバイスも含まれることが可能である。

【００９１】

汎用通信システムでは、プロセッサは、通常、インテルコーポレーションから入手可能な周知のＰｅｎｔｉｕｍ（登録商標）プロセッサなどの市販されるプロセッサである。他の多数のプロセッサが利用可能である。そのようなプロセッサは、普通、例えば、マイク

ロソフトコーポレーションから入手可能な、Ｗｉｎｄｏｗｓ（登録商標）９５（登録商標）、Ｗｉｎｄｏｗｓ（登録商標）９８（登録商標）、Ｗｉｎｄｏｗｓ（登録商標）ＮＴ（登録商標）、Ｗｉｎｄｏｗｓ（登録商標）２０００（登録商標）、またはＷｉｎｄｏｗｓ（登録商標）ＸＰ（登録商標）、アップルコンピュータから入手可能なＭＡＣ　ＯＳ（operating system）　Ｓｙｓｔｅｍ　Ｘ（商標）、サンマイクロシステムズから入手可能なＳｏｌａｒｉｓ（商標）　Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ、または様々なソースから入手可能なＵＮＩＸ（登録商標）であることが可能なオペレーティングシステムを実行する。他の多数のオペレーティングシステムも使用することができる。

【００９２】

プロセッサとオペレーティングシステムは一緒に、アプリケーションプログラム群が高水準プログラミング言語で書かれるコンピュータプラットフォームを定義する。本発明は、特定のコンピュータシステムプラットフォーム、プロセッサ、オペレーティングシステム、またはネットワークに限定されないことを理解されたい。また、本発明は、特定のプログラミング言語またはコンピュータシステムに限定されないことも、当業者には明白なはずである。さらに、他の適切なプログラミング言語、および他の適切なコンピュータシステムも使用できることを認識されたい。

【００９３】

コンピュータシステムの１つまたは複数の部分は、通信ネットワークに結合された１つまたは複数のコンピュータシステム（図示せず）にわたって分散させることができる。それらのコンピュータシステムも、汎用コンピュータシステムであることが可能である。例えば、本発明の様々な態様は、１つまたは複数のクライアントコンピュータにサービスを提供するように構成された（例えば、サーバ群）、または分散システムの一環として全体的タスクを実行するように構成された１つまたは複数のコンピュータシステムの間で分散させることもできる。例えば、本発明の様々な態様は、本発明の様々な実施形態に従って様々な機能を実行する、１つまたは複数のサーバシステムの間に分散されたコンポーネントを含む、クライアントーサーバシステム上で実行してもよい。それらのコンポーネントは、通信プロトコル（例えば、ＳＩＰまたはＴＣＰ／ＩＰ）を使用して通信ネットワーク（例えば、インターネット）を介して通信する、実行可能コード、中間（例えば、ＩＬ）コード、または解釈される（例えば、Ｊａｖａ（登録商標））コードであることが可能である。本発明は、いずれの特定のシステム上、またはグループのシステム上で実行されることにも限定されないことを認識されたい。

【００９４】

以上、本発明のいくつかの例示的な実施形態を説明してきたが、以上の実施形態は、単に例として提示され、例示的であるに過ぎず、限定するものではないことが、当業者には明白であろう。多数の変更形態、および他の例示的な実施形態が、当業者が理解する範囲（ｓｃｏｐｅ）に含まれ、本発明の範囲に含まれるものと企図される。詳細には、本明細書で提示した例の多くは、方法上の動作またはシステム要素の特定の組合せに関わるが、それらの動作、およびそれらの要素を他の形で組み合わせて、同一の諸目的を達することもできることを理解されたい。１つの実施形態だけに関連して説明した動作、要素、および特徴は、その他の実施形態における類似した役割から除外されるものではない。さらに、クレーム要素（ｃｌａｉｍ　ｅｌｅｍｅｎｔ）を修飾する特許請求の範囲における「第１の」や「第２の」などの順序を表す語の使用は、それ自体で、優先度、優先順位、またはあるクレーム要素が別のクレーム要素に先行する順位、あるいは方法の動作が実行される時間的順序を表すものではなく、単に、ある名前を有する１つのクレーム要素を、（順序を表す語以外は）同一の名前を有する別のクレーム要素と区別するラベルとして使用して、クレーム要素を区別している。

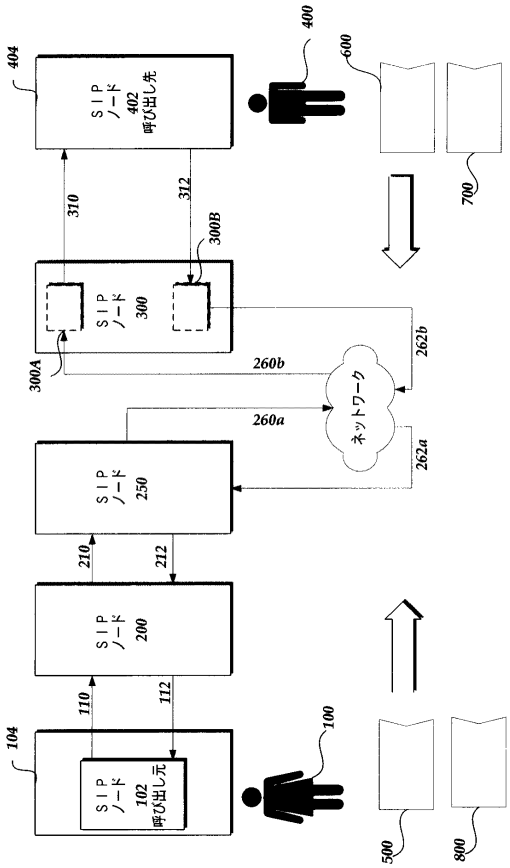
【図面の簡単な説明】

【００９５】

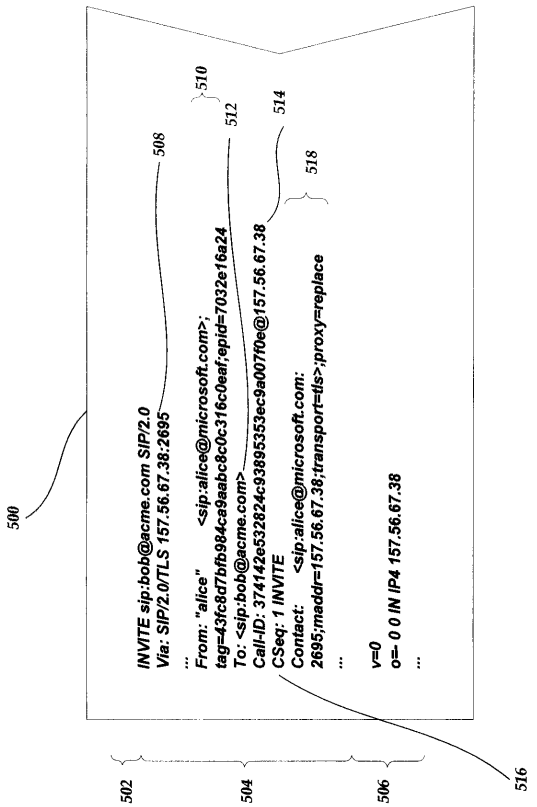
【図１】本発明の一実施形態による２つの「ＳＩＰ」（セッション開始プロトコル）クライアント間のＩＮＶＩＴＥ要求－応答経路を示す概略図である。

【図２】図１による典型的なＩＮＶＩＴＥ要求を示す図である。
【図３】図１による典型的な一組のＶＩＡヘッダを示す図である。
【図４】図１による典型的な一組のＲＥＣＯＲＤ－ＲＯＵＴＥヘッダを示す図である。
【図５】図２のＩＮＶＩＴＥ要求に対する典型的な応答を示す図である。
【図６】図１の呼び出し先ＳＩＰノードによって生成された典型的な要求を示す図である。
【図７】図１の呼び出し元ＳＩＰノードによって生成された典型的な要求を示す図である。
【図８】本発明の一実施形態による典型的なＳＩＰサーバを示す図である。
【図９】本発明の一実施形態によるキー情報のデータベースからの典型的なテーブルを示す図である。
【図１０】本発明の一実施形態による、どのようにＶＩＡ署名を生成することができるかを示す流れ図である。
【図１１】本発明の一実施形態による、どのようにＶＩＡヘッダを検証するかを示す流れ図である。
【図１２】本発明の一実施形態による、どのようにＲＯＵＴＥ　ＳＥＴ署名およびＲＥＣＯＲＤ－ＲＯＵＴＥ署名を生成することができるかを示す流れ図である。
【図１３】本発明の一実施形態による、どのようにＲＥＣＯＲＤ－ＲＯＵＴＥ署名を検証するかを示す流れ図である。
【図１４】本発明の一実施形態による、どのようにセッションキーをサーバのプール内のサーバにインポートすることができるかを示す流れ図である。
【符号の説明】
【００９６】
１００、４００　ユーザ
１０４、４０４　コンピュータシステム
１０２、２００、２５０、３００、４０２　ＳＩＰノード
５００　ＩＮＶＩＴＥ要求
６００　応答メッセージ
７００　ダイアログ内要求
８００　受信された要求

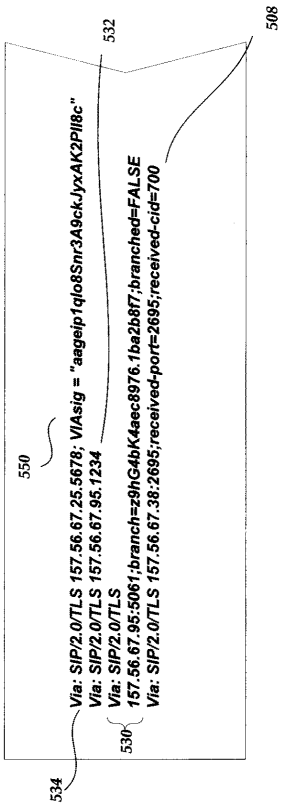
【図１】


SIP ノード 402 呼び出し先
SIP ノード 300
SIP ノード 250
SIP ノード 200
SIP ノード 102 呼び出し元
ネットワーク
404
400
600
700
310
312
300B
300A
260b
262b
260a
262a
210
212
110
112
104
100
500
800

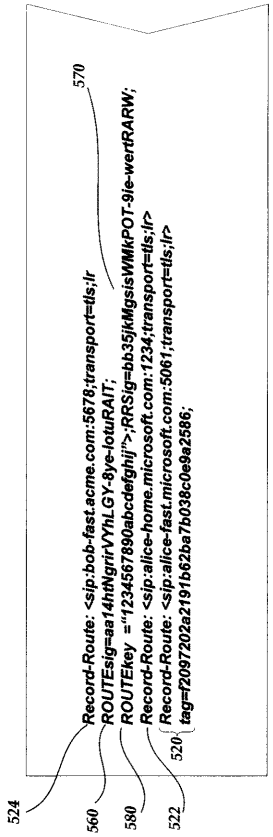
【図２】


INVITE sip:bob@acme.com SIP/2.0
Via: SIP/2.0/TLS 157.56.67.38:2695
...
From: "alice" <sip:alice@microsoft.com>;
tag=43fc8d7bfb9844e9aabc8c0c316c0eaf;epid=7032e16a24
To: <sip:bob@acme.com>
Call-ID: 374142e532824c93895353ec9a007f0e@157.56.67.38
CSeq: 1 INVITE
Contact: <sip:alice@microsoft.com:
2695;maddr=157.56.67.38;transport=tls>;proxy=replace
...
v=0
o=- 0 0 IN IP4 157.56.67.38
...
500
502
504
506
508
510
512
514
516
518

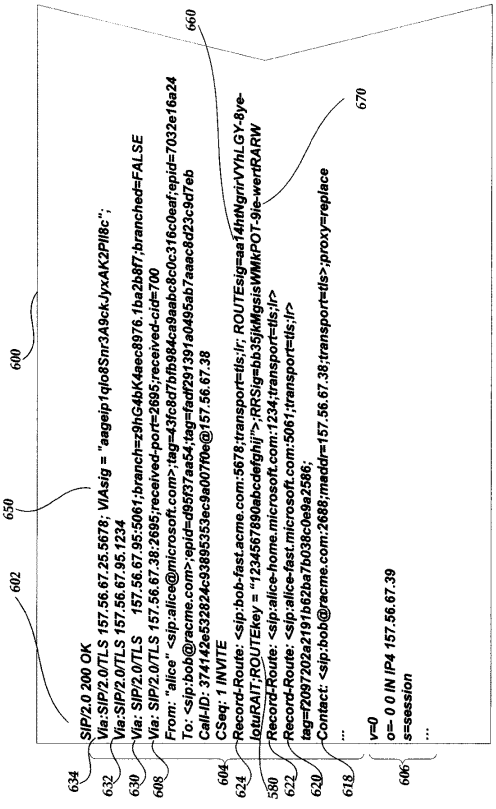
【図３】


Via: SIP/2.0/TLS 157.56.67.25.5678; VIAsig = "aagejp1qlo8Snr3A9ckJyxAK2Pll8c"
Via: SIP/2.0/TLS 157.56.67.95.1234
Via: SIP/2.0/TLS
157.56.67.95:5061;branch=z9hG4bK4aec8976.1ba2b8f7;branched=FALSE
Via: SIP/2.0/TLS 157.56.67.38:2695;received-port=2695;received-cid=700
508
532
550
530
534

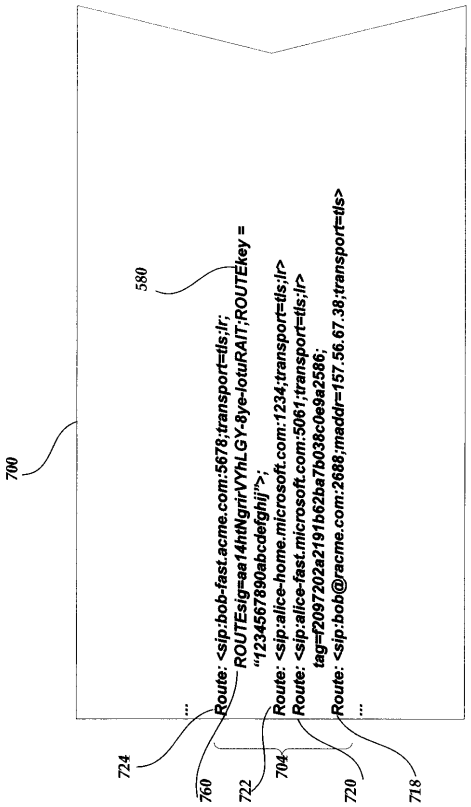
【図４】


Record-Route: <sip:bob-fast.acme.com:5678;transport=tls;lr
ROUTEsig=aa14h8NgrirVYhLGY-8ye-lotuRAIT;
ROUTEkey ="1234567890abcdefghij">;RRSig=bb35jkMgsisWMkPOT-9ie-wertRARW;
Record-Route: <sip:alice-home.microsoft.com:1234;transport=tls;lr>
Record-Route: <sip:alice-fast.microsoft.com:5061;transport=tls;lr>
tag=2097202a2191b62ba7b038c0e9a2586;
570
524
560
580
522
520

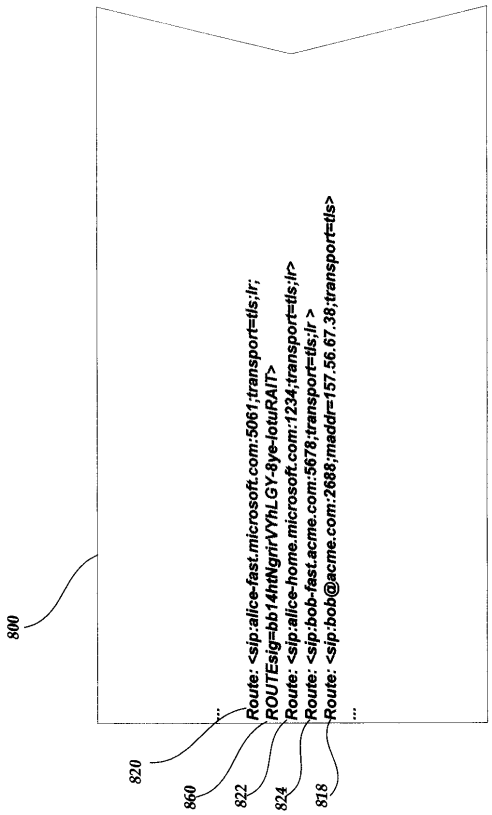
【図５】


600
650
602
660
670
SIP/2.0 200 OK
Via:SIP/2.0/TLS 157.56.67.25.5678; VIAsig = "aagejp1qlo8Snr3A9ckJyxAK2Pll8c";
Via:SIP/2.0/TLS 157.56.67.95.1234
Via: SIP/2.0/TLS 157.56.67.95:5061;branch=z9hG4bK4aec8976.1ba2b8f7;branched=FALSE
Via: SIP/2.0/TLS 157.56.67.38:2695;received-port=2695;received-cid=700
From: "alice" <sip:alice@microsoft.com>;tag=43fc8d7bfb984ca9aabc8c0c316c0eaf;epid=7032e16a24
To: <sip:bob@racme.com>;epid=d9f37aa54;tag=faaff291391a0495ab7aaec8d23c9d7eb
Call-ID: 374142e532824c93895353ec9a007f0e@157.56.67.38
CSeq: 1 INVITE
Record-Route: <sip:bob-fast.acme.com:5678;transport=tls;lr; ROUTEsig=aa14htNgrirVYhLGY-8ye-
lotuRAIT;ROUTEkey = "1234567890abcdefghij!">;RRSig=bb35jkMgsisWMkPOT-9le-wertRARW
Record-Route: <sip:alice-home.microsoft.com:1234;transport=tls;lr>
Record-Route: <sip:alice-fast.microsoft.com:5061;transport=tls;lr>
tag=f2097202a2191b62ba7b038c0e9a2586;
Contact: <sip:bob@racme.com:2688;maddr=157.56.67.38;transport=tls>;proxy=replace
...
v=0
o= 0 0 IN IP4 157.56.67.39
s=session
...
634
632
630
608
604
624
580
622
620
618
606

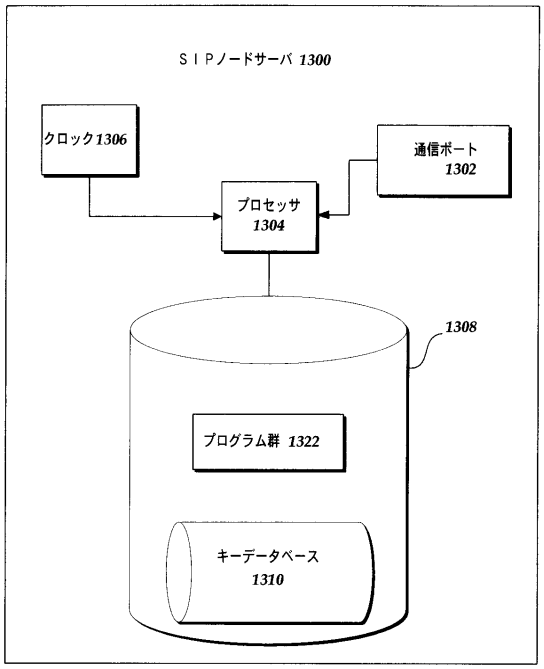
【図６】


700
580
...
Route: <sip:bob-fast.acme.com:5678;transport=tls;lr;
ROUTEsig=aa14htNgrirVYhLGY-8ye-lotuRAIT;ROUTEkey =
"1234567890abcdefghij!">;
Route: <sip:alice-home.microsoft.com:1234;transport=tls;lr>
Route: <sip:alice-fast.microsoft.com:5061;transport=tls;lr>
tag=f2097202a2191b62ba7b038c0e9a2586;
Route: <sip:bob@racme.com:2688;maddr=157.56.67.38;transport=tls>
...
724
760
722
704
720
718

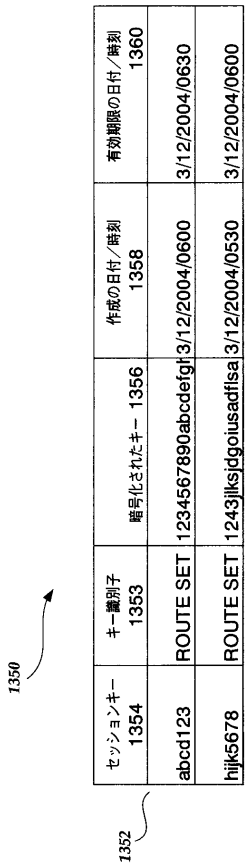
【図７】


800
...
Route: <sip:alice-fast.microsoft.com:5061;transport=tls;lr;
ROUTEsig=bb14htNgrirVYhLGY-8ye-lotuRAIT>
Route: <sip:alice-home.microsoft.com:1234;transport=tls;lr>
Route: <sip:bob-fast.acme.com:5678;transport=tls;lr >
Route: <sip:bob@acme.com:2688;maddr=157.56.67.38;transport=tls>
...
820
860
822
824
818

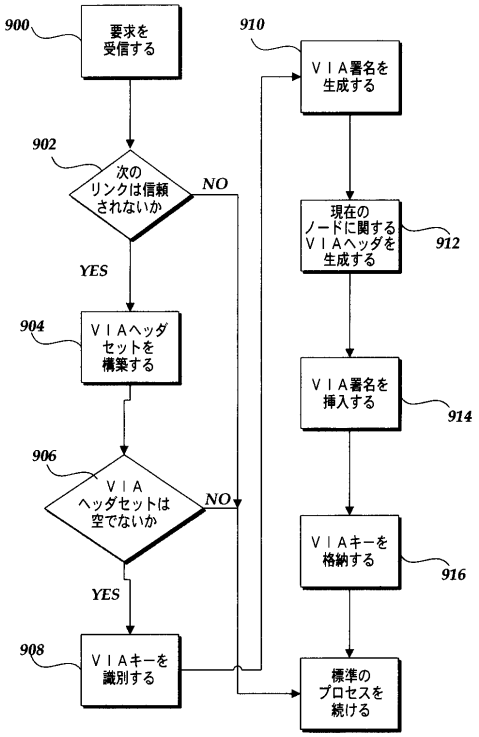
【図８】


SIPノードサーバ 1300
クロック1306
通信ポート
1302
プロセッサ
1304
1308
プログラム群 1322
キーデータベース
1310

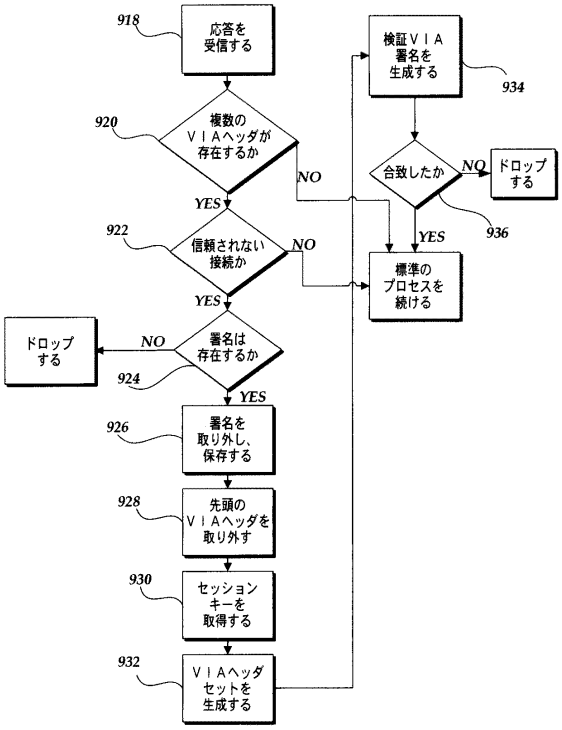
【図９】



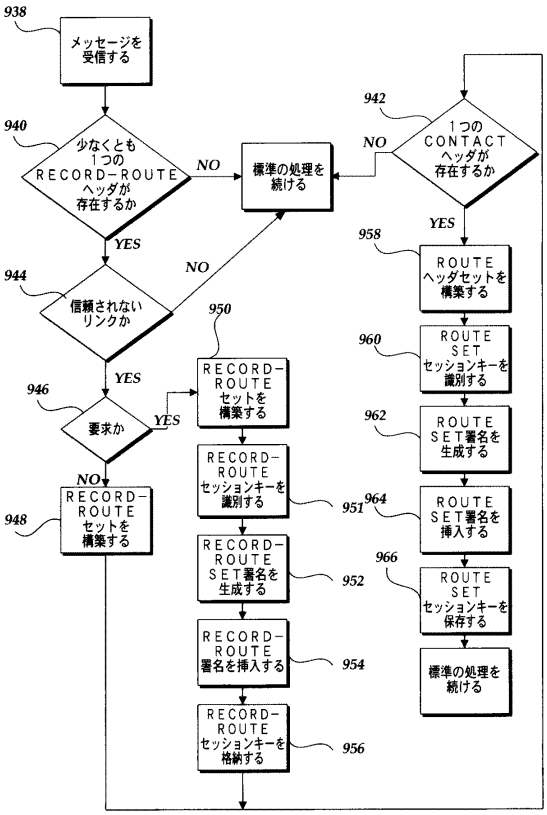
【図１０】



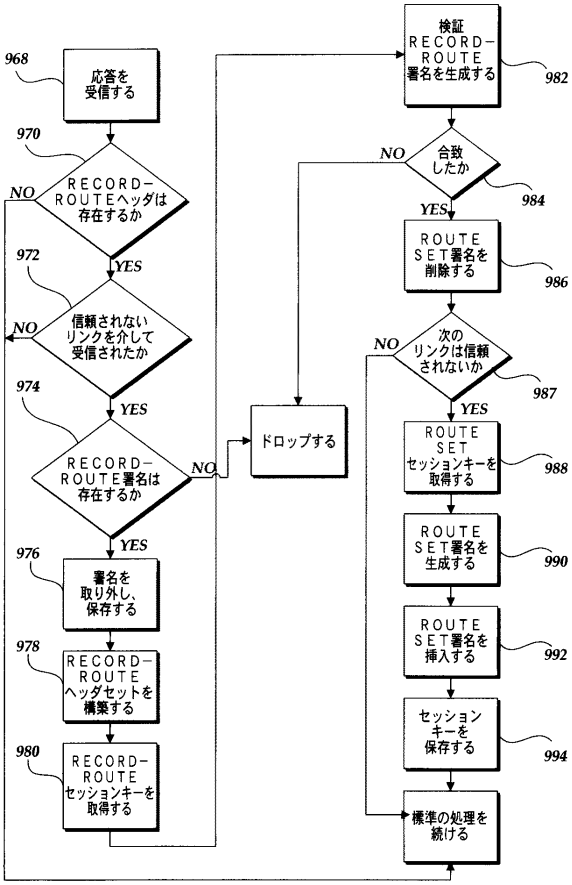
【図１１】



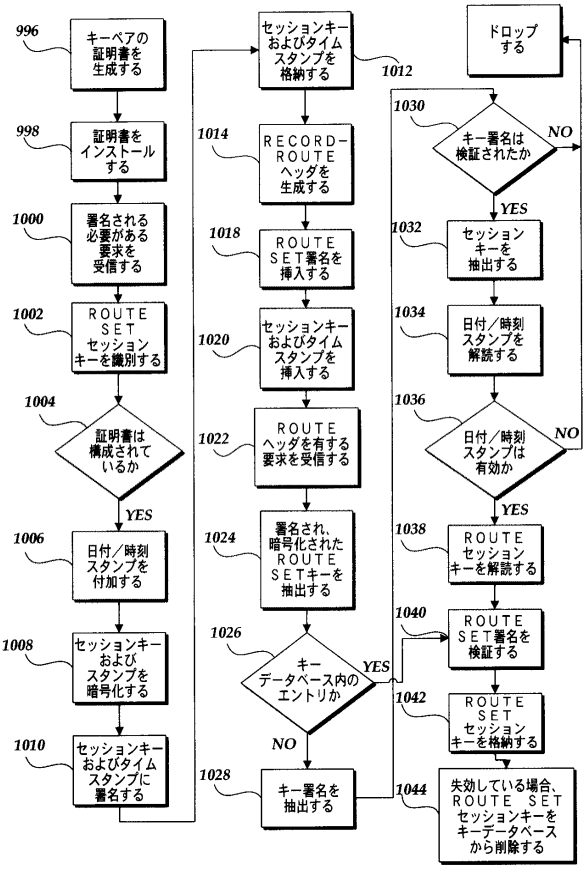
【図１２】



【図１３】


968
応答を受信する
970
RECORD-ROUTEヘッダは存在するか
NO
YES
972
信頼されないリンクを介して受信されたか
NO
YES
974
RECORD-ROUTE署名は存在するか
NO
YES
976
署名を取り外し、保存する
978
RECORD-ROUTEヘッダセットを構築する
980
RECORD-ROUTEセッションキーを取得する
ドロップする
検証RECORD-ROUTE署名を生成する
982
合致したか
NO
YES
984
ROUTE SET署名を削除する
986
次のリンクは信頼されないか
NO
YES
987
ROUTE SETセッションキーを取得する
988
ROUTE SET署名を生成する
990
ROUTE SET署名を挿入する
992
セッションキーを保存する
994
標準の処理を続ける

【図１４】


996
キーペアの証明書を生成する
998
証明書をインストールする
1000
署名される必要がある要求を受信する
1002
ROUTE SETセッションキーを識別する
1004
証明書は構成されているか
YES
1006
日付／時刻スタンプを付加する
1008
セッションキーおよびスタンプを暗号化する
1010
セッションキーおよびタイムスタンプに署名する
セッションキーおよびタイムスタンプを格納する
1012
1014
RECORD-ROUTEヘッダを生成する
1018
ROUTE SET署名を挿入する
1020
セッションキーおよびタイムスタンプを挿入する
1022
ROUTEヘッダを有する要求を受信する
1024
署名され、暗号化されたROUTE SETキーを抽出する
1026
キーデータベース内のエントリか
YES
NO
1028
キー署名を抽出する
ドロップする
1030
キー署名は検証されたか
NO
YES
1032
セッションキーを抽出する
1034
日付／時刻スタンプを解読する
1036
日付／時刻スタンプは有効か
NO
YES
1038
ROUTEセッションキーを解読する
1040
ROUTE SET署名を検証する
1042
ROUTE SETセッションキーを格納する
1044
失効している場合、ROUTE SETセッションキーをキーデータベースから削除する

フロントページの続き

(72)発明者　ジニャン　ス
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　サンカラン　ナラヤナン
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　バデム　エイデルマン
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　西田　聡子

(56)参考文献　特開２００３－１０８５２７（ＪＰ，Ａ）
特表平０８－５０７４１６（ＪＰ，Ａ）
特表２００２－５１２４８７（ＪＰ，Ａ）
国際公開第２００３／０６０６７３（WO，Ａ１）
米国特許出願公開第２００２／０１２９２３６（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３６
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　２９／０６