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

特許第5334104号
(P5334104)

(45)発行日　平成25年11月6日(2013.11.6)　(24)登録日　平成25年8月9日(2013.8.9)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A
H04L 12/22 (2006.01)　H04L 12/22

請求項の数 12　(全 21 頁)

(21)出願番号　特願2008-537721 (P2008-537721)
(86)(22)出願日　平成18年10月3日 (2006.10.3)
(65)公表番号　特表2009-514349 (P2009-514349A)
(43)公表日　平成21年4月2日 (2009.4.2)
(86)国際出願番号　PCT/US2006/038240
(87)国際公開番号　WO2007/053255
(87)国際公開日　平成19年5月10日 (2007.5.10)
審査請求日　平成21年10月1日 (2009.10.1)
(31)優先権主張番号　60/731,798
(32)優先日　平成17年10月31日 (2005.10.31)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/335,487
(32)優先日　平成18年1月19日 (2006.1.19)
(33)優先権主張国　米国 (US)

前置審査

(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　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100153028
弁理士　上田　忠

最終頁に続く

(54)【発明の名称】全交換セッションセキュリティ

(57)【特許請求の範囲】
【請求項１】
２つのサーバ間の通信を安全にすることを促進するシステムであって、
メッセージを送信するサーバを認証する相互認証コンポーネントであって、前記送信するサーバは前記２つのサーバの一方である、相互認証コンポーネントと、
前記メッセージを受信するサーバを認可する相互認可コンポーネントであって、前記受信するサーバは前記２つのサーバの他方である、相互認可コンポーネントと、
前記メッセージのための通信チャネルを暗号的に安全にするチャネル暗号化コンポーネントであって、前記チャネル暗号化コンポーネントは、前記通信チャネルを安全にするために自己署名ＲＳＡ証明書を含むＸ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構を利用し、前記Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、証明書検証なしで利用され、インテグリティおよびプライバシ保護を提供するためにさらに利用され、認証を提供するために利用されるのではなく、前記Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩと連係して動作する、チャネル暗号化コンポーネントと、
前記認証されたサーバおよび認可されたサーバのそれぞれのアイデンティティを検証するチャレンジ／レスポンスコンポーネントであって、前記Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩに基づくハッシュアルゴリズムが使用される、チャレンジ／レスポンスコンポーネントと
を備えることを特徴とするシステム。
【請求項２】

前記相互認証コンポーネントはケルベロス暗号機構であり、前記相互認可コンポーネントはケルベロス暗号機構であることを特徴とする請求項１に記載のシステム。

【請求項３】

前記メッセージはＳＭＴＰメッセージであることを特徴とする請求項１に記載のシステム。

【請求項４】

２つのサーバ間の通信を安全にすることを促進するシステムであって、

メッセージを送信するサーバを認証する相互認証コンポーネントであって、前記送信するサーバは前記２つのサーバの一方である、相互認証コンポーネントと、

前記メッセージを受信するサーバを認可する相互認可コンポーネントであって、前記受信するサーバは前記２つのサーバの他方である、相互認可コンポーネントと、

前記メッセージのための通信チャネルを暗号的に安全にするチャネル暗号化コンポーネントであって、前記チャネル暗号化コンポーネントは、自己署名証明書を含むＡｎｏｎｙｍｏｕｓＴＬＳ機構を利用し、前記自己署名証明書は、前記ＡｎｏｎｙｍｏｕｓＴＬＳ機構によってオンザフライで生成され、前記ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、チャレンジレスポンスの前記自己署名証明書の公開鍵を使用することによってマン・イン・ザ・ミドル（ＭＩＴＭ）攻撃に対して前記通信チャネルを安全にする前記相互認可コンポーネントと緊密に結合されたシーケンスであり、前記相互認可コンポーネントは、様々なセキュリティパッケージトークンを運ぶ認証拡張を備え、前記ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、証明書検証なしで、インテグリティおよびプライバシ保護を提供するために利用され、認証を提供するために利用されるのではない、チャネル暗号化コンポーネントと、

前記送信するサーバおよび受信するサーバのそれぞれのアイデンティティを検証するチャレンジ／レスポンスコンポーネントであって、ＭＵＴＵＡＬＧＳＳＡＰＩに基づくハッシュアルゴリズムが使用される、チャレンジ／レスポンスコンポーネントと

を備えることを特徴とするシステム。

【請求項５】

２つのサーバ間のＳＭＴＰトラフィックを安全にするコンピュータ実行方法であって、

前記ＳＭＴＰトラフィックを送信するサーバを認証するステップと、

前記ＳＭＴＰトラフィックを受信するサーバを認可するステップと、

前記ＳＭＴＰトラフィックの送信を促進する通信チャネルを暗号化するステップであって、前記暗号化するステップは、前記通信チャネルを安全にするために自己署名ＲＳＡ証明書を含むＸ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構を利用し、前記Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、証明書検証なしで利用され、インテグリティおよびプライバシ保護を提供するためにさらに利用され、認証を提供するために利用されるのではなく、前記Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩと連係して動作する、ステップと、

前記送信するサーバと前記受信するサーバの間の通信を安全にするためにチャレンジレスポンス・プロトコルを利用するステップであって、前記Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩに基づくハッシュアルゴリズムが使用される、ステップと

を備えることを特徴とする方法。

【請求項６】

前記認証するステップおよび認可するステップはケルベロス暗号技術を利用することを特徴とする請求項５に記載の方法。

【請求項７】

前記チャレンジレスポンス・プロトコルを利用して前記受信するサーバにチャレンジを送るステップをさらに備えることを特徴とする請求項６に記載の方法。

【請求項８】

認可されていないマン・イン・ザ・ミドル攻撃を回避するために前記受信するサーバからのレスポンスを分析するステップをさらに備えることを特徴とする請求項７に記載の方法。

【請求項９】
２つのサーバ間のＳＭＴＰトラフィックを安全にするコンピュータ実行方法であって、
前記ＳＭＴＰトラフィックを送信するサーバを認証するステップと、
前記ＳＭＴＰトラフィックを受信するサーバを認可するステップと、
前記ＳＭＴＰトラフィックの送信を促進する通信チャネルを暗号化するステップであって、前記暗号化するステップは、自己署名証明書を含むＡｎｏｎｙｍｏｕｓＴＬＳ機構を利用し、前記自己署名証明書は、前記ＡｎｏｎｙｍｏｕｓＴＬＳ機構によってオンザフライで生成され、前記ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、チャレンジレスポンスの前記自己署名証明書の公開鍵を使用することによってマン・イン・ザ・ミドル（ＭＩＴＭ）攻撃に対して前記通信チャネルを安全にする前記相互認可コンポーネントと緊密に結合されたシーケンスであり、前記相互認可コンポーネントは、様々なセキュリティパッケージトークンを運ぶ認証拡張を備え、前記ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、証明書検証なしで、インテグリティおよびプライバシ保護を提供するために利用され、認証を提供するために利用されるのではない、ステップと、
前記送信するサーバおよび受信するサーバのそれぞれのアイデンティティを検証するステップであって、ＭＵＴＵＡＬＧＳＳＡＰＩに基づくハッシュアルゴリズムが使用される、ステップと
を備えることを特徴とする方法。
【請求項１０】
２つのＥｘｃｈａｎｇｅサーバ間の通信のセキュリティを促進するシステムであって、
メッセージを送信するサーバを認証する手段であって、前記送信するサーバは前記２つのＥｘｃｈａｎｇｅサーバの一方である、手段と、
前記メッセージを受信するサーバを認可する手段であって、前記受信するサーバは前記２つのＥｘｃｈａｎｇｅサーバの他方である、手段と、
前記メッセージのための通信チャネルを安全にする手段であって、前記安全にする手段は、自己署名ＲＳＡ証明書を含むＸ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構であり、前記Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、証明書検証なしで利用され、インテグリティおよびプライバシ保護を提供するためにさらに利用され、認証を提供するために利用されるのではなく、前記Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩと連係して動作する、手段と、
前記送信するサーバおよび前記受信するサーバのアイデンティティを検証するチャレンジ／レスポンス機構であって、前記Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩに基づくハッシュアルゴリズムが使用される、チャレンジ／レスポンス機構と
を備えることを特徴とするシステム。
【請求項１１】
前記送信するサーバを認証する手段および前記受信するサーバを認可する手段はケルベロス暗号機構であることを特徴とする請求項１０に記載のシステム。
【請求項１２】
２つのＥｘｃｈａｎｇｅサーバ間の通信のセキュリティを促進するシステムであって、
メッセージを送信するサーバを認証する手段であって、前記送信するサーバは前記２つのＥｘｃｈａｎｇｅサーバの一方である、手段と、
前記メッセージを受信するサーバを認可する手段であって、前記受信するサーバは前記２つのＥｘｃｈａｎｇｅサーバの他方である、手段と、
前記メッセージのための通信チャネルを安全にする手段であって、前記安全にする手段は、自己署名証明書を含むＡｎｏｎｙｍｏｕｓＴＬＳ機構であり、前記自己署名証明書は、前記ＡｎｏｎｙｍｏｕｓＴＬＳ機構によってオンザフライで生成され、前記ＡｎｏｎｙｍｏｕｓＴＬＳ機構は、チャレンジレスポンスの前記自己署名証明書の公開鍵を使用することによってマン・イン・ザ・ミドル（ＭＩＴＭ）攻撃に対して前記通信チャネルを安全にする前記認可する手段と緊密に結合されたシーケンスであり、前記認可する手段は、様々なセキュリティパッケージトークンを運ぶ認証拡張を備え、前記ＡｎｏｎｙｍｏｕｓＴ

ＬＳ機構は、証明書検証なしで、インテグリティおよびプライバシ保護を提供するために利用され、認証を提供するために利用されるのではない、手段と、

前記送信するサーバおよび前記受信するサーバのアイデンティティを検証するチャレンジ／レスポンス機構であって、ＭＵＴＵＡＬＧＳＳＡＰＩに基づくハッシュアルゴリズムが使用される、チャレンジ／レスポンス機構と

を備えることを特徴とするシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、セッションセキュリティに関する。より詳細には、本発明は、全電子メールおよびコラボレーションソフトウェアのセッションセキュリティのためのプロトコルに関する。

【背景技術】

【０００２】

２つのメールサーバ間のトラフィックを安全にすることは、電子データおよび通信のプライバシを維持するために決定的に重要である。たとえば、２つのＥｘｃｈａｎｇｅブランドサーバ間の通信を安全にすることは、電子メールで秘密情報を日常的に送受信する個人および団体には特に有用であり得る。従来のＳＳＬ／ＴＬＳアプローチを使用することは、非常に複雑な証明書ベースの公開鍵インフラストラクチャ（ＰＫＩ）を配備することを必要とする。このことは、メールサーバ、たとえばＥｘｃｈａｎｇｅブランドサーバの多くのユーザのためにＳＭＴＰ（simple mail transfer protocol）トラフィックを安全にすべくＳＳＬ／ＴＬＳを使用するのに非常に大きな障害であることが分かっている。

【０００３】

認証は、コンピュータシステムにログオン中のユーザの識別を検証するプロセス、または送信されたメッセージの保全性を検証するプロセスを参照することができる。多くの場合、認証プロセスを容易にするために認証トークンが利用される。たとえば、認証トークンは、認可されたユーザに渡され、電子メッセージの将来のアクセスおよび／または送信のためにユーザによって所有し保持されることができる。

【０００４】

１つの一般的なネットワーク認証は、ケルベロス（Kerberos）認証プロトコルである。この特定のプロトコルは、安全でないネットワークを介して通信する個人が非常に安全なやり方で互いに自分の身元（identity）を証明することができるようにする。ケルベロス認証プロトコルは、送信データの保全性を保証する上に、盗聴および／または再生攻撃の防止を容易にする。通常、ケルベロスプロトコルは、ユーザとサービスの両方がそれぞれの身元を検証することを要求することにより相互認証が提供されるクライアント－サーバモデルで利用される。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

下記は、本発明のいくつかの態様の基本的な理解を提供するために、本発明の簡略化された要約を提示する。この要約は、本発明の広範囲の概要ではない。この要約は、本発明の主要な／決定的に重要な構成要素を識別すること、または本発明の範囲を定義することを意図するものではない。この要約の唯一の目的は、後ほど提示されるより詳細な説明の序として簡略化された形で本発明のいくつかの概念を提示することである。

【０００６】

本明細書で開示され添付の特許請求の範囲に記載された本発明は、その一態様において、全電子メールおよびコラボレーションソフトウェア（たとえばＥｘｃｈａｎｇｅブランドサーバ）セッションセキュリティのためのプロトコルを備える。例として、同じ団体の中にある、または複数の団体にまたがっている２つのサーバ間のトラフィックを保証することは、しばしば、非常に問題が多い。したがって、従来のＳＳＬ／ＴＬＳアプローチは

、非常に複雑な証明書ベースの公開鍵インフラストラクチャ（ＰＫＩ）を配備することを必要とする。このことは、Ｅｘｃｈａｎｇｅブランドサーバなどのメールサーバの多くのユーザのためにＳＭＴＰトラフィックを安全にすべくＳＳＬ／ＴＬＳを使用するのに非常に大きな障害であることが分かっている。さらに、Ｅｘｃｈａｎｇｅブランドサーバのセキュリティ要件は、相互「認証」だけでなく、相互「認可」をも必要とする。

【０００７】

当然のことながら、２つのＥｘｃｈａｎｇｅブランドサーバ間では、クライアントの役割とサーバの役割に事実上違いはない－－両方とも同等のパーティである。言い換えれば、ちょうど、受信側（サーバ）が、送信側（クライアント）が情報を送信するのを認可することが重要であるのと同様に、送信側は、受信側が情報開示を防止するための情報を受信するのを認可すべきである。この双方向セキュリティプロトコルは、従来のシステムでは不可能であった。

【課題を解決するための手段】

【０００８】

本明細書で開示される新規のシステムおよび／またはプロトコルは、その一態様において、同じ森（たとえば団体）の中にあるのと、異種の森にまたがっているのと、いずれの２つのサーバ、たとえばＥｘｃｈａｎｇｅブランドサーバ間にも、相互に認証され、認可され、暗号化されたチャネルを提供することができる。一態様では、システムは、さらに追加の管理費（administrative overhead）を必要とすることなく「アウトオブザボックス（out-of-the-box）」で利用されることができる。

【０００９】

一態様では、本発明は、複数のメールサーバ間の（たとえばＥｘｃｈａｎｇｅ団体の中の、および／または間の）安全な通信を容易にするために暗号プロトコルトランスポート層セキュリティ（ＴＬＳ：Transport Layer Security）、相互汎用セキュリティサービスアプリケーションプログラムインターフェース（ＭＵＴＵＡＬＧＳＳＡＰＩ：mutual generic security service application program interface）および／またはチャレンジ（challenge）／応答システムを提供する。一態様は、安全な送信を容易にするために前述の３つのプロトコルすべてを利用することを対象とする。他の態様は、相互認可を可能にするＭＵＴＵＡＬＧＳＳＡＰＩを対象とする。

【００１０】

サーバ間のＳＭＴＰトラフィックを安全にすることは、全メールサーバセキュリティの不可欠な部分である。本明細書で開示され添付の特許請求の範囲に記載された新規の諸態様は、２つのサーバのエンドポイントの相互認証および認可を提供し、通信チャネルを暗号化する。アウトオブザボックスで、本発明は、ＳＭＴＰトラフィックの真正さ、プライバシおよび保全性を保証することができる真のピアツーピアセキュリティを可能にする。

【００１１】

概要的に言えば、３つのサブプロトコルは所望の結果を達成することができる。第１に、一態様によれば、通信チャネルを暗号化するために自己署名証明書によるＴＬＳが利用されることができる。このＴＬＳの使用は、前述のようにかなり大きな管理費を追加するＰＫＩ（公開鍵インフラストラクチャ）の配備を必要としないことが理解されるであろう。ＰＫＩは管理費の増加につながる可能性があるが、この、および他の知られている１つ以上の証明書は、本明細書に記載の本発明の新規性に関連して利用されることができることが理解されるべきである。次に、相互認可を可能にすることもできる相互認証（たとえばケルベロス認証）が利用されることができる。最後に、ＴＬＳによって安全にされる２つのエンドポイントが相互認証（たとえばケルベロス）をネゴシエーションしたのと完全に同じエンドポイントであることを保証するためにチャレンジ／応答プロトコルが利用されることができる。このチャレンジ／応答プロトコルは、マン・イン・ザ・ミドル（ＭＩＴＭ）攻撃を防止するのに特に有用であることが理解されるであろう。

【００１２】

本発明の他の態様では、ユーザが自動的に行われることを望む動作を推量するまたは予

測するために、確率および／または統計ベースの分析を利用する人工知能構成要素が提供される。

【００１３】

前述の目的および関連目的の達成のために、本発明のいくつかの例示的態様が本明細書で以下の説明および添付の図面に関連して説明される。しかし、これらの態様は、本発明の原理が利用されることができる様々な方法のいくつかを示すだけであり、本発明は、すべてのそのような態様およびそれらの同等物を含むことを意図するものである。本発明の他の利点および新規の特徴は、図面と併せて考察された場合、本発明の以下の詳細な説明から明らかになるであろう。

【発明を実施するための最良の形態】

【００１４】

次に、本発明は、全体にわたって同様の参照番号は同様の要素を指す図面を参照しながら説明される。以下の説明では、説明のために、本発明の徹底的な理解を提供すべく多数の特定の細目が述べられる。しかし、本発明は、これらの特定の細目なしで実施されることができることは明らかであり得る。他の場合には、本発明の説明を容易にするために、よく知られている構造および装置がブロック図の形で示される。

【００１５】

本出願では、用語「構成要素（component）」および「システム」は、コンピュータ関連エンティティ、つまり、ハードウェア、ハードウェアとソフトウェアの組合せ、ソフトウェア、または実行中のソフトウェアのいずれかを指すことを意図するものである。たとえば、構成要素は、プロセッサ上で稼動中のプロセス、プロセッサ、オブジェクト、実行可能物、実行中のスレッド、プログラム、および／またはコンピュータであるが、それまたはそれらであることに限定されない。説明として、サーバ上で稼動中のアプリケーションおよびそのサーバは、両方とも構成要素であり得る。実行のプロセスおよび／またはスレッドの中に１つまたは複数の構成要素が存在することができ、１つの構成要素は、１つのコンピュータ上に局限される（localize）ことができ、および／または２つ以上のコンピュータ間に分散されることができる。

【００１６】

本明細書では、用語「推量する」または「推量」は、一般に、イベントおよび／またはデータを介して得られた１組の観察結果から、システム、環境、および／またはユーザの状態について論理的に考えるまたは推論するプロセスを指す。推論は、特定のコンテキストまたは動作を識別するために利用されることができ、または、たとえば、状態に関する確率分布を生成することができる。推論は、確率的であり得る－－すなわち、データおよびイベントの考察に基づくインタレスト（interest）の状態に関する確率分布の計算結果であり得る。推論はまた、１組のイベントおよび／またはデータからより高いレベルのイベントを構成するために利用される技術を指すことができる。そのような推論の結果として、１組の観察されたイベントおよび／または格納されているイベントデータから、それらのイベントが密接な時間的接近に相関していてもいなくても、およびそれらのイベントおよびデータが１つまたは複数のイベントおよびデータソースに由来していてもいなくても、新規のイベントまたは動作の構成が生じる。

【００１７】

最初に図面を参照すると、図１は、複数の電子メールサーバ間の全セッションセキュリティを容易にするシステム１００を示す。一般に、システム１００は、２つの異種の電子メールサーバ（１０４、１０６）間の安全な通信を容易にする通信セッションセキュリティ構成要素１０２を含むことができる。図１に示されているシステム１００は、２つの電子メール構成要素を示しているが、本明細書に記載された新規の概念および機構は、いかなる数のサーバを用いて構成されたネットワークによってでも利用されることができることが理解されるべきである。さらに、「電子メール」サーバが図示されているが、新規のセキュリティ概念および／または機構は、本発明の要旨および範囲ならびに添付の特許請求の範囲から逸脱することなく、いかなる形態のデータ通信にも適用されることができる

ことが理解されるべきである。

【００１８】

本明細書で開示され添付の特許請求の範囲に記載された本発明は、その一態様では、全電子メールおよびコラボレーションソフトウェア（たとえばＥｘｃｈａｎｇｅブランドサーバ）セッションセキュリティを可能にするプロトコルを備える。例として、および図１に示されているように、新規のシステムは、同じ団体の中にある、または複数の団体にまたがっている２つのサーバ（１０４、１０６）間のトラフィックを安全にすることができるが、これはしばしば非常に問題が多い。

【００１９】

当然のことながら、従来のＳＳＬ／ＴＬＳアプローチは、非常に複雑な証明書ベースの公開鍵インフラストラクチャ（ＰＫＩ）を配備することを必要とする。この従来のアプローチは、Ｅｘｃｈａｎｇｅブランドサーバなどのメールサーバの多くのユーザのためにＳＭＴＰトラフィックを安全にすべくＳＳＬ／ＴＬＳを使用するのに非常に大きな障害であることが分かっている。さらに、Ｅｘｃｈａｎｇｅブランドサーバのセキュリティ要件は、相互「認証」だけでなく、相互「認可」をも必要とする。

【００２０】

本明細書に記載の諸態様は、Ｅｘｃｈａｎｇｅブランドサーバを対象とするが、本明細書に記載の新規の態様および機能は、本開示の要旨および範囲ならびに添付の特許請求の範囲から逸脱することなく、いかなる通信および／またはデータトラフィックサーバを用いてでも利用されることができることが理解されるべきである。引き続き図１を参照すると、明らかなように、２つのＥｘｃｈａｎｇｅブランドサーバ（たとえば１０４、１０６）間では、クライアントの役割とサーバの役割に事実上違いはない－－両方とも同等のパーティである。言い換えれば、ちょうど受信側（サーバ）が、送信側（クライアント）が情報を送信するのを認可することが重要であるのと同様に、送信側は、受信側が情報開示を防止するための情報を受信するのを認可すべきである。この双方向セキュリティプロトコルは、従来のシステムでは不可能であったことを当業者は理解するであろう。

【００２１】

本明細書で開示される新規のシステム１００および／またはプロトコルは、同じ森（たとえば団体）の中にあるのと、複数の森にまたがっているのと、いずれの２つのサーバ（たとえば１０４、１０６）、たとえばＥｘｃｈａｎｇｅブランドサーバ間にも、（通信セッションセキュリティ構成要素１０２を介して）相互に認証され、認可され、暗号化されたチャネルを提供することができる。一態様では、システムは、さらに追加の管理費を必要とすることなく「アウトオブザボックス」で利用されることができる。

【００２２】

図２は、本発明の一態様による安全な通信を容易にする方法を示す。説明を簡単にするために、たとえば流れ図の形で本明細書に示されている１つまたは複数の方法は一連の動作として示され説明されているが、本発明によるいくつかの動作は、本明細書に示され記載されたものとは異なる順序で、および／または他の動作と同時に生じることもあるので、本発明は、動作の順序によって限定されないことが理解され認識されるべきである。たとえば、ある方法は、代替として、状態図においてなど、一連の相互関係のある状態またはイベントとして表されることができることを当業者は理解し認識するであろう。さらに、すべての例示された動作が本発明による方法を実施することを必要とするとは限らないこともあり得る。

【００２３】

符号２０２で、送信チャネルが暗号化される。通信チャネルを暗号化するために、前述のように、および以下でより詳細に説明されるように、トランスポート層セキュリティ（ＴＬＳ）または同等の暗号技術が利用されることができる。符号２０４で、送信側の認証および受信側の認可が遂行される。一態様では、送信側および受信側の認証および／または認可を容易にするために、新規のＭＵＴＵＡＬＧＳＳＡＰＩプロトコルが利用されることができる。

【００２４】
通信チャネルが暗号化され、送信側および受信側が認証され通信することを認可された後は、セッションセキュリティはさらに安全になることができる。符号２０６で、エンティティ間のデータの通信および／または送信をより安全にするために、チャレンジ／応答機構が利用されることができる。これらの新規のプロセスステップは、個々にならびに組み合わせて、以下の諸図を参照しながらより詳細に説明される。
【００２５】
図３は、本明細書および添付の特許請求の範囲に記載の本発明の新規の機能によるシステム１００の代替ブロック図を示す。詳細には、通信セッションセキュリティコンポーネント１０２は、チャネル暗号化コンポーネント３０２、認証／認可コンポーネント３０４、およびチャレンジ／応答コンポーネント３０６を含むことができる。これら３つのコンポーネント３０２、３０４、３０６は、２つの異種のメールサーバ１０４、１０６間のデータトラフィックを安全にすることを容易にすることが理解され認識されるであろう。
【００２６】
これらのサブ・コンポーネントはそれぞれ、以下の図４を参照しながらより具体的な例に関してより詳細に説明される。特定のプロトコルが図４に記載の態様に従って利用されるが、本明細書に記載の本発明の主旨および範囲から逸脱することなく他の暗号化、認証／認可およびチャレンジ／応答機構を利用する代替態様が存在しうることを理解するべきである。したがって、これらの代替態様は、本開示の範囲および添付の特許請求の範囲に含まれるものとする。
【００２７】
図４は、本発明の一態様によるシステム１００のより具体的な例を示す。この態様では、本発明は、複数のメールサーバ１０４、１０６間の（たとえばインターネットを介した）安全な通信を容易にするために、暗号プロトコルトランスポート層セキュリティ（ＴＬＳ）４０２、相互汎用セキュリティサービスアプリケーションプログラムインターフェース（ＭＵＴＵＡＬＧＳＳＡＰＩ）４０４およびチャレンジ／応答システム４０６を提供する。より詳細には、一態様は、安全な送信を容易にするために、３つの前述のプロトコル４０２、４０４、４０６すべてを対象とする。他の態様は、２つの電子メールサーバ間の新規の相互認証および／または認可を可能にする新規のＭＵＴＵＡＬＧＳＳＡＰＩ１０２を対象とする。
【００２８】
サーバ（たとえば１０４、１０６）間のＳＭＴＰトラフィックを安全にすることは、全体的なメールサーバセキュリティの不可欠な部分である。本明細書で開示され添付の特許請求の範囲に記載された新規の諸態様は、２つのサーバのエンドポイントの相互認証および認可を提供し、通信のチャネルを暗号化する。アウトオブザボックスで、本発明は、ＳＭＴＰトラフィックの真正さ、プライバシおよび保全性を保証することができる真のピアツーピアセキュリティを可能にすることができる。
【００２９】
概要的に言えば、３つのサブプロトコル４０２、４０４、４０６は所望の結果を達成することができる。最初に、通信チャネルを暗号化するために、自己署名証明書によるＴＬＳコンポーネント４０２を利用することができる。このＴＬＳコンポーネント４０２の使用は、前述のようにかなり大きな管理費を追加するＰＫＩ（公開鍵インフラストラクチャ）の配備を必要としないことが理解されるであろう。次に、相互認可を可能にすることもできる相互認証（たとえばケルベロス認証４０４）を利用することができる。最後に、ＴＬＳによって安全にされる２つのエンドポイントが、相互認証（たとえばケルベロス）をネゴシエーションしたのと完全に同じエンドポイントであることを保証するために、チャレンジ／応答プロトコル４０６を利用することができる。このチャレンジ／応答プロトコル４０４は、マン・イン・ザ・ミドル（ＭＩＴＭ）攻撃を防止するのに特に有用であり得ることが理解されるであろう。
【００３０】

前述のように、以下の諸態様はＥｘｃｈａｎｇｅブランドサーバのシナリオにおいて本発明の新規性を利用することを対象とするが、新規の諸態様は、当技術分野で知られているいかなる電子メールサーバおよび／またはデータトラフィックサーバに関連してでも利用できることが理解されるべきである。図４の通信セッションセキュリティコンポーネント１０２に関して上記で説明されたように、トランスポート認証および認可コンポーネントは、Ｅｘｃｈａｎｇｅブランドセキュリティ全体の不可欠な部分である。詳細には、この構成要素、たとえば通信セッションセキュリティコンポーネント１０２は、２つのＥｘｃｈａｎｇｅブランドサーバのエンドポイントを相互に認証し、認可し、チャネルを暗号化することができる。デフォルトで、システムは、ＳＭＴＰトラフィックの真正さ、プライバシおよび保全性を保証することができる真のピアツーピアセキュリティを提供することができる。

【００３１】

Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩコンポーネント１０２に関して、Ｘ－ＥＸＰＳは、様々なセキュリティパッケージトークンを運ぶことができるＥｘｃｈａｎｇｅブランド特有の認証拡張である。Ｅｘｃｈａｎｇｅブランド１２の前に、ＧＳＳＡＰＩ（ＳｐＮｅｇｏパッケージ）は、２つのサーバ（たとえば１０４、１０６）間で認証するために使用されるデフォルトパッケージであったことが理解されるであろう。ＳＭＴＰトラフィックを暗号化することができないことを別にして、ＧＳＳＡＰＩは、従来のウィンドウズ（登録商標）ダムクライアントモデル（windows dumb client model）に従う。これは、ネゴシエーションの後で、クライアントはサーバトークンを所有しないことを意味する。

【００３２】

サーバトークンなしでは、クライアントは、サーバがクライアントを認可するのと同じやり方で、クライアントが許可されているサーバとの適切な対話を認可することができない。前述のように、Ｅｘｃｈａｎｇｅブランドのシナリオでは、クライアントとサーバの役割の点では２つのＥｘｃｈａｎｇｅブランドサーバ間にはほとんど違いはない。両方とも、しばしば同等のパーティであり、唯一の違いは、クライアントが常に会話の開始パーティであることである。したがって、本明細書で開示され添付の特許請求の範囲に記載された新規の相互認可は、情報開示を防止するのに決定的に重要である。

【００３３】

本発明によれば、（Ｅｘｃｈａｎｇｅブランドのシナリオで説明されたように）、ケルベロスＳＳＰＩを利用することができるＭＵＴＵＡＬＧＳＳＡＰＩが導入される。従来のＳｐＮｅｇｏを（ケルベロスとＮＴＬＭとの間でネゴシエーションすることができる）ケルベロスに置き換える１つの理由は、ダウングレード攻撃による不具合（exploit）を防止することである。ＭＵＴＵＡＬＧＳＳＡＰＩは、両方のエンド（サーバ$_1$１０４、サーバ$_2$１０６）がケルベロス会話を開始することができ、その結果、両方とも相手のアクセストークンを入手することができる。

【００３４】

次に、図５を参照すると、一態様では、完全なＭＵＴＵＡＬＧＳＳＡＰＩバッファが、図示されている構造を有することができる。より詳細には、サイズヘッダ５０２、５０４は、バイト単位の各ペイロードセクションの（たとえば、４バイトの固定長の１６進法の値での）サイズを示すことができる。図示されているように、セキュリティブロブペイロード（Security Blob Payload）５０６は、双方向認証ブロブを運ぶことができる。同様に、チャレンジ／応答ペイロード５０８は、ＭＩＴＭ攻撃を防止するためにケルベロス（クライアント－＞サーバ）セッション鍵、ＴＬＳセッション鍵および自己署名ＲＳＡ証明書公開鍵を結合することを可能にすることができるチャレンジ／応答データを運ぶことができる。

【００３５】

次に、Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩ＋Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳの議論に移ると、ケルベロスによって生成されたトークンはＭＩＴＭ攻撃に対して脆弱であり

得るので、本発明は、チャネルを暗号化するために、ネゴシエーションから得られたセッション鍵を利用する。より詳細には、暗号化のためにケルベロスセッション鍵を使用するのではなく、本発明の一態様は同じ目的を達成するためにケルベロスとＴＬＳの組合せを利用する。本質的に、ケルベロスは認証を容易にすることができ、ＴＬＳは暗号化を容易にすることができ、チャレンジ／応答サブプロトコルはＭＩＴＭ攻撃の不具合を防止することができる。この態様は以下でより詳細に説明される。

【００３６】

動作中には、ＭＵＴＵＡＬＧＳＳＡＰＩネゴシエーションの１つの効果は、両方のエンドポイント（たとえばサーバ１０４、１０６）が共有秘密鍵（たとえばケルベロスセッション鍵）を有することである。実際、両側とも、双方向通信から２つのセッション鍵を有する。本発明は、チャレンジ応答のためにクライアント－＞サーバのものを使用する。さらに、両側とも、リモート側のトークンへのアクセス権を所有する。

【００３７】

ＭＩＴＭ攻撃を防止するために、２つのタスクが遂行される。第１に、トークンバッファの保全性およびプライバシがＴＬＳの下で保護されなければならない。第２に、チャレンジ／応答プロトコルが、ＭＵＴＵＡＬＧＳＳＡＰＩをネゴシエーションした両方のエンドポイントはまたＴＬＳをネゴシエーションしたのと同じパーティであることを証明しなければならない。自己署名ＲＳＡ証明書の公開鍵は、ＭＩＴＭがクライアントとサーバの両方に攻撃者と同じＴＬＳセッション鍵をネゴシエーションさせることができないように、チャレンジ応答プロトコルのハッシュに含まれる。マン・イン・ザ・ミドル攻撃は、攻撃者が同時に３つの鍵（ＴＬＳセッション鍵、ケルベロスセッション鍵およびＲＳＡ証明書公開鍵）すべてを所有しているわけではないので、排除される。

【００３８】

本発明の新規の特徴は、Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳと呼ばれる新規の拡張の導入である。動作中、Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳは、証明書検証がないことを除いて、ＳＴＡＲＴＴＬＳのように振る舞う。したがって、ＴＬＳは、本発明に関連して、保全性およびプライバシ保護を提供するために利用されるのであって、必ずしも認証を提供するためではないことが理解されるべきである。Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳによって使用される証明書は、メモリストアで生成された自己署名ＲＳＡ証明書である。Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳは、Ｘ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩと連係して動作する。さらに、本発明は、このプロトコルシーケンスを実施する。さらに、サーバは、「ＭＵＴＵＡＬＧＳＳＡＰＩＨＡＳＨ」と呼ばれる新規の拡張の下で受け入れ可能であると考えるチャレンジ－応答サブプロトコルで使用されるハッシュアルゴリズムを通知することができる。クライアントは適切と考えるものを選択し、サーバに送信される第１のブロブ（たとえば図５の５０６）にその選択を示すことができる。

【００３９】

図６は、通常の成功したＸ－ＡｎｏｎｙｍｏｕｓＴＬＳ＋ＭＵＴＵＡＬＧＳＳＡＰＩセッションの下での例示的プロトコルシーケンスを示す。下記は図６の動作説明による動作である。

【００４０】

１）ＳｍｔｐＯｕｔがそれ自体のサーバＦＱＤＮ（ＳｍｔｐＯｕｔＦＱＤＮ）と共にｅｈｌｏをＳｍｔｐＩｎに送信する。

【００４１】

２）ＳＭＴＰ　ＲＦＣによって、ＳｍｔｐＩｎがそれ自体のＦＱＤＮ（ＳｍｔｐＩｎＦＱＤＮ）ならびにｘ－ａｎｏｎｙｍｏｕｓｔｌｓを通知するバナーと共に応答する。ＳｍｔｐＩｎはまた、同時にｓｔａｒｔｔｌｓを通知することができる。ＭＵＴＵＡＬＧＳＳＡＰＩは、ｘ－ａｎｏｎｙｍｏｕｓｔｌｓが確立されるまで通知されない。

【００４２】

３）ＳｍｔｐＯｕｔは、ＳｍｔｐＩｎとのｘ－ａｎｏｎｙｍｏｕｓｔｌｓネゴシエーションをすることを選択する。結果として、ＴＬＳセッションが確立される。

【００４３】
４）ＳＭＴＰ　ＲＦＣによって、ＳｍｔｐＯｕｔが別のｅｈｌｏをＳＭＴＰに送信する。
【００４４】
５）ＳｍｔｐＩｎは、今度はＸ－ＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩのサポートを示すバナーと共に応答する。同時に、ｓｔａｒｔｔｌｓおよびｘ－ａｎｏｎｙｍｏｕｓｔｌｓは両方とも、セッションがすでにＴＬＳになっているので、バナーから除去される。さらに、ＳｍｔｐＩｎはまた、ＭＵＴＵＡＬＧＳＳＡＰＩプロトコルで使用されるハッシュ法としてＳＨＡ２５６およびＳＨＡ１を両方ともサポートすることを通知する。
【００４５】
６）ＳｍｔｐＯｕｔが、ｅｈｌｏ応答で取得されたＳｍｔｐＩｎＦＱＤＮを使用してＳｍｔｐＩｎのためのケルベロスチケットを取得する。チケットは、上記の図ではＩＳＣ１として表されている。この時点で、ＳｍｔｐＯｕｔは、ケルベロスセッション鍵ならびにＴＬＳ共有秘密鍵を取得している。したがって、ＳｍｔｐＯｕｔは、チャレンジ＝ＳＨＡ２５６（ＫｅｒｂｅｒｏｓＫｅｙ＋ＴＬＳＫｅｙ＋ＣｅｒｔＰｕｂＫｅｙ）を構成することができる。ＳｍｔｐＯｕｔは、より安全なのでＳＨＡ２５６を選択する。最後に、ＳｍｔｐＯｕｔは、選択したハッシュ法、ケルベロスチケット、およびチャレンジをＳｍｔｐＩｎに送信する。この時点で、ＳｍｔｐＯｕｔに関する限り、アウトバウンド（outbound）ケルベロス認証は終了し、チャレンジは送信されてしまっているが、応答は検証されていない。
【００４６】
７）ＳｍｔｐＩｎがステップ６におけるペイロードを解析する。ＳｍｔｐＩｎは、ＳｍｔｐＯｕｔがチャレンジ／応答サブプロトコルで使用されるハッシュのためにＳＨＡ２５６を選択したことを知っている。ＳｍｔｐＩｎが、ＳｍｔｐＯｕｔのケルベロスチケット（ＩＳＣ１）を検証する。ケルベロスの下で、このコールは、成功するかまたは別のチケットトークンを生成せずに失敗するはずである。チケット検証が成功した場合、ＳｍｔｐＩｎはＳｍｔｐＯｕｔのチャレンジを検証し、応答を生成する。成功した場合、ＳｍｔｐＩｎはＳｍｔｐＯｕｔを認証してしまっている。ＳｍｔｐＩｎは、ＳｍｔｐＯｕｔへのチケットを取得しようとする前に、ＳｍｔｐＯｕｔのトークンに対する完全な認可チェックをする。認証も認可も完了した後で、ＳｍｔｐＩｎは、ＳｍｔｐＯｕｔにアクセスするためにケルベロスチケット（ＩＳＣ２）を取得しようとする。最後に、ＳｍｔｐＩｎは、ＩＳＣ２および応答をＳｍｔｐＯｕｔに送信し返す。この時点で、ＳｍｔｐＩｎは、ＳｍｔｐＯｕｔを十分に認証し認可してしまっている。
【００４７】
８）ＳｍｔｐＯｕｔは、ＩＳＣ２＋応答を解析する。ＳｍｔｐＯｕｔは、最初に応答を検証する。成功した場合、ＳｍｔｐＯｕｔは、ＳｍｔｐＩｎのトークンを取得するためにＩＳＣ２を検証し始める。これも成功した場合、ＳｍｔｐＯｕｔは、ＳｍｔｐＩｎを認可するためにステップ７の場合と同じ認可チェックを行う。次いで、ＳｍｔｐＯｕｔは、ＳｍｔｐＩｎを十分に認証し認可してしまう。
【００４８】
９）ＳｍｔｐＩｎ側のいかなるフレーズにおけるいかなるエラー（たとえば、ケルベロスチケットの取得または検証の失敗、またはチャレンジ検証時のエラー）も、サーバ側に５ｘｘエラーを送信させ切断させる。同様に、ＳｍｔｐＯｕｔ側のこのプロトコルシーケンスにおけるいかなるエラーも、ＳｍｔｐＯｕｔ側にセッションをキャンセルさせドロップさせる。
【００４９】
次に、チャレンジ／応答機構の議論に移ると、チャレンジ／応答の１つの目的は、両側が同じケルベロスおよびＴＬＳセッション鍵、ならびに自己署名ＲＳＡ証明書の公開鍵を有していることを証明することである。ケルベロスプロトコルに基づいて、ＳｍｔｐＯｕｔは常にチャレンジャである。いかなるハッシュアルゴリズムでも、本発明の代替態様で

利用可能なことが理解されるべきである。一態様では、
チャレンジ＝ＳＨＡ２５６（ＫｅｒｂｅｒｏｓＫｅｙ＋ＴｌｓＫｅｙ＋ＣｅｒｔＰｕｂＫｅｙ）
応答＝ＳＨＡ２５６（チャレンジ＋ＫｅｒｂｅｒｏｓＫｅｙ＋ＴｌｓＫｅｙ＋ＣｅｒｔＰｕｂＫｅｙ）
である。

【００５０】

サーバがそれ自体のデータに基づいて同じハッシュを計算した場合、チャレンジャは３つの鍵すべての所有を証明する。攻撃者は３つの鍵すべてを知ることができるわけではないことが理解されるであろう。応答者は、３つの鍵およびチャレンジのバージョンをハッシュの中に入れることにより３つの鍵すべての所有を証明することができる。相手は、同じ情報を所有している唯一の他のパーティなので、検証することができるであろう。攻撃者（ＭＩＴＭ）は、ＣｅｒｔＰｕｂＫｅｙがチャレンジ応答に含まれているので、クライアントおよびサーバに別個のＴＬＳセッションを行わせ、それでもなお同じＴＬＳセッション鍵を生成させることはできない。これは、本質的に、ＴＬＳに対する従来のＭＩＴＭ攻撃を防止する証明書検証に相当する。

【００５１】

認証ステートマシン（state machine）に関して、各側は、ネゴシエーション状態を追跡するために、以下の状態変数を有する。

【００５２】

・Ｎｏｎｅ
・ＩｎｂｏｕｎｄＳｅｃｕｒｅｄ
・ＯｕｔｂｏｕｎｄＳｅｃｕｒｅｄ
・Ｓｕｃｃｅｓｓ－－インバウンドおよびアウトバウンドが両方とも安全にされ、チャレンジ／応答が検証される。

【００５３】

両方の認証指示が成功であった場合、安全なチャネルが確立されることができる。さらに、チャレンジ／応答状態が検証されることができる。さらに、各側は、認可チェックのためにリモート（remote）のアクセストークン（access token）を所有している。

【００５４】

本発明は、ＴＬＳ＋ＭＵＴＵＡＬＧＳＳＡＰＩのセキュリティ分析を開示する。ハッカーは多分３つの鍵（たとえば、ケルベロス、ＴＬＳセッション鍵およびＣｅｒｔＰｕｂＫｅｙ）すべてを知ることができるわけではないので、ＴＬＳ＋ＭＵＴＵＡＬＧＳＳＡＰＩはＭＩＴＭ攻撃を防止することができる。ハッカーがサーバＡおよびサーバＢとの別個のＴＬＳ会話を真ん中に挿入しこれに関与した場合、攻撃者はケルベロスセッション鍵のないチャレンジ応答によって検出されるであろう。攻撃者は検出されないチャネルを復号または改変することはできないであろうから、ハッカーはサーバＡとサーバＢとの間の直接ＴＬＳ会話を盗聴することはできないであろう。

【００５５】

前述のように、ＭＩＴＭ攻撃を防止するために、ＣｅｒｔＰｕｂＫｅｙ（または同等物）がチャレンジ応答プロトコルに含まれなければならない。これを実施するために、ｘ－ａｎｏｎｙｍｏｕｓｔｌｓは、自己署名ＲＳＡ証明書（または同等物）をオンザフライで生成し、それをインメモリストア（in-memory store）に格納する。ＲＳＡ鍵交換の下で、クライアントがサーバの証明書を検証しない場合、ＭＩＴＭ攻撃は、クライアントとサーバの両方に攻撃者と同じＴＬＳセッション鍵を生成させることが可能である。ＭＩＴＭ攻撃は、そうすることができる場合、チャレンジ／応答プロトコルの目的を無効にする。したがって、本発明は、この攻撃を無効にするために、チャレンジ応答にＲＳＡ証明書の公開鍵を含める。

【００５６】

それでもなお、可能な攻撃は、ＴＬＳとＭＵＴＵＡＬＧＳＳＡＰＩの結合を解くために

、プロトコル実施エラーを利用することができる。したがって、本発明の新規の設計は、Ｘ－ＡｎｏｎｙｍｏｕｓＴＬＳおよびＥＸＰＳ　ＭＵＴＵＡＬＧＳＳＡＰＩが緊密に結合されたシーケンスであることを強調する。最後に、いかなる他のセキュリティ対策の場合とも同様に、両側のサーバの完全な妥協が、ＴＬＳ＋ＭＵＴＵＡＬＧＳＳＡＰＩ機構を完全に無効にする。

【００５７】

次に、図７を参照すると、セッションセキュリティに関する開示されたアーキテクチャを実行するために動作可能なコンピュータのブロック図が示されている。本発明の様々な態様のための追加のコンテキストを提供するために、図７および以下の議論は、本発明の様々な態様が実施されることができる適切なコンピューティング環境７００の簡潔な一般的説明を提供することを意図するものである。本発明は、上記で、１つまたは複数のコンピュータ上で実行することができるコンピュータ実行可能命令の一般的コンテキストで説明されてきたが、本発明はまた、他のプログラムモジュールと併せて、および／またはハードウェアとソフトウェアの組合せとして、実施されることができることを当業者は理解するであろう。

【００５８】

一般に、プログラムモジュールは、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施するルーチン、プログラム、コンポーネント、データ構造などを含む。さらに、本発明の方法は、シングルプロセッサまたはマルチプロセッサコンピュータシステム、ミニコンピュータ、メインフレームコンピュータ、ならびにそれぞれが１つまたは複数の関連装置に動作可能に結合されたパーソナルコンピュータ、ハンドヘルドコンピューティング装置、マイクロプロセッサベースのまたはプログラマブルコンシューマ電子機器などを含めて、他のコンピュータシステム構成で実施されることができることを当業者は理解するであろう。

【００５９】

本発明の図示されている諸態様はまた、いくつかのタスクが通信ネットワークを介してリンクされたリモート処理装置によって実行される分散コンピューティング環境で実施されることができる。分散コンピューティング環境では、プログラムモジュールは、ローカルメモリ記憶装置とリモートメモリ記憶装置の両方に配置されることができる。

【００６０】

コンピュータは、通常、様々なコンピュータ可読媒体を含む。コンピュータ可読媒体は、コンピュータによってアクセス可能ないかなる利用可能な媒体でもよく、揮発性媒体と不揮発性媒体、取り外し可能な媒体と取り外し不可能な媒体の両方を含む。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備えることができる。コンピュータ記憶媒体は、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他のデータの格納のためのいかなる方法または技術ででも実施される揮発性媒体と不揮発性媒体、取り外し可能な媒体と取り外し不可能な媒体の両方を含む。コンピュータ記憶媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）または他の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置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ために使用されることができ、コンピュータによってアクセス可能な他のいかなる媒体をも含むが、それらに限定されない。

【００６１】

通信媒体は、通常、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、あるいは、搬送波または他のトランスポート機構などの変調データ信号内の他のデータを包含し、いかなる情報配送媒体をも含む。用語「変調データ信号」は、信号内の情報をエンコードするようなやり方で設定または変更された特性のうちの１つまたは複数を有する信号を意味する。通信媒体は、例として、しかし限定としてではなく、有線ネットワークまたは直接有線接続などの有線媒体、ならびに音響、ＲＦ、赤外線および他の無線媒体などの無線媒体を含む。上記のいずれかの組合せもまた、コンピュータ可読媒体の範囲内に含ま

れるべきである。

【００６２】

再度図７を参照すると、本発明の様々な態様を実施するための例示的環境７００は、コンピュータ７０２を含み、コンピュータ７０２は処理ユニット７０４、システムメモリ７０６およびシステムバス７０８を含む。システムバス７０８は、システムメモリ７０６を含むがそれに限定されないシステム構成要素を処理ユニット７０４に結合する。処理ユニット７０４は、様々な市販のプロセッサのいずれでもよい。デュアルマイクロプロセッサおよび他のマルチプロセッサアーキテクチャもまた処理ユニット７０４として利用されることができる。

【００６３】

システムバス７０８は、（メモリコントローラのある、またはない）メモリバス、周辺バス、および様々な市販のバスアーキテクチャのいずれかを使用するローカルバスにさらに相互接続するいくつかのバス構造タイプのいずれでもよい。システムメモリ７０６は、読み出し専用メモリ（ＲＯＭ）７１０およびランダムアクセスメモリ（ＲＡＭ）７１２を含む。基本入出力システム（ＢＩＯＳ）は、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭなどの不揮発性メモリ７１０に格納されており、そのＢＩＯＳには、起動中などにコンピュータ７０２の中の構成要素間で情報を転送するのに役立つ基本ルーチンが入っている。ＲＡＭ７１２は、データをキャッシュするためのスタティックＲＡＭなどの高速ＲＡＭも含む。

【００６４】

コンピュータ７０２は、適切なシャーシ（chassis）（図示されていない）で外部使用のために構成されてもよい内蔵ハードディスクドライブ（ＨＤＤ）７１４（たとえばＥＩＤＥ、ＳＡＴＡ）、（たとえば、取り外し可能なディスケット７１８から読み出すまたはそれに書き込むための）磁気フロッピー（登録商標）ディスクドライブ（ＦＤＤ）７１６、および（たとえば、ＣＤ－ＲＯＭディスク７２２を読む、またはＤＶＤなど他の高容量光媒体から読み出すまたはそれに書き込むための）光ディスクドライブ７２０をさらに含む。ハードディスクドライブ７１４、磁気ディスクドライブ７１６および光ディスクドライブ７２０は、それぞれ、ハードディスクドライブインターフェース７２４、磁気ディスクドライブインターフェース７２６および光ドライブインターフェース７２８によってシステムバス７０８に接続されることができる。外付けドライブ実装形態のためのインターフェース７２４は、ユニバーサルシリアルバス（ＵＳＢ）技術とＩＥＥＥ１３９４インターフェース技術の少なくとも１つまたは両方を含む。他の外付けドライブ接続技術は、本発明の企図の範囲内にある。

【００６５】

ドライブおよびそれらの関連コンピュータ可読媒体は、データの不揮発性ストレージ、データ構造、コンピュータ実行可能命令などを提供する。コンピュータ７０２では、ドライブおよび媒体は、適切なデジタルフォーマットのいかなるデータのストレージにも対応する。上記のコンピュータ可読媒体の説明は、ＨＤＤ、取り外し可能な磁気ディスケット、およびＣＤまたはＤＶＤなどの取り外し可能な光媒体に言及しているが、ジップドライブ（zip drives）、磁気カセット、フラッシュメモリカード、カートリッジなど、コンピュータによって読み出し可能な他のタイプの媒体もまた例示的動作環境で使用されてもよいこと、さらに、いかなるそのような媒体にも本発明の方法を実施するためのコンピュータ実行可能命令が入っていてもよいことが当業者によって理解されるべきである。

【００６６】

いくつかのプログラムモジュールは、オペレーティングシステム７３０、１つまたは複数のアプリケーションプログラム７３２、他のプログラムモジュール７３４およびプログラムデータ７３６を含むドライブおよびＲＡＭ７１２に格納されることができる。オペレーティングシステム、アプリケーション、モジュール、および／またはデータのすべてまたは一部は、ＲＡＭ７１２にキャッシュされることもできる。本発明は、様々な市販のオペレーティングシステムまたはオペレーティングシステムの組合せを用いて実施されることができることが理解される。

【００６７】
ユーザは、コマンドおよび情報を１つまたは複数の有線／無線入力装置、たとえばキーボード７３８、およびマウス７４０などのポインティングデバイスを介して、コンピュータ７０２に入力することができる。他の入力装置（図示されていない）には、マイクロホン、ＩＲリモートコントロール、ジョイスティック、ゲームパッド、スタイラスペン、タッチスクリーンなどが含まれ得る。これらおよび他の入力装置は、しばしば、システムバス７０８に結合されている入力装置インターフェース７４２を介して処理ユニット７０４に接続されるが、パラレルポート、ＩＥＥＥ１３９４シリアルポート、ゲームポート、ＵＳＢポート、ＩＲインターフェースなど、他のインターフェースによって接続されることができる。

【００６８】
モニタ７４４または他のタイプの表示装置も、ビデオアダプタ７４６などのインターフェースを介してシステムバス７０８に接続される。モニタ７４４のほかに、コンピュータは通常スピーカ、プリンタなど、他の周辺出力装置（図示されていない）を含む。

【００６９】
コンピュータ７０２は、リモートコンピュータ７４８など、１つまたは複数のリモートコンピュータへの有線および／または無線通信を介した論理接続を使用してネットワーク接続された環境で動作することができる。リモートコンピュータ７４８は、ワークステーション、サーバコンピュータ、ルータ、パーソナルコンピュータ、ポータブルコンピュータ、マイクロプロセッサベースのエンタテインメント機器、ピアデバイスまたは他の一般的なネットワークノードでもよく、簡潔のためにメモリ／記憶装置７５０だけしか図示されていないが、通常、コンピュータ７０２に関して記述される要素の多くまたはすべてを含む。図示された論理接続は、ローカルエリアネットワーク（ＬＡＮ）７５２および／またはより大きなネットワーク、たとえば広域ネットワーク（ＷＡＮ）７５４への有線／無線接続を含む。そのようなＬＡＮおよびＷＡＮネットワーキング環境は、オフィスや会社では普通であり、それらのすべてがインターネットなどのグローバル通信ネットワークに接続することができるイントラネットなどの企業全体のコンピュータネットワークを容易にする。

【００７０】
ＬＡＮネットワーク環境で使用される場合、コンピュータ７０２は、有線および／または無線通信ネットワークインターフェースまたはアダプタ７５６を通してローカルネットワーク７５２に接続される。アダプタ７５６は、無線アダプタ７５６と通信するためにその上に配置された無線アクセスポイントを含むこともできるＬＡＮ７５２への有線または無線通信を容易にすることができる。

【００７１】
ＷＡＮネットワーク環境で使用される場合、コンピュータ７０２は、モデム７５８を含んでもよく、またはＷＡＮ７５４上の通信サーバに接続される、または、インターネットとしてなど、ＷＡＮ７５４を介した通信を確立する他の手段を有する。内蔵でも外付けでもよく、有線装置でも無線装置でもよいモデム７５８は、シリアルポートインターフェース７４２を介してシステムバス７０８に接続される。ネットワーク接続された環境では、コンピュータ７０２に関して図示されているプログラムモジュールまたはその一部は、リモートメモリ／記憶装置７５０に格納されることができる。図示されているネットワーク接続は例示的であり、コンピュータ間の通信リンクを確立する他の手段が使用されることができることが理解されるであろう。

【００７２】
コンピュータ７０２は、無線通信に動作可能に配置された任意の無線装置またはエンティティ、たとえば、プリンタ、スキャナ、デスクトップコンピュータおよび／またはポータブルコンピュータ、携帯情報端末、通信衛星、無線で検出可能なタグに関連付けられた機器または場所（たとえばキオスク、新聞売り場、トイレ）の任意の一部分、および電話機と通信するように動作可能である。これは少なくともＷｉ－Ｆｉ無線技術およびブルー

トゥース（商標）無線技術を含む。したがって、通信は、従来のネットワークの場合と同様に予め定義された構造でもよく、または単に少なくとも２つの装置間のアドホック通信でもよい。

【００７３】

Ｗｉ－Ｆｉ、すなわちワイヤレスフェデリティは、ワイヤなしで、家庭のソファ、ホテルのベッドルーム、または会議中の会議室からインターネットへの通信を可能にする。Ｗｉ－Ｆｉは、そのような装置、たとえばコンピュータが室内および戸外で、すなわち基地局の範囲内のどこででも、データを送受信することができるようにする携帯電話で使用されるものと同様の無線技術である。Ｗｉ－Ｆｉネットワークは、安全で信頼できる高速無線接続を提供するために、ＩＥＥＥ８０２．１１（ａ、ｂ、ｇなど）と呼ばれる無線技術を使用する。Ｗｉ－Ｆｉネットワークは、コンピュータを相互に、インターネットに、および（ＩＥＥＥ８０２．３またはイーサネット（登録商標）を使用する）有線ネットワークに接続するために使用されることができる。Ｗｉ－Ｆｉネットワークは、たとえば１１Ｍｂｐｓ（８０２．１１ａ）または５４Ｍｂｐｓ（８０２．１１ｂ）データ速度で、無許可の２．４ＧＨｚおよび５ＧＨｚ無線帯域で、または、両方の帯域（デュアルバンド）を含む製品で動作し、したがって、ネットワークは、多くのオフィスで使用される１０ＢａｓｅＴ有線イーサネット（登録商標）ネットワークと同様のリアルワールドパフォーマンス（real-world performance）を提供することができる。

【００７４】

次に、図８を参照すると、本発明による例示的コンピューティング環境８００の概略ブロック図が示されている。システム８００は、１つまたは複数のクライアント８０２を含む。クライアント８０２は、ハードウェアおよび／またはソフトウェア（たとえばスレッド、プロセス、コンピューティング装置）でよい。クライアント８０２は、たとえば、本発明を利用することにより、クッキーおよび／または関連コンテキスト情報を収容することができる。

【００７５】

システム８００はまた、１つまたは複数のサーバ８０４を含む。サーバ８０４も、ハードウェアおよび／またはソフトウェア（たとえばスレッド、プロセス、コンピューティング装置）でよい。サーバ８０４は、たとえば、本発明を利用することにより変換を行うスレッドを収容することができる。クライアント８０２とサーバ８０４との間の１つの可能な通信は、２つ以上のコンピュータプロセス間で送信されるように適応されたデータパケットの形ででもよい。データパケットは、クッキーおよび／または関連コンテキスト情報を含むことができる。システム８００は、クライアント８０２とサーバ８０４との間の通信を容易にするために利用されることができる通信フレームワーク８０６（たとえば、インターネットなどのグローバル通信ネットワーク）を含む。

【００７６】

有線（光ファイバを含む）および／または無線技術を介して通信を容易にすることができる。クライアント８０２は、クライアント８０２にローカルな情報（たとえばクッキーおよび／または関連コンテキスト情報）を格納するために利用されることができる１つまたは複数のクライアントデータストア８０８に動作可能に接続される。同様に、サーバ８０４は、サーバ８０４にローカルな情報を格納するために利用されることができる１つまたは複数のサーバデータストア８１０に動作可能に接続される。

【００７７】

上記で説明されてきたものは、本発明の実施例を含む。もちろん、本発明を説明するために、構成要素または方法のすべての考えられる組合せを記述することは不可能であるが、本発明の多くの別の組合せおよび変更が可能であることを当業者は理解することができる。したがって、本発明は、添付の特許請求の範囲の要旨および範囲に入るすべてのそのような改変形態、変更形態および変形形態を包含することを意図するものである。さらに、用語「含む（includes）」は、本明細書または特許請求の範囲で使用される限り、当該用語は、「備える（comprising）」が請求項における移行語（transitional word）とし

て利用される場合に解釈されるように、用語「備える（comprising）」と同様に包括的であることを意図するものである。

【図面の簡単な説明】

【００７８】

【図１】本発明の一態様による全交換セッションセキュリティを容易にするシステムを示す図である。

【図２】本発明の一態様による送信セキュリティを容易にする手順の例示的フロー図である。

【図３】本発明の一態様によるチャネル暗号化コンポーネント、認証／認可コンポーネント、およびチャレンジ／応答コンポーネントを利用する一般的なシステムのブロック図である。

【図４】本発明の一態様による安全な通信を容易にするためにＴＬＳコンポーネント、ケルベロス認証コンポーネントおよびＲＳＡ証明書コンポーネントを利用する特定のシステムのブロック図である。

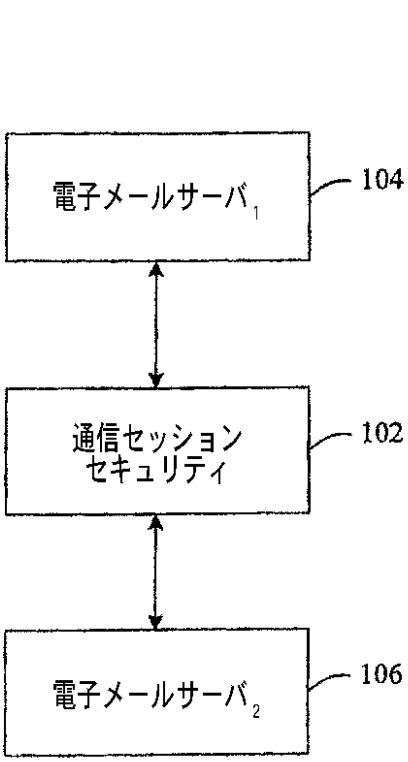
【図５】本発明の一態様による完全なＭＵＴＵＡＬＧＳＳＡＰＩバッファの例示的構造を示す図である。

【図６】本発明の一態様による通常の成功したｘ－ａｎｏｎｙｍｏｕｓｔｌｓ＋ＭＵＴＵＡＬＧＳＳＡＰＩセッションの下での例示的プロトコルシーケンスを示す図である。

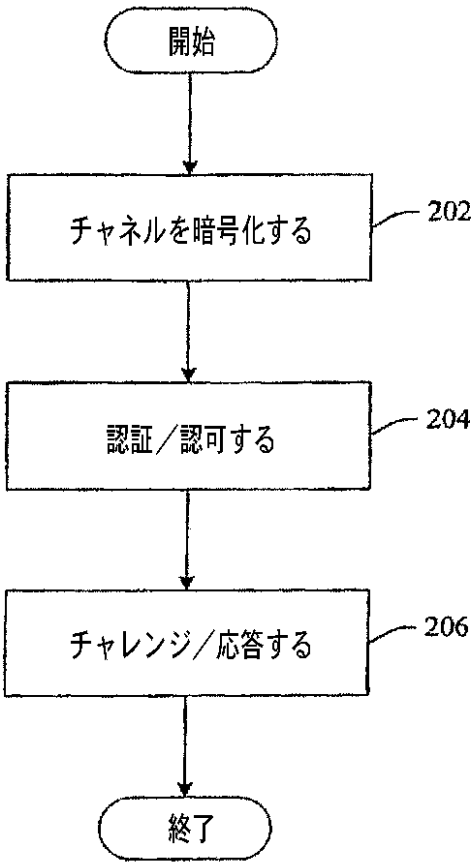
【図７】開示されたアーキテクチャを実行するように動作可能なコンピュータのブロック図である。

【図８】本発明による例示的コンピューティング環境の概略ブロック図である。

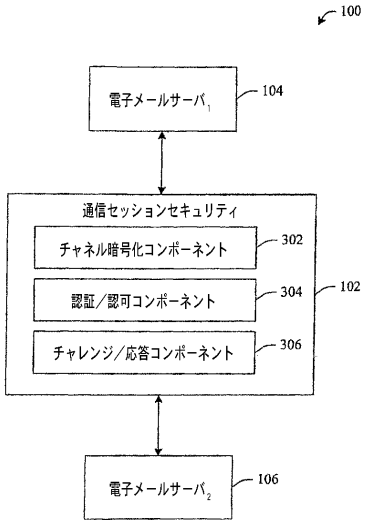
【図１】



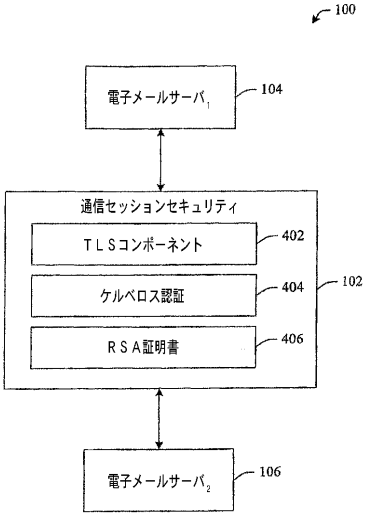
【図２】



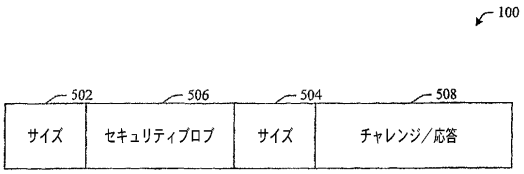
【図３】


100
電子メールサーバ1
104
通信セッションセキュリティ
チャネル暗号化コンポーネント
302
認証／認可コンポーネント
304
102
チャレンジ／応答コンポーネント
306
電子メールサーバ2
106

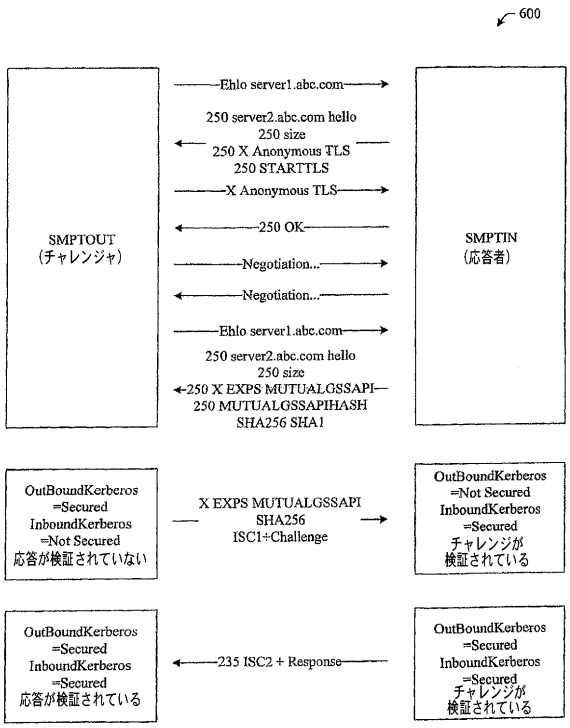
【図４】


100
電子メールサーバ1
104
通信セッションセキュリティ
TLSコンポーネント
402
ケルベロス認証
404
102
RSA証明書
406
電子メールサーバ2
106

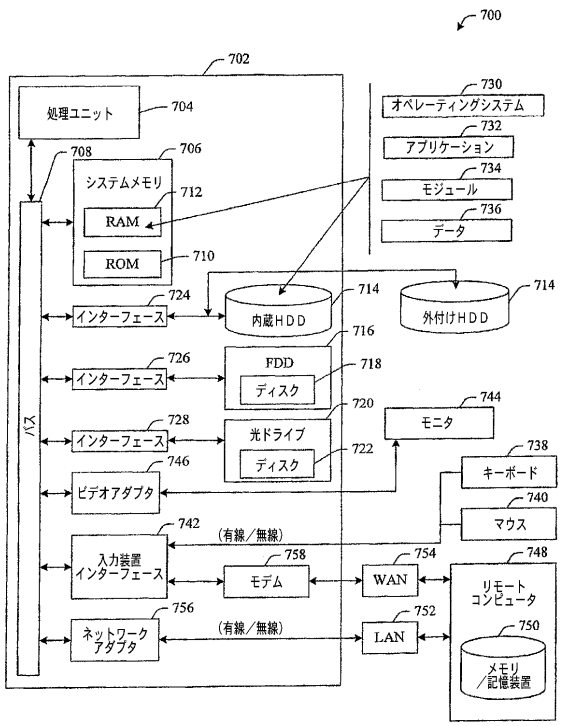
【図５】


100
502
506
504
508
サイズ
セキュリティブロブ
サイズ
チャレンジ／応答

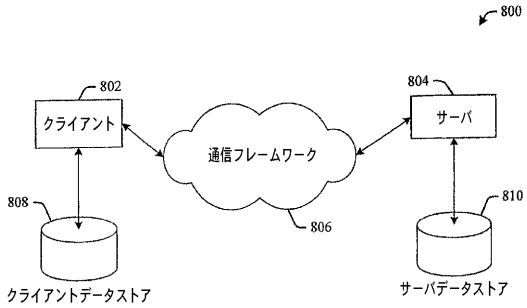
【図６】


600
SMPTOUT
（チャレンジャ）
SMPTIN
（応答者）
Ehlo server1.abc.com
250 server2.abc.com hello
250 size
250 X Anonymous TLS
250 STARTTLS
X Anonymous TLS
250 OK
Negotiation...
Negotiation...
Ehlo server1.abc.com
250 server2.abc.com hello
250 size
250 X EXPS MUTUALGSSAPI
250 MUTUALGSSAPIHASH
SHA256 SHA1
OutBoundKerberos
=Secured
InboundKerberos
=Not Secured
応答が検証されていない
X EXPS MUTUALGSSAPI
SHA256
ISC1+Challenge
OutBoundKerberos
=Not Secured
InboundKerberos
=Secured
チャレンジが
検証されている
OutBoundKerberos
=Secured
InboundKerberos
=Secured
応答が検証されている
235 ISC2 + Response
OutBoundKerberos
=Secured
InboundKerberos
=Secured
チャレンジが
検証されている

【図７】


700
702
処理ユニット
704
システムメモリ
706
708
RAM
712
ROM
710
バス
インターフェース
724
内蔵HDD
714
外付けHDD
714
FDD
716
ディスク
718
インターフェース
726
光ドライブ
720
ディスク
722
インターフェース
728
ビデオアダプタ
746
入力装置
インターフェース
742
ネットワーク
アダプタ
756
モデム
758
WAN
754
LAN
752
リモート
コンピュータ
748
メモリ
／記憶装置
750
オペレーティングシステム
730
アプリケーション
732
モジュール
734
データ
736
モニタ
744
キーボード
738
マウス
740
（有線／無線）
（有線／無線）

【図８】


800
802
クライアント
804
サーバ
通信フレームワーク
806
808
クライアントデータストア
810
サーバデータストア

フロントページの続き

(74)代理人 100120112
弁理士 中西 基晴
(74)代理人 100147991
弁理士 鳥居 健一
(74)代理人 100119781
弁理士 中村 彰吾
(74)代理人 100162846
弁理士 大牧 綾子
(74)代理人 100173565
弁理士 末松 亮太
(74)代理人 100138759
弁理士 大房 直樹
(74)代理人 100091063
弁理士 田中 英夫
(74)代理人 110001243
特許業務法人 谷・阿部特許事務所
(72)発明者 ハオ ツァン
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 インターナショナル パテンツ内
(72)発明者 サミュエル ジェイ. ニーリー
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 インターナショナル パテンツ内
(72)発明者 トレバー フリーマン
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 インターナショナル パテンツ内

審査官 青木 重徳

(56)参考文献 米国特許出願公開第２００３／０２３３５７７（ＵＳ，Ａ１）
特開２００３－１７９５９２（ＪＰ，Ａ）
国際公開第２００５／０３１５８６（WO，Ａ１）
P. Hoffman, “SMTP Service Extension for Secure SMTP over Transport Layer Security”, Network Working Group Request for Comments: 3207, [online], ２００２年 2月, Obsoletes: 2487, [retrieved on 2012-06-04]. Retrieved from the Internet, ＵＲＬ, <http://www.ietf.org/rfc/rfc3207.txt>
Will Price, Michael Elkins, “Extensions to TLS for OpenPGP keys”, TLS Working Group INTERNET-DRAFT, [online], ２００２年 2月１８日, <draft-ietf-tls-openpgp-02.txt>, [retrieved on 2012-06-04]. Retrieved from the Internet, ＵＲＬ, <http://www7b.biglobe.ne.jp/~k-west/SSLandTLS/draft-ietf-tls-openpgp-02.txt>
A. Medvinsky, M. Hur, “Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)”, Network Working Group Request for Comments: 2712, [online], １９９９年１０月, Category: Standards Track, [retrieved on 2012-06-05]. Retrieved from the Internet, ＵＲＬ, <http://www.ietf.org/rfc/rfc2712.txt>
“SMTP および Exchange Server 2003 について”, [online], ２００５年 5月 4日, [retrieved on 2012-06-04]. Retrieved from the Internet, ＵＲＬ, <http://technet.microsoft.com/ja-jp/library/aa996068%28v=exchg.65%29.aspx>
小林信博, 中川路哲男, “認証・認可情報流通基盤について”, 情報処理学会研究報告, 日本, 社団法人情報処理学会, ２００３年 5月１６日, Ｖｏｌ．２００３，Ｎｏ．４５，ｐ．２９－

３４
Paul Robichaux, “Windows Server：システム管理者の視点　ExchangeでSSL証明書が使いやすくなってきた”, ＩＴ　ｐｒｏ, ［オンライン］, ２００６年１０月２３日, ［平成２４年　５月１０日検索］, インターネット, ＵＲＬ, <http://itpro.nikkeibp.co.jp/article/COLUMN/20061020/251415/>
N. Zhang, Q. Shi, M. Merabti, “An efficient protocol for anonymous and fair document exchange”, COMPUTER NETWORKS, ２００３年　1月１５日, Volume 41, Issue 1, p.19-28
Ibrahim Hajjeh, Ahmed Serhrouchni, Frederique Tastet, “ISAKMP Handshake for SSL/TLS”, IEEE Global Telecommunications Conference 2003 (GLOBECOM 2003), [online], ２００３年１２月, Volume 3, p.1481-1485, [retrieved on 2012-05-10]. Retrieved from the Internet, ＵＲＬ, <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01258484>
Joseph Hui, “TLS Pathsec Protocol”, TLS Working Group INTERNET-DRAFT, [online], ２００１年１２月, <draft-ietf-tls-pathsec-00.txt>, [retrieved on 2012-05-11]. Retrieved from the Internet, ＵＲＬ, <http://www7b.biglobe.ne.jp/~k-west/SSLandTLS/draft-ietf-tls-pathsec-00.txt>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　１２／２２
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ　Ｘｐｌｏｒｅ