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

特許第5186648号
(P5186648)

(45)発行日　平成25年4月17日(2013.4.17)　(24)登録日　平成25年2月1日(2013.2.1)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675B
G09C 1/00 (2006.01)　　G09C 1/00 640E
　　H04L 9/00 675Z

請求項の数 28　(全 18 頁)

(21)出願番号　特願2009-530328 (P2009-530328)
(86)(22)出願日　平成19年2月5日 (2007.2.5)
(65)公表番号　特表2010-505334 (P2010-505334A)
(43)公表日　平成22年2月18日 (2010.2.18)
(86)国際出願番号　PCT/US2007/003219
(87)国際公開番号　WO2008/039227
(87)国際公開日　平成20年4月3日 (2008.4.3)
審査請求日　平成22年2月4日 (2010.2.4)
(31)優先権主張番号　60/827,118
(32)優先日　平成18年9月27日 (2006.9.27)
(33)優先権主張国　米国 (US)

(73)特許権者　510252586
セキュアオース　コーポレイション
ＳＥＣＵＲＥＡＵＴＨ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　９２６１８　カリフォルニア州　アーバイン　リサーチ　ドライブ　８９６５
(74)代理人　100068755
弁理士　恩田　博宣
(74)代理人　100105957
弁理士　恩田　誠
(74)代理人　100142907
弁理士　本田　淳

最終頁に続く

(54)【発明の名称】安全なオンライン取引を容易にするシステム及び方法

(57)【特許請求の範囲】
【請求項１】
クライアント及びサーバを相互に認証する方法であって、
前記サーバから前記クライアントへトークンを送信すること、
前記サーバと前記クライアントとの間に、安全なデータ転送リンクを確立することであって、前記安全なデータ転送リンクの確立中にサーバ証明書が前記クライアントへ送信される、安全なデータ転送リンクを確立すること、
フル要求ユニフォーム・リソース・ロケータ（ＵＲＬ）識別子、クライアント証明書、前記サーバ証明書、前記トークン、およびクライアント秘密鍵に対応する認証識別子を含む応答パケットを前記サーバへ送信することであって、前記クライアント秘密鍵が、前記クライアント証明書と関連付けられている、応答パケットを前記サーバへ送信すること、
前記応答パケットを検証すること
を備える方法。
【請求項２】
前記認証識別子は、前記応答パケットの暗号学的ハッシュであり、前記認証識別子が、前記クライアント秘密鍵で署名される、請求項１に記載の方法。
【請求項３】
前記応答パケットを検証することは、前記サーバに関連するＵＲＬに対して、前記応答パケット内のフル要求ＵＲＬ識別子を検証することをさらに含む、請求項１に記載の方法。

【請求項４】
前記応答パケットを検証することは、前記サーバ上に格納された前記トークンに対して、前記応答パケット内の前記トークンを検証することをさらに含み、前記応答パケット内の前記トークン及び前記サーバ上に格納された前記トークンは、固有コードを含む、請求項１に記載の方法。
【請求項５】
前記応答パケットを検証することは、前記応答パケット内の前記サーバ証明書の第２のコピーに対して、前記サーバ内に格納された前記サーバ証明書の第１のコピーを検証することをさらに含む、請求項２に記載の方法。
【請求項６】
前記応答パケットを検証することは、前記応答パケット上のクライアント署名に対して、前記クライアント証明書を検証することをさらに含み、前記クライアント署名は、前記クライアント秘密鍵に関連する、請求項１に記載の方法。
【請求項７】
前記クライアント証明書は、有効期限が切れていない、請求項６に記載の方法。
【請求項８】
前記クライアント証明書は、前記サーバに関連する組織に対して発行されている、請求項６に記載の方法。
【請求項９】
前記クライアント証明書は、認可された認証局に関連する証明書サーバから発行され、
前記クライアントは、前記サーバに関連する組織に接続されている、
請求項１に記載の方法。
【請求項１０】
前記方法は、前記クライアント証明書を発行する前に、チャレンジ応答シーケンスで前記クライアントを検証することをさらに含む、請求項８に記載の方法。
【請求項１１】
前記チャレンジ応答シーケンスに対する応答は、ユーザに関連する所定の電話装置へ送信される、請求項１０に記載の方法。
【請求項１２】
前記チャレンジ応答シーケンスに対する応答は、ユーザに関連する所定の電子メールアドレスへ送信される、請求項１０に記載の方法。
【請求項１３】
サーバに対してクライアントを認証する方法であって、
前記サーバからトークンを受信すること、
前記サーバと前記クライアントとの間に安全なデータ転送リンクを確立することであって、前記安全なデータ転送リンクの確立中に、サーバ証明書が前記サーバから受信される、安全なデータ転送リンクを確立すること、
フル要求ＵＲＬ識別子、クライアント証明書、前記サーバ証明書、前記トークン、およびクライアント秘密鍵に対応する認証識別子を含む応答パケットを前記サーバへ送信することであって、前記クライアント秘密鍵が前記クライアント証明書に関連する、応答パケットを前記サーバへ送信すること、
を備える方法。
【請求項１４】
前記認証識別子は、前記応答パケットの暗号学的ハッシュであり、前記認証識別子が、前記クライアント秘密鍵で署名される、請求項１３に記載の方法。
【請求項１５】
前記クライアント証明書は、認可された認証局に関連する証明書サーバから発行され、
前記クライアントは、前記サーバに関連する組織に接続されている、
請求項１３に記載の方法。
【請求項１６】

前記方法は、前記クライアント証明書を発行する前に、チャレンジ応答シーケンスで前記クライアントを検証することをさらに含む、請求項１３に記載の方法。
【請求項１７】
前記チャレンジ応答シーケンスは、ユーザに関連する所定の電話装置へ送信される、請求項１６に記載の方法。
【請求項１８】
前記チャレンジ応答シーケンスに対する応答は、ユーザに関連する所定の電子メールアドレスへ送信される、請求項１６に記載の方法。
【請求項１９】
クライアントに対してサーバを認証する方法であって、
前記サーバから前記クライアントへトークンを送信すること、
前記サーバと前記クライアントとの間に安全なデータ転送リンクを確立することであって、前記安全なデータ転送リンクの確立中に、サーバ証明書が前記クライアントへ送信される、安全なデータ転送リンクを確立すること、
フル要求ＵＲＬ識別子、クライアント証明書、前記サーバ証明書、前記トークン、およびクライアント秘密鍵に対応する認証識別子を含む応答パケットを前記サーバへ送信することであって、前記クライアント秘密鍵が前記クライアント証明書に関連する、応答パケットを前記サーバへ送信すること
を備える方法。
【請求項２０】
前記認証識別子は、前記応答パケットの暗号学的ハッシュであり、前記認証識別子は、前記クライアント秘密鍵で署名される、請求項１９に記載の方法。
【請求項２１】
前記応答パケットを検証することは、前記サーバに関連するＵＲＬに対して、前記応答パケット内のフル要求ＵＲＬ識別子を検証することをさらに含む、請求項１９に記載の方法。
【請求項２２】
前記応答パケットを検証することは、前記サーバ上に格納されたトークンに対して、前記応答パケット内のトークンを検証することをさらに含み、前記応答パケット内の前記トークン及び前記サーバ上に格納された前記トークンが固有コードを含む、請求項１９に記載の方法。
【請求項２３】
前記応答パケットを検証することは、前記応答パケット内に格納されたサーバ証明書の第２のコピーに対して、前記サーバ内上に格納された前記サーバ証明書の第１のコピーを検証することをさらに含む、請求項１９に記載の方法。
【請求項２４】
前記応答パケットを検証することは、前記応答パケット上のクライアント署名に対して、前記クライアント証明書を検証することをさらに含み、前記クライアント署名は、前記クライアント秘密鍵に関連する、請求項１９に記載の方法。
【請求項２５】
前記クライアント証明書は、有効期限が切れていない、請求項２４に記載の方法。
【請求項２６】
前記クライアント証明書は、前記サーバに関連する組織に対して発行される、請求項２４に記載の方法。
【請求項２７】
前記クライアント証明書は、認可された認証局に関連する証明書サーバから発行される、請求項１９に記載の方法。
【請求項２８】
コンピュータによって読取り可能なプログラム記憶媒体であって、クライアント及びサーバを相互に認証する方法を実行するための前記コンピュータによって実行可能な命令か

らなる１つ以上のプログラムを備える前記プログラム記憶媒体であって、
前記方法が、
前記サーバから前記クライアントへトークンを送信すること、
前記サーバと前記クライアントとの間に、安全なデータ転送リンクを確立することであって、前記安全なデータ転送リンクの確立中にサーバ証明書が前記クライアントへ送信される、安全なデータ転送リンクを確立すること、
フル要求ＵＲＬ識別子、クライアント証明書、前記サーバ証明書、前記トークン、およびクライアント秘密鍵に対応する認証識別子を含む応答パケットを前記サーバへ送信することであって、前記クライアント秘密鍵が、前記クライアント証明書と関連付けられている、応答パケットを前記サーバへ送信すること、
前記応答パケットを検証することを備える、プログラム記憶媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般に、安全なデータ通信における認証のための方法及びシステムに関する。より具体的には、本発明は、公開鍵基盤（ＰＫＩ）の証明書を含む複数の要因を用いて、クライアント及びサーバを双方向で認証する方法及びシステムに関する。

【０００２】

本出願は、２００６年９月２７日に出願された、「ＭＵＬＴＩ－ＦＡＣＴＯＲ ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ ＩＮＣＳ ＰＲＯＤＵＣＴ ＳＥＣＵＲＥＡＵＴＨ ＩＳＡ ＵＮＩＱＵＥ ＴＥＣＨＮＯＬＯＧＹ ＴＯ ＡＵＴＨＥＮＴＩＣＡＴＥ ＵＳＥＲＳ ＴＯ ＯＮＬＩＮＥ ＩＴ ＲＥＳＯＵＲＣＥＳ．ＳＥＣＵＲＥＡＵＴＨ ＩＳ ＵＮＩＱＵＥ ＩＮ ＩＴＳ ＡＢＩＬＩＴＹ ＴＯ ＵＴＩＬＩＺＥ Ｘ５０９ ＣＥＲＴＩＦＩＣＡＴＥＳ，ＩＮ Ａ ＮＯＮ－ＰＨＩＳＨＡＢＬＥ ＭＡＮＮＥＲ，ＴＯ ＡＵＴＨＥＮＴＩＣＡＴＥ ＡＮＤ ＩＤＥＮＴＩＦＹ ＵＳＥＲＳ ＷＩＴＨＯＵＴ ＦＯＲＣＩＮＧ ＡＮ ＥＮＴＥＲＰＲＩＳＥ ＴＯ ＨＯＳＴ Ａ ＰＫＩ ＩＮＦＲＡＳＴＲＵＣＴＵＲＥ．ＳＰＥＣＩＦＩＣＡＬＬＹ ＭＦＡＳ ＵＮＩＱＵＥ ＩＮＴＥＬＬＥＣＴＵＡＬ ＰＲＯＰＥＲＴＹ ＰＲＯＶＩＤＥＳ Ｘ５０９ ＳＥＣＵＲＥ ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ ＷＩＴＨＯＵＴ ＲＥＱＵＩＲＩＮＧ ＴＨＥ ＥＮＴＥＲＰＲＩＳＥ ＴＯ ＤＥＰＬＯＹ ＣＬＩＥＮＴ－ＳＩＤＥ ＳＳＬ」という名称の米国特許仮出願第６０／８２７，１１８号に関し、出願の利益を主張し、出願明細書の全体を本願明細書に組み込む。

【背景技術】

【０００３】

銀行取引、金融サービス、行政、教育及び様々な会社は全て、高度なコンピュータシステムやインターネット等のデータ通信ネットワークに依存している。そのような高度性は、ビジネスが行われる際の速度や利便性を大幅に向上させているが、多くの脆弱性が、やりとりされる極秘及び機密のデータの安全性を危険にさらしている。基本的に、電子商取引は、典型的には、ネットワークを介して通信するサーバコンピュータシステム及びクライアントコンピュータシステムを含む。多数のクライアントが所定のサーバにアクセスできるように、または、所定のサーバが多数のサーバにアクセスできるように、追加的なクライアントコンピュータシステムまたはサーバコンピュータシステムをネットワークに接続してもよい。このオープンネットワーク環境において、データセキュリティに関する主要な関心事は、３つある。第１に、クライアントが自身により主張されるクライアントであることを、サーバは保証されなければならない。第２に、サーバが自身により主張されるサーバであることを、クライアントは保証されなければならない。第３に、正当なサーバと正当なクライアントとの間でやりとりされるいかなる情報も、ネットワーク上の他のどのコンピュータによっても傍受されたり、または変えられたりしてはならない。

【０００４】

電子バンキング構成において、例えば、銀行は、バンキングサーバにアクセスするユー

ザＩＤを認証しなければならず、その結果、特定の顧客のみに関連する取引が許可され、且つバンキングサーバにアクセスしているユーザが、顧客として、または、顧客のみによって権限が与えられた者として確認される。クライアントは、バンキングサーバが、本当に、銀行によって運用されているサーバであること、およびバンキングサーバが、悪意のある団体によって運用されている、類似したサーバでないことを確認しなければならない。これは、フィッシング攻撃として知られており、この場合、偽装サーバは、正当なサーバと似ており、ユーザをだまして、銀行口座番号、社会保障番号、パスワード等の機密情報を提供させる。誤った債務情報、逮捕歴、刑事上の有罪判決、信用力の喪失、名誉毀損等を含む情報を有する犯罪者によって、多くの害悪が顧客に与えられる可能性がある。これらのことは、個人情報窃盗犯罪として知られている。機密情報が、オープンネットワークを通じて伝送される場合、このような情報は、暗号化されなければならず、あるいは、別の方法で、クライアント及びサーバの以外の他の何らかのシステムに対して理解不能になるようにしなければならない。ネットワークのオープン性は、コンピュータシステムを、繰り返し攻撃しやすくし、この場合、有効データの伝送は傍受され、後で不正目的または悪意の目的のために繰り返される。例えば、パスワードまたは他の認証情報は、傍受されて、後に、機密情報にアクセスするのに用いられる可能性がある。さらに、ネットワーク上で伝達される情報は、介入者攻撃の場合のように、修正可能であってはならない。このことは、アタッカーリーディング、信用できなくなったリンクの認識を伴わない、正当なクライアントとサーバとの間でのデータの挿入及び修正を含む。

【０００５】

様々な方法が、クライアントＩＤを認証または確認するのに用いられる。認証は、ユーザが知っている何か、ユーザが持っている何か、およびユーザが誰かを含む１つ以上のファクターを利用することができる。ほとんどの場合、追加コスト、および追加的な認証ファクターに関する複雑性のために、単一のファクターのみが用いられる。このようなシングルファクター認証システムにおいて、最も一般的なことは、アクセスを制限するためのパスワードまたは個人識別番号（ＰＩＮ）の使用である。別の実例は、対応するＰＩＮを伴うＡＴＭカードである。サーバは、ユーザ名及び対応するパスワード／ＰＩＮのリストを保持し、入力されたユーザ名とパスワード／ＰＩＮの組合せがリストとの比較の後に正しいと判断された場合、システムへのアクセスが許可される。パスワード及びＰＩＮの秘密性は、少なくとも理論的には、無許可のユーザがコンピュータシステムにアクセスすることを防ぐ。この技術は、許可されたユーザが、しばしば、誤ってまたは無意識に、パスワードまたはＰＩＮを無許可のユーザに明かしてしまうため、効果がない。さらに、文字、数字及び符号の組合せのあらゆる入力を伴う総当り法ならびに辞書ベースの方法は、このような認証システムの有効性を危うくする可能性がある。パスワードは暗記しなければならないため、ユーザは、しばしば覚えるのが簡単な言葉を選んでしまい、辞書的な攻撃によって打ち破られやすくなる。一方、パスワードに複雑性が要求されればされるほど、パスワードは、コンピュータ周辺にある、正当なユーザ及び悪意のあるユーザの両方にとってアクセスし易いものに書かれるであろう。米国連邦金融機関検査協議会（ＦＦＩＥＣ）が強く主張しているように、シングルファクター認証は、特に、金融または銀行取引関連のオンラインサービスにおいて、実質的な弱点である。

【０００６】

パスワードに加えて、ユーザが有する何かを含む追加的なファクターを利用することができる。これは、外部周辺ポートを介してクライアントコンピュータに接続されている簡単な装置、ならびに上記したようなユーザ名やパスワードと共に入力される固有コードまたはワンタイムパスワード（ＯＴＰ）を生成する高機能トークンを含む。現在利用可能なトークンベースの認証システムは、時間同期されたＯＴＰを利用するＲＳＡ　ＳｅｃｕｒｅＩＤ、および数学アルゴリズムベースのＯＴＰを利用するベリサインユニファイドオーセンティケーションを含む。安全性は大幅に向上するが、トークン装置は、ライセンスが高価であり、維持するのにコストがかかり、ユーザにとって持ち運びが厄介である。何かの小さなデバイスと同様に、トークンは、無くしやすいものである。無くした場合、取換

えには、何日かまたは何週間かかかり、追加的なコスト及び生産性の損失が生じる。

【０００７】

第３の認証ファクターは、指紋、網膜や顔のパターン、声の特徴及び筆跡パターン等の人に固有の生体属性を利用する。しかし、生体認証は、指紋及び網膜スキャナ、マイクロフォン等を含むこのようなデータを取得するための専用のハードウェアの配置を要する。さらに、取得したデータを、登録データとも呼ばれる既存のユーザデータと比較するために、専用のデータベース及びソフトウェアが必要である。従って、このような配置のコストは非常に高く、たいてい大きな組織に限られる。加えて、生体測定の読取りは、１つの取得と次の取得の間で一貫性がない可能性があり、それにより、検出漏れが生じる。アプリケーション及びデータへのアクセスを安全にするために、ポータブルコンピュータにおける指紋識別が普及してきているが、登録データベースを維持する必要性から、他のコンピュータシステムを用いて認証するこのようなデバイスの使用は一般的ではない。

【０００８】

サーバコンピュータシステムを認証するために、およびデータ伝送が傍受されないことを確実にするために、トランスポートレイヤセキュリティ（ＴＬＳ）プロトコルが多く利用される。ＴＬＳは、盗聴、改ざん及び偽造から守る、安全なデータ交換の安全性を実現できる暗号プロトコルであり、ウェブ閲覧、電子メール、ファイル転送及び他の電子取引を保証するのに用いられている。より具体的には、ＴＬＳは、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、ファイル転送プロトコル（ＦＴＰ）、シンプルメール転送プロトコル（ＳＭＰＴ）等のアプリケーション層プロトコルの下であり、かつ転送制御プロトコル（ＴＣＰ）またはユーザデータグラムプロトコル（ＵＤＰ）等のトランスポートレベルプロトコルの上のプロトコル層で機能する。ＴＬＳプロトコルにおいては、国際電気通信連合の電気通信標準化部門（ＩＴＵ－Ｔ）のＰＫＩ標準Ｘ．５０９に準拠する公開鍵基盤（ＰＫＩ）の様々なコンポーネントが用いられる。

【０００９】

一般的に、公開鍵暗号は、受信者及び送信者の双方によって保持される公開鍵と秘密鍵の固有のペアを必要とする。送信者の秘密鍵は、送信者によってのみ保持され、受信者の秘密鍵は、受信者によってのみ保持される。送信者の公開鍵は、分配されて受信者によって保持され、受信者の公開鍵も分配されて送信者によって保持される。メッセージを送信する際、送信者の秘密鍵及び受信者の公開鍵が、メッセージを暗号化するために用いられる。メッセージは、受信者により、受信者の秘密鍵及び送信者の公開鍵を用いて解読される。受信者は、公開鍵と秘密鍵の固有のペアを有する必要はないが、その代わりに、ワンタイム暗号を利用する。

【００１０】

しかし、ＴＬＳは、通常、サーバ側ベースでのみ実施され、サーバのみが認証される。例えば、クライアントのブラウザからウェブサーバへ安全なＨＴＴＰ接続を確立すると、クライアントブラウザは、ウェブサーバに関連するデジタル証明書を検索する。公開鍵を含む証明書は、ブラウザにより、ウェブサーバのＩＤを認証し、後続のデータを暗号化する際に用いるために、ウェブサーバに返信されるセッション鍵を暗号化するのに用いられる。サーバ証明書の正当性を保証するために、証明書は、認証局（ＣＡ）によって署名される。

【００１１】

クライアント側ＴＬＳの実施は、サーバとクライアントの間の二者間の信頼を確立し個人情報犯罪及びフィッシング攻撃を防ぐが、多くの著しい欠陥がある。より具体的には、クライアントは、ＣＡによって正当に署名された証明書を取得または購入する必要がある。従って、証明書の所有に関連する複雑さがユーザの負担になる。加えて、サーバ上のクライアント証明を実施することは、追加的なサーバ及びメンテナンスが必要であるという点において厄介なプロセスである。サーバによって実行できる他の中心的な機能性に加えて、ユーザ証明書を発行するように構成してもよい。

【発明の概要】

【発明が解決しようとする課題】
【００１２】
従って、当該技術においては、トークン、またはクライアント側ＴＬＳの配置等のハードウェア装置を要することなく、クライアント及びサーバを認証する方法及びシステムに対する需要がある。また、このような認証が、優れたマルチファクターである必要性がある。さらに、認証信任状を用いて、暗号化されたデータ通信セッションを開始する改良された方法及びシステムに対する需要がある。また、当該技術においては、既存のサーバ及びクライアントを用いて構成する、および統合するのが容易な認証システムに対する需要がある。
【課題を解決するための手段】
【００１３】
本発明の一態様によれば、クライアント及びサーバを互いに認証する方法が提供される。方法は、サーバからクライアントへトークンを送信することで始めることができる。また、方法は、サーバとクライアントとの間に安全なデータ転送リンクを確立することを含む。サーバ証明書は、安全なデータ転送リンクの確立中に、クライアントへ送信することができる。方法は、応答パケットのサーバへの送信を続けることができ、パケットは、フル要求ユニフォーム・リソース・ロケータ（ＵＲＬ）識別子、クライアント証明書、サーバ証明書及びトークンを含んでもよい。また、応答パケットは、秘密鍵で署名された認証識別子を含んでもよい。また、方法は、応答パケットの内容を検証することも含んでもよい。
【００１４】
認証は、安全なデータ転送リンクとは別に行われるため、クライアント側認証のためにウェブサイトを変換する必要はない。また、クライアント証明書を記憶または検索するためのユーザ動作は必要なく、クライアント上での証明書管理は、安全性を危うくすることなく、大幅に簡素化される。
【００１５】
本発明の別の態様によれば、方法は、応答パケットの検証を続けることができ、サーバに関連するＵＲＬに対する応答パケット内のフル要求ＵＲＬ識別子を検証することを含んでもよい。さらに、応答パケットを検証することは、サーバ上に記憶されているトークンに対して、応答パケット内のトークンを検証することを含んでもよい。応答パケット内のトークン及びサーバ上に記憶されているトークンは、固有コードを含んでもよい。応答パケットを検証する方法は、応答パケット内のサーバ証明書の第２のコピーに対して、サーバ上に記憶されているサーバ証明書の第１のコピーを検証することも含んでもよい。追加的な検証は、応答パケット上のクライアント署名に対して、クライアント証明書を検証することを含んでもよい。クライアント署名は、クライアント秘密鍵と関連付けることができる。これらの検証は、クライアントとサーバとの間の通信が安全であり、介入者攻撃および／またはリプレー攻撃を受け易くなくないことを保証し、この場合、応答パケットの内容の改ざんが行われる可能性がある。上記の検証のいずれかに失敗した場合、接続は、危険にさらされていると見なされ、それ以上の送信は行われないことになる。
【００１６】
クライアント証明書は、公認された認証局に関連する認証サーバから発行することができ、またクライアントは、サーバに関連する組織に接続することができる。クライアント証明書を発行する前に、クライアントとサーバを互いに認証する方法は、チャレンジ応答シーケンスを用いてクライアントを検証することを含んでもよい。チャレンジ応答シーケンスに対する応答は、ユーザに関連する所定の電話装置へ送信することができ、または、ユーザに関連する電子メールアドレスへ送信してもよい。従って、組織が、証明書の取消しを発行し、管理し、および追跡する必要はない。従って、組織が、クライアント側認証のためのサーバを設置して構成する必要はない。
【００１７】
本発明の別の態様によれば、クライアント及びサーバを双方向で認証するシステムが提

供される。システムは、サーバに関連するサーバ認証モジュールを含んでもよい。サーバ認証モジュールは、サーバ証明書及びトークンを格納するメモリを含んでもよい。さらに、サーバ認証モジュールは、トークン及びサーバ証明書をクライアントへ送信するように機能することができる。本発明のさらに別の態様によれば、クライアントに関連するクライアント認証モジュールが提供される。クライアント認証モジュールは、クライアント証明書、トークン、フル要求ＵＲＬ識別子及びサーバ証明書を格納するメモリを含むことができ、また、サーバ証明書、トークン及びフル要求ＵＲＬ識別子を含む認証パケットを送信するように機能することができる。認証パケットは、クライアント証明書で署名することができる。

【００１８】

本発明は、添付図面と共に読めば、以下の詳細な説明を参照することにより、理解されるであろう。

【図面の簡単な説明】

【００１９】

【図１】様々な相互接続されたサーバ及びクライアントを含む、本発明の一態様を実施することのできる環境を示すブロック図である。

【図２】本発明の一態様によるクライアントとサーバを双方向で認証する方法を示すフローチャートである。

【図３】クライアント及びサーバを認証するためのデータ交換を示すシーケンス図である。

【図４】クライアントとサーバとの間のＴＬＳ接続の確立を示すシーケンス図である。

【図５】様々なサブパーツを含む、本発明の態様によるデジタル証明書の一実施形態である。

【図６】ユーザ証明書、フル要求ＵＲＬ、トークン及びサーバ証明書を含む応答パケットの一実施形態である。

【図７ａ】応答パケットの検証を説明するフローチャートである。

【図７ｂ】応答パケットの検証を説明するフローチャートである。

【図７ｃ】応答パケットの検証を説明するフローチャートである。

【図８】証明書及び電話サーバが、サードパーティプロバイダによって制御される、クライアント及びサーバを相互に認証する第１の例示的な構成である。

【図９】証明書及び電話サーバが、サーバを制御する組織によって制御される、クライアント及びサーバを相互に認証する第２の例示的な構成である。

【図１０】ウェブサービスへの安全なアクセスが提供される、クライアント及びサーバを相互に認証する第３の構成である。

【００２０】

同じ構成要素を表すために、図面及び詳細な説明の全体を通して、共通の参照符号が用いられている。

【発明を実施するための形態】

【００２１】

本願明細書に開示されている様々な実施形態のこれら及び他の特徴及び利点は、以下の説明及び図面に関して理解されるであろうし、同じ符号は、全体を通して同じ部材を指す。

【００２２】

添付図面に関連して以下に記載されている詳細な説明は、本発明の現時点で好適な実施形態の説明として意図されており、また、本発明を構成または利用することのできる唯一の形態を表すことを意図していない。説明は、図示されている実施形態と関連して本発明を展開し、および機能させるためのステップの機能及びシーケンスについて記載している。しかし、同じであるまたは同等の機能及びシーケンスを、本発明の精神及び範囲に包含されることも意図されている異なる実施形態によって実現することができることを理解すべきである。

【００２３】
さらに、第１の及び第２の等の関係を示す用語は、単に、構成要素間の実際の関係や順序を要することなく、または示唆することなく、一方の構成要素と他方の構成要素を区別するために用いられている。
【００２４】
図１を参照すると、例示的なコンピュータネットワーク１０は、種々のデータ処理装置またはコンピュータ１２、１４を含んでいる。より具体的には、コンピュータ１２は、クライアントとして機能するパーソナルコンピュータまたはワークステーションとすることができ、また、中央演算処理装置、記憶装置等を収容するシステムユニット１６を含んでもよい。また、コンピュータ１２は、表示装置１８と、キーボード２０ａ及びマウス２０ｂ等の入力装置２０とを含むこともできる。システムユニット１６は、中央演算処理装置によって実行される、予めプログラムされている命令の制御及びフローを変更する様々な入力を入力装置２０から受取る、かつこのような実行の結果が表示装置１８に示されることは理解されよう。コンピュータ１４は、データまたはサービスをクライアントコンピュータ１２へ提供するサーバとすることができる。この点に関して、「クライアント」という用語は、データまたはサービスの要求者としてのコンピュータ１２の役割を指すこと、また、「サーバ」という用語は、このようなデータまたはサービスを提供するサーバ１４の役割を指すことは理解されよう。また、コンピュータ１２が、１つのトランザクションでデータまたはサービスを要求することができ、かつ１つのトランザクションでデータまたはサービスを提供することができ、従ってその役割をクライアントからサーバへ、あるいはその逆に変更することができる。
【００２５】
コンピュータ１２、１４は、ネットワーク接続２４を介して、インターネット２２等の広域ネットワークに接続されている。クライアントコンピュータ１２からの要求及びサーバコンピュータ１４からの要求データは、ネットワーク接続２４を介して配信される。本発明の実施形態によれば、サーバコンピュータ１４はウェブサーバであり、クライアントコンピュータ１２は、サーバコンピュータ１４によって提供されるドキュメントを表示装置１８上に視覚的に描画するＭｉｃｒｏｓｏｆｔ　Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ等のウェブ閲覧アプリケーションを含む。図１に示すネットワークトポロジーは、単に例証として示されており、限定的ではなく、また、他のどのような種類のローカルエリアネットワークまたは広域ネットワークも、本発明の範囲から逸脱することなく、容易に置き換えることができることは、正しく理解されるであろう。周知のデータ伝送プロトコルを、ネットワーク接続２４及びインターネット２２に利用することができることは、理解されよう。
【００２６】
さらに別の実施例として、第１のサーバコンピュータ１４ａは、口座情報及び資金振替機能を実行できる電子バンキング用ウェブサーバとすることができる。追加的なユーザも意図されており、この場合、第１のサーバコンピュータ１４ａは、メールサーバ、オンラインショッピングサイトまたはＭｉｃｒｏｓｏｆｔ　ＮＥＴアプリケーションのホストとなる。第１のクライアントコンピュータ１２ａ上のユーザは、第１のサーバコンピュータ１４ａにログオンして、ウェブブラウザを用いて、勘定残高を検索し、資金を別の口座へ振り替える。この例示的文脈において、情報セキュリティに関する考慮すべき事柄の一つは、第１のクライアントコンピュータ１２ａ上のユーザが誰であるかを確証することを含む。例えば、第２のクライアントコンピュータ１２ｂ上の悪意のあるユーザは、第１のクライアントコンピュータ１２ａ上のユーザの全ての信任状を有していて、かかるアクセスが不正であることを認識することなく、第１のサーバコンピュータ１４ａにログオンする可能性がある。別の考慮すべき事柄は、第１のサーバコンピュータ１４ａが、第１のクライアントコンピュータ１２ａ上のユーザが顧客である銀行の制御下にあることを確証することである。第２のサーバコンピュータ１４ｂは、フィッシングを試みて、第１のサーバコンピュータ１４ａになりすまし、第１のクライアントコンピュータ１２ａが、第２のサ

ーバコンピュータ１４ｂへ誤って誘導される可能性がある。加えて、第１のクライアントコンピュータ１２ａと第１のサーバコンピュータ１４ａの間の全ての正当なデータ転送は、第３のクライアントコンピュータ１２ｃ、第２のクライアントコンピュータ１２ｂ及び第２のサーバコンピュータ１４ｂを含む他のコンピュータのいずれかによって傍受されるべきではない。

【００２７】

本発明の一態様は、クライアントコンピュータ１２及びサーバコンピュータ１４を互いに認証する方法に関する。図２のフローチャート及びさらに図３のシーケンス図を参照すると、方法は、安全ではないデータリンク２７を通じて、クライアントコンピュータ１２からサーバコンピュータ１４へトークン２６を送信するステップ２００で始まる。しかし、トークン２６の送信前に、サーバコンピュータ１４との安全ではない接続２７を開始するクライアントコンピュータ１２の追加的なステップがあってもよい。例えば、ユーザは、サーバコンピュータ１４のネットワークアドレスを、クライアントコンピュータ１２上のブラウザアプリケーションに入力することができ、この時点で、サーバコンピュータ１４上のファイルまたはページに対する要求がなされる。トークン２６は、証明書要求識別子とも呼ばれており、特定の要求を識別する任意の値を含む。以下においてさらに詳細に説明するように、トークン２６は、証明書要求識別子によって参照されるトランザクションのみが、有効であると確実に見なされるように、サーバコンピュータ１４上に保持される。この任意の値がリプレー攻撃を防ぐことは理解されよう。本発明の一実施形態によれば、トークン２６は、証明書検索スクリプト２８を伴い、スクリプトは、ブラウザに、クライアントコンピュータ１２を認証するプロセスを始めるように指示する。

【００２８】

その後、ステップ２１０に従って、安全なデータ転送リンク３０は、フル要求ＵＲＬ３２を用いて、クライアントコンピュータ１２によって開始される。好適な実施形態によれば、安全なデータ転送リンク３０は、対称ＴＬＳリンクである。図４のシーケンス図を詳細に参照すると、クライアントコンピュータ１２は、同期またはＳＹＮパケット３４を送信することにより、サーバコンピュータ１４への接続を開始する。その後、サーバコンピュータ１４は、同期及び肯定応答、またはＳＹＮ＋ＡＣＫパケット３６をクライアントコンピュータ１２へ送信する。クライアントコンピュータ１２は、受信時に、肯定応答またはＡＣＫパケット３８をサーバコンピュータ１４へ返送する。当然、この送信は、ＴＣＰ、ＴＬＳプロトコルの下のプロトコル層に関連する。

【００２９】

クライアントコンピュータ１２とサーバコンピュータ１４の間のＴＣＰ接続を確立するとき、ＣＬＩＥＮＴ＿ＨＥＬＬＯコマンド４０が、クライアントコンピュータ１２からサーバコンピュータ１４へ送られる。このパケットは、クライアントコンピュータ１２によってサポートされているＴＬＳの最新バージョン、クライアントコンピュータ１２によってサポートされている暗号及びデータ圧縮方法、セッション識別子及び任意のデータを含む。ＣＬＩＥＮＴ＿ＨＥＬＬＯコマンドを受信すると、サーバコンピュータ１４は、ＳＥＲＶＥＲ＿ＨＥＬＬＯコマンド４２を送信する。ＳＥＲＶＥＲ＿ＨＥＬＬＯコマンド４２は、ＴＬＳのバージョン、暗号、および選択されているデータ圧縮方法を含む。加えて、これまで設定されていたセッション識別子ならびに追加的な任意のデータも含まれている。その後、サーバコンピュータ１４は、サーバ証明書４６を含むＣＥＲＴＩＦＩＣＡＴＥコマンド４４と、サーバコンピュータ１４が、当ハンドシェイキング段階を完了したことを示すＳＥＲＶＥＲ＿ＤＯＮＥコマンド４８とを送信する。

【００３０】

サーバ証明書４６は、Ｘ．５０９の規格に準拠していると理解される。より具体的には、図５を参照して、サーバ証明書４６に格納されているデータは、バージョン番号５１と、シリアルナンバー５２と、発行者識別子５４と、有効性識別子５５と、公開鍵アルゴリズム識別子５７ａ及びサブジェクト公開鍵５７ｂを含むサブジェクト公開鍵情報５７と、証明書署名５９とを含む。バージョン番号５１は、特定の証明書のために用いられるＸ．

５０９規格のバージョンを識別し、シリアルナンバー５２は、特定のＣＡによって割当てられた固有番号である。発行者識別子５４は、証明書を発行したＣＡの名称を含み、有効性識別子５５は、開始から終了までの有効期限を含む。サブジェクト識別子５６は、証明書が発行される対象の人、グループまたは組織の名前を含む。サブジェクト公開鍵アルゴリズム識別子５７ａは、サブジェクト公開鍵５７ｂを生成するのに用いられるアルゴリズムを示し、サブジェクト公開鍵５７ｂは、証明書に関連する公開鍵を含む。証明書署名５９は、ＣＡによって生成された署名を含む。さらに深く理解されるように、サーバ証明書４６は、対応するサーバ秘密鍵５０を含む。

【００３１】

サーバ証明書４６の信頼性を確認した後、クライアントコンピュータ１２は、ＣＥＲＴＩＦＩＣＡＴＥ＿ＶＥＲＩＦＹコマンド６６を送信する。また、クライアントコンピュータ１２は、第１のＣＨＡＮＧＥ＿ＣＩＰＨＥＲ＿ＳＰＥＣコマンド６８を、その直後に第１のＦＩＮＩＳＨＥＤコマンド７０を送信する。これは、現在のセッションが暗号化されている間にクライアントコンピュータ１２によって送信される、後続のＴＬＳレコードデータの内容を示す。第１のＦＩＮＩＳＨＥＤコマンド７０は、変更が行われていないことを保証するために、これまでに送信された全てのハンドシェイクコマンドのダイジェストを含む。次に、サーバコンピュータ１４は、第２のＣＨＡＮＧＥ＿ＣＩＰＨＥＲ＿ＳＰＥＣコマンド７２を、その直後に第２のＦＩＮＩＳＨＥＤコマンド７４を送信する。第１のＣＨＡＮＧＥ＿ＣＩＰＨＥＲ＿ＳＰＥＣコマンド６８と同様に、第２のＣＨＡＮＧＥ＿ＣＩＰＨＥＲ＿ＳＰＥＣコマンド７２は、現在のセッションが暗号化されている間にサーバコンピュータ１４によって送信される、後続のＴＬＳレコードデータを示す。第２のＦＩＮＩＳＨＥＤコマンド７４は、サーバコンピュータ１４からクライアントコンピュータ１２へのこれまでの全てのハンドシェイクコマンドを含む。クライアントコンピュータ１２は、サーバ証明書４６内のサブジェクト公開鍵５７ｂで暗号化されている、生成された対称鍵を送信する。サーバ秘密鍵５０は、サーバコンピュータ１４による受信時に、対称鍵に対する解読のために用いられ、クライアントコンピュータ１２への後続の送信は、この秘密鍵を用いて暗号化されることになる。

【００３２】

上記したように、クライアントコンピュータ１２は、本発明の態様に従って、サーバ証明書４６を安全に検索する。具体的には、クライアントコンピュータ１２とサーバコンピュータ１４との間のＴＬＳ接続３０を確立するプロセスに従って、サーバ証明書４６が送信される。一実施形態において、クライアントコンピュータ１２は、以下にさらに詳細に説明するように、ＴＬＳ接続３０の外部での使用のために、サーバ証明書４６を格納する。

【００３３】

図２及び図３に戻って、クライアントコンピュータ１２及びサーバコンピュータ１４を相互に認証する方法は、応答パケット７６をサーバコンピュータ１４へ送信するステップ２２０を続ける。図６に示すような詳細において、応答パケット７６は、フル要求ＵＲＬ３２、トークン３６、サーバ証明書４６及びクライアント証明書７８で構成されている。クライアント証明書７８の構造は、図５に示すように、サーバ証明書４６の構造と同じであり、バージョン５１、シリアルナンバー５２、発行者５４、有効性識別子５５、サブジェクト識別子５６、サブジェクト公開鍵情報５７ａ、５７ｂ及び証明書署名５９を含む。本発明の一実施形態によれば、証明書の記憶場所からクライアント証明書７８を検索するのに、Ｍｉｃｒｏｓｏｆｔ　ＣｒｙｐｔｏＡＰＩライブラリが利用される。サーバ証明書４６と同様に、クライアント証明書７８は、対応する秘密鍵であるクライアント秘密鍵８０も有している。応答パケット７６は、クライアント秘密鍵８０に関連付けられた追加的な認証識別子を含む。本発明の一実施形態によれば、このような認証識別子は、応答パケット７６の内容の暗号学的ハッシュ７７である。単に例証として、および非限定的に、メッセージダイジェストアルゴリズム－２（ＭＤ２）ハッシュ関数が用いられるが、メッセージダイジェストアルゴリズム－５（ＭＤ５）、セキュアハッシュアルゴリズム（ＳＨＡ

）等の他の何らかのハッシュ関数を、本発明の範囲から逸脱することなく、代用することができる。その結果として生じる暗号学的ハッシュ７７は、クライアント秘密鍵８０によって署名される。

【００３４】

ステップ２３０に従って、方法は、応答パケット７６の内容の正当性を検証することを含む。まず、応答パケット７６自体の信頼性が検証される。上記したように、応答パケット７６は、クライアント秘密鍵８０で署名されている暗号学的ハッシュ７７を含む。図７ａ～図７ｃを参照して、ステップ３００に従って、クライアント側暗号学的ハッシュ７７aが、クライアント証明書７８を用いて解読される。サーバ側暗号学的ハッシュが、サーバ１４上に存在するように、応答パケット７６に対して演算される。サーバ側暗号学的ハッシュは、比較ステップ３１２ごとに、応答パケット７６を伴うクライアント側暗号学的ハッシュ７７と比較される。値が一致しない場合には、応答パケット７６は改ざんされていると見なされ、ステップ３１５のように、いかなる接続も終了される。値が一致した場合には、以下に説明するように、応答パケット７６の内容のさらなる検証が続けられる。

【００３５】

このようなさらなる検証は、応答パケット７６の構成要素を、既知の応答パケットのコピーと比較することを含む。まず、クライアント証明書７８の署名が、ステップ３２０ごとに検証され、この場合、サブジェクト公開鍵情報５７ｂの正当性が確認される。その後、証明書署名５９及び発行者識別子５４は、正当に認可されたＣＡが、クライアント証明書７８に署名していることを検証するために、ステップ３３０ごとに調べられる。サブジェクト識別子５６もまた、クライアント証明書７８が、正当に認可された組織に対して発行されたことを検証するために、ステップ３４０ごとに調べられる。一実施形態によれば、正当に認可された組織は、サーバコンピュータ１４を介した制御を有する正当な組織を指す。また、クライアント証明書７８は、ステップ３５０ごとに、クライアント証明書７８の有効性識別子５５を、現在の日付と比較することにより、有効であるか、および有効期限が切れていないかが検証される。上記の検証ステップのいずれかに失敗した場合は、クライアント証明書７８は、改ざんされていると見なされて、ステップ３１５ごとに接続が切り離される。

【００３６】

また、フル要求ＵＲＬ３２、トークン２６及びサーバ証明書４６を含む、応答パケット７６内の残りの構成要素も、その正当性が確認される。上記したように、トークン２６または証明書要求識別子は、サーバコンピュータ１４内に格納される。ステップ３６０ごとに、トークン２６のこのように格納された値は、応答パケット７６内のトークン２６の値と比較される。マッチング値が、リプレー攻撃が行われていないことを確かめることは理解されよう。ステップ３７０におけるフル要求ＵＲＬ３２に関して、その値が、サーバコンピュータ１４の実際のＵＲＬに対して確認される。このことは、クライアントコンピュータ１２を、悪意のあるサーバへリダイレクトするフィッシング攻撃が行われていないことを確認することであると理解されよう。応答パケット７６に含まれているサーバ証明書４６に関しては、ステップ３８０ごとに、サーバコンピュータ１４上に存在するサーバ証明書４６と比較される。このことは、応答パケット７６を介して返送されるものとは対照的に、サーバ証明書４６が、サーバコンピュータ１４上に格納されたものとは異なるため、介入者攻撃を防ぐ。これらの状況に沿って、上記の検証のいずれかに失敗した場合、サーバコンピュータ１４とクライアントコンピュータ１２の間の接続は即座に遮断され、サーバコンピュータ１４へのこれ以上のアクセスは、許可されない。しかし異常がない場合、クライアントコンピュータ１２は、認証され、サーバコンピュータ１４へのアクセスを続ける。正しく認識されるように、上記の確認は、１つ以上のセキュリティ違反を発見する。

【００３７】

図８を参照して、本発明の別の態様によれば、クライアントコンピュータ１２は、クライアント認証モジュール８２を含み、サーバコンピュータ１４は、サーバ認証モジュール

８４を含む。クライアント認証モジュール８２は、トークン２６、スクリプト２８、サーバ証明書４６及びクライアント証明書７８の検索を含む、上記したようなクライアント側のプロセス、ならびにクライアント秘密鍵８０で署名した後の、応答パケット７６の送信を処理するように理解されている。一実施形態によれば、クライアント認証モジュール８２は、クライアントコンピュータ１２上のウェブブラウザを介して、単一のユーザインタラクションでインストールされるＡｃｔｉｖｅ－Ｘコンポーネントである。しかし、ブラウザに追加することのできる代替の実行可能なコンポーネントも、本発明の範囲内にあると見なされている。サーバ認証モジュール８４は、トークン２６及びサーバ証明書４６の送信、ならびに受信した応答パケット７６の検証を含む、上記したサーバ側のプロセスを処理するように理解されている。従って、クライアント認証モジュール８２とサーバ認証モジュール８４は、互いに通信し、また、クライアント側ＴＬＳの配置を伴うことなく、共にＸ．５０９の認証スキームを実施する。

【００３８】

上記した方法は、クライアント証明書７８及び対応するクライアント秘密鍵８０が、既にクライアントコンピュータ１２上に存在していることを前提としていることは、よく認識されよう。サーバ認証モジュール８４は、クライアント証明書７８がクライアントコンピュータ１２上に存在するか否かを判断することができ、存在していない場合には、サーバ認証モジュール８４は、証明書サーバ８６に警告する。クライアントコンピュータ１２に対してクライアント証明書及びクライアント秘密鍵を発行する前に、証明書及び秘密鍵に関連するユーザは、帯域外の手順で認証される。一実施形態によれば、サーバ認証モジュール８４は、電話サーバ８８に、ユーザの制御下で、ワンタイムパスワードを携帯電話または固定電話へ配信するように通知する。別法として、電子メールまたはショートメッセージサービス（ＳＭＳ）のテキストメッセージを送信してもよい。音声認識、ＩＰアドレス検証等の他の帯域外の認識技術も意図されている。ワンタイムパスワードの入力は、サーバ認証モジュール８４を有するサーバコンピュータ１４を介して処理することができる。代わりに、または、上記の自動的ではない認証に加えて、ユーザは、追加的な知識ベースの認証によって提示することができる。例えば、好きな色、出身高校及び他の同様の質問をユーザに尋ねてもよい。

【００３９】

正しい応答を提供した場合、サーバ認証モジュール８４は、証明書サーバ８６に、クライアント秘密鍵及び対応するクライアント証明書を生成して、クライアントコンピュータ１２上に格納するように指示する。後の検索、およびサーバ認証モジュール８４による使用のために、追加的な認証情報を、企業データベース９０に格納してもよい。上記の処理手順は、サーバコンピュータ１４を有するクライアントコンピュータシステム１２上のブラウザに「登録」し、そのようなブラウザを、有効に第２の認証ファクター（「ユーザが有する何か」）にすることは理解されよう。

【００４０】

上記したように、発行者識別子５４は、正当に認可されたＣＡが、クライアント証明書７８を発行し、署名したことを確認するために調べられる。図８に示す実施形態によれば、証明書サーバ８６はＣＡであり、サーバコンピュータ１４及び企業データベース９０を管理する組織とは別の正当なサードパーティプロバイダの管理内にあると理解されよう。図９に示す代替的な構成においては、証明書サーバ８６及び電話サーバ８８は、サーバコンピュータ１４を管理する同じ組織によって管理され、維持される。図１０に示すさらに別の構成においては、ウェブサービス９２に対して、安全なアクセスが可能になっている。理解されるように、ウェブサービス９２という用語は、マシン間の相互作用をサポートする標準化されたシステムを指す。この場合、クライアントコンピュータ１２は、サーバコンピュータ１４に関して認証するためのクライアント認証モジュール８２を利用する。このようにして生成されたクライアント証明書７８は、Ｗ３クライアントを認証して、クライアント証明書７８を介してウェブサービス９２に関して認証するのに利用される。

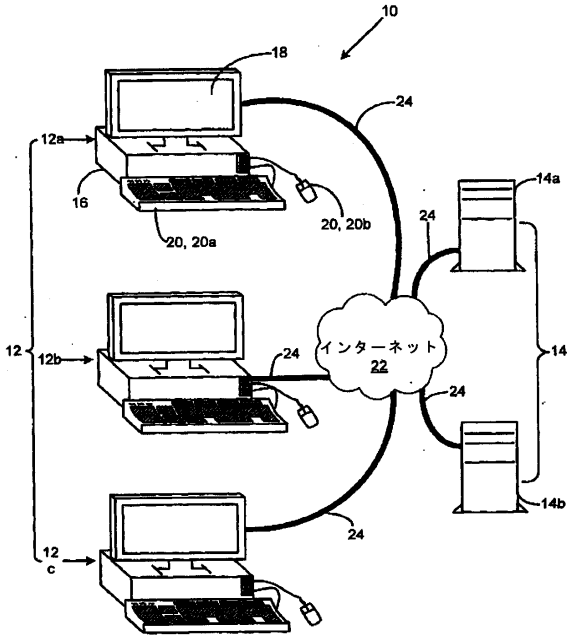
【００４１】

上記の構成に加えて、クライアント認証モジュール８２及びサーバ認証モジュール８４を、双方向の認証を要する幅広いアプリケーションに統合することができることが明確に意図されている。単に例証として、および非限定的に、アプリケーションは、．ＮＥＴアプリケーションにおける．ＮＥＴ方式の認証、Ｍｉｃｒｏｓｏｆｔ　Ｏｕｔｌｏｏｋ　Ｗｅｂ　Ａｃｅｓｓ及びＭｉｃｒｏｓｏｆｔ　Ｓｈａｒｅｐｏｉｎｔ、ならびに適切なクライアント及びサーバ認証を要するエンフォースメントポイントを有する他の何らかのシステムを含む。

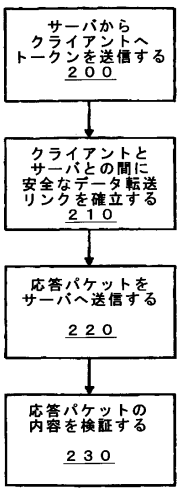
【００４２】

本願明細書に示されている具体例は、例示的なものであり、また、本発明の実施形態の説明のためのみのものであり、本発明の原理及び概念的態様の最も有用かつ容易に理解される説明であると思われることを提供するためにある。この点に関して、本発明の基本的理解に必要なこと以上の詳細を示す試みはなされておらず、上記説明は、図面と共に、当業者に対して、本発明のいくつかの形態を実際にどのように具体化するかを明らかにする。

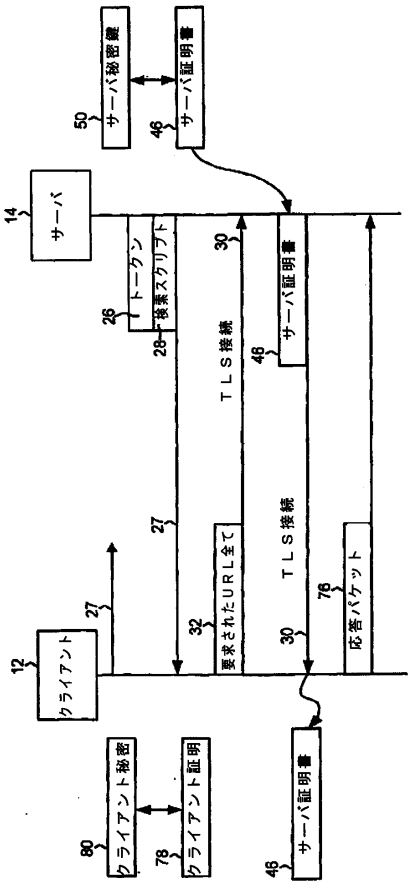
【図１】



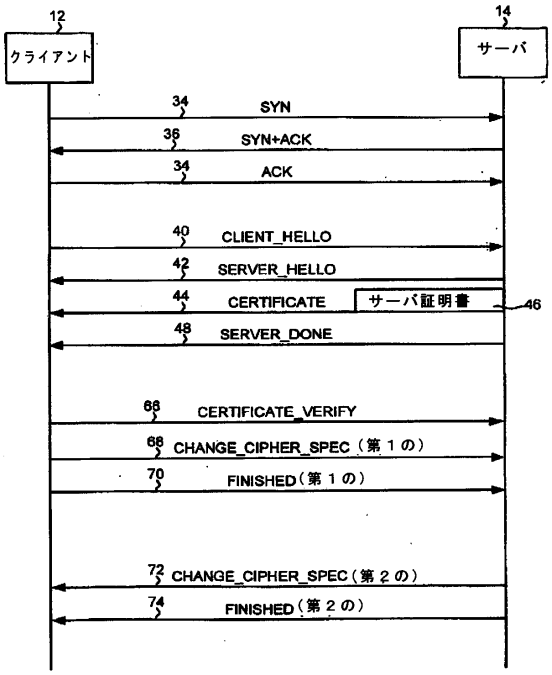
【図２】



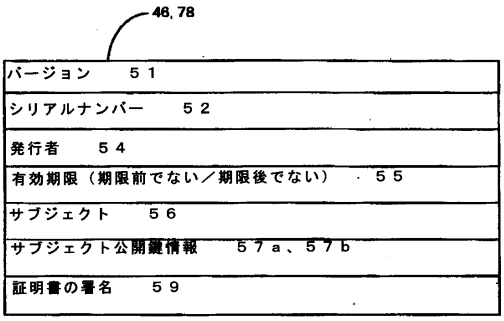
【図３】



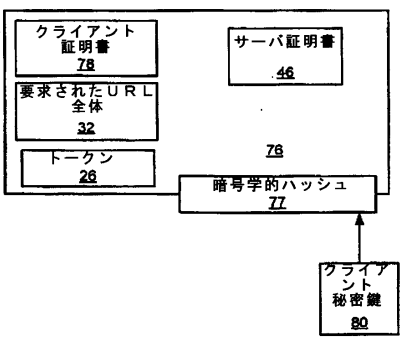
【図４】



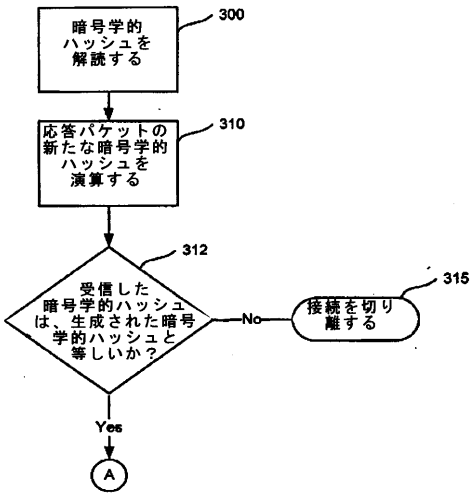
【図５】



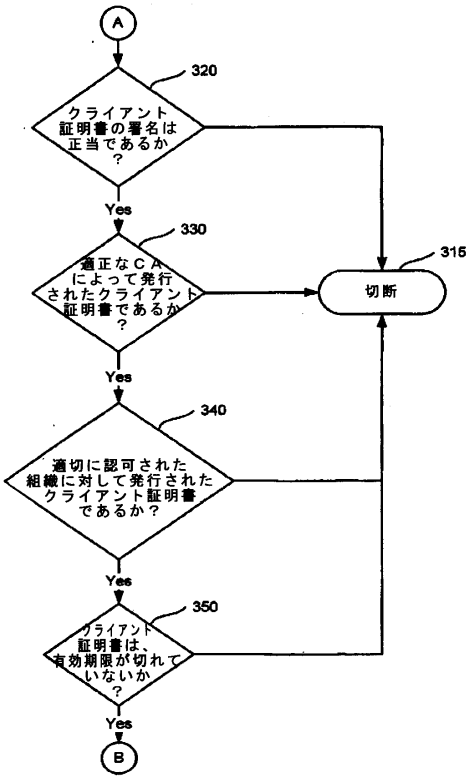
【図６】



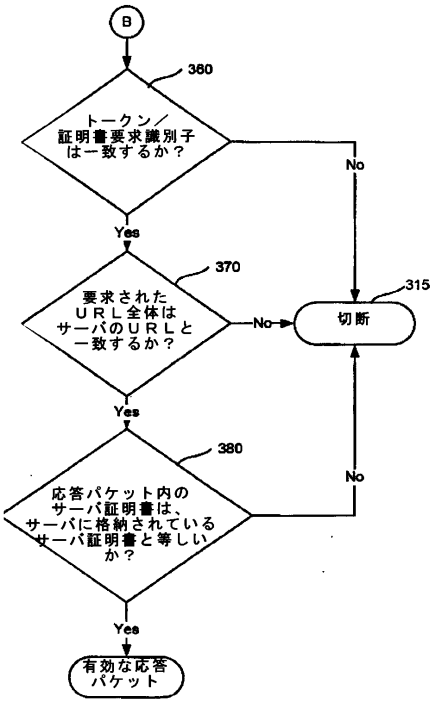
【図７ａ】



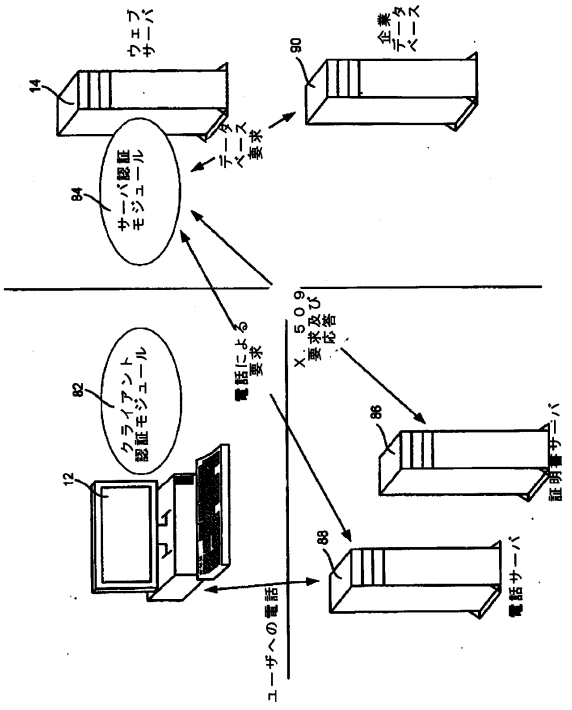
【図７ｂ】


A
320
クライアント証明書の署名は正当であるか？
Yes
330
適正なＣＡによって発行されたクライアント証明書であるか？
315
切断
Yes
340
適切に認可された組織に対して発行されたクライアント証明書であるか？
Yes
350
クライアント証明書は、有効期限が切れていないか？
Yes
B

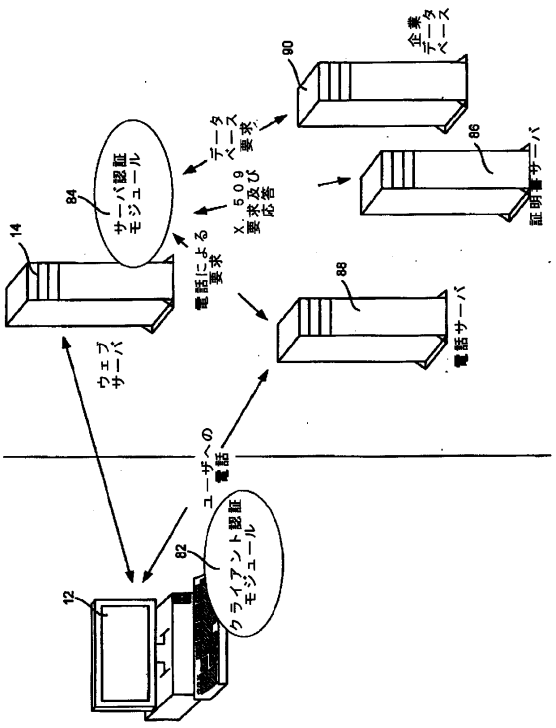
【図７ｃ】


B
360
トークン／証明書要求識別子は一致するか？
No
Yes
370
要求されたＵＲＬ全体はサーバのＵＲＬと一致するか？
No
315
切断
Yes
380
応答パケット内のサーバ証明書は、サーバに格納されているサーバ証明書と等しいか？
No
Yes
有効な応答パケット

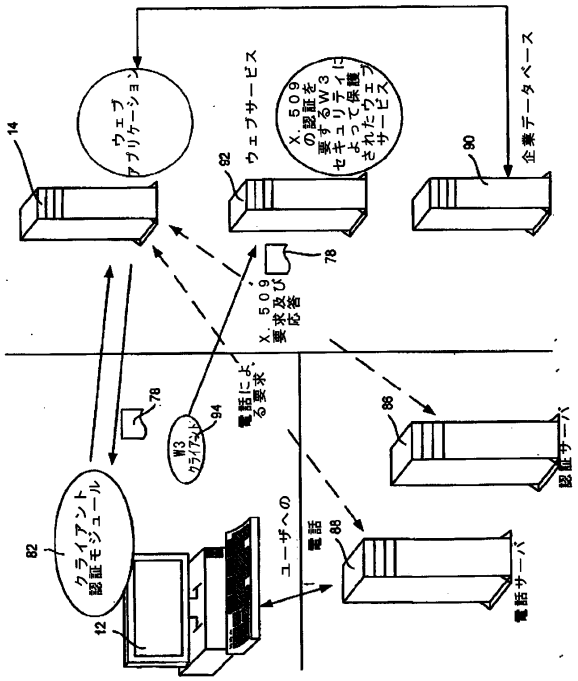
【図８】


ウェブサーバ
14
企業データベース
90
データベース要求
サーバ認証モジュール
84
電話による要求
X.509要求及び応答
クライアント認証モジュール
82
証明書サーバ
86
12
電話サーバ
88
ユーザへの電話

【図９】


企業データベース
90
データベース要求
X.509要求及び応答
証明書サーバ
86
サーバ認証モジュール
84
14
電話による要求
88
電話サーバ
ウェブサーバ
ユーザへの電話
クライアント認証モジュール
82
12

【図１０】


ウェブ
アプリケーション
14
ウェブサービス
82
X.509
の認証を
実装するW3
セキュリティに
よって保護
されたウェブ
サービス
企業データベース
90
78
X.509
要求及び
応答
電話による
要求
78
94
W3
クライアント
86
認証サーバ
82
クライアント
認証モジュール
ユーザへの
電話
88
電話サーバ
12

フロントページの続き

(72)発明者 ランド、クレイグ
アメリカ合衆国 ９２６１２ カリフォルニア州 アーバイン ビジネス センター ドライブ ２１０２ スイート １３０
(72)発明者 グラジェック、ギャレット
アメリカ合衆国 ９２６４７ カリフォルニア州 ハンティントン ビーチ フォーリング ウォーター ドライブ ６２８２
(72)発明者 ムーア、スティーブン
アメリカ合衆国 ９７２１７ オレゴン州 ポートランド テリー ストリート １５０５ アパートメント ナンバー３

審査官 松平 英

(56)参考文献 特開２００５－０１８７４９（ＪＰ，Ａ）
特表２００２－５３８７０１（ＪＰ，Ａ）
特開２００３－００５６４０（ＪＰ，Ａ）
特開２００４－２４２１９５（ＪＰ，Ａ）
特開２００６－０７２４９３（ＪＰ，Ａ）
特開２００６－１７１８９２（ＪＰ，Ａ）
特表２００８－５４４４０５（ＪＰ，Ａ）
本城 信輔 他，プライバシに配慮したWWWにおける個人属性認証・アクセス制御システム，情報処理学会論文誌，日本，社団法人情報処理学会，２００２年 ８月１５日，第４３巻 第８号，ｐ．２５７３～２５８６
飯田 恭弘 他，ユーザを識別しない認証方式の実装と評価，第６２回（平成１３年前期）全国大会講演論文集（３），社団法人情報処理学会，２００１年 ３月１３日，ｐ．３－３０１～３－３０２

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/00
G09C 1/00
G06F 21/20
G06F 21/24
H04W 4/00
H04L 12/00
H04L 29/00