(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4744785号
(P4744785)
(45)発行日　平成23年8月10日(2011.8.10)　(24)登録日　平成23年5月20日(2011.5.20)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G06F 21/20	(2006.01)	G06F	15/00	330B
H04L 9/08	(2006.01)	H04L	9/00	601B

請求項の数 12　(全 20 頁)

(21)出願番号　特願2003-109094(P2003-109094)
(22)出願日　平成15年4月14日(2003.4.14)
(65)公開番号　特開2004-48679(P2004-48679A)
(43)公開日　平成16年2月12日(2004.2.12)
審査請求日　平成18年4月4日(2006.4.4)
(31)優先権主張番号　10/146686
(32)優先日　平成14年5月15日(2002.5.15)
(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　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行
(74)代理人　100091063
弁理士　田中　英夫

最終頁に続く

(54)【発明の名称】セッションキー・セキュリティプロトコル

(57)【特許請求の範囲】
【請求項１】
第１ネットワークサーバー、第２ネットワークサーバー及びクライアントコンピュータがデータ通信ネットワークに結合されているマルチサイト認証システムにおいて情報を安全にする方法であって、
前記クライアントコンピュータによる前記第２ネットワークサーバーへのアクセスに応答して、前記第１ネットワークサーバーが、前記クライアントコンピュータのユーザーに関連付けられた情報を含む認証チケットを生成するステップと、
前記第１ネットワークサーバーが、前記第１ネットワークサーバーと前記第２ネットワークサーバーとにより共有され且つランダムに発生されるセッションキーを用いて、前記認証チケットの内容を暗号化するステップと、
前記第１ネットワークサーバーが、前記第２ネットワークサーバーに関連する公開キーを用いて前記セッションキーを暗号化するステップと、
前記第１ネットワークサーバーが、前記クライアントコンピュータを前記認証チケットと共に前記第１ネットワークサーバーから前記第２ネットワークサーバーにリダイレクトするステップと、
前記第２ネットワークサーバーが、該第２ネットワークサーバーに関連付けられた個人キーを用いて前記セッションキーを解読し、解読された前記セッションキーを用いて前記認証チケットの内容を解読するステップと、
前記第１ネットワークサーバーが、該第１ネットワークサーバーに関連付けられた個人

キーを用いて前記認証チケットのための署名を生成するステップと
を備えることを特徴とする方法。
【請求項２】
前記署名が、前記第２ネットワークサーバーのためのアドレス情報を含んでおり、
前記第２ネットワークサーバーが、前記署名を正当化するため、前記署名の中の前記アドレス情報を同定する
ことを特徴とする、請求項１に記載の方法。
【請求項３】
前記第１ネットワークサーバーから前記第２ネットワークサーバーへ、プライバシー保護機能が強化されたプロトコルを用いて前記認証チケットを送ることを特徴とする、請求項１又は２に記載の方法。
【請求項４】
前記クライアントコンピュータのブラウザを介して、前記第２ネットワークサーバーにより提供されるサービスに対する要求を前記クライアントコンピュータから受け取ることを特徴とする、請求項１～３のうちの何れか１つに記載の方法。
【請求項５】
前記第２ネットワークサーバーが、前記データ通信ネットワークに結合される１つ以上の他のネットワークサーバーにより前記ユーザーに提供されるサービスへのゲートウェイを提供するポータルであることを特徴とする、請求項１～４のうちの何れか１つに記載の方法。
【請求項６】
前記第１ネットワークサーバー及び前記第２ネットワークサーバーがウェブサーバーであり、前記データ通信ネットワークがインターネットであることを特徴とする、請求項１～５のうちの何れか１つに記載の方法。
【請求項７】
認証サーバーとウェブサーバーとクライアントコンピュータとがデータ通信ネットワークに結合され、情報を安全にするマルチサイト認証システムであって、
前記クライアントコンピュータによる前記ウェブサーバーへのアクセスに応答して、前記認証サーバーが、前記クライアントコンピュータのユーザーからのログイン情報を検索し、
前記のユーザー認証の後に、前記認証サーバーが、前記ユーザーに関連付けられた情報を含む認証チケットを生成し、
前記認証サーバーが、前記認証サーバーと前記ウェブサーバーとにより共有され且つランダムに発生されるセッションキーを用いて、前記認証チケットの内容を暗号化し、
前記認証サーバーが、前記ウェブサーバーに関連する公開キーを用いて前記セッションキーを暗号化し、
前記認証サーバーが、前記クライアントコンピュータを前記認証チケットと共に前記認証サーバーから前記ウェブサーバーにリダイレクトし、
前記ウェブワークサーバーが、該ウェブサーバーに関連付けられた個人キーを用いて前記セッションキーを解読し、解読された前記セッションキーを用いて前記認証チケットの内容を解読し、
前記認証サーバーが、前記認証チケットのための署名を生成するための個人キーを備え、
前記署名が、前記ウェブサーバーのためのアドレス情報を含み、
前記ウェブサーバーが、前記署名の中の該ウェブサーバーのためのアドレス情報を同定して前記署名を正当化する
ことを特徴とするシステム。
【請求項８】
前記認証チケットが、前記セッションキーによって暗号化された内容と前記セッションキーと前記署名とを含むことを特徴とする、請求項７に記載のシステム。

【請求項９】
前記認証サーバーが、前記ユーザーから検索されたログイン情報と比較するためのログイン情報を記憶するデータベースを備えることを特徴とする、請求項７又は８に記載のシステム。
【請求項１０】
第１ネットワークサーバーと第２ネットワークサーバーとクライアントコンピュータとがデータ通信ネットワークに結合されているマルチサイト認証システムにおいて情報を安全にする方法であって、
前記クライアントコンピュータによる前記第２ネットワークサーバーへのアクセスに応答して、前記第１ネットワークサーバーが、前記クライアントコンピュータのユーザーに関連付けられた情報を含む認証チケットを生成するステップと、
前記第１ネットワークサーバーが、前記第１ネットワークサーバーと前記第２ネットワークサーバーとにより共有され且つランダムに発生されるセッションキーを用いて、前記認証チケットの内容を暗号化するステップと、
前記第１ネットワークサーバーが、該第１ネットワークサーバーと関連付けられた個人キーを用いて、前記認証チケットのための署名を生成するステップであって、前記署名が前記第２ネットワークサーバーのためのアドレス情報を含んでいるステップと、
前記第１ネットワークサーバーが、前記第２ネットワークサーバーに関連する公開キーを用いて前記セッションキーを暗号化するステップと、
前記第１ネットワークサーバーが、前記クライアントコンピュータを前記認証チケットと共に前記第１ネットワークサーバーから前記第２ネットワークサーバーにリダイレクトするステップと、
前記第２ネットワークサーバーが、該第２ネットワークサーバーに関連付けられた個人キーを用いて前記セッションキーを解読し、解読された前記セッションキーを用いて前記認証チケットの内容を解読し、前記署名の中の前記アドレス情報を同定して前記署名を正当化するステップと、
を備えることを特徴とする方法。
【請求項１１】
前記第１ネットワークサーバーから前記第２ネットワークサーバーへ、プライバシー保護機能が強化されたプロトコルを用いて前記認証チケットを送ることを特徴とする、請求項１０に記載の方法。
【請求項１２】
前記のプライバシー保護機能が強化されたプロトコルが、セキュアソケットレイヤ・プロトコルであることを特徴とする、請求項１１に記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、コンピュータネットワーク環境に関するものであり、特に、本発明は、セッションキー・セキュリティ・プロトコルを用いることによりマルチサイトユーザ認証システムにおけるセキュリティの改善に関するものである。
【０００２】
【従来の技術】
ウェブサイトすなわちインターネットサイトは、非常にしばしば、多数のユーザーに対して情報、製品、サービスなどを提供する。多くのウェブサイトは、そのウェブサーバーがユーザーにアクセスを許可する前に、「登録する」ことをユーザーに要求する。登録の間、ユーザーは、典型的には、個人的情報、たとえば、ユーザー名、アカウント番号、住所、電話番号、電子メールアドレス、コンピュータ・プラットフォーム、年齢、性、趣味などを入力する。登録情報は、トランザクション（たとえば、商品や金銭の取引）を完了するために必要であることがある。また、この情報は、典型的には、たとえば特別なプロモーション、新製品、ウェブサイトの新しい特徴などを知らせるために、ウェブサイトがユ

ーザーに直接に（たとえば電子メールにより）接触することを可能にする。さらに、ウェブサイトの運営者が将来の販売活動をよりよく目標を定めるように、または、サイトにより提供されるコンテンツを調整するように、ウェブサイトはしばしばユーザー情報を集める。

【０００３】

はじめてユーザーを登録するとき、ウェブサイトは、典型的には、ユーザーがログインＩＤと関連するパスワードを選択することを求める。ログインＩＤは、ウェブサイトがユーザーを同定して、そのユーザーがウェブサイトをしばしば訪れるときにユーザー情報を検索することを可能にする。一般的に、ログインＩＤは、２人のユーザーが同じログインＩＤを持たないように、そのウェブサイトにおいて一意でなければならない。ログインＩＤに関連するパスワードは、そのウェブサイトに後で訪れるときにユーザーを認証することを可能にする。また、パスワードは、他人（そのパスワードを知らない人）が、そのユーザーのログインＩＤを用いてウェブサイトをアクセスすることを防止する。このパスワード保護は、そのウェブサイトが、そのユーザーについての個人情報または秘密情報を格納しているなら、特に重要である。

【０００４】

もしユーザーがいくつかの異なるウェブサイトを訪ねるなら、各ウェブサイトは、そのユーザーについての、ユーザー名、郵便の住所、電子メールアドレスなどの同様な登録情報の入力を要求することがある。短時間に多くのウェブサイトを訪ねるとき、同一のデータについてのこの繰り返し入力は単調で退屈である。多くのウェブサイトは、そのサイトで提供される情報にアクセスする前に登録することをユーザーに要求する。このため、ユーザーは、そのサイトが関心のある情報を含んでいるかを決める前に、まず、要求される情報を入力しなければならない。

【０００５】

多くのウェブサイトでは、入力した後で、ユーザーは、各ウェブサイトまたは他のインターネットサービスで使用される特定のログインＩＤとパスワードを記憶せねばならない。正しいログインＩＤとパスワードがなければ、ユーザーは、登録情報を再入力しなければならない。１人のユーザーは、異なるウェブサイトで異なるログインＩＤと関連するパスワードを持つことが多い。たとえば、ボブ・スミスという名のユーザーがあるサイトでログインＩＤとして「smith」を選択するとする。もしそのサイトにすでに「smith」というログインＩＤのユーザーがいた場合、または、そのサイトが６字以上のログインＩＤを要求するならば、そのユーザーは、異なるログインＩＤを選択せねばならない。多数のウェブサイトを訪ねた後で、ボブ・スミス（Bob Smith）は、smith、smith1、bsmith、smithb、bobsmith、bob_smith、smithbobなどの異なる多数のログインＩＤを持っていることがある。さらに、異なるパスワードは、異なるウェブサイトでの異なるパスワード要求（たとえばパスワードの長さの要求、各パスワードが１字以上の数字および／または少なくとも１字の大文字を含むという要求）により異なるログインＩＤと関連されることがある。こうして、ボブ・スミスは、定期的に訪ねるすべてのウェブサイトについて、ウェブサイト、ログインＩＤおよびパスワードのリストを維持せねばならない。

【０００６】

【発明が解決しようとする課題】

現在利用可能な複数サイトのユーザー認証システムが、多数の関連のあるウェブサーバーまたはウェブサービスにアクセスするために、ウェブユーザーが１つのログインＩＤ（及び関連するパスワード）を維持することを可能にしているけれども、さらに改善することが求められている。たとえば、認証データは、もともと、典型的には傷つきやすく、保護されねばならない。このため、多数の関連するウェブサイトと、認証機能を実行する認証サーバーとの間のセキュリティが重要である。

【０００７】

ケルベロス（Kerberos）認証などの現在利用できるネットワーク認証プロトコルは、ネットワークにログインしようとするユーザーの身元を認証し通信を暗号化するための共用の

キーすなわち唯一のキーを使用する。共用キーの使用（しばしば対称キー暗号化という）は、新しいウェブサービスが認証サービスを使用するのためキーを供給する処理を要求する。ケルベロスシステムでは、認証サーバー（ケルベロスサービスすなわちキー配布センター（KDC)）は、その認証サービスを使用するすべての関連するサーバーに共用キーを配布せねばならず、また、そのキーを定期的に新しくせねばならない。キー配布センターは、しばしばキーを郵送で発行する。残念ながら、共用キーを提供する必要性は、新しくウェブサービスに入るときやアクセス中の維持（定期的なキーの変更）を行うときに、かなりの複雑さをもたらす。さらに、多数の認証サービスプロバイダが連合する環境では、キー配布はさらに複雑になる。

【０００８】

関連するサイトが２以上の独立のキー配布センター(KDC)から「kerb」チケットを受け取ることを決定するとき、キー配布はさらに複雑になる。また、認証システム対応サーバーのためのキーは、２つのキー配布センターで構成されねばならない。いいかえれば、関連するサイトをサポートするサイトが増えるほど、キー配布処理が複雑になる。さらに、もし複数のキー配布センターが連合する場合、キーをすべて共用せねばならず、キー配布の複雑性が増える。

【０００９】

また、キーは、キー配布センター(KDC)で、または、いずれかの関連サイトで盗まれる危険性があり、これは、セキュリティプロトコルのいずれかのところでキーの信用性を傷つける危険性をもたらす。たとえば、認証サービスに人が侵入すると、すべての関連するサーバーのすべてのキーが盗まれる可能性がある。これがあると、関連するサーバーの全体のネットワークにわたってすべてのキーを新しくするのに必要な時間のため、認証サービスが本質的にシャットダウンする。

【００１０】

公開キーインフラ構造(PKI)は、また、暗号化やディジタル認証をサポートするために使用できる。公開キー暗号化は、２つのキー、すなわち、１つの公開キーと１つの個人キーとを使用する。公開キーを用いて暗号化されたデータは、個人キーによってのみ復号化でき、また、その逆もある。公開キーインフラ構造は文書を認証し、ディジタル署名をするのに有用なプロトコルを提供するけれども、スケーラブルで複数プラットフォームで動作する認証システムでは、うまく動かない。たとえば、公開キーインフラ構造のシステムは、一般的に非常に長いキー（典型的には、５１２ビット以上、これに対し、共用キーは２００ビットより短い）を必要とするため、大量のデータを扱うときはあまりにも遅く動作する。キーが長くなるほど、より大きな計算能力が暗号化と復号化のために必要となる。

【００１１】

さらに、公開キーインフラ構造(PKI)はキーが同期されることを必要とする。公開キーインフラ構造は、２つのキー(公開キーと個人キー）を持ち、これらの２つのキーは同期していなければならない。そのような１対のキーを取り消し、新しい対のキーを作るための、十分確立されたプロトコル／処理がある。

【００１２】

これらの理由のため、特にスケーラブル／複数プラットフォームの認証システムで使用するため、共用の対称キープロトコルにおける上述の問題を最小にする、改良されたセキュリティプロトコルが望まれている。

【００１３】

この発明の目的は、マルチサイト認証システムにおけるセキュリティを改善することである。

【００１４】

【課題を解決するための手段および発明の効果】

この発明は、複数サイトユーザー認証システムのための改良されたセキュリティを提供することにより、上述の要望にかない従来の技術のいくつかの短所を解決する。好ましくは、この発明は、セキュリティを公開キーインフラ構造(ＰＫＩ)の特徴で適応することによ

り、スケーラブルで複数プラットフォームで動作する認証システムの複雑さを減らす。これは、共用対称キープロトコルに固有の問題を最小にし、すでに存在している使用中のシステム／ソフトウェアの継続使用を可能にする。このことは、コストを著しく低下し、産業界における広い採用を促がす。

【００１５】

だれかが認証サービスの個人キーを盗んでも、本発明による改良プロトコルにより、認証サービスは、残っている信頼できる、サービスが委託されているサイトを崩壊することなく、その個人キーを急速に更新できる。同様に、目的先のサービス（すなわち対応ウェブサーバ）で個人キーが盗まれても、その行先のサービスは、認証サービスが新しいキーを発行するのを待つよりは、それ自体の個人キーと公開キーを更新する処理を独立に開始できる。

【００１６】

また、この発明は、セキュリティの危険を分離するため、目的先のサービスが多数の対の個人キーと公開キー（すなわち、委託されている認証サービスあたり１つ）を持つことを可能にする。この発明は、公開キーインフラ構造の考えを共用キー認証プロトコルに適用し、認証サービスにおけるキーの信用を傷つけることに関連するセキュリティの危険を除去できるので、プロトコルを強化する。さらに、ここに説明した発明の特徴は、現在使用されている技術よりも実行が容易であり、また、経済的に実行でき、事業として実用的である。

【００１７】

簡単に説明すると、本発明の第１の観点を具体化した方法は、データ通信ネットワークに結合される第１と第２のネットワークサーバーを含むマルチサイト認証システムにおける情報セキュリティを提供する。この方法では、第１ネットワークサーバーは、認証チケットを生成し、その認証チケットの内容を暗号化する。認証チケットは、データ通信システムに結合されるクライアントコンピュータのユーザーと関連される情報を含む。第１ネットワークサーバーは、第１と第２のネットワークサーバーにより共用される対称キーを用いて、認証チケットの内容を暗号化する。この方法では、さらに、第２ネットワークサーバーと関連される公開キーを用いて共用キーを暗号化し、第１のネットワークサーバーから第２のネットワークサーバーに、前記の認証チケットを持っているクライアントコンピュータを向ける(direct)。

【００１８】

本発明の第２の観点を具体化したシステムは、マルチサイト認証システムと関連される認証サーバーを含む。認証サーバーは、クライアントコンピュータのユーザーを認証するために、そのユーザーからログイン情報を検索する。さらに、認証サーバーは、ユーザーを認証した後で、クライアントコンピュータのユーザーに関連された情報を含む認証チケットを生成する。認証サーバーは、チケットの内容を暗号化するため、認証システム対応サーバーにより共用されている共用対称キーを用いる。認証システム対応サーバーは、公開キーを備え、認証サーバーは、この公開キーを用いて、前記の共用キーを暗号化する。

【００１９】

本発明の他の観点を具体化した方法では、第１ネットワークサーバーから、クライアントコンピュータのユーザーに関連付けられた情報を含む認証チケットを生成し、第１ネットワークサーバーと関連付けられた個人キーを用いて、チケットのための署名を生成する。この署名は、第２ネットワークサーバーのためのアドレスを含む。この方法では、さらに、第１のネットワークサーバーから第２のネットワークサーバーに、プライバシー保護機能が強化されたプロトコルを用いて、前記のチケットを持っているクライアントコンピュータをリダイレクトし、第２ネットワークサーバーにより、署名を正当化するため署名の中の第２ネットワークサーバー自身のアドレス情報を同定する。

【００２０】

本発明の観点を具体化するセキュリティプロトコルは、共用対称キー、公開キー及び個人キーを含む。第１ネットワークサーバーと第２ネットワークサーバーは共用対称キーを共

用する。共用対称キーを用いて、第１ネットワークサーバーは、認証チケットの内容を暗号化する。また、第１ネットワークサーバーは、公開キーを用いて共用対称キーを暗号化する。この公開キーは、第２ネットワークサーバーと関連付けられている。第２ネットワークサーバーは、第２ネットワークサーバーの個人キーを用いて、暗号化された共用キーを解読し、解読された共用キーを用いてチケットの内容を解読する。

【００２１】

また、本発明の観点を具体化するコンピュータにより読み出し可能な記録媒体は、第２ネットワークサーバー及びクライアントコンピュータとともにデータ通信ネットワークに結合されている第１ネットワークサーバーにおいて情報を安全にする認証において、クライアントコンピュータのユーザーに関連付けられた情報を含む（認証）チケットを生成するステップと、第１ネットワークサーバーと第２ネットワークサーバーにより共用されている共用対称キーを用いて、チケットの内容を暗号化するステップと、第２のネットワークサーバーに関連する公開キーを用いて、前記の共用キーを暗号化するステップと、前記のチケットを持っているクライアントコンピュータを第１のネットワークサーバーから第２のネットワークサーバーに向けるステップとからなるプログラムを記録する。

【００２２】

また、この発明は、種々の他の方法や装置を含む。

【００２３】

この発明の他の種々の特徴は、部分的に明らかであるが、一部は、後で指摘される。

【００２４】

【発明の実施の形態】

以下、添付の図面を参照して本発明の実施の形態を説明する。

図１は、本発明が使用されるネットワーク環境の１例を示す。クライアントコンピュータシステム１２は、データ通信ネットワーク１４に結合される。この例では、ネットワーク１４は、インターネット（またはワールド・ワイド・ウェブ）である。しかし、この発明は、他の任意のデータ通信システムに適用できる。多くの認証システム対応サーバー(第２ネットワークサーバー)１６、１８、２０も、ネットワーク１４に結合される。また、クライアントコンピュータシステム１２は、ネットワーク１４を介して認証システム対応サーバー１６、１８、２０にアクセスできる。認証システム対応サーバー１６、１８、２０は、また、「ウェバサーバー」や「ネットワークサーバー」ともいう。ネットワークに結合される認証サーバー(第１ネットワークサーバー)２４は、認証サーバー２４自体、クライアントコンピュータシステム１２及びウェブサーバー１６，１８，２０の間で通信を可能にする。認証システム対応サーバーとは、マルチサイト認証システムに参加しているウェブサーバーであり、認証サーバー２４による認証サービスに対応している。「認証サーバー」というが、この実施の形態での認証サーバー２４は、ウェブブラウザや他のウェブサーバーと相互作用できるウェブサーバーでもある。この例では、データは、情報を交換するためにインターネットで一般に使用されているＨＴＴＰ（ハイパー・テキスト・トランスファー・プロトコル)を用いて、認証サーバー２４、クライアントコンピュータシステム１２及びウェブサーバー１６，１８，２０の間で通信される。

【００２５】

認証データベース２６は、認証サーバー２４と結合される。認証データベース２６は、クライアントコンピュータシステム１２のユーザーを（ネットワークの他のユーザーと同様に）認証するのに必要な情報を含み、また、ユーザーが認証システム対応サーバーにアクセスするとき、ユーザープロファイル情報のどの要素が認証システム対応サーバーに提供されるべきであるかを明らかにする。認証データベース２６は認証サーバー２４とは別に示されているが、発明の他の実施の形態では、認証データベース２６は認証サーバー２４に含まれていてもよい。たとえば、複数の認証サーバー２４が連合する環境では、複数の認証サーバー２４が認証サービスを提供するために使用される（図では、第２の認証サーバー２４は、一部が破線で示されている）。

【００２６】

この発明は、図１に示されるマルチサイトユーザー認証システムのための、改善されたセキュリティを提供する。好ましくは、この発明は、２重キー暗号システムの特徴を用いてセキュリティプロトコルを適用することにより、スケーラブルで複数プラットフォームで動作する認証システムの構築の複雑さを減少する。これは、共用対称キープロトコルに固有の問題を最小にし、すでに使用されているシステム／ソフトウェアの使用を可能にする。これにより、費用を大きく減少し、産業界における広い採用を促進する。

【００２７】

以下に説明する認証プロセスを実行する前に、クライアントコンピュータシステム１２のユーザーと、認証システム対応サーバー１６、１８、２０のオペレータはともに認証サーバー２４で「登録」する。この登録は、認証サーバーに必要な情報を提供するための１回のプロセスである。クライアントコンピュータシステム１２のユーザーは、たとえば、ユーザーの名前、郵便の住所、電子メールアドレス、および／または、ユーザーまたはクライアントコンピュータについての他の情報を提供することにより、認証サーバーで登録する。ユーザー登録処理の一部として、ユーザーは、ログインＩＤを割り当てられ、または、選択する。このログインＩＤは、共通のログインＩＤであり、認証システム対応サーバー（たとえばサーバー１６，１８，２０）にアクセスするために使用される。ログインＩＤは、ここでは、「ユーザー名」、「ログイン名」ともいう。さらに、ユーザーは、認証の目的で使用される、ログインＩＤに関連するパスワードを選択する。認証サーバーで登録しログした後で、ユーザーは、どの認証システム対応サーバー（すなわち、同じ認証サーバーに登録している認証システム対応サーバー）も、追加の認証なしに、関連するユーザープロフィールにすでに含まれているユーザー情報を再入力することなしに、訪ねられる。

【００２８】

認証システム対応サーバー１６，１８，２０の操作者は、その認証システム対応サーバーについての情報（たとえばサーバー名やインターネットアドレス）を提供することにより、認証サーバーに登録する。さらに各認証システム対応サーバー１６，１８，２０は、その認証要求についての情報を提供する。認証のための要求は、ユーザーによる最後のログインから認証情報の提供までに許される最長時間により特定できる。また、この要求は、ユーザーによる認証情報の最後の「リフレッシュ」により特定できる。

【００２９】

認証情報のリフレッシュ（refresh）とは、そのユーザーがなおクライアントコンピュータシステムを操作していることを確認するためユーザーにパスワードを再入力させることをいう。認証サーバーからログアウトせずにユーザーがコンピュータシステムから離れるとき、他の人がそのユーザーのログインＩＤを用いて認証システム対応サーバーにアクセスすることが可能ならば、認証情報の定期的な再入力は有用である。もしユーザーが許可された最長時間がすぎた後で認証システム対応サーバー１６，１８，２０へのアクセスを要求するなら、認証サーバー２４は、そのユーザーを再認証する（すなわちリフレッシュする）。こうして、中心の認証サーバーはあるけれども、認証システム対応サーバー１６，１８，２０は、認証サーバーに強制される認証要求を確立できる。認証サーバー２４に登録した後で、認証システム対応サーバー１６，１８，２０は、認証サーバーにも登録しているユーザーを認証するために、認証サーバーを使用できる。

【００３０】

先に説明したように、共用対称キー・セキュリティプロトコル（たとえばケルベロスプロトコル）は、認証サービスと目的先サービスとの間で認証を行うために使用できる。この場合、認証サービスは、典型的には、ユーザー名／パスワード（またはパスワードに相当するもの）を受け取る。このユーザー名／パスワードの確認のとき、認証サービスは、目的先サービスにチケットを発行する。共用サービスと目的先サービスにのみ知られている共用対称キーがそのチケットを暗号化するので、このチケットは、単独で、ユーザーの身元の目的先サービスを保証する。また、このプロトコルは、そのチケットが、委託されている目的先サービスによってのみ使用可能であることや、そのチケットが、委託されてい

るソース（すなわち認証サービス）からきたことの保証を認証サービスに提供する。さらに、このプロトコルは、認証サービスと目的先サービスの両方に、内容（コンテンツ）が他の誰にも見えないことを保証する。すべてのこれらの保証は、その内容を暗号化し解読する唯一の方法が共用対称キーの知識によるという事実に基づいている。典型的には、すべての目的先サービスがそれ自体のキーを持ち、そのため、認証サービスはすべてのキーを知っているが、各目的先サービスはそれ自体のキーのみを知っている。

【００３１】

当業者に理解されるように、公開キーインフラ構造(ＰＫＩ)は、複数のキーが同期されることを要求する。ＰＫＩは２つのキー(公開キーと個人キー(秘密キーともいう))を持ち、これらの２つのキーは同期された状態でなければならない。そのような一対のキーを呼び出し新しい一対のキーを生成するため、よく確立されたプロトコル／処理がある。この発明は、この１対のキーの認証局とキーの持主にこの問題をゆだね、これにより、共用キー認証システムからキー配布を除く。発明のこの観点が以下により詳細に説明される。

【００３２】

多数の暗号アルゴリズム（たとえば３ＤＥＳやＨＭＡＣ－ＲＣ４）が、暗号化されたものの内容をキーの知識なしに解読することがほとんど不可能なものとして産業界でよく受け入れられている。したがって、キーの保護がセキュリティプロトコルの極端に重要な観点になる。先に説明したように、従来の共用キーシステムでは、認証サービスは、キーを目的先サービスに安全に送らねばならない。また、プロトコルは、キーが盗まれても、その害が最小になるように、キーを定期的に改める手段を取る。残念ながら、これは、マルチサイトユーザー認証システムにおいてセキュリティをはなはだしく複雑にする。さらに、もし目的先サービスが１以上の認証サービスを同じプロトコルで委託することを選ぶなら、共用対称キーは、すべての認証サービスの間で共用されねばならない。このことは、共用対称キーの配布や更新をさらに複雑にする。

【００３３】

発明の１つの実施形態において、ランダムに生成された、使い捨てのセッションキーが共用キーの代わりに用いられる。認証サービス２４は、目的先サービス（すなわち１つの認証システム対応サーバー１６，１８，２０）の公開キーを用いてセッションキーを暗号化する。また、認証サービス２４は、内容を署名するために個人キーを用いる。こうして、この発明は、共用対称キーのセキュリティの性質を保持するが、その欠点は保持しない。この発明のセッションキー・セキュリティプロトコルは、以下のことを保証する。（ａ）認証チケットがその認証システム対応サーバー１６，１８，２０においてのみ使用できること。（ｂ）内容が、正しいソース（すなわち、認証サーバー２４）からくること。（ｃ）チケットの内容が、ソースと目的先（すなわち、認証サーバーと認証システム対応サーバー）によってのみ知られていること。（ｄ）認証システム対応サーバーがその署名を否認できないこと。チケットの内容の知識は、もしチケットが認証情報のみを含み、個人的なユーザーデータを含まないならば、ソースと目的先に限定される必要はない。この場合、内容は、他のどの場所でも使用できず、したがって、保護される必要がない。当業者は、署名アルゴリズムを含む業務はありふれていて、署名アルゴリズムは、署名されるデータの中で、よく知られた、前もって定義された身元確認を行う手段である。発明の１つの実施形態では、これが含まれているか、または、共通のアルゴリズムが認証サーバー２４とサイト２６により仮定される。

【００３４】

理解されるように、認証チケットをＳＳＬ（セキュアソケットレイヤ)または同様な技術を介して送ることは、認証プロトコルに複雑さを加えることなく、ソースと目的先のみがチケットの内容を知っていることを保証する。

【００３５】

発明のこの実施形態のセッションキー・セキュリティプロトコルは、公開キー暗号システムの考え（すなわち委託されている者（サーバー）を同定するためにディジタル証明書を用いる公開キーインフラ構造(ＰＫＩ)）を共用キー環境に適用する。一般に、公開キーシ

ステムは、１つのキーが公開キーであり他方が個人キーである１対のキーすなわち２つのキーの暗号化を使用する。たとえば、公開キーは、１つのメッセージを暗号化し、次に受け取り人の個人キーがメッセージを解読する。公開キーにより暗号化されたデータは、公開キーによって解読できるのみである。さらに、１対の公開キーと個人キーは、１つのキーの知識が他方のキーを明かさないように、異なる値を持つ。したがって、認証サーバー２４は、セキュリティの危険を生じることなく、第３者に公開キーを発行できる。ＰＫＩは、しばしば、ＳＳＬなどのプロトコルにおける証明書と関連して使用される。

【００３６】

好ましくは、この発明は、共用対称キープロトコルの基本的性質を維持する。すなわち、この発明は、チケットの内容や、その内容の関連するすべての解釈を変更しない。一般に、認証サーバー２４がチケットの内容を暗号化しようとするとき、(共用対称キーと同じ暗号強度／長さの）ランダムのセッションキーを生成する。認証サーバー２４は、共用対称キーシステムにおけるのと同一の暗号アルゴリズムを用いて、チケットの内容を暗号化するため、このランダムのセッションキーを用いる。認証サーバー２４は、次に、目的先（すなわち認証システム対応サーバー１６，１８，２０）の公開キーでランダムのセッションキーを暗号化する。

【００３７】

さらに、認証サーバー２４は、その個人キーを使用して、チケット内容のダイジェストメッセージの暗号化の計算（Encrypt（Digest(ticket content)）により署名を作る。

【００３８】

図２は、本発明の具体例を説明するフロー図の１例であり、クライアントコンピュータのユーザーが関連サーバーにアクセスしようとするときのクライアントコンピュータ１２、少なくとも１つの認証システム対応サーバー１６及び認証サーバー２４の間の相互作用を説明する。その考え方が、本発明のマルチサイトユーザー認証システムを利用する認証システム対応サーバー１８，２０や他の任意の対応ウェブサーバーにも適用できるけれども、以下の説明は、単純化するため、認証システム対応サーバー１６に向けられる。

【００３９】

図２に示す例は、クライアントコンピュータシステム１２のユーザーが認証システム対応サーバー１６にまだログしていず、認証サーバー２４によりまだ認証されていない状況を表わす。発明の１実施形態では、複数の認証サーバー２４が連合される環境を提供する。図２において、ラベルＡ～Ｇで表わした線は、認証プロセスにおける情報またはアクティビティの流れを表わす。線における矢印は、処理の流れの方向を示す。ラベルＡは、処理の開始を示し、ラベルＧは処理の終了を示す。図３は、図２の処理の関連するフロー図の１例である。

【００４０】

図２と図３の処理の流れでは、ステップ３２で、クライアントコンピュータシステム１２のユーザーは、認証システム対応サーバー１６を介して利用できるポータルサービス（たとえばhttp://www.msn.comのインターネットサービスのＭＳＮネットワーク）にアクセスすることにより開始する。ステップ３２において、ユーザーは、ポータルを通して利用できる１つのサービスを選択する。たとえば、ユーザーは、１つのリンク（たとえば、http://eshop.msn.com）をクリックすることにより、オンライン・ネットワークサービスや他のウェブサービスにアクセスする(線Ａ参照)。

【００４１】

ステップ３４とステップ３６に進んで、認証システム対応サーバー１６は、サインイン・インタフェース（たとえば、「ログインするためここをクリックしてください。」)をユーザーに提供する。サインインは、オンライン認証サービスに入るときの署名である。ユーザーがサインイン・インタフェースでクリックすると、次に、認証システム対応サーバー１６のポータルサービスは、クライアントコンピュータシステムを、認証サーバー（たとえばマイクロソフト社のパスポート・サインイン・サービス（Passport sign-in service))により提供されるマルチサイトユーザー認証システムにリダイレクトする（redirect

）（線Ｂ参照)。図２と図３の例では、認証システム対応サーバー１６は、クライアントコンピュータシステム１２をlogin.authsite.comにリダイレクトし、クライアントコンピュータシステム１２は、ステップ３６で、ポータルにより発行されるリダイレクトコマンドに従う。

【００４２】

ステップ４０で、認証サーバー２４は、そのユーザーがすでに認証されたことを示す*.authsite.comドメインでの認証クッキーがあるか否かを決定する。もしなければ、ステップ４８で、認証サーバー２４のlogin.authsite.comでのユーザーインタフェースモジュールが、ユーザー名／パスワードを受け取るユーザーインタフェースページに応答する（線Ｃ参照）。ステップ５０で、ユーザーは、ユーザー名／パスワードを入力し、login.passport.comで認証サーバー２４にその情報を通知（post）する（線Ｄ参照)。次に、ステップ５２は、認証サーバー２４は、ユーザーにより提供されるユーザー名／パスワードを確認する(有効にする）（線Ｅ参照)。

【００４３】

もしステップ５２での確認が成功するならば、認証サーバー２４は、希望のウェブサービスの場所を探し、クライアントコンピュータシステム１２を、暗号化されたチケット／プロファイル情報とともに適当なサービス（たとえば、http://eshop.smn.com/)にリダイレクトする（線Ｆ参照)。いいかえれば、認証サーバー２４は、認証データベース２６から適当な場所の情報を検索して、選択されたサービスを提供するサーバー１６（またはサーバー１８，２０）の場所を同定する。発明の１実施形態によれば、セキュリティプロトコルは、チケットのメッセージの内容（たとえばユーザー名とパスパード）を暗号化するため一般的なセッションキーを用いる。次に、認証サーバー２４は、認証システム対応サーバー１６の公開キーを使用してセッションキーを暗号化し、次に、それ自身の個人キーを用いてチケットを署名する。

【００４４】

次にステップ６０で、クライアントコンピュータ１２は、認証システム対応サーバー１６（たとえばhttp://eshop.msn.com）でのウェブサービスへのリダイレクトに従う（線Ｇ参照）。この例では、認証システム対応サーバー１６は、その公開キーと署名とに基づいてチケットの内容を確認する。次に、認証システム対応サーバー１６は、その個人キーを用いてセッションキーを解読し、次に、セッションキーを用いて認証チケットのメッセージ内容を解読する。別の方法では、認証サーバー２４がそのウェブサイトの公開キーを持っていないならば、クライアントコンピュータ１２は、http://eshop.msn.comへのリダイレクトに従って、ＳＳＬ（セキュアソケットレイヤ)の使用を保証する。

【００４５】

ステップ５２に戻って説明すると、もしユーザーが入力した情報が正しくなければ（すなわち、認証データベース２６に格納されている情報と合わなければ）、認証サーバー２４は、ウェブページを生成しユーザーに通信して、ログインＩＤとパスワードの組み合わせが正当でないことを示す。ログインＩＤ、パスワードの誤りの場合、セキュリティの心配のため、たとえば、ユーザーがログインを試みることができる回数を制限してもよい。

【００４６】

この実施形態では、認証サーバー２４は、暗号化されたランダムなキーと署名とを、そのランダムなキーで暗号化されないチケットの一部として追加する。認証サーバー２４は目的先サービス（認証システム対応サーバー１６，１８，２０の１つ）の公開キーでセッションキーを暗号化する。また、認証サーバー２４は、内容を署名するため個人キーを使用する。このように、この発明は、共用対称キーのセキュリティの性質を保持するが、その短所は持っていない。この発明のセッションキー・セキュリティプロトコルは、特定の認証システム対応サーバー１６のみが認証チケットを使用できることを認証サーバー２４に保証する。同様に、この発明は、チケットが正しいソース(すなわち認証サーバー２４)から来たことを目的先サービス（すなわち認証システム対応サーバー１６）に保証する。これは、認証サービスの公開キーで署名を確認することにより達成される。さらに、ソース

と目的先（すなわち、認証サーバーと認証システム対応サーバー）のみがチケットの内容を知っている。

【００４７】

たとえば、チケットｔは、以下の形式を取る。

ｔ＝$Encrypt_{sessionkey}$(ユーザー名 + ...)$PKIEncrypt_{PP3}$(セッションキー)$PKISignature_{PVP}$(全内容)

すなわち、チケットｔは、メッセージの内容（ユーザー名など）のセッションキーによる暗号化データ、セッションキーの公開キーＰＰ３による暗号化データおよびチケットの内容の公開キーＰＶＰによる署名からなる。ここで、ＰＰ３は第３者(認証システム対応サーバー)の公開キーであり、ＰＶＰは認証サーバー２４の公開キーである。

【００４８】

もしチケットが認証情報のみを含み、個人的なユーザー情報を含まないならば、チケットの内容の知識は、ソースと目的先に限定されない。この例では、内容は、他の任意の場所で使用できず、第３者の攻撃者にとってほとんど価値がない。セッションキー・セキュリティプロトコルの１例では、チケットの内容の知識をソースと目的先に限定する必要は、目的先の公開キーの知識を要求しないことにより緩和される。セキュリティチケットは単純に暗号化されない。チケットが異なる目的先により使用可能でないことを保証するため、チケットは、署名の一部として目的先のアドレス(たとえばドメイン名）を含む。こうして、目的先サービスは、署名を使用する前に、それ自体のサイトドメインで署名を確認できる。

【００４９】

たとえば、チケットtは以下の形式をとる。

t={PUID + sign in time + ... + $siteID_3$($siteDomain_3$)}

ここで、ＰＵＩＤは認証サーバー２４により確立される一意の身元識別データ（ID)を示し、sign_in_timeはサインイン時間を示し、siteID(siteDomain)は、サイトドメインsiteDomainのサイトの身元識別データ（ID）を示し、添字の３は第３者を示す。

【００５０】

ＳＳＬ／ＴＬＳなどの改ざんに強くプライバシー保護機能が強化されたプロトコルにより、暗号化されない認証チケットを送信することも、ソース（認証サーバ）と目的先（認証システム対応サーバー）のみがチケットの内容を知ることを保証することが、理解されるべきである。認証サーバー２４は認証システム対応サーバー１６の公開キーを知る必要がないので、発明のこの実施形態は、さらに、キー供給システムを単純にする。

【００５１】

図３のフローは、マイクロソフト社のパスポート・サインイン・サービスなどの認証サービスに関して、セッションキー・セキュリティプロトコルを示す。これがケルベロスプロトコルにも適用可能であることが理解されるべきである。以下に、分散マルチサイトユーザー認証システム（たとえば、マイクロソフト社のパスポート・サインイン・サービス）により利用されケルベロスプロトコルに適用される「パスポート」プロトコルに適用されるセッションキー・セキュリティプロトコルを説明する。

【００５２】

次に、そのようなセッションキー・セキュリティプロトコルの例を説明する。第１の例は、分散マルチサイトユーザー認証システム（たとえばマイクロソフト社のパスポート・サインイン・サービス)により使用されるセッションキー・セキュリティプロトコルである。

【００５３】

パスポートチケット（Ticket）の構造は以下のとおりである。

```
Ticket={
        memberidLow  integer
        memberidHigh integer
        lastRefresh  integer
        lastLogin    integer
        currentTime  integer
}
```

チケットの内容は、身元識別データmemberid、最後のリフレッシュ時間lastRefresh、最後のログイン時間lastLogin、現在の時間currentTimeを含む。

【００５４】

チケットのすべての内容は、共用キーを用いてPassport 2.1にまで暗号化される。

【００５５】

（１）目的先の公開キーの知識なしに、サイトの情報(サイトの身元識別データsiteIDなど）と署名(signature)がチケットの一部に追加できる。

```
Ticket={
        memberidLow  integer
        memberidHigh integer
        lastRefresh  integer
        lastLogin    integer
        currentTime  integer
        siteID       integer
        siteDomain (optional)
        signature
}
```

【００５６】

署名は以下のパスポートの個人キーに基づいている。

Encrypt (Digest (ticket content except signature itself))

これは、署名自体を除くチケットの内容のダイジェストメッセージの暗号化データである。チケットの内容が第３者に見えないことを保証するため、チケットの内容は、ＳＳＬ／ＴＬＳネットワークプロトコルを通してのみ転送される。メンバーＩＤ（memberid）が保護されるべき重大な価値がないと認証サービスが決定する場合には、ＳＳＬ／ＴＬＳは要求されない。

【００５７】

最新のウェブの標準に従うため、この実施形態におけるパスポートの実行サービスは、チケット構造をｘｍｌ文書フォーマットに変更する。

【００５８】

（２）目的先の公開キーの知識を用いて、チケットは以下のように暗号化される。

```
Ticket={
            EncryptedContent{
            memberidLow  integer
                  memberidHigh integer
            lastRefresh  integer
                  lastLogin    integer
            currentTime  integer
            }
            EncryptedSessionKey
            Signature
}
```

ここで、EncryptedSessionKeyは、目的先の公開キーを用いて暗号化されたランダムのセッションキーであり、Signatureは、パスポートの個人キーを用いて暗号化された、署名以外のチケットのダイジェストメッセージであり、EncryptedContentは、セッションキーを通している。

【００５９】

第２の例は、ケルベロスプロトコルに適用されるセッションキー・セキリティプロトコルである。

ケルベロスサービスチケットの構造は以下のとおりである。

```
Ticket ::= [APPLICATION1]SEQUENCE{
            tkt-vno[0]      INTEGER,
            realm[1]        Realm,
            sname[2]        PrincipalName,
            enc-part[3]     EncryptedData, --EncTicketPart
            extensions[4]   TicketExtensions OPTIONAL
}
```

【００６０】

いまEncryptedDataは共用キーを用いて暗号化されている。１つの実施形態では、チケットの１つの拡張データextensionはチケットキーを運ぶために追加され、このチケットキーは、EncryptedDataを暗号化するために使用される。PKI-Ticket-Extensionは、対象(sname)の公開キーにより暗号化されるチケットキーを含む。チケットキーが、委託されているキー配布センターからくることを証明するため、PKI-Ticket-ExtensionPKI-Ticketは、また、キー配布センターによるEncryptedDataの署名を含む。

【００６１】

```
PKI-Ticket-Extension:{
        te-type[0]      INTEGER
        te-TicketKey[1]
        te-Signature[2]
}
```

ここで、te-TicketKeyは対象(sname)の公開キーにより暗号化されたチケットキーすなわちEncrypt（TicketKey)であり、te-Signatureは、キー配布センターの個人キーにより暗号化されたデータEncryptedDataのダイジェストメッセージの署名すなわちEncrypt(Digest(EncryptedData))である。

【００６２】

図４は、コンピュータ７０の形での一般目的のコンピュータ装置の１例を示す。発明の１つの実施形態では、コンピュータ７０などのコンピュータは、クライアントコンピュータシステム１２、認証サーバー２４、ユーザーインタフェースサーバー２８、または他の認証システム対応サーバー１６，１８，２０での使用に適している。

【００６３】

この実施形態において、コンピュータ７０は、１以上のプロセッサまたはプロセシングユニット（ＣＰＵなど）７２とシステムメモリ７４を持つ。また、システムバス７６は、システムメモリ７４を含む種々の部品をプロセッサ７２に接続する。バス７６は、メモリバスまたはメモリコントローラ、ペリフェラルバス、ＡＧＰ（accelerated graphics port）、種々のバスアーキテクチャを用いるプロセッサバスまたはローカルバスを含むバス構造の中の１以上のいずれかの種類のバス構造を表わす。バス構造の例として、ＩＳＡ（Industry Standard Architecture)バス、ＭＣＡ（Micro Channel Architecture)バス、ＥＩＳＡ（Enhanced ISA)バス、ＶＥＳＡ（Video Electronics Standards Association)ローカルバス、メザニンバスとしても知られるＰＣＩ(Peripheral Component Interconnect)バスが挙げられるが、これらには限定されない。

【００６４】

コンピュータ７０は、典型的には、少なくとも、コンピュータにより読み出し可能な記録媒体を備える。コンピュータにより読み出し可能な記録媒体は、揮発性と不揮発性の媒体や取り外し可能な媒体と取り外し不可能な媒体を含み、コンピュータ７０によりアクセスできる利用可能な媒体である。コンピュータにより読み出し可能な媒体の例は、コンピュータ記憶媒体と通信媒体であるが、これに限定されない。コンピュータ記憶媒体は、コンピュータにより読み出し可能な命令、データ構造、プログラムモジュールまたは他のデータなどの情報の格納のための任意の方法または技術において実現される、揮発性媒体や不揮発性媒体と、取り外し可能な媒体と取り外し不可能な媒体を含む。たとえば、コンピュータ格納媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤ（ディジタルバーサタイルディスク）または他の光記録媒体、磁気カセット、磁気テープ、磁気ディスク記録媒体または他の磁気記録媒体、または、所望の情報を格納しコンピュータ７０によるアクセスできる他の任意の媒体を含む。通信媒体は、典型的には、搬送波または他の送信メカニズムなどの変調されたデータ信号の形として表わされている、コンピュータにより読み出し可能な命令、データ構造、プログラムモジュールまたは他のデータなどの情報であり、任意の情報伝達媒体を含む。当業者は、この変調されたデータ信号をよく知っており、このデータ信号は、信号中の情報を符号化するように設定されまたは変更された１以上の特性を備える。有線ネットワークまたは直接配線（direct-wired）ネットワークなどの有線媒体と、音響媒体、ＲＦ媒体、赤外媒体、他の無線媒体などの無線媒体は、通信媒体の例である。また、以上のものの組み合わせも、コンピュータにより読み出し可能な媒体の例である。

【００６５】

システムメモリ７４は、揮発性媒体や不揮発性媒体と、取り外し可能な媒体と取り外し不可能な媒体の形態のコンピュータ記録媒体を含む。図示された例では、システムメモリ７４は、ＲＯＭ７８とＲＡＭ８０を含む。ＢＩＯＳ (basic input/output system)は、たとえば立ち上げの際のコンピュータ７０内の要素の間の情報伝達に役立つ基本的なルーチンを含み、典型的にはＲＯＭ７８に記憶される。ＲＡＭ８０は、典型的には、プロセッシングユニット７２により直ちにアクセス可能であり、および／または、現在動作されているデータおよび／またはプログラムのモジュールを含む。１例では、図４は、ＯＳ（オペレーティングシステム）８４、アプリケーションプログラム８６、他のプログラムモジュール８８およびプログラムデータ９０を含むが、これに限定されない。

【００６６】

コンピュータ７０は、また、取り外し可能／取り外し不可能の揮発性／不揮発性のコンピュータ記録媒体を含んでいてもよい。たとえば、図４は、取り外し可能な不揮発性磁気媒体に読み書きするハードディスクドライブ９４を示す。また、図４は、取り外し可能な不揮発性磁気ディスク９８に読み書きする磁気ディスクドライブ９６と、ＣＤ－ＲＯＭまたは他の光媒体などの取り外し可能な光ディスク１０２に読み書きする光ディスクドライブ１００を示す。この動作環境において使用可能な他の取り外し可能／取り外し不可能の揮発性／不揮発性のコンピュータ記録媒体の例は、磁気テープカセット、フラッシュメモリカード、ＤＶＤ、ディジタルビデオテープ、固体ＲＡＭ、固体ＲＯＭなどであるが、これに限定されない。ハードディスクドライブ８４、磁気ディスクドライブ９６および光ディスクドライブ１００は、典型的には、インタフェース１０６などの不揮発性メモリインタフェースによりシステムバス７６に接続されている。

【００６７】

上に説明されず４２に示されているドライブまたは他の大量記憶装置とそれに関連するコンピュータ記録媒体は、コンピュータ７０のため、コンピュータにより読み出し可能な命令、データ構造、プログラムモジュールおよび他のデータを記憶する。図４において、たとえば、ハードディスクドライブ９４は、オペレーティングシステム１１０、アプリケーションプログラム１１２、他のプログラムモジュール１１４およびプログラムデータ１１６を記憶するものとして示されている。なお、これらの部分は、オペレーティングシステム８４、アプリケーションプログラム８６、他のプログラムモジュール８８およびプログラムデータ９０と同じであっても異なっていてもよい。オペレーティングシステム１１０、アプリケーションプログラム１１２、他のプログラムモジュール１１４およびプログラムデータ１１６は、ここでは、異なる参照数字で示されていて、少なくともそれらが異なる複製であることを示している。

【００６８】

ユーザーは、キーボード１２０、（たとえばマウス、トラックボール、ペン、タッチパッドなどの）ポインティングデバイス１２２などの入力装置によりコンピュータ７０に命令と情報を入力できる。他の入力装置(図示しない）は、マイクロフォン、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナなどを含む。これらや他の入力装置は、システムバス７６に接続されるユーザー入力インタフェース１２４を介してプロセッシングユニット７２に接続されるが、しかし、パラレルポート、ゲームポート、またはＵＳＢなどの他のインターフェース構造やバス構造に接続できる。モニター１２８または他の種類の表示装置は、ビデオインタフェース１３０などのインタフェースを介してシステムバス７６に接続される。モニター１２８に加え、コンピュータは、しばしば、出力周辺インタフェース(図示しない）に接続できるプリンタ、スピーカーなどの他の周辺出力装置(図示しない）を含む。

【００６９】

コンピュータ７０は、リモートコンピュータ１３４などの１以上のリモートコンピュータへの論理接続を用いるネットワーク環境において動作できる。このリモートコンピュータ１３４は、たとえば、パーソナルコンピュータ、サーバー、ルーター、ネットワークＰＣ、ピア装置または他の共通のネットワークノードであり、典型的には、コンピュータ７

０について先に説明した要素の多くまたはすべてを含む。図４に示される論理接続は、ＬＡＮ（ローカルエリアネットワーク）１３６とＷＡＮ（ワイドエリアネットワーク）１３８を含むが、また、他のネットワークを含んでいてもよい。そのようなネットワーク環境は、事務所、企業に広がるコンピュータネットワーク、イントラネット、グローバルコンピュータネットワーク(たとえばインターネット)においてありふれている。

【００７０】

ローカルエリアネットワーク環境において使用されるとき、コンピュータ７０は、ネットワークインタフェースまたはアダプタ１４０を介してＬＡＮ１３６に接続される。ワイドエリアネットワークで使用されるとき、コンピュータ７０は、典型的には、インターネットなどのＷＡＮ１３８での通信を確立するモデム１４２または他の手段を含む。モデム１４２は、内蔵モデムや外付けモデムのユーザー入力インタフェース１３４または他の適当なメカニズムを介してシステムバス７６に接続される。ネットワーク環境では、コンピュータ７０に関して説明されたプログラムモジュールまたはその一部が、リモート記憶装置(図示しない）に記憶できる。たとえば、図４は、メモリ装置に常駐するリモートアプリケーションプログラム１４４を示す。図示されるネットワーク接続は１例であり、コンピュータの間に通信リンクを確立する他の手段も使用できる。

【００７１】

一般的に、コンピュータ７０のデータプロセッサは、コンピュータにより読み出し可能なコンピュータの種々の記録媒体において異なる時間に格納される命令によりプログラムされる。プログラムとオペレーティングシステムは、典型的には、たとえば、フレキシブルディスクやＣＤ－ＲＯＭで配布される。それからコンピュータの２次的メモリにインストールされ、または、ロードされる。実行時には、それらは、コンピュータの１次メモリに少なくとも部分的にロードされる。ここで説明する発明は、これらおよび他の種々の種類のコンピュータに読み出し可能な記録媒体を含み、そこに、マイクロプロセッサまたは他のデータプロセッサとともに後で説明されるステップを実行する命令またはプログラムを含む。また、この発明は、以下に説明する方法と技術によりプログラムされるときのコンピュータ自体を含む。

【００７２】

図に示すため、オペレーティングシステムなどの、プログラムと他の実行可能なプログラム部分は、ここでは別々のブロックで示される。そのようなプログラムやプログラム部分は、コンピュータの異なる記憶部品に異なる時間に存在し、コンピュータのデータプロセッサにより実行される。

【００７３】

この発明は、コンピュータ７０を含むコンピュータシステム環境において説明されたが、多数の一般目的または特定目的のコンピュータシステムの環境または構成において動作する。コンピュータシステム環境は、発明の用途や機能の範囲について制限を与えるものではない。さらに、コンピュータシステム環境は、例として示された動作環境において説明された部分または複数の部分の組み合わせに関連した依存性や要求を持つものとして解釈されてはならない。周知のコンピュータシステム環境／構成の例は、これらに限定されないが、パーソナルコンピュータ、携帯またはラップトップ装置、マルチプロセッサシステム、マイクロプロセッサを用いたシステム、セットトップボックス、プログラマブル家電機器、ネットワークＰＣ、ミニコン、メインフレームコンピュータ、および、上述のいずれかのシステム、装置などを含む分散コンピュータ環境である。

【００７４】

この発明は、１以上のコンピュータまたは他の装置により実行される、プログラムモジュールなどの、コンピュータによる実行される命令の一般的な文脈で説明できる。一般的には、プログラムモジュールは、これらには限定されないが、タスクを行いまたは抽象データタイプを実現するルーチン、プログラム、オブジェクト、コンポーネント(component)およびデータ構造を含む。また、この発明は、通信ネットワークを通してリンクされているリモートプロセッシング装置によりタスクが行われる分散コンピュータ環境において

具体化できる。分散コンピュータ環境では、プログラムモジュールは、メモリ格納装置を含むローカルおよびリモートのコンピュータ格納媒体の中に位置される。

【００７５】

本発明は、２キーシステムに基づくセッションキー・セキュリティプロトコルを用いる共用対称キープロトコルに固有の問題を本質的に除去する。好ましくは、セッションキープロトコルは、すでに存在する対象のシステム／ソフトウェアを用いて経済的に使用することを可能にする。また、このプロトコルは、産業により広く採用されることを促進する。

【００７６】

さらに、本発明は、プロトコルのいずれかの端でキーが傷つけられるという危険を除く点で強いプロトコルを提供する。たとえば、認証サービスに人が侵入するとすべての認証システム対応サーバーの全キーが盗まれた可能性がある。これは、認証システム対応サーバーの全ネットワークにわたってすべてのキーを再設定するために必要な期間のため、認証サービスの停止を生じる。対照的に、この発明のセキュリティプロトコルは、認証システム対応サーバーを混乱させることなく認証サービスが急速に盗まれたキーを置き換えることを可能にする。同様に、もし目的先のサービスで個人キーが盗まれると、その目的先のサービスは、認証サービスが新しいキーを発行するのを待つよりは、それ自体の個人キーと公開キーを再設定するサービスを独立に開始できる。さらに、本発明は、セキュリティの危険を分離するため、目的先のサービスが多数の個人／公開キーの対（たとえば、認証サービスが委託する認証サービス当り１個の対）を持つことを可能にする。

【００７７】

以上に説明したことからわかるように、本発明の目的が達成され、好ましい結果が得られている。

【００７８】

なお、上述の構成と方法は本発明の範囲から離れることなしに種々に変更できるので、発明の詳細な説明と図面に記載された内容は例として解釈されるべきであり、限定するものとして解釈されるべきではない。

【図面の簡単な説明】

【図１】　本発明が使用されるネットワーク環境の１例のブロック図

【図２】　クライアントコンピュータのユーザーが関連サーバーにアクセスしようとするときの、図１のクライアントコンピュータ、関連サーバー及び認証サーバーの間の相互作用を説明する１例のフローチャート

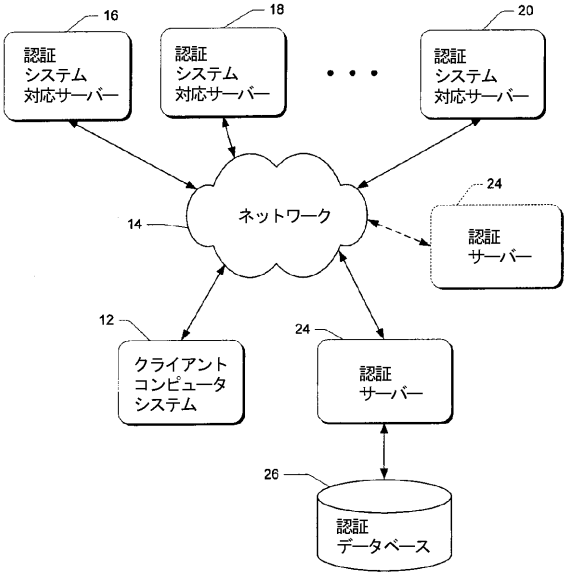
【図３】　クライアントコンピュータのユーザーが関連サーバーにアクセスしようとするときの、図１のクライアントコンピュータ、関連サーバー及び認証サーバーの間の相互作用を説明する１例のフローチャート

【図４】　図１のシステムに使用されるコンピュータの部分を示すブロック図

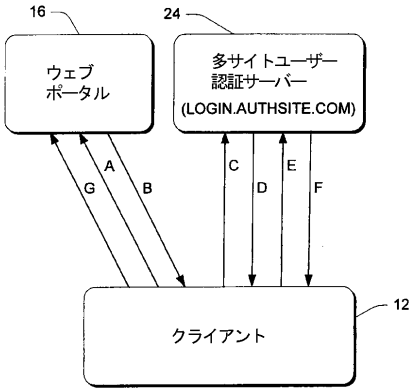
【符号の説明】

１２　クライアントコンピュータシステム、　１４　ネットワーク、　１６、１８、２０　認証システム対応サーバー、　２４　認証サーバー、　２６　認証データベース、　７０　コンピュータ、　７２　プロセッサまたはプロセシングユニット、　９０　プログラムデータ、　９４　ハードディスクドライブ、　９８　不揮発性磁気ディスク、　１０２　光ディスク。

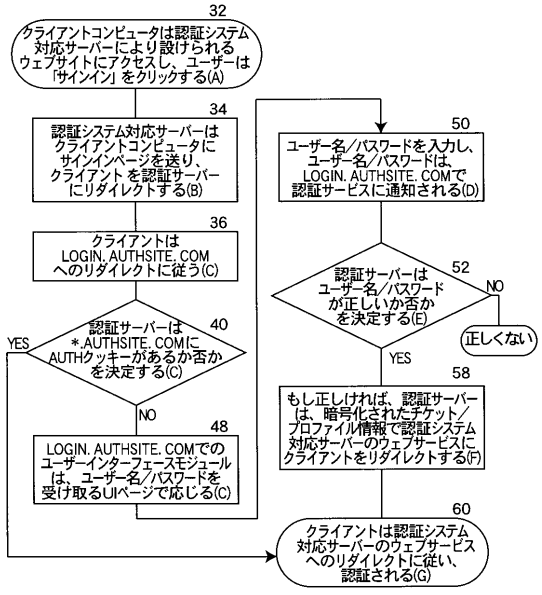
【図１】


16
認証
システム
対応サーバー
18
認証
システム
対応サーバー
20
認証
システム
対応サーバー
14
ネットワーク
24
認証
サーバー
12
クライアント
コンピュータ
システム
24
認証
サーバー
26
認証
データベース

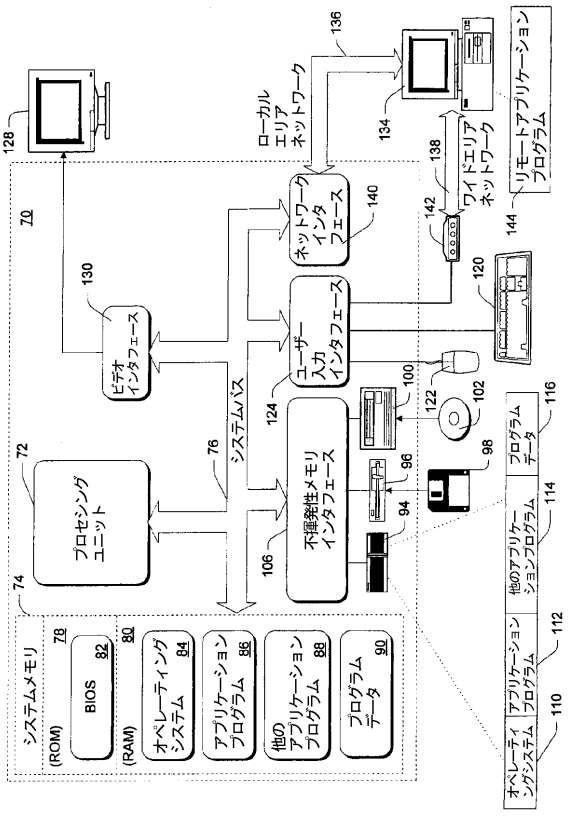
【図２】


16
ウェブ
ポータル
24
多サイトユーザー
認証サーバー
(LOGIN.AUTHSITE.COM)
A
B
C
D
E
F
G
12
クライアント

【図３】


32
クライアントコンピュータは認証システム対応サーバーにより設けられるウェブサイトにアクセスし、ユーザーは「サインイン」をクリックする(A)
34
認証システム対応サーバーはクライアントコンピュータにサインインページを送り、クライアントを認証サーバーにリダイレクトする(B)
36
クライアントはLOGIN.AUTHSITE.COMへのリダイレクトに従う(C)
40
認証サーバーは*.AUTHSITE.COMにAUTHクッキーがあるか否かを決定する(C)
YES
NO
48
LOGIN.AUTHSITE.COMでのユーザーインターフェースモジュールは、ユーザー名/パスワードを受け取るUIページで応じる(C)
50
ユーザー名/パスワードを入力し、ユーザー名/パスワードは、LOGIN.AUTHSITE.COMで認証サービスに通知される(D)
52
認証サーバーはユーザー名/パスワードが正しいか否かを決定する(E)
NO
正しくない
YES
58
もし正しければ、認証サーバーは、暗号化されたチケット/プロファイル情報で認証システム対応サーバーのウェブサービスにクライアントをリダイレクトする(F)
60
クライアントは認証システム対応サーバーのウェブサービスへのリダイレクトに従い、認証される(G)

【図４】


128
136
ローカル
エリア
ネットワーク
134
138
ワイドエリア
ネットワーク
144
リモートアプリケーション
プログラム
70
ネットワーク
インタ
フェース
140
142
130
ビデオ
インタフェース
120
ユーザー
入力
インタフェース
100
122
102
124
システムバス
76
不揮発性メモリ
インタフェース
96
98
94
106
72
プロセシング
ユニット
74
システムメモリ
78
(ROM)
BIOS
82
80
(RAM)
オペレーティング
システム
84
アプリケーション
プログラム
86
他の
アプリケーション
プログラム
88
プログラム
データ
90
プログラム
データ
116
他のアプリケー
ションプログラム
114
アプリケーション
プログラム
112
オペレーティ
ングシステム
110

フロントページの続き

(72)発明者 ウェイーキアン・エム・グオ
アメリカ合衆国９８００６ワシントン州ベルビュー、１３３アベニュー・サウスイースト４６１６番
(72)発明者 ジョン・エイチ・ハワード
アメリカ合衆国９８０７４ワシントン州サマミッシュ、ノースイースト・１８ストリート２５０２５番
(72)発明者 クォック・ダブリュー・チャン
アメリカ合衆国９８００７ワシントン州ベルビュー、ノースイースト・５７ストリート１４５５２番

審査官 青木 重徳

(56)参考文献 特開２００１－２０２４３７（ＪＰ，Ａ）
特開２００２－１３２７３０（ＪＰ，Ａ）
特開２００１－１７７５１３（ＪＰ，Ａ）
特開２００２－０３２３４４（ＪＰ，Ａ）
特開２００２－０７３８５９（ＪＰ，Ａ）
一松信，“データ保護と暗号化の研究”，日本，日本経済新聞社，１９８３年 7月２９日，１版１刷，ｐ．５９－６５，コンピュータ・ネットワークの安全性
Larry J. Hughes, Jr. 著／長原宏治 監訳，“インターネット・エキサイティングテクノロジーシリーズ インターネットセキュリティ”，日本，株式会社インプレス，１９９７年 2月２１日，初版，ｐ．９４－１０２，システム管理者のためのリスクマネージメント

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32
G06F 21/20
H04L 9/08