(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4886508号
(P4886508)
(45)発行日　平成24年2月29日(2012.2.29)　(24)登録日　平成23年12月16日(2011.12.16)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B

請求項の数 2 (全 17 頁)

(21)出願番号	特願2006-519925 (P2006-519925)	(73)特許権者	390009531
(86)(22)出願日	平成16年7月9日 (2004.7.9)		インターナショナル・ビジネス・マシーンズ・コーポレーション
(65)公表番号	特表2009-514262 (P2009-514262A)		INTERNATIONAL BUSINESS MASCHINES CORPORATION
(43)公表日	平成21年4月2日 (2009.4.2)		アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(86)国際出願番号	PCT/EP2004/051435	(74)代理人	100108501
(87)国際公開番号	WO2005/015872		弁理士　上野　剛史
(87)国際公開日	平成17年2月17日 (2005.2.17)	(74)代理人	100112690
審査請求日	平成19年7月4日 (2007.7.4)		弁理士　太佐　種一
審判番号	不服2010-2571 (P2010-2571/J1)	(74)代理人	100091568
審判請求日	平成22年2月5日 (2010.2.5)		弁理士　市位　嘉宏
(31)優先権主張番号	10/621,927		
(32)優先日	平成15年7月17日 (2003.7.17)		
(33)優先権主張国	米国(US)		

早期審査対象出願

最終頁に続く

(54)【発明の名称】既存のＳＳＬセッションを中断することなく証明書ベースの認証にステップアップするための方法及びシステム

(57)【特許請求の範囲】

【請求項１】

認証操作を実行するための方法であって、

クライアント装置からの第１のリソース要求をサーバで受信するステップと、

前記第１のリソース要求に応答する前に前記第１のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアント装置との間にＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）セッションを確立するステップと、

前記ＳＳＬセッションを介して前記サーバと前記クライアント装置との間で前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアント装置に第１のリソース応答を送信するステップと、

前記クライアント装置からの第２のリソース要求を、前記ＳＳＬセッションを介して前記サーバで受信するステップと、

前記第２のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記ＳＳＬセッションを介して前記サーバによって前記クライアント装置において実行可能モジュールの実行を開始させるステップと、

前記クライアント装置においてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記ＳＳＬセッションを介して前記サーバで受信するステップと、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記

サーバから前記クライアント装置に第２のリソース応答を送信するステップと、
を含む方法。
【請求項２】
認証操作を実行するための方法であって、
クライアント装置からの第１のリソース要求をサーバで受信するステップと、
前記第１のリソース要求に応答する前に前記第１のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアント装置との間にＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）セッションを確立するステップと、
前記ＳＳＬセッションを介して非証明書ベースの認証操作を実行するステップと、
前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアント装置に第１のリソース応答を送信するステップと、
前記非証明書ベースの認証操作を実行した後で、前記クライアント装置からの第２のリソース要求を、前記ＳＳＬセッションを介して前記サーバで受信するステップと、
前記第２のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記ＳＳＬセッションを介して前記サーバから前記クライアント装置に実行可能モジュールをダウンロードするステップと、
前記クライアント装置においてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記ＳＳＬセッションを介して前記サーバで受信するステップと、
前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアント装置に第２のリソース応答を送信するステップと、
を含む方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、改良されたデータ処理システムに関し、具体的には、マルチコンピュータ・データ転送のための方法及び装置に関する。さらにより具体的には、本発明は、暗号を用いるマルチコンピュータ通信のための方法及び装置を提供する。
【背景技術】
【０００２】
ｅコマース・ウェブ・サイト及びウェブ・アプリケーションは、ユーザに代わって、コンピュータ・ネットワーク上で取引を実行する。ユーザは、多くの場合、セキュリティの目的で、適切なレベルまで自分の身元を確実に証明するために、認証手続きを通過しなければならない。
【０００３】
多くのコンピュータ・システムは、異なるセキュリティのレベルに合わせて異なるタイプの認証を有する。例えば、正しいユーザ名とパスワードとの組み合わせがユーザによって与えられる第１レベルの認証の完了に成功した後で、システムは、ウェブ・サイト上のリソースの特定の組へのアクセスを提供することができる。第２レベルの認証が、例えばスマートカードのようなハードウェア・トークンを提示することをユーザに対して求める場合があり、その後そのユーザには、より厳しく管理されたウェブ・サイト上のリソースへのアクセスが提供される。第３レベルの認証が、例えば指紋走査又は虹彩走査を通じて何らかの形式のバイオメトリック・データを提供することをユーザに対して求める場合があり、その後そのシステムは、ウェブ・サイト上の極めて重要なリソースまたは機密リソースへのアクセスを提供する。
【０００４】
ある認証レベルから次のレベルに移行する処理は、「ステップアップ認証」と呼ばれる。すなわち、ユーザは、より重要なリソースへのアクセスを得るために、システムの要求に応じて、あるレベルの認証から上位レベルにステップアップする。

【０００５】
ｅコマース・ウェブ・ベースの環境においては、コンピュータ・システムは、ウェブ・サイトにアクセスするための正面玄関すなわち監視ゲート（ｓｅｎｔｒｙ　ｇａｔｅ）として、認証サービスを実装することが多い。これらの認証サービスは、ユーザがいずれかのリソースにアクセスする前に認証されることを確実にするように、アプリケーションの前、すなわちユーザとアプリケーションとの間に位置する。これらの認証サービスは、ウェブ・サーバ・プラグイン、リバース・プロキシ、又は他の同様な技術として実装することができる。これらの認証サービスに伴う潜在的な問題は、これらの認証サービスはユーザ名／パスワード認証を用いることが多く、クライアント・ベースの証明書を用いる認証方法にステップアップすることができないという点である。証明書ベースの認証手続きは、一般に、ユーザ名／パスワードベースの認証手続きより上位レベルのセキュリティを達成すると考えられている。

【０００６】
証明書ベースの認証は、公開鍵／秘密鍵からなる非対称暗号鍵対の使用を含むものである、デジタル証明書は、認証されたユーザの識別情報を公開暗号鍵と結びつける。証明書ベースの認証手続きの際、ユーザは、自分自身のデジタル証明書を認証サービスに提供し、自らが公開鍵に対応する秘密暗号鍵にアクセスできることを証明する必要がある。例えば、認証サービスは、何らかの形式のチャレンジ・データをユーザのクライアント・コンピュータに与え、次いでユーザのクライアント・コンピュータは、ユーザの秘密暗号鍵を用いてチャレンジ・データに署名し、認証サービスは、ユーザの公開鍵を用いてデジタル署名を検証することができる。秘密鍵は、識別情報が証明書に格納されたユーザによって常に秘密に保たれているはずであるため、認証サービスが、チャレンジ・データがユーザの秘密鍵を用いて適切に署名されたと判断したときは、該認証サービスは、ユーザの識別情報を高いレベルまで検証したことになる。

【発明の開示】
【発明が解決しようとする課題】
【０００７】
証明書ベースの認証手続きにステップアップする操作は、不可能であることが多い。問題は、典型的には、相互認証されたＳＳＬセッションが、ユーザ名／パスワードの組み合わせといった下位レベルの非証明書ベースの認証についてクライアントとサーバとの間にすでに確立されていることから生じる。ほとんどの市販製品の場合、例えばＳＳＬスタックが何らかの方法でオペレーティング・システムに組み込まれている場合など、証明書ベースの認証手続きを必要とする認証サービスがＳＳＬスタックを制御しない場合には、該認証サービスは、新たなＳＳＬセッションを強制的に確立することができない。したがって、認証サービスは、アクティブなＳＳＬセッション上ですでに行われたユーザ名／パスワードをベースとする認証手続きから、そのアクティブなＳＳＬセッションを維持したまま証明書ベースの認証手続きにステップアップすることができない。

【０００８】
したがって、何らかの目的で認証サービスによって要求される上位レベルのセキュリティを獲得するために、以前に確立されたＳＳＬセッションを終了又は再折衝することなく、非証明書ベースの認証手続きから証明書ベースの認証手続きにステップアップすることが可能な方法及びシステムを有することは有益であろう。

【課題を解決するための手段】
【０００９】
本発明の第１の態様によれば、認証操作を実行するための方法であって、サーバとクライアントとの間のＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）セッションを介して非証明書ベースの認証操作を実行するステップと、該記非証明書ベースの認証操作を実行した後で、該ＳＳＬセッションを介して該サーバから該クライアントに実行可能モジュールをダウンロードするステップと、該クライアントにおいてデジタル証明書を用いて該実行可能モジュールによって生成されたデジタル署名を該サーバで受信するステップと

、証明書ベースの認証操作を、該証明書ベースの認証操作の完了前に該ＳＳＬセッションを終了又は再折衝することなく、該サーバと該クライアントとの間の該ＳＳＬセッションを介して実行するステップと、を含む方法が提供される。

【発明を実施するための最良の形態】

【００１０】

本発明の特性と考えられる新規な特徴は、特許請求の範囲に記載される。発明自体、更なる目的、及びその利点は、添付の図面を参照して読んだ時に、以下の詳細な説明を参照することによって最も良く理解されるであろう。

【００１１】

一般に、本発明が備えるか又は本発明に関連する装置は、様々なデータ処理技術を含む。したがって、本発明をより詳細に説明する前に、背景技術として、分散データ処理システム内のハードウェア・コンポーネント及びソフトウェア・コンポーネントの典型的な構成を説明する。

【００１２】

ここで図を参照すると、図１は、各々が本発明の一部を実装することができるデータ処理システムの典型的なネットワークを示す。分散データ処理システム１００はネットワーク１０１を含み、ネットワーク１０１は、分散データ処理システム１００内で相互に接続された種々の装置及びコンピュータ間に通信リンクを提供するために用いることができる媒体である。ネットワーク１０１は、電線又は光ファイバ・ケーブルなどの永久的な接続、又は、電話回線若しくは無線通信を通じて形成される一時的な接続を含むことができる。図示された例においては、サーバ１０２及びサーバ１０３は、ストレージ・ユニット１０４と共にネットワーク１０１に接続される。さらに、クライアント１０５～１０７もまた、ネットワーク１０１に接続される。クライアント１０５～１０７及びサーバ１０２～１０３は、メインフレーム、パーソナル・コンピュータ、携帯情報端末（ＰＤＡ）などといった種々のコンピューティング装置によって表すことができる。分散データ処理システム１００は、図示されていない付加的なサーバ、クライアント、ルータ、他の装置、及びピアツーピア・アーキテクチャを含むことができる。

【００１３】

図示された例においては、分散データ処理システム１００は、Ｌｉｇｈｔｗｅｉｇｈｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ（ＬＤＡＰ）、Ｔｒａｎｐｏｒｔ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ（ＴＣＰ／ＩＰ）、Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ（ＨＴＴＰ）、Ｗｉｒｅｌｅｓｓ Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｔｏｃａｌ（ＷＡＰ）などといった、相互に通信するための種々のプロトコルを用いるネットワーク及びゲートウェイの世界規模の集合体を表すネットワーク１０１を有するインターネットを含むことができる。当然のことながら、分散データ処理システム１００は、例えば、イントラネット、ローカル・エリア・ネットワーク（ＬＡＮ）、又は広域エリア・ネットワーク（ＷＡＮ）などの、多くの異なるタイプのネットワークを含むこともできる。例えば、サーバ１０２は、クライアント１０９と、無線通信リンクを組み込んだネットワーク１１０とを直接サポートする。ネットワーク対応電話１１１は、無線リンク１１２を介してネットワーク１１０に接続し、ＰＤＡ１１３は、無線リンク１１４を介してネットワーク１１０に接続する。電話１１１及びＰＤＡ１１３はまた、Ｂｌｕｅｔｏｏｔｈ（商標）無線技術などの適切な技術を用いる無線リンク１１５を介して互いの間で直接データを転送し、いわゆるパーソナル・エリア・ネットワーク（ＰＡＮ）又はパーソナル・アドホック・ネットワークを形成することができる。同様の方法で、ＰＤＡ１１３は、無線通信リンク１１６を介してＰＤＡ１０７にデータを転送することができる。

【００１４】

本発明は、種々のハードウェア・プラットフォーム上に実装することができる、すなわち、図１は、異種コンピューティング環境の一例であり、本発明についてのアーキテクチャ上の制限として意図するものではない。

【００１５】
ここで図２を参照すると、図は、図１において示されるシステムのような、本発明を実装することができるデータ処理システムの典型的なコンピュータ・アーキテクチャを示す。データ処理システム１２０は、内部システム・バス１２３に接続された１つ又は複数の中央演算処理装置（ＣＰＵ）１２２を含み、内部システム・バス１２３は、ランダム・アクセス・メモリ（ＲＡＭ）１２４と、読み取り専用メモリ１２６と、プリンタ１３０、ディスク・ユニット１３２、又は音声出力システムなどのような図示されない他の装置といった種々のＩ／Ｏ装置をサポートする入力／出力アダプタ１２８とを、相互接続する。システム・バス１２３はまた、通信リンク１３６へのアクセスを提供する通信アダプタ１３４を接続する。ユーザ・インターフェース・アダプタ１４８は、キーボード１４０及びマウス１４２、又はタッチ・スクリーン、スタイラス、マイクロフォンなどのような図示されない他の装置といった種々のユーザ装置を接続する。ディスプレイ・アダプタ１４４は、システム・バス１２３をディスプレス装置１４６に接続する。
【００１６】
当業者であれば、図２のハードウェアは、システム実装に応じて変えることができることが分かるであろう。例えば、システムは、Ｉｎｔｅｌ（商標）Ｐｅｎｔｉｕｍ（商標）ベースのプロセッサ及びデジタル信号プロセッサ（ＤＳＰ）などの１つ又は複数のプロセッサと、１つ又は複数のタイプの揮発性メモリ及び不揮発性メモリとを有するものとすることができる。図２に示されるハードウェアに加えて、又はこれに代えて、他の周辺装置を用いることができる。図示された例は、本発明に関してアーキテクチャ上の制限を意味することを意図するものではない。
【００１７】
本発明は、種々のハードウェア・プラットフォーム上に実装することができることに加えて、種々のソフトウェア環境において実装することができる。典型的なオペレーティング・システムを用いて、各々のデータ処理システム内のプログラム実行を制御することができる。例えば、１つのデバイスがＵｎｉｘ（商標）オペレーティング・システムを動作させることができる一方で、別のデバイスは、単純なＪａｖａ（商標）ランタイム環境を含む。代表的なコンピュータ・プラットフォームは、画像ファイル、ワード・プロセッシング・ファイル、Ｅｘｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＸＭＬ）、Ｈｙｐｅｒｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＨＴＭＬ）、Ｈａｎｄｈｅｌｄ Ｄｅｖｉｃｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＨＤＭＬ）、Ｗｉｒｅｌｅｓｓ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＷＭＬ）などの様々なフォーマット、並びに、他の様々なフォーマット及びファイル・タイプを持つハイパーテキスト文書にアクセスするための周知のソフトウェア・アプリケーションであるブラウザを含むことができる。
【００１８】
本発明は、図１及び図２に関して上述したように、種々のハードウェア・プラットフォーム及びソフトウェア・プラットフォーム上に実装することができる。しかしながら、本発明は、より特定的には、改良された認証サービスに向けられる。改良された認証サービスをより詳細に説明する前に、典型的な認証サービスを説明する。
【００１９】
本明細書における図の説明は、クライアント装置又は該クライアント装置のユーザによる特定の動作を伴う。当業者であれば、クライアントとの間の応答及び／又は要求は、時にはユーザによって開始され、時には、多くの場合クライアントのユーザに代わって、該クライアントによって自動的に開始されることが分かるであろう。したがって、図の説明においてクライアント又はクライアントのユーザというときには、「クライアント」及び「ユーザ」という用語は、説明される処理の意味に大きな影響を与えることなく交換可能に用いることができることを理解すべきである。
【００２０】
ここで図３を参照すると、データ・フロー図は、クライアントがサーバにおける保護リソースへのアクセスを試みるときに用いることができる典型的な認証処理を示す。図示さ

れるように、クライアント・ワークステーション１５０のユーザは、該クライアント・ワークステーション上で実行する該ユーザのウェブ・ブラウザを通じ、コンピュータ・ネットワークを介して、サーバ１５１上の保護リソースへのアクセスを求める。保護リソースとは、アクセスが制御又は制限されているリソース（アプリケーション、オブジェクト、文書、ページ、ファイル、実行可能コード、又は他のコンピュータ・リソース、通信形式リソースなど）である。保護リソースは、認証され且つ許可されたユーザによってのみアクセス可能な、Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）、又はより一般的には、Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒ（ＵＲＩ）によって特定される。コンピュータ・ネットワークは、図１又は図２に示されるように、インターネット、イントラネット、又は他のネットワークとすることができ、サーバは、ウェブ・アプリケーション・サーバ（ＷＡＳ）、サーバ・アプリケーション、サーブレット・プロセスなどとすることができる。

【００２１】

処理は、ユーザが、「ｉｂｍ．ｃｏｍ」ドメイン内のウェブ・ページのようなサーバ・サイドの保護リソースを要求したときに開始される（ステップ１５２）。「サーバ・サイド」及び「ユーザ・サイド」という用語は、それぞれ、ネットワーク環境内のサーバ及びクライアントにおける動作又はエンティティを指す。ウェブ・ブラウザ（又は、関連するアプリケーション若しくはアプレット）は、「ｉｂｍ．ｃｏｍ」ドメインをホスティングするウェブ・サーバに送信されるＨＴＴＰ要求を生成する（ステップ１５３）。「要求」及び「応答」という用語は、メッセージ、通信プロトコル情報、又は他の関連情報などの、特定の操作に必要とされる情報の転送に適したデータ・フォーマット設定を含むことが理解されるべきである。

【００２２】

サーバは、このクライアントについてアクティブなセッションがないものと判断し（ステップ１５４）、そのため、サーバは、該サーバと該クライアントとの間に、該クライアントと該サーバとの間の多数の情報転送を伴うＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）セッションの確立を開始し、完了する。ＳＳＬセッションが確立された後は、該ＳＳＬセッション内でその後の通信メッセージが転送されるが、該ＳＳＬセッション内の通信メッセージは暗号化されているため、いずれの秘密情報も安全に保たれる。

【００２３】

しかしながら、サーバは、ユーザが保護リソースにアクセスすることが可能になる前に該ユーザの識別情報を判断する必要があり、そのため、該サーバは、何らかのタイプの認証チャレンジをクライアントに送信することによって認証処理を実行するようにユーザに要求する（ステップ１５６）。認証チャレンジは、ＨＴＭＬ形式などの様々なフォーマットとすることができる。次いで、ユーザは、ユーザ名又は他のタイプのユーザ識別子などの要求された情報又は必要な情報を、関連するパスワード又は他の形式の秘密情報と共に提供する（ステップ１５７）。

【００２４】

認証応答情報はサーバに送信され（ステップ１５８）、その時点で、サーバは、例えば以前に提出された登録情報を検索し、提示された認証情報をユーザの格納済み情報と照合することによって、ユーザ又はクライアントを認証する（ステップ１５９）。認証が成功した場合には、認証されたユーザ又はクライアントについてアクティブなセッションが確立される。

【００２５】

次いで、サーバは、初めに要求されたウェブ・ページを検索して、ＨＴＴＰ応答メッセージをクライアントに送信し（ステップ１６０）、それにより、保護リソースについてのユーザの当初要求を実現する。この時点で、ユーザは、ブラウザ・ウィンドウ内のハイパーテキスト・リンクをクリックすることによって「ｉｂｍ．ｃｏｍ」内の別のページを要求することができ、該ブラウザは、別のＨＴＴＰ要求メッセージをサーバに送信する（ステップ１６２）。この時点で、サーバは、ユーザがアクティブなセッションを有している

ことを認識し（ステップ１６３）、該サーバは、別のＨＴＴＰ応答メッセージにおいて、要求されたウェブ・ページをクライアントに返信する（ステップ１６４）。

【００２６】

ここで図４を参照すると、ブロック図は、複数の認証サーバを含むエンタープライズ・ドメインについての典型的なデータ処理システムを示す。典型的な企業コンピューティング環境又はインターネット・ベースのコンピューティング環境の場合と同様に、エンタープライズ・ドメイン１７０は、ユーザ１７１が、例えばクライアント装置１７３上のブラウザ・アプリケーション１７２を用いることによってネットワーク１７４を介してアクセスすることが可能な制御されたリソースのホストとして機能する。アプリケーション・サーバ１７５は、ウェブ・ベースのアプリケーションを介して、又はレガシ・アプリケーションを含む他のタイプのアプリケーションを介してアクセス可能なリソースをサポートする。認証サーバ１７６は、ユーザ名／パスワード、Ｘ．５０９証明書、又はセキュア・トークンなどの様々な認証機構をサポートする。エンタープライズ・ドメイン１７０は、複数のサーバをサポートする。プロキシ・サーバ１７７は、エンタープライズ・ドメイン１７０に代わって、広範囲の機能を実行する。プロキシ・サーバ１７７は、例えばアプリケーション・サーバのコンテンツをミラーリングするためにウェブ・ページをキャッシュすること、又は、入力データストリーム・フィルタ・ユニット１７９及び出力データストリーム・フィルタ・ユニット１８０を通して、着信及び発信するデータストリームにフィルタをかけることなどのプロキシ・サーバ１７７の機能を制御するために、管理上、設定ファイル及びエンタープライズ・ポリシー・データベース１７８を介して設定することができる。入力データストリーム・フィルタ・ユニット１７９は、要求が着信したときに複数の検査を実行することができ、一方、出力データストリーム・フィルタ・ユニット１８０は、応答を発信するときに複数の検査を実行することができ、各々の検査は、種々のエンタープライズ・ポリシー内に指定された目標及び条件に従って実行することができる。

【００２７】

エンタープライズ・ドメイン１７０は、許可サーバ１８１を含む。許可サーバ１８１の許可ポリシー管理ユニット１８２は、ユーザ・レジストリ１８３及びアクセス制御リスト（ＡＣＬ）データベース１８４内の情報を管理する。ポリシー管理ユニット１８２は、ユーザがドメイン１７０内のアプリケーション・サーバ１７５によって提供される特定のサービスにアクセスすることを許可されるかどうかを、これらのサービスについてのユーザ要求に対するポリシーを検査することによって判断する。本明細書の例は、ユーザが、認証された後に全ての制御されたリソースにアクセスすることを許可されるものと仮定するが、本発明の様々な実施形態は、本発明の範囲に影響を与えることなく代替的な許可処理を組み込むことができることに注意すべきである。

【００２８】

エンタープライズ・ドメイン１７０内の上記のエンティティは、多くのコンピューティング環境内の典型的なエンティティを表す。図３に関して示されたように、ウェブ・ベースのアプリケーションは、種々の手段を利用して、多くの場合はＨＴＭＬ形式内のユーザ名／パスワードの組み合わせとして認証情報を入力するように、ユーザに指示することができる。図４に示される例においては、ユーザ１７１は、クライアント１７３がリソースにアクセスする前に認証されることを要求される場合があり、その後、図３において上述されたものと同様の方法で、クライアント１７３についてのセッションが確立される。図４においては、入力データストリーム・フィルタ・ユニット１７９は、クライアント１７３からの着信要求を受信した後で、クライアント１７３がすでにセッションを確立済みであるかどうかを判断することができ、確立されていない場合には、ユーザ１７１を認証するために認証サーバ１７６上の認証サービスを呼び出すことができる。クライアント１７３がすでにセッションを確立済みである場合には、制御されたリソースへのアクセスを承諾する前に着信要求に対して付加的な検査を実行することかでき、この付加的な検査は、エンタープライズ認証ポリシーの中で指定することができる。

【００２９】

ここで本発明に焦点を移すと、幾つかのシステムはステップアップ認証手続きを実行する必要があることが上記された。しかしながら、ユーザ名／パスワードの組み合わせといった下位レベルの非証明書ベースの認証手続きについてクライアントとサーバとの間にＳＳＬセッションが確立された場合に、認証サービスと該ユーザのブラウザ又は同様のクライアント・アプリケーションとの間で相互認証されたアクティブなＳＳＬセッションを維持しながら、下位レベルの非証明書ベースの認証手続きから上位レベルの証明書ベースの認証手続きにステップアップする操作は不可能であることもまた指摘された。本発明は、既存のＳＳＬセッションを介してユーザ又はユーザのクライアント装置についての証明書ベースの認証手続きを実行するサーバ・サイドの認証サービスを持つことによって、この問題への解決策を提供する。本発明は、残りの図面に関連して以下により詳細に説明される。

【００３０】

ここで図５を参照すると、ブロック図は、本発明に係るステップアップ認証処理を含むように拡張された認証サービスを示す。クライアント２００は、図４に関して上述されたものと同様の方法で、様々なウェブ・アプリケーションからリソース及びサービスにアクセスするためのウェブ・ブラウザ・アプリケーション２０２又は同様のクライアント・アプリケーションを実行する。ブラウザ２０２は、仮想マシンを含むことができるランタイム環境２０４をサポートし、ランタイム環境２０４は、アプレット又はプラグインなどの、様々なタイプのダウンロード可能な実行可能ソフトウェア・モジュールを実行することができる。ブラウザ２０２及びサポートされたアプレット／プラグインは、クライアントがユーザのデジタル証明書及び／又は暗号鍵を保持する鍵データストア２０６にアクセスすることができる。さらに、ブラウザ２０２及びサポートされた実行可能モジュールは、クライアント２００において生成された署名のログを収める署名ログ２０８にアクセスすることができる。署名ログ２０８はまた、クライアント２００からの署名の提出に応答してウェブ・サーバから戻された署名記録／受け取りを収めることができる。

【００３１】

ドメイン２１０は、アプリケーション・サーバ及び認証サーバを備え、そのうちの少なくとも１つは、本発明のステップアップ認証機能を実装するためのステップアップ認証処理ユニット２１４を含む認証サービス２１２をサポートする。認証サービス２１２はまた、以下により詳細に説明されるように、クライアントから受信するデジタル署名を検証するためのデジタル署名検証ユニット２１６と、認証サービス２１２からの要求に応答してクライアントから戻された受信済み署名の記録を格納するための署名ログ２１８とをサポートする。

【００３２】

ここで図６を参照すると、フローチャートは、相互認証されたアクティブなＳＳＬセッションを維持しながら、下位レベルの非証明書ベースの認証手続きから上位レベルの証明書ベースの認証手続きにステップアップするための処理を示す。図３に関して上述されたように、保護リソースにアクセスするためのユーザ要求を受信したことに応答して、例えばクライアント装置上のブラウザ・アプリケーションにおけるユーザ動作に応答して生成されたＨＴＴＰ要求メッセージの形式のウェブ・ページ要求の結果として、サーバにおいて典型的な非証明書ベースの認証操作を行うことができる（ステップ３０２）。相互認証されたＳＳＬセッションをクライアントとサーバとの間に確立した後で、該サーバは、該ＳＳＬセッションを介して、非証明書ベースの認証操作、例えば有効なユーザ名／パスワードの組み合わせ又は他の何らかの秘密情報を提供するためのクライアント／ユーザに対するチャレンジを実行する（ステップ３０４）。非証明書ベースの認証操作の完了が成功した場合には、サーバは、例えば応答メッセージを戻すか又は他の何らかの動作を実行することによって、初めに要求されたリソースをクライアントに提供する（ステップ３０６）。

【００３３】

しかしながら、図３が非証明書ベースの認証操作のみを示すのに対して、図６は、本発

明が証明書ベースの認証操作によってもたらされるような上位レベルのセキュリティにステップアップするための処理を提供する方法を示すことにより続けられるという点で、図６は図３と異なる。

【００３４】

非証明書ベースの認証操作が完了し、以前の非証明書ベースの認証操作によって保護されるクライアント・セッションの間にサーバが保護リソースを提供した後のある時点で、該サーバは、上位レベルのセキュリティによって制御される保護リソース、すなわちその特定のリソースへのアクセスがより制限される保護リソースについての要求を受信する（ステップ３０８）。それに応答して、サーバは、該サーバとクライアントとの間に以前に確立されたＳＳＬセッションを介して、該クライアントについての証明書ベースの認証操作を実行する（ステップ３１０）が、これは、その時点のＳＳＬセッションを中断すること、その時点のＳＳＬセッションを再折衝すること、又はその時点のＳＳＬセッションを終了することなく行われる。証明書ベースの認証操作の完了が成功した場合には、サーバは、例えば応答メッセージを戻すか又は他の何らかの動作を実行することによって、より制限されたリソースをクライアントに提供し、処理は終了する。このように、非証明書ベースの認証操作のために以前に用いられたものと同じＳＳＬセッションを介して、証明書ベースの認証操作が行われる。

【００３５】

「非証明書ベースの認証操作」という用語の使用は、ユーザ／クライアントの識別情報を判断するための第１の認証操作がデジタル証明書を使用しないという事実を指すことに留意すべきである。（非証明書ベースの認証操作において使用される秘密情報、例えばパスワードを安全に伝送するために用いられる場合がある）ＳＳＬセッションを確立するためにクライアント・サイドのデジタル証明書を用いることは、本明細書では、非証明書ベースの認証操作における証明書の使用とは見なされない。

【００３６】

ここで図７を参照すると、フローチャートは、本発明の実施形態に係るステップアップした証明書ベースの認証操作のための、サーバにおける具体的な処理の更なる詳細を示す。図７に示される処理は、主として、図６におけるステップ３０８～３１２についての更なる詳細を提供するものである。図７の処理におけるステップは、サーバ・サイドのデータ処理システム、例えば図５において示される分散データ処理システムと同様のシステム内で行われ、説明を容易にするために、処理をその全体が１つのサーバ内で行われるよう説明するが、処理は、複数のサーバ、アプリケーション、及び／又は装置にわたって実装することができるであろう。本例は、ＨＴＴＰメッセージ及びＨＴＭＬページの使用を説明するが、本発明は、他のプロトコル及びメッセージ／文書フォーマットをサポートするように実装することができる。

【００３７】

処理は、非証明書ベースの認証操作、例えば図６におけるステップ３０２～３０６に示されるような非証明書ベースの認証操作がＳＳＬセッションを介して行われた後で、サーバがクライアントからのリソース要求を受信することによって始まる（ステップ４０２）。したがって、サーバは、すでに該サーバとアクティブなセッションを確立したクライアントからリソース要求を受信したことを認識し、図３とは対照的に、該サーバは、認証操作を完了するように直ちにクライアントに求めるのではなく、該要求に応答することに進む。

【００３８】

次いで、サーバは、要求されたリソースへのアクセスが、クライアントとの間ですでに完了した非証明書ベースの認証操作によって提供された下位レベルのセキュリティではなく、証明書ベースの認証操作によって提供することができる上位レベルのセキュリティを必要とすることを決定する（ステップ４０４）。サーバは、本発明の範囲に影響を与えることなく、種々の処理を通じてこの決定を行うことができる。１つの例として、着信リソース要求は、図４におけるサーバ１７７などのプロキシ・サーバによって、フィルタをか

けるか又は走査することができる。要求されたＵＲＩを着信要求メッセージから抽出した後で、抽出されたＵＲＩは、該抽出されたＵＲＩに関連するポリシーと照合される。関連するポリシーは、いずれかの認証要件又は他のセキュリティ手順を含む、ＵＲＩに適切に応答するために実行されるべき適切な動作を示す。ポリシーが、要求に応答する前に証明書ベースの認証操作の完了が成功しなければならないことを示す場合、及び、要求しているクライアントとの間で証明書ベースの認証操作がまだ完了していない場合には、図７において示される処理の残りのステップに示すように、認証のレベルをステップアップするための手続きが開始される。この例においては、アプリケーション・サーバは、認証要件を認識していないが、他の実施形態は、本発明の範囲に影響を与えることなく、何らかの方法でアプリケーション・サーバを関与させることができる。

【００３９】

次いで、サーバは、ソフトウェア・モジュールをサーバからクライアントにダウンロードすること、及び／又は、クライアントにおいてソフトウェア・モジュールの実行を開始させることに進む（ステップ４０６）。ソフトウェア・モジュールをダウンロードする方法又は実行を開始させる方法は、変えることができる。第１の実施形態においては、サーバは、例えばクライアントからの初めの要求、すなわち証明書ベースの認証操作を必要とすることが決定された要求に対するＨＴＴＰ応答メッセージのコンテンツ・ペイロードとして戻されるＨＴＭＬウェブ・ページ内にＪａｖａアプレットを埋め込むことによって、アプレット又はプラグインをブラウザなどのクライアント・アプリケーションにダウンロードする。それに応答して、ブラウザは、そのアプレットをウェブ・ページの通常の解釈及び処理の一部として読み込む。

【００４０】

代替的な実施形態においては、サーバは、特定のＭＩＭＥ（Ｍｕｌｔｉｐｕｒｐｏｓｅ Ｉｎｔｅｒｎｅｔ Ｍａｉｌ Ｅｘｔｅｎｓｉｏｎ）タイプを有するコンテンツを含むことを示すメッセージ本文をクライアントに戻すことができる。それに応答して、クライアントのブラウザ・アプリケーションは、特定のＭＩＭＥタイプを処理することができるものとして以前にブラウザに登録された適切なプラグインを読み込む。幾つかの場合においては、特定のＭＩＭＥタイプについてのプラグインが登録されていない場合には、ブラウザは、適切なプラグインを探すようにユーザに指示する。このように、ブラウザは、サーバがソフトウェア・モジュールをクライアントにダウンロードする必要がないように、後述される処理ステップを行うことができるソフトウェア・モジュールを予め持つことができる。

【００４１】

いずれの場合においても、保護リソースについての要求を送信するクライアント・アプリケーションは、以前にアクティブにされたＳＳＬセッションを維持し、サーバは、証明書ベースの認証手続きについてのクライアント・サイドのステップを行うソフトウェア・モジュールを該クライアント・アプリケーションに実行させるために、該ＳＳＬセッションを介して適切なメッセージを該クライアント・アプリケーションに送信するが、幾つかの場合においては、サーバはソフトウェア・モジュールをダウンロードすることもでき、別の場合においては、ソフトウェア・モジュールはすでにクライアントに存在しているものとすることができる。本発明は、標準的なインターネット関連プロトコル及び仕様に準拠するため、本発明は、クライアント・アプリケーションがサーバ・サイドの認証要件に応答するためのビルトイン機能を持つことを前提としないステップアップ認証操作の方法を提供する。サーバは、周知のインターネット関連技術及びワールド・ワイド・ウェブ関連技術を通じて、ブラウザ及び同様のクライアント・アプリケーションの拡張性を利用することによって、必要な機能を持つソフトウェア・モジュールを提供することができる。

【００４２】

引き続き図７を参照すると、サーバは、次に、ソフトウェア・モジュールによってデジタル署名されることになるチャレンジ・データをダウンロードする（ステップ４０８）。チャレンジ・データは、クライアントにおけるアプレット、プラグイン、又は他のソフト

ウェア・モジュール内にあり、該チャレンジ・データ上にデジタル署名を生成するデジタル署名アルゴリズムへの入力として用いることができる何らかのタイプのデータ項目である。チャレンジ・データのフォーマットは、使用されるデジタル署名アルゴリズムによって決まるものとすることができ、本発明は、１つ又は複数の標準的な又は専用のデジタル署名アルゴリズムをサポートすることができる。

【００４３】

サーバは、ダウンロードされるアプレットと共にチャレンジ・データをダウンロードすることができ、又は、チャレンジ・データは、後のメッセージに入れて送信することができる。代替的には、クライアントにおけるアプレット、プラグイン、又は他のソフトウェア・モジュールは、チャレンジ・データを要求することができ、サーバは、それに応答してチャレンジ・データを戻す。代替的には、クライアントは、例えばサーバによって以前にクライアントに戻されたキャッシュ済みウェブ・ページなどのチャレンジ・データをすでに持っている場合がある。

【００４４】

その後のいずれかの時点において、サーバは、クライアントからデジタル署名を受信し（ステップ４１０）、該サーバは、ユーザ／クライアントの適切な公開鍵証明書を用いて該デジタル署名を検証する（ステップ４１２）。サーバは、ディレクトリから公開鍵証明書を検索することができ、又は、公開鍵証明書は、クライアントからのデジタル署名を伴うメッセージを添付することができ、公開鍵証明書の信頼性は、認証局及び種々の証明書取り消し機構を通じて検証可能である。有効な公開鍵証明書に示される個人／エンティティのみが、公開鍵に対応する秘密鍵を所有するはずであるため、デジタル署名が検証された場合には、クライアントは、非対称の公開暗号鍵／秘密暗号鍵の対における公開鍵に対応する秘密鍵を所有しており、それによってクライアント／ユーザの識別情報を立証することを示している。デジタル署名の検証に成功した場合には、サーバは、否認防止を目的として、例えば、該デジタル署名の複製、検証可能なタイムスタンプ、及び該デジタル署名を受信したＩＰアドレスと共にデータベース記録を生成することによって、デジタル署名の受信を記録することができる（ステップ４１４）。デジタル署名の検証に成功することによって、証明書ベースの認証操作が完了し、結果として、サーバは、該サーバが証明書ベースの認証操作を試みる前にクライアントによって要求されたリソースへのアクセスを提供し（ステップ４１６）、それによって、図７に示される処理を終了する。

【００４５】

ここで図８を参照すると、フローチャートは、本発明の実施形態に係るステップアップした証明書ベースの認証操作のための、クライアントにおける処理を示す。サーバ・サイドの処理を示す図７とは対照的に、図８は、クライアント・サイドの処理を示す。処理は、クライアントがサーバとの間でＳＳＬセッションをすでに確立し、該サーバとの間で非証明書ベースの認証操作を完了することに成功した後で、該クライアントがリソースについての要求メッセージを該サーバに送信することによって始まる（ステップ５０２）。要求に応答して、クライアントは、証明書ベースの認証操作をサポートするソフトウェア・モジュールを含むか、又はそのようなソフトウェア・モジュールの実行を開始させる、応答メッセージを受信する（ステップ５０４）。クライアントは、ブラウザなどのクライアント・アプリケーションによってサポートされる仮想マシン内で実行可能なＪａｖａアプレットなどのアプレットを受信することができる。代替的に、クライアントは、特定のＭＩＭＥタイプのコンテンツを含むメッセージを受信し、それにより、クライアント・アプリケーションを作動させて、示されるＭＩＭＥタイプを有するオブジェクトを処理するプラグインを起動することができる。

【００４６】

さらに、クライアント・アプリケーションは、デジタル署名を生成する時に用いられるチャレンジ・データを受信することができる（ステップ５０６）。代替的に、クライアント・アプリケーションは、デジタル署名アルゴリズムへの入力として用いることができるデータ項目をすでに持っている場合もある。いずれの場合においても、クライアントによ

って用いられるデジタル署名アルゴリズムへの入力データは、該入力データ上に生成されるデジタル署名をサーバが検証するために、該サーバに知られていなければならない。したがって、デジタル署名アルゴリズムへの入力データは、クライアントによって選択され、それに続いて、例えば生成されたデジタル署名と共にＳＳＬセッションを介してサーバに送ることができる。

【００４７】

クライアント・アプリケーションは、デジタル署名を生成することを開始させられた後、又はデジタル署名を生成することを決定した後のいずれかの時点において、デジタル署名を生成し（ステップ５０８）、該デジタル署名をサーバに送信する（ステップ５１０）。さらに、クライアント・アプリケーションは、タイムスタンプ、及び場合によっては否認防止手続きに役立つ他の情報と共に、デジタル署名の生成を記録することができる（ステップ５１２）。デジタル署名が適切に生成された場合には、クライアントは、以前に確立されたＳＳＬセッションを介してステップアップした証明書ベースの認証操作を完了することに成功したことになり、次いでクライアントは、例えばウェブ・ページを受信することによって要求したリソースへのアクセスを受け（ステップ５１４）、それによりクライアント・サイドの処理を終了する。

【００４８】

デジタル署名を生成し、検証する方法は、本発明の範囲に影響を与えることなく、周知の規格又は専用の処理に従って変えることができる。例えば、以前に確立されたＳＳＬセッションを介してステップアップした証明書ベースの認証処理を実行するというサーバの決定に応答して、クライアントのブラウザが、埋め込まれたアプレットを持つＨＴＭＬページを受信した時に、クライアント・サイドの処理を行うことができる。ブラウザは、ウェブ・ページを処理し、クライアント上のファイルなどの鍵データストアの識別子を、その鍵データストアのロックを解除するパスワードと共に入力するようにユーザに指示するアプレットを実行する。アプレットがユーザに指示する機構又は他の方法で作動する機構は、本発明の実装形態に応じて変えることができる。アプレットは、保留中の要求についてデジタル署名を作成する必要性を説明するブラウザ・ウィンドウ内のウェブ・ページを提示することによってユーザに指示することができ、提示されたウェブ・ページは、ユーザがデジタル署名についての要求を承認又は非承認とすることができるようにするＯＫボタン及びキャンセル・ボタンを有することができる。さらに、提示されたウェブ・ページは、ユーザがチャレンジ・データを見直すことができるように、署名されている該チャレンジ・データを確認表示することができる。

【００４９】

典型的には、鍵データストアは、非対称暗号機能のための秘密鍵／公開鍵対のうちの秘密鍵を保持する。鍵データストアは、ブラウザ・アプリケーション、アプレット、又はクライアント・オペレーション・システムといった種々のエンティティによって管理することができる。ブラウザは、暗号情報の使用に関する種々の規格に準拠するものとすることができる。例えば、「ＰＫＣＳ＃７：Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ｍｅｓｓａｇｅ Ｓｙｎｔａｘ」、ＲＦＣ（Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ）２３１５、Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ（ＩＥＴＦ）は、デジタル署名及びデジタル・エンベロープなどのデータに適用される暗号方式を有するデータについての一般的な構文を記述するＰＫＣＳ（Ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ｓｙｓｔｅｍ）仕様である。別の例として、「ＰＫＣＳ＃１１：Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ｔｏｋｅｎ Ｉｎｔｅｒｆａｃｅ Ｓｔａｎｄａｒｄ」、ＲＳＡ Ｓｅｃｕｒｉｔｙ, Ｉｎｃ．は、暗号情報を保持し、暗号機能を実行する装置のためのアプリケーション・プログラミング・インターフェース（ＡＰＩ）を記述するＰＫＣＳ仕様である。

【００５０】

ユーザが、要求された情報を入力し、該ユーザの秘密鍵の使用を承認することを示した後で、アプレットは、好ましくはＷｏｒｌｄ Ｗｉｄｅ Ｗｅｂ Ｃｏｎｓｏｒｔｉｕｍ

（Ｗ３Ｃ）によって標準化されたＸＭＬデジタル署名の形式で、デジタル署名を生成する。デジタル署名は、続いて検証されることになるデータ項目の組、すなわちいわゆる「署名情報」に適切な署名アルゴリズムを適用することによって作成され、このシナリオにおいては、署名されたデータは、最低限は、チャレンジ・データを含むことになる。ＸＭＬ署名は、デジタル署名を検証するのに用いられるべきユーザの公開鍵証明書を含むことができる、いわゆる「キー情報」も含む。次いで、アプレットは、ＸＭＬ署名をウェブ・サーバに送信し、デジタル署名を生成する処理が完了する。

【００５１】

本発明の利点は、上述された詳細な説明を考慮すれば明らかとなるはずである。本発明は、ユーザ名／パスワードの組み合わせといった下位レベルの非証明書ベースの認証手続きについてクライアントとサーバとの間にＳＳＬセッションが確立された場合に、認証サービスとユーザのブラウザ又は同様のクライアント・アプリケーションとの間で相互認証されたアクティブなＳＳＬセッションを維持しながら、下位レベルの非証明書ベースの認証手続きから上位レベルの証明書ベースの認証手続きにステップアップするための認証操作を提供する。

【００５２】

本発明は、既存のＳＳＬセッションを介してユーザ又はユーザのクライアント装置についての証明書ベースの認証手続きを実行するサーバ・サイドの認証サービスを持つことによって、この問題への解決策を提供する。認証サービスは、必要に応じて、既存のＳＳＬセッションを介して実行可能モジュールをクライアントにダウンロードする。次いで、実行可能モジュールは、クライアント・サイドのデジタル証明書を用いてデジタル署名を生成し、該デジタル署名は、以前に確立されたＳＳＬセッションを介して戻される。認証サービスがデジタル署名を検証した後、証明書ベースの認証手続きは完了する。このようにして、認証サービスは、既存のＳＳＬセッションを終了又は再折衝する必要なく、証明書ベースの認証にステップアップすることができる。

【００５３】

完全に機能するデータ処理システムを背景として本発明を説明したが、当業者であれば、本発明の処理は、配布を行うのに実際に用いられる特定のタイプの信号支持媒体に関わらず、コンピュータ可読媒体内の命令の形態で、及び他の様々な形態で、配布できることが分かるであろうということに留意することが重要である。コンピュータ可読媒体の例には、ＥＰＲＯＭ、ＲＯＭ、テープ、紙、フロッピー（商標）ディスク、ハード・ディスク・ドライブ、ＲＡＭ、及びＣＤ－ＲＯＭなどの媒体、並びに、デジタル通信リンク及びアナログ通信リンクなどの伝送タイプの媒体が含まれる。

【００５４】

方法は、一般に、所望の結果に至る自己矛盾のない一連のステップであると理解される。これらのステップは、物理量の物理的な操作を必要とする。必須ではないが通常は、これらの量は、格納するか、転送するか、組み合わせるか、比較するか、又は他の方法で操作することが可能な電気的信号又は磁気的信号の形態をとる。時には、主に一般的な用法であるという理由で、これらの信号を、ビット、値、パラメータ、項目、要素、記号、文字、語、数などと呼ぶのが都合がよい。しかしながら、これらの用語の全て及び同様の用語は、適切な物理量と関連付けられるものであり、これらの量に付される都合の良いラベルに過ぎないことに留意されたい。

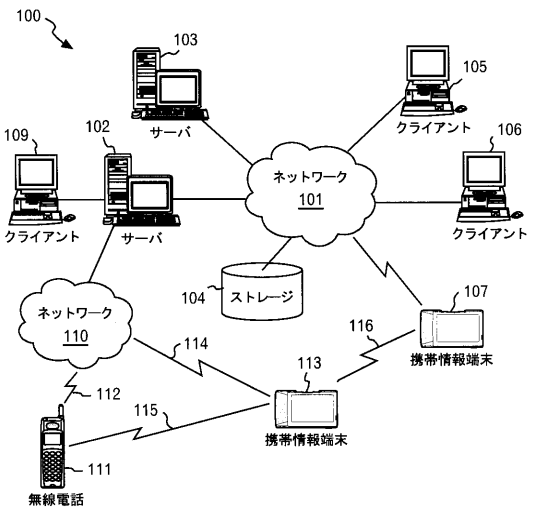
【００５５】

本発明の説明は、例示の目的で提示されたものであって、包括的であること、又は、開示された実施形態に限定されることを意図するものではない。当業者であれば、多くの修正及び変形が明らかであろう。本実施形態は、本発明の原理及びその実際の用途を説明するために、並びに、考え得る他の用途に適合するような種々の修正を伴う種々の実施形態を実施するために当業者以外の者が本発明を理解することが可能になるように、選択されたものである。

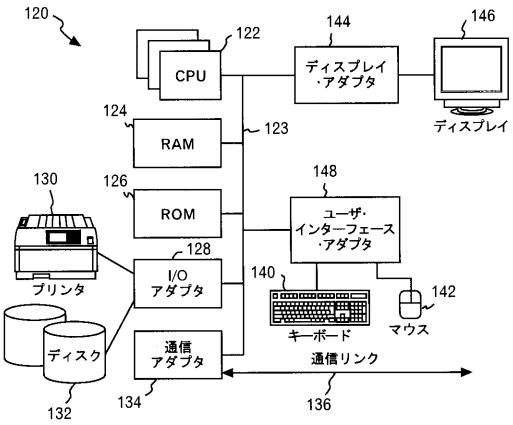
【図面の簡単な説明】

【００５６】
【図１】各々が本発明を実装することができるデータ処理システムの典型的なネットワークを示す。
【図２】本発明を実装することができるデータ処理システム内で用いることができる典型的なコンピュータ・アーキテクチャを示す。
【図３】クライアントがサーバにおける保護リソースへのアクセスを試みるときに用いることができる典型的な認証処理を説明するデータ・フロー図を示す。
【図４】複数の認証サーバを含むエンタープライズ・ドメインについての典型的なデータ処理システムを示すブロック図を示す。
【図５】本発明に係るステップアップ認証処理を含むように拡張された認証サービスを示すブロック図を示す。
【図６】相互認証されたアクティブなＳＳＬセッションを維持しながら、下位レベルの非証明書ベースの認証手続きから上位レベルの証明書ベースの認証手続きにステップアップするための処理を示すフローチャートを示す。
【図７】本発明の実施形態に係るステップアップした証明書ベースの認証操作のための、サーバにおける具体的な処理の更なる詳細を説明するフローチャートを示す。
【図８】本発明の実施形態に係るステップアップした証明書ベースの認証操作のための、クライアントにおける処理を説明するフローチャートを示す。

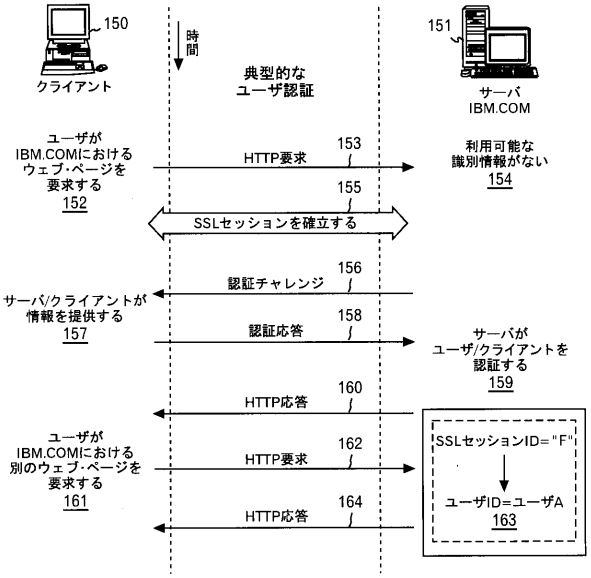
【図１】



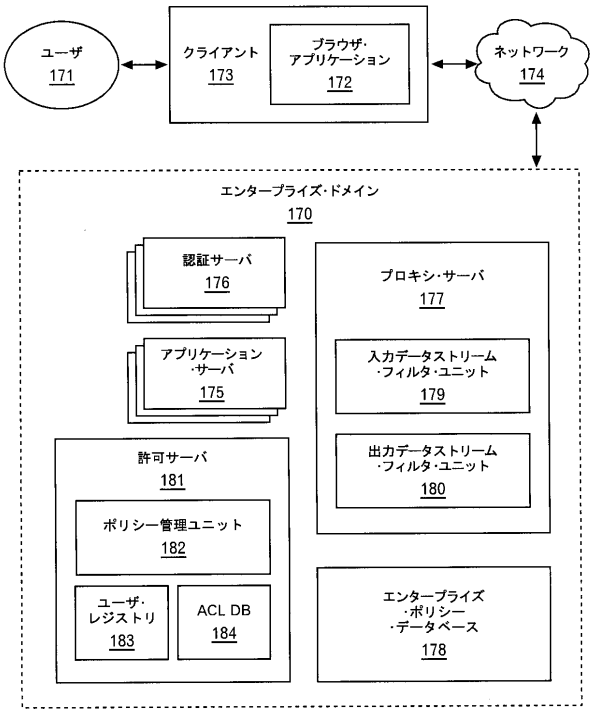
【図２】



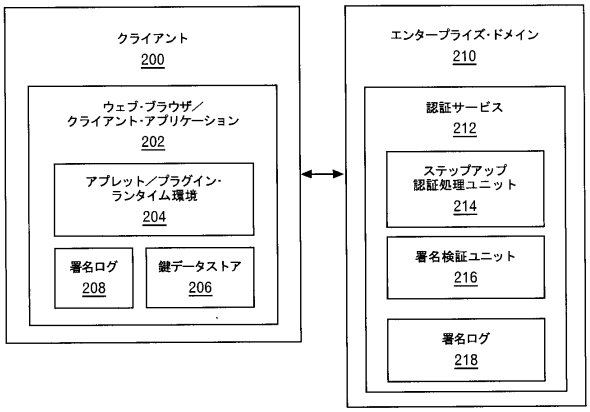
【図３】


150
クライアント
時間
典型的な
ユーザ認証
151
サーバ
IBM.COM
ユーザが
IBM.COMにおける
ウェブ・ページを
要求する
152
HTTP要求
153
利用可能な
識別情報がない
154
155
SSLセッションを確立する
認証チャレンジ
156
サーバ/クライアントが
情報を提供する
157
認証応答
158
サーバが
ユーザ/クライアントを
認証する
159
HTTP応答
160
SSLセッションID="F"
ユーザID=ユーザA
163
ユーザが
IBM.COMにおける
別のウェブ・ページを
要求する
161
HTTP要求
162
HTTP応答
164

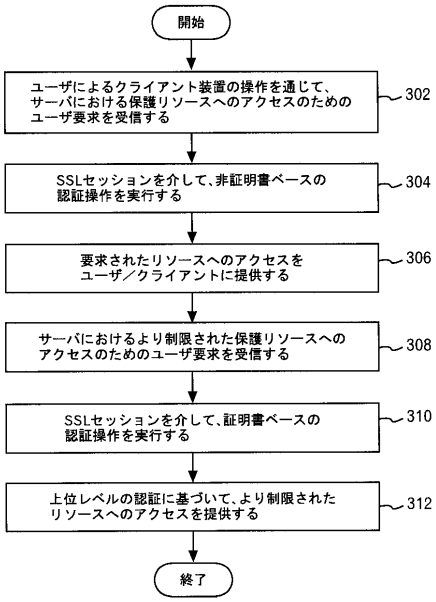
【図４】


ユーザ
171
クライアント
173
ブラウザ・
アプリケーション
172
ネットワーク
174
エンタープライズ・ドメイン
170
認証サーバ
176
アプリケーション
・サーバ
175
プロキシ・サーバ
177
入力データストリーム
・フィルタ・ユニット
179
出力データストリーム
・フィルタ・ユニット
180
許可サーバ
181
ポリシー管理ユニット
182
ユーザ・
レジストリ
183
ACL DB
184
エンタープライズ
・ポリシー
・データベース
178

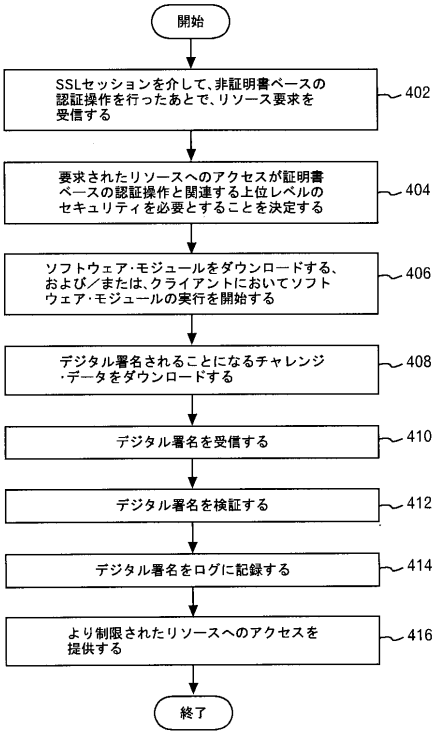
【図５】


クライアント
200
ウェブ・ブラウザ/
クライアント・アプリケーション
202
アプレット/プラグイン・
ランタイム環境
204
署名ログ
208
鍵データストア
206
エンタープライズ・ドメイン
210
認証サービス
212
ステップアップ
認証処理ユニット
214
署名検証ユニット
216
署名ログ
218

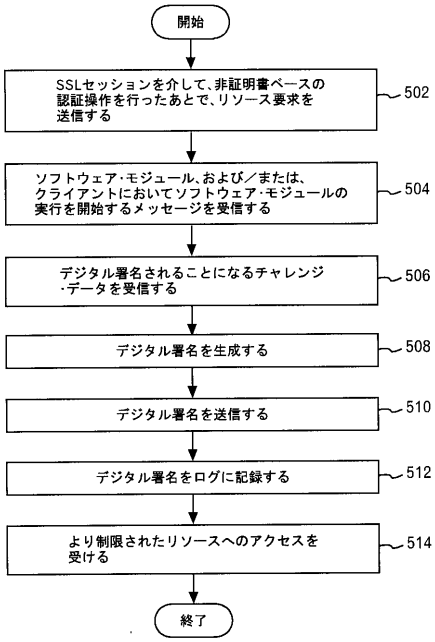
【図６】


開始
ユーザによるクライアント装置の操作を通じて、
サーバにおける保護リソースへのアクセスのための
ユーザ要求を受信する
302
SSLセッションを介して、非証明書ベースの
認証操作を実行する
304
要求されたリソースへのアクセスを
ユーザ/クライアントに提供する
306
サーバにおけるより制限された保護リソースへの
アクセスのためのユーザ要求を受信する
308
SSLセッションを介して、証明書ベースの
認証操作を実行する
310
上位レベルの認証に基づいて、より制限された
リソースへのアクセスを提供する
312
終了

【図７】


開始
SSLセッションを介して、非証明書ベースの認証操作を行ったあとで、リソース要求を受信する
402
要求されたリソースへのアクセスが証明書ベースの認証操作と関連する上位レベルのセキュリティを必要とすることを決定する
404
ソフトウェア・モジュールをダウンロードする、および／または、クライアントにおいてソフトウェア・モジュールの実行を開始する
406
デジタル署名されることになるチャレンジ・データをダウンロードする
408
デジタル署名を受信する
410
デジタル署名を検証する
412
デジタル署名をログに記録する
414
より制限されたリソースへのアクセスを提供する
416
終了

【図８】


開始
SSLセッションを介して、非証明書ベースの認証操作を行ったあとで、リソース要求を送信する
502
ソフトウェア・モジュール、および／または、クライアントにおいてソフトウェア・モジュールの実行を開始するメッセージを受信する
504
デジタル署名されることになるチャレンジ・データを受信する
506
デジタル署名を生成する
508
デジタル署名を送信する
510
デジタル署名をログに記録する
512
より制限されたリソースへのアクセスを受ける
514
終了

フロントページの続き

(72)発明者　アシュレー、ポール、アンソニー
オーストラリア国　４０６５　クイーンズランド州　バードン　ボウマン・パレード　４９
(72)発明者　マピディ、スリダール
アメリカ合衆国　７８７５９　テキサス州　オースチン　ヤーポン・ドライブ　６６２３
(72)発明者　バンデンバウバー、マーク
アメリカ合衆国　７８６８１　テキサス州　ラウンドロック　ウィットワース・レーン　８０１３

合議体
審判長　山崎　達也
審判官　殿川　雅也
審判官　石井　茂和

(56)参考文献　特開２００２－００７３４５号公報

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/00