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

特許第4632315号
(P4632315)

(45)発行日　平成23年2月16日(2011.2.16)　(24)登録日　平成22年11月26日(2010.11.26)

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

請求項の数 7　(全 23 頁)

(21)出願番号　特願2006-516130 (P2006-516130)
(86)(22)出願日　平成16年6月8日 (2004.6.8)
(65)公表番号　特表2009-514046 (P2009-514046A)
(43)公表日　平成21年4月2日 (2009.4.2)
(86)国際出願番号　PCT/EP2004/051002
(87)国際公開番号　WO2005/003934
(87)国際公開日　平成17年1月13日 (2005.1.13)
審査請求日　平成19年6月7日 (2007.6.7)
(31)優先権主張番号　10/610,980
(32)優先日　平成15年7月1日 (2003.7.1)
(33)優先権主張国　米国 (US)

(73)特許権者　390009531
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
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
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
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】グリッド・アクセス及びネットワーク・アクセスを提供するシングル・サインオン操作のための方法及びシステム

(57)【特許請求の範囲】
【請求項１】
ユーザ装置をネットワークに接続するためのネットワーク・アクセス装置と、ユーザ情報を認証するためのネットワーク・アクセス認証サーバと、サービスの提供を共有するように編成されたグリッドとが前記ネットワークに接続され、前記ユーザ装置が前記グリッドにシングル・サインオンするために行う認証操作のための方法であって、
ユーザ名及びパスフレーズを取得し、前記ネットワーク・アクセス装置を介して前記ネットワーク・アクセス認証サーバに送信して、ネットワーク・アクセス認証操作を開始するステップと、
前記ユーザ名及びパスフレーズにより正常認証した前記ネットワーク・アクセス認証サーバによって、前記ユーザ名及びパスフレーズと関連して格納されている公開鍵証明書及び秘密鍵のうち当該公開鍵証明書からコピーされた情報を含み当該秘密鍵を用いて電子署名されたプロキシ証明書を、前記ネットワークにアクセスするセッションのために用いられるネットワーク・アクセス・パラメータの組を含む情報と共に受信するステップと、
前記受信した情報から前記プロキシ証明書を抽出するステップと、
抽出した前記プロキシ証明書を格納するステップと、
前記ネットワーク・アクセス装置を介して、受信した前記ネットワーク・アクセス・パラメータを用いてトランザクション要求メッセージを前記グリッドに送信するステップと、
前記グリッド内にサブミットされるジョブに、格納した前記プロキシ証明書を添付し、

前記グリッドに提供するステップと、
を含む方法。
【請求項２】
前記グリッドに対する操作が、Ｇｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）を用いるソフトウェアによって行われる、請求項１に記載の方法。
【請求項３】
前記ネットワーク・アクセス認証操作が、遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコルを用いて行われる、請求項１に記載の方法。
【請求項４】
請求項１～３のいずれか一項に記載の各方法をコンピュータに実行させるプログラム。
【請求項５】
ユーザ装置をネットワークに接続するためのネットワーク・アクセス装置と、ユーザ情報を認証するためのネットワーク・アクセス認証サーバと、サービスの提供を共有するように編成されたグリッドとが前記ネットワークに接続され、前記ユーザ装置は前記グリッドにシングル・サインオンするために行う認証操作のための装置であって、
ユーザ名及びパスフレーズを取得し、前記ネットワーク・アクセス装置を介して前記ネットワーク・アクセス認証サーバに送信して、ネットワーク・アクセス認証操作を開始するための手段と、
前記ユーザ名及びパスフレーズにより正常認証した前記ネットワーク・アクセス認証サーバによって、前記ユーザ名及びパスフレーズと関連して格納されている公開鍵証明書及び秘密鍵のうち当該公開鍵証明書からコピーされた情報を含み当該秘密鍵を用いて電子署名されたプロキシ証明書を、前記ネットワークにアクセスするセッションのために用いられるネットワーク・アクセス・パラメータの組を含む情報と共に受信するための手段と、
前記受信した情報から前記プロキシ証明書を抽出するための手段と、
抽出した前記プロキシ証明書を格納するための手段と、
前記ネットワーク・アクセス装置を介して、受信した前記ネットワーク・アクセス・パラメータを用いてトランザクション要求メッセージを前記グリッドに送信するための手段と、
前記グリッド内にサブミットされるジョブに、格納した前記プロキシ証明書を添付し、前記グリッドに提供する手段と、
を備える装置。
【請求項６】
前記グリッドに対する動作が、Ｇｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）を用いるソフトウェアによって行われる、請求項５に記載の装置。
【請求項７】
前記ネットワーク・アクセス認証操作が、遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコルを用いて行われる、請求項５に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、改善されたデータ処理システムに関し、特に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。さらにより特定的には、本発明は、コンピュータ間認証のための方法及び装置を提供する。
【背景技術】
【０００２】
企業は、一般に、保護されたリソースへのセキュアなアクセスを、インターネットを含む様々なネットワーク全体にわたって、ユーザフレンドリな方法で、権限のあるユーザに提供することを望んでいる。遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ；Ｒｅｍｏｔｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｄｉａｌ－Ｉｎ　Ｕｓｅｒ　Ｓｅｒｖｉｃｅ）プロトコルは、ネットワークに対する遠隔アクセスを保護し、極めて一般的に用い

られる、サーバ認証及びアカウンティング・プロトコルである。しかしながら、適切に認証されたユーザがネットワークにアクセスした後に、ネットワーク上の悪意のあるユーザが、該ユーザからの電子メッセージを傍受するか、又は該ユーザからのメッセージになりすますこともできる。電子通信の保全性及びプライバシについての懸念は、インターネットベースのサービスの導入と共に増大している。電子通信を保護するために、非対称暗号鍵などの様々な暗号技術及び認証技術が開発されてきた。

【０００３】

暗号鍵の使用を取り入れた一般的でセキュアなコンピュータ・フレームワークを形成するために、デジタル証明書についての規格であるＸ．５０９のセットが公表された。Ｘ．５０９デジタル証明書は、Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ（ＩＥＴＦ）によって採用された国際電気通信連合（ＩＴＵ；Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｕｎｉｏｎ）規格である。Ｘ．５０９デジタル証明書は、証明書内の主体者名によって識別される可能性のある証明書所有者を公開暗号鍵でバインドして暗号化する。この暗号化バインディングは、Ｘ．５０９証明書のためのインターネット公開鍵基盤（ＰＫＩＸ；Ｐｕｂｌｉｃ Ｋｅｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ ｆｏｒ Ｘ．５０９ ｃｅｒｔｉｆｉｃａｔｅ）内の、認証局（ＣＡ；ｃｅｒｔｉｆｙｉｎｇ ａｕｔｈｏｒｉｔｙ）と呼ばれる信頼性のあるエンティティの関与に基づいている。結果として、証明書所有者とその公開鍵との間の強力な信用できる関連性が公開情報となるが、不正防止及び信頼性を維持することができる。この信頼性の重要な態様が、証明書が公開されて使用される前に認可局が該証明書に印を押す電子署名である。それに続いて、サービスを使用するために証明書をシステムに提示したときはいつも、主体者が認証される前にその署名が検証される。認証処理が正常に完了した後に、証明書所有者は、特定の情報、サービス、又は他の制御されたリソースにアクセスすることができる、すなわち、証明書所有者は、特定のシステムにアクセスする権限が与えられることになる。

【０００４】

主としてハイパーテキスト転送プロトコル（ＨＴＴＰ；ＨｙｐｅｒＴｅｘｔ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ）のような通信プロトコルの導入によるが、それほどではないにせよＸ．５０９証明書のような規格の導入も含めて、インターネット関連技術及びウェブ関連技術の広範な導入は、何千もの組織及び企業並びに何百万人もの個人によって物理的に支持されている相互接続されたコンピュータのグローバル・ネットワークの成長を可能にした。最近、企業は、多くのコンピュータの計算能力を、個々のコンピュータ上では局所的な自律制御を維持しながら計算能力及びデータストア能力を全体で共有するための多くのコンピュータについての論理編成であるグリッドに編成するよう努力している。これらの企業の多くは、ＧＧＦ社によって支援され、グリッド・コンピューティングについてのコミュニティ主導の規格を開発するＧｌｏｂａｌ Ｇｒｉｄ Ｆｏｒｕｍ（商標）内で協力している。

【０００５】

Ｇｌｏｂｕｓ Ｐｒｏｊｅｃｔ（商標）は、グリッド関連技術を開発する政府機関、企業、及び大学によって支援された１つの取り組みであり、これが、グリッド概念をウェブ・サービスに基づくサービス指向フレームワークに組み込む構想であるＯｐｅｎ Ｇｒｉｄ Ｓｅｒｖｉｃｅｓ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＯＧＳＡ）の開発をもたらした。Ｇｌｏｂｕｓ Ｔｏｏｌｋｉｔ（商標）は、グリッド使用可能アプリケーションを開発するためのソフトウェア・プログラミング・ツールを提供するＯｐｅｎ Ｇｒｉｄ Ｓｅｒｖｉｃｅｓ Ａｒｃｈｉｔｅｃｔｕｒｅの実装形態であり、Ｇｒｉｄ Ｓｅｃｕｒｉｔｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ（ＧＳＩ）は、セキュリティ機能を実装するＧｌｏｂｕｓ Ｔｏｏｌｋｉｔ（商標）の一部である。ＧＳＩは、グリッド内におけるユーザ認証のための基準としてＸ．５０９証明書を用いる。

【０００６】

セキュアな認証機構を提供することによって、保護されたリソースに対する無権限アク

セスの危険性が減少するが、同じ認証機構が、該保護されたリソースとのユーザ対話に対する障壁となる場合がある。ユーザは、一般に、アプリケーションに対応する特定のシステムの各々を保護する認証障壁を意識せずに、１つのアプリケーションとの対話から別のアプリケーションとの対話に移動する能力を望んでいる。

【０００７】

習熟するにつれてユーザは、コンピュータ・システムが、ユーザの負担が減少するようにその動作を調整することを期待している。この種の期待は、認証処理にも当てはまる。ユーザは、一旦コンピュータ・システムによって認証されると、ユーザには見えないことがあるコンピュータ・アーキテクチャの様々な境界を意識することなく、ユーザの作業セッションの間を通じて又は少なくとも特定の期間の間、認証証明書を有効とすべきであると考える可能性がある。所与の時間枠でユーザに複数の認証処理を行わせることがユーザ効率に重大な影響を与える場合があるため、企業は、一般に、ユーザ効率が従業員の生産性又は顧客満足に関係するかどうかにかかわらず、ユーザをなだめるためばかりでなくユーザ効率を向上させるために、企業の運用システムの特性におけるこうした期待に応えようとする。

【０００８】

ユーザ及びコンピュータ・システム管理者にかかる認証負担を軽減するために、様々な技術が用いられてきた。これらの技術は、ユーザがサインオン操作を完了した、すなわち認証された後は、続いて別の認証操作を行う必要がないという共通の目的を有するため、一般に、「シングル・サインオン（ＳＳＯ；ｓｉｎｇｌｅ－ｓｉｇｎ－ｏｎ）」処理と呼ばれる。その目標は、ユーザが、該ユーザのセッションの際に一度の認証処理を完了することしか求められないことである。

【０００９】

グリッドの高度分散性のため、シングル・サインオン機能の概念をグリッド・アーキテクチャ基盤に組み込むための取り組みが行われてきた。例えば、Ｇｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）は、Ｘ．５０９プロキシ証明書の使用を通してシングル・サインオン機能を実行する、すなわち、グリッド内の複合サービスのユーザが、用いられるサービス毎に認証チャレンジを通過する必要がないように、グリッド内のリソースにシングル・サインオン機能が適用される。

【００１０】

しかしながら、ユーザは、典型的には、グリッド内のサービスにアクセスしようと試みる前に、はじめにネットワークにアクセスするために認証チャレンジを通過する必要がある。ユーザは、ネットワークに対する認証操作を完了した後に、ネットワークを介してグリッド内のリソーソにアクセスしようと試みることができる。したがって、ユーザは、典型的には、グリッド内のリソースにアクセスするために２つの認証チャレンジを通過する必要があり、これは、シングル・サインオン操作の概念に反し、シングル・サインオン機能をグリッド基盤に組み込む努力を損なうものである。

【発明の開示】

【発明が解決しようとする課題】

【００１１】

したがって、正常に完了したときには、ネットワークへのアクセスを可能にすると同時に、引き続きネットワークを介してアクセスされるグリッド内のリソースへのアクセスを可能にするシングル・サインオン操作を提供するための方法を有することが有利であろう。ＲＡＤＩＵＳサーバ及びＧｌｏｂｕｓ（商標）使用可能グリッドなどの、標準仕様に従って一般に実装されるエンティティに適合するシングル・サインオン操作を提供することは特に有利であろう。

【課題を解決するための手段】

【００１２】

ＲＡＤＩＵＳサーバなどのネットワーク・アクセス認証サーバのためのユーザ・レジストリが、ユーザの秘密鍵及びユーザの公開鍵証明書を保持するように構成されており、こ

れらは、例えばＲＡＤＩＵＳプロトコルに従って実行されるネットワーク・アクセス認証操作の際に、該ネットワーク・アクセス認証サーバが使用可能である。ネットワーク・アクセス認証サーバは、ユーザ・レジストリ内の情報を用いて、ユーザのネットワーク・アクセス認証操作の際にユーザについてのプロキシ証明書を生成することができる。プロキシ証明書は、ネットワーク・アクセス装置を介してネットワーク・アクセス・パラメータと共にユーザ装置に戻される。プロキシ証明書は、ユーザ装置の適切な場所に格納され、該プロキシ証明書は、次に、ジョブがグリッドにサブミットされるときにグリッド・クライアント・アプリケーションが使用可能である。

【００１３】

その後のいずれかの時点で、グリッド・クライアント・アプリケーションは、グリッドへのジョブのサブミットを準備する。グリッド・クライアント・アプリケーションが、ネットワーク・アクセス認識操作の際に以前に格納された、有効で新しいプロキシ証明書を発見したときは、該グリッド・クライアント・アプリケーションは、新たなプロキシ証明書の生成を見合わせる。したがって、新たなプロキシ証明書がその時点でユーザ装置上に生成される必要がないという事実によって、新たなプロキシ証明書の生成と関連する認証操作についての必要性は取り除かれる。

【００１４】

第１の態様から見ると、本発明は、認証操作のための方法を提供するものであり、該方法は、ネットワーク・アクセス装置を介してユーザ装置からネットワーク・アクセス認証サーバに対するネットワーク・アクセス認証操作を開始するステップと、該ネットワーク・アクセス認証操作の正常完了に応答して、ネットワーク・アクセス・パラメータの組を含む情報を該ユーザ装置で受信するステップと、該受信した情報からプロキシ証明書を抽出するステップと、該プロキシ証明書を該ユーザ装置に格納するステップとを含む。

【００１５】

好ましくは、本発明は、ネットワーク・アクセス装置を介してトランザクション要求メッセージをグリッドに送信するステップと、プロキシ証明書を該グリッドに提供するステップとを含む。

【００１６】

好ましくは、本発明は、グリッドに対する操作がＧｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）を用いるソフトウェアによって行われる方法を提供する。

【００１７】

好ましくは、本発明は、ネットワーク・アクセス認証操作が遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコルを用いて行われる方法を提供する。

【００１８】

第２の態様から見ると、本発明は、認証操作のための方法を提供するものであり、該方法は、ユーザ装置のために、ネットワーク・アクセス装置を介してネットワーク・アクセス認証サーバでネットワーク・アクセス認証操作を行うステップと、該ネットワーク・アクセス認証サーバでプロキシ証明書を生成するステップと、該ネットワーク・アクセス認証操作の正常完了に応答して、ネットワーク・アクセス・パラメータの組を含む情報を該ユーザ装置に送信するステップとを含み、該情報は、該生成されたプロキシ証明書を含む。

【００１９】

好ましくは、本発明は、ネットワーク・アクセス認証操作を開始したエンティティに関連付けられるプロキシ証明書を提供する。

【００２０】

好ましくは、本発明は、ネットワーク・アクセス認証サーバにおいてユーザ・レジストリから公開鍵証明書及び関連する秘密鍵を取得するステップと、該公開鍵証明書からの情報をプロキシ証明書に挿入するステップと、該秘密鍵を用いて該プロキシ証明書に電子署名するステップとをさらに含む方法を提供する。

【００２１】

好ましくは、本発明は、ネットワーク・アクセス認証操作が遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコルを用いて行われる方法を提供する。

【００２２】

好ましくは、本発明は、プロキシ証明書がＲＡＤＩＵＳプロトコルにおけるベンダ特有の属性の中に送信される方法を提供する。

【００２３】

第３の態様から見ると、本発明は、認証操作のためのデータ処理システムに用いるコンピュータ可読媒体内のコンピュータ・プログラムを提供するものであり、該コンピュータ・プログラムは、ネットワーク・アクセス装置を介してユーザ装置からネットワーク・アクセス認証サーバに対するネットワーク・アクセス認証操作を開始するための手段と、該ネットワーク・アクセス認証操作の正常完了に応答して、ネットワーク・アクセス・パラメータの組を含む情報を該ユーザ装置で受信するための手段と、該受信した情報からプロキシ証明書を抽出するための手段と、該プロキシ証明書を該ユーザ装置に格納するための手段とを含む。

【００２４】

好ましくは、本発明は、ネットワーク・アクセス装置を介してトランザクション要求メッセージをグリッドに送信するための手段と、プロキシ証明書を該グリッドに提供するための手段とをさらに含むコンピュータ・プログラムを提供する。

【００２５】

好ましくは、本発明は、グリッドに対する操作がＧｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）を用いるソフトウェアによって行われるコンピュータ・プログラムを提供する。

【００２６】

好ましくは、本発明は、ネットワーク・アクセス認証操作が遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコルを用いて行われるコンピュータ・プログラムを提供する。

【００２７】

第４の態様から見ると、本発明は、認証操作のためのデータ処理システムに用いるコンピュータ可読媒体内のコンピュータ・プログラムを提供するものであり、該コンピュータ・プログラムは、ユーザ装置のために、ネットワーク・アクセス装置を介してネットワーク・アクセス認証サーバでネットワーク・アクセス認証操作を行うための手段と、該ネットワーク・アクセス認証サーバでプロキシ証明書を生成するための手段と、該ネットワーク・アクセス認証操作の正常完了に応答して、ネットワーク・アクセス・パラメータの組を含む情報を該ユーザ装置に送信するための手段とを含み、該情報は、該生成されたプロキシ証明書を含む。

【００２８】

好ましくは、本発明は、プロキシ証明書がネットワーク・アクセス認証操作を開始したエンティティに関連付けられるコンピュータ・プログラムを提供する。

【００２９】

好ましくは、本発明は、ネットワーク・アクセス認証サーバにおいてユーザ・レジストリから公開鍵証明書及び関連する秘密鍵を取得するための手段と、該公開鍵証明書からの情報をプロキシ証明書に挿入するための手段と、該秘密鍵を用いて該プロキシ証明書に電子署名するための手段とを含むコンピュータ・プログラムを提供する。

【００３０】

好ましくは、本発明は、ネットワーク・アクセス認証操作が遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコルを用いて行われるコンピュータ・プログラムを提供する。

【００３１】

好ましくは、本発明は、プロキシ証明書がＲＡＤＩＵＳプロトコルにおけるベンダ特有の属性の中に送信されるコンピュータ・プログラムを提供する。

【００３２】

第５の態様から見ると、本発明は、認証操作のための装置を提供するものであり、該装置は、ネットワーク・アクセス装置を介してユーザ装置からネットワーク・アクセス認証サーバに対するネットワーク・アクセス認証操作を開始するための手段と、該ネットワーク・アクセス認証操作の正常完了に応答して、ネットワーク・アクセス・パラメータの組を含む情報を該ユーザ装置で受信するための手段と、該受信した情報からプロキシ証明書を抽出するための手段と、該プロキシ証明書を該ユーザ装置に格納するための手段とを含む。

【００３３】

好ましくは、本発明は、ネットワーク・アクセス装置を介してトランザクション要求メッセージをグリッドに送信するための手段と、プロキシ証明書を該グリッドに提供するための手段とをさらに含む装置を提供する。

【００３４】

好ましくは、本発明は、グリッドに対する操作がＧｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）を用いるソフトウェアによって行われる装置を提供する。

【００３５】

好ましくは、本発明は、ネットワーク・アクセス認証操作が遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコルを用いて行われる装置を提供する。

【００３６】

第６の態様から見ると、本発明は、認証操作のための装置を提供するものであり、該装置は、ユーザ装置のために、ネットワーク・アクセス装置を介してネットワーク・アクセス認証サーバでネットワーク・アクセス認証操作を行うための手段と、該ネットワーク・アクセス認証サーバでプロキシ証明書を生成するための手段と、該ネットワーク・アクセス認証操作の正常完了に応答して、ネットワーク・アクセス・パラメータの組を含む情報を該ユーザ装置に送信するための手段とを含み、該情報は、該生成されたプロキシ証明書を含む。

【００３７】

好ましくは、本発明は、プロキシ証明書がネットワーク・アクセス認証操作を開始したエンティティに関連付けられる装置を提供する。

【００３８】

好ましくは、本発明は、ネットワーク・アクセス認証サーバにおいてユーザ・レジストリから公開鍵証明書及び関連する秘密鍵を取得するための手段と、該公開鍵証明書からの情報をプロキシ証明書に挿入する手段と、該秘密鍵を用いて該プロキシ証明書に電子署名するための手段とをさらに含む。

【００３９】

好ましくは、本発明は、ネットワーク・アクセス認証操作が遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコルを用いて行われる装置を提供する。

【００４０】

好ましくは、本発明は、プロキシ証明書がＲＡＤＩＵＳプロトコルにおけるベンダ特有の属性の中に送信される装置を提供する。

【発明を実施するための最良の形態】

【００４１】

本発明の実施形態は、添付図面を参照して、単なる例示の目的で以下に詳細に説明される。

一般に、本発明を構成するか、又は本発明に関連させることができる装置は、幅広いタイプの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、背景として、分散データ処理システム内のハードウェア及びソフトウェア・コンポーネントの典型的な編成を説明する。

【００４２】

ここで図面を参照すると、図１は、データ処理システムの典型的なネットワークを示すものであり、データ処理システムの各々は、本発明の一部を実装することができる。分散

データ処理システム１００はネットワーク１０１を含み、このネットワーク１０１は、分散データ処理システム１００内で相互に接続される様々な装置及びコンピュータ間の通信リンクを提供するのに用いることができる媒体である。ネットワーク１０１は、電線若しくは光ファイバ・ケーブルなどの永久的接続、又は、電話若しくは無線通信を介して形成される一時的接続を含むものとすることができる。図示される例においては、サーバ１０２及びサーバ１０３は、記憶ユニット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、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）などといった様々なコンピュータ装置によって表される。分散データ処理システム１００は、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。

【００４３】

図示される例においては、分散データ処理システム１００は、ライトウェイト・ディレクトリ・アクセス・プロトコル（ＬＤＡＰ；Ｌｉｇｈｔｗｅｉｇｈｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）、転送制御プロトコル／インターネット・プロトコル（ＴＣＰ／ＩＰ；Ｔｒａｎｓｐｏｒｔ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ；ＨｙｐｅｒＴｅｘｔ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ）、無線アプリケーション・プロトコル（ＷＡＰ；Ｗｉｒｅｌｅｓｓ Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）などといった、相互に通信するための様々な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）といった、多数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、無線通信リンクを取り入れたネットワーク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に接続され、ＰＤＡ１１３は、無線リンク１１４を介してネットワーク１１０に接続される。電話１１１及びＰＤＡ１１３は、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を介してデータを両者間で直接転送し、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もできる。同様に、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。本発明は、様々なハードウェア・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、異機種コンピューティング環境の一例であって、本発明のアーキテクチャ上の制限として意図されるものではない。

【００４４】

ここで図２を参照すると、図面は、図１に示されるような、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つ又はそれ以上の中央処理装置（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）と、読取専用メモリ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ていない他の装置などの、様々なＩ／Ｏ装置に対応する入力／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へのアクセスを可能にする通信アダプタ１３４を接続する。ユーザ・インタフェース・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、マイクロホンなどのような図示されていない他の装置などの、様々な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をディスプレイ装置１４６に接続する。

【００４５】

当業者であれば、図２のハードウェアはシステム実装形態に応じて変わる場合があ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つ又はそれ以上のプロセッサと、１つ又はそれ以上の種類の揮発性メモリ及び不揮発性メモリとを備え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、又はその代わりに、他の周辺装置を用いることができる。図示される例は、本発明に対する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。

【００４６】

本発明は、様々なハードウェア・プラットフォーム上に実装することができるのに加えて、様々な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、ある装置はＵｎｉｘ（商標）オペレーティング・システムを作動させることができるが、別の装置は簡単な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、図形ファイル、文書処理ファイル、拡張可能マークアップ言語（ＸＭＬ；ｅＸｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）、ハイパーテキスト・マークアップ言語（ＨＴＭＬ；ＨｙｐｅｒＴｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）、携帯装置マークアップ言語（ＨＤＭＬ；Ｈａｎｄｈｅｌｄ Ｄｅｖｉｃｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）、無線マークアップ言語（ＷＭＬ；Ｗｉｒｅｌｅｓｓ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）、並びに、他の様々なフォーマット及びタイプのファイルなどといった、様々なフォーマット及び言語の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。

【００４７】

本明細書の図面の説明は、ユーザ装置又は装置のユーザのいずれかによる特定の行為に関わるものである。当業者であれば、クライアントとの間の応答及び／又は要求が、ある場合にはユーザによって開始され、他の場合にはクライアントのユーザに代わることが多い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、図面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に言及するときは、「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、交換可能に用いられる場合があることを理解すべきである。

【００４８】

本発明は、図１及び図２に関して上述されたように、様々なハードウェア及びソフトウェア・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、より特定的には、本発明は、デジタル証明書を用いる改善された認証操作に向けられる。改善された認証サービスをより詳細に説明するのに先立って、非対称暗号鍵及びデジタル証明書の使用を説明する。

【００４９】

デジタル証明書は、通信又はトランザクションに関与する各々のパーティが、公開鍵及び秘密鍵と呼ばれる鍵のペアを有する公開鍵暗号に対応する。各々のパーティの公開鍵は公開されるが、秘密鍵は秘密に保たれる。公開鍵は、特定のエンティティに関連する数字であり、そのエンティティと信用できる対話を持つ必要があるすべての人に知られるように意図されるものである。秘密鍵は、特定のエンティティにのみ知られることを前提とする、すなわち秘密に保たれる数字である。典型的な非対称暗号システムにおいて、秘密鍵は、厳密に１つの公開鍵に対応する。

【００５０】

公開鍵暗号システムにおいては、すべての通信は公開鍵のみを伴い、秘密鍵は決して送信又は共有されないため、機密メッセージは、公開情報のみを用いて生成し、対象とする受信者が占有する秘密鍵のみを用いて復号することができる。さらに、公開鍵暗号は、暗号化によるプライバシのためだけでなく、電子署名による認証のために用いることができる。暗号化は、秘密復号鍵なしには誰も読み取ることができない形式へのデータ変換であり、すなわち、暗号化は、情報のコンテンツを、暗号化されたデータを見ることはできても対象ではないすべての人から隠された状態に維持することによって、プライバシを保証する。認証は、デジタル・メッセージの受信者が送信者の同一性及び／又は該メッセージ

の完全性を確信することができる処理である。

【００５１】

例えば、送信者がメッセージを暗号化するときは、受信者の公開鍵を用いて、オリジナル・メッセージ内のデータを暗号化されたメッセージの内容に変換する。送信者は、対象とする受信者の公開鍵を用いてデータを暗号化し、受信者は、その秘密鍵を用いて、該暗号化されたメッセージを復号化する。

【００５２】

データを認証するときは、署名者の秘密鍵を用いてデータから電子署名を計算することによって、該データに署名することができる。データが電子署名されると、データは、署名者の身元と、該データが該署名者から送出されたことを証明する署名と共に、格納することができる。署名者は、その秘密鍵を用いてデータに署名し、受信者は、該署名者の公開鍵を用いて署名を検証する。

【００５３】

証明書は、個人、コンピュータ・システム、そのシステム上で作動する特定のサーバなどのようなエンティティの同一性及び鍵所有権について保証するデジタル文書である。証明書は、認証局によって発行される。認証局（ＣＡ）は、他の人々又はエンティティのために証明書に署名するか、又はそれを発行することを委託された、通常はトランザクションに対して信用できるサード・パーティであるエンティティである。ＣＡは、通常は、証明書に署名したエンティティを信用することを可能にする公開鍵とその所有者との間のバインディングの保証について、何らかの種類の法的責任を有する。このような商業用の認証局が多く存在する。これらの認証局は、証明書を発行するときに、エンティティの同一性及び鍵所有権を確認する責任がある。

【００５４】

認証局がエンティティに対して証明書を発行する場合には、該エンティティは、公開鍵と該エンティティについての幾つかの情報を提供しなければならない。特別に装備されたウェブ・ブラウザなどのソフトウェア・ツールは、この情報に電子署名し、それを認証局に送信することができる。認証局は、信用できるサード・パーティの認証局サービスを提供する会社である。次いで、認証局は、証明書を生成し、それを戻すことになる。証明書は、シリアル番号及び該証明書が有効な日付などといった他の情報を含むことができる。認証局により提供される値の一部は、様々な認証サービス実務（ＣＳＰ）において公に公開されている検証要件に部分的に基づく、中立的で信用できる紹介サービスとして機能することになる。

【００５５】

ＣＡは、要求するエンティティの公開鍵を他の識別情報と共に埋め込み、次いで該ＣＡの秘密鍵を用いてデジタル証明書に署名することによって、新たなデジタル証明書を作成する。次いで、トランザクション又は通信の間にデジタル証明書を受信する誰もが、ＣＡの公開鍵を用いて、該証明書内の署名された公開鍵を検証することができる。その目的は、ＣＡの署名がデジタル証明書上の不正防止シールとして機能し、これにより該証明書のデータの完全性を保証することである。

【００５６】

証明書処理の他の態様も標準化されており、Ｘ．５０９公開鍵基盤（ＰＫＩＸ）に関するさらなる情報を、ｗｗｗ．ｉｅｔｆ．ｏｒｇのＩｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ（ＩＥＴＦ）から入手することができる。例えば、証明書要求メッセージ・フォーマット（ＲＦＣ２５１１）は、信頼するパーティがＣＡからの証明書を要求するときにはいつでも用いるために推奨されるフォーマットを指定する。証明書を転送するための証明書管理プロトコルも公表されている。本発明は、デジタル証明書を処理する分散データ処理システムにあるため、図３及び図４を用いて、デジタル証明書に関する幾つかの有用な背景情報を示す。

【００５７】

ここで図３を参照すると、ブロック図は、個人がデジタル証明書を取得する典型的な方

法を示す。何らかのタイプのクライアント・コンピュータを通して操作しているユーザ１５２は、公開／秘密鍵のペア、例えばユーザ公開鍵１５４及びユーザ秘密鍵１５６をあらかじめ取得又は生成している。ユーザ１５２は、ユーザ公開鍵１５４を含む証明書１５８についての要求を生成し、該要求を、ＣＡ公開鍵１６２及びＣＡ秘密鍵１６４を所有する認証局１６０に送信する。認証局１６０は、何らかの方法でユーザ１５２の同一性を検証し、ユーザ公開鍵１５４を含むＸ．５０９デジタル証明書１６６を生成する。証明書全体は、ＣＡ秘密鍵１６４を用いて署名され、該証明書は、ユーザの公開鍵、該ユーザに関連する名前、及び他の属性を含む。ユーザ１５２は、新たに生成されたデジタル証明書１６６を受信し、次いでユーザ１５２は、信用できるトランザクション又は信用できる通信を行うために、必要に応じてデジタル証明書１６６を提示することができる。ユーザ１５２からデジタル証明書１６６を受信するエンティティは、検証するエンティティが使用可能な（又は取得可能な）、認証局の公開鍵証明書において公開されるＣＡ公開鍵１６２を用いることによって、ＣＡの署名を検証することができる。

【００５８】

ここで図４を参照すると、ブロック図は、エンティティがデジタル証明書を用いてインターネット・システム又はアプリケーションに認証される典型的な方法を示す。ユーザ１７２は、ホスト・システム１７８上のアプリケーション１７６に送信される（又はそれによって取得可能である）Ｘ．５０９デジタル証明書１７４を所有し、アプリケーション１７６は、デジタル証明書を処理し、使用するためのＸ．５０９機能を備える。ユーザ１７２は、秘密鍵を用いて、アプリケーション１７６に送信するデータに署名するか、又はそれを暗号化する。

【００５９】

証明書１７４を受信又は取得するエンティティは、アプリケーション、システム、サブシステムなどとすることができる。証明書１７４は、ユーザ１７２のために何らかのタイプのサービスを行うことができるアプリケーション１７６に対してユーザ１７２を識別する主体者名又は主体者識別子を含む。証明書１７４を用いるエンティティは、ユーザ１７２からの署名又は暗号化されたデータに対して該証明書を用いる前に、該証明書の信頼性を検証する。

【００６０】

ホスト・システム１７８はまた、ユーザ１７２にシステム１７８内のサービス及びリソースにアクセスする権限を与える、すなわち、ユーザの身元をユーザ特権と照合するのに用いられるシステム・レジストリ１８０を含むことができる。例えば、システム管理者は、ユーザの身元を特定のセキュリティ・グループに属するように構成することができ、該ユーザは、該セキュリティ・グループ全体が利用可能であるように構成されるリソースのみにアクセスできるように制限される。このシステムにおいては、認証スキームを課すための様々な周知の方法を利用することができる。

【００６１】

従来技術に関して既述したように、デジタル証明書を適切に確認するために、アプリケーションは、該証明書が取り消されたどうかを調べなければならない。認証局が証明書を発行するときは、認証局は、該証明書を識別する固有のシリアル番号を生成し、このシリアル番号は、Ｘ．５０９証明書内の「シリアル番号」フィールドに格納される。典型的には、取り消されたＸ．５０９証明書は、該証明書のシリアル番号によってＣＲＬ内で識別される、すなわち、取り消された証明書のシリアル番号は、ＣＲＬ内のシリアル番号のリストに現れる。

【００６２】

証明書１７４が依然として有効であるかどうかを判断するために、アプリケーション１７６は、証明書取り消しリスト（ＣＲＬ）をＣＲＬレポジトリ１８２から取得し、該ＣＲＬを確認する。アプリケーション１７６は、取得したＣＲＬ内のシリアル番号のリストと証明書１７４内のシリアル番号を比較し、一致するシリアル番号が存在しない場合には、該アプリケーション１７６は、証明書１７４を有効にする。ＣＲＬが一致するシリアル番

号を持つ場合には、証明書１７４は拒否されるべきであり、アプリケーション１７６は、あらゆるコントローラ・リソースへのアクセスに対するユーザの要求を拒否する適切な手段をとることができる。

【００６３】

ここで図５を参照すると、ブロック図は、ネットワークを介してネットワーク及びグリッドにアクセスするユーザ装置を含む典型的なデータ処理システムを示す。ユーザ装置２００は、ネットワーク・アクセス装置２０４を介してネットワーク２０２上のデータを送受信する。ユーザ装置２００は、図１に示されるクライアント１０５～１０７と同様であり、一方、ネットワーク２０２は、図１のネットワーク１０１と同様である。ネットワーク・アクセス装置２０４は、ネットワーク・アクセス・サーバ、Ｅｔｈｅｒｎｅｔ（商標）スイッチ、無線アクセス・ポイント、又は、遠隔認証ダイヤルイン・ユーザ・サービス（ＲＡＤＩＵＳ）プロトコル若しくは接続を認証及び許可するための同様のプロトコルを作動させることができる他のタイプのネットワーク・アクセス装置とすることができる。

【００６４】

ネットワーク・アクセス認証サーバ２０６は、適切なプロトコルを用いて、ユーザがネットワークに接続することを認証及び許可する要求を処理する、すなわち、好ましい実施形態においては、サーバ２０６はＲＡＤＩＵＳプロトコルに対応するものであり、この場合には、ネットワーク・アクセス装置２０４はＲＡＤＩＵＳクライアントとみなされ、ユーザ装置２００はアクセス・クライアントとみなされることになる。サーバ２０６は、様々なエンティティ、例えば、デスクトップ・コンピュータなどの多くのアクセス・クライアントを運用する企業、又はアクセス・クライアントを操作する個人ユーザにそのサービスを販売するインターネット・サービス・プロバイダ（ＩＳＰ）が、運用することができる。

【００６５】

サーバ２０６は、データベース又は他のタイプのデータストアとすることができるユーザ・レジストリ２０８内にユーザ情報を格納し、それを取り出す。ユーザ・レジストリ２０８は、各々のユーザについて、サーバ２０６によってネットワーク・アクセスが制御されることになるアカウント情報を格納する。サーバ２０６の運用のためのシステム管理者が、各々のユーザについて登録操作を完了するものと仮定することができる。ユーザ・レジストリ２０８は、ユーザ装置２００を操作する特定のユーザについてのアカウント情報２１０を含むように示されているが、他のユーザについてのアカウント情報をユーザ・レジストリ２０８内に格納することもでき、アカウント情報２１０は、その特定のユーザのユーザ名２１２及びパスフレーズ２１４を含む。

【００６６】

サーバ２０６がＲＡＤＩＵＳプロトコルに従って動作しているものとすると、ユーザ装置２００は、以下の単純な例において、ネットワーク２０２にアクセスすることができる。ユーザ装置２００は、例えば、次にダイヤルアップ・ネットワーク・プログラムを自動的に起動するウェブ・ブラウザ・アプリケーションをユーザ装置２００のユーザが起動するのに応答して、ネットワーク・アクセス装置２０４を用いてポイント・ツー・ポイント・プロトコル（ＰＰＰ）認証操作を開始する。ネットワーク・アクセス装置２０４は、ユーザ名及びパスフレーズについての要求に応答し、ユーザ装置２００は、ユーザからユーザ名及びその関連するパスフレーズを取得し、その値のペアをネットワーク・アクセス装置２０４に戻し、ネットワーク・アクセス装置２０４は、該ユーザ名及びパスフレーズをＲＡＤＩＵＳサーバ２０６に送信する、すなわち、該パスフレーズは、処理全体を通して適切な暗号化によって保護されるものと仮定することができる。ＲＡＤＩＵＳサーバ２０６は、受信したユーザ名／パスフレーズの組み合わせをユーザ・レジストリ２０８内の情報を用いて確認し、受け入れ応答又は拒否応答によって応答する。ユーザ情報が正常に確認されたと仮定すると、ＲＡＤＩＵＳサーバ２０６は、例えばユーザ装置２００に割り当てられるＩＰアドレスなどのセッションのために用いられるパラメータを記述する属性－値のペアのリストといった、サービスをユーザ装置２００に提供するのに必要な設定情報

を、ネットワーク・アクセス装置２０４に戻す。ネットワーク・アクセス装置２０４は、情報をユーザ装置２００に戻し、ユーザ装置２００は、データをネットワーク２０２上に伝送するデータ・トラフィックをネットワーク・アクセス装置２０４に送信し始める。

【００６７】

ネットワーク２０２内のサービスにアクセスする必要がある場合は、ユーザ装置２００上で実行するアプリケーションは、関連するユーザ公開鍵証明書２２０と共に保護された形式のユーザ秘密鍵２１８を格納するクライアント・データストア２１６にアクセスすることができ、ユーザ秘密鍵２１８は、パスフレーズ２１４又は他の何らかの秘密情報を用いて暗号化するか、又は他の何らかの手段によって保護することができる。ユーザ装置２００は、ウェブ・ブラウザ・アプリケーションなどの多くの異なる種類のアプリケーションに対応するものとすることができ、クライアント・データストア２１６は、様々なアプリケーション内部の、又はそれらによって制御される記憶域を含む、様々な異なる形式の１つ又はそれ以上のデータストアとして実装することができる。

【００６８】

ユーザ装置２００はまた、グリッド・クライアント・アプリケーション２３０、すなわち、グリッド２３４内のサービス／リソース２３２を要求するか又はそれにアクセスすることが可能なクライアント・アプリケーションに対応するものであり、すなわち、グリッド・クライアント・アプリケーション２３０の形式を、例えば独立型プログラム、アプレット、又は何らかの形式のソフトウェア・モジュールといったものに変えることができる。上述のように、グリッドは、個々のコンピュータ上では局所的な自律制御を維持しながら計算能力及びデータストア能力を全体で共有するための、多くのコンピュータについての論理／仮想編成である。グリッドが１つ又はそれ以上のネットワーク内の物理的にサポートされた要素の仮想編成であり、ネットワーク２０２が（インターネットを含むことができる）１つ又はそれ以上のネットワークを表すため、グリッド２３４は、図５においてはネットワーク２０２内のリソースの一部として示される。

【００６９】

本発明の好ましい実施形態においては、グリッド・クライアント・アプリケーション２３０は、Ｇｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）に従って作動し、その態様は簡単に後述される。ジョブは、「ｇｌｏｂｕｓｒｕｎ」コマンドの使用によってグリッドにサブミットされ、各々のジョブには、ユーザ又はグリッド・クライアントを認証するのに用いられるＸ．５０９プロキシ証明書が添付される。したがって、プロキシ証明書は、ジョブをグリッド上で実行することが可能になる前に生成されなければならない。

【００７０】

グリッド・クライアントによってプロキシ証明書がグリッド・サービスに伝送されるときは、該グリッド・クライアントは、他のグリッド・サービスに許可されるよう、あたかもグリッド・クライアントであるかのようにグリッド・サービスに権利を与える。ジョブがグリッド内で処理されるときは、多数のサービスをトリガーして、サブミットされたジョブの処理を支援することができる。プロキシ証明書がグリッド内でジョブに添付されるため、プロキシ証明書によってグリッド内でのシングル・サインオン操作が容易になり、認証チャレンジは、グリッド・リソース又はサービスへのアクセス毎に生成されない。

【００７１】

プロキシ証明書は、典型的には数時間のオーダーの限られた存続時間を持つ短期セッションの証明書である。特定のプロキシ証明書は特定の公開鍵証明書に基づくものであり、公開鍵証明書内で識別される主体者がプロキシ証明書を生成することができる。公開鍵証明書内の特定の公開鍵に対応する秘密鍵を用いてプロキシ証明書に電子署名し、これにより、以下により詳細に説明されるように、該プロキシ証明書をＸ．５０９証明書の使用に内在する階層的信用パスに従って確認することが可能になる。

【００７２】

図５に示される例においては、グリッド認証局（ＣＡ）２３６が、例えば図３及び図４について上述されたものと同じ方法で、グリッド２３４内で証明書を用いるユーザに証明

書を発行する。代替的な実施形態においては、例えば、グリッド２３４に対応する組織に加えて他の組織についての証明書を発行することを委託されたサード・パーティのベンダといった、グリッドから独立した異なるＣＡを利用することができる。しかしながら、グリッド２３４においてシングル・サインオン操作の恩恵を被るために、グリッド２３４内のすべてのリソースがＣＡ２３６などの所与のＣＡを信用することを前提とすべきである。換言すれば、グリッドＣＡ２３６は、グリッド２３４に関してルートＣＡであると考えられる。しかしながら本発明に関しては、公開鍵証明書２２０のユーザ／主体者及びグリッド・リソース／サービス２３２の両方がグリッドＣＡ２３６を信用すると仮定すれば十分である。

【００７３】

公開鍵証明書２２０は、その秘密鍵を用いてＣＡ２３６によって署名された。一般に、ユーザ装置２００が、トランザクション要求メッセージをサービス２３２に送信することによってサービス２３２とのトランザクションを開始するときは、ユーザ装置２００は、その秘密鍵２１８を用いてトランザクション関連メッセージに署名する。ユーザ装置２００が、公開鍵証明書２２０のコピーをトランザクション関連メッセージと共にサービス２３２に伝送するか、又は、サービス２３２が、ＬＤＡＰディレクトリなどの既知の場所から公開鍵証明書２２０のコピーを取得することができる。サービス２３２は、トランザクション関連メッセージに署名するのに用いられた秘密鍵２１８に対応する、公開鍵証明書２２０内の公開鍵を用いて、該トランザクション関連メッセージ上の電子署名を確認する。

【００７４】

同様に、サービス２３２は、公開鍵証明書２２０に署名するのに使用されたＣＡの秘密鍵に対応する、ＣＡ２３６の公開鍵証明書のコピーにおける公開鍵を用いて、公開鍵証明書２２０の受信又は取得されたコピーの信頼性を確認する。サービス２３２が既知の場所からＣＡ２３６の公開鍵証明書２２０のコピーを取得するか、又はＣＡ２３６の公開鍵証明書２２０のコピーがトランザクション関連メッセージと共に伝送されることもあり、ユーザ装置２００は、ＣＡ公開鍵証明書２３８のコピーを格納することができる。このようにして、信用、信用パス、又は証明書パスのいわゆる階層チェーンが形成され、必要に応じて、ルートＣＡまで信用パスを進んで確認を行うことができる。サービス２３２は暗黙的にＣＡ２３６を信用するため、サービス２３２は、トランザクション関連メッセージを、公開鍵証明書２２０内で識別される主体者によって生成されたことが確実なものとして信用すると考えられる。

【００７５】

同様に、ユーザ装置２００は、秘密鍵２１８を用いて署名されるプロキシ証明書２４０を生成する認証局として機能することができ、生成されたプロキシ証明書は、固有名と、非対称暗号鍵ペアの公開鍵とを含む。プロキシ証明書２４０がユーザ装置２００によってサービス２３２に伝送されたときは、サービス２３２は、公開鍵証明書２２０と、ＣＡ公開鍵証明書２３８と、必要に応じて信用パスにおける他の証明書とを用いて、プロキシ証明書２４０の信用パスを確認することができる。プロキシ証明書２４０の性質により、サービス２３２は、他のサービスに対してユーザ装置２００の代わりのプロキシとして機能することができる。

【００７６】

上述のように、グリッド・クライアント・アプリケーション２３０は、本発明の好ましい実装形態においてはＧｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）に従って作動し、プロキシ証明書は、Ｇｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（登録商標）を用いてジョブをグリッド上で実行することが可能となる前に生成されなければならない。「ｇｒｉｄ－ｐｒｏｘｙ－ｉｎｉｔ」コマンドはプロキシ証明書を生成し、該プロキシ証明書は特定のファイルに格納される。１つの実装形態においては、ファイルは、ファイル名が「ｘ５０９ｕｐ＿ｕ＜ｕｉｄ＞」であり、ユーザ識別子が「ｇｒｉｄ－ｐｒｏｘｙ－ｉｎｉｔ」コマンドを実行しているユーザに関連するパス名「／ｔｍｐ／＜ｆｉｌｅｎａｍｅ＞」に格納される。このフ

ァイルは、プロキシ証明書の対応する秘密鍵及び該プロキシ証明書が基づいている公開鍵証明書のコピーと共に、該プロキシ証明書を格納する。

【００７７】

プロキシ証明書に電子署名するのに用いられるユーザの秘密鍵は、異なるファイル内に暗号化された状態のまま残され、１つの実装形態においては、該秘密鍵は、「＄ＨＯＭＥ／．ｇｌｏｂｕｓ／ｕｓｅｒｋｅｙ．ｐｅｍ」ファイルに格納される。秘密鍵は、ユーザのグリッド・パスフレーズを用いてアクセスすることが可能であり、１つの実装形態においては、このパスフレーズは、ユーザの公開鍵証明書が「ｇｒｉｄ－ｃｅｒｔ－ｒｅｑｕｅｓｔ」コマンドの使用を通じてグリッド認証局によって生成されたときに該ユーザによって設けられたものと同じパスフレーズである。

【００７８】

したがって、ユーザがグリッド・クライアント・アプリケーション２３０を作動させるときは、グリッド・クライアント・アプリケーション２３０は、特定のファイルに格納されているプロキシ証明書を使用する、すなわち、「ｇｒｉｄ－ｐｒｏｘｙ－ｉｎｉｔ」は、プロキシ証明書を生成するために前もって実行されているはずである。「ｇｌｏｂｕｓｒｕｎ」コマンドが呼び出されるときには、実行ルーチンは、グリッド内にサブミットされるジョブに添付するプロキシ証明書を取り出すファイル場所を分かっている。

【００７９】

上述のように、プロキシ証明書の使用を通じて実装されるグリッドのシングル・サインオン機能は、グリッド内のリソースに適用されるのみである。したがって、ユーザは、ネットワーク・アクセス認証サーバを通じてネットワークに対する認証操作を完了した後に、グリッド・クライアント・アプリケーションによってグリッドに対する別の認証操作を完了することに取り組むことになる。したがって、従来技術においては、ユーザは典型的には、グリッド内のリソースにアクセスする２つの認証チャレンジを通過する必要があり、これは、シングル・サインオン操作の概念に反し、シングル・サインオン機能をグリッド基盤に組み込む取り組みを減少させるものである。本発明は、この問題に対する解決策を提供する。

【００８０】

ここで図６を参照すると、ブロック図は、本発明の実施形態に従って、ネットワーク及びグリッドにアクセスするユーザ装置を含むデータ処理システムを示す。図６は図５に類似するものであり、同じ要素数字は、同じ機能を指す。しかしながら、図６の例においては、ユーザ・レジストリ内のユーザ・アカウント情報が、各グリッド・ユーザの保護された秘密鍵２１８及び公開鍵証明書２２０のコピーを含むように変更されている。さらに、図６におけるネットワーク・アクセス認証サーバ及びユーザ装置は、付加的な機能を含むように変更されている。図６においては、ネットワーク・アクセス認証サーバ２５０は、グリッド・プロキシ証明書生成器２５２を含み、ユーザ装置２６０は、修正されたダイヤルアップ・プログラム２６２を含む。修正されたアカウント情報及び付加的な機能を利用する方法を、さらにより詳細に説明する。

【００８１】

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従ってグリッド関連情報をユーザ・レジストリ内に確立するための処理を示す。処理は、ＲＡＤＩＵＳサーバなどのネットワーク・アクセス認証サーバによって用いられるユーザ・レジストリ・データベース内にユーザ・アカウントを確立する典型的なユーザ登録操作で開始し（ステップ３０２）、このユーザ登録操作は、図５に示されるデータ処理システム内で必要とされるユーザ登録操作と実質的に同様である。続いて、ネットワーク・アクセス認証サーバは、ユーザ・レジストリを用いて、ユーザがネットワークへのアクセスを許可されるべきかどうかを判断する。

【００８２】

しかしながら、図５に示されるデータ処理システムとは対照的に、図６に示されるデータ処理システムは、特定のユーザが本発明の利益を得ることになる場合には、その特定の

ユーザのアカウント情報内に付加的な情報を格納することが必要である。したがって、ユーザ登録操作の際に、ユーザの秘密鍵及びユーザの公開鍵証明書もまた、ユーザの他のアカウント情報と関連して格納され（ステップ３０４）、これで、修正された登録処理を完了する。ユーザの秘密鍵は、何らかの方法で、例えばユーザのパスフレーズを用いて暗号化することによって、保護されることが好ましいであろう。これらのデータ項目は、帯域外処理を通じてアカウント登録器に転送することができ、例えば、システム管理者が、ユーザから直接該ユーザの秘密鍵及び該ユーザの公開鍵証明書を取得する責任を負うことになる。

【００８３】

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従って、ネットワーク・アクセスのための認証操作をグリッド・アクセスのための認証操作と統合してネットワーク及びグリッドの複合型シングル・サインオン操作を提供するためのサーバ側の処理を示す。図８は、サーバ上で行われるシングル・サインオン操作のための処理の一部を示し、一方、図９は、ユーザ装置上で行われるシングル・サインオン操作のための処理の一部を示す。処理は、ネットワーク・アクセス認証サーバがネットワーク・アクセス認証操作を実行することから開始する（ステップ４０２）。ユーザが正常に認証されるものと仮定し、そうでない場合には、適切な拒否応答が戻されることになる。例えば、図６に示されるようなグリッド・プロキシ証明書生成器機能などの拡張機能を有するＲＡＤＩＵＳサーバは、図５に関して上述されたように、ＲＡＤＩＵＳプロトコルに従って認証操作を実行する。

【００８４】

しかしながら、正常認証についてのネットワーク・アクセス・パラメータを戻す前に、ネットワーク・アクセス認証サーバは、例えばユーザ・アカウント・レジストリからのコピーなどの、ユーザの秘密鍵のコピーとユーザの公開鍵証明書のコピーとを取得し（ステップ４０４）、ユーザの秘密鍵が保護されている場合には、ユーザの秘密鍵の暗号化されたコピーは復号化される。ユーザのアカウント情報は、例えば図７に示される処理の完了によって、ユーザの秘密鍵のコピーとユーザの公開鍵証明書のコピーとを含むものと仮定するが、ステップ４０４及び４０６は、グリッドにアクセスしない一部のユーザが存在する場合には、選択的な方法で制御することができる。例えば、ユーザのアカウント情報は、ユーザが統合型ネットワーク・グリッドのシングル・サインオン操作の必要性を有するグリッド・ユーザであるかどうかを示す値を含むことができる。

【００８５】

ユーザがグリッドへのアクセスを必要とすると仮定すると、ネットワーク・アクセス認証サーバは、上述と同様の方法でプロキシ証明書を生成し（ステップ４０６）、該プロキシ証明書は、ユーザの公開鍵証明書からコピーされた何らかの情報、例えば「Ｓｕｂｊｅｃｔ」識別子を含み、該プロキシ証明書は、ユーザの秘密鍵を用いて電子署名される。次いで、ネットワーク・アクセス認証サーバは、ネットワーク・アクセス・パラメータと共にプロキシ証明書を戻し（ステップ４０８）、これによって統合型認証処理を終了する。例えば、図６に示されるようなグリッド・プロキシ証明書生成器機能などの拡張機能を有するＲＡＤＩＵＳサーバは、ベンダがＲＡＤＩＵＳプロトコル内の拡張属性に対応できるようにするベンダ特有の属性（ＶＳＡ；ｖｅｎｄｏｒ－ｓｐｅｃｉｆｉｃ　ａｔｔｒｉｂｕｔｅｓ）の中にプロキシ証明書を戻すことができる。

【００８６】

ここで図９を参照すると、フローチャートは、本発明の実施形態に従い、ネットワーク・アクセスのための認証操作をグリッド・アクセスのための認証操作と統合してネットワーク及びグリッドの複合型シングル・サインオン操作を提供するためのクライアント側の処理を示す。処理は、ユーザ装置が、ネットワークにアクセスしようとすると同時に、ネットワーク・アクセス認証操作を開始し、それに関与することから始まる（ステップ５０２）。

【００８７】

その後のいずれかの時点で、ネットワーク・アクセス認証サーバからネットワーク・アクセス・パラメータの組が戻され、ユーザ装置は、それを、ネットワーク上で通信するための適切なネットワーク・パケットを生成する際に用いるために格納する。ユーザ装置上には、修正されたダイヤルアップ・プログラムが既に構成されており、該修正されたダイヤルアップ・プログラムは、ネットワーク・アクセス認証操作に関わるものであり、該修正されたダイヤルアップ・プログラムは、戻されたネットワーク・アクセス・パラメータを処理する。ネットワーク・アクセス・パラメータが戻される際に、修正されたダイヤルアップ・プログラムは、プロキシ証明書の存在を検出する（ステップ５０４）。変更されたダイヤルアップ・プログラムは、プロキシ証明書を抽出し、それをユーザ装置上の適切なファイルに格納し（ステップ５０６）、これによって処理を終了する。例えば、Ｇｌｏｂｕｓ　Ｔｏｏｌｋｉｔ（商標）を用いるアプリケーションがユーザ装置に構成されている場合には、修正されたダイヤルアップ・プログラムは、プロキシ証明書を含むファイルを生成する。

【００８８】

本発明においては、典型的なユーザ装置及び典型的なネットワーク・アクセス認証サーバを、プロキシ証明書の転送を受け入れるように修正した。本発明の異なる実施形態においては、プロキシ証明書がネットワーク・アクセス認証サーバからユーザ装置に伝送される方法を変えることができる。本発明の好ましい実施形態においては、ユーザ装置及びネットワーク・アクセス認証サーバは、後述の機能に対応する。

【００８９】

ユーザ装置は、Ｂｌｕｎｋらによる「ＰＰＰ　Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（ＥＡＰ）」、ＲＦＣ２２８４、Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ（ＩＥＴＦ）、１９９８年3月、の中で定義されている、（ポイント・ツー・ポイント・プロトコル（ＰＰＰ）に関連し、ＥＡＰと略される）ＰＰＰ拡張可能認証プロトコル（Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を用いてネットワーク・アクセス装置と通信する。ＲＦＣ２２８４の中で記述されるように、ＰＰＰは、ポイント・ツー・ポイント・リンク上でマルチ・プロトコル・データグラムを転送するための標準的な方法を提供する。ポイント・ツー・ポイント・リンク上で通信を確立するために、ＰＰＰリンクの各々の端末は、まずリンク制御プロトコル（ＬＣＰ；Ｌｉｎｋ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）パケットを送信して、リンク確立フェーズの間にデータ・リンクを構成しなければならない。リンクが確立された後、ＰＰＰは、ネットワーク層プロトコル・フェーズに移る前に任意の認証フェーズを準備する。デフォルト設定では認証は必須ではないが、リンクの認証が求められる場合には、実装形態では、リンク確立フェーズの間に認証プロトコル設定オプション（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ－Ｐｒｏｔｏｃｏｌ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｏｐｔｉｏｎ）を指定しなければならず、ＥＡＰが、特定の認証プロトコルを定める。接続認証フェーズに到達すると、エンドポイント装置（「ピア」と呼ばれることもある）は、ＥＡＰタイプとして知られる特定のＥＡＰ認証スキームの使用をネゴシエートする。

【００９０】

ＥＡＰは、要求パケット及び応答パケットを定め、各々の要求は、どの情報が要求されているかを示すタイプ・フィールドを有する。ＥＡＰは、要求／応答交換に用いられる初期ＥＡＰタイプの組を定める。ＥＡＰタイプについて取り決められると、ＥＡＰは、ユーザ装置（アクセス・クライアント）と、接続のパラメータ及び必要性に基づいて変わる場合があるネットワーク・アクセス認証サーバ（例えば、ＲＡＤＩＵＳサーバ）との間において、メッセージの制約のない交換を可能にする。エンドポイント間の対話は、認証情報及び応答についての一連の要求からなる。

【００９１】

本発明は、典型的にはユーザ入力を必要とする一般的なトークン・カードに対応するために用いられるＥＡＰ定義「タイプ６」を使用することができる。要求は、典型的には、

ＡＳＣＩＩテキスト・メッセージを含む。応答は、典型的には、認証に必要なトークン・カード情報を含み、典型的には、これは、ユーザによってトークン・カード装置から読み出され、次いでＡＳＣＩＩテキストとして入力される情報である。

【００９２】

好ましい実施形態においては、認証情報（ユーザ名／パスフレーズ）がユーザ装置から要求され、該ユーザ装置から受信された後に、プロキシ証明書は、プロキシ証明書を保持するのに十分な最大６４キロバイトの可変長を有することができる「タイプ６」のＥＡＰ要求としてユーザ装置に転送され、該プロキシ証明書は、ＵＵエンコーディングなどの様々なアルゴリズムに従って全ＡＳＣＩＩテキスト文字列に変換することができる。

【００９３】

このように、このデータ・フィールドは、ＥＡＰ仕様書によって予定されているもの以外のデータ・ペイロードを運ぶように「オーバーロード」される。したがって、ユーザからのＥＡＰ応答のコンテンツは、確認通知又は種々のダミー・データなどの様々な情報を持つことができる。

【００９４】

ＥＡＰは、両方のエンドポイントにおいて認証プラグイン・モジュールを受け入れるように設計され、それにより、機会を有するベンダが新しい認証スキームを提供することが可能になる。ユーザ装置上の修正されたダイヤルアップ・プログラムは、オーバーロードされた「タイプ６」のＥＡＰ要求を認識し、ＡＳＣＩＩテキストのコンテンツ・ペイロードを抽出する、すなわち、該プログラムは必要に応じて、例えばＵＵデコーディング・アルゴリズムによってＡＳＣＩＩテキストを変換して、プロキシ証明書を取得し、次いで、それを適切な場所に、例えば上述のグリッド・クライアント・アプリケーションによって用いられるファイルに格納する。

【００９５】

ネットワーク・アクセス装置は、単に認証パケットの内容を転送するのみであり、したがって、該ネットワーク・アクセス装置は、プロキシ証明書が転送される方法には影響を受けない。ＲＡＤＩＵＳプロトコルを実装する本発明の好ましい実施形態においては、ネットワーク・アクセス装置は、該ネットワーク・アクセス装置を介してあらゆるＥＡＰタイプのＥＡＰメッセージをＲＡＤＩＵＳサーバに受け渡すことである、いわゆる「ＥＡＰ ｏｖｅｒ ＲＡＤＩＵＳ」に対応する。アクセス・クライアント（ユーザ装置）とＲＡＤＩＵＳサーバとの間で送信されるＥＡＰメッセージは、「ＥＡＰメッセージ」属性としてフォーマットされ、ＲＡＤＩＵＳメッセージに入れてネットワーク・アクセス装置とＲＡＤＩＵＳサーバとの間で送信される。したがって、ネットワーク・アクセス装置は、アクセス・クライアントとＲＡＤＩＵＳサーバとの間でＥＡＰメッセージを受け渡すパススルー装置となり、ＥＡＰメッセージの処理は、ネットワーク・アクセス装置ではなく、アクセス・クライアント及びＲＡＤＩＵＳサーバにおいて行われる。

【００９６】

ネットワーク・アクセス装置は単に、認証プロトコルであるＥＡＰのネゴシエーションと、ＲＡＤＩＵＳサーバへのＥＡＰメッセージの受け渡しとに対応する必要があるのみであり、これは、多くの市販されているネットワーク・アクセス装置によって提供される機能である。「ＥＡＰメッセージ」属性は、Ｒｉｇｎｅｙらの「ＲＡＤＩＵＳ Ｅｘｔｅｎｓｉｏｎｓ」、ＲＦＣ２８６９、ＩＥＴＦ、２０００年６月、において定義されていることに留意されたい。したがって、本発明の好ましい実施形態においては、ネットワーク・アクセス装置は、ＥＡＰを使用し、かつ、その認証プロバイダとしてＲＡＤＩＵＳを使用するように構成される。接続試行が行われるときは、ユーザ装置は、ネットワーク・アクセス装置との間でＥＡＰの使用をネゴシエーションする。ユーザ装置がＥＡＰメッセージをネットワーク・アクセス装置に送信したときは、該ネットワーク・アクセス装置は、該ＥＡＰメッセージをＲＡＤＩＵＳメッセージとしてカプセル化し、構成されたＲＡＤＩＵＳサーバにそれを送信する。ＲＡＤＩＵＳサーバは、ＥＡＰメッセージを処理し、ＲＡＤＩＵＳ形式の該ＥＡＰメッセージをネットワーク・アクセス装置に返信し、次いで、ネッ

トワーク・アクセス装置は、該ＥＡＰメッセージをユーザ装置に転送する。

【００９７】

本発明の利点は、上述された詳細な説明から明らかであろう。ＲＡＤＩＵＳサーバなどのネットワーク・アクセス認証サーバのためのユーザ・レジストリは、ユーザの秘密鍵及びユーザの公開鍵証明書を保持するように構成されており、これらは、例えばＲＡＤＩＵＳプロトコルに従って実行されるネットワーク・アクセス認証操作の際に、該ネットワーク・アクセス認証サーバが使用可能である。ユーザ・レジストリ内の情報を用いると、ネットワーク・アクセス認証サーバは、ユーザのネットワーク・アクセス認証操作の際にユーザについてのプロキシ証明書を生成することができる。プロキシ証明書は、ネットワーク・アクセス装置を介してネットワーク・アクセス・パラメータと共にユーザ装置に戻される。プロキシ証明書は、ユーザ装置の適切な場所に格納され、該プロキシ証明書は、次に、ジョブがグリッドにサブミットされるときにグリッド・クライアント・アプリケーションが使用可能である。

【００９８】

その後のいずれかの時点で、グリッド・クライアント・アプリケーションは、グリッド内へのジョブのサブミットを準備する。グリッド・クライアント・アプリケーションが、ネットワーク・アクセス認証操作の際に以前に格納された有効で新しいプロキシ証明書を発見したときは、該グリッド・クライアント・アプリケーションはそれを用いる。したがって、新たなプロキシ証明書がその時点でユーザ装置上に生成される必要がないという事実によって、新たなプロキシ証明書の生成と関連する認証操作についての必要性が取り除かれる。このように、ネットワーク・アクセス及びグリッド・アクセスに対して１回のみ認証操作が行われ、これによりネットワーク及びグリッドのユーザはシングル・サインオンを体験することになる。

【００９９】

十分に機能するデータ処理システムに即して本発明を説明したが、当業者であれば、本発明の処理が、分散を実現するのに実際に用いられる信号支持媒体の特定の種類にかかわらず、コンピュータ可読媒体内の命令の形態及び様々な他の形態で分散させられ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として、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、デジタル及びアナログ通信リンクなどの伝送タイプの媒体が挙げられる。

【０１００】

方法は、一般に、所望の結果につながる一連の自己矛盾のないステップであるように考えられている。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。通常は、必須ではないが、こうした量は、格納し、転送し、組み合わせ、比較し、他の方法で操作することが可能な電気的又は磁気的信号の形態をとる。主に一般的な使用のために、これらの信号を、ビット、値、パラメータ、項目、要素、オブジェクト、記号、文字、用語、番号などと呼ぶことが都合がよい場合がある。しかしながら、これらの用語及び同様の用語のすべては、適切な物理量に関連するものであり、これらの量に使用される便利な表示にすぎないことに留意すべきである。

【０１０１】

本発明の説明は、例示の目的で提示されたが、網羅的であること、又は開示された実施形態に制限されることを意図するものではない。当業者には、多くの修正及び変形が明らかであろう。実施形態は、本発明の原理及びその実際の応用を説明し、他の考えられる用途に適する様々な修正を伴った種々の実施形態を実装するために当業者以外の者が本発明を理解できるように、選択された。

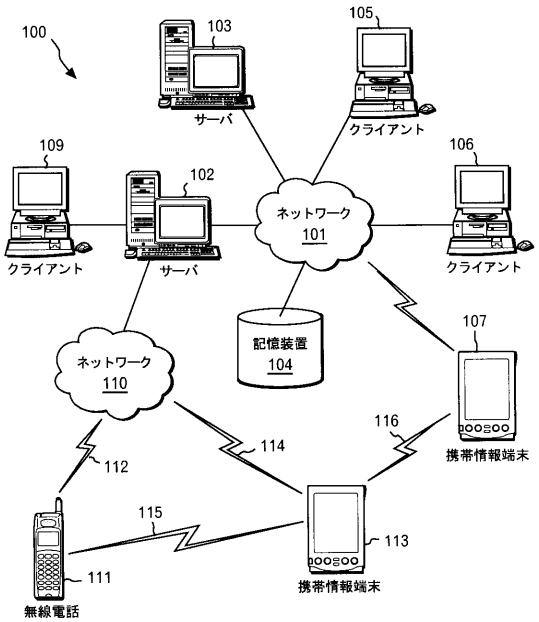
【図面の簡単な説明】

【０１０２】

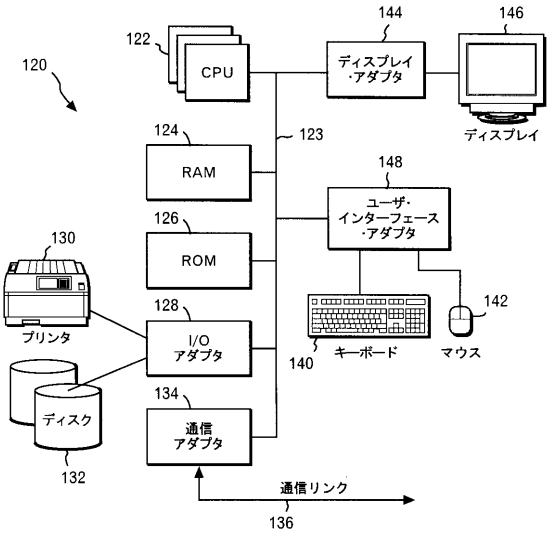
【図１】各々が本発明を実装することができるデータ処理システムの典型的なネットワークを示す。

【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可能な典型的なコンピュータ・アーキテクチャを示す。
【図３】エンティティがデジタル証明書を取得する典型的な方法を示す。
【図４】エンティティが分散データ処理システム内でデジタル証明書を用いることができる典型的な方法を示すブロック図を表す。
【図５】ネットワークを介してネットワーク及びグリッドにアクセスするユーザ装置を含む典型的なデータ処理システムを示すブロック図を表す。
【図６】本発明の実施形態に従ってネットワーク及びグリッドにアクセスするユーザ装置を含むデータ処理システムを示すブロック図を表す。
【図７】本発明の実施形態に従ってユーザ・レジストリ内にグリッド関連情報を確立するための処理を示すフローチャートを表す。
【図８】本発明の実施形態に従って、ネットワーク・アクセスのための認証操作をグリッド・アクセスのための認証操作と統合して複合型ネットワーク－グリッド・シングル・サインオン操作を提供するためのサーバ側の処理を示すフローチャートを表す。
【図９】本発明の実施形態に従って、ネットワーク・アクセスのための認証操作をグリッド・アクセスのための認証操作と統合して複合型ネットワーク－グリッド・シングル・サインオン操作を提供するためのクライアント側の処理を示すフローチャートを表す。

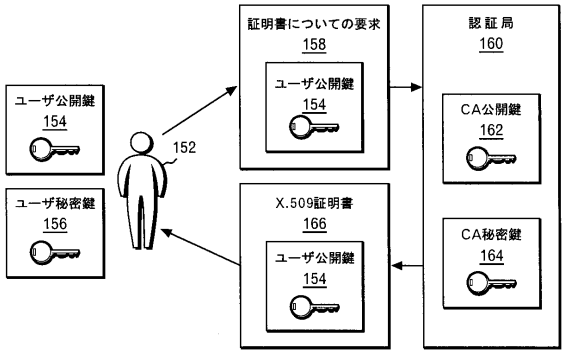
【図１】



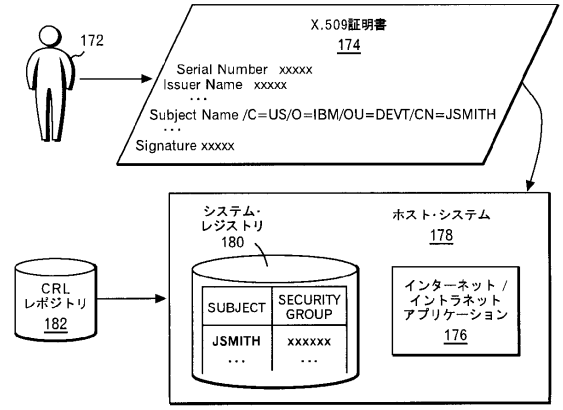
【図２】



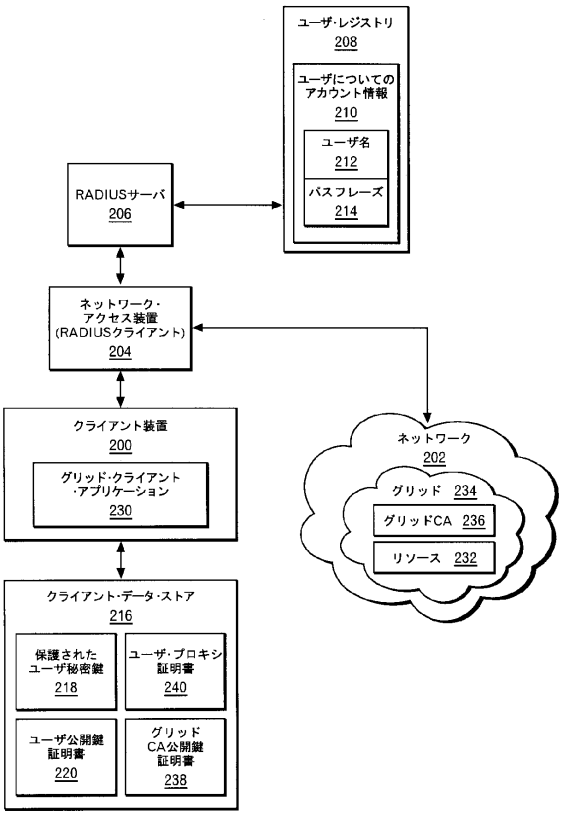
【図３】



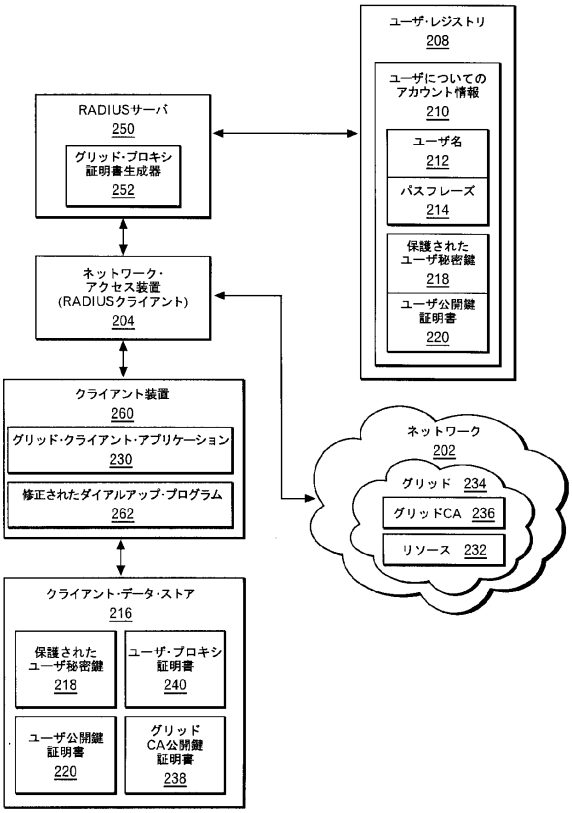
【図４】



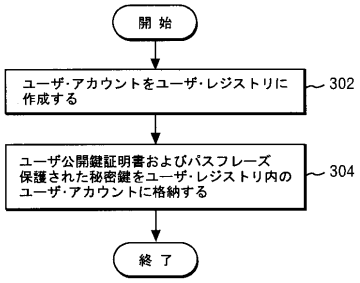
【図５】



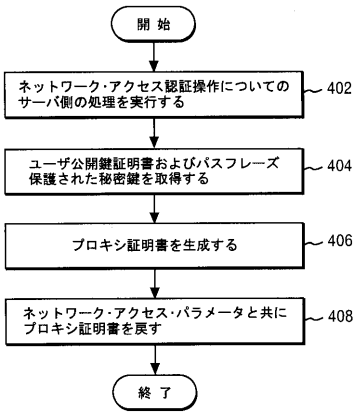
【図６】



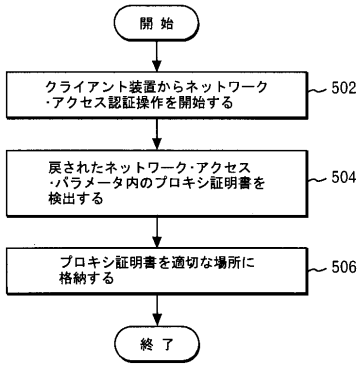
【図７】



【図８】



【図９】


開始
クライアント装置からネットワーク・アクセス認証操作を開始する
502
戻されたネットワーク・アクセス・パラメータ内のプロキシ証明書を検出する
504
プロキシ証明書を適切な場所に格納する
506
終了

フロントページの続き

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 ジェンティ、デニス、マリー
アメリカ合衆国 ７８７１７ テキサス州 オースチン デニス・ドライブ １６５０７
(72)発明者 マレン、ショーン、パトリック
アメリカ合衆国 ７８６１０ テキサス州 ブダ カントリー・オークス ３９

審査官 間野 裕一

(56)参考文献 特開２００２－２７８９３３（ＪＰ，Ａ）
米国特許出願公開第２００２／０１４４１１９（ＵＳ，Ａ１）
市川昊平他，ジョブ特性を考慮した優先制御機構を有する脳機能解析システムの設計と構築，情報処理学会研究報告，社団法人情報処理学会，２００３年 6月１３日，第２００３巻，第６２号，第３７－４２頁，２００３－ＨＰＣ－９４－７
山田英之，リモート接続のユーザー認証技術，日経コミュニケーション，日経ＢＰ社，１９９６年 8月 5日，第２２７号，第１２４－１３１頁
中田秀基，グリッドコンピューティングの現在を探る，Ｓｏｆｔｗａｒｅ Ｄｅｓｉｇｎ，株式会社技術評論社，２００３年 6月１８日，第１５２号，第１０２－１１３頁

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