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

特許第5139423号
(P5139423)

(45)発行日　平成25年2月6日(2013.2.6)　(24)登録日　平成24年11月22日(2012.11.22)

(51)Int.Cl.		F I		
G06F 21/57	(2013.01)	G06F	21/00	157A
G06F 21/44	(2013.01)	G06F	21/20	144C
H04L 9/32	(2006.01)	H04L	9/00	673A

請求項の数 15　(全 29 頁)

(21)出願番号	特願2009-512167 (P2009-512167)
(86)(22)出願日	平成19年5月25日 (2007.5.25)
(65)公表番号	特表2009-538478 (P2009-538478A)
(43)公表日	平成21年11月5日 (2009.11.5)
(86)国際出願番号	PCT/US2007/012512
(87)国際公開番号	WO2007/139944
(87)国際公開日	平成19年12月6日 (2007.12.6)
審査請求日	平成22年5月24日 (2010.5.24)
(31)優先権主張番号	11/441,588
(32)優先日	平成18年5月26日 (2006.5.26)
(33)優先権主張国	米国(US)

(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　100089705
弁理士　社本　一夫
(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

最終頁に続く

(54)【発明の名称】ネットワーク資源に対するシングルサインオン及び安全なアクセスのためのポリシ駆動の証明情報委譲

(57)【特許請求の範囲】

【請求項１】

ネットワークコンピューティング環境においてユーザ証明情報をクライアントからサーバに委譲（delegate）する方法であって、

前記ネットワークコンピューティング環境におけるサーバのアプリケーション、サービス又は資源の少なくとも１つに対しクライアントから、前記クライアントから前記サーバへのユーザ証明情報の委譲に関係する要求を送信するステップ、

前記クライアントと前記サーバとの間のハンドシェイクを開始するステップであって、該ステップが、前記サーバの公開鍵（K_{pub}）を前記クライアントにより受信するステップを含む、ステップ、

前記クライアントと前記サーバとの間の通信を認証する認証メカニズムとして利用するために、前記クライアントと前記サーバとの間で共有される認証パッケージを選択するように前記サーバとネゴシエートするステップ、

前記認証メカニズムとしての前記選択された認証パッケージを利用して前記サーバを認証するステップ、

該認証するステップに従って認証が発生したか否かを判断すると共に、認証が発生した場合のみ、前記クライアントと前記サーバとの間で通信されるメッセージの暗号化に対し共有秘密を確立することを含め、前記クライアントと前記サーバとの間でセッションを確立するステップ、

前記要求に対する前記ユーザ証明情報の送信に先立って、ユーザ証明情報に対して定義

された少なくとも１つの事前定義ポリシに従ってポリシチェックを実行し、前記サーバが前記ユーザ証明情報によって信頼することができるか否かを確定するステップ、
前記サーバの公開鍵（K_{pub}）を認証するステップ、および、
前記サーバを前記事前定義ポリシに従って信頼することができる場合、前記ユーザ証明情報を前記サーバに送信し、前記クライアントからの前記サーバの前記要求されたアプリケーション、サービス又は資源の前記少なくとも１つへのアクセスを取得するステップ、を含む、方法。

【請求項２】
請求項１に記載の方法において、前記少なくとも１つの事前定義ポリシは、ユーザ証明情報のクライアントからサーバへの前記委譲を制御及び制限するように使用される複数のポリシである、方法。

【請求項３】
請求項２に記載の方法において、前記複数のポリシは、前記クライアントで実行しているトロイ又はマルウェア、デフォルトグループポリシ設定及び前記クライアントの管理者によって構成可能なグループポリシ値、及びドメインネームサービス（ＤＮＳ）ポイズニングのうちの少なくとも１つを含む広範囲の攻撃を軽減して、不正サーバへの転換及びサービス許否攻撃を回避するための要件を記述するものである、方法。

【請求項４】
請求項２に記載の方法において、前記複数のポリシは、前記サーバのサービスプリンシパル名（ＳＰＮ）のリストに基づいて委譲を許容するか又は拒否するかの少なくとも一方のポリシを含む、方法。

【請求項５】
請求項１に記載の方法において、前記実行するステップは、前記認証メカニズムの相対強度に従ってポリシチェックを実行するステップを含む、方法。

【請求項６】
請求項１に記載の方法において、前記実行するステップは、前記ユーザ証明情報のタイプに基づいて定義される少なくとも１つの事前定義ポリシに従ってポリシチェックを実行するステップを含む、方法。

【請求項７】
請求項６に記載の方法において、前記実行するステップは、前記ユーザ証明情報が新規の証明情報であるか、保存されている証明情報であるか、又はデフォルト証明情報であるかに基づいて定義される少なくとも１つの事前定義ポリシに従ってポリシチェックを実行するステップを含む、方法。

【請求項８】
請求項１に記載の方法において、前記ユーザの証明情報を送信するステップは、ローカルセキュリティシステムの信頼されたサブシステムのみが平文フォーマットでの前記ユーザ証明情報にアクセスすることができるフォーマットで前記ユーザの証明情報を送信するステップを含む、方法。

【請求項９】
請求項８に記載の方法において、前記ポリシチェックを実行するステップは、ローカルセキュリティ機関（ＬＳＡ）によって実行され、前記信頼されたサブシステムは、前記ＬＳＡの信頼されたサブシステムである、方法。

【請求項１０】
請求項１に記載の方法であって、前記クライアントと前記サーバとの間の前記セッションを確立した後、前記サーバの公開鍵を認証するステップをさらに含む、方法。

【請求項１１】
請求項１に記載の方法において、前記ハンドシェイクは、セキュアソケットレイヤ（ＳＳＬ）プロトコル又はトランスポート層セキュリティ（ＴＬＳ）プロトコルに従うハンドシェイクである、方法。

【請求項１２】

請求項１に記載の方法において、前記ネゴシエートするステップは、単純な保護されている汎用セキュリティサービスアプリケーションプログラムインタフェース（Simple and Protected Generic Security Service Application Program Interface）（ＧＳＳＡＰＩ）ネゴシエーションメカニズム（ＳＰＮＥＧＯ）ネゴシエーションを使用してネゴシエートするステップを含む、方法。

【請求項１３】

請求項１に記載の方法において、前記選択される認証パッケージは、ケルベロス又はＮＴローカルエリアネットワーク（ＬＡＮ）マネージャ（ＮＴＬＭ）である、方法。

【請求項１４】

請求項１に記載の方法において、前記共有秘密は共有セッションキーである、方法。

【請求項１５】

請求項１～１４のいずれか１項に記載の方法のすべてのステップをコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワークコンピューティング環境におけるアプリケーション、資源及び／又はサービスに対するシングルサインオン及び安全なアクセスのためのポリシ駆動の証明情報（credential）委譲（delegation）に関する。

【背景技術】

【０００２】

クライアントを介してアクセスされるサーバアプリケーションでは、そのサーバアプリケーションによって使用可能となるシナリオをサポートするために、クライアントのユーザの証明情報がサーバに委譲されることが必要である場合がある。このような委譲状況では、サーバアプリケーションが、ユーザが単純にサーバアプリケーションのローカルユーザとしてログインするときに利用可能な機能をエミュレートするために、リモート端末のユーザのパスワードがサーバ側で必要となる。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

しかしながら、サーバアプリケーションの機能にアクセスするために証明情報をクライアントからサーバアプリケーションに委譲する現行のシステムは、十分に安全ではなく、すなわち、ユーザの証明情報をクライアントからサーバに委譲する／送信するときの保護が不十分であり、ユーザの証明情報は特定の形態の攻撃を受け易いままである。現在、たとえば、サーバ側又はクライアント側のいずれかにおける呼出しアプリケーションは、ユーザの平文の証明情報にアクセスできる場合があり、そのため、ユーザの証明情報は幾分か安全でない。さらに、目下、いかなるタイプのユーザ証明情報、すなわちユーザ名／パスワード、スマートカードＰＩＮ、ワインタイムパスコード（ＯＴＰ）等にも適用される、クライアントからユーザへのユーザ証明情報の委譲を制御及び制限するポリシ駆動の方法はない。

【課題を解決するための手段】

【０００４】

本発明に関して後により詳細に説明するように、現行の技術水準のこれらの欠点及び他の欠点に対し改良を行うことが望ましい。

【０００５】

上記を鑑みて、本発明は、ネットワークコンピューティング環境において、任意のアプリケーションが、ユーザの証明情報を、クライアントからクライアント側セキュリティサポートプロバイダ（ＳＳＰ）ソフトウェアを介して、ターゲットサーバにサーバ側ＳＳＰソフトウェアを介して安全に委譲するのを可能にする、証明情報セキュリティサポートプロバイダ（Ｃｒｅｄ　ＳＳＰ）を提供する。一実施形態では、Ｃｒｅｄ　ＳＳＰは、クラ

イアントのオペレーティングシステムの一部として含まれてもよい、セキュリティサポートプロバイダインタフェース（ＳＳＰＩ）ソフトウェアを介してユーザに利用可能となる。本発明のＣｒｅｄ　ＳＳＰは、部分的に、ユーザ証明情報のクライアントからサーバへの委譲を制御及び制限するの使用される、広範囲の攻撃に対して安全なデフォルトポリシを含むポリシのセットに基づく、安全なソリューションを提供する。それらのポリシは、あらゆるタイプのユーザ証明情報に対するものとすることができ、所与の委譲状況、ネットワーク状態、信頼レベル等に対して適切な委譲を行うことができるように、広範囲の攻撃を軽減するように、種々のポリシが設計される。さらに、信頼されたサブシステム、たとえばローカルセキュリティ機関（ＬＳＡ）の信頼されたサブシステムのみが、平文の証明情報にアクセスすることができ、それによって、サーバ側のＣｒｅｄ　ＳＳＰを使用するＳＳＰＩ　ＡＰＩの呼出しアプリケーションも、クライアント側のＣｒｅｄ　ＳＳＰを使用するＳＳＰＩ　ＡＰＩの呼出しアプリケーションも、平文の証明情報にアクセスすることができない。

【０００６】

本発明の他の特徴については後述する。

【０００７】

ネットワークコンピューティング環境における資源に対するシングルサインオン及び安全なアクセスのためのポリシ駆動の証明情報委譲について、添付図面に関連してさらに説明する。

【発明を実施するための最良の形態】

【０００８】

概説

背景技術において述べたたように、サーバシナリオをサポートするためにユーザの証明情報をサーバに委譲する必要のあるクライアント／サーバアプリケーションがある。ターミナルサーバは、１つのこのような例であり、そこでは、サーバの機能をクライアント側でエミュレートするために、ユーザのパスワードがサーバ側で使用される場合がある。しかしながら、上述したように、従来技術による委譲技法は、ユーザの証明情報がサーバに送信されるとき、ユーザの証明情報に対し十分な保護を提供しない。

【０００９】

本発明のＣｒｅｄ　ＳＳＰは、クライアントのオペレーティングシステムの既存のセキュリティサポートプロバイダインタフェース（ＳＳＰＩ）インフラストラクチャを介して利用可能となり得る、「セキュリティサービスプロバイダ」と称されることもある新たな「セキュリティサポートプロバイダ」である。本発明のＣｒｅｄ　ＳＳＰによって、アプリケーションは、クライアントから、たとえばクライアント側ＳＳＰソフトウェアを介して、ターゲットサーバに、たとえばサーバ側ＳＳＰソフトウェアを介して、ユーザの証明情報を委譲することができる。例示的な非限定的実施形態では、本発明のＣｒｅｄ　ＳＳＰを、ターミナルサーバに含めることができる。しかしながら、本発明のＣｒｅｄ　ＳＳＰを、他のアプリケーションが利用してもよく、適用可能なオペレーティングシステムのＳＳＰＩを使用して任意の内部のアプリケーション又はサードパーティアプリケーションに利用可能となるようにしてもよい。

【００１０】

Ｃｒｅｄ　ＳＳＰソリューションは、ユーザの証明情報のクライアントからサーバへの委譲を制御及び制限するのに使用することができるポリシのセットを提供する、より安全なソリューションである。ポリシは、クライアントのマシンで実行しているマルウェアを含む、広範囲の攻撃に対処するように設計されている。本発明のＣｒｅｄ　ＳＳＰは、クライアントマシンがデフォルトで広範囲の攻撃を軽減することができるようにするポリシ設定を介する特定の構成である、「デフォルトで安全な」ポリシを含む。本発明のポリシのセットは、限定されないがユーザ名／パスワード、スマートカードＰＩＮ、ワンタイムパスコード（ＯＴＰ）等を含む、いかなるタイプのユーザ証明情報を保護することにも適用可能である。信頼されたサブシステムのみが平文の証明情報にアクセスすることができ

るため、本発明のＣｒｅｄ　ＳＳＰは、サーバ側又はクライアント側の（Ｃｒｅｄ　ＳＳＰ　ＡＰＩの）呼出しアプリケーションが、平文の証明情報にアクセスすることができないように、ユーザの証明情報を保護する。

【００１１】

たとえば、Microsoftのターミナルサーバ（ＴＳ）は、端末／クライアントに対してMicrosoftのＷｉｎｄｏｗｓ（登録商標）オペレーティングシステム製品のアプリケーション及び「デスクトップ」体験の提供を許可するために、ユーザに対し、端末／クライアントにおけるサインオン証明情報を提供し、それらのサインオン証明情報をサーバに委譲するように要求する場合がある、サーバ／クライアント製品の一例である。ＴＳを、概して３つの主な部分、すなわちマルチユーザコアサーバと、Ｗｉｎｄｏｗｓ（登録商標）デスクトップインタフェースがサーバによって端末に送信されることを可能にするリモートデスクトッププロトコル（ＲＤＰ）と、各端末で実行するクライアントソフトウェアとを含むものとして考えることができる。本発明の１つの非限定的実施形態では、本発明の証明情報セキュリティサポートプロバイダのプロトコルを、ターミナルサーバソフトウェアに関連して実施してもよい。

補足的状況

本明細書では、さまざまな実施形態のうちのいくつかを、認証及び証明情報委譲の技術分野の当業者に一般に理解される用語に関連して説明する。このセクションは、当業者の知識を代用することは意図されておらず、非網羅的な概説とみなされるべきであるが、後により詳細に説明するように、本発明のさまざまな実施形態の動作の状況において利用されるいくつかの用語に対し、いくつかの追加の状況及び背景を有利に提供するものと考えられる。

【００１２】

このため、本明細書では、当業者によって一般的に既知である以下の用語に対する追加の状況及び背景について提供する。すなわち、ケルベロス、Ｗｉｎｄｏｗｓ（登録商標）ＮＴローカルエリアネットワーク（ＬＡＮ）マネージャ（ＮＴＬＭ）、単純な保護されている汎用セキュリティサービスアプリケーションプログラムインタフェース（ＧＳＳＡＰＩ）ネゴシエーションメカニズム（略してＳＰＮＥＧＯ）、ローカルセキュリティ機関（ＬＳＡ）、セキュリティサポートプロバイダインタフェース（ＳＳＰＩ）及びセキュアソケットレイヤ（ＳＳＬ）プロトコル並びに例示的なＷｉｎｄｏｗｓ（登録商標）認証インフラストラクチャである。

ケルベロス

ケルベロスは、コンピュータネットワークにおけるサービスへの要求を認証する安全な方法である。ケルベロスは、地獄への入口の番をする神話上の頭が３つある犬からその名前を借りており、ユーザに、認証プロセスから、後にサーバから特定のサービスを要求するのに使用することができる暗号化「チケット」を要求させ、それによって、ユーザのパスワードがネットワークを通過する必要がないようにする。ケルベロスは、クライアントと、クライアントにおけるユーザによるログイン要求を含む、サーバへのアクセスを許可するサーバ側ソフトウェアとを含む。しかしながら、サーバは、そのアプリケーション、資源及び／又はサービスへのアクセスの要求に応じる前に、ケルベロス「チケット」を要求する。適切なケルベロスチケットを取得するために、クライアントによって認証サーバ（ＡＳ）に対して認証要求がなされる。ＡＳは、ユーザ名から取得されるユーザのパスワードと、要求されたサービスを表すランダム値とに基づいて、暗号鍵でもある「セッションキー」を作成する。この意味で、セッションキーは、実質的には「チケット認可チケット（ticket-granting ticket）」である。

【００１３】

次に、取得されたチケット認可チケットがチケット認可サーバ（ticket-granting server）（ＴＧＳ）に送信される。ＴＧＳは、ＡＳと物理的に同じサーバであってもよいが、機能的に異なるサービスを実行する。ＴＳＧは、要求されたサービスに対してサーバに送信することができるチケットを返す。サービスは、チケットが無効である場合にそのチケ

ットを拒否するか、又はそのチケットを有効なチケットとして受け入れてサービスを実行する。ＴＧＳから受け取られるチケットにはタイムスタンプが刻印されているため、チケットによって、一定時間期間内に、サーバのサービスのユーザの使用を再認証する必要なく、同じチケットを使用して追加の要求を行うことが可能である。他方で、限られた時間期間チケットを有効にすることによって、許可されたユーザ以外の誰かがチケットを再使用することができる可能性を低減する。当業者は、インタフェース、プロトコル、ペイロード及びドライバレベルでのケルベロス認証プロセスの詳細がはるかに複雑であり得ること、及びユーザ手続きが実施態様によって幾分異なる場合があることを理解することができる。

Ｗｉｎｄｏｗｓ（登録商標）　ＮＴ　ＬＡＮマネージャ（ＮＴＬＭ）

ケルベロスの代替物であるＮＴＬＭは、さまざまなＭｉｃｒｏｓｏｆｔネットワークプロトコル実施態様で使用され、ＮＴＬＭセキュリティサポートプロバイダ（ＮＴＬＭＳＳＰ）によってサポートされる、認証プロトコルである。ＮＴＬＭは、最初は、安全な分散コンピューティング環境（ＤＣＥ）／リモートプロシージャコール（ＲＰＣ）通信の認証及びネゴシエーションに使用されたが、統合されたシングルサインオンメカニズムとしても使用される。

【００１４】

ＮＴＬＭは、認証のためにチャレンジ・レスポンスメカニズムを採用し、そこでは、クライアントが、サーバにパスワードを送信することなく自身の身元を証明することができる。チャレンジ・レスポンスメカニズムは、一般にタイプ１（ネゴシエーション）、タイプ２（チャレンジ）及びタイプ３（認証）とも称される３つのメッセージを含む。高レベルでは、ＮＴＬＭによって、まず、クライアントはサーバに対し、クライアントによってサポートされサーバに要求される機能のリストを含むタイプ１メッセージを送信する。サーバは、サーバによってサポートされ合意された特徴のリストと、サーバによって生成されるチャレンジとを含むタイプ２メッセージで、クライアントに応答する。クライアントは、クライアントユーザのドメイン及びユーザ名を含むクライアントに関するいくつかの情報とタイプ２チャレンジに対する１つ又は複数の応答とを含むタイプ３メッセージで、チャレンジに応答する。タイプ３メッセージにおける応答（複数可）は、サーバに対し、クライアントユーザがアカウントパスワードを知っていることを証明するため、重要なものである。

セキュアチャネル（Ｓｃｈａｎｎｅｌ）

Ｓｃｈａｎｎｅｌとしても知られるセキュアチャネルは、暗号化を通じて身元認証及び強化された通信セキュリティを提供するセキュリティプロトコルのセットを含む、セキュリティサポート／サービスプロバイダ（ＳＳＰ）である。Ｓｃｈａｎｎｅｌは、主に、ハイパーテキスト転送プロトコル（ＨＴＴＰ）通信のためにセキュリティの強化を必要とするインターネットアプリケーションに使用されている。Ｓｃｈａｎｎｅｌセキュリティプロトコルによって、サーバがその身元の証明をクライアントに提供するサーバ認証が要求される。そのため、Ｓｃｈａｎｎｅｌプロトコルは、サーバ及び任意選択でクライアントを認証するのに使用することができるＳｃｈａｎｎｌ証明情報を利用する。クライアント認証は、サーバによって常に要求される可能性がある。Ｓｃｈａｎｎｅｌ証明情報はＸ．５０９証明書である。証明書からの公開鍵及び秘密鍵情報を使用して、サーバ及び任意選択でクライアントが認証される。これらの鍵はまた、クライアント及びサーバがセッションキーを生成し交換するのに必要な情報を交換する間に、メッセージ完全性を提供するのにも使用される。Ｓｃｈａｎｎｅｌは、後により詳細に参照するＳＳＬプロトコル及びＴＬＳプロトコルを実装する。

単純で保護されたＧＳＳＡＰＩネゴシエーションメカニズム（ＳＰＮＥＧＯ）

ＳＰＮＥＧＯは、ピアが、いずれのＧＳＳＡＰＩメカニズムが共有されるかを確定し、１つを選択し、次に、共有ＧＳＳＡＰＩメカニズムによってセキュリティコンテキストを確立する、標準汎用セキュリティサービスアプリケーションプログラムインタフェース（ＧＳＳＡＰＩ）擬似メカニズムである。ＳＰＮＥＧＯの仕様は、１９９８年１２月付けの

「GSS-API Negotiation Mechanism」と題するインターネット技術タスクフォース（Internet Engineering Task Force）の草案ＲＦＣ２４７８に見ることができる。

【００１５】

ＳＰＮＥＧＯの使用は、たとえば、最初に閲覧ソフトウェアＩｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒで実装され、Ｗｉｎｄｏｗｓ（登録商標）統合認証として知られるシングルサインオン機能を提供した、認証拡張機能である、「ＨＴＴＰネゴシエート」に見ることができる。ＳＰＮＥＧＯのネゴシエート可能なサブメカニズムにはＮＴＬＭ及びケルベロスがあり、それらは共にアクティブディレクトリを使用する可能性がある。

【００１６】

ＧＳＳＡＰＩは、異なるセキュリティメカニズムの上に階層化されることが可能な汎用インタフェースを提供し、それによって、通信しているピアが同じセキュリティメカニズムに対するＧＳＳＡＰＩ証明情報を取得すると、それらの間にセキュリティコンテキストを確立することができる。しかしながら、ＧＳＳＡＰＩは、ＧＳＳＡＰＩピアが共通のセキュリティメカニズムを有するか否かを確立することができるようにする方法について規定していない。

【００１７】

ＳＰＮＥＧＯによって、ＧＳＳＡＰＩピアは、それらの証明情報が共通のＧＳＳＡＰＩセキュリティメカニズム（複数可）を共有するか否かを帯域内で確定し、共有する場合、選択された共通のセキュリティメカニズムに対し通常のセキュリティコンテキスト確立を呼び出すことができ、それによって、異なるセキュリティメカニズム、所与のセキュリティメカニズム内での異なるオプション、又はいくつかのセキュリティメカニズムからの異なるオプションのネゴシエーションが可能になる。これは、複数のセキュリティメカニズムをサポートするＧＳＳＡＰＩ実施態様に基づくアプリケーションに対して最も有用である。共通のセキュリティメカニズムが識別されると、それは、そのコンテキスト確立中にメカニズムに固有のオプションをネゴシエートしてもよい。

【００１８】

ＳＰＮＥＧＯによって、ネゴシテーションデータは、コンテキストレベルトークンにカプセル化される。このため、ＧＳＳＡＰＩの呼出し側は、ネゴシテーショントークンの存在に気付く必要はなく、擬似セキュリティメカニズムの存在にのみ気付けばよい。

【００１９】

ＳＰＮＥＧＯのネゴシエーションモデルは以下のように作用する。イニシエータは、１つのセキュリティメカニズムか又はセキュリティメカニズムの順序付きリストを提案し、ターゲットは、提案されたセキュリティメカニズムを受け入れるか、若しくは提供されたセットから１つを選択するか、又は提案された値（複数可）を拒否する。そして、ターゲットは、イニシエータに対してその選択を通知する。

【００２０】

このプロトコルは、その基本形式において、余分なラウンドトリップが必要である。ネットワークコネクションセットアップは、いかなるネットワークインフラストラクチャにおいても重要な性能特性であり、ＷＡＮリンク、パケット無線ネットワーク等にわたる余分なラウンドトリップが実際に重大である場合がある。このような余分なラウンドトリップを回避するために、イニシエータに対する好ましいメカニズムの初期セキュリティトークンを、初期トークンに埋め込むことができる。ターゲットの好ましいメカニズムがイニシエータの好ましいメカニズムと一致する場合、ネゴシエーションプロトコルを使用することによっていかなる追加のラウンドトリップももたらされない。

【００２１】

ＳＰＥＮＧＯはまた、ターゲットによって選択される基礎となるメカニズムが、完全性保護が可能である場合、ネゴシエーションを保護する技法も提供する。イニシエータによって提案されるメカニズムが完全性保護をサポートする場合、又は選択されたメカニズムが完全性保護をサポートする場合、ネゴシエーションメカニズムは保護される。それは、これが、両ピアによってサポートされる適切なメカニズムが選択されたことを保証するた

めである。
ローカルセキュリティ機関（ＬＳＡ）
ＬＳＡは、一般化された概念ではあるが、ローカルログオン及びリモートログオン両方に対してユーザを確認する役割を担う、ＭｉｃｒｏｓｏｆｔのＷｉｎｄｏｗｓ（登録商標）オペレーティングシステム技術のログオンプロセスの重要な要素である。ＬＳＡはまた、ローカルセキュリティポリシも維持する。
【００２２】
マシンに対するローカルの対話型ログオンの間に、人は、ログオンダイアログに対して自身の名前及びパスワードを入力する。この情報はＬＳＡに渡され、次にＬＳＡは、適切な認証パッケージを呼び出す。パスワードは、一方向ハッシュ関数を使用して、非可逆秘密鍵フォーマットで送信される。次に、ＬＳＡは、セキュリティアカウントマネージャ（ＳＡＭ）データベースに対しユーザのアカウント情報を問い合わせる。提供された鍵がＳＡＭの鍵と一致する場合、ＳＡＭは、ユーザのセキュリティ識別子（ＳＩＤ）とユーザが属する任意のグループのＳＩＤとを返す。そして、ＬＳＡは、これらのＳＩＤを使用して、セキュリティアクセストークン（複数可）を生成する。この説明は、ユーザがローカルアカウントを有する場合に当てはまり、マシンに対してユーザを認証するためにケルベロスサービスチケットが取得されるドメインアカウントとは対照的である。
セキュリティサポートプロバイダインタフェース（ＳＳＰＩ）
ＳＳＰＩは、ユーザを認証する、すなわち、ユーザが、自身が本人であると主張する者であること、又は最低限、ユーザが、特定のユーザアカウントに関連付けられる秘密、たとえばパスワードを知っていることを確認するメカニズムを定義する。
【００２３】
このような認証されたコネクションに対して使用される証明情報は、以下のものがあり得る。すなわち、（１）クライアントマシンとサーバマシンとの間の既存の認証されたリンク（たとえば、既存のドライブマッピング）の証明情報、（２）サーバがこのアカウントに関連付けられるＳＩＤを理解する場合の、クライアントユーザのアカウントの証明情報、すなわち、これは、クライアント及びサーバの両方が同じドメインを信頼し、ユーザアカウントがそのドメインからのものであることを意味する、（３）クライアントユーザ名及びパスワードと一致する場合（この場合、クライアントユーザのアカウントとユーザがサーバで使用するアカウントとは別個である）の、サーバにおけるローカルアカウントの生の証明情報（たとえば、名前及びパスワード）及び（４）ユーザによって明示的に渡される証明情報（たとえば名前及びパスワード）である。ＳＳＰＩは、呼出しアプリケーション（クライアントプロセス及びサーバプロセス）に対し、基礎となるセキュリティプロバイダが満足するまでデータブロックを往復して送信するように要求することによって作用する。
【００２４】
クライアントは、セキュリティダイナミックリンクライブラリ（ＤＬＬ）をロードし、パッケージ（ＮＴＬＭ、ケルベロス等、セキュリティプロバイダに対する別の用語）を選択した後、ローカル又はクライアントＳＳＰＩを初期化し、第１のデータのセットを検索してサーバに送信する。一方、サーバは、サーバＳＳＰＩを初期化し、第１のデータのセットを受け取った後、それをサーバＳＳＰＩに供給し、サーバＳＳＰＩは、その第１のデータのセットを処理して、その結果第２のデータのセットが生じる。折り返し、サーバはその結果としての第２のデータのセットに対してチェックを実行し、データが０より大きい場合、クライアントに第２のデータのセットを送信し、クライアントは次にそれをクライアントＳＳＰＩに供給する。次に、クライアントＳＳＰＩは、第３のデータのセットがサーバに送信されることを要求するか、又はアプリケーションに対し認証が完了したことを通知する。これは、クライアントＳＳＰＩ及びサーバＳＳＰＩの両方が、他方から受け取られるデータに満足するまで続く。
【００２５】
この時点で、サーバは、（特に）クライアントのユーザ名を問い合わせされることがで

きる、コンテキストハンドルを保持する。クライアントによって使用されるオプションに応じて、サーバはまた、コンテキストを使用してクライアントに成り済ますこと、メッセージに署名するか又はメッセージを暗号化すること等が可能になってもよい。もう１つの任意選択のステップが実行されてもよい。送受信サイクルを終了するために、セキュリティプロバイダによっては、CompleteAuthToken（ＣＡＴ）と称される事前定義された終了ステップを要求してもよい。

セキュアソケットレイヤ（ＳＳＬ）プロトコル及びトランスポート層セキュリティ（ＴＬＳ）プロトコル

共にＳｃｈａｎｎｅｌによって実装される、セキュアソケットレイヤ（ＳＳＬ）プロトコル及びその後続プロトコルであるトランスポート層セキュリティ（ＴＬＳ）プロトコルは、インターネット上で安全な通信を提供する暗号法プロトコルである。ＳＳＬ３．０とＴＬＳ１．０との間にはわずかな相違があるが、プロトコルは実質的に同じままである。「ＳＳＬ」という用語は、文脈によって明確にされない限り、両プロトコルを指す場合がある。

【００２６】

ＳＳＬ／ＴＳＬプロトコルは、暗号法を使用してインターネットを介してエンドポイント認証及び通信プライバシを提供する。通常の使用では、サーバは認証され（すなわち、その身元は保証され）、一方、クライアントは認証されないままであるが、相互の認証はクライアントに対し公開鍵インフラストラクチャ（ＰＫＩ）展開を介して実行され得る。これらのプロトコルによって、クライアント／サーバアプリケーションは、盗聴、改ざん及びメッセージ偽造を防止するように設計された方法で通信することができる。

例示的な非限定的Ｗｉｎｄｏｗｓ（登録商標）認証インフラストラクチャ

１つの例示的な非限定的認証インフラストラクチャは、セキュリティサービス／サポートプロバイダ（ＳＳＰ）ソフトウェアを介して異なる認証方法をサポートするＷｉｎｄｏｗｓ（登録商標）オペレーティングシステム技術によって提供される。

【００２７】

一実施態様では、Ｗｉｎｄｏｗｓ（登録商標）は、上述した３つの主なＳＳＰをサポートする。すなわち、ケルベロス、ＮＴＬＭチャレンジ／レスポンス及びＳＣｈａｎｎｅｌセキュリティプロトコルである。ケルベロスはＷｉｎｄｏｗｓ（登録商標）２０００におけるデフォルト認証方法であるが、セキュリティサポートプロバイダインタフェースすなわちＳＳＰＩを通じて他の方法を使用してもよい。さらに、たとえば、Ｗｉｎｄｏｗｓ（登録商標）は、以下のネットワークＳＳＰを使用することによって、デジタル証明書を用いて認証サービスを提供することができる。すなわち、分散パスワード認証（ＤＰＡ）（インターネット認証プロトコル）、拡張認証プロトコル（ＥＡＰ）（ポイント・ツー・ポイント（ＰＰＰ）プロトコルへの拡張）、並びに、ＳＳＬ、ＴＬＳ及びプライベート通信技術を含む公開鍵ベースのプロトコルである。

ネットワーク資源に対するシングルサインオン及び安全なアクセスのためのポリシ駆動の証明情報委譲

上述したように、本発明は、アプリケーションが、ユーザの証明情報をクライアントから、たとえばクライアント側ＳＳＰソフトウェアを介して、ターゲットサーバに、たとえばサーバ側ＳＳＰソフトウェアを介して委譲することを可能にする、拡張証明情報セキュリティサポートプロバイダ（Ｃｒｅｄ　ＳＳＰ）ソフトウェアを提供する。本発明のＣｒｅｄ　ＳＳＰを、適用可能なＳＳＰＩ、たとえばオペレーティングシステムアプリケーションプラットフォームと統合されるＳＳＰＩを使用して、オペレーティングシステムの任意のネイティブアプリケーション又は任意のサードパーティアプリケーションによって利用することができる。

【００２８】

図１は、平文の証明情報を呼出しアプリケーション（複数可）に晒すことなく、証明情報のクライアントからサーバへの安全な委譲を可能にする、本発明のＣｒｅｄ　ＳＳＰアーキテクチャの概略ブロック図である。一実施形態では、Ｃｒｅｄ　ＳＳＰは、２つのパ

ッケージのセットとして実装される。すなわち、クライアントコンピューティング装置又はサーバコンピューティング装置のための、装置Ｄのクライアント（又はアプリケーション）側ＣｒｅｄＳＳＰパッケージClient-Side_CredSSP及びＬＳＡ側ＣｒｅｄＳＳＰパッケージLSA_CredSSPである。

【００２９】

クライアント側パッケージClient-side_CredSSPは、クライアント側セキュリティサポートプロバイダインタフェースClient-side_CredSSPインタフェースＩ１の呼出し側に晒され、Ｓｃｈａｎｎｅｌネゴシエーションを提供すると共に、Ｓｃｈｅｎｎｅｌパッケージ機能、及びLSA-side Cred SSPインタフェースＩ２を介するＬＳＡ側パッケージLSA_CredSSPとの通信を晒す、クライアント側セキュリティサポートプロバイダソフトウェアである。本発明によれば、ユーザプロセスにおいてＳｃｈａｎｎｅｌネゴシエーション及び機能を処理することによって、ＬＳＡによる実行と比較して、より高速なencryptMessage操作及びdecryptMeesage操作が容易になる。

【００３０】

本発明によれば、ＬＳＡパッケージLSA_CredSSPは、ＳＰＮＥＧＯネゴシエーションと証明情報暗号化／解読及び証明情報転送を提供すると共に、本発明のポリシの上述したセットに従って定義されるポリシに対するポリシチェックを実行する。

【００３１】

上述したように、且つ例示的な非限定的実施形態において図２Ａ及び図２Ｂに示すように、本発明は、証明情報をターミナルサーバ２５０に委譲するターミナルサーバクライアント２００と関連して実施される。

【００３２】

図２Ａに示すように、ターミナルサーバクライアント２００の実施態様は、ローカルプロシージャコール（ＬＰＣ）２１５を利用して、セキュア認証ライブラリ２０５を介してＬＳＡサーバプロセス２２５と対話し、それはプロセス境界２２０を越えてデータを送信することを含む。関数２１０は、セキュア認証ライブラリ２０５で実行し、セキュアソケットレイヤ／セキュリティコンテキスト初期化（SSL.ISC）関数とセキュアソケットレイヤ／メッセージ暗号化（SSL.EM）関数とを含む、ＣｒｅｄＳＳＰセキュリティコンテキスト初期化（CredSSP.ISC）関数を含むことができる。関数２３０は、ＬＳＡサーバプロセス２２５で実行し、ＳＰＮＥＧＯ／セキュリティコンテキスト初期化（SPNEGO.ISC）関数とＳＰＮＥＧＯ／メッセージ暗号化（SPNEGO.EM）関数とを含む、ＣｒｅｄＳＳＰセキュリティコンテキスト初期化（CredSSP.ISC）関数を含むことができる。

【００３３】

図２Ｂに示すように、ターミナルサーバ２５０の実施態様は、ローカルプロシージャコール（ＬＰＣ）２６５を利用して、セキュア認証ライブラリ２５５を介してＬＳＡサーバプロセス２７５と対話し、それはプロセス境界２７０を横断することを含む。関数２６０は、セキュア認証プロセス２０５で実行し、セキュアソケットレイヤ／セキュリティコンテキスト受入れ（SSL.ASC）関数とセキュアソケットレイヤ／メッセージ解読（SSL.DM）関数とを含む、ＣｒｅｄＳＳＰセキュリティコンテキスト受入れ（CredSSP.ASC）関数を含むことができる。関数２８０は、ＬＳＡサーバプロセス２７５で実行し、ＳＰＮＥＧＯ／セキュリティコンテキスト受入れ（SPNEGO.ASC）関数とＳＰＮＥＧＯ／メッセージ解読（SPNEGO.DM）関数とを含む、ＣｒｅｄＳＳＰセキュリティコンテキスト受入れ（CredSSP.ASC）関数を含むことができる。

【００３４】

本発明のＣｒｅｄＳＳＰによって利用される例示的な非限定的プロトコルを、図３の流れ図において例示的に示す。３００において、クライアントとサーバとの間で最初のＳＳＬ／ＴＬＳハンドシェイクが行われる。３０５において、ＳＰＮＥＧＯネゴシエーションが発生して、認証メカニズム（たとえば、ケルベロス若しくはＮＴＬＭ、又はクライアント及びサーバによって理解される他の適切なネゴシエーションメカニズム）が選択される。３１０及び３１５において、ネゴシエートされた認証メカニズムを使用して、サーバが

クライアントに認証され、クライアントがサーバに認証される。

【００３５】

３２０において、ステップ３１０及び／又は３１５に従ってクライアントとサーバとの間で適切な認証が達成された場合、次に３３０において、すべてのさらなるトラフィックに関して共有秘密（たとえば共有鍵）が確立される。しかしながら、有利には、３２０において、クライアントとサーバとの間で適切な認証が確立されなかった場合、３２５においてセッションは作成されず、多量の計算コスト及びトラフィックは回避される。従来は、たとえば、ターミナルサーバの従来の実施態様では、セッションが作成された後に認証を実行する試みが開始されたため、認証の実行にはよりコストがかかった。対照的に、本発明のＣｒｅｄ　ＳＳＰのプロトコルによれば、クライアントとサーバとの間のセッションは、ＳＰＮＥＧＯ選択認証メカニズムによるクライアント及びサーバの認証が達成されない限り作成されない。

【００３６】

このため、３２０において、選択された認証メカニズムを使用して適切な認証が実行されたとすると、３３０においてクライアントとサーバとの間のすべてのさらなるトラフィックに対し、共有鍵が確立される。しかしながら、閾値認証が発生したというだけでは、依然としてサーバが必ずしもクライアントに信頼されていることを意味するわけではない。このため、この時点で、クライアントとサーバとの間でセッションが作成されているが、サーバは信頼されているとみなされる場合もあれば、信頼されていないとみなされる場合もある。したがって、本発明のグループポリシ３３５を使用して、クライアントマシンのＬＳＡ　Ｃｒｅｄ　ＳＳＰは、３４０においてポリシチェックを実行して、ユーザ証明情報を委譲すべきか否かを判断する。サーバが信頼されていない場合、３４５において、証明情報は委譲されない。３４０のポリシチェックによってサーバ関係が信頼される場合、３５０において、サーバの公開鍵が認証されることによって、不正（rogue）ソフトウェアオブジェクトが、サーバの挙動及び公開鍵を模倣する「中間者（man-in-the-middle）」攻撃の回避に役立つ。このため、３５０においてサーバの公開鍵が認証されない場合、３５５において中間者攻撃の危険に従って証明情報が委譲されない。３６０において、ＬＳＡの信頼されたサブシステムによってのみ理解される証明情報に対し、暗号化フォーマットが適用される。４６５において、暗号化された証明情報は、クライアントからサーバに委譲される。暗号化フォーマットを、ＬＳＡの信頼されたサブシステムによってのみ理解されるようにすることによって、有利には、本発明のＬＳＡ及びＣｒｅｄ　ＳＳＰに対するクライアント及びサーバの呼出しアプリケーションは、平文の証明情報に対し不適切なアクセスを行うことができない。

【００３７】

図４は、本発明の証明情報委譲プロトコルのより詳細な実施態様を、例示的な非限定的流れ図として示す。４００において、クライアントとサーバとの間でＳＳＬ／ＴＬＳハンドシェイクが完了し、クライアントとサーバとの間でＳＳＬ／ＴＬＳ暗号化鍵$K_{SSL/TLS}$が確立される。K_{pub}は、サーバの証明書における公開鍵である。次に、４１０において、暗号化されたＳＳＬ／ＴＬＳチャネルを介して、ＳＰＮＥＧＯパッケージを使用して、クライアント及びサーバの相互認証が完了する。クライアント／サーバ信頼関係に応じて、ケルベロス又はＮＴＬＭパッケージのいずれかがネゴシエートされ使用される。ＮＴＬＭがネゴシエートされる場合、サーバは、クライアントに対しパスワードを知っていることを証明するが、同じドメインの他のサーバはパスワードにアクセスすることができる。K_{spnego}は、ケルベロスサブセッションキーか又はＮＴＬＭセッションキーのいずれかであり、ＳＰＮＥＧＯ交換の完了時に両側によって共有される。

【００３８】

４２０において、クライアントマシンのＬＳＡ　Ｃｒｅｄ　ＳＳＰは、サーバのサービスプリンシパル名（ＳＰＮ）、サーバ認証情報（ＰＫＩ／ＫＲＢ対ＮＴＬＭ）及びグループポリシ設定に基づいてポリシチェックを実行して、ユーザの証明情報をサーバに委譲すべきか否かを判断する。そして、４３０において、以下の例示的な認証交換を実行するこ

とによって、$K_{SSL/TLS}$がターゲットサーバに属し中間者に属していないことを確認する。

【００３９】

C→S：｛｛K_{pub}｝K_{spnego}｝$K_{SSL/TLS}$

S→C：｛｛$K_{pub}+1$｝K_{spnego}｝$K_{SSL/TLS}$

$K_{SSL/TLS}$は、すべてのクライアント／サーバ通信を暗号化するのに使用されることに留意されたい。さらに、このサーバ認証ステップは、ＰＫＩベースの信頼がない場合、ケルベロス又はＮＴＬＭに基づいてもよい。上述したように、ケルベロスベース認証に対するＳＳＬ／ＴＬＳ認証されたチャネルの安全なバインディングを、ＳＳＬ／ＴＬＳの最上位で実行してもよい。言い換えれば、本発明は、ＳＳＬ／ＴＬＳネゴシエートされたマスタ／セッションキーを認証するために、ケルベロスベースの証明情報を安全に利用してもよく、それは、ＳＳＬ／ＴＬＳクライアントとＳＳＬ／ＴＬＳサーバとの間にＰＫＩ信頼がない場合に特に有用であり得る。

【００４０】

最後に、４４０において、ユーザの証明情報（たとえばパスワード）を、以下のシンボリックなデータ交換に従って本発明の信頼されたＬＳＡサブシステムによる以外の平文の証明情報レビューを防止する方法で、サーバに委譲してもよい。

【００４１】

C→S：｛｛パスワード｝K_{spnego}｝$K_{SSL/TLS}$

上述したように、たとえば図３のステップ３４０（及びグループポリシ３３５）及び図４のステップ４２０において、本発明によるクライアントの証明情報の委譲を制御及び制限して、広範囲のセキュリティ攻撃を軽減するのに、ポリシが利用される。上述したように、本発明のＬＳＡパッケージは、ＳＰＮＥＧＯネゴシエーションと、証明情報暗号化／解読と、証明情報転送とを提供する。本発明のＬＳＡパッケージはまた、本発明によって定義されるポリシに対しポリシチェックも実行する。本発明のグループポリシ設定の目的は、ユーザの証明情報が、認証されていないサーバ、たとえば不正者の管理制御下にあるか又は攻撃者に晒されているマシンに委譲されないことを確実にすることである。信頼は、たとえばＰＫＩ、ケルベロス又はＮＴＬＭ認証に基づいて、クライアントとサーバとの間の認証を容易にするように存在する可能性があるが、このような信頼は、ターゲットサーバがユーザの証明情報によって信頼されていることを意味するものではないことに留意されたい。このため、本発明は、ターゲットサーバを委譲された証明情報によって信頼することができることを確実にするポリシ調査（consultation）を含む。

【００４２】

図５は、呼出しアプリケーション（複数可）に平文の証明情報を晒すことなく、クライアントからサーバへの証明情報の安全な委譲を可能にする、本発明のＣｒｅｄ　ＳＳＰアーキテクチャの例示的な非限定的ブロック図である。図１と同様に、Ｃｒｅｄ　ＳＳＰは、クライアントＣ及びサーバＳの両方における２つのパッケージのセット、すなわちクライアント側パッケージ及びＬＳＡ側パッケージとして実装される。クライアントＣでは、これはクライアント側ＣｒｅｄＳＳＰ及びＬＳＡ側ＣｒｅｄＳＳＰになる。サーバＳでは、これはクライアント側ＣｒｅｄＳＳＰ’及びＬＳＡ側ＣｒｅｄＳＳＰ’になる。図５は、本発明によって、ユーザの平文の証明情報が、サーバ５１０のサーバアプリケーション、資源又はサービスＡＲＳを要求しているクライアント５００の呼出しアプリケーションＣＡに決して格納されず且つそれによってアクセス可能でないことを示す。ＬＳＡの信頼されたサブシステム部分を区分している点線は、ＬＳＡの信頼されたサブシステム部分のみが、ユーザの平文の証明情報にアクセスすることができる、すなわち解読／暗号化する能力を有することを示す。さらに、図５は、クライアントマシンのＬＳＡ側ＣｒｅｄＳＳＰが、後により詳細に説明するように、本発明のグループポリシＧＰを調査することを示す。

【００４３】

これに関して、表IIIにおいて後に示すグループポリシ設定は、ユーザの証明情報によ

っていずれのサーバが信頼されているかを定義しており、各設定は、サービスプリンシパル名（ＳＰＮ）のリストであり、一実施形態では、ワイルドカードが許容される。文字列認識技術における当業者が理解することができるように、ワイルドカードは、ＳＰＮのアルファベットにおいて許容可能な任意の文字又は文字列を表すことができる、「＊」等の文字を言う。このため、本発明によれば、たとえば、以下の表IIIに示すグループポリシ（ＧＰ）設定によって定義されるように、サーバがクライアントに認証され、且つサーバのＳＰＮがポリシチェックに合格する場合にのみ、ユーザの証明情報を委譲する。

【００４４】

表IIIにおいて以下に定義されるユーザ証明情報を委譲するポリシ設定は、限定されないが表Iに列挙する攻撃を含む種々の攻撃を軽減するように設計されている。

【００４５】

【表１】

1	トロイ又はマルウェアが、クライアントマシンにおいて、管理者モードではなく、たとえば制限されたユーザアクセス（ＬＵＡ）モードで実行している可能性がある。
2	デフォルトＧＰ設定対管理者によって構成され得る他のＧＰ値（ワイルドカードの誤用を含む）。
3	ドメインネームサービス（ＤＮＳ）ポイズニング。クライアントがホスト名を解決するとき、不正サーバと通信している場合がある。
4	ケルベロス鍵配布センタ（ＫＤＣ）におけるサービス拒否攻撃。

表Ｉ－ポリシ設定が軽減する攻撃のタイプ

本発明によっていずれのポリシが定義されるか（以下の表IIIにおいて例示的な非限定的形式で定義される）に関してなされる判断は、図３～図５及び証明情報のタイプに関連して上述したように、クライアントとサーバとの間でネゴシエートされる認証プロトコルによって決まる所与の状況に適用される。図６は、本発明による、ポリシが基づいてもよい、新規の証明情報と、デフォルト証明情報と、保存された証明情報とを含む、３つの例示的な証明情報のタイプを示す。新規の証明情報は、ＣｒｅｄＵＩ６１０等の証明情報ユーザインタフェースを介してリアルタイムに入力される証明情報である。保存された証明情報は、かつては新規の証明情報として入力され、ＣｒｅｄＭａｎ６００等の証明情報マネージャによってさらに再使用されるために、たとえば限られた期間格納されている証明情報である。保存された証明情報は、セキュリティの観点から、新規の証明情報より脆弱であるものとみなされる。さらに安全でないのはデフォルト証明情報であり、それは、名前が示唆するように、他の証明情報を使用する他の命令がない場合にＬＳＡ６２０によって使用されるように指定されているデフォルトの証明情報である。たとえば、デフォルト証明情報は、ログオン時刻に入力された証明情報を含んでもよい。デフォルト証明情報は、いくつかのＷｅｂサイト証明情報等、セキュリティの向上が必要でないいくつかの状況の場合に、十分であることもある。また、デフォルト証明情報は、それほど安全ではないが、ＬＳＡ６２０に即時に利用可能であるという利点がある。このため、図６に示すようにターミナルサーバクライアントＴＳＣによる要求に関連して利用してもよい３つのタイプの証明情報がある。表IIは、この例示的な非限定的実施形態で考えられる３つのタイプの証明情報、すなわち新規、保存及びデフォルトを示す。

【００４６】

【表２】

新規の証明情報	ＣｒｅｄＵＩ等のユーザインタフェースを介して収集され、ＳＳＰＩに直接渡される（たとえば AcquireCredentialsHandle コールに渡される）ユーザの証明情報
デフォルト証明情報	ユーザが最初にシステムにサインオンしたときに最初に提供した証明情報（ＳＳＰが利用可能）
保存された証明情報	ユーザが証明情報マネージャ（たとえばＣｒｅｄＭａｎ）に保存するよう決めた特定のターゲットサーバに関する証明情報

表Ⅱ－証明情報のタイプ

上述したように、以下の表IIIは、本発明による、クライアントによるサーバへのユーザ証明情報の委譲を制御／制限するグループポリシ（ＧＰ）設定の例示的な非限定的セットを含む。コンピュータネットワーキング技術における当業者が理解することができるように、Termsrv/*は、サービスがTermsrvであり、スラッシュ「／」の後に指定されているホストマシンが、＊ワイルドカードに一致するいかなるターゲットサーバであってもよい、ＳＰＮのセットを表す。

【００４７】

【表３－１】

#	ＧＰ設定 （ＳＰＮのリスト）	デフォルト値	コメント
1	AllowDefCredentials 意味：デフォルト証明情報で認証する場合にパスワードを列挙されたターゲットに渡してもよい	ヌル	デフォルト設定：デフォルトで、デフォルト証明情報の委譲（ユーザが最初にサインオンしたときに入力したもの）は、いかなるマシンにも許可されない。これは、ポリシチェックが失敗するため、クライアントマシンで（ＬＵＡモードで）実行しているマルウェアが、Ｃｒｅｄ　ＳＳＰを呼び出すことによって、（他のすべての要素、すなわち認証方式にも関わらず）デフォルト証明情報を委譲することができないことを意味する。
2	AllowSavedCredentials 意味：保存された証明情報で認証する場合に、パスワードを列挙されたターゲットに渡してもよい	Ｔｅｒｍｓｒｖ／*	デフォルト設定：デフォルト値は、ユーザの保存された証明情報の、いかなるマシンで実行しているターミナルサービスへの委譲も許可する。これは、ユーザが先にログインし自身の証明情報をＣｒｅｄＭａｎに保存するよう決めたサーバに適用されることに留意されたい。（ターゲットサーバ名はユーザの証明情報と共にＣｒｅｄＭａｎに格納される。）
3	AllowFreshCredentials 意味：新規の証明情報で認証する場合に、パスワードをターゲットに渡してもよい。	Ｔｅｒｍｓｒｖ／*	上記設定と比較すると、AllowFreshCredentials の場合、マルウェアがサイレントログインを実行している可能性がない（ユーザが最初に入力要求されていない場合、AllowSavedCredentials 及び AllowDefCredentials ポリシ設定は有効でないものと想定）。

【００４８】

【表３－２】

4	DenyDefCredentials 意味：デフォルト証明情報で認証する場合に、パスワードを列挙されたターゲットに渡してはならない。	ＮＵＬＬ	この設定は、ユーザのデフォルト証明情報をいずれのサーバに委譲することができるかをさらに制限するのに使用され、単独ではエクスプロイトの機会を提供しない。 しかしながら、管理者は、DenyDefCredentials 設定及び AllowDefCredentials 設定の組合せを介して、デフォルト証明情報のポリシを構成している場合、依然として注意するべきである。 AllowDefCredentials が広範囲のサーバのセットをカバーする場合、DenyDefCredentials を介して表される例外のリストは、所与の環境においてすべての信頼されないサーバを包括的にカバーしない場合がある。これは、新たなサーバがオンラインになる際に、経時的に特定の問題となる可能性がある。 さらに、管理特権を有するマルウェアは、DenyDefCredentials リストから信頼されていないサーバを除去することができる。しかしながら、管理特権を有するマルウェアは、このような場合にユーザのパスワードを取得する多数の方法があるため、「ゲームオーバ」状況である。
5	DenyFreshCredentials 意味：保存された証明情報で認証する場合に、パスワードを列挙されたターゲットに渡してはならない。	ＮＵＬＬ	この設定は、ユーザの保存された証明情報をいずれのサーバに委譲することができるかに対しさらに制限するのに使用され、単独ではエクスプロイトの機会を提供しない。

【００４９】

【表３－３】

6	DenyFreshCredentials 意味：新規の証明情報で認証する場合に、パスワードを列挙されたターゲットに渡してはならない。	ＮＵＬＬ	この設定は、ユーザの保存された証明情報をいずれのサーバに委譲することができるかに対しさらに制限するのに使用され、単独ではエクスプロイトの機会を提供しない。
7	AllowDefCredentialsWhenNTLMOnly 意味：認証パッケージがＮＴＬＭのみであり、且つユーザがデフォルト証明情報で認証する場合、パスワードを列挙されたターゲットに渡すことを許可する。	ＮＵＬＬ	ケルベロス及びＰＫＩベースの信頼がＮＴＬＭより強力な認証方法を提供するため、デフォルトでこの設定はオフである。
8	AllowSavedCredentialsWhenNYLMOnly 意味：認証がＮＴＬＭのみであり、且つユーザが保存された証明情報で認証する場合、パスワードを列挙されたターゲットに渡すことを許可する。	Ｔｅｒｍｓｒｖ／* （不参加） ＮＵＬＬ （参加）	ＮＴＬＭプロトコルにおける固有の脆弱性に対処するため、ユーザ証明情報の委譲は、ドメイン不参加マシンでのみデフォルトで許可される（この場合、サーバ認証は、ターゲットスタンドアロンマシンによって達成されることが保証される。） ドメイン参加の場合、デフォルトで、ＮＴＬＭ単独では許可されない（サーバ認証はケルベロス又はＰＫＩに基づく。）
9	AllowFreshCredentialsWhenNTLMOnly 意味：認証がＮＴＬＭのみであり、且つユーザが新規の証明情報で認証する場合、パスワードを列挙されたターゲットに渡すことを許可する。	Ｔｅｒｍｓｒｖ／*	

表Ⅲ－ユーザ証明情報の委譲を制御／制限するグループポリシ設定

要約すると、本発明のＣｒｅｄ　ＳＳＰソリューションは、クライアントからサーバへのユーザ証明情報の委譲を制御及び制限するのに使用することができるポリシのセットを提供することによって、従来より安全なソリューションを提供する。表IIIのポリシの例示的な非限定的セットが示すように、ポリシは、クライアントのマシンで実行しているマルウェアを含む広範囲の攻撃に対処するように設計される。さらに、本発明のＣｒｅｄ ＳＳＰは、「デフォルトで安全な」ポリシを含み、それは、クライアントマシンがデフォ

ルトで広範囲の攻撃を軽減することができるようにするポリシ設定を介する特定の構成である。さらに、本発明のポリシのセットは、限定されないがユーザ名／パスワード、スマートカードＰＩＮ、ワンタイムパスコード（ＯＴＰ）等を含むいかなるタイプのユーザ証明情報の保護にも適用可能である。本発明のＣｒｅｄ　ＳＳＰは、ＬＳＡの信頼されたサブシステムのみが平文の証明情報にアクセスすることができるため、サーバ又はクライアント側の（Ｃｒｅｄ　ＳＳＰ　ＡＰＩの）呼出しアプリケーションはユーザの平文の証明情報へのアクセスを決して与えられないため、ユーザ証明情報に対しさらなる保護を提供する。

例示的なネットワーク環境及び分散環境

当業者は、本発明を、コンピュータネットワークの一部として又は分散コンピューティング環境において配備することができる、任意のコンピュータ又は他のクライアント装置若しくはサーバ装置に関連して実施することができることを理解することができる。これに関して、本発明は、本発明によるクライアントからサーバへ証明情報を委譲するプロセスに関連して使用することができる、いかなる数のメモリ又は記憶ユニット、及びいかなる数の記憶ユニット又はボリュームにわたって発生するいかなる数のアプリケーション及びプロセスを有する、いかなるコンピュータシステム又は環境にも関連する。本発明は、サーバコンピュータ及びクライアントコンピュータが、リモート記憶装置又はローカル記憶装置を有する、ネットワーク環境又は分散コンピューティング環境に配備される環境に適用され得る。本発明はまた、リモート又はローカルサービス及びプロセスに関連して情報を生成、受信、及び送信する、プログラミング言語機能、解釈及び実行機能を有する、スタンドアロンコンピューティング装置にも適用可能である。

【００５０】

分散コンピューティングは、コンピューティング装置とシステムとの間の交換による、コンピュータ資源及びサービスの共有を提供する。これらの資源及びサービスには、情報の交換、キャッシュ記憶、及び、ファイル等のオブジェクトのディスク記憶が含まれる。分散コンピューティングは、ネットワーク接続性を利用し、クライアントがそれらの集合的な力を活用して企業全体の利益を得ることができるようにする。これに関して、種々の装置が、本発明の証明情報をクライアントからサーバに委譲するシステム及び方法を関与させ得るアプリケーション、オブジェクト又は資源を有することができる。

【００５１】

図７Ａは、例示的なネットワークコンピューティング環境又は分散コンピューティング環境の概略図を提供する。分散コンピューティング環境は、コンピューティングオブジェクト１０ａ、１０ｂ等と、コンピューティングオブジェクト又は装置１１０ａ、１１０ｂ、１１０ｃ等とを含む。これらのオブジェクトは、プログラム、メソッド、データストア、プログラマブルロジック等を含むことができる。オブジェクトは、ＰＤＡ、オーディオ／ビデオ装置、ＭＰ３プレイヤ、パーソナルコンピュータ等のような、同じか又は異なる装置の部分を含んでもよい。各オブジェクトは、通信ネットワーク１４を用いて互いに通信することができる。このネットワークは、それ自体が図７Ａのシステムにサービスを提供する他のコンピューティングオブジェクト及びコンピューティング装置を含んでもよく、それ自体が複数の相互接続されたネットワークを表してもよい。本発明の一態様によれば、各オブジェクト１０ａ、１０ｂ等、又は１１０ａ、１１０ｂ、１１０ｃ等は、本発明による証明情報をクライアントからサーバに委譲するシステム及び方法と共に使用するのに適している、ＡＰＩ、又は他のオブジェクト、ソフトウェア、ファームウェア及び／若しくはハードウェアを利用することができる、アプリケーションを含んでもよい。

【００５２】

１１０ｃ等のオブジェクトを、別のコンピューティング装置１０ａ、１０ｂ等又は１１０ａ、１１０ｂ等でホストしてもよいということも理解することができる。このため、図示する物理的環境は接続された装置をコンピュータとして示している可能性があるが、このような図は単に例示的なものであり、物理的環境は、代替的に、ＰＤＡ、テレビ、ＭＰ３プレイヤ等のようなさまざまなデジタル装置、インタフェース等のソフトウェアオブジ

ェクト、ＣＯＭオブジェクト等を含むように示すか又は説明されてもよい。

【００５３】

分散コンピューティング環境をサポートする種々のシステム、コンポーネント及びネットワーク構成がある。たとえば、コンピューティングシステムを、有線システム又は無線システムによって、ローカルネットワーク又は広く分散したネットワークによって、互いに接続することができる。目下、ネットワークの多くはインターネットに結合されており、インターネットは、広く分散したコンピューティングに対するインフラストラクチャを提供し、多くの異なるネットワークを包含する。本発明による証明情報をクライアントからサーバへの委譲に付随することになる例示的な通信のために、インフラストラクチャのうちのいずれを使用してもよい。

【００５４】

ホームネットワーキング環境には、電力線、データ（無線及び有線両方）、音声（たとえば電話）、及びエンターテイメントメディア等、各々が一意のプロトコルをサポートすることができる、少なくとも４つの異なるネットワーク移送媒体が存在する。光スイッチ及び器具等の大部分の家庭用制御装置は、接続のために電力線を使用することができる。データサービスは、ブロードバンド（たとえばＤＬＳ又はケーブルモデムのいずれか）として家庭に入ることができ、無線（たとえばＨｏｍｅＲＦ又は８０２．１１Ｂ）接続又は有線（たとえばＨｏｍｅ　ＰＮＡ、Ｃａｔ　５、イーサネット（登録商標）、さらには電力線）接続を使用して、家庭内でアクセス可能である。音声トラフィックは、有線（たとえばＣａｔ　３）又は無線（たとえば携帯電話）として家庭に入ることができ、Ｃａｔ　３配線を使用して家庭内で分配されることが可能である。エンターテイメントメディア、又は他のグラフィカルデータは、衛星又はケーブルによって家庭に入ることができ、通常、家庭において同軸ケーブルを使用して分配される。ＩＥＥＥ１３９４及びＤＶＩもまた、メディア装置のクラスタ用のデジタル相互接続である。これらのネットワーク環境のすべて、及びプロトコル標準規格として出現し得るか又はすでに出現している他のネットワーク環境を、インターネット等の広域ネットワークによって外部の世界に接続され得る、イントラネット等のネットワークを形成するように相互接続することができる。要約すれば、データの格納及び伝送のために、種々の異なる資源が存在し、したがって、進歩しているコンピューティング装置には、本発明による証明情報のクライアントからサーバへの委譲中等、プログラムオブジェクトに付随してアクセスされるか又は利用されるデータ等のデータを共有する方法が必要になる。

【００５５】

インターネットは、一般に、コンピュータネットワーキングの技術において既知である、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）のプロトコル一式を利用するネットワーク及びゲートウェイの集まりを指す。インターネットを、ユーザがネットワーク（複数可）を介して情報と対話し情報を共有することができるようにするネットワーキングプロトコルを実行しているコンピュータによって相互接続される、地理的に分散したリモートコンピュータネットワークのシステムとして述べることができる。したがって、このような広範にわたる情報共有のために、一般にインターネット等のリモートネットワークは、これまで、開発者が、専用の動作又はサービスを実行するソフトウェアアプリケーションを本質的に制限なく設計することができる、オープンシステムにまで発展してきた。

【００５６】

このため、ネットワークインフラストラクチャによって、クライアント／サーバ、ピア・ツー・ピア又はハイブリッドアーキテクチャ等のネットワークトポロジのホストが可能になる。「クライアント」は、関連していない別のクラス又はグループのサービスを使用するクラス又はグループのメンバである。このため、コンピューティングにおいて、クライアントは、別のプログラムによって提供されるサービスを要求する、プロセス、すなわち大まかには命令又はタスクのセットである。クライアントプロセスは、他のプログラム又はサービス自体に関するいかなる作業詳細も「知る」必要なく、要求したサービスを利

用する。クライアント／サーバアーキテクチャ、特にネットワークシステムでは、クライアントは、通常、別のコンピュータ、たとえばサーバによって提供される共有ネットワーク資源にアクセスするコンピュータである。図７Ａの図では、例として、コンピュータ１１０ａ、１１０ｂ等をクライアントと考えることができ、コンピュータ１０ａ、１０ｂ等をサーバと考えることができ、その場合、サーバ１０ａ、１０ｂ等は、後にクライアントコンピュータ１１０ａ、１１０ｂ等に複製されるデータを保持するが、環境に応じて、いかなるコンピュータも、クライアント、サーバ又はその両方とみなすことができる。これらのコンピューティング装置のいずれもが、本発明による証明情報のクライアントからサーバへの委譲を含む可能性のあるデータを処理しているか又はサービス若しくはタスクを要求していてもよい。

【００５７】

サーバは、通常、インターネット等のリモートネットワーク又はローカルネットワークにわたってアクセス可能なリモートコンピュータシステムである。クライアントプロセスは、第１のコンピュータシステムにおいてアクティブであってもよく、サーバプロセスは第２のコンピュータシステムにおいてアクティブであってもよく、それらは通信媒体を介して互いに通信し、それによって分散機能が提供され、複数のクライアントがサーバの情報収集能力を利用することができるようになる。本発明の証明情報をクライアントからサーバに委譲する技法に従って利用される任意のソフトウェアオブジェクトを、複数のコンピューティング装置又はオブジェクトにわたって分散することができる。

【００５８】

クライアント（複数可）及びサーバ（複数可）は、プロトコル層（複数可）によって提供される機能を利用して互いに通信する。たとえば、ハイパーテキスト転送プロトコル（ＨＴＴＰ）は、ワールドワイドウェブ（WWW）又は「Ｗｅｂ」と共に使用される一般的なプロトコルである。通常、インターネットプロトコル（ＩＰ）アドレス等のコンピュータネットワークアドレス、又はユニバーサルリソースロケータ（ＵＲＬ）等の他の参照を使用して、サーバコンピュータ又はクライアントコンピュータを互いに対して識別することができる。ネットワークアドレスを、ＵＲＬアドレスと称することができる。通信を、通信媒体によって提供してもよく、たとえば、クライアント（複数可）及びサーバ（複数可）を、大容量通信のためにＴＣＰ／ＩＰ接続（複数可）を介して互いに結合してもよい。

【００５９】

このため、図７Ａは、本発明を実施することができる、サーバ（複数可）がネットワーク／バスを介してクライアントコンピュータ（複数可）と通信する、例示的なネットワーク環境又は分散環境を示す。より詳細には、複数のサーバ１０ａ、１０ｂ等が、ＬＡＮ、ＷＡＮ、イントラネット、インターネット等であることができる通信ネットワーク／バス１４を介して、ポータブルコンピュータ、ハンドヘルドコンピュータ、シンクライアント、ネットワークアプライアンス、又は本発明によるＶＣＲ、ＴＶ、オーブン、照明、ヒータ等のような、他の装置等の複数のクライアント又はリモートコンピューティング装置１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ等と相互接続される。このため、本発明は、共にユーザ証明情報をサーバに委譲することが望ましい、いかなるコンピューティング装置にも適用され得ることが企図される。

【００６０】

通信ネットワーク／バス１４がインターネットであるネットワーク環境では、たとえば、サーバ１０ａ、１０ｂ等はＷｅｂサーバであってもよく、クライアント１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ等は、ＨＴＴＰ等の複数の既知のプロトコルのうちのいずれかを介してそれと通信する。分散コンピューティング環境の特徴であり得るように、サーバ１０ａ、１０ｂ等はまた、クライアント１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ等としての役割を果たしてもよい。

【００６１】

上述したように、適切な場合は、通信は有線若しくは無線、又は組合せであってもよい

。クライアント装置１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ等は、通信ネットワーク／バス１４を介して通信してもしなくてもよく、独立した通信が関連してもよい。たとえば、ＴＶ又はＶＣＲの場合、その制御に対してネットワーク化態様があってもなくてもよい。各クライアントコンピュータ１１０ａ、ｌ１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ等及びサーバコンピュータ１０ａ、１０ｂ等に、さまざまなアプリケーションプログラムモジュール又はオブジェクト１３５ａ、１３５ｂ、１３５ｃ等を備えてもよく、且つファイル又はデータストリームを格納してもよく、又はファイル又はデータストリームの一部（複数可）をダウンロード、伝送又は移行してもよい、さまざまなタイプの記憶要素又はオブジェクトへの接続又はアクセスを備えてもよい。コンピュータ１０ａ、１０ｂ、１１０ａ、１１０ｂ等のうちの任意の１つ又は複数は、本発明によって処理されるか又は保存されるデータを格納するデータベース又はメモリ２０等、データベース２０又は他の記憶要素の保守及び更新に関与してもよい。このため、本発明を、コンピュータネットワーク／バス１４にアクセスしそれと対話することができるクライアントコンピュータ１１０ａ、１１０ｂ等と、クライアントコンピュータ１１０ａ、１１０ｂ等及び他の同様の装置並びにデータベース２０と対話することができるサーバコンピュータ１０ａ、１０ｂ等とを有するコンピュータネットワーク環境で利用することができる。

例示的なコンピューティング装置

上述したように、本発明は、一次アプリケーションを装置の二次アプリケーションからの干渉から保護することが望まれ得るいかなる装置にも適用される。したがって、本発明に関連して、すなわち装置がサーバに証明情報を委譲するよう望む可能性のある任意の場所（たとえば、携帯電話等のポータブル装置を介するＧＳＭネットワーク）で使用するために、ハンドヘルド装置、ポータブル装置及び他のコンピューティング装置並びにすべての種類のコンピューティングオブジェクトが考えられることを理解されたい。したがって、図７Ｂにおいて後述する以下の汎用リモートコンピュータは単なる一例であり、本発明を、ネットワーク／バス相互運用性及び対話を有するいかなるクライアントで実施してもよい。このため、本発明を、ごくわずかな又は最低限のクライアント資源が関与するネットワークホストサービスの環境、たとえば、クライアント装置が、アプライアンスに配置されたオブジェクト等、単にネットワーク／バスに対するインタフェースとしての役割を果たすネットワーク環境で実施してもよい。

【００６２】

必須ではないが、本発明を、部分的に、装置又はオブジェクトに対するサービスの開発者によって使用されるために、オペレーティングシステムを介して実施してもよく、且つ／又は本発明の構成要素（複数可）に関連して動作するアプリケーションソフトウェア内に含めてもよい。ソフトウェアを、クライアントワークステーション、サーバ又は他の装置等、１つ又は複数のコンピュータによって実行されている、プログラムモジュール等のコンピュータ実行可能命令の一般的な状況で説明することができる。当業者は、本発明を、他のコンピュータシステム構成及びプロトコルで実施してもよいということを理解するであろう。

【００６３】

このため、図７Ｂは、本発明を実施することができる適切なコンピューティングシステム環境１００ａの一例を示すが、先に明らかにしたように、コンピューティングシステム環境１００ａは、コンピューティング装置に対する適切なコンピューティング環境の単なる一例であり、本発明の使用又は機能の範囲に関していかなる限定も示唆するように意図されていはいない。コンピューティング環境１００ａは、例示的な動作環境１００ａに例示する構成要素のうちのいずれか１つ又は組合せに関連する任意の依存性又は要件を有するものとしても解釈されるべきではない。

【００６４】

図７Ｂを参照すると、本発明を実施する例示的なリモート装置は、コンピュータ１１０ａの形態の汎用コンピューティング装置を備える。コンピュータ１１０ａの構成要素には、限定されないが、処理ユニット１２０ａと、システムメモリ１３０ａと、システムメモ

リを含むさまざまなシステムコンポーネントを処理ユニット１２０ａに結合するシステムバス１２１ａとが含まれることができる。システムバス１２１ａは、さまざまなバスアーキテクチャのうちの任意のものを使用する、メモリバス又はメモリコントローラ、周辺バス、及びローカルバスを含む、いくつかのタイプのバス構造のうちの任意のものであることができる。

【００６５】

コンピュータ１１０ａは、通常、種々のコンピュータ可読媒体を備える。コンピュータ可読媒体は、コンピュータ１１０ａがアクセスすることができるいかなる利用可能媒体であってもよい。限定としてではなく例として、コンピュータ可読媒体は、コンピュータ記憶媒体及び通信媒体を含んでもよい。コンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール又は他のデータ等の情報を格納する任意の方法又は技術で実装される、揮発性及び不揮発の両方、取外し可能及び取外し不可能の両方の媒体を含む。コンピュータ記憶媒体は、限定されないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ又は他のメモリ技術、ＣＤＲＯＭ、デジタル多用途ディスク（ＤＶＤ）若しくは他の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置若しくは他の磁気記憶装置、又は、所望の情報を格納するのに使用することができると共にコンピュータ１１０ａがアクセスすることができる他の任意の媒体を含む。通信媒体は、通常、コンピュータ可読命令、データ構造、プログラムモジュール又は他のデータを、搬送波又は他の搬送メカニズム等の変調データ信号で具現化し、任意の情報配信媒体を含む。

【００６６】

システムメモリ１３０ａは、読出し専用メモリ（ＲＯＭ）及び／又はランダムアクセスメモリ（ＲＡＭ）等の揮発性及び／又は不揮発性メモリの形態のコンピュータ記憶媒体を備えることができる。立ち上げ時等にコンピュータ１１０ａ内の要素間で情報を転送するのに役立つ基本ルーチンを含む基本入出力システム（ＢＩＯＳ）をメモリ１３０ａに格納することができる。メモリ１３０ａは、通常、処理ユニット１２０ａによって即座にアクセス可能であり且つ／又は処理ユニット１２０ａで目下動作しているデータ及び／又はプログラムモジュールも含む。限定としてではなく例として、メモリ１３０ａはまた、オペレーティングシステム、アプリケーションプログラム、他のプログラムモジュール及びプログラムデータを含むことができる。

【００６７】

コンピュータ１１０ａはまた、他の取外し可能／取外し不可能、揮発性／不揮発性コンピュータ記憶媒体を備えることができる。たとえば、コンピュータ１１０ａは、取外し不可能な不揮発性磁気媒体に対し読出し又は書込みを行うハードディスクドライブ、取外し可能な不揮発性磁気ディスクに対し読出し又は書込みを行う磁気ディスクドライブ、及び／又はＣＤ－ＲＯＭ若しくは他の光媒体等、取外し可能な不揮発性光ディスクに対し読出し又は書込みを行う光ディスクドライブを含んでもよい。例示的な動作環境で使用することができる他の取外し可能／取外し不可能な揮発性／不揮発性コンピュータ記憶媒体には、限定されないが、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、半導体ＲＡＭ、半導体ＲＯＭ等が含まれる。ハードディスクドライブは、通常、インタフェース等の取外し不可能なメモリインタフェースを通じてシステムバス１２１ａに接続され、磁気ディスクドライブ又は光ディスクドライブは、通常、インタフェース等の取外し可能なメモリインタフェースによってシステムバス１２１ａに接続される。

【００６８】

ユーザは、キーボード、及び一般にマウス、トラックボール又はタッチパッドと称されるポインティングデバイス等の入力装置を通じて、コンピュータ１１０ａにコマンド及び情報を入力することができる。他の入力装置には、マイクロフォン、ジョイスティック、ゲームパッド、パラボラアンテナ、スキャナ等が含まれ得る。これらの及び他の入力装置は、システムバス１２１ａに結合されたユーザ入力１４０ａ及び関連インタフェース（複数可）を通じて処理ユニット１２０ａに接続されることが多いが、パラレルポート、ゲー

ムポート又はユニバーサルシリアルバス（ＵＳＢ）等の他のインタフェース及びバス構造によって接続されてもよい。システムバス１２１ａにグラフィックスサブシステムもまた接続してもよい。モニタ又は他のタイプの表示装置もまた、出力インタフェース１５０ａ等のインタフェースを介してシステムバス１２１ａに接続され、出力インタフェース１５０ａはビデオメモリと通信することができる。モニタに加えて、コンピュータもまた、出力インタフェース１５０ａを通じて接続され得るスピーカ及びプリンタ等の他の周辺出力装置を含んでもよい。

【００６９】

コンピュータ１１０ａは、装置１１０ａとは異なる、メディア機能等の機能を有することができる、リモートコンピュータ１７０ａ等の１つ又は複数の他のリモートコンピュータとの論理接続を使用する、ネットワーク環境又は分散環境において動作することができる。リモートコンピュータ１７０ａは、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピア装置若しくは他の一般的なネットワークノード、又は他の任意のリモートメディア消費若しくは伝送装置であってもよく、コンピュータ１１０ａに対して上述した要素のうちの任意のもの又はすべてを含んでもよい。図７Ｂに示す論理接続は、ローカルエリアネットワーク（ＬＡＮ）又は広域ネットワーク（ＷＡＮ）等のネットワーク１７１ａを含むが、他のネットワーク／バスを含んでもよい。このようなネットワーキング環境は、家庭、オフィス、企業規模のコンピュータネットワーク、イントラネット及びインターネットにおいて一般的である。

【００７０】

ＬＡＮネットワーキング環境で使用される場合、コンピュータ１１０ａは、ネットワークインタフェース又はアダプタを通じてＬＡＮ１７１ａに接続される。ＷＡＮネットワーキング環境で使用される場合、コンピュータ１１０ａは、通常、インターネット等のＷＡＮを介した通信を確立するためのネットワークコンポーネント（ネットワークカード、モデム等）又は他の手段を備える。内蔵であっても外付けであってもよい、ネットワークに接続する手段を、入力１４０ａのユーザ入力インタフェース又は他の適切なメカニズムを介してシステムバス１２１ａに接続することができる。ネットワーク環境では、コンピュータ１１０ａに対して示すプログラムモジュール又はその一部を、リモートメモリ記憶装置に格納することができる。図示し説明するネットワーク接続は例示的なものであり、コンピュータ間の通信リンクを確立する他の手段を使用してもよいということが理解されよう。

例示的な分散コンピューティングフレームワーク又はアーキテクチャ

パーソナルコンピューティング及びインターネットの収束に鑑みて、さまざまな分散ンコンピューティングフレームワークが開発されている。個人及びビジネスユーザにも同様に、アプリケーション及びコンピューティング装置に対するシームレスに相互運用可能且つウェブ対応インタフェースが提供され、コンピューティングアクティビティがますますＷｅｂブラウザ又はネットワーク志向になってきている。

【００７１】

たとえば、ＭＩＣＲＯＳＯＦＴ（登録商標）の管理コードプラットフォーム、すなわち．ＮＥＴは、サーバと、Ｗｅｂベースのデータ記憶及びダウンロード可能デバイスソフトウェア等のビルディングブロックサービスとを含む。概して、ＮＥＴプラットフォームは、（１）コンピューティング装置の全範囲を合わせて機能させ、それらのすべてにおいてユーザ情報を自動的に更新及び同期させる機能、（２）ＨＴＭＬではなくＸＭＬを多用することで可能となるＷｅｂページ用の強化された対話機能、（３）たとえば電子メール又はＯｆｆｉｃｅ．ＮＥＴ等のソフトウェア等のさまざまなアプリケーションを管理するための、製品及びサービスに対するカスタマイズされたアクセス、及び中央の起点からユーザへのそれらの送達を特徴とするオンラインサービス、（４）情報へのアクセスの効率及び容易さと共に、ユーザ及び装置間での情報の同期を向上させる集中データストレージ、（５）電子メール、ファックス及び電話等のさまざまな通信媒体を統合する機能、（６）再使用可能なモジュールを作成し、それによって生産性を向上させると共に、プログラミ

ングエラーの数を低減する機能、並びに（７）同様に多くの他のクロスプラットフォーム及び言語の統合機能を提供する。

【００７２】

本明細書において、いくつかの例示的な実施形態を、コンピューティング装置に常駐するアプリケーションプログラミングインタフェース（ＡＰＩ）等のソフトウェアに関して説明しているが、本発明の１つ又は複数の部分を、オペレーティングシステム、又は「仲介人（middle man）」オブジェクト、コントロールオブジェクト、ハードウェア、ファームウェア、中間言語命令又はオブジェクト等を介して実装してもよく、それによって、本発明による証明情報をクライアントからサーバに委譲する方法を、ＮＥＴコード等の管理コードによって使用可能となる言語及びサービスのすべてに含めてもよく、それらにおいてサポートしてもよく、又はそれらを介してアクセスしてもよく、他の分散コンピューティングフレームワークでも同様である。

【００７３】

アプリケーション及びサービスが、本発明の証明情報をクライアントからサーバに委譲するシステム及び方法を使用することを可能にする、たとえば、適切なＡＰＩ、ツールキット、ドライバコード、オペレーティングシステム、コントロール、スタンドアロンソフトウェアオブジェクト又はダウンロード可能ソフトウェアオブジェクト等、本発明を実施する複数の方法がある。本発明は、ＡＰＩ（又は他のソフトウェアオブジェクト）の観点から、同様に、本発明に従ってダウンロードされたプログラムを受け取るソフトウェアオブジェクト又はハードウェアオブジェクトから、本発明を使用することを企図している。このため、本明細書に記載した本発明のさまざまな実施態様は、全体としてハードウェアに、部分的にハードウェアに且つ部分的にソフトウェアに、且つソフトウェアにある態様を有してもよい。

【００７４】

上述したように、本発明の例示的な実施形態を、さまざまなコンピューティング装置及びネットワークアーキテクチャに関連して説明したが、基礎となる概念を、証明情報をクライアントからサーバに委譲することが望ましい、いかなるコンピューティング装置又はシステムにも適用することができる。たとえば、本発明のアルゴリズム（複数可）及びハードウェアインプリメンテーションを、コンピューティング装置のオペレーティングシステムに適用してもよく、装置上の別個のオブジェクトとして、別のオブジェクトの一部として、再使用可能なコントロールとして、サーバからダウンロード可能なオブジェクトとして、装置又はオブジェクトとネットワークとの間の「仲介人」として、分散オブジェクトとして、ハードウェアとして、メモリ内で、上述したもののうちのいずれかの組合せ等として提供してもよい。本明細書において例示的なプログラミング言語、名前及び例をさまざまな選択肢の代表として選択しているが、これらの言語、名前及び例は、限定するものとして意図されていない。当業者は、本発明のさまざまな実施形態によって達成される機能と同じか、同様か又は等価な機能を達成する、オブジェクトコード及び命名法を提供する多数の方法があることを理解するであろう。

【００７５】

上述したように、本明細書に記載したさまざまな技法を、ハードウェア若しくはソフトウェア、又は適切な場合はそれらの両方の組合せに関連して実装してもよい。このため、本発明の方法及び装置、又はそのいくつかの態様又は一部は、フロッピー（登録商標）ディスケット、ＣＤ－ＲＯＭ、ハードドライブ、又は他の任意の機械可読記憶媒体等の有形媒体で具現化されるプログラムコード（すなわち命令）の形態をとってもよく、プログラムコードがコンピュータ等の機械にロードされ、その機械によって実行されるとき、機械は、本発明を実施する装置となる。プログラムコードをプログラム可能コンピュータで実行する場合、コンピューティング装置は一般に、プロセッサと、プロセッサによって読出し可能な記憶媒体（揮発性及び不揮発性メモリ並びに／又は記憶要素を含む）と、少なくとも１つの入力装置と、少なくとも１つの出力装置とを含む。たとえばデータ処理ＡＰＩ、再使用可能コントロール等を使用して、本発明の証明情報をクライアントからサーバに

委譲する方法を実装するか又は利用することができる１つ又は複数のプログラムは、コンピュータシステムと通信する高水準手続き型又はオブジェクト指向プログラミング言語で実施されることが好ましい。しかしながら、望ましい場合、プログラム（複数可）を、アセンブリ言語又は機械言語で実装することができる。いずれの場合も、言語はコンパイル型言語であってもインタプリタ型言語であってもよく、ハードウェアインプリメンテーションと結合されてもよい。

【００７６】

本発明の方法及び装置を、電気的配線又はケーブル布線を介して、光ファイバを通じて、又は他の任意の伝送形態を介して等、何らかの伝送媒体によって伝送されるプログラムコードの形式で具現化された通信を介して実施してもよく、プログラムコードが、ＥＰＲＯＭ、ゲートアレイ、プログラマブルロジックデバイス（ＰＬＤ）、クライアントコンピュータ等のような、機械によって受け取られロードされるとき、機械は、本発明を実施する装置となる。汎用プロセッサで実装される場合、プログラムコードはプロセッサと結合して、本発明の機能を呼び出すように動作する一意の装置を提供する。さらに、本発明に関連して使用される任意の記憶技法は、常にハードウェア及びソフトウェアの組合せであってもよい。

【００７７】

本発明を、さまざまな図の好ましい実施形態に関連して説明したが、本発明から逸脱することなく、本発明の同じ機能を実行するために、他の同様の実施形態を使用してもよく、又は説明した実施形態に対し変更及び追加を行ってもよいことが理解されるであろう。たとえば、本発明の例示的なネットワーク環境を、ピア・ツー・ピアネットワーク環境等のネットワーク環境の状況で説明しているが、当業者は、本発明がそれに限定されず、本明細書で説明したような方法を、ゲームコンソール、ハンドヘルドコンピュータ、ポータブルコンピュータ等の任意のコンピューティング装置又は環境に、有線であるか無線であるかに関わらず適用してもよく、通信ネットワークを介して接続されると共にネットワークにわたって対話するいかなる数のこのようなコンピューティング装置に適用してもよいということを理解するであろう。さらに、特に無線ネットワーク装置の数が急増し続けているため、ハンドヘルド装置オペレーティングシステム及び他のアプリケーション特定オペレーティングシステムを含む種々のコンピュータプラットフォームが企図されるということが強調されるべきである。

【００７８】

例示的な実施形態は、特定のプログラミング言語制約の文脈で本発明を利用することに言及しているが、本発明はそのように限定されるものではなく、証明情報をクライアントからサーバに委譲する方法を提供するための任意言語で実装することができる。さらに、本発明を複数の処理チップ又は装置内で又はそれらにわたって実施してもよく、同様に格納を複数の装置にわたって行ってもよい。したがって、本発明は、いかなる単一の実施形態にも限定されるべきではなく、添付の特許請求の範囲による広さ及び範囲内で解釈されるべきである。

【図面の簡単な説明】

【００７９】

【図１】証明情報のクライアントからサーバへの安全な委譲を可能にする、本発明の証明情報セキュリティサポートプロバイダアーキテクチャの概略ブロック図である。

【図２Ａ】証明情報をターミナルサーバに委譲する、証明情報セキュリティサポートプロバイダアーキテクチャの例示的な非限定的実施態様を示す図である。

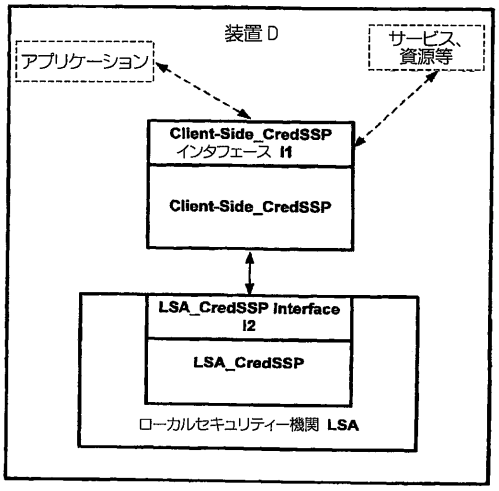
【図２Ｂ】証明情報をターミナルサーバに委譲する、証明情報セキュリティサポートプロバイダアーキテクチャの例示的な非限定的実施態様を示す図である。

【図３】本発明の証明情報セキュリティサポートプロバイダアーキテクチャによって利用される、例示的な非限定的プロトコルの流れ図である。

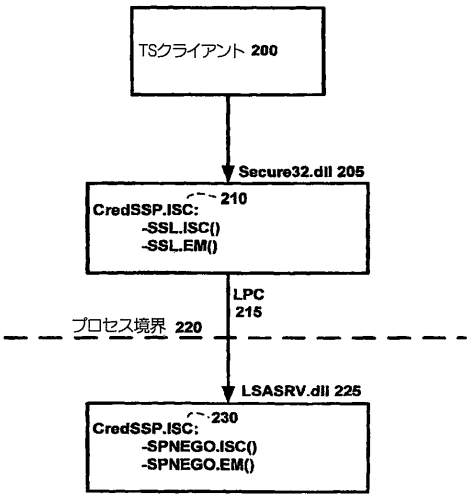
【図４】本発明の証明情報セキュリティサポートプロバイダアーキテクチャによって利用されるプロトコルの例示的な非限定的実施態様の流れ図である。

【図５】本発明による、グループポリシに基づく証明情報のクライアントからサーバへの安全な委譲を可能にする、証明情報セキュリティサポートプロバイダの概略ブロック図である。
【図６】本発明による、攻撃の脅威によってポリシレベルで考慮され得る３つの異なるタイプの証明情報の概略ブロック図である。
【図７Ａ】本発明を実施することができる例示的なネットワーク環境を表すブロック図である。
【図７Ｂ】本発明を実施することができる例示的な非限定的コンピューティングシステム環境を表すブロック図である。

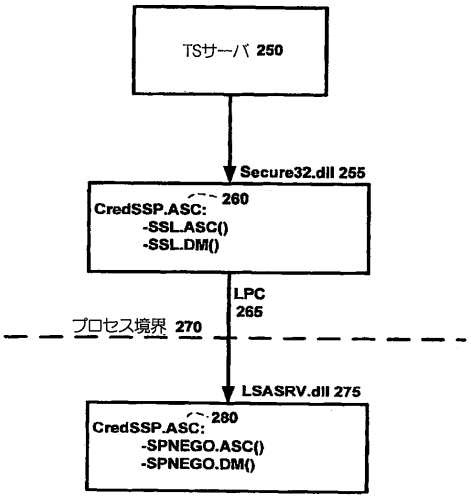
【図１】



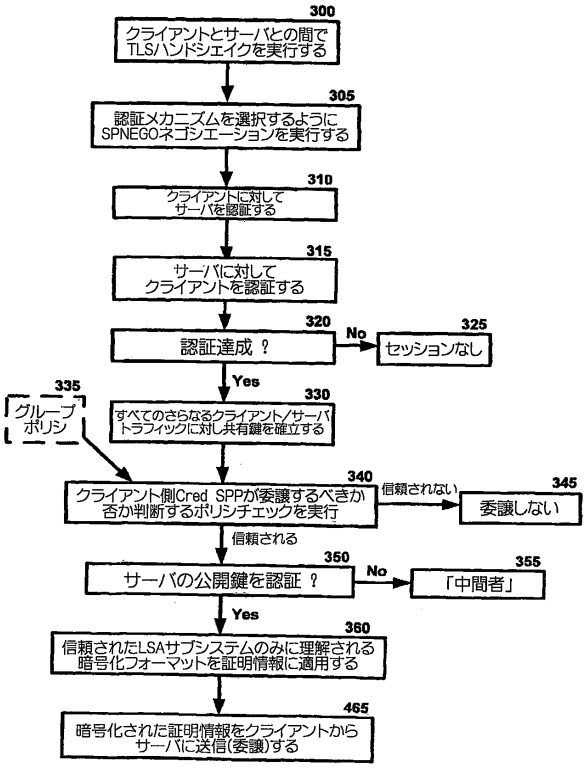
【図２Ａ】



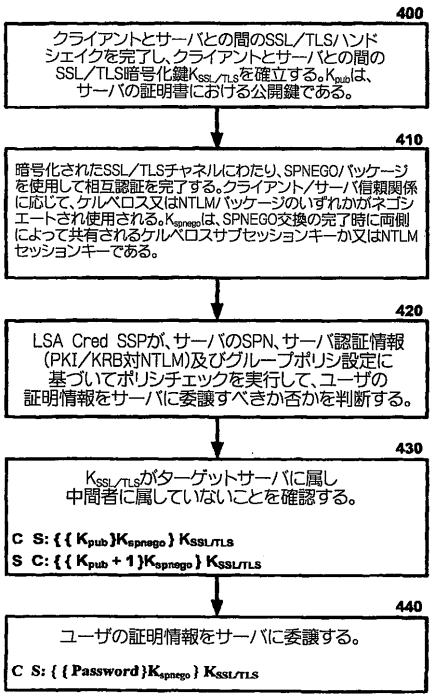
【図２Ｂ】


TSサーバ 250
Secure32.dll 255
260
CredSSP.ASC:
-SSL.ASC()
-SSL.DM()
LPC
265
プロセス境界 270
LSASRV.dll 275
280
CredSSP.ASC:
-SPNEGO.ASC()
-SPNEGO.DM()

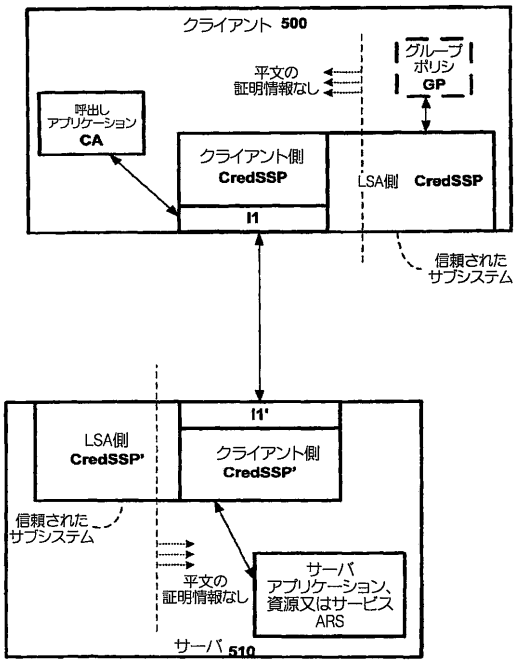
【図３】


300
クライアントとサーバとの間で
TLSハンドシェイクを実行する
305
認証メカニズムを選択するように
SPNEGOネゴシエーションを実行する
310
クライアントに対して
サーバを認証する
315
サーバに対して
クライアントを認証する
320
認証達成 ？
No
325
セッションなし
Yes
335
グループ
ポリシ
330
すべてのさらなるクライアント/サーバ
トラフィックに対し共有鍵を確立する
340
クライアント側Cred SPPが委譲するべきか
否か判断するポリシチェックを実行
信頼されない
345
委譲しない
信頼される
350
サーバの公開鍵を認証 ？
No
355
「中間者」
Yes
360
信頼されたLSAサブシステムのみに理解される
暗号化フォーマットを証明情報に適用する
465
暗号化された証明情報をクライアントから
サーバに送信(委譲)する

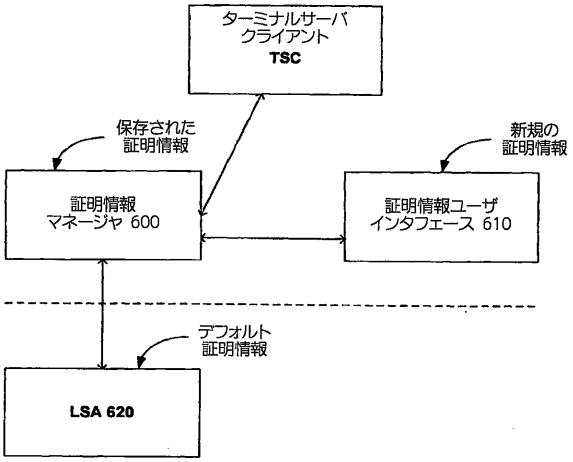
【図４】


400
クライアントとサーバとの間のSSL/TLSハンド
シェイクを完了し、クライアントとサーバとの間の
SSL/TLS暗号化鍵$K_{SSL/TLS}$を確立する。K_{pub}は、
サーバの証明書における公開鍵である。
410
暗号化されたSSL/TLSチャネルにわたり、SPNEGOパッケージ
を使用して相互認証を完了する。クライアント/サーバ信頼関係
に応じて、ケルベロス又はNTLMパッケージのいずれかがネゴシ
エートされ使用される。K_{spnego}は、SPNEGO交換の完了時に両側
によって共有されるケルベロスサブセッションキーか又はNTLM
セッションキーである。
420
LSA Cred SSPが、サーバのSPN、サーバ認証情報
(PKI/KRB対NTLM)及びグループポリシ設定に
基づいてポリシチェックを実行して、ユーザの
証明情報をサーバに委譲すべきか否かを判断する。
430
$K_{SSL/TLS}$がターゲットサーバに属し
中間者に属していないことを確認する。
C S: {{ K_{pub} }K_{spnego} } $K_{SSL/TLS}$
S C: {{ K_{pub} + 1 }K_{spnego} } $K_{SSL/TLS}$
440
ユーザの証明情報をサーバに委譲する。
C S: {{ Password }K_{spnego} } $K_{SSL/TLS}$

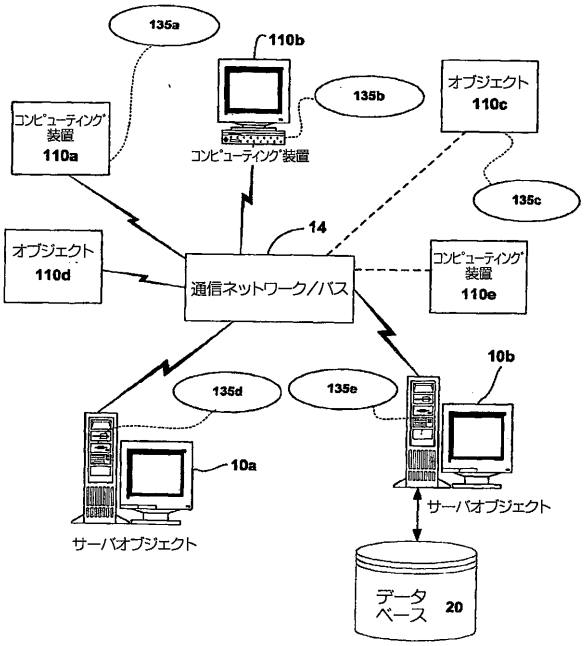
【図５】


クライアント 500
グループ
ポリシ
GP
平文の
証明情報なし
呼出し
アプリケーション
CA
クライアント側
CredSSP
LSA側 CredSSP
I1
信頼された
サブシステム
I1'
LSA側
CredSSP'
クライアント側
CredSSP'
信頼された
サブシステム
平文の
証明情報なし
サーバ
アプリケーション、
資源又はサービス
ARS
サーバ 510

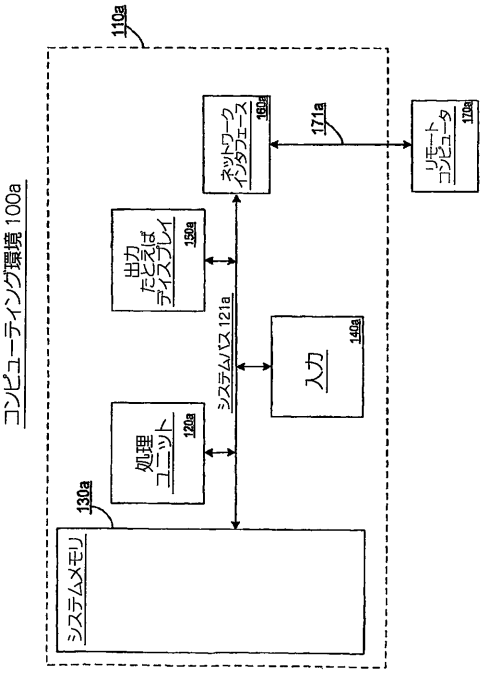
【図６】


ターミナルサーバ
クライアント
TSC
保存された
証明情報
新規の
証明情報
証明情報
マネージャ 600
証明情報ユーザ
インタフェース 610
デフォルト
証明情報
LSA 620

【図７Ａ】


135a
110b
135b
オブジェクト
110c
コンピューティング
装置
110a
コンピューティング装置
135c
14
オブジェクト
110d
通信ネットワーク／バス
コンピューティング
装置
110e
10b
135d
135e
10a
サーバオブジェクト
サーバオブジェクト
データ
ベース 20

【図７Ｂ】


110a
コンピューティング環境 100a
ネットワーク
インタフェース
160a
171a
リモート
コンピュータ
170a
出力
たとえば
ディスプレイ
150a
システムバス 121a
入力
140a
処理
ユニット
120a
130a
システムメモリ

フロントページの続き

(74)代理人 100153028
弁理士 上田 忠
(72)発明者 メドヴィンスキー, ゲナディ
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 アイラック, クリスチャン
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 ハギウ, コスティン
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 パーソンズ, ジョン・イー
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 ファタラ, モハメッド・イマッド・エル・ディン
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 リーチ, ポール・ジェイ
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 カメル, タレック・ブハー・エルーディン・マハムード
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ

審査官 市川 武宜

(56)参考文献 特開２００３－０３０１５０（ＪＰ, Ａ）
特開２００３－１０８５２７（ＪＰ, Ａ）
特開２００５－１２３９９６（ＪＰ, Ａ）
特表２００７－５３５０３０（ＪＰ, Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/00
G06F 21/20
H04L 9/32