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

特許第4843320号
(P4843320)

(45)発行日　平成23年12月21日(2011.12.21)　(24)登録日　平成23年10月14日(2011.10.14)

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

請求項の数 9　(全 12 頁)

(21)出願番号　特願2006-19773(P2006-19773)
(22)出願日　平成18年1月27日(2006.1.27)
(65)公開番号　特開2006-229948(P2006-229948A)
(43)公開日　平成18年8月31日(2006.8.31)
審査請求日　平成20年9月25日(2008.9.25)
(31)優先権主張番号　11/057,812
(32)優先日　平成17年2月14日(2005.2.14)
(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】記憶媒体に対するリモート・サービス・インターフェースのサービス担当ユーザを確実に認証する方法およびシステム

(57)【特許請求の範囲】

【請求項１】

第１サーバおよび第２サーバとネットワークを介して接続されたクライアントによる前記第２サーバに接続された装置へのリモート・アクセスを可能にする方法であって、前記方法は、

前記第１サーバが、前記クライアントから前記ネットワークを介して、前記クライアントのユーザの個人情報を受け取るステップと、

前記第１サーバが、前記個人情報に対応する前記ユーザの少なくとも１つの個人属性を含む暗号化されたユーザ証明書を生成するステップと、

前記第１サーバが、前記ネットワークを介して、前記暗号化されたユーザ証明書を前記クライアントに送信するステップと、

前記第２サーバが、前記クライアントから前記ネットワークを介して、前記暗号化されたユーザ証明書を受け取るステップと、

前記第２サーバが、前記暗号化されたユーザ証明書を検証するステップと、

前記第２サーバが、前記ユーザ証明書の検証結果に基づいて、前記クライアントによる前記装置へのリモート・アクセスを容易にするリモート・アクセス情報を生成して、前記ネットワークを介して前記クライアントに送信するステップとを含み、

前記リモート・アクセス情報は、ユーザ・アカウントと、前記ユーザによる前記装置へのアクセスを許可するランダム・パスワードとを含む、方法。

【請求項２】

前記個人情報は、ユーザ識別標識、ユーザ・パスワード、およびユーザ・パスフレーズを含む、請求項１に記載の方法。
【請求項３】
前記暗号化されたユーザ証明書が、前記個人情報の少なくとも一部分を前記第１サーバにより暗号化されたものを更に含む、請求項１または２に記載の方法。
【請求項４】
前記暗号化されたユーザ証明書が、前記ユーザによる前記装置へのリモート・アクセスに関連した少なくとも１つの動作上の属性を前記第１サーバにより暗号化されたものを更に含む、請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記暗号化されたユーザ証明書が、特定のセキュリティを前記暗号化されたユーザ証明書に加えるアプリケーション特有のデータのセットを前記第１サーバにより暗号化されたものを更に含む、請求項１～４のいずれか１項に記載の方法。
【請求項６】
前記暗号化されたユーザ証明書が、前記ユーザを認証することに関連した少なくとも独特のキーを前記第１サーバにより暗号化されたものを更に含む、請求項１～５のいずれか１項に記載の方法。
【請求項７】
前記ユーザ・アカウントおよび前記ランダム・パスワードは、前記ユーザ証明書に関連する前記装置に対するアクセス期間を通して有効である、請求項１～６のいずれか１項に記載の方法。
【請求項８】
前記暗号化されたユーザ証明書がアクセス期間を通して有効であり、前記アクセス期間の終了時には無効になる、請求項７に記載の方法。
【請求項９】
第１サーバと、装置が接続された第２サーバと、前記第１サーバおよび第２サーバとネットワークを介して接続されたクライアントとを含むシステムであって、
前記第１サーバは、
前記クライアントから前記ネットワークを介して、前記クライアントのユーザの個人情報を受け取る手段と、
前記個人情報に対応する前記ユーザの少なくとも１つの個人属性を含むユーザ証明書を暗号化し、前記ネットワークを介して、前記暗号化されたユーザ証明書を前記クライアントに送信する手段とを含み、
前記第２サーバは、
前記クライアントから前記ネットワークを介して、前記暗号化されたユーザ証明書を受け取る手段と、
前記暗号化されたユーザ証明書を検証する手段と、
前記ユーザ証明書の検証結果に基づいて、前記クライアントによる前記装置へのリモート・アクセスを容易にするリモート・アクセス情報を生成する手段と、
前記ネットワークを介して前記クライアントに前記リモート・アクセス情報を送信する手段とを含み、
前記リモート・アクセス情報は、ユーザ・アカウントと、前記ユーザによる前記装置へのアクセスを許可するランダム・パスワードとを含む、システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概していえば、装置にリモート・アクセスしようとするユーザの認証に関するものである。詳しく言えば、本発明は、サービス担当者が、記憶媒体を遠隔的にサービスするための適正なアクセス・レベル（例えば、サービス、サポート、または機能拡張）を有する許可されたサービス担当者であるということを検証しない方法で記憶媒体へのリモ

ート・アクセスに関してサービス担当者を認証する方法およびシステムに関するものである。

【背景技術】

【０００２】

現在、遠隔のサービス担当者のためのサービス・インターフェースが企業レベルのテープ・コントローラ製品に対して存在する。このインターフェースは、サービス担当者がテープ・コントローラへの動作関係の接続を、私設ネットワークを介して確立することによって起動される。サービス担当者の認証は、そのサービス担当者がコントローラにより制御されるテープ媒体を遠隔的にサービスするための適正なアクセス・レベルを有する許可されたサービス担当者であるという検証を必要とする。特に、認証は、サービス担当者がテープ・コントローラから私設ネットワークを介して認証キー（authentication key）を得ること、サービス担当者がアクセス・サーバから公衆ネットワークを介して認証キーに対応するシステム・パスワードを得ること、およびサービス担当者が私設ネットワークを介してテープ・コントローラにシステム・パスワードを提供し、それによってテープ媒体に対する所望のアクセスを得ること、に順次関与する。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

コンピュータ業界にとっての課題は、私設ネットワークを介して記憶媒体を遠隔的にアクセスするためのサービス担当者、およびサーバによって制御される任意のタイプの装置に１つのネットワークを介してリモート・アクセスすることを望んでいる他の任意の人、に関する上記認証のユーザ利便性および処理効率を改良することであり、本発明の目的はそのための方法およびシステムを提供することである。

【課題を解決するための手段】

【０００４】

本発明の１つの実施例は、第１クライアントおよび第２クライアントが１つの装置を遠隔的にアクセスしようとするユーザの認証を確立することを可能にするための方法である。その方法は、第１クライアントが、ユーザに関する個人情報の第１セットを、第１ネットワークを介して第１サーバに提供すること、第１クライアントが、暗号化されたユーザ証明書を第１サーバから第１ネットワークを介して受け取ること、（なお、その暗号化されたユーザ証明書は、個人情報の第１セットに対応するユーザに関する少なくとも１つの個人属性を第１サーバにより暗号化することを含む）、第２クライアントが、暗号化されたユーザ証明書を、第２ネットワークを介して第２サーバに提供すること、および、第２クライアントが、リモート・アクセス情報を第２サーバから第２ネットワークを介して受け取ること、（なお、そのリモート・アクセス情報は、第２サーバによるその暗号化されたユーザ証明書の検証に対する応答に基づいてそのユーザによる第２ネットワークを介した装置へのリモート・アクセスを容易にする）を含む。

【０００５】

本発明の第２実施例は、第１サーバおよび第２サーバが、第２サーバと動作関係に接続された装置を遠隔的にアクセスしようとするユーザを認証することを可能にするための方法である。その方法は、第１サーバが、ユーザの個人情報の第１セットを第１クライアントから第１ネットワークを介して受け取ること、第１サーバが、暗号化されたユーザ証明書を、第１ネットワークを介して第１クライアントに提供すること、（なお、その暗号化されたユーザ証明書は、個人情報の第１セットに対応するそのユーザに関する少なくとも１つの個人属性を第１サーバにより暗号化することを含む）、第２サーバが、暗号化されたユーザ証明書を第２クライアントから第２ネットワークを介して受け取ること、および、第２サーバが、リモート・アクセス情報を、第２ネットワークを介して第２クライアントに提供すること、（なお、リモート・アクセス情報は、第２サーバによるその暗号化されたユーザ証明書の検証に対する応答に基づいてそのユーザによる第２ネットワークを介した装置へのリモート・アクセスを容易にする）を含む。

【０００６】
本発明の第３実施例は、ユーザに関する個人情報の第１セットを第１クライアントから第１ネットワークを介して受け取るための手段と、暗号化されたユーザ証明書を、第１ネットワークを介して第１クライアントに提供するための手段と、（なお、その暗号化されたユーザ証明書は、個人情報の第１セットに対応するユーザに関する少なくとも１つの個人属性を第１サーバにより暗号化することを含む）、暗号化されたユーザ証明書を第２クライアントから第２ネットワークを介して受け取るための手段と、リモート・アクセス情報を、第２ネットワークを介して第２クライアントに提供するための手段と、（なお、そのリモート・アクセス情報は、第２サーバによるその暗号化されたユーザ証明書の検証に対する応答に基づいて第２ネットワークを介した装置へのユーザによるリモート・アクセスを容易にする）を含むシステムである。
【０００７】
本発明の第４実施例は、プロセッサと、暗号化されたユーザ証明書をユーザに提供するためにそのプロセッサによって動作し得る命令を記憶するメモリとを含むサーバである。それらの命令は、ユーザに関する個人情報のセットをクライアントからネットワークを介して受け取るステップと、ユーザの個人情報のセットに対応するユーザの少なくとも１つの個人属性を暗号化したものを含む暗号化されたユーザ証明書を、ユーザの個人情報のセットを受け取ったことに応答して生成するステップと、その暗号化されたユーザ証明書を、ネットワークを介してクライアントに提供するステップとを実行する。
【０００８】
本発明の第５実施例は、プロセッサと、プロセッサによって動作し得る命令を記憶し、リモート・アクセス情報をユーザに提供するためのメモリとを含むサーバである。それらの命令は、ユーザの少なくとも１つの個人属性を暗号化したものを含むそのユーザの暗号化されたユーザ証明書をクライアントからネットワークを介して受け取るステップと、サーバにより動作上の制御を受ける装置へのユーザによるリモート・アクセスを容易にするリモート・アクセス情報を、その暗号化されたユーザ証明書の検証に基づいて生成するステップと、リモート・アクセス情報を、ネットワークを介してクライアントに提供するステップと、を実行する。
【０００９】
本発明の上記実施例および別の実施例、目的、特徴、および利点は、本願において示された本発明の種々の実施例に関する以下の詳細な説明から更に明らかになるであろう。その詳細な説明および図面は、「特許請求の範囲」によって定義される本発明およびその均等物の範囲を限定するのではなく、単に本発明を説明および図解するだけのものである。
【発明を実施するための最良の形態】
【００１０】
図１は、本発明を実施するための例示的な動作環境を示す。図１を参照すると、本発明は、Ｘ（X≥１）番までの装置５０（例えば、テープ記憶媒体）をユーザ１０がアクセスするのを容易にする確実な低オーバヘッドのユーザ認証装置６０を提供する。このために、ユーザ認証装置６０は、図２～図６に関連して後述されるように、本発明の種々の方法を具現化するための新たな且つ独特のユーザ証明モジュール６１および新たな且つ独特のユーザ・リモート・アクセス・モジュール６２を使用する。クライアント１１（例えば、ウェブ・ブラウザ）および証明サーバ３０（例えば、ウェブ・ベースのサーバ）がネットワーク２０（例えば、公衆ネットワーク）に物理的に接続され、それによってクライアント１１および証明サーバ３０は、ハードウェアまたはソフトウェアあるいはその両方を使用するユーザ証明モジュール６１を操作するように一般的な方法で動作関係に接続することが可能である。なお、モジュール６１は、暗号化されたユーザ証明書をユーザ１０に提供する目的で、図２に示されるフローチャート７０を具現化するよう構造的に構成されたハードウェアまたはソフトウェアあるいはそれらの両方を使用する。
【００１１】
更に図２を参照すると、フローチャート７０のステージＳ７２は、ユーザ１０によりネ

ットワーク２０を介して提供された個人情報ＰＩ１をモジュール６１が受け取ることを含む。個人情報ＰＩ１は、モジュール６１が、例えば、ユーザ識別標識およびユーザ・パスワードのようなユーザ１０を認識することを可能にするユーザ１０に関する情報を含む。

【００１２】

フローチャート７０のステージＳ７４は、モジュール６１が１つまたは複数の変数に基づいて１つの暗号化されたユーザ証明書ＥＵＣを生成することを含む。１つの実施例では、次のような４つ変数をステージ７４の期間中に利用することが可能である。第１の変数はユーザ１０によって提供された個人情報ＰＩ１である。第２の可能な変数は、ユーザ１０によって提供された個人情報ＰＩ１に対応するユーザ１０の１つまたは複数の個人属性を含む。なお、その個人属性は、例えば、ユーザ識別標識およびユーザ・パスワードの形式のユーザ１０に関する個人情報に対応する装置５０をアクセスするための、ユーザ１０のアクセス・レベルのような個人属性である。そのような例に対して、モジュール６１は、ユーザ１０のアクセス・レベルをユーザ識別標識およびユーザ・パスワードに関連付けるユーザ１０のためのファイルを保持することが可能であり、それによって、モジュール６１は、ユーザ識別標識およびユーザ・パスワードをユーザ１０から受け取ったときユーザ１０のアクセス・レベルを取り出すことが可能である。

【００１３】

第３の変数は、例えば、暗号化されたユーザ証明書ＥＵＣのアクセス期間が満了してしまったか否かに関する決定を容易にするためのタイムスタンプのような、装置５０をアクセスすることに関連した１つまたは複数の動作上の属性を含む。もう１つの例示的な動作上の属性は、例えば、ユーザ１０によるリモート・サービスを必要とする装置５０による動作上の障害または機能不全のような、ユーザ１０が装置５０を遠隔的にアクセスする必要性を誘起したイベントに対応するイベント識別標識である。

【００１４】

第４の変数は、ユーザ認証を暗号化する目的でモジュール６１と関連付けられた公開キーまたは秘密キーである暗号化キーＥＫである。

【００１５】

個人情報ＰＩ１、ユーザ１０の個人属性、装置を遠隔的にアクセスすることに関連した動作上の属性、または暗号化キーＥＫ、あるいはそれらの幾つかに基づいてモジュール６１がこのような暗号化されたユーザ証明書を生成する技術は際限のないものである。従って、図３に示されたフローチャート８０によって表されるステージＳ７４の一実施例に関する下記の説明はステージＳ７４の範囲に関する限定ではない。

【００１６】

更に図３を参照すると、フローチャート８０のステージＳ８２は、モジュール６１が個人情報ＰＩ１を処理してユーザ識別標識、ユーザ・パスワード、およびユーザ・パスフレーズを取り出すことを含む。ユーザ識別標識およびユーザ・パスワードは、モジュール６１がユーザ１０を識別することを可能にし、一方、ユーザ・パスフレーズはモジュール６１に更なるセキュリティを提供する。

【００１７】

フローチャート８０のステージＳ８４は、モジュール６１がステージＳ８２の期間中に有効なユーザ・パスフレーズによってユーザ１０を識別することができたことに応答して、モジュール６１が未暗号化のユーザ・データを生成することを含む。ステージＳ８４の一実施例では、モジュール６１は、（１）ユーザ１０のユーザ識別標識、（２）ユーザ１０のアクセス・レベル、および（３）未暗号化のユーザ・データがモジュール６１によって生成された時間を指定するタイムスタンプ、から順次に構成された未暗号化のユーザ・データをストリングＵＳＥＲＤＡＴＡ１として作成するための作成コマンドを実行する。ストリングＵＳＥＲＤＡＴＡ１は、更に、（４）未暗号化のユーザ・データにアプリケーション特有の機能を加えるためのアプリケーション特有のデータ、および（５）例えば、アクセス期間（その結果生じる暗号化されたユーザ証明書はその期間中は有効である）を指定する期間キーおよびストリングＵＳＡＤＡＴＡ１に更なるセキュリティを加えるため

のランダム・データを含むランダム・キーのような１つまたは複数の独特のキー、を含むことが可能である。更に、ユーザ１０による遠隔接続の検査を維持するためのキー、装置５０をサービスするために必要な時間を記録するためのキー、ユーザ１０がクライアントを介して動作関係に接続され得るシステムを制限するためのキー、ユーザ１０のアカウントに適合した自動サーチ・レポートおよび任意の関連した地理的属性を生成するためのキーのような更なるキーを使用することも可能である。

【００１８】

ステージＳ８４の第２の実施例では、モジュール６１は、（１）ユーザ１０のユーザ識別標識、（２）ユーザ１０のユーザ・アクセス・レベル、（３）未暗号化のユーザ・データが生成された時間を指定するタイムスタンプ、および（４）ユーザ１０が装置５０を遠隔的にアクセスする必要性を誘起した特定のイベントの通知を表すイベント識別標識、から順次に構成された未暗号化のユーザ・データをストリングＵＳＥＲＤＡＴＡ２として作成するための作成コマンドを実行する。ストリングＵＳＥＲＤＡＴＡ２は、更に、（５）アプリケーション特有のデータおよび（６）前述のような１つまたは複数の独特のキーを含むことが可能である。

【００１９】

フローチャート８０のステージＳ８６は、未暗号化のユーザ・データを暗号化するためにモジュール６１が暗号化アルゴリズムを利用することを含む。ステージＳ８６の一実施例では、モジュール６１は、非対称暗号化アルゴリズムＡＣＡ（例えば、Rivest-Shamir-Adleman および Rabin）を利用して秘密暗号化キーＥＫおよび未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ１から、暗号化されたユーザ・データＥＮＣＤＡＴＡ１を作成する作成コマンドを実行する。ステージＳ８６の第２の実施例では、モジュール６１は、非対称暗号化アルゴリズムＡＣＡを利用して秘密暗号化キーＥＫおよび未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ２から、暗号化されたユーザ・データＥＮＣＤＡＴＡ２を作成する作成コマンドを実行する。

【００２０】

ステージＳ８８は、モジュール６１が更なる暗号化アルゴリズムを使用して、暗号化されたユーザ・データを、暗号化されたユーザ証明書に変換することを含む。ステージＳ８８の一実施例では、モジュール６１が、対称暗号化アルゴリズムＳＣＡ（例えば、ＸＯＲ）を利用してユーザ・パスフレーズおよび暗号化されたユーザ・データＥＮＣＤＡＴＡ１から、暗号化されたユーザ証明書ＵＳＥＲＣＥＲＴ１を作成する作成コマンドを実行する。ステージＳ８８の第２実施例では、モジュール６１が、対称暗号化アルゴリズムＳＣＡを利用してユーザ・パスフレーズおよび暗号化されたユーザ・データＥＮＣＤＡＴＡ２から、暗号化されたユーザ証明書ＵＳＥＲＣＥＲＴ２を作成する。フローチャート８０はステージＳ８８の完了時に終了する。

【００２１】

図１および図２を再び参照すると、モジュール６１はステージＳ７４の終了時にフローチャート７０のステージＳ７６に進む。ステージＳ７６は、モジュール６１がネットワーク２０を介してユーザ１０に、暗号化されたユーザ証明書ＥＵＣを提供することを含む。１つの実施例では、モジュール６１は、暗号化されたユーザ証明書ＥＵＣをＵＳＥＲＣＥＲＴ１またはＵＳＥＲＣＥＲＴ２としてベース６４フォーマットで提供し、それによってその暗号化されたユーザ証明書をテキストとして使用可能なものにし、それにより、複写／貼り付け、テキストとしての保存、およびモデムを介した転送、のような操作がユーザ１０にとって単純化される。

【００２２】

フローチャート７０はステージＳ７６の完了時に終了する。当業者には、フローチャート７０に関する上記の説明から、フローチャート７０の種々の利点が明らかであろう。特に、ユーザ１０の或る程度の確実な認証をカスタマイズする機能は、（１）ユーザ１０の個人情報、（２）ユーザ１０に関連した個人属性、（３）ユーザ１０による装置５０へのリモート・アクセスに関連した動作上の属性、（４）未暗号化のユーザ・データの構造、

（５）秘密暗号化キー、および（６）暗号化アルゴリズムＡＣＡおよびＳＣＡ、というアプリケーション特有の性質および複雑性に基づく。更に、上記の要素は、モジュール６１に対して恒久的に設定するか、あるいはモジュール６１に関連したアプリケーション特有のポリシに従って定期的にまたは散発的に置換または修正あるいはその両方を行うことが可能である。

【００２３】

図１を参照すると、クライアント１２（例えば、テープ・アプリケーション）および装置サーバ４０（例えば、テープ・コントローラ）がネットワーク２１（例えば、私設ネットワーク）に物理的に接続され、それによって、クライアント１２およびサーバ４０はモジュール６２を動作させるように一般的な方法で動作関係に接続され得る。なお、モジュール６２は、モジュール６１によってユーザ１０に以前に提供された暗号化されたユーザ証明書に基づいて、ユーザ１０による装置５０へのリモート・アクセスを容易にする目的で、図４に示されたフローチャート９０を具現化するように構成されたハードウェアおよびソフトウェアを使用する。

【００２４】

更に図４を参照すると、フローチャート９０のステージ９２は、モジュール６２がユーザ１０によりネットワーク２１を介して提供された個人情報ＰＩ２および暗号化されたユーザ証明書ＥＵＣを受け取ることを含む。個人情報ＰＩ２は、モジュール６１がユーザ１０を識別することを可能にするユーザ１０に関する情報（例えば、ユーザ識別標識およびユーザ・パスワード）およびユーザ１０が望んでいる装置１０へのリモート・アクセスの性質を決定するための情報を含む。暗号済みユーザ証明書ＥＵＣはユーザ１０の個人情報の暗号化、ユーザ１０の個人属性、ユーザ１０による装置５０へのリモート・アクセスに関連した動作上の属性、アプリケーション特有のセキュリティ・データ、または１つもしくは複数の独特のキーあるいはそれら幾つかを含む。

【００２５】

フローチャート９０のステージＳ９４は、モジュール６２が１つまたは複数の変数に基づいてリモート・アクセス情報ＲＡＩを生成することを含む。１つの実施例では、次のような３つの変数をステージＳ９４の期間中に利用することが可能である。第１および第２の変数は、ユーザ１０によって提供された個人情報ＰＩ２および暗号化されたユーザ証明書ＥＵＣである。第３の変数は、暗号化されたユーザ証明書を暗号化解除するためにモジュール６２に関連した公開または秘密暗号化解除キーＤＫである。

【００２６】

モジュール６２が個人情報ＰＩ１、暗号化されたユーザ証明書ＥＵＣ、または暗号化解除キーＤＫあるいはそれらの幾つかに基づいてリモート・アクセス情報を生成する技術は制限のないものである。従って、図６に示されたフローチャート９０によって表されるステージＳ９４の一実施例に関する下記の説明はステージＳ９４の範囲に関する限定ではない。

【００２７】

更に図５を参照すると、フローチャート１００のステージＳ１０２は、モジュール６２がユーザ識別標識、ユーザ・パスワード、ユーザ・パスフレーズ、およびアクセス・レベル要求を取り出すために個人情報ＰＩ２を処理することを含む。ユーザ識別標識およびユーザ・パスワードは、モジュール６２がユーザ１０を識別することを可能にし、一方、ユーザ・パスフレーズはモジュール６２に更なるセキュリティを提供する。アクセス・レベル要求は、モジュール６２が、ユーザ１０が希望する装置５０へのリモート・アクセスの性質を決定することを可能にする。更に、モジュール６２は、例えば、暗号化されたユーザ証明書ＥＵＣがＵＳＥＲＣＥＲＴ１のフォーマットまたはＵＳＥＲＣＥＲＴ２のベース６４フォーマットのものであるときのような必要時にその暗号化されたユーザ証明書ＥＵＣを解読する。

【００２８】

フローチャート１００のステージＳ１０４は、モジュール６２が、暗号化されたのユー

ザＥＵＣを、暗号化されたのユーザ・データに変換するために暗号化アルゴリズムを利用することを含む。ステージＳ１０８の一実施例では、モジュール６２が対称暗号化アルゴリズムＳＣＡを利用して（図３のＳ８８参照）ユーザ・パスフレーズおよび暗号化されたユーザ証明書ＵＳＥＲＣＥＲＴ１から、暗号化されたのユーザ・データＥＮＣＤＡＴＡ１を作成する作成コマンドを実行する。ステージＳ１０８の第２実施例では、モジュール６２は、対称暗号化アルゴリズムＳＣＡを利用して（図３のＳ８８参照）ユーザ・パスフレーズおよび暗号化されたユーザ証明書ＵＳＥＲＣＥＲＴ２から、暗号化されたユーザ・データを作成する作成コマンドを実行する。

【００２９】

フローチャート１００のステージＳ１０６は、モジュール６２が別の暗号化アルゴリズムを利用して、暗号化されたユーザ・データを暗号化解除することを含む。ステージＳ１０６の一実施例では、モジュール６２が、非対称暗号化アルゴリズムＡＣＡ（図３のＳ８６参照）を利用して公開暗号化解除キーＤＫおよび暗号化されたユーザ・データＥＮＣＤＡＴＡ１から未暗号化のユーザ・データＵＳＥＲＤＡＴＡ１を作成する作成コマンドを実行する。ステージＳ１０６の第２実施例では、モジュール６２は、非対称暗号化アルゴリズムＡＣＡ（図３のＳ８６参照）を利用して公開暗号化解除キーＤＫおよび暗号化されたユーザ・データＥＮＣＤＡＴＡ１から、暗号化されたユーザ・データＵＳＥＲＤＡＴＡ２を作成する作成コマンドを実行する。

【００３０】

フローチャート１００のステージＳ１０８は、モジュール６２が未暗号化のユーザ・データを検証することを含む。１つの実施例では、モジュール６２は、ユーザ１０の個人情報、ユーザ１０の個人属性、ユーザ１０による装置５０へのリモート・アクセスに関連した動作上の属性、アプリケーション特有のセキュリティ・データ、または未暗号化のユーザ・データにリストされた独特のキーあるいはそれらの幾つかを検証する。モジュール６２がステージＳ１０８の期間中にユーザ１０を認証する技術は制限のないものである。従って、図６に示されるフローチャート１１０によって表されたステージＳ１０８の一実施例に関する下記の説明はステージＳ１０８の範囲に関する限定ではない。

【００３１】

更に図６を参照すると、フローチャート１１０は、前述のように、未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ１及び未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ２に基づいてユーザ１０を認証するために実施される。フローチャート１１０のステージＳ１１２は、ユーザ１０によって提供されたユーザＩＤが、未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ１及び未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ２においてリストされたＵＳＥＲＩＤ属性に適合するということを、モジュール６２が検証することを含む。フローチャート１１０のステージＳ１１４は、ユーザ１０によって提供されたアクセス・レベル要求が、未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ１及び未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ２においてリストされたアクセス・レベル属性に適合するということを、モジュール６２が検証することを含む。

【００３２】

フローチャート１１０のステージＳ１１６は、未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ２においてリストされたイベントＩＤが、ユーザ１０による装置５０へのリモート・アクセスの必要性を誘起した特定のイベントをユーザ１０に通知するために以前に生成された適正なイベントＩＤに適合するということを、モジュール６２が検証することを含む。ステージＳ１１６は、未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ１に適用し得ない。

【００３３】

フローチャート１１０のステージＳ１１８は、未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ１および未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ２においてリストされたタイムスタンプが未暗号化のユーザ・データ・ストリングＵＳＥＲＤ

ＡＴＡ１及び未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ２に対するアクセス期間よりも小さい経過時間（age）を有するということを、モジュール６２が検証することを含む。前述のように、アクセス期間は、独特のキーとしてまたはモジュール６２のアプリケーション特有のポリシに基づいて、未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ１及び未暗号化のユーザ・データ・ストリングＵＳＥＲＤＡＴＡ２においてリストすることが可能である。

【００３４】

フローチャート１１０のステージＳ１２０は、モジュール６２が、アクセス期間を通して有効であるランダム・パスワードを用いてローカル・ユーザ・アカウントを設定することを含む。そのローカル・ユーザ・アカウントおよびランダム・パスワードは、リモート・アクセス情報ＲＡＩに含まれる必要があるとき、モジュール６２によってフォーマットされる。フローチャート１００および１１０はステージ１２０の完了時に終了する。

【００３５】

再び図１および図４を参照すると、モジュール６２はステージＳ９４の完了時にフローチャート９０のステージＳ９６に進む。ステージＳ９６は、モジュール６２がネットワーク２１を介してユーザ１０にリモート・アクセス情報ＲＡＩを提供することを含む。フローチャート９０はステージＳ９６の完了時に終了する。フローチャート９０に関する前述の説明からフローチャート９０の種々の利点、特に、確実な且つ低オーバヘッドの態様で装置５０のリモート・アクセスのためにユーザ１０を認証する機能が当業者には明らかであろう。

【００３６】

本発明の原理に基づいたユーザ１０の完全な認証を容易に理解するために、図２および図４を参照して、ユーザ１０が有効且つ正確な個人情報および暗号化されたユーザ証明書を提供することに基づく実際的な形でフローチャート７０および９０を説明した。ユーザ１０が無効のあるいは不正確な個人情報または暗号化されたユーザ証明書あるいはその両方を提供したことに応答して、フローチャート７０および９０を任意のステージで終了させることも可能であることは当業者には明らかであろう。

【００３７】

図１～図６を参照すると、１つの実用的な実施例では、モジュール６１および６２（図１）が、それぞれのサーバ３０および４０(図１)のメモリ内に設けられたソフトウェア・モジュールとして具体化され、それによって、それぞれのサーバ３０および４０のプロセッサが図２～図６に示された例のように本発明の種々のオペレーションを遂行するためにモジュール６１および６２を実行することが可能である。モジュール６１および６２は、それらがソフトウェア・モジュールとして組み込まれるとき、当業者が図２～図６に関する説明を理解することによって如何なる一般的なプログラミング言語においても書くことが可能である。

【００３８】

図１を参照すると、本発明の理解を容易にするために図示のような動作環境が提供されたことによって、本発明を実施するための別の動作環境が当業者には明らかであろう。例えば、それは、ワイヤライン接続、ワイヤレス接続、またはそれの混成体が具現化される場合の動作環境、クライアント１１および１２が同じ物理的コンピュータ・プラットフォーム(例えば、ワークステーション)におけるクライアント・アプリケーションとして具現化される場合の動作環境、または、ネットワーク２０および２１が同じ物理的ネットワーク上に存在する別々の異なる仮想ネットワークである場合の動作環境である。

【００３９】

図３および図５を参照すると、秘密暗号化キー（ＰＥＫ）および公開暗号化解除キー（ＰＤＫ）が選択され、それによってＡＣＡ（ＰＥＫ、ＡＣＡ（ＰＤＫ、データ））の非対称暗号化アルゴリズムＡＣＡの具現化がデータを同じくするＡＣＡ（ＰＤＫ，ＡＣＡ（ＰＥＫ，データ））の具現化に等しくなることが推奨される。更に、秘密暗号化キーおよび公開暗号化解除キーが選択され、それによってＡＣＡ（任意のキー、ＡＣＡ（ＰＥＫ｜Ｐ

ＤＫ，データ）の非対称暗号化アルゴリズムＡＣＡの具現化がそのデータに等しいことが推奨される。更に、秘密暗号化キーの如何なる妥協案も、それぞれのモジュール６１および６２に対する秘密暗号化キーおよび公開暗号化解除キーの対の再生および配布をトリガすることが可能である。

【００４０】

開示された本発明の実施例が現時点では好適な実施例であると考えられるが、本発明の真意および範囲から逸脱することなく種々の変更および修正を施すことが可能である。本発明の範囲は「特許請求の範囲」に示され、均等物の意味および範囲内となるすべての変更がそれに包含されるものと考えられる。

【図面の簡単な説明】

【００４１】

【図１】本発明を実施するための例示的な動作環境を示す図である。

【図２】本発明の一実施例に従って、暗号化されたユーザ証明書を提供する方法を表すフローチャートである。

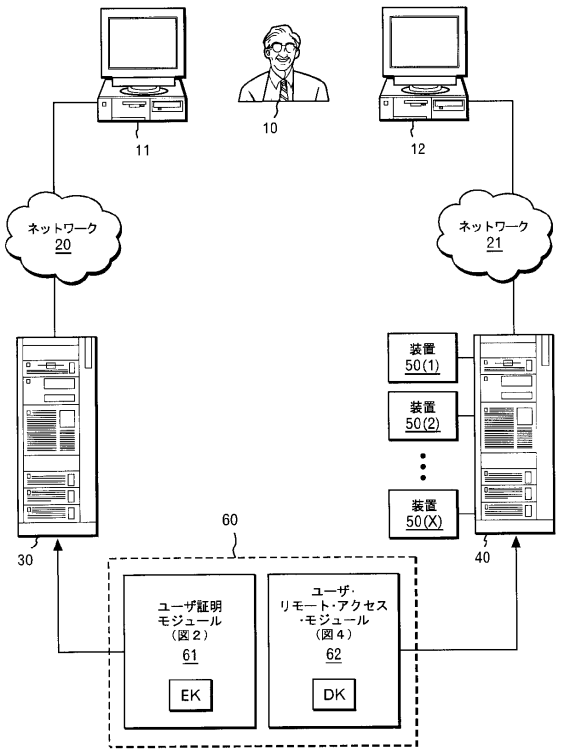
【図３】本発明の一実施例に従って、暗号化されたユーザ証明書を生成する方法を表すフローチャートである。

【図４】本発明の一実施例に従って、ユーザ装置アクセス方法を表すフローチャートである。

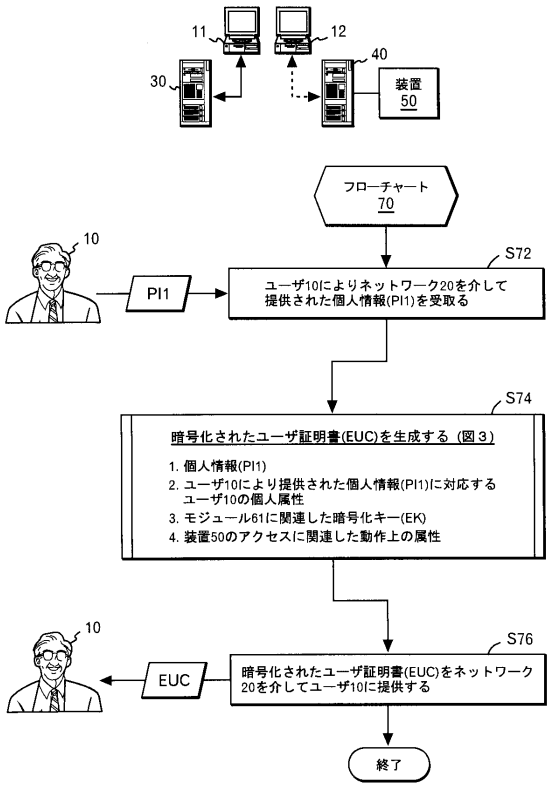
【図５】本発明の一実施例に従って、アクセス情報を生成する方法を表すフローチャートである。

【図６】本発明の一実施例に従って、ユーザ認証方法を表すフローチャートである。

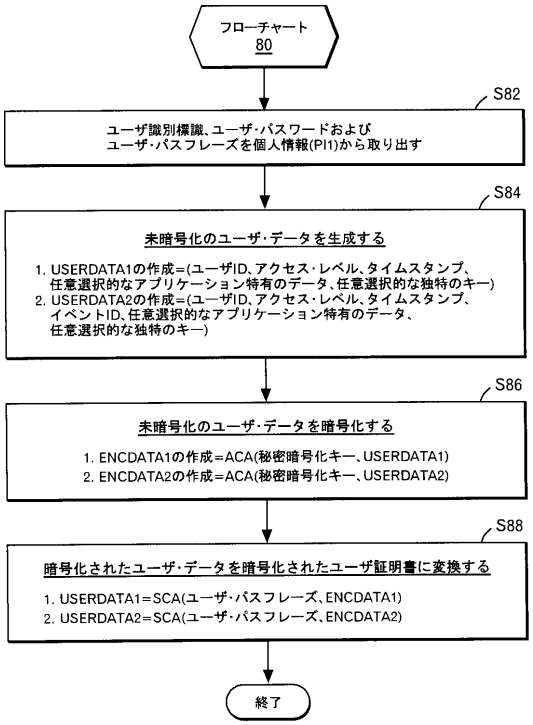
【図１】



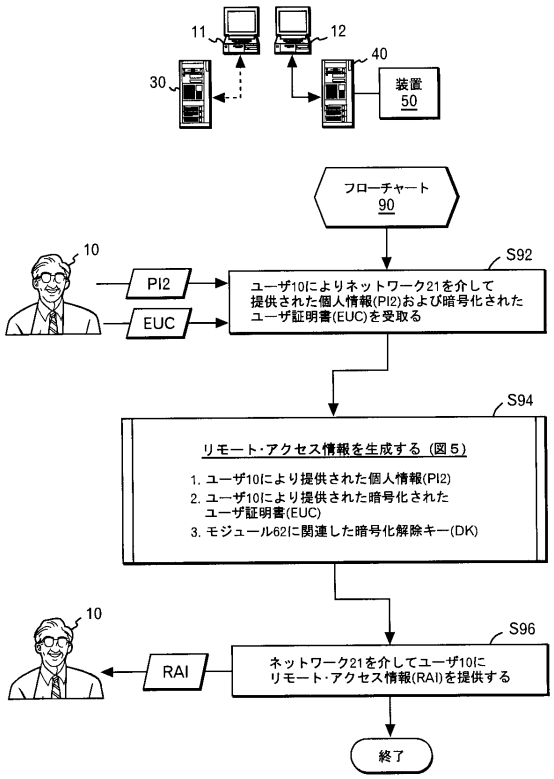
【図２】



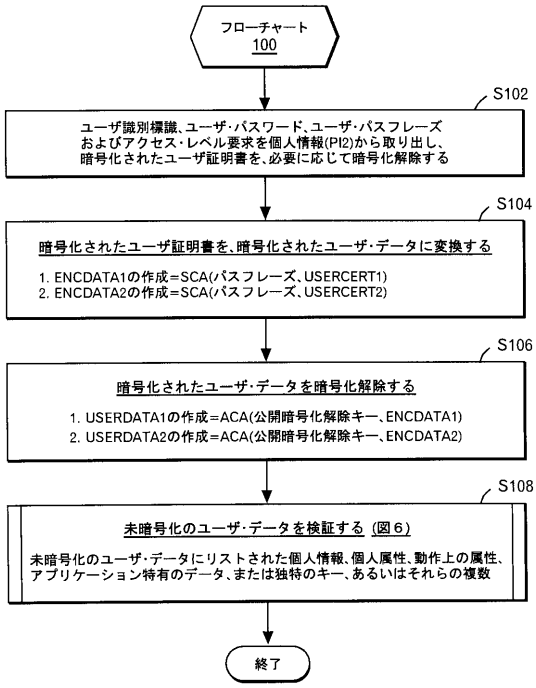
【図３】


フローチャート
80
S82
ユーザ識別標識、ユーザ・パスワードおよび
ユーザ・パスフレーズを個人情報(PI1)から取り出す
S84
未暗号化のユーザ・データを生成する
1. USERDATA1の作成=(ユーザID、アクセス・レベル、タイムスタンプ、
任意選択的なアプリケーション特有のデータ、任意選択的な独特のキー)
2. USERDATA2の作成=(ユーザID、アクセス・レベル、タイムスタンプ、
イベントID、任意選択的なアプリケーション特有のデータ、
任意選択的な独特のキー)
S86
未暗号化のユーザ・データを暗号化する
1. ENCDATA1の作成=ACA(秘密暗号化キー、USERDATA1)
2. ENCDATA2の作成=ACA(秘密暗号化キー、USERDATA2)
S88
暗号化されたユーザ・データを暗号化されたユーザ証明書に変換する
1. USERDATA1=SCA(ユーザ・パスフレーズ、ENCDATA1)
2. USERDATA2=SCA(ユーザ・パスフレーズ、ENCDATA2)
終了

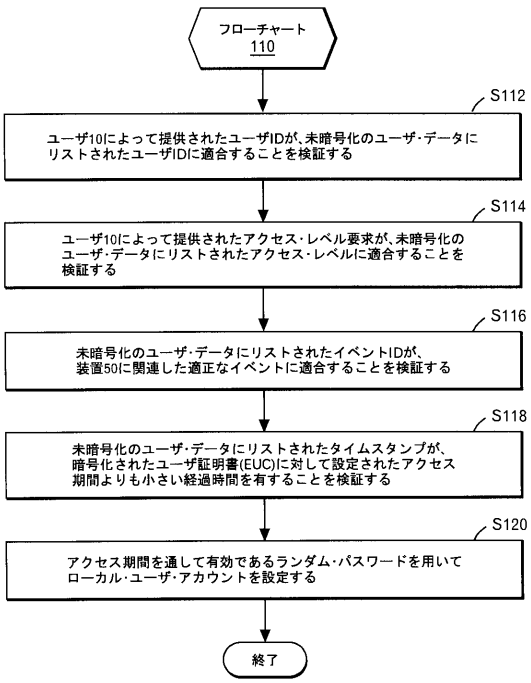
【図４】


11
12
40
30
装置
50
フローチャート
90
10
PI2
EUC
S92
ユーザ10によりネットワーク21を介して
提供された個人情報(PI2)および暗号化された
ユーザ証明書(EUC)を受取る
S94
リモート・アクセス情報を生成する（図５）
1. ユーザ10により提供された個人情報(PI2)
2. ユーザ10により提供された暗号化された
ユーザ証明書(EUC)
3. モジュール62に関連した暗号化解除キー(DK)
10
RAI
S96
ネットワーク21を介してユーザ10に
リモート・アクセス情報(RAI)を提供する
終了

【図５】


フローチャート
100
S102
ユーザ識別標識、ユーザ・パスワード、ユーザ・パスフレーズ
およびアクセス・レベル要求を個人情報(PI2)から取り出し、
暗号化されたユーザ証明書を、必要に応じて暗号化解除する
S104
暗号化されたユーザ証明書を、暗号化されたユーザ・データに変換する
1. ENCDATA1の作成=SCA(パスフレーズ、USERCERT1)
2. ENCDATA2の作成=SCA(パスフレーズ、USERCERT2)
S106
暗号化されたユーザ・データを暗号化解除する
1. USERDATA1の作成=ACA(公開暗号化解除キー、ENCDATA1)
2. USERDATA2の作成=ACA(公開暗号化解除キー、ENCDATA2)
S108
未暗号化のユーザ・データを検証する（図６）
未暗号化のユーザ・データにリストされた個人情報、個人属性、動作上の属性、
アプリケーション特有のデータ、または独特のキー、あるいはそれらの複数
終了

【図６】


フローチャート
110
S112
ユーザ10によって提供されたユーザIDが、未暗号化のユーザ・データに
リストされたユーザIDに適合することを検証する
S114
ユーザ10によって提供されたアクセス・レベル要求が、未暗号化の
ユーザ・データにリストされたアクセス・レベルに適合することを
検証する
S116
未暗号化のユーザ・データにリストされたイベントIDが、
装置50に関連した適正なイベントに適合することを検証する
S118
未暗号化のユーザ・データにリストされたタイムスタンプが、
暗号化されたユーザ証明書(EUC)に対して設定されたアクセス
期間よりも小さい経過時間を有することを検証する
S120
アクセス期間を通して有効であるランダム・パスワードを用いて
ローカル・ユーザ・アカウントを設定する
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 アンドリュー・ジー・アワーセルト
アメリカ合衆国８５７１８、アリゾナ州、ツーソン、ノース・リオ・ドライブ、ナンバー３１３４３５８

審査官 青木 重徳

(56)参考文献 特開２００５－０１１２３９（ＪＰ，Ａ）
特開２００４－３４１８９７（ＪＰ，Ａ）
特開２００４－０４６４３０（ＪＰ，Ａ）
特表２００５－５１２３９６（ＪＰ，Ａ）
Larry J. Hughes, Jr. 著／長原宏治 監訳, “インターネットセキュリティ”, 日本, 株式会社インプレス, １９９７年 2月２１日, 初版, ｐ．９４－１２１
Bruce Schneier, “APPLIED CRYPTOGRAPHY, SECOND EDITION”, 米国, John Wiley & Sons, Inc., １９９６年, p.52-53
時庭康久, 泉祐市, 後沢忍, 渡辺晃, 稲田徹, “情報セキュリティ ネットワークセキュリティ“ＭＥＬＷＥＬＬ””, 三菱電機技報, 日本, 三菱電機エンジニアリング株式会社, １９９８年 5月２５日, 第７２巻, 第5号, ｐ．２８－３１

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００