(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4892011号
(P4892011)
(45)発行日　平成24年3月7日(2012.3.7)　(24)登録日　平成23年12月22日(2011.12.22)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	21/20	133
H04L 9/32	(2006.01)	H04L	9/00	673A
G09C 1/00	(2006.01)	G09C	1/00	640E

請求項の数 24　(全 33 頁)

(21)出願番号　特願2008-558066 (P2008-558066)
(86)(22)出願日　平成20年2月7日(2008.2.7)
(86)国際出願番号　PCT/JP2008/052055
(87)国際公開番号　WO2008/099756
(87)国際公開日　平成20年8月21日(2008.8.21)
審査請求日　平成21年3月18日(2009.3.18)
(31)優先権主張番号　特願2007-28500 (P2007-28500)
(32)優先日　平成19年2月7日(2007.2.7)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100121706
弁理士　中尾　直樹
(74)代理人　100128705
弁理士　中村　幸雄
(74)代理人　100147773
弁理士　義村　宗洋
(74)代理人　100066153
弁理士　草野　卓
(72)発明者　鶴岡　行雄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】クライアント装置、鍵装置、サービス提供装置、ユーザ認証システム、ユーザ認証方法、プログラム、記録媒体

(57)【特許請求の範囲】
【請求項１】
ネットワークを介してサービス提供装置に接続されるクライアント装置であって、
ユーザＩＤ、公開鍵、秘密鍵及びサーバ証明書をサービス毎に関連付けて登録するサービス情報データベースを保持するクライアント認証情報管理部と、制御部と、クライアント認証部と、鍵生成部とを備え、
さらに、
前記制御部が、ユーザ登録要求及びサービス要求を前記サービス提供装置へ送信する要求機能と、
前記クライアント認証部が、前記サービス提供装置からのサーバ認証情報及び認証要求を検証するサーバ認証機能と、
前記クライアント認証部が、ユーザＩＤ、パスワード、ユーザ属性及び前記鍵生成部で生成させた公開鍵に対する署名を、前記鍵生成部で当該公開鍵と対応して生成させた秘密鍵を用いて求め、ユーザＩＤ、パスワード、ユーザ属性、公開鍵及び署名を含むユーザ情報を前記サービス提供装置へ送信するユーザ情報送信機能と、
前記クライアント認証情報管理部が、ユーザＩＤ、公開鍵、秘密鍵及びサーバ証明書を含むサービス情報をサービス毎に関連付けてサービス情報データベースに登録するサービス情報登録機能と、
前記クライアント認証部が、前記サービス提供装置からの認証要求に含まれる認証ポリシーから特定した認証法がパスワード認証であれば、パスワードから当該パスワードの所

有を確認できるパスワード認証情報を計算し、当該パスワード認証情報、認証法及びユーザＩＤを含む認証応答を前記サービス提供装置へ送信し、また、認証ポリシーから特定した認証法が公開鍵認証であれば、認証法、ユーザＩＤ及び認証要求に含まれるチャレンジに対する署名１を計算し、該署名１、認証法、ユーザＩＤを含む認証応答を前記サービス提供装置へ送信し、また、認証ポリシーから特定した認証法が公開鍵とパスワードを組み合わせた認証であれば、認証法、ユーザＩＤ、認証要求に含まれるチャレンジ及びパスワードに対する署名２を計算し、該署名２、認証法、ユーザＩＤを含む認証応答を前記サービス提供装置へ送信する認証応答機能を

備えるクライアント装置。

【請求項２】

ネットワークを介してサービス提供装置に接続されるクライアント装置に接続される鍵装置であって、

ユーザＩＤ、公開鍵、秘密鍵及びサーバ証明書をサービス毎に関連付けて登録するサービス情報データベースを保持するクライアント認証情報管理部と、クライアント認証部と、鍵生成部とを備え、

さらに、

前記クライアント認証部が、前記サービス提供装置側からのサーバ認証情報及び認証要求を検証するサーバ認証機能と、

前記クライアント認証部が、ユーザＩＤ、パスワード、ユーザ属性及び前記鍵生成部で生成させた公開鍵に対する署名を、前記鍵生成部で当該公開鍵と対応して生成させた秘密鍵を用いて求め、ユーザＩＤ、パスワード、ユーザ属性、公開鍵及び署名を含むユーザ情報をサービス提供装置側へ送信するユーザ情報送信機能と、

前記クライアント認証部が、前記サービス提供装置からの認証要求に含まれる認証ポリシーから特定した認証法がパスワード認証であれば、パスワードから当該パスワードの所有を確認できるパスワード認証情報を計算し、当該パスワード認証情報、認証法及びユーザＩＤを含む認証応答をサービス提供装置側へ送信し、また、認証ポリシーから特定した認証法が公開鍵認証であれば、認証法、ユーザＩＤ及び認証要求に含まれるチャレンジに対する署名１を計算し、該署名１、認証法、ユーザＩＤを含む認証応答をサービス提供装置側へ送信し、また、認証ポリシーから特定した認証法が公開鍵とパスワードを組み合わせた認証であれば、認証法、ユーザＩＤ、認証要求に含まれるチャレンジ及びパスワードに対する署名２を計算し、該署名２、認証法、ユーザＩＤを含む認証応答をサービス提供装置側へ送信する認証応答機能と、

前記クライアント認証情報管理部が、ユーザＩＤ、公開鍵、秘密鍵及びサーバ証明書を含むサービス情報をサービス毎に関連付けてサービス情報データベースに登録するサービス情報登録機能を、

備える鍵装置。

【請求項３】

請求項１記載のクライアント装置であって、

前記クライアント認証部は、認証の強度と同意確認のレベルとの組み合わせからなる認証ポリシー毎に認証法を登録する認証法対応表を格納し、

前記認証応答機能では、前記サービス提供装置からの認証要求に含まれる認証ポリシーに対応する認証法を前記認証法対応表から前記クライアント認証部が全て読み出し、そのうちでユーザから選択された認証法あるいは実行可能な認証法を、認証ポリシーから特定した認証法とする

ことを特徴とするクライアント装置。

【請求項４】

請求項２記載の鍵装置であって、

前記クライアント認証部は、認証の強度と同意確認のレベルとの組み合わせからなる認証ポリシー毎に認証法を登録する認証法対応表を格納し、

前記認証応答機能では、前記サービス提供装置からの認証要求に含まれる認証ポリシー

に対応する認証法を前記認証法対応表から前記クライアント認証部が全て読み出し、そのうちでユーザから選択された、あるいは実行可能な認証法を、認証ポリシーから特定した認証法とする
ことを特徴とする鍵装置。
【請求項５】
請求項３記載のクライアント装置であって、
前記ユーザ情報送信機能は、前記クライアント認証部が、ユーザ側が要求する認証ポリシーであるユーザポリシー、ユーザＩＤ、パスワード、ユーザ属性及び前記鍵生成部で生成させた公開鍵に対する署名を、前記鍵生成部で当該公開鍵と対応して生成させた秘密鍵を用いて求め、ユーザポリシー、ユーザＩＤ、パスワード、ユーザ属性、公開鍵及び署名を含むユーザ情報を前記サービス提供装置へ送信する機能である
ことを特徴とするクライアント装置。
【請求項６】
請求項４記載の鍵装置であって、
前記ユーザ情報送信機能は、前記クライアント認証部が、ユーザ側が要求する認証ポリシーであるユーザポリシー、ユーザＩＤ、パスワード、ユーザ属性及び前記鍵生成部で生成させた公開鍵に対する署名を、前記鍵生成部で当該公開鍵と対応して生成させた秘密鍵を用いて求め、ユーザポリシー、ユーザＩＤ、パスワード、ユーザ属性、公開鍵及び署名を含むユーザ情報をサービス提供装置へ送信する機能である
ことを特徴とする鍵装置。
【請求項７】
ネットワークを介してクライアント装置と接続されるサービス提供装置であって、
ユーザＩＤ、パスワード、ユーザ属性及び公開鍵をユーザ毎に関連付けて登録するユーザ情報データベースを保持するサービス提供装置認証情報管理部と、サービス提供部と、サービス提供装置認証部とを備え、
さらに、
前記サービス提供装置認証部が、前記クライアント装置からのユーザ登録要求に応じてサーバ証明書及び署名を含むサーバ認証情報を前記クライアント装置に送信する登録要求応答機能と、
前記サービス提供装置認証部が、前記クライアント装置からのユーザ情報を受信して署名を検証し、検証に成功した場合は、前記サービス提供装置認証情報管理部が、ユーザＩＤ、パスワード、ユーザ属性及び公開鍵を含むユーザ情報をユーザ毎に関連付けてユーザ情報データベースに登録するとともに、ユーザ登録成功を表すメッセージを前記クライアント装置へ送信するユーザ登録機能と、
前記サービス提供装置認証部が、前記クライアント装置からのサービス要求に応じて当該サービスの認証法を示す認証ポリシー、サーバ証明書及び署名を含む認証要求を前記クライアント装置へ送信するサービス要求応答機能と、
前記サービス提供装置認証部が、前記クライアント装置からの認証応答を受信して当該認証応答に含まれる認証法を確認し、当該確認に成功した場合は、前記サービス提供装置認証情報管理部が、前記認証応答に含まれるユーザＩＤに対応するエントリーを特定し、さらに確認した認証法に応じた認証処理を行う認証処理機能と、
前記サービス提供部が、サービス提供の可否を判定し、提供可であればサービスを提供するサービス提供機能を
備えたサービス提供装置。
【請求項８】
請求項７記載のサービス提供装置であって、
前記認証ポリシーは、サービスの認証法がパスワード認証か公開鍵認証か公開鍵とパスワードを組み合わせた認証かを示すものであり、
前記認証処理機能は、前記認証法に応じた認証処理として、確認した認証法がパスワード認証であれば、認証応答に含まれるユーザＩＤに対応するエントリーからパスワードを

取得して前記認証応答に含まれるパスワードもしくはパスワード認証情報と照合し、確認した認証法が公開鍵認証であれば、前記エントリーから公開鍵を取得して前記認証応答に含まれる署名１の正当性を確認し、確認した認証法が公開鍵とパスワードを組み合わせた認証であれば、前記エントリーから公開鍵を取得して前記認証応答に含まれる署名２の正当性を確認して検証する

ことを特徴とするサービス提供装置。

【請求項９】

請求項７または８記載のサービス提供装置であって、

ユーザＩＤ、パスワード及び公開鍵をユーザ毎に関連付けて登録する認証情報変換データベースを保持する認証情報変換部も備え、前記サービス提供装置認証情報管理部は、ユーザＩＤ、パスワード及びユーザ属性をユーザ毎に関連付けて登録するユーザ情報データベースを保持する構成部であり、

さらに、

前記ユーザ登録機能は、前記サービス提供装置認証部が、前記クライアント装置からのユーザ情報を受信して署名を検証し、検証に成功した場合は、前記サービス提供装置認証情報管理部が、前記ユーザ情報のうちユーザＩＤ、パスワード及びユーザ属性をユーザ情報データベースに登録し、前記認証情報変換部が、ユーザ情報のうちユーザＩＤ、パスワード及び公開鍵を認証情報変換データベースに登録するとともに、ユーザ登録成功を表すメッセージを前記クライアント装置へ送信する機能であり、

前記認証処理機能が、前記サービス提供装置認証部が、前記クライアント装置からの認証応答を受信して当該認証応答に含まれる認証法を確認し、当該確認に成功した場合は、確認した認証法がパスワード認証であれば、当該認証応答からパスワードもしくはパスワード認証情報を取得し、また、確認した認証法が公開鍵認証であれば、前記認証情報変換部が、前記認証応答に含まれるユーザＩＤで認証情報変換データベースを検索して該当するユーザのエントリーを特定し、公開鍵を取得して前記認証応答に含まれる署名１の正当性を確認し、前記エントリーからパスワードを取得し、また、確認した認証法が公開鍵とパスワードを組み合わせた認証であれば、前記認証情報変換部が、前記認証応答に含まれるユーザＩＤで認証情報変換データベースを検索して該当するユーザのエントリーを特定し、公開鍵を取得して前記認証応答に含まれる署名２の正当性を確認し、前記エントリーからパスワードを取得し、前記サービス提供装置認証情報管理部が、前記認証応答に含まれるユーザＩＤでユーザ情報データベースを検索して該当するユーザのエントリーを特定し、当該エントリーのパスワードと前記認証情報変換部が取得したパスワードを照合して検証する機能である、

ことを特徴とするサービス提供装置。

【請求項１０】

請求項７から９のいずれかに記載のサービス提供装置であって、

前記サービス要求応答機能が前記クライアント装置へ送信する認証ポリシーは、認証の強度と同意確認のレベルとの組み合わせを示す認証ポリシーである

ことを特徴とするサービス提供装置。

【請求項１１】

請求項１０記載のサービス提供装置であって、

前記ユーザ登録機能が、前記サービス提供装置認証部が、前記クライアント装置からのユーザ情報を受信して署名を検証し、検証に成功した場合は、前記サービス提供装置認証情報管理部が、ユーザポリシー、ユーザＩＤ、パスワード、ユーザ属性及び公開鍵を含むユーザ情報をユーザ情報データベースに登録するとともに、ユーザ登録成功を表すメッセージを前記クライアント装置へ送信する機能であり、

前記サービス要求応答機能が、前記サービス提供装置認証部が、前記クライアント装置からのサービス要求に応じて当該サービスに対応する認証ポリシーであるサービスポリシーと前記ユーザポリシーとから認証ポリシーを決定し、決定した認証ポリシー、サーバ証明書及び署名を含む認証要求を前記クライアント装置へ送信する機能である

ことを特徴とするサービス提供装置。
【請求項１２】
請求項１記載のクライアント装置と、
請求項７から９のいずれかに記載のサービス提供装置と、
前記クライアント装置と前記サービス提供装置とを接続するネットワーク
を備えるユーザ認証システム。
【請求項１３】
請求項２記載の鍵装置と、
前記鍵装置に接続されるクライアント装置と、
請求項７から９のいずれかに記載のサービス提供装置と、
前記クライアント装置と前記サービス提供装置とを接続するネットワーク
を備えるユーザ認証システム。
【請求項１４】
請求項３記載のクライアント装置と、
請求項１０記載のサービス提供装置と、
前記クライアント装置と前記サービス提供装置とを接続するネットワーク
を備えるユーザ認証システム。
【請求項１５】
請求項４記載の鍵装置と、
前記鍵装置に接続されるクライアント装置と、
請求項１０記載のサービス提供装置と、
前記クライアント装置と前記サービス提供装置とを接続するネットワーク
を備えるユーザ認証システム。
【請求項１６】
請求項５記載のクライアント装置と、
請求項１１記載のサービス提供装置と、
前記クライアント装置と前記サービス提供装置とを接続するネットワーク
を備えるユーザ認証システム。
【請求項１７】
請求項６記載の鍵装置と、
前記鍵装置に接続されるクライアント装置と、
請求項１１記載のサービス提供装置と、
前記クライアント装置と前記サービス提供装置とを接続するネットワーク
を備えるユーザ認証システム。
【請求項１８】
ネットワークで接続されたクライアント装置とサービス提供装置とを動作させ、ユーザの認証を行うユーザ認証方法であって、
前記クライアント装置が、ユーザ登録要求を前記サービス提供装置へ送信する登録要求ステップと、
前記サービス提供装置が、前記ユーザ登録要求に応じてサーバ証明書及び署名を含むサーバ認証情報を前記クライアント装置に送信する登録要求応答ステップと、
前記クライアント装置が、前記サーバ認証情報を検証する認証情報検証ステップと、
前記クライアント装置が、ユーザＩＤ、パスワード、ユーザ属性及び公開鍵に対する署名を、当該公開鍵と対応して生成させた秘密鍵を用いて求め、ユーザＩＤ、パスワード、ユーザ属性、公開鍵及び署名を含むユーザ情報を前記サービス提供装置へ送信するユーザ情報送信ステップと、
前記サービス提供装置が、前記ユーザ情報の署名を検証し、検証に成功した場合は、ユーザＩＤ、パスワード、ユーザ属性及び公開鍵を含むユーザ情報をユーザ毎に関連付けて登録するとともに、ユーザ登録成功を表すメッセージを前記クライアント装置へ送信するユーザ登録ステップと、

前記クライアント装置が、ユーザＩＤ、公開鍵、秘密鍵及びサーバ証明書を含むサービス情報をサービス毎に関連付けてサービス情報データベースに登録するサービス情報登録ステップと、
前記クライアント装置が、サービス要求を前記サービス提供装置へ送信するサービス要求ステップと、
前記サービス提供装置が、前記サービス要求に応じて当該サービスの認証法を示す認証ポリシー、サーバ証明書及び署名を含む認証要求を前記クライアント装置へ送信するサービス要求応答ステップと、
前記クライアント装置が、前記認証要求を検証する認証要求検証ステップと、
前記クライアント装置が、認証要求に含まれる認証ポリシーを参照して決定した認証法に応じた認証応答を計算して、前記サービス提供装置へ送信する認証応答ステップと、
前記サービス提供装置が、前記認証応答に含まれる認証法を確認し、確認に成功した場合は、確認した認証法に応じた認証処理を行う認証処理ステップと、
前記サービス提供装置が、サービス提供の可否を判定し、提供可であればサービスを提供するサービス提供ステップ
を有するユーザ認証方法。
【請求項１９】
請求項１８記載のユーザ認証方法であって、
前記認証ポリシーは、サービスの認証法がパスワード認証か公開鍵認証か公開鍵とパスワードを組み合わせた認証かを示すものであり、
前記認証応答ステップは、認証ポリシーを参照して決定した認証法が、パスワード認証であれば、パスワードから当該パスワードの所有を確認できるパスワード認証情報を計算し、当該パスワード認証情報、認証法及びユーザＩＤを含む認証応答を前記サービス提供装置へ送信し、また、認証ポリシーを参照して決定した認証法が公開鍵認証であれば、認証法、ユーザＩＤ及び認証要求に含まれるチャレンジに対する署名１を計算し、該署名１、認証法、ユーザＩＤを含む認証応答を前記サービス提供装置へ送信し、また、認証ポリシーを参照して決定した認証法が公開鍵とパスワードを組み合わせた認証であれば、認証法、ユーザＩＤ、認証要求に含まれるチャレンジ及びパスワードに対する署名２を計算し、該署名２、認証法、ユーザＩＤを含む認証応答を前記サービス提供装置へ送信するものであり、
前記サービス提供装置が行う前記認証処理ステップは、認証法に応じた認証処理として、確認した認証法がパスワード認証であれば、ユーザＩＤに対応するパスワードを取得して前記認証応答に含まれるパスワードもしくはパスワード認証情報と照合し、また、確認した認証法が公開鍵認証であれば、ユーザＩＤに対応する公開鍵を取得して前記認証応答に含まれる署名１の正当性を確認し、また、確認した認証法が公開鍵とパスワードを組み合わせた認証であれば、ユーザＩＤに対応する公開鍵を取得して前記認証応答に含まれる署名２の正当性を確認して検証する
ことを特徴とするユーザ認証方法。
【請求項２０】
請求項１８または１９記載のユーザ認証方法であって、
前記ユーザ登録ステップは、前記サービス提供装置が、前記ユーザ情報の署名を検証し、検証に成功した場合は、前記ユーザ情報のうちユーザＩＤ、パスワード及びユーザ属性をユーザ情報データベースに登録し、ユーザ情報のうちユーザＩＤ、パスワード及び公開鍵を認証情報変換データベースに登録するとともに、ユーザ登録成功を表すメッセージを前記クライアント装置へ送信するステップであり、
前記認証処理ステップは、前記サービス提供装置が、前記認証応答に含まれる認証法を確認し、当該確認に成功した場合は、確認した認証法がパスワード認証であれば、当該認証応答からパスワードもしくはパスワード認証情報を取得し、また、確認した認証法が公開鍵認証であれば、前記認証応答に含まれるユーザＩＤで前記認証情報変換データベースを検索してユーザＩＤに対応する公開鍵を取得し、前記認証応答に含まれる署名１の正当

性を確認し、ユーザＩＤに対応するパスワードを取得し、また、確認した認証法が公開鍵とパスワードを組み合わせた認証であれば、前記認証応答に含まれるユーザＩＤで認証情報変換データベースを検索してユーザＩＤに対応する公開鍵を取得し、前記認証応答に含まれる署名２の正当性を確認し、ユーザＩＤに対応するパスワードを取得し、前記認証応答に含まれるユーザＩＤでユーザ情報データベースを検索してユーザＩＤに対応するパスワードと前記取得したパスワードを照合して検証するステップである
ことを特徴とするユーザ認証方法。
【請求項２１】
請求項１８から２０のいずれかに記載のユーザ認証方法であって、
前記認証応答ステップでは、認証要求に含まれる認証ポリシーに対応する認証法のうちで、選択された認証法あるいは実行可能な認証法を、認証ポリシーから特定した認証法とし、
前記サービス要求応答ステップでは、前記クライアント装置へ送信する認証ポリシーが、認証の強度と同意確認のレベルとの組み合わせを示す認証ポリシーである
ことを特徴とするユーザ認証方法。
【請求項２２】
請求項２１記載のユーザ認証方法であって、
前記ユーザ情報送信ステップは、前記クライアント装置が、ユーザ側が要求する認証ポリシーであるユーザポリシー、ユーザＩＤ、パスワード、ユーザ属性及び公開鍵に対する署名を、当該公開鍵と対応して生成させた秘密鍵を用いて求め、ユーザポリシー、ユーザＩＤ、パスワード、ユーザ属性、公開鍵及び署名を含むユーザ情報を前記サービス提供装置へ送信するステップである
ことを特徴とするユーザ認証方法。
【請求項２３】
請求項１から１１のいずれかに記載の装置として、コンピュータを動作させるプログラム。
【請求項２４】
請求項２３記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザを認証し、認証したユーザにサービスを提供するユーザ認証システム、ユーザ認証方法、およびユーザ認証システムを構成するクライアント装置、鍵装置、サービス提供装置、並びに各装置としてコンピュータを動作させるプログラム、そのプログラムを記録した記録媒体に関する。
【背景技術】
【０００２】
インターネットを始めとするネットワークの普及により、オンラインショッピングやコンテンツサービスなどのオンラインサービスが増加している。通常のオンラインサービスにおいては、ユーザにサービスを提供するサービス提供装置と、サービス提供装置に対してユーザ認証を行うクライアント装置とがそれぞれネットワークに接続される。そして、ユーザはクライアント装置を介してサービス提供装置に対してユーザ認証を行う。また、サービス提供装置はユーザ認証の結果に基づいてサービスを提供する。
【０００３】
このようなユーザ認証の方法としては、実現が容易なパスワード認証が広く普及している。パスワード認証において安全性を高めるには、サービス毎に異なり、かつ、なるべく長いパスワードを設定する必要がある。しかし、この場合、ユーザはどのサービスにどのようなパスワードを設定したかを全て記憶しなければならず、煩雑である。したがって、実際には共通のパスワードや覚え易い短いパスワードを設定しがちであり、安全性の確保が困難であるという問題があった。またパスワード認証では、フィッシング等によるパス

ワード漏洩の危険性があることも問題であった。

【０００４】

このため、パスワード認証に、公開鍵暗号系に基づく認証方式（以下、公開鍵認証）を組み合わせる技術が提案されている。例えば、特許文献１に示される利用者認証システムでは、端末装置、業務サーバ、代理認証機構がそれぞれネットワークに接続される。そして、利用者が端末装置を介して業務サーバを利用する際に、代理認証機構が業務サーバに代わって端末装置を利用する利用者を認証し、正当性が検証された場合に業務サーバの一連の処理を実行するものになっている。代理認証機構は、ユーザＩＤやパスワード等の利用者認証情報を用いた認証を行う。代理認証機構は、さらに、代理認証機構から端末装置に送られたセッションＩＤに対して端末装置の秘密鍵で計算したディジタル署名（以下、署名）を端末装置から受け取り、この署名を検証することで、より強い認証を行う。また、一つの代理認証機構を複数の業務サーバの認証に用いることで、業務サーバ利用料を集計し、利用料の徴収を代行することができる。代理認証機構を付加することで業務サーバの変更なく利用できる。

【特許文献１】特開２００２－１３２７２７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

前述したように、特許文献１に示される利用者認証システムでは、代理認証機構の付加によって、既存の業務サーバを変更することなく、パスワード認証よりも安全な認証手段を提供できる。

前述の従来技術では、代理認証機構と業務サーバとが分離しているため、業務サーバを利用する利用者のユーザＩＤ及びパスワードを予め代理認証機構に登録する事前設定が必要となる。オンラインサービスには事前の登録なく利用する形態も多いが、このようなオンラインサービスの突発的な利用には、前述の従来技術は適していない。

【０００６】

また、提供するサービスによっては、パスワード認証で十分な内容の場合や、署名を生成する機能を具備しない端末を利用する場合などもある。このように、必要とされる又は提供可能な認証手段は、利用ごとに異なる。このため、サービスの内容や利用者端末の環境によって認証手段を切り替えできることが好ましい。しかし、前記利用者認証システムでは、代理認証機構と業務サーバとが分離しており、端末と業務サーバの持つ情報を交換する処理手順になっていないため、認証手段の切り替えは困難である。

【０００７】

また、通常の典型的なサービス、例えばＷｅｂによるオンラインショッピングなどでは、ユーザから見たパスワード認証の手順が一連のサービス提供手順の中に埋め込まれている。公開鍵認証の手順も、サービス提供手順と違和感なく組み合わせることが必要である。しかし、従来の利用者認証システムでは、代理認証機構があらかじめ認証する必要がある。したがって、サービス提供手順の中に埋め込んで公開鍵認証を行うのは困難である。

【０００８】

また、パスワード認証は、その性質上、本人しか知り得ない情報の提供を確認する効果（同意確認を取る効果）がある。一方、公開鍵認証は、一般的には同意確認を取る効果を持っていない。従って、公開鍵認証を行う装置に同意確認を取る機能を備えさせる場合には、パスワード認証と公開鍵認証を組み合わせる必要がある。さらにその際、事後に確認できるような方法で同意確認の証拠が残せることが望ましい。

しかし、前記利用者認証システムでは、代理認証機構と業務サーバとが分離している点、同意確認を証明可能な形態で業務サーバに伝える手順になっていない点などにより、強い認証と同意確認の両立が困難である。

【０００９】

本発明はこのような問題に鑑みてなされたものである。本発明の目的は、代理認証機構などの第三者による事前の設定が必要なく、パスワード認証と公開鍵認証とを切り替え可

能なユーザ認証システムおよびユーザ認証方法を提供することにある。本発明のさらなる目的は、公開鍵認証の認証強度とパスワード認証の同意確認を両立させ、安全で確実なユーザ認証システムおよび方法を提供することにある。

【課題を解決するための手段】

【００１０】

本発明のユーザ認証システムは、クライアント装置とサービス提供装置とこれらを接続するネットワークで構成される。また、クライアント装置は、鍵装置と接続されてもよい。

本発明のクライアント装置は、ユーザＩＤ、公開鍵、秘密鍵及びサーバ証明書をサービス毎に関連付けて登録するサービス情報データベースを保持するクライアント認証情報管理部と、制御部と、クライアント認証部と、鍵生成部とを備え、さらに、要求機能、サーバ認証機能、ユーザ情報送信機能、サービス情報登録機能、認証応答機能を備える。

【００１１】

要求機能は、制御部が、ユーザ登録要求及びサービス要求をサービス提供装置へ送信する。サーバ認証機能は、クライアント認証部が、サービス提供装置からのサーバ認証情報及び認証要求を検証する。ユーザ情報送信機能は、クライアント認証部が、ユーザＩＤ、パスワード、ユーザ属性及び鍵生成部で生成させた公開鍵に対する署名を、鍵生成部で生成させた秘密鍵を用いて求め、ユーザＩＤ、パスワード、ユーザ属性、公開鍵及び署名を含むユーザ情報をサービス提供装置へ送信する。サービス情報登録機能は、クライアント認証情報管理部が、ユーザＩＤ、公開鍵、秘密鍵及びサーバ証明書を含むサービス情報をサービス情報データベースに登録する。

【００１２】

認証応答機能は、クライアント認証部が、認証要求に含まれる認証ポリシーから特定した認証法がパスワード認証であれば、パスワードから当該パスワードの所有を確認できるパスワード認証情報を計算し、当該パスワード認証情報、認証法及びユーザＩＤを含む認証応答をサービス提供装置へ送信する。また、認証ポリシーから特定した認証法が公開鍵認証であれば、認証法、ユーザＩＤ及び認証要求に含まれるチャレンジに対する署名１を計算し、該署名１、認証法、ユーザＩＤ及び認証要求に含まれるチャレンジを含む認証応答をサービス提供装置へ送信する。また、認証ポリシーから特定した認証法が公開鍵とパスワードを組み合わせた認証であれば、認証法、ユーザＩＤ、認証要求に含まれるチャレンジ及びパスワードに対する署名２を計算し、該署名２、認証法、ユーザＩＤ及び認証要求に含まれるチャレンジを含む認証応答をサービス提供装置へ送信する。

【００１３】

なお、クライアント装置が鍵装置と接続されたときは、クライアント装置は制御部を備え、要求機能を有していればよい。この場合は、鍵装置が、クライアント認証情報管理部、クライアント認証部、鍵生成部を備え、サーバ認証機能、ユーザ情報送信機能、サービス情報登録機能、認証応答機能を有する。

【００１４】

本発明のサービス提供装置は、ユーザＩＤ、パスワード、ユーザ属性及び公開鍵をユーザ毎に関連付けて登録するユーザ情報データベースを保持するサービス提供装置認証情報管理部と、サービス提供部と、サービス提供装置認証部とを備え、さらに、登録要求応答機能、ユーザ登録機能、サービス要求応答機能、認証処理機能、サービス提供機能を備える。登録要求応答機能は、サービス提供装置認証部が、クライアント装置からのユーザ登録要求に応じてサーバ証明書及び署名を含むサーバ認証情報を前記クライアント装置に送信する。ユーザ登録機能は、サービス提供装置認証部が、クライアント装置からのユーザ情報を受信して署名を検証し、検証に成功した場合は、サービス提供装置認証情報管理部が、ユーザＩＤ、パスワード、ユーザ属性及び公開鍵を含むユーザ情報をユーザ情報データベースに登録するとともに、ユーザ登録成功を表すメッセージをクライアント装置へ送信する。サービス要求応答機能は、サービス提供装置認証部が、クライアント装置からのサービス要求に応じて当該サービスの認証法がパスワード認証か公開鍵認証か公開鍵とパ

スワードを組み合わせた認証かを示す認証ポリシー、サーバ証明書及び署名を含む認証要求をクライアント装置へ送信する。

【００１５】

認証処理機能は、サービス提供装置認証部が、クライアント装置からの認証応答を受信して当該認証応答に含まれる認証法を確認する。そして、確認に成功した場合は、サービス提供装置認証情報管理部が、認証応答に含まれるユーザＩＤに対応するエントリーを特定する。さらに、サービス提供装置認証情報管理部が、確認した認証法がパスワード認証であれば、エントリーからパスワードを取得して認証応答に含まれるパスワードもしくはパスワード認証情報と照合する。また、確認した認証法が公開鍵認証であれば、エントリーから公開鍵を取得して認証応答に含まれる署名１の正当性を確認する。また、確認した認証法が公開鍵とパスワードを組み合わせた認証であれば、エントリーから公開鍵を取得して認証応答に含まれる署名２の正当性を確認して検証する。

【００１６】

サービス提供機能は、サービス提供部が、サービス提供の可否を判定し、提供可であればサービスを提供する。

【発明の効果】

【００１７】

本発明のユーザ認証システムによれば、ユーザがクライアント装置を介してサービス提供装置にユーザ登録する際、クライアント装置が、ユーザＩＤ、パスワード、ユーザ属性及び公開鍵に前記公開鍵と対応する秘密鍵で署名を行い、ユーザＩＤ、パスワード、ユーザ属性、公開鍵及び署名を少なくとも含むユーザ情報をサービス提供装置に送信する。そして、ユーザ情報を受信したサービス提供装置が前記公開鍵を用いて署名を検証し、検証が成功した場合にユーザ情報、即ちパスワードと公開鍵とが関連付けられた情報を格納するようになっている。このようにパスワードと公開鍵とが安全に関連付けられているため、パスワード認証と公開鍵認証とを容易に切り替えて利用することができる。

【００１８】

また、ユーザがクライアント装置を介してサービス提供装置にサービス要求する際、サービス提供装置がサービスの認証法がパスワード認証か公開鍵認証かパスワードおよび公開鍵を組み合わせた認証かを示す認証ポリシーを含む認証要求をクライアント装置へ送信する。そして、クライアント装置が、パスワード認証であれば、ユーザより入力されたパスワード等から当該パスワードの所有を確認できるパスワード認証情報を計算する。また、公開鍵認証であれば、ユーザＩＤ及び認証要求に含まれるチャレンジに対して秘密鍵で署名を行う。また、パスワード及び公開鍵を組み合わせた認証であれば、ユーザＩＤ、認証要求に含まれるチャレンジ及びユーザより入力されたパスワードに対して秘密鍵で署名を行う。そして、クライアント装置は、これらを含む認証応答をサービス提供装置に送信する。このため、公開鍵認証の強度とパスワードの持つ同意確認機能を両立させることができる。

【００１９】

また、サービス提供装置がパスワードと公開鍵とを関連付けて記憶しているので、公開鍵認証を行った場合でも、認証後の処理がパスワード認証と共通化できる。さらに、特許文献１ではネットワーク上に代理認証機構を設ける必要があるが、本発明では、クライアント装置、サービス提供装置の他に追加装置を設ける必要はない。このため、パスワード認証のみを利用する従来のサービス提供装置から、本発明のサービス提供装置に容易に移行することもできる。

【図面の簡単な説明】

【００２０】

【図１】実施例１のユーザ認証システムの概要を示す構成図である。

【図２】実施例１のクライアント装置の構成図である。

【図３】実施例１のサービス提供装置の構成図である。

【図４】実施例１のクライアント装置のサービス情報データベースの構成図である。

【図５】実施例１のサービス提供装置のユーザ情報データベースの構成図である。
【図６】実施例１のユーザ認証システムにおけるユーザ登録の処理フローを示す流れ図である。
【図７】実施例１のユーザ情報の詳細を示す説明図である。
【図８】実施例１のユーザ認証システムにおけるユーザ認証の処理フローを示す流れ図である。
【図９】実施例１の認証要求の詳細を示す説明図である。
【図１０】図１０Ａは、認証法がＰＷの場合の実施例１の認証応答の詳細を示す説明図である。図１０Ｂは、認証法がＰＫの場合の実施例１の認証応答の詳細を示す説明図である。図１０Ｃは、認証法がＰＫＰＷの場合の実施例１の認証応答の詳細を示す説明図である。
【図１１】実施例２のサービス提供装置の構成図である。
【図１２】実施例２のサービス提供装置のユーザ情報データベースの構成図である。
【図１３】実施例２のサービス提供装置の認証情報変換データベースの構成図である。
【図１４】実施例２のユーザ認証システムにおけるユーザ登録の処理フローを示す流れ図である。
【図１５】実施例２のユーザ認証システムにおけるユーザ認証の処理フローを示す流れ図である。
【図１６】実施例３のユーザ認証システムの概要を示す構成図である。
【図１７】実施例３のクライアント装置の構成図である。
【図１８】実施例３の鍵装置の構成図である。
【図１９】実施例３の鍵装置のサービス情報データベースの構成図である。
【図２０】実施例３のユーザ認証システムにおけるユーザ登録の処理フローを示す流れ図である。
【図２１】実施例３のユーザ認証システムにおけるユーザ認証の処理フローを示す流れ図である。
【図２２】図２２Ａは、実施例４のユーザ認証システムにおける認証法対応表の例を示す説明図である。図２２Ｂは、実施例４のユーザ認証システムにおける認証法対応表の別の例を示す説明図である。
【図２３】実施例４変形例のユーザ情報の詳細を示す説明図である。
【図２４】図２４Ａは、実施例４変形例のユーザポリシーの具体例を示す説明図である。図２４Ｂは、実施例４変形例のユーザポリシーの別の具体例を示す説明図である。
【図２５】実施例４変形例のサービス提供装置のユーザ情報データベースの構成図である。
【図２６】実施例４変形例のユーザ認証システムにおけるユーザ認証の処理フローを示す流れ図である。
【図２７】図２７Ａは、実施例５のユーザ認証システムにおけるサービス要求のデータ形式を示す説明図である。図２７Ｂは、実施例５のユーザ認証システムにおける認証要求のデータ形式を示す説明図である。図２７Ｃは、実施例５のユーザ認証システムにおける認証応答のデータ形式を示す説明図である。
【図２８】実施例５変形例のユーザ認証システムにおける認証要求のデータ形式を示す説明図である。
【図２９】実施例５変形例のユーザ認証システムにおける認証スクリプトの内容を示す説明図である。
【図３０】実施例６のユーザ認証システムにおける鍵更新の処理フローを示す流れ図である。
【図３１】実施例６の鍵情報の詳細を示す説明図である。
【図３２】実施例７のユーザ認証システムにおける登録抹消の処理フローを示す流れ図である。
【発明を実施するための最良の形態】

【００２１】
以下では、説明の重複を避けるため同じ機能を有する構成部や同じ処理を行う処理ステップには同一の番号を付与し、説明を省略する。
【００２２】
［実施例１］
図１は、実施例１のユーザ認証システムの構成を示す。クライアント装置１００とサービス提供装置２００は、ネットワーク１０を介して互いに通信可能なように接続される。ネットワーク１０は、例えばインターネットや企業内網である。サービス提供装置２００は、ユーザにサービスを提供する装置であり、例えばＷｅｂサーバなどである。クライアント装置１００は、サービス提供装置２００に対してユーザ認証を行うために認証応答を送信する装置であり、例えばブラウザ機能を備えた携帯電話、パーソナルコンピュータ、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）等である。なお、複数のクライアント装置１００および複数のサービス提供装置２００が、ネットワーク１０に接続される構成でもよい。
【００２３】
図２は、実施例１のクライアント装置の構成例を示す。クライアント装置１００は、ネットワークインターフェース１１０、制御部１２０、認証部１３０、認証情報管理部１４０、鍵生成部１５０、入力部１６０及び出力部１７０を含んで構成されている。
【００２４】
ネットワークインターフェース１１０はネットワーク１０に接続され、サービス提供装置２００との通信を行う。制御部１２０は当該クライアント装置１００全体の制御を行うものであり、例えばブラウザプログラムとして実現してもよい。
【００２５】
認証部１３０は、ネットワークインターフェース１１０を介してサービス提供装置２００から認証要求を受信し、ユーザ認証に必要な認証応答をネットワークインターフェース１１０を介してサービス提供装置２００に送信する。また、認証部１３０は、出力部１７０や入力部１６０を介してプロンプトの表示や、パスワードの入力、同意確認など、ユーザとの情報のやりとりを行う。
【００２６】
認証情報管理部１４０は、ユーザ認証のための認証応答生成に必要な鍵情報をサービス提供装置２００の証明書と関連付けて格納するもので、後述するサービス情報データベースを保持している。鍵生成部１５０は、認証情報管理部１４０に格納される鍵情報を生成する。
【００２７】
入力部１６０はユーザからの入力を受け付けるキーボードやマウス等である。出力部１７０は情報をユーザに出力（提示）するディスプレイ等である。
図３は、実施例１のサービス提供装置の構成例を示す。サービス提供装置２００は、ネットワークインターフェース２１０、サービス提供部２２０、認証部２３０及び認証情報管理部２４０を含んで構成されている。
【００２８】
ネットワークインターフェース２１０は、ネットワーク１０に接続され、クライアント装置１００との通信を行う。サービス提供部２２０は、認証が成功したユーザに対してサービス提供の可否を判定し、提供可であればサービスを提供する。提供するサービスとしては、例えば、クライアント装置１００へのコンテンツのオンライン配信、商品をユーザに発送するための受注処理などである。また、サービス提供部２２０は、サービス毎の認証ポリシー（後述する）を記憶している。
【００２９】
認証部２３０は、ネットワークインターフェース２１０を介してクライアント装置１００に認証要求を送信し、その応答としてクライアント装置１００から認証応答を受信する。認証情報管理部２４０は、ユーザ認証のための認証応答の確認に必要な鍵情報やパスワ

ードを、提供するサービスと関連付けて格納するもので、後述するユーザ情報データベースを保持している。

【００３０】

図４は、クライアント装置１００の認証情報管理部１４０が保持するサービス情報データベースの構成例を示す。各行が、一つのサービスと対応している。以下、各列について説明する。第１列にはサービスを提供するサービス提供装置のサーバ証明書が格納される。第２列にはサービス利用についてユーザに割り当てられているユーザＩＤが格納される。第３列にはサービス利用時の認証応答の検証に用いられる公開鍵が格納される。第４列にはサービス利用時の認証応答の生成に用いられる秘密鍵が格納される。

【００３１】

図５は、サービス提供装置２００の認証情報管理部２４０が保持するユーザ情報データベースの構成を示す。各行が一人のユーザと対応している。第１列にはサービスを利用するユーザのユーザＩＤが格納される。第２列にはサービス利用時のユーザ認証に用いられるユーザのパスワードが格納される。第３列にはサービス利用時の認証応答の検証に用いられるユーザの公開鍵が格納される。第４列にはサービス利用時に必要となるユーザ属性が格納される。ユーザ属性とは、例えばコンテンツ配信のためのクライアント装置１００のＩＰアドレス、商品発送のためのユーザの住所、決済のためのユーザのカード番号等である。

【００３２】

ユーザ登録

まず、ユーザがクライアント装置１００を介してサービス提供装置２００にユーザ登録を行う場合の手順を説明する。図６は、ユーザ登録の処理フローを示している。クライアント装置１００の制御部１２０は、ネットワークインターフェース１１０を介してサービス提供装置２００にユーザ登録要求を送信する（Ｓ１）。ユーザ登録要求とは、例えば、Ｗｅｂページで特定のサービスへの登録を決定したときに送信されるＨＴＴＰリクエストなどである。また、ユーザ登録要求は、利用するサービスを識別するためのインデックス情報を含んでもよい。インデックス情報とは、例えば前記ＨＴＴＰリクエストに含まれるＵＲＩなどである。

【００３３】

ユーザ登録要求を受信したサービス提供装置２００は、認証部２３０においてサーバ認証情報を生成する。サービス提供装置２００は、生成したサーバ認証情報を、ネットワークインターフェース２１０を介してクライアント装置１００に送信する（Ｓ２）。サーバ認証情報は、ディジタル署名やサーバ証明書等を含み、サービス提供装置２００の正当性が確認できるものである。

なお、サービス提供装置２００は、サーバ認証情報と一緒に、クライアント装置１００に、クライアント装置１００の処理フローを決めるプログラムも送ってもよい。このように、プログラムをステップＳ２で送ることで、クライアント装置１００はあらかじめプログラムを記録しておく必要がなくなる。つまり、クライアント装置１００は、後述するサーバ認証（Ｓ３）、鍵生成（Ｓ７）、署名計算（Ｓ８）などの個別の機能やデータベースを備えておけばよく、処理手順を記録しておく必要がない。このように処理手順を記載したプログラムを処理ごとに送れば、処理の追加や変更が容易になる。

【００３４】

サーバ認証情報を受信したクライアント装置１００は、認証部１３０によりサーバ認証情報を検証する（Ｓ３）。この検証が失敗した場合、クライアント装置１００はユーザ登録手順を終了する。検証が成功した場合、クライアント装置１００は以下の処理を行う。

以降に送受信されるデータのインテグリティ保証や秘匿性の実現のため、クライアント装置１００とサービス提供装置２００との間で保護チャネルを確立する（Ｓ４）。なお、Ｓ２～Ｓ４の手順はＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）などの既存のプロトコルを利用するものであってもよい。

【００３５】

クライアント装置１００の出力部１７０は、ユーザに対して、ユーザＩＤとパスワードを決定し入力するよう促す旨のメッセージを出力する。そして、クライアント装置１００の入力部１６０は、ユーザが入力したユーザＩＤとパスワードを受け付ける（Ｓ５）。クライアント装置１００の制御部１２０は、サービス提供装置２００のサービス提供部２２０と通信を行い、ユーザＩＤを決定する（Ｓ６）。なお、本実施例ではユーザがユーザＩＤを決定し、クライアント装置よりサービス提供装置へ送信する手順で説明した。しかし、サービス提供装置がユーザＩＤを決定し、クライアント装置に通知する手順であってもよい。

【００３６】

続いてクライアント装置１００の鍵生成部１５０が、鍵ペアを生成する（Ｓ７）。鍵ペアとは公開鍵暗号系で用いる秘密鍵と公開鍵のペアである。クライアント装置１００は、ユーザ登録に必要なユーザ情報を収集すると共にディジタル署名（以下、署名）を計算する（Ｓ８）。

【００３７】

図７は、ユーザ情報の例を示している。ユーザ情報は、ユーザＩＤ、パスワード、公開鍵、ユーザ属性、タイムスタンプ、署名を含む。ユーザ属性とは、サービス提供に必要なユーザに関する情報である。例えば住所、氏名やカード番号等である。署名は、ユーザ情報のうちの署名以外の情報に対して秘密鍵を用いて計算されたものである。なお、ユーザ情報は、その署名を検証するための公開鍵を含んでいる。したがって、ユーザ情報は、自己署名証明書としても機能する。

【００３８】

ユーザ登録の手順の説明に戻ると、クライアント装置１００の制御部１２０は、ネットワークインターフェース１１０を介して、図７に示されるユーザ情報をサービス提供装置２００に送信する（Ｓ９）。ユーザ情報を受信したサービス提供装置２００は、認証部２３０によりユーザ情報の正当性を検証する（Ｓ１０）。具体的には、認証部２３０は、ユーザ情報に含まれる公開鍵を用いてユーザ情報に含まれる署名を検証し、さらにユーザ情報に含まれるタイムスタンプが正しいことを確認する。

【００３９】

この検証が失敗した場合、サービス提供装置２００は、ユーザ登録結果として「ＮＧ」をクライアント装置１００に送信する（Ｓ１２）。検証が成功した場合、サービス提供装置２００は以下の処理を行う。サービス提供装置２００の認証情報管理部２４０は、ユーザ情報をユーザ情報データベースに登録する（Ｓ１１）。なお、ユーザ情報データベースの構成は前述した通りである。サービス提供装置２００は、ネットワークインターフェース２１０を介してユーザ登録結果として「ＯＫ」を、クライアント装置１００に送信する（Ｓ１２）。

【００４０】

ユーザ登録結果が「ＮＧ」の場合、クライアント装置１００は、ユーザ登録手順を終了する。ユーザ登録結果が「ＯＫ」の場合、クライアント装置１００の認証情報管理部１４０は、サービス情報（ステップＳ２で受信したサーバ証明書にユーザＩＤ、公開鍵、秘密鍵を対応付けた情報）をサービス情報データベースに登録する（Ｓ１３）。なお、サービス情報データベースの構成は、前述した通りである。サービス提供装置２００は、ユーザ情報の検証後にユーザ情報を登録することで、クライアント装置１００で保持される鍵ペアとユーザが記憶するパスワードとの関連付けが保証される。さらに、鍵ペアと登録時にユーザが入力した属性情報との関連付けが保証される。

【００４１】

ユーザ認証

図８は、ユーザ認証を行う場合の手順を示している。クライアント装置１００の制御部１２０は、ネットワークインターフェース１１０を介してサービス提供装置２００にサービス要求を送信する（Ｓ２０）。サービス要求とは、例えば、Ｗｅｂページで特定のサービスの利用を決定したときに送信されるＨＴＴＰリクエストなどである。また、サービス

要求は、利用するサービスを識別するためのインデックス情報を含んでもよい。インデックス情報とは、例えば前記ＨＴＴＰリクエストに含まれるＵＲＩなどである。

【００４２】

サービス要求を受信すると、サービス提供装置２００のサービス提供部２２０は、要求されたサービスに対する認証ポリシーを取得する（Ｓ２１）。認証ポリシーとは、例えば、サービス提供に必要な認証の強度や同意確認の有無などである。本実施例では、認証ポリシーとして、公開鍵認証を要求（ＰＫ）、パスワード認証を要求（ＰＷ）、公開鍵とパスワードの組み合わせによる認証を要求（ＰＫＰＷ）の３種類とする。認証ポリシーの取得は、サービスごとにあらかじめ記憶された認証ポリシーを読み出すことなどにより行う。

【００４３】

サービス提供装置２００の認証部２３０は、認証要求を生成し、ネットワークインターフェース２１０を介してクライアント装置１００に送信する（Ｓ２２）。なお、サービス提供装置２００は、認証要求と一緒に、クライアント装置１００に、クライアント装置１００の処理フローを決めるプログラムも送ってもよい。このように、プログラムをステップＳ２２で送ることで、クライアント装置１００はあらかじめプログラムを記録しておく必要がなくなる。つまり、クライアント装置１００は、後述するサーバ認証（Ｓ２３）、署名計算（Ｓ２９）などの個別の機能やデータベースを備えておけばよく、処理手順を記録しておく必要がない。このように処理手順を記載したプログラムを処理ごとに送れば、処理の追加や変更が容易になる。

【００４４】

図９は、認証要求の形式の例を示している。認証要求は、認証ポリシー、チャレンジ、確認メッセージ、タイムスタンプ、署名、サーバ証明書を含む。認証ポリシーはステップＳ２１で取得したものである。チャレンジは、クライアント装置１００が、認証要求に対する認証応答を計算するために用いる値であり、具体的には乱数等が用いられる。チャレンジは、保護されたチャネル上でパスワード認証を要求する場合には省略しても良い。確認メッセージは、認証時にユーザに表示されるメッセージであり、ユーザの同意確認を取りたい内容を表す。なお、確認メッセージは省略することもできる。タイムスタンプは、認証要求を生成した日時を確認するための情報である。署名は、前記認証ポリシー、チャレンジ、タイムスタンプに対してサービス提供装置２００の保持する秘密鍵で計算した署名である。サーバ証明書は署名を検証するための公開鍵を含む証明書である。

【００４５】

ユーザ認証の手順の説明に戻る。認証要求を受信すると、クライアント装置１００の認証部１３０は、認証要求を検証する（Ｓ２３）。具体的には、受信したサーバ証明書に含まれる公開鍵で、認証要求に含まれる署名を検証し、サーバ証明書の内容を確認する。

この検証が失敗した場合、クライアント装置１００は、ユーザ認証手順を終了する。検証が成功した場合、クライアント装置１００は、以下の処理を行う。まず、以降に送受信されるデータのインテグリティ保証や秘匿性の実現のため、必要に応じて、クライアント装置１００とサービス提供装置２００は、保護チャネルを確立する（Ｓ２４）。なお、Ｓ２２～Ｓ２４の手順はＳＳＬなどの既存のプロトコルを利用するものであってもよい。続いてクライアント装置１００は、サービス提供装置２００から受信した認証要求に含まれる認証ポリシーを参照し、認証法を選択する（Ｓ２５）。具体的には、参照した認証ポリシーを用いる、あるいは参照した認証ポリシーと、クライアント装置１００が保持する認証ポリシーから計算された新たな認証ポリシーを用いる等である。

【００４６】

選択した認証法がＰＷであれば、クライアント装置１００は、以下を実行する。まず、認証要求に確認メッセージが含まれる場合は、出力部１７０が、確認メッセージを出力する。認証要求に確認メッセージが含まれない場合は、出力部１７０が、ユーザＩＤとパスワードの入力を促す旨のメッセージを出力する（Ｓ２６）。そして、入力部１６０は、ユーザから入力されたユーザＩＤとパスワードを受け付ける（Ｓ２７）。なお、ユーザＩＤ

は、例えば次の手順で取得してもよい。まず、Ｓ２２で受信したサーバ証明書を用いて、認証情報管理部１４０に保持されたサービス情報データベースを検索し、そのサービスのエントリーを特定する。そして、そのエントリーのユーザＩＤのフィールドを参照してユーザＩＤを取得する。　次に、クライアント装置１００の認証部１３０は、入力されたパスワード等からパスワード認証情報を計算する（Ｓ２８）。ここで、パスワード認証情報は、パスワード、チャレンジ、クライアント装置１００のＩＰアドレス等を入力として計算されたハッシュ値などである。つまり、パスワード認証情報は、パスワードの所有を確認できる情報である。なお、パスワード認証情報の代わりにパスワード自体を用いることもできる。しかし、その場合は、パスワードが認証応答の一部としてネットワーク１０を通ってサービス提供装置２００に送信される。したがって、ステップＳ２４で、クライアント装置１００とサービス提供装置２００が、保護チャネルを確立していることが望ましい。クライアント装置１００の制御部１２０は、図１０Ａに示すような、認証法（ＰＷ）、ユーザＩＤ、パスワードもしくはパスワード認証情報からなる認証応答を生成する（Ｓ３０）。

【００４７】

選択した認証法がＰＫであれば、クライアント装置１００の認証部１３０は、認証法（ＰＫ）、ユーザＩＤ、チャレンジ、タイムスタンプに対する署名１を計算する（Ｓ２９）。なお、署名１は、認証応答として送信する情報のうち、署名自身を除いた全ての情報に対して計算される。クライアント装置１００のＩＰアドレスなどを認証応答に追加する場合には、それらも署名計算の入力となる。また、チャレンジは、認証要求に含まれるチャレンジと同一である。タイムスタンプは認証応答を生成した時刻を表すものである。署名に用いる秘密鍵は次の手順で取得する。まず、ステップＳ２２で受信したサーバ証明書を用いて、認証情報管理部１４０のサービス情報データベースを検索し、そのサービスのエントリーを特定する。そして、そのエントリーの秘密鍵のフィールドを参照して秘密鍵を取得する。クライアント装置１００の制御部１２０は、図１０Ｂに示すような、認証法（ＰＫ）、ユーザＩＤ、チャレンジ、タイムスタンプ、署名１からなる認証応答を生成する（Ｓ３０）。

【００４８】

選択した認証法がＰＫＰＷであれば、クライアント装置１００の出力部１７０は、認証要求に確認メッセージが含まれる場合は、確認メッセージを出力する。また、クライアント装置１００の出力部１７０は、認証要求に確認メッセージが含まれない場合は、ユーザＩＤとパスワードの入力を促す旨のメッセージを出力する（Ｓ２６）。そして、入力部１６０は、ユーザが入力したユーザＩＤとパスワードを受け付ける（Ｓ２７）。次に、クライアント装置１００の認証部１３０は、認証法（ＰＫＰＷ）、ユーザＩＤ、チャレンジ、パスワード、確認メッセージ、タイムスタンプに対する署名２を計算する（Ｓ２９）。クライアント装置１００のＩＰアドレスなどを認証応答に追加する場合には、それらも署名計算の入力となる。なお、署名に用いる秘密鍵は、認証方法（ＰＫ）の場合と同様に、認証情報管理部１４０のサービス情報データベースに格納された秘密鍵を用いる。次に、クライアント装置１００の制御部１２０は、図１０Ｃに示すような、認証法（ＰＫＰＷ）、ユーザＩＤ、チャレンジ、タイムスタンプ、署名２からなる認証応答を生成する（Ｓ３０）。

【００４９】

なお、パスワードおよび確認メッセージが認証応答に含まれないのは、以下の理由による。パスワードは、サービス提供装置２００の認証情報管理部２４０のユーザ情報データベースを、ユーザＩＤに基づいて検索すれば取得可能である。署名２を検証することで、ユーザがクライアント装置１００に正しくパスワードを入力したことが確認できるので、パスワードを認証応答に含めなくても良い。同様に、確認メッセージもサービス提供装置２００により特定可能である。よって、署名２の検証を行うために確認メッセージを認証応答に含めなくてもよい。

【００５０】

クライアント装置１００は、上述のとおり認証法ごとに生成された認証応答を、ネットワークインターフェース１１０を介してサービス提供装置２００に送信する（Ｓ３１）。認証応答を受信すると、サービス提供装置２００の認証部２３０は、受信した認証応答に含まれる認証法が、ステップＳ２２で送信した認証要求に含まれる認証ポリシーと整合するかを確認する（Ｓ３２）。

【００５１】

さらに、認証部２３０は、認証処理を行う（Ｓ３３）。具体的には、認証部２３０は、認証応答に含まれるユーザＩＤに基づいて、認証情報管理部２４０のユーザ情報データベースを検索し、該当するユーザのエントリーを特定する。そして、各認証法に応じて次の処理を実行する。認証応答に含まれる認証法がＰＷの場合には、認証部２３０は、ユーザのエントリーからパスワードを取得し、認証応答に含まれるパスワードもしくはパスワード認証情報と整合するかを確認する。認証応答に含まれる認証法がＰＫの場合には、認証部２３０は、ユーザのエントリーから公開鍵を取得し、この公開鍵を用いて認証応答情報に含まれる署名１の正当性を確認する。さらに、認証部２３０は、タイムスタンプが適正であるか（現在時刻に近い時刻を表しているか）、およびチャレンジがステップＳ２２の認証要求として送られたものと同じであるかの確認を行う。認証応答に含まれる認証法がＰＫＰＷの場合には、認証部２３０は、ユーザのエントリーから公開鍵を取得し、この公開鍵を用いて認証応答情報に含まれる署名２の正当性を確認する。署名２の検証には、ステップＳ２９で署名２を生成したときと同じ署名対象を取得する必要がある。署名対象の一つであるパスワードは、ユーザのエントリーを参照して取得できる。確認メッセージは、ステップＳ２２でクライアント装置１００に送信した確認メッセージを参照して取得できる。つまり、署名２を検証するために、認証応答にパスワードや確認メッセージを含める必要はない。認証部２３０は、さらに、認証法がＰＫの場合と同様に、タイムスタンプが適正であるか、およびチャレンジがステップＳ２２で認証要求として送られたものと同じであるかの確認を行う。

【００５２】

認証法毎の認証応答の検証が成功した場合には、サービス提供部２２０は、認証応答に含まれたユーザＩＤ（認証が成功したユーザＩＤ）により特定されるユーザに対して、Ｓ２０で要求されたサービス提供の可否を判断する（Ｓ３４）。具体的には、サービス提供部２２０は、ユーザＩＤで特定されるユーザに対して提供可能なサービスを予め登録したサービス提供部２２０に含まれる認可データベース等（図示せず）により、サービス提供の可否を判断する。認証および認可が成功した場合には、サービス提供装置２００はユーザにサービスを提供する（Ｓ３５）。以上の認証および認可が失敗した場合、サービス提供装置２００は、サービス要求の結果として「ＮＧ」を、ネットワークインターフェース２１０を介してクライアント装置１００に送信する（Ｓ３５）。

【００５３】

なお、認証法がＰＫＰＷの場合には、上述のようにユーザがパスワードを知っていることが確認できるため、認証応答としてパスワードを送信する必要がない。したがって、より安全である。また、ステップＳ３２で署名の検証に成功した場合、ユーザ認証で利用されるクライアント装置１００が持つ鍵ペアは、サービス提供装置２００の認証情報管理部２４０に保持されたユーザ情報データベースに含まれる公開鍵に対応することが保証される。さらには、ユーザ認証で利用されるクライアント装置１００が持つ鍵ペアは、ユーザ登録に成功したクライアント装置１００の持つ鍵ペアに対応することが保証される。つまり、ユーザ認証時に利用されるクライアント装置とユーザ登録時に利用されたクライアント装置とが同一であることが保証される。また、登録時と認証時に入力したパスワードの一致により、それぞれの時点でクライアント装置１００を操作するユーザが同一であることが保証される。

【００５４】

また、ＰＫＰＷによる認証の場合、認証応答には、パスワードに対して秘密鍵で計算した署名が含まれる。このことによりパスワードを知っているユーザを、秘密鍵と対応する

公開鍵に関連付けることができる。さらに、公開鍵により、そのユーザを、サービス提供装置２００の認証情報管理部２４０に保持されたユーザ情報データベースに登録されているユーザ属性に関連付けることができる。以上により、認証を行うユーザが、ユーザ登録時に登録されたユーザ属性を持つユーザ本人であることが保証される。

【００５５】

また、ＰＫＰＷによる認証の場合、認証応答には、秘密鍵を用いて確認メッセージから求めた署名が含まれる。クライアント装置１００が、ユーザが入力したパスワードを保存しない場合、署名を検証することで、認証時にユーザがパスワードを入力したことを保証できる。さらに、出力部１７０が、認証要求に含まれる確認メッセージをユーザに出力している場合には、ユーザのみが知るパスワードを入力したことをもって、確認メッセージに対する同意確認を行うことができる。

【００５６】

なお、本実施例では、ユーザがサービス提供装置２００からサービスを受ける際に、クライアント装置１００は、サービス提供装置２００がクライアント装置１００に送信した認証要求に含まれるサーバ証明書の正当性を検証する。そして、クライアント装置１００は、検証が成功したサーバ証明書に関連付けられているサービス情報を特定する。さらに、クライアント装置１００は、認証要求に含まれる認証ポリシーと、クライアント装置１００が保持する認証ポリシーから計算された認証ポリシーとに基づき、特定されたサービス情報に含まれる秘密鍵もしくはパスワードを選択または組み合わせて、認証応答を生成し、サービス提供装置２００に送信する。このような手順で認証を行うので、サービス提供装置２００に成りすましてユーザのパスワードを不正に取得することが困難になり、安全なユーザ認証を実現できる。

【００５７】

なお、本実施例において、ユーザ登録手順のＳ９で送信されるユーザ情報、ユーザ認証手順のＳ２２で送信される認証要求、Ｓ３１で送信される認証応答は、ＳＡＭＬ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｅｒｔｉｏｎ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）等の標準プロトコルに従うものであってもよい。

【００５８】

［実施例２］

実施例２のユーザ認証システムのシステム構成は、実施例１（図１）と同じである。図１１は、実施例２のサービス提供装置の機能構成例を示している。サービス提供装置３００は、実施例１のサービス提供装置２００の認証情報管理部２４０に代えて認証情報管理部３４０を含むとともに、認証情報変換部３５０を新たに含んでいる。認証情報管理部３４０は、ユーザ認証のために必要なパスワードを、提供するサービスと関連付けて格納している。認証情報変換部３５０は、必要に応じて、公開鍵認証（ＰＫもしくはＰＫＰＷ）の結果を正しいパスワードに変換する。

【００５９】

図１２は、サービス提供装置３００の認証情報管理部３４０が保持するユーザ情報データベースの構成を示している。各行が一人のユーザと対応している。また、第１列には、サービスを利用するユーザに割り当てられているユーザＩＤが格納される。第２列には、サービス利用時のユーザ認証に用いられるユーザのパスワードが格納される。第３列には、サービス利用時に必要となるユーザ属性が格納される。なお、認証情報管理部３４０が保持するユーザ情報データベースは、パスワード認証を行うサービスに共通の典型的なユーザ情報データベースであり、従来、用いられているものと同じと考えてよい。

【００６０】

図１３は、サービス提供装置３００の認証情報変換部３５０が保持する認証情報変換データベースの構成を示している。各行が一人のユーザと対応している。また、第１列には、サービスを利用するユーザに割り当てられているユーザＩＤが格納される。第２列には、サービス利用時のユーザ認証に用いられるユーザのパスワードが格納される。第３列には、サービス利用時の認証応答の検証に用いられるユーザの公開鍵が格納される。なお、

認証情報変換部３５０が保持する認証情報変換データベースは、図１２に示したユーザ情報データベースと組み合わせることで、本発明のユーザ認証を実現するものである。

【００６１】

ユーザ登録

本実施例のユーザ認証システムで、ユーザがクライアント装置１００を介してサービス提供装置３００にユーザ登録を行う場合の手順について説明する。図１４は、実施例２のユーザ認証システムでのユーザ登録の処理フローを示している。ステップＳ１からステップＳ１０までは、実施例１（図６）と同じである。

【００６２】

ステップＳ１０において、クライアント装置１００から受信したユーザ情報の正当性の検証に成功したサービス提供装置３００は、ユーザＩＤ、パスワード、公開鍵、ユーザ属性、タイムスタンプ、署名からなるユーザ情報のうち、ユーザＩＤ、パスワード、ユーザ属性の組を認証情報管理部３４０のユーザ情報データベースに登録する（Ｓ１４）。そして、サービス提供装置３００は、ユーザＩＤ、公開鍵、パスワードの組を認証情報変換部３５０の認証情報変換データベースに登録する（Ｓ１５）。続くステップＳ１２以降の手順も、実施例１（図６）と同じである。

【００６３】

ユーザ認証

次に、実施例２のユーザ認証システムで、ユーザがクライアント装置１００を介してサービス提供装置３００に対して認証を行う場合の手順について説明する。図１５は、実施例２のユーザ認証システムでの認証の処理フローを示している。なお、ステップＳ２０からステップＳ３２までは、実施例１（図８）と同じである。

ステップＳ３２の次に、サービス提供装置３００の認証部２３０は、認証法に応じた以下のパスワード取得処理を行う（Ｓ３６）。

【００６４】

認証応答に含まれる認証法がＰＷの場合、認証部２３０は、認証応答に含まれるパスワードもしくはパスワード認証情報を取得する。

認証応答に含まれる認証法がＰＫの場合、認証部２３０は、認証応答に含まれるユーザＩＤに基づいて、認証情報変換部３５０に保持された認証情報変換データベースを検索し、該当するユーザのエントリーを特定する。認証部２３０は、このエントリーの公開鍵を用いて認証応答に含まれる署名１の正当性を確認する。認証部２３０は、さらに、タイムスタンプが適正であるか（現在時刻に近い時刻を表しているか）、および、チャレンジがステップＳ２２の認証要求として送られたものと同じであるかの確認を行う。認証部２３０は、この確認に成功した場合に前記エントリーのパスワードを取得する。

【００６５】

認証応答に含まれる認証法がＰＫＰＷの場合、認証部２３０は、認証応答に含まれるユーザＩＤに基づいて、認証情報変換部３５０に保持された認証情報変換データベースを検索し、該当するユーザのエントリーを特定する。認証部２３０は、このエントリーの公開鍵を用いて認証応答に含まれる署名２の正当性を確認する。認証部２３０は、この確認に成功した場合に前記エントリーのパスワードを取得する。なお、署名２の正当性の確認については実施例１と同様である。

【００６６】

認証法に従ったパスワード取得処理が終了した後、サービス提供装置３００の認証部２３０は、ステップＳ３１において受信した認証応答に含まれるユーザＩＤと、ステップＳ３６において取得したパスワードもしくはパスワード認証情報とによりパスワード認証処理を行う（Ｓ３７）。具体的には、認証部２３０は、認証情報管理部３４０に保持されたユーザ情報データベースをユーザＩＤに基づいて検索し、該当するユーザのエントリーを特定する。このエントリーに含まれるパスワードと、ステップＳ３６において取得したパスワードもしくはパスワード認証情報とを照合することで認証を行う。ステップＳ３７の認証処理の終了後、ステップＳ３４の認可処理を実行する。ステップＳ３４を含めて、そ

れ以降の処理は、実施例１と同じである。

【００６７】

実施例２のユーザ認証システムでは、サービス提供装置３００の認証部２３０が、認証情報変換部３５０を用いて、各認証法それぞれに異なる認証応答を、ユーザＩＤとパスワードもしくはパスワード認証情報との組に変換する。そして、認証部２３０が、この組と、認証情報管理部３４０に保持されたユーザ情報データベースとを用いてパスワード認証を行っている。なお、ユーザ情報データベースは従来のパスワード認証に基づくものである。つまり、認証情報変換部３５０の変換情報データベースを、ユーザ情報データベースに付加することで本発明の効果を生じさせている。

【００６８】

このように構成することによって、従来のパスワード認証に基づくサービス提供装置に対して少ない変更で、より強固でかつ同意確認機能を持つユーザ認証システムに変更することができる。また、提供するサービス毎に異なる認証要求に応じた複数の認証法を容易に切り替えて利用することができる。そして、認証法の違いをサービスから隠蔽することで、サービス開発が容易となる。なお、本実施例の構成は、サービス提供装置３００内に変換データベースを付加するものであって、従来技術のようにサービス提供装置の外に、代理認証機構を設置するものではない。このことにより、サービス提供装置と代理認証機構の分離に伴う問題、即ち提供するサービスに応じた認証ポリシーに基づく認証法のネゴシエーションが困難であること、サービス提供装置に対するサーバ認証を行いその結果に基づきユーザ認証を行うことが困難であること、サービス提供装置と代理認証機構との間で情報を安全にやり取りするための手順が別途必要であること、などが生じない。したがって、複数の認証法を容易に切り替える柔軟なユーザ認証を実現できる。

【００６９】

［実施例３］

図１６は、実施例３のユーザ認証システムの構成を示している。クライアント装置４００とサービス提供装置２００は、ネットワーク１０を介して互いに通信可能なように接続される。また、クライアント装置４００と鍵装置５００は、互いに通信可能なように接続される。

【００７０】

鍵装置５００は、クライアント装置４００に対してユーザ認証機能を提供するものである。具体的には、実施例１のクライアント装置１００が持つ構成要素のうち、ユーザ認証にかかわる構成要素を抜き出して分離したものであり、鍵装置５００とクライアント装置４００を合わせてクライアント装置１００と同様の機能を備える。

【００７１】

このような構成をとる目的は、複数のクライアント装置４００を利用する場合でも、共通の鍵装置５００と組み合わせて利用することで認証設定の共通化が図れるようにすること、および、クライアント装置４００を変更する場合でもサービスが継続して受けられるようにすることである。例えば、鍵装置５００が携帯電話、クライアント装置４００がＰＣ等であってもよい。

【００７２】

図１７は、実施例３のクライアント装置の構成例を示している。クライアント装置４００は、クライアント装置１００と同様にネットワークインターフェース１１０及び制御部１２０を含み、さらに鍵装置５００と通信するためのＰＡＮ（Ｐｅｒｓｏｎａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）インターフェース４１０を含んでいる。ＰＡＮの例としては、ＢｌｕｅｔｏｏｔｈやＵＷＢ（Ｕｌｔｒａ　Ｗｉｄｅ　Ｂａｎｄ）などの無線通信、ＩｒＤＡなどの赤外線通信、ＵＳＢなどの有線通信などがあげられる。

【００７３】

図１８は、実施例３の鍵装置５００の構成を示している。鍵装置５００は、クライアント装置１００と同じように、認証部１３０、認証情報管理部１４０、鍵生成部１５０、入力部１６０、出力部１７０を含む、さらにクライアント装置４００と通信するためのＰＡ

Ｎインターフェース５１０を含んでいる。

【００７４】

図１９は、鍵装置５００の認証情報管理部１４０が保持するサービス情報データベースの構成を示している。これは、図４のサービス情報データベースに、パスワードを格納するため列（第５列）を追加したものである。これは、鍵装置５００でユーザのパスワードを記憶することをサービス提供装置２００が許可した場合に、当該サービスを利用するためのパスワードを当該サービスに関連付けて記憶するためのものである。このように、サービスに関連付けてパスワードを記憶することで、ユーザによるパスワードの入力を省略でき、利便性が向上する。

【００７５】

ユーザ登録

図２０は、実施例３のユーザ認証システムでのユーザ登録の処理フローを示している。サービス提供装置２００は、パスワード記憶ポリシーを、サーバ認証情報に含めてクライアント装置４００に送信する（Ｓ４０）。なお、サーバ認証情報は、パスワード記憶ポリシーを含むこと以外、実施例１のステップＳ２で送信されるものと同一である。また、パスワード記憶ポリシーは、鍵装置５００でユーザのパスワードを記憶することを許可するか否かを表すフラグであり、そのフラグがＹＥＳを示す場合、鍵装置５００はユーザのパスワードを記憶することができる。一方、フラグがＮＯを示す場合、鍵装置５００はユーザのパスワードを記憶することができない。この場合、ユーザはサービス利用時の認証の都度、パスワードを入力する必要がある。

【００７６】

クライアント装置４００の制御部１２０は、受信した情報がサーバ認証情報であることを判断した場合、受信したサーバ認証情報を、ＰＡＮインターフェース４１０を介して鍵装置５００に送信する（Ｓ４１）。

サーバ認証情報を受信した鍵装置５００は、実施例１のクライアント装置１００と同様に、ステップＳ３からステップＳ８まで、およびステップＳ１２を実行する。

【００７７】

引き続いて実行されるステップＳ４２において、ステップＳ４１で受信したサーバ認証情報に含まれるパスワード記憶ポリシーがＹＥＳであった場合は、鍵装置５００は、サーバ証明書、ユーザＩＤ、公開鍵、秘密鍵、パスワードをサービス情報データベースの１つのエントリーとして追加する。一方、ステップＳ４１で受信したパスワード記憶ポリシーがＮＯであった場合には、鍵装置５００は、上記パスワードに代えて、パスワードが記憶されていない旨を表す記号（例えば「－」など）を用いてエントリーを追加する（Ｓ４２）。次に、鍵装置５００は、ＰＡＮインターフェース５１０によりサービス登録結果をクライアント装置４００に送信する（Ｓ４３）。

【００７８】

ユーザ認証

図２１は、実施例３のユーザ認証システムのユーザ認証の処理フローを示している。ステップＳ２２で、サービス提供装置２００からの認証要求を受信したクライアント装置４００では、制御部１２０が受信した情報が認証要求であることを判断した場合、ＰＡＮインターフェース４１０が受信した認証要求を鍵装置５００に送信する（Ｓ４４）。認証要求を受信した鍵装置５００は、実施例１のクライアント装置１００と同様に、ステップＳ２３からＳ２６までを実行する。

【００７９】

次に、鍵装置５００は、ＩＤとパスワードが必要な場合には、サーバ証明書に基づき、認証情報管理部１４０に格納されたサービス情報データベースを検索し、サービスに対応するエントリーを特定する。特定したエントリーのパスワードのフィールドに値が記憶されている場合には、その値をパスワードとして取得する（Ｓ４５）。また、ユーザＩＤフィールドの値を、ユーザＩＤとして取得する（Ｓ４５）。一方、特定したエントリーのパスワードのフィールドに値が記憶されていない場合には、実施例１のステップＳ２７と同

様に、入力部１６０がユーザＩＤとパスワードを受け付ける（Ｓ４５）。引き続いて、実施例１のクライアント装置１００と同様に、ステップＳ２８からＳ３１までを実行する。

【００８０】

実施例３のユーザ認証システムでは、クライアント装置４００ではなく、鍵装置５００により、ユーザ認証を行う。このため、クライアント装置４００が複数ある場合でも、１つの鍵装置５００により認証設定が共通化できる。つまり、複数のクライアント装置４００に、それぞれ認証設定をする必要がない。よって、利便性が向上する。またクライアント装置４００を変更する場合も移行が簡単になる。

実施例１のクライアント装置１００がＰＣ等のオープンプラットフォームで構成される場合、パスワード入力を代行するブラウザソフトやミドルウェアが動作している場合もあり得る。この場合、ユーザはパスワード入力を省略できるので便利になる。しかし、反面、ユーザからのパスワード入力を期待しているサービス提供装置２００にとっては、安全性の低下となる恐れがある。

【００８１】

実施例３のユーザ認証システムでは、クライアント装置４００をオープンプラットフォームで構成しつつ、認証処理を行う鍵装置５００をクローズドプラットフォームとして構成できる。このように構成することで、クライアント装置４００を汎用化しつつ、鍵装置５００がパスワード記憶ポリシーを強制することができる。具体的に言うと、鍵装置５００は、ステップＳ４０で送信されるパスワード記憶ポリシーに基づき、パスワードの記憶の可否を制御できる。

【００８２】

［実施例４］

実施例４は、実施例１の認証法の選択をより詳細に規定したものである。実施例４のユーザ認証システムのシステム構成は、実施例１（図１）と同一である。また、クライアント装置１００およびサービス提供装置２００の構成も、実施例１（図２、図３）と同一である。

【００８３】

図２２Ａは、クライアント装置１００の認証部１３０に格納された認証法対応表の内容が示されている。認証法対応表は、要求される認証のレベルに対して具体的にどの認証法を用いて認証するかの対応を表すものである。

行は同意確認のレベルを表している。２行目は同意確認のレベル０に対応している。同意確認のレベル０は、認証の際に同意確認が不要であることを表す。３行目は同意確認のレベル１に対応している。同意確認のレベル１は、認証の際に同意確認が必要であることを表す。列は認証強度のレベルを表している。２列目は強度のレベル０に対応している。強度のレベル０は、低強度の認証で十分であることを表す。３列目は強度のレベル１に対応している。強度のレベル１は、中強度の認証が必要であることを表す。４列目は強度のレベル２に対応している。強度のレベル２は、高強度の認証が必要であることを表す。

【００８４】

ここで、必要とされる認証強度のレベルＳと同意確認のレベルＣとの組＜Ｓ，Ｃ＞を認証ポリシーと呼ぶこととする。例えば＜１，０＞は、少なくとも強度のレベルが１以上、かつ同意確認のレベルが０以上となる認証法が要求されることを表す。認証強度と同意確認のレベルの組み合わせ（認証ポリシー）により分類された表の各要素の内容は、それぞれに対応する認証法を表している。その記号の意味は以下の通りである。

ＮＡ（Ｎｏ　Ａｃｔｉｏｎ）はユーザの認証操作が不要なもの、例えばユーザＩＤの通知などを示している。ＯＫはＯＫボタンをクリックするなどの単純な操作を示している。ＰＫは公開鍵に基づく認証を示している。ＰＷはパスワードに基づく認証を示している。ＰＫＰＷは公開鍵とパスワードの組み合わせによる認証法を示している。

【００８５】

例えば、認証ポリシー＜１，０＞に適合する認証法はＰＫ，ＰＷおよびＰＫＰＷの３通りである。なお、その性質から明らかなように、ポリシーは束による半順序構造を持つ。

例えば、あるポリシーＰ１＝＜Ｓ１，Ｃ１＞に適合する認証法Ｘは、Ｐ２≦Ｐ１となるポリシーＰ２（Ｐ２＝＜Ｓ２，Ｃ２＞としたとき、Ｓ２≦Ｓ１かつＣ２≦Ｃ１が成り立つようなＰ２）に対しても適合する。また表から分かるように、ＮＡは＜０，０＞に、ＯＫは＜０，１＞に、ＰＷは＜１，１＞に、ＰＫは＜２，０＞に、ＰＫＰＷは＜２，１＞にそれぞれ適合する。

【００８６】

ユーザ登録

実施例４のユーザ認証システムでユーザ登録を行う処理フローは、実施例1（図６）と同じである。

【００８７】

ユーザ認証

図８は、実施例４のユーザ認証システムのユーザ認証の処理フローを示している。ステップＳ２２の認証要求に含まれる認証ポリシーは、上述した形式とする。即ち、必要とされる認証強度のレベルＳと同意確認のレベルＣの組＜Ｓ，Ｃ＞で表されている。なお、本実施例の認証ポリシーも、サービス提供装置２００のサービス提供部２２０にサービス毎に記憶されている。ステップＳ２３，Ｓ２４は実施例１と同じである。

【００８８】

ステップＳ２５の認証の選択は次のように行われる。例えば、クライアント装置１００の認証部１３０に格納された認証法対応表が図２２Ａに示されるものであって、ステップＳ２２でクライアント装置１００がサービス提供装置２００から受信した認証ポリシーが＜１，０＞である場合、認証法としてはＰＫ、ＰＷまたはＰＫＰＷが該当する。そして、ユーザの好み等により、例えばＰＫが選択される。また、認証ポリシーが＜２，０＞である場合、認証法としてはＰＫまたはＰＫＰＷが該当するが、例えば、より簡易なＰＫが選択される。

【００８９】

別の例として、クライアント装置１００が認証法ＰＫに対応していない場合、認証法対応表は、例えば図２２Ｂに示されるものとする。このとき、クライアント装置１００が受信した認証ポリシーが＜１，０＞である場合、認証法としてはＰＷのみが該当するため、ＰＷが選択される。また認証ポリシーが＜２，０＞である場合も、認証法としてＰＷのみが該当するため、ＰＷが選択される。但し、後者の場合は、サービス提供装置２００は、ステップＳ３２で認証法ＰＷが認証ポリシー＜２，０＞を満たしていないことを確認する。このような場合は、サービス提供装置２００は、提供するサービスを限定して認可を行うなどの制御を行えばよい。

【００９０】

上述したように、サービス提供装置２００からクライアント装置１００に送信される認証ポリシーに自由度を持たせることによって、クライアント装置１００において、より柔軟な認証法の選択が可能となる。例えば、クライアント装置１００がサポートする認証法への適合や、要求されるレベルより強い認証法の選択が可能となる。また本実施例では、認証ポリシーの要素として認証強度と同意確認のレベルを扱ったが、これに限らない。例えば、生体認証情報の有無、否認不可性の有無など、他の要素を追加することもできる。

【００９１】

［実施例４変形例］

本変形例は、サービス提供装置２００からクライアント装置１００に送信される認証ポリシーの選択に関して、クライアント装置１００からの要求を、予めサービス登録時に送信しておく手順を追加したものである。

【００９２】

本変形例のユーザ認証システムのシステム構成は、実施例１（図１）と同一である。また、クライアント装置１００およびサービス提供装置２００の構成も、実施例１（図２、図３）と同一である。また、本変形例のユーザ認証システムでの、ユーザ登録の処理フローも、実施例１（図６）と同一である。

図２３は、ステップＳ９でクライアント装置１００からサービス提供装置２００に送信されるユーザ情報が示されている。これは、図７で示される実施例１のユーザ情報に、ユーザポリシーが付加されている。ユーザポリシーとは、サービス利用時にサービス提供装置からクライアント装置に送信される認証要求に含まれる認証ポリシーを決定するための、ユーザからの要求である。なお、認証ポリシーは、ユーザポリシーと、サービス提供装置が提供するサービス毎に予め決められたサービスポリシーとから後述する手順で計算される。

【００９３】

図２４Ａは、ユーザポリシーの具体例を示している。例えば、図２４Ａの２行目、３列目の内容は＜２，０＞となっている。また図において２行目、３列目の位置はサービスポリシー＜１，０＞を表している（認証強度がレベル１、同意確認がレベル０に該当する）。この意味は、あるサービスのサービスポリシーが＜１，０＞の場合に、認証ポリシーとして代わりに＜２，０＞を用いて欲しいという、ユーザポリシーを表している。同様に、図の全ての欄（即ち、対応する全てのサービスポリシー）で、認証ポリシーとしてレベル２の認証強度を指定している。このように、ポリシー間の変換規則としてユーザポリシーを規定している。

【００９４】

この例では、ユーザポリシーが、サービスポリシーよりも厳しい認証ポリシーを要求するものになっている。例えば、クライアント装置１００が、認証法として強度２を持つＰＫを常に利用可能であり、ユーザが強度１以下の認証法で認証されたくない場合に有効である。このようにユーザが要求する理由としては、弱い強度の認証法でサービス提供装置とクライアント装置が合意した場合には、第３者によるなりすましの危険が高まるためである。

【００９５】

図２４Ｂは、ユーザポリシーの別の具体例を示している。例えば、クライアント装置１００が、ポリシー＜１，１＞以下に適合するＰＷを常に利用可能な場合に、このようなポリシーを用いればよい。但し、サービスポリシーが＜０，１＞の場合には、認証法としてＰＷで合意するように認証ポリシーが＜１，１＞に変換されるが、サービスポリシーが＜１，０＞であった場合は、ＰＷよりも利用が容易なＰＫで合意するよう認証ポリシーは＜２，０＞に変換されるようになっている。

【００９６】

ステップＳ９でクライアント装置１００からユーザ情報を受信したサービス提供装置２００は、実施例１（図６）と同様にステップＳ１０およびＳ１１を実行する。図２５は、サービス提供装置２００の認証情報管理部２４０が保持するユーザ情報データベースの構成を示している。各行が一人のユーザと対応している。なお、この形式は、図５で示した実施例１のユーザ情報データベースの形式に、ユーザポリシーが付加されたものである。

【００９７】

ユーザ認証

図２６は、本変形例のユーザ認証システムでの、ユーザ認証の処理フローを示している。まず、クライアント装置１００の入力部１６０は、ユーザＩＤを受け付ける（Ｓ５０）。クライアント装置１００の制御部１２０は、ネットワークインターフェース１１０を介してサービス提供装置２００にサービス要求を送信する（Ｓ５１）。このサービス要求には、Ｓ５０で入力したユーザＩＤが含まれる。

【００９８】

サービス要求を受信すると、サービス提供装置２００は、サービス要求に含まれるユーザＩＤに基づいて、認証情報管理部２４０に保持されたユーザ情報データベースを検索し、該当するユーザのエントリーを特定する。サービス提供装置２００は、さらに、特定したエントリーのユーザポリシーのフィールドを参照し、ユーザポリシーを取得する。同時に、サービス要求に含まれるインデックス情報により要求するサービスを特定し、そのサービスに関連するサービスポリシーを取得する。そして、サービス提供装置２００は、取

得されたサービスポリシーとユーザポリシーにより認証ポリシーを決定する（Ｓ５２）。

【００９９】

例えば、ユーザポリシーが図２４Ｂで示されたものであり、サービスポリシーが＜０，１＞の場合には、図２４Ｂのなかでポリシー＜０，１＞に該当する箇所、即ち３行２列目を参照して認証ポリシー＜１，１＞を得る。また、サービスポリシーが＜１，０＞の場合には、同様に認証ポリシー＜２，０＞を得る。

引き続きサービス提供装置２００からは、決定された認証ポリシーを含む認証要求を、クライアント装置１００へ送信する（Ｓ２２）。ステップＳ２３，Ｓ２４は、実施例１と同じである。

【０１００】

次に、クライアント装置１００は、実施例４と同様に認証法の選択を行う（Ｓ５３）。ステップＳ２２においてサービス提供装置２００から送信された認証要求に確認メッセージが含まれる場合には、クライアント装置１００の出力部１７０は、実施例１と同様に確認メッセージをユーザに対して出力する（Ｓ２６）。そして必要に応じて、入力部１６０は、パスワードを受け付ける（Ｓ５４）。以降の処理は実施例１（図８）と同じである。

登録時にクライアント装置１００からサービス提供装置２００へユーザポリシーを送信することで、ユーザ側からの認証ポリシーの制御が可能となる。これは、例えば、クライアント装置１００が常に認証法ＰＫに適応しており、ユーザが認証法をＰＫ以上にしたい場合などに有効である。そして、低いレベルで認証法が合意することによる安全性の低下を、ユーザ側からの要求により防ぐことができる。

【０１０１】

［実施例５］

実施例５は、実施例１のユーザ認証システムをＷｅｂアプリケーションに適用したものである。具体的には、ＨＴＭＬのＦＯＲＭを用いて実現したものである。図２７は、実施例５のユーザ認証システムのユーザ認証で送信されるメッセージの形式を示している。

【０１０２】

図２７Ａは、図８のステップＳ２０で送信されるサービス要求のメッセージ内容を示している。「／ｆｏｒｍ．ｈｔｍｌ」により、要求するサービス及びステップＳ２２で返信される認証要求のメッセージの形式を指定している。図２７Ｂは、図８のステップＳ２２で送信される認証要求のメッセージ形式を示している。６行目の「＜ａｕｔｈ...＞」が拡張されたタグであり、このタグを受信すると、クライアント装置１００の認証部１３０は、選択した認証法に応じたステップＳ２３～Ｓ２９の処理を実行する。ユーザにより認証ボタンが押されると、認証部１３０は、図２７Ｃに示される認証応答を生成する（Ｓ３１）。そして、クライアント装置は、認証応答をサービス提供装置２００に送信する（Ｓ３２）。認証応答を受信したサービス提供装置２００は、図２７Ｃに示される認証応答の１行目に指定された「ａｕｔｈｅｎｔｉｃａｔｅ．ｃｇｉ」を起動し、ステップＳ３２以降の処理が実行される。

【０１０３】

［実施例５変形例］

図２８は、実施例５変形例のユーザ認証システムにおける認証要求のデータ形式を示している。図２９は、実施例５変形例のユーザ認証システムにおける認証スクリプトの内容を示している。本変形例では、ステップＳ２２でサービス提供装置２００からクライアント装置１００に送信される認証要求メッセージは、図２７Ｂに代わって図２８に示される形式とする。この形式では、認証要求に含まれる情報はＩＮＰＵＴタグにより記述されている。また、ステップＳ２３～Ｓ２９で実行される認証法に応じた認証処理は、図２８の４行目で指定された、クライアント装置１００の認証部１３０に格納された認証スクリプト「ａｕｔｈＳｃｒｉｐｔ．ｊｓ」を実行することでなされる。認証スクリプトの内容は図２９に示されている通りである。

【０１０４】

以上のようにユーザ認証手順を構成すれば、Ｗｅｂアプリケーションに本発明のユーザ

認証システムを適用することができる。なお、拡張タグを用いた例では、クライアント装置１００で認証スクリプトを実行する必要がないため、より安全である。また、認証スクリプトを用いた例は、クライアント装置１００に認証タグなどの機能を追加することなく、容易に実現できる。

【０１０５】

［実施例６］

実施例６では、サービス提供装置２００の認証情報管理部２４０が記録しているユーザ情報の中の公開鍵を更新する手順を説明する。本実施例のユーザ認証システムのシステム構成は、実施例１（図１）と同一である。また、クライアント装置１００およびサービス提供装置２００の構成も、実施例１（図２、図３）と同一である。図３０は、本実施例のユーザ認証システムでの公開鍵更新の処理フローを示している。

【０１０６】

クライアント装置１００の制御部１２０は、ネットワークインターフェース１１０を介してサービス提供装置２００に鍵更新要求を送信する（Ｓ６０）。ステップＳ２～ステップＳ７の処理は、実施例１のユーザ登録の処理（図６）と同じである。ただし、実施例１のユーザ登録では、ユーザＩＤを決定する処理（Ｓ６）が存在した。しかし、本実施例は、ユーザ情報の公開鍵だけを更新する処理なので（ユーザＩＤは既に決まっているので）、ユーザＩＤを決定する処理（Ｓ６）は存在しない。そして公開鍵と秘密鍵の組が新たに生成される（以下、それぞれ公開鍵２、秘密鍵２とする）（Ｓ７）。

【０１０７】

ステップＳ７の後、クライアント装置１００は、ユーザ登録に必要な鍵情報を計算する（Ｓ６１）。鍵情報は、ユーザＩＤ、パスワードまたはパスワード認証情報、公開鍵２、タイムスタンプ、およびこれら３要素を含む署名対象に対して秘密鍵２を用いて計算した署名３、前記の署名対象と署名３からなる情報に対して古い秘密鍵を用いて計算した署名４からなる（図３１）。なお、鍵情報には、公開鍵２の有効期間を含めてもよい。公開鍵の有効期間も登録すれば、有効期限を過ぎた公開鍵を自動的に消去できる。なお、鍵情報からパスワードまたは署名４のいずれかを省略してもよい。クライアント装置１００の制御部１２０は、ネットワークインターフェース１１０を介して、鍵情報をサービス提供装置２００に送信する（Ｓ６２）。

【０１０８】

鍵情報を受信したサービス提供装置２００は、認証部２３０により鍵情報の正当性を検証する（Ｓ６３）。具体的には、認証部２３０は、鍵情報に含まれるユーザＩＤに基づいて、サービス提供装置認証情報管理部２４０のユーザ情報データベースを検索し、該当するユーザのエントリーを特定する。そして、ユーザのエントリーからパスワードを取得して、前記鍵情報に含まれるパスワードもしくはパスワード認証情報と整合するか確認する。また、前記エントリーから公開鍵を取得し、この公開鍵を用いて鍵情報に含まれる署名４を検証する。さらに、鍵情報に含まれる公開鍵２を用いて鍵情報に含まれる署名３を検証し、鍵情報に含まれるタイムスタンプが正しいことを確認する。

【０１０９】

ステップＳ６３の鍵情報の正当性の検証が成功した場合、サービス提供装置２００の認証情報管理部２４０は、前記特定したユーザのエントリーの公開鍵を鍵情報に含まれる公開鍵２に更新する（Ｓ６４）。サービス提供装置２００は、ネットワークインターフェース２１０を介して鍵更新結果として「ＯＫ」を、クライアント装置１００に送信する（Ｓ６５）。なお、鍵情報の正当性の検証（Ｓ６３）が失敗した場合には、サービス提供装置２００は、鍵更新結果として「ＮＧ」をクライアント装置１００に送信する（Ｓ６５）。

鍵更新結果が「ＯＫ」の場合、クライアント装置１００の認証情報管理部１４０は、サービス情報（ステップＳ２で受信したサーバ証明書にユーザＩＤ、公開鍵、秘密鍵を対応付けた情報）の公開鍵を、新たに生成した公開鍵２に更新する（Ｓ６６）。鍵更新結果が「ＮＧ」の場合、クライアント装置１００は、鍵更新手順を終了する。

【０１１０】

このような処理によるので、実施例１のユーザ登録の手順で登録されたユーザ情報の公開鍵を更新できる。上述したように、実施例６では、クライアント装置とサービス提供装置間で相互に認証を行った後、公開鍵を更新する。よって、正規のユーザに成りすまして公開鍵を更新することは困難である。したがって、安全に公開鍵を更新できる。

【０１１１】

［実施例７］

実施例７では、サービス提供装置２００の認証情報管理部２４０が記録しているユーザ情報を抹消する手順を説明する。本実施例のユーザ認証システムのシステム構成は、実施例１（図１）と同一である。また、クライアント装置１００およびサービス提供装置２００の構成も、実施例１（図２、図３）と同一である。図３２は、本実施例のユーザ認証システムでのユーザ登録抹消の処理フローを示している。

【０１１２】

クライアント装置１００の制御部１２０は、ネットワークインターフェース１１０を介してサービス提供装置２００にユーザ登録抹消要求を送信する（Ｓ７０）。ステップＳ２１～ステップＳ３３の処理は、実施例１のユーザ認証の処理（図８）と同じである。

認証法毎の認証応答の検証（Ｓ３３）が成功した場合には、サービス提供装置２００の認証情報管理部２４０は、認証応答に含まれたユーザＩＤ（認証が成功したユーザＩＤ）により特定されるユーザ情報を、ユーザ情報データベースから抹消する（Ｓ７１）。認証および登録抹消が成功した場合には、サービス提供装置２００は、クライアント装置１００に、ユーザ登録抹消結果として「ＯＫ」を送信する（Ｓ７２）。認証または登録抹消が失敗した場合、サービス提供装置２００は、クライアント装置１００に、ユーザ登録抹消結果として「ＮＧ」を送信する（Ｓ７２）。

【０１１３】

ユーザ登録抹消結果が「ＯＫ」の場合、クライアント装置１００の認証情報管理部１４０は、サービス情報をサービス情報データベースから抹消する（Ｓ７３）。ユーザ登録抹消結果が「ＮＧ」の場合、クライアント装置１００は、ユーザ登録抹消の手順を終了する。上述したように、実施例７では、クライアント装置とサービス提供装置間で相互に認証を行った後、ユーザ登録を抹消する。よって、ユーザに成りすましてユーザ登録を抹消することや、サービス提供装置に成りすましてユーザ登録抹消要求を不正に取得することは困難である。したがって、安全にユーザ登録を抹消できる。

【０１１４】

なお、上述の実施例は、いずれもユーザ情報にクライアント装置の秘密鍵で署名を行うことで、自己署名証明書の機能を生じさせるものである。これに加えて、クライアント装置に格納される鍵ペアに対する信頼された第三者機関が発行した証明書を、ユーザ情報とともにサービス提供装置に送信するようにしてもよい。このようにすれば、ユーザ本人からの情報に加えて第三者機関の保証が可能となり、ユーザとサービス提供者の間で係争が生じた場合に、ユーザの特定が可能となる。

なお、以上説明したクライアント装置、サービス提供装置は、その機能を実現するためのプログラムを、コンピュータ読取可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータに読み込ませ、実行するものであってもよい。コンピュータ読取可能な記録媒体とは、フレキシブルディスク、光磁気ディスク、ＣＤ－ＲＯＭ、フラッシュメモリ等の記録媒体、コンピュータシステムに内蔵されるハードディスク装置等の記憶装置を指す。さらに、コンピュータ読取可能な記録媒体は、インターネットを介してプログラムを送信する場合のように、短時間、動的にプログラムを保持するもの（伝送媒体もしくは伝送波）、その場合のサーバとなるコンピュータ内の揮発性メモリのように、一定時間プログラムを保持しているものを含む。

【図１】

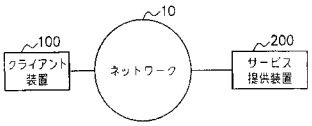


図1

【図２】

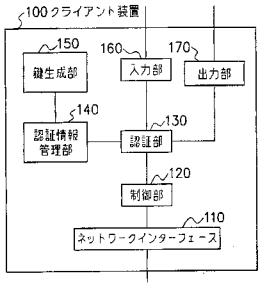


図2

【図３】

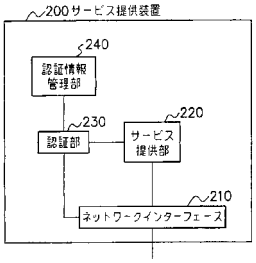


図3

【図４】

サーバ証明書	ユーザＩＤ	公開鍵	秘密鍵
証明書1	1001	48572096872	5353453656
証明書2	2002	63560398634	7767547375
⋮	⋮	⋮	⋮

図4

【図５】

ユーザＩＤ	パスワード	公開鍵	ユーザ属性
1001	abcdef	48572096872	ＩＰアドレス1、住所1、カード番号1
1002	defghi	87039834096	ＩＰアドレス2、住所2、カード番号2
⋮	⋮	⋮	⋮

図5

【図６】

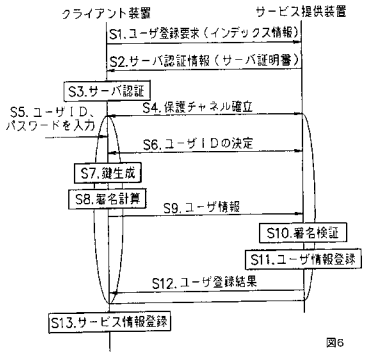


図6

【図７】

ユーザＩＤ	パスワード	公開鍵	ユーザ属性	タイムスタンプ	署名

図7

【図８】

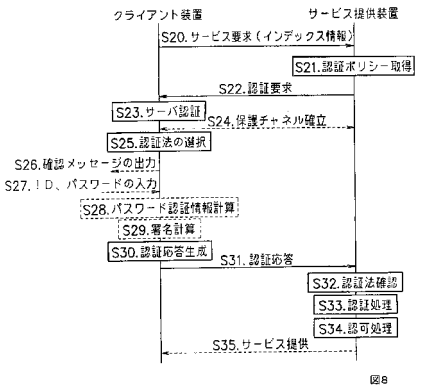


図8

【図９】

認証ポリシー	チャレンジ	確認メッセージ	タイムスタンプ	署名	サーバ証明書

図9

【図１０】

図10A

認証法	ユーザＩＤ	パスワード、または パスワード認証情報

図10B

認証法	ユーザＩＤ	チャレンジ	タイムスタンプ	署名１

図10C

認証法	ユーザＩＤ	チャレンジ	タイムスタンプ	署名２

【図１１】

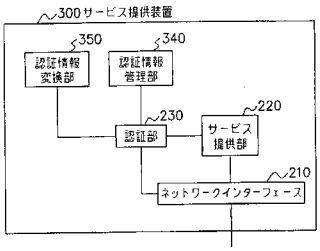


図11

【図１２】

ユーザＩＤ	パスワード	ユーザ属性
1001	abcdef	ＩＰアドレス１、住所１、カード番号１
1002	defghi	ＩＰアドレス２、住所２、カード番号２
⋮	⋮	⋮

図12

【図１３】

ユーザＩＤ	パスワード	公開鍵
1001	abcdef	48572096872
1002	defghi	87039834096
⋮	⋮	⋮

図13

【図１４】

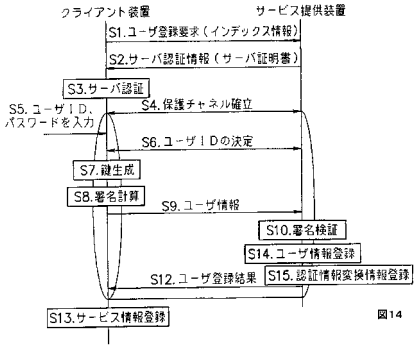


図14

【図１５】

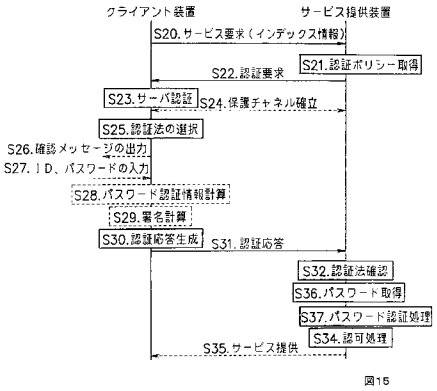


図15

【図１６】

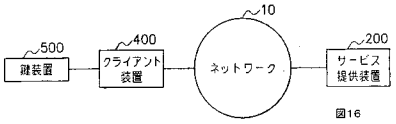


図16

【図１７】

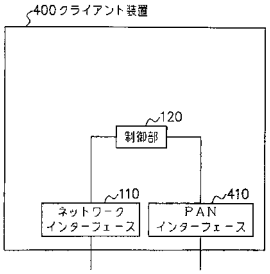


図17

【図１８】

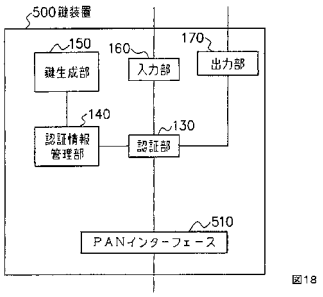


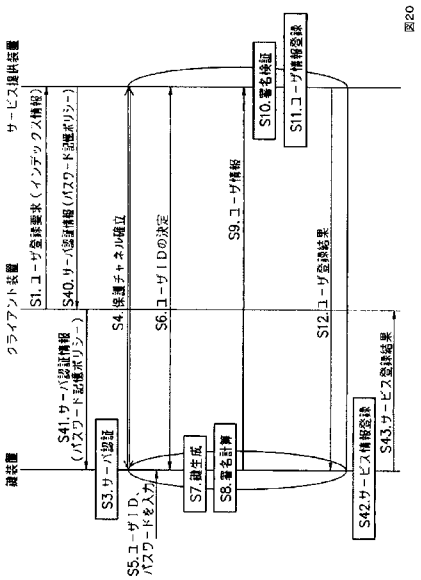
図18

【図１９】

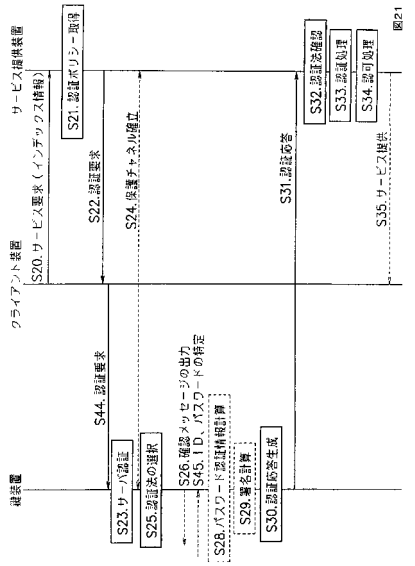
サーバ証明書	ユーザＩＤ	公開鍵	秘密鍵	パスワード
証明書１	1001	48572096872	5353453656	abcdef
証明書２	2002	63560398634	7767547375	–
⋮	⋮	⋮	⋮	⋮

図19

【図２０】



【図２１】



【図２２】

図22A

同意確認 ＼ 強度	0（低）	1（中）	2（高）
0（なし）	NA,PK,OK,PW,PKPW	PK,PW,PKPW	PK,PKPW
1（あり）	OK,PW,PKPW	PW,PKPW	PKPW

図22B

同意確認 ＼ 強度	0（低）	1（中）	2（高）
0（なし）	NA,OK,PW	PW	(PW)
1（あり）	OK,PW	PW	(PW)

【図２３】

ユーザＩＤ	パスワード	公開鍵	ユーザ属性	タイムスタンプ	ユーザポリシー	署名

図23

【図２４】

図24A

同意確認 ＼ 強度	0（低）	1（中）	2（高）
0（なし）	<2,0>	<2,0>	<2,0>
1（あり）	<2,1>	<2,1>	<2,1>

図24B

同意確認 ＼ 強度	0（低）	1（中）	2（高）
0（なし）	<0,0>	<2,0>	<2,0>
1（あり）	<1,1>	<1,1>	<2,1>

【図２５】

ユーザＩＤ	パスワード	公開鍵	ユーザ属性	ユーザポリシー
1001	abcdef	48572096872	ＩＰアドレス１、住所１、カード番号１	ポリシー１
1002	defghi	87039834096	ＩＰアドレス２、住所２、カード番号２	ポリシー２
⋮	⋮	⋮	⋮	⋮

図25

【図２６】

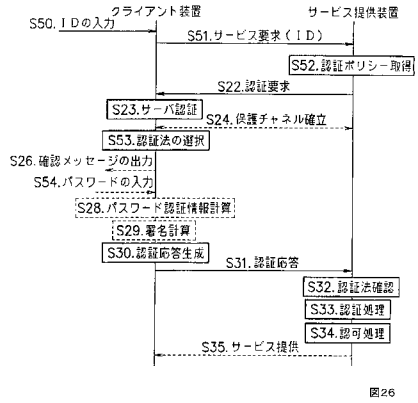


図26

【図２７】

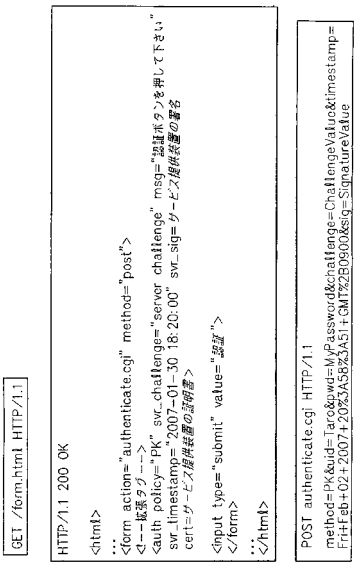


図27A　図27B　図27C

【図２８】

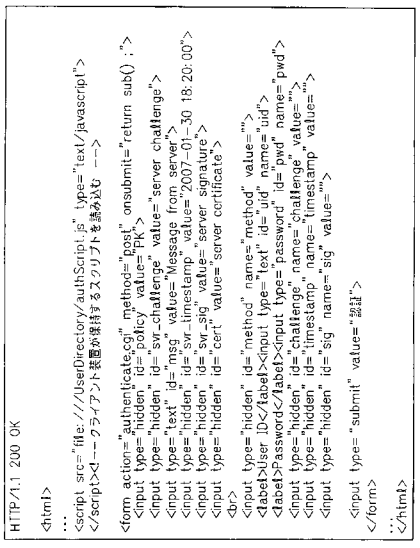


図28

【図２９】

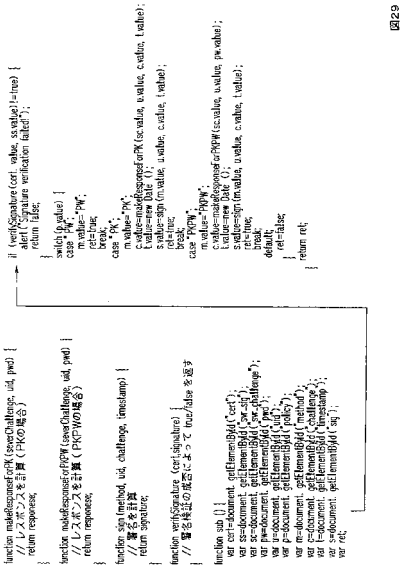


図29

【図３０】

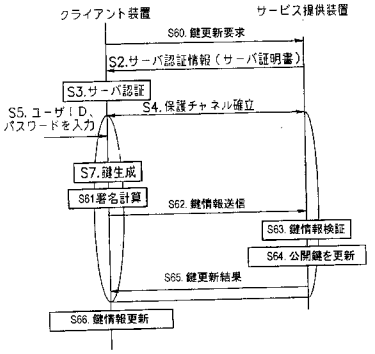


図30

【図３１】

ユーザID	パスワード、または パスワード認証情報	公開鍵2	タイムスタンプ	署名3	署名4

図31

【図３２】

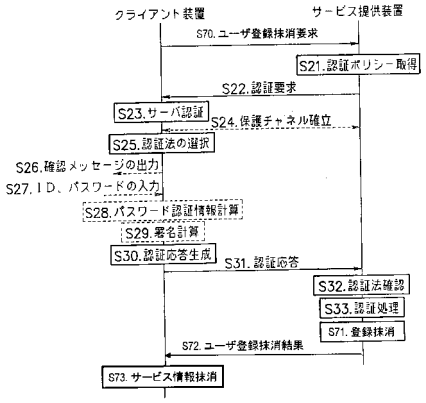


図32

フロントページの続き

(72)発明者　折原　慎吾
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　唐澤　圭
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　高橋　健司
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　児玉　崇晶

(56)参考文献　特開２００４－０２１６８６（ＪＰ，Ａ）
特開２００６－３３１１２０（ＪＰ，Ａ）
特開２００６－２５１８６８（ＪＰ，Ａ）
特開２００４－３３４８６０（ＪＰ，Ａ）
特開２００６－３０２２１０（ＪＰ，Ａ）
特開２００４－３４８３０８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/20
G09C　1/00
H04L　9/32