(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2011-3100
(P2011-3100A)
(43)公開日　平成23年1月6日(2011.1.6)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B017
G06F 21/24	(2006.01)	G06F	12/14	530D	5B285
H04L 9/32	(2006.01)	H04L	9/00	675D	5J104

審査請求 未請求　請求項の数 8　ＯＬ　（全 21 頁）

(21)出願番号　特願2009-147030 (P2009-147030)
(22)出願日　平成21年6月19日 (2009.6.19)

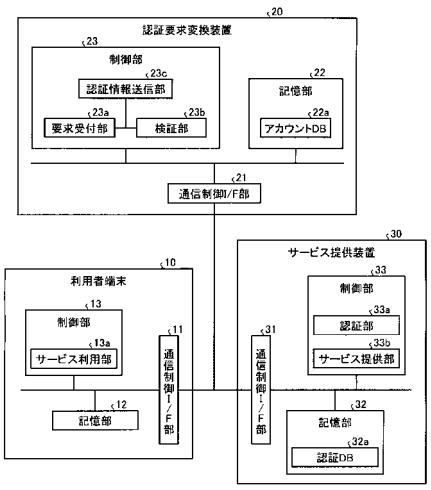
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100089118
弁理士　酒井　宏明
(74)代理人　100114306
弁理士　中辻　史郎
(72)発明者　中嶋　良彰
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　橋本　正一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B017 BA05

最終頁に続く

(54)【発明の名称】認証要求変換装置、認証要求変換方法および認証要求変換プログラム

(57)【要約】
【課題】既存システムに変更を加えることなく、安全なユーザ認証を提供することを課題とする。
【解決手段】認証要求変換装置は、利用者識別情報と検証情報とサービス用認証情報とを対応付けて記憶する識別情報記憶手段を有する。そして、認証要求変換装置は、利用者識別情報を含む認証要求を利用者端末から受信する。続いて、認証要求変換装置は、受信された認証要求に含まれる利用者識別情報に対応付けられた検証情報を識別情報記憶手段から取得し、識別情報記憶手段から取得した検証情報を用いて、認証要求を送信した利用者端末が正当な利用者であるか否を検証する。その後、認証要求変換装置は、利用者端末が正当な利用者であると検証された場合に、認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報を識別情報記憶手段から取得し、認証要求を送信した利用者端末を介して、取得したサービス用認証情報をサービス提供装置に送信する。
【選択図】図２



【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を提供するサービス提供装置と、前記サービスを利用する利用者端末とのそれぞれに接続される認証要求変換装置であって、
前記利用者端末の利用者を特定する利用者識別情報と、前記利用者が正当な利用者であることを検証するための情報を示す検証情報と、前記サービス提供装置が利用者認証に用いる情報を示すサービス用認証情報とを対応付けて記憶する識別情報記憶手段と、
前記サービスを利用するための利用者認証を要求する認証要求であって、前記利用者識別情報と要求者の本人性を表す認証情報を含む認証要求を前記利用者端末から受信する要求受付手段と、
前記要求受付手段によって受信された認証要求に含まれる利用者識別情報に対応付けられた検証情報を前記識別情報記憶手段から取得し、前記識別情報記憶手段から取得した検証情報を用いて、前記認証要求に含まれる認証情報を検証して前記利用者端末が正当な利用者であるか否を検証する検証手段と、
前記検証手段によって前記利用者端末が正当な利用者であると検証された場合に、前記受信された認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報を前記識別情報記憶手段から取得し、前記認証要求を送信した利用者端末を介して、取得したサービス用認証情報を前記サービス提供装置に送信する認証情報送信手段と、
を有することを特徴とする認証要求変換装置。
【請求項２】
前記認証要求は、前記利用者端末が利用を希望するサービスを提供するサービス提供装置を特定するサービス提供装置情報を含むものであって、
前記認証情報送信手段は、前記認証要求に含まれるサービス提供装置情報を用いて、前記認証要求を送信した利用者端末を介することなく、前記取得したサービス用認証情報を前記サービス提供装置に直接送信することを特徴とする請求項１に記載の認証要求変換装置。
【請求項３】
前記識別情報記憶手段に記憶されるサービス用認証情報を、所定の契機で新たに生成して更新するとともに、生成した新たなサービス用認証情報をサービス提供装置に送信する認証情報更新手段をさらに備えたことを特徴とする請求項１または２に記載の認証要求変換装置。
【請求項４】
前記識別情報記憶手段に記憶されるサービス用認証情報を更新するタイミングを記憶する更新ポリシーをさらに有し、
前記認証情報更新手段は、前記更新ポリシーに従って、前記新たなサービス用認証情報を生成して、前記識別情報記憶手段に記憶されるサービス用認証情報を更新するとともに、生成した新たなサービス用認証情報をサービス提供装置に送信することを特徴とする請求項３に記載の認証要求変換装置。
【請求項５】
前記識別情報記憶手段は、前記利用者識別情報と、前記検証情報と、暗号化されたサービス用認証情報とを対応付けて記憶するものであって、
前記要求受付手段は、前記サービスを利用するための利用者認証を要求する認証要求であって、前記利用者識別情報と前記暗号化されたサービス用認証情報を復号する復号鍵を含む認証要求を前記利用者端末から受信し、
前記認証情報送信手段は、前記検証手段によって前記利用者端末が正当な利用者であると検証された場合に、前記受信された認証要求に含まれる利用者識別情報に対応付けて前記識別情報記憶手段に記憶されるサービス用認証情報を、前記受信された認証要求に含まれる復号鍵で復号し、前記認証要求を送信した利用者端末を介して、復号したサービス用認証情報を前記サービス提供装置に送信することを特徴とする請求項１～４のいずれか一つに記載の認証要求変換装置。

【請求項６】
前記認証情報送信手段は、前記受信された認証要求に含まれる利用者識別情報に対応付けて前記識別情報記憶手段に記憶されるサービス用認証情報を、前記サービス提供装置との間で共通に保持する共通鍵を用いて暗号化して、前記サービス提供装置に送信することを特徴とする請求項１～５のいずれか一つに記載の認証要求変換装置。
【請求項７】
前記サービスを利用するための利用者認証を要求する認証要求であって、前記利用者識別情報と要求者の本人性を表す認証情報を含む認証要求を前記利用者端末から受信する要求受付工程と、
前記要求受付工程によって受信された認証要求に含まれる利用者識別情報に対応付けられた検証情報を、ネットワークを介してサービスを利用する利用者端末の利用者を特定する利用者識別情報と、前記利用者が正当な利用者であることを検証するための情報を示す検証情報と、前記サービスを提供するサービス提供装置が利用者認証に用いる情報を示すサービス用認証情報とを対応付けて記憶する識別情報記憶部から取得し、前記識別情報記憶部から取得した検証情報を用いて、前記認証要求に含まれる認証情報を検証して前記利用者端末が正当な利用者であるか否を検証する検証工程と、
前記検証工程によって前記利用者端末が正当な利用者であると検証された場合に、前記受信された認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報を前記識別情報記憶部から取得し、前記認証要求を送信した利用者端末を介して、取得したサービス用認証情報を前記サービス提供装置に送信する認証情報送信工程と、
を含んだことを特徴とする認証要求変換方法。
【請求項８】
前記サービスを利用するための利用者認証を要求する認証要求であって、前記利用者識別情報と要求者の本人性を表す認証情報を含む認証要求を前記利用者端末から受信する要求受付手順と、
前記要求受付手順によって受信された認証要求に含まれる利用者識別情報に対応付けられた検証情報を、ネットワークを介してサービスを利用する利用者端末の利用者を特定する利用者識別情報と、前記利用者が正当な利用者であることを検証するための情報を示す検証情報と、前記サービスを提供するサービス提供装置が利用者認証に用いる情報を示すサービス用認証情報とを対応付けて記憶する識別情報記憶部から取得し、前記識別情報記憶部から取得した検証情報を用いて、前記認証要求に含まれる認証情報を検証して前記利用者端末が正当な利用者であるか否を検証する検証手順と、
前記検証手順によって前記利用者端末が正当な利用者であると検証された場合に、前記受信された認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報を前記識別情報記憶部から取得し、前記認証要求を送信した利用者端末を介して、取得したサービス用認証情報を前記サービス提供装置に送信する認証情報送信手順と、
をコンピュータに実行させることを特徴とする認証要求変換プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証要求変換装置、認証要求変換方法および認証要求変換プログラムに関する。
【背景技術】
【０００２】
従来より、インターネットの普及や高速なネットワーク回線の普及に伴い、インターネットなどのネットワークを介して、多種多様のサービスをユーザに提供するサービス提供システムが増えている。
【０００３】
このようなサービス提供システムは、悪質なユーザの排除や公序良俗の遵守の観点から、不特定多数のユーザに提供するシステム形態よりも、予め登録された特定のユーザに対

してのみサービスを提供するシステム形態の方が多く利用されている。予め登録された特定のユーザに対してサービスを提供するサービス提供システムとしては、業務システムや会員制サービスなどがあるが、いずれのサービスであっても、パスワード認証によるユーザ認証によって、特定のユーザを判別しているのが一般的である。

【先行技術文献】

【非特許文献】

【０００４】

【非特許文献１】“本人認証の現状に関する調査報告書”、［online］、［平成２１年４月２３日検索］、インターネット＜http://www.ipa.go.jp/security/fy14/reports/authentication/index.html＞

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかしながら、上述した従来の技術では、パスワード認証のようなセキュリティリスクを抱えた認証方式が依然として広く利用されているため、提供されるサービス提供セキュリティレベルも低いという課題があった。

【０００６】

具体的には、パスワードはユーザの記憶力に依存する方式であるため、ユーザ間およびサービス提供システム間でセキュリティレベルを一定に保つことが難しい。また、複数のサービス提供システムを利用する場合、全ての同じパスワードを利用すると、パスワードを盗聴された場合のリスクが高く、全て別々のパスワードを利用すると、パスワードとサービス提供システムとの対応付けを管理しておく必要がある。したがって、いずれの場合であっても、ユーザの負担が大きい。

【０００７】

また、パスワード認証よりも安全な認証方式を既存のサービス提供システムに導入する手法も考えられるが、既存のシステムへの導入は、設備変更やシステムの再設計など様々なコストが生じる。そのため、現実的ではなく、導入を実行する企業も少ない。

【０００８】

本発明は、上記に鑑みてなされたものであって、既存システムに変更を加えることなく、安全なユーザ認証を提供することが可能である認証要求変換装置、認証要求変換方法および認証要求変換プログラムを提供することを目的とする。

【課題を解決するための手段】

【０００９】

上述した課題を解決し、目的を達成するために、本発明は、ネットワークを介してサービスを提供するサービス提供装置と、前記サービスを利用する利用者端末とのそれぞれに接続される認証要求変換装置であって、前記利用者端末の利用者を特定する利用者識別情報と、前記利用者が正当な利用者であることを検証するための情報を示す検証情報と、前記サービス提供装置が利用者認証に用いる情報を示すサービス用認証情報とを対応付けて記憶する識別情報記憶手段と、前記サービスを利用するための利用者認証を要求する認証要求であって、前記利用者識別情報を含む認証要求と要求者の本人性を表す認証情報を前記利用者端末から受信する要求受付手段と、前記要求受付手段によって受信された認証要求に含まれる利用者識別情報に対応付けられた検証情報を前記識別情報記憶手段から取得し、前記識別情報記憶手段から取得した検証情報を用いて、前記認証要求を送信した利用者端末が正当な利用者であるか否を検証する検証手段と、前記検証手段によって前記利用者端末が正当な利用者であると検証された場合に、前記受信された認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報を前記識別情報記憶手段から取得し、前記認証要求を送信した利用者端末を介して、取得したサービス用認証情報を前記サービス提供装置に送信する認証情報送信手段と、を有することを特徴とする。

【発明の効果】

【００１０】

本発明にかかる認証要求変換装置は、既存システムに変更を加えることなく、安全なユーザ認証を提供することが可能であるという効果を奏する。

【図面の簡単な説明】

【００１１】

【図１】図１は、認証要求変換装置を含むサービス提供システムの全体構成を示す図である。

【図２】図２は、実施例１に係るサービス提供システムを構成する各装置のブロック図である。

【図３】図３は、アカウントＤＢに記憶される情報の例を示す図である。

【図４】図４は、認証要求変換装置のおける認証処理にＳＳＬクライアント認証を用いる場合の認証要求の例を示す図である。

【図５】図５は、認証ＤＢに記憶される情報の例を示す図である。

【図６】図６は、実施例１に係るサービス提供システムによる処理の流れを示すシーケンス図である。

【図７】図７は、実施例１に係る認証要求変換装置による処理の流れを示すフローチャートである。

【図８】図８は、実施例２に係るサービス提供システムによる処理の流れを示すシーケンス図である。

【図９】図９は、実施例３に係るサービス提供システムによるサービス用認証情報登録処理の流れを示すシーケンス図である。

【図１０】図１０は、実施例３に係るサービス提供システムによる利用者検証処理の流れを示すシーケンス図である。

【図１１】図１１は、認証要求変換装置２０が、利用者端末１０が正当な利用者であると検証し、利用者端末のサービス用認証情報をサービス提供装置３０に送信する際に、サービス用認証情報を暗号化して送信する場合のサービス提供システムによる処理の流れを示すシーケンス図である。

【発明を実施するための形態】

【００１２】

以下に、本発明にかかる認証要求変換装置、認証要求変換方法および認証要求変換プログラムの実施例を図面に基づいて詳細に説明する。なお、この実施例によりこの発明が限定されるものではない。

【実施例１】

【００１３】

［認証要求変換装置を含むシステムの全体構成］

まず、開示する認証要求変換装置を含むサービス提供システムの全体構成について説明する。図１は、認証要求変換装置を含むサービス提供システムの全体構成を示す図である。

【００１４】

図１に示すように、サービス提供システムは、利用者端末と、認証要求変換装置と、サービス提供装置とがインターネットなどのネットワークを介して相互に通信可能に接続される。なお、ここでは、利用者端末やサービス提供装置がそれぞれ１台の場合を図示しているが、あくまで例示であり、これに限定されるものではない。

【００１５】

かかる利用者端末は、ネットワークを介して提供されるサービスを利用するユーザ端末であり、パスワードやＰＫＩ（Public Key Infrastructure）等の認証機能や暗号機能を備えた端末である。このような利用者端末として、例えば、パーソナルコンピュータやワークステーション、家庭用ゲーム機、インターネットＴＶ、ＰＤＡ、携帯電話、ＰＨＳの如き移動体通信端末などがある。

【００１６】

サービス提供装置は、ネットワークを介して利用者端末にサービスを提供するサーバで

あり、例えば、Ｗｅｂサーバ、あるいはＨＴＴＰ（HyperText Transfer Protocol）やその他のプロトコルを利用してサービスを提供するアプリケーションサーバ等である。また、サービス提供装置は、ユーザ認証を行って、許可した利用者端末に対してのみサービスを提供する。

【００１７】

サービス提供装置が実施するユーザ認証には、パスワード認証など様々な認証手法を用いることができる。例えば、サービス提供装置は、パスワード認証を用いる場合、『サービスの利用者を特定する「ＩＤ（ユーザＩＤ）」と「パスワード」』を対応付けた認証ＤＢを有しており、利用者端末から受け付けたＩＤとパスワードを認証ＤＢ内に記憶している場合にのみ、利用者端末にサービスを提供する。他の認証手法を用いたサービス提供装置について、当該認証手法の実施に必要な情報を記憶した認証ＤＢをあらかじめ備えておくことによって同様に実現することができる。

【００１８】

なお、サービス提供装置が提供するサービスとしては、検索エンジン、ショッピング、銀行等の取引、オークション、音楽ダウンロードなど様々なサービスを提供することができ、特に限定されるものでない。

【００１９】

そして、認証要求変換装置は、サービス提供装置と利用者端末とのそれぞれに接続されるサーバであり、当該装置を利用者端末から一意に指定し、接続するために用いる情報（以下、アドレス情報）が割り当てられている。例えば、このようなアドレス情報として、ＵＲＬ（Uniform Resource Locator）、ＩＰアドレス、ホスト名等を用いることができる。

【００２０】

また、認証要求変換装置は、複数のサービス提供装置の認証処理を変換する場合に備え、認証要求変換装置内にてサービス提供装置を一意に識別するサービス（以下、サービス識別情報と等価）とサービス提供装置のアドレス情報（例えば、ＵＲＬ等）の対応関係を管理するＤＢ（以下、サービスアドレス情報ＤＢ）を有しておく。例えば、Ｗｅｂブラウザ等によって実現される利用者端末がサービスＩＤを指定（例えば、ＵＲＬにサービスＩＤを含める等の方法によって指定）した上で認証要求変換装置にアクセス（認証要求を送信）することによって、認証要求変換装置は指定されたサービスＩＤとサービスアドレス情報ＤＢとから接続すべきサービス提供装置のアドレス情報（例えば、ＵＲＬ等）を特定することができる。

【００２１】

認証要求変換装置は、「サービス識別情報、利用者識別情報、検証情報、サービス用認証情報」の情報の組を記憶するアカウントＤＢを有している。当該情報のうち「利用者識別情報」と「検証情報」は利用者認証変換装置が用いる認証方式に依存し、「サービス用認証情報」はサービス提供装置が用いる認証方式に依存する。

【００２２】

例えば、認証要求変換装置が、利用者端末をＳＳＬクライアント認証、すなわちＰＫＩを利用して認証する場合、「利用者識別情報」として「公開鍵証明書」または「公開鍵証明書を一意に識別可能な情報（例えば、発行者とシリアル番号の組、あるいは公開鍵）」の情報をアカウントＤＢに記憶する。また、ＳＳＬクライアント認証を用いる場合、認証要求に含まれる「認証情報」をＳＳＬクライアント認証にて取得した要求者の公開鍵証明書とする方法が考えられるため、この場合、「検証情報」として「公開鍵証明書のハッシュ値（フィンガープリント）」をアカウントＤＢに記憶しておく方法がある。一方、サービス提供装置が用いる認証方式が「パスワード認証」である場合には、「サービス用認証情報」として「ＩＤとパスワード」をアカウントＤＢに記憶しておく方法がある。

【００２３】

上記のようなアカウントＤＢへの情報の登録は、利用者が予め登録する方法が最も基本的な方法であるが、利用者端末から受信した認証要求に含ませておき、認証要求の処理時

に登録処理を合わせて実施する方法を用いても良い。また、例えば、認証要求変換装置は、「利用者識別情報」として「公開鍵証明書」、「サービス用識別情報」として「ＩＤ・パスワード」とを受け付け、「検証情報」である公開鍵証明書のハッシュ値は公開鍵証明書から算出するようにして一部を機械的に生成して登録する方法を用いても良い。なお、公開鍵証明書のハッシュ値（フィンガープリント）としては、ＰＫＩにおける公開鍵証明書としてASN.1オブジェクトである「X.509形式」を用いた場合、公開鍵証明書のフィンガープリントの算出は、一般に、このASN.1オブジェクトのバイナリ表現であるＤＥＲ形式にて表現された公開鍵証明書のデータ全体に対して、Message Digest Algorithm 5やSecure Hash Algorithm等のハッシュ関数を適用することによって算出することができる。

【００２４】

このようなアカウントＤＢを備えた上で、認証要求変換装置は、サービスを利用するための利用者認証を要求する認証要求であって、利用者識別情報を含む認証要求を利用者端末から受信する（図１の（１）参照）。続いて、認証要求変換装置は、受信された認証要求に含まれる利用者識別情報に対応付けられた検証情報をアカウントＤＢから取得し、アカウントＤＢから取得した検証情報を用いて、認証要求に含まれる認証情報を検証することによって、認証要求を送信した利用者端末が正当な利用者であるか否を検証する（図１の（２）参照）。

【００２５】

上記の動作を、認証手法としてＰＫＩ、およびＳＳＬを用いた実装方法を例に説明する。この場合、利用者端末がＳＳＬ対応Ｗｅｂブラウザを用いて認証要求変換装置にアクセスするとＳＳＬクライアント認証が行なわれ、結果として、利用者識別情報および認証情報として利用者の公開鍵証明書を含む認証要求が認証要求変換装置に渡る。続いて、認証要求変換装置は、受信した認証要求から利用者識別情報（この例では公開鍵証明書）を取得し、アカウントＤＢから当該利用者識別情報と一致する情報の検証情報を取得する。また、受信した認証要求から認証情報（この例では公開鍵証明書）を取得し、このハッシュ値を算出してアカウントＤＢから取得した検証情報に含まれるハッシュ値と一致する場合に、認証要求を送信した利用者端末が正当な利用者であると判定し、一致しない場合には不正な利用者であると判定する。

【００２６】

続いて、認証要求変換装置は、利用者端末が正当な利用者であると検証された場合に、受信された認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報をアカウントＤＢから取得し、認証要求を送信した利用者端末を介して（例えば、Ｗｅｂブラウザを介したリダイレクトによる方法を用いて）、サービス提供装置に送信する（図１の（３）参照）。上記の例で説明すると、認証要求変換装置は、利用者端末が正当な利用者であると検証された場合に、受信した公開鍵証明書に対応する「ＩＤ、パスワード」をアカウントＤＢから取得する。そして、認証要求変換装置は、取得した「ＩＤ、パスワード」を、利用者端末（Ｗｅｂブラウザ、等）を介したリダイレクトによってサービス提供装置に送信する。

【００２７】

そして、サービス提供装置は、認証要求変換装置から受信した「ＩＤ、パスワード」が自装置の認証ＤＢに記憶されている場合、当該認証要求を送信した利用者端末に対して、サービスを提供する（図１の（４）と（５）参照）。

【００２８】

このように、開示する認証要求変換装置が利用者端末に対して独自の認証方式（上記の例の場合、ＰＫＩ）を用いた認証処理を既存のサービス提供装置に代わって実行するため、結果として既存のサービス提供装置に改良を加えることなく利用者端末がサービス提供装置を利用する際に行なわれる認証処理の方式を別の方式（例えば、より安全な方式）に変換し、サービス提供システム全体の機能を高度化（例えば、セキュリティ強化による信頼性の向上）することができる。

【００２９】
［サービス提供システムの構成］
次に、図２を用いて、図１に示したサービス提供システムを構成する各装置の構成について説明する。図２は、実施例１に係るサービス提供システムを構成する各装置のブロック図である。
【００３０】
（利用者端末の構成）
まず、利用者端末の構成について説明する。利用者端末１０は、図２に示すように、通信制御Ｉ／Ｆ部１１と、記憶部１２と、制御部１３とを有するが、この機能部は例示であり、マウス、キーボードなどの入力部やディスプレイなどの表示部など他の機能部を有していてもよい。
【００３１】
通信制御Ｉ／Ｆ部１１は、認証要求変換装置２０やサービス提供装置３０との間でやり取りする各種情報に関する通信を制御する。具体的には、通信制御Ｉ／Ｆ部１１は、認証要求変換装置２０に対する認証要求の送信、認証要求変換装置２０からの認証要求結果の受信、サービス提供装置３０に対するサービス利用要求（ユーザ認証要求）の送信を行なうインタフェースである。
【００３２】
記憶部１２は、制御部１３による各種処理に必要なデータおよびプログラムを格納するとともに、例えば、ＳＳＬブラウザで利用する秘密鍵や公開鍵証明書などを記憶する。制御部１３は、ＯＳ（Operating System）などの制御プログラム、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有するとともに、サービス利用部１３ａを有する。
【００３３】
サービス利用部１３ａは、ＳＳＬ対応Ｗｅｂブラウザ等を利用して認証要求変換装置２０のＵＲＬの入力を利用者端末から受け付けると、認証要求変換装置２０に接続する。このようにして、認証要求変換装置２０に接続するサービス利用部１３ａは、サービスを利用するための利用者認証を要求する認証要求であって、利用者端末の利用者を一意に識別する利用者識別情報（例えば、ID、X.509公開鍵証明書、等）および利用者の本人性を表す認証情報（例えば、パスワード、X.509公開鍵証明書、等）を含む認証要求を認証要求変換装置２０に送信する。このとき、認証要求変換装置２０に対して認証要求とあわせてサービスＩＤを送信してもよい。例えば、認証要求変換装置２０のアドレス情報としてＵＲＬを用い、ＵＲＬのパラメタにサービスＩＤを含める方法、等がある。これによって、例えば、ダウンロードサービスの場合にはＩＤ＝０１、ショッピングの場合にはＩＤ＝０２のように、利用者が入力したＵＲＬによって特定されるサービスＩＤが入力された認証要求が認証要求変換装置２０に送信される。
【００３４】
また、認証要求変換装置２０がアカウントＤＢにて記憶するサービス用認証情報の初期登録、あるいは更新のための情報を利用者が利用者端末１０において指定可能とする場合には、サービス利用部１３ａが、認証要求を認証要求変換装置２０に送信する前に、入力画面を用いて利用者からサービス用認証情報の入力を受け付け、受け付けた当該サービス用認証情報を含めた上で認証要求を認証要求変換装置２０に送信する機能を備えても良い。
【００３５】
（認証要求変換装置の構成）
次に、認証要求変換装置の構成について説明する。認証要求変換装置２０は、図２に示すように、通信制御Ｉ／Ｆ部２１と、記憶部２２と、制御部２３とを有するが、この機能部は例示であり、マウス、キーボードなどの入力部やディスプレイなどの表示部など他の機能部を有していてもよい。
【００３６】

通信制御Ｉ／Ｆ部２１は、利用者端末１０やサービス提供装置３０との間でやり取りする各種情報に関する通信を制御する。具体的には、通信制御Ｉ／Ｆ部２１は、認証要求の利用者端末１０からの受信、認証結果の利用者端末１０への送信、サービス用認証情報（ＩＤ・パスワード）のサービス提供装置３０への送信を行なう。

【００３７】

記憶部２２は、制御部２３による各種処理に必要なデータおよびプログラムを格納するとともに、特に、アカウントＤＢ２２ａを有する。また、記憶部２２は、サービス提供装置のＵＲＬ、ＩＰアドレス、等（前述したアドレス情報に相当する情報）の記憶、およびサービス提供装置を特定するサービスＩＤとサービス提供装置のＵＲＬとを対応付ける情報（前述したサービスアドレス情報ＤＢに相当する情報）の記憶等を行なう。

【００３８】

アカウントＤＢ２２ａは、例えば、アカウントＤＢ２２ａは、図３に示すように、「サービス識別情報、利用者識別情報、検証情報、サービス用認証情報」として「サービスＩＤ＝０１、公開鍵証明書、公開鍵証明書のハッシュ値、ＩＤ・パスワード」を記憶する。なお、図３は、アカウントＤＢに記憶される情報の例を示す図である。

【００３９】

制御部２３は、ＯＳ（Operating System）などの制御プログラム、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有し、アカウントＤＢ２２ａの更新を行なう等する制御部であり、特に、要求受付部２３ａと、検証部２３ｂと、認証情報送信部２３ｃとを有する。

【００４０】

要求受付部２３ａは、サービスを利用するための利用者認証を要求する認証要求を利用者端末１０から受信する。要求受付部２３ａは、認証要求を利用者端末１０から受信すると、受信した認証要求を後述する検証部２３ｂに出力する。

【００４１】

例えば、要求受付部２３ａは、図４に示すように、「サービス識別情報、利用者識別情報、認証情報」により構成される認証要求を利用者端末から受信する。図４は、認証要求変換装置のおける認証処理にＳＳＬクライアント認証を用いる場合の認証要求の例を示す図である。

【００４２】

検証部２３ｂは、要求受付部２３ａによって受信された認証要求に含まれる利用者識別情報に対応付けられた検証情報をアカウントＤＢ２２ａから取得し、アカウントＤＢ２２ａから取得した検証情報を用いて、認証要求に含まれる認証情報を検証することによって、認証要求を送信した利用者端末が正当な利用者であるか否を検証し、検証結果（ＯＫまたはＮＧ）を認証情報送信部２３ｃに出力する。なお、この検証処理の具体的な実装方法としては、例えば、前述した方法（ＳＳＬクライアント認証と公開鍵証明書を用いる方法、等）がある。

【００４３】

認証情報送信部２３ｃは、検証部２３ｂによって利用者端末１０が正当な利用者であると検証された場合に、受信された認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報をアカウントＤＢ２２ａから取得し、認証要求を送信した利用者端末１０を介して（例えば、Ｗｅｂブラウザを介したリダイレクトによる方法を用いて）、取得したサービス用認証情報をサービス提供装置３０に送信する。一方、認証情報送信部２３ｃは、検証部２３ｂによって利用者端末１０が不正な利用者であると検証された場合に、認証が不可であり、サービスを利用することができないことを示すサービス利用拒否応答を利用者端末１０に送信する。

【００４４】

なお、制御部２３は、新しいサービス用認証情報を内部にて自動生成し、アカウントＤＢ２２ａにて記憶するサービス用認証情報を更新する機能を有するとともに、認証情報送信部２３ｃによってサービス提供装置３０が有する認証ＤＢ３２ａが記憶するサービス用

認証情報を更新するために、サービス提供装置３０に対してサービス用認証情報の更新要求を送信する処理を行なう機能を有する場合がある。この時、サービス提供装置３０におけるサービス用認証情報の更新機能の実装形態として、更新前のサービス用認証情報を用いた認証によって当該更新要求の正当性を確認する形態が一般的であるため、認証情報送信部２３ｃは当該更新要求の送信にあたって、更新前のサービス用認証情報をあわせて送信してサービス提供装置における当該認証処理に対応する機能も有する。また、当該更新要求を受信したサービス提供装置３０は、自身が有する認証ＤＢ３２ａを更新し、更新が終了したことを認証要求変換装置２０に送信する。

【００４５】

認証要求変換装置２０がアカウントＤＢ２２ａにて記憶するサービス用認証情報の初期登録、あるいは更新のための情報を利用者が利用者端末１０から指定可能とする場合、要求受付部２３ａが受信した認証要求はサービス用認証情報を含んでいる場合がある。この場合、認証要求変換装置２０は、当該認証要求に含まれるサービス用認証情報を用いて、上記の自動生成の場合と同様の方法によって、アカウントＤＢ２２ａ、および認証ＤＢ３２ａが記憶するサービス用認証情報を更新する機能を有する。

【００４６】

（サービス提供装置の構成）

次に、サービス提供装置の構成について説明する。サービス提供装置３０は、図２に示すように、通信制御Ｉ／Ｆ部３１と、記憶部３２と、制御部３３とを有するが、この機能部は例示であり、マウス、キーボードなどの入力部やディスプレイなどの表示部など他の機能部を有していてもよい。

【００４７】

通信制御Ｉ／Ｆ部３１は、利用者端末１０や認証要求変換装置２０との間でやり取りする各種情報に関する通信を制御する。具体的には、通信制御Ｉ／Ｆ部３１は、利用者端末１０のサービス用認証情報（例えば、ＩＤ、パスワードなど）を含む認証要求を認証要求変換装置２０から受信したり、利用者端末１０に対してサービスを提供したりする。

【００４８】

記憶部３２は、制御部２３による各種処理に必要なデータおよびプログラムを格納するとともに、特に、認証ＤＢ３２ａを有する。例えば、記憶部３２は、サービスＩＤとサービス内容とを対応付けて記憶する。

【００４９】

認証ＤＢ３２ａは、サービスの利用を要求する利用者端末が正当な利用者であるか否かを認証するための情報を記憶する。例えば、認証ＤＢ３２ａは、図５に示すように、利用者端末が正当な利用者であるか否かを認証するための情報を示す「サービス用認証情報」として「ＩＤ・パスワード」を記憶している。図５は、認証ＤＢに記憶される情報の例を示す図である。

【００５０】

制御部３３は、ＯＳ（Operating System）などの制御プログラム、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有するとともに、認証部３３ａと、サービス提供部３３ｂとを有する。

【００５１】

認証部３３ａは、サービスの利用を要求する利用者端末が正当な利用者であるか否かを認証するユーザ認証を実施する。例えば、認証部３３ａは、認証要求変換装置２０から受信したサービス用認証情報（例えば、「ＩＤ・パスワード」）が認証ＤＢ３２ａに記憶されている場合には、認証許可をサービス提供部３３ｂに出力する。一方、認証部３３ａは、認証要求変換装置２０から受信したサービス用認証情報（例えば、「ＩＤ・パスワード」）が認証ＤＢ３２ａに記憶されていない場合には、認証拒否をサービス提供部３３ｂに出力する。

【００５２】

サービス提供部３３ｂは、認証部３３ａによって認証が許可された利用者端末に対して

サービスを提供する。具体的には、サービス提供部３３ｂは、認証部３３ａから認証許可が通知された場合には、認証要求を受信したＷｅｂブラウザを介してサービスを利用者端末１０に提供する。また、サービス提供部３３ｂは、認証部３３ａから認証拒否が通知された場合には、要求元に対してサービスの利用を拒否する。

【００５３】

［サービス提供システムによる処理］

次に、図６を用いて、実施例１に係るサービス提供システムによる処理の流れを説明する。図６は、実施例１に係るサービス提供システムによる処理の流れを示すシーケンス図である。なお、ここで説明するシーケンス図では、認証要求変換装置２０は、図３に示すような情報を記憶したアカウントＤＢ２２ａを備えているものとして説明する。

【００５４】

このような状態において、図６に示すように、利用者の指示操作によって、利用者端末１０のサービス利用部１３ａとして、例えばＳＳＬ対応Ｗｅｂブラウザ等を起動する（ステップＳ１０１）。続いて、利用者端末１０のサービス利用部１３ａは、利用者によって入力されたアドレス情報（ＵＲＬ等）によって認証要求変換装置２０にアクセスすることで、認証要求変換装置２０に対して認証要求を送信する（ステップＳ１０２）。このとき、例えば、アドレス情報（ＵＲＬのパラメタ等）にサービスを特定するサービスＩＤが含めておくことによって、認証要求とともにサービスＩＤを認証要求変換装置２０に送信することが可能である。

【００５５】

すると、認証要求変換装置２０の要求受付部２３ａは、利用者端末１０から送信された認証要求を受信する（ステップＳ１０３）。続いて、検証部２３ｂは、受信した認証要求から「サービスＩＤ」と「利用者識別情報」を取得し、取得した「サービスＩＤ」と「利用者識別情報」に対応するアカウント情報をアカウントＤＢ２２ａから特定する（ステップＳ１０４）。

【００５６】

そして、検証部２３ｂは、特定したアカウント情報の「検証情報」を用いて、利用者認証を実施する（ステップＳ１０５）。例えば、検証部２３ｂは、認証要求から「認証情報」として取得した「公開鍵証明書」のハッシュ値を算出し、算出したハッシュ値と、アカウントＤＢ２２ａから特定した「公開鍵証明書のハッシュ値」とが一致する場合に認証許可（検証ＯＫ）と判定し、一致しない場合に認証拒否（検証ＮＧ）と判定する。

【００５７】

ここで、検証部２３ｂによって認証許可（検証ＯＫ）と判定され（ステップＳ１０６肯定）、かつ認証要求がサービス用認証情報を含む場合には、制御部２３は、アカウントＤＢ２２ａにおいて特定したアカウント情報のサービス用認証情報を、認証要求に含まれるサービス用認証情報にて更新（ステップＳ１０７）し、認証情報送信部２３ｃは、サービス用認証情報の更新要求をサービス提供装置３０に送信することによってサービス提供装置３０側のサービス用認証情報を更新して（ステップＳ１０８）、ステップＳ１１１に進む。この時、サービス提供装置３０は、受信したサービス用認証情報で認証ＤＢ３２ａを更新し（ステップＳ１０９）、更新が終了したことを認証要求変換装置２０に送信する（ステップＳ１１０）ものとする。なお、検証部２３ｂによって認証許可（検証ＯＫ）と判定（ステップＳ１０６肯定）されていても、認証要求がサービス用認証情報を含まない場合には、ステップＳ１０７～ステップＳ１１０の処理を省略して、ステップＳ１１１に進む。

【００５８】

ステップＳ１１１～ステップＳ１１２では、認証情報送信部２３ｃは、受信された認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報をアカウントＤＢ２２ａから取得し、認証要求を送信した利用者端末１０が認証要求を送信した利用者端末１０を介して、取得したサービス用認証情報をサービス提供装置３０に送信する。

【００５９】

このようにして、認証要求変換装置２０から利用者端末１０を介して受信したサービス提供装置３０は、受信したサービス用認証情報と一致するサービス用認証情報を認証ＤＢ３２ａに記憶しているか否かによって、ユーザ認証を実施する（ステップＳ１１３とステップＳ１１４）。そして、サービス提供装置３０は、一致するサービス用認証情報を記憶している場合に認証許可と判定し（ステップＳ１０５肯定）、認証を許可した利用者端末１０に対してサービスを提供する（ステップＳ１１６とステップＳ１１７）。

【００６０】

一方、ステップＳ１０６において、検証部２３ｂによって、認証拒否（検証ＮＧ）と判定された場合（ステップＳ１０６否定）、認証要求変換装置２０の認証情報送信部２３ｃは、サービス利用拒否を利用者端末１０に応答する（ステップＳ１１８）。また、ステップＳ１１５において、サービス提供装置３０は、一致するサービス用認証情報を記憶していない場合に認証拒否と判定し（ステップＳ１１５否定）、サービス利用拒否を利用者端末１０に応答する（ステップＳ１１９）。

【００６１】

［認証要求変換装置による処理］

次に、図７を用いて、実施例１に係る認証要求変換装置２０による処理の流れを説明する。図７は、実施例１に係る認証要求変換装置による処理の流れを示すフローチャートである。なお、ここで説明するシーケンス図では、認証要求変換装置２０は、図３に示すような情報を記憶したアカウントＤＢ２２ａを備えているものとして説明する。

【００６２】

図７に示すように、認証要求変換装置２０の要求受付部２３ａは、利用者端末１０から送信された認証要求を受信すると（ステップＳ２０１肯定）、検証部２３ｂが、受信された認証要求から利用者識別情報（例えば、公開鍵証明書など）を取得し（ステップＳ２０２）、取得した利用者識別情報に対応するアカウント情報をアカウントＤＢ２２ａから特定する（ステップＳ２０３）。

【００６３】

続いて、検証部２３ｂは、特定したアカウント情報に含まれる検証情報を用いて、認証要求を送信した利用者端末１０が正当な利用者であるか否を検証する（ステップＳ２０４）。

【００６４】

ここで、検証部２３ｂによって認証許可（検証ＯＫ）と判定され（ステップＳ２０５肯定）かつ認証要求がサービス用認証情報を含む場合には、制御部２３は、認証要求に含まれるサービス用認証情報によるアカウントＤＢ２２ａの更新、および認証情報送信部２３ｃによるサービス提供装置３０のサービス用認証情報の更新依頼の送信を行ない（ステップＳ２０６）、ステップＳ２０７に進む。

【００６５】

ステップＳ２０７では、更新が終了したことをサービス提供装置３０から通知された認証要求変換装置２０の認証情報送信部２３ｃが、認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報をアカウントＤＢ２２ａから取得し、認証要求を送信した利用者端末１０を介してサービス提供装置３０に送信する。

【００６６】

一方、ステップＳ１０６にて、検証部２３ｂによって認証拒否（検証ＮＧ）と判定された場合、認証情報送信部２３ｃはサービス利用拒否を利用者端末１０に応答する（ステップＳ２０８）。

【００６７】

［実施例１による効果］

このように、実施例１によれば、既存のシステム（サービス提供装置）に改良を加えることなく、他の認証方式（例えば、サービス提供装置が用いている認証方式よりも安全な認証方式）によって利用者端末を認証することができる。このようにして、より安全な認証方式に容易に切り替えることができれば、サービス提供システム全体の信頼性も容易に

向上させることができる。

【００６８】

さらに、実施例１によれば認証要求変換装置２０を用いたサービス提供システムにおいては、認証処理に関わる処理のみが認証要求変換装置２０を介して行なわれ、認証後のサービス利用中においては利用者端末１０とサービス提供装置３０とが直接通信を行なう形態となり認証要求変換装置２０を介する必要がないため、システム全体として効率的な通信処理が可能となる。

【００６９】

また、サービス用認証情報の初期登録および更新にあたっては、認証要求変換装置２０に送信する認証要求にサービス用認証情報を含めて送信するだけで、認証要求変換装置２０がサービス用認証情報を登録または更新することが可能であるため、サービス用認証情報のオンライン登録、およびオンライン更新による最新化が可能となり、運用効率の良いシステムを構成可能となる。例えば、認証要求変換装置２０は、利用者端末１０から初めてアクセスを受け付けた際に、認証要求送信ボタンとサービス用認証情報入力領域とを含めた画面を利用者端末１０に表示する。利用者は、登録したいサービス用認証情報を入力して認証要求送信ボタンを押下することによって、認証要求変換装置２０にサービス用認証情報を登録することができる。また、サービス用認証情報の更新に関しても、同様に更新用画面を認証要求変換装置が利用者端末１０に表示することによってユーザに更新を促すことができ、サービス提供装置３０の種類に依らず、統一的なサービス用認証情報の更新手順を実現することが可能となる。

【００７０】

また、実施例１によれば、更新のためのサービス用認証情報として利用者が入力した情報を必ずしも用いる必要はなく、利用者端末１０の内部にて自動的に生成したサービス用認証情報を認証要求に含めて認証要求変換装置２０に送信しても良い。また、認証要求変換装置２０の内部で自動的に生成したサービス用認証情報を用いて、サービス用認証情報を更新しても良い。その結果、いずれの方法においても、利用者の手を介さないことによる利用者の手間の軽減と、利用者からサービス用認証情報を伏せることによる安全性の向上の利点を得ることができる。

【実施例２】

【００７１】

ところで、実施例１では、認証要求変換装置２０は、利用者端末１０を介したリダイレクトで、サービス用認証情報をサービス提供装置３０に送信したが、これに限定されるものではなく、認証要求変換装置２０は、利用者端末１０を介することなく、サービス用認証情報をサービス提供装置３０に直接送信することもできる。

【００７２】

そこで、実施例２では、図８を用いて、認証要求変換装置２０は、利用者端末１０を介することなく、サービス用認証情報をサービス提供装置３０に直接送信する例について説明する。図８は、実施例２に係るサービス提供システムによる処理の流れを示すシーケンス図である。なお、ここで説明するシーケンス図では、認証要求変換装置２０は、図３に示すような情報を記憶したアカウントＤＢ２２ａを備えているものとして説明する。また、以下、ステップＳ３０１～ステップＳ３１０は、実施例１におけるステップＳ１０１～ステップＳ１１１と共通したシーケンスであるため説明を省略し、ステップＳ３１２以降から説明をはじめる。

【００７３】

実施例のステップＳ１１１～ステップＳ１１２においては、認証情報送信部２３ｃは、受信された認証要求に含まれる利用者識別情報に対応付けられたサービス用認証情報をアカウントＤＢ２２ａから取得し、認証要求を送信した利用者端末１０が認証要求を送信した利用者端末１０を介して、取得したサービス用認証情報をサービス提供装置３０に送信した。一方、実施例２においては、ステップＳ３１１～ステップＳ３１２においてサービス用認証情報をサービス提供装置３０に直接送信する。

【００７４】
認証要求変換装置２０からサービス用認証情報を直接受信したサービス提供装置３０は、受信したサービス用認証情報と一致するサービス用認証情報を認証ＤＢ３２ａに記憶しているか否かによって、ユーザ認証を実施する（ステップＳ３１３とステップＳ３１４）。そして、サービス提供装置３０は、一致するサービス用認証情報を記憶している場合に認証許可と判定し（ステップＳ３１５肯定）、認証を許可した利用者端末に対してサービスを提供する（ステップＳ３１６とステップＳ３１７）。
【００７５】
一方、ステップＳ３０６において、検証部２３ｂによって、認証拒否（検証ＮＧ）と判定された場合（ステップＳ３０６否定）、認証要求変換装置２０の認証情報送信部２３ｃは、サービス利用拒否を利用者端末１０に応答する（ステップＳ３１８）。また、ステップＳ３１５において、サービス提供装置３０は、一致するサービス用認証情報を記憶していない場合に認証拒否と判定し（ステップＳ３１５否定）、サービス利用拒否を利用者端末１０に応答する（ステップＳ３１９）。
【００７６】
このように、実施例２によれば、既存のサービス提供装置３０が認証に用いるサービス用認証情報が利用者端末１０に対して開示されることがないため、利用者端末１０および利用者端末１０との通信経路上でのサービス用認証情報の漏洩のリスクを回避することができる。
【実施例３】
【００７７】
ところで、開示する認証要求変換装置２０は、サービス用認証情報を暗号化して記憶しておくこともできる。そこで、実施例３では、図９と図１０とを用いて、サービス用認証情報を暗号化して記憶させる場合について説明する。ここでは、サービス用認証情報の登録処理と認証処理とのそれぞれについて説明する。なお、サービス用認証情報の登録処理は、例えば、ＳＳＬクライアント認証処理の過程において実行される。
【００７８】
（登録処理）
図９は、実施例３に係るサービス提供システムによるサービス用認証情報登録処理の流れを示すシーケンス図である。図９において、ステップＳ４０１とステップＳ４０２は利用者端末１０が認証要求変換装置２０にアクセスし、サービス用認証情報の初期登録を行なう処理に相当する。アクセスを受けた認証要求変換装置２０は、利用者端末１０に対応した暗号鍵・復号鍵を生成する（ステップＳ４０３）。なお、このシーケンスは１つの実装例であり暗号鍵・復号鍵の生成契機を限定するものではなく、ステップＳ４０８までの間であればどの時点で暗号鍵・復号鍵を生成しても良い。
【００７９】
そして、認証要求変換装置２０は、サービス用認証情報の入力を受け付ける画面を利用者端末１０に表示し（ステップＳ４０４とステップＳ４０５）、サービス用認証情報の入力を受け付けると（ステップＳ４０６とステップＳ４０７）、受信したサービス用認証情報をステップＳ４０３にて生成した暗号鍵により暗号化し、利用者識別情報と検証情報と対応付けてアカウントＤＢ２２ａに格納する（ステップＳ４０８）。
【００８０】
その後、認証要求変換装置２０は、ステップＳ４０３にて生成した復号鍵に相当する情報を含む情報であり、利用者端末がアクセス時に用いる情報として、例えば復号鍵に相当する情報を含むアドレス情報（復号鍵に相当する情報を含むＵＲＬ等）を生成して利用者端末１０に送信し（ステップＳ４０９）、利用者端末１０は、ユーザの操作によって、受信した当該情報を利用者端末１０の内部に登録する（ステップＳ４１０とステップＳ４１１）。なお、復号鍵は、ステップＳ４１１の実施後、認証要求変換装置２０内部から即時または経過時間等の一定の条件が成立後に削除するようにしても良い。このようにすることによって、復号鍵を利用者に通知後は、認証要求変換処理時以外に、認証要求変換装置

内に復号鍵が存在しない状態を実現することが可能となり、復号鍵の漏洩の可能性を低減し、安全性を高めることができる。

【００８１】

（認証処理）

図１０は、実施例３に係るサービス提供システムによる利用者検証処理の流れを示すシーケンス図である。図１０に示すように、利用者端末１０は、利用者の指示操作によって、利用者端末１０（Ｗｅｂブラウザ等）の動作を開始する（ステップＳ５０１）。続いて、利用者端末１０において、復号鍵に相当する情報を含むアドレス情報（ＵＲＬ等）を利用者が選択（ステップＳ５０２）することによって、復号鍵に相当する情報を含む認証要求が認証要求変換装置２０に対して送信される（ステップＳ５０３）。

【００８２】

すると、認証要求変換装置２０の要求受付部２３ａは、利用者端末１０から送信された認証要求を受信する（ステップＳ５０４）。続いて、検証部２３ｂは、受信した認証要求から「利用者識別情報」と「サービスＩＤ」を取得し、取得した「利用者識別情報」と「サービスＩＤ」に対応するアカウント情報をアカウントＤＢ２２ａから特定する（ステップＳ５０５）。そして、検証部２３ｂは、特定したアカウント情報に含まれる「検証情報」を用いて、利用者認証を実施する（ステップＳ５０６）。

【００８３】

なお、上記のステップＳ５０４～ステップＳ５０６の処理は、実施例１の同様のステップと共通する部分であるため、より詳しくは実施１を参照されたい。

【００８４】

検証部２３ｂによって認証許可（検証ＯＫ）と判定されると（ステップＳ５０７肯定）、認証情報送信部２３ｃは、利用者端末１０から認証要求（ＵＲＬパラメタ等）に含まれる復号鍵に相当する情報を取得し、認証要求に含まれる「利用者識別情報」に対応付けられたアカウントＤＢ２２ａに格納されているサービス用認証情報（暗号化済みのサービス用認証情報）を取得し、これを復号してサービス用認証情報（暗号化前のサービス用認証情報）を取得する（ステップＳ５０８）。

【００８５】

なお、ステップＳ５０９以降のシーケンスについては、実施例１におけるステップＳ１０７以降と同様である。

【００８６】

なお、ステップＳ５０９～ステップＳ５１２の処理は、認証要求にサービス用認証情報が付加されている場合に実行される処理であり、必ずしも行う必要はない。

【００８７】

このように、実施例３によれば、既存のサービス提供装置で用いるサービス用認証情報を、認証要求変換装置２０内にアカウント情報として登録する際に、ユーザ本人以外に対して秘密にすることができ、認証要求変換装置２０に対する盗難等によるセキュリティ侵害のリスクを低減することができる。

【実施例４】

【００８８】

ところで、認証要求変換装置２０は、利用者端末１０が正当な利用者であると検証し、利用者端末のサービス用認証情報をサービス提供装置３０に送信するのに際して、暗号化して送信することもできる。

【００８９】

図１１は、認証要求変換装置２０が、利用者端末１０が正当な利用者であると検証し、利用者端末のサービス用認証情報をサービス提供装置３０に送信する際に、サービス用認証情報を暗号化して送信する場合のサービス提供システムによる処理の流れを示すシーケンス図である。実施例１との差分は、ステップＳ６１２とステップ６１３において、認証要求変換装置２０は、サービス提供装置３０との間であらかじめ共有された暗号鍵を用いてサービス用認証情報を暗号化した上で、当該サービス用認証情報をサービス提供装置３

０に送信する点である。また、ステップＳ６１４とステップＳ６１５において、サービス提供装置３０は、上記のようにして暗号化された状態のサービス用認証情報をあらかじめ認証要求変換装置２０との間で共有された復号鍵を用いて復号してサービス用認証情報を取得する点も実施例１との差分となる点である。他のシーケンスについては、実施例１と同様である。なお、認証要求変換装置２０からサービス提供装置３０に対して暗号化済みのサービス用認証情報の送信する際には、実施例２のようにサービス用提供装置３０に対して直接送信する方法でも良い。

【００９０】

このように、実施例４によれば、認証要求変換装置２０は、サービス提供装置３０との間で共通に保持する暗号鍵で暗号化したサービス用認証情報をサービス提供装置３０に送信することができる。その結果、サービス用認証情報が盗聴されて悪用されることを防止することができ、システム全体の信頼性を向上させることができる。特に、実施例２の方式において上記方式を提供することによって、利用者端末２０におけるサービス用認証情報の漏洩のリスクを低減することができる。

【実施例５】

【００９１】

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。そこで、以下に異なる実施例を説明する。

【００９２】

（更新ポリシー）

上述した実施例では、認証要求変換装置２０は、受信した認証要求にサービス用認証情報（ＩＤ・パスワード）が含まれている場合に、アカウントＤＢ２２ａの更新およびサービス提供装置３０への更新依頼を行う例について説明したがこれに限定されるものではない。

【００９３】

具体的には、任意の更新契機が設定可能な更新ポリシーを保持しておき、当該更新ポリシーに従って、アカウントＤＢ２２ａの更新およびサービス提供装置３０への更新依頼を行うようにしてもよい。例えば、認証要求変換装置２０は、「サービス用認証情報の更新は不要」や「前回更新日時からｎ日（例えば、３０日）以上経過した場合に更新」などを更新ポリシーとして保持しておき、認証要求を受信したか否かに関わらず、この更新ポリシーに記憶される契機に到達した場合に、アカウントＤＢ２２ａの更新およびサービス提供装置３０への更新依頼を行うようにしてもよい。また、更新される新たなサービス用認証情報（ＩＤ・パスワード）は、認証要求変換装置内で作成してもよく、利用者端末から受け付けてもよい。

【００９４】

（検証手法）

また、上述した実施例では、認証要求変換装置における認証処理をＳＳＬクライアント認証により実現する方法を中心に述べたが認証方式はこれに限定されるものではなく、様々な方式を用いることができる。表（１）に示すように、「利用者識別情報」として「利用者を一意に割り振った「利用者ＩＤ」」を用いる方法でも良い。また、認証方式として、利用者端末の「ＩＰアドレス」を条件として認証を行なう端末認証、利用者端末が用いる通信回線の回線IDを条件として認証を行なう回線認証、利用者端末に接続された「トークン」の正当性（ＩＣカード）をワンタイムパスワードやトークン内部の秘密鍵によって検証するトークン認証など、多様な認証方式を用いることができる。

【００９５】

【表１】

(表1)

認証方式	利用者識別情報	検証情報
SSL認証	公開鍵証明書	証明書を検証するためのフィンガープリント
Password認証	利用者ID	Passwordを照合するための情報 (パスワードそのものや、パスワードのハッシュ値、等)
端末認証	利用者ID	端末のIPアドレス等
回線認証	利用者ID	アクセス回線の回線ID等
トークン認証	利用者ID	トークンが生成するレスポンスの検証情報

【００９６】

（システム）

また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明した処理（例えば、音声認識処理など）の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情については、特記する場合を除いて任意に変更することができる。

【００９７】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、各装置にて行なわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

【００９８】

（プログラム）

なお、本実施例で説明した認証要求変換方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することができる。

【産業上の利用可能性】

【００９９】

以上のように、本発明にかかる認証要求変換装置、認証要求変換方法および認証要求変換プログラムは、ネットワークを介してサービスを提供するサービス提供装置と、前記サービスを利用する利用者端末とのそれぞれに接続される装置に有用であり、特に、既存システムに変更を加えることなく、安全なユーザ認証を提供することに適している。

【符号の説明】

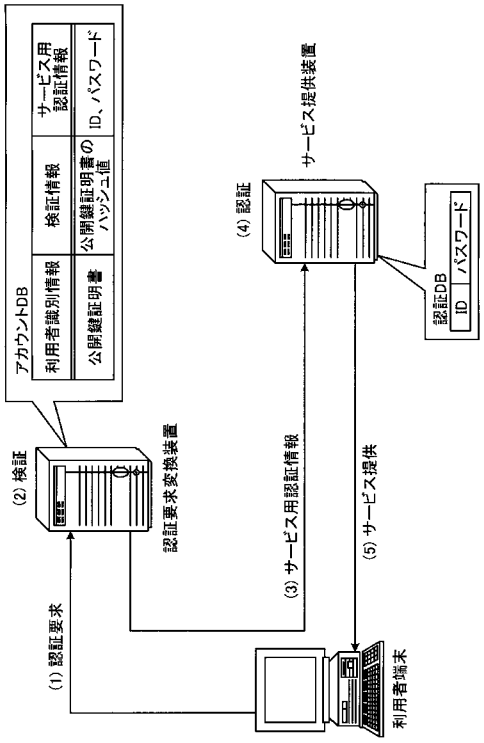
【０１００】

１０　利用者端末

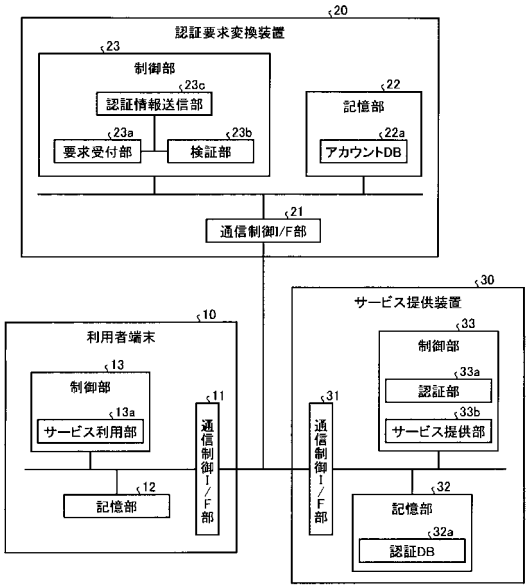
１１　通信制御Ｉ／Ｆ部

１２　記憶部
１３　制御部
１３ａ　サービス利用部
２０　認証要求変換装置
２１　通信制御Ｉ／Ｆ部
２２　記憶部
２２ａ　アカウントＤＢ
２３　制御部
２３ａ　要求受付部
２３ｂ　検証部
２３ｃ　認証情報送信部
３０　サービス提供装置
３１　通信制御Ｉ／Ｆ部
３２　記憶部
３２ａ　認証ＤＢ
３３　制御部
３３ａ　認証部
３３ｂ　サービス提供部

【図１】



【図２】



【図３】

サービス識別情報	利用者識別情報	検証情報	サービス用認証情報
サービスID=01	公開鍵証明書	公開鍵証明書のハッシュ値	ID、パスワード

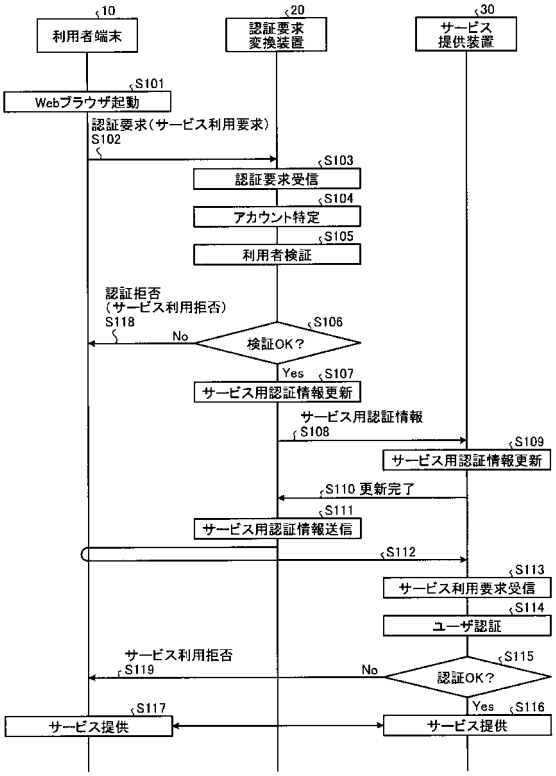
【図４】

サービス識別情報	利用者識別情報	認証情報
サービスID=01	公開鍵証明書	公開鍵証明書

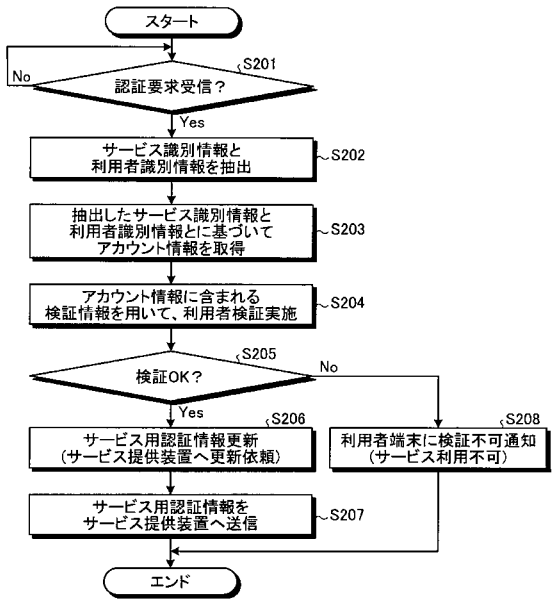
【図５】

サービス用認証情報
ID、パスワード

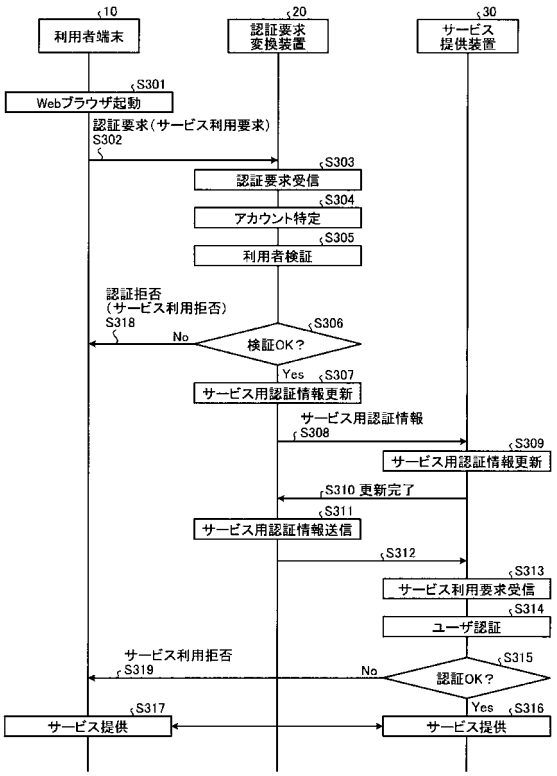
【図６】



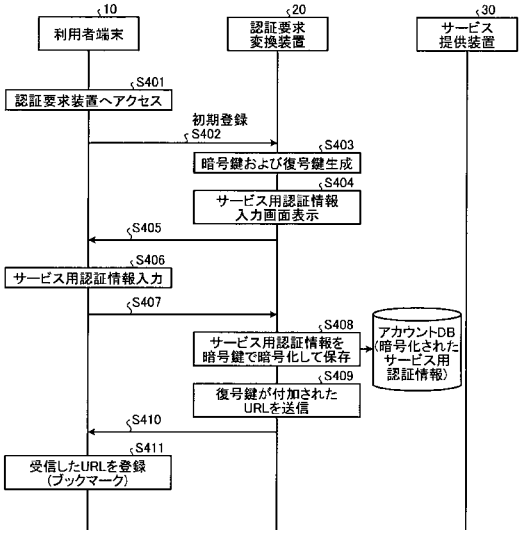
【図７】



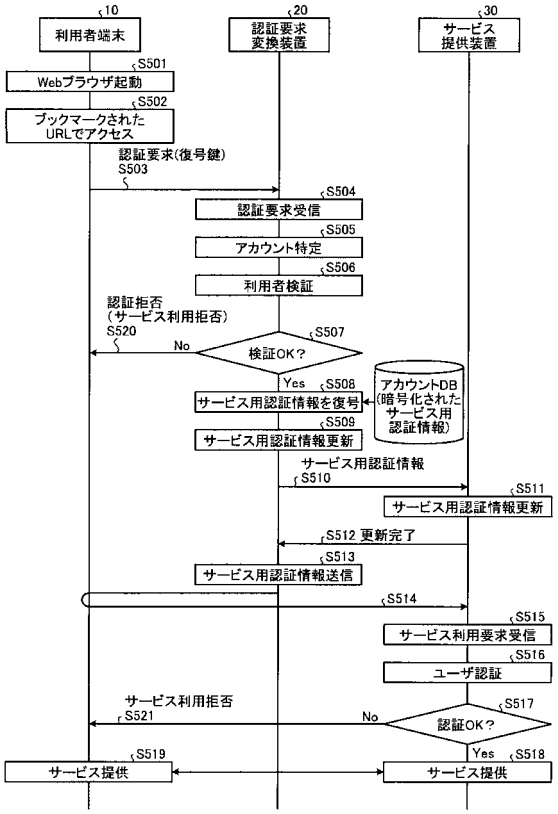
【図８】



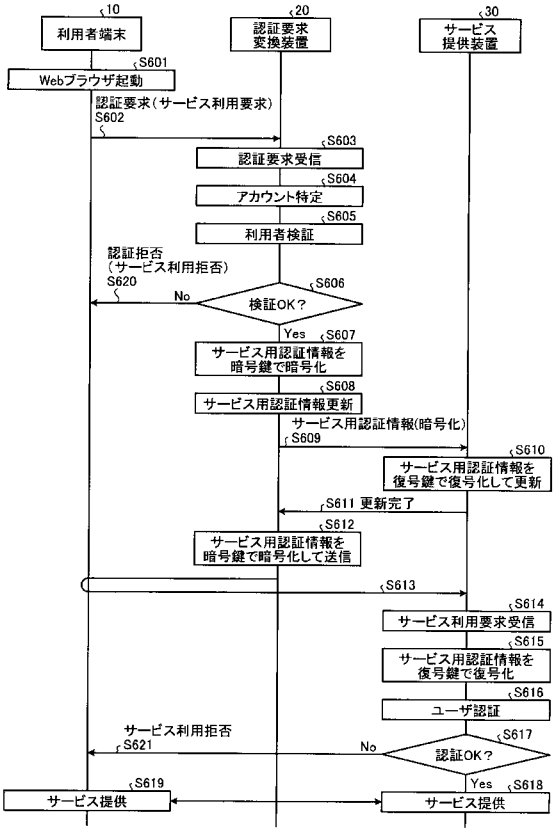
【図９】


10
利用者端末
20
認証要求
変換装置
30
サービス
提供装置
S401
認証要求装置へアクセス
初期登録
S402
S403
暗号鍵および復号鍵生成
S404
サービス用認証情報
入力画面表示
S405
S406
サービス用認証情報入力
S407
S408
サービス用認証情報を
暗号鍵で暗号化して保存
アカウントDB
(暗号化された
サービス用
認証情報)
S409
復号鍵が付加された
URLを送信
S410
S411
受信したURLを登録
(ブックマーク)

【図１０】


10
利用者端末
20
認証要求
変換装置
30
サービス
提供装置
S501
Webブラウザ起動
S502
ブックマークされた
URLでアクセス
認証要求(復号鍵)
S503
S504
認証要求受信
S505
アカウント特定
S506
利用者検証
認証拒否
(サービス利用拒否)
S520
No
S507
検証OK?
Yes
S508
サービス用認証情報を復号
アカウントDB
(暗号化された
サービス用
認証情報)
S509
サービス用認証情報更新
サービス用認証情報
S510
S511
サービス用認証情報更新
S512 更新完了
S513
サービス用認証情報送信
S514
S515
サービス利用要求受信
S516
ユーザ認証
サービス利用拒否
S521
No
S517
認証OK?
Yes
S518
サービス提供
S519
サービス提供

【図１１】


10
利用者端末
20
認証要求
変換装置
30
サービス
提供装置
S601
Webブラウザ起動
認証要求(サービス利用要求)
S602
S603
認証要求受信
S604
アカウント特定
S605
利用者検証
認証拒否
(サービス利用拒否)
S620
No
S606
検証OK?
Yes
S607
サービス用認証情報を
暗号鍵で暗号化
S608
サービス用認証情報更新
サービス用認証情報(暗号化)
S609
S610
サービス用認証情報を
復号鍵で復号化して更新
S611 更新完了
S612
サービス用認証情報を
暗号鍵で暗号化して送信
S613
S614
サービス利用要求受信
S615
サービス用認証情報を
復号鍵で復号化
S616
ユーザ認証
サービス利用拒否
S621
No
S617
認証OK?
Yes
S618
サービス提供
S619
サービス提供

フロントページの続き

Ｆターム(参考) 5B285 AA01 AA04 BA03 BA08 CA42 CA43 CA44 CA45 CB07 CB43
CB44 CB47 CB50 CB52 CB55 CB58 CB62 CB72 CB73 CB95
DA05
5J104 AA07 EA05 JA03 JA21 KA02 KA03 MA01 NA02 NA05 NA37
NA38