(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3675701号
(P3675701)
(45)発行日　平成17年7月27日(2005.7.27)　(24)登録日　平成17年5月13日(2005.5.13)

(51)Int.Cl.[7]	F I		
G06K 19/10	G06K	19/00	S
G06F 15/00	G06F	15/00	330G
G06F 17/60	G06F	17/60	242
G09C 1/00	G09C	1/00	660A
H04L 9/32	H04L	9/00	673A

請求項の数 12　(全 20 頁)　最終頁に続く

(21)出願番号　特願2000-224193(P2000-224193)
(22)出願日　平成12年7月25日(2000.7.25)
(65)公開番号　特開2002-42102(P2002-42102A)
(43)公開日　平成14年2月8日(2002.2.8)
審査請求日　平成14年6月25日(2002.6.25)

(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　100071113
弁理士　菅　隆彦
(72)発明者　藤村　考
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　大嶋　嘉人
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　西原　琢夫
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】利用者認証方法、サービス登録方法、認証カード、サービス登録・利用者認証プログラムを記録した記録媒体、認証機関装置及びサービス提供装置

(57)【特許請求の範囲】
【請求項１】
提示された認証カードの利用者をサービス提供装置が識別する認証方法であって、
第１ステップとして、前記サービス提供装置が、認証カードの提示を契機に、乱数を発生し、当該生成した乱数と、そのサービスを特定するサービス識別子と、当該サービスを認証するためにサービス鍵を用いてサービス認証情報生成手段により生成したサービス認証情報を当該認証カードに送信し、
第２ステップとして、当該認証カードが、前記サービス識別子、前記サービス鍵、利用者識別子からなるサービス情報をサービス管理テーブルからサービス識別子を基に検索し、前記サービス情報からサービス毎かつ認証カード毎にユニークに付与されている利用者識別子と、前記サービス鍵を取得し、当該サービス鍵に基づいて前記サービス認証情報の正当性を認証して、当該認証に成功すると、認証カード固有の情報として予め認証カードに記録されているカード識別子を、予め認証カードに記録されているカード鍵で暗号化してカード認証情報を生成した後に、当該検索した利用者識別子と当該生成したカード認証情報を当該サービス提供装置に送信し、
第３ステップとして、当該サービス提供装置が、当該送信されたカード認証情報を認証機関装置に送信し、
第４ステップとして、当該認証機関装置が、当該送信されたカード認証情報を、予め認証機関装置のカード鍵蓄積手段に記録されているカード鍵で復号化してカード識別子を取得し、当該取得したカード識別子が無効化されていないことを判定し、当該判定の結果を

前記サービス提供装置に送信する、
以上の一連の処理を順次踏んで認証カードの利用者を識別する、
ことを特徴とする利用者認証方法。
【請求項２】
前記認証方法は、
前記第２ステップにおける認証に成功すると、当該検索した利用者識別子と前記送信された乱数とを含む情報を当該検索したサービス鍵で暗号化して利用者識別子認証情報を生成し、前記カード認証情報と共に前記サービス提供装置に送信される利用者識別子に代えて当該生成した利用者識別子認証情報を、当該サービス提供装置に送信し、
前記第３ステップにおける認証機関装置への送信に先立ち、前記送信された利用者識別子認証情報をサービス鍵で復号化して乱数を取り出し、前記生成した乱数と一致するか否かを検証して、利用者識別子の正当性を判定する、
ことを特徴とする請求項１に記載の利用者認証方法。
【請求項３】
前記認証方法は、
前記サービス提供装置と前記認証カードとをネットワークを介して各種のデータの送受信を行って為される、
ことを特徴とする請求項１又は２に記載の利用者認証方法。
【請求項４】
利用者認証に使用されるカードであって、
当該カード固有のカード識別子を蓄積するカード識別子蓄積手段と、
当該カードのカード鍵を蓄積するカード鍵蓄積手段と、
サービス毎及びカード毎に一意に付与される利用者識別子、サービス識別子、サービス鍵を含む複数のサービス情報を記録したサービス管理テーブルを蓄積するサービス管理テーブル蓄積手段と、
後に前記カード識別子が無効化されていないことを判定するため、当該カード識別子をカード鍵で暗号化してカード認証情報を生成するカード認証情報生成手段と、
前記サービス管理テーブルから取り出したサービス識別子とサービス提供装置から送信されたサービス認証情報から取り出したサービス識別子との等否を検証することにより、サービスを認証するサービス認証手段と、
前記サービス提供装置から送信されたサービス識別子を用いて前記サービス管理テーブルから利用者識別子を検索する検索手段と、
前記サービス管理テーブル蓄積手段にサービス情報を記録することによって、前記サービス管理テーブルに新しいサービス情報を登録するサービス情報登録手段と、を有する、
ことを特徴とする認証カード。
【請求項５】
前記カードは、
前記サービス管理テーブルから、前記サービス提供装置から送信されたサービス識別子に対応するサービス鍵を検索する前記検索手段と、
前記利用者識別子に代えて前記サービス提供装置に送信するため、当該利用者識別子を含む情報をサービス鍵で暗号化して利用者識別子認証情報を生成する利用者識別子認証情報生成手段と、を有する、
ことを特徴とする請求項４に記載の認証カード。
【請求項６】
認証カードに記録されて利用されるサービス登録・利用者認証プログラムを記録した記録媒体であって、
前記サービス登録・利用者認証プログラムが、
サービス管理テーブルに、サービス識別子、サービス鍵、及びサービス毎にかつ認証カード毎に一意に付与される利用者識別子を含む複数のサービス情報を登録する手続きと、
認証カード固有のカード識別子を含む情報を、認証カードのカード鍵により暗号化して

カード認証情報を生成する手続きと、
前記サービス管理テーブルから、サービス識別子を基に利用者識別子及びサービス鍵を同時に検索する利用者識別子・サービス鍵検索手続きと、
前記サービス管理テーブルから取り出したサービス識別子とサービス提供装置から送信されたサービス認証情報から取り出したサービス識別子との等否を検証することにより、サービスを認証するサービス認証手続きと、
利用者識別子と前記サービス提供装置から送信された乱数とを含む情報を、サービス鍵により暗号化して利用者識別子認証情報を生成する手続きと、を一連に順次踏んでサービス登録・利用者認証を行うプログラムである、
ことを特徴とするサービス登録・利用者認証プログラムを記録した記録媒体。

【請求項７】
認証カードの有効性を検証する認証機関装置であって、
カード鍵を蓄積するカード鍵蓄積手段と、
サービス提供装置から、サービス識別子、サービス鍵、利用者識別子、カード認証情報、乱数を受信する通信手段と、
各認証カードに登録されている利用者識別子、サービス識別子、サービス鍵を含む複数のサービス情報を記録したサービス管理テーブルを蓄積する認証カード管理テーブル蓄積手段と、
カード認証情報を前記カード鍵で解読して、当該取得したカード識別子が無効化されていないことを判定する、カード認証情報解読手段と、
前記判定により有効となった場合に、前記サービス管理テーブルに前記サービス提供装置から受信した、前記利用者識別子、前記サービス識別子、前記サービス鍵を含む新しいサービス情報を前記認証カードに登録するサービス管理テーブル登録手段と、を具備する、
ことを特徴とする認証機関装置。

【請求項８】
前記認証機関装置は、
旧認証カードの代替としての新認証カードの認証に関する情報を登録する装置でもあり、
前記サービス提供装置から、新認証カードのカード認証情報、利用者情報を含む認証カード再発行に係るデータを受信する前記通信手段と、
新認証カードのカード認証情報を前記カード鍵で解読して取得したカード識別子が無効化されていないことを判定する前記カード認証情報解読手段と、
前記判定に合格した場合に、旧認証カードに対するサービス管理テーブルの内容を、新認証カードに対するサービス管理テーブルとして記録する前記サービス管理テーブル登録手段と、を備える、
ことを特徴とする請求項７に記載の認証機関装置。

【請求項９】
前記認証機関装置は、
前記利用者情報からカード識別子を検索する前記利用者情報記録検索手段と、
カード識別子と利用者情報との関係を記録する前記認証カード管理テーブル蓄積手段と、
前記検索されたカード識別子を無効化する認証カード無効化手段と、
を備える、
ことを特徴とする請求項８に記載の認証機関装置。

【請求項１０】
利用者に対してサービスを提供する提供装置であって、
サービスを特定するサービス識別子を蓄積するサービス識別子蓄積手段と、
サービスを認証するサービス鍵を蓄積するサービス鍵記録手段と、
乱数を発生する乱数発生手段と、

前記乱数と、サービス識別子と、サービスを認証するためにサービス鍵を用いてサービス認証情報生成手段により生成したサービス認証情報を認証カードに送信すると共に、サービス毎かつ認証カード毎に一意に付与されている利用者識別子、カード認証情報を当該認証カードから受信する認証カードアクセス手段と、

当該受信したカード認証情報を認証機関装置に送信する通信手段と、

当該通信手段を介して、認証機関装置から正常終了の通知を受信すると、利用者識別子を基にサービスを提供するサービス提供手段と、を具備する、

ことを特徴とするサービス提供装置。

【請求項１１】

前記提供装置は、

認証カードに対して利用者識別子を生成する利用者識別子生成手段と、

サービス識別子とサービス鍵と利用者識別子とを含むサービス登録要求を前記認証カードに対して送信し、当該認証カードからカード認証情報を受信する前記認証カードアクセス手段と、

認証機関装置に対して、前記サービス識別子と前記サービス鍵と前記利用者識別子と前記受信したカード認証情報を含むサービス登録要求を送信する前記通信手段と、を備える、

ことを特徴とする請求項１０に記載のサービス提供装置。

【請求項１２】

前記提供装置は、

暗号化する為に用いる乱数を生成する乱数生成手段と、

前記生成した乱数を前記サービス識別子と前記サービス認証情報と共に前記認証カードに送信し、当該認証カードから利用者識別子に代えて利用者識別子認証情報を受信する前記認証カードアクセス手段と、

前記利用者識別子認証情報をサービス鍵で復号化して取得した乱数及び利用者識別子が、それぞれ、前記乱数生成手段により生成した乱数、前記利用者識別子生成手段により生成された利用者識別子と一致するかを検証して当該利用者識別子の正当性を判定する前記利用者識別子解読手段と、を具備する、

ことを特徴とする請求項１０又は１１に記載のサービス提供装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、利用者の認証、認証カードに関し、特に一枚の認証カードを複数のサービス提供者で共有する場合に、利用者のプライバシーを保護することを可能とすると共に、紛失、盗難等の後の再発行処理を容易にした、利用者認証方法、サービス登録方法、認証カード、サービス登録・利用者認証プログラムを記録した記録媒体、認証機関装置及びサービス提供装置に関する。

【０００２】

【従来の技術】

近年、ＩＣカードを利用して利用者を認証し、ポイントカード、会員サービス等の各種サービスを提供することが行われているところであるが、多くの場合、ＩＣカードの発行は、サービス提供者毎に行われている為、利用者は各種サービス毎に何枚ものカードを持ち運ぶ必要があり、また、サービス提供者は、ＩＣカードの発行のコストを負担しなければならないといった問題がある。

【０００３】

そこで、近年、一枚のＩＣカードに複数のアプリケーションを搭載するマルチアプリケーションのＩＣカード実現方法が多数提案され、例えば、MAOSCO,LtdのMULTOSカードや、Sun Microsystems,Inc.のJavaCardなどがあり、これらを使用すれば、例えば、一枚のＩＣカードに複数アプリケーションを搭載できる為、当然ながら、認証機能を有する複数のアプリケーションを搭載させることにより、多目的の認証カードとして利用可能となる。

【０００４】
しかし、かかる実現方法では、第１に、認証カードの紛失、盗難があった場合には、それに伴うカードの無効化処理、新しい認証カードに対するアプリケーションの再ローディングについてもサービス提供者毎に個別に行う必要があるので、利用者は多くのサービス提供者に個別に連絡をとり、無効化処理、再ローディングを繰り返し行うことが必要となると共に、第２に、一枚のＩＣカードに複数のアプリケーションを搭載すると、必要なメモリが増え、カードそのもののコストが高価となる等の問題もある。
【０００５】
そこで、かかる問題を解決する為現実的な方法として、例えば、行政機関、クレジットカード会社、認証機関等が発行した一枚のＩＣカードを利用して、かかるＩＣカードの識別子を利用者識別子として各サービス提供者の顧客管理データベースに登録しておき、サービスを提供する際に、顧客管理データベースを参照して、例えば、ポイントカード、会員サービスを提供する方法が考えられる。
【０００６】
この方法では、各サービス提供者は、各々で管理する顧客管理データベースへのアクセスが必須となるが、ＩＣカードに必要な機能は利用者識別子の提示機能と、そのＩＣカードが本物であることを認証する機能のみで足り、前述した問題は大幅に解消される。
【０００７】
【発明が解決しようとする課題】
しかし、ＩＣカード自体の識別子を利用者識別子として認証に用いる方法では、一方で個人の自己情報であるプライバシーの保護に配慮を要しなければならない重大な問題がある。
【０００８】
例えば、ＩＣカードに氏名、住所といった個人情報が記載されていなくても、多数のサービスで同一の利用者識別子が使用されることになると、顧客の詳細な購買行為などの追跡が可能となる。
【０００９】
また、あるサービス提供者に、購入した商品の配達先等のプライバシー情報を通知した場合には、もし、そのサービス提供者が利用者識別子とプライバシー情報との関係を公開すると、かかるプライバシー情報を利用者から直接知らされていない他のサービス提供者までもが、容易に顧客のプライバシー情報を入手できてしまう。
【００１０】
また、ＩＣカードの紛失、盗難などにより、ＩＣカードを無効力化し、新たな利用者識別子を提示する認証カードを再発行する場合には、各サービス提供者の顧客データベースに登録してある利用者識別子を再登録する必要があるので、ＩＣカードへのアプリケーションの再ローディングは不要となったとしても、各サービス提供者がすべき再発行処理が完全になくなるわけではなく残存する。
【００１１】
そこで、本発明の解決すべき主要な目的は、以下の通りである。
【００１２】
本発明の第１の目的は、一枚のＩＣカードを用いながら、複数のサービス提供者毎に固有の利用者識別子を提示することを可能とする、利用者認証方法、サービス登録方法、認証カード、サービス登録・利用者認証プログラムを記録した記録媒体、認証機関装置及びサービス提供装置を提供することにある。
【００１３】
本発明の第２の目的は、ＩＣカードから提示された利用者識別子が本物であることを安全に認証できる、利用者認証方法、サービス登録方法、認証カードサービス登録・利用者認証プログラムを記録した記録媒体、認証機関装置及びサービス提供装置を提供することにある。
【００１５】

本発明の他の目的は、明細書、図面、特に、特許請求の範囲における各請求項の記載から自ずと明らかとなろう。

【００１６】

【課題を解決するための手段】

本発明認証方法は、上記課題の解決に当たり、認証カードを提示されたサービス提供装置が、認証カードの提示を契機に、そのサービスを特定するサービス識別子及び当該サービスを認証するためにサービス鍵を用いてサービス認証情報生成手段により生成したサービス認証情報を当該認証カードに送信し、そして、当該認証カードが、当該送信されたサービス識別子を用いて、サービス管理テーブルから利用者識別子を検索し、当該サービス認証装置を認証して、当該認証に成功すると、認証カード固有の情報であるカード識別子をカード鍵で暗号化してカード認証情報を生成した後に、当該検索した利用者識別子と当該生成したカード認証情報を当該サービス提供装置に送信し、続いて、当該サービス提供装置が、当該送信されたカード認証情報を認証機関装置に送信し、その後、当該認証機関装置が、当該送信されたカード認証情報を、カード鍵で復号化してカード識別子を取得し、当該取得したカード識別子が無効化されていないことを判定し、、当該判定の結果を当該サービス提供装置に送信する、以上の一連の処理を順次踏んで認証カードの利用者を識別する、特徴的構成手法を講じる。

【００１７】

本発明登録方法は、上記課題の解決に当たり、サービス提供装置が、そのサービスの登録対象である利用者を識別する利用者識別子を個別に生成して、当該生成した利用者識別子と、サービスを特定するサービス識別子と、サービスを認証するサービス鍵とを、提示された認証カードに送信し、そして、当該認証カードが、当該送信された利用者識別子、サービス識別子及びサービス鍵を、自らのサービス管理テーブルに記録して、当該認証カード固有の情報であるカード識別子を含んだ情報をカード鍵により暗号化してカード認証情報を生成して、当該サービス提供装置に送信し、続いて、当該サービス提供装置が、当該利用者識別子、当該サービス識別子、当該サービス鍵及び当該カード認証情報を、認証機関装置に送信し、その後、当該認証機関装置は、当該カード認証情報をカード鍵により復号することによりカード識別子を取得して、当該取得したカード識別子の有効性を判定し、当該判定に合格した場合には、当該認証カードに対して登録されたサービスを管理するサービス管理テーブルに、当該利用者識別子、当該サービス識別子、当該サービス鍵を記録する特徴的構成手法を講じる。

【００１８】

本発明カードは、上記課題の解決に当たり、カード固有のカード識別子を蓄積するカード識別子蓄積手段と、カードのカード鍵を蓄積するカード鍵蓄積手段と、サービス毎及びカード毎に一意に付与される利用者識別子、サービス識別子、サービス鍵を含む複数のサービス情報を記録したサービス管理テーブルを蓄積するサービス管理テーブル蓄積手段と、後にカード識別子が無効化されていないことを判定するため、当該カード識別子をカード鍵で暗号化してカード認証情報を生成するカード認証情報生成手段と、サービス管理テーブルから取り出したサービス識別子とサービス提供装置から送信されたサービス認証情報から取り出したサービス識別子との等否を検証することにより、サービスを認証するサービス認証手段と、サービス提供装置から送信されたサービス識別子を用いて当該サービス管理テーブルから利用者識別子を検索する検索手段と、サービス管理テーブル蓄積手段にサービス情報を記録することによって、当該サービス管理テーブルに新しいサービス情報を登録するサービス情報登録手段と、を有する特徴的構成手段を講じる。

【００１９】

本発明記録媒体は、上記課題の解決に当たり、サービス管理テーブルに、サービス識別子、サービス鍵、及びサービス毎にかつ認証カード毎に一意に付与される利用者識別子を含む複数のサービス情報を登録する手続きと、認証カード固有のカード識別子を含む情報を、認証カードのカード鍵により暗号化してカード認証情報を生成する手続きと、サービス管理テーブルから、サービス識別子を基に利用者識別子及びサービス鍵を同時に検索す

る利用者識別子・サービス鍵検索する手続きと、サービス管理テーブルから取り出したサービス識別子とサービス提供装置から送信されたサービス認証情報から取り出したサービス識別子との等否を検証することにより、サービスを認証するサービス認証手続きと、利用者識別子を含む情報を、サービス鍵により暗号化して利用者識別子認証情報を生成する手続きと、を一連に順次踏んでサービス登録・利用者認証を行う特徴的プログラムを記録する。

【００２０】

本発明認証機関装置は、上記課題の解決に当たり、カード鍵を蓄積するカード鍵蓄積手段と、外部と各種データを送受信する通信手段と、各認証カードに登録されている利用者識別子、サービス識別子、サービス鍵を含む複数のサービス情報を記録したサービス管理テーブルを蓄積する認証カード管理テーブル蓄積手段と、カード認証情報を処理して当該取得したカード識別子が無効化されていないことを判定するカード認証情報解読手段と、当該判定により有効となった場合に、当該サービス管理テーブルに当該新しいサービス情報を認証カードに登録するサービス管理テーブル登録手段と、を具備する特徴的構成手段を講じる。

【００２１】

本発明提供装置は、上記解決に当たり、サービスを特定するサービス識別子を蓄積するサービス識別子蓄積手段と、サービスを認証するサービス鍵を蓄積するサービス鍵記録手段と、乱数を発生する乱数発生手段と、当該乱数と、サービス識別子と、サービスを認証するためにサービス鍵を用いてサービス認証情報生成手段により生成したサービス認証情報を認証カードに送信すると共に、サービス毎かつ認証カード毎に一意に付与されている利用者識別子、カード認証情報を当該認証カードから受信する認証カードアクセス手段と、当該受信したカード認証情報を認証機関装置に送信する通信手段と、当該通信手段を介して、認証機関装置から正常終了の通知を受信すると、利用者識別子を基にサービスを提供するサービス提供手段と、を具備する特徴的構成手段を講じる。

【００２２】

更に、具体的詳細に述べると、上記課題の解決は、本発明が次に列挙する新規な特徴的構成手法又は手段の採用により、上記目的を達成するようになされる。

【００２３】

本発明認証方法の第１の特徴は、提示された認証カードの利用者をサービス提供装置が識別する認証方法であって、第１ステップとして、前記サービス提供装置が、認証カードの提示を契機に、乱数を発生し、当該生成した乱数と、そのサービスを特定するサービス識別子と、当該サービスを認証するためにサービス鍵を用いてサービス認証情報生成手段により生成したサービス認証情報を当該認証カードに送信し、第２ステップとして、当該認証カードが、前記サービス識別子、前記サービス鍵、利用者識別子からなるサービス情報をサービス管理テーブルからサービス識別子と基に検索し、前記サービス情報からサービス毎かつ認証カード毎にユニークに付与されている利用者識別子と、サービス鍵を取得し、前記サービス鍵に基づいて前記サービス認証情報の正当性を認証して、当該認証に成功すると、認証カード固有の情報として予め認証カードに記録されているカード識別子を、予め認証カードに記録されているカード鍵で暗号化してカード認証情報を生成した後に、当該検索した利用者識別子と当該生成したカード認証情報を当該サービス提供装置に送信し、第３ステップとして、当該サービス提供装置が、当該送信されたカード認証情報を認証機関装置に送信し、第４ステップとして、当該認証機関装置が、当該送信されたカード認証情報を、予め認証機関装置のカード鍵蓄積手段に記録されているカード鍵で復号化してカード識別子を取得し、当該取得したカード識別子が無効化されていないことを判定し、当該判定の結果を前記サービス提供装置に送信する、以上の一連の処理を順次踏んで認証カードの利用者を識別してなる、利用者認証方法の構成採用にある。

【００２４】

本発明認証方法の第２の特徴は、上記本発明認証方法の第１の特徴における前記認証方法が、前記第２ステップにおける認証に成功すると、当該検索した利用者識別子と前記送

信された乱数とを含む情報を当該検索したサービス鍵で暗号化して利用者識別子認証情報を生成し、前記カード認証情報と共に前記サービス提供装置に送信される利用者識別子に代えて当該生成した利用者識別子認証情報を、当該サービス提供装置に送信し、前記第３ステップにおける認証機関装置への送信に先立ち、前記送信された利用者識別子認証情報をサービス鍵で復号化して乱数を取り出し、前記生成した乱数と一致するか否かを検証して、利用者識別子の正当性を判定してなる、利用者認証方法の構成採用にある。

【００２５】

本発明認証方法の第３の特徴は、上記本発明認証方法の第１又は第２の特徴における前記認証方法が、前記サービス提供装置と前記認証カードとをネットワークを介して各種のデータの送受信を行って為されてなる、利用者認証方法の構成採用にある。

【００２９】

本発明カードの第１の特徴は、利用者認証に使用されるカードであって、当該カード固有のカード識別子を蓄積するカード識別子蓄積手段と、当該カードのカード鍵を蓄積するカード鍵蓄積手段と、サービス毎及びカード毎に一意に付与される利用者識別子、サービス識別子、サービス鍵を含む複数のサービス情報を記録したサービス管理テーブルを蓄積するサービス管理テーブル蓄積手段と、後に前記カード識別子が無効化されていないことを判定するため、当該カード識別子をカード鍵で暗号化してカード認証情報を生成するカード認証情報生成手段と、前記サービス管理テーブルから取り出したサービス識別子とサービス提供装置から送信されたサービス認証情報から取り出したサービス識別子との等否を検証することにより、サービスを認証するサービス認証手段と、前記サービス提供装置から送信されたサービス識別子を用いて前記サービス管理テーブルから利用者識別子を検索する検索手段と、前記サービス管理テーブル蓄積手段にサービス情報を記録することによって、前記サービス管理テーブルに新しいサービス情報を登録するサービス情報登録手段と、を有してなる、認証カードの構成採用にある。

【００３０】

本発明カードの第２の特徴は、上記本発明カードの第１の特徴における前記カードが、前記サービス管理テーブルから、前記サービス提供装置から送信されたサービス識別子に対応するサービス鍵を検索する前記検索手段と、前記利用者識別子に代えて前記サービス提供装置に送信するため、当該利用者識別子を含む情報をサービス鍵で暗号化して利用者識別子認証情報を生成する利用者識別子認証情報生成手段と、を有してなる、認証カードの構成採用にある。

【００３１】

本発明記録媒体の第１の特徴は、認証カードに記録されて利用されるサービス登録・利用者認証プログラムを記録した記録媒体であって、前記サービス登録・利用者認証プログラムが、サービス管理テーブルに、サービス識別子、サービス鍵、及びサービス毎にかつ認証カード毎に一意に付与される利用者識別子を含む複数のサービス情報を登録する手続きと、認証カード固有のカード識別子を含む情報を、認証カードのカード鍵により暗号化してカード認証情報を生成する手続きと、前記サービス管理テーブルから、サービス識別子を基に利用者識別子及びサービス鍵を同時に検索する利用者識別子・サービス鍵検索手続きと、前記サービス管理テーブルから取り出したサービス識別子とサービス提供装置から送信されたサービス認証情報から取り出したサービス識別子との等否を検証することにより、サービスを認証するサービス認証手続きと、利用者識別子と前記サービス提供装置から送信された乱数を含む情報を、サービス鍵により暗号化して利用者識別子認証情報を生成する手続きと、を一連に順次踏んでサービス登録・利用者認証を行うプログラムである、サービス登録・利用者認証プログラムを記録した記録媒体の構成採用にある。

【００３２】

本発明認証装置の第１の特徴は、認証カードの有効性を検証する認証機関装置であって、カード鍵を蓄積するカード鍵蓄積手段と、サービス提供装置から、サービス識別子、サービス鍵、利用者識別子、カード認証情報、乱数を受信する通信手段と、各認証カードに登録されている利用者識別子、サービス識別子、サービス鍵を含む複数のサービス情報を

記録したサービス管理テーブルを蓄積する認証カード管理テーブル蓄積手段と、カード認証情報を前記カード鍵で解読して、当該取得したカード識別子が無効化されていないことを判定する、カード認証情報解読手段と、前記判定により有効となった場合に、前記サービス管理テーブルに前記サービス提供装置から受信した、前記利用者識別子、前記サービス識別子、前記サービス鍵を含む新しいサービス情報を前記認証カードに登録するサービス管理テーブル登録手段と、を具備してなる、認証機関装置の構成採用にある。

【００３３】

本発明認証装置の第２の特徴は、上記本発明機関装置の第１の特徴における前記認証機関装置が、旧認証カードの代替としての新認証カードの認証に関する情報を登録する装置でもあり、前記サービス提供装置から、新認証カードのカード認証情報、利用者情報を含む認証カード再発行に係るデータを受信する前記通信手段と、新認証カードのカード認証情報を前記カード鍵で解読して取得したカード識別子が無効化されていないことを判定する前記カード認証情報解読手段と、前記判定に合格した場合に、旧認証カードに対するサービス管理テーブルの内容を、新認証カードに対するサービス管理テーブルとして記録する前記サービス管理テーブル登録手段と、を備てなる、認証機関装置の構成採用にある。

【００３４】

本発明認証装置の第３の特徴は、上記本発明機関装置の第２の特徴における前記認証装置が、前記利用者情報からカード識別子を検索する前記利用者情報記録検索手段と、カード識別子と利用者情報との関係を記録する前記認証カード管理テーブル蓄積手段と、前記検索されたカード識別子を無効化する認証カード無効化手段と、を備えてなる、認証機関装置の構成採用にある。

【００３５】

本発明提供装置の第１の特徴は、利用者に対してサービスを提供する提供装置であって、サービスを特定するサービス識別子を蓄積するサービス識別子蓄積手段と、サービスを認証するサービス鍵を蓄積するサービス鍵記録手段と、乱数を発生する乱数発生手段と、前記乱数と、サービス識別子と、サービスを認証するためにサービス鍵を用いてサービス認証情報生成手段により生成したサービス認証情報を認証カードに送信すると共に、サービス毎かつ認証カード毎に一意に付与されている利用者識別子、カード認証情報を当該認証カードから受信する認証カードアクセス手段と、当該受信したカード認証情報を認証機関装置に送信する通信手段と、当該通信手段を介して、認証機関装置から正常終了の通知を受信すると、利用者識別子を基にサービスを提供するサービス提供手段と、を具備してなる、サービス提供装置の構成採用にある。

【００３６】

本発明提供装置の第２の特徴は、上記本発明提供装置の第１の特徴における前記提供装置が、認証カードに対して利用者識別子を生成する利用者識別子生成手段と、サービス識別子とサービス鍵と利用者識別子とを含むサービス登録要求を前記認証カードに対して送信し、当該認証カードからカード認証情報を受信する前記認証カードアクセス手段と、認証機関装置に対して、前記サービス識別子と前記サービス鍵と前記利用者識別子と前記受信したカード認証情報を含むサービス登録要求を送信する前記通信手段と、を備えてなる、サービス提供装置の構成採用にある。

【００３７】

本発明提供装置の第３の特徴は、上記本発明提供装置の第１又は第２の特徴における前記提供装置が、暗号化する為に用いる乱数を生成する乱数生成手段と、前記生成した乱数を前記サービス識別子と前記サービス認証情報と共に前記認証カードに送信し、当該認証カードから利用者識別子に代えて利用者識別子認証情報を受信する前記認証カードアクセス手段と、前記利用者識別子認証情報をサービス鍵で復号化して取得した乱数及び利用者識別子が、それぞれ、前記乱数生成手段により生成した乱数、前記利用者識別子生成手段により生成された利用者識別子と一致するかを検証して当該利用者識別子の正当性を判定する前記利用者識別子解読手段と、を具備してなる、サービス提供装置の構成採用にある。

【００３９】
【発明の実施の形態】
以下、添付図面を参照しながら、本発明の実施の形態について詳説する。
【００４０】
（カード例、認証装置例、登録装置例を含めたシステム例）
図１は、本発明の一実施形態であるシステム全体の構成図である。
図２、３、４は、それぞれ、同システムにおける認証カード、サービス提供装置、認証機関装置のそれぞれ構成図である。
【００４１】
＜システム構成＞
同システムは、利用者を識別する為の利用者識別子を提示する認証カード１と、サービス提供者毎に複数存在し得るサービス提供装置２と、認証カード１が本物であるか否かを認証する認証機関装置３と、サービス提供装置２、認証機関装置３を各々接続するネットワーク装置４と、により構成される。
【００４２】
＜認証カード＞
認証カード１は、認証カード固有のカード識別子（以下、ＣＩＤとする）を蓄積するＣＩＤ蓄積手段１１と、認証機関装置３のカード鍵（以下、ＩＫとする）を蓄積するＩＫ蓄積手段１２と、サービス（サービス提供装置２）毎に与えられる、サービス識別子（以下、ＳＩＤとする）、サービス鍵（以下、ＳＶＫとする）及び利用者識別子（以下、ＵＩＤとする）の３組を含むサービス情報なる集合を複数記録したサービス管理テーブル（以下、ＳＶＴとする）を蓄積するＳＶＴ蓄積手段１３と、ＣＩＤを含む情報をＩＫで暗号化するなどしてカード認証情報（以下、ＡＣＩＤとする）を生成するＡＣＩＤ生成手段１４と、ＵＩＤを含む情報をＳＶＫで暗号化するなどして利用者識別子認証情報（以下、ＡＵＩＤとする）を生成するＡＵＩＤ生成手段１５と、サービスを認証するサービス認証手段１６と、サービス毎に、認証カード１毎にユニークに付与されているＵＩＤとＳＶＫとをＳＶＴから検索するＵＩＤ・ＳＶＫ検索手段１７と、新しいサービス情報を登録するサービス情報登録手段１８と、ＡＵＩＤ等のデータをサービス提供装置２に送る手段（図示せず）と、を具備する。
【００４３】
ここで、ＣＩＤ、ＩＫ、ＳＶＴはアクセス保障された領域に格納され、外部から直接読み書きを不可能にする様に、ＣＩＤ蓄積手段１１、ＩＫ蓄積手段１２、ＳＶＴ蓄積手段１３が構成される。
【００４４】
本実施形態例では、認証カード１のＩＫと、認証機関装置３が保有するＩＫとは、共通の鍵であり、カード鍵なる名称で呼ぶことにするが、公開鍵方式で実現することも可能であり、この場合、認証機関装置３に秘密鍵を保有し、その秘密鍵に対応する公開鍵を認証カード１が保持する構成にすればよい。
【００４５】
また、認証カード１は、ＩＣカード、携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータ等で実現することも可能で、認証カード１は、携帯電話、携帯情報端末、パーソナルコンピュータ等と一体構成も可能である。故に、本発明カードは、カードなる名称、形状等に限定されるものではなく、認証カード１自体の機能を具備する物も当然含まれる。
【００４６】
＜サービス提供装置＞
サービス提供装置２は、サービスを特定するＳＩＤを蓄積するＳＩＤ蓄積手段２１と、サービスの提供者を認証する為のＳＶＫを記録するＳＶＫ記録手段２２と、認証カード１と各種のデータの送受信を行う認証カードアクセス手段２３と、サービスに必要となる顧客情報を管理する顧客情報データベース２４と、認証機関装置３と各種のデータを送受信

する通信手段２５と、ロイヤリティ・ポイント等のサービスを提供するサービス提供手段２６と、ＡＵＩＤをＡＶＫにより復号するなどしてＡＵＩＤを解読するＡＵＩＤ解読手段２８と、暗号化、認証の際に用いられる乱数（以下、Ｒとする）を生成するＲ生成手段２９と、ＳＩＤを含む情報をＳＶＫで暗号化するなどしてサービス識別子認証情報（以下、ＡＳＩＤとする）を生成するＡＳＩＤ生成手段２Ａとを、具備する。

【００４７】

尚、顧客管理データベース２４が管理する内容は、サービスに依存して様々な内容がカスタマ情報として記録され、ＵＩＤにより検索できる構成である。

【００４８】

＜認証機関装置＞

認証機関装置３は、認証機関装置の鍵（この実施形態例ではカード鍵と共通）ＩＫを蓄積するＩＫ蓄積手段３１と、各種データをサービス提供装置２と送受信する通信手段３２と、認証カード１固有のＣＩＤと、その認証カード１が利用される際のサービス情報を管理するＳＶＴとの集合から構成され、利用者の各認証カード１を管理する認証カード管理テーブル（以下、ＶＣＴとする）を蓄積するＶＣＴ蓄積手段３３と、サービス情報を登録するサービス情報登録手段３４と、ＡＣＩＤを処理して取得するＣＩＤの有効性を判定するなどＡＣＩＤの解読を行うＡＣＩＤ解読手段３５と、通信手段３２からの利用者情報からＣＩＤを検索する利用者情報記録検索手段３６と、利用者情報記録検索手段３６により当該検索されたＣＩＤを無効化する認証カード無効化手段３７と、認証カード無効化手段３７により無効化されたか否かを判別する認証カード無効化判別手段３８と、を具備する。

【００４９】

本発明の一実施形態例として、認証機関装置３のＶＣＴで管理されるＣＩＤとＳＶＴとは、認証カード１で管理されるＣＩＤとＳＶＴとに、それぞれ等しい情報を用いることとするも、これに限定されず別の実施形態例として、認証機関装置３のＶＣＴのＣＩＤと、認証カード１のＣＩＤとが一対一の対応関係にあるハッシュ値などの別の情報を用いることもできる。また、ＶＣＴのＳＶＴには、認証カード１のＳＶＴに記録されているＳＩＤ、ＳＶＫ、ＵＩＤの３組以外の、例えば登録日などの運用上必要なデータを含めることも可能である。

【００５１】

（認証方法、サービス登録方法を含めた方法例）

前述の、カード例、認証装置例、提供装置例を含めたシステム例におけるシステムを例として、１．認証カード発行の手順、２．認証カードに新しいサービスを登録する手順、３．認証カード提示の手順の順に従い、認証方法例、サービス登録方法例を含めた方法例につき、詳説する。

【００５２】

＜１．認証カード発行手順＞

図５は、認証カード発行手順を示すフロー図である。同図を用いて説明する。

【００５３】

利用者は、ＫＩＯＳＫ、電気店、クレジットカード会社、銀行又は行政機関等の認証カード発行機関から認証カード１を購入等の行為により受理する（ＳＴ１‐１）。

【００５４】

このＳＴ１－１では予め認証カード発行機関により、認証カード１固有の識別子であるＣＩＤと、ＩＫとが認証カード１のＣＩＤ蓄積手段１１、ＩＫ蓄積手段１２に格納されているものとし、ＳＶＴについては、ＳＴ１－１では、必ずしも予め格納しておく必要性はなく、ＳＶＴの内容は、図５の説明で後述する方法により必要に応じて、追加可能である。尚、本実施形態例では、認証カード発行機関が、認証機関装置３の運用管理することにするが、別機関によってなされてもよい。

【００５５】

認証カード発行時には、必要に応じて、運転免許証等の身分証明書を提示し、認証機関装置３に通知し、ＣＩＤと実名等の利用者情報との関係を利用者情報記録検索手段３６によ

り記録しておく（ＳＴ１‐２）。但し、その必要性は、認証カード１の発行ポリシーに依存し、本発明の必須要件ではない。

【００５６】

＜２．認証カードに新しいサービスを登録する手順＞

図６は、前述した１．認証カード発行手順に基づき、利用者が予め保有する認証カード１に対して、サービス提供者の店頭などにおいて、新たにサービス固有のサービスを登録する手順を示すフロー図である。同図を用いて詳説する。

【００５７】

サービス提供装置２は、そのサービスで管理したい登録対象の利用者の識別子であるＵＩＤを、ＵＩＤ生成手段２７により生成する（ＳＴ２－１）。

サービス提供装置２は、Ｒ生成手段２９によりＲを生成する(ＳＴ２－２)。

【００５８】

サービス提供装置２は、そのサービスを特定するＳＩＤと、そのサービス提供者であることを認証する為のＳＶＫとを、それぞれ、ＳＩＤ蓄積手段２１、ＳＶＫ記録手段２２から取り出した後に、ＳＴ２‐１で生成したＵＩＤと共に、認証カードアクセス手段２３により、新しいサービス情報の組（ＳＩＤ、ＳＶＫ、ＵＩＤ）を、ＳＴ２－２で生成した乱数Ｒと共に認証カード１に送る（ＳＴ２－３）。

【００５９】

尚、別の実施形態例にあっては、ＳＩＤ＝ＳＶＫ又はＳＩＤ＝ｈ（ＳＶＫ）とすることにより、ＳＶＫを省略することもでき、ここでは、ｈは、ＭＤ５、ＳＨＡ等の一方向ハッシュ関数とする。

【００６０】

認証カード１は、受信したサービス情報の組をＳＶＴ蓄積手段１３に記録する（ＳＴ２－４）。

【００６１】

認証カード１は、ＣＩＤを認証する為のＡＣＩＤをＡＣＩＤ生成手段１４により生成する（ＳＴ２‐５）。

ＡＣＩＤとして、本実施形態例においては、ＩＫによりＣＩＤを含むデータを暗号化したEnc_{IK}（ＣＩＤ｜｜Ｒ）を用いる。ここで、Enc_{K}（ｍ）は、暗号鍵Ｋによりメッセージｍの暗号文とし、Ｘ｜｜Ｙは、メッセージＸとメッセージＹの連結を表す。

【００６２】

サービス提供装置２は、認証カードアクセス手段２３により認証カード１からＡＣＩＤを読み込む（ＳＴ２－６）。

サービス提供装置２は、ＳＩＤ、ＳＶＫ、ＵＩＤ、ＡＣＩＤ、Ｒを、通信手段２５により認証機関装置３に送信する（ＳＴ２－７）。

認証機関装置３は、ＡＣＩＤ解読手段３５により、受信したＡＣＩＤから、Dec_{IK}（ＡＣＩＤ）を計算し、ＣＩＤとＲとを取り出す（ＳＴ２－８）。ここで、Dec_{K}（ｍ）は、暗号鍵Ｋによるメッセージｍの復号文である。

【００６３】

認証機関装置３は、サービス提供装置２から受信したＲと、ＳＴ２－８で解読して取得したＲとが一致するか否かを検証する（ＳＴ２－９）。

当該ＳＴ２－９で一致した場合には、認証機関装置３は、ＣＩＤに該当する認証カード１が無効化されてないかを、認証カード無効化判別手段３８により確認する（ＳＴ２－１０）。本実施形態例では、認証機関装置３が無効化された認証カード１のＣＩＤのリストを管理し、当該リストに含まれるか否かで確認することで、容易に実現できるが、これに限定されない。

【００６４】

認証機関装置３は、上記ＳＴ２－９及びＳＴ２‐１０に成功すると、ＶＣＴ蓄積手段３３に含まれるＣＩＤ毎に管理しているＳＶＴにサービス情報（ＳＩＤ、ＳＶＫ、ＵＩＤ）を追加する（ＳＴ２－１１）。この様に、認証機関装置３も各認証カード１に記録されたＳ

ＶＴと同じＳＶＴを保有する。これは、後述する認証カード１の再発行に際しサービス提供者に何ら手続きを要しないようにするものである。

【００６５】

認証機関装置３は、その後、通信手段３２を用いて、正常終了したことをサービス提供装置２に通知する（ＳＴ２－１２）。

尚、本実施形態においては、サービス提供装置２と認証機関装置３との間は、安全な通信路が存在すると仮定しているが、仮定できない場合には、ＳＶＫ等を用いて結果を通知するなどして容易に実施できる。

【００６６】

＜３．認証カード提示の手順＞

図９は、利用者がサービスを受ける為に、サービス提供者の店頭などで認証カード１を提示した場合の手順を示すフロー図である。同図を用いて詳説する。

【００６７】

認証カード１が、サービス提供装置２に挿入されることを契機として、以下の処理が開始することになる。

サービス提供装置２は、Ｒ生成手段２９によりＲを生成する（ＳＴ３－１）。

【００６８】

サービス提供装置２は、ＳＩＤ、ＳＶＫを、それぞれＳＩＤ蓄積手段２１、ＳＶＫ記録手段２２から取り出し、サービスを認証する為のＡＳＩＤをＡＳＩＤ生成手段２Ａにより生成する（ＳＴ３－２）。ここで、ＡＳＩＤとしては、例示として、ＳＶＫによりＳＩＤを含むデータを暗号化したEnc_{SVK}（ＳＩＤ｜｜Ｒ）を用いるが、別の実施形態例としては、ＡＳＩＤとしてＳＶＫそのものを送り、これをパスワードのような簡易な認証情報として利用することもできる（この場合にはＳＴ３－１は不要となる）。

【００６９】

サービス提供装置２では、認証カードアクセス手段２３により前記ＳＴ３－１、ＳＴ３－２で生成したＲ及びＡＳＩＤをＳＩＤと共に認証カード１に送る（ＳＴ３－３）。

認証カード１は、ＵＩＤ・ＳＶＫ検索手段１７により、ＳＶＴから、受信したＳＩＤに対応するＳＶＫとＵＩＤとを検索して取り出す（ＳＴ３－４）。

【００７０】

認証カード１は、サービス認証手段１６により、Dec_{SVK}（ＡＳＩＤ）を計算し、ＳＩＤとＲを取り出し、取り出したＳＩＤとＲが、受信したＳＩＤとＲにそれぞれ等しいかを検証することにより、サービス提供装置２を認証する（ＳＴ３－５）。尚、ＡＳＩＤとしてＳＶＫをそのまま利用する場合には、ＳＩＤとＳＶＫの組がＳＶＴに登録されているかを確認することで、サービス提供者２を認証する。

【００７１】

認証カード２は、前記ＳＴ３－５に成功すると、それぞれ、ＡＣＩＤ生成手段１４、ＡＵＩＤ生成手段１５により、ＡＣＩＤ、ＡＵＩＤを、Enc_{IK}（ＣＩＤ｜｜Ｒ）、Enc_{SVK}（ＵＩＤ｜｜Ｒ）から生成する（ＳＴ３－６）。

サービス提供装置２は、認証カードアクセス手段２３により前記ＳＴ３－６により生成したＡＵＩＤとＡＣＩＤを受信する（ＳＴ３－７）。

【００７２】

サービス提供装置２は、ＡＵＩＤ解読手段２８により、Dec_{SVK}（ＡＵＩＤ）を計算し、ＵＩＤとＲとを取り出し、かように得たＲが、既に認証カード１に対して送ったＲと等しいことを確認する（ＳＴ３－８）。

【００７３】

当該ＳＴ３－８により確認した後、通信手段２５により、ＡＣＩＤとＲを認証機関装置３に送る（ＳＴ３－９）。

認証機関装置１は、ＡＣＩＤを、ＡＣＩＤ解読手段３５によりDec_{IK}（ＡＣＩＤ）から、ＣＩＤとＲとを取り出し、かように得たＲが前記ＳＴ３－９により受信したＲと等しいことを確認する（ＳＴ３－１０）。

【００７４】
当該ＳＴ３－１１により確認した後、認証機関装置３は、そのＣＩＤに対する認証カード３が無効化されていないかを認証カード無効化判別手段３８により確認する（ＳＴ３－１１）。
認証確認装置３は、前記ＳＴ３－１０、ＳＴ３－１１の何れにも成功すると、正常終了をサービス提供装置２に送る（ＳＴ３－１２）。
【００７５】
サービス提供装置２は、前記ＳＴ３－１２の正常終了を受信すると、既に得ているＵＩＤを基にそのサービス固有のデータベース（顧客管理データベース２４）を利用して、ポイントのチャージを行うなど多種多様なサービスを提供する（ＳＴ３－１３）。
尚、別構成としては、前記ＳＴ３－７でＡＵＩＤを送らず、前記ＳＴ３－１２で認証機関装置３からＵＩＤを送ることも可能である。
【００７６】
また、別構成としては、前記ＳＴ３－９乃至ＳＴ３－１２を省略し、例えば、高価な取引を行う場合、認証カード１が一定期間使用されなかった場合、ロイヤリティ・ポイントのチャージではなく引き出しの場合、といった高い信用が必要な場合のみ、認証機関装置３にカード無効化確認を要求することもできる。
また、認証機関装置３へのカード無効化確認要求毎にサービス提供者に対して認証手数料を課金することも容易に実現できる。
【００８７】
（記録媒体例）
本発明の一実施形態であるサービス登録・利用者認証プログラムを記録した記録媒体例を説明する。
【００８８】
本記録媒体例は、前述の認証カード１に記録等されて使用される、サービス登録・利用者認証プログラムを記録した媒体であって、当該サービス登録・利用者認証プログラムは、▲１▼ＳＶＴに、ＳＩＤ、ＳＶＫ、及びサービス毎にかつ認証カード毎に一意に付与されるＵＩＤを含むサービス情報を登録する手続きと、▲２▼認証カード固有のＣＩＤを含む情報を、認証カードのＩＫにより暗号化するなどしてＡＣＩＤを生成する手続きと、▲３▼当該▲１▼の手続きにより登録されたＳＶＴから、ＵＩＤ、ＳＶＫを検索するＵＩＤ・ＳＶＫ検索手続きと、▲４▼サービスを認証するサービス認証手続きと、▲５▼ＵＩＤを含む情報を、ＳＶＫにより暗号化するなどしてＡＵＩＤを生成する手続きと、を組み合わせてサービス登録・利用者認証を行うプログラムである。詳細は、上記にて詳説した通りである。
【００８９】
以上、本発明の実施の形態を説明したが、本発明は、必ずしも上記した事項に限定されるものではなく、本発明の目的を達し下記する効果を奏する範囲において、適宜変更実施可能である。
【００９０】
例えば、図８は、通信回線を介した本発明の一実施形態の別例を示した図であり、同図では、認証カード１をサービス提供装置２に挿入する代わりに、自宅等のパーソナルコンピュータ、携帯情報端末（ＰＤＡ）、携帯電話などの利用者端末装置５に挿入し、利用者端末装置５とサービス提供装置２との間は、インタネット等のネットワーク装置４を介して行う構成である。
【００９１】
この構成では、サービス提供装置２は、認証カードアクセス手段２３を利用して認証カード１にアクセスする処理を、通信手段２５を利用して利用者端末装置５と通信路を確立して利用者端末装置５を介して間接的に認証カード１にアクセルする処理とすることで、前記した実施形態例と同様に実施できる。
【００９２】

更には、利用者端末装置５と認証カード１とを縮退させて、認証カード１の機能を利用者端末装置５で行うこともできる。これは、ＩＣカードＲ／Ｗがない環境下においては、現実的な実施例といえる。

以上の様に、各サービス提供装置２と認証カード１（認証カードの機能を具備する物も可）とを直接的又は間接的にネットワークを介して接続して各種データの送受信を行う様になされるのである。

【００９３】

また、前記した全ての発明の実施形態にて、ＳＩＤ、ＵＩＤの構造については、説明していないが、図９に示す様に、ＳＩＤとしてインタネットのドメイン名やインタネットアドレス等を用いることにより、利用者端末装置が、ＳＩＤ、ＳＶＫ、ＵＩＤ及びサービス提供装置２から生成して提供されるＲから、ＡＵＩＤ及びＡＣＩＤを生成する。

【００９４】

更に、「http://www.a-company.com/service.cgi?auid=Zs2w3qQx&acid=8YcB40qU」の様なＵＲＩ(Universal Resource Identifier)を作成できる様にすることにより、このＵＲＩで参照されるＷＷＷページ等を介して、▲１▼取引の履歴（顧客管理データベースを検索して表示）、▲２▼獲得ポイントの表示、▲３▼各サービス提供者から顧客へのメッセージや広告の掲示、▲４▼利用者からの配達先の住所、氏名等の情報の書き込み、▲５▼利用者からのアンケート等のデータ収集といった、様々なサービスを行うことが可能となる。

【００９５】

特に、図８に示した構成において、特に利用者端末装置５が、百貨店、会員制スポーツ施設等に設置され、その設置された利用者端末装置５に認証カード１が提示された場合に、常に当該設置された箇所固有のＳＩＤ、ＡＳＩＤを与える様にセットしておくのみで、当該利用者端末装置５をあたかも専用端末の様に使用することができる。

【００９６】

【発明の効果】

本発明によれば、以下述べる極めて優れた効果を奏するものである。

利用者が既に保持している認証カードに、ポイントカード等の機能を、店頭などで追加できるので、各サービス提供者がそれぞれ別の認証カードを発行する必要がなくなるので、認証カードの発行コストを削減できる。また利用者は、サービス提供者毎に何枚ものカードを持ち運ぶ必要がなくなる。

【００９７】

また、利用者はサービス提供者毎に別の利用者識別子が与えられるので、故意又は誤って、あるサービス提供者が利用者識別子と住所等のプライバシー情報との関係が外部に漏らしたとしても、利用者識別子しか知らされていない他のサービス提供者は、この情報を利用して顧客情報を取得することはできないので、プライバシーの保護が図れる。

【００９８】

また、認証カードを発行する際に、その認証機関装置に実名等の利用者情報を登録することにより、この認証カードを用いて不正取引が行われた場合、裁判所の許可を得ることなどにより、認証カード発行機関は利用者識別子と実名等のプライバシー情報との関係を関係者に知らせることで関係者は実名等を知ることができる。これにより、匿名でありながら、高額な電子商取引を安心して行うことができる。

【００９９】

また、サービス提供者毎に識別子が異なるので、裁判所の許可を得ることなどにより、利用者識別子と実名等のプライバシー情報との関係（間接的に実名等）が公開された場合でも、他のサービス提供者が実名を知ることはできないので、プライバシーの保護を図ることができる。

【０１００】

また、センタにある認証機関装置に、認証カードが適用されている全てのサービス情報が保持されているので、このサービス情報を認証機関装置から取得し認証カードに書き込む

ことで、容易に認証カードの再発行ができ、認証カード紛失などの際の無効化及び再発行の手続きが大幅に簡略化できる。

【０１０１】

また、かように再発行された場合であっても、同一のサービス提供者は、同一の利用者識別子を取得でき、各サービス提供者の顧客管理データベースの利用者識別子を変更する必要性がないので、各サービス提供者の再発行時の顧客管理コストと大幅に低減できる。

また、認証カードは、紛失時のみならず、一定期間毎の更改又は更新し、認証の為の鍵を交換することも容易になるので、安全性の観点からも望ましい。

【０１０２】

また、サービス提供者は、必ずしも認証機関装置に問合せしなくても、利用者識別子を安全に取得でき、例えば、高価な取引を行う場合、認証カードが一定期間以上使用されなかった場合、ロイヤリティ・ポイントのチャージではなく引き出し場合、その他高い信用が必要な場合のみ、認証機関装置に認証カード無効化の確認を要求することもでき、通信コストの削減などの恩恵を受ける。

以上、本発明により、上記列挙した効果を初め多数の優れた効果を奏する。

【図面の簡単な説明】

【図１】　本発明の一実施形態であるシステム全体の構成図である。

【図２】　本発明の一実施形態である認証カードの構成図である。

【図３】　本発明の一実施形態であるサービス提供装置の構成図である。

【図４】　本発明の一実施形態である認証機関装置の構成図である。

【図５】　本発明の一実施形態である認証カードの発行手順を示すフロー図である。

【図６】　本発明の一実施形態である認証カードに新しいサービスを登録する手順を示すフロー図である。

【図７】　本発明の一実施形態である認証カード提示の際の手順を示すフロー図である。

【図８】　本発明の一実施形態である図１とは別のシステム全体の構成図である。

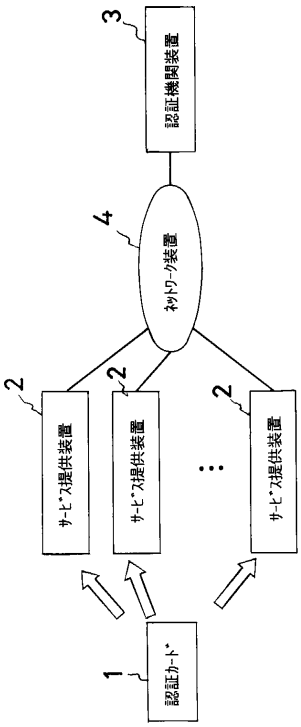
【図９】　本発明の一実施形態におけるサービス管理テーブルの一例である。

【符号の説明】

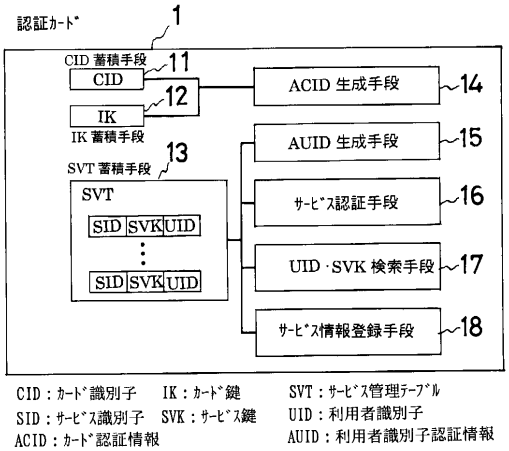
１…認証カード
２…サービス提供装置
３…認証機関装置
５…ネットワーク装置
６…利用者端末装置
１１…ＣＩＤ蓄積手段
１２…ＩＫ蓄積手段
１３…ＳＶＴ蓄積手段
１４…ＡＣＩＤ生成手段
１５…ＡＵＩＤ生成手段
１６…サービス認証手段
１７…ＵＩＤ・ＳＶＫ検索手段
１８…サービス情報登録手段
２１…ＳＩＤ蓄積手段
２２…ＳＶＫ記録手段
２３…認証カードアクセス手段
２４…顧客管理データベース
２５…通信手段
２６…サービス提供手段
２７…ＡＵＩＤ解読手段
２８…Ｒ生成手段
２Ａ…ＡＳＩＤ生成手段
３１…ＩＫ蓄積手段

３２…通信手段
３３…ＶＣＴ蓄積手段
３４…ＳＶＴ登録手段
３５…ＡＣＩＤ解読手段
３６…利用者情報記録検索手段
３７…認証カード無効化手段
３８…認証カード無効化判別手段

【図１】

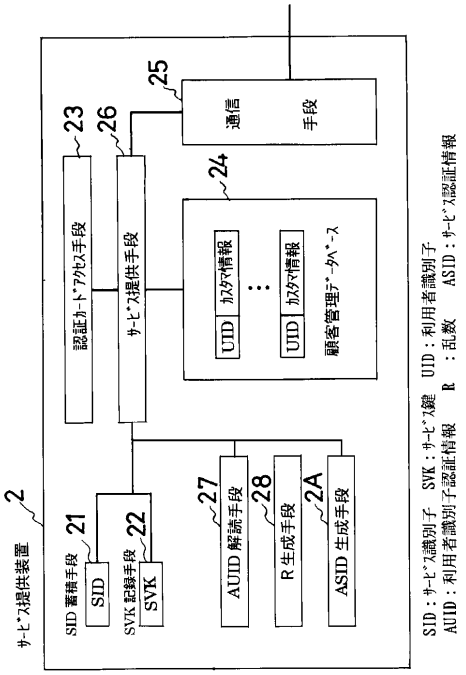


【図２】

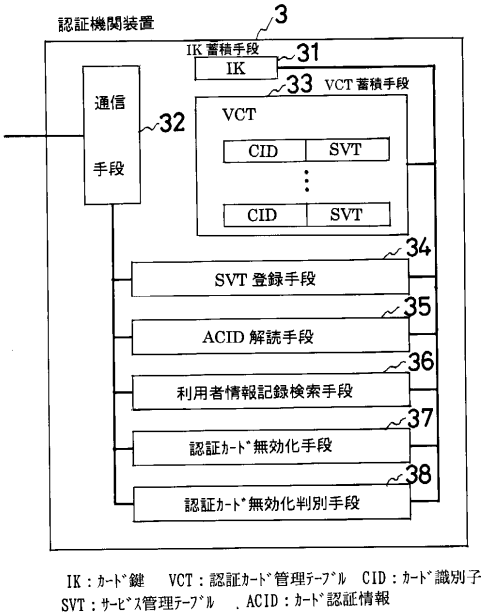


CID：カード識別子　IK：カード鍵　SVT：サービス管理テーブル
SID：サービス識別子　SVK：サービス鍵　UID：利用者識別子
ACID：カード認証情報　AUID：利用者識別子認証情報

【図３】

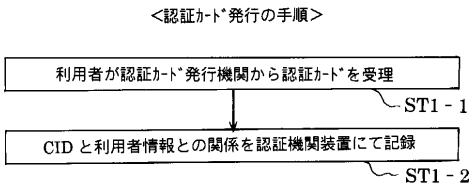


【図４】

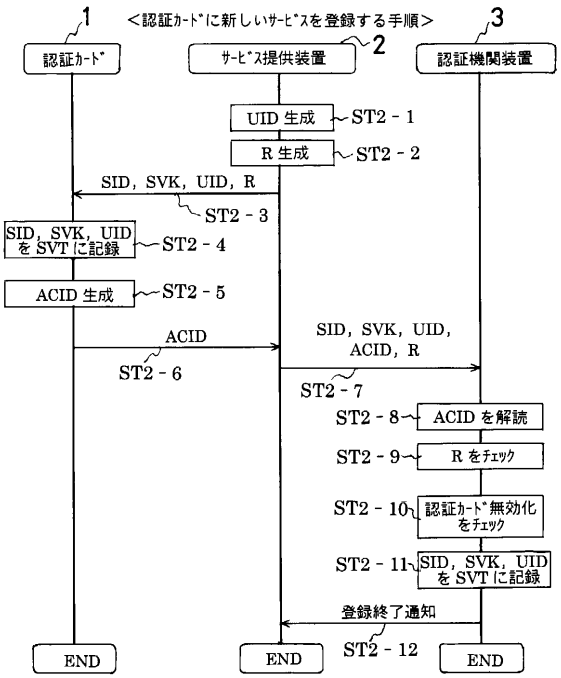


IK：カード鍵　VCT：認証カード管理テーブル　CID：カード識別子
SVT：サービス管理テーブル　．ACID：カード認証情報

【図５】

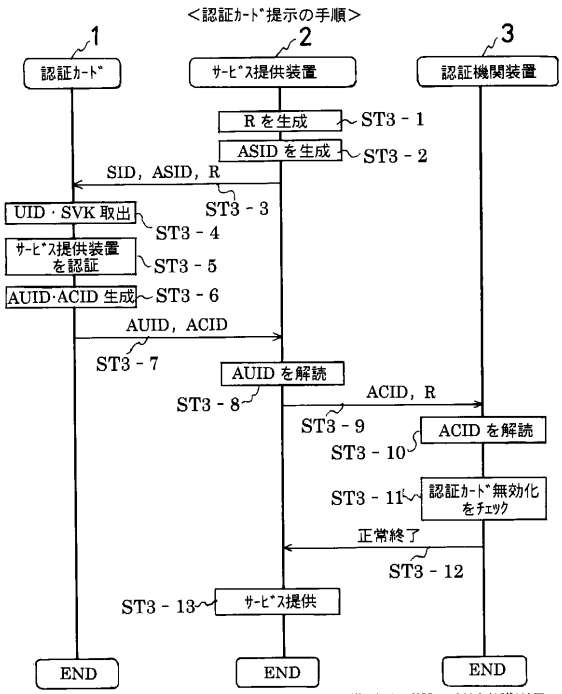


【図６】



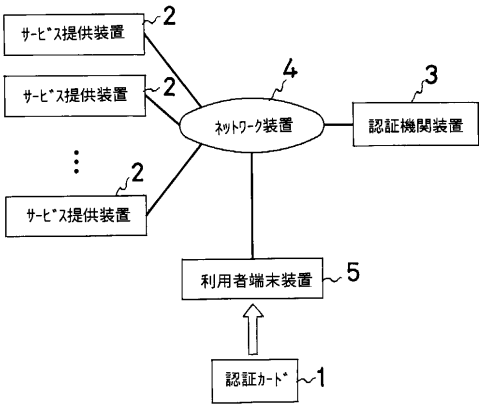
UID ：利用者識別子　R：乱数　SID：サービス識別子　SVK：サービス鍵
SVT ：サービス管理テーブル　ACID：カード認証情報

【図７】



R：乱数　ASID：サービス認証情報　SID ：サービス識別子　UID：利用者識別子
SVK：サービス鍵　AUID：利用者識別子認証情報　ACID：カード認証情報

【図８】



【図９】

ｻｰﾋﾞｽ識別子 SID	ｻｰﾋﾞｽ鍵 SVK	利用者識別子 UID
www.a-company.com	aZq23sDx	11111111
www.b-company.com	Mh434522	22222222
www.c-company.com	203Qmps3	33333333
www.d-company.com	777aspWq	44444444

フロントページの続き

(51)Int.Cl.[7] FI
H04L 9/00 673C
H04L 9/00 673E

審査官 大塚 良平

(56)参考文献 特開平１０－２２２６１８（ＪＰ，Ａ）
特開昭６１－２９６４８７（ＪＰ，Ａ）
特開平０３－２２４０４７（ＪＰ，Ａ）
特開昭６２－２７４４６３（ＪＰ，Ａ）
特開平１１－２８２９９８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G06K17/00-19/10