(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4388039号
(P4388039)
(45)発行日　平成21年12月24日(2009.12.24)　(24)登録日　平成21年10月9日(2009.10.9)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330B
G06Q 20/00 (2006.01)　　G06F 17/60 414

請求項の数 1　(全 30 頁)

(21)出願番号　特願2006-188341(P2006-188341)
(22)出願日　平成18年7月7日(2006.7.7)
(65)公開番号　特開2008-15924(P2008-15924A)
(43)公開日　平成20年1月24日(2008.1.24)
審査請求日　平成18年7月10日(2006.7.10)

(73)特許権者　593022629
株式会社ジェーシービー
東京都港区南青山五丁目１番２２号
(74)代理人　100134588
弁理士　吉浦　洋一
(74)代理人　100100402
弁理士　名越　秀夫
(74)代理人　100088214
弁理士　生田　哲郎
(74)代理人　100087686
弁理士　松本　雅利
(72)発明者　田中　俊
東京都港区南青山５丁目１番２２号　株式会社ジェーシービー　国際インフラ推進部内

最終頁に続く

(54)【発明の名称】ネット決済システム

(57)【特許請求の範囲】
【請求項１】
ネット決済補助装置と、クレジットカードのカード契約者が利用する契約者端末と、前記契約者の本人認証を行う複数の認証サーバと、前記クレジットカードの加盟店が利用する加盟店端末と、前記加盟店端末と前記認証サーバとの間を仲介する仲介サーバとを用いたネット決済システムであって、
前記ネット決済補助装置は、
ディスプレイと駆動用電源とカードスロットとを備えており、認証処理用のＣＰＵとメモリとを備えていない、可搬型のネット決済補助装置であって、
前記カードスロットは、ＣＰＵとメモリとを備えたＩＣカードの着脱が可能であり、
前記ＩＣカードのメモリには、
クレジットカードのカード契約者の識別情報を少なくとも含むカード情報が、外部から読み出せないような状態で予め格納されたカード情報格納部と、
前記契約者の本人認証を行なうための、暗証番号または前記契約者の生体的特徴を示す生体情報である認証情報が、外部から読み出せないような状態で予め格納された認証情報格納部と、
前記カード情報に関連付けられ前記契約者に固有のＯＴＰ生成情報が、外部から読み出せないような状態で予め格納されたＯＴＰ生成情報格納部と、を備えており、
前記ＩＣカードのＣＰＵには、
前記ネット決済補助装置から入力された入力情報と、前記ＩＣカードのメモリの認証情

報格納部に格納された認証情報とを比較することによって、前記ネット決済補助装置の操作者が、前記契約者であるか否かの本人認証を行ない、本人確認がなされた場合、前記ＩＣカードのメモリの前記カード情報格納部から前記識別情報を読み出して、前記ネット決済補助装置のディスプレイに表示する認証手段と、

前記識別情報が表示された後、前記ＯＴＰ生成情報を用いてワンタイムパスワードを生成し、前記ネット決済補助装置のディスプレイに表示するＯＴＰ生成手段と、を備えており、

前記ネット決済システムにおいて、

前記ネット決済補助装置に挿入された前記ＩＣカードの認証手段は、

前記ネット決済補助装置に入力された入力情報と、前記認証情報格納部に格納している認証情報とを比較することで本人認証を行い、前記本人確認がなされた場合、前記カード情報格納部に格納している前記契約者の識別情報を読み出し、前記ディスプレイに表示を行い、

前記加盟店端末は、

前記契約者から入力を受け付けた、前記ネット決済補助装置のディスプレイに表示された識別情報を前記契約者端末から少なくとも受信し、前記契約者の注文情報と前記識別情報と前記加盟店を識別する加盟店識別情報とを前記仲介サーバに送信し、

前記仲介サーバは、

前記加盟店端末から受信した加盟店識別情報が、前記仲介サーバで予め保有している加盟店識別情報と一致するか否かの確認を行い、一致している場合には、その加盟店識別情報とともに受信した識別情報を用いて、クレジットカード決済の認証を行うための認証サーバを特定し、その特定した認証サーバに対して前記識別情報を送信し、

前記認証サーバは、

前記受信した識別情報がその認証サーバに予め登録されているかを確認することによって、前記契約者が前記ネット決済補助装置を用いたネット商取引サービスを受けられる契約者であるか否かの認証を行い、その認証結果を前記仲介サーバを介して前記加盟店端末に送信し、

前記加盟店端末は、

前記認証結果が正当なものであれば、前記契約者端末に対して、前記認証結果と、前記認証サーバへのアクセス先を示す情報とを送信し、

前記ネット決済補助装置に挿入された前記ＩＣカードのＯＴＰ生成手段は、

所定のタイミングにおける日時情報または利用回数情報を、前記ＯＴＰ生成情報により暗号化することでワンタイムパスワードを生成して前記ディスプレイに表示を行い、

前記認証サーバは、

前記加盟店端末から受信した前記認証サーバへのアクセス先を示す情報によるアクセスを前記契約者端末から受け付け、前記契約者から入力を受け付けた、前記ネット決済補助装置のディスプレイに表示されたワンタイムパスワードと、前記識別情報とを前記契約者端末から受信し、その受信した識別情報に対応するＯＴＰ生成情報を特定することで、前記受信したワンタイムパスワードと前記特定したＯＴＰ生成情報とを用いて前記契約者の本人認証を行い、前記ワンタイムパスワードによる認証結果と前記加盟店端末へのアクセス先を示す情報とを前記契約者端末に送信し、

前記加盟店端末は、

前記認証サーバから受信した前記加盟店端末へのアクセス先を示す情報によるアクセスを前記契約者端末から受け付け、前記契約者端末が前記認証サーバから受信したワンタイムパスワードによる認証結果を前記契約者端末から受信し、そのワンタイムパスワードによる認証結果が正当である場合に、アクワイアラが利用するアクワイアラ端末に対して、前記契約者の識別情報を含む取引データと前記ワンタイムパスワードによる認証結果とを送信することで、前記アクワイアラ端末を介してイシュアが利用するイシュア端末に対して、前記クレジットカード決済のためオーソリ要求を送信し、前記注文情報における金額分の与信枠を決済用に確保したことを示す、前記オーソリ要求に対する結果を前記イシュ

ア端末から前記アクワイアラ端末を介して受信する、
ことを特徴とするネット決済システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネット決済システムに関する。
【背景技術】
【０００２】
従来、携帯電話機にクレジットカードや銀行カード等のカード識別情報（カード番号）及び暗証番号を格納しておき、携帯電話機に入力された暗証番号と、格納されている暗証番号とが一致した時に、携帯電話機のディスプレイ上にカード番号を表示することによって、カードとしても機能する携帯電話機がある（例えば、特許文献１参照）。
【０００３】
しかし、このようなカード機能付き携帯電話機には、以下に説明する課題があった。
【０００４】
【特許文献１】特開２００２－６４５９７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
特許文献１に記載されたカード機能付き携帯電話機へのデータの格納、抹消等が通信によって行なわれる。つまり、この携帯電話機は、ネットワークに接続されることが前提となる。
【０００６】
このように、ネットワークに接続可能な携帯電話機に、カード番号や暗証番号を格納しておくと、不正アクセス等により、悪意の第三者によって、これらのカード番号や暗証番号が盗聴、改竄される危険性が少なからずあり、セキュリティ上問題となる。
【０００７】
そこで、携帯電話機をネットワークに接続不可能な構成にすれば、上述の盗聴や改竄の恐れはなくなるかもしれない。
【０００８】
しかし、携帯電話機は、基本となる通話機能に加え、ネットワーク通信機能を有するのが一般的となりつつある昨今、携帯電話機をネットワークに接続不可能な構成とすることは、現実的に困難である。また、現状の携帯電話機の構成を維持したまま、格納されているカード番号や暗証番号を外部から読み出せないようにするためには、暗号化プログラム等を備える必要があり、構成が複雑となる。
【０００９】
また、特許文献１の携帯電話機の場合、上述のネットワークを介した不正アクセスによらずとも、携帯電話機のディスプレイに表示されたカード番号を、一度、第三者に盗み見られてしまうと、第三者がそのカード番号を用いて、インターネット上でクレジット決済によるネット商取引を行なうことが可能となってしまい、この点でのセキュリティも低い。
【００１０】
尚、本件特許出願人は、上記のような、カード番号のみでネット商取引を行なうことが出来るという事情に鑑みて、カード番号の提示に加え、カード会員が予め定めた固定パスワードの提示によってカード会員の本人認証を経なければ、ネット商取引が行えないというネット決済システムの運用を開始している。
【００１１】
しかし、この固定パスワードも、一度、第三者に知られてしまえば、やはり第三者がカード会員になりすましてネット商取引を行なうことが可能となってしまい、必ずしも安全なものとは言えない。

【００１２】
本発明は、以上のような従来の問題点に鑑みてなされたものであって、その目的とするところは、不正アクセス等によりカード番号や暗証番号を盗聴、改竄される危険性がなく、かつ、より安全にネット商取引を行なうことが出来るネット決済補助装置を用いたネット決済システムを提供することにある。
【課題を解決するための手段】
【００１３】
請求項１の発明は、ネット決済補助装置と、クレジットカードのカード契約者が利用する契約者端末と、前記契約者の本人認証を行う複数の認証サーバと、前記クレジットカードの加盟店が利用する加盟店端末と、前記加盟店端末と前記認証サーバとの間を仲介する仲介サーバとを用いたネット決済システムであって、前記ネット決済補助装置は、ディスプレイと駆動用電源とカードスロットとを備えており、認証処理用のＣＰＵとメモリとを備えていない、可搬型のネット決済補助装置であって、前記カードスロットは、ＣＰＵとメモリとを備えたＩＣカードの着脱が可能であり、前記ＩＣカードのメモリには、クレジットカードのカード契約者の識別情報を少なくとも含むカード情報が、外部から読み出せないような状態で予め格納されたカード情報格納部と、前記契約者の本人認証を行なうための、暗証番号または前記契約者の生体的特徴を示す生体情報である認証情報が、外部から読み出せないような状態で予め格納された認証情報格納部と、前記カード情報に関連付けられ前記契約者に固有のＯＴＰ生成情報が、外部から読み出せないような状態で予め格納されたＯＴＰ生成情報格納部と、を備えており、前記ＩＣカードのＣＰＵには、前記ネット決済補助装置から入力された入力情報と、前記ＩＣカードのメモリの認証情報格納部に格納された認証情報とを比較することによって、前記ネット決済補助装置の操作者が、前記契約者であるか否かの本人認証を行ない、本人確認がなされた場合、前記ＩＣカードのメモリの前記カード情報格納部から前記識別情報を読み出して、前記ネット決済補助装置のディスプレイに表示する認証手段と、前記識別情報が表示された後、前記ＯＴＰ生成情報を用いてワンタイムパスワードを生成し、前記ネット決済補助装置のディスプレイに表示するＯＴＰ生成手段と、を備えており、前記ネット決済システムにおいて、前記ネット決済補助装置に挿入された前記ＩＣカードの認証手段は、前記ネット決済補助装置に入力された入力情報と、前記認証情報格納部に格納している認証情報とを比較することで本人認証を行い、前記本人確認がなされた場合、前記カード情報格納部に格納している前記契約者の識別情報を読み出し、前記ディスプレイに表示を行い、前記加盟店端末は、前記契約者から入力を受け付けた、前記ネット決済補助装置のディスプレイに表示された識別情報を前記契約者端末から少なくとも受信し、前記契約者の注文情報と前記識別情報と前記加盟店を識別する加盟店識別情報とを前記仲介サーバに送信し、前記仲介サーバは、前記加盟店端末から受信した加盟店識別情報が、前記仲介サーバで予め保有している加盟店識別情報と一致するか否かの確認を行い、一致している場合には、その加盟店識別情報とともに受信した識別情報を用いて、クレジットカード決済の認証を行うための認証サーバを特定し、その特定した認証サーバに対して前記識別情報を送信し、前記認証サーバは、前記受信した識別情報がその認証サーバに予め登録されているかを確認することによって、前記契約者が前記ネット決済補助装置を用いたネット商取引サービスを受けられる契約者であるか否かの認証を行い、その認証結果を前記仲介サーバを介して前記加盟店端末に送信し、前記加盟店端末は、前記認証結果が正当なものであれば、前記契約者端末に対して、前記認証結果と、前記認証サーバへのアクセス先を示す情報とを送信し、前記ネット決済補助装置に挿入された前記ＩＣカードのＯＴＰ生成手段は、所定のタイミングにおける日時情報または利用回数情報を、前記ＯＴＰ生成情報により暗号化することでワンタイムパスワードを生成して前記ディスプレイに表示を行い、前記認証サーバは、前記加盟店端末から受信した前記認証サーバへのアクセス先を示す情報によるアクセスを前記契約者端末から受け付け、前記契約者から入力を受け付けた、前記ネット決済補助装置のディスプレイに表示されたワンタイムパスワードと、前記識別情報とを前記契約者端末から受信し、その受信した識別情報に対応するＯＴＰ生成情報を特定することで、前記受信したワ

ンタイムパスワードと前記特定したＯＴＰ生成情報とを用いて前記契約者の本人認証を行い、前記ワンタイムパスワードによる認証結果と前記加盟店端末へのアクセス先を示す情報とを前記契約者端末に送信し、前記加盟店端末は、前記認証サーバから受信した前記加盟店端末へのアクセス先を示す情報によるアクセスを前記契約者端末から受け付け、前記契約者端末が前記認証サーバから受信したワンタイムパスワードによる認証結果を前記契約者端末から受信し、そのワンタイムパスワードによる認証結果が正当である場合に、アクワイアラが利用するアクワイアラ端末に対して、前記契約者の識別情報を含む取引データと前記ワンタイムパスワードによる認証結果とを送信することで、前記アクワイアラ端末を介してイシュアが利用するイシュア端末に対して、前記クレジットカード決済のためオーソリ要求を送信し、前記注文情報における金額分の与信枠を決済用に確保したことを示す、前記オーソリ要求に対する結果を前記イシュア端末から前記アクワイアラ端末を介して受信する、ネット決済システムである。

【００１５】

請求項１の発明によれば、ネット決済補助装置によって契約者の本人認証の結果、本人確認がなされなければ、契約者自身であってもカード情報を知ることが出来ず、カード情報は、外部から読み出せないような状態で格納されているので、カード情報が露出している従来のクレジットカードと異なり、カード情報の秘匿性が高まり、ネット商取引におけるカード情報の不正使用が防止される。

【００１６】

また、ネット決済補助装置は可搬型であるので、契約者がどこにいても、携帯電話、自宅のパソコン、出先のパソコンを用いて、安全なネット商取引を行なうことが出来、ネット商取引の利便性が増す。

【００１７】

また、契約者の本人認証に、ネット決済補助装置に格納された契約者固有のＯＴＰ生成情報に基づいて作成されたワンタイムパスワードを用いるので、第三者が、仮にワンタイムパスワードを入手しても、次のネット商取引には使えない。

【００１８】

ワンタイムパスワード生成用のＯＴＰ生成情報は、外部から読み出せないような状態で格納されているので、契約者本人であっても、ＯＴＰ生成情報を知ることは出来ず、ネット決済補助装置を操作している契約者本人のみが生成結果のワンタイムパスワードを知ることが出来る。つまり、第三者によるワンタイムパスワード生成は出来ないので、より、ネット商取引の安全性が保証される。

【００１９】

しかも、このワンタイムパスワードの生成は、ネット決済補助装置にカード情報が表示された後でなければ、行なわれないようになっているので、ネット決済補助装置を有していない第三者は、識別情報のみを知っていても、ワンタイムパスワードの生成が出来ない。また、第三者がネット決済補助装置を盗んだとしても、ネット決済補助装置に入力する認証情報がなければ、ワンタイムパスワードの生成が出来ない。

【００２０】

つまり、契約者は、ネット決済補助装置の認証手段によって本人認証を受けた後、更に、認証サーバによって本人認証を受けることになり、最終的にネット商取引が可能となるまでに２種類の異なる認証情報に基づく本人認証を経なければいけないので、第三者によるなりすましがより防止され、ネット商取引の安全性が高まる。

【００２２】

また、認証情報として暗証番号を用いれば、入力手段及び認証手段を比較的安価に構成することが出来るので、ネット決済補助装置の利用促進が図られる。

【００２４】

また、認証情報として生体情報を用いれば、高精度で契約者の本人認証が行えるようになるので、仮にネット決済補助装置を盗まれても、悪用される恐れのないネット決済補助装置となる。

【発明の効果】
【００３０】
本発明のネット決済補助装置によれば、ネット決済補助装置によって契約者の本人認証の結果、本人確認がなされなければ、契約者自身であってもカード情報を知ることが出来ず、カード情報は、外部から読み出せないような状態で格納されているので、カード情報が露出している従来のクレジットカードと異なり、カード情報の秘匿性が高まり、ネット商取引におけるカード情報の不正使用が防止される。
【００３１】
また、ネット決済補助装置は可搬型であるので、契約者がどこにいても、携帯電話、自宅のパソコン、出先のパソコンを用いて、安全なネット商取引を行なうことが出来、ネット商取引の利便性が増す。
【００３２】
また、契約者の本人認証に、ネット決済補助装置に格納された契約者固有のＯＴＰ生成情報に基づいて作成されたワンタイムパスワードを用いるので、第三者が、仮にワンタイムパスワードを入手しても、次のネット商取引には使えない。
【００３３】
ワンタイムパスワード生成用のＯＴＰ生成情報は、外部から読み出せないような状態で格納されているので、契約者本人であっても、ＯＴＰ生成情報を知ることは出来ず、ネット決済補助装置を操作している契約者本人のみが生成結果のワンタイムパスワードを知ることが出来る。つまり、第三者によるワンタイムパスワード生成は出来ないので、より、ネット商取引の安全性が保証される。
【００３４】
しかも、このワンタイムパスワードの生成は、ネット決済補助装置にカード情報が表示された後でなければ、行なわれないようになっているので、ネット決済補助装置を有していない第三者は、識別情報のみを知っていても、ワンタイムパスワードの生成が出来ない。また、第三者がネット決済補助装置を盗んだとしても、ネット決済補助装置に入力する認証情報がなければ、ワンタイムパスワードの生成が出来ない。
【００３５】
つまり、契約者は、ネット決済補助装置の認証手段によって本人認証を受けた後、更に、認証サーバによって本人認証を受けることになり、最終的にネット商取引が可能となるまでに２種類の異なる認証情報に基づく本人認証を経なければいけないので、第三者によるなりすましがより防止され、ネット商取引の安全性が高まる。
【発明を実施するための最良の形態】
【００３６】
以下、本発明の好適な実施の形態について、添付図面に基づいて詳細に説明する。図１（ａ）は、ネット決済補助装置１の外観図であり、図１（ｂ）は、ネット決済補助装置１の電気的ハードウェアの構成図である。
【００３７】
ネット決済補助装置１は、クレジットカードやデビットカード等のカード契約者の契約者端末（携帯電話やパーソナルコンピュータ等）と、契約者の本人認証を行なう認証サーバ（通常、カード会社が保有）が、相互にネットワーク接続されたネット決済システムにおいて、契約者が当該契約者の識別情報を用いた決済により、ネットショッピング等のネット商取引を行なう際に用いられるものであり、図１（ａ）に示されるように、手のひらに収まる程度の外形を有し、薄型で持ち運びが可能な筐体１０で構成され、筐体１０の外表面に、ディスプレイ１１と、キー操作部１２が露出している。
【００３８】
尚、本実施例のディスプレイ１１は、８桁の表示ディスプレイであり、キー操作部１２は、０～９までのテンキー１２ａと、スタートキー１２ｂとから構成される。
【００３９】
筐体１０の内部は、図１（ｂ）に示すように、ディスプレイ１１、キー操作部１２の他

、カード情報格納部１３、認証情報格納部１５、認証手段１４、ＯＴＰ生成手段１６、ＯＴＰ生成情報格納部１７、計時手段１８として各々機能するためのハードウェア（ＣＰＵ、メモリ）と、これらのハードウェア電気部品（ディスプレイ１１、キー操作部１２、ＣＰＵ、メモリ）を駆動するための駆動用電源１９（電池）によって構成される。

【００４０】

尚、本実施例の筐体１１には、ディスプレイ１１とキー操作部１２と駆動用電源１９の他、ＳＩＭ等のＩＣカードを内蔵するスロットが設けられており、当該スロットにＩＣカードを挿入して用いる。そして、上記ＣＰＵとメモリは、このＩＣカードに含まれるものを使用する。後述するように、カード情報格納部１３、認証情報格納部１５、ＯＴＰ生成情報格納部１７には、契約者毎に異なる情報が記憶されるので、このような情報をＩＣカードのメモリに格納して、スロットに挿入して用いることで、筐体１１自体は、契約者によらず、共通のものでよく、また、筐体１１自体に個人情報を保有しないので、筐体１１の生産性が向上するとともに、筐体１１の取り扱い、管理が容易となる。

【００４１】

また、本実施例の駆動用電源１９は、ボタン電池であるが、太陽電池や充電池等であってもよい。また、ネット決済補助装置１は、通常時は電源オフ状態にしておき、例えば、キー操作部１２のいずれかのキー操作があった場合に、電源起動するようになっていてもよい。

【００４２】

本実施例のカード情報格納部１３、認証情報格納部１５、ＯＴＰ生成情報格納部１７は、具体的には、後述するカード情報、認証情報、ＯＴＰ生成情報を各々格納するメモリによって構成されており、メモリは、物理的には、これら情報をまとめて格納する１つのメモリであってもよいし、２以上のメモリであってもよい。

【００４３】

本実施例の認証手段１４及びＯＴＰ生成手段１６は、具体的には、メモリに格納されたプログラムによって構成されており、ネット決済補助装置１内のＣＰＵが、当該プログラムをメモリから読み出して実行することによって、これら認証手段１４及びＯＴＰ生成手段１６の機能が実現されることになる。尚、ＣＰＵ、メモリを備えないネット決済補助装置においては、認証手段１４、ＯＴＰ生成手段１６の機能が、電子部品を用いて回路的に実現されてもよい。

【００４４】

本実施例のネット決済補助装置１は、クレジットカードブランドとのライセンス契約に基づいてクレジットカードを発行するイシュア（デビットカードであれば、デビットカードを発行する銀行もしくはカード発行会社）から個々のカード会員である契約者に対し、イシュアにおいて契約者毎に固有のカード情報、認証情報、ＯＴＰ生成情報がメモリに記録された状態で、配布（配布形態は、貸与、譲渡いずれもよい）されるものであり、配布後は、メモリ（カード情報格納部１３、認証情報格納部１５、ＯＴＰ生成情報格納部１７）の格納内容を、外部から読み出すことが出来ないように構成されている。

【００４５】

また、ネット決済補助装置１を配布された契約者自身であっても、メモリの記録内容を外部から読み出すことは出来ない。契約者自身は、契約者の本人認証が行なわれ、本人と確認された場合に限り、カード情報がディスプレイ１１に表示されることによって、当該カード情報のみ、知ることが出来、それ以外の状態においては、カード情報は秘匿化されている。

【００４６】

メモリの格納内容を、外部から読み出すことが出来ないようになっているのは、ネット決済補助装置１がインターネット等のネットワークに接続されるインターフェースを備えていない、ネット非接続型の端末であるからである。

【００４７】

尚、メモリの格納内容の盗聴、改竄に対する更なるセキュリティ向上のため、ネット決

済補助装置１または、ネット決済補助装置１に内蔵されるＳＩＭ等のＩＣカードが、耐タンパ性（分解して、メモリから直接記録内容を読み出そうとすると、メモリの記録内容が消去されたり、プログラムが起動しなくなる性質）を備えていてもよい。

【００４８】

以下、ネット決済補助装置１の各部の詳細について説明する。

【００４９】

カード情報格納部１３は、契約者の識別情報を少なくとも含むカード情報が、外部から読み出せないような状態で予め格納されたメモリであり、本実施例のカード情報は、契約者固有の識別情報（カード番号）と、有効期限と、セキュリティコード（所定の方法により予め暗号化した３桁の１０進数。通常、プラスチックタイプのクレジットカードのサインパネルに印字されている。この数字によって、カードの真正性を確認することが出来る）から構成される。また、名義人名が含まれていてもよい。また、単にカード情報が識別情報のみで構成されていてもよい。また、有効期限、セキュリティコード、名義人名の全てをカード情報が含む必要はなく、適宜１以上組み合わせてカード情報が構成されていてもよい。

【００５０】

認証情報格納部１５は、契約者が定めた暗証番号や、契約者の指紋、虹彩、声帯、顔写真等の生体的特徴を数値化した生体情報等、契約者の本人認証を行なうための認証情報が、外部から読み出せないような状態で予め格納されたメモリである。

【００５１】

尚、認証情報格納部１５に格納される認証情報は、ネット決済システムにおける認証サーバが契約者の本人認証に用いる認証情報とは異なり、ネット決済補助装置１が契約者の本人認証を行なうために必要な認証情報である。また、認証サーバにおける認証情報とネット決済補助装置１における認証情報は、種類が異なるものである。

【００５２】

ＯＴＰ生成情報格納部１７は、ネット決済補助装置１に固有のＯＴＰ生成情報が、外部から読み出せないような状態で予め格納されたメモリであり、本実施例のＯＴＰ生成情報は、ネット決済補助装置１に固有の共通鍵であり、共通鍵は、ＯＴＰ生成手段１６で生成されたワンタイムパスワードの検証を行なうサーバ（後述の実施例における認証サーバ）において、カード情報格納部１３に格納されている識別情報と関連付けられている。

【００５３】

尚、共通鍵は、ネット商取引において、契約者の本人認証を行なう認証サーバと、ネット決済補助装置１のみに格納された鍵であり、本実施例では、後述のＯＴＰ生成手段１６が、ワンタイムパスワードを生成するのに用いられる。

【００５４】

認証手段１４は、ネット決済補助装置１の操作者が、カード情報格納部１３に格納されている識別情報を利用可能な契約者（カード会員）であるか否かの本人認証を行なう手段であり、入力手段（本実施例では、テンキー１２ａ）から入力された入力情報と、認証情報格納部１５に格納されている認証情報と一致するか確認し、一致した場合に、ネット決済補助装置１の操作者が当該契約者本人であるものとして、カード情報格納部１３に格納されているカード情報のうち、少なくとも識別情報を読み出して、ディスプレイ１１に表示する手段である。

【００５５】

本実施例の認証手段１４は、操作者が、キー操作部１２のスタートキー１２ｂを押下することで、スタートキー１２ｂの押下検出を受けて起動する。更にその後、操作者が、入力手段に相当するテンキー１２ａを押下して４桁の数字を入力すると、認証手段１４は、入力された数字が、認証情報格納部１５に格納されている暗証番号と一致するか否かを確認し、一致した場合にディスプレイ１１にカード情報を表示する。

【００５６】

認証情報が本実施例のように暗証番号であれば、入力手段としてテンキーがあればよく

、入力情報と認証情報の一致判定処理も容易に行なわれるので、比較的安価な構成でネット決済装置１が実現され、ネット決済装置１の利用促進が図られる。

【００５７】

本実施例の認証情報は４桁の暗証番号となるが、認証方法及び認証情報は、これに限らず、複数の認証方法による認証手段が適宜、組み合わせられてもよく、複数の認証手段を採用すれば、それだけ認証精度が高まり、第三者によるネット決済補助装置の悪用が防止される。

【００５８】

例えば、認証手段１４が、バイオメトリクス認証方法を採用していれば、認証情報は、バイオメトリクス情報（指紋、虹彩、声帯、顔写真等の生体的特徴を数値化したデータ）となり、また、入力手段は、これらのバイオメトリクス情報を入力するスキャナー、マイク、ディジタルカメラ等となる。

【００５９】

バイオメトリクス認証方法は、高精度な認証方法であるから、仮にネット決済補助装置１を第三者に盗まれても、ネット決済補助装置１が配布された契約者でなければ、ネット決済補助装置１を使うことが出来ず、悪用が防止される。

【００６０】

また、本実施例の認証情報である暗証番号には、数字の他、アルファベットが含まれていてもよく、その場合は、テンキーの他にアルファベットキーをネット決済補助装置が備える必要がある。

【００６１】

ＯＴＰ生成手段１６は、認証手段１４によって、カード情報が表示された後、ＯＴＰ生成情報格納部１７に格納されたＯＴＰ生成情報（本実施例では、共通鍵）に基づいて、ワンタイムパスワードを生成し、ディスプレイ１１に表示する手段である。

【００６２】

このワンタイムパスワードは、契約者端末から認証サーバに送信され、認証サーバが契約者の本人認証を行なう際に、認証サーバでＯＴＰ生成情報に基づいて生成されたワンタイムパスワードとの照合に用いられる。そして、これらワンタイムパスワードの照合結果が一致し、認証サーバによって本人確認がなされた場合、当該契約者の識別情報を用いた決済によるネット商取引が可能となる。

【００６３】

本実施例では、認証手段１４による認証が行なわれ、カード情報がディスプレイ１１に表示された後に、操作者がスタートキー１２ｂを押下すると、スタートキー１２ｂを押下したことが、ＯＴＰ生成手段１６を起動させる契機となり、ワンタイムパスワードが生成・表示される。

【００６４】

尚、本実施例のＯＴＰ生成手段１６は、詳細は後述する時間同期方式により、ワンタイムパスワードを生成するものとするが、その他の生成方式、例えば、カウンタ同期方式や、チャレンジ＆レスポンス方式により、ワンタイムパスワードが生成されてもよい。

【００６５】

計時手段１８は、本実施例のＯＴＰ生成手段１６が時間同期方式によりワンタイムパスワードを生成するために必要となる手段であり、計時する手段である。尚、計時手段１８は、リアルタイムクロックによって構成されていてもよいし、また、計時プログラムがメモリに格納され、当該計時プログラムをＣＰＵが読み出して実行し計時機能を実現するようになっていてもよい。また、ＯＴＰ生成手段１６が、時間同期方式以外の方式でワンタイムパスワードを生成する場合には、計時手段１８は不要であり、代わりに、各生成方式に必要な手段が付加されることとなる。

【００６６】

本実施例では、ＯＴＰ生成手段１６は、前述したように、認証手段１４がディスプレイ１１にカード情報を表示したのを受けて、スタートキー１２ｂの押下検出待ち状態となる

。ＯＴＰ生成手段１６は、スタートキー１２ｂの押下が検出されると、押下検出を計時手段１８に伝達する。計時手段１８は、スタートキー１２ｂが押下検出された日時を計時し、日時データ（年月日時分秒。秒は３０秒単位）をＯＴＰ生成手段１６に引き渡す。

【００６７】

そして、ＯＴＰ生成手段１６は、ＯＴＰ生成情報格納部１７から、共通鍵を読み出し、引き渡された日時データを読み出した共通鍵で暗号化し、これを十進数に変換し、ディスプレイ１１に表示する。尚、本実施例の暗号化方式は、共通鍵暗号方式を採用しているが、その他の暗号化方式でもよい。

【００６８】

以上説明したネット決済補助装置１によれば、ネット決済補助装置１によって契約者の本人認証が行なわれ、本人と確認された場合に、認証手段１４が表示したカード情報は、カード決済が可能な加盟店のウェブサイト又は認証サーバから送信され契約者端末に表示されるカード情報入力画面に入力された後、ウェブサイト又は認証サーバに送信可能にされる。

【００６９】

このように、ネット決済補助装置１によって契約者の本人認証が行なわれ、本人と確認されなければ、すなわち、入力された入力情報が、ネット決済補助装置に格納されている認証情報と一致しなければ、契約者自身であってもカード情報を知ることが出来ず、カード情報は、外部から読み出せないような状態で格納されているので、カード情報が露出している従来のクレジットカードと異なり、カード情報の秘匿性が高まり、ネット商取引におけるカード情報の不正使用が防止される。

【００７０】

また、ネット決済補助装置は可搬型であるので、契約者がどこにいても、携帯電話、自宅のパソコン、出先のパソコンを用いて、安全なネット商取引を行なうことが出来、ネット商取引の利便性が増す。

【００７１】

また、ＯＴＰ生成手段１６が表示したワンタイムパスワードは、契約者の本人認証を行う認証サーバから送信され契約者端末に表示されるワンタイムパスワード入力画面に入力された後、認証サーバに送信可能にされるとともに、認証サーバが生成したワンタイムパスワードとの照合により、一致した場合に、本人確認がなされ、契約者の識別情報を用いた決済によるネット商取引が可能にされる。

【００７２】

このように、契約者の本人認証に、ネット決済補助装置に格納された契約者固有のＯＴＰ生成情報に基づいて作成されたワンタイムパスワードを用いるので、第三者が、仮にワンタイムパスワードを入手しても、次のネット商取引には使えない。

【００７３】

ワンタイムパスワード生成用のＯＴＰ生成情報は、外部から読み出せないような状態で格納されているので、契約者本人であっても、ＯＴＰ生成情報を知ることは出来ず、ネット決済補助装置を操作している契約者本人のみが生成結果のワンタイムパスワードを知ることが出来る。つまり、第三者によるワンタイムパスワード生成は出来ないので、より、ネット商取引の安全性が保証される。

【００７４】

しかも、このワンタイムパスワードの生成は、ネット決済補助装置にカード情報が表示された後でなければ、行なわれないようになっているから、ネット決済補助装置を有していない第三者は、識別情報のみを知っていても、ワンタイムパスワードの生成が出来ない。また、第三者がネット決済補助装置を盗んだとしても、ネット決済補助装置に入力する認証情報がなければ、ワンタイムパスワードの生成が出来ない。

【００７５】

つまり、契約者は、ネット決済補助装置の認証手段によって本人認証を受けた後、更に、認証サーバによって本人認証を受けることになり、最終的にネット商取引が可能となる

までに２種類の異なる認証情報に基づく本人認証を経なければいけないので、第三者によるなりすましがより防止され、ネット商取引の安全性が高まる。

【００７６】

尚、認証情報格納部１５は、上述した認証情報の他、認証手段１４が行なう一致判定処理で、入力情報と認証情報が一致しなかった場合に、入力情報の再入力を受付ける回数（エラー許容回数）を予め格納してもよい。その場合、ネット決済補助装置１又は認証手段１４は、計数手段（カウンタ）をも備える構成となる。

【００７７】

そして、認証手段１４が一致判定処理を行なうフローにおいて、入力情報と認証情報が一致しなかった場合、その都度、計数手段が１からカウントアップを行い、カウントアップされた数字と、エラー許容回数とを比較して、カウントアップされた数字がエラー許容回数を上回った場合には、以降、認証手段１４は、自身の処理が行なわれないようにし、更に、ＯＴＰ生成手段１６が起動しないようにし、認証フロー及びＯＴＰ生成フローが行なわれないようにする。

【００７８】

これにより、悪意の第三者が、ネット決済補助装置１を盗用して、認証情報を手当たり次第に入力した結果、カード情報やワンタイムパスワードがディスプレイ１１に表示されてしまうのを防止することが出来る。

【００７９】

尚、カウントアップされた数字がエラー許容回数を上回ることなく、入力情報と認証情報が一致した場合には、認証手段１４は、ディスプレイ１１にカード情報の表示を行なうことにするが、この時に、カウントアップされた数字は、０にリセット（初期化）されるものとする。

【００８０】

ここで、ネット決済補助装置１を操作手順及びディスプレイ１１の画面遷移の一例を図５に示す。尚、本実施例のディスプレイ１１は、８桁の英数字・記号表示用ディスプレイである。

【００８１】

まず、操作者によってスタートキー１２ｂが押下されると、ネット決済補助装置１の電源が起動し（Ｓ２００）、ディスプレイ１１に、「ＡＰＰＬＩ」と表示される（Ｓ２１０）ので、更にスタートキー１２ｂが押下された後（Ｓ２２５）カード情報を表示させたい場合は、操作者はテンキー１２ａの「１」を押下し（Ｓ２３０）、認証情報（暗証番号）の変更を行ないたい場合は、テンキー１２ａの「２」を押下する（Ｓ３３０）。

【００８２】

「１」が押下された場合（Ｓ２３０）、ディスプレイ１１に「ＰＩＮ」と表示されるので、操作者は認証情報として４桁の暗証番号をテンキー１２ａの中から選択して押下する（Ｓ２４０）。その後、スタートキー１２ｂが押下され（Ｓ２４５）、押下された暗証番号が、認証情報格納部１５に格納されている認証情報と一致すれば、カード情報格納部１３に格納されているカード情報のうち、まず、識別情報（以下、カード番号という）の上８桁がディスプレイ１１に表示される（Ｓ２５０）。

【００８３】

続いて、スタートキー１２ｂが押下されると（Ｓ２５５）、カード番号の下８桁がディスプレイ１１に表示される（Ｓ２６０）。

【００８４】

続いて、スタートキー１２ｂが押下されると（Ｓ２６５）、有効期限とセキュリティコードがディスプレイ１１に表示される（Ｓ２７０）。尚、Ｓ２６５とＳ２７０のフローは必須ではなく、カード情報のうちカード番号のみが表示されるものであってもよい。

【００８５】

続いて、スタートキー１２ｂが押下されると（Ｓ２７５）、ディスプレイ１１に「ＯＴＰ＝１」と表示され、ワンタイムパスワードを生成・表示するか、終了するか否かの選択

がなされる。ここで、スタートキー１２ｂが押下された後（Ｓ２９０）、テンキー１２ａの「１」が押下されると（Ｓ２９５）、ディスプレイ１１に、認証情報の入力を促す「ＰＩＮ」が表示されるので（Ｓ３０５）、操作者は、再び４桁の暗証番号をテンキー１２ａから押下し、スタートキー１２ｂを押下する（Ｓ３１０）。

【００８６】

押下された暗証番号が、認証情報格納部１５に格納されている認証情報と一致すれば、ＯＴＰ生成情報格納部１７に格納されているＯＴＰ生成情報に基づき、ワンタイムパスワードが生成され、これがディスプレイ１１に表示される（Ｓ３１５）。

【００８７】

再び、スタートキー１２ｂが押下されると（Ｓ３２０）、ネット決済補助装置１の電源が遮断される。

【００８８】

テンキー１２ａの「１」以外のキーが押下されるか、いずれのキーも押下されず、予め決められた所定時間が経過した場合には（Ｓ３００）、自動的にネット決済補助装置１の電源が遮断される。

【００８９】

尚、Ｓ２４０とＳ３０５で入力される暗証番号は、カード情報表示用とワンタイムパスワード生成用とで、別々の暗証番号でもよく、その場合は、認証情報格納部１５に、それぞれの暗証番号が区別して格納されている。

【００９０】

また、本実施例では、ワンタイムパスワードをディスプレイ１１に表示するフロー（Ｓ３１５）の前に、Ｓ３０５で、操作者に再度、認証情報の入力を促したが、Ｓ３０５を省略して、Ｓ３１０のスタートキー１２ｂの押下のみで、ワンタイムパスワードが生成されてもよい。

【００９１】

Ｓ２２５の後、テンキー１２ａの「２」が押下された場合には（Ｓ３３０）、ディスプレイ１１に「ＣＨＡＮＧＥ？」と表示される（Ｓ３３５）。

【００９２】

スタートキー１２ｂが押下されると（Ｓ３４０）、ディスプレイ１１に「ＰＩＮ」と表示され、暗証番号の入力が促されるので、操作者は、テンキー１２ａから４桁の暗証番号を押下後（Ｓ３４５）、更に、スタートキー１２ｂを押下し（Ｓ３５０）、押下された暗証番号が、認証情報格納部１５に格納されている認証情報と一致すれば、変更後の暗証番号の入力を促す「ＮＥＷ１」がディスプレイ１１に表示されるので、操作者は変更後の暗証番号をテンキー１２ａから押下し（Ｓ３５５）、更に、スタートキー１２ｂを押下する（Ｓ３６０）。

【００９３】

次に、ディスプレイ１１には、再度、変更後の暗証番号の入力を促す「ＮＥＷ２」がディスプレイ１１に表示されるので、操作者は変更後の暗証番号を再度テンキー１２ａから押下し（Ｓ３６５）、更に、スタートキー１２ｂを押下する（Ｓ３７０）。

【００９４】

Ｓ３５５で押下された暗証番号と、Ｓ３６５で押下された暗証番号が一致していれば、ディスプレイ１１に、暗証番号の変更が完了した旨を表す「ＣＯＭＰＬＥＴＥ」が表示される（Ｓ３７５）ので、その確認を経た後、スタートキー１２ｂが押下されると（Ｓ３８０）、暗証番号の変更手続が完了し、電源が遮断される。

【００９５】

尚、セキュリティ向上のため、Ｓ３５５とＳ３６５で、テンキー１２ａから入力がなされても、入力された値は、ディスプレイ１１上に表示されないことが望ましい。

【実施例１】

【００９６】

以下、図１に示したネット決済補助装置１を配布されたクレジットカード契約者である

クレジットカード会員（以下、カード会員という）が、当該ネット決済補助装置１を用いて、通信機能を有するパソコンや携帯電話から、当該カード会員のカード番号を用いた決済により、ネットショッピング等のネットワーク商取引（以下、ネット商取引という）を行なう場合の一実施例について説明する。

【００９７】

本実施例のネット決済システムのシステム構成とネットワーク接続関係を図２のシステム構成図に示す。また、本実施例のネット決済システムにおけるネット商取引のフローを、図３のフローチャートに示す。

【００９８】

尚、本実施例で、ネット決済システムにおけるネット商取引サービスを提供するのは、クレジットカードブランドである。

【００９９】

カード会員は、予め、イシュアに対してクレジットカードの申込みを行い、クレジットカードの発行を受けるとともに、イシュアから、個々のカード会員に固有の認証情報（カード会員がクレジットカード申込み時に登録した暗証番号や指紋情報等の生体情報）、カード情報（個々のカード会員に固有のカード番号、有効期限）、ＯＴＰ生成情報（共通鍵）が格納されたネット決済補助装置１の配布を受けているものとする。

【０１００】

また、本実施例では、図１（ｂ）に示したネット決済補助装置１の構成のうち、ディスプレイ１１とキー操作部１２と駆動用電源１９を除く構成は、ＳＩＭ等のＩＣカードに予め格納されており、筐体１０に設けられたＩＣカードスロット（図示せず）に当該ＩＣカードが挿入されることで、ネット決済補助装置１の機能が実現されるが、必ずしも、ネット決済補助装置がＩＣカードを備えていなくてもよく、ＩＣカードを備えていない場合は、ネット決済補助装置自身が、ＣＰＵやメモリを備えていればよい。

【０１０１】

また、本実施例のネット決済補助装置１は、カード会員の識別情報を用いた決済、すなわち、カード決済、を利用したネット商取引に用いられるものとするが、カード会員が、ネット商取引のみを希望し、従来のプラスチックタイプの磁気カード、ＩＣカード等からなるクレジットカードによるリアルの対面取引を希望しない場合には、クレジットカードの発行は受けなくてもよい。

【０１０２】

また、クレジットカードブランドが、イシュアの業務も行なっているような場合は、クレジットカードブランドから、ネット決済補助装置１が配布されてもよい。

【０１０３】

会員端末２は、契約者の端末であり、カード会員が、ネット決済補助装置１を用いてネット商取引を行なうための端末であり、通信機能とブラウザ表示機能を少なくとも有するパーソナルコンピュータ、携帯電話等の端末である。

【０１０４】

加盟店端末３は、会員端末２に仮想店舗（ウェブサイト）を提供して、商品やサービスの注文を受付けるとともに、注文したカード会員の本人認証をイシュア側に依頼し、カード会員の本人認証が行なわれた後、アクワイアラ（クレジットカードブランドとのライセンス契約に基づき、加盟店の獲得・契約・管理業務を行なう）に対して、オーソリ（注文された商品やサービスの金額分の与信枠がカード会員に残っているかどうかを調べ、与信枠が残っている場合にその金額分を決済用に確保すること）を依頼する端末である。

【０１０５】

アクワイアラ端末４は、加盟店端末３から受けたオーソリ依頼を、イシュア側に再依頼（オーソリ再仕向）する端末である。

【０１０６】

仲介サーバ５は、加盟店端末３と後述の認証サーバ７の仲介役を担う、すなわち、会員端末２と加盟店端末３との間でカード会員の認証サービスを仲介する役割を担うサーバで

ある。

【０１０７】

仲介サーバ５は、本実施例ではクレジットカードブランドが運営するサーバであり、ネット決済補助装置１を用いたネット商取引サービスに対応している加盟店を識別する加盟店識別情報と、ネット決済補助装置１を用いたネット商取引サービスに対応しているイシュアを識別するイシュア識別情報とを格納している。

【０１０８】

尚、本実施例のネット決済システムにおいて、ネット決済補助装置１を用いないネット商取引サービスが混在する場合には、仲介サーバ５は、ネット決済補助装置１を用いたネット商取引サービスに未対応の加盟店及びイシュアの識別情報を、上記加盟店識別情報及びイシュア識別情報と区別して格納している必要がある。

【０１０９】

イシュア端末６は、アクワイアラ端末４から受けたオーソリ依頼を引受け、オーソリを行なう端末である。

【０１１０】

認証サーバ７は、ネット商取引を行なう際に、オーソリに先立ち、カード会員の本人認証を行なうサーバである。本実施例では、認証サーバ７は、イシュアが運営するサーバであり、イシュア端末６に接続されており、ネット決済補助装置１を用いてネット商取引を行なうことが可能なカード会員のカード情報（カード番号、有効期限）及びＯＴＰ生成情報（ネット決済補助装置１に固有の共通鍵）を、互いに関連付けられた状態で格納している。つまり、１カード会員につき、カード情報とＯＴＰ生成情報とが関連付けられて、認証サーバ７に格納されている。

【０１１１】

尚、認証サーバ７へのこれらの情報の格納は、カード会員にネット決済補助装置１を配布するのと同時期、もしくはその前後に行なわれる。

【０１１２】

図２において、会員端末２、加盟店端末３、仲介サーバ５、認証サーバ７間は、それぞれ、インターネット等のネットワーク９ａによって接続されており、加盟店端末３、アクワイアラ端末４、イシュア端末６は、それぞれ専用回線９ｂによって接続されている。

【０１１３】

尚、イシュア端末６及び認証サーバ７は、イシュア毎に個別に用意され、それぞれが会員端末２、アクワイアラ端末４、仲介サーバ５にネットワーク９ａ、専用回線９ｂで接続されることになる。

【０１１４】

また、加盟店端末３も、加盟店毎に個別に用意され、それぞれが会員端末２、仲介サーバ５、アクワイアラ端末４にネットワーク９ａ、専用回線９ｂで接続されることになる。

【０１１５】

以下、図３のフローチャート及び図２のシステム構成図に基づいて、ネット決済補助装置１を用いたネット商取引の流れを説明する。カード会員は、会員端末２から、ネットワーク９ａを介して、仮想店舗（Ｗｅｂサイト）である加盟店端末３にアクセスし、商品やサービスを閲覧する。そして、注文する商品や希望のサービスが決まったら、会員端末２は、加盟店端末３に、注文商品や希望サービスに関してカード決済によるネット商取引を希望する旨を送信する。

【０１１６】

加盟店端末３は、会員端末２に、図４（ａ）に示されるようなカード情報入力画面１００を表示させ、会員端末２に、カード番号及びカードの有効期限を入力して、送信するように依頼する。

【０１１７】

そこで、カード会員が、ネット決済補助装置１のスタートキー１２ｂを押下すると、ネット決済補助装置１の認証手段１４が起動し、ネット決済補助装置１が認証待ち状態とな

る。続けて、カード会員は、本人認証のために必要な入力情報（本実施例では、４桁の暗証番号）をテンキー１２ａから入力する。尚、ここで入力される４桁の暗証番号は、予め、カード会員がカード申込み時に決めておき、既にネット決済補助装置１内の認証情報格納部１５に格納されているものである。

【０１１８】

認証手段１４は、認証情報格納部１５に格納されている認証情報を読み出し、テンキー１２ａから入力された入力情報と一致するかどうか確認する。そして、両者が一致した場合、認証手段１４は、カード情報格納部１３からカード情報としてのカード番号と有効期限を読み出し、ディスプレイ１１に表示する。

【０１１９】

そして、カード番号と有効期限を全てディスプレイ１１に表示し終えると、認証手段１４は、表示し終えた旨を、ＯＴＰ生成手段１６に伝達する。これによって、ＯＴＰ生成手段１６は、後述するワンタイムパスワード生成待ち状態となる。

【０１２０】

尚、本実施例では、ディスプレイ１１の表示可能桁数が８桁に限られているため、認証手段１４は、カード情報格納部１３から読み出したカード番号を上８桁と下８桁とに分割処理した上で、ディスプレイ１１にまず、カード番号の上８桁を表示する。カード会員は、その表示に基づき、カード情報入力画面１００のカード番号入力欄１００ａにカード番号の上８桁を入力する。

【０１２１】

カード番号の上８桁の入力が終わると、カード会員はスタートキー１２ｂを押下する。認証手段１４は、スタートキー１２ｂの押下検出を受けて、カード番号の下８桁をディスプレイ１１に表示する。カード会員は、その表示に基づき、カード情報入力画面１００のカード番号入力欄１００ａにカード番号の下８桁を入力する。

【０１２２】

カード番号の下８桁の入力が終わると、カード会員はスタートキー１２ｂを押下する。認証手段１４は、スタートキー１２ｂの押下検出を受けて、有効期限を４桁（MM（月）／ＹＹ（年））で表示する。カード会員は、その表示に基づき、カード情報入力画面１００の有効期限入力欄１００ｂに、有効期限を入力する。

【０１２３】

尚、ディスプレイの表示領域、表示可能桁数に余裕がある場合には、当然、カード番号が一度に全て、ディスプレイに表示されてもよいし、また、カード番号と有効期限が一度に全て表示されてもよい。また逆に、ディスプレイの表示可能桁数が８桁より少ない場合は、認証手段１４は、表示可能桁数に合わせて、カード情報格納部１３から読み出したカード情報を予め分割しておき、スタートキー１２ｂその他、任意のキーの押下検出により順次、分割されたカード情報を表示してもよい。

【０１２４】

以上のように、ネット決済補助装置１は、入力された入力情報が、認証情報格納部１５に格納されている認証情報と一致した場合にのみ、ディスプレイ１１上にカード情報を表示するので、認証情報を知らなければ、第三者が、ネット決済補助装置１を盗んだとしても、内部のカード情報を知ることが出来ない。従って、カード情報が印字されている従来のクレジットカードに比べて安全性が高く、カード情報をネット商取引に悪用される心配がない。

【０１２５】

カード会員が、カード番号及び有効期限の入力を終えると（尚、図４のカード情報入力画面１００には示されていないが、注文した商品・サービス名、金額、注文日、加盟店名、商品の発送先等の情報が同一画面内に表示されていてもよい）、カード情報入力画面１００内の送信ボタン１００ｃをクリックする。送信ボタン１００ｃがクリックされることにより、加盟店端末３側に、入力されたカード情報が送信される（Ｓ１０）。

【０１２６】

会員端末２から、注文した商品・サービス名、金額、注文日、加盟店名、商品の発送先等に関する注文情報と、注文商品の決済に用いるカードのカード番号や有効期限等のカード情報を受信した加盟店端末３は、受信したカード情報に加え、加盟店毎に付与された加盟店識別情報を、ネットワーク９ａを介して接続された仲介サーバ５に送信し、カード会員がネット決済補助装置１を用いたネット商取引サービスを受けられる会員であるか否かの確認（認証実行可否確認）を要求する（Ｓ２０）。

【０１２７】

仲介サーバ５は、受信した加盟店識別情報が、保有している加盟店識別情報と一致するか否かの確認（加盟店認証）を行なう。これらの情報が一致すれば、ネット決済補助装置１を用いたネット商取引サービスに参加している加盟店の加盟店端末３から仲介サーバ５にアクセスがあったということになる。一致しなければ、ネット決済補助装置１を用いたネット商取引サービスに参加していない加盟店端末３からのアクセスであるか、不正アクセスであるため、以後のフローには進まない。

【０１２８】

仲介サーバ５は、ネット決済補助装置１を用いたネット商取引サービスに参加している加盟店端末３から受信したカード会員のカード情報に基づいて、当該カード会員のカード番号が発行されたイシュアを特定し、特定されたイシュアの認証サーバ７に、カード情報を送信し、カード会員がネット決済補助装置１を用いたネット商取引サービスを受けられる会員であるか否かの確認（認証実行可否確認）を要求する（Ｓ３０）。

【０１２９】

本実施例の仲介サーバ５には、イシュアを識別するイシュア識別情報が格納されており、仲介サーバ５は、受信したカード情報に基づいてイシュア識別情報を検索して、イシュアを特定する。

【０１３０】

つまり、本実施例の仲介サーバ５は、直接、認証実行可否確認を行なうのではなく、加盟店認証を行なうとともに、加盟店端末３から受信したカード情報に基づいて、カード会員のカード番号が発行されたイシュアを特定し、特定されたイシュアの認証サーバ７にカード情報を転送し、当該認証サーバ７から受信した認証実行可否確認結果を加盟店端末３に転送する役割を担っている。

【０１３１】

尚、本実施例では、仲介サーバ５は、クレジットカードブランドが運営しているサーバであるが、これを個々の加盟店端末３が備えていてもよく、その場合は、直接、加盟店端末３から認証サーバ７に、認証実行可否確認が要求されることになる。また、認証サーバ７において、加盟店認証が行なわれてもよい。

【０１３２】

認証サーバ７は、仲介サーバ５から受信したカード情報が認証サーバ７に登録されているか否かを確認することによって、当該カード情報を有するカード会員がネット決済補助装置１を用いたネット商取引サービスを受けられるカード会員であるか否かの確認（認証実行可否確認）を行ない、その結果を、仲介サーバ５に返信する（Ｓ４０）。尚、認証実行可否確認結果は、仲介サーバ５から受信したカード情報が認証サーバ７に登録されていれば「可」であり、登録されていなければ「否」である。

【０１３３】

そして、認証実行可否確認結果を受信した仲介サーバ５は、その結果を加盟店端末３に転送する（Ｓ５０）。

【０１３４】

カード会員の認証実行可否確認結果が「可」である場合には、このカード会員がネット決済補助装置１を用いたネット商取引サービスを受けられるということであるから、加盟店端末３は、このカード会員の本人認証要求を行なうフローに進む（Ｓ６０）。具体的には、加盟店端末３は、会員端末２に対し、認証実行可否結果とともに、先に認証実行可否確認を行なったイシュアの認証サーバ７のＵＲＬ情報を送信する。

【０１３５】
加盟店端末３から認証要求を受けた会員端末２は、受信したＵＲＬに基づき、先に仲介サーバ５がアクセスしたのと同一の認証サーバ７にアクセスし、認証要求を行なう（Ｓ７０）。尚、Ｓ７０のフローは、Ｓ６０から一連の流れとして行なわれ、会員端末２として用いられるパーソナルコンピュータや携帯電話のブラウザが一般的に備えるリダイレクト機能等を用いて実現可能であり、カード会員が意識することなく、会員端末２内部で自動的に処理されるフローである。
【０１３６】
認証サーバ７は、会員端末２に、ワンタイムパスワードの送信を促し、会員端末２から受信したワンタイムパスワードに基づいて、カード会員の認証を行なう（Ｓ８０）。
【０１３７】
具体的には、認証サーバ７は、アクセスしてきた会員端末２から、カード情報及び注文情報を受信して、このカード情報を有するカード会員が、先ほど、加盟店端末３から仲介サーバ５を介して、認証実行可否確認要求を受けたカード会員であるか否かを確認する。この確認は、予め定められた所定時間前に仲介サーバ５から当該カード会員のカード情報を受信したか否かのログを残しておき、会員端末２から受信したカード会員のカード情報が、所定時間前にログに残されたカード情報に一致するか否かを確認することで行なわれる。
【０１３８】
尚、注文情報は、会員端末２からではなく、Ｓ２０，３０のフローにおいて、加盟店端末３から仲介サーバ５を介して認証サーバ７に送信されていてもよいし、加盟店端末３から会員端末２に、認証サーバ７のＵＲＬ情報が送信される際、一緒に送信され、会員端末２が認証サーバ７にアクセスする際に、認証サーバ７に転送されるようになっていてもよい。
【０１３９】
また、認証サーバ７が、アクセスしてきた会員端末２のカード会員と、加盟店端末３から認証実行可否確認要求を受けたカード会員と同一であるか否かの確認は、カード情報の照合のみならず、注文情報を、会員端末２及び加盟店端末３（直接的には仲介サーバ５）の双方から受信して、それらの照合を併用して行なわれてもよい。
【０１４０】
認証サーバ７が、先に認証実行可否確認要求を受けたカード会員のネット決済補助装置１からのアクセスであることを確認したら、認証サーバ７は、受信した注文情報に基づき、図４（ｂ）に示されるようなワンタイムパスワード入力画面１０１を作成し、アクセスのあった会員端末２に送信する。
【０１４１】
図４（ｂ）のワンタイムパスワード入力画面１０１には、カード会員がネット商取引を行なう相手である加盟店名と、注文しようとしている商品・サービスの金額、注文日が、表示されている。
【０１４２】
会員端末２にワンタイムパスワード入力画面１０１が表示されると、カード会員は、ネット決済補助装置１のスタートキー１２ｂを押下する。ネット決済補助装置１のＯＴＰ生成手段１６は、スタートキー１２ｂ押下を検出すると、ワンタイムパスワード生成待ち状態から、ワンタイムパスワード生成フローに移行する。
【０１４３】
ＯＴＰ生成手段１６は、ＯＴＰ生成情報格納部１７に格納された共通鍵を読み出し、計時手段１８によって計時された、スタートキー１２ｂが押下された日時から成る日時データ（年月日秒、秒は３０秒単位）を、この共通鍵で暗号化することでワンタイムパスワードを生成し、これを１０進数にし、ディスプレイ１１に表示する。尚、本実施例の暗号化方式は共通鍵暗号方式を採用している。また、本実施例のディスプレイ１１の表示可能桁数は８桁なので、ディスプレイ１１には生成されたワンタイムパスワードの上６～８桁を

表示することにする。

【０１４４】

カード会員は、会員端末２に表示されたワンタイムパスワード入力画面１０１のパスワード入力欄１０１ａに、ネット決済補助装置１のディスプレイ１１に表示されたワンタイムパスワードを入力し、送信ボタン１０１ｂをクリックすると、入力されたワンタイムパスワードが認証サーバ７に送信される。

【０１４５】

尚、ワンタイムパスワードの入力が終わった後は、カード会員が、ネット決済補助装置１のスタートキー１２ｂを再押下することで、ネット決済補助装置１のディスプレイ１１に表示されているワンタイムパスワードを非表示とすることがセキュリティの観点から望ましい。また同時に、電源もオフされるのが、省エネの観点から望ましい。

【０１４６】

会員端末２からワンタイムパスワードを受信した認証サーバ７は、まず、この会員端末２が、先に、ワンタイムパスワードの送信を要求した相手であることを、会員端末２の識別番号等の照合や、当該会員端末２個別に生成されて送信されたワンタイムパスワード入力画面１０１に対する返信か否かの確認により、確認する。

【０１４７】

確認後、認証サーバ７は、ワンタイムパスワードの送信を要求する前に受信していたカード会員のカード情報に基づき、ＯＴＰ生成情報の中から、このカード番号に関連付けて登録されている共通鍵を取出し、認証サーバ７が会員端末２からワンタイムパスワードを受信した日時からなる日時データ（年月日秒、秒は３０秒単位）を、この共通鍵で暗号化してワンタイムパスワードを生成し、これを十進数に変換する。尚、本実施例の暗号化方式は、共通鍵暗号方式を採用している。

【０１４８】

このようにして認証サーバ７は、認証サーバ７で生成されたワンタイムパスワードと、先に会員端末２から受信したワンタイムパスワードとが、一致するか否かを確認する。一致すれば、このワンタイムパスワードは、確かに、ネット決済補助装置１と認証サーバ７のみに格納された共通鍵によって、ほぼ同時刻に作成されたワンタイムパスワードであることが証明される。

【０１４９】

つまり、ワンタイムパスワードを認証サーバ７に送信した会員端末２の操作者が、当該ワンタイムパスワードの生成に用いられた共通鍵及び、当該共通鍵に関連付けられたカード情報が格納されたネット決済補助装置１の操作者であり、かつ、当該カード情報を利用可能なカード会員本人であり、これによって、ネット商取引を依頼してきたカード会員の本人確認がされたことになる。

【０１５０】

尚、ワンタイムパスワード生成方式が、本実施例のように時間同期方式を採用している場合、ネット決済補助装置１がワンタイムパスワード生成に用いる日時と、認証サーバ７がワンタイムパスワード生成に用いる日時とは、厳密には同じにならず、よって、認証サーバ７がワンタイムパスワードを生成してから、カード会員が、ネット決済補助装置１のスタートキー１２ｂを押下して、ネット決済補助装置１がワンタイムパスワードを生成するまでの時間差を考慮して、本実施例では、日時データの秒分解能を３０秒としている。

【０１５１】

しかし、両者によって生成されたワンタイムパスワードが完全に一致しない限り、カード会員の真正性を認めないというのでは、カード会員がネット決済補助装置１のスタートキー１２ｂを押下してワンタイムパスワードが生成されてから、認証サーバ７が、会員端末２からワンタイムパスワードを受信するまでの間、３０秒以上経過してしまった場合に、それだけで、ワンタイムパスワードが不一致となり、認証されないという事態が増え、かえってネット商取引の利便性が損なわれることになってしまう。

【０１５２】

従って、認証サーバ７は、会員端末２から受信したワンタイムパスワードが一致しなかった場合でも、会員端末２からワンタイムパスワードを受信した日時を、前後Ｎ回×３０秒分ずらして、認証サーバ７側でワンタイムパスワードを生成し直して、会員端末２側で生成されたワンタイムパスワードと一致すれば、カード会員の本人確認がされたものとする。

【０１５３】

尚、Ｎは、セキュリティ精度を考慮して、予め決定しておく。すなわち、セキュリティ精度を高くしたい時は、Ｎを小さく設定し、セキュリティ精度を低くしてカード会員側の利便性を優先したい場合は、Ｎを大きく設定しておく。

【０１５４】

認証サーバ７は、ワンタイムパスワード照合によるカード会員の認証結果を、会員端末２に送信する（Ｓ９０）。尚、具体的には、認証サーバ７は、会員端末２に対し、認証結果に加え、加盟店端末３のＵＲＬ情報を送信し、会員端末２から加盟店端末３に認証結果が転送されるようにしておく。

【０１５５】

認証結果を受信した会員端末２は、当該認証結果（本人認証ＯＫ、本人認証ＮＧ）を更に、加盟店端末３に転送する（Ｓ１００）。尚、Ｓ１００のフローは、Ｓ７０同様、Ｓ９０から一連の流れとして行なわれ、会員端末２のブラウザのリダイレクト機能によって実現可能であり、実際には、カード会員が意識することなく、会員端末２内部で自動的に処理されるフローである。

【０１５６】

加盟店端末３は、会員端末２から認証結果を受信し、認証の結果、カード会員の本人確認がされた場合（本人認証ＯＫ）には、アクワイアラに、当該カード会員のオーソリ要求をするため、アクワイアラ端末４に、カード会員のカード情報と、決済希望金額（カード会員が注文しようとしている商品・サービスの金額）からなる取引データに加え、当該認証結果を送信する（Ｓ１１０）。尚、取引データは、Ｓ１０で、会員端末２から、注文情報とカード情報の送信があった時点で既に生成されて、加盟店端末３に記憶されたものが、読み出されてもよい。

【０１５７】

アクワイアラ端末４は、加盟店端末３から受信した取引データと認証結果に基づき、本人認証ＯＫのカード会員のカード番号に基づいて、カード発行元であるイシュアを特定し、特定されたイシュアのイシュア端末６に、取引データと認証結果を転送する（Ｓ１２０）。

【０１５８】

取引データと認証結果を受信したイシュア端末６は、図示しない会員データベースに格納されている会員毎の会員情報や与信情報に基づいて、取引データに含まれる決済希望金額が、オーソリを依頼されたカード会員の与信枠の範囲内か否かを確認する。決済希望金額が与信枠の範囲内であれば、オーソリＯＫとして、決済希望金額分の与信枠を確保する。

【０１５９】

そして、イシュア端末６は、オーソリの結果（オーソリＯＫ、オーソリＮＧ）をアクワイアラ端末４に送信し（Ｓ１３０）、更に、アクワイアラ端末４は、加盟店端末３に、オーソリ結果を転送する（Ｓ１４０）。

【０１６０】

そして、加盟店端末３は、アクワイアラ端末４からオーソリ結果を受信した後、その結果を会員端末２に通知する（Ｓ１５０）。具体的には、オーソリ結果がＯＫだった場合には、加盟店とカード会員との間で、当該カード会員のカード番号を用いた決済によるネット商取引が成立した旨の画面を会員端末２に送信し、会員端末２に表示する。またオーソリ結果がＮＧだった場合には、ネット商取引が不成立の旨の画面を会員端末２に送信、表示する。

【０１６１】
尚、本実施例では、認証サーバ７におけるワンタイムパスワードを用いた本人認証は、会員端末２と加盟店端末３との間でネット商取引が行なわれる都度、行なわれる。つまり、本実施例のＯＴＰ生成手段１６で生成されるワンタイムパスワードは、１回限りのネット商取引に有効なものであるから、仮にネット決済補助装置を所持していない第三者がワンタイムパスワードを盗聴しても、第三者が、カード会員になりすまして以降のネット商取引を行なうことは出来ず、ネット商取引の安全性が更に向上する。
【実施例２】
【０１６２】
次に、ネット決済補助装置１ａ（図示せず）を配布されたカード会員が、当該ネット決済補助装置１ａを用いて、通信機能を有するパソコンや携帯電話から、当該カード会員のカード番号を用いた決済により、ネット商取引を行なう場合の一実施例について説明する。
【０１６３】
先の実施例１と、本実施例との相違点は、ネット決済補助装置が備えるＯＴＰ生成手段１６のワンタイムパスワード生成方法と、ＯＴＰ生成情報格納部１７の格納内容と、図３における会員端末２と認証サーバ７（本実施例では認証サーバ７ａとする）との間の認証フロー（Ｓ８０，Ｓ９０）の内容である。
【０１６４】
すなわち、先の実施例１では、ワンタイムパスワード生成方法を、時間同期方式としていたが、本実施例では、利用回数同期方式を採用する。これに伴い、本実施例のネット決済補助装置１ａにおいては、図１に記載されていた計時手段１８が、計数手段１８ａ（図示せず）に代わる。
【０１６５】
ネット決済補助装置１，１ａと認証サーバ７，７ａに関し、上述した相違点以外の構成及び、Ｓ８０，Ｓ９０以外のフローについては、図１～図３に示された実施例と同一であるので、以下、図１～図３を用いて、図３のＳ８０，Ｓ９０の部分のみの詳細フローを説明する。
【０１６６】
本実施例のＯＴＰ生成情報格納部１７に格納されるＯＴＰ生成情報は、ネット決済補助装置１ａに固有の共通鍵と、利用回数情報とから構成される。
【０１６７】
このうち、共通鍵は、ＯＴＰ生成情報格納部１７内に書き換え不可能な状態で格納され、ＯＴＰ生成手段１６で生成されたワンタイムパスワードの検証を行なう認証サーバ７ａにおいて、カード情報格納部１３に格納されているカード番号と関連付けられている。
【０１６８】
利用回数情報は、共通鍵同様、認証サーバ７ａにおいて、カード情報格納部１３に格納されているカード番号と関連付けられている。
【０１６９】
つまり、これらのＯＴＰ生成情報は、カード番号と関連付けられた状態で、認証サーバ７ａにも格納されており、認証サーバ７ａが会員端末２からワンタイムパスワードを受信した際、会員端末２同様、認証サーバ７ａでもワンタイムパスワードを生成して、これらが一致するかどうかを確認することによって、ワンタイムパスワードの妥当性検証、カード会員の認証を行なう。
【０１７０】
また、利用回数情報は、ＯＴＰ生成手段１６からの書き換え指令があった場合のみ、書き換えが可能な情報であり、計数手段１８ａによって、０回、１回、２回というように１ずつ加算されるか又は、１００回、９９回、９８回というように、１ずつ減算された後、加算又は減算後の数値が、ＯＴＰ生成情報格納部１７に格納されて、利用回数情報が更新される。尚、加算か減算かは、予め決められている。

【０１７１】
尚、計数手段１８ａは、ＯＴＰ生成手段１６に含まれていてもよいし、ＯＴＰ生成手段１６と別に設けられていてもよいが、後者の場合は、ＯＴＰ生成手段１６が計数手段１８ａを制御して、利用回数情報の書き換えが行なわれる必要がある。
【０１７２】
図３のＳ８０において、まず、認証サーバ７ａは、会員端末２に、ワンタイムパスワードの送信を促し、会員端末２から受信したワンタイムパスワードに基づいて、カード会員の認証を行なう。
【０１７３】
具体的には、認証サーバ７ａは、アクセスしてきた会員端末２から、カード情報及び注文情報を受信して、このカード情報を有するカード会員が、先ほど、加盟店端末３から仲介サーバ５を介して、認証実行可否確認要求を受けたカード会員であるか否かを確認する。この確認は、予め定められた所定時間前に仲介サーバ５から当該カード会員のカード情報を受信したか否かのログを残しておき、会員端末２から受信したカード会員のカード情報が、所定時間前にログに残されたカード情報に一致するか否かを確認することで行なわれる。
【０１７４】
尚、注文情報は、会員端末２からではなく、Ｓ２０，３０のフローにおいて、加盟店端末３から仲介サーバ５を介して認証サーバ７ａに送信されていてもよいし、加盟店端末３から会員端末２に、認証サーバ７ａのＵＲＬ情報が送信される際、一緒に送信され、会員端末２が認証サーバ７ａにアクセスする際に、認証サーバ７ａに転送されるようになっていてもよい。
【０１７５】
また、認証サーバ７ａが、アクセスしてきた会員端末２のカード会員と、加盟店端末３から認証実行可否確認要求を受けたカード会員と同一であるか否かの確認は、カード情報の照合のみならず、注文情報を、会員端末２及び加盟店端末３（直接的には仲介サーバ５）の双方から受信して、それらの照合を併用して行なわれてもよい。
【０１７６】
認証サーバ７ａが、先に認証実行可否確認要求を受けたカード会員のネット決済補助装置１からのアクセスであることを確認したら、認証サーバ７ａは、受信した注文情報に基づき、図４（ｂ）に示されるようなワンタイムパスワード入力画面１０１を作成し、アクセスのあった会員端末２に送信する。
【０１７７】
図４（ｂ）のワンタイムパスワード入力画面１０１には、カード会員がネット商取引を行なう相手である加盟店名と、注文しようとしている商品・サービスの金額、注文日が、表示されている。
【０１７８】
会員端末２にワンタイムパスワード入力画面１０１が表示されると、カード会員は、ネット決済補助装置１のスタートキー１２ｂを押下する。ネット決済補助装置１のＯＴＰ生成手段１６は、スタートキー１２ｂ押下を検出すると、ワンタイムパスワード生成待ち状態から、ワンタイムパスワード生成フローに移行する。
【０１７９】
ＯＴＰ生成手段１６は、ＯＴＰ生成情報格納部１７に格納された共通鍵と利用回数情報を読み出し、当該利用回数情報を、共通鍵で暗号化してワンタイムパスワードを生成し、これを１０進数にし、ディスプレイ１１に表示する。
【０１８０】
尚、本実施例では、利用回数情報を所定のワンタイムパスワード生成アルゴリムを用いて、ワンタイムパスワードを生成している。
【０１８１】
また、本実施例のディスプレイ１１の表示可能桁数は８桁なので、ディスプレイ１１に

は生成されたワンタイムパスワードの上６～８桁を表示することにする。

【０１８２】

尚、ＯＴＰ生成情報は、上記の利用回数情報と共通鍵の他に、その他、ネット決済補助装置１ａと認証サーバ７ａの両者しか知り得ない任意の情報（例えば、ポリシー等）を含んでいてもよく、その場合、利用回数情報と、当該任意の情報が、共通鍵で暗号化され、ワンタイムパスワードが生成されてもよい。

【０１８３】

ＯＴＰ生成手段１６は、ワンタイムパスワードを生成した後、計数手段１８ａに、先に読み出した利用回数情報を１、加算又は減算させて、ＯＴＰ生成情報格納部１７の利用回数情報を書き換え、更新する。

【０１８４】

カード会員は、会員端末２に表示されたワンタイムパスワード入力画面１０１のパスワード入力欄１０１ａに、ネット決済補助装置１のディスプレイ１１に表示されたワンタイムパスワードを入力し、送信ボタン１０１ｂをクリックすると、入力されたワンタイムパスワードが認証サーバ７ａに送信される。

【０１８５】

尚、ワンタイムパスワードの入力が終わった後は、カード会員が、ネット決済補助装置１のスタートキー１２ｂを再押下することで、ネット決済補助装置１のディスプレイ１１に表示されているワンタイムパスワードを非表示とすることがセキュリティの観点から望ましい。また同時に、電源もオフされるのが、省エネの観点から望ましい。

【０１８６】

会員端末２からワンタイムパスワードを受信した認証サーバ７ａは、まず、この会員端末２が、先に、ワンタイムパスワードの送信を要求した相手であることを、会員端末２の識別番号等の照合や、当該会員端末２個別に生成されて送信されたワンタイムパスワード入力画面１０１に対する返信か否かの確認により、確認する。

【０１８７】

確認後、認証サーバ７ａは、ワンタイムパスワードの送信を要求する前に受信していたカード会員のカード情報に基づき、ＯＴＰ生成情報の中から、このカード番号に関連付けて登録されている共通鍵と利用回数情報を取出し、利用回数情報を共通鍵で暗号化してワンタイムパスワードを生成し、これを十進数に変換する。

【０１８８】

尚、本実施例では、利用回数情報を所定のワンタイムパスワード生成アルゴリムを用いて、ワンタイムパスワードを生成している。また、ＯＴＰ生成情報に、任意の情報が含まれていれば、利用回数情報に加え、当該任意の情報も合わせて共通鍵で暗号化する。

【０１８９】

このようにして、認証サーバ７ａは、認証サーバ７ａで生成されたワンタイムパスワードと、先に会員端末２から受信したワンタイムパスワードとが、一致するか否かを確認する。一致すれば、このワンタイムパスワードは、確かに、ネット決済補助装置１と認証サーバ７ａのみに格納された利用回数情報と共通鍵とによって作成されたワンタイムパスワードであることが証明される。

【０１９０】

つまり、ワンタイムパスワードを認証サーバ７ａに送信した会員端末２の操作者が、当該ワンタイムパスワードの生成に用いられた利用回数情報と共通鍵及び、当該共利用回数情報と通鍵に関連付けられたカード情報が格納されたネット決済補助装置１の操作者であり、かつ、当該カード情報を利用可能なカード会員本人であり、これによって、ネット商取引を依頼してきたカード会員の本人確認がされたことになる。

【０１９１】

認証サーバ７ａは、ワンタイムパスワード照合によるカード会員の認証結果（本人認証ＯＫ、本人認証ＮＧ）を、会員端末２に送信するとともに、先のワンタイムパスワード生成に用いた利用回数情報を、予め決められた演算方法により加算又は減算し、その演算結

果を認証サーバ７ａ内の利用回数情報として書き換え、更新する（Ｓ９０）。
【０１９２】
尚、ワンタイムパスワード生成方式が、本実施例のように利用回数同期方式を採用している場合、会員端末２及びネット決済補助装置１ａの操作者が正当なカード会員であったとしても、ネット決済補助装置１ａがワンタイムパスワード生成に用いる利用回数情報と、認証サーバ７ａがワンタイムパスワード生成に用いる利用回数情報とが異なり、ワンタイムパスワードが一致しない場合がある。
【０１９３】
カード会員が、ネット決済補助装置１ａでワンタイムパスワードを生成しても、それが必ず、認証サーバ７ａに送信される保証はなく、カード会員が、ネット商取引を途中で中断してしまう場合や、また、そもそもネット商取引を行なっていないにもかかわらず、ネット決済補助装置１ａを操作して、いたずらにワンタイムパスワードを生成してしまうことがある。そのような場合には、ネット決済補助装置１ａの利用回数情報は更新されるのに、認証サーバ７ａの利用回数情報は更新されないので、当然、生成されるワンタイムパスワードも異なるものになってしまう。
【０１９４】
しかし、両者によって生成されたワンタイムパスワードが完全に一致しない限り、カード会員の真正性を認めないというのでは、認証ＮＧが増え、かえってネット商取引の利便性が損なわれることになってしまう。
【０１９５】
従って、認証サーバ７ａは、会員端末２から受信したワンタイムパスワードが一致しなかった場合でも、認証サーバ７ａに格納されている利用回数情報を所定範囲（例えば、利用回数情報＋Ｎ）で変更して、認証サーバ７ａ側でワンタイムパスワードを生成し直して、会員端末２側で生成されたワンタイムパスワードと一致すれば、カード会員の本人確認がされたものとする。
【０１９６】
尚、Ｎは、セキュリティ精度を考慮して、予め決定しておく。すなわち、セキュリティ精度を高くしたい時は、Ｎを小さく設定し、セキュリティ精度を低くしてカード会員側の利便性を優先したい場合は、Ｎを大きく設定しておく。
【０１９７】
以上のように、本発明のネット決済補助装置を用いてネット商取引を行なうと、カード情報をカード情報入力画面に入力する際、ネット決済補助装置に入力された入力情報が、ネット決済補助装置に格納されている認証情報と一致しなければ、カード会員自身であってもカード情報を知ることが出来ないので、カード情報が露出している従来のクレジットカードと異なり、カード情報の秘匿性が高まり、ネット商取引におけるカード情報の不正使用が防止される。
【０１９８】
また、ネット決済補助装置は可搬型であるので、カード会員がどこにいても、携帯電話、自宅のパソコン、出先のパソコンを用いて、安全なネット商取引を行なうことが出来、ネット商取引の利便性が増す。
【０１９９】
また、ネット商取引が行なわれる際のカード会員の本人認証は、ネット決済補助装置で生成されるワンタイムパスワードと、認証サーバで生成されるワンタイムパスワードとが一致するか否かによって行なわれる。
【０２００】
このワンタイムパスワードは、ネット決済補助装置に固有で、ネット決済補助装置及び認証サーバのみに格納され、かつ、カード会員自身でさえも知ることが出来ない共通鍵を用いて、所定キーの押下が検出された日時からなる日時データもしくはワンタイムパスワードの生成都度、更新される利用回数情報を暗号化したものである。
【０２０１】

つまりは、ネット決済補助装置を操作しているカード会員のみが作成可能な認証情報であるから、ネット決済補助装置を所持していない第三者が、カード会員になりすましてネット商取引を行なうことは出来ず、ネット商取引の安全性が更に向上する。

【０２０２】

しかも、このワンタイムパスワードの生成は、ネット決済補助装置にカード情報が表示された後でなければ、行なわれないようになっているので、ネット決済補助装置を有していない第三者は、カード番号のみを知っていても、ワンタイムパスワードの生成が出来ない。また、第三者がネット決済補助装置を盗んだとしても、ネット決済補助装置に入力する認証情報がなければ、ワンタイムパスワードの生成が出来ない。つまり、第三者は、ネット決済補助装置の入手有無にかかわらず、カード会員になりすましたネット商取引を行なうことが出来ないので、ネット商取引の安全性が保証される。

【０２０３】

尚、ワンタイムパスワードの生成方法は、上記実施例の時間同期方式に限らず、ネット決済補助装置と認証サーバとの間で、ネット決済補助装置を所有するカード会員の本人認証が行える方式であればよい。

【０２０４】

また、ネット決済補助装置は、ネット非接続型の構成を採用しているから、一度、ネット決済補助装置に格納されたカード情報、認証情報、ＯＴＰ生成情報は、不正アクセス等により読み出すことが出来ず、ネット決済補助装置を配布されたカード会員さえもが読み出すことが出来ないようになっている。

【０２０５】

仮に、ネット決済補助装置が、パーソナルコンピュータや携帯電話等の端末に接続可能であるとすると、ネット決済補助装置と端末を接続中に、何らかの不具合が発生した場合、不具合の原因が、ネット決済補助装置側にあるのか、端末側にあるのかという責任分解点が不明確となる。従って、ネット非接続型の構成を採用しているネット決済補助装置は、責任分解点が明確となる意味でも、有効である。

【０２０６】

ここで、ネット決済補助装置を持たないカード会員が、本実施例のネット決済システムで、ネット商取引を行なう場合の事前登録のシステム構成及びフローを図６に示す。

【０２０７】

カード会員は、会員ＰＣから、カード会社（クレジットカードブランド又はイシュア）が運営するカード会員向けのＷＥＢサイトにアクセスし、カード会員だけが知る会員情報（生年月日、電話番号、口座番号等）を入力して、ＷＥＢサイトに送信する（図６中、（１））。

【０２０８】

会員情報を受信したカード会社のＷＥＢサイトは、当該会員情報が登録されているカード会社の基幹システムにアクセスし、受信した会員情報と、基幹システムに登録されている会員情報との照合を基幹システムに依頼する（図６中、（２））。基幹システムは、ＷＥＢサイトに照合結果を返信する（図６中、（３））。

【０２０９】

照合結果がＯＫであれば、カード会員の本人確認が行なわれたものとし、ＷＥＢサイトから、会員ＰＣに、パスワードの登録を要求する。会員ＰＣは、パスワードをＷＥＢサイトに送信する（図６中、（４））。

【０２１０】

会員ＰＣからパスワードを受信したＷＥＢサイトは、当該パスワードをカード会社の認証サーバ７に登録する（図６中、（５））。

【０２１１】

ここで登録されるパスワードは、固定パスワードであり、ネット決済補助装置で生成されるようなワンタイムパスワードではない。つまり、ネット決済補助装置を持たないカード会員が、ネット決済システム上でネット決済を行なう場合の、カード会員の認証方法は

、固定パスワードによる方法しかなく、カード番号と固定パスワードが第三者に一度知られてしまうと、以後は、第三者がカード会員になりすましてネット決済を行なうことが可能となってしまう。

【０２１２】

また、ネット決済補助装置を持たないカード会員は、パスワードを登録するために、カード会社のＷＥＢサイトにアクセスして、本人認証を経た後にパスワード登録作業を行なわなければならず、カード会員側の負担が大きい。

【０２１３】

更に、カード会員のみならず、カード会社側においても、パスワードをカード会員に登録させるためのＷＥＢサイトの構築、カード会員の本人認証を行なうための基幹システムの構築が必要となる。

【０２１４】

また、ネット決済補助装置は、通常、カード番号が露出しておらず、カード会員のみが知り得るもしくは、カード会員のみが有する認証情報の入力がなければ、カード番号が表示されない構成となっており、更に、ネット決済の際に、カード会員の本人認証に用いられるパスワードは、固定パスワードではなく、ワンタイムパスワードであるので、第三者がカード会員になりすましてネット商取引を行なうことは極めて困難となる。

【０２１５】

以上、ネット決済補助装置１の実施例につき説明したが、本発明のネット決済補助装置は、上記実施例で説明した構成要件の全てを備えたネット決済補助装置１に限定されるものではなく、各種の変更及び修正が可能であり、個々の目的実現に必要な構成要件を任意に組み合わせて、本発明のネット決済補助装置を構成することが可能である。又、かかる変更及び修正についても本発明の特許請求の範囲に属することは言うまでもない。

【０２１６】

例えば、実施例では、クレジットカードのカード番号を用いたネット決済について説明したが、少なくともカード番号によってネット決済を行なうことが可能なカードであれば、クレジットカード以外に、デビットカード等のカードによる実施例も、本発明の特許請求の範囲に属する。

【０２１７】

また、本実施例では、カード決済を利用したネット商取引に用いられるものとしたが、カード会員が、ネット商取引のみを希望し、従来のプラスチックタイプの磁気カード、ＩＣカード等からなるクレジットカードによるリアルの対面取引を希望しない場合には、クレジットカードの発行は受けなくてもよく、本発明のネット決済補助装置の所有者が、従来のプラスチックタイプのクレジットカードを必ずしも有している必要はない。

【０２１８】

また、例えば、実施例では、１のネット決済補助装置１のカード情報格納部１３に、１種類のカード情報を有する１カード会員のカード情報を格納し、認証情報格納部１５に１種類の認証情報を格納した場合を説明したが、複数のカード番号がカード情報格納部１３に格納されてもよい。その場合の認証情報は、複数のカード番号を表示するために共通の認証情報であってもよいし、カード番号と認証情報がそれぞれ対応し、入力された認証情報によって、ディスプレイ１１に表示されるカード番号が異なるようになっていてもよい。

【０２１９】

また、親子クレジットカード等、同一又は複数のカード番号を、複数人が使用する場合は、それぞれの人によって異なる認証情報が認証情報格納部１５に格納されていてもよいし、共通の認証情報が格納されていてもよい。

【０２２０】

また、上記実施例においては、カード情報とＯＴＰ生成情報が、ネット決済補助装置１，１ａ及び認証サーバ７，７ａで、それぞれ、関連付けられている旨を述べたが、カード情報の盗聴を防止するため、カード情報とＯＴＰ生成情報が、直接的ではなく間接的に関

連付けられていても、特許請求の範囲に含まれるものとする。

【０２２１】

具体的には、図３のＳ１０において会員端末２で入力されたカード情報が、Ｓ２０，３０で、加盟店端末３、仲介サーバ５を経由して、最終的に認証サーバ７，７ａに送信されることになるが、認証サーバ７，７ａはこの際、受信したカード情報のうち、カード番号を、当該カード番号とは異なるユニークな番号に変換して、仲介サーバ５を経由して、加盟店端末３に送信する（Ｓ４０，５０において）。

【０２２２】

更に、このユニークな番号は、加盟店端末２から会員端末２に送信され、会員端末２を経由して認証サーバ７，７ａに送信される（Ｓ６０，７０において）。

【０２２３】

当該ユニークな番号を受信した認証サーバ７，７ａは、最初にカード番号をユニークな番号に変換したのとは逆の変換ルールによって、ユニークな番号をカード番号に変換し、変換されたカード番号に関連付けられているＯＴＰ生成情報をワンタイムパスワードの生成に用いることになる。

【０２２４】

このように、カード番号とカード番号以外のユニークな番号とＯＴＰ生成情報とが関連付けられることによって、Ｓ１０，Ｓ２０，Ｓ３０でカード番号が送信される以外は、ネットワーク９ａ上を、カード番号が流れることがないので、カード番号を盗聴される可能性が大幅に下がり、セキュリティ向上に寄与する。

【０２２５】

また、上記実施例では、会員端末２が加盟店端末３にカード情報を送信し、認証サーバ７，７ａが、加盟店端末３からの依頼に基づき、図２のＳ８０においてカード会員の本人認証を行なう場合について説明したが、本発明は必ずしもこれに限らない。

【０２２６】

例えば、先に会員端末２が認証サーバ７，７ａにアクセスして、認証サーバ７，７ａがカード会員専用の認証情報入力画面を会員端末２に送信し、当該認証入力画面に入力されたカード情報とワンタイムパスワードに基づいて、会員端末２と認証サーバ７，７ａとの間でカード会員の本人認証を行なっておき、その結果、本人と確認されて以降、所定条件（例えば、所定時間、所定回数、所定加盟店等）内で、会員端末２が、加盟店端末３のウェブサイトにアクセスして、ネット商取引を行えるようになっていてもよい。

【０２２７】

つまり、本発明のネット決済補助装置は、会員端末２と、カード会社側の認証サーバ７，７ａとの間で、カード会員の本人認証に用いられ、認証後、実際に加盟店のウェブサイト等においてネット商取引が出来るようになることを基本としており、必ずしも、加盟店端末２からの本人認証依頼を前提としているものではない。

【０２２８】

本発明に於ける各手段、データベースは、その機能が論理的に区別されているのみであって、物理上あるいは事実上は同一の領域を為していても良い。又データベースの代わりにデータファイルであっても良いことは言うまでもなく、データベースとの記載にはデータファイルをも含んでいる。

【０２２９】

上記実施例では、ネット決済システム上の端末やサーバが、クレジットカードブランド（ネット商取引サービスの提供主体）、イシュア（カード会員の獲得・カード会員へのカード発行主体）、アクワイアラ（加盟店の獲得・契約・管理主体）、加盟店のそれぞれが運営するものである旨を説明したが、これらは全て概念上・役割上、区別されるものであり、物理的には、イシュアとアクワイアラが同一である場合もあるし、また、クレジットカードブランド、イシュア、アクワイアラが同一である場合もある。

【０２３０】

従って、例えば、本明細書において、ネット決済補助装置１，１ａは、イシュアから配

布されることに限定されるものではない。また、必ずしもネット決済システムの提供主体がクレジットカードブランドである必要もない。また、イシュア端末６と認証サーバ７，７ａとアクワイアラ端末４が同一であってもよい。また、仲介サーバ５が、その他の端末やサーバのいずれかと同一であってもよい。

【０２３１】

尚、本発明を実施するにあたり本実施態様の機能を実現するソフトウェアのプログラムを記録した記憶媒体をシステムに供給し、そのシステムのコンピュータが記憶媒体に格納されたプログラムを読み出し実行することによっても実現される。

【０２３２】

この場合、記憶媒体から読み出されたプログラム自体が前記した実施態様の機能を実現することとなり、そのプログラムを記憶した記憶媒体は本発明を構成する。

【０２３３】

プログラムを供給する為の記憶媒体としては、例えば磁気ディスク、ハードディスク、光ディスク、光磁気ディスク、磁気テープ、不揮発性のメモリカード等を使用することができる。

【０２３４】

又、コンピュータが読み出したプログラムを実行することにより、上述した実施態様の機能が実現されるだけではなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているオペレーティングシステムなどが実際の処理の一部又は全部を行い、その処理によって前記した実施態様の機能が実現される場合も本発明に含まれる。

【０２３５】

更に、記憶媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わる不揮発性あるいは揮発性の記憶手段に書き込まれた後、そのプログラムの指示に基づき、機能拡張ボードあるいは機能拡張ユニットに備わる演算処理装置などが実際の処理の一部あるいは全部を行い、その処理により前記した実施態様の機能が実現される場合も本発明に含まれる。

【図面の簡単な説明】

【０２３６】

【図１】本発明のネット決済補助装置の外観及び電気的ハードウェア構成を示す構成図である。

【図２】ネット決済補助装置を用いたネット決済システムの概略接続構成図である。

【図３】ネット決済システムにおけるネット商取引のプロセスフローの一例を示す図である。

【図４】ネット決済システムにおけるネット商取引のプロセスフローにおいて、会員端末に表示される画面の一例を示す図である。

【図５】ネット決済補助装置の操作手順及びディスプレイ画面遷移を示す図である。

【図６】ネット決済補助装置を用いないネット決済システムをカード会員が利用するに際し、事前に、カード会員の本人認証のためのパスワードを登録するために必要なシステムの概略接続構成図である。

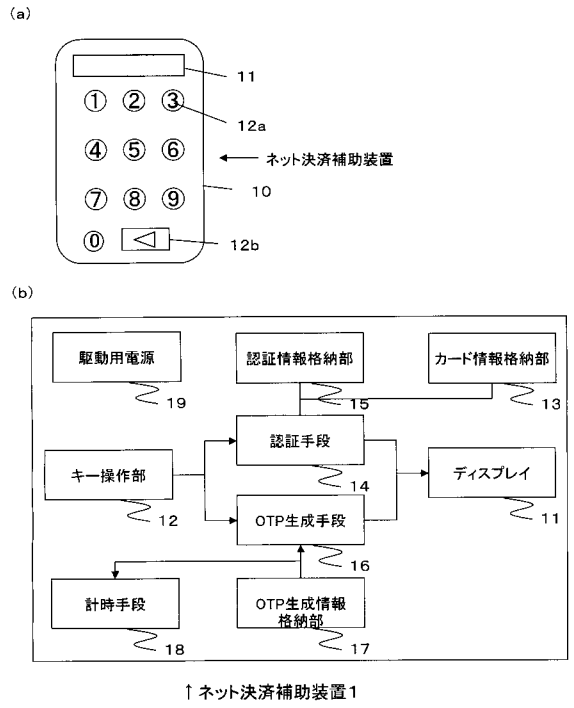
【符号の説明】

【０２３７】

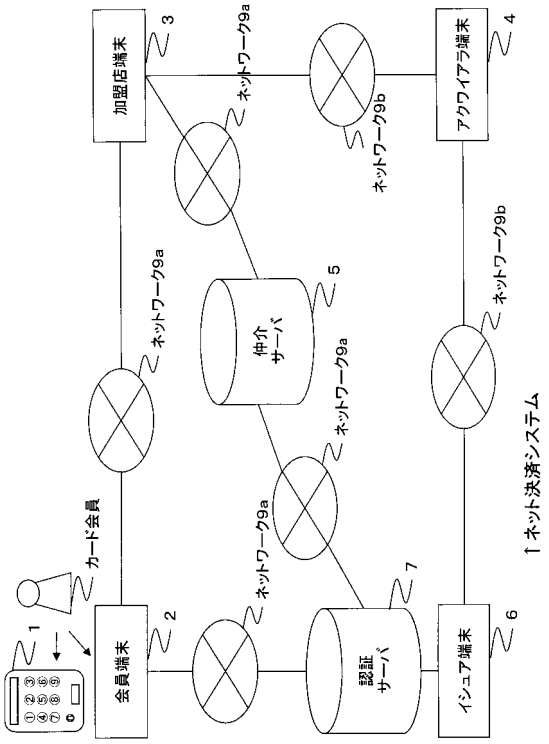
１：ネット決済補助装置
１０：筐体
１１：ディスプレイ
１２：キー操作部
１２ａ：テンキー
１２ｂ：スタートキー
１３：カード情報格納部
１４：認証手段
１５：認証情報格納部

１６：ＯＴＰ生成手段
１７：ＯＴＰ生成情報格納部
１８：計時手段
１９：駆動用電源
２：会員端末
３：加盟店端末
４：アクワイアラ端末
５：仲介サーバ
６：イシュア端末
７：認証サーバ
９ａ：ネットワーク
９ｂ：専用回線

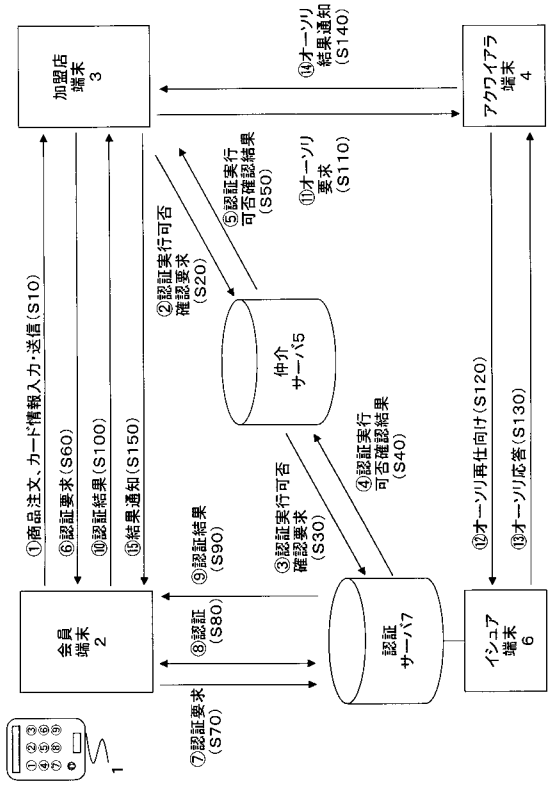
【図１】



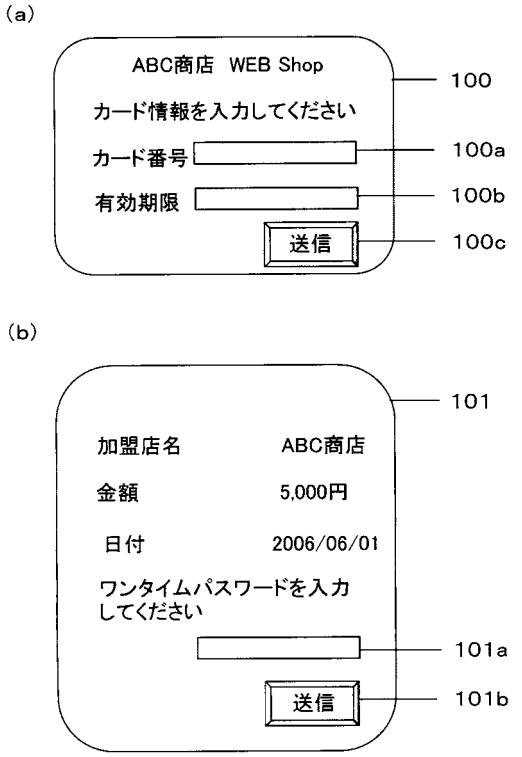
【図２】



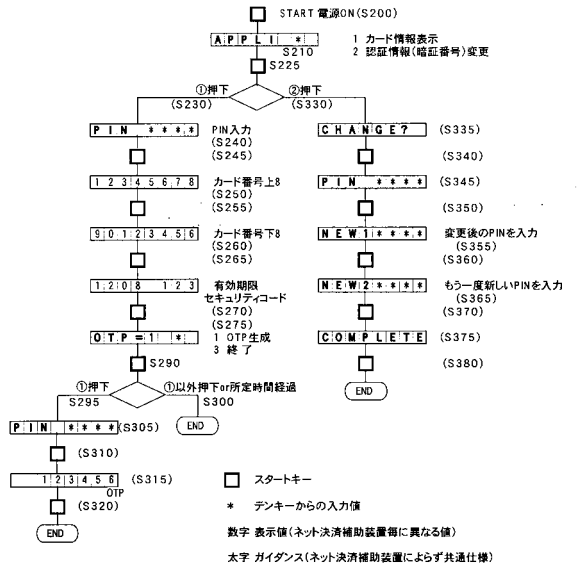
【図３】


加盟店端末 3
アクワイアラ端末 4
④オーソリ結果通知 (S140)
⑤認証実行可否確認結果 (S50)
①オーソリ要求 (S110)
②認証実行可否確認要求 (S20)
仲介サーバ5
①商品注文、カード情報入力・送信(S10)
⑥認証要求(S60)
⑩認証結果(S100)
⑮結果通知(S150)
⑨認証結果 (S90)
③認証実行可否確認要求 (S30)
④認証実行可否確認結果 (S40)
⑫オーソリ再仕向け(S120)
⑬オーソリ応答(S130)
会員端末 2
⑧認証 (S80)
認証サーバ7
イシュア端末 6
⑦認証要求 (S70)
1

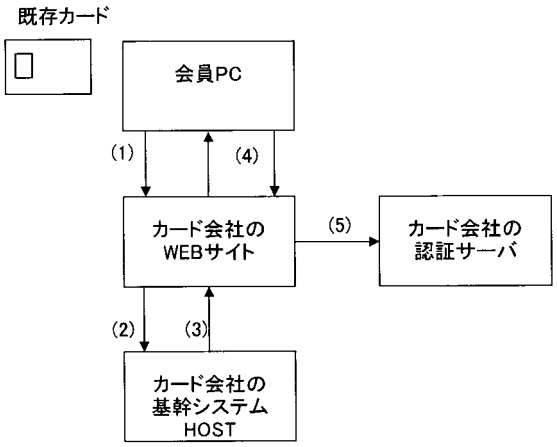
【図４】


(a)
ABC商店 WEB Shop
カード情報を入力してください
カード番号
有効期限
送信
100
100a
100b
100c
(b)
101
加盟店名 ABC商店
金額 5,000円
日付 2006/06/01
ワンタイムパスワードを入力してください
送信
101a
101b

【図５】


START 電源ON(S200)
APLI **
S210
1 カード情報表示
2 認証情報(暗証番号)変更
S225
①押下 (S230)
②押下 (S330)
PIN ****
PIN入力 (S240) (S245)
1 2 3 4 5 6 7 8
カード番号上8 (S250) (S255)
9 0 1 2 3 4 5 6
カード番号下8 (S260) (S265)
1 2 0 8 1 2 3
有効期限 セキュリティコード (S270) (S275)
OTP=1 **
1 OTP生成
3 終了
S290
①押下 S295
①以外押下or所定時間経過 S300
END
PIN **** (S305)
(S310)
1 2 3 4 5 6 OTP
(S315)
(S320)
END
CHANGE? (S335)
(S340)
PIN **** (S345)
(S350)
NEW1**** 変更後のPINを入力 (S355) (S360)
NEW2**** もう一度新しいPINを入力 (S365) (S370)
COMPLETE (S375)
(S380)
END
スタートキー
* テンキーからの入力値
数字 表示値(ネット決済補助装置毎に異なる値)
太字 ガイダンス(ネット決済補助装置によらず共通仕様)

【図６】


既存カード
会員PC
(1)
(4)
カード会社のWEBサイト
(5)
カード会社の認証サーバ
(2)
(3)
カード会社の基幹システムHOST

フロントページの続き

(72)発明者　川勝　実之
東京都港区南青山５丁目１番２２号　株式会社ジェーシービー　国際インフラ推進部内

審査官　鳥居　稔

(56)参考文献　特開２００８－００９９００（ＪＰ，Ａ）
特開２００２－１６３５８４（ＪＰ，Ａ）
特開平１１－２８２９８２（ＪＰ，Ａ）
特開２００６－１４６９１４（ＪＰ，Ａ）
特開２００６－０７２８９０（ＪＰ，Ａ）
特開平１１－３１６７４０（ＪＰ，Ａ）
特開２００１－３１２４７７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｑ　２０／００
Ｈ０４Ｌ
Ｇ０９Ｃ