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

特許第5589471号
(P5589471)

(45)発行日　平成26年9月17日(2014.9.17)　(24)登録日　平成26年8月8日(2014.8.8)

(51)Int.Cl.		F I		
G06Q 40/02	(2012.01)	G06Q	40/02	160
G06F 21/30	(2013.01)	G06F	21/20	
G06Q 20/34	(2012.01)	G06Q	40/02	100
G06K 19/10	(2006.01)	G06Q	20/34	
G06K 17/00	(2006.01)	G06K	19/00	R

請求項の数 6　(全 13 頁)　最終頁に続く

(21)出願番号　特願2010-63552(P2010-63552)
(22)出願日　平成22年3月19日(2010.3.19)
(65)公開番号　特開2011-197985(P2011-197985A)
(43)公開日　平成23年10月6日(2011.10.6)
審査請求日　平成25年1月11日(2013.1.11)

(73)特許権者　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100122529
弁理士　藤枡　裕実
(74)代理人　100135954
弁理士　深町　圭子
(74)代理人　100119057
弁理士　伊藤　英生
(74)代理人　100131369
弁理士　後藤　直樹
(74)代理人　100164987
弁理士　伊藤　裕介
(74)代理人　100171859
弁理士　立石　英之

最終頁に続く

(54)【発明の名称】ロイヤリティ管理システム，ロイヤリティ管理方法及びトークン

(57)【特許請求の範囲】

【請求項１】

ＩＣカードと協働してパスコードを生成するトークンと，前記トークンが生成したワンタイムパスワード（ＯＴＰ）を認証する認証装置とから少なくとも構成され，

前記ＩＣカードは，所定のカウンタに基づいた認証コードを生成する認証コード生成手段を備え，

前記トークンは，所定の手順に従って前記ＩＣカードに認証コード生成させ，前記認証コードの全て又は一部と，前記トークンに記憶された会社コードを含むＯＴＰを生成するＯＴＰ生成手段を備え，

前記認証装置は，ネットワークを介して受信した前記ＯＴＰに含まれる会社コードと，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードが異なる場合，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードと前記ＯＴＰに含まれる会社コードを含む利用ログを記憶する利用ログ記憶手段を備えている，

ことを特徴とするロイヤリティ管理システム。

【請求項２】

前記認証装置は，ネットワークを介して受信した前記ＯＴＰに含まれる前記認証コードを認証するＯＴＰ認証手段を備え，前記認証装置の前記利用ログ記憶手段は，前記ＯＴＰに含まれる前記認証コードの認証に成功すると，前記認証コードの認証方法に対応した前記利用ログを記憶することを特徴とする，請求項１に記載のロイヤリティ管理システム。

【請求項３】

前記認証装置の前記ＯＴＰ認証手段が，ネットワークを介して受信したシードを用いて前記認証コードを認証した場合，前記認証装置の前記利用ログ記憶手段は，前記シードの全て又は一部を前記利用ログに含ませることを特徴とする，請求項２に記載のロイヤリティ管理システム。

【請求項４】

ＩＣカードと協働してパスコードを生成するトークンと，前記トークンが生成したワンタイムパスワード（ＯＴＰ）を認証する認証装置を利用したロイヤリティ管理方法であって，

前記トークンが，所定の手順に従って前記ＩＣカードに認証コード生成させ，前記認証コードの全て又は一部と，前記トークンに記憶された会社コードを含むＯＴＰを生成するステップａ，

前記認証装置が，ネットワークを介して受信した前記ＯＴＰに含まれる会社コードと，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードが異なる場合，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードと前記ＯＴＰに含まれる会社コードを含む利用ログを記憶するステップｂ，

が実行されることを特徴とするロイヤリティ管理方法。

【請求項５】

前記ステップｂにおいて，前記認証装置は，ネットワークを介して受信した前記ＯＴＰに含まれる前記認証コードを認証し，前記ＯＴＰに含まれる前記認証コードの認証に成功したときのみ，前記利用ログを記憶する処理を実行することを特徴とする，請求項４に記載のロイヤリティ管理方法。

【請求項６】

前記ステップｂにおいて，前記認証装置は，ネットワークを介して受信したシードを用いて前記認証コードを認証した場合，前記シードの全て又は一部を前記利用ログに含ませることを特徴とする，請求項５に記載のロイヤリティ管理方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は，キャッシュカードなどのＩＣカードと共に利用されるトークンの利用を管理する技術に係わる。

【背景技術】

【０００２】

ネットワーク社会の到来を受けて，数多くの仮想店舗がネットワーク上に開設され，キャッシュカードなどの金融決済系のカードを利用したネットワーク決済が普及しているが，ネットワーク決済では不正が絶えず，ネットワーク決済時の不正行為に対する何らかの対応が必要となっている。

【０００３】

不正行為を低減するためには，ネットワーク決済時におけるカード保有者の認証が必要で，例えば，特許文献１において，ネットワーク決済時にカード保有者を強く認証し、かつ，カードの存在ならびにカード保有者が取引を始めたことの明らかな証拠を提供できる発明が開示されている。

【０００４】

カード保有者の認証として，パスワードを用いてカード保有者を認証することが古くから行われているが，フィッシングサイトなどによってパスワードが漏洩してしまうと，漏洩したパスワードが不正利用されてしまうため，特許文献１や特許文献２で開示されているように，高いセキュリティが要求されるネットワーク決済には，固定のパスワードではなく，ユーザ認証する毎に異なるワンタイムパスワードを利用することが増えている。

【０００５】

ユーザ認証する毎に異なるワンタイムパスワードは，パーソナルコンピュータに実装されたアプリケーションを利用してソフトウェア的に生成することも可能であるが，ＯＴＰ

の生成に利用する機密データ（例えば，暗号鍵）がパーソナルコンピュータから漏洩してしまう可能性があるため，特許文献３で開示されているようなトークンとキャッシュカードを協働させてＯＴＰを生成させることが一般的になっている。

【０００６】

トークンと金融系カードを協働させてＯＴＰを生成する場合，金融系カードを発行した会社がトークンをユーザに配布することになる。現状では，トークンを複数の金融機関で共有利用可能なケースにおいても，ユーザが複数の金融系カードを所持する場合，金融機関毎にトークンがユーザに配布されている。これは，トークンを配布した金融機関のみがトークン費用を負担することになるため，配布した金融機関が共有利用を許可しないとうい問題があった。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特表２００５－５１９３７５号公報

【特許文献２】特許第４３８８０３９号公報

【特許文献３】特表２００７－５０３６４６号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

そこで，本発明は，トークンに挿入されたＩＣカードの発行会社とトークンを配布した会社が異なる場合，トークンの利用に係わるロイヤリティを算出できるシステム，方法及びトークン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する第１の発明は，ＩＣカードと協働してパスコードを生成するトークンと，前記トークンが生成したワンタイムパスワード（ＯＴＰ）を認証する認証装置とから少なくとも構成されるシステムであって，前記ＩＣカードは，所定のカウンタに基づいた認証コードを生成する認証コード生成手段を備え，前記トークンは，所定の手順に従って前記ＩＣカードに認証コード生成させ，前記認証コードの全て又は一部と，前記トークンに記憶された会社コードを含むＯＴＰを生成するＯＴＰ生成手段を備え，前記認証装置は，ネットワークを介して受信した前記ＯＴＰに含まれる会社コードと，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードが異なる場合，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードと前記ＯＴＰに含まれる会社コードを含む利用ログを記憶する利用ログ記憶手段を備えていることを特徴とするロイヤリティ管理システムである。

【００１０】

第１の発明のように，ネットワークを介して受信した前記ＯＴＰに含まれる会社コードと，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードが異なる場合，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードと前記ＯＴＰに含まれる会社コードを含む利用ログを記憶しておけば，一定期間毎に前記利用ログを集計することで，前記を配布していないにも係わらず，前記トークンを利用した会社に対するロイヤリティを算出できるようになる。

【００１１】

更に，第２の発明は，前記認証装置は，ネットワークを介して受信した前記ＯＴＰに含まれる前記認証コードを認証するＯＴＰ認証手段を備え，前記認証装置の前記利用ログ記憶手段は，前記ＯＴＰに含まれる前記認証コードの認証に成功すると，前記認証コードの認証方法に対応した前記利用ログを記憶することを特徴とする第１の発明に記載のロイヤリティ管理システムである。

【００１２】

前記ＯＴＰに含まれる前記認証コードの認証に成功したときのみ，所定のサービスの利

用がユーザに許可されるため，第２の発明のように，前記ＯＴＰに含まれる前記認証コードの認証に成功したときのみ，前記利用ログを記憶するようにすることが望ましい。
【００１３】
更に，第３の発明は，前記認証装置の前記ＯＴＰ認証手段が，ネットワークを介して受信したシードを用いて前記認証コードを認証した場合，前記認証装置の前記利用ログ記憶手段は，前記シードの全て又は一部を前記利用ログに含ませることを特徴とする第２の発明に記載のロイヤリティ管理システムである。
【００１４】
第３の発明のように，前記シードの全て又は一部を前記利用ログに含ませておけば，前記利用ログに含ませたデータに対応させて，ロイヤリティを算出できるようになる。
【００１５】
更に，第４の発明は，ＩＣカードと協働してパスコードを生成するトークンと，前記トークンが生成したワンタイムパスワード（ＯＴＰ）を認証する認証装置を利用した方法であって，前記トークンが，所定の手順に従って前記ＩＣカードに認証コード生成させ，前記認証コードの全て又は一部と，前記トークンに記憶された会社コードを含むＯＴＰを生成するステップａ，前記認証装置が，ネットワークを介して受信した前記ＯＴＰに含まれる会社コードと，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードが異なる場合，前記認証コードを生成した前記ＩＣカードの発行会社の会社コードと前記ＯＴＰに含まれる会社コードを含む利用ログを記憶するステップｂが実行されることを特徴とするロイヤリティ管理方法である。
【００１６】
更に，第５の発明は，前記ステップｂにおいて，前記認証装置は，ネットワークを介して受信した前記ＯＴＰに含まれる前記認証コードを認証し，前記ＯＴＰに含まれる前記認証コードの認証に成功したときのみ，前記利用ログを記憶する処理を実行することを特徴とする第４の発明に記載のロイヤリティ管理方法である。
【００１７】
更に，第６の発明は，前記ステップｂにおいて，前記認証装置は，ネットワークを介して受信したシードを用いて前記認証コードを認証した場合，前記シードの全て又は一部を前記利用ログに含ませることを特徴とする第５の発明に記載のロイヤリティ管理方法である。
【発明の効果】
【００１９】
このように，上述した本発明によれば，トークンに挿入されたＩＣカードの発行会社とトークンを配布した会社が異なる場合，トークンの利用に係わるロイヤリティを算出できるシステム，方法及びトークンを提供することを目的とする。
【図面の簡単な説明】
【００２０】
【図１】ロイヤリティ管理システムの構成を説明する図。
【図２】トークンを説明する図。
【図３】認証装置に備えられた機能を説明する図。
【図４】ロイヤリティ管理システムで実行される処理を説明するフロー図。
【図５】ＯＴＰ生成処理の詳細を説明するフロー図。
【図６】ＯＴＰ認証処理の詳細を説明するフロー図。
【図７】ＯＴＰ生成処理の補足図。
【発明を実施するための形態】
【００２１】
ここから，本願発明の実施形態について，本願発明の技術分野に係わる当業者が，本願発明の内容を理解し，本願発明を実施できる程度に説明する。
【００２２】
図１は，本実施形態に係わるロイヤリティ管理システム１の構成を説明する図である。

本実施形態は，インターネットバンキングに利用するトークン２のロイヤリティ管理に，本発明を適用した形態で，図１で図示したロイヤリティ管理システム１には，ユーザが所持するＩＣカードとして，ＩＣカード型のキャッシュカード３と，ＩＣカード（ここでは，キャッシュカード３）と協働してワンタイムパスワード（OTP: One-Time Password）を生成するトークン２と，トークン２で生成されたＯＴＰを認証する機能を備えた認証装置６と，トークン２で生成されたＯＴＰが入力される端末装置４（例えば，パーソナルコンピュータ）と，インターネットバンキングの機能を備えたＷｅｂサーバ５が含まれ，端末装置４，認証装置６及びＷｅｂサーバ５はそれぞれインターネット７に接続されている。

【００２３】

本実施形態において，トークン２には，トークン２をユーザに配布した金融機関系の会社（例えば，銀行）の会社コードである金融機関コードが少なくとも記憶され，トークン２がキャッシュカード３と協働して生成するＯＴＰには，キャッシュカード３で生成された認証コードなどに加え，トークン２に記憶された金融機関コードが含まれる。

【００２４】

本実施形態において，認証装置６は，Ｗｅｂサーバ５を経由して，トークン２が生成したＯＴＰが送信されると，ＯＴＰに含まれる認証コードを認証すると共に，ＯＴＰから金融機関コードを抽出し，認証コードを生成したキャッシュカード３の発行会社の金融機関コードとＯＴＰから抽出した金融機関コードが異なる場合，認証コードを生成したキャッシュカード３の発行会社のインターネットバンキングの処理にトークン２が利用されたことを示す利用ログを記憶する。

【００２５】

トークン２に挿入されたキャッシュカード３の発行会社とトークン２を配布した会社が異なる場合，このキャッシュカード３の発行会社のインターネットバンキングの処理にトークン２が利用されたことを示す利用ログを記憶しておけば，一定期間毎にこの利用ログを集計することで，トークン２を配布していないにも係わらず，インターネットバンキングの処理にトークン２を利用した会社に対するロイヤリティを算出できるようになる。

【００２６】

ここから，図１で図示したロイヤリティ管理システム１に含まれるトークン２，キャッシュカード３及び認証装置６についてそれぞれ説明する。

【００２７】

まず，ユーザが所持するキャッシュカード３ついて説明する。ユーザが所持するキャッシュカード３は，全銀協ＩＣキャッシュカード標準仕様に準拠したＩＣカードで，キャッシュカード３には，インターネットバンキングを利用するためのアプリケーションが実装されている。

【００２８】

全銀協ＩＣキャッシュカード標準仕様に準じたＩＣカードについての詳細は，全銀協ＩＣキャッシュカード標準仕様等の様々な文献に記載されているため，ここではキャッシュカード３の詳細な説明は省くが，認証コードの生成には，全銀協ＩＣキャッシュカード標準仕様で定義されているGenerateAC1（Generate Application Cryptogram）コマンドが利用され，GenerateAC1コマンドのレスポンに含まれる暗号文であるＡＣ（Application Cryptogram）が認証コードとして利用される。

【００２９】

GenerateAC1コマンドのレスポンに含まれるＡＣは，キャッシュカード３の内部に記憶されるＡＴＣ（Application Transaction Counter）に基づき所定のアルゴリズムに従い生成されるデータで，ＡＴＣはキャッシュカード３が取引に利用される毎にインクリメントされるため，カウンタ同期方式のＯＴＰの認証コードとしてＡＣを利用できる。

【００３０】

図２はトークン２を説明する図で，図２（ａ）はトークン２の外観を説明する図で，図２（ｂ）はトークン２の内部回路を説明する図である。

【００３１】

図２（ａ）で図示したように，トークン２には，ユーザが所持するキャッシュカード３を挿入する挿入口２３と，ＯＴＰに含ませる認証コードのシード（例えば，取引関連データ）の入力に利用されるテンキー２１と，トークン２に入力されたデータやトークン２が生成したＯＴＰなどの表示に利用されるディスプレイ２２と，ＯＴＰの生成方法を選択するための選択ボタン２０a，ｂが備えられている。

【００３２】

なお，図２（ａ）で図示した選択ボタン２０aは，認証コードのシードの入力を必要としないＯＴＰの生成方法を実行させるためのボタンで，選択ボタン２０ｂは，認証コードのシード（例えば，チャレンジ，取引種別や取引金額など）の入力を必要とするＯＴＰの生成方法を実行させるためのボタンである。

【００３３】

図２（ｂ）で図示したように，トークン２には，挿入口２３から挿入されたキャッシュカード３とデータ通信するリーダライタ回路２ｂと，ディスプレイ２２を制御するディスプレイ駆動回路２ｃと，選択ボタン２０a，ｂ及びテンキー２１に対応する信号を発生させる入力回路２ｄと，ＣＰＵ，ＲＡＭ及びＲＯＭなどを有し，コンピュータプログラムに従い所定の処理を実行する制御チップ２aを備えて，本実施形態では，キャッシュカード３を利用してＯＴＰを生成するＯＴＰ生成手段２００がコンピュータプログラムによってトークン２に備えられている。なお，本実施形態において，ＯＴＰ生成手段２００は，上述した２つのＯＴＰの生成方法に対応している。

【００３４】

次に，認証装置６について説明する。図３は，認証装置６に備えられた機能を説明する図である。認証装置６は汎用のウェブサーバを利用して実現される装置で，図３に図示したように，認証装置６には，コンピュータプログラムによって実現される手段として，Ｗｅｂサーバ５から転送されるＯＴＰを認証するＯＴＰ認証手段６０と，Ｗｅｂサーバ５から転送されるＯＴＰを利用し，トークン２の利用状況を示す利用ログを記憶する利用ログ記憶手段６１が少なくとも備えられる。

【００３５】

なお，認証装置６のデータ記憶デバイス（例えば，ハードディスク）には，利用ログ記憶手段が利用ログを記憶する利用ログＤＢ６２（DB: DataBase）が設けられ，更に，ユーザ毎に，ＯＴＰを認証するために必要なデータが記憶されている。更に，図１に図示していないが，認証装置６には，暗号鍵を生成する機能を備えたホストセキュリティモジュールが接続され，このホストセキュリティモジュールにはＯＴＰを認証する際に必要となる暗号鍵（ここでは，イッシュア鍵）が記憶されている。

【００３６】

ここから，本実施形態におけるロイヤリティ管理システム１で実行される処理を説明しながら，トークン２及び認証装置６が備えている機能について詳細に説明する。

【００３７】

図４は，ロイヤリティ管理システム１で実行される処理を説明するフロー図で，図５は，トークン２で実行されるＯＴＰ生成処理の詳細を説明するフロー図で，図６は，認証装置６で実行されるＯＴＰ認証処理の詳細を説明するフロー図である。

【００３８】

まず，図４を参照しながら，ロイヤリティ管理システム１で実行される処理について説明する。キャッシュカード３を所持するユーザがＷｅｂサイトにログインするとき，端末装置４上で動作するブラウザがユーザによって操作され，端末装置４は，Ｗｅｂサーバ５のログインページへアクセスする（Ｓ１）。

【００３９】

Ｗｅｂサーバ５は，Ｗｅｂサーバ５のログインページへ端末装置４からアクセスがあると，Ｗｅｂサーバ５へログインするためログインページを端末装置４へ送信し（Ｓ２），端末装置４上で起動しているブラウザにログインページが表示される（Ｓ３）。

【００４０】

なお，端末装置４のブラウザ上に表示されるログインページには，端末装置４を操作するユーザのＩＤを入力する入力フォームと，トークン２で生成されたＯＴＰを入力する入力フォームが含まれる。

【００４１】

ユーザは，端末装置４のブラウザ上にログインページが表示されると，ユーザが所持しているキャッシュカード３をトークン２に挿入した後，トークン２のテンキー２１を操作し，認証装置６に認証させるＯＴＰを生成するＯＴＰ生成処理（Ｓ４）がトークン２で実行される。

【００４２】

ここから，図５を参照しながら，認証装置６に認証させるＯＴＰを生成するＯＴＰ生成処理（Ｓ４）の詳細について説明する。図７は，ＯＴＰ生成処理（Ｓ４）の補足図である。

【００４３】

ユーザがトークン２を利用してＯＴＰを生成するとき，ユーザは，キャッシュカード３をトークン２の挿入口へ挿入した後，ＯＴＰの生成方法を選択する（Ｓ１０）。本実施形態では，トークン２のテンキーに含まれる選択ボタン２０ａ，ｂのいずれかをユーザが選択して押すことでＯＴＰの生成方法が選択され，ここでは，選択ボタン２０ａが押されたことにする。

【００４４】

ＯＴＰの生成方法が選択されると，トークン２のＯＴＰ生成手段２００が作動し，ＯＴＰ生成手段２００は，まず，インターネットバンキングで利用するアプリケーションを選択する（Ｓ１１）。具体的に，トークン２のＯＴＰ生成手段２００は，全銀協ＩＣキャッシュカード標準仕様に準じた手順で，キャッシュカード３に実装されているアプリケーションの中から，インターネットバンキングで利用するアプリケーションを選択する。

【００４５】

トークン２のＯＴＰ生成手段２００は，インターネットバンキングで利用するアプリケーションを選択すると，トークン２に挿入されたキャッシュカード３から，Get Processing OptionコマンドやREADコマンドなどを利用して，アプリケーションデータを読み取る（Ｓ１２）。このアプリケーションデータには，全銀協ＩＣキャッシュカード標準仕様で定義されているＰＳＮ（Application Primary Account Number Sequence Number）やCDOL1,2(Card Risk Management Data Object Lists)が含まれる。

【００４６】

トークン２のＯＴＰ生成手段２００は，アプリケーションデータをキャッシュカード３から読み取ると，全銀協ＩＣキャッシュカード標準仕様で定義されているGenerateAC1コマンドのコマンドメッセージをキャッシュカード３へ送信し，キャッシュカード３からGenerateAC1コマンドのレスポンスを受信する（Ｓ１３）。なお，ここでは，選択ボタン２０ａが押されているため，GenerateAC1コマンドのデータフィールドには，認証コードのシードとして，トークン２に予め記憶されているデフォルトデータが含まれる。なお，選択ボタン２０ｂが押されたときは，Ｓ１２ａが実行される。

【００４７】

トークン２からGenerateAC1コマンドのコマンドメッセージが送信されると，キャッシュカード３は，キャッシュカード３内部に記憶しているＩＣカード個別鍵とこの時のＡＴＣからセッション鍵を生成し，生成したセッション鍵を用いてトークン２から受信したデフォルトデータの暗号文を生成し，GenerateAC1コマンドのレスポンスを生成する。

【００４８】

なお，本実施形態では，GenerateAC1コマンドのレスポンスには，CID(Cryptogram Information Data)， ATC(Application Transaction Counter)，認証コードとして利用されるAC(Application Cryptogram)に加え， IAD(Issuer Application Data)が含まれる。

【００４９】

トークン２のＯＴＰ生成手段２００は，GenerateAC1コマンドのレスポンスをキャッシ

ュカード３から受信すると，GenerateAC1コマンドのレスポンスを利用し，トークンデータをトークン２の内部で生成する（Ｓ１４）。

【００５０】

図７では，ＰＳＮ，ＣＩＤ，ＡＴＣ，ＡＣ，IAD，金融機関コードから構成されるトークンデータ８ａを例示している。ＰＳＮは，トークン２のＯＴＰ生成手段２００がキャッシュカード３から読み出したアプリケーションデータに含まれ，ＣＩＤ，ＡＴＣ，ＡＣ，IADはGenerateAC1コマンドのレスポンスに含まれ，金融機関コードはトークン２に記憶されている。

【００５１】

トークン２のＯＴＰ生成手段２００は，トークンデータをトークン２の内部に生成すると，トークンデータを圧縮することでＯＴＰを生成する（Ｓ１５）。

【００５２】

図７では，トークンデータの圧縮に，認証装置６側でＯＴＰを認証するときに利用するビットが示されるＩＰＢ８ｂ（Issuer Proprietary Bitmap)が用いられ，ＩＰＢ８ｂにおいて「１」であるビットに対応するトークンデータ８ａのみをＯＴＰに用いることで，トークンデータ８ａを圧縮した圧縮データ８ｃが生成される。

【００５３】

なお，本実施形態では，金融機関コードをＯＴＰに含ませるため，図７で図示したＩＰＢ８ｂでは，金融機関コードに対応するＩＰＢ８ｂのビットは全て「１」にしている。

【００５４】

トークン２はＯＴＰを生成すると，ＯＴＰを１０進数で表した値をディスプレイ２２に表示させ（Ｓ１６），この手順は終了する。このとき，トークン２のディスプレイ２２に表示した値がＯＴＰであることをユーザに通知する文字列（例えば，「One-Time Password=」）を表示させるとよい。

【００５５】

例えば，図７では，ＩＰＢ８ｂを用いてトークンデータ８ａを圧縮した圧縮データ８ｃを１０進数に変換したＯＴＰ８ｄが表示されることになる。

【００５６】

ここから，図４の説明に戻る。ＯＴＰ生成処理（Ｓ４）が実行されると，トークン２のディスプレイ２２にＯＴＰが表示され，ユーザは，ユーザがユーザ自身のＩＤと，トークン２のディスプレイ２２に表示されたＯＴＰをログインページに入力し（Ｓ５），ログインページ上で所定の操作を行うと，ユーザがログインしたユーザのＩＤ，ＯＴＰが少なくともＷｅｂサーバ５へ送信され，Ｗｅｂサーバ５は，端末装置４から受信したユーザのＩＤ及びＯＴＰを認証装置６へ転送し（Ｓ６），ＯＴＰの認証を認証装置６へ委任する。

【００５７】

認証装置６は，ユーザのＩＤ及びＯＴＰがＷｅｂサーバ５から転送されると，認証装置６は，所定のアルゴリズムに従い，Ｗｅｂサーバ５から転送されたＯＴＰを認証するOTP認証処理（Ｓ７）を実行する。

【００５８】

そして，認証装置６は，Ｗｅｂサーバ５から転送されたＯＴＰを認証すると認証結果をＷｅｂページへ送信し（Ｓ８），Ｗｅｂサーバ５は該認証結果と共に，該認証結果に応じてログイン結果を表示するＷｅｂページを端末装置４へ送信し，端末装置４のブラウザ上に認証結果が表示されて（Ｓ９），この手順を終了する。

【００５９】

ここから，図６を参照しながら，認証装置６に認証させるＯＴＰを生成するＯＴＰ認証処理（Ｓ７）について説明する。

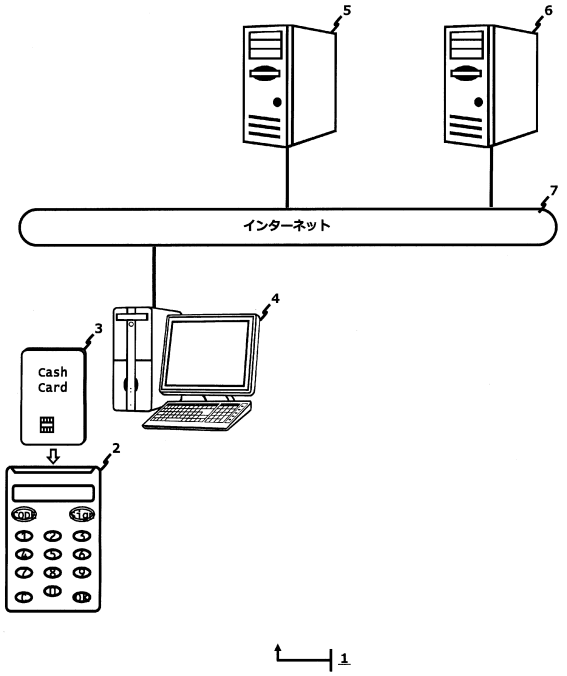
【００６０】

ユーザのＩＤ及びＯＴＰなどがＷｅｂサーバ５から転送されると認証装置６のＯＴＰ認証手段６０が作動し，認証装置６のＯＴＰ認証手段６０は，ＯＴＰを認証する処理を開始する（Ｓ２０）。

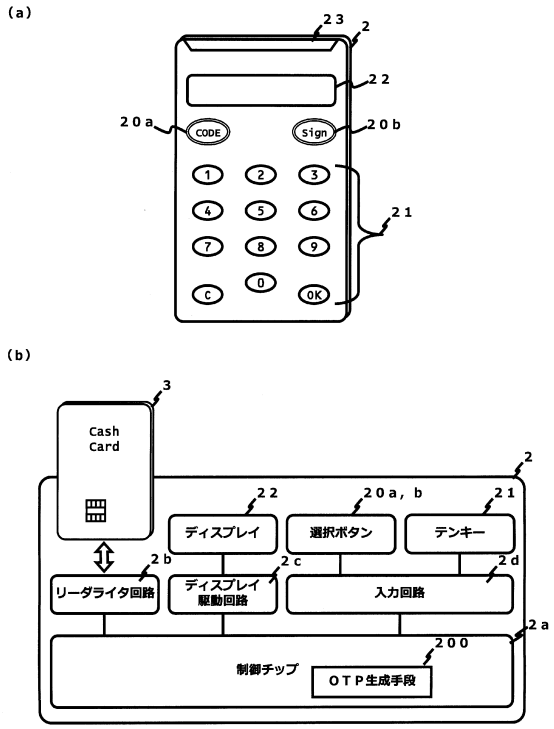
【００６１】
認証装置６は，ユーザのＩＤに関連付けて，ユーザが所持しているキャッシュカード３に記憶されているＰＡＮ（Application Primary Account Number），ＰＳＮや，前回の認証で利用されたＡＴＣなどを記憶し，認証装置６のＯＴＰ認証手段６０は，端末装置４から送信されたＩＤに関連付けられたＰＡＮとＰＳＮを連結したデータと，認証装置６で記憶しているイッシュア鍵からＩＣカード個別鍵を生成する（Ｓ２１）。
【００６２】
次に，認証装置６のＯＴＰ認証手段６０は，受信したＯＴＰに含まれるＡＴＣを抽出する（Ｓ２２）。図７で図示したＩＰＢでは，ＡＴＣの下位７ビットのみがＯＴＰに含まれることになるため，認証装置６は，ＯＴＰからＡＴＣの下位７ビットを抽出することになる。
【００６３】
そして，認証装置６のＯＴＰ認証手段６０は，ＯＴＰからＡＴＣの下位７ビットを抽出すると，Ｗｅｂサーバ５側で記憶している前回のＡＴＣの上位９ビットを抽出する（Ｓ２３）。
【００６４】
そして，認証装置６のＯＴＰ認証手段６０は，前回のＡＴＣの上位９ビットとＯＴＰから抽出した下位７ビットを連結した１６ビットのＡＴＣとＩＣカード個別鍵からセッション鍵を生成し（Ｓ２４），ここでは，トークン２に記憶されているデフォルトデータと同じデータを認証シードとし，セッション鍵を用いてＡＣを算出し（Ｓ２５），算出したＡＣとＯＴＰに含まれるＡＣを比較する（Ｓ２６）。
【００６５】
認証装置６側で演算したＡＣとＯＴＰに含まれるＡＣが一致すると見なせるとき，認証装置６の利用ログ記憶手段６１を作動させて，ＯＴＰに含まれる金融機関コードと，認証コードを生成したキャッシュカード３の発行会社の金融機関コードを比較し（Ｓ２７），一致しないと見なせるとき，図６の手順は終了する。
【００６６】
本実施形態において，認証コードを生成したキャッシュカード３の発行会社の金融機関コードは，ユーザのＰＡＮに含まれ，ＯＴＰに含まれる金融機関コードと，該キャッシュカード３の発行会社の金融機関コードが一致すると見なせるときは図６の手順は終了し，一致しないと見なせるとき，認証装置６の利用ログ記憶手段６１は，ユーザのＩＤ，金融機関コード，このときの日時などを利用ログとして利用ログＤＢ６２に記憶し（Ｓ２８），図６の手順は終了する。
【００６７】
ここまで，トークン２の選択ボタン２０ａが押された場合について説明したが，トークン２の選択ボタン２０ｂが押された場合は，トークン２がGenerateAC1コマンドを送信する前に，CDOL1で指定される取引関連データ（例えば，取引金額）などのシードをユーザに入力させるＳ１２ａが実行される。
【００６８】
CDOL1で指定される取引関連データとは，例えば，取引金額などを意味し，これらの値は，Ｗｅｂサーバ５のＷｅｂページに入力された値になり，取引関連データをユーザに入力させるとき，トークン２のＯＴＰ生成手段２００は，ユーザに入力要求する項目に該当する文字列（例えば，「Transaction?」）をディスプレイ２２に表示させ，ユーザに，取引関連データの項目の値を入力させる。
【００６９】
更に，認証コードのシードにチャレンジが含まれるとき，Ｗｅｂサーバ５のＷｅｂページにチャレンジが表示され，チャレンジをユーザに入力させるとき，トークン２のＯＴＰ生成手段２００は，ユーザに入力要求する項目に該当する文字列（例えば，「Challenge?」）をディスプレイ２２に表示させ，ユーザに，Ｗｅｂサーバ５のＷｅｂページに表示されたチャレンジを入力させる。

【００７０】
　また，選択ボタン２０ｂが押されたとき，Ｗｅｂサーバ５から認証装置６へ取引関連データやチャレンジなどのシードが送信され，認証装置６のＯＴＰ認証手段６０は，Ｗｅｂサーバから送信されたシードを用いてＡＣを算出することになる。
【００７１】
　更に，選択ボタン２０ｂが押されたとき，Ｗｅｂサーバ５から認証装置６へ認証コードのシードが送信されるため，利用ログＤＢ６２に記憶する利用ログには，認証コードのシードの全て又は一部を含ませるとよい。
【００７２】
　なお、本発明は、これまで説明した実施の形態に限定されることなく、種々の変形や変更が可能である。
【符号の説明】
【００７３】
１　ロイヤリティ管理システム
２　トークン
２０ａ，ｂ　選択ボタン
２１　テンキー
２２　ディスプレイ
２００　ＯＴＰ生成手段
３　キャッシュカード
４　端末装置
５　Ｗｅｂサーバ
６　認証装置
６０　ＯＴＰ認証手段
６１　利用ログ記憶手段
６２　利用ログＤＢ

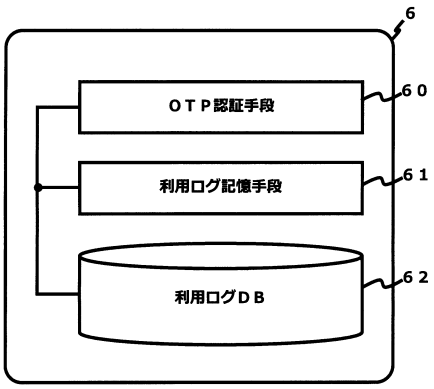
【図１】


5
6
7
インターネット
4
3
Cash
Card
2
1

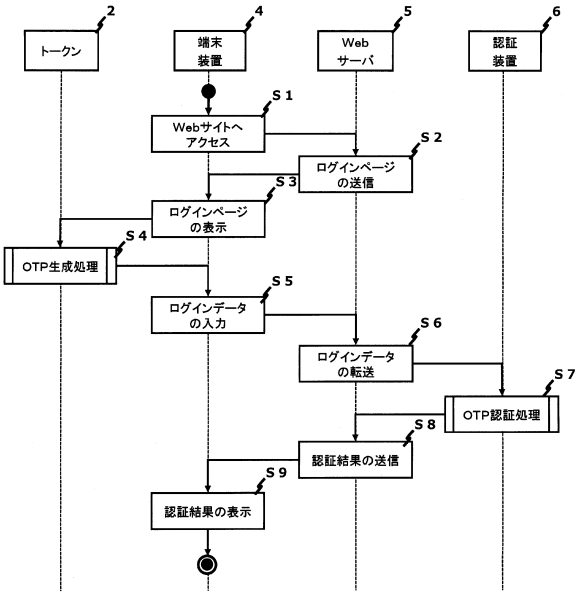
【図２】


(a)
23
2
22
20a
CODE
sign
20b
1
2
3
4
5
6
7
8
9
C
0
OK
21
(b)
3
Cash
Card
2
22
20a, b
21
ディスプレイ
選択ボタン
テンキー
2b
2c
2d
リーダライタ回路
ディスプレイ
駆動回路
入力回路
2a
200
制御チップ
OTP生成手段

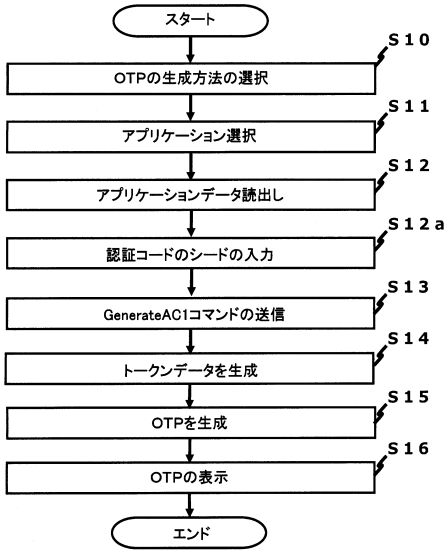
【図３】


6
60
OTP認証手段
61
利用ログ記憶手段
62
利用ログDB

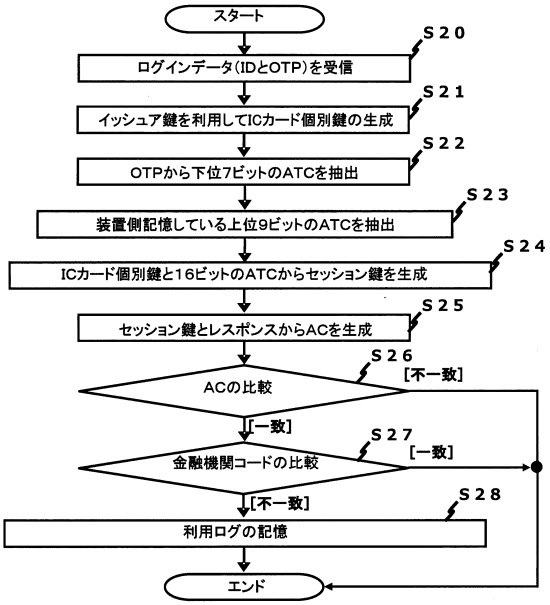
【図４】


2
トークン
4
端末
装置
5
Web
サーバ
6
認証
装置
S1
Webサイトへ
アクセス
S2
ログインページ
の送信
S3
ログインページ
の表示
S4
OTP生成処理
S5
ログインデータ
の入力
S6
ログインデータ
の転送
S7
OTP認証処理
S8
認証結果の送信
S9
認証結果の表示

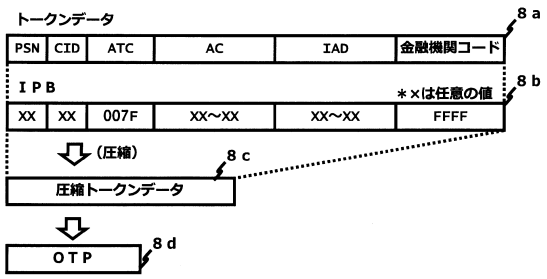
【図５】


スタート
S10
OTPの生成方法の選択
S11
アプリケーション選択
S12
アプリケーションデータ読出し
S12a
認証コードのシードの入力
S13
GenerateAC1コマンドの送信
S14
トークンデータを生成
S15
OTPを生成
S16
OTPの表示
エンド

【図６】


スタート
S20
ログインデータ(IDとOTP)を受信
S21
イッシュア鍵を利用してICカード個別鍵の生成
S22
OTPから下位7ビットのATCを抽出
S23
装置側記憶している上位9ビットのATCを抽出
S24
ICカード個別鍵と16ビットのATCからセッション鍵を生成
S25
セッション鍵とレスポンスからACを生成
S26
ACの比較
[不一致]
[一致]
S27
金融機関コードの比較
[一致]
[不一致]
S28
利用ログの記憶
エンド

【図７】


トークンデータ
8a
PSN
CID
ATC
AC
IAD
金融機関コード
IPB
＊×は任意の値
8b
XX
XX
007F
XX～XX
XX～XX
FFFF
(圧縮)
8c
圧縮トークンデータ
OTP
8d

フロントページの続き

(51)Int.Cl. FI
G06K 17/00 T

(72)発明者 加田 好美
東京都新宿区市谷加賀町一丁目１番１号 大日本印刷株式会社内

審査官 本郷 彰

(56)参考文献 特開２００７－２６５１７０（ＪＰ，Ａ）
特表２００５－５１９３７５（ＪＰ，Ａ）
特表２００７－５０３６４６（ＪＰ，Ａ）
特許第４３８８０３９（ＪＰ，Ｂ２）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ ４０／０２
Ｇ０６Ｆ ２１／３０
Ｇ０６Ｋ １７／００
Ｇ０６Ｋ １９／１０
Ｇ０６Ｑ ２０／３４