(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2016-9375
(P2016-9375A)
(43)公開日　平成28年1月18日(2016.1.18)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 20/40	(2012.01)	G06Q	20/40	110	5L055
G06Q 20/24	(2012.01)	G06Q	20/24		
G06Q 20/34	(2012.01)	G06Q	20/34		
G06F 21/62	(2013.01)	G06F	21/24	166A	

審査請求 未請求　請求項の数 8　ＯＬ　（全 17 頁）

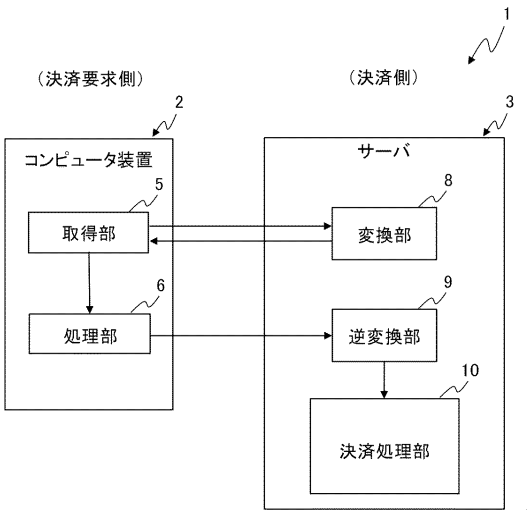
(21)出願番号　特願2014-130300 (P2014-130300)
(22)出願日　平成26年6月25日 (2014.6.25)

(71)出願人　303013763
ＮＥＣエンジニアリング株式会社
神奈川県川崎市中原区下沼部１７５３番地
(74)代理人　100109313
弁理士　机　昌彦
(74)代理人　100124154
弁理士　下坂　直樹
(72)発明者　荻野　守彦
神奈川県川崎市中原区下沼部１７５３番地
ＮＥＣエンジニアリング株式会社内

Ｆターム(参考)　5L055 AA52　AA66　AA75

(54)【発明の名称】決済システムおよび決済処理方法

(57)【要約】
【課題】　コストを抑制しながら情報漏洩に対するセキュリティーを強化する。
【解決手段】　サーバ３の変換部８は、コンピュータ装置２からのカード番号を乱数であるトークンに変換し当該トークンをコンピュータ装置２に返信する。トークンは、発信元のコンピュータ装置２あるいは当該コンピュータ装置２を使用して決済を要求する事業者を識別可能な番号を含んでいる。逆変換部９は、決済の要求とトークンとが送信されてきた場合にトークンを変換元のカード番号に戻す。決済処理部１０は、決済の要求に応じて、カード番号を利用した決済を処理する。コンピュータ装置２の取得部５は、カード番号をサーバ３に送信することによって当該カード番号に対応するトークンを取得する。処理部６は、カード番号とトークンとのうちのトークンのみを保持し、カード番号に代えてトークンをカード番号として用いて、カード番号を利用する処理を実行する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
決済に利用されるカードを識別するカード番号に基づいた決済を要求する決済要求側のコンピュータ装置と、
前記コンピュータ装置からの決済の要求に応じて、そのコンピュータ装置から送信されてきた前記カード番号に基づいて決済を処理する決済処理部を備えたサーバと
を備え、
前記サーバは、さらに、
前記コンピュータ装置から受け取った前記カード番号を乱数であるトークンに変換し当該トークンを前記コンピュータ装置に返信する変換部と、
前記コンピュータ装置から決済の要求と前記トークンとが送信されてきた場合に、前記トークンと当該トークンに変換される前の変換元の前記カード番号とが関連付けられている変換データに基づき、前記送信されてきたトークンを変換元の前記カード番号に戻し当該カード番号を前記決済処理部に供給する逆変換部と
を備え、
前記コンピュータ装置は、
前記カード番号を前記サーバに向けて送信することによって当該カード番号に対応する前記トークンを前記サーバから取得する取得部と、
前記カード番号と前記トークンとのうちの前記トークンのみを保持し、前記カード番号に代えて前記トークンを前記カード番号として用いて、前記カード番号を利用する処理を実行する処理部と
を備えており、
前記トークンは、変換元の前記カード番号を前記サーバに送信した発信元の前記コンピュータ装置あるいは当該コンピュータ装置を使用して決済を要求する事業者を識別可能な番号を含んでいる決済システム。
【請求項２】
前記トークンの桁数は、変換元の前記カード番号の桁数と同じである請求項１記載の決済システム。
【請求項３】
前記逆変換部は、前記トークンと、当該トークンを送信してきた発信元の前記コンピュータ装置あるいは当該コンピュータ装置を使用している事業者を識別する発信元識別情報とに基づいて、前記トークンに対する認証処理を実行し、前記トークンを承認しないと判断した場合には警報を発する請求項１又は請求項２に記載の決済システム。
【請求項４】
前記サーバ装置は、さらに、
前記逆変換部が警報を発した場合に、警戒が必要な事態が発生したことを報知する報知部と、
前記逆変換部による認証処理によって前記トークンが承認されなかった場合に、前記トークンを送信してきた発信元の前記コンピュータ装置あるいは当該コンピュータ装置を使用している事業者との取り引きを中断する中断部と
を備えている請求項３に記載の決済システム。
【請求項５】
前記変換部は、前記コンピュータ装置から受け取った前記カード番号に対する認証処理を実行し、当該認証処理により前記カード番号を承認した場合に、前記カード番号を前記トークンに変換する請求項１乃至請求項４の何れか一つに記載の決済システム。
【請求項６】
前記逆変換部は、前記サーバが保持しているデータを前記コンピュータ装置に送信する処理が前記サーバにより実行される場合に、送信対象の前記データに前記カード番号が含まれている場合には、そのカード番号を前記変換データに基づき前記トークンに変換し、前記送信対象のデータに含まれる前記カード番号を前記トークンに変更する請求項１乃至

請求項５の何れか一つに記載の決済システム。
【請求項７】
前記サーバを複数備え、
前記コンピュータ装置は、さらに、
決済を要求する取り引き先の前記サーバを変更する指令を受けた場合に、取り引きを停止する前記サーバに向けて、情報の返還を要求すると共に当該サーバによって生成された前記トークンを送信することによって、当該トークンに変換される前の変換元の前記カード番号を取得し、さらに、当該カード番号を変更後の取り引き先の前記サーバに向けて送信することによって当該カード番号に対応する前記トークンを変更後の取り引き先の前記サーバから取得する変更部を備えている請求項１乃至請求項６の何れか一つに記載の決済システム。
【請求項８】
決済に利用されるカードを識別するカード番号に基づいた決済を要求する決済要求側のコンピュータ装置からの決済の要求に応じて、そのコンピュータ装置から送信されてきた前記カード番号に基づいて決済を処理するサーバが、前記コンピュータ装置から受け取った前記カード番号を乱数であるトークンに変換し当該トークンを前記コンピュータ装置に返信し、
前記コンピュータ装置から決済の要求と前記トークンとが送信されてきた場合に、前記トークンと当該トークンに変換される前の変換元の前記カード番号とが関連付けられている変換データに基づき、前記トークンを変換元の前記カード番号に戻し当該カード番号に基づいた決済処理を前記サーバが実行し、
また、変換元の前記カード番号を前記サーバに送信した発信元の前記コンピュータ装置あるいは当該コンピュータ装置を使用して決済を要求する事業者を識別可能な番号が含まれるように前記カード番号を前記トークンに前記サーバが変換する決済処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、クレジットカード等のカードを利用した決済システムにおいて、情報漏洩に対するセキュリティーを強化する技術に関する。
【背景技術】
【０００２】
商品やサービスを購入する代金の決済方法の一つとして、クレジットカードやデビットカード等のカード（決済カード）を利用するカード決済が有る。このカード決済を実現するために、例えば、商品やサービスを販売する店は、所有しているコンピュータ装置を、取り引き対象のカード会社のサーバに接続することによって、決済システムを構築する。この決済システムは、決済カードのカード番号等の情報が漏洩することを防止するために、通常、ＰＣＩ ＤＳＳ（Payment Card Industry Data Security）と呼ばれるセキュリティー基準の要件を満たすように構築される。
【０００３】
なお、決済システムのセキュリティーを強化する手段として、特許文献１（特開２０１１－２０９８６１号公報）には、次のような手段が提案されている。つまり、特許文献１には、決済カード（取引カード）のカード番号とは別に、取り引きの利用制限に応じて代替番号を発行し、この代替番号を利用して決済（取り引き）が処理される構成が示されている。
【０００４】
また、特許文献２（特開２００５－２９３３４３号公報）には、ネットワークを利用した電子商取引に関する構成が示されている。すなわち、特許文献２の構成では、決済に要する情報が、商品を購買する購買者から販売者に送信されることなく、購買者が選択した与信機関に送信されることによって、決済が行われる。この構成は、決済に要する情報（個人情報）が販売者に流れないので、個人情報が漏洩する危険性を低減できる。

【０００５】
さらに、特許文献３（特開２０１１－１２８８９８号公報）には、クレジットカードを利用する取り引き内容に応じたサブ番号を生成し、カード番号に代えて、そのサブ番号を利用して決済を処理する構成が示されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２０１１－２０９８６１号公報
【特許文献２】特開２００５－２９３３４３号公報
【特許文献３】特開２０１１－１２８８９８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
ところで、ＰＣＩ ＤＳＳは、保護対象に指定されているクレジットカード番号等の情報を保持する部分や通信経路部分に適用される。決済システムを構築する際には、そのＰＣＩ ＤＳＳの適用範囲に応じて費用が掛かる。つまり、ＰＣＩ ＤＳＳに準拠するために、保護対象の情報を秘匿する手段を講じる等の対策に費用が掛かる。
【０００８】
また、カード決済に必要なカード番号等の情報を情報通信網（インターネット）を利用して不正に取得する手口が巧妙になってきており、情報漏洩に対するセキュリティーの強化が要望されている。
【０００９】
本発明は上記課題を解決するために考え出された。すなわち、本発明の主な目的は、決済システムにおいて、コストを抑制しながら、情報漏洩に対するセキュリティーを強化できる技術を提供することにある。
【課題を解決するための手段】
【００１０】
上記目的を達成するために、本発明の決済システムは、
決済に利用されるカードを識別するカード番号に基づいた決済を要求する決済要求側のコンピュータ装置と、
前記コンピュータ装置からの決済の要求に応じて、そのコンピュータ装置から送信されてきた前記カード番号に基づいて決済を処理する決済処理部を備えたサーバと
を備え、
前記サーバは、さらに、
前記コンピュータ装置から受け取った前記カード番号を乱数であるトークンに変換し当該トークンを前記コンピュータ装置に返信する変換部と、
前記コンピュータ装置から決済の要求と前記トークンとが送信されてきた場合に、前記トークンと当該トークンに変換される前の変換元の前記カード番号とが関連付けられている変換データに基づき、前記送信されてきたトークンを変換元の前記カード番号に戻し当該カード番号を前記決済処理部に供給する逆変換部と
を備え、
前記コンピュータ装置は、
前記カード番号を前記サーバに向けて送信することによって当該カード番号に対応する前記トークンを前記サーバから取得する取得部と、
前記カード番号と前記トークンとのうちの前記トークンのみを保持し、前記カード番号に代えて前記トークンを前記カード番号として用いて、前記カード番号を利用する処理を実行する処理部と
を備えており、
前記トークンは、変換元の前記カード番号を前記サーバに送信した発信元の前記コンピュータ装置あるいは当該コンピュータ装置を使用して決済を要求する事業者を識別可能な

番号を含んでいる。
【００１１】
　また、本発明の決済処理方法は、
　決済に利用されるカードを識別するカード番号に基づいた決済を要求する決済要求側のコンピュータ装置からの決済の要求に応じて、そのコンピュータ装置から送信されてきた前記カード番号に基づいて決済を処理するサーバが、前記コンピュータ装置から受け取った前記カード番号を乱数であるトークンに変換し当該トークンを前記コンピュータ装置に返信し、
　前記コンピュータ装置から決済の要求と前記トークンとが送信されてきた場合に、前記トークンと当該トークンに変換される前の変換元の前記カード番号とが関連付けられている変換データに基づき、前記トークンを変換元の前記カード番号に戻し当該カード番号に基づいた決済処理を前記サーバが実行し、
　また、変換元の前記カード番号を前記サーバに送信した発信元の前記コンピュータ装置あるいは当該コンピュータ装置を使用して決済を要求する事業者を識別可能な番号が含まれるように前記カード番号を前記トークンに前記サーバが変換する。
【発明の効果】
【００１２】
　本発明によれば、決済システムにおいて、コストを抑制しながら、情報漏洩に対するセキュリティーを強化できる。
【図面の簡単な説明】
【００１３】
【図１】本発明に係る第１実施形態の決済システムの構成を簡略化して表すブロック図である。
【図２】本発明に係る第２実施形態の決済システムの構成を簡略化して表すブロック図である。
【図３】第２実施形態の決済システムにて使用される加盟店情報をイメージで表す図である。
【図４】第２実施形態において、カード番号から変換されるトークンを説明する図である。
【図５】第２実施形態の決済システムにおける決済処理の流れを説明するシーケンス図である。
【図６】第２実施形態の決済システムにおけるファイル送信を含む処理の流れを説明するシーケンス図である。
【図７】第２実施形態におけるサーバが実行するトークン変換動作の一例を表すフローチャートである。
【図８】第２実施形態におけるサーバが実行するトークン不正利用の回避動作の一例を表すフローチャートである。
【図９】本発明に係る第３実施形態の決済システムの構成を説明するブロック図である。
【発明を実施するための形態】
【００１４】
　以下に、本発明に係る実施形態を図面を参照しつつ説明する。
【００１５】
　（第１実施形態）
　図１は、本発明に係る第１実施形態の決済システムの構成を簡略化して表すブロック図である。この第１実施形態の決済システム１は、決済に利用されるカード（例えば、クレジットカードやデビットカード）を識別するカード番号に基づいた決済を行うシステムである。この決済システム１は、決済要求側のコンピュータ装置２と、決済側のサーバ３とを備えている。なお、この決済システム１は、決済要求側のコンピュータ装置２として、複数のコンピュータ装置を備えることができるが、図１では、図示の簡略化のために、１つのコンピュータ装置２のみを表している。

【００１６】
サーバ３は、変換部８と、逆変換部９と、決済処理部１０とを備えている。変換部８は、コンピュータ装置２から受け取ったカード番号を乱数であるトークンに変換し当該トークンをコンピュータ装置２に返信する機能を備えている。サーバ３には、変換部８により生成（変換）されたトークンと、当該トークンに変換される前の変換元のカード番号とが関連付けられているデータが変換データとして保持される。
【００１７】
この第１実施形態では、その生成されるトークンは、変換元のカード番号をサーバ３に送信した発信元のコンピュータ装置２あるいは当該コンピュータ装置２を使用して決済を要求する事業者を識別可能な番号を含んでいる。なお、コンピュータ装置２を使用する事業者とは、この決済システム２に加盟している加盟店や決済代行業者を含んでいる。
【００１８】
逆変換部９は、コンピュータ装置２から決済の要求とトークンとが送信されてきた場合に、変換データに基づき、トークンを変換元のカード番号に戻し当該カード番号を決済処理部１０に出力する機能を備えている。
【００１９】
決済処理部１０は、コンピュータ装置２からの決済の要求に応じて、カード番号を利用した決済を処理する機能を備えている。
【００２０】
決済要求側のコンピュータ装置２は、取得部５と、処理部６とを備えている。取得部５は、カード番号をサーバ３に向けて送信することによって当該カード番号に対応するトークンを取得する機能を備えている。つまり、この第１実施形態では、取得部５がサーバ３に向けてカード番号を送信すると、サーバ３の変換部８がそのカード番号をトークンに変換し、当該トークンがコンピュータ装置２に返信されてくる。
【００２１】
処理部６は、カード番号とトークンとのうちのトークンのみを保持し、カード番号に代えてトークンをカード番号として用いて、カード番号を利用する処理を実行する機能を備えている。例えば、処理部６は、決済の要求と共に、カード番号に代えてトークンをサーバ３に送信する。これにより、サーバ３は、逆変換部９と決済処理部１０の機能によって、決済処理を実行し、この処理の結果を処理部６に通知する。これにより、処理部６は、決済処理の結果を例えば表示部（図１では図示せず）に表示する。
【００２２】
この第１実施形態の決済システム１は、決済要求側のコンピュータ装置２が、カード番号を保持せずカード番号に代えてトークンを保持し、当該トークンをカード番号として利用して処理を実行可能な構成を備えている。そのように、コンピュータ装置２がカード番号を持たないので、決済システム１は、コンピュータ装置２からカード番号が漏洩する危険性を低減できる。
【００２３】
また、この第１実施形態では、カード番号をトークンに変換する変換部８をサーバ３に設けたので、カード番号をトークンに変換する際に必要な情報（例えば、変換鍵等の情報）を決済要求側のコンピュータ装置２が保持しなくともよい。これにより、決済システム１は、次のような効果を得ることができる。例えば、仮に、コンピュータ装置２からトークンを含む情報が漏洩したとしても、コンピュータ装置２から漏洩した情報の中には、変換鍵等の情報は無いことから、決済システム１は、漏洩したトークンがカード番号に戻される事態を回避できる。このため、この第１実施形態の決済システム１は、情報漏洩に起因したカード番号の不正利用を防止できる。
【００２４】
さらにまた、トークンは、変換元のカード番号を送信した発信元のコンピュータ装置２、あるいは、当該コンピュータ装置２を使用して決済を要求する事業者を識別可能な番号を含んでいる。これにより、決済システム１は、次のような事態を防止できる。すなわち

、仮に、事業者Ａが持つコンピュータ装置２からトークンが漏洩し、事業者Ｂが持つコンピュータ装置２が利用されてその漏洩したトークンに基づいた決済がサーバ３に要求されたとする。この場合に、サーバ３は、トークンに含まれる事業者を識別する番号に基づいて、トークンが正規のコンピュータ装置２から送信されていないことを検知することができる。このため、決済システム１は、トークンの不正使用を防止できる。

【００２５】

このように、この第１実施形態の決済システム１は、コンピュータ装置２からの情報漏洩に対する対策が強化されており、セキュリティーを強化できる。

【００２６】

さらに、この第１実施形態の決済システム１は、カード番号等の保護対象の情報をコンピュータ装置２が持たないため、情報漏洩に対するセキュリティー対策を強化する部分を少なくできる。これにより、決済システム１は、情報漏洩に対するセキュリティーの低下を招くことなく、セキュリティー対策費用を抑制できる。

【００２７】

さらに、この第１実施形態では、サーバ３は、逆変換部９を備え、コンピュータ装置２から受け取ったトークンを逆変換部９によって変換元のカード番号に変換する機能を備えている。このため、カード番号を用いた処理を実行する機能を備えたサーバ３は、その機能部分を大きく変更することなく、この決済システム１に適用することができる。

【００２８】

（第２実施形態）

以下に、本発明に係る第２実施形態を説明する。

【００２９】

図２は、第２実施形態の決済システムの構成を簡略化して表すブロック図である。この第２実施形態の決済システム２０は、第１実施形態と同様に、決済に利用されるカード（例えば、クレジットカードやデビットカード）を識別するカード番号に基づいた決済を行うシステムである。この決済システム２０は、端末装置２１と、サーバ２２とを備えている。それら端末装置２１とサーバ２２は、スイッチングセンタとも呼ばれる専用の情報通信網２３を利用して接続することによって、通信可能である。

【００３０】

端末装置２１は、この決済システム２０に加盟している事業者である加盟店が所持し、商品やサービスの代金を決済する要求を送信する決済要求側のコンピュータ装置である。なお、決済システム２０に加盟している加盟店は複数有ることから、決済システム２０を構成する端末装置２１も複数有る。これら端末装置２１は、以下に述べるような共通の構成を備えているので、図２では、図示の簡略化を図るために、端末装置２１は１台のみ表されている。また、この第２実施形態では、決済システム２０に加盟しているカード会社も複数有ると想定しており、カード会社に備えられるサーバ２２も複数有る。これらサーバ２２は、以下に述べるような共通の構成を備えているので、図２では、図示の簡略化を図るために、サーバ２２は１台のみ表されている。

【００３１】

端末装置２１は、制御装置２４と、記憶装置２５と、入力装置２６と、表示部２７とを備えている。入力装置２６は、クレジットカードやデビットカード等の決済に利用するカード（以下、決済カードとも記す）から当該決済カードが保持しているカード記録情報を読み取り、制御装置２４に出力する構成を備えている。そのカード記録情報は、例えば、決済カードに備えられている磁気ストライプに保持されている情報であり、カード番号と、決済カードの所有者の氏名と、決済カードの有効期限と、カード認証用のコードとが含まれる。

【００３２】

表示部２７は、液晶画面等を備えたディスプレイ装置であり、この表示部２７の表示制御は、制御装置２４が行う。

【００３３】

記憶装置２５は、各種データやコンピュータプログラム（プログラム）が記憶される記憶媒体（図示せず）を備えている。この記憶媒体には、例えば、端末装置２１の動作を制御する制御手順が表されているコンピュータプログラムが格納されている。また、当該記憶媒体には、決済システム２０に加盟しているカード会社の識別情報と、当該カード会社のサーバ２２に接続するアドレス情報とが関連付けられている加盟カード会社情報が格納されている。

【００３４】

制御装置２４は、ＣＰＵ（Central Processing Unit）を備え、当該ＣＰＵが記憶装置２５から読み込んだコンピュータプログラムを実行することにより、端末装置２１の全体的な動作を制御する機能を備えている。例えば、制御装置２４は、決済に関わる機能部として、取得部２９と、処理部３０とを有している。

【００３５】

取得部２９は、入力装置２６によってカード記録情報が読み取られると、このカード記録情報からカード番号を抽出し、当該カード番号をサーバ２２に向けて情報通信網２３を利用して送信する機能を備えている。この第２実施形態では、取得部２９がカード番号を送信する送信先のサーバ２２のアドレス情報は、処理部３０から与えられる構成となっている。また、この第２実施形態では、取得部２９は、カード番号をサーバ２２に送信する際には、トークン変換要求電文に、送信対象のカード番号を添付し、当該電文を送信する。そのトークン変換要求電文とは、カード番号を乱数であるトークンに変換する要求を表す電文である。この電文には、当該電文を発信した発信元の端末装置２１のアドレス情報、および、当該端末装置２１を使用（所有）している決済システム２０の加盟店（事業者）に固有の加盟店識別情報（発信元識別情報）も添付される。

【００３６】

さらに、取得部２９は、サーバ２２から、トークンが添付されたトークン変換要求電文が返信されてくると、その電文からトークンを抽出し、当該トークンを処理部３０に供給する機能を備えている。

【００３７】

処理部３０は、カード番号を利用する処理を実行する機能を備えている。例えば、処理部３０は、入力装置２６が決済カードからカード記録情報を読み取ると、当該カード記録情報からカード番号を抽出する。そして、処理部３０は、カード番号から、決済に使用するカード会社の識別情報を抽出し、当該識別情報を記憶装置２５に格納されているカード会社情報に照合することにより、決済を要求するカード会社のサーバ２２のアドレス情報を読み出す。処理部３０は、その読み出したアドレス情報を取得部２９にトークン変換要求電文（カード番号）の送信先のアドレス情報として出力する。

【００３８】

また、処理部３０は、取得部２９からトークンを受け取ると、入力装置２６が決済カードから読み取ったカード記録情報のカード番号を消去し、受け取ったトークンをカード番号として含むカード記録情報を例えば記憶装置２５に格納する。

【００３９】

さらに、処理部３０は、カード番号を利用する処理をサーバ２２に対して要求する場合には、カード番号としてトークンを取引要求電文に添付し、当該電文を、処理を要求するカード会社のサーバ２２に送信する。その取引要求電文とは、サーバ２２に対して要求する処理の内容を含む電文である。その要求する処理としては、与信処理（決済を許可するか否かを判断する処理）や、売上処理（支払いを確定する処理）や、洗い替え処理（カードの有効性をチェックし、最新の情報に更新する処理）や、取消処理（決済を取り消す処理）などがある。

【００４０】

さらに、処理部３０は、カード番号を利用する上記以外の処理を実行する場合にも、カード番号としてトークンを利用して処理が実行される。上記のように、端末装置２１は、カード番号に対応するトークンをカード会社のサーバ２２から取得する処理以外の処理に

関しては、カード番号としてトークンを利用して処理が実行される。

【００４１】

さらにまた、処理部３０は、処理の結果等を表示部２７に表示すべく表示部２７の表示制御を実行する機能を備えている。また、処理部３０は、処理の結果とトークンとを関連付けて記憶装置２５に格納する機能を備えている。

【００４２】

サーバ２２は、決済を実行するカード会社に属し、この決済システム２０に加盟している加盟店からの要求に応じて決済に関わる処理を実行する機能を備えている。このサーバ２２は、制御装置３１と、記憶装置３２とを備えている。記憶装置３２は、各種データやコンピュータプログラム（プログラム）を記憶する記憶媒体を有し、当該記憶媒体には、サーバ２２の全体的な動作を制御する制御手順を表すコンピュータプログラムが格納されている。

【００４３】

制御装置３１は、例えばＣＰＵ（Central Processing Unit）を備え、このＣＰＵが記憶装置３２から読み込んだコンピュータプログラムを実行することにより、サーバ２２の全体的な動作を制御する構成を備える。この制御装置３１は、決済に関わる機能部として、決済処理部３４と、トークン部３５とを備えている。

【００４４】

決済処理部３４は、端末装置２１から、トークン変換要求電文を受け取った場合には、このトークン変換要求電文をトークン部３５に出力する機能を備えている。また、この決済処理部３４は、トークン部３５から、トークンが添付されたトークン変換要求電文を受け取った場合には、そのトークン変換要求電文を端末装置２１に返信する機能を備えている。さらに、決済処理部３４は、端末装置２１から、トークンが添付された取引要求電文を受け取った場合には、その取引要求電文をトークン部３５に出力する機能を備えている。さらにまた、決済処理部３４は、トークン部３５から、カード番号が添付された取引要求電文を受け取った場合には、そのカード番号に基づいて、取引要求電文にて要求されている処理を実行する機能を備えている。さらに、決済処理部３４は、その取引要求電文に応じた処理により、カード番号が含まれているファイル等のデータを加盟店に向けて返信する場合には、その送信対象のデータ（ファイル）をトークン部３５に出力する機能を備えている。

【００４５】

トークン部３５は、変換部３７と、逆変換部３８と、中断部３９と、報知部４０とを備えている。変換部３７は、決済処理部３４から、トークン変換要求電文を受け取った場合には、そのトークン変換要求電文からカード番号を抽出し、このカード番号をトークン（乱数）に変換する機能を備えている。この第２実施形態では、変換部３７は、次のようにカード番号をトークンに変換する。

【００４６】

例えば、この第２実施形態では、決済システム２０に加盟している加盟店毎に、トークン変換鍵と、トークンとして使用する番号帯（以下、トークン番号帯とも記す）とが設定されている。トークン変換鍵とは、カード番号をトークンに変換するアルゴリズムを表すデータである。また、トークン番号帯（番号範囲）は、他の加盟店に対して設定されたトークン番号帯と重複しない番号帯である。カード番号には、決済を要求するカード会社を識別する番号が含まれており、トークン番号帯は、そのカード会社の識別番号が設定される番号帯（番号範囲）と重複しないように設定されている。それら設定されたトークン変換鍵とトークン番号帯の情報は、対応する加盟店の識別情報に関連付けられた状態で加盟店情報として記憶装置３２に格納されている。図３は、その加盟店情報をイメージで表した図である。なお、加盟店が同じでも、カード会社が異なると、加盟店に対して設定されるトークン変換鍵は異なる。

【００４７】

さらに、この第２実施形態では、変換部３７により変換（生成）されるトークンは、当

該トークンに変換される前の変換元のカード番号と同じ桁数を備えている。図４は、変換部３７により変換されるトークンの構成を説明するイメージ図である。このトークンには、先頭から設定の桁数まで（つまり、カード番号におけるカード会社を識別する番号が配置される部分）の値として、加盟店毎に設定されているトークン番号帯内の値が、変換元のカード番号を発信した加盟店の番号として与えられる。この加盟店番号は、前述の如く、カード会社を識別する番号帯から外れた番号であることから、この加盟店番号の配置位置の番号をチェックすることにより、電文から抽出した番号列がトークンとカード番号の何れであるかを識別できる。

【００４８】

また、この第２実施形態では、トークンには、残りの桁の値として、加盟店毎に設定されているトークン変換鍵でもって変換対象のカード番号を変換した値がカード変換番号として与えられる。上記のように、この第２実施形態では、トークンは、カード決済を要求する発信元の加盟店の情報が含まれる。このため、同じカード番号であっても、カードを利用する加盟店が異なると、カード番号は、異なるトークンに変換されることになる。

【００４９】

この第２実施形態では、変換部３７は、トークンをさらに別のトークンに変換してしまう事態を防止する機能を備えている。すなわち、変換部３７は、受け取ったトークン変換要求電文にカード番号として添付されている番号列を抽出し、さらに、この番号列から、カード会社識別番号が配置されている部分の番号を抽出する。そして、変換部３７は、そのカード会社識別番号としての番号列を、記憶装置３２に予め格納されているカード会社識別番号の番号帯の情報に照合し、抽出した番号列がその番号帯内にあるか否かを判断する。これにより、変換部３７は、トークン変換要求電文から抽出した番号列がカード番号であり、トークンではないことを確認する。

【００５０】

この確認の後に、変換部３７は、トークン変換要求電文から加盟店識別情報を抽出し、記憶装置３２の加盟店情報から、その加盟店識別情報に関連付けられているトークン番号帯の情報とトークン変換鍵を読み出す。そして、変換部３７は、その読み出したトークン番号帯の情報とトークン変換鍵を利用して、トークン変換要求電文から抽出したカード番号をトークンに変換する。なお、変換部３７は、トークン変換要求電文から抽出した番号列がトークンであると判断した場合には、トークンへの変換処理を中止する。つまり、変換部３７は、トークンをさらにトークンに変換することを回避する。また、この状態は、異常であることから、変換部３７は、警戒信号を中断部３９と報知部４０に送信する。

【００５１】

さらに、変換部３７は、変換したトークンと、当該トークンに変換される前の変換元のカード番号とが関連付けられているデータ（変換データ）を生成し、当該変換データを記憶装置３２に格納する機能を備えている。さらにまた、変換部３７は、生成したトークンをカード番号に代えてトークン変換要求電文に添付し、当該トークン変換要求電文を決済処理部３４に出力する。これにより、決済処理部３４の機能によって、トークンが添付されたトークン変換要求電文は、端末装置２１に返信される。

【００５２】

さらに、変換部３７は、決済処理部３４から受け取った送信対象のファイル等のデータにカード番号が含まれている場合には、記憶装置３２の変換データに基づき、そのカード番号を、当該カード番号に関連付けられているトークンに変換する機能を備えている。そして、変換部３７は、カード番号に代わって変換後のトークンを含む送信対象のデータを決済処理部３４に出力する。これにより、決済処理部３４の機能によって、送信対象のデータが、当該データを要求した加盟店の端末装置２１に送信される。つまり、サーバ２２は、カード番号を含む様々なデータを保持しているのに対し、端末装置２１は、カード番号を保持しておらず、カード番号としてトークンを保持している。このため、カード番号を含むデータがサーバ２２から端末装置２１に送信されても、端末装置２１は、そのデータを用いる例えば有効性判定処理（洗い替え処理）等の処理を行うことができない。この

ような問題を防止するために、この第２実施形態では、上記のように、サーバ２２から端末装置２１に送信されるデータは、カード番号をトークンに変換した後に、送信される。

【００５３】

逆変換部３８は、端末装置２１が送信した取引要求電文を決済処理部３４から受け取った場合には、取引要求電文からトークンを抽出し、抽出したトークンを記憶装置３２に格納されている変換データに基づいて変換元のカード番号に変換する機能を備えている。

【００５４】

この第２実施形態では、逆変換部３８は、さらに、次のようなセキュリティー機能も備えている。つまり、逆変換部３８は、取引要求電文からトークンだけでなく加盟店識別情報をも抽出する。そして、逆変換部３８は、その加盟店識別情報に関連付けられているトークン番号帯の情報を記憶装置３２から読み出す。さらに、逆変換部３８は、抽出したトークンにおける加盟店番号が、その読み出したトークン番号帯に含まれる場合には、そのトークンは正規の加盟店から送信されたと判断し、トークンを承認する。そして、逆変換部３８は、そのように承認したトークンを前記の如く変換データに基づいて変換元のカード番号に変換し、当該カード番号を取引要求電文に添付し、決済処理部３４に出力する。これにより、決済処理部３４は、トークンではなく、カード番号に基づいた処理を実行することができる。

【００５５】

これに対し、逆変換部３８は、抽出したトークンの加盟店番号が、取引要求電文の加盟店識別情報に関連付けられているトークン番号帯から外れている場合には、当該トークンは不正利用されている可能性が高いと判断する。そして、逆変換部３８は、そのトークンを承認せず、変換元のカード番号への変換処理は中止する。さらに、逆変換部３８は、トークンを承認しなかった場合には、その旨を知らせる警戒信号を中断部３９と報知部４０に送信する。

【００５６】

中断部３９は、変換部３７又は逆変換部３８から警戒信号を受けた場合には、トークンを送信してきた加盟店との決済処理を中断する指示を決済処理部３４に向けて出力する機能を備えている。これにより、決済処理部３４は、その中断処理対象の加盟店との決済を中断する。なお、例えば、サーバ２２の管理者等により中断解除の指令が加えられた場合に、決済処理部３４は、その決済の中断状態を解除する。

【００５７】

報知部４０は、変換部３７又は逆変換部３８から警戒信号を受けた場合には、警戒が必要な事態が発生したことを知らせる報知処理を実行する機能を備えている。例えば、その報知処理として、報知部４０は、予め定められた通報先（例えば、サーバ２２の管理者のコンピュータ装置）に、異常発生とその内容を連絡するメールを送信する。その通報先のメールアドレスは、予め、異常発生時のメール通報先の情報として、記憶装置３２に登録されている。

【００５８】

この第２実施形態の決済システム２０は、端末装置２１（加盟店）がカード番号に代えてトークンを保持し、また、トークンが加盟店に応じた情報（番号）を含んでいることから、第１実施形態と同様の効果を得ることができる。つまり、決済システム２０は、コストを抑制しつつ、端末装置２１からの情報漏洩に対するセキュリティーを強化できる。

【００５９】

また、この第２実施形態の決済システム２０は、トークンに対するチェック機能を有していることから、トークンの不正利用を防止できる。

【００６０】

さらに、この決済システム２０は、逆変換部３８を備え、当該逆変換部３８によりトークンをカード番号に戻す機能を備えているので、カード番号を利用した処理を実行する決済処理部３４は、大きな変更を行うことなく、カード番号を用いる処理を実行できる。換言すれば、決済システム２０は、サーバ２２において、カード番号を用いる処理を大きく

変更することなく、トークンを利用した決済取引の仕組みを導入することができる。

【００６１】

以下に、決済システム２０における決済処理の主な流れを図５を利用して説明する。図５は、決済システム２０における決済処理の流れを説明するシーケンス図である。

【００６２】

例えば、端末装置２１は、入力装置２６が決済カードからカード記録情報を読み取ると（ステップＳ１０１）、処理部３０により、そのカード記録情報に基づき決済を要求するカード会社を特定する。そして、端末装置２１は、取得部２９により、カード記録情報から抽出したカード番号をトークン変換要求電文に添付し、当該電文を、決済を要求するカード会社のサーバ２２に向けて送信する（ステップＳ１０２）。

【００６３】

サーバ２２の決済処理部３４は、カード番号が添付されたトークン変換要求電文を受け取ると（ステップＳ１０３）、その電文を変換部３７に出力する。変換部３７は、トークン変換要求電文を受け取ると、その電文に添付されているカード番号をトークンに変換する（ステップＳ１０４）。そして、変換部３７は、変換したトークンと当該トークンに変換される前の変換元のカード番号が関連付けられた変換データを作成し、当該変換データを記憶装置３２に格納する。また、変換部３７は、その変換したトークンをカード番号に代えてトークン変換要求電文に添付し、当該電文を決済処理部３４に出力する。決済処理部３４は、トークンが添付されたトークン変換要求電文を受け取ると（ステップＳ１０５）、当該トークン変換要求電文を端末装置２１に返信する。

【００６４】

端末装置２１は、トークン変換要求電文が返信されてくると、当該電文からトークンを抽出し、この抽出したトークンを取引要求電文（ここでは、決済要求電文）に添付する。そして、端末装置２１は、その電文を、決済を要求するカード会社におけるサーバ２２に向けて出力する（ステップＳ１０７）。

【００６５】

サーバ２２の決済処理部３４は、決済要求電文を受け取ると（ステップＳ１０８）、その電文を逆変換部３８に出力する。逆変換部３８は、決済要求電文からトークンを抽出し、当該トークンを変換データに基づいてカード番号に変換する（ステップＳ１０９）。このトークンから戻された（変換された）カード番号を含む決済要求電文は決済処理部３４に戻される。これにより、決済処理部３４は、カード番号を利用して決済処理を実行する（ステップＳ１１０）。然る後に、決済処理部３４は、処理が終了すると、カード番号を含む処理結果を変換部３７に出力する。これにより、変換部３７は、処理結果に含まれているカード番号を変換データに基づきトークンに変換する（ステップＳ１１１）。そして、変換部３７は、カード番号に代えてトークンを含む処理結果を決済処理部３４に出力する。決済処理部３４は、そのトークンを含む処理結果を端末装置２１に送信する（ステップＳ１１２）。端末装置２１は、受け取ったトークンと処理結果を保存する（ステップＳ１１３）。

【００６６】

次に、決済システム２０におけるファイル送信（転送）を含む処理の主な流れを図６を利用して説明する。図６は、ファイル送信を含む処理（例えば、売上処理や有効性判定処理（洗い替え処理））の流れを説明するシーケンス図である。

【００６７】

例えば、端末装置２１は、売上処理や洗い替え処理によりファイルをサーバ２２に送信（転送）する場合には、取引要求電文に送信対象のファイルを添付し、処理を要求するカード会社のサーバ２２に向けて取引要求電文を送信（転送）する（ステップＳ２０１）。端末装置２１は、カード番号を保持していないので、その送信したファイルには、カード番号としてのトークンが含まれている。

【００６８】

サーバ２２の決済処理部３４は、ファイルが添付された取引要求電文を受け取ると（ス

テップＳ２０２）、当該取引要求電文を逆変換部３８に出力する。逆変換部３８は、取引要求電文に添付されているファイルからトークンを抽出し、抽出したトークンを変換データに基づいて変換元のカード番号に変換する（ステップＳ２０３）。そして、逆変換部３８は、変換したカード番号をファイルに書き込み、当該ファイルを添付した取引要求電文を決済処理部３４に出力する。

【００６９】

決済処理部３４は、カード番号を含むファイルに基づいて、取引要求電文により要求されている処理を実行する（ステップＳ２０４）。決済処理部３４は、処理が終了すると、処理結果を含むファイルを取引要求電文と共に変換部３７に出力する。変換部３７は、受け取った取引要求電文に添付されているファイルからカード番号を抽出し、当該抽出したカード番号をトークンに変換する（ステップＳ２０５）。そして、変換部３７は、カード番号をトークンに置き換えたファイルを取引要求電文に添付し当該取引要求電文を決済処理部３４に出力する。決済処理部３４は、トークンを含むファイルを備えた取引要求電文を端末装置２１に返信する（ステップＳ２０６）。端末装置２１は、ファイルを受け取ると、そのファイルを使用した処理を実行する。例えば、端末装置２１は、記憶装置２５に保持しているトークンを、受け取ったファイルに照合することによって、トークン（つまり、カード番号）の有効性を判定する。

【００７０】

次に、サーバ２２におけるトークン変換動作に係る動作例を図７を利用して説明する。図７は、サーバ２２の制御装置３１によるトークン変換の動作例を表すフローチャートである。

【００７１】

ここでは、端末装置２１は、カード番号をカード記録情報の状態でトークン変換要求電文に添付する場合と、カード記録情報から抽出したカード番号をトークン変換要求電文に添付する場合とがあるとする。

【００７２】

例えば、制御装置３１は、トークン変換要求電文を受け取ると（ステップＳ３０１）、変換部３７により、そのトークン変換要求電文から、添付されているデータを抽出する（ステップＳ３０２）。そして、制御装置３１は、その添付されているデータがカード番号であるか否か（カード番号であるかカード記録情報であるか）を判断する（ステップＳ３０３）。これにより、制御装置３１は、添付のデータがカード番号そのものではなくカード記録情報であると判断した場合には、そのカード記録情報からカード番号を抽出する（ステップＳ３０４）。

【００７３】

制御装置３１は、添付のデータがカード番号であると判断した場合、または、カード記録情報からカード番号を抽出した後に、トークン変換要求電文に含まれている情報に基づいて、当該電文を発信した発信元を特定する（ステップＳ３０５）。そして、制御装置３１は、記憶装置３２から発信元の加盟店情報を読み出し（ステップＳ３０６）、加盟店情報に含まれているトークン変換鍵とトークン番号帯の情報とに基づいて、変換対象のカード番号をトークンに変換する（ステップＳ３０７）。

【００７４】

このようにして制御装置３１は、端末装置２１の要求に応じて、カード番号をトークンに変換する。

【００７５】

次に、サーバ２２におけるトークン不正利用を防止する動作例を図８を利用して説明する。図８は、サーバ２２の制御装置３１によるトークン不正利用を防止する動作例を表すフローチャートである。

【００７６】

例えば、制御装置３１は、端末装置２１からカード番号を含む電文を受け取ると（ステップＳ４０１）、この電文からカード番号を抽出する（ステップＳ４０２）。そして、制

御装置３１は、その抽出したカード番号が真にカード番号であるか否かを判断する（ステップＳ４０３）。これにより、制御装置３１は、真にカード番号であることを確認すると、当該カード番号を変換部３７によりトークンに変換する（ステップＳ４０４）。これにより、制御装置３１は、正常にトークン変換動作を終了する。そして、制御装置３１は、引き続き、端末装置２１から受け取った電文に含まれている要求の処理を行う。

【００７７】

一方、ステップＳ４０３の判断動作により、制御装置３１は、電文にカード番号として添付されていた番号列がカード番号ではなくトークンであったと判断した場合には、次のように動作する。すなわち、制御装置３１は、そのトークンから、記憶装置３２の加盟店情報を利用して、そのトークンを含む電文を送信（発信）した発信元の端末装置２１（加盟店）を特定する（ステップＳ４０５）。その後、制御装置３１は、逆変換部３８により、そのトークンを変換データに基づいてカード番号に変換する（ステップＳ４０６）。

【００７８】

然る後に、制御装置３１は、そのカード番号が取り扱っている番号であるか否かを判断する（ステップＳ４０７）。そして、制御装置３１は、取り扱っている番号であると判断した場合には、報知部４０により、予め定められている通報先に例えば電子メールを利用して、警戒すべき事態が発生したことを通報する（ステップＳ４０８）。さらに、制御装置３１は、中断部３９により、トークンを発信した加盟店との取り引きを中断する（ステップＳ４０９）。

【００７９】

そして、制御装置３１は、トークンに対応する変換元のカード番号を取り扱っている場合にも取り扱っていない場合にも、トークンを発信した端末装置２１に向けてエラーメッセージを返信する（ステップＳ４１０）。これにより、トークン不正利用を防止する動作が終了する。

【００８０】

（第３実施形態）

以下に、本発明に係る第３実施形態を説明する。なお、この第３実施形態の説明において、第２実施形態と同一名称部分には同一符号を付し、その共通部分の重複説明は省略する。

【００８１】

この第３実施形態の決済システム２０は、第２実施形態の構成に加えて、加盟店が、取り引きするカード会社を変更する場合を考慮した機能を備えている。すなわち、この第３実施形態では、図９に示されるように、端末装置２１の制御装置２４は、機能部として、変更部２８を備えている。なお、図９においては、第３実施形態の決済システム２０における構成の説明に主に関係のある部分が抜き出されて表されている。

【００８２】

変更部２８は、取り引きするカード会社を変更する指令が例えば端末装置２１の操作者により加えられた場合に、次のように動作する機能を備えている。すなわち、変更部２８は、取り引きを停止するカード会社（例えば、図９におけるカード会社α）により生成されたトークンを取引要求電文の一つである情報返還要求電文に添付し、そのカード会社に送信する。

【００８３】

情報返還要求電文は取引要求電文の一つであることから、この第３実施形態では、サーバ２２の制御装置３１は、情報返還要求電文が加えられると、第２実施形態で述べた取引要求電文が加えられた処理を実行する。つまり、制御装置３１の決済処理部３４は、その電文を逆変換部３８に出力する。逆変換部３８は、電文に添付されているトークンをカード番号に変換し、当該カード番号を情報返還要求電文に添付し、決済処理部３４に出力する。決済処理部３４は、そのカード番号が添付された情報返還要求電文を端末装置２１に返信する。

【００８４】

変更部２８は、さらに、そのカード番号が添付された情報返還要求電文が返信されてきた場合には、そのカード番号を保持することなく、当該カード番号をトークン変換要求電文に添付する。そして、変更部２８は、その電文を、取り引きを開始する変更後のカード会社（例えば、図９におけるカード会社β）に向けて送信する。これにより、変更後のカード会社βの制御装置３１は、第２実施形態で述べたように、そのトークン変換要求電文に応じて、変換部３７により、カード番号をトークンに変換し、変換したトークンをトークン変換要求電文に添付して返信する。この新たなトークンは、取り引きを停止するカード会社αにより生成されたトークンとは異なる番号列となる。

【００８５】

変更部２８は、返信されてきたトークン変換要求電文に添付されているトークンを新たなトークンとして記憶装置２５における変更前のトークンに上書きする。

【００８６】

この第３実施形態においては、端末装置２１は、変更部２８を備えているので、第２実施形態の効果に加えて、さらに次のような効果を得ることができる。すなわち、端末装置２１は、取り引きするカード会社を変更する場合に、端末装置２１の操作者がカード番号を取り扱うことなく、取り引きを停止するカード会社から変更後のカード会社にカード番号等の情報を移行できる。このこともカード番号等の情報が漏洩する事態の防止に寄与する。つまり、この第３実施形態の決済システム２０は、情報漏洩に対するセキュリティーをより強化することができる。

【００８７】

（その他の実施形態）

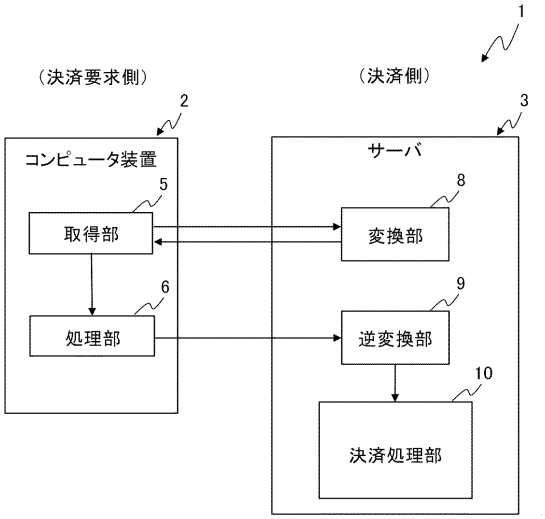
なお、この発明は第１～第３の実施形態に限定されず、様々な実施の形態を採り得る。例えば、第２と第３の実施形態では、決済要求側のコンピュータ装置として店舗に設置されている端末装置２１を例にしており、当該端末装置２１の入力装置２６は、決済カードからカード記録情報を読み取る構成を備えている。これに対し、決済要求側のコンピュータ装置は、決済代行業者のコンピュータ装置であってもよく、この場合には、例えば、入力装置２６は、インターネット等の情報通信網を利用して決済カードのカード番号を受け取る通信部としての機能を備える。

【符号の説明】

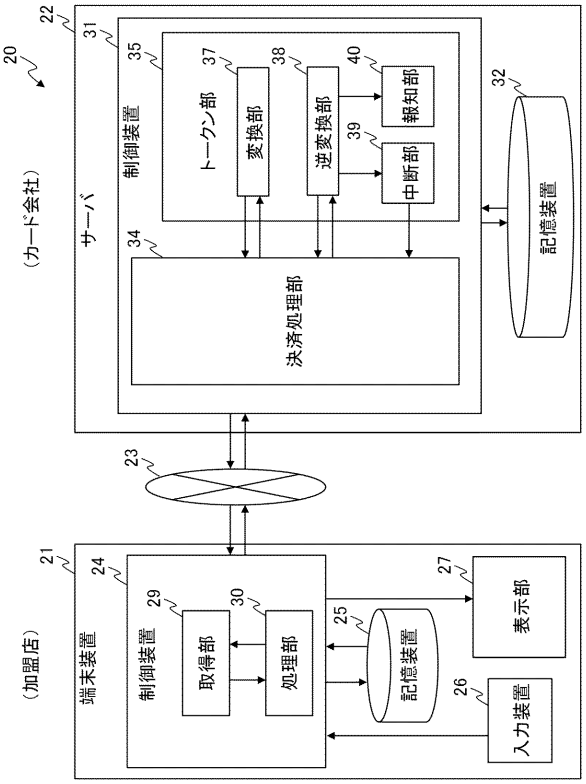
【００８８】

１，２０　決済システム
２　コンピュータ装置
３，２２　サーバ
５，２９　取得部
６，３０　処理部
８，３７　変換部
９，３８　逆変換部
１０，３４　決済処理部

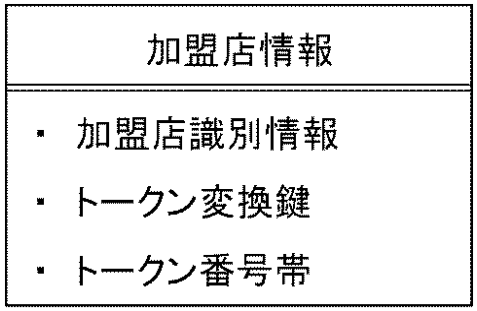
【図１】


1
（決済要求側）
（決済側）
2
3
コンピュータ装置
サーバ
5
8
取得部
変換部
6
9
処理部
逆変換部
10
決済処理部

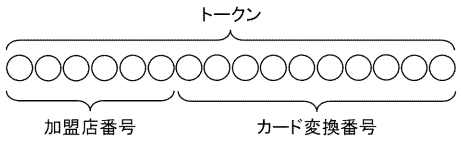
【図２】


20
22
31
（カード会社）
サーバ
制御装置
35
トークン部
37
変換部
38
逆変換部
40
報知部
39
中断部
32
記憶装置
34
決済処理部
23
21
24
（加盟店）
端末装置
制御装置
29
取得部
30
処理部
25
記憶装置
27
表示部
26
入力装置

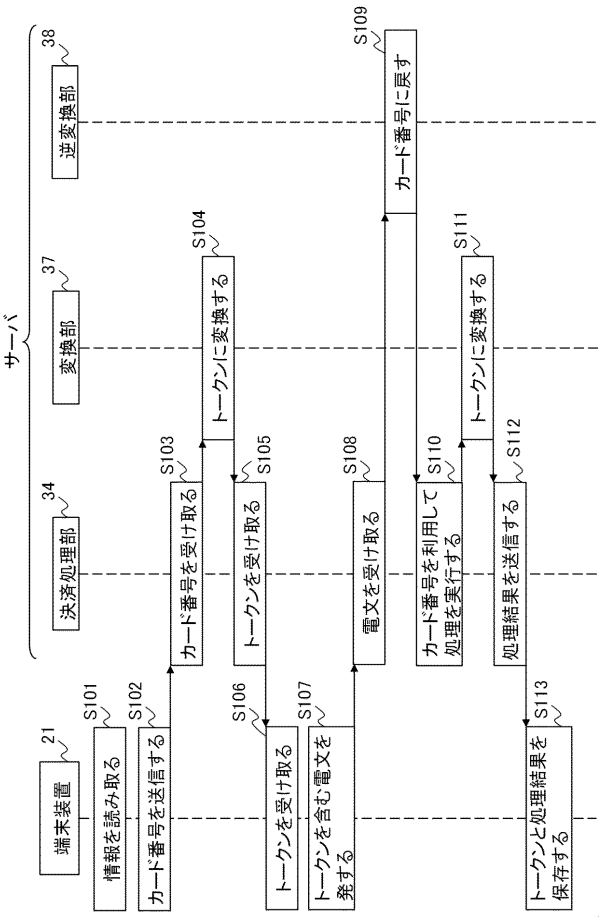
【図３】


加盟店情報
▪ 加盟店識別情報
▪ トークン変換鍵
▪ トークン番号帯

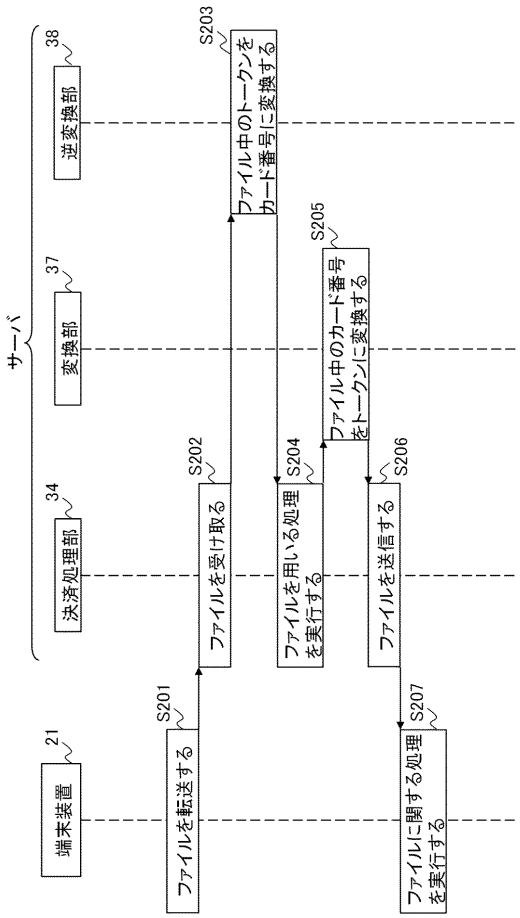
【図４】


トークン
加盟店番号
カード変換番号

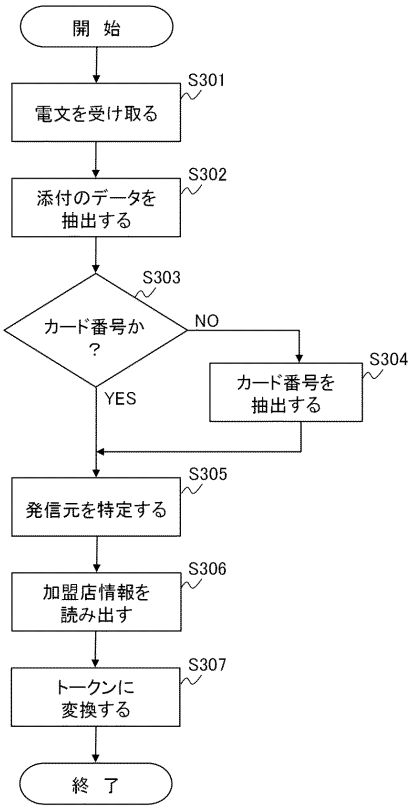
【図５】


サーバ
38
逆変換部
37
変換部
34
決済処理部
21
端末装置
S101
情報を読み取る
S102
カード番号を送信する
S103
カード番号を受け取る
S104
トークンに変換する
S105
トークンを受け取る
S106
トークンを受け取る
S107
トークンを含む電文を発する
S108
電文を受け取る
S109
カード番号に戻す
S110
カード番号を利用して処理を実行する
S111
トークンに変換する
S112
処理結果を送信する
S113
トークンと処理結果を保存する

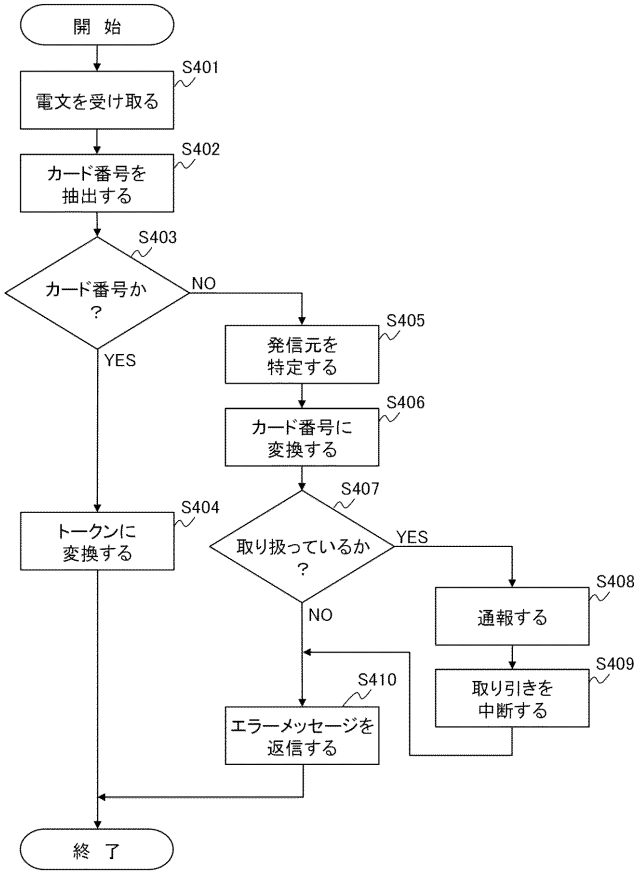
【図６】


サーバ
逆変換部
38
変換部
37
決済処理部
34
端末装置
21
S201
ファイルを転送する
S202
ファイルを受け取る
S203
ファイル中のトークンをカード番号に変換する
S204
ファイルを用いる処理を実行する
S205
ファイル中のカード番号をトークンに変換する
S206
ファイルを送信する
S207
ファイルに関する処理を実行する

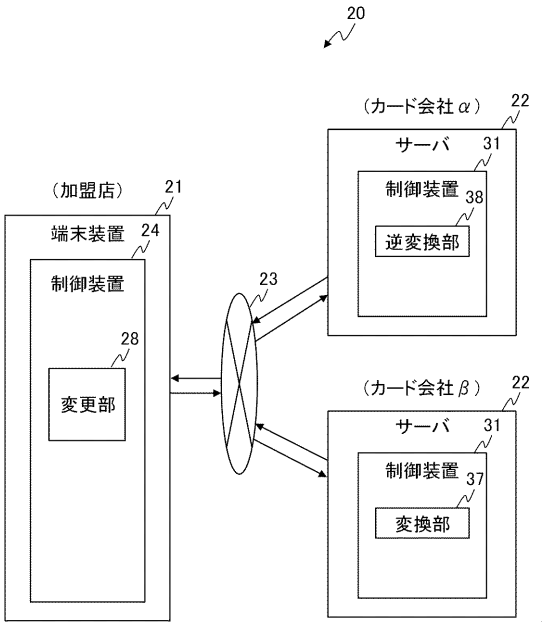
【図７】


開 始
S301
電文を受け取る
S302
添付のデータを抽出する
S303
カード番号か？
NO
YES
S304
カード番号を抽出する
S305
発信元を特定する
S306
加盟店情報を読み出す
S307
トークンに変換する
終 了

【図８】


開 始
S401
電文を受け取る
S402
カード番号を抽出する
S403
カード番号か？
NO
YES
S404
トークンに変換する
S405
発信元を特定する
S406
カード番号に変換する
S407
取り扱っているか？
YES
NO
S408
通報する
S409
取り引きを中断する
S410
エラーメッセージを返信する
終 了

【図９】


20
（加盟店）
21
端末装置
24
制御装置
28
変更部
23
（カード会社α）
22
サーバ
31
制御装置
38
逆変換部
（カード会社β）
22
サーバ
31
制御装置
37
変換部