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

特許第5657895号
(P5657895)

(45)発行日　平成27年1月21日(2015.1.21)　(24)登録日　平成26年12月5日(2014.12.5)

(51)Int.Cl.　F I
G06Q 20/40 (2012.01)　G06Q 20/40 110
G06Q 20/42 (2012.01)　G06Q 20/42
G06Q 40/02 (2012.01)　G06Q 40/02 160

請求項の数 28　(全 24 頁)

(21)出願番号　特願2009-551832 (P2009-551832)
(86)(22)出願日　平成20年2月27日 (2008.2.27)
(65)公表番号　特表2010-520534 (P2010-520534A)
(43)公表日　平成22年6月10日 (2010.6.10)
(86)国際出願番号　PCT/US2008/055195
(87)国際公開番号　WO2008/106560
(87)国際公開日　平成20年9月4日 (2008.9.4)
審査請求日　平成23年2月25日 (2011.2.25)
(31)優先権主張番号　11/680,594
(32)優先日　平成19年2月28日 (2007.2.28)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　508168790
ビザ　ユー．エス．エー．インコーポレイテッド
アメリカ合衆国　９４１２８－８９９９
カリフォルニア、　サンフランシスコ、ピー．オー．ボックス　８９９９
(74)代理人　110000855
特許業務法人浅村特許事務所
(72)発明者　ハマド、アイマン
アメリカ合衆国、カリフォルニア、プレザントン、コルテ　モンタナス　６０４８
(72)発明者　ディクソン、フィリップ　ビー．
アメリカ合衆国、カリフォルニア、サンディエゴ、ジュンカス　コート　７３８９

最終頁に続く

(54)【発明の名称】トランジット検証値を使用したデータカードの認証

(57)【特許請求の範囲】
【請求項１】
携帯型消費者機器であって、
プロセッサと、
前記プロセッサに接続されたメモリと、からなり、
前記メモリは、
小売りアプリケーションデータを受け取り、それを処理して小売り決済の承諾または拒否を行う発行者の小売り処理システムで使用するための予め定められた小売アプリケーションデータフィールド構造を有し、小売りアプリケーションデータに関連する小売り会員番号（ＰＡＮ）を含む、小売り決済に関連して使用するための小売りアプリケーションデータと、
トランジット機関業者のトランジット料金装置で使用するためのアクセス決済データフィールド構造を有し、アクセス決済に関連して使用するためのアクセス決済アプリケーションデータであって、此処でアクセス決済アプリケーションデータのアクセス決済データフィールド構造は、小売りアプリケーションデータフィールド構造に類似し、トランジット検証値が有効でありアクセス決済ＰＡＮがトランジット機関業者のネガティブ・リストに含まれていないと判断されるとき携帯型消費者機器を認証するためにトランジット環境のトランジット料金装置によって使用される当該アクセス決済ＰＡＮおよび当該トランジット検証値を含む、アクセス決済アプリケーションデータと、を格納しており、トランジット検証値は、携帯型消費者機器と関連してオフライン検証処理に適合し、携帯型消費

者機器が偽造でないことを認証するためにトランジット環境のトランジット料金装置によって使用され且つ動的な値として組み込まれて携帯型消費者機器の１つ以上のプロセッサによって可変である、
前記携帯型消費者機器。
【請求項２】
請求項１記載の携帯型消費者機器において、アクセス決済アプリケーションデータのアクセス決済データフィールド構造が、磁気ストライプデータ（ＭＳＤ）構造に一致し、アクセス決済ＰＡＮがＭＳＤ構造の商業分野コード（ＭＣＣ）に関連している、前記携帯型消費者機器。
【請求項３】
請求項２記載の携帯型消費者機器において、ＭＣＣデータがトランジット分野に対応し、トランジットＭＣＣの範囲外の携帯型消費者機器の全てのアクセス決済を発行者が拒否する、前記携帯型消費者機器。
【請求項４】
請求項２記載の携帯型消費者機器において、トランジット検証値がＭＳＤ構造の個人識別番号（ＰＩＮ）データフィールドに格納される、前記携帯型消費者機器。
【請求項５】
請求項２記載の携帯型消費者機器において、前記ＭＳＤ構造が、携帯型消費者機器に格納するための発行者指定データを含む、前記携帯型消費者機器。
【請求項６】
請求項１記載の携帯型消費者機器が更に、携帯型消費者機器のアクセス決済アプリケーションデータに格納するための発行者指定データを含む、前記携帯型消費者機器。
【請求項７】
請求項１記載の携帯型消費者機器において、携帯型消費者機器が非接触スマートカード機器を含む、前記携帯型消費者機器。
【請求項８】
アクセス決済アプリケーションデータを含む携帯型消費者機器であって、
プロセッサと、
前記プロセッサに接続されたメモリと、からなり、
前記メモリは、
携帯型消費者機器と関連してオフライン検証処理に適合したトランジット検証値を含む、アクセス決済データを含むアクセス決済アプリケーションデータストリングを格納するように構成されており、
ここで、アクセス決済アプリケーションデータはトランジット機関業者のトランジット料金装置で使用するためのアクセス決済データフィールド構造とアクセス決済会員番号（ＰＡＮ）を有し、此処でアクセス決済データフィールド構造は、携帯型消費者機器の発行者の小売り処理システムで使用するための小売りアプリケーションデータフィールド構造に類似しており、発行者は小売りアプリケーションデータを受け取り、それを処理して小売り決済の承諾または拒否を行い、その小売りアプリケーションデータフィールド構造は小売りアプリケーションデータに関連する小売り会員番号（ＰＡＮ）を含み、
ここでアクセス決済アプリケーションデータのアクセス決済データフィールド構造は磁気ストライプデータ（ＭＳＤ）構造に一致し、アクセス決済ＰＡＮとトランジット検証値は、トランジット検証値が有効でありアクセス決済ＰＡＮがトランジット機関業者のネガティブ・リストに含まれていないと判断されるとき携帯型消費者機器を認証するためにトランジット環境のトランジット料金装置によって使用され、携帯型消費者機器と関連してオフライン検証処理に適合したトランジット検証値は、携帯型消費者機器が偽造でないことを認証するためにトランジット環境のトランジット料金装置によって使用され、且つ動的な値として組み込まれて携帯型消費者機器の１つ以上のプロセッサによって可変である、前記携帯型消費者機器。
【請求項９】

請求項８記載の携帯型消費者機器において、トランジット検証値がＭＳＤ構造の個人識別番号（ＰＩＮ）データフィールドに格納される、前記携帯型消費者機器。
【請求項１０】
請求項８記載の携帯型消費者機器において、携帯型消費者機器が更に小売りデータストリングを格納するように構成されており、ここで小売りデータストリングはトランジット処理システムからはアクセスされず、またアクセス決済データストリングは小売りシステムの小売りＰＯＳ端末からはアクセスされない、前記携帯型消費者機器。
【請求項１１】
請求項８記載の携帯型消費者機器において、アクセス決済アプリケーションデータはアクセス決済ＰＡＮを含み、これはアクセス決済を選択的に承諾するために発行者によって使用される、前記携帯型消費者機器。
【請求項１２】
請求項１１記載の携帯型消費者機器において、アクセス決済ＰＡＮがＭＳＤ構造の商業分野コード（ＭＣＣ）に関連する、前記携帯型消費者機器。
【請求項１３】
請求項１２記載の携帯型消費者機器において、ＭＣＣデータがトランジット分野に対応し、トランジットＭＣＣの範囲外の携帯型消費者機器の全てのアクセス決済を発行者が拒否する、前記携帯型消費者機器。
【請求項１４】
請求項８記載の携帯型消費者機器が更に、携帯型消費者機器のアクセス決済アプリケーションデータ内にデータを格納するための発行者指定データファイルを含む、前記携帯型消費者機器。
【請求項１５】
請求項１４記載の携帯型消費者機器において、発行者指定データファイルがＭＳＤデータ構造内にある、前記携帯型消費者機器。
【請求項１６】
請求項８記載の携帯型消費者機器において、トランジット検証値が携帯型消費者機器の使用中に携帯型消費者機器のプロセッサによって動的に変更される、前記携帯型消費者機器。
【請求項１７】
請求項８記載の携帯型消費者機器において、携帯型消費者機器が非接触スマートカード機器を含む、前記携帯型消費者機器。
【請求項１８】
トランジット機関業者のコンピュータによってアクセス決済を処理するための方法であって、この処理方法が、
アクセス決済アプリケーションデータを携帯型消費者機器からトランジット機関業者のコンピュータが受け取り当該コンピュータに接続されたメモリに格納し、ここで受け取られたデータはアクセス決済データストリングからのデータを含み、これは携帯型消費者機器と関連してオフライン検証処理を行うのに適合したトランジット検証値を含み、
ここで、アクセス決済アプリケーションデータは機関業者のトランジット料金装置で使用するためのアクセス決済データフィールド構造とアクセス決済会員番号（ＰＡＮ）を有し、ここでアクセス決済データフィールド構造は携帯型消費者機器の発行者の小売り処理システムで使用するための小売りアプリケーションデータフィールド構造に類似していて、発行者は小売りアプリケーションデータを受け取りそれを処理して小売り決済を承諾または拒否し、また小売りアプリケーションデータフィールド構造は小売りアプリケーションデータに関連した小売り会員番号（ＰＡＮ）を含み、
ここでアクセス決済アプリケーションデータのアクセス決済データフィールド構造が磁気ストライプデータ（ＭＳＤ）構造に一致し、
受け取ったアクセス決済アプリケーションデータを処理し、ここでアクセス決済アプリケーションデータの処理がトランジット検証値の処理を含み、

トランジット検証値が有効でありアクセス決済ＰＡＮがトランジット機関業者のネガティブ・リストに含まれていないと判断され、携帯型消費者機器がトランジット環境のトランジット料金装置で確認されているとき、当該携帯型消費者機器が認証されていることを示し、携帯型消費者機器が偽造でないことを認証するためにトランジット環境のトランジット料金装置によって使用され、且つ動的な値として組み込まれて携帯型消費者機器の１つ以上のプロセッサによって可変である、前記方法。

【請求項１９】

請求項１８記載の方法において、トランジット検証値がＭＳＤ構造の個人識別番号（ＰＩＮ）データフィールドを占める、前記方法。

【請求項２０】

請求項１８記載の方法において、携帯型消費者機器がアクセス決済データストリングを含み、また小売りデータストリングを含み、データの受け取りが携帯型消費者機器から、小売りデータストリングはトランジット処理システムからはアクセスされずアクセス決済データストリングは小売り処理システムの小売りＰＯＳ端末からはアクセスされないように読み取ることを含む、前記方法。

【請求項２１】

請求項１８記載の方法において、アクセス決済ＰＡＮはアクセス決済を選択的に承諾するように発行者によって使用される、前記方法。

【請求項２２】

請求項２１記載の方法において、アクセス決済ＰＡＮがＭＳＤ構造の商業分野コード（ＭＣＣ）に関連する、前記方法。

【請求項２３】

請求項１８記載の方法において、ＭＣＣデータがトランジット分野に対応し、トランジットＭＣＣの範囲外の携帯型消費者機器の全てのアクセス決済を発行者が拒否する、前記携帯型消費者機器。

【請求項２４】

請求項１８記載の方法が更に、携帯型消費者機器の発行者自由裁量データフィールドから読み取られたデータの処理を含む、前記方法。

【請求項２５】

請求項２４記載の方法において、発行者自由裁量データフィールドがＭＳＤデータ構造に入る、前記方法。

【請求項２６】

請求項１８記載の方法において、受け取ったデータの処理が携帯型消費者機器から受け取られた、動的に変化するトランジット検証値の正当性確認を行うことを含む、前記方法。

【請求項２７】

請求項１８記載の方法において、アクセス決済アプリケーションデータの受け取りが非接触スマートカード機器を含む携帯型消費者機器からの読み取りを含む、前記方法。

【請求項２８】

請求項１記載の携帯型消費者機器であって、小売りアプリケーションデータまたはアクセス決済アプリケーションデータの少なくとも１つが１つ以上のアクセス条件を含み、前記小売り処理システムの読み取り機は前記アクセス決済アプリケーションデータにアクセスできず、そして前記トランジット機関業者のトランジット料金装置は前記小売りアプリケーションデータにアクセスできない、前記携帯型消費者機器。

【発明の詳細な説明】

【技術分野】

【０００１】

（関連出願の相互参照）

本出願は米国特許出願１１／６８０，５９４号、２００７年２月２８日出願、名称「トランジット検証値を使用したデータカードの認証（Authentication of a Data Card Usin

g a Transit Verification Value）」エイ・ハマッド（A. Hammad）およびピー・ディクソン（P. Dixon）に付与、に対して優先権を主張する。この特許出願の内容は、全ての目的に対してその全てを参照することにより此処に組み込まれている。特許明細書、名称「通行料金徴収のための不正防止（Fraud Prevention for Transit Fare Collection）」エイ・ハマッド（A. Hammad）その他に付与、米国特許出願番号第１１／６８０，５８９号、２００７年２月２８日出願、および「オフライン環境に於ける携帯型消費者機器の認証（Verification of a Portable Consumer Device in an Offline Environment）」エイ・ハマッド（A. Hammad）その他に付与、出願番号第１１／６８０，５９２号、２００７年２月２８日出願、および「通行料金徴収で使用される銀行発行非接触支払いカード」エイ・ハマッド（A. Hammad）その他に付与、米国特許出願番号第１１／５６６，６１４号、２００６年１２月４日出願、および「自動車通行料金支払い」エイ・ハマッド（A. Hammad）その他に付与、米国特許出願番号第１１／５３６，２９６号、２００６年９月２８日出願は、全ての目的に対してそれらの全てを参照することにより此処に組み込まれている。

【背景技術】

【０００２】

本発明は、支払いカード（payment card）およびスマートカード（smart card）の様な、携帯型消費者機器で処理される金融決済に関する。

【０００３】

携帯型消費者機器は多くの形式を取ることができて、非常に多種の金融決済で使用されている。これらの機器には、例えばスマートカード、支払いトークン（payment token）、クレジットカード、デビットカード（debit card）、非接触カード（contactless card）等が含まれる。金融決済には、小売り購入、通行料徴収、イベント会場へのアクセス（access to venues）等が含まれる。その様な全ての取引に於いて、機器使用者（消費者）は第１に便利さ、決済業務の容易さ、および決済の迅速さに関心を持つ。企業および掛け金回収者およびカード発行者は、詐欺行為の防止に懸念があり、これは最終的に消費者のコストを増加させる。

【０００４】

詐欺行為防止は典型的に、カード使用者がそのカードを使用する権利があるかの認証、およびその使用者の口座に所望の決済に十分な残高が在るかの照合を含む。従来の支払いカードシステムは承認処理と使用者認証要求を使用し、これは企業、回収者および発行者のシステムとデータをチェックするために、処理ネットワーク上でのオンラインデータ通信を含む。その様なシステムは通常、使用者がそのカードをカード読み取り機またはその他の機構に通して、そのシステムがカードからデータを読み取り、また場合によってはカードにデータを書き込むことが出来ることが必要である。その様な処理は詐欺行為を防止する上では効果的であろうが、この様な手順はカード使用の認証のための決済時間を増加させ、使用者に対して効率的で利便性の高い使い勝手を与えることは困難である。

【０００５】

その様な支払いカードシステムで直面する問題があるため、決済システムの一部として非接触「スマート」カードまたは非接触スマートチップを使用する関心が高まってきている。スマートカードは一般的に、マイクロプロセッサと１つまたは複数のメモリチップのいずれかが組み込まれたポケットサイズカード（またはその他の携帯型支払い機器）、または非プログラマブル・ロジックを具備した１つまたは複数のメモリチップとして定義される。マイクロプロセッサ型カードは典型的にある種のデータ処理機能、例えば加算、消去を実行可能であるか、そうでなければそのカード上のメモリ場所内に格納されている情報を操作することができる。これと対照的に、メモリチップ型カード（例えば、プリペイド電話カード）は、読み取り装置で操作されるデータを保持するファイルとしてのみ動作可能であり、予め定められた操作、例えばメモリまたは保護メモリ内に保持されている前払い残高から料金を借方勘定処理するなどを実行する。スマートカードは、磁気ストライプカード（例えば従来型クレジットカード）とは違って、種々の機能を実行し、また種々

の型式の情報をカード上に収納することが可能である。従って用途によっては、使用者認証または決済時の記録を保存する目的で遠隔データベースにアクセスする必要が無い場合もある。スマートチップは半導体素子であり、これは全てではないにしてもスマートカード機能のほとんどを実行することが可能であるが、別の機器の中に組み込まれていても良い。

【０００６】

スマートカードは一般的に２つの種類に分けられる；接触型と非接触型である。接触型スマートカードは接点を含む形のものであり、この接点はカードのデータ並びに機能にアクセス可能であり、典型的には何らかの形式の端末またはカード読み取り機を介して行われる。非接触スマートカードは、直接接触を必要とせずにカード読み取り機または端末と通信するための手段が組み込まれたスマートカードである。従って、その様なカードはそれらをカード読み取り機または端末の近くを通過させることにより、効率的に「さっと通される（swiped）」はずである。その様な非接触カードは典型的にカード読み取り機または端末とＲＦ（無線周波）技術を用いて通信しており、此処でアンテナに近づくとカードと読み取り機または端末とのデータ転送が引き起こされる。非接触カードは銀行その他の用途での使用が見られるが、それは決済を完了させる際に個人の財布またはポケットから取り出す必要が無いからである。更にその様なカードへの関心の高まりを受けて、非接触スマートカードの動作とインタフェースを規定する規格が開発されてきており、例えばＩＳＯ１４４３規格である。種々の金融決済、例えば小売り支払いおよび通行料金徴収、は非接触スマートカードのＩＳＯ１４４３規格に準拠している。

【０００７】

しかしながらアプリケーションによっては、従来型オンライン認証および検証の仕組みに適合するためにそれらの機能が制限されるものがある。例えば、通行料徴収およびイベント会場アクセス（venue access）では、入場を希望する人々の長蛇の列は、使用者にとって決済速度が第1の関心事であることを意味する。これは通行料支払いおよび徴収処理過程が、従来型オンライン認証および承認処理過程を用いては効果的に実行できないことを意味している。これは問題であり、それは効果的な詐欺行為防止方法は典型的にそのカード使用者がアクセスする権利を有し、所望の決済に対して十分な資金を持っていることの認証を必要とするからである。加えて、異なる料金徴収システムでは典型的に異なる認証要求、料金徴収、および付随的なデータ要求を持つ。これは１つのスマートカードが、料金徴収環境の中で使用することが望まれる場合、使用者が利用しようと望むシステムに関連するデータを含んでいなければならないことを意味する。これは１人の使用者が複数のシステム、例えば複数の交通機関または単一の地理的領域内または異なる都市または地域の複数のイベント会場を利用したいと望む場合、非常に大きな問題となる。

【０００８】

更に、交通は典型的に実際の旅行距離、行き先、顧客種類、および／また使用時間に依存して必要とされる異なる料金計算および料率での駅間の移動を含み、料金は駅への入場および退場場所、方向、旅行モード、顧客の部類およびおそらくは１日の時間帯に基づいて計算される必要がある。これは各々の駅または経路でのスマートカード端末／読み取り機が、使用者のカードに記憶されているかまたはそこから読み取られたデータに基づいてこれらの計算を実行できる必要があり、その結果カード端末／読み取り機はそのカードに先行の駅で書き込まれたデータにアクセス出来なければならない。これは端末および／または料金処理システムに膨大な処理負荷を課し、その様なシステムのインフラストラクチャの実現コストを増加させる。料金料率およびその他の関連する情報は一般的に時間によって変化するので、これはまたその様なシステムへの要求を増大させる。

【０００９】

関連する問題点は支払いカード上の秘密データ保護の必要性である。単一カード上に複数の勘定のためのデータを提供することにより、使用者が複数の勘定に対する決済を許す単一の支払いカードを持ち運ぶ事を可能とすることが知られている。このような方法により、コンビネーション・カード（combination card）の一部分を使用者の銀行決済カード

として利用し、カードの別の部分をこれに代わるサービス提供者、例えば交通機関またはイベント会場アクセスに対する個別業者勘定に利用することが可能である。コンビネーション・カードは認証用の秘密データおよびその他の形式の識別データを含むはずであり、それらは販売決済において従来からある時点での支払いを行う際に銀行決済を行うために必要なものである。代替機関またはイベント会場での安全保障上の不安があるため、代替決済処理工程の銀行データへのアクセスを許可することは望ましくないはずである。これは使用者が彼らの代替決済活動を彼らの標準銀行決済勘定に連結させてその代替決済支払いを完了させたいと望む場合、または使用者が代替決済勘定のために残高を「補填（load）」して、その銀行決済勘定を使用したいと所望する場合に問題を引き起こしかねない。

【００１０】

更に詳細には、交通料金徴収、イベント会場入場料支払い、および同種のものはオフラインで処理されなければならないが、それは例えば地下鉄改札口またはバス料金箱の交通料金徴収装置では、決済速度が要求されるからである。その様な環境では、決済承認を得るために発行者にオンラインで接続するための効果的で十分な時間が無く、また典型的な運輸環境で必要とされるように１分間あたり３０から４０人の乗客の流れを処理する時間も必要である。偽造カード攻撃の可能性および組織詐欺の可能性を抑止するために何らかの形式のオフラインカード認証が必要とされる。解決される必要のあるこれらおよびその他の問題には下記が含まれる：

・偽造カードの使用および考えられる際限のない詐欺行為を止めさせるためにカード認証が実施されなければならない（交通料金装置においてオフラインで）。しかしながら既存のＭＳＤアプリケーションを用いたカード認証に対しては何ら準備されていない。

・鍵（key）の管理は多者対多者関係（業者達および複数の発行者）の中で生じる問題である。例えば、発行者／業者関係の確立に先行して如何にして対称鍵を交換するか？

・適切なファイル空間を生成することおよびカードメモリの管理を調整することは難しく、特に関係者（発行者および業者）がカード発行前に関係を持っていない場合である。

・交通ネガティブ・リスト（negative list）管理は１つの問題であるが、それは非接触発行が拡大したり／または偽造カード攻撃が生じた場合に、ネガティブ・リストが無制限に拡大する可能性があるためである。

【００１１】

上記の問題を解決するための１つの技術は、交通顧客に彼らのカードを、料金徴収に最初に使用する前に事前登録することを必要とし、その時点で鍵とファイルがそのカードに追加されるはずである。しかしながら、交通機関は一般的に全ての人が彼らのカードを最初に使用する前に登録することを望まないと意思表示している。

【００１２】

解決するための別の技術は、そのカードが交通で使用される前に、交通機関および発行者が事前契約を結びまた関係を結ぶことを必要とする。この環境下において、発行者がカード発行に先だってそのカード上に機関鍵とファイルを発行することが可能である。しかしながら交通機関は一般的に、各々の発行者との関係を保持しなければならないことを望まないと意思表示している。交通機関は全ての交通使用可能カードが、事前通知または契約を結ぶことなく彼らのシステム内で動作することを望んでいる。

【００１３】

決済時間処理を最少とし、効果的な詐欺防止を担保することの可能な、決済システムで使用できる支払い決済処理が必要である。本発明はこの要求を満足する。

（概要）

【００１４】

本発明に基づく決済処理は、携帯型消費者機器のアクセス決済アプリケーション（access transaction application）からデータを受け取ることを含み、此処で受信されたデータは、トランジット検証値を含むアクセス決済データストリング（access transaction data string）からのデータを含み、此処でトランジット検証値を除けば、アクセス決済データストリングは小売りデータを含む小売りデータストリングと基本的に類似しており、

此処でアクセス決済データストリングはアクセス決済処理システムでの使用に適合されていて、小売りデータストリングは小売り処理システムで使用するように適合されている。決済処理は更にトランジット検証値を含む受信データの処理を含む。この様にして、本発明は決済処理時間を最少としかつ、効果的な詐欺防止を担保する決済システムを提供する。

【００１５】

関連する特徴として、クレジットカードまたは支払いカードの様な、携帯型消費者機器はアクセス決済アプリケーションデータ同様に小売りアプリケーションデータを含むことも可能である。小売りアプリケーションデータは小売り決済との関連において使用されるものであり、発行者の小売り処理システムで使用するための予め定められたデータフィールド構造を有するデータは、小売りアプリケーションデータを受け取り、小売り決済を認証するかまたは拒否するかの処理を行い、この小売りアプリケーションデータは携帯型消費者機器に関連する会員番号（PAN：primary account number）を含む。アクセス決済アプリケーションデータはアクセス決済に関連して使用するためのものであり、業者の読み取り機で使用するための予め定められたデータフィールド構造を有するデータであって、アクセス決済アプリケーションデータの予め定められたデータフィールド構造は、小売りアプリケーションデータフィールド構造に基本的に類似しており、その違いはアクセス決済アプリケーションがＰＡＮ以外に選択的承認データを含むことであり、これは携帯型消費者機器に関連しておりアクセス決済を承認するか拒否するために発行者により使用される。

【００１６】

本発明のその他の目的および特長は、当業者には本発明の詳細な説明と添付図を参照することにより明らかとなろう。

【図面の簡単な説明】

【００１７】

【図１】図１は本発明に基づき構築された携帯型消費者機器を表す。

【００１８】

【図２】図２は図１に図示された携帯型消費者機器上に格納されたデータの階層表現である。

【００１９】

【図３】図３はその中で図１の携帯型消費者機器が使用される処理システムを表す。

【００２０】

【図４】図１に図示された携帯型消費者機器のための、図３に示す決済処理システムで実行される操作を図示する流れ図である。

【００２１】

【図５】図５は本発明に基づき構築された非接触スマートカードを含む図１の携帯型消費者機器を図示する。

【００２２】

【図６】図６は図１に図示する携帯型消費者機器上のトランジット（交通）ＭＳＤ情報のデータ記録割付の図である。

【００２３】

【図７】図７は図１に図示する携帯型消費者機器上のトランジット（交通）アプリケーションファイルのデータファイル構造の図である。

【００２４】

（詳細な説明）

本発明に基づき構築された実施例の以下の説明は交通システムへのアクセスを提供するようになされているが、本発明は他の型式の環境へのアプリケーションも同様に有することは理解されよう。特に、本発明はイベント会場または施設へのアクセスが所望される際の決済にも有用である。その点において、此処で使用されているように「アクセス決済」、「イベント会場アクセスアプリケーション」、および類似の用語は、使用者が携帯型消

費者機器を用いて電車、コンサート会場、飛行機、乗換駅、職場、有料道路など、特定の施設へアクセスするような全ての決済を含むように意図している。アクセスは通常、ゲートまたは鉄道の駅での料金箱の様なアクセス機器を通して許可される。「アクセス決済」は何らかの種類（例えば、交通勘定から前納金を差し引く）の支払いを含むことが可能であるが、「アクセス決済」は「支払い決済」の決済とは異なる型式であり、この支払い決済は販売の現場で物品またはサービスに対する支払いを許す決済を含む。「支払い決済」において、人は特定の場所へアクセスするために携帯型消費者機器を使用せず、販売現場で物品またはサービスに対する支払いを行うために携帯型消費者機器を使用する。従って、本発明の説明において、「トランジットシステム」および「アクセス決済」の両方は、特定の建物、システム、施設またはイベント会場へのアクセスが所望される様な、一般的な決済を表現するように意図している。

【００２５】

従来型小売り販売決済処理システムにおいて、電子支払い決済はその決済を行う消費者が適切に認証されていて、その決済を行うために十分な残高または貸付限度額を有する場合に認可される。逆に、消費者の勘定に十分な残高が残っていないかまたは貸付限度額が無い場合、または消費者の携帯型消費者機器がブラックリスト（例えば、盗難の可能性が示されている）に載っている場合、電子支払い決済は認可されないはずである。以下の説明において、「回収者（acquirer）」は典型的に企業体（例えば商業銀行）であり、これは特定の取引先と取引関係を有する。「発行者」は典型的に企業体（例えば銀行）であり、これはクレジットまたはデビットカードの様な携帯型消費者機器を消費者に発行する。企業体によっては、発行者と回収者機能の両方を実施するものもある。

【００２６】

本発明の実施例に基づく携帯型消費者機器は任意の好適な形式を取りうる。例えば、携帯型消費者機器は手持ち式で小型にして、消費者の財布および／またはポケットの中に適合する（例えばポケットサイズ）ようにできる。例えば、携帯型消費者機器はスマートカード、通常のクレジットまたはデビットカード（磁気ストライプ付きでマイクロプロセッサ無し）、キーホルダ機器（例えば、Exxon-Mobil 社から市販されているSpeedpass^{TM}）などが含まれる。本発明に基づき構築することの可能な携帯型消費者機器のその他の例には、携帯電話機、携帯端末（PDA：personal digital assistants）、ポケットベル、支払いカード（payment card）、セキュリティーカード（security cards）、アクセスカード、スマートメディア（smart media）、トランスポンダ（transponda）などが含まれる。

【００２７】

図示を目的として、本発明の実施例は一義的に非接触スマートカードとの関連で説明されるが、本発明の実施例はそれに制限されるものではない。本発明の交通システムへのアクセスを行う実施例において、非接触スマートカードは典型的に交通システム料金徴収機構と短距離通信手法、例えば近距離通信（NFC：near field communication）機能を用いて通信を行う。その様なＮＦＣ技術はＩＳＯ規格１４４４３，ＲＦＩＤ，Bluetooth^{TM}および近赤外通信手法を含む。

【００２８】

従来の運用において、承諾要求メッセージは消費者が物品またはサービスを購入する途中またはその後に、販売現場（POS：point of sale）で携帯型消費者機器（例えば、クレジットカードまたはデビットカードまたは携帯機器）を使用して作り出される。今回の場合、携帯型消費者機器は二機能スマートカードである。承諾要求メッセージは業者に設置されているＰＯＳ端末から、その業者の回収者、決済処理システム、そして発行者へ送ることができる。「承諾要求メッセージ」は電子支払い決済を行う承諾要求を含むことができる。それは１つまたは複数の口座名義人の会員番号、通貨、販売量、業者取引証印、受人都市、受人州／国などを含むはずである。承諾要求メッセージは安全な暗号手法（例えば、１２８ビットＳＳＬまたは同等レベル）を用いて、データが危険に晒されるのを防止するために保護されている。

【００２９】
図１はアクセス決済処理システムと関連して使用するための、本発明に基づき構築された携帯型消費者機器１００を図示する。この機器は２つの決済アプリケーション、第１決済アプリケーションと第２決済アプリケーション用に構成されている。このカードの第１決済アプリケーションは交通アプリケーションの様なアクセス決済１０２用である。第２決済アプリケーションは小売り決済アプリケーション１０６を含む。携帯型消費者機器は先に述べたごとく種々の構造の中に組み込むことが可能であり、スマートカード、クレジットまたはデビットカード、キーホルダ、無線携帯電話機、携帯端末（ＰＤＡ）、ポケットベル、支払いカード、セキュリティーカード、アクセスカード、スマートメディア、トランスポンダなどが含まれる。これらの構造のいずれにおいても、携帯型消費者機器は発行者（例えば、銀行または金融機関）に関連して具備されており、これは機器と共にアクセス決済用の発行者処理を提供する。

【００３０】
交通機関での使用の様なアクセス決済に関連して、携帯型消費者機器１００は検証値データ（この説明の中ではまた「トランジットカード検証値（Transit Card Verification Value）」（ＴＣＶＶ）と呼ばれる）を含む、データ要素が具備されている。機器１００のデータ領域内にＴＣＶＶを設定するための選択肢は多数存在し、これらに限定するわけではないが、発行者自由裁量データ空間、同様に現在個人識別番号（PIN : Personal Identification Number）情報を保持しているデータ追尾位置などを含む。１例として、ＴＣＶＶデータは機器１００の上に従来型小売り決済フォーマット用に記録されているＰＩＮデータと置き換えることが可能である。トランジットアプリケーション１０２はまた、阻止データを含むようにトランジットデータファイルを格納して、これはアクセス決済処理システム１０４で読み取られて問題、例えば詐欺の可能性が検出された場合に決済実施処理を中止することも可能である。従って、携帯型消費者機器１００は、料金徴収場所、改札口、イベント会場入り口などに設置された処理読み取り機１０４でのトランジットサービスと関連して使用できる。その様な徴収場所設置機器は、代替機関、回収者、および発行者処理システムを含む、後に続く処理用のオフライン入口点である。

【００３１】
図１に図示される実施例において、小売り決済アプリケーション１０６は、小売り決済システムの、小売り決済ＭＳＤ（磁気ストライプデータ: magnetic stripe data）またはＭＳＩ（磁気ストライプイメージ:magnetic stripe image）フォーマット、例えば従来型使用者ＰＩＮデータが含まれる、に基づいてデータを格納するように構成されており、トラック１およびトラック２を含む。小売りアプリケーション１０６は機器１００が、小売り（オンライン）環境の中で、販売点（POS : point-of sale）場所１０８に設置された小売り処理読み取り機において、小売り決済用に使用されることを許している。従って、機器１００は２つの用途をサポートしており、使用者が単一の機器を持つことにより、従来型小売り支払いシステム決済とまた本発明に基づくトランジットシステム決済を実行できるようにしている。

【００３２】
本発明に基づく携帯型消費者機器１００は、先に述べた従来型システムの問題を解決するために構成要素の組み合わせを用いている。小売り決済アプリケーション１０６は従来型のやり方で、小売り場所での非接触決済処理で典型的に使用されている機構を変更することなく機能する。先に注意したように、トランジット環境は小売り決済を処理せず、この方法では料金を徴収しない。しかしながら、アクセス決済アプリケーション１０２はトランジット環境でのオフライン処理に適応することが可能であり、この中でアクセス決済アプリケーション１０２ファイル構造を以下に説明する。小売り処理システム１０８の読み取り機はトランジットアプリケーション１０２へアクセスすることはなくアクセス決済処理システム１０４の読み取り機は小売りアプリケーション１０６にアクセスすることは無い。当業者には、異なるアプリケーション１０２，１０６へのアクセス特権の分離を容易にするために、機器１００でどの様にデータを構成すべきかは理解されよう。

【００３３】
従って携帯型消費者機器１００、例えば非接触スマートカード、は磁気ストライプデータフォーマットに基づくデータを格納するように構成された検証データ領域を含み、これはトラック１およびトラック２決済システム定義内のデータフィールドを特定する。他にも選択肢はあるが、このデータを個人識別番号（ＰＩＮ）データを含むフィールドに含めて、ＰＩＮデータフィールドがＰＩＮデータの代わりに検証値データを含むようにすることができる。従って非接触スマートカード携帯型消費者機器は従来型磁気ストライプデータ（ＭＳＤ）フォーマットと互換性のある処理読み取り機で使用することができて、ＭＳＤフォーマットのデータフィールドを認識するので、従来型処理装置との統合は容易に実現できる。処理読み取り機は、携帯型消費者機器が非接触スマートカード、キーホルダ、トークン機器（token device）、無線電話機などの様な先に説明した形式のいずれを採ろうと、実現されたシステムの携帯型消費者機器と適切にインタフェースするように構成できることは理解されるであろう。

【００３４】
検証値データは機器１００から容易に読み取れるので、迅速なオフライン決済処理が評価されるトランジット環境の様な、アクセス決済に適している。この様にして、従来型ＭＳＤフォーマットのカード検証値は「トランジットカード検証値（transit Card Verification Value）」（此処ではＴＣＶＶと呼ぶ）を含むが、ＴＣＶＶは例えばイベント会場への入場の様な種々の環境で使用できることは理解されよう。

【００３５】
カードデータ階層

【００３６】
図２は、本発明に基づき構築された携帯型消費者機器１００（図１）の階層データ構造を示し、小売りおよびアクセス決済情報が個別に設置されて構成された非接触スマートカード２００として組み込まれている。図２において、非接触スマートカードデータ構造は階層２００の最上部に、階層の一方の側にアクセス決済ファイル２０２、そしてもう一方の側に小売りＭＳＤアプリケーション２０４が描かれている。非接触スマートカード２００の小売りアプリケーション２０４は小売りアプリケーション１０６（図１）に関係する。データ階層のアクセス決済ファイル２０２は、トランジットアプリケーション１０２（図１）に関係する、トランジットＭＳＤアプリケーション情報２０６を含み、またカード認証および阻止データ２０８および発行者指定ファイル２１０を含む補助トランジットファイルを含むことが可能であり、以下に更に詳細に説明する。

【００３７】
磁気ストラスイプデータ（ＭＳＤ）小売り決済フォーマットは当業者には良く知られている。非接触スマートカード２００の小売りＭＳＤアプリケーション２０４およびトランジットＭＳＤアプリケーション情報２０６は、金融決済カード用のＩＳＯ３５８３規格に基づくＭＳＤ小売り決済フォーマットに従って構成されており、これはトラック１およびトラック２データ要素を含む決済トラックデータの使用を特定している。

【００３８】
トランジットＭＳＤアプリケーション情報２０６は非接触ＭＳＤアプリケーションフォーマットのトランジット特有バージョンを含む。トランジットＭＳＤアプリケーションは非接触カード２００の機能を提供し、ユニークな口座情報を非接触決済用のカード発行者の仕様で定義されたカード保有者「磁気ストライプデータ」の形式で、ＭＳＤ仕様を用いて提供する。トランジットＭＳＤアプリケーション情報２０６は従来型小売りＭＳＤアプリケーション情報２０４とは別に具備されている。小売りＭＳＤアプリケーション情報２０４はトランジットＭＳＤアプリケーション側２０６には格納されておらず、そこからアクセスすることは出来ない、逆もまた同様である。いずれか一方または両方のＭＳＤアプリケーションインスタンス２０４，２０６はアプリケーション間の区別を確実にするために１つまたは複数のアクセス条件を含むはずである。すなわち、カード２００のアクセスコードまたは同様のものは、小売り決済処理システム１０８（図１）の読み取り機がトラ

ンジットファイル２０６にはアクセス出来ず、またトランジット処理システム１０４（図１）の読み取り機が小売りファイル２０４にはアクセスできないように構成されている。

【００３９】

トランジットＭＳＤアプリケーション情報２０６は発行者に対して、トランジットアプリケーションを選択的に承諾するという条件で、カード２００の使用をトランジット目的にのみ制限するという能力を提供する。選択的承諾は、カード１００のアクセス決済部分１０２（図１）への鍵として処理することにより、好適にカードの使用を制限することができる。これは例えばトランジットまたはアクセス環境において特に重要であり、これらの場所ではカード所有者データが輸送機関車両の料金徴収箱または展示館の入り口または回転式改札口でしばしば記録され、それらは特に安全では無いからである。発行者およびカード所有者は当然のことながら、口座番号等の安全に関して心配している。図２に図示する実施例において、トランジットＭＳＤアプリケーション２０６は会員番号（PAN：Primary Account Number）に関連している。アクセス処理システム１０４はトランジットＰＡＮを読み取り、選択的承諾処理を与える。

【００４０】

更に詳細には選択的承諾は、カード２００から読み取られたトランジットＰＡＮに関連するカード所有者データを料金徴収装置（例えば、運賃徴収箱、展示館入り口、回転式改札口など）に格納し、カード発行者に対してＰＡＮデータの使用が特定の承認場所または特定アプリケーションに制限できるように構成することを許可することにより提供される。この様にして、発行者はトランジットアプリケーションおよび関連するデータの選択的承諾を実行することが可能である。カード２００がトランジットＰＡＮデータで承諾されたもの以外の使用に供される場合、そのカードの使用は拒否される。例えば、トランジットＰＡＮデータはＩＳＯ８５８３規格の下で記述されているような商業分野コード（MCC：merchant category code）に関連することも可能である。徴収箱内に格納されたカード所有者に障害が生じる場合、そのデータはＭＣＣデータの制限されたグループ、例えば交通機関などのみに関連する場合がある。障害が生じたカード所有者のトランジットＰＡＮデータを使用する全ての試みは、承諾されたアプリケーション以外での購入は拒絶される。この様にして、決済カードとして使用するための工業規格ＭＣＣデータに基づくカードの決済処理システムによりフィルタが掛けられる。従って、トランジットＭＳＤアプリケーション情報２０６はカードを承諾されていない目的以外、例えばトランジット分野以外の購入、で使用する試みをフィルタリングして排除するために使用できる。この様にして、トランジットＰＡＮデータはアクセス決済に対してのみ有用であり、障害のあるカード所有者トランジットアプリケーションデータからの損失のリスクが最小化される。

【００４１】

処理システム

【００４２】

図３は図１の携帯型消費者機器１００が使用される処理システムを図示する。この記述の中で携帯型消費者機器はトランジットＭＳＤアプリケーションデータを含む、非接触スマートカードとして説明されている。非接触スマートカード３０２が使用に供されると、これは料金徴収またはイベント会場入り口の非接触処理読み取り機３０４で読み取られる。処理読み取り機において、トランジットＭＳＤアプリケーションは決済トラックデータ（payment track data）を提供し、これにはカード所有者トランジット口座（トランジットＰＡＮ）情報、有効期限、サービスコードなどが含まれる。非接触処理読み取り機またはトランジット料金装置３０４はまた、何らかの暗号鍵およびカード上の認証データを処理するための関連するアルゴリズムを有し、従って取引時点でカードを認証する。トランジットＰＡＮおよび有効期限情報が料金装置３０４において、販売時点（POS：point of sale）でカード３０２を検証するために使用されるその他のデータと共に有効であると確認されると、カード所有者は徴収装置を通過するかまたは入場を許可される。

【００４３】

料金徴収装置３０４は続いてトランジットＰＡＮ情報をトランジットシステムデータネ

ットワーク３０６経由で、トランジット中央コンピュータ３０８に日時および取引場所と共に転送する。トランジット中央コンピュータ３０８は料金徴収装置３０４からの情報および非接触カード（これはトランジットＰＡＮによりユニークに識別される）からの決済履歴に基づき、トランジット機関業者により定められた料金方針と共に料金計算を実行する。カード情報は典型的に機関業者コンピュータシステム３０８へ、料金決算ＰＯＳが発生して幾らか後に転送される。データが転送されるまでの時間は数秒から数分、またはもっと長い時間の可能性がある。例えば、輸送バスの場合、料金徴収データは輸送機関業者中央コンピュータ３０８に、そのバスが終点またはその日の終わりに機関業者施設に戻るまで転送されない可能性がある。

【００４４】

機関業者中央コンピュータ３０８では、その業者によって定義されるように決済処理が実行される。例えば、業者は決済モデルを種々の仕組みで実現する場合がある、例えば一時決済現金支払い；多数決済の時間または価格に基づく合算金額への合算処理；および事前支払い勘定、此処では委任勘定が生成されて、そこから時間または金額に基づいて委任勘定の補給が必要となるまで、各決済額が減額される。料金計算ＰＯＳ決済処理が完了した後、トランジット機関業者コンピュータ３０８は機関業者決済回収者３１０を通して決済総額を処理する。その後その決済はカード発行者３１２によって承認または拒否される。例えば、発行者はカード所有者データを、処理中の決済に対して承諾されていないトランジットＰＡＮを含むものとして、そのトランジットＰＡＮをＭＣＣデータに対して比較して認識するかも知れない。この場合、発行者３１２はその決済を拒否する公算が大きい。

【００４５】

カード処理

【００４６】

図４は非接触カード１００で行われるトランジット料金徴収の処理操作を図示する流れ図であり、これは図３に図示された操作を更に説明している。最初の操作は、第１の流れ図ボックス４０２で示されるように、カードがトランジット料金徴収装置において、非接触処理読み取り機で読み取られた時に発生する。非接触カードのトランジットＭＳＤアプリケーション情報は、トランジットＰＡＮ，有効期限、サービスコードなどを含む、決済トラックデータを提供する。

【００４７】

ボックス４０４において、ＴＣＶＶ，トランジットＰＡＮおよび有効期限が料金徴収装置で検証され、トランジットＰＡＮがネガティブ・リスト上に含まれるか審査される（以下に更に説明される。）トランジットＰＡＮがネガティブ・リスト上に見つからない場合、そのカードは認証されたと判断され、そのトランジットＰＡＮはその決済の日時および場所と共に、トランジット中央コンピュータに転送される。そのカードが認証されるものと判断されると、トランジット顧客は更なる別の料金処理無しでトランジットシステムへの入場が許可される。追加料金処理は以下に説明するように必要とされるが、顧客が決済領域へ移動する動きはこの追加処理によって妨げられることは無い。

【００４８】

ボックス４０６において、トランジット中央コンピュータは料金計算を、そのカード（トランジットＰＡＮでユニークに識別される）の決済履歴に基づき、トランジット業者の定める料金方針に従って実行する。従って、使用者の残高勘定と現行料金課金はボックス４０６で折り合いが付けられる。ボックス４０８において、決済処理がトランジット業者またはイベント会場の定めるように実行される。種々の決済モデルを提供することが可能であり、以下の決済例を含む：一時決済現金支払い；多数決済の時間または価格に基づく合算金額への合算処理；および事前支払い勘定、此処では委任勘定が生成されて、そこから時間または金額に基づいて委任勘定の補給が必要となるまで、各決済額が減額される。最後に、ボックス４１０において、トランジット中央コンピュータにおいて、支払い処理がひとたび完了すると、機関業者はトランジット側またはカードに記憶されたデータを用

いて、発行者に承認または拒否を求めることにより、彼らの回収者を通して決算総額を処理する。

【００４９】

図５は、携帯型消費者機器がトランジットシステムで使用するための非接触決済スマートカード５００を含む実施例を示す。図５はスマートカード５００の裏面５０２を示す。スマートカードは基板５０４を含み、これはプラスティック基材である。別の携帯型消費者機器では、その携帯型消費者機器が無線電話機または携帯端末の場合、格納容器または内部回路基盤の様な構造を含む。カード５００は、関連するトランジット処理システムのオフライン読み取り機と通信するためのインタフェースを含む、コンピュータ読み取り可能構成要素５０６を含む。コンピュータ読み取り可能構成要素５０６はメモリを具備したロジック回路を有するプロセッサチップ５０６（ａ）およびアンテナ素子５０６（ｂ）を含むことが可能である。アンテナ素子は一般的にコイル形状で具備されており、基板５０４の中に組み込まれている。アンテナ素子５０６（ｂ）は内部または外部電源から電力を供給されており、カード読み取り機へのデータの非接触転送を可能としている。プロセッサチップメモリ５０６（ａ）は此処に記述されている補助検証値を格納しており、またトラック１およびトラック２データおよび、従来型決済システムに関連する発行者検証値を格納するためにも使用可能である。メモリはまた発行者指定データファイルを格納することも可能であり、これは以下に詳細に説明する。図５において、プロセッサチップ５０６（ａ）およびアンテナ素子５０６（ｂ）は共に基板５０４の中に組み込まれており、従って点線で図示されている。

【００５０】

必要であれば、カード５００の裏面５０２は、決済システムの接触型（オンライン）読み取り機で処理するためのデータを格納する、磁気媒体または素材５１０を含むことも可能である。裏面５０２上のオプションである磁気媒体５１０の下には署名ブロック５１２があって、その上にカード所有者の署名が書き込まれ、その署名ブロックの上には４桁のカード番号値（図５では「９０１２」と示されている）および別の３桁のＣＶＶ値５１４が印刷されており、これは典型的なオンライン金融決済処理のためのものである。

【００５１】

図６はカードに格納されるトランジットＭＳＤアプリケーション情報に関連するデータストリング６００を示す。このデータストリングは料金徴収等を処理する処理システム１０４で使用される、アクセス決済データストリングを含む。すなわち、トランジットＭＳＤ情報は検証および認証を実行する料金徴収装置または入場ゲートでのカード処理（すなわち、図４のボックス４０４の処理）を可能とする。当業者には明らかなように、従来型小売りカードは小売りデータストリングを含み、これはアクセスデータストリング６００と類似のデータフィールド構成を含み、小売りＭＳＤデータ記録フォーマットによれば、これは「トラック２」データと呼ばれるものを含む。従来型トラック２小売りＭＳＤデータ構造は３８位置データ構造を含む。トランジットアプリケーションに関しては、データストリング６００は、使用者のトランジットＰＡＮ情報を含む位置１－１６、データフィールド分離帯である位置１７、カードの有効期限を含む位置１８－２１、サービスコードを含む位置２２－２４、および非接触決済を処理するために特定のデータを含む位置２５－３７を含む。例えば、位置２５－２９は個人識別番号またはその他の検証データに割り当てることができる。

【００５２】

データフォーマット

【００５３】

トランジットＭＳＤ情報２０６（図２）の中で、データ記録位置は先に説明したようにトランジットカード検証値（ＴＣＶＶ）を含む。このＴＣＶＶは静的なものとして、発行時または製造時にカード上に格納され後ほど変更されるものとするか、またはＴＣＶＶは、良く知られている従来型小売り決済カードのｄＣＶＶフィールドの機能と類似の動的フィールドとすることも可能である。動的フィールドとして実施する場合、ＴＣＶＶ値は携

帯型消費者機器のプロセッサ５０６（ａ）により変更することが可能である。トランジットＭＳＤ情報の別のデータフィールドは小売りカードのＭＳＤ内の対応するフィールドと相似または基本的に類似のデータを含む。対応する小売りデータは「小売りＭＳＤ」または小売りデータストリングと呼ぶことができる。トランジットＭＳＤ　ＴＣＶＶおよび小売りＭＳＤは共に携帯型消費者機器のコンピュータ読み取り可能構成部品、例えば図５に図示されたプロセッサ５０６（ａ）のメモリ、上に格納される。

【００５４】

ＴＣＶＶに関して図６には特定の個数が示されているが、本発明の実施例に基づく検証値は任意の好適な個数または型式を採ることができる。ＴＣＶＶ検証値は本発明の実施例において３，４，５またはそれ以上の証印（indicia）を持つことができる。図６に示されたトラック２データのこれらの位置は例示のみを目的とするものであり、ＴＣＶＶの実際の位置はこれに代わってトラック１の中に格納することが可能である。種々のトラック１データフィールドをこの目的のために使用可能であり、発行者任意裁量データフィールド、名称フィールドまたはその他を含む。

【００５５】

図示された実施例において、ＴＣＶＶデータは完全または部分暗号文を含み、これは情報管理鍵、またはユニークなカード値および暗号化鍵に基づいている。暗号化アルゴリズムおよび鍵の使用は、対称（すなわちトリプルＤＥＳ）または公開鍵基盤（すなわちＲＡＳ）を含む。カードの発行者はこのデータを、カードを個人化する時点でトランジットＭＳＤアプリケーションのトラックデータの中に設定する。公開鍵基盤の場合、追加のデータ要素が必要であり、トラックデータの外側に格納されて、トランジット料金決済の途中にトラックデータと共にトランジット非接触読み取り機で読み取られる。非接触読み取り機またはトランジット料金装置は暗号化鍵とＴＣＶＶ用のアルゴリズムを有し、従って決済時点でＴＣＶＶ値の認証を行う。この認証は先に述べたようにトランジットおよびイベント会場アクセス換気用での処理に必要な短時間で行うことができる。

【００５６】

先に説明したように、ＴＣＶＶデータは従来型小売りＭＳＤ処理に基づく従来型ＭＳＤ決済の中には存在しない料金装置によるカード認証機構を提供する。非接触カード１００のＴＣＶＶデータは、適切なまたは期待されるＴＣＶＶ値を有していないということによって、偽造品の可能性があるカードを示す能力を与えるために具備されている。

【００５７】

発行者指定データファイル

【００５８】

携帯型消費者機器１００によって提供されるカード盗難および詐欺を防止するために具備されている別の手段は、アクセス決済ファイル２０２（図２）の中に格納されているデータファイル２０８，２１０を使用することを含む。その様な追加手段はアクセス決済機関業者、例えばトランジット機関が、携帯型消費者機器１００が将来使用されることを拒否できるような機構を含む。例えば、料金徴収を行うトランジット場所において、カード２００と共に使用される非接触処理読み取り機は小売り側２０４からはカード所有者データを読み取らないように構成されているが、アクセス決済２０２用のデータに関連して２つの機能を実行することが可能である。第１のトランジット機能はトランジットＭＳＤアプリケーション２０６用のデータを読み取ることであり、第２の機能はアクセス決済ファイル２０２の補助ファイル構造と通信することである。アクセス決済ファイル構造は認証および阻止データ２０８並びに発行者指定ファイル２１０を含む。発行者指定ファイルの構造はサイズ（データ容量）および機器１００内のファイル位置、およびそこに含まれるデータへのアクセスを得るために必要な任意の鍵に関係する。ファイル２１０内に含まれるデータのファイルフォーマットは一般的に、特定ファイルが割り当てられている機関業者または他の団体で指定される。鍵は典型的にファイルへのアクセスを得るために、指定された機関業者に与えられた暗号化鍵を含む。

【００５９】

ネガティブ・リスト処理

【００６０】

非接触カードの様な機器が、例えばトランジット料金装置の様なアクセス決済端末１０４でひとたび読み取られると、決済データがトランジット中央コンピュータへ送られ、そこで料金計算と決済の処理がなされる。先に説明したＴＣＶＶ処理に加えて、トランジット機関業者はカードの将来的使用を拒否するためにネガティブ・リストを使用する。その様な処理が例えば図４のボックス４０４に図示されており、以下に更に説明する。

【００６１】

従来から、トランジット機関業者は無効口座番号の彼ら自身のネガティブ・リストを時々保守している。発行者によって発行され料金徴収装置に提示されたトランジットカードは、トランジット機関業者ネガティブ・リストに対してチェックされる。無効ＰＡＮのリストがトランジット料金装置での決済中に検索され、そのカードＰＡＮがリスト上に発見されると、その決済は拒否される。例えばトランジット環境のアクセス決済ネガティブ・リストは典型的に１００，０００から２百万個の範囲である。トランジット料金装置はその様な情報を格納するためのメモリ量に制限があり、その様な情報を検索するための時間にも制約がある。本発明に基づき構築された携帯型消費者機器は更に効率的なネガティブ・リスト処理を提供する。

【００６２】

本発明に基づくネガティブ・リスト処理は、例えばトランジット機関業者口座番号またはトランジットＰＡＮの様な、カードのユニークな非小売り識別情報に基づき、カードの将来使用を拒否するために使用される。アクセス決済処理中に、機関業者は口座情報またはネガティブ・リスト上に存在しているといういずれかの理由により、カードを無効と識別する。いずれの場合も、発行者はその決済に対する支払いを拒否するかまたはそうでなければそのアクセスが拒否されることを表示する。発行者がアクセス決済支払いを辞退する場合、提出した機関業者はそのカードを機関業者ネガティブ・リストに追加することにより、次回決済時にそのカードの使用を拒否することが知れる。従ってトランジット機関業者自体がそのカードの使用を拒否することを承知することができる。

【００６３】

阻止データ

【００６４】

本発明によれば、トランジット機関業者はまた、拒否カードを表示するためにカードまたはその他の携帯型消費者機器のトランジットアプリケーションファイル２０８（図２）内に格納された阻止データを書き込むことが可能である。その様なデータは承諾されていないかまたは認証されていない特定の携帯型消費者機器の、効率的な制御および決済処理の停止を行うために使用することができる。阻止データは処理読み取り機１０４（すなわち、トランジット料金徴収装置またはイベント会場アクセス場所）で、カードから読み取られ、そのカードが以前にネガティブ・リスト上に存在すると識別され、それ以降の使用が阻止されていることを表示する。すなわち、カードがネガティブ・リスト上に存在すると識別されると、それが偽造カードと疑われるか、または紛失または盗難カードの可能性があるか、または債務不履行口座または嫌疑口座に関連するカードである。これらの状況のいずれかにあると、以降の処理は停止される。これは阻止データに「阻止」状態と設定することにより実施される。トランジット機関業者は、カード上の阻止データが阻止状態の場合、料金装置に続く処理を実行せず、料金計算および回収者並びに発行者を含む処理も行わない。すなわち、処理は未遂カードの使用がなされた料金装置の次には進まず、そのカード所有者は入場が拒否される。そのカードが既に阻止されておらず、ネガティブ・リスト上に存在すると識別されない場合、カード使用者は入場が許され、後続の処理が続いて実行される。

【００６５】

此処で使用されるように、「阻止データ」は携帯型消費者機器上に格納することが可能で、決済および／またはイベント会場または輸送システムへのアクセスの認証を行うこと

の出来る、任意の好適なデータを含む。従って、携帯型消費者機器が使用される、与えられた決済処理システムに対して、システムの処理読み取り機は携帯型消費者機器から阻止データを読み取るように構成されている。阻止データは任意の好適な形式を取り得る。例えば、阻止データは１つまたは複数の文字またはビット値を有する、予め定められたデータストリングとして実現できる。好適な実施例において、阻止データはデータの１バイトの形式である。例えば、阻止データは「非阻止」状態を表示するためにゼロの値にセットすることが可能であり、そのカードがネガティブ・リスト上に発見されると、阻止データは「阻止」状態を表示するために非ゼロの値にセットできる。

【００６６】

携帯型消費者機器上の阻止データは処理読み取り機などで変更することができる。此処で使用されているように「処理読み取り機」は、携帯型消費者機器とインタフェースすることができて、読み取りおよび／またはそこへデータの書き込みを行う任意の好適な装置を含む。阻止データが１バイト形式のデータの場合、携帯型消費者機器上に必要とされるメモリ装置は最少とできる。阻止データファイル構造は発行者によって指定され、データの読み取りまたは書き込みの際に暗号認証を必要とする。この様にして、阻止データは認証カードを支援するが、それは適切な暗号化鍵を具備していないカードは直ちに偽造または詐欺と識別されるからである。加えて、阻止データを使用することにより、阻止データが携帯型消費者機器上に存在しない場合に必要なブラックリストまたはネガティブ・リストのサイズを、著しくかつ好適に最少とすることが可能であるが、それはカード識別子番号（例えばトランジットＰＡＮ）を、それがひとたび阻止されると（すなわち阻止データが「阻止」状態にセットされると）、ネガティブ・リスト上から取り除くことが可能だからである。カード上の阻止データが阻止状態にセットされると、そのカードが提示された全てのアクセス決済読み取り機は、暗号化された阻止データを読み取り、そのカードが阻止されていると判断しその使用が拒否される。この判断は、例えばネガティブ・リストの調査の様な更に別の処理無しで実行される。この様にして、ネガティブ・リストのサイズは更に効率的に管理され、阻止されたカードの状態は加入している期間業者にネットワーク・データ・トラヒックを介さずに通信され、徴収読み取り機での迅速な処理速度は確保され、一方で阻止カードの検出の保証が得られる。

【００６７】

ネガティブ・リストは本発明によれば、詐欺検出の効率的な手段を提供するように管理されている。元々、トランジット機関業者がカードが決済に対して無効であるか否かを知るための手段は、発行者からの拒否された支払い決済を受け取ることを含んでいる。発行者がトランジット乗車の支払い決済を拒否すると、これはそのカードが無効であることを示し、従ってトランジット機関業者の中央コンピュータ３０８（図３）はそのカードをネガティブ・リストに追加することにより、次回決済に際してそのカードの使用を拒否することが分かる。カードがネガティブ・リストに追加された後、料金徴収装置は最終的に機関業者中央コンピュータと通信して、更新されたネガティブ・リストを承知することになる（図４のボックスと添付の文章を参照）。決済カードの発行が増加すると、ネガティブ・リストが拡大する傾向もまた増加する。紛失または盗難クレジットカードは拒否されるべきであり、トランジットで使用された場合にはトランジット機関業者のネガティブ・リストに追加される必要がある。異なるＰＡＮを用いて再発行される全てのカードはまた、使用廃止されるために元のＰＡＮも必要とする。また偽造カードはおそらく発行者によって拒否されるのでネガティブ・リスト上に記入される。これら全ての環境において、ネガティブ・リストはトランジット料金装置またはイベント会場アクセス場所において迅速にチェックされ、その決済処理を停止するかまたは継続するか迅速に判断される。

【００６８】

カード１００は一般的にカード有効期限が切れた時点でネガティブ・リストから取り除かれ、それが決してトランジット機関業者で再び使用されることが無いように保証し、これによりその機関業者が不払いに会うことを制限している。その他のトランジット機関業者処理は、制限されたネガティブ・リストファイル空間を効果的に管理するように設計さ

れた予め定められた規則に基づいて記入を削除または追加することにより、ネガティブ・リストのサイズを制御している。先に説明した阻止ビット処理はネガティブ・リストのサイズを管理する１つの手段を提供し、その様なカード状態情報用に必要なデータ記憶容量を削減している。当業者は、小売りカードに関連したネガティブ・リストのサイズを制御するための別の技術になじみ深いであろう。これらの技術は此処に説明するトランジット非接触カードに関連して適用することが可能であり、以下の例を含む。

【００６９】

ひとたびトランジットＰＡＮがネガティブ・リストに載ると、そのカード番号を用いた決済が予め定められた時間、例えば数日間、行われない場合に除去することができるが、別の決済が同一ＰＡＮ情報で拒否されると、そのカードトランジットＰＡＮは再びネガティブ・リストに追加される。別の例では、以前に拒否された決済が再び発行者に提示されると、その口座が未だに無効であるかを確認するためにチェックされ、そのカードが再提出に際して承諾された場合、そのカードはネガティブ・リストから取り除くことができる。

【００７０】

先に説明したように、トランジットＭＳＤアプリケーションとカード認証および阻止データの組み合わせにより、全ての機関業者に標準的なやり方で全ての有効化された非接触カードを処理する能力を提供する。この処理はトランジットで使用される全ての料金決済カードで処理を統一するために必要とされ、全ての発行者および機関業者が、トランジットシステムで出会う全ての一時使用者またはカードを処理できるようにする。これらの処理はトランジット能力を含む全ての非接触決済カードで必須と考えられる。この手法は先に説明した多くの従来の問題を解決し、種々の利益を提供する：

・カード認証機能（ＴＣＶＶおよび／またはトランジットファイル内のカード認証データ）を含むことにより、偽造カードの可能性が取り除かれる。

・各々のトランジット場所でカードの事前登録が不要。一時使用者または市外訪問者がトランジットＭＳＤを使用して何時でも決済処理を可能とする。

・ＴＣＶＶ用共通鍵セットおよびファイル認証が使用され、全ての発行者に対してカードの個人化用に、または全ての機関業者に対してＴＣＶＶ検証および／またはファイル認証用に分配される。

・発行者／機関業者にとって事前契約が不要。標準化されたＭＳＤおよび認証および阻止アクセスが全ての発行者および機関業者に対して確立されている。

・発行者商標（例えばVisa　USA）はカード阻止データを設定するための規則を設置できる。１つの機関業者での「阻止」データの設定は、ネガティブ・リストデータを通すことなく他の機関業者でも使用可能である。１つの機関業者でのネガティブ・リスト処理は、全ての加入機関業者の保護に役立つ。阻止データの除去は最良実施例に基づく機関業者契約を必要とする顧客サービス処理を通してまたは予め定められた規則を通して実施される。

・トランジット決済は階層化された決済認証を通して保護されている：

１．料金装置において：偽造カードはＴＣＶＶおよび／またはファイル認証によって阻止される。

２．トランジット機関業者において：詐欺検証規則およびネガティブ・リスト。

３．発行者において：ＴＣＶＶ，ｄＣＶＶおよびＡＴＣで検証。

【００７１】

先に説明した安全保障手法に加えて、アクセス決済機関業者はカードのオプションファイル機能を用いて、カード発行者と連動して、更に詳細な料金徴収機能を実現できる。このファイル機能は此処に説明されている決済カードが先に定義した処理を超えることを可能とする。例えば、これらのオプションファイル記憶機能を具備したカードは、彼らのカードを追加特権用に登録することを望む個人が使用することが可能である。カード上に予め定義されたファイル空間は、発行者が所望するように特定の機関業者に、発行者がトランジット機関業者と構築した関係に基づいて、割り当てられかつ指定されている。カード

上のこれらの発行者指定ファイル空間は、トランジット機関業者によって彼ら自身の目的のために使用される、例えば：
・トランジットシステムで小売りカードＰＡＮの使用を最少とするために、カード上に非ＰＡＮトランジットＩＤを含める。
・所望であればカード上に料金結果を含める。
・所望であればカード上に顧客分類を含める。
・次回決済手順で使用するため、または決済の隙間を埋めるために機関業者中央コンピュータへ転送するためにカード上に決済履歴を含める。
・機関業者で定められたその他の使用特定情報を含める。

【００７２】

発行者指定ファイル構造の１例が図７の階層化データファイル構造で図示されており、これはカード１００（図１）上に格納されている。図２に関連して先に説明したように、アクセス決済トランジットファイルはトランジットＭＳＤアプリケーションおよびカード認証および阻止データ２０８を含む補助データファイル、およびオプションの発行者指定ファイル２１０を含む。図７はカードデータファイル構造７００を示し、これは第１ファイルＥＦ００で表されるカード認証および阻止データファイル００、および１つまたは複数の、ファイルＥＦ０１，ＥＦ０２，ＥＦ０３，．．．，ＥＦｎｎで表された、発行者指定データファイル０１，０２，０３，．．．，ｎｎを含む。これらの発行者指定ファイルは予め定められたサイズおよび型式である。例えば、発行者は１００バイトの１５個の指定されたデータファイルＥＦ０１からＥＦ１５を指定し、各々はアクセス用のＩＳＯ７８１６　ＡＰＤＵ命令を用いた透過ファイル構造に基づいている。発行者は各々のファイルに対して認証鍵を指定しても良い。ひとたび発行者が１つの機関業者と関係を持つと、カードの個人化または発行の前または後のいずれかに、１つまたは複数のデータファイルが発行者によって指定され、その時点で認証鍵が機関業者に対してアクセス用に提供される。トランジット機関業者は彼ら自身の目的で所望するように、１００バイトデータファイルの使用を定義することが出来ると見込まれている。すなわち、発行者指定ファイルへのアクセスは発行者の制御下にあり、発行者と契約をはたした機関業者は、発行者から認証鍵を受け取ることによりそのファイル空間へのアクセスを行うことができる。

【００７３】

ファイル構築およびカード上のファイルデータの初期化に関して多くのオプションが可能である。例えば、トランジット機関業者はこれらを発行者と共にカード発行に先立って予め定義することができる。この環境下において、カード所有者は郵送で事前搭載されたカードを受け取り、そのカードを更に別の処置をすることなくトランジットシステムで使用することができる。しかしながら、もっとも有りそうなことはカード所有者がトランジットシステムで使用するためのファイルデータをロードするために、１回カード事前登録処理を実施するように要求されることである。この処理はトランジット機関業者によって実施され、本人自ら顧客サービスを訪問することを含むかまたは、トランジットシステムの無人キオスクまたは切符販売機の処理として実施されることも可能である。

【００７４】

非接触カードの様な携帯型消費者機器上に例示化されている発行者指定データファイルは、事実上、市場価値を有する商品を含む。例えば、発行者はカード上のファイル空間の使用に対してトランジット機関業者に、多くの考えられる決済モデル、例えばカード毎、決済毎、またはファイル空間の１回料金に基づき、課金する場合もある。この様にして非接触カードは此処に説明したように、発行者はビジネス事例を創作し、その様な市場価値を利用することを可能とする。

【００７５】

従って、カード上のトランジットＭＳＤアプリケーションは、此処に説明したように料金徴収またはイベント会場入り口において、処理時間を最少としながらオフライン決済を可能とする便利でかつ安全な機能を提供する。これらの機能の中で、カードのトランジット側は特定のトランジットシステムまたはイベント会場へのアクセス使用に限定すること

が可能であり、小売り購入には使用することが出来ない。カードの両領域上のデータファイル構造のため、カードは小売りとトランジット２つの使用を支持しており、従来型工業二重使用カードプログラムガイドラインに従っている。加えて、トランジット領域上のカードデータはＴＣＶＶデータを含み、トランジット料金装置がそのカードが偽造では無いことを認証出来るようにしている。その様な情報を提供する際に、カードデータはトランジット料金徴収装置で検証するための、会員番号（ＰＡＮ）と有効期限情報を含む。カードのその他の機能はトランジット料金徴収装置においてＰＡＮデータに基づき、機関業者が開発したネガティブ・リスト管理技術を用いて、ネガティブ・リスト登録を支援する能力である。

【００７６】

非接触カード処理読み取り機設備は、カードの小売り側からの情報読み取りは防止するように好適に構成されている。カードの小売り側では、典型的な決済処理が実行され、従来型ＭＳＤ小売り決済用の動的カード検証値の様な小売り決済機能を含む。その様な小売り処理は典型的にオンラインで実行され、従って決済処理読み取り機とそれに関連する決済システムネットワークとの通信が認証のために必要とされる。先に説明したように、此処に記述した検証値データは、トランジット環境で要求されるオフライン検証を可能とする。

【００７７】

説明したように、携帯型消費者機器は２つのアプリケーション領域、アクセス決済アプリケーション２０２（例えばトランジット）と少なくとも１つの追加アプリケーション領域２０４（例えば小売り）を有する、二重使用カードとして構成できる。所望であれば、複数の追加アプリケーション領域を用意することが出来る。複数使用カードに関して、カードの各々の追加アプリケーション領域は、データストリング、検証値、発行者指定データファイルなどを含む、図２に図示された並列データ階層２０２の様な、対応する個別ファイル階層を有するように構成できる。その様な場合、１つのシステムの処理読み取り機は、カードのそれらに対応するアプリケーション領域のみにアクセスし、カードのその他のアプリケーション領域の如何なるデータにもアクセスしない。

【００７８】

非接触スマートカードとして此処に説明された携帯型消費者機器は便利に使用されるが、それは此処に説明した非接触スマートカードを所有する使用者がトランジットシステムまたはイベント会場に関連する端末との通信距離を通過する際、この非接触スマートカードは近領域通信機能を介して料金徴収システムと通信することが可能である。この様にしてスマートカードは使用者を識別し、認証データ（例えば暗号化鍵またはその他の形式の認証／検証形式）を交換し、料金計算に必要なデータを提供したり、またはその他の口座に関係するデータを徴収システムに提供するように使用することができる。更に、このデータは必要であればトランジット機関業者および／または決済処理団体に、口座管理またはその他の機能のために提供される。

【００７９】

本発明によれば、小売り決済支払いおよびトランジット料金決済（またはその他のイベント会場アクセス）環境の両方で利用される、非接触スマートカードまたは携帯型消費者機器用の構造およびアーキテクチャが記述されている。カード上のデータはカード製造者、カード発行者により、または製造および発行に続く時点で用意される。カードはトランジットシステムデータを格納するための指定ファイル格納領域を含み、複数のトランジットシステムへのアクセスを提供するために、カードの制限された記憶容量を効率的に使用することを可能としている。

【００８０】

今まで述べたように、記述されたトランジットシステムアプリケーションに加えて、本発明の非接触スマートカードはまた種々のイベント会場；これらは例えば遊園地、劇場、料金徴収所、またはその他の処理時間に制約の有る特定アクセス制御と支払いデータを必要とする場所を含む、へのアクセスを許可するように構成できる。トランジット料金また

はその他のアクセス料金の決済は支払いアプリケーション口座をトランジスタ実とまたはその他の使用にリンクさせることで実施できる。このリンク付けは決済アプリケーションデータの安全性を保証するために、認証および／または口座データの代理物を用いて実施される。

【００８１】

先に説明した本発明のある種の構成要素は、コンピュータソフトウェアを使用したモジュール方式または統合化方式の制御ロジックの形式で実現することができる。此処に提供された開示および教えに基づき、通常の技術を有する当業者は、ハードウェアおよびハードウェアとソフトウェアかを組み合わせを使用して本発明を実現するための、その他のやり方および／または方法を知り、理解することが出来るであろう。

【００８２】

この明細書に記述された全てのソフトウェア構成要素または機能は、任意の好適なコンピュータ言語、例えば従来型またはオブジェクト指向技術を用いた、Java，C++またはPerlを使用したプロセッサで実行されるソフトウェアコードとして実現できる。ソフトウェアコードは一連の指令、または命令としてコンピュータ読み取り可能媒体、例えば随意アクセス・メモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、ハードディスクまたはフロッピーディスクの様な磁気媒体、またはＣＤ－ＲＯＭの様な光媒体上に格納することができる。全てのその様なコンピュータ読み取り可能媒体は単一計算装置上またはその内部に存在し、１つのシステムまたはネットワーク内の異なる計算装置上またはその内部に存在する。

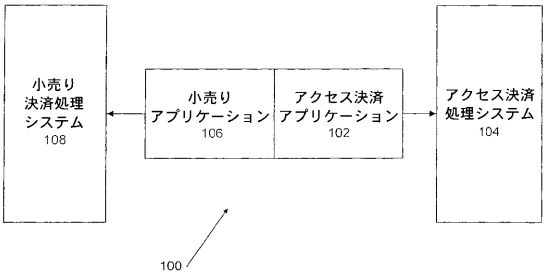
【００８３】

或る実施例の事例を詳細に説明しかつ添付図に示してきたが、その様な実施例は単に図示目的のみであって、広範な発明を制限することは意図しておらず、本発明は図示され説明された特定の構成並びに構造に制限されるものでは無く、何故ならば通常の技量を有する当業者には種々のその他の修正変更が可能であることを理解されたい。

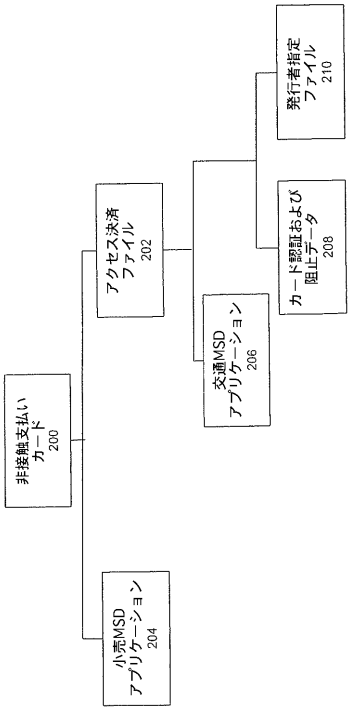
【００８４】

此処で使用されているように、「a」、「an」または「the」は、その反対として特に断られていない限り「少なくとも１つ（at least one）」を意味するものと意図している。

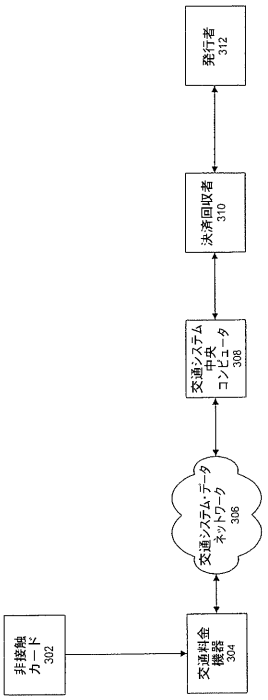
【図１】


小売り
決済処理
システム
108
小売り
アプリケーション
106
アクセス決済
アプリケーション
102
アクセス決済
処理システム
104
100

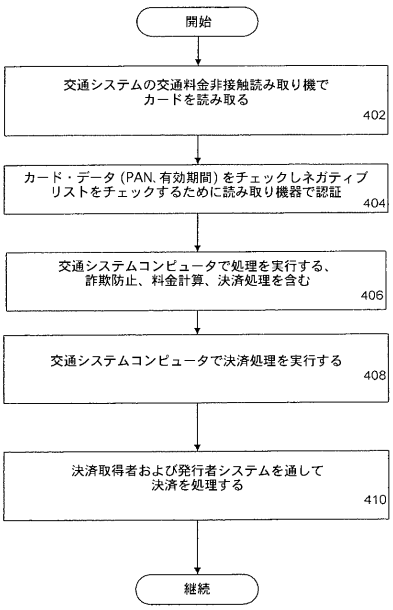
【図２】


発行者指定
ファイル
210
アクセス決済
ファイル
202
カード認証および
阻止データ
208
交通MSD
アプリケーション
206
非接触支払い
カード
200
小売MSD
アプリケーション
204

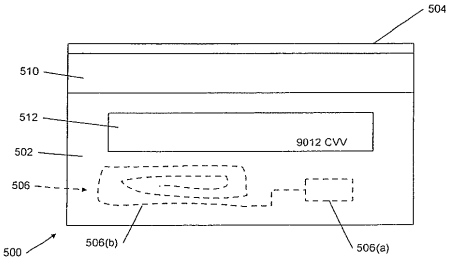
【図３】


発行者
312
決済回収者
310
交通システム
中央
コンピュータ
308
交通システム・データ
ネットワーク
306
非接触
カード
302
交通料金
機器
304

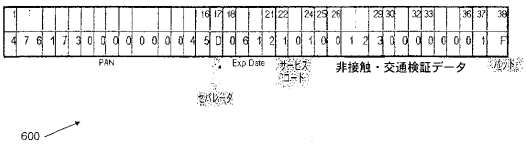
【図４】


開始
交通システムの交通料金非接触読み取り機で
カードを読み取る
402
カード・データ（PAN, 有効期間）をチェックしネガティブ
リストをチェックするために読み取り機器で認証
404
交通システムコンピュータで処理を実行する、
詐欺防止、料金計算、決済処理を含む
406
交通システムコンピュータで決済処理を実行する
408
決済取得者および発行者システムを通して
決済を処理する
410
継続

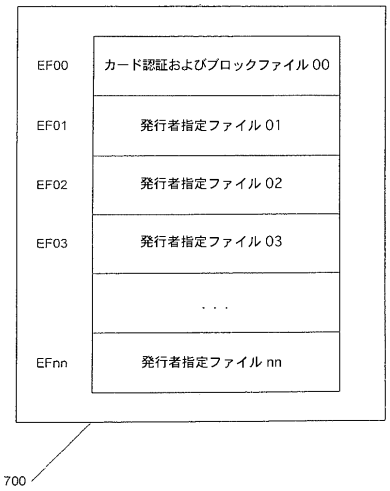
【図５】


504
510
512
9012 CVV
502
506
500
506(b)
506(a)

【図６】


PAN
Exp Date
サービス
コード
非接触・交通検証データ
600

【図７】


EF00
カード認証およびブロックファイル 00
EF01
発行者指定ファイル 01
EF02
発行者指定ファイル 02
EF03
発行者指定ファイル 03
. . .
EFnn
発行者指定ファイル nn
700

フロントページの続き

審査官　塩田　徳彦

(56)参考文献　国際公開第９９／００９５０２（WO，Ａ１）
特開２００５－１２２２６６（ＪＰ，Ａ）
特表２００４－５３３０４５（ＪＰ，Ａ）
特開２０００－１２３１３９（ＪＰ，Ａ）
特開２００２－１３３４４８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００　－　５０／３４