(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6386567号
(P6386567)
(45)発行日　平成30年9月5日(2018.9.5)　(24)登録日　平成30年8月17日(2018.8.17)

(51)Int.Cl.　F I
G06Q 20/38 (2012.01)　G06Q 20/38 310

請求項の数 16 (全 53 頁)

(21)出願番号	特願2016-548003(P2016-548003)
(86)(22)出願日	平成26年10月14日(2014.10.14)
(65)公表番号	特表2016-539442(P2016-539442A)
(43)公表日	平成28年12月15日(2016.12.15)
(86)国際出願番号	PCT/US2014/060523
(87)国際公開番号	WO2015/054697
(87)国際公開日	平成27年4月16日(2015.4.16)
審査請求日	平成29年9月29日(2017.9.29)
(31)優先権主張番号	61/890,162
(32)優先日	平成25年10月11日(2013.10.11)
(33)優先権主張国	米国(US)
(31)優先権主張番号	61/906,377
(32)優先日	平成25年11月19日(2013.11.19)
(33)優先権主張国	米国(US)

早期審査対象出願

(73)特許権者　505468864
ビザ　インターナショナル　サービス　アソシエーション
アメリカ合衆国、９４１２８－８９９９　カリフォルニア州、サン　フランシスコ、ピー．オー．　ボックス　８９９９
(73)特許権者　516108384
マスターカード　インターナショナル　インコーポレイテッド
アメリカ合衆国　１０５７７　ニューヨーク、パーチェス、パーチェス　ストリート　２０００
(74)代理人　110000855
特許業務法人浅村特許事務所

最終頁に続く

(54)【発明の名称】ネットワーク・トークン・システム

(57)【特許請求の範囲】
【請求項１】
コンピュータによって、要求元からオーソリゼーション要求メッセージを受信するステップであって、前記オーソリゼーション要求メッセージがカード会員番号を表す決済トークンを含み、前記カード会員番号がイシュアによって割り当てられ、前記オーソリゼーション要求メッセージが前記カード会員番号を使用して決済トランザクションを遂行することを求めるものであるステップと、
前記コンピュータによって、前記決済トークンに関連するトークン保証レベルを、前記トークン保証レベルを生成するために使用されたデータと共に受信するステップと、
前記コンピュータによって、前記オーソリゼーション要求メッセージを、前記トークン保証レベル及び当該トークン保証レベルを生成するために使用された前記データを含むように修正するステップと、
前記コンピュータによって、前記修正されたオーソリゼーション要求メッセージを、前記イシュアに承認を求めて送信するステップとを含み、
前記トークン保証レベルが、前記決済トークンと前記決済トークンによって表される前記カード会員番号の間の関係における信頼のレベルを表し、
前記トークン保証レベルが、識別・確認方法を行うエンティティに基づく、方法。
【請求項２】
前記オーソリゼーション要求メッセージを受信する前に、
前記コンピュータによって、前記決済トークンを前記カード会員番号を表すように生

成することを求めるトークン生成メッセージを受信するステップであって、前記トークン生成メッセージが、前記決済トークンに関連付けられる要求トークン保証レベルを含むステップと、

前記コンピュータによって、前記決済トークン及び前記決済トークンに関連付けられた前記トークン保証レベルを生成するステップと、

前記決済トークン、前記トークン保証レベル、及び前記決済トークンに関連付けられた前記カード会員番号をレポジトリに保管するステップとをさらに含む、

請求項１に記載の方法。

【請求項３】

前記要求トークン保証レベルが、生成されて前記レポジトリに保管される前記トークン保証レベルと異なる、請求項２に記載の方法。

【請求項４】

前記トークン保証レベルが、前記決済トークンが生成されるときに使用される識別・確認方法に基づく、請求項１に記載の方法。

【請求項５】

前記トークン保証レベルが、前記決済トークンに追加の識別・確認方法が行われたときに更新される、請求項４に記載の方法。

【請求項６】

第１の識別・確認方法の結果が第１のトークン保証レベルとなり、第２の識別・確認方法の結果が前記第１のトークン保証レベルとは異なる第２のトークン保証レベルとなる、請求項４に記載の方法。

【請求項７】

前記コンピュータによって、前記オーソリゼーション要求メッセージに応答して生成されたオーソリゼーション応答メッセージを前記イシュアから受信するステップと、

前記コンピュータによって、前記トークン保証レベルを含む前記オーソリゼーション応答メッセージを前記要求元に送信するステップとをさらに含む、

請求項１に記載の方法。

【請求項８】

１つ又は複数のカード会員番号と前記１つ又は複数のカード会員番号に対して生成された１つ又は複数の決済トークンとの間の１対１のマッピングを保管するレポジトリと対話するステップをさらに含む、

請求項１に記載の方法。

【請求項９】

プロセッサと、

前記プロセッサに結合された非一時的コンピュータ可読媒体とを含むシステムであって、

前記非一時的コンピュータ可読媒体がコードを含み、前記コードが前記プロセッサに実行されたときに、前記プロセッサに、

要求元からオーソリゼーション要求メッセージを受信するステップであって、前記オーソリゼーション要求メッセージがカード会員番号を表す決済トークンを含み、前記カード会員番号がイシュアによって割り当てられ、前記オーソリゼーション要求メッセージが前記カード会員番号を使用して決済トランザクションを遂行することを求めるものであるステップと、

前記決済トークンに関連するトークン保証レベルを、前記トークン保証レベルを生成するために使用されたデータと共に受信するステップと、

前記オーソリゼーション要求メッセージを、前記トークン保証レベル及び当該トークン保証レベルを生成するために使用された前記データを含むように修正するステップと、

前記修正されたオーソリゼーション要求メッセージを、前記イシュアに承認を求めて送信するステップとを行わせ、

前記トークン保証レベルが、前記決済トークンと前記決済トークンによって表される前

記カード会員番号の間の関係における信頼のレベルを表し、
前記トークン保証レベルが、前記決済トークンが生成されるときに使用された識別・確認方法の１つ又は複数及び、識別・確認方法を行うエンティティに基づく、システム。
【請求項１０】
前記コードが前記プロセッサに実行されたときに、前記オーソリゼーション要求メッセージを受信するステップの前に、前記プロセッサに、
前記決済トークンを前記カード会員番号を表すように生成することを求めるトークン生成メッセージを受信するステップであって、前記トークン生成メッセージが、前記決済トークンに関連付けられる要求トークン保証レベルを含むステップと、
前記決済トークン及び前記決済トークンに関連付けられた前記トークン保証レベルを生成するステップと、
前記トークン保証レベル、及び前記決済トークンに関連付けられた前記カード会員番号をレポジトリに保管するステップとをさらに行わせる、請求項９に記載のシステム。
【請求項１１】
前記要求トークン保証レベルが、生成されて前記レポジトリに保管される前記トークン保証レベルと異なる、請求項１０に記載のシステム。
【請求項１２】
前記トークン保証レベルが、前記決済トークンに追加の識別・確認方法が行われたときに更新される、請求項９に記載のシステム。
【請求項１３】
第１の識別・確認方法の結果が第１のトークン保証レベルとなり、第２の識別・確認方法の結果が前記第１のトークン保証レベルとは異なる第２のトークン保証レベルとなる、請求項９に記載のシステム。
【請求項１４】
前記コードが前記プロセッサに実行されたときに、前記プロセッサに、
前記オーソリゼーション要求メッセージに応答して生成されたオーソリゼーション応答メッセージを前記イシュアから受信するステップと、
前記トークン保証レベルを含む前記オーソリゼーション応答メッセージを前記要求元に送信するステップとをさらに行わせる、請求項９に記載のシステム。
【請求項１５】
１つ又は複数のカード会員番号と前記１つ又は複数のカード会員番号に対して生成された１つ又は複数の決済トークンとの間の１対１のマッピングを保管するレポジトリをさらに含み、
前記コードが前記プロセッサに実行されたときに、前記プロセッサに、
前記レポジトリとの対話を行わせる、
請求項９に記載のシステム。
【請求項１６】
コンピュータによって、決済トークン及び前記決済トークンに関連付けられたトークン保証レベルを生成するステップであって、前記決済トークンがイシュアによって割り当てられたカード会員番号を表すステップと、
前記コンピュータによって、前記決済トークンを要求元に送信するステップと、
前記コンピュータによって、前記要求元からオーソリゼーション要求メッセージを受信するステップであって、前記オーソリゼーション要求メッセージが前記決済トークンを含み、前記オーソリゼーション要求メッセージが前記カード会員番号を使用して決済トランザクションを遂行することを求めるものであるステップと、
前記コンピュータによって、前記オーソリゼーション要求メッセージを、前記トークン保証レベル及び当該トークン保証レベルを生成するために使用されたデータを含むように修正するステップと、
前記コンピュータによって、前記修正されたオーソリゼーション要求メッセージを、前記イシュアに承認を求めて送信するステップとを含み、

前記トークン保証レベルが、前記決済トークンと前記決済トークンによって表される前記カード会員番号の間の関係における信頼のレベルを表し、
前記トークン保証レベルが、識別・確認方法を行うエンティティに基づく、方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本出願は米国特許法第１１９条（ｅ）の定めにより、２０１３年１０月１１日に出願された「Ｎｅｔｗｏｒｋ　Ｔｏｋｅｎ　Ｓｙｓｔｅｍ」と題する米国仮特許出願第６１／８９０１６２号及び２０１３年１１月１９日に出願された「Ｎｅｔｗｏｒｋ　Ｔｏｋｅｎ　Ｓｔａｎｄａｒｄｓ」と題する米国仮特許出願第６１／９０６３７７号の利益を主張し、それらの開示の全体があらゆる目的のために参照により本明細書に組み込まれる。
【背景技術】
【０００２】
決済業界は、偽造、アカウントの悪用、その他の形の不正行為に対する保護が強化された決済フォーム・ファクタのサポートに向けて進化している。カードが介在するトランザクションはＩＣカードで十分に保護されるが、カードが介在しない複合的なトランザクション環境にも、アカウント名義人データの無認可使用を最小限に抑え、また、チャネルをまたぐ不正行為を防止する、さらに進んだ保護に対する同様の需要がある。これらの需要に対処するために、トークン化システムはかなり有望である。
【０００３】
従来の電子決済トランザクションでは、トランザクションのライフサイクル中に消費者のカード会員番号（ＰＡＮ：Ｐｒｉｍａｒｙ　Ａｃｃｏｕｎｔ　Ｎｕｍｂｅｒ）情報が、関係する様々なエンティティに露出される。ＰＡＮは販売店端末から、アクワイアラ・システム、決済処理ネットワーク、決済ゲートウェイなどに渡される。
【０００４】
トランザクションのライフサイクルの様々な時点でＰＡＮが露出される可能性があることから、決済トランザクションを遂行するために決済「トークン」が開発されてきた。決済トークンはＰＡＮの追加セキュリティ層として働き、事実上ＰＡＮの代理／代用物となる。よって、決済を開始するとき又はトランザクションをサブミットするときに、ＰＡＮの代わりに決済トークンが使用されることがある。ＰＡＮの代わりに決済トークンを使用すると、実際のＰＡＮは公表されないので、不正行為のリスクを削減することができる。
【０００５】
決済トークンの使用に向けた従来の取り組みは有用だが、さらにいくつかの問題を解決する必要がある。例えば、実際のＰＡＮは対応するトークンからは明らかではないので、そのトークンの提供元又はそのトークンのイシュア（ｉｓｓｕｅｒ）を特定することは困難である。一方では、トークンは情報の隠蔽を目的とする。しかし他方では、決済トークンから、そのトークンの提供元又はイシュア、そのトークンを使おうとしているユーザが実際にカード名義人本人であるかの信頼のレベル、及びその信頼のレベルを判断するために使用されるデータを特定することが有用なこともある。現在、この情報を特定するための技法は存在しない。
【０００６】
さらに、従来、トークンは特定のネットワーク又は決済処理システムに制限されており、決済ネットワーク間の相互運用性をサポートしていない。したがって、様々な決済システムへのトークンの適応及び統合は限定的である。
【０００７】
本発明の実施例は、これらの問題及びその他の問題を、個別及び集合的に解決する。
【発明の概要】
【発明が解決しようとする課題】
【０００８】
本発明の実施例は、トークン保証レベル及びトークン保証レベルを生成するために使用

されるデータを、トークンと共に提供することを目的とする。トークンが発行される時点で、トークン要求元によって合法的に使用されていたＰＡＮにそのトークンが置き換わることを保証するためのステップが行われてもよい。このプロセスは識別・確認（ＩＤ＆Ｖ：Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ ａｎｄ Ｖｅｒｉｆｉｃａｔｉｏｎ）として知られ、トークンが要求されるたびに行われてもよい。行われるＩＤ＆Ｖのタイプ及びＩＤ＆Ｖを行うエンティティを考慮して、所与のトークンにトークン保証レベルが割り当てられてもよい。異なるＩＤ＆Ｖの結果が異なるトークン保証レベルになってもよい。イシュアは、トークンを使用する決済トランザクションを認可（オーソリゼーション）する前に、そのトークンに関連付けられる保証のレベル及び保証のレベルを生成するために使用されたデータを欲してもよい。所与のトークンに割り当てられる保証レベルが時間と共に変化して、不正関連チャージバックなどの、信頼レベルに影響する不正なトランザクションとのなんらかの関係のような因子に基づいて再調整されてもよい。

【課題を解決するための手段】

【０００９】

例示的一実施例によれば、ある方法が提供される。この方法は、ある要求元からオーソリゼーション要求メッセージをコンピュータによって受信するステップを含む。オーソリゼーション要求メッセージはカード会員番号を表す決済トークンを含む。カード会員番号はイシュアによって割り当てられてもよい。オーソリゼーション要求メッセージは、カード会員番号を使用した決済トランザクションの遂行を求めるものである。方法は、トークンに関連付けられたトークン保証レベルを、そのトークン保証レベルを生成するために使用されたデータと共に、コンピュータによって受信するステップもまた含む。トークン保証レベルは、決済トークンと決済トークンによって表されるカード会員番号との間の関係における信頼のレベルを表してもよい。トークン保証レベルは、決済トークンが生成されるときに使用される識別・確認方法に基づいてもよい。いくつかの実施例では、トークン保証レベルは識別・確認方法を行うエンティティに基づく。さらにこの方法は、オーソリゼーション要求メッセージを、トークン保証レベル及びトークン保証レベルを生成するために使用されたデータを含むようにコンピュータによって修正するステップを含む。この方法は、修正されたオーソリゼーション要求メッセージを、コンピュータによってイシュアに承認を求めて送信するステップをさらに含む。

【００１０】

様々な実施例によれば、方法は、オーソリゼーション要求メッセージを受信する前に、カード会員番号を表すように決済トークンを生成することを求めるトークン生成メッセージをコンピュータによって受信するステップをさらに含む。トークン生成メッセージは、決済トークンに関連付けられるよう要求されるトークン保証レベルを含んでもよい。この方法は、コンピュータによって、決済トークン及び決済トークンに関連付けられるトークン保証レベルを生成するステップ並びに、決済トークン、トークン保証レベル、及び決済トークンに関連付けられたカード会員番号をレポジトリに保管するステップをさらに含んでもよい。

【００１１】

いくつかの実施例では、方法はまた、１つ又は複数のカード会員番号と１つ又は複数のカード会員番号に対して生成された１つ又は複数の決済トークンとの間の１対１のマッピングを保管するレポジトリと対話するステップを含んでもよい。

【００１２】

別の実施例は、上記の方法を行うように構成された装置、システム、及びコンピュータ可読媒体に向けられる。

【００１３】

別の例示的実施例はある方法を目的とし、この方法は、決済トークン及び決済トークンに関連付けられるトークン保証レベルをコンピュータによって生成するステップを含み、決済トークンはイシュアによって割り当てられたカード会員番号を表す。この方法はまた、決済トークンをコンピュータによって要求元に送信するステップと、オーソリゼーショ

ン要求メッセージをコンピュータによって要求元から受信するステップとを含む。オーソリゼーション要求メッセージは決済トークンを含んでもよい。オーソリゼーション要求メッセージはカード会員番号を使用した決済トランザクションの遂行を求めるものである。この方法は、オーソリゼーション要求メッセージを、トークン保証レベル及びトークン保証レベルを生成するために使用されたデータを含むようにコンピュータによって修正するステップと、修正されたオーソリゼーション要求メッセージをコンピュータによってイシュアに承認を求めて送信するステップとをさらに含んでもよい。

【００１４】

これら、及びその他の実施例について、下記にさらに詳細に説明する。

【図面の簡単な説明】

【００１５】

【図１】本発明の例示的一実施例による、トークン化エコシステム環境内の様々なエンティティ相互作用の概観を示すシステム及びフローを示す図である。

【図２】本発明の例示的一実施例による、決済ネットワークがトークン・サービス・プロバイダとして働くトークン化エコシステム環境内の様々なエンティティ相互作用の概要を示すシステム及びフローを示す図である。

【図３】本発明の例示的一実施例による、販売店端末トランザクションでのモバイル・デバイスのオーソリゼーション・フローのためのシステム及びフローを示す図である。

【図４】本発明の例示的一実施例による、モバイル・ウォレット／デジタル・ウォレット電子商取引トランザクションのオーソリゼーション・フローのためのシステム及びフローを示す図である。

【図５】本発明の例示的一実施例による、カード・オン・ファイル電子商取引トランザクションのオーソリゼーション・フローのためのシステム及びフローを示す図である。

【図６】本発明の例示的一実施例による、販売店端末トランザクションでのスキャンのためのオーソリゼーション・フローのためのシステム及びフローを示す図である。

【図７】本発明の例示的一実施例による、トークン・トランザクションのキャプチャ及び精算プロセスのためのシステム及びフローを示す図である。

【図８】本発明の例示的一実施例による、トークン・トランザクションのチャージバック要求プロセスのためのシステム及びフローを示す図である。

【図９】本発明の例示的一実施例によるトークン・サービスの実施に伴う様々な役割の概要を示す図である。

【図１０】本発明の実施例による例示的コンピュータ・システムを示す図である。

【発明を実施するための形態】

【００１６】

本発明の実施例は、トークンの生成、確認、認定、及び決済処理ネットワーク間での使用を可能にする、トークン・サービスの相互運用性のフォーマット及び機能を含むネットワーク・トークン・システムを実施及び提供するための方法、装置、コンピュータ可読媒体及びシステムに向けられている。

【００１７】

トークンは、決済エコシステム内でカード会員番号（ＰＡＮ）に置き換わる代用値を含む。決済トークンを使用して、決済トランザクションが開始されてもよい。

【００１８】

不正使用に対する保護を決済トークンによって強化するために、トークンは、特定の販売店又はチャネルなどの特定の領域内に限定して使用されてもよい。これらの基本的な使用規制はトークンの利点であり、本実施例はそれらの実装のための方法について説明する。

【００１９】

さらに、トークンが発行される時点で、そのトークンがトークン要求元によって合法的に使用されていたＰＡＮに置き換わることを保証するためのステップが行われてもよい。このプロセスは識別・確認（ＩＤ＆Ｖ）として知られ、トークンが要求されるたびに行われてもよい。所与のトークンに、行われるＩＤ＆Ｖのタイプを考慮して、トークン保証レ

ベルが割り当てられてもよい。異なるＩＤ＆Ｖの結果が異なるトークン保証レベルになってもよい。例えば、信頼されないエンティティがＩＤ＆Ｖを行わない場合又は、最小限のＩＤ＆Ｖしか行わない場合はトークン保証レベルが低くなることがあり、信頼されるエンティティが詳細なＩＤ＆Ｖを行う場合は高いトークン保証レベルが得られる可能性が高い。したがって、トークンに関連付けられる保証レベルは、トークンが生成されるときに行われるＩＤ＆Ｖ方法と、ＩＤ＆Ｖ方法を行ったエンティティとに依存する。イシュアが、トークンを使用する決済トランザクションを認可（オーソリゼーション）する前に、そのトークンに関連付けられる保証のレベル及び保証のレベルを生成するために使用されたデータを欲してもよい。

【００２０】

決済エコシステム内のすべての利害関係者に利益があり、そのことが、トークン採用の促進の一助となる場合がある。まず、より安全な新しい決済の手法、承認レベルの向上、及び、データ漏洩の発生に続く不正のリスクの削減によって、イシュア及びカード名義人が利益を得られる場合がある。次に、特定の領域に制限されている限りトークン・データベースはあまり魅力的な標的にはならないので、アクワイアラ（ａｃｑｕｉｒｅｒ）及び販売店が経験するオンライン攻撃及びデータ漏洩の恐れが減少する場合がある。アクワイアラ及び販売店はまた、トークンが大口トランザクションに対してより高い保証レベルを提供し得ることからも利益を得られる場合がある。加えて、相互運用性を促進し、ネットワーク及びその参加者のデータ保護プロセスを削減するために役立つオープン・フォーマットを、決済処理ネットワークが採用できる場合もある。さらに、イシュアが、トークンを含むトランザクション要求を承認すべきかの判断を、そのトークンに関連付けられるトークン保証レベル及びトークン保証レベルの生成に使用されたデータに基づいて行うことが可能な場合もある。

【００２１】

本発明の実施例は、トークン化エコシステム環境（トークン化ランドスケープ）について説明し、トークン化をサポートするために必要なエンティティの役割を定め、本発明の実施例の影響を特定し、トークンの要求、トークンの発行及びプロビジョニング、並びにトランザクション処理に関連付けられたデータ・フィールドを指定し、必要なアプリケーション・プログラミング・インタフェース（ＡＰＩ：Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍｍｉｎｇ　Ｉｎｔｅｒｆａｃｅ）を特定してもよい。本発明の実施例は、決済業界内の相互運用性を保持するように設計される。実施例は、トークンに関連付けられるトークン保証レベルをトークン保証レベルの生成に使用されたデータと共にオーソリゼーション要求メッセージ内に提供するようにさらに設計され、そのメッセージは、例えばイシュアに送信される。

【００２２】

本発明の実施例はまた、トークン化エコシステムの詳細な説明、用語定義、責任、及びエコシステム内のエンティティに特定の規制を提供するように意図される。下記に、例示的ユースケース、関係するトランザクション・フロー、及び、従来のオーソリゼーション、キャプチャ、精算、例外処理などの決済機能の間を流れるトランザクション・フロー内の特定のフィールドについて説明する。

【００２３】

特定の実施例及び実例について説明する前に、本明細書で使用されるいくつかの用語を下記に定義する。

【００２４】

「トークン」は、ある決済アカウントの、カード会員番号（ＰＡＮ）などのアカウント識別子の代替となる識別子を含んでもよい。例えば、トークンは、元のアカウント識別子に置き換えて使用され得る一連の数字及び／又は英数字を含んでもよい。例えば、ＰＡＮ「４１４７　０９００　００００　１２３４」の代わりにトークン「４９００　００００　００００　０００１」が使用されてもよい。いくつかの実施例では、トークンは「フォーマット保持型」で、既存の決済処理ネットワークで使用されているアカウント識別子に

準拠する数字フォーマット（例えば、ＩＳＯ８５８３金融トランザクション・メッセージ・フォーマットなど）を有してもよい。いくつかの実施例では、トークンをＰＡＮの代わりに使用して、決済トランザクションを開始、認可（オーソリゼーション）、確定又は、解決してもよいし、通常は元の信用情報が提供される他のシステム内で元の信用情報を表してもよい。いくつかの実施例では、トークン値から元のＰＡＮ又は他のアカウント識別子が計算的に導出されて復元されることのないようにトークン値が生成されてもよい。さらに、いくつかの実施例では、トークンを受け取るエンティティがそれをトークンであると識別すると共にそのトークンを発行したエンティティを認知することができるように、トークン・フォーマットが構成されてもよい。

【００２５】

決済ネットワークによって決済アカウントのイシュアに「銀行識別番号（ＢＩＮ：Ｂａｎｋ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）」が割り当てられてもよい。ＢＩＮは、そのＢＩＮを割り当てた決済ネットワークを、そのＢＩＮ及び関連するアカウントの範囲に基づいて特定できるように、業界のアカウント及びイシュアの識別仕様（例えば、ＩＳＯ７８１２）に準拠してもよい。

【００２６】

いくつかの実施例ではトークン・フォーマットによって、決済システム内のエンティティがトークンに関連付けられたイシュアを特定することができてもよい。例えば、トークンのフォーマットに、あるエンティティがイシュアを特定できるようにするトークン・イシュア識別子が含まれてもよい。例として、トークン・イシュア識別子は、既存の決済フローをサポートするために、元のＰＡＮのイシュアのＢＩＮに関連付けられていてもよい。トークン・イシュア識別子は、そのイシュアのＢＩＮと異なる番号でもよく、また固定番号でもよい。例えば、あるイシュアについて、イシュアのＢＩＮが４１２３４５であるときに、トークン・イシュア識別子が４２８３２５というトークンＢＩＮでもよく、この番号は、そのイシュアから発行されるか、そのイシュアに対して発行されるすべてのトークンについて固定でもよい。いくつかの実施例では、トークン・イシュア識別子の範囲（例えば、イシュアのトークンＢＩＮの範囲）は関連するイシュアのカードの範囲と同じ属性を有してもよく、イシュア識別子ルーティング表（例えば、ＢＩＮルーティング表）に含ませることができる。イシュア識別子ルーティング表は、決済システム内の関連するエンティティ（例えば、販売店及びアクワイアラ）に提供されてもよい。

【００２７】

「トークンＢＩＮ」とは、トークン発行のみを目的として設計された特定のＢＩＮを指し、ＢＩＮ表の中でフラグ付けによってトークンＢＩＮであることが示されてもよい。トークンＢＩＮは２つの目的を有してはならず、また、カード会員番号（ＰＡＮ）とトークンの両方を発行するために使用されてもならない。

【００２８】

「トークン・イシュア識別子の範囲（イシュアＢＩＮの範囲）」は、事前に割り当てられた１組のトークン・イシュア識別子（例えば６桁のトークンＢＩＮ）から作られる固有識別子（例えば６～１２桁の）を指してもよい。例えば、いくつかの実施例では、あるイシュアに関連付けられたイシュアＢＩＮの範囲のそれぞれにトークンＢＩＮの範囲を１つ又は複数割り当てることができる。いくつかの実施例では、トークンＢＩＮの範囲は決済トークンを生成するために使用されてもよいが、決済トークン以外を生成するために使用されてはならない。いくつかの実施例では、トークンは、例えばＬｕｈｎチェック又はチェックサム認定などの、決済システム内の複数の異なるエンティティによって設定され得るアカウント番号の基本的な認定規則に沿ってもよい。いくつかの実施例では、決済トークン・イシュア識別子が、あるイシュアの実際のイシュア識別子（例えばＢＩＮ）にマッピングされてもよい。例えば、ある決済トークン・イシュア識別子が６桁の数値を含み、その数値があるイシュアに関連付けられていてもよい。例として、決済トークン・イシュア識別子を含む任意のトークンが特定のイシュアに関連付けられていてもよい。そのように、トークン・イシュア識別子に関連付けられた対応するイシュア識別子の範囲を使用し

てイシュアが特定されてもよい。例えば、決済トークン「５４００　０００　０００　０００１」に対応する決済トークン・イシュア識別子「５４０００」を、決済アカウント識別子「５５３１４１　０９００　０００　１２３４」に対応するイシュア識別子「５５３１４１」にマッピングすることができる。いくつかの実施例では、決済トークン・イシュア識別子は、あるイシュアに対して固定である。例えば、ある決済トークン・イシュア識別子（例えば「５４０００」）が第１のイシュアに対応し、別の決済トークン・イシュア識別子（例えば「５５０００」）が第２のイシュアに対応してもよく、第１及び第２の決済トークン・イシュア識別子はネットワーク・トークン処理システム内のすべてのエンティティに通知せずに変更又は修正されてはならない。いくつかの実施例では、決済トークン・イシュア識別子の範囲が、あるイシュア識別子に対応してもよい。例えば、「４９０００」～「４９０００２」の決済トークン・イシュア識別子を含む決済トークンが第１のイシュアに対応し（例えば、イシュア識別子「４１４７０９」にマッピングされる）、「５２０００」～「５２０００２」の決済トークン・イシュア識別子を含む決済トークンが第２のイシュアに対応してもよい（例えば、実際のイシュア識別子「５１７５４８」にマッピングされる）。トークンＢＩＮの範囲及びそれらのＢＩＮの範囲からのトークンの割り当てが、トランザクションを受け取ってルーティングの決定を行う当事者のために利用に供されてもよい。

【００２９】

「トークン・サービス・システム」は、トークンの要求、生成及び発行、並びに、トークンからカード会員番号（ＰＡＮ）への確定済みのマッピングをレポジトリ（例えば、トークン保管庫（ｔｏｋｅｎ　ｖａｕｌｔ））内で維持することを容易にするシステムを指す。トークン・サービス・システムは、トークンとＰＡＮの紐付けの信頼レベルを示すトークン保証レベルを所与のトークンについて確定してもよい。トークン・サービス・システムは、トークンを使用してサブミットされた決済トランザクションのトークン処理を、そのトークンをデトークン化して実際のＰＡＮを取得することによってサポートしてもよい。様々な実施例で、トークン・サービス・システムは、トークン要求元及び、そのトークン要求元と対話するトークン・サービス・プロバイダを含んでもよい。

【００３０】

「トークン・サービス・プロバイダ」は、トークンを生成、処理、及び維持する、トークン・サービス・システム内の１つ又は複数のサーバ・コンピュータを含むエンティティを指してもよい。トークン・サービス・プロバイダは、生成されたトークンが保管されるトークン保管庫を含むか、又はそれと通信状態にあってもよい。具体的には、トークン保管庫は、トークン及びそのトークンによって表されるカード会員番号（ＰＡＮ）との間の１対１のマッピングを維持してもよい。トークン・サービス・プロバイダは、そのトークン・サービス・プロバイダへサブミットされる可能性のあるＰＡＮのトークンを発行するためのトークンＢＩＮとして、使用許可済みのＢＩＮを確保しておくことができてもよい。トークン化エコシステム内の様々なエンティティが、トークン・サービス・プロバイダの役割を引き受けてもよい。例えば、決済ネットワーク及び、イシュア又はそのエージェントが本発明の実施例によってトークン・サービスを実装することによってトークン・サービス・プロバイダになってもよい。トークン・サービス・プロバイダは、報告ツールに出力される、承認済み、保留中、又は拒否されたトークン要求に関する報告又はデータを提供してもよく、これには、割り当てられた任意のトークン要求元ＩＤが含まれる。トークン・サービス・プロバイダは、トークンベースのトランザクションに関するデータ出力を報告ツール及びアプリケーションに提供して、そのトークン及び／又はＰＡＮが報告出力に適していることを示してもよい。

【００３１】

「トークン保管庫」は、確定されたトークン－ＰＡＮ間マッピングを維持するレポジトリを指してもよい。様々な実施例によれば、トークン要求元のその他の属性をトークン保管庫が維持してもよく、その属性は登録の時点で決定されてもよく、また、トランザクション処理中にドメイン制限又は他の規制を適用するためにトークン・サービス・プロバイ

ダが使用してもよい。トークン保管庫は、トークン・サービス・システムの一部であってもよい。いくつかの実施例では、トークン保管庫はトークン・サービス・プロバイダの一部として提供されてもよい。或いは、トークン保管庫は、トークン・サービス・プロバイダからアクセス可能な遠隔レポジトリであってもよい。トークン保管庫に保管及び管理されるデータ・マッピングの機密性の理由から、トークン保管庫は、基礎的な、強力な物理的・論理的セキュリティによって保護されてもよい。

【００３２】

「識別・確認（ＩＤ＆Ｖ）方法」を使用して、トークン要求元によって合法的に使用されていたＰＡＮにその決済トークンが置き換わることが保証されてもよい。ＩＤ＆Ｖ方法の例は、アカウント確認メッセージ、カード会員番号（ＰＡＮ）の評価に基づくリスク・スコア、及び、イシュア又はそのエージェントによるワンタイム・パスワードを使用したアカウント名義人の確認が含まれてもよいが、これらに限定されない。例示的ＩＤ＆Ｖ方法は、ユーザ署名、パスワード、オフライン又はオンラインの個人識別番号（ＰＩＮ：Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）、オフライン又はオンラインの暗号化ＰＩＮ、オフラインＰＩＮと署名の組み合わせ、オフラインの暗号化ＰＩＮと署名の組み合わせ、ユーザ生体認証（例えば、音声認識、指紋照合など）、パターン、グリフ、ナレッジベースのチャレンジ・レスポンス認証、ハードウェア・トークン（複数のソリューションが選択可能）、使用制限付きのワンタイム・パスワード（ＯＴＰ：Ｏｎｅ　Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ）、ソフトウェア・トークン、２段階認証プロセス（例えば、電話を使用）などの情報を使用して行われてもよい。ＩＤ＆Ｖを使用して、トークンとＰＡＮの紐付けに関して信頼レベルが確定されてもよい。

【００３３】

「トークン保証レベル」は、トークン・サービス・プロバイダがトークンとＰＡＮの紐付けの信頼レベルを示せるようになる指示子又は値を指してもよい。トークン保証レベルは、行われた識別・確認（ＩＤ＆Ｖ）のタイプ及びＩＤ＆Ｖを行ったエンティティに基づいて決定されてもよい。トークン保証レベルは、トークンの発行時に設定されてもよい。トークン保証レベルは、追加のＩＤ＆Ｖが行われた場合に更新されてもよい。

【００３４】

「要求トークン保証レベル」は、トークン要求元によってトークン・サービス・プロバイダに要求されるトークン保証レベルを指してもよい。要求トークン保証レベルは、トークンの生成／発行を求めて要求元からトークン・サービス・プロバイダに送信されるトークン要求メッセージのフィールドに含まれてもよい。

【００３５】

「割り当てられるトークン保証レベル」は、トークン化エコシステム内のあるエンティティによって行われた識別・確認（ＩＤ＆Ｖ）プロセスの結果としてトークン・サービス・プロバイダがトークンに割り当てる実際の（すなわち生成された）値を指してもよい。割り当てられるトークン保証レベルは、トークン要求メッセージに応答してトークン要求元に返されてもよい。割り当てられるトークン保証レベルは、トークン要求メッセージに含まれる要求トークン保証レベルとは異なってもよい。

【００３６】

「トークン属性」は、トークンに関する任意の特徴又は情報を含んでもよい。例えば、トークン属性は、トランザクション・システム内で、あるトークンをどのように使用、配信、発行できるか、又は、データをどのように操作してもよいかを判断できる情報を含んでもよい。例えば、トークン属性は、トークンのタイプ、使用頻度、トークンの有効日付及び／又は有効時刻、関連するトークンの数、トランザクション・ライフサイクルの有効日付、及び、トークン化エコシステム内の任意のエンティティに関する任意の追加情報を含んでもよい。例えば、トークン属性は、そのトークンに関連付けられたウォレット識別子、追加のアカウント・エイリアス又はその他のユーザ・アカウント識別子（例えば、Ｅメール・アドレス、ユーザ名など）、デバイス識別子、インボイス番号などを含んでもよい。いくつかの実施例では、トークン要求元がトークンの生成を要求する時点でトークン

属性を提供してもよい。いくつかの実施例では、ネットワーク・トークン・システム、そのネットワーク・トークン・システムに関連付けられた決済ネットワーク、イシュア、又はそのトークンに関連付けられた任意の他のエンティティが、特定のトークンに関連付けられたトークン属性を決定及び／又は提供してもよい。

【００３７】

トークン属性は、トークンがどのように使用されてもよいかを示すトークンのタイプを特定してもよい。決済トークンは、ある消費者アカウント及び／又はカードのための最初の、及び／又は後続のトランザクションの生成に、実際のアカウント識別子（例えば、ＰＡＮ）の代わりに使用できる高価値トークンを含んでもよい。別のトークン・タイプとして、それぞれ固定的及び変動的なトークンのための「固定」又は「変動」のトークン・タイプがあってもよい。

【００３８】

「トークン提示モード」は、トランザクションのためにトークンがサブミットされる方法を示す。トークン提示モードのいくつかの非限定的な実例は、機械可読コード（例えば、クイック・レスポンス・コード（ＱＲＣ：Ｑｕｉｃｋ　Ｒｅｓｐｏｎｓｅ　Ｃｏｄｅ）、バーコードなど）、モバイル非接触モード（例えば、近距離通信（ＮＦＣ：Ｎｅａｒ－Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）通信）、電子商取引遠隔モード、電子商取引近接モード、及び、トークンをサブミットするためのその他の任意の適切なモードを含んでもよい。トークンは、任意の数の異なる方法によって提供されてもよい。例えば一実装例では、トークンは、ウォレット・プロバイダ、モバイル・アプリケーション又はその他のモバイル・デバイス上のアプリケーションによって生成される機械可読コードに埋め込まれて、モバイル・デバイスのディスプレイに表示されもよい。機械可読コードは店頭でスキャン可能であり、そのコードを通してトークンが販売店に渡される。モバイル非接触モードは、ＮＦＣを通してトークンを非接触メッセージで渡すことを含んでもよい。電子商取引遠隔モードは、消費者又はウォレット・プロバイダによって小売りアプリケーション又はその他のモバイル・アプリケーションを使用して、トークンを、オンライン・トランザクションを通して、又は電子商取引トランザクションとしてサブミットすることを含んでもよい。電子商取引近接モードは、消費者によって、販売店店頭でモバイル・デバイス上のウォレット・アプリケーションからトークンをサブミットすることを含んでもよい。

【００３９】

「トークン化」は、データが代替データに置き換えられるプロセスである。例えば、決済アカウント識別子（例えば、カード会員番号（ＰＡＮ））をその決済アカウント識別子に関連付けられた代替番号（例えばトークン）に置き換えることによって、そのカード会員番号がトークン化されてもよい。さらに、トークン化は、代替の値（すなわちトークン）に置き換えられてもよい他のどのような情報にも適用され得る。トークン化は、トランザクションの効率を向上させ、トランザクションのセキュリティを強化し、サービスの透明性を改善し、又は、第３者の関与を可能にする方法を提供するために使用されてもよい。

【００４０】

「トークン交換」又は「デトークン化」は、トークン化の期間中に置き換えられていたデータを復旧させるプロセスである。例えば、トークン交換は、あるカード会員番号（ＰＡＮ）がトークン化されている期間に決済トークンに関連付けられていた対応ＰＡＮに決済トークンを置き換えることを含んでもよい。このように、デトークン化は、トークンを、保管されているトークン－ＰＡＮ間マッピングに基づいて関連するＰＡＮ値に戻すプロセスを指してもよく、マッピングは例えばトークン保管庫に保管されていてもよい。関連するトークンと交換にＰＡＮを取り込む能力は、明確に認可（オーソリゼーション）されたエンティティ、個人、アプリケーション、又はシステムに制限されてもよい。さらに、他の任意の情報にデトークン化又はトークン交換が適用されてもよい。いくつかの実施例では、ＩＳＯメッセージ、アプリケーション・プログラミング・インタフェース（ＡＰＩ

）、又は別のタイプのウェブ・インタフェース（例えば、ウェブ要求）などのトランザクション的なメッセージを介してトークン交換が行われてもよい。

【００４１】

「トークン要求元」は、本発明の実施例によってトークン化を実装しようとするエンティティを指してもよい。トークン要求元は、カード会員番号（ＰＡＮ）をトークン化するよう求める要求を、トークン・サービス・プロバイダにトークン要求メッセージをサブミットすることによって開始してもよい。本明細書で述べる様々な実施例によれば、トークン要求メッセージに応答して要求元がトークンを受け取った後は、トークン要求元がトークンに関連付けられたＰＡＮを保管しておく必要がなくてもよい。要求元は、トークンに関連付けられたアクションを行うように構成されたアプリケーション、デバイス、プロセス、又はシステムであってもよい。例えば、要求元はネットワーク・トークン・システムへの登録の要求、トークン生成の要求、トークンの有効化、トークンの無効化、トークン交換、その他のトークンのライフサイクル管理に関するプロセス、及び／又は、その他のトークンに関する任意のプロセスを行うことができる。要求元は、任意の適切な通信ネットワーク及び／又はプロトコルを通して（例えば、とりわけ、ＨＴＴＰＳ、ＳＯＡＰ、及び／又はＸＭＬインタフェースを使用して）ネットワーク・トークン・システムとやりとりしてもよい。トークン要求元のいくつかの非限定的な実例は、例えば、カード・オン・ファイル販売店、アクワイアラ、アクワイアラ・プロセッサ、販売店の代理の役割をする決済ゲートウェイ、ペイメント・イネーブラ（例えば、相手先ブランド製造元（ＯＥＭ：Ｏｒｉｇｉｎａｌ Ｅｑｕｉｐｍｅｎｔ Ｍａｎｕｆａｃｔｕｒｅｒ）、モバイルネットワーク・オペレータなど）、デジタル・ウォレット・プロバイダ、イシュア、第３者ウォレット・プロバイダ、及び／又は決済処理ネットワークを含んでもよい。いくつかの実施例では、トークン要求元は複数のドメイン及び／又はチャネルについてトークンを要求することができる。トークン要求元は、トークン化エコシステム内でトークン・サービス・プロバイダによって一意に登録及び特定されてもよい。トークン・サービス・プロバイダはトークン要求元の登録時に、トークン・サービス・システムへの参加を求めるトークン要求元の申請を正式に処理してもよい。トークン・サービス・プロバイダは、トークン要求元を認定して正式に承認し、適切なドメイン制限規制を確立するために、要求元の性質及び関連するトークン使用法に係わる情報を収集してもよい。登録に成功したトークン要求元にトークン要求元識別子を割り当て、それをトークン保管庫に入力して維持することもできる。トークン要求元は無効化されてもよいし、又は新しいトークン要求元識別子を割り当てられてもよい。この情報は、トークン・サービス・プロバイダによる報告及び監査の対象となってもよい。

【００４２】

「トークン要求元識別子（ＩＤ：Ｉｄｅｎｔｉｆｉｅｒ）」は、あるネットワーク・トークン・システムに関連付けられたエンティティに関連付けられた任意の文字、数字、又は他の識別子を含んでもよい。いくつかの実施例では、同一のトークン要求元に関連付けられたトークン要求に対して各ドメインに固有のトークン要求元ＩＤが割り当てられてもよい。例えば、あるトークン要求元ＩＤによって、トークン要求元（例えば、モバイル・デバイス、モバイル・ウォレット・プロバイダなど）とトークン・ドメイン（例えば、電子商取引、非接触など）とのペアリングを特定することができる。トークン要求元ＩＤは、任意のフォーマット又はタイプの情報を含んでもよい。例えば一実施例では、トークン要求元ＩＤは、１０桁又は１１桁の文字及び／又は数字（例えば、４６７８０１２３４５）などの英数字の値を含んでもよい。いくつかの実施例では、トークン要求元ＩＤは、ネットワーク・トークン・システムなどのトークン・サービス・プロバイダのコード（例えば、最初の３桁）を含んでもよく、残りの桁がトークン・サービス・プロバイダによって要求元のエンティティ（例えば、モバイル・ウォレット・プロバイダ）及びトークン・ドメイン（例えば、非接触、電子商取引など）に割り当てられてもよい。

【００４３】

「トークン要求指示子」は、それを含むメッセージがトークン要求に関係することを示

すために使用される指示子を指してもよい。任意選択として、アカウント状態チェックが行われる理由をイシュアに通知するために、識別・確認（ＩＤ＆Ｖ）方法の一部としてトークン要求指示子がイシュアに渡されてもよい。

【００４４】

「トークン・ドメイン」は、トークンの発行時に確定することができる、決済トランザクションのトークンの適切な使用を可能にする因子を表してもよい。トークン・ドメインの例は、ＰＯＳ入力モード及び、トークンがどこで使用可能なのかを一意に特定する販売店識別子を含んでもよいが、これらに限定されない。トークン発行ステップの一部として、決済トランザクションで適切なトークンの使用を強制できるようにするための１組のパラメータ（すなわち、トークン・ドメイン制限規制）がトークン・サービス・プロバイダによって確定されてもよい。例えば、トークン・ドメイン制限規制は、非接触提示モード又は電子商取引の提示モードなどの特定の提示モードにトークンの使用を制限してもよい。いくつかの実施例では、トークン・ドメイン制限規制は、一意に特定することが可能な特定の販売店店頭のみにトークンの使用を制限してもよい。いくつかの例示的トークン・ドメイン制限規制では、所与のトランザクションに固有のトークン暗号文の存在を確認することが要求されてもよい。

【００４５】

「トークン有効期限」は、トークン・サービス・プロバイダによって生成されてトークン保管庫に保管されるトークンの有効日付／有効時刻を指してもよい。トークン有効期限は、相互運用性を確保し、トークン化の実施の影響を最小限に抑えるために、トランザクション処理中にトークン化エコシステムのエンティティの間で受け渡されてもよい。トークン有効期限は、業界の標準に従う数値（例えば、４桁の数値）であってもよい。

【００４６】

「トークン相互運用性」は、本発明の実施例に定められた新しいデータ・フィールド及びデータ・フィールド値と共にトークンを使用するときに、既存の相互運用性機能を通した当事者間のトランザクションの処理及び交換が保持されることを保証するためのプロセスを指してもよい。

【００４７】

「トークン処理」は、カード会員番号（ＰＡＮ）の代わりにトークンが存在するトランザクション処理を指してもよい。トークンは、ネットワーク全体を通した相互作用の観点から処理される。トークン処理は、トランザクションを完了するために、トークンのデトークン化にトークン保管庫を使用することをさらに含む。トークン処理は、オーソリゼーション、キャプチャ、精算、例外処理を含む決済プロセスにまたがってもよい。

【００４８】

「消費者」は、１つ又は複数の個人アカウント及び／又は消費者デバイスに関連付けられた個人又はユーザを含んでもよい。消費者はまた、カード名義人、アカウント名義人、又はユーザと称されてもよい。

【００４９】

「カード会員番号（ＰＡＮ）」は、あるＢＩＮに関連付けられたアカウントの範囲内でイシュアによって生成される業界標準に準拠する可変長（例えば１３桁～１９桁）のアカウント番号であってもよい。

【００５０】

「カード・オン・ファイル（ＣＯＦ：Ｃａｒｄ－Ｏｎ－Ｆｉｌｅ）」販売店は、アカウントの詳細（例えば、カードの詳細、決済アカウント識別子、ＰＡＮなど）をトランザクションで使用するために保管する任意のエンティティを含んでもよい。例えば、ＣＯＦエンティティは、毎月の公共料金の決済（支払い）、定期的な購買トランザクション、又は他の定期的又は将来のトランザクションなどの様々なタイプの定期的決済のために、店舗の決済情報をファイルに保管してもよい。将来のトランザクションのために決済認証情報及び／又は関連するトークンがエンティティに保管されるので、ＣＯＦエンティティによって開始されるトランザクションは、カード非介在（ＣＮＰ：Ｃａｒｄ－Ｎｏｔ－Ｐｒｅ

ｓｅｎｔ）トランザクションを含む。別のタイプのカード非介在（ＣＮＰ）トランザクションには、遠隔当事者間（例えば、消費者デバイスと小売りＷｅｂサーバ・コンピュータとの間）で開始される電子商取引（「電子商取引」）トランザクションが含まれる。

【００５１】

「オーソリゼーション要求メッセージ」は、決済トランザクションに対するオーソリゼーションを要求するために決済処理ネットワーク及び／又は決済アカウントのイシュアに送信される電子メッセージであってもよい。いくつかの実施例によるオーソリゼーション要求メッセージはＩＳＯ８５８３に準拠してもよく、この標準は、決済デバイス又は決済アカウントを使用して消費者によって行われる決済に関連付けられた電子トランザクション情報を交換するシステムのための標準である。本発明のいくつかの実施例では、オーソリゼーション要求メッセージは、決済トークン、有効日付、トークン提示モード、トークン要求元識別子、トークン暗号文、トークン保証レベル、及びトークン保証レベルの生成に使用されたデータを含んでもよい。決済トークンは、決済トークン・イシュア識別子を含んでもよく、それがイシュアの実際のイシュア識別子の代わりとなってもよい。オーソリゼーション要求メッセージはまた、「識別情報」に対応する追加のデータ要素を含んでもよく、これには、例えば、サービス・コード、ＣＶＶ（カード確認値：Ｃａｒｄ Ｖｅｒｉｆｉｃａｔｉｏｎ Ｖａｌｕｅ）若しくはＣＶＣ（カード確認コード：Ｃａｒｄ Ｖｅｒｉｆｉｃａｔｉｏｎ Ｃｏｄｅ）、ｄＣＶＶ（変動カード確認値：ｄｙｎａｍｉｃ Ｃａｒｄ Ｖｅｒｉｆｉｃａｔｉｏｎ Ｖａｌｕｅ）若しくはｄＣＶＣ（変動カード確認コード：ｄｙｎａｍｉｃ Ｃａｒｄ Ｖｅｒｉｆｉｃａｔｉｏｎ Ｃｏｄｅ）、トークン暗号文、有効日付などがある。オーソリゼーション要求メッセージはまた、現在のトランザクションに関連付けられた任意の情報（例えば、トランザクション量、販売店識別子、販売店の場所など）などの「トランザクション情報」並びに、ある決済トランザクションを識別及び／又は認可（オーソリゼーション）するか判断するために使用されてもよい任意の他の情報を含んでもよい。

【００５２】

「オーソリゼーション応答メッセージ」は、発行元の金融機関（すなわちイシュア）又は決済処理ネットワークによって生成される、オーソリゼーション要求メッセージへの電子メッセージ応答であってもよい。オーソリゼーション応答メッセージはオーソリゼーション・コードを含んでもよく、このコードは、オーソリゼーション要求メッセージに応答してアカウント発行元の銀行が電子メッセージで販売店のアクセス・デバイス（例えば、ＰＯＳ端末）に（直接又は決済処理ネットワークを通して）返す、トランザクションの承認を示すコードであってもよい。このコードはオーソリゼーションの証明の役割を果たしてもよい。前述したように、いくつかの実施例では、決済処理ネットワークがオーソリゼーション応答メッセージを生成し、且つ／又は販売店に転送してもよい。

【００５３】

「サーバ・コンピュータ」は、通常、高性能なコンピュータ又はコンピュータのクラスタであってもよい。例えば、サーバ・コンピュータは大型メインフレーム、ミニコンピュータのクラスタ、１ユニットとして機能するサーバのグループなどであることができる。サーバ・コンピュータは、決済処理ネットワーク、ウォレット・プロバイダ、販売店、認証クラウド、アクワイアラ、又はイシュアなどのエンティティと関連付けられていてもよい。

【００５４】

「イシュア」は、決済アカウントのイシュアを含むことができる。決済アカウント（１つ又は複数の決済デバイスに関連付けられていてもよい）は、クレジットカードのアカウント、当座預金口座、普通預金口座、消費者に割り当てられた販売店アカウント、又は前払い口座を含む任意の適切な決済アカウントを指してもよい。

【００５５】

「エージェント」は、イシュアによって指名され、イシュアの代理として特定の機能を行うエンティティであってもよい。例示的な機能には、カード処理、３Ｄセキュア・プロ

トコルを使用したカード名義人の確認、及びトークン・サービスを含んでもよい。例えば、識別・確認（ＩＤ＆Ｖ）のために３Ｄセキュア・サービスを提供するアクセス制御サーバ（ＡＣＳ：Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｓｅｒｖｅｒ）がイシュアのエージェントであってもよい。

【００５６】

「決済ネットワーク」は、お金、商品、又はサービスのために決済デバイスによって行われる、トランザクションの受容、送信、又は処理に使用される電子決済システムを指してもよい。決済ネットワークは、イシュア、アクワイアラ、販売店、及び決済デバイスのユーザの間で情報及び資金を伝達してもよい。

【００５７】

Ｉ．トークン化エコシステム環境

本発明の実施例によって概説され、且つ本発明の実施例自体に従う様式でなされるトークン・ソリューションの実装には、図１に示されるトークン化エコシステム環境内の多数のエンティティが関与する。

【００５８】

図１は、本発明の例示的一実施例による、トークン化エコシステム環境１００内の様々なエンティティ対話の概観を示すシステム及びフロー図を示す。トークン化エコシステム環境１００はアカウント名義人１０２、販売店１０６、アクワイアラ１０８、決済ネットワーク１１０及びイシュア１０４を含んでもよい。トークン要求元１１４及びトークン・サービス・プロバイダ１１６がトークン・サービス・システム１１２を形成してもよく、このシステムもまたトークン化エコシステム環境１００の一部である。トークン・サービス・プロバイダ１１６はトークン保管庫１１８及びサーバ・コンピュータ１２０（図１０に詳細を示すものなど）を含んでもよい。下記に説明するように、トークン化エコシステム環境１００の様々なエンティティがトークン要求元１１４の役割を引き受けてもよい。同様に、トークン化エコシステム環境１００の複数の異なるエンティティがトークン・サービス・プロバイダ１１６の役割を引き受けてもよい。各エンティティの役割について、以下により詳しく説明する。

【００５９】

イシュア１０４は、決済トランザクションのためのアカウント（例えば、クレジット・アカウント、デビット・アカウントなど）を発行したビジネス・エンティティ（例えば銀行）のイシュア・プロセッサを表してもよい。いくつかの実装例では、イシュア１０４に関連付けられたビジネス・エンティティ（銀行）は、アクワイアラ１０８としてもまた機能してもよい。イシュア１０４は、あるアカウント名義人１０２の要求に応じて、そのアカウント名義人１０２にカード会員番号（ＰＡＮ）によって表されるアカウントを発行してもよい。アカウント名義人１０２はそのアカウントを使用して、決済トランザクションを行ってもよい。イシュア１０４は、トークン化エコシステム環境１００内でオーソリゼーション及び継続的なリスク管理の責任を負ってもよい。イシュア１０４が、決済トランザクション要求を適切に処理するために、本発明の実施例に定められるとおりに、そのイシュアに渡されるメッセージ又はそのイシュアが渡すメッセージ内に提供されるいかなるデータ・フィールドにも対応することが必要であってもよい。

【００６０】

アカウント名義人１０２が、イシュア１０４によって発行されたアカウント（ＰＡＮによって表される）を使用して販売店１０６との決済トランザクションを行うことを希望してもよい。本明細書で述べるセキュリティの目的から、アカウント名義人１０２が販売店１０６とのＰＡＮの共有を希望しないことがある。それに従って、ＰＡＮを表すトークンがトークン・サービス・システム１１２によって生成され、販売店のサーバ１０６（例えば、販売店のサーバ又はコンピュータ）に渡されてもよい。

【００６１】

いくつかの実施例では、トークンは近距離通信（ＮＦＣ）（例えば、店頭ユースケース）を通して渡されてもよい。さらに別の実施例では、販売店１０６が既にアカウント名義

人１０２のＰＡＮを知っていてもよい（例えば、カード・オン・ファイルユースケース）。例えば、カード・オン・ファイル販売店は、各種の定期決済（例えば、毎月の公共料金の決済）などの将来の決済の目的でアカウント名義人１０２のアカウント情報を（例えば、販売店データベースの）ファイルに保管してもよい。いくつかの実装形態では、アカウント名義人１０２は、カード・オン・ファイル・サービスのために１つ又は複数の販売店１０６に登録してもよい。販売店１０６がカード・オン・ファイル販売店である場合には、販売店１０６がトークン要求元１１４であってもよい。販売店１０６がトークン要求元１１４であるとき、販売店１０６は、本発明の実施例で参照されることのあるトークン・サービスＡＰＩの実施を提供することが必要になってもよい。様々なユースケースについて下記に詳細に説明する。

【００６２】

様々な実施例によれば、カード・オン・ファイル販売店、アクワイアラ、アクワイアラのプロセッサ、販売店の代理の決済ゲートウェイ、ペイメント・イネーブラ（例えば、相手先ブランド製造（ＯＥＭ）装置の製造元）、デジタル・ウォレットのプロバイダ、又はイシュアがトークン要求元１１４の役割を引き受けてもよい。トークン要求元１１４はトークン・サービス・プロバイダ１１６（すなわち、サービス・プロバイダ１１６のサーバ・コンピュータ１２０）に登録してもよい。トークン・サービス・プロバイダ１１６への登録が成功した後に、トークン要求元１１４にトークン要求元ＩＤが割り当てられてもよい。トークン要求元１１４はトークン・サービス・プロバイダ１１６に登録された後に、指定されたトークンＡＰＩを実装してもよい。本発明の実施例と共に使用されることのある様々なＡＰＩについて、図９と共に下記で説明する。トークン要求元１１４はトークン・サービス・プロバイダ１１６と共に、ＡＰＩ内に指定されるプロセス及び技法に従ってトークン要求を開始することができる。トークン要求は、トークン・サービス・プロバイダ１１６にトークン要求メッセージを渡すことによって開始されてもよい。トークン要求メッセージは、トークン要求元情報又はトークン要求元ＩＤ、トークン・ドメイン制限規制、そのトークンによって表される（例えば置き換えられる）ＰＡＮ、及び、任意選択として要求トークン保証レベルを含んでもよい。

【００６３】

トークン・サービス・プロバイダ１１６がトークン要求元１１４から送信されたトークン要求メッセージを処理するときに、トークン・サービス・プロバイダ１１６がトークンを発行してもよい。発行されたトークンはトークン保管庫１１８に保管されると共にトークン要求元１１４に提供されてもよい。トークン・サービス・プロバイダ１１６が、トークン－ＰＡＮ間マッピングを特定し、後続のトランザクション処理で使用するためにトークン保管庫１１８に保管してもよい。トークン保管庫１１８はまた、その要求を開始したトークン要求元のトークン要求元ＩＤを取得して保管することによって、生成された各トークンを恒久的にトークン要求元１１４に関連付けてもよい。

【００６４】

いくつかの実施例では、トークン・サービス・プロバイダ１１６によって生成されたトークンにトークン有効期限が付随してもよい。トークン有効期限は、ＰＡＮ有効期限のフォーマットに適合してもよく、また、実際のＰＡＮと同じ日付でもよいし、又は異なる日付でもよい。様々な実施例で、トークン要求元１１４からの要求に応答して生成されるトークンは、そのトークンが発行されたトークン・ドメイン内のトランザクションに対してのみ妥当である。

【００６５】

したがって、トークン・サービス・プロバイダ１１６は、トークンを生成し、且つ／又はトークン要求元１１４に提供することを認可（オーソリゼーション）され得るトークン化エコシステム環境１００内のエンティティであってもよい。いくつかの実施例では、トークン要求元１１４はトークン・サービス・プロバイダ１１６に登録されてもよい。本発明の例示的実施例によれば、決済ネットワーク１１０、イシュア１０４、又はイシュア１０４のエージェントがトークン・サービス・プロバイダ１１６の役割を負ってもよい。

【００６６】
トークン・サービス・プロバイダ１１６が、トークン発行のために認可（オーソリゼーション）された当事者としての資格の中の多数の個別機能について責任を負ってもよい。トークン・サービス・プロバイダ１１６の機能のうち１つ又は複数がサーバ・コンピュータ１２０によって行われてもよい。トークン・サービス・プロバイダ１１６が、生成されたトークン及び、トークンとそのトークンによって表されるＰＡＮとの間のマッピングを保管するトークン保管庫１１８の継続的な動作及び維持の責任を負ってもよい。トークン・サービス・プロバイダ１１６が、トークンの生成及び発行、並びに生成されたトークンへのセキュリティ及び規制の適用の責任を負ってもよい。トークン・サービス・プロバイダ１１６がトークン要求元１１４を登録して、生成されたトークンを要求元のデバイスにプロビジョニングしてもよい。

【００６７】
トークン・サービス・プロバイダ１１６が、トークン要求元１１４、トークン保管庫１１８、トークン・プロビジョニング・プラットフォーム、及びトークン・レジストリのために、そのトークン・サービス・プロバイダ１１６が独占所有権を有するアプリケーション・プログラミング・インタフェース（ＡＰＩ）を構築及び／又は管理する責任を負ってもよい。ＰＡＮとトークンの不慮の重複をある程度避けるために、トークン・サービス・プロバイダ１１６は、トークンＢＩＮが従来のＢＩＮとは確実に別に管理されるようにしてもよい。トークン・サービス・プロバイダ１１６は、すべての既存トランザクション・プロセスにわたってＰＡＮのプロダクト及びその他の属性が確実に保持される方法でトークンＢＩＮを使用して、トークンを生成してもよい。

【００６８】
様々な実施例によれば、トークン・サービス・プロバイダ１１６が、あるアカウントに関連付けられたＰＡＮに対するトークンを発行するとき、そのトークンがそのアカウントを表すように発行されたことをアカウント名義人１０２が知らなくてもよい。いくつかの実施例では、アカウント名義人１０２がトークン生成時の識別・確認（ＩＤ＆Ｖ）プロセスに参加するよう依頼されてもよい。例えば、アカウント名義人１０２は、トークンが確実に、アカウント名義人１０２によって正当に所有されているアカウントに対して生成されるようにするために、識別情報を提供するよう依頼されてもよい。

【００６９】
行われたＩＤ＆Ｖのタイプに基づいて、トークン・サービス・プロバイダ１１６はトークンの発行時に、生成されたトークンに関連付けられたトークン保証レベルを生成してもよい。トークン保証レベルは、決済トークンとその決済トークンによって表されるＰＡＮとの間の関係の信頼のレベルを表してもよい。例えば、高いトークン保証レベルが、そのトークンとＰＡＮとの関係がオーソリゼーション済みのアカウント名義人から信頼されていることを表し、この保証レベルでは決済（支払い）によって開始される安全で信頼できる決済トランザクションがサポートされてもよい。生成されるトークン保証レベルは、トークン要求元１１４によってトークン要求メッセージ内で任意選択としてトークン・サービス・プロバイダ１１６に提供されることのある要求トークン保証レベルとは異なってもよい。いくつかの実施例では、行われたＩＤ＆Ｖのタイプ又はＩＤ＆Ｖを行ったエンティティに基づいて、生成されるトークン保証レベルが要求トークン保証レベルと同じであってもよい。トークン保証レベルは割り当てられた後に変更されてもよく、及び、信頼レベルに影響することのある、報告された不正又は不正関連チャージバックなどの要因に基づいて再計算されてもよい。

【００７０】
トークン・サービス・プロバイダ１１６によって生成されるトークン保証レベルは、行われたＩＤ＆Ｖ及びＩＤ＆Ｖを行うエンティティに基づいてもよい。ＩＤ＆Ｖ方法は、特定のトークン保証レベルを提供するために単独で、又は組み合わせて使用されてもよい。トークン・サービス・プロバイダ１１６は、１つ又は複数のＩＤ＆Ｖ方法を実装してもよい。加えて、トークン・サービス・プロバイダ１１６は、要求されたトークン保証レベル

に適するＩＤ＆Ｖ方法がトークンの発行時には毎回確実に行われるようにしてもよい。
【００７１】
ＩＤ＆Ｖステップは、トークン・サービス・プロバイダ１１６、トークン要求元１１４、又は第３者によって行われてもよい。ＩＤ＆Ｖステップがトークン・サービス・プロバイダ１１６以外のエンティティによって行われる事例では、そのステップが行われて結果の成果物が提供されたことを証明するための確認可能な証拠が提供されてもよい。確認可能な証拠は、ＩＤ＆Ｖ処理を行うエンティティによってトークン・サービス・プロバイダ１１６に提供され、トークン・サービス・プロバイダ１１６が立証し得る、どのような値から成ってもよい。認定可能な証拠の例には、暗号文又はオーソリゼーション・コードが含まれてもよい。これらは、そのＩＤ＆Ｖが行われない状況を除き、すべてのＩＤ＆Ｖ方法に適用されてもよい。トークン・サービス・プロバイダ１１６は、行われたＩＤ＆Ｖ並びに、トークン要求元の登録時にトークン要求元１１４によって提供されたトークンの保管及び用法の情報に基づいて、トークン保証レベルを適切な値に設定してもよい。
【００７２】
本発明の様々な実施例によれば、トークン保証レベルは、行われたＩＤ＆Ｖ方法、ＩＤ＆Ｖを行うエンティティ、及び評価の結果を確証するトークン・サービス・プロバイダ１１６に応じて、無保証から高保証までの範囲にわたってもよい。例示的なＩＤ＆Ｖ方法には、（１）ＩＤ＆Ｖを行わない、（２）アカウント確認、（３）トークン・サービス・プロバイダのリスク・スコア、（４）トークン要求元データを使用したトークン・サービス・プロバイダのリスク・スコア、及び（５）イシュアによるアカウント名義人認証が含まれるが、これらに限定されない。前述のＩＤ＆Ｖ方法は単に説明の目的で提供されており、本発明の実施例によって追加のＩＤ＆Ｖ方法が定められ、行われてもよいことが、当業者には理解される。
【００７３】
（１）ＩＤ＆Ｖを行わない
トークン発行時にＩＤ＆Ｖ方法を行わずにトークンが発行される場合、トークン保証レベルは、「無保証」を示してもよい（例えば、トークン保証レベル値が「無保証」に設定されてもよい）。いくつかの実施例では、ＩＤ＆Ｖを行わない場合は、その結果、発行されたトークンに最も低いトークン保証レベルが割り当てられてもよい。それでも、トークンのユースケース及びトークン・サービス・プロバイダの規則に応じて、このトークンを使用して決済トランザクションが開始されてもよいが、トークン保証が伴わないか、又は低いトークン保証が伴ってもよい。本発明の実施例によって、無保証レベルのトークンの使用に追加の制限が実施されてもよい。
【００７４】
（２）アカウント確認
アカウント確認は、ＰＡＮが有効且つ妥当であるか認定するための基本アカウント認定チェックを行うＩＤ＆Ｖ保証方法を表してもよい。様々な実施例で、アカウント確認は、０ドル・オーソリゼーション、カード確認番号の認定、及び、郵便番号及び住所の確認を含む。このアカウント確認方法は、例えば、トークン要求元１１４によって行われ、トークン・サービスＡＰＩを介してトークン・サービス・プロバイダ１１６に報告されてもよい。このアカウント確認方法はまた、トークン発行時にトークン・サービス・プロバイダ１１６によって行われてもよい。トークン発行時にアカウント確認を行うことによってトークンが発行される場合、トークン保証レベルは「トークン要求元により確認済み」又は「トークン要求元により保証済み」を示してもよい（例えば、トークン保証レベルの値がそれらのレベルに設定されてもよい）。
【００７５】
（３）トークン・サービス・プロバイダによる保証
トークン・サービス・プロバイダによる保証は、トークン・サービス・プロバイダ１１６が、あるＰＡＮのトークン化を求める要求が十分な信頼レベルで保証される可能性についてリスクベースの評価を行うことを伴うＩＤ＆Ｖ保証方法のタイプである。トークン・

サービス・プロバイダ１１６は、トークン・サービス・プロバイダ１１６によって維持管理されているリスク及び認証のデータを使用して、このリスクベースの評価を行う。トークン・サービス・プロバイダ保証を使ってトークンが発行される場合、トークン保証レベルが「トークン・サービス・プロバイダにより保証済み」を示してもよい（例えば、トークン保証レベルの値がそのレベルに設定されてもよい）。いくつかの実施例では、トークン・サービス・プロバイダによる保証の結果、発行されるトークンに中程度のトークン保証レベルが割り当てられてもよい。

【００７６】

（４）要求元データを使用したトークン・サービス・プロバイダによる保証

要求元データを使用したトークン・サービス・プロバイダによる保証は、不正が予想されるトークン要求元１１４によって提供されたデータ要素の使用を伴うＩＤ＆Ｖ保証方法である。例えば、トークン要求元１１４が、他の情報の中でもとりわけ、名義人の年齢及び履歴、請求先／出荷先の住所及び連絡先情報、ＩＰアドレス、デバイスＩＤ及びデバイス情報、地理位置、並びにトランザクション速度を提供してもよい。トークン・サービス・プロバイダ１１６は、このＩＤ＆Ｖ方法を実装するために適切な評価技法及びツールを整備してもよく、また、ＰＡＮに関連するトークン・サービス・プロバイダのリスク及び認証のデータと結果のＩＤ＆Ｖデータを併用して割り当てられるトークン保証レベルを決定してもよい。トークン・サービス・プロバイダ保証を使ってトークンが発行される場合、トークン保証レベルは「トークン要求元データを使用してトークン・サービス・プロバイダにより保証済み」を示してもよい（例えば、トークン保証レベルの値がそのレベルに設定されてもよい）。いくつかの実施例では、トークン・サービス・プロバイダによる保証の結果、発行されるトークンに中程度のトークン保証レベルが割り当てられてもよい。

【００７７】

（５）イシュアによるアカウント名義人確認

イシュアによるアカウント名義人確認は、トークンとＰＡＮを完全に結びつけるために必要な保証を確実にするためのアカウント名義人確認のために、イシュア１０４又はイシュアのエージェントと対話することを伴うＩＤ＆Ｖ方法である。確認に使用される方法は、アカウント名義人が認証プロセス中に使用することのあるデバイスのタイプ（例えば、携帯電話、コンピュータなど）に基づいて、許容される程度のユーザ体験を提供するように実施されてもよい。いくつかの実施例では、デバイス・ガイドラインが作成され、それに従って一貫したユーザ体験が確保されてもよい。イシュア１０４が可能な限り最もインテリジェントな体験をアカウント名義人１０２に提供するために、イシュアによる認証は、トークン要求元１１４からの入力データ及びスコアを活用するように設計されてもよい。このデータを使用することにより、イシュア１０４は、プロセスに余分なステップを追加する必要なく、真正なオーソリゼーション済みのアカウント名義人１０２が実際にトークンを要求している（又は、真正なオーソリゼーション済みのアカウント名義人１０２についてトークンが要求されている）と確信することができる。アカウント名義人１０２から要求又は取得される入力データには、とりわけ、地理位置、デバイス情報、ＩＰアドレス、消費者情報（例えば、Ｅメール・アドレス、携帯電話番号、固定電話番号、確証済みの出荷先住所、消費者ＩＤ＆Ｖ、及び取引年数）、及びアカウント情報（例えば、ウォレット内の時間の長さ、及び／又は、アカウント活動の情報（例えば、「なし」、「最近」、「最近以外」などの））が含まれてもよい。イシュアによるアカウント名義人確認を使ってトークンが発行される場合、トークン保証レベルは「イシュアにより保証済み」を示してもよい（例えば、トークン保証レベルの値がそのレベルに設定されてもよい）。いくつかの実施例では、イシュアによるアカウント名義人確認の結果、発行されるトークンに高い、又は最も高いトークン保証レベルが割り当てられてもよい。

【００７８】

様々な実施例によれば、イシュアによるアカウント名義人確認は、３Ｄセキュア・アクセス制御サーバ（ＡＣＳ）、認証コードを使用したモバイルバンキングによるアカウント名義人確認を介して、連合ログイン・システムを介して、又は、トークン要求元からのデ

ータ及び共有秘密、ワンタイム・パスワード（ＯＴＰ）、アクティベーション・コード、若しくはその他のイシュア１０４とアカウント名義人１０２との間のその他の共有秘密の生成、配信、及び認定が可能なＡＰＩ機能を介して行われてもよい。イシュア１０４が、トークンを要求しているアカウント名義人１０２を明示的な確認方法（例えば、ＯＴＰ又はアクティベーション・コードを使用して）によって確認する必要があると判断した場合、共有秘密が帯域外チャネルでカード名義人１０２に配信されてもよい。

【００７９】

イシュア１０４は、アカウント名義人認証に複数の方法を使用してもよい。いくつかの実施例によれば、アカウント名義人の認証時、固定のパスワード及び認証サービスへの加入は、ＩＤ＆Ｖ方法に許可されなくてもよい。逆に、前述したように、イシュア１０４によるアカウント名義人認証にワンタイム・パスワードが使用されてもよい。ＯＴＰが使用される場合、イシュア１０４は、そのＯＴＰの長さが少なくとも６桁以上８桁以下であり、そのＯＴＰが統一された方法で生成されたものであり、好ましい配信方法がイシュア１０４からアカウント名義人１０２の消費者デバイスへのセキュアなチャネル（例えば、消費者デバイスにインストールされたモバイルバンキング・アプリケーション）であることを要求してもよい。

【００８０】

図１に戻ると、トークン及び関連するトークン保証レベルが生成されると、トークン・サービス・プロバイダ１１６は生成されたトークン、そのトークンによって表されるＰＡＮ、そのトークンに関連付けられたトークン保証レベル、及び、トークン保証レベルを生成するために使用されたデータ（例えば、行われたＩＤ＆Ｖのタイプ、ＩＤ＆Ｖの実行時に使用されたデータ、ＩＤ＆Ｖを行うエンティティなど）を、トークン保管庫１１８などのレポジトリに保管してもよい。

【００８１】

トークン保管庫１１８は、トークンの生成及び発行の能力を提供し、トークン－ＰＡＮ間のマッピングを確定及び維持管理し、トランザクション処理の間、基礎的なセキュリティ及びドメイン制限などの関連する処理規制を提供する。トークン保管庫１１８は、オーソリゼーション、精算、及び例外処理トランザクション処理などのトランザクション処理中にトークン－ＰＡＮ間マッピングを利用に供するための機構を提供してもよい。トークン保管庫１１８は、所与のＰＡＮにマッピングされたすべての関連トークンを、そのＰＡＮのライフサイクルを通して維持することが必要であってもよい。

【００８２】

トークン・サービス・プロバイダ１１６によって生成されたトークンは、トークン要求元１１４のトークン要求に応答してトークン要求元１１４に提供されてもよい。前述したように、トークン要求元１１４がトークン・サービス・プロバイダ１１６に登録されてもよい。登録時にトークン要求元１１４に割り当てられたトークン要求元ＩＤをトークン・サービス・プロバイダ１１６が認識すれば、トークン・サービス・プロバイダ１１６は生成されたトークンをトークン要求元１１４に提供してもよい。トークンの発行は、トークン要求元１１４へのトークンのプロビジョニングを伴ってもよい。トークンのプロビジョニングは、トークンが生成され、保証ステップが完了した後に行われてもよい。トークンのプロビジョニングは、トークン要求元１１４とトークン・サービス・プロバイダ１１６との間のインタフェースを通して行われてもよい。

【００８３】

トークン要求元１１４がアカウント名義人１０２である場合は、アカウント名義人１０２がトークンを受信したときに、そのトークンを決済オーソリゼーション要求メッセージ内で販売店１０６に提示してもよい。或いは、トークン要求元１１４が販売店１０６である場合は、トークン・サービス・プロバイダ１１６によって直接販売店１０６にトークンが提供されてもよい。販売店１０６は決済オーソリゼーション要求メッセージを生成してもよい。決済オーソリゼーション要求メッセージは、その決済オーソリゼーション要求メッセージに含まれるトークンによって表されるカード会員番号を使用した決済トランザク

ションの遂行を求めるものでもよい。販売店１０６は、トークンを含む決済オーソリゼーション要求メッセージをアクワイアラ１０８に送信して、さらなる処理を求めてもよい。

【００８４】

アクワイアラ１０８は、販売店１０６と取引関係を有するエンティティ（例えば銀行）のためのシステム（アクワイアラのコンピュータ又はサーバ）であってもよい。アクワイアラ１０８は、販売店１０６のための金融アカウントを発行及び管理してもよい。一般に、アクワイアラ１０８がトークン化エコシステム環境１００内で、オーソリゼーション、キャプチャ、精算、及び例外処理の責任を負ってもよい。アクワイアラ１０８は、販売店１０６及び決済処理ネットワーク１１０と通信可能に結合されていてもよい。アクワイアラのコンピュータ１０８は、トークンを含むオーソリゼーション要求メッセージを決済処理ネットワークのコンピュータ１１０を介してイシュアのコンピュータ１０４にルーティングするように構成されていてもよい。アクワイアラのコンピュータ１０８はまた、イシュアのコンピュータ１０４から受信したオーソリゼーション応答メッセージを、決済処理ネットワークのコンピュータ１１０を介して販売店のコンピュータ１０６にルーティングしてもよい。

【００８５】

決済ネットワーク１１０（決済処理ネットワークとも称する）は、イシュア１０４及びアクワイアラ１０８と通信可能に結合されていてもよい。決済ネットワーク１１０は、オーソリゼーションサービス並びに決済トランザクションの精算及び決算のサービスを提供するように構成されてもよい。決済ネットワーク１１０は、データ処理サブシステム及び、インターネットを含む有線又は無線ネットワークを含んでもよい。決済ネットワーク１１０はサーバ・コンピュータを含んでもよい。いくつかの実装例では、決済ネットワーク１１０は、アクワイアラ１０８から受信したオーソリゼーション要求メッセージを、通信チャネルを介してイシュア１０４に転送してもよい。アクワイアラ１０８から受信されるオーソリゼーション要求メッセージはトークンを含んでもよい。

【００８６】

決済ネットワーク１１０はトークン・サービス・プロバイダ１１６と通信して、そのトークンに関連付けられたトークン保証レベルを取得してもよい。トークン保証レベルは、決済トークンとその決済トークンによって表されるＰＡＮとの間の関係の信頼のレベルを表してもよい。トークン保証レベルは、トークンが生成されるときにトークン・サービス・プロバイダ１１６によって生成されてもよく、決済トークンと共にトークン保管庫１１８内に保管されてもよい。決済ネットワーク１１０は、アクワイアラ１０８から受信したオーソリゼーション要求メッセージを修正して、トークン保証レベル及びトークン保証レベルを生成するために使用されたデータ（例えば、行われたＩＤ＆Ｖのタイプ、ＩＤ＆Ｖの実行時に使用されたデータ、ＩＤ＆Ｖを行ったエンティティなど）を含むようにしてもよい。決済ネットワーク１１０はオーソリゼーション要求メッセージを修正して、オーソリゼーション要求メッセージに含まれるトークンによって表されるＰＡＮを含むようにしてもよい。決済ネットワーク１１０は次に、修正されたオーソリゼーション要求メッセージをイシュア１０４に転送してもよい。決済ネットワーク１１０はイシュアのコンピュータ１７０からオーソリゼーション応答メッセージを受信し、受信したオーソリゼーション応答メッセージをアクワイアラ１０８に転送してもよい。いくつかの実施例では、決済ネットワーク１１０はイシュア１０４から受信したオーソリゼーション応答メッセージを修正した後に、そのオーソリゼーション応答メッセージをアクワイアラ１０８に転送してもよい。例えば、決済ネットワーク１１０は、オーソリゼーション応答メッセージにＰＡＮが含まれる場合はオーソリゼーション応答メッセージを修正してＰＡＮを取り除くように（例えば、トークンでＰＡＮを置き換える）修正してもよいし、オーソリゼーション応答メッセージにＰＡＮの最後の４桁を含ませるようにしてもよい。

【００８７】

本発明の様々な実施例によれば、決済ネットワーク１１０はトークン・サービス・プロバイダ１１６として働いてもよい。決済ネットワーク１１０がトークン・サービス・プロ

バイダ１１６として働く例示的実施例について、図２を参照しながら下記に詳細に説明する。トークン・サービス・プロバイダ１１６として働く決済ネットワーク１１０は、自らが独占所有権を有するトークン要求元ＡＰＩ、トークン保管庫、トークン・プロビジョニング・プラットフォーム、及びトークン・レジストリの構築及び／又は管理の責任を負ってもよい。トークン・サービス・プロバイダ１１６ではない決済ネットワーク１１０は、トークンの相互運用性を確保するためのデトークン化の目的で、トークン・サービス・プロバイダ１１６とのメッセージの交換を可能にする処理機能の実装をサポートしてもよい。

【００８８】

図２は、本発明の例示的一実施例による、決済ネットワーク２１０がトークン・サービス・プロバイダ２１６として働くトークン化エコシステム環境２００内の様々なエンティティ相互作用の概要を示すシステム及びフローを示す図である。図２に示されるエンティティのうちいくつかは、図１に示されるエンティティと同じであるか類似する。それらのエンティティの詳細な説明は図１に関して前述されており、そのとおりであるので、下記では省略される。

【００８９】

図２に示されるように、アカウント名義人１０２が販売店１０６との決済トランザクションの遂行を希望してもよい。アカウント名義人１０２が、決済アカウント識別子（例えば、カード会員番号（ＰＡＮ））を使用してトランザクションを開始できてもよい。加えて、アカウント名義人１０２は消費者デバイスを利用して、モバイル・デバイスのスキャン（例えば、ＱＲ（登録商標）コード又はバーコードを使用）、モバイル・デバイスによる販売店のアクセスデバイスのタップ（例えば、近距離通信（ＮＦＣ）トランザクション又はその他の非接触／近接トランザクション）、電子商取引トランザクション（例えばオンライン・トランザクション）を開始するためのコンピュータ又はその他のモバイル・デバイス上でのクリックなどの適切な任意のトランザクション・チャネルを通して、又は、トランザクションを開始してトークンを販売店のコンピュータに渡すことのできる任意の他のチャネルを通して、トランザクションを開始することができてもよい。例えば、いくつかの実施例では、セキュア・エレメント、モバイル・デバイスの他のセキュアなメモリ、又はホスト・カード・エミュレーションなどを使用する「クラウド」にプロビジョニングされたトークンを使った遠隔トランクションがモバイル・デバイスを使用して開始されてもよい。

【００９０】

アカウント名義人１０２がアカウント番号を表すトークンを含む決済デバイスを所持している場合は、アカウント名義人１０２は、販売店１０６の決済端末で決済デバイスをスキャン又はタップすることによってトークンを販売店１０６に提示してもよい。アカウント名義人１０２がトークンを所持していない場合は、アカウント名義人１０２（例えば、アカウント名義人１０２の決済デバイス）は、トークン要求元１１４に連絡してトークンを要求してもよい。或いは、販売店１０６がトークン要求元１１４に連絡して（又は、トークン要求元１１４になって）、アカウント名義人１０２が開始又は要求したトランザクションのためのトークンを取得してもよい。

【００９１】

トークン要求元１１４はトークン・サービス・プロバイダ２１６（すなわち図２の決済ネットワーク２１０）に登録して、トークン・サービス・プロバイダ２１６によって提供されるトークン要求元識別子を受け取ってもよい。トークン・サービス・プロバイダ２１６は、トークン要求元１１４として指定されることを要求するエンティティを登録するプロセスを確立してもよい。いくつかの実施例では、複数のトークン・サービス・プロバイダへのトークン要求元１１４として認識されることを選択するエンティティは、各トークン・サービス・プロバイダによって確立された独占所有権付きのプロセスに従って、各トークン・サービス・プロバイダに個別に登録してもよい。トークン・サービス・プロバイダ２１６は、トークン要求元１１４から収集すべき情報を判断した後に、トークン要求元

１１４を登録してもよい。トークン・サービス・プロバイダ２１６はまた、受け取った情報の収集、検討、及び承認のために自らが独占所有権を有するプロセスを確立してもよい。トークン要求元１１４から収集される情報の非制限的な例には、顧客確認（ＫＹＣ：Ｋｎｏｗ　Ｙｏｕｒ　Ｃｕｓｔｏｍｅｒ）情報、及び、加入しようとするトークン要求元がサポートし得るトークン・ユースケースが含まれ、そのユースケースには、任意の適切なドメイン制限及びその他のトランザクション規制が含まれてもよく、その情報はトークン保管庫２１８内に実装されていてもよい。登録機能の結果はトークン要求元１１４の候補の登録出願に対する承認又は拒否決定である。トークン要求元１１４がトークン・サービス・プロバイダ２１６によって承認されると、固有のトークン要求元ＩＤがトークン要求元１１４に割り当てられる。

【００９２】

トークン要求元の登録は、あるエンティティをトークン要求元１１４として加入させ、承認し、登録することによってトークン・サービス・システム２１６の完全性を確保し得る機能である。トークン・サービス・プロバイダ２１６（すなわち図２の決済ネットワーク２１０）は、トークン要求元１１４に少なくとも固有のトークン要求元ＩＤを割り当ててもよく、トークン要求元１１４及び関連するトークン要求元ＩＤのライフサイクル管理の責任を負ってもよい。登録の一部として、決済ネットワーク２１０は、トークン要求元１１４に関連付けられた要求トークン保証レベル及びドメイン制限規制を取り込んでもよい。決済ネットワーク２１０は、トークン・トランザクション処理の間にその制限を適用するために、そのドメイン制限がトークン保管庫２１８から確実に利用可能になるようにしてもよい。

【００９３】

トークン・サービス・プロバイダ２１６として働く決済ネットワーク２１０によって割り当てられるトークン要求元ＩＤは固有のものでもよく、同じ決済ネットワーク２１０又は別のトークン・サービス・プロバイダから割り当てられる他のトークン要求元ＩＤと重複しない。トークン要求元ＩＤは、例示的な規約に基づいて決済ネットワーク２１０によって割り当てられる１１桁の数値を含んでもよく、その規約では、第１～３桁がトークンサービスプロバイダ・コードを含み、第４～１１桁がトークン・サービス・プロバイダによって各要求元エンティティ及びトークン・ドメインに割り当てられてもよい。各トークン・サービス・プロバイダにトークンサービスプロバイダ・コードが割り当てられ、そのサービス・プロバイダ又は、本発明の実施例の管理、開発、及び維持を提供するサービス・プロバイダの集合体によって維持されてもよい。トークン要求元ＩＤは基礎的な制御データ要素であり、本明細書で説明するトランザクションに存在してもよい。

【００９４】

トークン要求元１１４は要求されるトークンに関連付けられる設定選好又はトークン属性を指定してもよい。設定選好又はトークン属性は、例えば、トークン・タイプ（例えば、固定又は変動）、サポートされるトークン提示モード（例えば、スキャン、非接触、電子商取引など）、及びトークン要求メッセージ内のその他の任意の適切なトークン設定情報を含んでもよい。トークン要求元１１４は、トークン要求メッセージをトークン・サービス・プロバイダ２１６に送信してもよい。したがって、トークン要求メッセージは、トークン要求元ＩＤ、トークン属性、トークン・ドメイン制限規制、トークンによって表される（例えば置き換えられる）ＰＡＮ、及び、任意選択として要求トークン保証レベルを含んでもよい。

【００９５】

トークン・サービス・プロバイダ２１６としての決済ネットワーク２１０は、承認済みの各トークン要求元１１４に関連付けられる予想保証レベルを決定する責任を負う。実際のトークン保証レベルは、トークンの生成時にＩＤ＆Ｖプロセスのタイプ及び成果に基づいて決定されてもよい。実際のトークン保証レベルは、要求されたトークン保証レベルとは異なってもよい。

【００９６】

トークン要求元１１４が意図したとおりにトークンが確実に使用されるように、トークンの基礎用法を管理及び認定するための追加の規制が必要なことがある。規制はトークン・サービス・プロバイダ２１６としての決済ネットワーク２１０によって、ユースケース、並びにトークン要求元の登録プロセス中に特定された販売店識別子及びトークン提示モードなどのトークン・ドメインを含む条件に基づいて定められ、実装されてもよい。トークン・ドメイン規制は、トークンのデータ漏洩の結果、それに続いて起こる甚大なレベルの不正を確実に防ぐことを目的としてもよい。所与のトークン要求元１１４に許可されるトークン・ドメイン規制は、トークン要求元の登録時に指定され、トークン・サービス・プロバイダ２１６としての決済ネットワーク２１０によって承認されたトークン・ユースケースに部分的に影響されて決まる。ドメイン制限規制は、トークン保管庫２１８に保管されてもよい。

【００９７】

トークン要求元１１４に関連するトランザクションを制限するために指定される他の規制には、決済オーソリゼーション要求メッセージのＰＯＳ入力モード・データ・フィールドで伝えられるトークン提示モード値の用法が含まれてもよい。トークン提示モード値によって、トークン要求元の登録時に合意されたトークン提示モードにのみトークンの使用が制限されてもよい。例えば、トークン要求元１１４がカード・オン・ファイルのユースケースに登録している場合、決済ネットワーク２１０は、そのトークン要求元のＩＤによる使用及び電子商取引を示すトークン提示モード値に限定してトークンを発行し、電子商取引のトランザクションのみが決済ネットワーク２１０による処理を許可されるようにしてもよい。その他の実施例では、トークン提示モードがＮＦＣのＰＯＳ提示モードである場合は、非接触チップのＰＯＳ入力モード値にのみトークンの使用が制限されてもよい。

【００９８】

販売店１０６がトークン要求元１１４である実施例では、アクワイアラ識別データ要素及びトークン暗号文と組み合わせてカード受容者ＩＤなどの販売店関連データ要素を使用し、トランザクション処理メッセージ内のこれらのフィールドを、トークン要求元の登録時に確認された情報に従ってトークン保管庫２１８内に制定された規制により比較又は認定することによって、トークンの使用が制限されてもよい。例示的実施例には、カード・オン・ファイル販売店が保持するＰＡＮのトークン化が含まれてもよい。

【００９９】

トークン要求元１１４からトークン要求メッセージを受信すると、決済ネットワーク２１０は、そのトークン要求メッセージで提供されたＰＡＮのためのトークンを生成してもよい。決済ネットワーク２１０は、トランザクションを遂行する人物が正当なアカウント名義人であるか確証するために、行われたＩＤ＆Ｖのタイプについて問い合わせてもよい。行われたＩＤ＆Ｖのタイプ及びＩＤ＆Ｖを行ったエンティティについての情報に基づいて、決済ネットワーク２１０は、生成されるトークンに関連付けられるトークン保証レベルもまた生成してもよい。トークン保証レベルは、生成される決済トークンとその決済トークンによって表されるＰＡＮとの間の関係の信頼のレベルを表してもよい。決済ネットワーク２１０は、ＰＡＮと生成されたトークンとの間の関連付けを、トークン保証レベル及びトークン保証レベルを生成するために使用されたデータと共にボールト２１８に保管してもよい。決済ネットワーク２１０は、トークンをトークン要求応答メッセージでトークン要求元１１４に提供してもよい。

【０１００】

トークン要求元１１４は販売店１０６にトークンを提示してもよく、販売店１０６が、そのトークンを含む決済オーソリゼーション要求メッセージを生成してもよい。販売店１０６は決済オーソリゼーション要求メッセージをアクワイアラ１０８に送信してもよく、次にアクワイアラ１０８が、その決済オーソリゼーション要求メッセージを決済ネットワーク２１０に渡してもよい。トークン要求元ＩＤもまた販売店１０６に渡される場合は、決済オーソリゼーション要求メッセージ内のトークン要求元ＩＤがトークン保管庫２１８内のトークンに関連付けられたトークン要求元ＩＤと一致しないとき、又はトークン暗号

文の認定に失敗したときには、そのトランザクションは正常に処理を行うことを許可されなくてもよい。

【０１０１】

決済オーソリゼーション要求メッセージを受信すると、決済ネットワーク２１０は、トークン保管庫２１８及び／又は他のネットワーク・サーバ（複数可）２２０と対話して、決済オーソリゼーション要求メッセージで提供されたトークンをデトークン化してもよい。具体的には、決済ネットワーク２１０は、デトークン化プロセスの結果として、そのトークンによって表されるＰＡＮを取り込んでもよい。決済ネットワーク２１０は次に、決済オーソリゼーション要求メッセージを修正して、トークンと共に（又はトークンの代わりに）ＰＡＮ、並びに、トークン保証レベル及びトークン保証レベルの生成に使用されたデータを含むようにしてもよい。決済ネットワーク２１０は修正された決済オーソリゼーション要求メッセージをイシュア１０４に送信してもよい。

【０１０２】

イシュア１０４は、決済オーソリゼーション要求メッセージ内のＰＡＮ、ＰＡＮを表すトークン、トークン保証レベル及びトークン保証レベルの生成に使用されたデータを受信すると、アカウントレベル認定及びオーソリゼーション・チェックを行ってもよい。イシュア１０４は決済オーソリゼーション応答メッセージを、決済トランザクションの承認又は拒否を行う決済ネットワーク２１０に送信してもよい。決済オーソリゼーション応答メッセージは、他のデータの中でもとりわけ、ＰＡＮ、トークン、トークン要求元情報又はトークン要求元ＩＤ、トークン・ドメイン制限規制、トークン保証レベル及びトークン保証レベルの生成に使用されたデータを含んでもよい。決済ネットワーク２１０は、決済オーソリゼーション応答メッセージを修正してＰＡＮをトークンに置き換えてもよい。いくつかの実施例では、決済ネットワーク２１０は決済オーソリゼーション応答メッセージにトークン保証レベルを含めてもよいが、トークン保証レベルの作成に使用されたデータを削除してもよい。決済オーソリゼーション要求メッセージ及び決済オーソリゼーション応答メッセージの内容については、下記に例示的ユースケースと共に詳細に説明する。決済ネットワーク２１０は修正済みの決済オーソリゼーション応答メッセージを、アクワイアラ１０８を介して販売店１０６に送信してもよい。販売店１０６は、オーソリゼーション応答メッセージに基づいて、アカウント名義人１０２とのトランザクションを完結してもよい。

【０１０３】

ＩＩ．例示的ユースケース

ここでは、図３～図８に示される例示的ユースケースのためのトークン・トランザクションの説明及び図を提供する。本発明の実施例に定められる例示的ユースケースには、店頭でのモバイル近距離通信（ＮＦＣ）（図３）、モバイル／デジタル・ウォレット電子商取引（図４）、カード・オン・ファイル電子商取引（図５）、店頭でのスキャン（図６）、精算及びキャプチャ処理（図７）、及び例外処理（図８）が含まれる。したがって、図３～図８は、認証、キャプチャ、精算、及び例外処理のトランザクション内に存在するデータ要素のうちのいくつかを、ユースケース及びそのデータ要素に応じて特定する。

【０１０４】

本発明の実施例に基づくトークン・サービスの実施には、図３～図８に示されるとおりに、メッセージのデータ・フィールドでトークン関連データを渡すことが含まれてもよい。図３～図８に示される例示的実施例では、決済ネットワークがトークン・サービス・プロバイダとして働く。ただし、本発明は図３～図８に示される例示的実施例に限定されない。例えば、前述したように、トークン化エコシステム環境内の他のエンティティがトークン・サービス・プロバイダとして働いてもよい。決済ネットワークがトークン・サービス・プロバイダとして働く場合、実施例は、トランザクション処理の間、決済ネットワークがトークンをＰＡＮにマッピングするためにトークン・トランザクションを確実に認知できるようにする。

【０１０５】

ユースケース１：店頭でのモバイルＮＦＣ
図３を参照すると、店頭でのモバイルＮＦＣのユースケース３００で、ＮＦＣ対応型モバイル・デバイス３０２を使用して販売店端末３０２で非接触決済が開始される。モバイル・デバイス３０２には、モバイル・デバイス３０２のセキュア・エレメントなどのセキュアなメモリ内に保管されたトークンがプロビジョニングされていてもよい。様々な実施例によれば、トークンのプロビジョニングは、前述したように、トークン・サービス・プロバイダと連絡するトークン要求元によって行われてもよい。
【０１０６】
トランザクションが開始されると、モバイル・デバイス３０２は、トークン、トークン有効期限、トークン暗号文、及びその他のチップ・データ要素を含む非接触トランザクション３０６を生成してもよい。これらのデータ要素は、図３に示されるように、非接触トランザクション３０６の専用データ・フィールドに含まれてもよい。様々な実施例によれば、モバイル・デバイス３０２はトークン・データ要素を販売店端末３０４に次のように渡してもよい。ＰＡＮデータ・フィールドＦ２でトークンが渡され、ＰＡＮ有効期限データ・フィールドＦ１４でＰＡＮ有効期限が渡され、トークン・データ要素に基づいてトークン暗号文が生成されてチップ暗号文データ・フィールドＦ５５で渡され、トークン提示モードがデータ・フィールドＦ２２で非接触トランザクションのためのＰＯＳ入力モードと設定され、その他のすべての非接触データ要素が生成されて後続の典型的な非接触通信に従って渡されてもよい。モバイル・デバイス３０２から生成されるトークン暗号文はドメイン制限規制フィールドとして働いてもよく、それをトークン・サービス・プロバイダが使用して、そのトークンを使用するトランザクションの完全性を認定してもよい。
【０１０７】
モバイル・デバイス３０２は、上記のデータ・フィールドを含む非接触トランザクション３０６を、ＮＦＣインタフェースを介して販売店ＰＯＳ端末３０４に渡してもよい。販売店端末３０４は、オーソリゼーション要求メッセージ３１０をアクワイアラ３０８に送信してもよい。販売店端末３０４がアクワイアラ３０８に送信するオーソリゼーション要求メッセージ３１０は、モバイル・デバイス３０２が販売店端末３０４に送信する非接触トランザクション３０６と同じデータ要素を含んでもよい。
【０１０８】
オーソリゼーション要求メッセージ３１０を受信すると、アクワイアラ３０８はチェックの処理を行って、トークン・サービス・プロバイダとして働く決済ネットワーク３１２にトークン・データ・フィールド及び非接触データを渡してもよい。アクワイアラ３０８が決済ネットワーク３１２に送信するオーソリゼーション要求メッセージ３１４は、オーソリゼーション要求メッセージ３１０及び非接触トランザクション３０６と同じデータ要素を含んでもよい。
【０１０９】
トークン・サービス・プロバイダとして働く決済ネットワーク３１２がトークン・トランザクションを処理してもよい。処理は、トークン保管庫３１３と連絡（又は対話）して、受け取ったトークンによって表されるＰＡＮを取り込むことを含んでもよい。決済ネットワーク３１２は、トークン保管庫３１３内のトークン－ＰＡＮ間マッピングの状態を確認して、そのトークンが有効状態にあるか確かめてもよい。決済ネットワーク３１２はオーソリゼーション要求メッセージ３１４で受け取ったトークン暗号文を認定してもよい。決済ネットワーク３１２はまた、受け取ったトークンに対してトークン保管庫３１３に保管されたドメイン制限規制を認定してもよい。決済ネットワーク３１２は、トークン保管庫３１３から、受け取ったトークンに関連付けられたトークン保証レベル及びトークン保証レベルの生成に使用されたデータを取り込んでもよい。決済ネットワーク３１２は次に、オーソリゼーション要求メッセージ３１４を修正して、修正されたオーソリゼーション要求メッセージ３１８を生成してもよい。修正されたオーソリゼーション要求メッセージでは、データ・フィールドＦ２でトークンがＰＡＮに置き換えられてもよく、データ・フィールドＦ１４でトークン有効期限がＰＡＮ有効期限に置き換えられてもよく、データ・

フィールドＦ２２でＰＯＳ入力モードが渡されてもよく、そのトークンのトークン・サービス・プロバイダによって認定の代行が完了したことをイシュアに伝えるための指示子がデータ・フィールドＦ６０．６に含まれてもよく、データ・フィールドＦ６２．２３でプロダクトＩＤが渡されてもよく、また、様々なトークン関連フィールドが含まれてもよい。例えば、トークン関連フィールドは、データ・フィールドＦ１２３－ＤＳＩ６８タグ１で渡されるトークン、トークン有効期限、データ・フィールドＦ１２３－ＤＳＩ６８タグ２で渡されるトークン保証レベル、トークン保証データ、及び、データ・フィールドＦ１２３－ＤＳＩ６８タグ３で渡されるトークン要求元ＩＤを含んでもよい。修正されたオーソリゼーション要求メッセージ３１８を生成すると、決済ネットワーク３１２は修正されたオーソリゼーション要求メッセージ３１８をイシュア３１６に送信してもよい。

【０１１０】

本明細書に示されるデータ・フィールドは説明のみを目的とし、制限を課すものと解釈されてはならない。同じ又は類似の情報が異なるデータ・フィールドで伝達されてもよい。例えば、トークン要求元ＩＤがデータ要素４８のサブ要素３３サブフィールド６で渡され、プロダクト・コードがデータ要素４８のサブ要素３３サブフィールド４で渡され、トークン保証レベルがデータ要素４８のサブ要素３３サブフィールド５で渡されてもよい。本明細書で説明される、情報を渡すために使用されるこれら及び他の任意のデータ・フィールドは本発明の範囲に含まれる。

【０１１１】

イシュア３１６は修正されたオーソリゼーション要求メッセージ３１８で提供される情報を使用して、アカウントレベル認定及びオーソリゼーション・チェックを完了してもよい。イシュアは、決済ネットワーク３１２にオーソリゼーション応答メッセージ３１９を送信してもよい。例えば、イシュア３１６はトークン情報を、オーソリゼーション応答メッセージ３１９の既定のデータ・フィールドで決済ネットワーク３１２に渡してもよい。イシュア３１６は、データ・フィールドＦ２でＰＡＮ、データ・フィールドＦ６２．２３でプロダクトＩＤ、データ・フィールドＦ１２３－ＤＳＩ６８タグ１でトークンを渡してもよい。

【０１１２】

オーソリゼーション応答メッセージ３１９をイシュア３１６から受信すると、決済ネットワーク３１２は、マッピングに基づいてＰＡＮをトークンに置き換えることによってオーソリゼーション応答メッセージ３１９を修正してもよい。決済ネットワーク３１２は、データ・フィールドＦ２内のトークン、データ・フィールドＦ１２３－ＤＳＩ６８タグ２内のトークン保証レベル、データ・フィールドＦ４４．１５内のＰＡＮの下４桁、データ・フィールド６２．２３内のＰＡＮプロダクトＩＤのうち１つ又は複数などのデータ要素を含む、修正されたオーソリゼーション応答メッセージ３２０を生成してもよい。決済ネットワーク３１２は修正されたオーソリゼーション応答メッセージ３２０をアクワイアラ３０８に送信してもよい。アクワイアラ３０８は次に、販売店端末３０４にオーソリゼーション応答メッセージ３２２を渡してもよい。オーソリゼーション応答メッセージ３２２は、修正されたオーソリゼーション応答メッセージ３２０と同じデータ・フィールドを含んでもよい。

【０１１３】

オーソリゼーション応答メッセージ３１９並びに修正されたオーソリゼーション応答メッセージ３２０及び３２２は、モバイル・デバイス３０２を使用してアカウント名義人によって開始されたトランザクションをイシュア３１６が承認したか否かを示してもよい。オーソリゼーション応答メッセージ３２２が販売店端末３０４に提供された後、トランザクションの成功又は失敗がアカウント名義人に通知されてもよい。

【０１１４】

ユースケース２：モバイル／デジタル・ウォレット電子商取引

図４を参照すると、モバイル／デジタル・ウォレット電子商取引のユースケース４００で、アカウント名義人４０２がモバイル／デジタル・ウォレットを使用して決済トランザ

クションを開始し、電子商取引サイトの販売店オーナー４０４に決済及びその他の情報を伝送する。モバイル／デジタル・ウォレットは、イシュア４１６、決済ネットワーク４１２又は、その他の第３者によって操作されてもよい。様々な実施例によれば、デジタル・ウォレットの操作者はトークン要求元であってもよい。

【０１１５】

図４で、ウォレット操作者は、セキュリティ又はその他の理由のためにＰＡＮをウォレット・プラットフォーム内に保管しておく必要がないように、既にトークン化を提供されていてもよい。使用中のウォレットを運用する電子商取引販売店４０４でアカウント名義人４０２が決済トランザクションを開始すると、ウォレットが、ＰＡＮの代わりのトークン及びその他の注文情報（例えば、出荷先住所）含む決済トランザクションメッセージ４０６を、ウォレットＡＰＩを介して販売店４０４に渡してもよい。

【０１１６】

トランザクションが開始されると、アカウント名義人４０２のモバイル・デバイス内の販売店アプリケーション／デジタル・ウォレットが決済アプリケーションと対話して、データ要素を決済トランザクション要求メッセージ４０６で販売店４０４に渡してもよい。決済トランザクション要求メッセージ４０６はメッセージのＰＡＮフィールドでトークンを渡し、メッセージのＰＡＮ有効期限データ・フィールドでトークン有効期限を渡してもよく、任意選択としてトークン・データ要素に基づいてトークン暗号文が生成されてメッセージのトークン暗号文フィールドで渡されてもよく、トークン提示モードがメッセージのＰＯＳ入力モード（電子商取引トランザクションとして）フィールドで渡されてもよい。決済トランザクション要求メッセージ４０６はまた、メッセージの任意選択フィールドにトークン要求元ＩＤを他のデータ要素と併せて含んでもよい。いくつかの実施例では、決済トランザクション要求メッセージ４０６は、図３に示される非接触トランザクション３０６と同じデータ・フィールドを含んでもよい。

【０１１７】

販売店端末４０４は、トークン・データ・フィールドを伝えるオーソリゼーション要求メッセージ４１０を生成してアクワイアラ４０８に送信してもよい。販売店端末４０４によってアクワイアラ４０８に送信されるオーソリゼーション要求メッセージ４１０は、決済トランザクション要求メッセージ４０６と同じデータ要素を含んでもよい。具体的には、オーソリゼーション要求メッセージ４１０は、ＰＡＮフィールドにトークン、ＰＡＮ有効期限フィールドにトークン有効期限、チップ暗号文フィールドにトークン暗号文、任意選択データ・フィールドにトークン要求元ＩＤを含んでもよく、トークン提示モードが電子商取引トランザクションのＰＯＳ入力モードに設定されてもよい。

【０１１８】

オーソリゼーション要求メッセージ４１０を受信すると、アクワイアラ４０８はチェックの処理を行って、トークン・サービス・プロバイダとして働く決済ネットワーク４１２にトークン・データ・フィールドを渡してもよい。アクワイアラ４０８が決済ネットワーク４１２に送信するオーソリゼーション要求メッセージ４１４は、オーソリゼーション要求メッセージ４１０と同じデータ要素を含んでもよい。

【０１１９】

トークン・サービス・プロバイダとして働く決済ネットワーク４１２がトランザクションを処理してもよい。処理は、トークン保管庫４１３と連絡（又は対話）して、受け取ったトークンによって表されるＰＡＮを取り込むことを含んでもよい。決済ネットワーク４１２は、トークン保管庫４１３内のトークン－ＰＡＮ間マッピングの状態を確認して、そのトークンが有効状態にあるか確かめてもよい。決済ネットワーク４１２はオーソリゼーション要求メッセージ４１４で暗号文を受け取った場合、そのトークン暗号文を認定してもよい。決済ネットワーク４１２はまた、受け取ったトークンに対してトークン保管庫４１３に保管されたドメイン制限規制を認定してもよい。決済ネットワーク４１２は、トークン保管庫４１３から、受け取ったトークンに関連付けられたトークン保証レベル及びトークン保証レベルの生成に使用されたデータを取り込んでもよい。決済ネットワーク４１

２は次に、オーソリゼーション要求メッセージ４１４を修正して、修正されたオーソリゼーション要求メッセージ４１８を生成してもよい。修正されたオーソリゼーション要求メッセージでは、トークンがＰＡＮに置き換えられてもよく、トークン有効期限がＰＡＮ有効期限に置き換えられてもよく、そのトークンのトークン・サービス・プロバイダによって認定の代行が完了したことをイシュアに伝えるための指示子が追加されてもよく、また、トークン関連の複数のフィールドがオーソリゼーション要求メッセージで渡されてもよい。トークン関連フィールドは、トークン、トークン有効期限、トークン保証レベル、トークン保証データ、及び、トークン要求元ＩＤを含んでもよい。修正されたオーソリゼーション要求メッセージ４１８を生成すると、決済ネットワーク４１２は修正されたオーソリゼーション要求メッセージ４１８をイシュア４１６に送信してもよい。

【０１２０】

イシュア４１６は修正されたオーソリゼーション要求メッセージ４１８で提供される情報を使用して、アカウントレベル認定及びオーソリゼーション・チェックを完了してもよい。イシュアは、決済ネットワーク４１２にオーソリゼーション応答メッセージ４１９を送信してもよい。オーソリゼーション応答メッセージ４１９をイシュア４１６から受信すると、決済ネットワーク４１２は、マッピングに基づいてＰＡＮをトークンに置き換えることによってオーソリゼーション応答メッセージ４１９を修正してもよい。決済ネットワーク４１２は、トークン、トークン保証レベル、ＰＡＮの下４桁、及びＰＡＮプロダクトＩＤなどのうち１つ又は複数などのデータ要素を含む、修正されたオーソリゼーション応答メッセージ４２０を生成してもよい。決済ネットワーク４１２は修正されたオーソリゼーション応答メッセージ４２０をアクワイアラ４０８に送信してもよい。アクワイアラは次に、販売店端末４０４にオーソリゼーション応答メッセージ４２２を渡してもよい。オーソリゼーション応答メッセージ４２２は、修正されたオーソリゼーション応答メッセージ４２０と同じデータ・フィールドを含んでもよい。

【０１２１】

オーソリゼーション応答メッセージ４１９並びに修正されたオーソリゼーション応答メッセージ４２０及び４２２は、アカウント名義人４０２によって開始されたトランザクションをイシュア４１６が承認したか否かを示してもよい。オーソリゼーション要求メッセージ４２２が販売店端末４０４に提供された後、トランザクションの成功又は失敗がアカウント名義人に通知されてもよい。

【０１２２】

ユースケース３：カード・オン・ファイル電子商取引

図５を参照すると、カード・オン・ファイル電子商取引のユースケース５００が示されている。図５で、データベースに既に保管されている決済アカウントデータ（例えば、ＰＡＮ及びＰＡＮ有効期限）を有する電子商取引販売店５０４が、ＰＡＮをトークンに置き換えることによって、データの保管に伴う根本的なセキュリティの露出を排除しようとしてもよい。したがって、カード・オン・ファイル電子商取引トランザクションに関連する実施例では、販売店５０４がトークン要求元であってもよい。トークンがカード・オン・ファイル販売店５０４に返されると、続いて処理されるすべての電子商取引トランザクションは、トークン化エコシステム環境内で渡されるトランザクションメッセージ内にそのトークン及びトークン有効期限を含んでもよい（ＰＡＮ及びＰＡＮ有効期限データ・フィールドで伝えられる）。

【０１２３】

決済トランザクションを開始するために、アカウント名義人５０２がカード・オン・ファイル販売店５０４にログインして、販売店ウェブサイトで電子商取引による購買を開始してもよい。販売店ウェブサイトは、決済トランザクション要求メッセージ内の専用フィールドで、トークン・データ要素を販売店プラットフォーム（例えば販売店サーバ５０４）に渡してもよい。様々な実施例によれば、販売店ウェブサイトは、次の形でトークン・データ要素を販売店サーバ５０４に渡してもよい。決済トランザクション要求メッセージのＰＡＮフィールドでトークンが渡されてもよく、メッセージのＰＡＮ有効期限フィール

ドでトークン有効期限が渡されてもよく、データ・フィールドで販売店識別子が渡されてもよく、トークン提示モードが電子商取引のＰＯＳ入力モードに設定されてもよく、メッセージの任意選択フィールドでトークン要求元ＩＤが渡されてもよく、任意選択のデータ要素であるトークン暗号文がトークン・データ・フィールドに基づいて生成され、メッセージの任意選択データ・フィールドで渡されてもよい。その他のすべての販売店識別子も生成され、決済トランザクション要求メッセージ内で渡されてもよい。様々な実施例によれば、トークン要求元ＩＤ及び関連する販売店識別子がドメイン制限規制フィールドとして働いて、トランザクションの完全性を認定するために使用されてもよい。

【０１２４】

販売店サーバ５０４は、トークン・データ・フィールドを伝えるオーソリゼーション要求メッセージ５１０を生成してアクワイアラ５０８に送信してもよい。したがって、販売店端末５０４によってアクワイアラ５０８に送信されるオーソリゼーション要求メッセージ５１０は、販売店ウェブサイトから販売店サーバ５０４に送信される決済トランザクション要求メッセージと同じデータ要素を含んでもよい。

【０１２５】

オーソリゼーション要求メッセージ５１０を受信すると、アクワイアラ５０８はチェックの処理を行って、トークン・サービス・プロバイダとして働く決済ネットワーク５１２にトークン・データ・フィールドを渡してもよい。アクワイアラ５０８が決済ネットワーク５１２に送信するオーソリゼーション要求メッセージ５１４は、オーソリゼーション要求メッセージ５１０と同じデータ要素を含んでもよい。

【０１２６】

トークン・サービス・プロバイダとして働く決済ネットワーク５１２がトークン・トランザクションを処理してもよい。処理は、トークン保管庫５１３と連絡（又は対話）して、受け取ったトークンによって表されるＰＡＮを取り込むことを含んでもよい。決済ネットワーク５１２は、トークン保管庫５１３内のトークン－ＰＡＮ間マッピングの状態を確認して、そのトークンが有効状態にあるか確かめてもよい。決済ネットワーク５１２はオーソリゼーション要求メッセージ５１４で受け取ったトークン暗号文を認定してもよい。決済ネットワーク５１２はまた、受け取ったトークンに対してトークン保管庫５１３に保管されたドメイン制限規制を認定してもよい。決済ネットワーク５１２は、トークン保管庫５１３から、受け取ったトークンに関連付けられたトークン保証レベル及びトークン保証レベルの生成に使用されたデータを取り込んでもよい。決済ネットワーク５１２は次に、オーソリゼーション要求メッセージ５１４を修正して、修正されたオーソリゼーション要求メッセージ５１８を生成してもよい。修正されたオーソリゼーション要求メッセージでは、トークンがＰＡＮに置き換えられてもよく、トークン有効期限がＰＡＮ有効期限に置き換えられてもよく、そのトークンのトークン・サービス・プロバイダによって認定の代行が完了したことをイシュアに伝えるための指示子が追加されてもよく、また、トークン関連の複数のフィールドがオーソリゼーション要求メッセージで渡されてもよい。トークン関連フィールドは、トークン、トークン有効期限、トークン保証レベル、トークン保証データ、及び、トークン要求元ＩＤを含んでもよい。修正されたオーソリゼーション要求メッセージ５１８を生成すると、決済ネットワーク５１２は修正されたオーソリゼーション要求メッセージ５１８をイシュア５１６に送信してもよい。

【０１２７】

イシュア５１６は修正されたオーソリゼーション要求メッセージ５１８で提供される情報を使用して、アカウントレベル認定及びオーソリゼーション・チェックを完了してもよい。イシュアは、決済ネットワーク５１２にオーソリゼーション応答メッセージ５１９を送信してもよい。オーソリゼーション応答メッセージ５１９をイシュア５１６から受信すると、決済ネットワーク５１２は、マッピングに基づいてＰＡＮをトークンに置き換えることによってオーソリゼーション応答メッセージ５１９を修正してもよい。決済ネットワーク５１２は、トークン、トークン保証レベル、ＰＡＮの下４桁、及びＰＡＮプロダクトＩＤのうち１つ又は複数などのデータ要素を含む、修正されたオーソリゼーション応答メ

ッセージ５２０を生成してもよい。決済ネットワーク５１２は修正されたオーソリゼーション応答メッセージ５２０をアクワイアラ５０８に送信してもよい。アクワイアラは次に、販売店端末５０４にオーソリゼーション応答メッセージ５２２を渡してもよい。オーソリゼーション応答メッセージ５２２は、修正されたオーソリゼーション応答メッセージ５２０と同じデータ・フィールドを含んでもよい。

【０１２８】

オーソリゼーション応答メッセージ５１９並びに修正されたオーソリゼーション応答メッセージ５２０及び５２２は、モバイル・デバイス５０２を使用してアカウント名義人によって開始されたトランザクションをイシュア５１６が承認したか否かを示してもよい。オーソリゼーション応答メッセージ５２２が販売店端末５０４に提供された後、トランザクションの成功又は失敗がアカウント名義人に通知されてもよい。

【０１２９】

ユースケース４：店頭でのスキャン

図６を参照すると、店頭でのモバイルＱＲＣ（クイック・レスポンス・コード）のユースケースが示されている。図６で、モバイル・デバイス６０２が販売店の店頭でＱＲＣリーダ６０４を使用してＱＲＣベースの決済を開始してもよい。いくつかの実施例では、モバイル・デバイス６０２内のアプリケーションが、決済が開始されるたびに安全な様式で変動ＱＲＣを生成してもよい。トランザクションが開始されると、モバイル・デバイス６０２は、トークン、トークン有効期限、及びトークン暗号文要素、並びにＱＲＣからのその他の任意のデータを含むトランザクション要求メッセージ６０６を生成し、そのトランザクション要求メッセージ６０６を販売店端末６０４に渡してもよい。

【０１３０】

トランザクションが開始されると、モバイル・デバイス６０２は、ＱＲＣ読み取り能力を有する販売店端末６０４と対話して、決済トランザクション要求メッセージ６０６で販売店端末６０４にデータ要素を渡してもよい。決済トランザクション要求メッセージ６０６は、メッセージのＰＡＮフィールドでトークンを伝え、メッセージのＰＡＮ有効期限フィールドでトークン有効期限、メッセージのデータ・フィールドでＱＲＣデータを伝えてもよく、任意選択としてトークン・データ要素に基づいてトークン暗号文が生成され、メッセージのトークン暗号文データ・フィールドで渡されてもよく、また、メッセージのＰＯＳ入力モードに（ＱＲＣベースのトランザクションとして）トークン提示モードが渡されてもよい。決済トランザクション要求メッセージ６０６はまた、メッセージの任意選択フィールドに、トークン要求元ＩＤをその他のデータ要素と共に含んでもよい。モバイル・デバイス６０２から任意選択としてトークン暗号文が生成され、そのトークンを使用するトランザクションの完全性を認定するためにトークン・サービス・プロバイダによって使用されてもよい。

【０１３１】

販売店端末６０４は、トークン・データ・フィールドを含むオーソリゼーション要求メッセージ６１０を生成してアクワイアラ６０８に送信してもよい。販売店端末６０４によってアクワイアラ６０８に送信されるオーソリゼーション要求メッセージ６１０は、決済トランザクション要求メッセージ６０６と同じデータ要素を含んでもよい。具体的には、オーソリゼーション要求メッセージ６１０は、ＰＡＮフィールドにトークン、ＰＡＮ有効期限フィールドにトークン有効期限、チップ暗号文フィールドにトークン暗号文、任意選択データ・フィールドにトークン要求元ＩＤを含んでもよく、トークン提示モードがＱＲＣベースのトランザクション及びＱＲＣデータのためのＰＯＳ入力モードに設定されてもよい。

【０１３２】

オーソリゼーション要求メッセージ６１０を受信すると、アクワイアラ６０８はチェックの処理を行い、トークン・サービス・プロバイダとして働く決済ネットワーク６１２にトークン・データ・フィールドを渡してもよい。アクワイアラ６０８が決済ネットワーク６１２に送信するオーソリゼーション要求メッセージ６１４は、オーソリゼーション要求

メッセージ６１０と同じデータ要素を含んでもよい。

【０１３３】

トークン・サービス・プロバイダとして働く決済ネットワーク６１２がトークン・トランザクションを処理してもよい。処理は、トークン保管庫６１３と連絡（又は対話）して、受け取ったトークンによって表されるＰＡＮを取り込むことを含んでもよい。決済ネットワーク６１２は、トークン保管庫６１３内のトークン－ＰＡＮ間マッピングの状態を確認して、そのトークンが有効状態にあるか確かめてもよい。決済ネットワーク６１２はオーソリゼーション要求メッセージ６１４でトークン暗号文が受け取られた場合は、そのトークン暗号文を認定してもよい。決済ネットワーク６１２はまた、受け取ったトークンに対してトークン保管庫６１３に保管されたドメイン制限規制を認定してもよい。決済ネットワーク６１２は、トークン保管庫６１３から、受け取ったトークンに関連付けられたトークン保証レベル及びトークン保証レベルの生成に使用されたデータを取り込んでもよい。決済ネットワーク６１２は次に、オーソリゼーション要求メッセージ６１４を修正して、修正されたオーソリゼーション要求メッセージ６１８を生成してもよい。修正されたオーソリゼーション・メッセージ６１８では、トークンがＰＡＮに置き換えられてもよく、トークン有効期限がＰＡＮ有効期限に置き換えられてもよく、そのトークンのトークン・サービス・プロバイダによって認定の代行が完了したことをイシュアに伝えるための指示子が追加されてもよく、また、トークン関連の複数のフィールドがオーソリゼーション要求メッセージで渡されてもよい。トークン関連フィールドは、トークン、トークン有効期限、トークン保証レベル、トークン保証データ、及び、トークン要求元ＩＤを含んでもよい。修正されたオーソリゼーション要求メッセージ６１８を生成すると、決済ネットワーク６１２は修正されたオーソリゼーション要求メッセージ６１８をイシュア６１６に送信してもよい。

【０１３４】

イシュア６１６は修正されたオーソリゼーション要求メッセージ６１８で提供される情報を使用して、アカウントレベル認定及びオーソリゼーション・チェックを完了してもよい。イシュアは、決済ネットワーク６１２にオーソリゼーション応答メッセージ６１９を送信してもよい。オーソリゼーション応答メッセージ６１９をイシュア６１６から受信すると、決済ネットワーク６１２は、マッピングに基づいてＰＡＮをトークンに置き換えることによってオーソリゼーション応答メッセージ６１９を修正してもよい。決済ネットワーク６１２は、トークン、トークン保証レベル、ＰＡＮの下４桁、及びＰＡＮプロダクトＩＤのうち１つ又は複数などのデータ要素を含む、修正されたオーソリゼーション応答メッセージ６２０を生成してもよい。決済ネットワーク６１２は修正されたオーソリゼーション応答メッセージ６２０をアクワイアラ６０８に送信してもよい。アクワイアラは次に、販売店端末６０４にオーソリゼーション応答メッセージ６２２を渡してもよい。オーソリゼーション応答メッセージ６２２は、修正されたオーソリゼーション応答メッセージ６２０と同じデータ・フィールドを含んでもよい。

【０１３５】

オーソリゼーション応答メッセージ６１９及び修正されたオーソリゼーション応答メッセージ６２０（及び６２２）は、アカウント名義人６０２によって開始されたトランザクションをイシュア６１６が承認したか否かを示してもよい。オーソリゼーション応答メッセージ６２２が販売店端末６０４に提供された後、トランザクションの成功又は失敗がアカウント名義人に通知されてもよい。

【０１３６】

キャプチャ及び精算のフロー

キャプチャ処理は、アカウント名義人から販売店への資金の移転を指してもよい。精算は、決済トランザクションの結果の資金の送信、照合、及び確証のプロセスを指してもよい。精算フローの間、精算メッセージがアクワイアラから決済ネットワークに渡されて、決済ネットワークからイシュアに渡されてもよい。本発明の実施例に定められる精算プロセスは、例えば決済ネットワークによって運用される精算システムによって実施されても

よい。

【０１３７】

図７は、あるトークン・トランザクションの例示的キャプチャ及び精算を示す。様々な実施例によれば、販売店７０２はトランザクションの開始時に消費者（例えばカード名義人）によって提供された情報に基づいてキャプチャファイル７０６を生成してもよい。キャプチャファイル７０６は、ＰＡＮデータ・フィールドＦ２にトークンを含み、ＰＡＮ有効期限データ・フィールドＦ１４にトークン有効期限を含んでもよい。販売店７０２は、キャプチャファイル７０６をアクワイアラ７０４に送信してもよい。

【０１３８】

アクワイアラ７０４は、キャプチャファイル４０６のデータ要素のチェックを処理してもよい。アクワイアラ７０４は、トークン・サービス・プロバイダとして働く決済ネットワーク７０８に渡される精算ファイル７１０を作成してもよい。精算ファイル７１０は、ＰＡＮフィールドＴＣＲ０にトークンを含み、ＰＡＮ有効期限データ・フィールドにトークン有効期限を含んでもよく、データ・フィールドＴＣＲ０でトークン提示モードがチャネル特定トランザクションのＰＯＳ入力モードに設定されてもよく、また、トークン・トランザクションに導入されてもよい新しいデータ・フィールドＴＣＲ１にトークン保証レベルを含んでもよい。いくつかの実施例では、精算ファイル７１０はまた、ファイルのデータ・フィールドＴＣＲ７に暗号文を含んでもよい。

【０１３９】

決済ネットワーク７０８が精算ファイル７１０を受信すると、決済ネットワーク７０８はトークン保管庫７１３と対話して、受け取ったトークンに対応するＰＡＮを取り込んでもよい。決済ネットワーク７０８は、トークン保管庫７１３内のトークン－ＰＡＮ間マッピングの状態を確認して、そのトークンが有効状態にあるか確かめてもよい。精算ファイル７１０に暗号文が含まれる場合は、決済ネットワーク７０８は、その暗号文を認定してもよい。決済ネットワーク７０８はまた、トークン保管庫７１３に保管されているドメイン制限規制を、受け取ったトークンに対して認定してもよい。

【０１４０】

決済ネットワーク７０８は次に、精算ファイル７１０を修正して、修正された精算ファイル７１４を生成してもよい。修正された精算ファイル７１４では、データ・フィールドＴＣＲ０でトークンがＰＡＮに置き換えられてもよく、そのトークンのトークン・サービス・プロバイダによって認定の代行が完了したことをイシュアに伝えるための指示子が追加されてもよく、また、トークン関連の複数のフィールドがオーソリゼーション要求メッセージで渡されてもよい。トークン関連フィールドは、データ・フィールドＴＣＲ５にトークン、データ・フィールドＴＣＲ１にトークン保証レベルを含んでもよい。いくつかの実施例では、修正された精算ファイル７１４のデータ・フィールドＴＣＲ７に暗号文が含まれてもよい。修正された精算ファイル７１４を生成すると、決済ネットワーク７０８は修正された精算ファイル７１４をイシュア７１２に送信してもよい。

【０１４１】

イシュア７１２は、修正された精算ファイル７１４で提供される情報を使用してアカウントレベル認定を完了し、精算プロセスを完了してもよい。

【０１４２】

例外フロー

例外処理は、チャージバック要求及び／又は、例えば、資金の不在若しくは顧客／決済／トランザクションの情報の不在に起因して処理することができなかった決済に関連してトークン化エコシステム環境内を流れるメッセージを指してもよい。いくつかの実施例では、例外処理はチャージバック処理を指し、チャージバック・メッセージがイシュアから決済ネットワークに流れ、決済ネットワークからアクワイアラに流れてもよい。

【０１４３】

図８は、チャージバック要求及びチャージバックデータ要素についての例示的トークン処理を示す。様々な実施例によれば、イシュア８０２は、元のトランザクションが妥当な

チャージバック要求であること及び、イシュア８０２が適切なチャージバック権を有することを認定した後に、チャージバックを申請してもよい。チャージバック・レコード・ファイル８０６がイシュア８０２によって生成され、決済ネットワーク８０４に送信されてもよい。チャージバック・レコード・ファイル８０６は、他のデータの中でもとりわけ、データ・フィールドＴＣＲ０にＰＡＮ（元の購買トランザクションで使用されたもの）、データ・フィールドＴＣＲ５にそのＰＡＮに対応するトークン、データ・フィールドにトークン保管庫８１３から取り込んだトークン保証レベルを含んでもよく、チャージバック・レコード・ファイル８０６の任意選択フィールドでトークン要求元ＩＤが渡されてもよい。

【０１４４】

決済ネットワーク８０４がチャージバック・レコード・ファイル８０６を受信すると、決済ネットワーク８０４はトークン保管庫８１３内のトークン－ＰＡＮ間マッピングの状態を確認して、そのトークンが有効状態にあるか確かめてもよい。イシュア８０２から送信されたチャージバック・レコード・ファイル８０３にトークンが含まれない場合は、決済ネットワーク８０４は、争点となっているトランザクションのトークンをトークン保管庫８１３から取り込んでもよい。決済ネットワーク８０４は次に、アクワイアラ８０８に送信される修正されたチャージバック・レコード・ファイル８１０を生成してもよい。修正されたチャージバック・レコード・ファイル８１０を生成するために決済ネットワーク８０４によって行われる修正は、ＰＡＮを対応するトークンで置き換えることを含んでもよく、任意選択として、修正されたチャージバック・レコード・ファイル８１０に、トークン要求元ＩＤ及びトークン保証レベルなどの１つ又は複数のトークン関連フィールドを含ませることを含んでもよい。

【０１４５】

修正されたチャージバック・レコード・ファイル８１０を受信すると、アクワイアラ８０８は、修正されたチャージバック・レコード・ファイル８１０に認定を行い、事例の調査に基づいて、別の紛争処理段階に移行するか、或いは、そのチャージバックを解決してもよい。

【０１４６】

ＩＩＩ．トークンサービスプロバイダ・アプリケーション・プログラム・インタフェース（ＡＰＩ）

図９は、トークンの発行及び処理（例えば、トークン・サービスの提供）を促進するための、トークン・サービス・プロバイダによるアプリケーションプログラムインタフェース（ＡＰＩ）の使用を示す。

【０１４７】

本発明の実施例は、トークンの要求、トークンの発行、ＩＤ＆Ｖの実行、デトークン化、トークンのルーティング、トークンのライフサイクル管理を促進するための、トークン化エコシステム環境９００内のトークン・サービス・プロバイダ９０４とその他のエンティティとの間の、１つ又は複数のＡＰＩ及び／又はメッセージング・インタフェースを通した対話について説明する。したがって、本発明の実施例は対話のための共通データ要素を制定し、トークン・サービス・プロバイダ９０４がそれをサポートしてもよい。いくつかの実施例によれば、本明細書に記載されるインタフェースは、トークン・サービス・プロバイダ９０４と対話するすべての関与エンティティによって利用されるために、トークン・サービス・プロバイダ９０４によって利用に供されてもよい。

【０１４８】

トークン・サービス・プロバイダ９０４は、トークン・サービス・プロバイダ９０４とのセキュアな対話の方法を通して認証されたエンティティとのインタフェース又はＡＰＩを確立及び使用する能力を提供してもよい。例えば、対話は、ウェブサービス、既存の決済ネットワークインタフェースを通したＩＳＯ８５８３メッセージ交換、及びファイル／バッチを含む認証済みの方法を介して行われてもよいが、これらの方法に限定されない。トークン化エコシステム環境９００内の、トークン要求元９０２、ＩＤ＆Ｖを行うエンテ

ィティ９０６、他のネットワーク９０８、決済ネットワーク９１０などの１つ又は複数のエンティティが、トークンサービスインタフェースを使用してもよい。

【０１４９】

インタフェースはトークン要求・発行インタフェース９１２、トークン保証（例えばＩＤ＆Ｖ）インタフェース９１４、デトークン化インタフェース９１６、トークン・ルーティング・インタフェース９１８、及びトークン・ライフサイクル管理インタフェースに分類されてもよい。定められた１つ又は複数のインタフェースによって、特定のトークン関連動作を行うためのメッセージ転送が可能になってもよい。

【０１５０】

トークン要求・発行インタフェース

前述したように、トークン・サービス・プロバイダ９０４は、登録されたトークン要求元９０２が使用して、元の決済信用情報を含むトークン要求メッセージをサブミットし、トークン・サービス・プロバイダ９０４からトークンを含むトークン応答メッセージを受信することのできるインタフェースを提供してもよい。トークン要求メッセージ及びトークン応答メッセージは、トークン要求元９０２とトークン・サービス・プロバイダ９０４との間でトークン要求・発行インタフェース９１２を通して渡されてもよい。

【０１５１】

トークン要求・発行インタフェース９１２は、要求されたＰＡＮに対するトークンの発行を求めるリアルタイム要求をサポートしてもよいし、又は、トークンがバルク量で生成及び発行され、トークン要求元９０２に返される場合は、セキュア・インタフェース・ファイルを通してイン・バルク要求をサポートしてもよい。トークン・サービス・プロバイダ９０４は、入力されたＰＡＮに基づいてトークンを生成するための適切な規制及びプロセスを実装してもよい。いくつかの実施例では、保証ステップは要求に基づいて行われてもよい。

【０１５２】

トークン要求メッセージ内の入力データ要素は、トークン要求元ＩＤ、ＰＡＮ、ＰＡＮ有効期限、及び要求保証レベルのうちの１つ又は複数を含んでもよい。任意選択のデータ要素は、請求先／出荷先住所及び郵便番号などの、トークン保証ＩＤ＆Ｖ方法を行うためのアカウント名義人データを含んでもよい。表１に、例示的トークン要求・発行インタフェース９１２を通して渡されるトークン要求メッセージの入力データ要素を示す。

【０１５３】

【表１】

フィールド名	長さ	フォーマット	説明
トークン要求元ＩＤ	11	数字	要求元に割り当てられる固有のＩＤ
ＰＡＮの長さ	1	バイナリ値	ＰＡＮフィールドの長さ
PAN	可変長 (13 桁～19 桁)	数字	トークンが要求されるＰＡＮ
ＰＡＮ有効期限	4	数字	トークンが要求されるＰＡＮの有効期限
要求保証レベル	2	数字	保証レベルが要求される場合に存在する
トークン保証レベル	2	数字	トークン要求元がＩＤ＆Ｖを行った場合に存在する
カード名義人データの長さ	2	バイナリ値	カード名義人データの長さは、存在しない場合は０でもよい
カード名義人データ	可変長	英数字	要求保証レベルをサポートするために必要なデータ。例として、請求先住所、出荷先住所、郵便番号、及びＣＶＶ２がある。

表１：トークン要求・発行インタフェースを通して渡される入力データ要素

【０１５４】

トークン要求メッセージに応答して、トークン要求・発行インタフェース９１２は１つ又は複数のデータ要素を含む応答メッセージを渡してもよく、これらのデータ要素は、要求の状態（例えば、要求が成功したか失敗したか）及び、要求が失敗した場合は失敗のタイプを示す理由コードを含むが、これらに限定されない。成功した要求に対しては、トークン及びトークン有効期限などの追加データ要素がトークン応答メッセージで返されてもよい。トークン発行時にトークン保証方法が行われた場合は、トークン要求・保証インタフェース９１２は任意選択として、割り当てられたトークン保証レベルをトークン要求元９０２に提供してもよい。表２に、例示的トークン要求・発行インタフェースを通して渡されるトークン応答メッセージの出力データ要素を示す。

【０１５５】

【表２】

フィールド名	長さ	フォーマット	説明
要求の状態	1	数字	要求の成功又は失敗を示す
理由コード	可変長	バイナリ値	要求の状態が「成功」ではない場合に存在する
トークン	可変長 (13 桁～19 桁)	数字	要求の状態が「成功」である場合に存在し、トークンがトークン・サービス・プロバイダによって生成される。
トークン有効期限	4	数字	要求の状態が「成功」である場合に存在し、トークン有効期限がトークン・サービス・プロバイダによって生成される。
トークン保証レベル	2	数字	要求の状態が「成功」であり、ＩＤ＆Ｖが要求された場合に存在する。

表２：トークン要求・発行インタフェースを通して渡される出力データ要素

【０１５６】

トークン保証（ＩＤ＆Ｖ）インタフェース

トークン保証（ＩＤ＆Ｖ）インタフェース９１４は、アカウント名義人情報及びＰＡＮを確認するためにトークンの発行時にＩＤ＆Ｖを行うことを求める要求を渡してもよい。トークン保証インタフェース９１４は、トークン・サービス・プロバイダ９０４とＩＤ＆Ｖを行うエンティティ９０６との間に提供されてもよい。いくつかの実施例では、トークン・サービス・プロバイダがＩＤ＆Ｖを行ってもよい。トークン・サービス・プロバイダ９０４がＩＤ＆Ｖのサポートを提供する場合は、トークン・サービス・プロバイダ９０４はＩＤ＆Ｖ方法をサポートするための１つ又は複数のインタフェースを実装してもよい。加えて、トークン・サービス・プロバイダ９０４は、要求トークン保証レベルに適したＩＤ＆Ｖ方法がトークンの発行時に確実に行われるようにしてもよい。表３に、例示的トークン保証（ＩＤ＆Ｖ）インタフェースを通して渡されるＩＤ＆Ｖ要求メッセージの入力データ要素を示す。

【０１５７】

【表３】

フィールド名	長さ	フォーマット	フィールドの説明
トランザクション・タイプ	2	数字	• NN – 購買 • NN – トークン発行 • NN – トークン再認定
カード名義人ＰＡＮ	可変長 (13 桁～19 桁)	数字	カード会員番号。トークンに紐付けられてもよい金融ＰＡＮ
カード有効期限	4	数字	金融ＰＡＮの有効期限
トークン要求元ＩＤ	11	数字	トークンを要求している登録済みエンティティに割り当てられた固有の値
要求保証レベル	2	数字	トークン要求元が実行を希望する認定のレベル、例えば無保証、トークン要求元認定済み、トークン要求元保証済み、トークン・サービス・プロバイダ保証済み、トークン要求元データを使用したトークン・サービス・プロバイダ保証済み、又はイシュア保証済みを示す
トークン所在場所	2	数字	トークンの保管場所を示す。０１－リモート／クラウド、０２－セキュア・エレメントなど。
プロトコル	2	数字	トークン要求元がカード名義人、モバイル・アプリケーションＡＰＩ及び／又はブラウザとの通信に使用するプロトコルを説明する。
アカウント確認結果	2	数字	アカウント確認が行われた場合に、その結果の「合格」又は「失格」を示す。
トークン要求元リスク評価	4	数字	トークン要求元から提供される不正リスク評価
住所相違の指示子	2	数字	出荷先と請求先の住所が異なる場合に記入される。
カード名義人請求先住所	可変長	英数字	住所（１行目）、住所（２行目）、市、州／郡、郵便番号、国コードなどのデータを含む。
デバイス情報	可変長	英数字	デバイス情報属性は信用情報に関する１組の属性から成る。これには、ＩＰアドレス、オペレーティングシステム、地理的位置、デバイスＩＤ及び、ラップトップ又は電話などのデバイス種別が含まれるが、これらに限定されない。
固定電話番号	16	数字	カード名義人によって提供された固定電話番号
携帯電話番号	16	数字	カード名義人によって提供された携帯電話番号
勤務先電話番号	16	数字	カード名義人によって提供された勤務先電話番号
アカウント情報	可変長	英数字	アカウント情報要素は決済アカウントに関する１組の属性から成り、Ｅメールアドレス、アカウントの使用年数、ファイル上のＰＡＮの数、及び平均トランザクション速度などがある。

表３：トークン保証（ＩＤ＆Ｖ）インタフェースを通して渡される入力データ要素

【０１５８】

ＩＤ＆Ｖ要求に応答して、トークン保証（ＩＤ＆Ｖ）インタフェース９１４は１つ又は複数のデータ要素を含む応答メッセージをトークン・サービス・プロバイダ９０４に渡してもよく、これらのデータ要素は、要求の状態（例えば、「成功」又は「失敗」）及び、ＩＤ＆Ｖに失敗した場合は失敗のタイプを示す理由コードを含むが、これらに限定されない。成功した要求に対しては、トークン保証（ＩＤ＆Ｖ）インタフェース９１４は、追加データ要素をＩＤ＆Ｖ応答メッセージで返してもよい。表４に、トークン保証（ＩＤ＆Ｖ）インタフェース９１４を通して渡されるＩＤ＆Ｖ応答メッセージの例示的出力データ要素を示す。

【０１５９】

【表４】

フィールド名	長さ	フォーマット	フィールドの説明
カード名義人ＰＡＮ	可変長 (13 桁～19 桁)	数字	カード会員番号。トークンに紐付けられてもよい金融ＰＡＮ
割り当てられた保証レベル	2	英数字	トークン要求元が希望する認定のレベルであり、ネットワークにより異なることがあることを示す。
確認値	可変長	英数字	確認値は認証を行うイシュア又はエンティティによって導出される。
確認アルゴリズム	可変長	英数字	確認値を生成するために使用されたアルゴリズムを示す。

表４：トークン保証（ＩＤ＆Ｖ）インタフェースによって渡される出力データ要素

【０１６０】

デトークン化インタフェース

デトークン化インタフェース９１６は、発行されたトークンを交換するために必要な機構を、認証済みのエンティティに元のＰＡＮ及びＰＡＮ有効期限の信用情報を返すことによって提供してもよい。トークン・サービス・プロバイダ９０４は、デトークン化処理のために他のネットワーク９０８と（デトークン化インタフェース９１６を介して）連絡してもよい。トークン・サービス・プロバイダ９０４は、デトークン化インタフェース９１６へのアクセスを可能にするために適切なセキュリティ規制を実装してもよい。トークン・サービス・プロバイダ９０４は、要求が認識及び認証済みのソースから確実に受け取られるようにしてもよい。いくつかの実施例では、トークン・サービス・プロバイダ９０４は決済ネットワークであってもよく、デトークン化は決済ネットワークによって処理されてもよい。表５に、デトークン化インタフェース９１６を通して渡されるデトークン化要求メッセージの例示的入力データ要素を示す。

【０１６１】

【表５】

フィールド名	長さ	フォーマット	説明
トークン要求元ＩＤ	11	数字	要求元に割り当てられた固有ＩＤ
トークン長	1	英数字	トークンの長さ
トークン	可変長 (13 桁～19 桁)	英数字	発行されたトークン
トークン有効期限	4	数字	発行されたトークンの有効期限

表５：デトークン化インタフェースを通して渡される入力データ要素

【０１６２】
デトークン化インタフェース９１６は、要求の状態（例えば、「成功」又は「失敗」）及び、ＩＤ＆Ｖに失敗した場合は失敗のタイプを示す理由コードなどの出力データ要素を含むデトークン化応答メッセージを渡してもよい。成功した要求に対しては、ＰＡＮ及びＰＡＮ有効期限がデトークン化応答メッセージで返されてもよい。表６に、デトークン化インタフェース９１６を通して渡されるデトークン化応答メッセージの例示的出力データ要素を示す。

【０１６３】
【表６】

フィールド名	長さ	フォーマット	説明
要求の状態	1	バイナリ値	要求の成功又は失敗を示す
理由コード	可変長	バイナリ値	要求の状態が「成功」ではない場合に存在する
ＰＡＮ長	1	バイナリ値	要求の状態が「成功」の場合に存在し、ＰＡＮフィールドの長さを示す
PAN	可変長 (13 桁～19 桁)	数字	要求の状態が「成功」の場合に存在し、ＰＡＮが記入される
ＰＡＮ有効期限	4	数字	要求の状態が「成功」の場合に存在し、ＰＡＮ有効期限が記入される

表６：デトークン化インタフェースを通して渡される出力データ要素

【０１６４】
トークン・ルーティング・インタフェース
トークン・ルーティング・インタフェース９１８は、あるトークン・トランザクションを、そのトランザクションを処理する責任を負う決済ネットワーク９１０にルーティングするために必要な機構を提供してもよい。決済ネットワークがトークン・サービス・プロバイダとして働く場合などの、いくつかの実施例では、ルーティングは、デトークン化のためのトークンをルーティングするデトークン化ルーティングもまた含んでもよい。表７に、トークン・ルーティング・インタフェース９１８を通して渡されるトークン処理メッセージの例示的入力データ要素を示す。

【０１６５】

【表７】

フィールド名	長さ	フォーマット	説明
トークン要求元ＩＤ	11	数字	要求元に割り当てられた固有ＩＤ
トークン長	1	バイナリ値	トークンの長さ
トークン	可変長 (13 桁～19 桁)	数字	発行されたトークン
トークン有効期限	4	数字	発行されたトークンの有効期限
トランザクション・データ要素の長さ	可変長	バイナリ値	その他のトランザクション・データ要素フィールドの長さは、存在しない場合は０でもよい
トランザクション・データ要素	可変長	実施例によって異なる	トークン・サービス・プロバイダが要求を行うための、その他のトランザクション・データ要素が必要に応じて記入される。内容は、トークン・サービス・プロバイダが所有権を有する。

表７：トークン・ルーティング・インタフェースを通して渡される入力データ要素

【０１６６】

トークン・ルーティング・インタフェース９１８は、要求の状態（例えば、「成功」又は「失敗」）及び、ＩＤ＆Ｖに失敗した場合は失敗のタイプを示す理由コードなどの出力データ要素を含むトークン処理応答メッセージを渡してもよい。成功した要求に対しては、ＰＡＮ及びＰＡＮ有効期限がトークン処理応答メッセージで返されてもよい。表８に、トークン・ルーティング・インタフェース９１８を通して渡されるトークン処理応答メッセージの例示的出力データ要素を示す。

【０１６７】

【表８】

フィールド名	長さ	フォーマット	説明
要求の状態	1	バイナリ値	要求の成功又は失敗を示す
理由コード	可変長	バイナリ値	要求の状態が「成功」ではない場合に存在する
ＰＡＮ長	1	バイナリ値	要求の状態が「成功」の場合に存在し、ＰＡＮフィールドの長さを示す
PAN	可変長 (13 桁～19 桁)	数字	要求の状態が「成功」の場合に存在し、ＰＡＮが記入される
ＰＡＮ有効期限	4	数字	要求の状態が「成功」の場合に存在し、ＰＡＮ有効期限が記入される
トランザクション・データ要素の長さ	可変長	バイナリ値	その他のトランザクション・データ要素フィールドの長さは、存在しない場合は０でもよい
トランザクション・データ要素	可変長	実施例によって異なる	ネットワークがトランザクションを続行するための、その他のトランザクション・データ要素が必要に応じて記入される。内容は、トークン・サービス・プロバイダが所有権を有する。

表８：トークン・ルーティング・インタフェースを通して渡される出力データ要素

【０１６８】

トークン・ライフサイクル管理インタフェース

ＰＡＮ及びＰＡＮ有効期限に対する変更、並びにマッピングの無効化を引き起こすイベントに起因して、トークン要求元９０２によってトークンに継続的管理及び更新が行われてもよい。トークン・サービス・プロバイダ９０４は、発行されたトークンに影響する変更を管理するインタフェースを通してライフサイクル更新を提供してもよい。ライフサイクル・イベントは、トークンの紐付け解除インタフェース、トークン保留インタフェース、トークン有効化インタフェース、トークン保証更新インタフェース、及びＰＡＭ属性更新インタフェースなどのインタフェースを使用して処理されてもよい。表９に、トークン・サービス・プロバイダ９０４によって利用に供されてもよい例示的ライフサイクル・イベントを示す。

【０１６９】

【表９】

インタフェース	イベント／説明	要求元	行われる処置
トークンの紐付け解除	• デバイスの紛失又は盗難 • 元の信用情報の期限切れ • トークン要求元が既にカード・オン・ファイルを保持していない • ＰＡＮの紛失又は盗難 • ＰＡＮに対する不正警告 • ＰＡＮに対する故障報告	トークン要求元 カード・イシュア 決済ネットワーク	トークンとＰＡＮの紐付けが解除され、以降のマッピングの使用が不可能にされる。
トークン保留	• 装置の紛失又は盗難に起因する一時的な無効化	トークン要求元	トークンＰＡＮ間マッピングが一時的に保留され、以降の使用が保留される。
トークンの有効化	• トークンＰＡＮ間マッピングを一時保留状態から再開する。	トークン要求元	トークンＰＡＮ間マッピングが一時的に保留された後に有効化され、以降の使用が許可される。
トークン保証の更新	• トークンに対するトークン保証レベルの継続的管理	トークン・サービス・プロバイダ	行われたＩＤ＆Ｖ方法に基づいてトークンＰＡＮ間マッピングに対するトークン保証レベルが更新される。
ＰＡＮ属性の更新	• ＰＡＮ有効期限などの元の信用情報に対する更新	トークン要求元	トークンＰＡＮ間マッピングの使用を延長するために、ＰＡＮ有効期限などのＰＡＮ属性に対する更新が行われる。

表９：ライフサイクル更新インタフェース

【０１７０】

本発明の実施例によって実装されるトークン・サービス・プロバイダによって、ＰＡＮ更新、装置の紛失又は盗難、及び顧客関係の終了によるトークンの無効化などのライフサイクル・イベントに起因するトークンＰＡＮ間マッピングの継続的変更が提供されてもよい。

【０１７１】

ＩＶ．技術的利点及びその他の仕様

本発明の様々な実施例によれば、トークンは、決済処理環境に価値を付加しながら、可視性を向上し、アカウント名義人情報を保護し得る。トークンはグローバル且つマルチ・チャネルで、ＢＩＮベースのトークンとの相互運用性をもち、基礎信用情報とのマッピング又は提携関係を有し、システム内で独立して識別可能であり、エコシステムへの影響を最小限に抑えるために既存のトークン化エコシステムによる受け渡し又はルーティングが可能であり、既存の決済技術（例えば、Ｗｅｂ、ＮＦＣ、ＰＯＳの標準）との互換性があり、代替決済チャネル技術（例えば、ＱＲコード）をサポートすることができ、静的又は動的（例えば、使用制限、時間制限）に配備可能で、異なるエンティティ及びタイプ（例えば、イシュア、ウォレット、販売店）による認証をサポートすることができ、また、すべての規制義務（例えばルーティング決定）との互換性をもつことができる。

【０１７２】

本発明の実施例は、トークン化エコシステム環境全体を通した実装の一貫性及び相互運用性を提供するために、既存データ・フィールドの使用、現行フィールド並びに新規フィールドへのトークン関連データの包含を含む。本発明のいくつかの実施例の一部として導入される１つ又は複数のデータ・フィールドは、任意選択でもよい。

【０１７３】

トランザクション・オーソリゼーション・メッセージ、特に、販売店からアクワイアラ

、アクワイアラから決済ネットワーク、そして決済ネットワークからイシュアに流れる要求メッセージ及び、対応するすべての応答メッセージが、本発明の実施例によって影響され得る。影響の範囲はユースケースによって異なり、関与する決済ネットワークの本発明の実施例に基づくトークン化ソリューションの実装の一部として、それらの決済ネットワークによって交信される認証メッセージの仕様に定められてもよい。

【０１７４】

本明細書に記載される様々な実施例によれば、決済ネットワークはトークン・サービス・プロバイダを使用して、発行されたトークンを受信したオーソリゼーション・メッセージ内のＰＡＮにマッピングした後に、イシュアにメッセージを送信してもよい。決済ネットワークは、アクワイアラに送り返される任意の応答メッセージにＰＡＮを戻してマッピングしてもよい。トークン・サービス・プロバイダは、紛失／盗難されたと見なされるトークンが保留とされた場合は、その旨を決済ネットワークに示してもよい。トークン・サービス・プロバイダは、受信したオーソリゼーション・メッセージ内のトークンを、トークン要求元ＩＤを含むデータ要素に照らして認定し、その結果をトークン・ドメイン制限規制内のトークンの妥当性に関して決済ネットワークに提供してもよい。ＰＡＮが漏洩しているか危険にさらされていると決済ネットワーク又はイシュアが見なした場合は、トークン・サービス・プロバイダは、該当するトークン要求元に漏洩を通知し、そのＰＡＮにマッピングされている関連トークンを無効化してもよい。トークン・サービス・プロバイダは、トークン及びＰＡＮのライフサイクル管理のユースケースの発展に伴ってそのような能力を継続的に追加及び実装してもよい。

【０１７５】

トークン処理及び、関与する決済ネットワークとトークン保管庫の統合によって、特定のドメイン制限規制を所与のトークン要求元及びユースケースのために定められるとおりに適用する能力が提供され得る。ドメイン制限規制は、トランザクション処理メッセージ内で特定の規制関連データ要素が利用可能か否かに依存し、また、このような規制関連データ要素によってトークンは確実に使用制限されるので、基礎的なデータ保全性にも依存する。

【０１７６】

消費者はトークンを使用して、既存のカード・オン・ファイルデータに置き換わるトークン信用情報を使用し、またセキュリティ機能が強化された決済トランザクションを行ってもよい。いくつかの実施例では、決済能力は、デバイス（例えば、携帯電話又はスマートフォン・デバイス）に内蔵されてもよい。いくつかの実施例では、デバイスは、そのデバイスを使用して行われるトランザクションをユーザが使用できるように、１つ又は複数の決済カードの有効化のためのプロンプトをユーザに提供するように構成されたアプリケーション又はソフトウェアを含んでもよい。サービス有効化のプロセスは、リスク評価及びトークン要求、ＩＤ＆Ｖプロセス、並びにトークンのプロビジョニングを含んでもよい。

【０１７７】

様々な実施例によれば、対面（又は店頭）体験によって、消費者がＰＯＳ端末で「タップ＆ペイ」を行うことが可能になってもよい。このプロセスは、決済ネットワークを通してイシュアにトークンを送信することを伴ってもよい。決済ネットワークは受信したトークンを使用してトークン／ＰＡＮ交換を行い、適切なＰＡＮをイシュアに送信してもよい。さらに、アプリ内体験によって消費者が、関与する証明済み販売店アプリケーションと行うトランザクションへの決済（支払い）を、デバイスでシングル・クリック又は選択を通して行うことが可能になってもよい。このプロセスは、決済ネットワークを通してイシュアにトークンを送信することを伴ってもよい。決済ネットワークは受信したトークンを使用してトークン／ＰＡＮ交換を行い、適切なＰＡＮをイシュアに送信してもよい。

【０１７８】

決済ネットワーク又はイシュアによって提供されるトークンは、元のアカウント信用情報（例えば、決済デバイス又は決済アカウント）に拘束されてもよく、近距離通信（ＮＦ

Ｃ）で使用するためにデバイス提供元及び、強化型電子商取引トランザクションにプロビジョニングされてもよい。いくつかの実施例では、消費者がデバイスを有効化すると、その消費者のオンファイルのアカウントが、決済ネットワークから取得したトークンに置き換えられてもよい。

【０１７９】

本発明の実施例は、既存のアクワイアラに第３者が実装し、そのトークン化エコシステム内でトークンを生成し、トークンＰＡＮ間マッピングを行う、既存トークン・ソリューションを排除しない。

【０１８０】

プロダクト・タイプ（例えば、デビット又はクレジット）などのプロダクト属性は、トークン化トランザクションに対して保持される。

【０１８１】

本発明の実施例によって実装された任意の配備済みトークン・サービス・システム内に、カード名義人ポートフォリオの移転に関連付けられたイシュア・ポートフォリオの変換が提供されてもよい。

【０１８２】

表１０は、本発明の様々な実施例によってアクワイアラが実装してもよい機能の一覧を示す。この表は、その機能がＮＦＣトランザクション又は電子商取引トランザクションに適用可能か否かを示す。

【０１８３】

【表１０】

機能	変更	NFC	電子商取引
トークン及びトークン有効期限をフィールド２及びフィールド１４で受け渡す。		✔	✔
トークンに基づく暗号文をフィールド５５、ＮＦＣトランザクションのための用法１で受け渡す。		✔	
トークンに基づく暗号文をフィールド１２６．９、電子商取引トランザクションのための用法で受け渡す。			✔
ＡＶＳデータをＴＬＶフォーマットフィールド１２３、用法２、既存のデータセットＩＤ６６ーＡＶＳデータで送る。	✔	✔	✔
トークン・データ要素をフィールド１２３、用法２、データセットＩＤ６８ー確認データ（トークン保証レベル、規制付き／規制なし；ＰＡＮの上９桁）で受け取る。	✔	✔	✔
ＰＡＮの下４桁をオーソリゼーション応答のフィールド４４．１５で受け取る。	✔	✔	✔
トークンをオーソリゼーション・メッセージで処理されたＴＣＲ０の位置５～２０で渡す。		✔	✔
トークン保証レベルをオーソリゼーション応答で受け取られたＴＣＲ１追加データ、位置６～７で渡す。	✔	✔	✔

表１０：アクワイアラによって実装される機能

【０１８４】

表１１は、アクワイアラを通して渡されるメッセージで送信されてもよいデータ要素の一覧を示す。

【０１８５】

【表１１】

データ案	説明	位置	新フィールド	BASE II
TC x5 及び TC x6, TCR 0*	トークン 注：トークンとＰＡＮの関係が見つからない場合は、ＢＡＳＥＩＩは、トークンとＰＡＮの関係が見つからないことを示す新しい返品理由コード９Ｅをトランザクションで返す。	5 – 20		✔
TC x5 及び TC x6, TCR 1	トークン保証レベル	6 - 7	✔	✔

表１１：アクワイアラによって受け渡されるデータ要素

【０１８６】

表１２は、本発明の様々な実施例によってイシュアが実装してもよい機能の一覧を示す。この表は、その機能がＮＦＣトランザクション又は電子商取引トランザクションに適用可能か否かを示す。

【０１８７】

【表１２】

機能	変更	NFC	電子商取引
トークンのためのＰＯＳ入力モードをフィールド２２で受け渡す。	✔	✔	
トークンに基づく暗号文をフィールド５５、ＮＦＣトランザクションのための用法１で受け取り、処理する。	✔	✔	
トークンに基づく暗号文を電子商取引トランザクションのためのフィールド１２６．９で受け取り、処理する。	✔		✔
ＡＶＳデータをＴＬＶフォーマットフィールド１２３、用法２、既存のデータセットＩＤ６６ーＡＶＳデータで受け取り、処理する。	✔	✔	✔
トークン・データ要素をフィールド１２３、用法２、データセットＩＤ６８ー確認データ（トークン、トークン要求元ＩＤ、トークン保証レベル）で受け取る。	✔	✔	✔
チップ・トランザクション指示子を新しい値（Ｖｉｓａ生成トークンデータ）で、フィールド６０．６で受け取り、処理する。	✔	✔	✔
トークン保証レベルをＴＣＲ１追加データ、位置６～７で受け取る。	✔	✔	✔
トークンをＴＣＲ５決済サービスデータ、位置１５０～１６５で受け取る。	✔	✔	✔
トークンをＴＣ５２取り出し要求レコード、位置８８～１０３でサブミットする。	✔	✔	✔
チャージバック例外処理、コピー要求のためにトークンをＰＡＮと共に保持及び返送する（ＢＡＳＥＩＩ経由ではＴＣ５２、ＳＭＳ経由では０６００）	✔	✔	✔

表１２：イシュアによって実装される機能

【０１８８】

表１３は、イシュアを通して渡されるメッセージで送信されてもよいデータ要素の一覧を示す。

【０１８９】

【表１３】

データ及び取り込み要求の案	説明	位置	新フィールド	BASE II
TC x5 及び TC x6, TCR 0	アカウント番号	5 - 20		✔
TC x5 及び TC x6, TCR 1	トークン保証レベル	6 - 7	✔	✔
TC x5 及び TC x6, TCR 5	トークン	150 - 165	✔	✔
TC 52, TCR 1	トークン	88 - 103	✔	✔

表１３：イシュアによって受け渡されるデータ要素

【０１９０】
表１０～表１３に示されるデータ・フィールドは説明のみを目的とし、制限を課すものと解釈されてはならない。同じ又は類似の情報が異なるデータ・フィールドで伝達されてもよい。本明細書で説明される、これら及び他の、情報を渡すために使用される任意のデータ・フィールドは本発明の範囲に含まれる。

【０１９１】
Ｖ．例示的システム
図１～図９に示される様々な参加者及び要素は、１つ又は複数のコンピュータ装置（例えば、サーバ・コンピュータ）を動作させて、本明細書に記載された機能を促進してもよい。図１～図９のいずれの要素も、任意の適切な数のサブシステムを使用して、本明細書に記載された機能を促進してもよい。そのようなサブシステム又は構成要素の例を図１０に示す。プリンタ１２０８、キーボード１２１６、固定ディスク１２１８（又は、コンピュータ可読媒体を含むその他の記憶装置）、ディスプレイ・アダプタ１２１０に結合されたモニタ１２１２などのサブシステム、及びその他が示されている。入出力（Ｉ／Ｏ）コントローラ１２０２に結合された周辺機器及びＩ／Ｏデバイスを、シリアルポート１２１５などの当技術分野で知られた任意の数の手段によってコンピュータ・システムに結合させることができる。例えば、シリアルポート１２１４又は外部インタフェース１２２０を使用して、インターネットなどの広域ネットワーク、マウス入力デバイス、又はスキャナなどにコンピュータ装置を接続することができる。システム・バスを介した相互接続によって、中央プロセッサ１２０６が各サブシステムと通信すること及びシステム・メモリ１２０４又は固定ディスク１２１８からの命令の実行を制御すること、並びに、サブシステム間での情報の交換が可能になる。

【０１９２】
前述した態様のいくつかに関する特定の詳細について、下記に説明する。特定の態様の特定の詳細が、本発明の趣旨及び範囲を逸脱することなく任意の適切な様式で組み合わされてもよい。

【０１９３】
コード又はコードの一部を格納するためのストレージ媒体又はコンピュータ可読媒体は、当技術分野で知られているか使用されている任意の適切な媒体を含んでもよく、これには、コンピュータ可読命令、データ構造、プログラム・モジュール又はその他のデータの保管及び／又は送信のために任意の方法又は技術で実装された、揮発性及び不揮発性、取り外し可能及び取り外し不可能な媒体などのストレージ媒体及び通信媒体が含まれるが、これらに限定されず、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュ・メモリ若しくはその他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ：Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）若しくはその他の光ストレージ、磁気カセット、磁気テープ、磁気ディスク・ストレージ若しくはその他の磁気ストレージ装置、データ信号、データ送信、又はその他の、所望の情報を保管又は送信するために使用されてもよく、コンピュータによってアクセスされてもよい任意の媒体を含む。本明細書に記載される開示及び

教示に基づいて、当業者は様々な実施例を実装するための他の手法及び／又は方法を知り得る。

【０１９４】

上記に説明したとおりの本発明は、コンピュータ・ソフトウェアを使用し、モジュラー形式又は統合形式で制御ロジックの形で実施されてもよい。本明細書に記載される開示及び教示に基づいて、当業者は、本発明をハードウェア及びハードウェアとソフトウェアとの組み合わせを使用して実装するための適切な他の手法及び／又は方法を知り得る。

【０１９５】

本出願に記載されるソフトウェア構成要素又は機能は、プロセッサにより実行されるソフトウェア・コードとして、例えばＪａｖａ（登録商標）、Ｃ＋＋又はＰｅｒｌなどの任意の適切なコンピュータ言語を使用し、例えば従来型又はオブジェクト指向の技法を使用して実装されてもよい。ソフトウェア・コードは、一連の命令又はコマンドとして、ランダム・アクセス・メモリ（ＲＡＭ：Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、読出し専用メモリ（ＲＯＭ：Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ハードドライブ若しくはフロッピー（登録商標）ディスクなどの磁気媒体、又はＣＤ－ＲＯＭなどの光媒体などのコンピュータ可読媒体に保管されてもよい。そのようなコンピュータ可読媒体はいずれも、単一のコンピュータ装置上又は装置内に常駐してもよいし、システム又はネットワーク内の異なるコンピュータ装置上又は装置内に存在してもよい。

【０１９６】

上記の記載は説明目的であり、制限を課すものではない。本開示を精査すれば、当業者には本発明の多くの変形形態が明らかになり得る。したがって、本発明の範囲は上記の記載への参照によって決定されるのではなく、係属中の特許請求の範囲全体又は相当範囲への参照によって決定されてもよい。

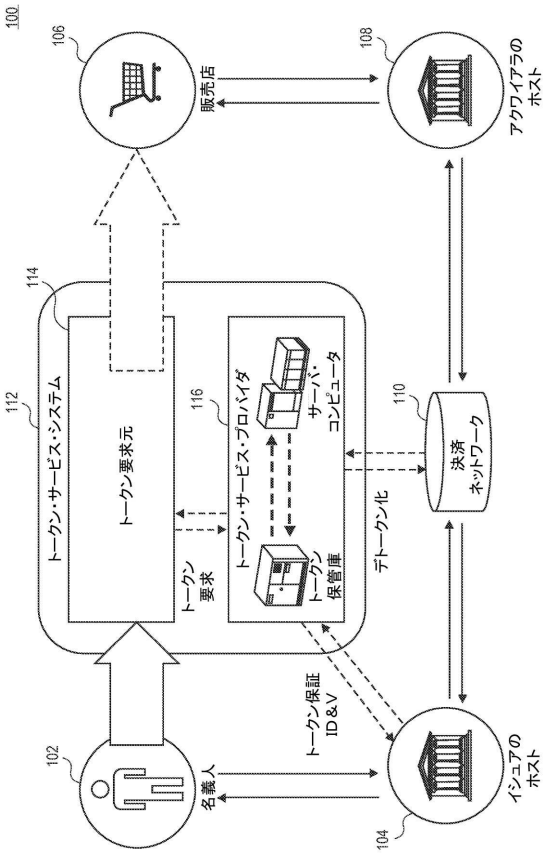
【０１９７】

いずれの実施例からの１つ又は複数の特徴も、本発明の範囲を逸脱することなく任意の他の実施例の１つ又は複数の特徴と組み合わされてもよい。

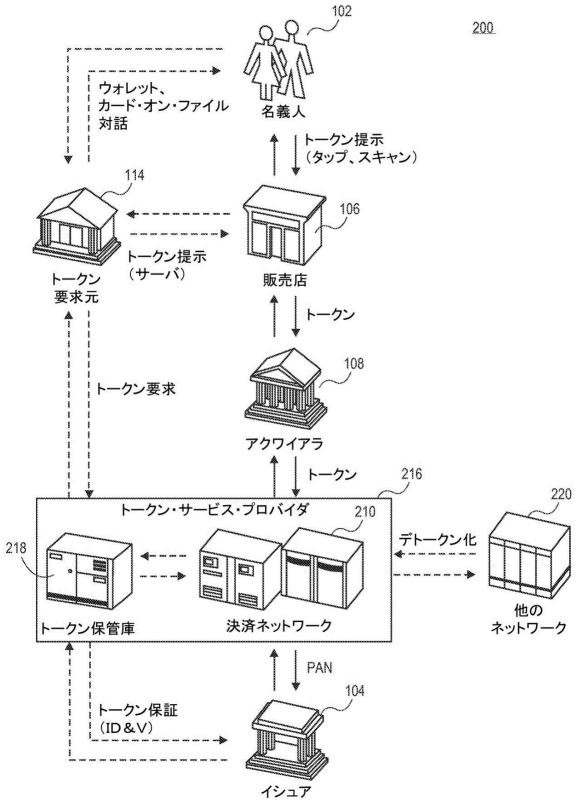
【０１９８】

単数で表される名詞は、特に断りのない限り、「１つ又は複数」を意味すると意図されている。

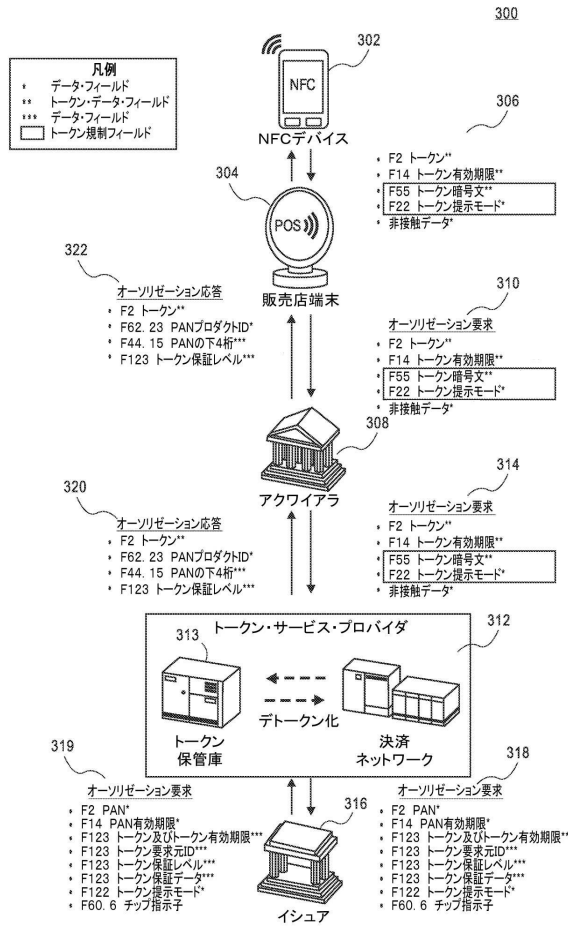
【図１】


100
106
販売店
108
アクワイアラのホスト
114
トークン・サービス・システム
トークン要求元
116
トークン・サービス・プロバイダ
サーバ・コンピュータ
トークン保管庫
110
決済ネットワーク
デトークン化
トークン要求
トークン保証 ID&V
102
名義人
イシュアのホスト
104

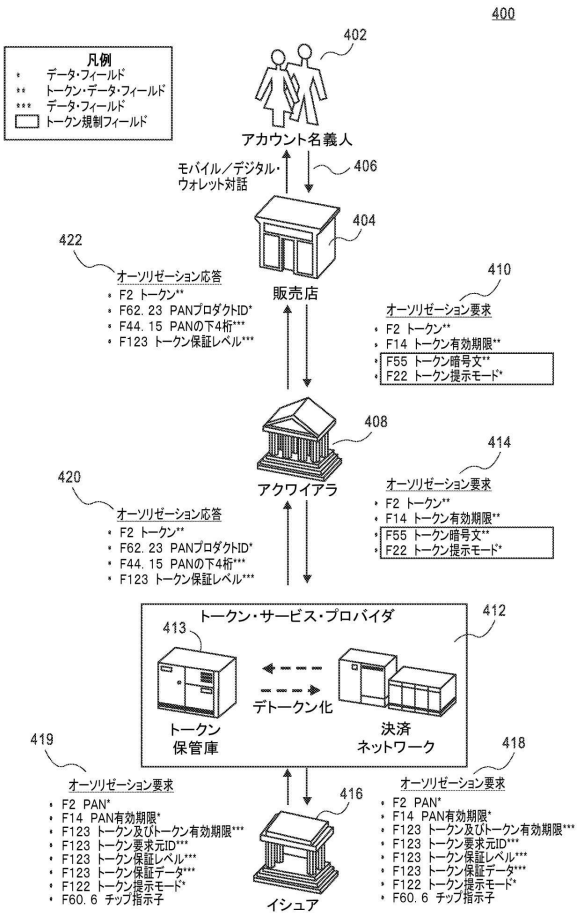
【図２】


200
102
名義人
ウォレット、カード・オン・ファイル対話
トークン提示（タップ、スキャン）
114
トークン要求元
トークン提示（サーバ）
106
販売店
トークン
108
アクワイアラ
トークン要求
トークン
216
トークン・サービス・プロバイダ
210
218
トークン保管庫
決済ネットワーク
デトークン化
220
他のネットワーク
PAN
104
トークン保証（ID&V）
イシュア

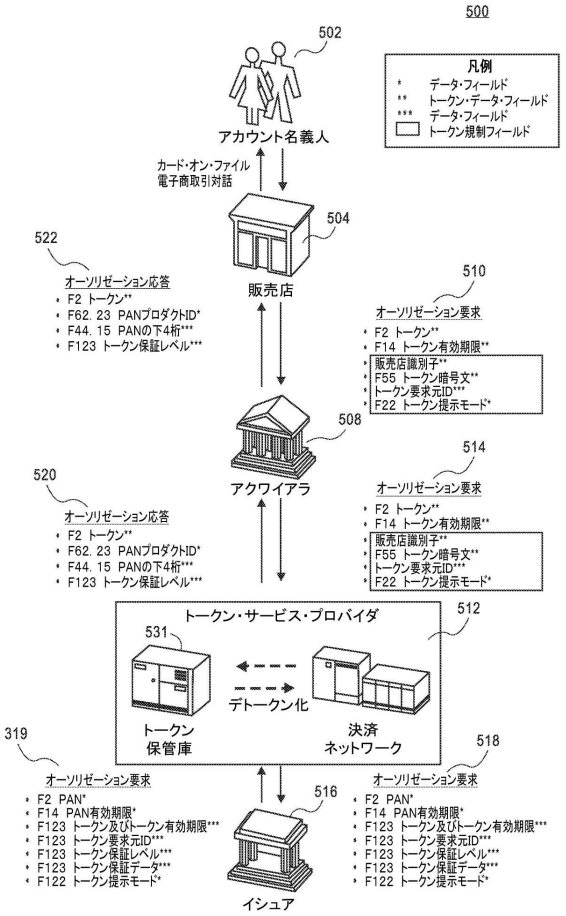
【図３】


300
凡例
* データ・フィールド
** トークン・データ・フィールド
*** データ・フィールド
トークン規制フィールド
302
NFC
NFCデバイス
306
F2 トークン**
F14 トークン有効期限**
F55 トークン暗号文**
F22 トークン提示モード*
非接触データ*
304
POS
販売店端末
322
オーソリゼーション応答
F2 トークン**
F62. 23 PANプロダクトID*
F44. 15 PANの下4桁***
F123 トークン保証レベル***
310
オーソリゼーション要求
F2 トークン**
F14 トークン有効期限**
F55 トークン暗号文**
F22 トークン提示モード*
非接触データ*
308
アクワイアラ
320
オーソリゼーション応答
F2 トークン**
F62. 23 PANプロダクトID*
F44. 15 PANの下4桁***
F123 トークン保証レベル***
314
オーソリゼーション要求
F2 トークン**
F14 トークン有効期限**
F55 トークン暗号文**
F22 トークン提示モード*
非接触データ*
312
313
トークン・サービス・プロバイダ
トークン保管庫
デトークン化
決済ネットワーク
319
オーソリゼーション要求
F2 PAN*
F14 PAN有効期限*
F123 トークン及びトークン有効期限***
F123 トークン要求元ID***
F123 トークン保証レベル***
F123 トークン保証データ***
F122 トークン提示モード*
F60. 6 チップ指示子
316
イシュア
318
オーソリゼーション要求
F2 PAN*
F14 PAN有効期限*
F123 トークン及びトークン有効期限***
F123 トークン要求元ID***
F123 トークン保証レベル***
F123 トークン保証データ***
F122 トークン提示モード*
F60. 6 チップ指示子

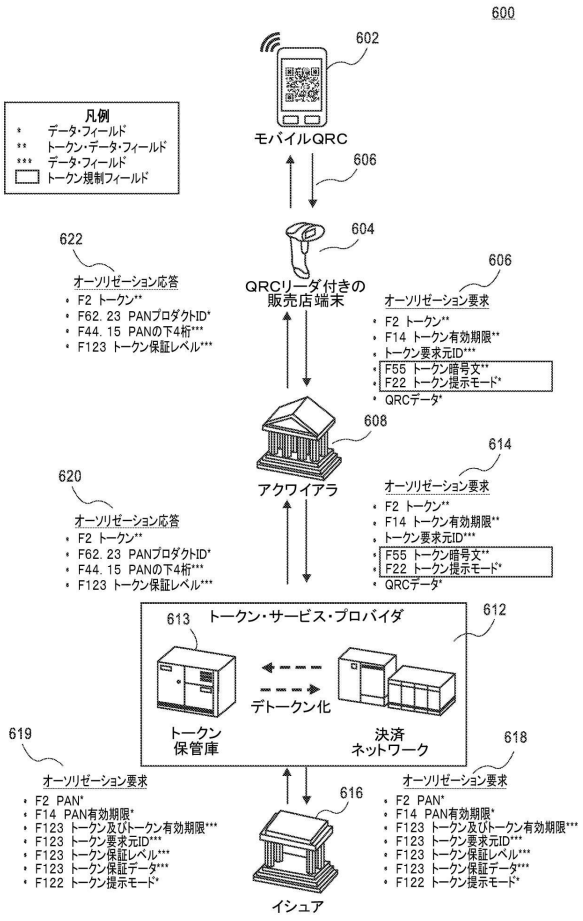
【図４】


400
凡例
* データ・フィールド
** トークン・データ・フィールド
*** データ・フィールド
トークン規制フィールド
402
アカウント名義人
モバイル／デジタル・ウォレット対話
406
404
販売店
422
オーソリゼーション応答
F2 トークン**
F62. 23 PANプロダクトID*
F44. 15 PANの下4桁***
F123 トークン保証レベル***
410
オーソリゼーション要求
F2 トークン**
F14 トークン有効期限**
F55 トークン暗号文**
F22 トークン提示モード*
408
アクワイアラ
420
オーソリゼーション応答
F2 トークン**
F62. 23 PANプロダクトID*
F44. 15 PANの下4桁***
F123 トークン保証レベル***
414
オーソリゼーション要求
F2 トークン**
F14 トークン有効期限**
F55 トークン暗号文**
F22 トークン提示モード*
412
413
トークン・サービス・プロバイダ
トークン保管庫
デトークン化
決済ネットワーク
419
オーソリゼーション要求
F2 PAN*
F14 PAN有効期限*
F123 トークン及びトークン有効期限***
F123 トークン要求元ID***
F123 トークン保証レベル***
F123 トークン保証データ***
F122 トークン提示モード*
F60. 6 チップ指示子
416
イシュア
418
オーソリゼーション要求
F2 PAN*
F14 PAN有効期限*
F123 トークン及びトークン有効期限***
F123 トークン要求元ID***
F123 トークン保証レベル***
F123 トークン保証データ***
F122 トークン提示モード*
F60. 6 チップ指示子

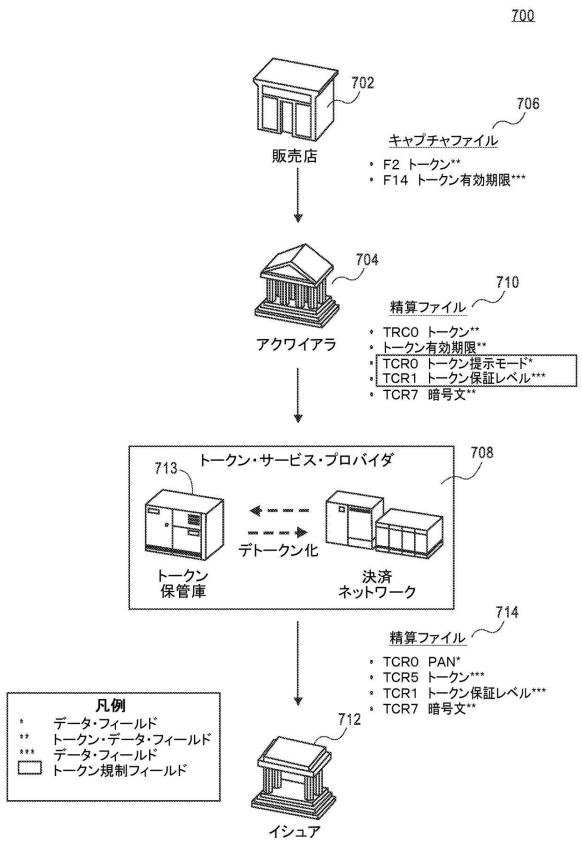
【図５】


500
502
アカウント名義人
凡例
* データ・フィールド
** トークン・データ・フィールド
*** データ・フィールド
トークン規制フィールド
カード・オン・ファイル
電子商取引対話
504
販売店
522
オーソリゼーション応答
• F2 トークン**
• F62. 23 PANプロダクトID*
• F44. 15 PANの下4桁***
• F123 トークン保証レベル***
510
オーソリゼーション要求
• F2 トークン**
• F14 トークン有効期限**
• 販売店識別子**
• F55 トークン暗号文**
• トークン要求元ID***
• F22 トークン提示モード*
508
アクワイアラ
520
オーソリゼーション応答
• F2 トークン**
• F62. 23 PANプロダクトID*
• F44. 15 PANの下4桁***
• F123 トークン保証レベル***
514
オーソリゼーション要求
• F2 トークン**
• F14 トークン有効期限**
• 販売店識別子**
• F55 トークン暗号文**
• トークン要求元ID***
• F22 トークン提示モード*
512
トークン・サービス・プロバイダ
531
トークン
保管庫
デトークン化
決済
ネットワーク
319
オーソリゼーション要求
• F2 PAN*
• F14 PAN有効期限*
• F123 トークン及びトークン有効期限***
• F123 トークン要求元ID***
• F123 トークン保証レベル***
• F123 トークン保証データ***
• F122 トークン提示モード*
518
オーソリゼーション要求
• F2 PAN*
• F14 PAN有効期限*
• F123 トークン及びトークン有効期限***
• F123 トークン要求元ID***
• F123 トークン保証レベル***
• F123 トークン保証データ***
• F122 トークン提示モード*
516
イシュア

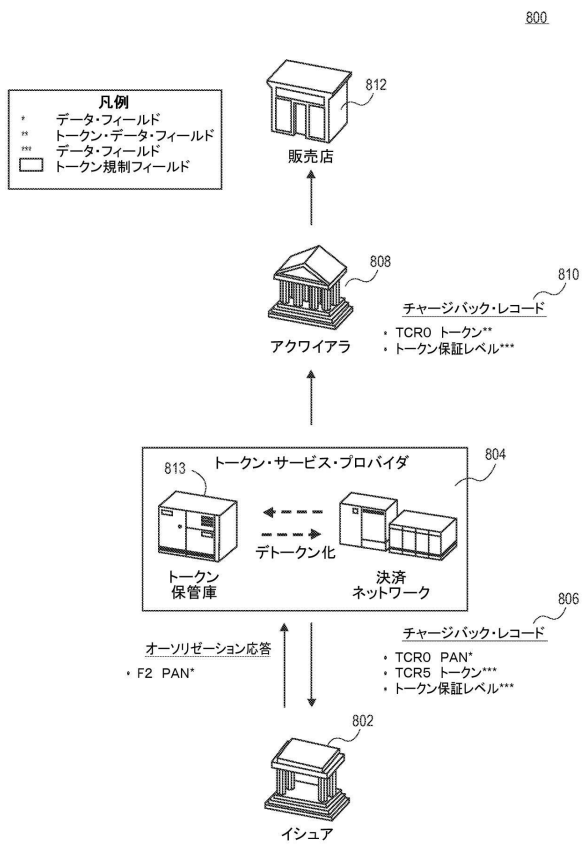
【図６】


600
602
モバイルQRC
凡例
* データ・フィールド
** トークン・データ・フィールド
*** データ・フィールド
トークン規制フィールド
606
604
QRCリーダ付きの
販売店端末
622
オーソリゼーション応答
• F2 トークン**
• F62. 23 PANプロダクトID*
• F44. 15 PANの下4桁***
• F123 トークン保証レベル***
606
オーソリゼーション要求
• F2 トークン**
• F14 トークン有効期限**
• トークン要求元ID***
• F55 トークン暗号文**
• F22 トークン提示モード*
• QRCデータ*
608
アクワイアラ
620
オーソリゼーション応答
• F2 トークン**
• F62. 23 PANプロダクトID*
• F44. 15 PANの下4桁***
• F123 トークン保証レベル***
614
オーソリゼーション要求
• F2 トークン**
• F14 トークン有効期限**
• トークン要求元ID***
• F55 トークン暗号文**
• F22 トークン提示モード*
• QRCデータ*
612
613
トークン・サービス・プロバイダ
トークン
保管庫
デトークン化
決済
ネットワーク
619
オーソリゼーション要求
• F2 PAN*
• F14 PAN有効期限*
• F123 トークン及びトークン有効期限***
• F123 トークン要求元ID***
• F123 トークン保証レベル***
• F123 トークン保証データ***
• F122 トークン提示モード*
618
オーソリゼーション要求
• F2 PAN*
• F14 PAN有効期限*
• F123 トークン及びトークン有効期限***
• F123 トークン要求元ID***
• F123 トークン保証レベル***
• F123 トークン保証データ***
• F122 トークン提示モード*
616
イシュア

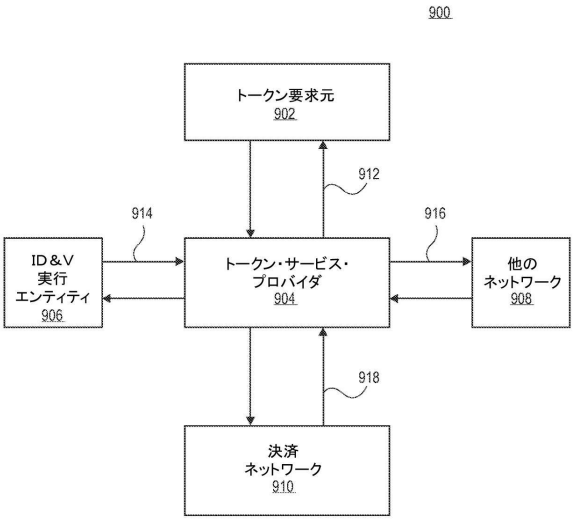
【図７】


700
702
販売店
706
キャプチャファイル
• F2 トークン**
• F14 トークン有効期限***
704
アクワイアラ
710
精算ファイル
• TRC0 トークン**
• トークン有効期限**
• TCR0 トークン提示モード*
• TCR1 トークン保証レベル***
• TCR7 暗号文**
708
713
トークン・サービス・プロバイダ
トークン
保管庫
デトークン化
決済
ネットワーク
714
精算ファイル
• TCR0 PAN*
• TCR5 トークン***
• TCR1 トークン保証レベル***
• TCR7 暗号文**
712
イシュア
凡例
* データ・フィールド
** トークン・データ・フィールド
*** データ・フィールド
トークン規制フィールド

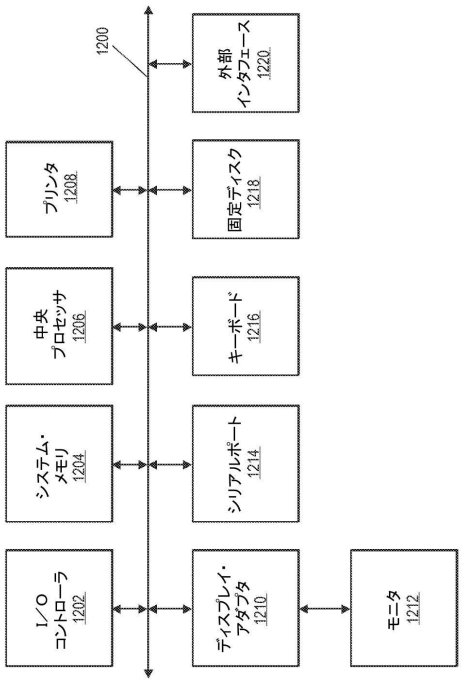
【図８】


800
凡例
* データ・フィールド
** トークン・データ・フィールド
*** データ・フィールド
トークン規制フィールド
812
販売店
808
アクワイアラ
810
チャージバック・レコード
• TCR0 トークン**
• トークン保証レベル***
813
トークン・サービス・プロバイダ
804
トークン
保管庫
デトークン化
決済
ネットワーク
806
チャージバック・レコード
• TCR0 PAN*
• TCR5 トークン***
• トークン保証レベル***
オーソリゼーション応答
• F2 PAN*
802
イシュア

【図９】


900
トークン要求元
902
912
914
916
ID＆V
実行
エンティティ
906
トークン・サービス・
プロバイダ
904
他の
ネットワーク
908
918
決済
ネットワーク
910

【図１０】


1200
外部
インタフェース
1220
プリンタ
1208
固定ディスク
1218
中央
プロセッサ
1206
キーボード
1216
システム・
メモリ
1204
シリアルポート
1214
I／O
コントローラ
1202
ディスプレイ・
アダプタ
1210
モニタ
1212

フロントページの続き

(72)発明者　パウエル、グレン　レオン
アメリカ合衆国、カリフォルニア、フレモント、マヤ　ストリート　４７８３０
(72)発明者　シーツ、ジョン　エフ.
アメリカ合衆国、カリフォルニア、サン　フランシスコ、エリザベス　ストリート　９１５
(72)発明者　ラザフォード、ブルース
アメリカ合衆国、コネティカット、スタンフォード
(72)発明者　ウィリアムソン、グレゴリー
アメリカ合衆国、コネティカット、スタンフォード
(72)発明者　アンダーソン、ジェームス
アメリカ合衆国、ニューヨーク、マウント　バーノン

審査官　貝塚　涼

(56)参考文献　米国特許出願公開第２０１２／００２３５６７（ＵＳ，Ａ１）
国際公開第２０１２／１５１５９０（WO，Ａ２）
米国特許出願公開第２００３／００２８４８１（ＵＳ，Ａ１）
米国特許出願公開第２０１２／０２５９７８４（ＵＳ，Ａ１）
久保渓，クレジットカード決済のセキュリティ 情報漏洩対策の勘所と、国際セキュリティ標準 ＰＣＩ ＤＳＳ，ＷＥＢ＋ＤＢ ＰＲＥＳＳ，日本，株式会社技術評論社，２０１３年　9月２５日，第７６巻，第５４－５８頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００　－　９９／００