

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成22年3月18日(2010.3.18)

【公表番号】特表2007-536619(P2007-536619A)

【公表日】平成19年12月13日(2007.12.13)

【年通号数】公開・登録公報2007-048

【出願番号】特願2007-511334(P2007-511334)

【国際特許分類】

G 0 6 Q 20/00 (2006.01)

G 0 6 Q 50/00 (2006.01)

H 0 4 L 9/32 (2006.01)

G 0 6 Q 40/00 (2006.01)

G 0 6 Q 10/00 (2006.01)

【F I】

G 0 6 F 17/60 4 1 4

G 0 6 F 17/60 Z E C

H 0 4 L 9/00 6 7 3 A

G 0 6 F 17/60 2 2 4

G 0 6 F 17/60 5 1 2

【誤訳訂正書】

【提出日】平成22年1月28日(2010.1.28)

【誤訳訂正1】

【訂正対象書類名】特許請求の範囲

【訂正対象項目名】全文

【訂正方法】変更

【訂正の内容】

【特許請求の範囲】

【請求項1】

個々の利用者と要求者との間のオンライン取引中に、信頼性の高い利用者情報を付加価値提供者に提供するための方法であって、

前記要求者のコンピュータが、前記利用者のコンピューティングデバイスから、前記オンライン取引中に前記利用者に関する利用者情報を収集し、

前記信頼機関のアクセス制御コンピュータが、前記オンライン取引中に、前記利用者の同一性の認証のために前記要求者のコンピュータから発行されたオンライン認証要求メッセージを、前記利用者のコンピューティングデバイスを介して受信し、

前記信頼機関のアクセス制御コンピュータが、前記オンライン取引中に、前記利用者から同一性認証用の証拠を受信し、

前記信頼機関のアクセス制御コンピュータが、前記オンライン取引中に、前記利用者に対して事前に指定された証拠を格納している利用者データベースを参照して、前記同一性認証用の証拠を、前記利用者に対して事前に指定された証拠と比較し、

前記信頼機関のアクセス制御コンピュータが、前記オンライン取引と前記利用者情報とを一意に識別する取引識別子を生成し、

前記信頼機関のアクセス制御コンピュータが、前記同一性認証用の証拠が、前記利用者に対して事前に指定された前記証拠に一致する場合に、前記利用者が認証された旨を前記要求者に通知するオンライン認証応答メッセージであって前記取引識別子を含むオンライン認証応答メッセージを、前記オンライン取引中に、前記利用者のコンピューティングデバイスを介して前記要求者のコンピュータに送信し、

前記要求者のコンピュータが、前記オンライン認証応答メッセージを受けた後に、前記

収集された利用者情報とともに前記取引識別子を前記付加価値提供者のコンピュータサーバに送信し、前記付加価値提供者のコンピュータサーバが前記利用者情報の真実性を確認する、方法。

【請求項 2】

請求項 1 に記載の方法であって、更に、

前記要求者のコンピュータが、前記収集された利用者情報を、前記付加価値提供者が前記収集された利用者情報の取得を望むか否かに関する一組の基準により評価し、

前記収集された利用者情報が前記一組の基準を満たすと判断された場合に、前記収集された利用者情報を前記付加価値提供者のコンピュータサーバに送信する、ことを含む、方法。

【請求項 3】

請求項 1 に記載の方法であって、更に、

前記信頼機関のアクセス制御コンピュータが、前記利用者による複数のオンライン取引にわたる前記利用者の行動を表す前記利用者情報を収集することを含む、方法。

【請求項 4】

請求項 1 に記載の方法であって、更に、

前記付加価値提供者が、部分的に前記利用者情報に基づいて、前記利用者に関連する特定の動作を行うことを含む、方法。

【請求項 5】

請求項 1 に記載の方法であって、

追加的な利用者情報が、前記信頼機関によってそれ以前に収集されていた前記認証応答メッセージ内に含まれており、

前記方法は、更に、

前記追加的な利用者情報を前記要求者のコンピュータから前記付加価値提供者のコンピュータサーバに送信することを含む、方法。

【請求項 6】

請求項 1 に記載の方法であって、前記信頼機関は、前記利用者の口座を維持する発行機関であり、

前記方法は、更に、

前記発行機関のアクセス制御コンピュータが、登録処理中に、前記口座の所有者としての前記利用者の同一性を確認して、前記事前に指定された証拠を前記口座と関連付けることを含む、方法。

【請求項 7】

請求項に記載の方法であって、更に、

前記信頼機関のアクセス制御コンピュータが、前記利用者情報と前記取引識別子とを、格納のために履歴サーバに送信し、

前記信頼機関のアクセス制御コンピュータが、前記利用者情報と前記取引識別子とを前記履歴サーバから取得し、

前記取得した利用者情報と前記取引識別子とを用いて、前記要求者と前記付加価値提供者との間の取引を完結させることを含む、方法。

【請求項 8】

請求項に記載の方法であって、更に、

前記信頼機関のアクセス制御コンピュータが、前記利用者情報と前記取引識別子とを、格納のために履歴サーバに送信し、

前記信頼機関のアクセス制御コンピュータが、前記利用者情報と前記取引識別子とを前記履歴サーバから取得し、

前記取得した利用者情報と前記取引識別子とを用いて、紛争解決またはデータマイニングを実行することを含む、方法。

【請求項 9】

請求項 1 に記載の方法であって、前記利用者情報は、前記オンライン取引の対象を表す

情報を含む、方法。

【請求項 10】

請求項 1 に記載の方法であって、前記利用者情報は、前記利用者に関する購入行動情報を含む、方法。

【請求項 11】

請求項 1 に記載の方法であって、更に、

前記利用者情報の前記付加価値提供者のコンピュータサーバへの送信前に、前記要求者と前記付加価値提供者とが、前記収集された利用者情報に基づいて契約に合意することを含む、方法。

【請求項 12】

請求項に記載の方法であって、更に、

前記利用者情報と引き換えに貨幣価値を前記付加価値提供者のコンピュータサーバから前記要求者のコンピュータに転送することを含む、方法。

【請求項 13】

請求項 1 に記載の方法であって、前記付加価値提供者は、運送会社、後続販売者、または、セキュリティ組織である、方法。

【請求項 14】

請求項 1 に記載の方法であって、更に、

前記要求者のコンピュータが、前記収集された利用者情報を複数の付加価値提供者のコンピュータサーバに送信し、

前記要求者のコンピュータが、前記利用者に関係するサービスの見積もりを、前記複数の付加価値提供者のコンピュータサーバの内の少なくとも 1 つから受信し、

前記要求者が、少なくとも前記受信された見積もりに基づいて、前記複数の付加価値提供者の内の 1 つを選択することを含む、方法。

【請求項 15】

請求項 1 に記載の方法であって、

前記利用者の前記コンピューティングデバイスは、コンピュータ、PDA、又は、携帯電話である、方法。

【請求項 16】

請求項 1 に記載の方法であって、

前記利用者情報は、利用者連絡先情報、利用者支払履歴情報、又は、利用者出荷履歴情報を含む、方法。

【請求項 17】

請求項 1 に記載の方法であって、

前記オンライン認証要求メッセージ及び前記オンライン認証応答メッセージは、前記コンピューティングデバイスのブラウザを介して送られる、方法。

【請求項 18】

請求項 1 に記載の方法であって、更に、

前記コンピューティングデバイスのインターネットブラウザを、前記要求者のコンピュータから前記アクセス制御コンピュータにリダイレクトすることによって、前記信頼機関のアクセス制御コンピュータが同一性認証トークンを受け取り、

前記コンピューティングデバイスのインターネットブラウザを、前記アクセス制御コンピュータから前記要求者のコンピュータにリダイレクトして戻すことを含む、方法。

【請求項 19】

個々の利用者と要求者との間のオンライン取引中に、信頼性の高い利用者情報を付加価値提供者に提供する認証システムであって、

前記要求者に、前記オンライン取引中に利用者情報を提供する利用者のコンピューティングデバイスと、

前記要求者の要求者サーバコンピュータであって、前記利用者のコンピューティングデバイスとの前記オンライン取引に従事するよう構成され、更に、前記利用者の同一性の認

証を要求するオンライン認証要求メッセージを、前記コンピューティングデバイスを介して信頼機関に送信するよう構成されている要求者サーバコンピュータと、

前記信頼機関のアクセス制御サーバであって、前記利用者のコンピューティングデバイスから同一性認証用の証拠を受信するよう構成され、更に、前記利用者に対して事前に指定された証拠を格納している利用者データベースを参照して、前記同一性認証用の証拠を、前記利用者に対して事前に指定された証拠と比較して、前記利用者が認証されたことを示すオンライン認証応答メッセージであって前記オンライン取引と前記利用者情報とを一意に識別する取引識別子を含むオンライン認証応答メッセージを前記要求者サーバコンピュータに送信するよう構成されているアクセス制御サーバと、

付加価値提供者のサーバコンピュータであって、前記利用者情報を前記要求者サーバコンピュータから受信するよう構成されているサーバコンピュータと、を備え、

前記要求者サーバコンピュータが前記利用者情報とともに前記取引識別子を前記付加価値提供者のサーバコンピュータに送信し、前記付加価値提供者のコンピュータサーバが前記利用者情報の真实性を確認する、システム。

【請求項 20】

請求項 19 に記載のシステムであって、

追加的な利用者情報が、前記信頼機関によってそれ以前に収集されていた前記認証応答メッセージに含まれる、システム。

【請求項 21】

請求項 19 に記載のシステムであって、更に、

前記利用者情報と前記取引識別子とが格納のために送信される先の履歴サーバを備える、システム。

【請求項 22】

請求項 19 に記載のシステムであって、前記利用者情報は、前記オンライン取引の対象を表す情報を含む、システム。

【請求項 23】

請求項 19 に記載のシステムであって、前記利用者情報は、前記利用者に関する購入行動情報を含む、システム。

【請求項 24】

請求項 19 に記載のシステムであって、前記付加価値提供者は、運送会社、後続販売者、または、セキュリティ組織である、システム。

【請求項 25】

請求項 19 に記載のシステムであって、更に、

前記利用者情報が送信される先の複数のサーバコンピュータであって、それぞれ、複数の付加価値提供者の内の 1 つに関連付けられているサーバコンピュータと、を備える、システム。

【請求項 26】

請求項 19 に記載のシステムであって、前記利用者のコンピューティングデバイスは、コンピュータ、PDA、または、携帯電話である、システム。

【請求項 27】

請求項 19 に記載のシステムであって、

前記コンピューティングデバイスはブラウザを含み、

前記オンライン認証要求メッセージ及び前記オンライン認証応答メッセージは、前記ブラウザを介して送られる、システム。

【請求項 28】

請求項 19 に記載のシステムであって、

前記コンピューティングデバイスはインターネットブラウザを含み、

前記インターネットブラウザは、前記要求者のコンピュータから前記アクセス制御コンピュータにリダイレクトされ、前記アクセス制御コンピュータから前記要求者のコンピュータにリダイレクトして戻される、システム。

【誤訳訂正 2】

【訂正対象書類名】明細書

【訂正対象項目名】全文

【訂正方法】変更

【訂正の内容】

【発明の詳細な説明】

【発明の名称】オンライン認証方法及びシステム

【技術分野】

【0001】

本発明は、オンライン取引中に口座保有者の同一性を認証する事に関し、特に、認証処理に関連する情報を付加価値提供者が共有及び使用する手法に関する

【背景技術】

【0002】

支払いカード（例えば、クレジットカード、デビットカード、又は価値格納カード）を使用した支払取引中には、カード保有者の口座の所有を検証し、不正使用等の様々な問題を回避することが重要である。支払者認証は、カード保有者の口座所有権を検証する処理である。カード保有者の口座所有権を認証する最も一般的な方法は、「カード有り」取引と呼ばれるものの間に、販売場所で日常的に発生する。カード有り取引には、販売者の代行者がカード保有者のカードを受け取り、口座の状態とクレジットラインの利用可能性とを検証するために支払カード端末に通し、カード裏面の署名が購入者の署名と一致するかを確認するためにチェックすることを含む。販売者がこの種の取引の特定の指針に従う場合、販売者は、割引額と手数料とを差し引いた、認証額の支払を保証される。ビザ インターナショナル サービス アソシエーション（Visa International Service Association）等のサービスプロバイダ（又はサービス組織）は、こうした特定の指針を提供してよい。

【発明の開示】

【発明が解決しようとする課題】

【0003】

一方、オンライン、郵便、又は電話で発生するような「カード無し」取引には、販売者に対して保証されない支払が関与する。保証が提供されないのは、主に、こうして非対面取引では支払者が認証されず、「カード無し」取引に多数のリスクが伴うためである。こうしたリスクは、オンライン販売者に対する支払取引のチャージバック、販売者とカード保有者との両方に対する詐欺、銀行に対する例外項目処理費用の増加、一部の顧客にオンラインでの購入を回避させ得る、オンラインでの商品及びサービスの購入が安全確実ではないという認識の増加等の問題が含まれる。リスクの具体的な例には、商品及びサービスをオンラインで購入するための盗難口座情報の不正使用、不正なオンライン購入を行うためのカード口座番号の偽造、ネットワークトラフィックからの平文口座情報の抽出が含まれる。

【0004】

電子商取引の予想される継続的な高成長を考えると、支払者を認証する方法を提供する事が重要である。オンライン取引の種類幅広さを考えると、取引に商業的側面が存在するか否かに関係なく、関係者の同一性を認証する方法を提供することも重要である。これは、カード保有者、販売者、金融機関から、政府機関に至る全ての取引参加者に利益をもたらす。オンライン取引中に顧客を認証することで、詐欺、紛争、回収、及びチャージバックのレベルが減少し、結果として、こうした事象のそれぞれに関連するコストが減少する。顧客を認証することで、セキュリティの問題にも対処するため、オンライン活動の増加につながる。オンライン取引中に関係者を認証するために使用される従来のシステムは、使用するのが難しく、複雑な設計を有し、システム関与者に大きな事前投資が求められ、相互運用性が不足していることから、広範囲には採用されていない。特定の従来のシステムでは、追加として、販売者、カード保有者、発行者、及び取得者による証明書の作成

、配布、及び使用が必要となる。こうした証明書の使用は、非常に負担となることが知られている。

【0005】

上記を鑑みると、オンライン取引において顧客の同一性を認証する改良されたシステムを提供するために、継続的な努力がなされている。更に、こうした認証処理に關与する者に利用可能な情報を有効に使用するために、継続的な努力がなされている。

【課題を解決するための手段】

【0006】

本発明は、オンライン取引中に利用者の同一性を認証する口座認証サービスを対象とする。認証サービスにより、信頼機関は、パスワード又はトークン等の様々な認証方法を使用して、要求する関係者（「要求者」）のために、口座保有者の同一性を検証できる。オンライン取引中における口座保有者の同一性認証は、口座保有者からパスワードを要求し、パスワードを検証し、口座保有者の信頼性が検証されたか否かを要求者に通知することを含む。口座認証サービスの代替実施形態は、顧客に関する情報が付加価値提供者と共有される提供対価構成要素を含む。顧客情報は、口座認証処理において関係者のそれぞれから収集されるため、顧客に関する詳細を数多く含む。付加価値提供者は、その後、この情報を様々な形で使用できる。關与する全ての関係者は、顧客情報を共有することで利益を享受可能であり、各関係者は、価値の取得を互いにどのように支援できるかについて合意できる。顧客と販売者との間で特定の取引を識別する取引識別子と顧客情報とを使用することで、関係者のそれぞれは、取引と、顧客情報に關連する任意の合意とについて監査できる。

【0007】

方法として、本発明の一実施形態は、少なくとも、利用者から同一性認証パスワードを受け取り、同一性認証パスワードを利用者の口座に事前指定したパスワードと比較することを含む。方法は、更に、利用者から受け取った同一性認証パスワードが口座に事前指定したパスワードと一致した場合に、利用者が口座の実際の所有者であることを要求者に通知することを含む。このようにして、信頼機関は、要求者のために、利用者が口座の実際の所有者であることを認証する。方法は、更に、利用者情報の付加価値提供者への送信を含む。一部の実施形態において、方法は、更に、利用者情報を一組の基準に照らして評価し、利用者情報が一組の基準を満たす場合に、利用者情報を付加価値提供者に送信することを含む。これにより、付加価値提供者は、所望の顧客情報を受け取ることができる。更に、要求者及び付加価値提供者のそれぞれは、利用者情報が付加価値提供者に送信される前に、条件として一組の権利及び義務に合意できる。追加として、取引識別子は、個別のオンライン取引と、關連づけられている顧客情報とを追跡するために使用できる。

【0008】

本発明の一実施形態において、要求者は、販売者であり、付加価値提供者は、顧客情報を使用して、販売者から購入製品を出荷可能な運送会社である。顧客情報は、製品を顧客に出荷するか、どのように出荷するかについて、運送会社が判断するのを助ける。

【0009】

本発明の別の実施形態において、要求者は、販売者であり、付加価値提供者は、顧客情報を使用して自分の商品又はサービスを顧客に売り込む後続販売者である。顧客情報は、顧客に連絡するか、どのように連絡するかについて、後続販売者が判断するのを助ける。

【0010】

本発明の別の実施形態において、付加価値提供者は、顧客情報を使用してセキュリティ問題を評価できるセキュリティ組織である。顧客情報は、考えられるセキュリティ問題に対処するか、どのように対処するかについて、セキュリティ組織が判断するのを助ける。

【0011】

本発明の上記及びその他の特徴及び利点について、以下の本発明の明細書と、本発明の原理を例示する添付図面とにおいて、更に詳細に提示する。

【発明を実施するための最良の形態】

【 0 0 1 2 】

本発明は、その更なる利点と共に、以下の説明を次の添付図面と併せて参照することにより、最も良く理解されよう。

【 0 0 1 3 】

本発明について、添付図面に例示した、いくつかの好適な実施形態を参照して、詳細に説明する。以下の説明では、本発明の完全な理解を提供するために、多数の具体的な詳細について述べる。しかしながら、こうした具体的な詳細の一部又は全部がなくとも、本発明を実施し得ることは、当業者には明白であろう。また、本発明を不必要に曖昧にしないために、周知の動作についての詳細な説明は省略する。

【 0 0 1 4 】

本説明は、図 1 において、本発明による一般的な口座認証システム及びプロトコルの概要から始める。口座認証システムは、関与する発行者、口座保有者、及び販売者へのサービスとして提供される。次に、図 2 乃至 7 において、オンライン支払取引に関連する口座認証システムについて説明する。オンライン支払取引の説明は、支払取引自体、システム設定、顧客登録、及び具体的なメッセージフローを対象とする。オンライン支払取引の説明は、非支払取引の説明に類似する。支払及び非支払取引は、両方とも、口座保有者の同一性の認証を含む。

【 0 0 1 5 】

次に図 8 において、提供対価構成要素を含む口座認証処理について説明する。価値は、最初に、顧客に関する情報を付加価値提供者と共有することで付加される。顧客情報は、口座認証処理において関係者のそれぞれから収集されるため、顧客に関する詳細を数多く含む。付加価値提供者は、その後、この情報を様々な形で使用できる。例えば、付加価値提供者は、焦点を絞った情報を顧客に提供可能であり、或いは、顧客に商品を発送可能である。関与する全ての関係者は、顧客情報を共有することで利益を享受可能であり、各関係者は、価値の取得を互いにどのように支援できるかについて合意できる。顧客と販売者との間で特定の取引を識別する取引識別子と顧客情報とを使用することで、関係者のそれぞれは、取引と、顧客情報に関連する任意の合意について監査できる。本願では、こうした情報の共有を、広範な用途で、広範な関係者の利益のために、どのようにして有利な形で使用できるかについて説明する。

【 0 0 1 6 】

口座認証システム

口座認証システムは、一方の関係者が特定の口座の所有者であると主張する別の関係者の同一性を物理的に検証できない取引中に、口座保有者の口座所有権を認証するように設計される。例えば、口座認証システムは、信頼機関が要求者のために利用者の同一性を認証する時に、様々な取引で使用できる。要求者とは、信頼機関に利用者の同一性の認証を要求する任意の個人又は団体である。信頼機関とは、利用者の同一性を認証可能で、利用者及び要求者が認証処理の実行を委ねる団体である。信頼機関は、利用者の同一性に関する誤り又は詐欺の際に、要求者の利益を保護することに合意できる。口座認証システムの重要な用途は、オンラインで、又は携帯電子機器を介して行われる、支払取引の分野である。

【 0 0 1 7 】

しかしながら、システムは、支払取引に加えて、多数の用途において有用となり得る本発明のシステムは、顧客の同一性の認証が必要となる様々な非支払状況において使用できる。例えば、非支払取引は、例えば、登録処理のため、インターネット web サイトにアクセスしてオンラインフォームに記入する顧客を認証する等の取引を含む。非支払取引は、僅かな例として、小売銀行業、卸売銀行業、医療業、保険業、及び仲買業の多数の態様を含む。小売銀行業には、デビットカード、購入カード、及び価値格納カード等のカードで使用する口座番号が関与する。非支払取引には、IDカード及びライセンス等のために、オンラインフォームを記入することが含まれる。例えば、米国自動車協会 (AAA) は、システムを使用して、顧客の一人の同一性を認証可能であり、電話カード会社は、シス

テムを使用して、特定のカードのユーザの同一性を認証できる。

【 0 0 1 8 】

図1は、様々なタイプの口座認証用途に対して口座認証システムを実施するためのシステムアーキテクチャ100の一実施形態を示している。システムアーキテクチャ100は、三つの領域、即ち、信頼機関領域103、相互運用領域104、及び要求者領域105を含む。

【 0 0 1 9 】

信頼機関領域と要求者領域は、それぞれ信頼機関又は要求者により完全に又は少なくとも部分的に制御される構成要素を内部に有する機能範囲を定める。相互運用領域は、信頼機関、要求者、及びサービス組織等の他の関係者が利用し得る構成要素を内部に有する機能範囲を定める。

【 0 0 2 0 】

信頼機関領域103は、信頼機関により主に制御される構成要素を含む。信頼機関の例は、発行銀行として知られる、支払カードを消費者に発行する金融機関である。具体的には、発行者、又はカード発行者は、カード供給者から受け取った新たなカードを個人化し、こうしたカードを顧客に発行する。個人化は、カード供給者又は個人化局が実行してもよい。金融機関に加え、発行者は、電気通信ネットワークオペレータ、サービス団体、販売者その他の組織、又は発行者を代行する代理業者等、任意の適切な発行団体であってよい。要求者領域105は、要求者により主に制御される構成要素を含む。要求者は、口座保有者の同一性の認証を要求する任意の関係者にすることができる。例えば、要求者は、クレジットカード口座の所有者であると主張する人物の同一性の認証を希望する販売者にできる。取得者は、要求者を支払体系に加入させ、要求者の口座を管理する金融機関にできる。取得者は、更に、オンライン販売者からの情報を電気通信ネットワークへ送る。別の実施形態において、販売者は、情報を直接、電気通信ネットワークへ送る。

【 0 0 2 1 】

相互運用領域104は、インターネットでサポート可能であり、信頼機関と要求者との両方に使用される構成要素を含む。

【 0 0 2 2 】

信頼機関領域103は、発行者口座保有者システム110と、加入サーバ112と、アクセス制御サーバ(ACS)114と、口座保有者ファイル118とを含む。システムが使用される特定の使用分野に応じて、信頼機関領域103には追加構成要素が含まれる。例えば、以下の支払取引では、支払取引に関して口座保有者の同一性を認証する目的で、それぞれの領域に追加構成要素が存在する。

【 0 0 2 3 】

加入サーバ112は、口座保有者が回答し、信頼機関が検証する一連の質問をwebインタフェース経由で提供することにより、口座保有者の口座認証システムへの加入を管理するコンピュータである。図1に示したように、信頼機関は、加入サーバ112を運用する。しかしながら、V i s a等のサービス組織は、信頼機関にかわって加入サーバ112を運用できる。信頼機関は、口座保有者の同一性の妥当性確認を支援するために、加入処理中に外部の団体が提供するweb対応の対話式「同一性認証サービス」を使用できる。

【 0 0 2 4 】

ACS114は、口座認証システムが提供する口座認証サービスに登録された口座保有者のデータベースを有するコンピュータである。ACS114は、各口座保有者の口座及びパスワード情報を含む。口座認証処理中、ACS114は、認証要求者にデジタル署名入り受取者を提供し、口座認証システムへのアクセスを制御し、口座保有者のサービスへの参加の妥当性を確認する。カード発行者、或いはV i s a等のサービス組織は、信頼機関のためにACS114を運用できる。口座認証サービスでは、何らかの追加口座保有者ソフトウェアを使用する必要はないが、随意的な口座保有者ソフトウェア及びハードウェアを配置してもよい。追加口座保有者ソフトウェアは、デジタル証明書、集積回路カード(チップカード)、及びチップカードリーダ等の追加的な認証手法をサポートできる。本

発明において、証明書を必要とする唯一のシステム参加者は、発行金融機関である。

【0025】

口座保有者ファイル118は、口座認証システムへの加入に成功した口座保有者に関する情報を格納するために、信頼機関が管理するデータベースである。発行者口座保有者システム110（又は信頼機関の口座保有者システム）は、信頼機関により制御され、口座保有者に関する情報を含む。こうした情報は、口座情報、口座保有者が利用するサービス等に関連する。発行者口座保有者システム110内の情報の一部は、口座保有者の口座認証サービスへの加入において使用できる。

【0026】

要求者領域105の要求者180は、通常、口座保有者の認証を希望する。関係者180は、認証プロトコルを円滑にする要求プラグインソフトウェア182を管理する。要求プラグインソフトウェア182は、第三の又は要求者のwebサイトに統合されるソフトウェアモジュールである。プラグインソフトウェアモジュール182は、口座認証システムと、要求者の処理ソフトウェア、例えば、販売者の支払処理ソフトウェアとの間のインタフェースを提供する。

【0027】

相互運用領域104は、ディレクトリサーバ128を含み、インターネットによりサポートされ、信頼機関と要求者との両方に使用される構成要素を含む。ディレクトリサーバ128は、要求者からの認証要求を、ACS114等の特定のACSへ送る。ディレクトリサーバ128は、カード体系管理者、或いはVisa等のサービス組織により運用される。相互運用領域104は、インターネット以外のネットワークでもサポートできる。

【0028】

支払取引の口座認証システム

次に、支払取引の分野において口座保有者を認証するためのシステムアーキテクチャについて説明する。支払用途の認証処理は非支払用途に類似するため、本節において説明する多数の一般的概念は、様々な使用分野へ応用できることに留意されたい。

【0029】

支払取引における認証システム及びプロトコルの使用例について以下に説明する。認証システムは、口座保有者がオンラインで買い物し、品目を「ショッピングカート」に追加し、オンライン販売者のチェックアウトページへ進み、オンライン販売者のチェックアウトフォームを記入する状況において有用となる。認証処理は、消費者が自分の希望する製品又はサービスの購入を決定した後、例えば、消費者が「購入」ボタンをクリックした後で行われる可能性がある。認証処理は、諸費者の支払取引における他の様々な時期に開始される可能性がある。認証処理は、支払ネットワークのいくつかのポイントに組み込まれたソフトウェアを利用することで、消費者にとって、殆どがトランスペアレントモードで実行される。システムは、認証サービスにより、口座保有者と口座保有者の金融機関との参加の妥当性確認を行う。その後、ウィンドウが作成され、ウィンドウの中で、口座保有者からの事前登録パスワードを要求することで、消費者は、自分の同一性を確認できる。消費者の同一性が確認された場合、支払情報と、消費者の認証の通知とが販売者へ返信される。その後、従来行われるように、販売者により支払取引が処理される。例えば、販売者は、注文確認メッセージを口座保有者のブラウザに送信してよい。

【0030】

図2は、支払取引における認証サービスをサポートするシステムアーキテクチャ200の一実施形態を模式的に示している。図1の一般的なシステムアーキテクチャ100と同様に、アーキテクチャ200は、三つの領域、即ち、発行者領域102、相互運用領域104、及び取得者領域106に分割される。図2の発行者領域102及び取得者領域106は、それぞれ図1の信頼機関領域103及び要求者領域105に類似する。

【0031】

発行者領域102は、加入サイト108と、発行者口座保有者システム110と、口座保有者クライアントデバイス122と、加入サーバ112と、アクセス制御サーバ(AC

S) 114と、発行者又は要求者同一性認証構成要素116と、口座保有者ファイル118とを含む。随意的に、発行者領域102は、承認口座保有者120の発行者ファイルを含むことができる。口座保有者は、利用者を示す別の用語であり、これは特定の同一性を有するものとして口座保有者が自らを提示するためである。加入サーバ112は、口座保有者が回答し、信頼機関が検証する一連の質問をwebインタフェース経由で提供することにより、口座保有者の口座認証システムへの加入を管理するコンピュータである。加入サーバ112は、インターネット支払ゲートウェイサービス124にインターネットを介して接続され、インターネット支払ゲートウェイサービス124は、次に電気通信ネットワーク126、例えば、ビザネット(VisaNet)に接続される。インターネット支払ゲートウェイサービス124により、加入サーバ112は、電気通信ネットワーク126と通信できる。支払ゲートウェイサービス124を介した接続により、加入サーバ112は、発行者の認証システム127に問い合わせを行い、加入中の口座保有者が有効なカード口座を有するかを判断できる。加入サイト108は、口座認証システムが提供する口座認証サービスに参加するために口座保有者が登録可能なインターネットwebサイトである。

【0032】

口座保有者クライアントデバイス122は、口座保有者が口座認証システムに参加するために使用する。具体的には、口座保有者クライアントデバイス122は、パーソナルコンピュータ、携帯電話、携帯情報端末、又はインタラクティブケーブルテレビ等、インターネットにアクセス可能な任意の機器にできる。一部の実施形態において、口座保有者クライアントデバイス122は、インターネットに接続できないが、しかしながら、インターネットに基づかないメッセージを処理可能な特殊なノードを介して、クライアントデバイス122からの入力及び出力メッセージが送られるため、こうしたデバイスも口座保有者により使用可能である。例えば、音声及び/又はテキストメッセージに基づくメッセージを送受信する携帯電話はインターネットに接続できないが、しかしながら、メッセージを異なる方法で送ることにより、口座認証システムで使用できる。ショートメッセージサービス(SMS)は、一般的に使用されるメッセージングシステムの例である。音声自動応答(IVR)ユニットは、音声チャネルを介した自動交換に使用できる。こうしたメッセージルーティングの仕組みについては、インターネット対応デバイスに関する以下の節において更に詳細に説明する。

【0033】

発行者口座保有者システム110は、口座保有者に関する情報を含む発行者制御システムである。このシステムの情報は、口座情報、口座保有者が利用するサービス等に関連する情報を含む。発行者口座保有者システム内の情報の一部は、口座保有者を口座認証システムへ加入させる処理において使用できる。

【0034】

発行者又は要求者同一性認証データベース116は、発行者又は要求者が口座保有者に関するファイル上に既に有している情報を含む。データベース116は、口座保有者を加入させるプロセスにおいて、口座保有者の同一性を検証するために、発行者により使用される。例えば、口座認証システムが提供するサービスへの登録に口座保有者が成功するためには、口座保有者登録処理中に口座保有者が入力した情報は、認証データベース116のファイル上に既に存在する情報と一致するべきである。エクイファクス(Equifax)のような会社を第三者にすることができる。

【0035】

相互運用領域104は、ディレクトリサーバ128と、認証履歴サーバ130と、受取マネージャ131とを含む。ディレクトリサーバ128は、要求者からの認証要求を特定のACSへ送る。ディレクトリサーバ128は、Visa等のサービス組織により運用される。認証履歴サーバ130及び受取マネージャ131は、署名入り受取書(例えば、以下に説明する支払要求応答メッセージのコピー)を認証済み支払取引毎に格納する。認証履歴サーバ130は、どの取引が認証されたかを検証する情報を含み、紛争解決処理中に

追加情報を提供する。認証履歴サーバ130及び受取マネージャ131は、サービス組織が運用する。発行者、取得者、又は販売者も、デジタル署名入り受取書のコピーを保持できる。

【0036】

取得者領域106は、販売者132と、妥当性確認サーバ136とを含む。MPI134は、販売者132の場所に常駐する。MPI134は、販売者の電子商取引webサイトに統合されるソフトウェアモジュールである。MPI134は、口座認証システムと、販売者の支払処理システムとの間のインタフェースを提供する。

【0037】

MPI134は、図1の要求プラグインソフトウェアモジュール182と同じソフトウェアモジュールであることに留意されたい。「販売者」という記述子は、MPI134に対して、プラグインソフトウェアモジュールを利用している要求関係者の種類を示すために使用している。しかしながら、本明細書全体で説明されるプラグインソフトウェアモジュールは、プラグインソフトウェアモジュール134を説明するために使用される形容詞にかかわらず、基本的には同じ形で機能すると理解されたい。本明細書全体での用語の使用を簡略化するため、「販売者」という形容詞は、プラグインソフトウェアモジュールを説明するために使用される。しかしながら、これは、販売者である要求関係者による使用のみに適したものであるとして、プラグインソフトウェアモジュール134を限定するものではない。更に、MPIは、販売者プラグインソフトウェアモジュールの頭文字として使用される。

【0038】

妥当性確認サーバ136は、支払取引中に口座認証システムが販売者に返送する受取書に署名するために使用されたカード発行者のデジタル署名を検証する。代替実施形態において、妥当性確認サーバ136の機能は、MPI134に含めてよい。別個の妥当性確認サーバ136の必要性は除去される。妥当性確認サーバ136は、販売者、取得者、又はサービス組織が運用する。

【0039】

一部の実施形態において、口座認証システムは、電子ワレット等の他の口座保有者アプリケーションとの相互運用が可能であり、サービスは、電子商取引マークアップ言語(EMVソフトウェア)に適合して運用できる。口座認証システムは、更に、紛争解決手順を実行する能力を提供する。例えば、販売者は、紛争の解決及びチャージバックの目的で、口座保有者の認証の証拠を提供するのに十分な情報を保持できる。

【0040】

設定及び登録の説明

次に、支払及び非支払取引の両方のための口座認証システムの設定について更に詳細に説明する。最初に、口座認証システムを使用できるように様々なシステム参加者を設定するのに必要な手順について説明する。次に、口座認証システムに登録するための口座保有者の処理について説明する。こうした段階を説明した後、支払取引の実際の認証についての説明を提供する。

【0041】

口座認証システムの設定は、システム内の全参加者のための設定手順を含む。設定手順は、一般に、支払及び非支払取引の両方の認証で同じである。こうした参加者には、販売者又は他の認証要求者といった団体と、金融機関又は他の信頼機関と、口座保有者とが含まれる。

【0042】

口座認証システムにサインアップしたオンライン販売者等の要求者は、図1のプラグインソフトウェアモジュール182及び図2のモジュール134のようなプラグインソフトウェアモジュールを受け取る。プラグインソフトウェアモジュールは、要求者が使用するコンピューティングプラットフォーム及びサーバソフトウェアに特有のものとするべきである。口座認証システムに参加する金融機関等の要求者は、カスタマイズした加入サイト

テンプレートに組み込むべきサービスロゴ及びマーケティングデザインを提供する。取得銀行である第三者は、更に、サービス組織認証局（C A）ルート証明書と、クライアント認証用のサービス組織認証局 S S L 証明書と、統合のサポートとを販売者に提供するべきである。

【 0 0 4 3 】

信頼機関は、口座認証システムを使用するための設定を可能とするために、信頼機関領域において指定された、全ての口座認証システムハードウェア及びソフトウェアのコピーを入手及びインストールするべきである。発行金融機関等の信頼機関は、更に、口座保有者同一性検証処理において使用されるべき同一性認証ポリシーと参加銀行識別番号（B I N）情報とを口座認証システムに提供する。随意的に、発行者は、口座保有者ファイル 1 1 8 への先行ロードのために、口座保有者認証情報を口座認証システムに提供できる。先行ロードは、大量の口座保有者のサポートを容易にする。例えば、信頼機関が口座保有者の全部又は大部分を口座認証サービスで有効にしたい場合、信頼機関は、個人識別番号（P I N 番号）を全ての口座保有者に送ることができる。その後、P I N 番号は、先行ロード済みパスワードにアクセスするために、各口座保有者が使用できる。この方法では、各口座保有者は正式な加入処理を通過する必要がないため、加入処理が迅速化される。口座保有者が先行ロード済みパスワードを初めて使用した後、口座所有者は、新たな覚えやすいパスワードを指定するオプションを有する。

【 0 0 4 4 】

口座保有者認証情報は、企業 I D、国コード、カード口座番号、カード有効期限、口座保有者名、「参加 B I N」データにおいて指定された発行者固有認証データ（例えば、母親の旧姓）といった情報と、請求先住所、発送先住所、社会保障番号、電話番号、勘定残高、取引履歴、及び運転免許証番号等、その他の情報とを含む。信頼機関は、更に、カード口座ポートフォリオに対する口座番号の範囲と、A C S の I P アドレス（U R L）とをディレクトリサーバへ提供するべきである。口座認証システムの支払での応用に関して、サービスは、口座保有者の登録が可能な、銀行ブランドの w e b サイトを介して提供できる。

【 0 0 4 5 】

図 3 は、一実施形態による、口座保有者が口座認証システムに登録する処理を示している。ステップ 1 に図示したように、口座保有者は、信頼機関、例えば、発行金融機関が維持する加入サーバインターネット w e b サイトを訪れる。口座保有者は、自分の口座番号を登録することで、口座認証システムに登録する。例えば、支払取引により、口座保有者は、自分のクレジットカード、チェックカード、又はデビットカードの口座番号を登録できる。非支払取引に関して、口座保有者は、保険又は仲買会社で保有する口座番号を登録できる。口座保有者は、一枚以上のカードを登録できる

【 0 0 4 6 】

ステップ 2 において、口座保有者は、主要口座番号（P A N）、名前、及びカード有効期限といった情報を入力する。この時点で、口座保有者は、追加情報を入力することもできる。例えば、住所、電子メールアドレス、買い物客 I D、口座検証値、口座保有者固有パスワード、及び発行者固有認証情報を更に入力できる。この情報は、図 4 に示したページ 3 0 0 のような加入 w e b サイトのページに入力できる。

【 0 0 4 7 】

要求された情報を口座保有者が加入サイト 1 0 8 に入力した後、口座認証システムは、信頼機関が相互運用領域 1 0 4 のディレクトリサーバ 1 2 8 に登録したカード範囲内に口座保有者の P A N が存在することを検証する。口座保有者の同一性は、様々な方法を使用して検証できる。第一に、先程述べたように、口座保有者の同一性は、要求者認証データベース、或いは信頼機関自身の認証データベースにより検証できる。追加として、検証は、信頼機関が提供する承認口座保有者 1 2 0 のファイルを使用し、状態チェック認証を信頼機関に送信し、応答を、金融機関が提供する先行ロード済み情報と比較することで実行できる。

【 0 0 4 8 】

P A Nが加入カード範囲に含まれない場合、加入は拒否され、加入処理は終了する。支払取引において、P A Nが加入カード範囲に含まれる場合、一ドル（又は他の任意の名目金額）の認証を、V i s a N e t等のサービス組織支払ネットワークを介して発行金融機関に提出する。一ドル取引の認証により、発行者は、カード口座状態を検証し、住所検証サービスを使用して住所を検証し、口座保有者検証値2（C V V 2）を検証できる。C V V 2は、支払カード裏面の署名欄に印刷された三桁の数字である。非支払取引では、P A Nが加入カード範囲に含まれる場合、一ドル取引は必要ない。

【 0 0 4 9 】

ステップ3において、口座保有者は、口座保有者の同一性対話式のリアルタイムオンラインセッションで検証するために、追加認証情報を求められる。一部の実施形態において、口座保有者は、認証取引中に口座保有者を認証するのに使用されるパスワードと「ヒントの質問及び回答」のペアとの入力を要求される。

【 0 0 5 0 】

ステップ4において、口座保有者の同一性が検証され、適切な応答が返送されると、認証メッセージが発行金融機関に送信される。次に、ステップ5において、加入サーバ112は、口座保有者情報をA C S 1 1 4に渡し、口座保有者ファイル118内の記録を設定する。口座保有者ファイル118は、金融機関B I N番号、口座番号、有効期限、姓名、運転免許証番号、請求先住所、社会保障番号、口座保有者のパスワード、口座保有者のパスワードの質問、口座保有者のパスワードの回答、口座保有者の電子メールアドレス、要求者の同一性スコア、その他の情報を格納できる。

【 0 0 5 1 】

一部の実施形態において、登録処理中、口座保有者には、個人保証メッセージ（P A M）と呼ばれる語句の入力を求めることができる。P A Mは、認証処理中に、信頼機関が口座保有者に後で提示する。信頼機関のみが口座保有者の指定P A Mを知っているため、口座保有者に対して、口座認証システムで使用されるダイアログウィンドウが信頼機関から供給されたことを保証できる。P A Mの例は、「空は青い」である。

【 0 0 5 2 】

口座保有者は、認証システムを使用するために、新しいクライアントソフトウェア又はデバイスを必要としないことに留意されたい。好適な実施形態において、口座保有者登録処理では、口座保有者と加入サーバとの間でインターネットを介して送信されるデータを保護するために、S S Lチャネル暗号化等のセキュリティプロトコルを利用する。

【 0 0 5 3 】

更に、登録又は加入処理中、各信頼機関は、独自の「利用規約」及び/又は「データプライバシーポリシー」を表示できる。各信頼機関は、登録処理を完了するために、登録中の口座保有者に規約及びポリシーの承諾又は拒否のいずれかを求める能力を有する。各口座保有者が承諾した「利用規約」及び/又は「データプライバシーポリシー」のバージョン番号は、信頼機関が保存するべきである。

支払取引の説明

【 0 0 5 4 】

全ての参加者を設定し、口座保有者が登録した後、口座認証が実行される。図5は、口座保有者がインターネットに接続されたコンピュータを使用する、中心的な口座認証システムを使用した認証支払取引を説明している。図5のステップ1において、口座保有者は、インターネット上の販売者の電子商取引サイトを訪れる。支払取引では、口座保有者が保持する最も一般的なタイプの口座は何らかのクレジット、デビット、又はチェックカード口座であるため、口座保有者は、カード保有者と呼ぶこともできる。口座保有者が購入を希望する製品又はサービスを選択した後、口座保有者は、チェックアウト処理を開始し、チェックアウトフォームを記入し、その後、「購入」ボタンをクリックする。

【 0 0 5 5 】

「購入」ボタンを選択した後、図5のステップ2に図示したように、M P Iが始動され

、検証処理を実行して、口座保有者の固有口座が口座認証システムに登録されているかを判断する。MPIは、口座保有者が口座認証システムに登録されているかを様々な方法で判断できる。例えば、口座保有者に関連するディレクタサーバ及びACSをチェックする二段階処理と、ACSのみをチェックする処理と、ディレトリサーバに保持されているものと同じ情報を含むキャッシュメモリを販売者がチェック可能な方法とを使用できる。

【0056】

二段階処理について説明する。この説明では、図2を参照する。第一のステップにおいて、MPIは、カード口座番号を識別し、ディレクタサーバ128に問い合わせを行って、口座番号が口座認証システムの参加者である発行銀行に関連する番号の範囲内にあることを検証する。口座番号がディレトリサーバ128で定義された口座番号範囲内に存在しない場合、発行者は登録されておらず、したがって口座保有者も登録されていない。この場合、口座番号が登録されていないことを販売者に通知し、MPI134は、取引の制御を販売者の店頭ソフトウェアへ戻す。この時点で、販売者の店頭ソフトウェアは、通常通りに取引を進めること、口座保有者に対する更なるサービスを拒否すること、或いは、代替の支払方法で継続することが可能となる。

【0057】

一方、口座番号がディレトリサーバ128に存在する口座番号の範囲内にあると判断された場合、検証処理の第二のステップが開始される。検証処理の第二のステップは、口座番号が加入しているかを判断するためにディレトリ128が口座番号をACSへ送信した時に開始される。カードが加入していない場合、加入処理は終了される。カードが加入していることをACSが示した場合、ACSは、ディレトリサーバを介して、URLインターネットアドレスをMPIへ返送する。次に、MPIは、口座保有者クライアントデバイス及びその常駐ブラウザを介して、ACSを呼び出す。ここでも、口座認証システムに多数のACSが存在可能であることに留意されたい。

【0058】

口座保有者が口座認証システムに登録されているかをチェックする第二の方法では、MPI134が、最初にディレトリサーバ128に問い合わせることなく、直接ACS114に問い合わせる。第三の方法では、上記の通り、販売者は、ディレトリサーバ128に保持されているものと同じ情報を含むキャッシュメモリを有する。これにより、販売者は、少なくとも予備的なチェックを実行できる。

【0059】

二台以上の物理的ディレトリサーバが口座認証システムに存在可能であることに留意されたい。しかしながら、論理的ディレトリサーバが一台のみ存在することが好ましい。言い換えると、全てのディレトリサーバは、同じ情報を含むという点において一致するべきである。

【0060】

口座保有者が口座認証システムの参加者である場合、ACS114は、口座保有者に対して銀行ブランドのウィンドウを表示する。銀行ブランドのウィンドウは、基本的な支払取引情報を含み、口座保有者に認証パスワード又はトークンを求める。口座保有者に認証パスワードを求める例示的なウィンドウ500については図6を参照されたい。口座保有者は、自分の認証パスワードを入力し、ACS114は、認証パスワードを検証する。ウィンドウ500のサイズ及びレイアウトは、口座保有者が使用するデバイスのパラメータに応じて変化する。現在、一般的であるように、口座保有者は、認証パスワードの正確な入力を特定の回数だけ試行できる。口座保有者が認証パスワードを正確に入力できない場合には、口座保有者の登録処理中に設定されたヒント質問により、口座保有者に指示できる。好ましくは、口座保有者は、ヒント質問に対して正しい回答を入力する機会を一度与えられる。

【0061】

正しい認証パスワード又はトークンが即座に入力された場合、或いは口座保有者がヒント質問に対して正しい応答を提供した場合、支払認証は継続する。次に、ACSは、発行

者の署名キー又はサービスプロバイダのキーを使用した受取へのデジタル署名へ進む。この受取書は、販売者名、カード口座番号、支払額、及び支払日を含む。一部の実施形態において、受取書は、支払認証応答 (P A R e s) メッセージのコピー、或いは P A R e s メッセージからコピーされた情報フィールドの少なくとも一部を有するメッセージである。認証履歴サーバ 130 は、取引データとして、販売者名、販売者 URL、カード口座番号、有効期限、支払額、支払日、発行者の支払署名、及び口座保有者の認証検証値を格納する。ACS は、口座保有者のブラウザを介して、口座保有者を MPI へリダイレクトする。この時点で、ACS は、販売者に対して、デジタル署名済み受取書と、口座保有者が認証された否かについての決定とを渡す。妥当性確認サーバ 136 は、取得者領域 106 において、支払受取書の署名に使用されたデジタル署名を検証するために、MPI 134 に使用される。デジタル署名の検証後、口座保有者は、「認証済み」と見なされる。一部の実施形態において、取引完了後、口座保有者は、更に、自分のカード口座を再登録し、将来のオンライン購入で使用する新しいパスワードを作成する能力を有する。

【0062】

ステップ 3 において口座保有者が認証された後、ステップ 4 では、特定の口座保有者の口座を許可する処理を開始する。許可とは、口座保有者が十分な信用を有し、特定の購入について良好な状態にあることを検証する処理を示す。対照的に、認証とは、口座保有者の同一性を検証する処理を示す。ステップ 4 において、販売者は、MPI を使用して、許可メッセージを Visa Net 等の支払ネットワークへ送信する。支払ネットワークは、次に、許可メッセージと電子商取引インジケータ (E C I) とを、発行金融機関へ転送する。許可メッセージは、この技術で一般に知られているものと同様である。許可メッセージは、特定の口座が良好な状態にあり、支払取引の要求購入額に対して十分なクレジットラインを有することを発行金融機関が販売者に対して検証できるように、発行者へ送信される。ECI は、インターネットを介して取引が完了したことを示し、メッセージセキュリティ (即ち、心配のないチャネル暗号化 (S S L)) のレベルと使用された認証とを示す。

【0063】

代替の実施形態において、販売者は、追加情報を許可メッセージと共に提供できる。例えば、更に送信できる情報は、口座保有者が認証に成功したかを示すフラグと、口座情報と、デジタル署名と、口座保有者検証値 2 と、取引識別子と、チップカード Europa y、Master card、及び Visa (E M V) 暗号文で認証されたオフライン P I N と、販売者に保証された支払を提供するのに必要なフィールドとである。発行金融機関の許可取引処理が完了した後、支払取引の制御は、支払ネットワークを介して、販売者の店頭ソフトウェアへ戻される。次に、発行者は、支払ネットワークを介して、許可応答を販売者へ返送する。図 5 のステップ 5 において、発行金融機関は、取引を許可又は拒絶する。一部の実施形態において、許可メッセージは、バッチ処理を行って、後の時点でまとめて送信できる。認証情報は、バッチ許可メッセージにも含まれる。

【0064】

取引識別子は、口座保有者を認証した ACS により作成され、一定の支払カードと、そのカードからの特定の支払取引とに固有の値である。発行者は、後に紛争が生じた時等、様々な目的で、取引識別子を使用して認証済み支払取引を一意に識別する。取引識別子は、特定のオンライン取引に関連するもの等、記録を一意に識別するのに適した多数のデータ形態を取ることが可能である。支払取引等、いくつかの実施の一つにおいて、取引識別子は、カード認証検証値 (C A V V) である。以下の説明において、取引識別子は C A V V と呼ばれる場合があるが、しかしながら、様々な種類の処理識別子も利用できることに留意されたい。

【0065】

アクセス制御サーバ (A C S) 114 は、他の様々な機能が可能である。例えば、ACS は、登録口座をデータベースから無効化できる。口座は、口座保有者又は発行者が、手動で無効化できる。ACS 114 は、口座保有者が交換用カードを受取時に、簡略化され

た更新登録処理を提供できる。ACS 114は、固有のアクセス制御情報を備えた、同じ登録口座の多数のユーザをサポートできる。支払取引又は口座更新のために、ユーザにACS 114への接続を提供する時、ACS 114は、パスフレーズ、デジタル署名、オンラインPIN番号、及び/又はチップカードEMV暗号文のオフラインPIN番号の一つ以上の機構を介して、登録口座の許可口座保有者として、ユーザの妥当性を確認できる。

【0066】

販売者132は、販売者がファイル上に口座保有者の口座情報を有する既存のシステムとの相互運用を行い、既存の販売者許可及び結成システムとの相互運用を行い、多数の販売者にサービスを提供する第三者をサポートし、販売者及び取得者間の様々な支払インタフェースをサポートし、電子商取引インジケータ(ECI)の値を設定する時に、取得者から支払ネットワーク許可メッセージに対する強制的な影響を最小化することができる。

【0067】

取引を販売者からACSへ送る一方法は、口座保有者の口座番号に基づいてサーバのアドレスを提供するディレクトリを有することである。こうした方法において、情報を送る要求は、認証された販売者からのみ受け付けられる。販売者からのアクティビティが、正常なアクティビティを上回る場合、口座認証システムは、アクセスが有効でなくなったことを示す取得者を有する販売者に対して、アクセスを拒否できる。これは、販売者の詐欺があり得るとみなされた場合に該当する。口座認証システムには販売者認証を配備可能だが、配備は必須ではない。販売者認証は、販売者の詐欺を最小化するのに役立つ。

【0068】

図7は、一実施形態による、消費者がインターネットに接続されたコンピュータを使用する、中心的な口座認証システムを使用した支払取引中に送信される、具体的なメッセージを示している。図7のメッセージは、図2に示した支払システムアーキテクチャに重ねている。メッセージと、それぞれのメッセージ内のデータフィールドとは、具体的な名称が記載されているが、こうした名称は認証プロトコルの性能に影響しないことを理解されたい。したがって、以下に説明するメッセージ及びデータフィールドには様々な名称を割り当て可能である。更に、本発明の代替実施形態において、図7において説明した具体的なメッセージは、変更又は省略が可能であり、及び/又は、認証プロセスの全体的な目標に影響を与えることなく、追加メッセージを追加できる。機能の追加及び通信の合理化といった様々な目的で、様々なメッセージを変更、追加、又は省略できる。更に、本明細書全体で説明するプロセスのメッセージフローは、代替実施形態において、上記のような利用で変更可能である。

【0069】

上記のように、支払取引は、口座保有者がブラウザを介して販売者のwebサイトを訪問し、購入する品目を選択した時に開始される。販売者の支払システムは、口座保有者に支払情報の入力を求める。一般に、支払情報の入力は、安全な環境で、例えば、SSL暗号化プロトコルを使用して行われるべきである。口座保有者が取引を確定させる準備が出来たことを示した時、販売者の支払システムは、MPI 134を呼び出す。次に、線1aにより示したように、MPI 134は、口座保有者のPANを含み得るACSの特定のURLについてディレクトリサーバ128をチェックし、口座保有者がサービスに加入していることを検証する。代替として、MPI 134は、この情報を含む自らのキャッシュメモリをチェックする。MPI 134は、更にACS 114をチェックし、口座保有者のPANが口座認証システムに登録されていることを検証する。MPI 134が自分のキャッシュをチェックできる場合、MPI 134は、ディレクトリ128の内容をローカルキャッシュにコピーする能力を有するべきである。この能力を使用する場合、販売者は、口座が加入範囲の一部であるかをキャッシュから即座に判断できる。販売者がこの機能を実施する場合、キャッシュの内容は、少なくとも24時間毎に期限切れとなり、更新されるべきである。キャッシュは、MPI 134がロードされた時、及びその後一定時間毎に要求されるべきである。

【0070】

M P I 1 3 4 は、口座保有者の P A N を使用して検証加入要求 (V E R e q) をフォーマットすることで、P A N を検索する。既に確立されていない場合、M P I 1 3 4 は、ディレクトリサーバ 1 2 8 又は A C S 1 1 4 との安全な接続を確立し、これらに対して自らを認証する。M P I 1 3 4 は、様々な位置で、口座保有者の P A N に対応するカード範囲エントリを検索する。

【 0 0 7 1 】

M P I 1 3 4 が検索を実行した後、V E R e q メッセージは、線 1 b に示したように直接的に、或いは、線 1 b に示したように最初にディレクトリサーバを通過した後、A C S 1 1 4 へ送信される。V E R e q メッセージがディレクトリサーバ 1 2 8 を介して A C S 1 1 4 へ送信された後、ディレクトリサーバ 1 2 8 は、V E R e q メッセージに含まれる口座保有者の P A N に対応するレコードを検索する。一致が不成功である場合、ディレクトリサーバ 1 2 8 は、U R L 値 (群) 無しで検証加入応答 (V E R e s) メッセージをフォーマットし、P A N 加入のステータス又は V E R e s ステータスの値を「N」に設定する。V E R e s メッセージは、その後、M P I に戻される。一方、一致に成功した場合、既に確立されていない場合、ディレクトリサーバ 1 2 8 は、A C S の U R L との安全な接続を確立し、これに対して自らを認証する。その後、V E R e q メッセージは、A C S の U R L に転送される。その U R L が利用できない場合、M P I は、(可能な場合) 次の A C S の U R L 値に進み、最大五個の A C S の U R L の検索を可能にするべきである。当然ながら、試行される U R L の数は可変である。全ての試行で不成功となった場合、V E R e s メッセージは、口座認証システムを使用して支払取引が処理できないことを販売者に対して示すために、V E R e s ステータスが「N」に設定された状態で、M P I に戻される。

【 0 0 7 2 】

V E R e q メッセージが A C S 1 1 4 に受け取られた後、A C S は、V E R e q メッセージから口座保有者の P A N を受け付け、口座保有者ファイル 1 1 8 に照らして検証する。一致が成功した場合、A C S は、P A N 加入のステータスを「Y」に設定し、A C S 1 1 4 が内部的に P A N に関連付けるシングルユースのプロキシ P A N を作成し、U R L フィールド (群) を V E R e q メッセージ内に配置する。一致が不成功である場合、A C S は、P A N 加入のステータスを「N」に設定する。したがって、線 2 a に示したように、A C S は、ディレクトリサーバ 1 2 8 を介して、V E R e s メッセージを M P I へ戻される。V E R e q メッセージが A C S へ直接送信される場合、V E R e s メッセージは、線 2 b に示したように、M P I へ直接返送される。

【 0 0 7 3 】

ディレクトリサーバ 1 2 8 のデータを M P I 1 3 4 でキャッシュすることにより、C R R e q 及び C R R e s メッセージペアの利用を容易にできる。C R R e q メッセージは、M P I のキャッシュを更新するために、M P I からディレクトリサーバへ送信され、関与するカード範囲のリストを要求する。C R R e s メッセージは、関与する範囲を含む応答である。

【 0 0 7 4 】

一部の実施形態において、口座認証システムは、Q u e r y A c c o u n t h o l d e r R e q 及び Q u e r y A c c o u n t h o l d e r R e s メッセージペアを使用して分散認証能力を口座保有者のクライアントデバイスが有するかを確認する。M P I は、クエリである Q u e r y A c c o u n t h o l d e r R e q メッセージを口座保有者クライアントデバイス 1 2 2 に対してフォーマット及び送信し、分散口座認証用口座保有者モジュールが常駐しているかを判断する。Q u e r y A c c o u n t h o l d e r R e q メッセージの送信は、線 3 により図 7 に図示している。任意の分散認証オプションが Q u e r y A c c o u n t h o l d e r R e s メッセージにより戻された場合、M P I は、口座保有者クライアントソフトウェアと直接通信し、認証ステップを実行する。Q u e r y A c c o u n t h o l d e r R e s メッセージの送信は、線 4 により図 7 に図示している。追加として、Q u e r y A c c o u n t h o l d e r R e q 及び Q u e r y A

ccount holder Resメッセージを使用することで、以下に説明する V E R e q 及び V E R e s メッセージを除去してよい。口座保有者クライアントソフトウェアは、発行者の A C S の U R L をソフトウェアに埋め込んで配置できる。M P I は、Q u e r y A c c o u n t h o l d e r R e q 及び Q u e r y A c c o u n t h o l d e r R e s メッセージを最初に完了させる。口座保有者クライアントソフトウェアが検出された場合、V E R e q 及び V E R e s メッセージを実施することなく、P A R e q メッセージを A C S 又は口座保有者クライアントソフトウェアに送信できる。

【0075】

V E R e s ステータスが「Y」に等しくない値を有する場合、販売者には、口座認証システムを使用して支払取引を処理できないことが通知される。しかしながら、V E R e s ステータスが「Y」の値を有する場合、M P I 1 3 4 は、支払認証要求メッセージ (P A R e q) をフォーマットする。M P I 1 3 4 は、線 5 に示したように、口座保有者クライアントデバイスブラウザを介して、P A R e q メッセージを発行者の A C S サーバへ送信する。

【0076】

M P I が P A R e q メッセージを発行者の A C S に渡した後、A C S は、口座保有者に対してウィンドウを表示する。ウィンドウは、支払認証応答 (P A R e q) メッセージに含まれる支払の詳細を、発行者のロゴ、サービス組織のマーク又はブランドロゴ、販売者名、販売者の場所 (U R L)、合計購入金額及び通貨、購入日、カード番号、分割 / 定期循環支払条件、注文に関する説明又は説明へのリンク、販売の特殊条件又はこの情報へのリンク、個人保証メッセージ、口座保有者のパスワード又は他の任意の種類の認証トークンの要求といった他の項目に加えて表示する。

【0077】

A C S は、口座保有者に適切なパスワードの入力を求める。A C S は、口座保有者の入力を受け付け、口座保有者ファイル 1 1 8 に照らして検証する。口座認証システムでは、例えば、正しいパスワードを入力する試行の失敗を一定回数 (例えば、三回) 認める。当然ながら、認める試行回数は変更できる。最終の試行失敗後、口座認証システムは、ヒント質問を表示してよい。口座保有者は、正しいヒント質問の応答を入力する必要がある。その後、口座保有者に関連するヒント質問が表示される。口座保有者は、正しい応答の入力を少なくとも一度試行できる。口座保有者が不正確な応答を提供した場合、口座認証システムを使用した取引を完了できないことを販売者に通知できる。口座保有者が正しい応答を提供した場合、パスワードが一致したかのように取引を処理するべきである。口座番号に対して二つ以上のエントリが存在する場合には、様々な口座保有者名がドロップダウンウィンドウに表示されることに留意されたい。その後、口座保有者は、自分の名前を選択できる。

【0078】

パスワードの一致後、A C S は、P A R e s メッセージを作成してデジタル署名する。A C S は、更に、S a v e R e c e i p t メッセージを生成し、線 7 で示したように、認証履歴サーバ 1 3 0 及び受取マネージャ 1 3 1 に送信する。線 7 a で示したように、S a v e R e c e i p t メッセージは、発行者がリアルタイムで支払許可要求と支払者認証取引とを照合できるように、認証履歴サーバ 1 3 0 から発行者許可及び清算システム 1 3 8 へ渡してもよい。S a v e R e c e i p t メッセージを発行者許可及び清算システム 1 3 8 へ送信することで、発行者は、認証要求が認証済みの購入に関するものかを同時に判断できる。次に、A C S は、線 6 で示したように、署名済みの P A R e s メッセージを M P I へ再びリダイレクトする。

【0079】

署名済み P A R e s メッセージを M P I 1 3 4 へ返送した後、M P I 1 3 4 を再始動させる。認証ステータスが「Y」である場合、M P I 1 3 4 は、P A R e s メッセージを妥当性確認サーバ 1 3 6 へ送信する。妥当性確認サーバの機能が M P I 1 3 4 によって提供される場合、M P I 1 3 4 は、P A R e s メッセージの署名の妥当性を確認し、署名妥当

性確認の結果を戻す。署名の妥当性が確認できない場合、M P I 1 3 4 は、口座認証システムを使用して取引を処理できないことを販売者に通知する。認証ステータスが「N」である場合、販売者は、口座保有者に追加情報を求めるプロンプトを送信するか、異なる支払カード又は支払い形態を使用することを口座保有者に要求するか、或いは非認証支払取引として支払取引を処理するべきである。

【 0 0 8 0 】

取得者領域 1 0 6 が妥当性確認サーバを含む場合、妥当性確認サーバ 1 3 6 は、P A R e s メッセージの署名の妥当性を確認する。妥当性確認サーバ 1 3 6 は、その後、署名妥当性確認の結果を M P I 1 3 4 へ戻す。署名の妥当性が確認できない場合、M P I は、口座認証システムを使用して取引を処理できないことを販売者に通知する。一方、署名の妥当性が確認された場合、販売者は、認証支払の許可を進める。P A R e s メッセージは、線 6 a で示したように、販売者から取得者支払プロセッサ 1 4 0 に渡してもよい。P A R e s メッセージは、その後、取得者から電気通信ネットワーク 1 4 2 を介して、発行者へ渡してよい。したがって、支払者認証結果は、標準の支払許可プロセスの一部として、発行者が利用可能になる。

【 0 0 8 1 】

次に、様々な伝送チャネルに関連するセキュリティ問題について説明する。基本線として、全ての伝送チャネルは、好ましくは、1 2 8 ビット S S L を使用して暗号化される。口座保有者と販売者との間のチャネルは、二つのチャネルを含む。販売者は、サービス組織が承認した認証局から入手した S S L 証明書を使用して、口座保有者が支払情報を入力する時に使用される接続を確保するべきである。販売者は、更に、サービス組織が承認した認証局から入手した S S L 証明書を使用して、P A R e s メッセージを口座保有者から M P I へ転送する時に使用される接続を確保するべきである。

【 0 0 8 2 】

口座保有者と A C S との間のチャネルは、サービス組織が承認した認証局から入手した S S L 証明書を使用して、A C S によって暗号化されるべきである。このチャネルは二つの目的で使用される。第一に、P A R e q メッセージを M P I から A C S へ送信するためであり、第二に、署名済み P A R e s メッセージを A C S から口座保有者へ送信するためである。

【 0 0 8 3 】

口座保有者と加入サーバとの間のチャネルは、サービス組織が承認した認証局から入手した S S L 証明書を使用して、加入サーバによって暗号化されるべきである。このチャネルは、口座保有者の加入情報を受け付けるのに使用される。

【 0 0 8 4 】

販売者とディレクトリサーバとの間、及びディレクトリサーバと A C S サーバとの間のチャネルは、V E R e q 及び V E R e s メッセージに含まれる P A N データと、V E R e s メッセージに含まれる A C S の U R L アドレスとを保護するために、サービス組織が発行した S S L 暗号化証明書により確保するべきである。

【 0 0 8 5 】

A C S と口座保有者との間のチャネルは、口座保有者のパスワードに対するプロンプトと、口座保有者が入力したパスワードとを保護するために暗号化されるべきである。このチャネルは、サービス組織が承認した認証局から入手した S S L 証明書により保護されるべきである。

【 0 0 8 6 】

殆どの取引について、支払認証要求及び応答メッセージは、一部として、メッセージバージョン番号と、販売者識別子と、販売者国コードと、注文番号と、購入日と、購入額と、取引ステータスと、購入条件とを含むフィールドを含んでいる。更に、Q u e r y A c c o u n t h o l d e r R e s メッセージは、通常、一部として、メッセージバージョン番号、販売者名、注文番号、購入日、購入額、カード有効期限、取引ステイン等のフィールドを含む。こうしたメッセージは、X M L (拡張マークアップ言語) 形式にできる。

【 0 0 8 7 】

非購入認証取引において、支払認証要求、支払認証応答、及び Query Account holder Res メッセージは、メッセージ拡張フィールドを含むことができる。この技術において周知であるように、メッセージ拡張フィールドは、拡張を添付するメッセージに関する追加要素を定義するデータフィールドである。こうした追加要素は、非支払取引を含む特定の取引を更に容易にするために使用できる。

【 0 0 8 8 】

付加価値提供構成要素による口座認証処理

図 8 は、付加価値提供の態様を含むオンライン口座認証に関連するシステムアーキテクチャの例と、一組のメッセージフローとを示す。付加価値提供の態様は、口座認証処理を介して数周した情報を付加価値提供者と共有することに関与する。こうした情報は、利用者に関係し、発行者又は信頼機関及び要求者が収集可能である。利用者情報は、利用者 1 2 2 の認証の根拠として供給されるため、高い完全性という価値を有する。利用者情報は、特定のオンライン取引を識別し、情報が本発明の認証処理に由来することを示す取引識別子によりマーク付けできる。付加価値提供情報は、一部の例として、出荷、後続販売、セキュリティチェック、及びワークフロー管理に関連する様々な目的で、付加価値提供者 1 9 6 が使用できる。関与する全関係者は、利用者情報を共有から利益を享受可能であり、各関係者は、価値の取得を互いにどのように支援できるかについて合意できる。例えば、要求者と付加価値提供者とは、利用者情報の共有に基づく追加契約条項に合意できる。

【 0 0 8 9 】

次に、利用者情報を付加価値提供者 1 9 6 へ送信することを含む認証処理について、図 8 を参照して説明する。図 8 について、支払取引に基づいて説明する。この説明に続いて、図 8 を、非支払取引に基づくものとして更に説明する。図 8 は、図 7 のメッセージを簡略化した形態で表している。

【 0 0 9 0 】

図 8 の口座認証システムアーキテクチャは、発行者領域 1 0 2 と、相互運用領域 1 0 4 と、取得者領域 1 0 6 と、付加価値提供領域 1 0 7 とを含む。発行者領域 1 0 2 は、利用者 1 2 2 と、ACS 1 1 4 と、発行者 1 9 0 とを含む。利用者 1 2 2 は、人間の利用者と、利用者クライアントデバイス、例えば、コンピュータ端末又はモバイルコンピューティングデバイスとを表す。発行者 1 9 0 は、利用者 1 2 2 に対して支払カードを発行可能なカード発行銀行を表す。相互運用領域 1 0 4 は、この例において Visa によって制御されるディレクトリである Visa ディレクトリ 1 2 8 と、認証履歴サーバ 1 3 0 と、Visa Net 1 9 4 とを含む。取得者領域 1 0 6 は、要求者 1 3 2 と、MPI 1 3 4 と、取得銀行 1 9 2 とを含む。要求者 1 3 2 は、様々な種類の関係者にできるが、しかしながら、要求者 1 3 2 は一般に販売者であるため、販売者という用語を要求者の代わりに使用できる。付加価値提供領域 1 0 7 は、付加価値提供者 1 9 6 と、付加価値制御サーバ 1 9 8 とを含む。

【 0 0 9 1 】

図 8 の支払取引は、番号 1 乃至 1 4 の方向矢印により説明する。支払取引は、ステップ 1 において、利用者が販売者の web サイトをブラウズし、購入を希望する品目をショッピングカートに追加し、購入を確定する時に開始される。この時点で、販売者 1 3 2 は、PAN、有効期限、及び住所情報を含め、支払取引を続けるのに必要なデータを有している。

【 0 0 9 2 】

ステップ 2 において、MPI 1 3 4 は、利用者の主要口座番号（該当する場合は、更にデバイス情報）を Visa ディレクトリサーバ 1 2 8 へ送信し、利用者の PAN が口座認証システムに加入しているかをチェックする。この処理は、販売者チェックアウト処理中、利用者からの最終の「購入」クリック確認後に発生する。「購入」クリックが行われた後、販売者のソフトウェアは、MPI 1 3 4 を呼び出し、検証加入要求（VEReq）メッセージをフォーマットする。MPI 1 3 4 は、現在、Visa ディレクトリサーバ 1 2

8との安全な接続を有しているかを判断する。安全な接続が確立されていない場合、M P I 1 3 4は、V i s aディレクトリサーバ1 2 8とのS S L接続を確立する。販売者1 3 2がS S Lクライアント証明書を発行したことをV i s aディレクトリサーバ構成が示す場合、V i s aディレクトリサーバ1 2 8は、販売者1 3 2に対して、S S Lセッションの確立中にS S Lクライアント証明書を提示することを求める。安全な接続が確立された後、M P I 1 3 4は、V E R e qメッセージをV i s aディレクトリサーバ1 2 8へ送る。様々な実施形態において、様々な購入注文確認処理を使用して「購入」クリック確認を完了できることに留意されたい。

【0093】

V E R e qメッセージは、認証処理中に送信される他の任意のメッセージと共に、オンライン認証処理が付加価値提供者との利用者情報の共有を伴うことを表すインジケータを含むことができる。

【0094】

ステップ3において、関与するカード範囲内にP A Nが存在するとV i s aディレクトリサーバ1 2 8が判断した場合、V i s aディレクトリサーバ1 2 8は、A C S 1 1 4等の適切なA C Sへの問い合わせを行い、P A Nについて認証（又は認証の試行の証明）が可能であるかを判断する。この処理は、V i s aディレクトリサーバ1 2 8がM P I 1 3 4からV E R e qメッセージを受取した後で発生する。

【0095】

関与するカード範囲内にP A Nが存在することをV i s aディレクトリサーバ1 2 8が検証するために、V i s aディレクトリサーバ1 2 8は、V E R e qメッセージの構文の妥当性を確認し、妥当性確認に失敗した場合にエラーを返す。V i s aディレクトリサーバ1 2 8は、V E R e qメッセージデータの妥当性を確認し、特定の要件が満たされることを確定する。第一に、取得者B I Nは、参加取得者を表すべきである。第二に、販売者I Dは、取得者B I Nによって特定された取得者の参加販売者を表すべきである。第三に、取得者のV i s a領域で、口座認証サービスのために販売者のパスワードが必要となる場合、パスワードの値が受け取られているべきであり、パスワードは、取得者B I Nと販売者I Dとの組み合わせに対して有効となるべきである。こうした要件のいずれかが満たされない場合、V i s aディレクトリサーバ1 2 8は、「N」に設定されたP A N認証可能性と、無効要求メッセージとを含む検証加入応答（V E R e s）をフォーマットする。このV E R e sは、口座識別子、A C SのU R L、及び支払プロトコルのデータフィールドを含まないことに留意されたい。V i s aディレクトリサーバ1 2 8がV E R e sメッセージをM P I 1 3 4へ返した後、支払取引は、様々な形で進む可能性がある。例えば、支払取引は完全に終了する可能性があり、支払取引は非認証取引として進む可能性があり、或いは、利用者は異なる口座番号の使用を試行できる。

【0096】

V i s aディレクトリサーバ1 2 8は、V E R e qメッセージにおいて受け取った利用者P A Nを含むカード範囲を指定するレコードを検索する。利用者P A Nが見つからない場合、V i s aディレクトリサーバ1 2 8は、「N」に設定されたP A N認証可能性を含み、口座識別子、A C SのU R L、支払プロトコル、及び無効要求のデータフィールドを含まないV E R e sメッセージをフォーマットする。その後、V i s aディレクトリサーバ1 2 8は、V E R e sメッセージをM P I 1 3 4へ返送し、口座認証は、以下説明するように、再び停止可能点に達する。

【0097】

利用者P A NがV i s aディレクトリサーバ1 2 8において見つかった場合、V i s aディレクトリサーバ1 2 8は、現在、適切なA C Sとの安全な接続を有しているかを判断する。安全な接続が確立されていない場合、V i s aディレクトリサーバ1 2 8は、A C SとのS S L接続を確立する。V i s aディレクトリサーバ1 2 8のS S Lクライアント証明書と、A C Sのサーバ証明書とについては、S S Lセッションの確立中に提示及び妥当性確認が行われるべきである。試行された第一のU R Lが利用できない場合、連続する

各URL値が試行される（提供された場合）。Visaディレクトリサーバ128は、各ACSに対して随意的に構成可能な四つまでの代替URLへの接続を試行できる。Visaディレクトリサーバ128がそれぞれの試行でURLに接続できない場合、Visaディレクトリサーバ128は、「N」に設定されたPAN認証可能性を含むが、口座識別子、ACSのURL、支払プロトコル、又は無効要求のデータフィールドを含まないVEResメッセージをフォーマットする。その後、Visaディレクトリサーバ128は、VEResメッセージをMPI134へ返送し、口座認証処理は停止可能点に達する。

【0098】

URLとの接続に成功した後、Visaディレクトリサーバ128は、VEReqメッセージからパスワードフィールドを除去し、メッセージをACSのURLへ転送する。

【0099】

ステップ4において、ACS114は、PANに関する認証が可能であるかを判断し、その後、Visaディレクトリサーバ128に対して判断を示す。この処理は、ACSがVisaディレクトリサーバ128を介してVEReqメッセージを受取後に発生する。ACS114は、VEReqの構文の妥当性を確認し、妥当性確認に失敗した場合にエラーを返す。支払取引を認証できない時、代わりに認証の試行の証明を提供できる場合があることに留意されたい。ACS114は、VEReqメッセージからの利用者PANを使用して、ACS114内に位置する利用者データベースに問い合わせ、利用者が加入しているかを判断する。PANが見つからない場合、ACS114は、「N」に設定されたPAN認証可能性を含み、口座識別子、ACSのURL、支払プロトコル、及び無効要求のデータフィールドを含まないVEResメッセージをフォーマットする。その後、ACS114は、VEResメッセージをVisaディレクトリサーバ128へ送信する。

【0100】

ステップ5において、Visaディレクトリサーバ128は、ACS114の判断をMPI134へ転送する。Visaディレクトリサーバ128の観点では、この処理は、Visaディレクトリサーバ128がVEReqメッセージをACSのURLへ転送した後発生する。ACS114の観点では、この処理は、ACS114がVEResメッセージをVisaディレクトリサーバ128へ送信した後発生する。

【0101】

Visaディレクトリサーバ128は、対応するVERes又はエラーを含むVEResメッセージを読む。Visaディレクトリサーバ128は、VEResメッセージの構文の妥当性を確認し、妥当性確認に失敗した場合にACS114へエラーを返す。ACSから受け取ったメッセージが構文的に正しい場合、Visaディレクトリサーバ128は、VERes又はエラーをMPI134へ転送する。ACSから受け取ったメッセージが構文的に正しくない場合、Visaディレクトリサーバ128は、「N」に設定されたPAN認証可能性を含み、口座識別子、ACSのURL、支払プロトコル、及び無効要求を含まないVEResメッセージをフォーマットする。Visaディレクトリサーバ128は、VEResメッセージをMPI132へ返し、場合によっては口座認証処理を停止する。MPI134の観点では、この処理は、MPI134がVEReqメッセージをVisaディレクトリサーバ128へ送った直後に発生する。Visaディレクトリサーバ128の観点では、この処理は、VisaディレクトリサーバがVEResメッセージをMPIへ転送した直後に発生する。MPI134は、対応するVERes又はエラーを含む応答を読む。エラーメッセージが受け取られた場合、口座認証処理を停止となり得る。

【0102】

上記の様々な理由により口座認証が終了となり得るポイントにおいて、販売者は、チェックアウト処理から利用可能な情報を使用して、通常の支払許可を進めることができる。この場合、販売者の支払システムは、この文書の範囲から外れた非認証電子商取引処理として、取引を処理するべきである。電子商取引インジケータは、認証の結果及びチェックアウト処理の特性に対応する値に設定されるべきであることに留意されたい。チェックア

ウト処理中に利用者が選択した口座を使用して、販売者が認証取引を処理できない場合、販売者は、取引を中止するか、或いは代替口座を選択するオプションを顧客に与えることができる。代替口座が選択された場合には、認証処理を繰り返すことができる。

【0103】

代替実施形態では、V i s aディレクトリサーバの内容を販売者132のローカルキャッシュメモリデバイスへコピーすることにより、各支払取引で利用者の口座認証システムへの参加を検証するためにV i sディレクトリサーバに問い合わせる必要性(ステップ2乃至5)は回避できる。この機能を使用する場合、販売者132は、口座が加入範囲の一部であるかを、キャッシュから即座に決定できる。この販売者132のローカルキャッシュを使用する代替手法は、M P I 1 3 4がカード範囲要求(C R R e q)メッセージをフォーマットし、V i s aディレクトリサーバ128へ送信することで開始される。キャッシュのロードが今回初めて行われる場合(或いは、キャッシュが消去されており、再ロードする必要がある場合)、C R R e qにはシリアル番号要素が含まれておらず、その結果、V i s aディレクトリサーバ128は、関与するカード範囲の全リストを返送する。その他の場合に、M P I 1 3 4は、直前に処理されたC R R e sからのシリアル番号を含め、その結果、V i s aディレクトリサーバは、以前のC R R e sからの変更のみを返送する。シリアル番号は、V i s aディレクトリサーバ128のカード範囲データベースの現在の状態を定義する値である。V i s aディレクトリサーバ128は、M P I 1 3 4にシリアル番号を提供する。特定の番号は、それを返送した特定のV i s aディレクトリサーバにとってのみ意味を有する。

【0104】

V i s aディレクトリサーバ128は、C R R e qの構文の妥当性を確認し、妥当性確認に失敗した場合にエラーを返す。V i s aディレクトリサーバ128は、関与する範囲を含むカード範囲応答をフォーマットし、M P I 1 3 4へ送信する。V i s aディレクトリサーバ128は、応答にシリアル番号を含める。M P I 1 3 4は、この値を保持し、翌日のC R R e qメッセージに含めるべきである。M P I 1 3 4は、C R R e sの構文の妥当性を確認し、妥当性確認に失敗した場合、V i s aディレクトリサーバ128にエラーを送信するべきである。M P I 1 3 4は、ローカルキャッシュを更新する。リストは、アクション要素が示す追加又は削除された範囲により、返送された順序で処理するべきである。C R R e sがシリアル番号についてエラー状態を示す場合、M P Iはキャッシュを消去し、シリアル番号のないC R R e qを提出するべきであることに留意されたい。

【0105】

利用者のP A Nについて認証が可能である時、M P I 1 3 4は、122の利用者クライアントデバイスを介して、支払者認証要求(P A R e q)メッセージをA C S 1 1 4へ送信する。ステップ6は、利用者クライアントデバイス122へ送信されたP A R e qメッセージを表す。この処理は、M P I 1 3 4がV i s aディレクトリサーバ128からV E R e sメッセージを受取直後に発生する。M P I 1 3 4は、V E R e sの構文の妥当性を確認し、妥当性確認に失敗した場合、V i s aディレクトリサーバにエラーを送信するべきである。M P I 1 3 4は、V E R e sにおいて受け取った口座識別子を含むP A R e qメッセージをフォーマットする。

【0106】

この認証プロセスの実施形態は、販売者132と発行者190との間で利用者関連情報を共有することを含む。発行者190及び販売者132のそれぞれは、単一又は多数の取引において、利用者に関する広範な情報を収集できる。こうした情報は、特定の利用者の購買習慣に関する情報を含む可能性がある。こうした情報は、販売者132、発行者190、及び付加価値提供者196といった様々な関係者にとって有用となる可能性がある。こうした顧客情報は、P A R e q及びP A R e sメッセージ内にこうした情報を含めることで、認証処理中に、販売者132と発行者190との間で共有できる。したがって、ステップ6において、販売者132は、利用者122に関する情報をP A R e qメッセージに含めることができる。

【0107】

M P I 1 3 4 は、次のフィールドを含むフォームを構築する：P A R e q、最終的な返答を送るべき販売者URLであるT e r m U r l、及びM D（「販売者データ」）フィールド。M Dフィールドは、販売者に返送すべき販売者状態データを含む。このフィールドは、販売者システムがセッション状態を扱う様々な方法に対応するために使用される。販売者システムが、何らかの更なる支援なしに、最終ポストを元のショッピングセッションに関連づけできる場合、M Dフィールドは空になり得る。販売者システムが一定のショッピングセッションに対する状態を維持しない場合、M Dは、販売者がセッションを継続するのに必要なあらゆるデータを運ぶ。このフィールドの内容は販売者の実施により変化するため、A C Sは、内容に関する仮定を含まずに、フィールドを変化させずに維持すべきである。

【0108】

M P I 1 3 4 は、利用者のブラウザにフォームをA C Sへポストさせることで、利用者のブラウザを介して、P A R e qをV E R e sにおいて受け取られたA C SのU R Lへ渡す。全ての接続は、利用者のブラウザに対応するためにH T P P Sとなる。

【0109】

ステップ7は、利用者クライアントデバイス122からA C S 1 1 4へ送信されるP A R e qメッセージを表す。この処理は、A C S 1 1 4がM P I 1 3 4からP A R e qを含むポストを受取後で発生する。以下の説明は、パスワードを使用して利用者認証が実行される場合に該当する。チップカード上のアプリケーションに依存するもの等、その他の方法も使用してよい。A C S 1 1 4は、P A R e qメッセージの妥当性を確認し、妥当性確認に失敗した場合にエラーを返す。妥当性確認に失敗した場合、A C S 1 1 4は、「N」に設定した取引ステータスと無効要求とを有するP A R e sメッセージをフォーマットする。

【0110】

ステップ8において、A C Sは、P A Nに適用可能な処理を使用して利用者を認証する。こうした処理は、発行者190と利用者122との間で事前に設定されたパスワード又はP I Nを要求すること、及び利用者にデータ課題を提示すること等の手法を一部として含む。データ課題は、例えば、利用者又は利用者クライアントデバイス122の同一性を認証する特定のデータ応答を利用者クライアントデバイス122が提供するのをA C S 1 1 4が要求することを含む可能性がある。一シナリオにおいて、A C S 1 1 4は、利用者122を認証する特定の暗号文をクライアント利用者デバイスが作成することを要求できる。代替として、A C S 1 1 4は、認証の試行の証明を生成できる。その後、A C S 1 1 4は、適切な値でP A R e sメッセージをフォーマットし、応答メッセージにデジタル署名を付与する。A C S 1 1 4は、パスワード、データ応答、又は暗号文を、A C S内に位置する利用者データベースに照らして検証する。A C S 1 1 4は、更に、各オンライン取引に対して、C A V V等の取引識別子を生成する。取引識別子は、特定のオンライン取引に関連づけされると共に、販売者132と発行者190との間で共有される顧客情報にも関連づけされる。

【0111】

ステップ9において、A C S 1 1 4は、P A R e sメッセージを利用者クライアントデバイス122へ返送する。発行者190が維持する利用者122関連情報と、取引識別子とは、P A R e sメッセージに含めることで販売者へ送信できる。

【0112】

A C S 1 1 4は、P A R e s及びM Dフィールドを含むフォームを構築する。A C S 1 1 4は、利用者のブラウザにフォームをM P Iへポストさせることで、利用者のブラウザを介して、署名済みP A R e sを販売者のU R L（M P Iからのポスト内のT e r m U r l）へ渡す。この処理において、ポップアップが閉じられ、制御は、販売者のブラウザウィンドウへ戻される。

【0113】

この時点で、ACS114は、更に、選択されたデータを認証履歴サーバ130へ送信できる。例えば、ACS114は、認証履歴サーバ130へ送信される支払者認証取引(PATransReq)メッセージをフォーマットする。

【0114】

認証処理中に保持及び/又は転送される利用者情報は、販売者132及び発行者190のそれぞれが格納できる。各関係者は、顧客情報の一部、或いは一組の顧客情報全体を格納できる。代替として、顧客情報の一部又は全ては、認証サーバ130に格納できる。

【0115】

ステップ10において、利用者クライアントデバイスは、PAResメッセージをMPI134へ送る。

【0116】

ステップ11において、MPI134は、ACS114がPAResメッセージに付与したデジタル署名の妥当性を確認する。デジタル署名の妥当性確認は、ACS114自体が実行可能であり、或いは、PAResメッセージを別個の妥当性確認サーバへ渡すことで実行できる。妥当性確認処理では、Visaルート証明書を使用して、PARes署名の妥当性を確認する。別個の妥当性確認サーバを使用して実施する場合、MPI134は、PAResを妥当性処理へ送信し、妥当性処理では、Visaルート証明書を使用して、PARes上の署名の妥当性を確認し、署名の妥当性確認の結果をMPIへ返す。

【0117】

ステップ12において、販売者132は、取得者192との許可の交換を進める。

【0118】

ステップ13において、販売者132は、特定の基準一式を使用して、所有している顧客情報を評価する。一組の顧客情報が基準を満たす場合、顧客情報と取引識別子とを付加価値提供者196へ送信する。基準は、付加価値提供者196が顧客情報の受取を希望するかを判断する様々な問題を中心として、様々に変更できる。こうした基準については、認証処理がどのように動作するかのもっと詳細な例を通して、更に詳細に説明する。

【0119】

ステップ14において、付加価値提供者196は、顧客情報と取引識別子とを、価値付加制御サーバ198等のデータベースに格納する。

【0120】

ステップ15は、様々な目的で発生する可能性がある、価値付加制御サーバ198と認証履歴サーバ130との間を行き来する通信を表している。こうした目的には、例えば、販売者132と付加価値提供者196との間の取引を終結させることと、紛争の解決と、データマイニングとが含まれる。

【0121】

本説明の以下の節では、本発明の様々な価値付加実施形態の更なる詳細について説明する。

【0122】

付加価値提供者としての出荷会社

次に、図8に示した認証システム及びプロセスについて、付加価値提供者196が出荷会社(「出荷者」)であり、出荷者200aと呼ばれる場合の実施形態により説明する。この実施形態において、利用者122は、利用者の住居又は他の郵送先住所へ出荷する必要のある製品を販売会社132から購入する。出荷者196へ送信される利用者又は顧客情報により、出荷者196は、商品を利用者122へ出荷できる。上記のように、顧客情報は、認証処理に由来するため、高度な完全性と豊富さを有する。したがって、情報の価値は、販売者132と付加価値提供者196とが互いに取引に参加するための基盤としての役割を果たす。取引の種類範囲は、大きく変化する可能性がある。一例において、出荷者196は、出荷者196が販売者132及び利用者122にとって低いコストで製品を進んで出荷する程度まで、顧客情報の完全性及び豊富さに依存する。こうしたケースは、利用者122がパッケージの販売者への返送を決して要求していないことが顧客情報

に記載されているために生じ得る。追加として、販売者 132 は、利用者 122 の返送要求に伴う出荷者の責任又はコストを快く免除するほどに、こうした顧客情報に依存できる。

【0123】

認証及び価値付加処理は、図 8 の番号付きステップにより説明した認証処理により開始される。ステップ 6 及び 7 において、販売者 132 は、維持している顧客情報を、発行者 190 へ送信される P A R e q メッセージに含めてよい。ステップ 9 及び 10 において、発行者 190 は、発行者 190 が維持している顧客情報を、販売者 132 へ送信される P A R e s メッセージに含めてよい。発行者 190 は、更に、特定のオンライン取引及び顧客情報に関連する取引識別子を生成する。

【0124】

顧客情報は、例えば、1) 名前、郵送先住所、電子メールアドレス、電話番号、及び F A X 番号といった消費者連絡先情報と、2) 全額支払いの回数及び滞納の回数といった顧客支払履歴と、3) 好適な出荷方法、返品サービスを要求せずに行われた出荷回数、及び定時出荷の回数といった出荷履歴とにすることができる。顧客情報は、発行者 190 及び販売者 132 が収集可能な任意の種類の情報を含むことができる。

【0125】

更にステップ 9 において、顧客情報は、販売者 132 及び発行者 190 の一方又は両方に格納される。代替として、顧客情報は、認証履歴サーバ 130 等のデータベースに格納される。

【0126】

ステップ 13 において、販売者 132 は、顧客情報を特定の基準により評価し、こうした情報を出荷者 196 へ送信するべきかを判断する。基準は、例えば、出荷者 196 がタスクを難なく完了可能であることを顧客情報が示す場合に、顧客情報が出荷者 196 へ送信されるように策定できる。基準は、顧客に関して利用可能な履歴情報を調査することで、特定の顧客への出荷のリスクを分析するのに役立つ。基準の例には、1) 顧客は、販売者との購入取引を特定の回数を超えて行っているか？、2) 出荷先住所は、特定の国、例えば、米国内か？、3) 顧客は、以前に購入代金を滞納したことがあるか？、4) 顧客は、以前に返品を要求したことがあるか？、5) 顧客は、新規顧客か？、6) 特定の金額以上の取引か？、7) 出荷先住所は検証済みか？、又は 8) 配達先の国は、低リスク又は高リスクの国か？が含まれる。販売者 132、出荷者 196、又は両関係者が、基準を設定できる。

【0127】

顧客情報が販売者の基準を満たす場合、顧客情報と取引識別子とは、出荷者 196 へ送信される。発行者 190 が取引識別子を生成するため、出荷者 196 に対して、情報の正確さが保証される。顧客情報に依存して、出荷者 196 は、難なく、したがって過剰なコストなしで、出荷可能であることが一定のレベルで保証された状態で、製品を顧客 122 に出荷する。顧客情報が提供する、出荷者 196 に対する問題のない取引の保証により、販売者 132 と出荷者 196 とは、互いに対して特別の配慮を提供し得る。例えば、出荷者 196 は、販売者 132 及び顧客 122 にとって低いコストで製品を進んで出荷し得る。更に、販売者 132 は、出荷者 196 に代わって、出荷するリスクの一部を負うことが可能であり、或いは販売者 132 は、出荷者 196 に対して運送費を部分的に補償することに合意できる。

【0128】

ステップ 14 において、出荷者 196 は、取引識別子と共に、顧客情報を価値付加制御サーバ 198 に格納する。出荷者 196 は、出荷ラベルに取引識別子を印刷した状態で、製品を顧客 122 へ出荷できる。

【0129】

ステップ 15 は、様々な目的で、取引識別子に関連する顧客情報と共に検索することを含む。こうした目的には、販売者 132 と付加価値提供者 196 との間の取引を終結させ

ること、紛争の解決、及び/又はデータマイニングが一部として含まれる。取引識別子は、特定の取引に対応するため、発行者190、販売者132、及び付加価値提供者196が各取引の情報を検証できるように、各取引の履歴を追跡するのに有用である。本発明により、販売者は、顧客が特定の購入を行っていないと主張する購入詐欺から、自らを更に保護することも可能となる。本発明により、出荷会社は、顧客が出荷を受け取っていないと偽って主張する出荷詐欺から、自らを更に保護することも可能となる。

【0130】

顧客情報は、「強制」又は「引き出し」の状況において、認証履歴サーバ(AHS)130から検索できる。「強制」の状況は、事象の発生が予測されるため、受取者である付加価値提供者196に顧客情報を強制する状況である。「引き出し」の状況は、不規則に起こる事象の発生時のみ、受取者が顧客情報を引き出す状況である。例えば、AHS130に格納された顧客情報及び取引識別子による検証を要する紛争が発生した時のみ、顧客情報を引き出すことができる。

【0131】

顧客情報及び取引識別子は、取引を終結させるためにAHS130から検索できる。こうした取引は、顧客情報の共有に基づいており、関係者のそれぞれが合意する追加条項を含む。様々な関係者が利益を享受可能な追加取引の基盤の役割を顧客情報が果たすことから、こうした取引は、価値付加取引と呼ばれる。例えば、価値付加取引の関係者は、追加的な事業機会を得ること、より競争力のある商品又はサービスコストを得ること、及び/又は、より有利な契約条項を得ることが可能となる。一部の取引において、出荷者196は、特定の条項にしたがって販売者132の製品を出荷することに合意する。こうした条項は、販売者132に請求される、より低い出荷コスト、及び/又は販売者132によるリスク及び責任の肩代わりを含むことができる。顧客情報及び取引識別子をチェックすることで、販売者132及び出荷者196は、出荷者が特定の出荷を行うことを検証できる。その後、例えば、販売者132は、出荷者196に割引運送料を支払う。取引を終結させるために顧客情報及び取引識別子を検索することは、こうした情報の検索が取引を終結させるための通常の処理である場合、強制取引となる。

【0132】

顧客情報及び取引識別子は、紛争解決の状況においても有用である。紛争は、販売者132、顧客122、及び出荷者196のいずれかの間で発生する可能性がある。紛争は、AHS130からの情報により、取引に関する事実を提供することで解決できる。紛争が発生した時には、顧客情報及び取引識別子を、こうした情報が格納されている場所から「引き出す」。販売者と出荷者との間の紛争は、各関係者間の価値付加取引の履行に関連する可能性がある。例えば、出荷サービスの支払に関する食い違いが生じた時、販売者132は、こうした情報を使用して、合意の上、割引運送料で出荷者196が出荷を行ったことを証明できる。或いは、例えば、出荷を受け取っていない、或いは出荷中に商品が損傷したと顧客が苦情を言った場合、出荷者196は、こうした取引の責任を販売者132が負うことを証明できる。一部の事例においては、発行者190が責任を負う場合がある。

【0133】

顧客情報及び取引識別子は、販売者132、発行者190、及び出荷者196のそれぞれがデータマイニングの目的でも使用できる。こうした関係者のそれぞれは、その取引を介して、特定の顧客について、その顧客の特色及び傾向を判断するために分析可能な情報を入手できる。こうした特色及び傾向は、販売者132、出荷者196、及び発行者190のそれぞれのマーケティングの目的で使用できる。販売者132は、顧客の特色及び傾向に関する情報を使用して、顧客に対する将来の販売及びマーケティング戦略を決定できる。出荷者196も、こうした情報をリスクの分析に使用して、例えば、問題に遭遇することなく顧客に製品を出荷できる確率を決定できる。発行者190は、こうした情報を使用して、将来、顧客に対して口座を発行することのリスクのレベルを決定可能であり、或いは、クレジットのレベルを引き上げるべきかを決定できる。

【0134】

追加として、任意の関係者は、情報を使用して、他の任意の関係者の特性を決定できる。例えば、出荷者は、特定の販売者と契約を結ぶことが賢い事業判断であるかを決定できる。こうした分析を行うために、顧客情報を分析して、販売者の詐欺履歴、チャージバック履歴、顧客の一般的な出荷相手国等を決定できる。こうした情報から、特定の業者との取引では、通常、出荷が容易であることが分かった場合、ある業者は、こうした業者と更に多くの仕事を行うことを判断できる。販売者は、こうしたデータを分析して、特定の出荷者により、出荷のニーズを満足させるべきかを決定できる。例えば、顧客データは、どの業者が配送成功率及び定時配送スコアを有するかを示すことができる。

【0135】

販売者132及び発行者190の一方又は両方が顧客情報を保持する実施形態において、顧客情報及び取引識別子は、対応する団体のそれぞれから検索できる。

【0136】

本発明の出荷の代替実施形態において、販売者132は、特定の取引の顧客データと取引識別子とのコピーを多数の出荷者へ送信できる。顧客データは認証処理に由来し、高い度合いの完全性を有するため、各出荷者196は、その取引のための出荷を実行することに興味を有し得る。各出荷者196が興味を有し得るのは、顧客情報の完全性が、取引に関する情報、例えば、出荷先住所の信頼性を保証するためである。更に重要なことに、顧客情報は販売者の基準を通過した後で各出荷者196へ送信されているため、各出荷者196では、出荷取引の問題に遭遇する確率が低いことが保証されている。代替方法において、出荷者196は、少なくとも、特定の取引に伴うリスクのレベルについて知識を得られる。更に、出荷者196は、販売者132又は発行者190が取引のリスクのコストを肩代わりすることに同意していることから、取引の製品を出荷することに興味を有し得る。こうした取引及び顧客に関する知識を有した状態で、出荷者196のそれぞれは、販売者132に出荷費用を入札できる。販売者132は、その後、一出荷者196を選択して製品を出荷できる。

【0137】

付加価値提供者としての後続販売者

図8に示した認証及び情報共有処理の代替実施形態において、付加価値提供者196は、後続販売者196である。この実施形態において、本発明は、後続販売者196について、更に一部のケースでは販売者132及び発行者190について、収入機会を増加させることができる。後続販売者196は、販売者132から顧客情報及び取引識別子を受け取り、こうした情報を使用して、自分の商品又はサービスを顧客122へ売り込む。後続販売者196は、任意の種類の商品又はサービスを提供できるが、販売者132が販売する商品又はサービスと何らかの関連性を有することが多い。顧客122が販売者132との取引の対象に関連する何かを購入する見込みが高くなり得ることから、販売者132からの顧客情報は、価値のあるものとなる。販売者132及び後続販売者196は、顧客情報に基づいて、互いに様々な契約を結ぶことができる。

【0138】

この処理も、図8の番号付きステップにより説明した認証処理により開始される。ステップ6、7、9、及び10において、販売者132及び後続販売者196は、以前に説明したように情報をPAReq及びPAResメッセージに含めることで、顧客122に関する情報を共有する。更に、発行者190は、特定のオンライン取引及び顧客情報に関連する取引識別子を生成する。顧客情報及び取引識別子は、発行者190、販売者132のそれぞれにより格納されるか、或いは認証履歴サーバ130等の単一のデータベース内に格納される。

【0139】

ステップ13において、販売者132は、顧客情報を評価して、顧客情報及び取引識別子を後続販売者196へ送信するべきかを判断する。こうした顧客情報は、例えば、顧客の平均出費額、顧客の最高出費額、顧客がいつ購入したか、顧客が誰から購入したか、顧客が何に出費したか、顧客の性別、及び顧客の人口統計学的情報に関連する。顧客の特性

に関する分析範囲は極めて広いことを理解されたい。顧客情報が基準を通過した場合、ステップ13において、情報は、後続販売者196へ送信される。

【0140】

顧客情報及び取引識別子を受け取ると、ステップ14において、後続販売者196は、顧客情報及び取引識別子を、価値付加制御サーバ198等のデータベースに格納する。この時、後続販売者196は、顧客情報を利用して、特定の顧客に焦点を絞ったマーケティング戦略を実行できる。顧客情報により、後続販売者196は、様々な顧客向けにマーケティング戦略を調整する方法について知ることができる。例えば、特定の取引での顧客の出費額に関する情報から、後続販売者196には、顧客122が興味を有し得る商品又はサービスの価格水準が分かる。更に、販売者132が販売した商品又はサービスに関する情報から、後続販売者196には、顧客122が購入を希望し得る関連商品又はサービスの種類が分かる。例えば、顧客が販売者132からCDプレイヤーを購入した場合、後続販売者196は、顧客122に特定のCDを販売できる。こうした取引は、「補完財」取引と呼ぶことができる。他の補完財には、例えば、コードレスドリル及び充電式電池、剃刀及び剃刀刃、芝刈り機及び肥料が含まれる。

【0141】

顧客情報の受取は、顧客情報により生じた後続販売者196の売り上げの一定のパーセンテージを販売者132及び/又は発行者190に提供するという後続販売者196からの合意を条件にできる。こうした販売及び類似する性質の販売は、例えば、「アップセル」及び「クロスセル」と呼ばれる。想像できるように、顧客情報の受取は、販売者132と後続販売者196との間の様々な合意を条件にできる。上記のように、顧客情報は、多数の詳細を含み、完全性が高いため、後続販売者196にとって独自の価値を有する。顧客情報は、販売者132及び発行者190の一方又は両方が収集したものであるため、多数の詳細を含む。販売者132及び発行者190のそれぞれは、顧客に関する特定の種類の情報を収集する独自の立場にある。最後に、顧客情報は、ステップ1乃至12で説明した認証処理を通過したものであるため、完全性が高い。

【0142】

ステップ15は、ここでも、販売者132と後続販売者196との間の取引を終結させること、紛争の解決、及び/又はデータマイニング等、様々な目的で、取引識別子を関連する顧客情報と共に検索することを含む。後続売り上げの一定のパーセンテージを販売者132へ送る前に、後続販売者196の売り上げに関する情報を検証する場合、ステップ15は、販売者132と後続販売者196との間の契約を成立させるのに必要となり得る。例えば、顧客情報及び取引識別子は、後続販売が顧客情報の結果であることを検証するために、販売者132又は後続販売者196が検索できる。こうした検証の後、一定の金額が販売者132へ送られる。この状況において、顧客情報は、契約を遂行するために、通常の営業過程として一方又は両方の販売者に強制可能であり、或いは、顧客情報は、食い違いを解消する必要がある場合のみ引き出せる。

【0143】

紛争の解決に関して、顧客情報及び取引識別子は、販売者132、後続販売者196、又は顧客122のいずれかの間で紛争が生じた場合に検索される。紛争は、違反が生じた恐れのある販売者132と後続販売者196との間の契約により発生する可能性がある。ここでも、販売者132が後続販売者196に顧客情報を送ることに合意する時、後続販売者196は、顧客情報から得られる売り上げを分け合うことを要求される場合がある。そのため、後続販売者196から販売者132へ支払うものに関して紛争が生じた時、顧客情報を引き出すことが可能である。関係者は、顧客情報及び取引識別子を照合し、後続販売者196による特定の販売が顧客情報に基づいて完了されたかを検証できる。

【0144】

後続販売者196による売り上げの一部が発行者190にも期待できる場合、顧客情報に関する一部の合意には、発行者190を関与させることができる。

【0145】

顧客情報は、データマイニングの目的でも使用可能であり、発行者 1 9 0、販売者 1 3 2、及び後続販売者 1 9 6 のそれぞれは、お互いと顧客とに関する知識を得ることができる。顧客情報の分析により、関係者は、お互いの将来の取引が好ましいかを知ることができる。

【 0 1 4 6 】

付加価値提供者としての様々な関係者

口座認証及び価値付加システムの代替実施形態では、様々な種類の関係者が、顧客 1 2 2、販売者 1 3 2、及び付加価値提供者 1 9 6 の役割を果たすことができる。顧客 1 2 2 及び販売者 1 3 2 の役割は、販売者 1 3 2 が顧客の同一性を認証する必要がある場合、互いにオンラインでやり取りする任意の関係者になり得る。販売者 1 3 2 が顧客 1 2 2 に何らかの商品又はサービスを販売する多数の商業的状況が想像できる。しかしながら、多数の非商業的状況も想像できる。一部の状況には、運転免許、入漁免許、建築免許、社会保障費、及び学校の受講登録といったオンライン登録が含まれる。関係者（販売者 1 3 2 等）が別の関係者（顧客 1 2 2 等）の同一性認証を要求するシナリオであると理解されたい。

【 0 1 4 7 】

販売者 1 3 2 等の同一性認証者が評価する基準は、様々な種類の付加価値提供者 1 9 6 に関連する可能性がある。基準は、通常、本発明により認証された同一性を有する顧客 1 2 2 等の関係者に関する情報の受取を、付加価値提供者 1 9 6 が希望するかに関連する。ステップ 13 で送信された顧客情報は、異なる付加価値提供者 1 9 6 のそれぞれに関連する可能性がある。顧客 1 2 2 が運転免許を申請する場合、顧客情報は、例えば、顧客の運転記録、運転している車、日常の運転、及び一般的な目的地に関連する可能性がある。付加価値提供者 1 9 6 は、運転に関連する商品又はサービスを顧客に販売することを希望する任意の関係者になり得る。例えば、付加価値提供者 1 9 6 は、排気ガス検査会社、修理店、又は自動車保険会社になり得る。別の実施形態において、付加価値提供者 1 9 6 は、運転に関連するものを何も販売しない場合もある。しかしながら、付加価値提供者 1 9 6 は、それでも顧客 1 2 2 が興味を持ち得る商品又はサービスを販売し得る。例えば、顧客情報は、顧客 1 1 2 が特定の種類の車を運転しており、したがって、顧客 1 1 2 が特定の種類の消費又はサービスに興味を有し得ることを示す場合がある。様々な種類の関係が顧客情報から抽出可能であり、したがって、付加価値提供者 1 9 6 によって有用となる可能性がある。

【 0 1 4 8 】

顧客 1 2 2 が入漁免許を入手する時、付加価値提供者 1 9 6 は、例えば、釣り具販売店、旅行代理店、又は衣料品店となり得る。ここでも、付加価値提供者 1 9 6 は、釣りに直接的に関連する会社である必要はない。付加価値提供者 1 9 6 に送信される顧客情報は、釣りに関する顧客の好みに関連する可能性がある。販売者 1 2 2 が評価する基準により、顧客 1 2 2 がどのような釣り具を好むか、どのような釣りが好みか、顧客 1 2 2 はどこへ釣りに行くのが好きか、及び顧客 1 2 2 が使用する衣類の種類を決定できる。

【 0 1 4 9 】

顧客情報は、更にワークフローの目的で付加価値提供者に送信できる。例えば、顧客 1 2 2 が建築許可又は免許を販売者 1 2 2 に申請した後、次のレベルの承認のために、顧客情報を別の政府機関へ送る必要が生じ得る。例えば、建物の建設中に防災安全検査を手配するために、消防署で顧客情報を受け取る必要が生じ得る。

【 0 1 5 0 】

販売者 1 2 2 及び付加価値提供者 1 9 6 のそれぞれは、顧客情報及び取引識別子の共有に基づいて、互いに価値付加関係を結ぶことが可能である。

【 0 1 5 1 】

一部の実施形態において、販売者 1 2 2 は、顧客情報及び取引識別子を多数の付加価値提供者に送信できる。販売者 1 2 2 は、各種類の付加価値提供者 1 9 6 のために、異なる又は同じ一組の基準を評価できる。各付加価値提供者 1 9 6 は、互いに並行して又は順番

に、タスクの実行へ進む。付加価値提供者 196は、顧客122が各付加価値提供者 196から直接通知を受けるように、それぞれのタスクをリアルタイムで実行可能であり、或いはタスクはオフラインで実行可能である。

【0152】

上記のように、ステップ15は、販売者132、付加価値提供者 196、及び発行者190のいずれかの間で契約を結ぶために、様々な目的で使用できる。

【0153】

付加価値提供者としてのセキュリティ組織

本発明の一部の実施形態は、国家安全保障等、セキュリティの目的で使用できる。こうした実施形態において、付加価値提供者 196は、安全保障問題の情報(データ)の検討を責務とする政府機関又は任意の組織にすることができる。販売者132は、顧客122との取引をオンラインで実行する任意の営利的、非営利的、政府、又は非政府機関にすることができる。例えば、販売者は、航空券予約会社、工具店、薬品供給業者、又は飛行訓練学校にすることができる。顧客情報の伝送の一部又は全部は、プライバシー及び市民権に関する法律で規制され得ることに留意されたい。

【0154】

販売者132は、セキュリティ関連の基準により顧客情報を評価し、特定の基準が満たされた時、情報を取引識別子と共に付加価値提供者 196へ送信する。例えば、基準により、顧客の購入品目、免許登録、旅行目的地、旅行頻度、その他のセキュリティ関連事項を評価できる。顧客情報及び取引識別子の受取後、付加価値提供者 196は、監視任務を実行できる。

【0155】

取引識別子は、必要な場合に、セキュリティ関連の業務監査を正確に追跡できるように顧客情報を記録する上で有用となる。これは、例えば、政府の命令によるセキュリティプロトコルの調査の際に必要となり得る。具体的には、販売者132は、セキュリティプロトコルに正確に従っていたことを証明する必要が生じ得る。一部の状況において、販売者132は、裁判所の命令による召喚状に応答する。顧客情報及び取引識別子は、ステップ15において、認証履歴サーバ130からの強制又は引き出しが可能である。ステップ15は、販売者132、報告者、及び付加価値提供者 196間で契約を結ぶために使用することもできる。例えば、販売者132は、有用な情報を報告したことに対する評価又は認定を受けることができる。この評価は、取引識別子を使用して、顧客情報に関するソース、日付、その他の詳細を証明した後で受け取ることができる。ステップ15は、更に、認証履歴サーバ130からデータを引き出し、セキュリティ関連問題のデータマイニングを行うために、様々な関係者が使用できる。顧客情報は、発行者190及び販売者132から収集するため、監視目的において非常に役立つ情報を多く含む可能性が高い。

【0156】

一部の実施形態において、付加価値提供者 196及び販売者132は、顧客情報を受信した直後に付加価値提供者 196が販売者132にメッセージを送信できるように、リアルタイムで互いに通信する。これにより、望ましくない状況を解決又は回避するために、即座に処置を講じることができる。

【0157】

好適なシステムネットワーク

図9は、本発明の実施形態を実施するのに適した電気通信ネットワーク800を示している。本発明では、任意の適切な電気通信ネットワークを使用してよく、以下に説明するもの等の様々なハードウェア、様々なソフトウェア、及び/又は様々なプロトコルを含んでよい。下記のネットワークは、図2の電気通信ネットワーク126の好適な実施形態である。ネットワーク800は、任意のバンクカード、旅行及び娯楽カード、及び他の自社ブランド及び専用カードを使用した購入及び現金取引をサポートする、世界的な電気通信ネットワークである。ネットワークは、他のネットワークのATM取引、紙の小切手を使用した取引、スマートカードを使用した取引、及び他の金融手段を使用した取引もサポー

トする。

【 0 1 5 8 】

こうした取引は、ネットワークの許可、決済、及び清算サービスにより処理される。許可は、販売を確定する前、或いは現金を分散させる前に、発行者が販売取引を承認又は拒否する時期である。決済は、顧客の口座へ転記するために、取引を取得者から発行者へ引き渡す時期である。清算は、決済された全取引について、各関係者の純財務状態を計算及び決定する処理である。実際の資金の交換は、別個の処理となる。

【 0 1 5 9 】

取引は、二重メッセージ又は単一メッセージ取引として、許可、決済、及び清算可能である。二重メッセージ取引は二度送信され、最初は、許可の判断に必要な情報のみ送信され、その後、決済及び清算のために追加情報が再び送信される。単一メッセージ取引は、許可のために一度送信され、決済及び清算情報も含まれる。通常、許可、決済、及び清算は、全てオンラインで行われる。

【 0 1 6 0 】

電気通信ネットワーク 8 0 0 の主要構成要素は、交換センタ 8 0 2 と、アクセスポイント 8 0 4、8 0 6 と、処理センタ 8 0 8、8 1 0 とである。名宛銀行及び要求者認証機関といった他の実体も、アクセスポイントを介してネットワークに接続する。交換センタは、世界のどこにでも位置し得るデータ処理センタである。一実施形態では、米国に二箇所、英国及び日本に一箇所ずつ存在する。各交換センタは、ネットワーク取引処理を実行するコンピュータシステムを収容する。交換センタは、IBM SNA プロトコルに基づく高速専用回線又は衛星接続を含む、ネットワークの電気通信設備の制御点として機能する。好ましくは、交換センタを遠隔実体に接続する回線 8 2 0 及び 8 2 2 は、IBM SNA - LUO 通信プロトコルに基づく専用の高帯域電話回路又は衛星接続を使用する。メッセージは、ISO 8 5 8 3 規格の任意の適切な実施を使用して、これらの回線を介して送信される。

【 0 1 6 1 】

アクセスポイント 8 0 4 又は 8 0 6 は、通常、処理センタに配置され、センタのホストコンピュータと交換センタとの間をインタフェースする小型コンピュータシステムである。アクセスポイントは、ホストと、取引の許可、決済、及び清算をサポートする交換センタとの間でのメッセージ及びファイルの送信を容易にする。リンク 8 2 6 及び 8 2 8 は、通常、センタ内のローカルリンクであり、センタにとって好ましい専用のメッセージ形式を使用する。

【 0 1 6 2 】

データ処理センタ（取得者、発行者、又はその他の実体内に位置するようなもの）は、販売者及び事業拠点をサポートする処理システムを収容し、顧客データ及び請求システムを維持する。好ましくは、各処理センタは、一箇所又は二箇所の交換センタとリンクされる。プロセッサは、最も近い交換センタに接続され、ネットワークが障害を受けた場合、ネットワークは、取引を自動的に二次的な交換センタへ送る。各交換センタは、他の全ての交換センタにもリンクされる。このリンクにより、処理センタは、一箇所以上の交換センタを介して互いに通信できる。更に、処理センタは、交換センタを介して、他のプログラムのネットワークにアクセスできる。更に、ネットワークは、全てのリンクが複数のバックアップを有する状態を確保する。ネットワークの一点から別の点への接続は、通常は固定リンクではなく、代わりに交換センタは、任意の伝送の時点で、可能な最善の経路を選択する。何らかの障害のあるリンクを迂回するルート変更は、自動的に行われる。

【 0 1 6 3 】

図 1 0 は、オンライン及びオフライン取引処理を提供するために交換センタに収容されたシステム 8 4 0 を示している。二重メッセージ取引では、許可システム 8 4 2 が許可を与える。システム 8 4 2 は、オンライン及びオフライン機能をサポートし、そのファイルには、内部システムテーブル、顧客データベース、及び販売者中央ファイルが含まれる。システム 8 4 2 のオンライン機能は、二重メッセージ許可処理をサポートする。この処理

は、ルーティングと、利用者及びカード検証及び代理処理と、ファイルメンテナンス等のその他の機能とを含む。オフライン機能は、報告と、請求と、リカバリブリテンの生成とを含む。報告は、許可報告、例外ファイル及びアドバイスファイルの報告、POS報告、及び請求報告を含む。システム842からシステム846へのブリッジにより、システム842を使用する構成要素は、システム846を使用する構成要素と通信し、外部ネットワークへのSMSゲートウェイにアクセスできる。

【0164】

決済及び清算システム844は、事前に許可された二重メッセージ取引を決済及び清算する。週六日、世界全体で稼働し、システム844は、金融及び非金融情報を収集し、報告を構成要素間で配信する。更に、手数料、使用量、及び清算総額を計算し、調整を支援するために報告を作成する。ブリッジは、システム844の処理センタとシステム846の処理センタとの間の交換部を形成する。

【0165】

単一メッセージシステム846は、完全な金融取引を処理する。システム846は、二重メッセージ認証及び決済取引も処理可能であり、ブリッジを使用してシステム842と通信し、必要に応じてネットワークの外部にアクセスする。システム846は、ビザ プラス インターリンク (Visa, Plus Interlink)、その他のカード取引を処理する。SMSファイルは、システムのアクセス及び処理を制御する内部システムテーブルと、PIN検証及び代理処理認証に使用される利用者データのファイルを含む提供者データベースとを含む。システム846のオンライン機能は、リアルタイム利用者取引処理、及び認証の例外処理と、完全な金融取引とを実行する。システム846は、調整及び清算の合計を蓄積する。システム846のオフライン機能は、清算及び資金振替要求を処理し、清算及び活動報告を提供する。清算サービス848は、Interlinkを含め、システム844及び846の清算機能を統合し、全製品及びサービス向けの単一のサービスとする。決済は、システム844及びシステム846によって引き続き別個に実行される。

【0166】

図11は、電気通信ネットワーク800の構成要素の別の図を示している。統合支払システム850は、全てのオンライン認証及び金融要求取引を処理するための主要システムである。システム850は、二重メッセージ及び単一メッセージ処理の両方を報告する。どちらの場合においても、清算は別個に行われる。三つの主なソフトウェアコンポーネントは、共通インタフェース機能852、認証システム842、及び単一メッセージシステム846である。

【0167】

共通インタフェース機能852は、交換センタにおいて受け取られた各メッセージに求められる処理を決定する。メッセージのソース(システム842、844、又は846)、処理要求の種類、及び処理ネットワークに基づいて、適切なルーティングを決定する。このコンポーネントは、初期メッセージ編集を実行し、必要な場合、メッセージを解析して、内容が基本構成規則に従う状態を確保する。機能852は、メッセージをシステム842又はシステム846の送信先へ送る。

【0168】

コンピュータシステムの実施形態

図12A及び12Bは、本発明の実施形態を実施するのに適したコンピュータシステム900を示す。図12Aは、コンピュータシステムの可能な物理的形態の一つである。当然ながら、コンピュータシステムは、集積回路、プリント回路基板、及び小型ハンドヘルドデバイスから、巨大なスーパーコンピュータまで、多くの物理形態を有し得る。コンピュータシステム900は、モニター902と、ディスプレイ904と、筐体906と、ディスクドライブ908と、キーボード910と、マウス912とを含む。ディスク914は、コンピュータシステム900との間でデータを転送するために使用されるコンピュータ読み取り可能な媒体である。

【 0 1 6 9 】

図 1 2 B は、コンピュータシステム 9 0 0 のブロック図の例である。システムバス 9 2 0 には、広範なサブシステムが取り付けられる。プロセッサ（群）9 2 2（中央演算処理装置又は CPU と呼ばれる）は、メモリ 9 2 4 を含む記憶装置に結合される。メモリ 9 2 4 は、ランダムアクセスメモリ（RAM）及び読み出し専用メモリ（ROM）を含む。この技術において周知であるように、ROM は、データ及び命令を CPU へ一方向で転送する役割を果たし、RAM は、通常、データ及び命令を双方向で転送するために使用される。こうしたタイプのメモリは、両方とも、以下に説明する任意の適切なコンピュータ読み取り可能な媒体を含んでよい。固定ディスク 9 2 6 も、CPU 9 2 2 に双方向で結合され、追加のデータ記憶容量を提供し、同じく以下に説明する任意のコンピュータ読み取り可能な媒体を含んでよい。固定ディスク 9 2 6 は、プログラム、データ、その他を格納するのに使用してよく、通常は、一次記憶装置より低速の二次記憶媒体（ハードディスク等）である。固定ディスク 9 2 6 内に保持される情報は、適切である場合には、標準的な方法で、メモリ 9 2 4 内に仮想メモリとして組み込んでよいことは理解されよう。リムーバブルディスク 9 1 4 は、以下に説明する任意のコンピュータ読み取り可能な媒体の形態を取り得る。

【 0 1 7 0 】

CPU 9 2 2 は、ディスプレイ 9 0 4、キーボード 9 1 0、マウス 9 1 2、及びスピーカ 9 3 0 等の様々な入出力デバイスにも結合される。一般に、入出力デバイスは、ビデオディスプレイ、トラックボール、マウス、キーボード、マイクロフォン、タッチセンシティブディスプレイ、トランスデューサカードリーダー、磁気又は紙テープリーダー、タブレット、スタイラス、音声又は手書き認識装置、生体認証リーダー、又は他のコンピュータのいずれかにしてよい。CPU 9 2 2 は、随意的に、ネットワークインタフェース 9 4 0 を使用して、別のコンピュータ又は電気通信ネットワークに結合され得る。こうしたネットワークインタフェースにより、CPU は、上記の方法ステップを実行する過程で、ネットワークから情報を受け取ること、或いはネットワークへ情報を出力することが考えられる。更に、本発明の方法の実施形態は、CPU 9 2 2 単独で実行し得るものであり、或いは、処理の一部を共有するリモート CPU と連動して、インターネット等のネットワーク上で実行し得る。

【 0 1 7 1 】

加えて、本発明の実施形態は、更に、様々なコンピュータ実施動作を実行するためにコンピュータコードを有するコンピュータ読み取り可能な媒体を備えたコンピュータストレージ製品に関する。媒体及びコンピュータコードは、本発明のために特別に設計及び構築されたものにしてよく、或いは、コンピュータソフトウェア技術に関する当業者に周知であり利用可能な種類のものにしてよい。コンピュータ読み取り可能な媒体の例には、一部として、ハードディスク、フレキシブルディスク、及び磁気テープといった磁気媒体と、CD-ROM 及びホログラフィックデバイスといった光学媒体と、フロプティカルディスク等の光磁気媒体と、特定用途向け集積回路（ASIC）、プログラム可能論理デバイス（PLD）、及び ROM 及び RAM デバイスといった、プログラムコードを格納及び実行するために特別に構成されたハードウェアデバイスとが含まれる。コンピュータコードの例には、コンパイラによって生成されるようなマシンコードと、インタプリタを使用してコンピュータで実行される高レベルコードを含むファイルとが含まれる。

【 0 1 7 2 】

以上、本発明について、いくつかの好適な実施形態により説明してきたが、本発明の範囲に含まれる変更、置換、及び等価物が存在する。更に、本発明の方法及び装置を実施する数多くの代替方法が存在することにも留意されたい。したがって、添付特許請求の範囲は、本発明の本来の趣旨及び範囲に入るこうした全ての変更、置換、及び等価物を含むものと解釈されるべきである。

【 図面の簡単な説明 】

【 0 1 7 3 】

【図 1】様々なタイプの口座認証用途に対して本発明の口座認証サービスを実施するためのシステムアーキテクチャの一実施形態を示す図である。

【図 2】支払取引における本発明の認証サービスをサポートするシステムアーキテクチャの一実施形態を示す図である。

【図 3】本発明の一実施形態による、口座保有者が口座認証システムに登録する処理を示す図である。

【図 4】口座保有者が口座認証システム加入処理中に情報を入力できるインターネットウェブページの一実施形態を示す図である。

【図 5】口座保有者がインターネットに接続されたコンピュータを使用する、口座認証システムにおける認証支払取引を説明する図である。

【図 6】口座保有者にパスワードを要求するウィンドウの例を示す図である。

【図 7】消費者がインターネットに接続されたコンピュータを使用する口座認証システムに重ね合わせて、支払取引中に送信されるメッセージの例を示す図である。

【図 8】付加価値提供の態様を含むオンライン口座認証に関連するシステムアーキテクチャの例と、一組のメッセージフローとを示す図である。

【図 9】本発明の実施形態を実施するのに適した電気通信ネットワークを示す図である。

【図 10】オンライン及びオフライン取引処理を提供するために交換センタに収容されたシステムを示す図である。

【図 11】電気通信ネットワークの構成要素の別の図である。

【図 12 A】本発明の実施形態を実施するのに適したコンピュータシステムを示す図である。

【図 12 B】本発明の実施形態を実施するのに適したコンピュータシステムを示す図である。

【誤訳訂正 3】

【訂正対象書類名】図面

【訂正対象項目名】図 8

【訂正方法】変更

【訂正の内容】

【図 8】