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

特許第5052673号
(P5052673)

(45)発行日　平成24年10月17日(2012.10.17)　(24)登録日　平成24年8月3日(2012.8.3)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	21/24	160C
G06Q 30/06	(2012.01)	G06F	17/60	310E
H04L 9/32	(2006.01)	G06F	17/60	302E
		H04L	9/00	673C
		H04L	9/00	675A

請求項の数 16　(全 34 頁)

(21)出願番号　特願2010-521830 (P2010-521830)
(86)(22)出願日　平成19年9月4日 (2007.9.4)
(65)公表番号　特表2010-537308 (P2010-537308A)
(43)公表日　平成22年12月2日 (2010.12.2)
(86)国際出願番号　PCT/US2007/077503
(87)国際公開番号　WO2009/029116
(87)国際公開日　平成21年3月5日 (2009.3.5)
審査請求日　平成22年2月18日 (2010.2.18)
(31)優先権主張番号　11/844,408
(32)優先日　平成19年8月24日 (2007.8.24)
(33)優先権主張国　米国(US)

(73)特許権者　509346829
ベネドール　コーポレイション
アメリカ合衆国、９３０２１－３５５２
カリフォルニア州、ムーアパーク、マヤ
サークル　１４１８３
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　キャロット、リチャード、エフ.
アメリカ合衆国、９３０２１－３５５２
カリフォルニア州、ムーアパーク、マヤ
サークル　１４１８３　ベネドール　コー
ポレイション内

審査官　和田　財太

最終頁に続く

(54)【発明の名称】ネットワークにおけるトランザクションセキュリティ

(57)【特許請求の範囲】
【請求項１】
暗号ストリームにおいて、名前識別子、顧客年齢識別子、住所識別子、および顧客合意識別子を含む顧客情報を暗号化する段階と、
購入された電子アイテムの購入トランザクションにおいて、前記暗号ストリームを顧客から販売者へと転送する段階と、
前記暗号ストリームを検証団体へとルーティングする段階と、
前記検証団体によって、前記暗号ストリームに基づいて、身元証明および支払承認のうち少なくとも１つを含む一意的なトランザクション識別子を生成する段階と、
前記検証団体によって、前記一意的なトランザクション識別子を前記販売者に転送する段階と、
前記販売者によって、前記暗号ストリームおよび前記一意的なトランザクション識別子のうち少なくとも一方を前記購入された電子アイテムに付加して、個人化電子アイテムを作成する段階と、
前記個人化電子アイテムを前記販売者から前記顧客へと供給する段階と
を備える方法であって、
前記暗号ストリームおよび前記一意的なトランザクション識別子には、前記顧客の支払に関する個人情報が含まれておらず、
前記個人化電子アイテムはそれぞれ、前記暗号ストリームがそれぞれ一意的であるので、供給される対象の前記顧客毎に異なっている方法。

【請求項２】
前記顧客情報を暗号化する段階はさらに、
ａ）第１のコンピュータデバイスを用いて前記顧客と前記検証団体とを接続する段階と、
ｂ）前記第１のコンピュータデバイスからハードウェア識別子を読み出す段階と、
ｃ）前記暗号ストリームに前記ハードウェア識別子を組み込む段階と、
ｄ）任意の購入トランザクションにおいて前記顧客が利用を所望する追加のコンピュータデバイスについてａ）からｃ）を繰り返す段階と
を有する請求項１に記載の方法。
【請求項３】
前記暗号ストリームを前記顧客から前記販売者へと転送する段階はさらに、
前記暗号ストリームを前記販売者へと転送するタイミングと略同じ時点であるが、実際に前記暗号ストリームを前記販売者へ転送するより前の時点において、前記暗号ストリームに、第２のハードウェア識別子群および日時スタンプを、前記暗号ストリームを実際に転送するコンピュータデバイスから組み込む段階と、
暗号化されていないルーティング識別子を前記暗号ストリームに添付する段階と
を有する請求項２に記載の方法。
【請求項４】
前記身元証明および前記支払承認は、前記販売者に対して、前記購入トランザクションの前記顧客が実在することを認め、前記販売者が取引している相手が前記顧客以外ではないことを前記販売者に保証して、前記トランザクション識別子によって前記販売者は前記購入トランザクションを署名有り処理で行うことができる請求項１に記載の方法。
【請求項５】
前記暗号ストリームが一意的であることによって、前記購入された電子アイテムの不正な複製の源を前記検証団体を介して特定することができる請求項１に記載の方法。
【請求項６】
暗号ストリームにおいて、名前識別子、顧客年齢識別子、住所識別子、および顧客合意識別子を含む顧客情報を暗号化する段階と、
購入された電子アイテムの購入トランザクションにおいて、前記暗号ストリームを顧客から販売者へと転送する段階と、
前記暗号ストリームを検証団体へとルーティングする段階と、
前記検証団体によって、前記暗号ストリームに基づいて、身元証明および支払承認のうち少なくとも１つを含む一意的なトランザクション識別子を生成する段階と、
前記検証団体が、顧客情報を格納している別個に設けられているデータベースと、前記暗号ストリームとを相互参照して、前記一意的なトランザクション識別子を生成する段階と、
前記検証団体によって、前記身元証明および前記支払承認のうち少なくとも１つを前記販売者に転送する段階と、
前記販売者によって、前記暗号ストリーム、前記身元証明、および前記支払承認のうち少なくとも１つを前記購入された電子アイテムに付加して、個人化電子アイテムを作成する段階と、
前記個人化電子アイテムを前記販売者から前記顧客へと供給する段階と
を備える方法であって、
前記暗号ストリーム、前記身元証明、および前記支払承認には、前記顧客の支払に関する個人情報が含まれておらず、
前記個人化電子アイテムはそれぞれ、前記暗号ストリームがそれぞれ一意的であるので、供給される対象の前記顧客毎に異なっている方法。
【請求項７】
前記顧客情報を暗号化する段階はさらに、
ａ）第１のコンピュータデバイスを用いて前記顧客と前記検証団体とを接続する段階と

、
ｂ）前記第１のコンピュータデバイスからハードウェア識別子を読み出す段階と、
ｃ）前記暗号ストリームに前記ハードウェア識別子を組み込む段階と、
ｄ）任意の購入トランザクションにおいて前記顧客が利用を所望する追加のコンピュータデバイスについてａ）からｃ）を繰り返す段階と
を有する請求項６に記載の方法。
【請求項８】
前記暗号ストリームを前記顧客から前記販売者へと転送する段階はさらに、
前記暗号ストリームを前記販売者へと転送するタイミングと略同じ時点であるが、実際に前記暗号ストリームを前記販売者へ転送するより前の時点において、前記暗号ストリームに、第２のハードウェア識別子群および日時スタンプを、前記暗号ストリームを実際に転送するコンピュータデバイスから組み込む段階と、
暗号化されていないルーティング識別子を前記暗号ストリームに添付する段階と
を有する請求項７に記載の方法。
【請求項９】
前記身元証明および前記支払承認は、前記販売者に対して、前記購入トランザクションの前記顧客が実在することを認め、前記販売者が取引している相手が前記顧客以外ではないことを前記販売者に保証して、前記トランザクション識別子によって前記販売者は前記購入トランザクションを署名有り処理で行うことができる請求項６に記載の方法。
【請求項１０】
前記相互参照する段階は、前記身元証明および前記支払承認を生成する前に、前記暗号ストリーム内に必要な証明情報が全て含まれているか否かを確認する段階を有する請求項６に記載の方法。
【請求項１１】
暗号ストリームにおいて、名前識別子、顧客年齢識別子、住所識別子、および顧客合意識別子のうち少なくとも１つを含む顧客情報を暗号化する段階と、
購入された電子アイテムの購入トランザクションにおいて、前記暗号ストリームを顧客から販売者へと転送する段階と、
前記暗号ストリームを検証団体へとルーティングする段階と、
前記検証団体によって、前記暗号ストリームに基づいて、一意的なトランザクション識別子を生成する段階と、
前記検証団体によって、一意的なトランザクション識別子を前記販売者に転送する段階と、
前記販売者によって、前記暗号ストリームを前記購入された電子アイテムに付加して、個人化電子アイテムを作成する段階と、
前記個人化電子アイテムを前記販売者から前記顧客へと供給する段階と
を備える方法であって、
前記暗号ストリームおよび前記一意的なトランザクション識別子には、前記顧客の支払に関する個人情報が含まれておらず、
前記個人化電子アイテムはそれぞれ、前記暗号ストリームがそれぞれ一意的であるので、供給される対象の前記顧客毎に異なっており、
前記顧客情報を暗号化する段階はさらに、
ａ）第１のコンピュータデバイスを用いて前記顧客と前記検証団体とを接続する段階と、
ｂ）前記第１のコンピュータデバイスからハードウェア識別子を読み出す段階と、
ｃ）前記暗号ストリームに前記ハードウェア識別子を組み込む段階と、
ｄ）任意の購入トランザクションにおいて前記顧客が利用を所望する追加のコンピュータデバイスについてａ）からｃ）を繰り返す段階と
を有し、
前記暗号ストリームを前記顧客から前記販売者へと転送する段階はさらに、

前記暗号ストリームを前記販売者へと転送するタイミングと略同じ時点であるが、実際に前記暗号ストリームを前記販売者へ転送するより前の時点において、前記暗号ストリームに、第２のハードウェア識別子群および日時スタンプを、前記暗号ストリームを実際に転送するコンピュータデバイスから組み込む段階と、
暗号化されていないルーティング識別子を前記暗号ストリームに添付する段階と
を有する、方法。
【請求項１２】
前記トランザクション識別子は、身元証明および支払承認のうちの少なくとも１つを含み、
前記身元証明および前記支払承認は、前記販売者に対して、前記購入トランザクションの前記顧客が実在することを認め、前記販売者が取引している相手が前記顧客以外ではないことを前記販売者に保証して、前記トランザクション識別子によって前記販売者は前記購入トランザクションを署名有り処理で行うことができる請求項１１に記載の方法。
【請求項１３】
前記暗号ストリームが一意的であることによって、前記購入された電子アイテムの不正な複製の源を前記検証団体を介して特定することができる請求項１１に記載の方法。
【請求項１４】
暗号ストリームにおいて、顧客合意識別子を含む顧客情報を暗号化する段階と、
財またはサービスを含む購入のための購入トランザクションにおいて、前記暗号ストリームを顧客から販売者へと転送する段階と、
前記暗号ストリームを検証団体へとルーティングする段階と、
前記検証団体によって、前記暗号ストリームに基づいて、身元証明および支払承認を生成する段階と、
前記検証団体によって、前記身元証明および前記支払承認のうち少なくとも１つを前記販売者に転送する段階と
を備える方法であって、
前記暗号ストリーム、前記身元証明、および前記支払承認には、前記顧客の支払に関する個人情報が含まれておらず、
前記顧客情報を暗号化する段階はさらに、
ａ）第１のコンピュータデバイスを用いて前記顧客と前記検証団体とを接続する段階と、
ｂ）前記第１のコンピュータデバイスからハードウェア識別子を読み出す段階と、
ｃ）前記暗号ストリームに前記ハードウェア識別子を組み込む段階と、
ｄ）任意の購入トランザクションにおいて前記顧客が利用を所望する追加のコンピュータデバイスについてａ）からｃ）を繰り返す段階と
を有し、
前記暗号ストリームを前記顧客から前記販売者へと転送する段階はさらに、
前記暗号ストリームを前記販売者へと転送するタイミングと略同じ時点であるが、実際に前記暗号ストリームを前記販売者へ転送するより前の時点において、前記暗号ストリームに、第２のハードウェア識別子群および日時スタンプを、前記暗号ストリームを実際に転送するコンピュータデバイスから組み込む段階と、
暗号化されていないルーティング識別子を前記暗号ストリームに添付する段階と
を有する、方法。
【請求項１５】
前記身元証明および前記支払承認は、前記販売者に対して、前記購入トランザクションの前記顧客が実在することを認め、前記販売者が取引している相手が前記顧客以外ではないことを前記販売者に保証して、トランザクション識別子によって前記販売者は前記購入トランザクションを「署名有り」処理で行うことができる請求項１４に記載の方法。
【請求項１６】
顧客のコンピュータ内に配置されているエンコーダであって、暗号ストリームにおいて

、名前識別子、顧客年齢識別子、住所識別子、および顧客合意識別子を含む顧客情報を暗号化するエンコーダと、
前記顧客のコンピュータ内に配置されている転送エージェントであって、購入された電子アイテムの購入トランザクションにおいて、前記暗号ストリームを前記顧客のコンピュータから販売者のコンピュータへと転送する転送エージェントと、
前記販売者のコンピュータと動作可能に接続されており、前記顧客のコンピュータおよび前記販売者とは別個に設けられている検証部と、
前記検証部に動作可能に接続されており、前記顧客情報を格納しているデータベースとを備えるシステムであって、
前記転送エージェントは、前記販売者のコンピュータから前記検証部へと前記暗号ストリームを転送させて、
前記検証部は、前記データベースに基づいて、身元証明および／または支払承認を含む一意的なトランザクション識別子を生成して、前記一意的なトランザクション識別子を前記販売者へ転送させて、
前記暗号ストリームおよび前記一意的なトランザクション識別子には、前記顧客の支払に関する個人情報が含まれておらず、
前記販売者によって、前記暗号ストリームおよび前記一意的なトランザクション識別子のうち少なくとも一方を前記購入された電子アイテムに付加して、前記販売者から前記顧客へと供給されるべき個人化電子アイテムを作成し、
前記個人化電子アイテムはそれぞれ、前記暗号ストリームがそれぞれ一意的であるので、供給される対象の前記顧客毎に異なっているシステム。

【発明の詳細な説明】

【関連出願】

【０００１】

本願は、現在係属中の米国特許出願第１０／９７０，０５１号（発明の名称：コンピュータネットワークで安全な購入トランザクションを提供するための方法および装置、出願日：２００４年１０月２１日）の一部継続出願である。当該米国特許出願は、米国特許第６，８３９，６９２号として特許された米国特許出願第０９／７２６，３０４号（出願日：２０００年１２月１日）の継続出願である。両特許文献は共に、全ての内容を本願に組み込む。

【０００２】

本願はさらに、現在係属中の米国特許仮出願第６０／８９０，２３０号（発明の名称：「取得された媒体または媒体コンテンツに対する暗号化された個別合意識別子」、出願日：２００７年２月１６日）に基づき優先権を主張する。当該仮出願の内容は全て、参照により本願に組み込まれる。

【技術分野】

【０００３】

本発明の実施形態は概して、電子商取引および同様のトランザクション、例えば、インターネット等のコンピュータネットワークを介した当事者間での財およびサービスの販売に対してセキュリティを提供することに関する。さらに、書類、プレゼンテーション、および作品の電子的形態等の電子商品の配信を追跡することに関する。また、配信された電子商品内の暗号化個別合意識別子を格納するための方法およびシステムに関する。

Ｉ．基礎の開示の「背景技術」および「発明の概要」

出願番号第１０／９７０，０５１

米国特許第６，８３９，６９２号

優先日：２０００年１２月１日

【０００４】

本発明は概して、ネットワーク上で行われる購入トランザクションに対してセキュリティを提供するためのシステムに関する。特に、暗号化情報のみを格納および提供する改良セキュリティシステムに関する。さらに、本発明は、ネットワーク上で行われる購入トラ

ンザクションについての顧客管理ルール、例えば、時間および価値の制限を提供するシステムに関する。

【背景技術】

【０００５】

パーソナルコンピュータおよびパーソナルコンピュータ同士を接続するネットワークの人気が高まった結果、電子商取引が最近数十年間の間に劇的に増加した。非常に人気の高いネットワークの一例として、ワールド・ワイド・ウェブ（ＷＷＷ）またはインターネットが挙げられる。しかし、電子商取引の発達を妨げてきた要因の一つに、簡便且つ安全な支払システムを実現できないことが挙げられる。

【０００６】

従来の電子商取引支払システムの多くでは、入念なパスワード／暗号化アルゴリズムが必要となり、煩雑でユーザにとっては使い難い。従来の電子商取引支払システムの中には、関係者全員がセキュリティ形式に合意する必要があるシステムもある。このようなシステムには、「クラブ」に加入して特定の暗号化形式に同意済みの関係者しか参加できないという問題がある。現在のネットワーク（例えば、インターネット）に商業サイトが参入および撤退するスピードを考えると、販売者に対して特定の形式に合意するよう求めるのは、現実的ではない。

【０００７】

電子商取引支払システムの中には、第三者のベンダーに対して事前支払を求めるシステムもあり、この場合は第三者のベンダーが前金に対して符号化されたクレジットを発行する。このような「財布」および「インターネットキャッシュ」の場合は、オンライントランザクションにおいてさらにもう一段階追加されるだけでなく、顧客情報が開示される段階が１つ増えることになる。さらに、このようなシステムでは、顧客および販売者の双方がさまざまなシステムバージョンに参加するべく登録する必要がある。

【０００８】

さらに、ユーザに特定のハードウェア（例えば、クレジットカードリーダー）を購入するよう求める電子商取引支払システムもある。このようなハードウェアは、本質的に独占的に所有されており、設置および利用が簡単ではない。また、ユーザは、別のコンピュータで購入を実行する場合にはハードウェアデバイスを持ち運ぶ必要があり、この種の支払システムが普及しない一因となっている。

【０００９】

支払システムの種類に関わらず、従来のシステムでは共通して、トランザクションを完了するためには顧客が個人情報を販売者、第三者、販売者の取引先の金融機関に対して提供しなければならないという点が問題である。この要件は、顧客が脅威にさらされるために、従来のシステムにおいて最大の障害である。顧客がハードウェアを追加するにしても、単純に第三者のベンダーを信頼して個人情報を渡すとしても、顧客の情報は他者のデータベースに格納されることになる。このように格納される記録は脆弱であり、潜在顧客および政策立案者にとっては深刻な懸念である。

【００１０】

問題は、インターネット等のネットワーク環境でビジネストランザクションを実行するために、顧客が個人情報、機密情報、および／または、秘密情報を何度開示しなければならないのかという点にある。

【発明の概要】

【発明が解決しようとする課題】

【００１１】

上記を鑑みて、本発明は、コンピュータネットワーク上での購入トランザクションにセキュリティを提供する構造および方法を提供することを目的とする。本発明では、顧客のコンピュータのストレージデバイスで顧客情報を暗号化して顧客コードを生成する（顧客のコンピュータは、コンピュータネットワークに接続されている）。そして、購入トランザクションではコンピュータネットワークを介して顧客コードを販売者に供給して、コン

ピュータネットワークを介して顧客コードを金融機関に転送するか、または、顧客コードの金融機関への転送を販売者に許可する。金融機関では、顧客コードを復号化して、情報を検証して、コンピュータネットワークを介して販売者に購入承認決定を返す。

【課題を解決するための手段】

【００１２】

本発明の重要な特徴は、暗号化された顧客情報、例えばクレジットカード番号等（「顧客コード」）は、販売者には入手不可能なので、販売者にセキュリティ対策またはプライバシー保護を委託することによる脆弱性を持たない。顧客コードは、顧客のストレージデバイスにのみ格納されており、暗号化されている。顧客はこのため、任意の暗号化情報、例えばクレジットカード番号を販売者に明らかにすることなく、販売者との間でトランザクションを完了することができる。金融機関では、具体的には、顧客の住所を、金融機関で保持している顧客の過去のアドレス情報と比較する。顧客は、承認されている発送先住所を複数持っている場合もある。顧客の住所と過去のアドレスが一致した場合にのみ、購入承認決定が与えられる。住所情報が正しくないために承認が与えられない場合の金融機関の選択肢には、（１）正しい住所を受け取ればトランザクションを承認する、（２）承認コードが発行される前に、顧客が住所情報を更新すれば、トランザクションを承認する、（３）承認を拒否する、がある。

【００１３】

ネットワーク環境に開示する前の時点で顧客情報を保護することによって、顧客は、オンラインでのクレジット機能の利用を、自身で制御することができると共に拡大することができるようになる。この点が、本発明と従来の電子商取引支払システムとの最大の違いである。

【００１４】

本発明によれば、顧客は、個人鍵またはアクセスコードを用いて自身の情報にアクセスできるようになるが、復号鍵または復号コードを所有するのは金融機関および金融機関の代理人のみである。このため、本発明によれば、手順を追加したり、第三者を経ることなく、そして顧客情報を多数のデータベースに開示することなく、顧客情報を安全に利用することができる。好ましい実施形態では、顧客コードには、暗号化されたクレジットカード情報が含まれる。

【００１５】

別の実施形態によると、本発明は、ストレージデバイスで多くの顧客コードを暗号化することができる。顧客コードはそれぞれ、特定の支払方法を含むとしてよい。これに代えて、１つの顧客コード群は、支払のためのクレジット機関を１つ特定することができ、顧客コード群の顧客コードはそれぞれ、ユーザ名が異なる。このような構成とすることによって、顧客コード群の各顧客コードのクレジット限度を固有値に設定することができ、顧客は単一のクレジット機関またはクレジット機能について更なるユーザを承認することができる。本発明はさらに、顧客のコンピュータにおいて顧客コードを解除するべくパスワードを用いる。

【００１６】

別の実施形態によると、本発明は、顧客コンピュータで動作するシステムを含む。本発明に係るシステムは、顧客コンピュータのストレージデバイスで顧客コードとして顧客情報を暗号化する暗号部と、コンピュータネットワークを介して購入トランザクションにおいて販売者に顧客コードを供給する供給部とを備える。顧客コンピュータは、コンピュータネットワークを介して顧客コードを金融機関に転送するネットワーク接続を有する。金融機関は、顧客コードを復号化して、コンピュータネットワークを介して販売者に購入承認決定を返す。

【００１７】

顧客コードは、暗号化された顧客住所情報が含まれているのが好ましく、当該システムはさらに、金融機関に設けられている比較部を備える。比較部は、顧客住所を、金融機関が保持している顧客の過去の住所と比較する。顧客住所と過去の住所とが一致している場

合にのみ、購入承認決定が与えられる。

【００１８】

当該システムは任意で、顧客コンピュータに対して外部に設けられ、コンピュータネットワークに接続されている、中間コード確認サイトを備えるとしてよい。中間コード確認サイトは、コンピュータネットワークを介して金融機関に顧客コードが転送される前に、顧客コードを受信する。中間コード確認サイトは、顧客コードが適切な暗号化形式であるか否かを確認する。

【００１９】

暗号部はさらに、ストレージデバイスで複数の顧客コードを暗号化するとしてよい。上述したように、各顧客コードが固有の支払システムを含むとしてよもいし、または、各顧客コード群が支払のために１つのクレジット組織を特定するとしてもよい。ある顧客コード群に含まれる顧客コードはそれぞれ、ユーザ名が異なり、クレジット限度も別々であるとしてよい。本発明に係るシステムはさらに、顧客コンピュータで顧客コードを解除するためのパスワードを受信することができるグラフィックユーザインターフェースを備える。

ＩＩ．一部継続出願の開示の「背景技術」および「発明の概要」

米国仮出願第６０／８９０，２３０号に基づく優先権の主張

優先日：２００７年2月１６日

【００２０】

インターネットの出現によって、コミュニケーションおよびビジネスのやり方が変わった。この変化と共に、インターネットの利用方法も進化してきた。コンピュータおよび技術によって新たな時代が開かれ、ソフトウェアがディスクにパッケージングされて販売された。これに続いて、ダウンロード可能な、または、その他の方法で移送可能な媒体、例えばデジタル形式の音楽および映画が登場した。この結果、許可されていないにも関わらず、このような製品の複製および販売で利益を得ようとするものが出てきた。これによって、基本的に２つのビジネスが誕生した。一方は他者の作品の海賊版を作成して利益を得ようとするビジネスで、他方はこのような海賊版作成行為を防止するビジネスである。インターネットが進化を続ける中、こういった媒体コンテンツのダウンロードおよび共有はますます多くなり、さらに複雑さが増すとともに、懸念も増加している。

【００２１】

同様に、問題のあるコンテンツを提供するサイト、例えばアダルト産業および、最近までは、ゲーム産業に関連するサイトは、高い人気を得ており、インターネットの性質上、そして法的権限管轄区域が統一されておらず強制力のある規則がないために、規制する上で悩みの種となっている。費用および労力を費やして、自主規制および訴追を課すべくさまざまな試みが実行されたが、未成年の保護、および、間違いなく国境を越えて行われている商取引の規制は、言葉を和らげて言っても困難であることが証明された。問題の複雑さは、従来の「事業が行われている場所」を持たない構造を、居住している場所の法律に応じてプライバシーの権利および法的保護の程度がさまざまである個人および団体の権利を侵害することなくどのように規制するか、という点にある。こういったプライバシーの権利および法的保護は、インターネット上での仮想法的権限管轄区域および商取引を規制する努力に対してバランスを保たなければならない。仮想環境における仮想商取引では、こういった権利の保護および訴追に関する権利および法的権限管轄区域に関して、合意を形成する必要がある。しかし、電子商取引の性格上、「個人情報盗難」および「身元詐称」に対して消費者の個人情報を保護しつつ、および、消費者および販売者のためにトランザクションを保護しつつ、消費者を識別する必要がさらに出てくる。

【００２２】

現時点においてはベンダーがインターネットトランザクションのリスクの大半を負っている。未成年が親のクレジットカード、デビットカード、またはプリペイドカードを「借用」した場合、別の人物に個人情報を盗まれた場合、閲覧が制限されているサイトに入るために年齢を偽ったりした場合、ベンダー側が支払を請求しても拒否される場合がある。

上述した事例はすべて、署名された受領書が存在しない「署名なし」のトランザクションのリスクを背負うのは銀行ではなく販売者であるので、提供するものに対して対価を要求する電子商取引の売り手側にとっては現実的な問題である。このため、トランザクションの詐欺、履行拒絶、および払い戻しは何百万ドルにものぼり、コストおよびリスクが高くなってしまう。

【００２３】

上記を鑑みて、本開示は、格納可能な形式で消費者の暗号化個別合意識別子を生成、記録、検証および作成する方法、システム、および構造を提供する。このような識別子は、コンピュータネットワークを通じて購入または取得された媒体に埋め込まれるとしてよく、販売によるトランザクションの承認、受領、および／または、記録に重ねられ、「人有り」／「署名有り」の検証機能が実現される。

【００２４】

当該方法は、ユーザが暗号化した任意または全ての合意識別子を利用することを含む。このような識別子は、ユーザのハードドライブまたは同様の用途のコンピュータストレージシステムへと格納される前、または格納される最中に作成される。当該方法およびシステムによると、暗号化された合意識別子は、暗号化された情報のうち名前、住所、または、クレジットカード番号／デビットカード番号／プリペイドカード番号等の所与の情報を、媒体の購入等のトランザクションの相手であるベンダーに開示することなく、利用することができるようになる。つまり、本明細書に記載する実施形態によると、ベンダーおよびベンダーのデータベースに対して消費者の身元情報およびその他の情報を常に登録または開示する必要がなくなる。

【００２５】

当該方法およびシステムによって、暗号化された合意識別子を、正規の使用条件および購入条件をユーザが受諾したことを確認する手段として利用することができるようになる。暗号化された合意識別子は、ダウンロード可能媒体に埋め込まれるとしてよい。当該方法およびシステムは、ユーザを報告すると共にユーザに対応する一意的なパスワード識別子を持つサブアカウントを作成および制御する。当該方法およびシステムでは、アカウントおよびサブアカウントを制御する責任を、メインの認可／登録ユーザに負わせる。暗号化された識別子によって、方法およびシステムは、取得媒体のアクセスおよび利用を保護すると共に、取得の目的である利用、条件および特権に制限することができるので、著作権およびその他の権利の保護を合意の上で実現すること可能となる。

【００２６】

より具体的には、本開示は、電子的に格納可能なアイテム（本明細書では、電子アイテムとも呼ぶ）、例えば、文学作品、音楽作品（録音）、および動画作品（映画、ショー、ビデオ等）について、コンピュータを用いて購入トランザクションを容易に行うためのシステムおよび方法を提供する。消費者は、例えば著作権等の権利の遵守することに同意する。

【００２７】

本明細書に記載する実施形態では、「顧客情報」を暗号ストリーム（顧客識別子（ＣＩＤ）コードとも呼ばれる）で暗号化する。このような顧客識別情報は、名前識別子（顧客の正式名であってもよいし、そうでなくてもよい）、顧客年齢識別子（生年月日、具体的な年齢、年齢範囲、年齢種別等であってよい）、住所識別子（顧客の住所であってもよいし、別の住所であってもよい）、および、顧客と、購入トランザクションを進める検証団体または金融機関（クレジット発行者）との間の契約上の合意を含むまたは識別する顧客合意識別子を含むとしてよい。

【００２８】

暗号ストリームの構成要素が特定されて合意が得られると、検証団体は、顧客情報を含むこの特定のストリーム（コンピュータ識別子を含む）を、単一且つ一意的な識別子を用いて、検索および特定するとしてよい。顧客情報は、検証データベースにのみ格納されて、暗号ストリームとして（暗号化されていないＢＩＮまたはクレジット発行者ルーティン

グ番号と共に）ベンダーに送信されるのは、当該識別子および販売時のコンピュータ識別子のみである。

【００２９】

このようなプログラムおよび参加者の目的の一つには、顧客の身元情報を保護しつつ、トランザクションに関与する全ての当事者によって利用され得る「検証された署名付きトランザクション」を実現することにある。

【００３０】

本明細書に記載する実施形態では、購入された電子アイテムの購入トランザクションにおいて、暗号ストリームを顧客から販売者へと転送する。検証団体は、クレジット発行者またはクレジット発行者の処理代行者または代理人（例えば、検証団体）であってよいが、身元証明および支払いの承認のために、支払処理に先立って、販売者が（購入代金と共に）送信する暗号ストリームを受信する。検証団体は、暗号ストリームと、顧客情報を有する別のデータベースとを相互参照して、身元証明および支払承認を生成する。この後、検証団体は、身元証明および支払承認を販売者に転送し、販売者は、顧客とのトランザクションを完了して、全ての当事者によって事前に合意された内容に従って検証された「署名付き」トランザクションとしてトランザクションの支払を処理する。

【００３１】

身元証明および支払承認では、販売者に対して、購入トランザクションの対象である顧客が実在することを確認する。この結果、販売者に対して、販売者がこの顧客以外との間でトランザクションを行っているのではないことを保証すると共に、顧客－クレジット発行者間の合意にしたがって検証されるトランザクションの条件を順守することに顧客が同意したことを保証する。顧客－クレジット発行者間の合意は、身元情報の保護および本明細書に記載する実施形態の利便性とある意味引き換えに、第三者のトランザクションにおいてこの合意が利用および信用されると予想される。

【００３２】

本明細書に記載する実施形態によると、暗号ストリームは、必ずしも顧客の個人情報ではないが、顧客およびクレジット発行者（例えば、銀行）によって、および、両者間で合意された識別子を含み、身元証明および支払承認は、顧客およびクレジット発行者によって、および、両者間で予想および合意されるように、一意的なトランザクションに限定される情報を含む。このような識別子は、暗号ストリームが例え復号化されても、ほとんど有用性がない。

【００３３】

本明細書に記載する実施形態の別の特徴として、暗号ストリームまたはトランザクションの検証が、販売者によって、購入された電子アイテム、例えばダウンロード可能デジタル媒体に付加されて、個人化電子アイテムを作成する点が挙げられる。暗号ストリームまたは固有のトランザクションの検証（本明細書では、両方まとめて、または、別個に、「トランザクション識別子」とも呼ぶ）は、顧客がトランザクション識別子を個人化電子アイテムから削除できないように、隠すこともできる。また、個人化電子アイテムは、暗号ストリームまたはトランザクション識別子が、部分的または全体的に、削除されるようなことがあれば、（個人化電子アイテムを開くことができないように、または、再生することができないように、等）機能を失わせることもできる。このため、個人化電子アイテムは、常にトランザクション識別子を保持することになり、（検証団体を通して）電子アイテムを購入した顧客を特定することができる。また、トランザクション識別子は、購入された電子アイテムの複製が全てトランザクション識別子を持つように付加される。このため、個人化電子アイテムの複製は全てトランザクション識別子を持つので、最初に当該電子アイテムを販売者から購入した顧客（複製の源）は常に、検証団体の安全なデータベースを参照することによって、特定され得る。「トランザクション識別子」は、検証団体が発行するものであり、一意的な識別子であるので、媒体埋め込み識別子としても利用可能であるとしてよい。

【００３４】

購入された電子アイテムにトランザクション識別子が付加されて個人化電子アイテムが作成された後、個人化電子アイテムは、販売者から顧客に与えられる。複数の異なる顧客に配信される個人化電子アイテムはそれぞれ、各トランザクション識別子が異なっており一意的であるので、異なる。このため、電子アイテムを最初に購入した顧客は、当該アイテムを複製した場合には特定される。また、各トランザクション識別子が一意的であるために、購入された電子アイテムの複製が無許可で作成された場合にはその源を、検証団体が保持する安全なデータベースによって、特定することができる。

【００３５】

顧客には、顧客登録時（顧客がクレジット発行者のアカウントを設定または修正する時）および電子アイテム購入時において、個人化電子アイテムの複製には常に顧客自身の情報が残る旨の通知または警告が与えられるとしてよい。また、電子アイテム購入時において、同様の通知または警告を表示して、条件を遵守することに同意している旨、および電子アイテムを無許可で利用または複製した場合には罰則が与えられる旨を顧客に通達することができる。個人化電子アイテムが開かれたり、再生等される度に、（または、最初の数回）、同様の警告を表示するとしてよい。このように継続的に警告を提示することは、所与のダウンロード可能媒体、例えば音楽について、実行するとしてもよいし、実行しないとしてもよい。このような警告によって、トランザクション識別子および／または暗号ストリームに基づけば検証団体が違法なアップロードまたは複製が自分によるものだと突き止めることが可能であることを顧客が認識し、警告に記載されている条件を遵守することに顧客が同意するので、このような警告は、販売者の権利を侵害して（例えば、違法なアップロードまたは複製によって）、顧客が他者に個人化電子アイテムの複製を渡さないようにすることを目的としている。同様に、使用には許可がいること、および、受諾したことを警告で通知することは、年齢に基づくアクセス、年齢または住所に基づく販売価格の決定等に利用されるとしてもよい。本明細書に記載する実施形態によれば、電子商取引およびその関係者を奨励、推進、および保護するような多岐にわたる顧客識別子が利用可能である。

【００３６】

著作権に関する警告等は、ダウンロード後のオーディオ媒体には利用できない場合がある。しかし、このような警告は、トランザクションの条件として警告に含まれる諸条件を顧客が遵守することに同意する限りにおいて、クレジット発行者との合意を遵守することに同意して諸条件に違反した場合にはその責任を負うことに同意する限りにおいて、ダウンロード前において重要である。当事者は、自らの行動および意思に責任を持つことに同意する。

【００３７】

顧客情報の暗号化は、例えば、以下のように実行されるとしてよい。まず、顧客は第１のコンピュータデバイスを用いてクレジット発行者と接続し、クレジット発行者は第１のコンピュータデバイスにソフトウェアをダウンロードする。ベンダー（本明細書では、「販売者」と同様の意味で用いられる場合もある）は、検証団体への登録のために顧客をクレジット発行者のサイトにリダイレクトすることによって、クレジット発行者の登録代理人として機能するとしてよい。このような構成の利点の例を挙げると、実在するクレジットカードユーザがプログラムにおいてカードを登録すると、このユーザ／顧客は、インターネット等のコンピュータネットワークにおける「カード」の利用を本明細書に記載する実施形態に制限するとしてよく、この結果「カード」を他者が無許可で使用しないように保護することができる。顧客は、有効な配送先住所、正年月日（年齢をグループ分けするため）、銀行口座番号、クレジットカード番号等の実在の秘密情報を渡して、または、格納することに同意する。顧客情報のうち、所与の項目（例えば、銀行口座番号およびクレジットカード番号）は、顧客のコンピュータデバイスには格納されず、その代わりにクレジット発行者または検証団体のデータベースにのみ保持されるが、この情報を具体的に参照する場合には、符号化された識別子または符号化されていない識別子を利用するとしてよい。顧客情報の他の項目または識別子（名前、住所、年齢関連情報等）は、暗号化され

て暗号ストリームを作成し、当該暗号ストリームは、顧客のコンピュータデバイスに格納され、一部分または全てが暗号化に先立って符号化されるとしてもよいし、符号化されないとしてもよい。

【００３８】

「クレジット発行者」という用語は、本明細書において、顧客にクレジット（信用取引）を与える団体を省略した表現である。クレジット発行者は、販売者、ベンダー、銀行、金融機関等であってよい。また、このような任意のクレジット発行者は、検証団体を含むとしてよく、代理人を立てることができるとしてよい。このため、「クレジット発行者」という用語は、上述した例のうちいずれか１つおよび全てを指す。クレジット発行者は、本明細書で説明するように、複数種類のクレジット発行者のうちいずれか１つであってもよい。種類のうち１つを挙げると、クレジットカード、デビットカードまたは同様の種類のカードの発行者がある。別の種類の発行者は、既存のクレジット手段所有者、例えば、既存のクレジットカード所有者に１つの団体で利用したいと思う「カード」を全て登録させて、処理代理人の役目を果たす団体であってよい。別の種類の発行者は、例えば、Ｍｉｃｒｏｓｏｆｔ（登録商標）、またはＹａｈｏｏ！（登録商標）、またはＧｏｏｇｌｅ（登録商標）等のカード／銀行に関係のない種類のクレジット発行者で、ケースバイケースで個人のクレジット枠を決定して、インターネット等のネットワークで個人が利用し得る、識別可能なクレジット額を与える。当業者であれば、数多くのその他の種類のクレジット発行者があり、ここには記載していないが、本明細書の実施形態の構成要素であることを理解されたい。

【００３９】

クレジットは、ネットワークを介してビジネスを行う加入ベンダーとの間で、時には検証を行うクレジット発行者またはその処理代行者によって、処理される。（この代替方法によれば、コンピュータ型のネットワークでは従来のクレジットカードが必要なく、必要なのは合法的な商取引の流れを追跡しつつトランザクションの当事者を保護することであることが分かる。）ベンダーは、自身のクレジット発行者を顧客に示して加入を勧めることによって、このようなプログラムを宣伝するとしてよい。この結果、顧客および顧客の身元情報が保護され、ベンダーの市場性が改善され、ベンダーには支払が保証され、払い戻しおよび詐欺が減少し、すべてベンダーの純利益の改善につながる。

【００４０】

銀行およびソフトウェア会社は、「ビジタ」のコンピュータにソフトウェアをダウンロードしなくてもコンピュータの身元情報を読み出して検証することができるが、ほかのタスクを実行するべくソフトウェアをダウンロードまたはインストールすることができる。顧客の承認を得て、クレジット発行者は、第１のコンピュータデバイスから、一意的なハードウェア識別子（マザーボード、ハードドライブ、プロセッサ等から得られるシリアル番号等）を読み出して登録する。このような一意的なハードウェア識別子は、暗号ストリームにも組み込まれる。顧客が、例えば複数のコンピュータおよびコンピュータデバイスを所有しているか、または、アクセスを持つ場合には、今後の購入トランザクションで利用するべく承認および登録したいと思っているほかのコンピュータデバイスについても、同じ工程を繰り返す。このようなプロセスは、顧客がクレジット発行者のアカウントを設定または修正している時点において実行され得る。

【００４１】

検証団体、金融機関、および／またはクレジット発行者（例えば、銀行）は、顧客との間で、暗号ストリームの構成要素を設定する。例えば、このプログラムをサポートするいずれのベンダーも従う最初の契約／合意を設定する。ベンダーが販売者銀行／取得者の合意の条件に基づいて従うのは、クレジット発行者と顧客との間の合意である。また、検証団体は、クレジット発行者、または、クレジット発行者が利用する処理代行人または代理人であってもよく、この処理代行人または代理人は顧客情報を有するデータベースにアクセスする。

【００４２】

顧客の種類の例をいくつか挙げると、（１）新規顧客（コンピュータネットワーククレジット、例えば、新規クレジットカード、新規デビットカード、または、給与デビットカード等のその他の形式の「負荷」カードに申し込む顧客）、（２）既に関係がある顧客（インターネット等のコンピュータネットワークでの購入に利用され得る既存のクレジット手段、例えば上の（１）に示したような種類のクレジットの所有者）、または（３）既にクレジット手段を持つ新規顧客（例えば上の（１）に示したような種類のクレジット手段／カードを既に持つ人物は、このような「カード」の一部または全てを単一の団体に登録して、この「プログラム」を登録した「カード」全てに付与させるとしてよい）、がある。

【００４３】

「クレジット」は、既存のクレジットカード、デビットカード等によって提供されるとしてもよいし、または、さまざまな規則および規制に従って、このようなクレジット、一種の電子信用状を識別可能な個人に与えたいと考えている別のクレジット供給元によって新規に発行される「クレジット」として提供されるとしてもよい。顧客とクレジット発行者とが、登録デバイスのハードウェア情報と共に、どの識別子を提供するかについて合意して、顧客が実在することを確認するのは、尚、既存の顧客であれば情報は既に銀行のデータベースに格納されていると思われるが、顧客の身元情報等の情報をこのようなクレジット発行者に登録するプロセスである。

【００４４】

顧客情報の構成要素、例えば、年齢特定等は、暗号ストリームに格納されているのではなく、データベースから推定され得る。しかし、正年月日または一意的な単語が、暗号ストリームの一部に含まれるとしてもよい。

【００４５】

別の実施形態によると、販売者が取引をしている相手が間違いなく顧客であることをさらに証明するためのプロセスの１つとして、暗号ストリームが販売者へと転送されるタイミングと略同じ時点において、しかし、（暗号ストリームを転送するプロセスの一部として）実際に暗号ストリームを販売者へ転送するより前の時点において、暗号ストリームに、第２のコンピュータハードウェア識別子群および日時スタンプを、暗号ストリームを実際に転送するコンピュータデバイスから組み込む段階を備える方法が提供される。このような構成とすることによって、悪意を持つ人物が暗号ストリームを不適切に複製できて、このような暗号ストリームの不正な複製を、おそらくクレジット発行者が供給する必要な暗号ストリーム作成および転送ソフトウェアを有するコンピュータ（検証団体に登録されている顧客のコンピュータのいずれでもないもの）で利用している場合、暗号ストリームの転送直前に読み出される第２のハードウェア識別子は、暗号ストリーム内のハードウェア識別子とは一致せず、検証団体はトランザクションを承認しないであろう。同様に、時間スタンプおよび日付スタンプに基づいて、販売者に供給される暗号ストリームを限定期間（例えば、分、時間、日数等）のみ有効とすることもできる。このようなプロセスによって、検証団体が実行する「顧客の存在」の証明プロセスをさらに向上させることができ、ベンダーに対して、取引相手が実際に顧客であってそれ以外の何者でもないことをさらに保証することができる。本明細書に記載する実施形態は、顧客が暗号ストリーム／署名を利用する場合は常に顧客が実在するか否かおよび条件に合意しているか否かを確認することに加えて、特定のベンダーの不正行為が現在または過去から問題となっている場合、クレジット発行者は、ベンダーのプログラムへの加入を拒絶することができる。このような構成とすることによって、さらに顧客および信頼の高いベンダーの保護が強化される。

【００４６】

顧客のコンピュータデバイスで暗号ストリームを作成すること、および、証明ステップのために販売者に暗号ストリームを転送することを目的として標準的なクレジット発行者ソフトウェアプログラムを利用することによって、当該ソフトウェアがあるデバイスが確実に特定される。このため、この識別子が担保の暗号ストリームに含まれる識別子と一致しない場合、トランザクションは承認されない。

【００４７】
本明細書に記載する実施形態はさらに、クレジット発行者によって顧客のコンピュータ内に設けられるエンコーダを利用する１以上のシステムを含む。このエンコーダは、暗号ストリーム内の顧客識別情報を暗号化する。さらに、クレジット発行者は、顧客のコンピュータ内および販売者に転送エージェントを設ける。この転送エージェントによって、購入された電子アイテムについての購入トランザクションにおいて、顧客のコンピュータから販売者のコンピュータへと暗号ストリームが転送される。
【００４８】
検証団体は、トランザクションの検証段階において、顧客のコンピュータおよび／または販売者のコンピュータに動作可能に接続されている検証部を有する。本明細書に記載する実施形態によると、顧客情報の安全性を高めるべく、検証部は、検証団体において維持されることによって、顧客のコンピュータおよび販売者とは別個に設けられる。顧客支払情報のデータベースは、検証団体内において維持されるとしてもよいし、または、検証団体とは別個に設けられるとしてもよい。どちらにしても、当該データベースは、検証部にのみ動作可能に接続され、顧客も販売者もアクセスできない。
【００４９】
本明細書に記載する方法の工程を実行するべく、転送エージェントは、販売者のコンピュータから検証部へと、支払の検証のために暗号ストリームを転送させる。検証部はさらに、データベースの情報に基づいて身元証明および支払承認を生成して、身元証明および支払承認を販売者へと転送する。繰り返し説明するが、暗号ストリーム、または、一意的な身元証明および支払承認が、販売者によって、購入された電子アイテムに付加されて、販売者から顧客へと供給される個人化電子アイテムを作成する。
【００５０】
本発明の実施形態の上記およびその他の側面は、以下に記載する説明および添付図面と共に参照することによって、より良く理解されるであろう。しかし、以下に記載する説明は、本発明の好ましい実施形態に言及すると共にそれらの具体的且つ詳細な内容を数多く挙げるが、本発明を例示するために記載されているのであって、本発明を限定するものではないと理解されたい。本発明の実施形態の範囲内において、本発明の精神から逸脱することなく、多くの点で変更および変形を成すとしてよく、本発明の実施形態はそのような変形を全て含むものである。
【図面の簡単な説明】
【００５１】
本発明の実施形態は、以下に記載する詳細な説明および添付図面を参照することによって明らかとなる。添付図面は以下の通りである。
【００５２】
【図１】本発明の一実施形態に係るアーキテクチャを示す概略図である。
【００５３】
【図２】本発明の実施形態を示すフローチャートである。
【００５４】
【図３】本発明の実施形態を示すフローチャートである。
【００５５】
【図４】本明細書に記載する実施形態に係るシステムを示す概略図である。
【００５６】
【図５】本明細書に記載する実施形態に係るシステムを示す概略図である。
【００５７】
【図６】本明細書に記載する実施形態に係る暗号ストリームを示す概略図である。
【００５８】
【図７】本明細書に記載する実施形態に係る方法を示すフローチャートである。
【００５９】
【図８】本明細書に記載する実施形態に係る方法を示すフローチャートである。

【００６０】
【図９】本明細書に記載する実施形態に係る方法を示すフローチャートである。
【００６１】
【図１０】本明細書に記載する実施形態に係るシステムを示す概略図である。
【発明を実施するための形態】
【００６２】
本発明の実施形態、ならびに、本発明のさまざまな特徴および利点を、添付図面に図示されると共に以下で詳細に記載される実施形態を参照しつつより詳細に説明する。実施形態は本発明を限定するものではない。図面に図示する特徴は、必ずしも実寸に即しているわけではないことに留意されたい。公知の構成要素および処理技術に関する説明は、本発明の実施形態を不必要にあいまいにすることを避けるべく省略する。本明細書に記載する具体例は、本発明の実施形態を実施し得る方法を理解しやすくすることと、当業者が本発明の実施形態を実施できるようにすることとを目的として記載しているに過ぎない。したがって、以下に記載する具体例は、本発明の実施形態の範囲を限定するものとして解釈されるべきではない。
Ｉ．基礎の開示の「発明を実施するための形態」
出願番号第１０／９７０，０５１号
米国特許第６，８３９，６９２号
優先日：２０００年１２月１日
【００６３】
以降では図面を参照しつつ説明するが、図１は、本発明の好ましい実施形態を示す概略図である。より具体的には、図１は、ネットワーク１７０に接続されているパーソナルコンピュータ１００を示す図である。さらに、コード確認サイト１３０、販売者サイト１４０、金融機関１５０、および、クレジット代理人１６０もまた、ネットワーク１７０に接続されている。図１に図示されている特徴の配置は、本発明を説明することを目的として、適宜選択されたものである。当業者であれば、本発明ではこのほかにも多くの別の配置が可能であることが分かるであろう。
【００６４】
パーソナルコンピュータ１００（本明細書では「顧客のコンピュータ」とも呼ばれる場合がある）は、ネットワーク１７０と接続可能な任意の形態のコンピュータデバイスを含む。このため、顧客のコンピュータ１００は、標準のデスクトップパーソナルコンピュータ、携帯可能コンピュータ、携帯情報端末（ＰＤＡ）、携帯電話等を含むとしてよい。好ましい実施形態によると、顧客のコンピュータ１００は、グラフィカルユーザインターフェース（ＧＵＩ）１１０と、例えば磁気ハードドライブ等の読み書きストレージデバイスであるストレージデバイス１１２とを有する。また、顧客のコンピュータ１００は、暗号化部１１４、ネットワーク接続１１６、供給部１１８、中央演算処理装置（ＣＰＵ）１２０を有する。
【００６５】
金融機関１５０は、後述するように、クレジット代理人１６０から取得した過去のアドレスのデータベース１５４と、顧客のアドレスをチェックするために利用される比較器１５２とを有する。
【００６６】
図１に示したシステムの動作を、図２にフローチャートで説明している。具体的には、本発明に係るシステムは、顧客のコンピュータ１００に付加される。顧客は、グラフィカルユーザインターフェース１１０を用いて、２００に示すように、本発明に係るシステムに今後アクセスするためのパスワードを作成するのが好ましい。顧客はその後、社会保障番号、住所、生年月日、親戚の名前、クレジットカード情報、銀行情報、職業情報等の個人情報を、グラフィカルユーザインターフェース１１０を介して、本発明に係るシステムへと提供する。暗号化部１１４は、２０２に示すように、即座にこの情報を暗号化して、暗号化された情報を顧客コードとしてストレージデバイス１１２に格納する。

【００６７】
本発明の重要な特徴は、顧客の個人情報が暗号化状態でのみ格納される点にある。このため、不当なユーザがユーザのストレージデバイス１１２にアクセスできたとしても、顧客の個人情報は暗号化されているために安全である。
【００６８】
暗号化プロセスには、３つの要素が含まれており、（１）金融機関で保持されている復号コードと対を成している暗号コード自体、（２）暗号化情報にアクセスするべく顧客が作成して管理している、顧客の個人鍵、パスワード、および／または個人アクセスコード、および（３）暗号化された情報は顧客のコンピュータのみでアクセスされるよう求める、顧客のコンピュータのシステム識別子、である。顧客の情報が入力されると、これら３つの要素およびいずれかの情報を再入力する必要があるか否かが、どの電子商取引トランザクションでも（例えば、二重鍵または公共鍵）、全ての当事者に明らかになる。
【００６９】
暗号化コードが不当な第三者の手に落ちても、この情報にアクセスするためには依然として、顧客の個人鍵が必要であると共に、アクセスは顧客の特定のストレージシステムから行わなければならない（例えば、顧客のコンピュータのシステム識別子が必要である）。不当なユーザはこの情報にアクセスするには復号コードが必要であり、この復号コードは金融機関（クレジット発行者）および金融機関の公認代理人のみが保持している。このような、本発明の好ましい実施形態の「公共鍵」または「二重鍵」の要素によって、顧客の情報の安全性が高められる。
【００７０】
不当ユーザが上述したような予防手段をくぐり抜けたとしても、本発明ではユーザに対して正当な発送先住所を供給するように要求する。この手順は、金融機関との間で別の安全なトランザクションを必要とし、電子メールで顧客に確認される。このようなステップによって、不当アクセスが非現実的になる。
【００７１】
本発明の別の実施形態によると、ユーザは複数の顧客コードを作成することができ、顧客コード毎にクレジット代理人が異なるとしてよい（例えば、クレジットカードが異なる）。このため、本発明によれば、ユーザは、所有しているクレジットカードそれぞれについて顧客コードを作成することができる。
【００７２】
さらに、同じクレジットカードについて多くの顧客コードを作成することもできる。このように追加で作成された顧客コードは、それぞれ使用限度額が異なるとしてもよい。このような構成とすることによって、ユーザは、予算等の理由に応じて顧客コードを変更することができる。例えば、本発明によればユーザは、個人的な予算またはビジネスの予算の項目毎に顧客コードを作成することができる。使用限度額に到達すると、予算情報が変更または更新されるまで、それ以上のトランザクション（購入）は行われない。予算プランは、定期的な予算を自動的に設定するべく、自動的に更新されるとしてもよい。この例としては、クレジットカードでインターネットサービスプロバイダ（ＩＳＰ）の月極め利用料金を所定期間、例えば１年間にわたって支払うための顧客コードが挙げられる。この顧客コードは、トランザクションに関して、毎月の限度額として月額ＩＳＰ料金を設定して、１２ヶ月という期限を設定する。本実施形態によるとさらに、顧客は、限度額を変更することによって、任意の時点でトランザクションを修正またはキャンセルすることができるようになるという利点が得られる。
【００７３】
同様に、親が子供それぞれについて顧客コードを作成して、各顧客コードの使用限度額を異ならせるとしてもよい。一実施形態によると、使用限度額は、定期的に更新されて、定期的に小遣いを与えるとしてもよい。本発明のこの側面によって、親は子供に対して毎月のインターネット小遣いを与えることができる。親は、別個に承認された顧客コードを１つ作成して、複数の周期的（例えば、月毎、または週毎）限度額を設定する。このよう

な構成とすることによって、親は、承認されたサブアカウントの作成および利用を管理するようになる。

【００７４】

本発明の上述したような側面が奏する効果は、金融機関が常に顧客へのクレジットの認定を管理する点にある。しかし、クレジットについて管理および利用が幅広くなり、顧客はその恩恵を受けるであろう。

【００７５】

顧客コードは、ユーザの名前、住所、およびクレジットカード番号を暗号化状態で含むことが好ましい。顧客コードが作成されてストレージ１１２に暗号化状態で格納されると、本発明は、顧客がネットワーク１７０を利用して購入を実行したいと思うまで、顧客のコンピュータ１００においてバックグラウンドで実施される。購入時には、ユーザはグラフィカルユーザインターフェース１１０によって複数の異なる支払オプション（顧客コード）を提示される。ユーザが適切な顧客コードを選択した後、供給部１１８は、２０４に示すように、販売者サイト１４０に向けてネットワーク１７０上で顧客コードを送信するための命令を発行することによって、販売者のサイト１４０に顧客コードを送信する準備を行う。

【００７６】

２０４に示した機能による処理は、図３により詳細に図示する。具体的には、本発明によれば、供給部１１８を用いて販売者のサイト１４０の適切な「チェックアウト」ボックスを自動的にポピュレートするための顧客コードが得られる。図３に示すように、顧客が販売者のサイトのチェックアウト（購入）ウィンドウに行くと（３００）、顧客はカーソルを適切なボックス（例えば、クレジットカード番号フィールド、顧客コードデータフィールド等）に合わせる（３０２）。販売者のサイト１４０の多くでは、顧客コードデータフィールドのスペースが無い場合がある。このため、本発明では、クレジットカード番号（またはその他の同様の支払フィールド）を販売者のサイトで利用できるようにしている。暗号化された顧客コードデータフィールドは、クレジットカード番号よりも長い。このため、本発明を取り入れるために販売者のサイト１４０で必要な修正点は、クレジットカード番号フィールドで受け入れ可能な暗号化データ列の長さを大きくする点のみである。

【００７７】

ユーザは、適切なボックスにカーソルを合わせると、キーボードの予め設定された機能キーを押下（または、グラフィカルユーザインターフェース上のボタンを選択）して（３０４）、ユーザＩＤおよびパスワードの入力ポップアップウィンドウを開く（３０６）。適切なユーザＩＤおよびパスワードを入力すると、顧客コードは全て販売者のサイトのフィールドにポピュレートされる（書き込まれる）。ユーザは、名前、住所等を入力する必要はない。このような情報は全て顧客コードに含まれているからである。後述するが、クレジットトランザクションが承認されると、金融機関１５０は、名前、発送先住所、クレジット承認番号（クレジットカード番号ではない）を、販売者のサイト１４０に返して、ユーザがこのような情報を入力しなくてすむようにする。

【００７８】

複数の異なるクレジットカードについて複数の顧客コードが作成されている場合、ユーザは、クレジット限度額が十分で、利子率が望ましい等の理由から購入を実行するためのクレジットカードに関する情報を含む顧客コードを選択することができる。顧客コード自体は、暗号化された個人情報データストリームであり、ある程度の長さがある。このため、グラフィカルユーザインターフェースは、ユーザによって利便性が高くなるように、省略された名前を載せた選択メニューを提供する。例えば、一実施形態によると、クレジットカードの省略名が記載されたプルダウンメニューが与えられて、使用すべき顧客コードをユーザに選択させる。ユーザが作成した顧客コードが１つのみである場合は、プルダウンメニューが含む顧客コードの省略名は１つのみである。同様に、適切な顧客コードを選択させるためにプルダウンメニューに記載する省略名は、予算カテゴリーまたは子供の名前であってもよい。

【００７９】
ユーザＩＤは、顧客コードの省略形である。ユーザＩＤ／パスワードが間違っていて（３１０）、ユーザＩＤ／パスワードの再入力のためにボックス３０４が再度表示されると、エラーメッセージが生成される。公知であるが、ユーザＩＤ／パスワードの再入力の許容回数は制限されている。
【００８０】
パスワード／ユーザＩＤが正しい場合（３０８）、顧客には支払に関してルールを設定する（３１２）という選択肢が与えられる。例えば、上述したように自動的に毎月ＩＳＰの支払を実行する、というようなルールを設定する。支払について特にルールを設定しない場合は、１回の直接的な支払を行うと仮定されて、ボックス３１６に進む。一方、支払ルールを設定する場合には、別のウィンドウが現れて（３１４）、ウィザードによって、顧客にトランザクション額、クレジット限度額の合計、および／または、期間等の支払オプションを設定させる。
【００８１】
３１６において、本発明では、既に暗号化されている顧客の秘密データに対して、購入特定トランザクション番号およびルール（ある場合）を付加する。本発明はさらに、必要なルーティング情報を添付する前に、このような追加データ（トランザクション番号、ルール等）を暗号化して、完成した顧客コードを自動的に顧客コードデータフィールドまたはクレジットカードフィールド３０２にポピュレートさせる。上述したように、顧客コードは、クレジットカード番号、ルール、トランザクション番号、顧客の名前、および住所等を含む複数のデータから成る暗号化データ列である。
【００８２】
図２に戻って、本発明の一実施形態によると、２０８に示すように、顧客コードを販売者サイト１４０に直接送信する。別の実施形態によると、コード確認サイト１３０が用いられる（２０６）。本実施形態によると、顧客コードは、供給部１１８によって、販売者サイト１４０ではなくコード確認サイト１３０へ送られる。コード確認サイト１３０は、クレジット代理人によって管理されており、クレジット代理人に公共鍵（例えば、暗号コードおよび復号コード）を周期的に更新または変更させて、顧客コードが適切な形式であるか否かを判断する。コード確認部１３０によって顧客コードが不適切であると判断された場合には、２１２に示すように、顧客コードが不適切である旨を説明するエラーレポートが発行される。顧客コードが適切である場合には、２１４に示すように、コード確認部１３０から販売者サイト１４０に送信される。
【００８３】
販売者サイト１４０は、顧客コードを受信すると、当該顧客コードを金融機関１５０に転送する。本発明は、どの時点においても暗号化されていない状態で機密情報が販売者に提供されることはない点を、重要な特徴がある。このため、販売者は、このような機密情報を取り扱う責任を負わなくて済む。
【００８４】
２１８に示すように、金融機関が顧客コードを復号する。続いて、金融機関は、クレジットトランザクションが受諾可能か否か（例えば、顧客が十分な利用可能クレジットを有しているか否か）確認している間に、比較器１５２を用いて、品物の発送先である発送先住所と、クレジット代理人１６０から金融機関に供給される承認発送先住所の履歴データベース１５４とを比較する。本発明のこの側面によって、顧客の住所以外の住所に、犯罪者によって品物が不適切に回されてしまう自体を防ぐことができる。
【００８５】
本発明の一実施形態によると、顧客は、直接クレジット代理人との間で、複数の承認発送先住所を登録することができる。このような複数の住所には、職場または自宅といった選択肢が含まれるとしてよい。それぞれの住所は、顧客のストレージデバイスに、別個の顧客コードとして別個の暗号シーケンスと共に、入力および格納されている。顧客が新規の顧客コードを設定する時点において、顧客の新規の承認住所が、顧客のコンピュータ１

００からクレジット代理人１６０に直接、ネットワーク１７０を介して（電子メールまたは同様の電子転送方式で）送信され、クレジット代理人１６０のデータベースに格納された、当該顧客に対応付けられている承認住所リストに追加される。

【００８６】

２２０に示すように、発送先住所がデータベース１５４に格納されている住所と一致して、且つ、顧客が十分なクレジットを有している場合、２２４に示すように、確認コード、名前、住所等の必要な情報が販売者１４０に送信される。この場合、「一致」という用語は、２つの住所が実質的に同一でなければならないことを意味する。このため、番地または郵便番号の一部が間違っていたり、または、町名が少し異なっている場合であれば、トランザクションを承認して、修正された住所が販売者に与えられる。しかし、発送先住所が、顧客について承認された住所と一致していない住所（例えば、別の州または都道府県、別の市、別の町等の住所）に変更されると、販売者サイト１４０に対してエラーレポートが発行されて、不適切なトランザクションがあった旨を説明する電子メールが顧客に送信される。

【００８７】

現時点においてクレジット代理人は、住所に基づいて、承認するか否かの判断を行っている。しかし、住所が「一致している」と判断する基準はさまざまである。本発明では、住所を「修正」することによって、承認においてエラーおよび詐欺行為を防止するシステムを構成している。このため、承認または修正された住所にのみ品物が発送されることを保証するのは、販売者の責任となる。本発明のこの側面によって、セキュリティを一段階追加することができ、顧客は承認していない発送物を「傍受」および返送することができる。

【００８８】

本発明の一実施形態によると、顧客は「ルール・ウィザード（３１４）」を用いて、「非永久的」発送先住所を一時的に追加することができる。このような構成とすることによって、顧客は他者にプレゼント等を贈ることができるようになる。このような臨時の変更を行うべく当該「ウィザード」にアクセスするためには、顧客のコンピュータのシステム識別子およびパスワードが必要となる。また、このように承認されていない住所へ発送する場合には、確認するための電子メールを顧客に送信して、トランザクションが詐欺である場合には顧客に注意を促すとしてよい。

【００８９】

上述したように、販売者サイト１４０には、顧客コードを受信するべく適切な形式を持つ入力フィールド（現在のクレジットカードフィールドであってよい）があることが好ましい。入力フィールドの形式は、クレジット代理人１６０によって定められ、金融機関１５０でも同様に必要となる。国内に存在するクレジット代理人１６０の数は比較的少ない（Ｖｉｓａ（登録商標）、ＭａｓｔｅｒＣａｒｄ（登録商標）、ＡｍｅｒｉｃａｎＥｘｐｒｅｓｓ（登録商標）等）。一般的に、クレジット代理人１６０は、クレジット代理人１６０と取引を行う、自身よりも数の多い金融機関１５０から提供されるべき情報の形式を、定めることができる。また、金融機関１５０と取引を望む販売者サイト１４０では、金融機関１５０（つまり、クレジット代理人１６０）のデータ形式の要件に従わなければならない。このため、本発明は、多数の販売者サイト１４０が常に加入および脱退しているネットワーク、例えばインターネットに利用可能である。より具体的には、販売者サイト１４０がネットワークに追加されると、各販売者サイト１４０は金融機関１５０の要件に従い、販売者サイト１４０に特定の形式の顧客コードデータフィールドを設ける。このため、ユーザは、顧客による購入が可能であるウェブサイトの圧倒的多数において、このような顧客コードデータフィールドを見ることになる。

【００９０】

言い換えると、本発明は、国内に存在する比較的少数のクレジット代理人１６０と協働して、販売者１４０が利用可能な形式（クレジットカード代理人によって異なる可能性はある）を確立させる。オンラインでのクレジットによる購入トランザクションの大半を担

うクレジット代理人１６０の数は限られているので、このような顧客コード入力フィールドの形式は、大多数の販売者サイト１４０で見られる。このため、本発明によれば、ユーザは、金融機関との取引を望む実質的に全ての販売者サイト１４０（購入トランザクションを完了させたいと願う実質的に全ての販売者サイト）にアクセスできるようになる。

【００９１】

クレジット代理人１６０の仕事は、顧客にクレジット（例えば、クレジットカード）を利用させることにある。本発明によれば顧客はセキュリティを得られる一方、管理および利用に関してさらに進化した特徴が得られると共に、クレジット代理人はクレジット機能を宣伝することができるという利点を得ることができる。また、このような利点を得るために、特別なステップは必要ない。本発明の利点は、顧客情報を繰り返し入力するステップまたは第三者のデータベースに顧客情報を入れるステップが必要なくなる点にある。

【００９２】

安全性に関する本発明の重要な特徴は、販売者サイト１４０が決して顧客の機密情報、例えばクレジットカード番号へのアクセスを得ることがないという点にある。逆に、販売者サイト１４０は、顧客１００からは暗号化された顧客コードを受信するのみで、金融機関１５０からはトランザクション確認コード（および、修正された住所）を受信するのみである。このため、ネットワーク１７０を介した上記のトランザクションのうちいずれかが傍受されたり、または、販売者サイトの記録に不当なアクセスが発生したりという事態が発生したとしても、顧客のクレジットカード情報は安全である。

【００９３】

また、本発明によれば、従来の安全なネットワークトランザクションに対応付けられる問題の多くが回避される。より具体的には、本発明の全ての構成要素が、完了されるべきトランザクションについて、整備されていなければならない。従来のシステムでは、全てのトランザクションについて１段階でセキュリティを提供しており、データベースが破られると、「安全な」サイトの記録がすべてアクセス可能になってしまう。本発明は、個々の記録を保護し、別のレベルのセキュリティを実現している。

【００９４】

本発明から得られる利点には、上記で詳述したように、個別の顧客のオンラインクレジットに対してセキュリティが得られる点、および、顧客がこのようなクレジットを管理して柔軟に利用できる点がある。

ＩＩ．一部継続出願の開示の「発明を実施するための形態」

米国仮出願第６０／８９０，２３０号に基づく優先権の主張

優先日：２００７年２月１６日

【００９５】

本質的に略全世界に及ぶインターネットは、現実には多くの法的権限管轄区域を対象としており、規制する上でさまざまな問題が生じるが、本発明はそのような問題を解決するためのもので、個々のトランザクションに関して個々の契約、インターネット商取引に従事する各当事者について、所定の権利および保護を定める契約を作成するシステムおよび方法を提供する。当事者間で同意する条件に強制力を持たせることによって、各当事者は互いに対する信頼が正当なものであると期待することができ（例えば、「年齢」の条件を満たしていると期待できる、または、トランザクションの実行および責任を取るべく承認されている人物であると期待できる）、本発明は、合意の元で承認された全ての購入の条件を遵守するという合意、当事者間での各トランザクション活動に対する合意等の合意を遵守する方法を定めることによって、商業活動が行われている仮想空間ではなく、各当事者の資産の法的権限管轄区域に基づいて、法的権利および強制可能な権利を定める。

【００９６】

本明細書に開示する実施形態の１つは、顧客とクレジット発行者との間で為される契約（顧客合意）をその中心的概念とする。この顧客合意によって、クレジット発行者は、証明者として機能していたとしても、または、承認された処理代行者または代理人を通していたとしても、顧客とさまざまな加入ベンダーとの間のトランザクションを承認および証

明することができる。顧客とベンダーとの間の合意内容は、顧客とクレジット発行者との間の合意の下で、さまざまなものが予想および許容され、顧客とクレジット発行者との間の合意の下で、クレジット発行者とベンダーとの合意にもさまざまなもの、直接的な合意または間接的な合意が予想および許容される。また、検証団体と、デビットカードおよび／あるいはプリペイドカードまたはその他の有効な資金提供者と、個々の顧客／消費者との間にも、合意または契約が為されている。尚、検証団体は、独立した団体であってもよいし、クレジットを発行する金融機関と協力しているとしてもよい。

【００９７】

顧客の合意は、本明細書に記載する実施形態に関する活動全ての中心を成すものである。顧客の合意によって、顧客が遵守すべき規則および条件が設定される。つまり、コンピュータネットワークにおいて個人の身元情報を保護する代価は、個人のオンラインでの身元情報を構築するすべての要素（例えば、同じコンピュータの他のユーザまたは同じコンピュータにアクセスを有する他の人物からこの個人を識別する識別子を持つ登録コンピュータ）について合意がある限り、自身が行ったトランザクションによって法的に拘束されるという個人の合意である。このような合意は、購入（つまり、責任を負うと共に支払うことに対する合意）、および、著作権または商標を尊重するというような条件への合意、および、このような公の権利についての刑法上および民法上の罰則への法的および個人的に責任を負うことへの合意を対象とする。最も重要な点は、クレジット発行者と顧客との間の合意／契約によって、クレジット発行者は、顧客の合意に言及すると共に、証明された顧客－ベンダー間の合意／トランザクションのいずれについてもこの合意の条件を付与することが許可される。顧客の合意は、クレジット発行者とベンダーとの間の合意に直接的または間接的に適用されるので、ベンダーは、クレジット発行者と顧客との間の合意に基づいて、顧客とベンダーとの間の合意を証明することができる。言い換えると、ベンダーへの支払は、この支払デバイスを利用することによって保証され、個人の安全な身元情報の開示、登録または放棄を必要とすることなく完了される。

【００９８】

顧客の合意は、本明細書に記載する実施形態にしたがって管理される関連トランザクション活動の中心を成す。このような関連トランザクション活動には、コンピュータネットワーク上で実行される顧客と販売者との間の証明可能な、財またはサービス等を対象とするトランザクション、および、最終的に契約によって、直接的または間接的に、ベンダーと金融機関との間で進められ（「ベンダーの合意」）、顧客とベンダーとの間のトランザクションについてのベンダーへの対価は保証され、または「抵当が設けられる」トランザクションが含まれる。顧客の合意に含まれる条件の下では、販売者に対する対価は、支払、信用度、販売者が提供するものの販売または利用する際の条件に対する合意、または、契約が対象とすると共に販売者に対する最初のトランザクションにおいて検証団体が確認する、顧客と販売者との間で為される合意のその他の任意の条件等であってよい。

【００９９】

本明細書に記載する実施形態にしたがって為された契約は、特に、使用条件、第三者の信頼、および、法的権限管轄区域を定める。このため、本明細書に記載する実施形態によると、当事者は、議論を解決するための適切な法的権限管轄区域が、販売者の事業所在地であること、販売者と取引を行う顧客の所在地であること、または、その他の任意の選択された場所であることに合意し得る。使用条件は、「人有り」（「署名有り」と同種）の保証書を含み、これは、販売者が取引する相手が、身元情報が判明している顧客に限られることを保証することと、払い戻しの危険性を被ることなく販売者に確実に支払が行われることとを目的としたものである。このような、人有り保証書は、検証団体が確認するトランザクションが実行される時点において登録顧客識別要素が全て提示されていることによって、得られる。

【０１００】

検証団体は、顧客とクレジット発行者との間の合意およびベンダーとクレジット発行者との間の合意の条件にしたがって、トランザクションの両側の当事者を確認して、購入／

「署名有り」の確認、著作権保護の合意、または、年齢証明の提示等全ての条件に強制力を持たせ、基準とする。基本的に、クレジット発行者が保有する顧客情報は、顧客の情報または顧客の身元情報を実際に明らかにすることなく、第三者によって利用され得る。この点において、クレジット発行者は、顧客および販売者の双方の代理である信用保有者として機能し、検証団体は個別の各トランザクションについてこの点を証明する。これは、トランザクションにおいて顧客の身元情報および販売者の権利を保護する担保型またはエスクロー型の要素となり、ベンダーはこの要素を別に利用するとしてよい。

【０１０１】

インターネット等のネットワークでの購入の一般的な条件には、銀行が発行したクレジットカードまたはデビットカードの利用が含まれる。実質的には、トランザクションがクレジットカードまたはプリペイドカードに基づいたものであろうとなかろうと、発行元の銀行は、ベンダーが実際に支払を受領するまで、当該カードに基づくクレジットを与える。一般的には、この支払手順において銀行は二役を兼任している。つまり、「発行元の銀行」という役割と、「取得側の銀行」の役割である。発行元として、銀行は、財、サービス等の購入に利用されるためのクレジットおよびカードを顧客に発行する。取得側として、銀行は、クレジットカードの利用によって発生する借金を取得すること（および支払を行うこと）に合意している。インターネット上の従来のクレジットカードトランザクションの条件で、「発行元」として機能する銀行は、未払い金額については支払および利子が必要であるという条件にしたがったカードの利用に関する合意を採用している。別の種類の合意の下で、「取得側」として機能する銀行は、販売者に対して、特にクレジットカード使用者の身元情報を証明することと、購入受領書へカード保有者の署名を得ることとを、要求する。これはクレジットカードトランザクションの非常に簡潔な説明であるが、インターネットを介したトランザクションまたは任意の同様のコンピュータ接続商取引システムについて、クレジットカードの不正利用および身元証明の問題を指摘するには十分である。

【０１０２】

ベンダーとクレジット発行者との間の合意にはさらに、正規のベンダーをスクリーニングするという役割もある。電子商取引詐欺の一形態として、ベンダー詐欺が挙げられる。詐欺の経歴を持つと知られているベンダーまたは詐欺の経歴の疑いがあるベンダーについては、合意を取り消すとしてもよいし、本明細書に記載するような署名有りの支払条件およびその他の著作権等の保護への参加を拒否するとしてもよい。このように適切なベンダーを選ぶステップは、顧客の保護および詐欺の抑制のために必要である。

【０１０３】

このような問題を鑑みて、本明細書に記載する実施形態に係るシステムおよびプロセスは、第三者検証団体が、販売者に対して顧客の存在を証明できるように、且つ、クレジット発行者と顧客との間の合意を証明できるように暗号化コード（「暗号ストリーム」）を利用する。当該合意の条件によって、検証団体は、顧客の身元情報およびベンダーとのトランザクションの条件、例えば「署名有り」の支払を遵守するという同意を確認することができる。これに代えて、暗号ストリームにおいて顧客の合意の識別子をただ参照するのではなく、トランザクションの受領書および条件全てを暗号化して暗号ストリームに含めるとしてもよい。

【０１０４】

顧客とベンダーとの間の合意は、クレジット発行者と顧客との間の合意、および、これに基づき、クレジット発行者とベンダーとの間の合意の条件の下で検証される。クレジット発行者と顧客との間の合意およびクレジット発行者とベンダーとの間の合意の遵守に合意することによって、顧客とベンダーとの間の合意の条件が保護される。顧客とベンダーとの間の合意は、クレジット発行者と顧客との間の合意およびクレジット発行者とベンダーとの間の合意の結果得られると予想されるもので、検証可能な暗号ストリームを提示することによってトリガされる顧客の要求に従って、クレジット発行者またはその代理人、例えば処理代行者が、顧客の存在およびトランザクションの条件に対する合意を確認する

と、全ての当事者はそれぞれの合意における自身に関する部分を遵守するものと期待される。

【０１０５】

このため、本明細書に記載する一部の実施形態によると、別個の顧客の合意（検証団体またはクレジット発行者と、顧客との間で為されるもの）および別個の販売者の合意（販売者と販売者の銀行との間で為されるもの）では、顧客および販売者に対して、販売者と顧客との間の購入トランザクションの時点において為される顧客の合意（販売者と顧客との間で為されるもの）を結ぶことを求める。本明細書に記載する実施形態では、顧客に対する保護をさらに向上されるべく、クレジット発行者に対して、ベンダーをスクリーニングする機能を与える。本明細書に記載する実施形態によれば、販売者と顧客との間において購入トランザクションが発生するたびに、新たな顧客の合意が為されるとしてもよい。このような合意は、特定のトランザクションについて適用される場合、販売者または媒体の知的財産権を守るべく特に顧客を拘束するものであり、特定のトランザクションについて適用される場合、顧客の存在、身元情報、年齢等に関して拘束力を持つ記述を含む。

【０１０６】

検証団体は、顧客とクレジット発行者との間の合意、およびこの合意に基づくほかの当事者とクレジット発行者との間の合意の条件に応じて拘束され、顧客の身元情報およびトランザクションを保護して、支払およびその他のトランザクションの条件（例えば、年齢、身元情報、居住区域、著作権条項の尊重および遵守への合意等）を販売者に代わって検証、承認、および保護する。

【０１０７】

暗号ストリームが形成される前に（購入トランザクションの時点において）、個々の顧客の身元情報を確認して、顧客が当座の顧客合意の条件を遵守することに合意するかどうかを検証するべく、所定の要素は提示されなければならない。このような要素には、他にもあるが、名前（必ずしもカード保有者の名前でなくてもよい）、発送先住所または居住状態を確認するための住所（必ずしもカード保有者の請求先住所でなくてもよい）、金融機関における顧客の固有のクレジット番号またはＩＤ、顧客がトランザクションについて承認する予定のコンピュータの登録ハードウェア識別子等が含まれるとしてよい。暗号ストリームは、このような要素、例えば、名前、住所、顧客の合意の識別子、コンピュータハードウェア識別子等のうち一部の要素に基づいて形成するが、顧客のクレジットカード番号または銀行口座番号等の機密情報は含まない。さらに、ＢＩＮ（銀行識別番号）またはその他のルーティング識別子、例えばＩＰアドレスは、暗号化されず、ルーティングを目的として暗号ストリームに追加される。

【０１０８】

このような登録の時点において作成されるクレジット発行者と顧客との間の合意の条件に従って、販売者との間でトランザクションを実行する際に検証団体が顧客の存在を確認できるように、暗号ストリームの必要な要素は全て提示されなければならない。このような情報は暗号化されているので、販売者は顧客の身元情報を認識しないとしてもよい。検証の結果、符号化された要素全ての存在が確認されると、トランザクションが承認されて、発送先情報が必要であれば、販売者に対して発送先が指定され、署名の受領および顧客の身元情報の確認という販売者の要求が満たされる（つまり、販売者に対して支払が行われ、および／または、販売者は、年齢証明および／または著作権等のトランザクション条件について償還請求を持つ）。

【０１０９】

本発明では、クレジット発行者との間で顧客が合意を形成する際に顧客によって設定される条件を用いる。この合意では、顧客の暗号ストリームの必要な要素が全て提示されている全てのトランザクションの責任を顧客が負うことを規定している。この合意ではさらに、著作権保護等の利用条件に対する合意の記録として顧客が取得している任意のデジタル媒体と共に暗号ストリームをダウンロードすることが許可されている。

【０１１０】

本発明の一側面によると、提示される全ての要素と共に用いられて署名として機能する「コード」であって、個々の顧客に一意的で、トランザクションにおいて顧客の存在を確認する、契約によって同意される「コード」を形成、検証および（必要であれば）埋め込むシステムおよび方法が提供される。販売者は、顧客の合意におけるトランザクションについて、顧客が同意している条件（身元情報および法的権限管轄区域も確認する）を利用する権利を持つ。本発明は、このようなトランザクションの条件に全ての当事者が契約上拘束される代わりに、身元情報を保護する。このため、本発明によれば、インターネット購入トランザクションを開始する顧客のプライバシーおよび身元情報を保護することができる一方、製品、サービス等を提供する販売者の権利および商業利益も保護することができる。本明細書に記載されている実施形態によれば、合意の条件が破られたり違反されたりしない限り、暗号化された状態を維持する等の方法で保護されている顧客の身元情報が保護される。

【０１１１】

米国特許出願第２００７／００６１５８０号（参照により本願に組み込まれる）に記載されているように、このような「コード」を削除すると、媒体は利用不可能となる。当該米国出願には、透かしまたはコードが無い場合には、購入された製品に対する電子格納媒体からのアクセスが出来ないようになることが開示されている。購入条件および著作権保護の条件に違反して媒体の複製を複数作成すると、これらの複製には「コード」が含まれているので、販売者は、クレジット発行者の合意の条件および法的権限管轄範囲にしたがって、これら複数の複製を作成した顧客を特定することができる。このため、顧客の合意は、購入時に特に合意された著作権保護の違反の訴追を実行するためのものである。

【０１１２】

要約すると、本発明は、インターネット等のコンピュータネットワークにおける商取引を奨励、保護および検証するための方法、システム、構造、および装置を提供する。具体的には、顧客の身元情報および金融情報等の顧客の権利、および、販売者の製品および／またはサービスに対する支払および販売者の管理および所有権を含む販売者の権利の保護および訴追における法的権限管轄区域を合意で決定しておくことによって、これらの権利を保護する。このため、本明細書に記載する実施形態では、顧客および販売者の合意の元、クレジット発行者および検証団体に契約で定められる機能を与えることによって、トランザクションについて当事者間で拘束力のある契約を締結する。本明細書に記載する実施形態では、トランザクションの要素のうち身元情報および信用度の要素が満たされているか否かを確認する一方、顧客の身元情報を保護し、販売者に対価が支払われることを保証する。このため、本発明は、トランザクションを完了させるためには暗号ストリームの構成要素全てが提示および証明されることを要求することによって、トランザクションにおいて「存在の証明」要素を確立するために、トランザクションに「署名あり」の要素を確立するために、顧客の「年齢」（例えば、「１８歳以上」または「２１歳以上」または「６５歳以上」）を確立するために、住居または配送の要素を確立するために、顧客の合意において顧客／販売者の関係を確立するために、（オンライン上で開示または格納する必要は必ずしもないが）顧客の身元情報を確立するために、利用されるとしてよい。

【０１１３】

以降では添付図面を参照しつつ説明するが、本発明の実施形態は、コンピュータネットワーク４０４におけるトランザクションの権利を保護する方法およびシステムを提供する。図４に示すように、顧客４０２、販売者４５０、および、検証団体４２０、および／または、金融機関４４０の間で結ばれる合意４２２の条件は、検証団体４２０によって格納される。検証団体４２０は、図５に示すように金融機関（クレジット発行者）４４０に含まれるとしてもよいし、図４に示すように金融機関４４０とは別としてもよい。図４に図示する顧客のコンピュータ４１０、検証団体４２０、金融機関４４０、および販売者４５０は１つであるが、当業者であれば想到するように、図４が図示する内容は本発明の実装例の１つに過ぎず、図５に示すように、顧客のコンピュータ４１０、検証団体４２０、金融機関４４０、および販売者４５０等を複数設けるとしてもよい（多くの場合はこのよう

に複数が設けられると考えられる）。このため、検証団体４２０は、購入トランザクション毎に１つの合意４２２を格納するので、複数の合意４２２を格納している。

【０１１４】

本発明の実施形態に係る方法は、クレジット発行者／検証団体４４０／４２０との間で成立した顧客の合意４２２を登録および格納する段階を有する。顧客情報はデータベース４３０に格納されている。データベース４３０は、図５に示すようにクレジット発行者／検証団体４４０／４２０の内部に設けられるとしてもよいし、図４に示すようにクレジット発行者／検証団体４４０／４２０とは別に設けられるとしてもよい。当業者であれば想到するであろうが、図４に図示するデータベース４３０は１つのみであるが、データベース４３０を複数設けて、その一部のデータベース４３０をクレジット発行者／検証団体の内部に設けるとしてもよい。また、顧客のコンピュータ４１０は、１以上のコンピュータネットワーク４０４を介して、販売者４５０および検証団体４２０に接続されている。

【０１１５】

顧客のコンピュータ４１０にあるエンコーダ４１２にアクセスするには、パスワードを用いる。エンコーダ４１２は、顧客登録プロセス時に、検証団体４２０によって顧客のコンピュータ４１０にダウンロードされる。エンコーダ４１２は、顧客情報を暗号化して、暗号ストリーム４１４を作成し、顧客のコンピュータ４１０に暗号ストリーム４１４を格納する。顧客情報は、非暗号化状態では、顧客のコンピュータに格納されない。また、暗号ストリームは、クレジットカード番号、銀行口座番号等に関連する顧客の個人的な金融情報は一切含んでおらず、このような情報が格納されるのはデータベース４３０のみである。

【０１１６】

また、検証団体は、顧客のコンピュータ４１０および販売者４５０に、転送エージェント４１６、４５６をダウンロードする。転送エージェント４１６は、購入された電子アイテム４５４の購入トランザクションにおいて、顧客のコンピュータから販売者のコンピュータ４５０に、暗号ストリーム４１４を転送させる。

【０１１７】

検証団体４２０は、顧客のコンピュータ４１０および販売者のコンピュータ４５０の両方に動作可能に接続されている検証部４２４を有する。本明細書に記載する実施形態によると、顧客情報の安全性を高めるべく、検証部４２４は、クレジット発行者／検証団体４４０／４２０に設けられることによって、顧客のコンピュータ４１０および販売者とは別個に設けられている。顧客の支払情報を格納しているデータベース４３０は、クレジット発行者／検証団体４４０／４２０の内部に設けられるとしてもよいし、または、検証団体４２０とは別個に設けられるとしてもよい。どちらの場合でも、データベース４３０は、検証部４２４にのみ動作可能に接続され、顧客および販売者はどちらも、当該データベースへのアクセスを有さない。

【０１１８】

本発明の実施形態に係る方法を段階毎に実行するべく、転送エージェント４１６が、販売者のコンピュータ４５０から検証部４２４へと、支払の検証のために（トランザクションの金額と共に）暗号ストリーム４１４を転送させる。検証部４２４はさらに、データベース４３０に基づいて支払の証明を生成して、支払いの証明を販売者４５０に転送する。販売者は、暗号ストリーム４１４および／またはトランザクション識別子を、購入された電子アイテムに付加して、（図６に示すように）個人化電子アイテム４５４を作成して、個人化電子アイテム４５４は、販売者４５０から顧客のコンピュータ４１０へと与えられる。

【０１１９】

暗号ストリーム４１４は、顧客の名前、顧客の発送先住所、顧客の生年月日、および顧客のハードウェアコンピュータ識別子等の情報を含むとしてよい。顧客の発送先住所は、どの暗号ストリーム４１４が販売者４５０に与えられるかに応じて選択される複数の有効発送先住所のうち１つの有効発送先住所を含むとしてよい。このため、本発明の実施形態

に係る方法によれば、顧客は、それぞれ有効な発送先住所が異なっている、複数の格納されている暗号ストリーム４１４のうちいずれかを選択することができる。本発明の実施形態に係る方法では、コンピュータネットワーク４０４を介したトランザクションにおいて、選択された暗号ストリーム４１４を、識別コード（ＣＩＤおよびルーティング識別子４１６）の一部であるコンピュータ識別子と共に、販売者４５０に供給する。

【０１２０】

暗号ストリーム４１４は、ルーティング識別子４１６を用いて、コンピュータネットワーク４０４を介して検証団体４２０に転送される。検証団体４２０は、暗号ストリーム４１４を復号化して、顧客の発送先住所識別子、名前識別子、年齢識別子等の識別子を、検証団体４２０が保有している承認済みの顧客識別子のうち対応するもの、例えば、名前、年齢、住所等の「識別子」と比較する。このような名前、年齢、住所等の「識別子」は、実際の名前、住所等であってもよいし、データベース４３０において名前、住所、年齢等を検索するべく検証団体４２０が用いるアルファベットおよび数字から成るコードであってもよい。全てが整っていれば、検証団体４２０は、コンピュータネットワーク４０４を介して販売者４５０に承認決定を返す。このようにして、検証団体４２０は、身元証明、支払承認等を生成することができる（そして、販売者に与える）。検証団体４２０は、検証団体４２０と顧客との間の合意４２２に従って、顧客の存在の証明および電子署名の条件が満たされていることを確認する。合意４２２では、顧客がトランザクションについて責任を負うことを販売者４５０に対して認めている。

【０１２１】

また、各暗号ストリーム４１４は、ほかの暗号ストリーム４１４の支払方法とは異なる固有の支払方法を含むとしてよい。これに代えて、複数の暗号ストリーム４１４から成る暗号ストリーム群が支払について１つのクレジット機関を特定しているが、当該暗号ストリーム群に含まれる各暗号ストリーム４１４は、ユーザ名、承認および登録されているデバイス／コンピュータ、年齢証明方法、および／または、顧客の住所が異なるとしてよい。

【０１２２】

サービスまたは有形財（例えば、ステレオ設備、フィルタ、書籍、日用雑貨、衣料品、家具、コンピュータ等）を含む購入トランザクションについては、顧客および支払承認の証明を与えることに本発明の実施形態を限定するとしてもよい。しかし、コンピュータネットワークを介して不適切な共有が発生し得る電子アイテムを含む購入トランザクションについては、本発明の実施形態に従って、電子アイテムに暗号ストリームまたはトランザクション識別子を付与してよい。このため、合意４２２の一部として、顧客は、図６に示すように、販売者４５０から取得した媒体または媒体コンテンツ４５４に対して、暗号ストリーム４１４およびルーティング識別子４１６を、埋め込むこと、刻みこむこと、および／または、添付することに合意する。検証団体は、暗号ストリーム４１４を販売者４５０に転送する前に、顧客の合意または顧客の合意の識別子を含み得る暗号ストリーム、または、トランザクション識別子を、暗号ストリーム４１４に付加して、顧客４０２と販売者４５０との間で為された顧客の合意４２２に容易にアクセスできるようにするとしてよい。

【０１２３】

また、このプロセスによって、顧客の合意４２２において確立された販売者４０４の権利を実施する法的権限管轄区域が確立される。承認決定は、暗号ストリーム４１４とデータベース４３０内に格納された顧客情報とが一致した場合にのみ、与えられる。当該方法によれば、検証団体４２０から顧客４１４に、トランザクションの確認を通達する旨の電子メールを送信することができる。暗号ストリーム４１４／ＣＩＤが顧客のストレージデバイス４０８に格納される場合は必ず、暗号化された状態で格納される。

【０１２４】

図７にフローチャートで示すように、本明細書において開示する方法によれば、電子的に格納可能なアイテム（本明細書では電子アイテムと呼ぶ場合もある）例えば、文学作品

、音楽作品（録音）、動画作品（映画、ショー、ビデオ等）等についてコンピュータを用いて購入トランザクションを容易に行うことができる。

【０１２５】

まず７００に示すように、顧客は検証団体との間で顧客合意を結ぶ。そして７０２において、本明細書に記載する実施形態によると、「顧客情報」を暗号化して、暗号ストリーム７０４を生成する。データ暗号化技術については、例えば、米国特許第７，２５７，２２５号および第７，２５１，３２６号（参照により本願に組み込まれる）に記載されており、本明細書では開示している実施形態に集中するべく当該プロセスの詳細は省略する。この顧客情報は、名前識別子（顧客の正式名であってもよいし、正式名でなくてもよい）、顧客の年齢識別子（特定の年齢、年齢の範囲、年齢分類であってよい）、住所識別子（顧客の住所または別の住所であってよい）を含むとしてよい。

【０１２６】

７０６において、本明細書に記載する実施形態は、購入された電子アイテムのための購入トランザクションにおいて、暗号ストリームを、顧客から販売者へと転送させる。検証団体は、７０８において、支払の証明のために販売者から送信される暗号ストリームを受信する。そして、検証団体は、受信した暗号ストリームと、顧客の支払情報を格納する別個に設けられているデータベースとを相互参照して（７１０）、身元証明および／または支払承認を含む一意的なトランザクション識別子を生成する。

【０１２７】

検証団体は、７１４において、一意的なトランザクション識別子を検証団体から販売者へと転送する。身元証明および支払承認は、販売者に対して、購入トランザクションの顧客が実在することを認め、トランザクションの相手が顧客以外ではないことを販売者に対して保証する。

【０１２８】

上述したように、暗号ストリーム７０４ならびに身元証明および支払承認７１０は、クレジットカード情報、銀行口座情報等の顧客の個人的な支払情報を含まず、一意的なトランザクション識別子となり得る。このため、暗号ストリームが復号化されても、顧客の支払情報は開示されることはないし、利用可能でもない。このように、顧客から提供される暗号ストリームは、販売者に与えられる前に、検証団体によって変更されて、実行中の購入トランザクションに固有のデータまたは情報を含められるか、または、暗号ストリームには一意的なトランザクション識別子が添付され得る。このような変更暗号ストリームまたは一意的なトランザクション識別子は、本明細書に記載の実施形態によると、本来の暗号ストリームに代わって、利用され得る。このため、本来の暗号ストリーム、変更暗号ストリーム、および／または、一意的なトランザクション識別子は、電子アイテムが顧客に提供される前に、電子アイテムに付加され得る。

【０１２９】

コンピュータネットワーク上で不正に複製および配信される可能性がある電子アイテムの取引が行われる実施形態については、７１６に示すように、暗号ストリームおよび／または一意的なトランザクション識別子が、販売者によって、購入された電子アイテムに付加されて、個人化電子アイテム７１８を生成する。暗号ストリームまたはトランザクション識別子は隠すことが可能であるので、顧客は、個人化電子アイテムから暗号ストリームまたはトランザクション識別子を削除できない。デジタル作品に情報を埋め込む技術は公知である（米国特許第６，６９１，２２９号および第５，８０９，１６０号を参照のこと、両米国特許の詳細な教示内容は、参照により、本願に組み込まれる）。また、暗号ストリームまたはトランザクション識別子が削除されるようなことがあれば、個人化電子アイテムを機能しなくさせるとしてもよい（個人化電子アイテムを開けなくさせるとしてもよいし、または、再生できないようにするとしてもよい）。デジタル作品へのアクセスを暗号ストリームまたは透かしを用いて管理する技術もまた公知である（米国特許第７，０６２，０６９号を参照のこと、本特許の詳細な教示内容は参照により本願に組み込まれる）。

【０１３０】
このように、個人化電子アイテムは常に暗号ストリームを保有して、個人化電子アイテムによって、電子アイテムを購入した顧客を（検証団体を介して）特定することができ、購入された電子アイテムの複製にはすべて、暗号ストリームまたはトランザクション識別子が含まれる。このため、個人化電子アイテムの複製には全て暗号ストリームが含まれているので、販売者から電子アイテムを元々購入した顧客（複製の源）を必ず特定することができる。
【０１３１】
購入された電子アイテムに暗号ストリームまたはトランザクション識別子が付加された後、個人化電子アイテムは、７２０において、販売者から顧客に与えられる。個人化電子アイテムは、付加される暗号ストリームまたはトランザクション識別子が一意的であるために、配信された顧客毎に異なっており、このような構成のために、電子アイテムを元々購入した顧客を、電子アイテムの複製によって特定することができる。また、暗号ストリームまたはトランザクション識別子はそれぞれ一意的であるので、検証団体を介して、購入された電子アイテムの不正複製の源を特定することができる。このため、７２２に示すように、本発明の実施形態に係る方法は、個人化電子アイテムに含まれている暗号ストリームに基づいて顧客を特定する段階を含み得る。
【０１３２】
顧客登録時（顧客がクレジット発行者においてアカウントを設定または修正する際）および電子アイテム購入時において、顧客には、顧客の情報は必ず個人化電子アイテムの複製に含まれる旨の通知または警告が与えられる。また、電子アイテム購入時、同様の通知または警告が表示されて、顧客に対して、電子アイテムの不正な利用または複製に対して規則および罰則が適用され、顧客はこれらの規則および罰則に拘束されることに同意している旨を通達し、個人化電子アイテムが開かれたり、再生等される度に（または最初の数回）、同様の警告が表示されるとしてよい。このような警告は、販売者の権利を侵害して（例えば、不正にアップロードまたは複製して）個人化電子アイテムの複製を他人に供給しないよう、顧客に求めることを意図している。このような警告によって、顧客は不正なアップロードまたは複製が、検証団体を介して暗号ストリームに基づき、自身まで追跡され得ることを認識して、警告に記載されている条件を遵守することに同意することに同意する。同様に、使用には許可がいること、および、受諾したことを警告で通知することは、年齢に基づくアクセス、年齢または住居に基づく販売価格の決定等にも利用され得る。本明細書に記載する実施形態によれば、電子商取引およびその関係者を奨励、推進および保護する顧客識別子を多岐にわたって実現することができる。
【０１３３】
顧客情報の暗号化７０２は、図８に示すように実行される。まず、顧客は第１のコンピュータデバイスを用いてクレジット発行者と接続を行って（８００）、検証団体は第１のコンピュータデバイスにソフトウェアをダウンロードする（８０２）。顧客は、検証団体に対して、例えば、有効発送先住所、生年月日（または年齢のグループ分類）、銀行口座番号、クレジットカード番号等の現存の秘密情報に対するアクセスを与えるか、または、アクセスすることに同意する（８０４）。顧客情報のうち所与の項目（例えば、銀行口座番号およびクレジットカード番号）は、顧客のコンピュータデバイスには格納されず、クレジット発行者および／または検証団体のデータベースにのみ保有されるが、このような情報を特に参照する場合には符号化された識別子または符号化されていない識別子を利用するとしてよい。顧客情報のその他の項目または識別子（名前、住所、年齢情報等）は、暗号化されて暗号ストリームを形成するとしてよい。暗号ストリームは、顧客のコンピュータデバイスに格納され、一部または全てが、暗号化前に符号化されるとしてもよいし、符号化されないとしてもよい。
【０１３４】
８０６において、クレジット発行者は、顧客の承認のもと、第１のコンピュータデバイスから一意的なハードウェア識別子（マザーボード、ハードドライブ、プロセッサ等のシ

リアル番号等）を読み出して登録する。このような一意的なハードウェア識別子は、８０８において、暗号ストリームに組み込まれる。そして、今後の購入トランザクションにおいて使用するべく顧客が承認および登録したいコンピュータデバイスがさらにあれば、同じ工程を繰り返す。このようなプロセスは、クレジット発行者におけるアカウントを顧客が設定または修正している際に実行されるとしてよい。

【０１３５】

本願では、「公共の」または「登録されていない」コンピュータを利用する場合もカバーする。「発行者アカウント」に「登録されていない」コンピュータからアクセスする場合、緊急アクセスを「許可」して、既存のアカウントについてそのコンピュータを「制限付」で承認することができる。この承認は、時間が制限されていたり（例えば、一回の購入について１５分）または利用が制限されていたりするとしてよい（例えば、使用／購入は一回に限る）。

【０１３６】

別の実施形態によると、販売者が取引している相手が間違いなく顧客であることをさらに証明するためのプロセスの１つとして、暗号ストリームが販売者へと転送されるタイミングと略同じ時点において、しかし、（暗号ストリームを転送するプロセスの一部として）実際に暗号ストリームを販売者へ転送するより前の時点において、本発明の実施形態に係る方法は、暗号ストリームに、暗号ストリームを実際に転送するコンピュータデバイスから、第２のハードウェア識別子群および日時スタンプを組み込むことができる。このため、図９に示すように、９００においてハードウェア識別子が暗号ストリームに追加された後、本発明の実施形態に係る方法は、９０２に示すように、販売者に接続されている実際のコンピュータから第２のハードウェア識別子群を読み出す。この第２のハードウェア識別子群（および時間スタンプおよび日付スタンプ）は、９０４において、暗号ストリームに付加されて、９０６において、変更暗号ストリーム（ハードウェア識別子群を両方有する）を販売者に送る。

【０１３７】

このような構成とすることによって、悪意を持つ人物が暗号ストリームを不適切に複製できて、このような暗号ストリームの不正な複製を、おそらくクレジット発行者が供給する必要な暗号ストリーム作成および転送ソフトウェアを有するコンピュータ（販売者に登録されている顧客のコンピュータのいずれでもないもの）で利用している場合、暗号ストリームの転送直前に読み出される第２のハードウェア識別子は、暗号ストリーム内のハードウェア識別子とは一致せず、検証団体はトランザクションを承認しないであろう。同様に、時間スタンプおよび日付スタンプに基づいて、販売者に供給される暗号ストリームを限定期間（例えば、分、時間、日数等）のみ有効とすることもできる。このようなプロセスによって、検証団体が実行する「顧客の存在」の証明プロセスをさらに向上させることができ、販売者に対して、取引相手が実際に顧客であってそれ以外の何者でもないことをさらに保証することができる。

【０１３８】

本発明の実施形態は、完全にハードウェアとして実装されるとしてもよいし、完全にソフトウェアとして実装されるとしてもよいし、ハードウェア構成要素およびソフトウェア構成要素を含むものとして実装されるとしてもよい。一実施形態によると、本発明は、ソフトウェアで実装される。ソフトウェアは、これに限定されないが、ファームウェア、常駐ソフトウェア、マイクロコード等である。

【０１３９】

さらに、本発明の実施形態は、コンピュータまたは任意の命令実行システムによって利用される、または、これらと共に利用されるプログラムコードを提供するコンピュータ利用可能媒体またはコンピュータ読み出し可能媒体からアクセス可能なコンピュータプログラム製品として実装されるとしてよい。本明細書では、コンピュータ利用可能媒体またはコンピュータ読み出し可能媒体は、命令実行システム、命令実行装置、または命令実行デバイスによって利用される、またはこれらと共に利用されるプログラムを、有する、格納

する、通信する、伝播させる、または移送する装置であればどのような装置であってもよい。

【０１４０】

媒体は、電子的、磁気的、光学的、電磁的、赤外線、あるいは半導体のシステム（あるいは、装置、あるいはデバイス）または伝播媒体であってよい。コンピュータ読み出し可能媒体の例を挙げると、半導体メモリあるいは固体メモリ、磁気テープ、取り外し可能コンピュータディスケット、ランダムアクセスメモリ（ＲＡＭ）、リードオンリーメモリ（ＲＯＭ）、硬い磁気ディスク、および光学ディスクが含まれる。光学ディスクの現時点における例を挙げると、コンパクトディスク－リードオンリーメモリ（ＣＤ－ＲＯＭ）、コンパクトディスク－リード／ライト（ＣＤ－Ｒ／Ｗ）、およびＤＶＤ等がある。

【０１４１】

プログラムコードを格納および／または実行するのに適しているデータ処理システムは、システムバスを介してメモリ要素と直接的または間接的に結合されている少なくとも１つのプロセッサを備える。メモリ要素は、プログラムコードを実際に実行する際に利用されるローカルメモリ、バルクストレージ、および、実行中にバルクストレージからコードを取得すべき回数を減らすべく少なくとも一部のプログラムコードを一時的に格納するキャッシュメモリを含むとしてよい。

【０１４２】

入出力（Ｉ／Ｏ）デバイス（これらに限定されないが、キーボード、ディスプレイ、ポインティングデバイス等）は、直接的に、または、入出力コントローラを介在させて、システムに結合されるとしてよい。システムにはさらに、ネットワークアダプタを結合させて、データ処理システムと、別のデータ処理システムまたはリモートプリンタあるいはリモートストレージデバイスとを、私有または公共のネットワークを介在させて、結合するとしてよい。現在利用可能な種類のネットワークアダプタの数例を挙げると、モデム、ケーブルモデム、およびイーサネット（登録商標）カード等がある。

【０１４３】

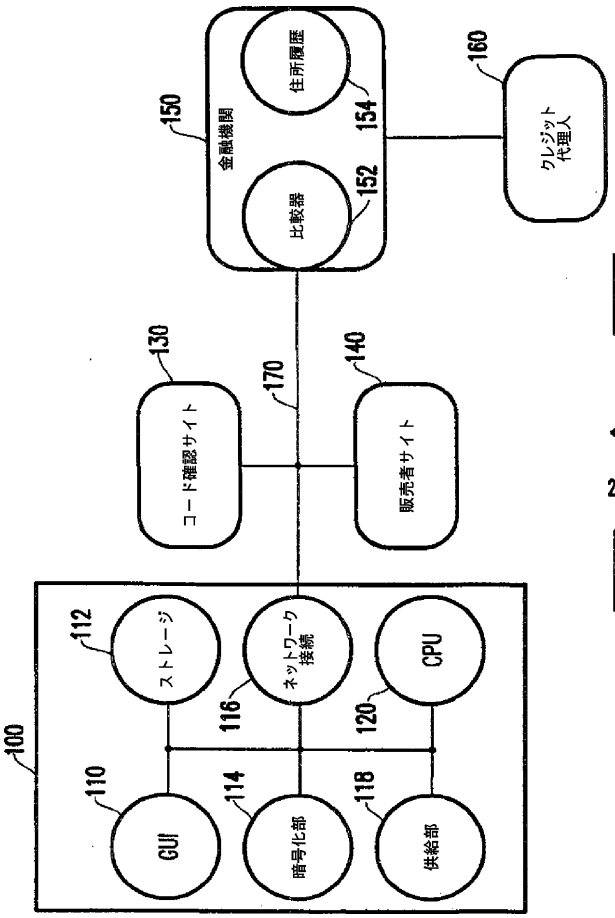
本発明の実施形態を実施するための代表的なハードウェア環境を図１０に示す。同図に示す概略図は、本発明の実施形態に係る情報処理／コンピュータシステムのハードウェア構造を説明するためのものである。当該システムは、プロセッサまたは中央演算処理装置（ＣＰＵ）１０を少なくとも１つ備える。ＣＰＵ１０は、システムバス１２を介して、ランダムアクセスメモリ（ＲＡＭ）１４、リードオンリーメモリ（ＲＯＭ）１６、および入出力（Ｉ／Ｏ）アダプタ１８等のさまざまなデバイスに相互接続される。Ｉ／Ｏアダプタ１８は、ディスク部１１およびテープドライブ１３、またはシステムによって読み出し可能なその他のプログラムストレージデバイス等の周辺機器に接続され得る。当該システムは、プログラムストレージデバイスに格納されている本発明に係る命令を読み出して、これらの命令に従って本発明の実施形態に係る方法を実行することができる。当該システムはさらに、キーボード１５、マウス１７、スピーカー２４、マイクロフォン２２、および／または、タッチスクリーンデバイス（不図示）等のその他のユーザインターフェースデバイスをバス１２に接続して、ユーザ入力を収集するユーザインターフェースアダプタ１９を備える。さらに、通信アダプタ２０は、バス１２をデータ処理ネットワーク２５に接続して、ディスプレイアダプタ２１は、バス１２をディスプレイデバイス２３に接続する。ディスプレイデバイス２３は、モニタ、プリンタ、または送信器等の出力デバイスとして実現され得る。

【０１４４】

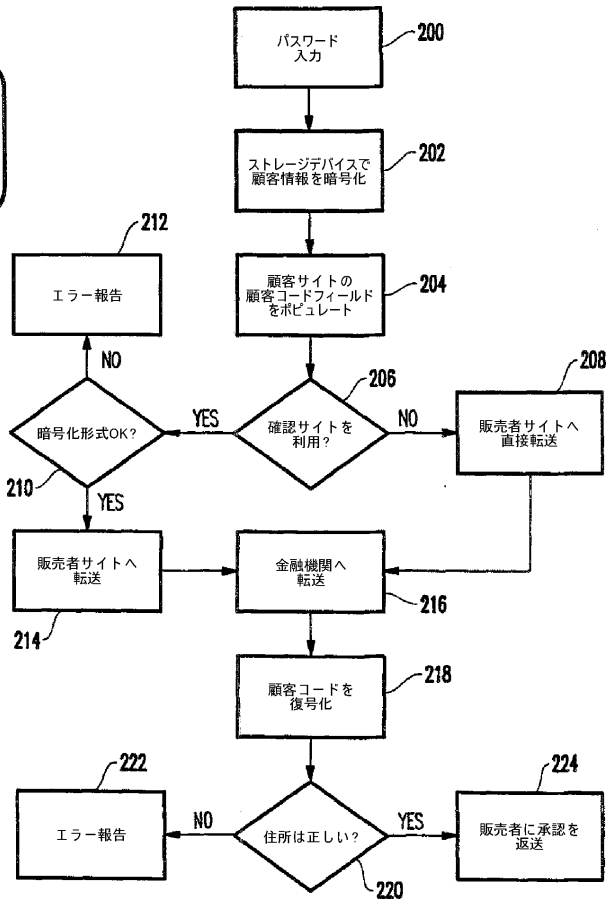
具体的な実施形態を上述したが、上記の説明によって本発明の一般的な内容が完全に明らかとなったと思われる。この一般的な内容に、現在の知識を応用することによって、さまざまな用途に応じて、本発明の包括的な概念から逸脱することなく、上述した具体的な実施形態を容易に変形および／または適合させることができる。このため、これらの変形例および適合例は、本明細書で開示される実施形態の均等物の定義および範囲に基づいて理解されるべきである。本明細書で使用した表現または用語は、本発明の説明を目的とす

るものであって、本発明を限定するものではないと理解されたい。このため、本発明の実施形態は好ましい実施形態に基づいて説明してきたが、当業者であれば、本願請求項の精神および範囲を超えない程度に好ましい実施形態を変形して、本発明の実施形態を実施し得ることに想到するであろう。

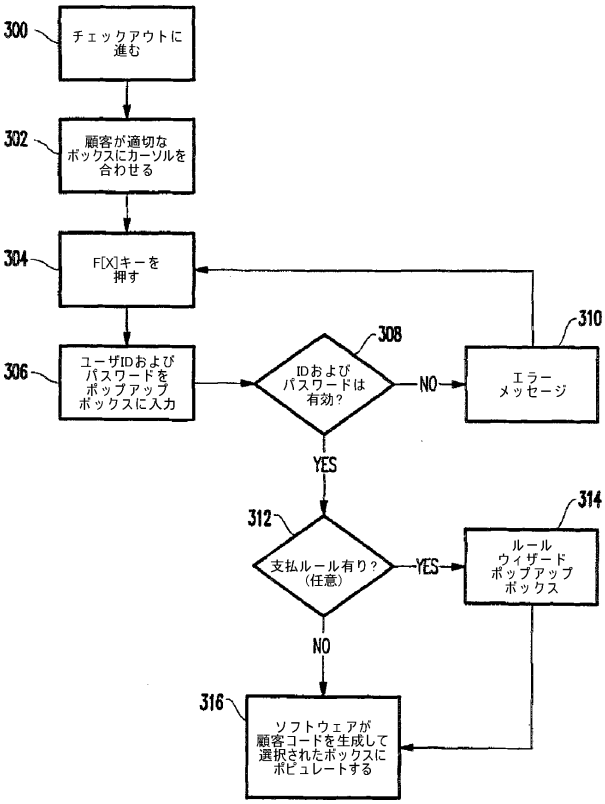
【図１】



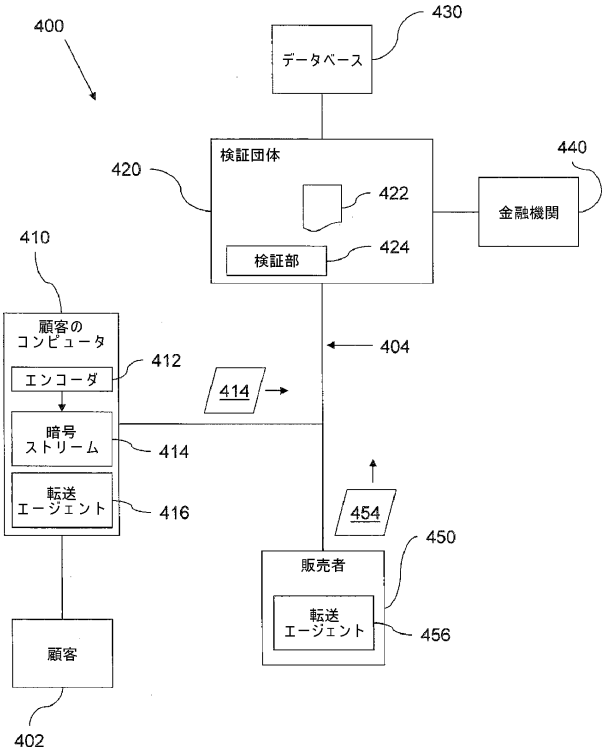
【図２】



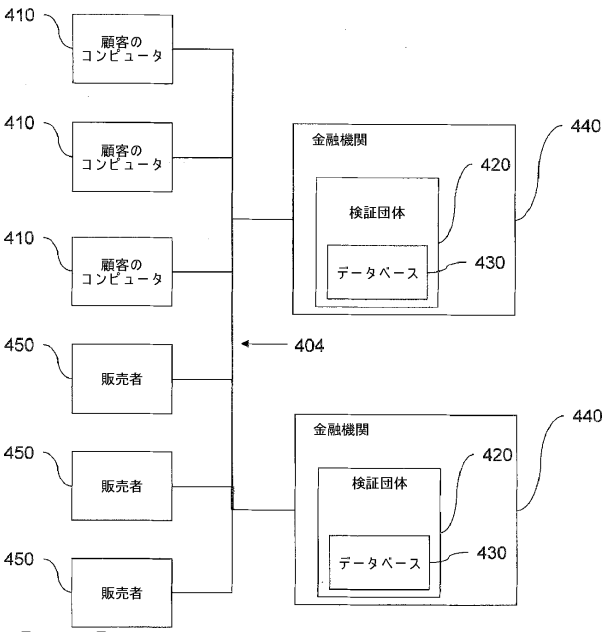
【図３】


300
チェックアウトに進む
302
顧客が適切なボックスにカーソルを合わせる
304
F[X]キーを押す
306
ユーザIDおよびパスワードをポップアップボックスに入力
308
IDおよびパスワードは有効?
NO
310
エラーメッセージ
YES
312
支払ルール有り?(任意)
YES
314
ルールウィザードポップアップボックス
NO
316
ソフトウェアが顧客コードを生成して選択されたボックスにポピュレートする

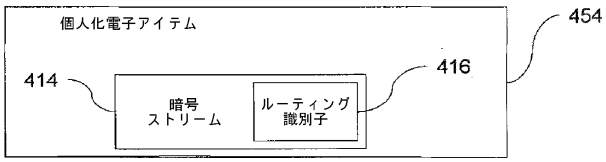
【図４】


400
データベース
430
検証団体
420
422
検証部
424
金融機関
440
410
顧客のコンピュータ
412
エンコーダ
414
暗号ストリーム
414
転送エージェント
416
404
414
454
販売者
450
転送エージェント
456
顧客
402

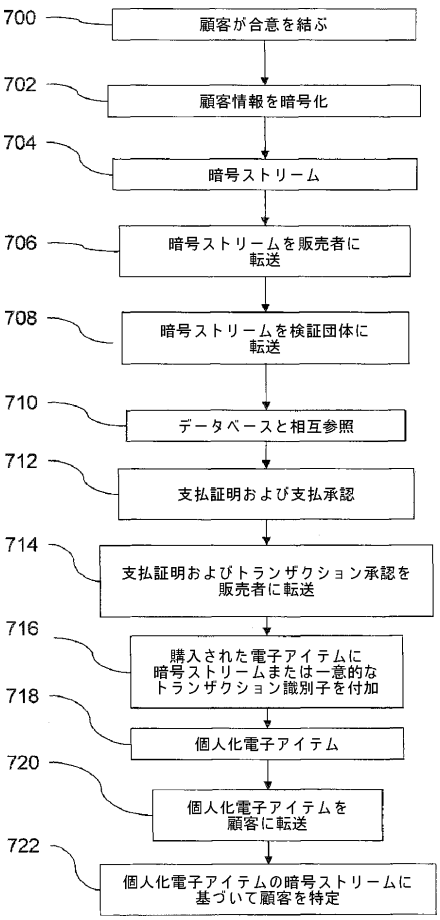
【図５】


410
顧客のコンピュータ
410
顧客のコンピュータ
410
顧客のコンピュータ
450
販売者
450
販売者
450
販売者
金融機関
検証団体
データベース
420
430
440
404
金融機関
検証団体
データベース
420
430
440

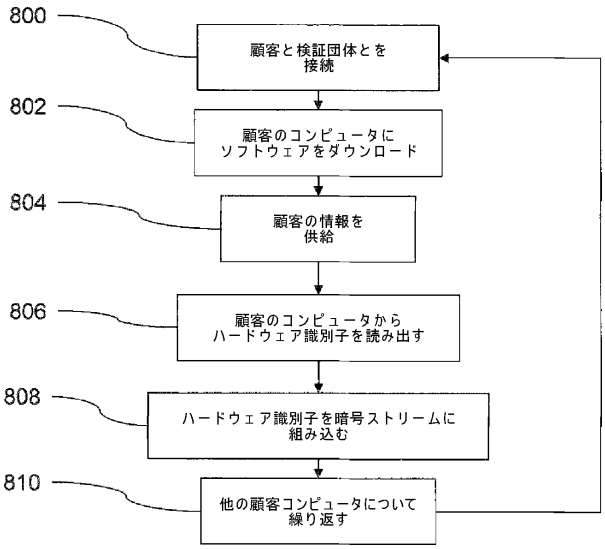
【図６】


個人化電子アイテム
414
暗号ストリーム
ルーティング識別子
416
454

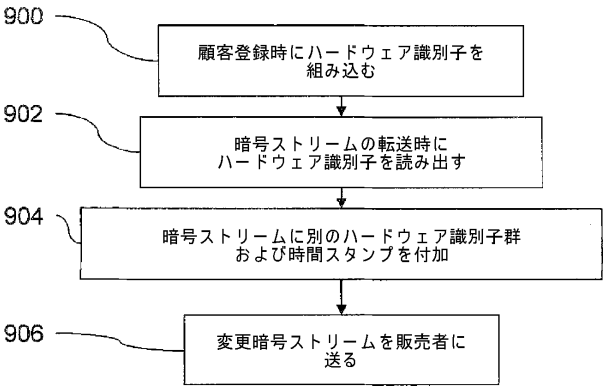
【図７】


700
顧客が合意を結ぶ
702
顧客情報を暗号化
704
暗号ストリーム
706
暗号ストリームを販売者に転送
708
暗号ストリームを検証団体に転送
710
データベースと相互参照
712
支払証明および支払承認
714
支払証明およびトランザクション承認を販売者に転送
716
購入された電子アイテムに暗号ストリームまたは一意的なトランザクション識別子を付加
718
個人化電子アイテム
720
個人化電子アイテムを顧客に転送
722
個人化電子アイテムの暗号ストリームに基づいて顧客を特定

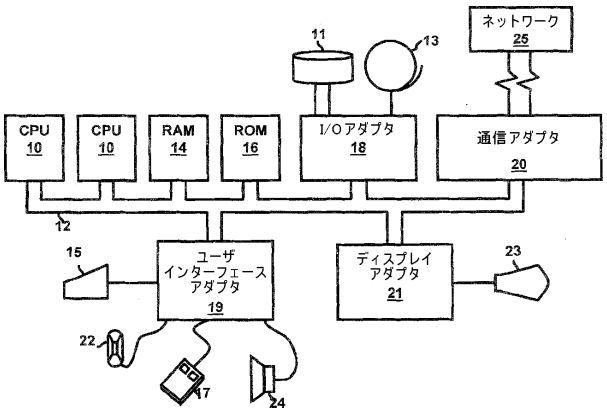
【図８】


800
顧客と検証団体とを接続
802
顧客のコンピュータにソフトウェアをダウンロード
804
顧客の情報を供給
806
顧客のコンピュータからハードウェア識別子を読み出す
808
ハードウェア識別子を暗号ストリームに組み込む
810
他の顧客コンピュータについて繰り返す

【図９】


900
顧客登録時にハードウェア識別子を組み込む
902
暗号ストリームの転送時にハードウェア識別子を読み出す
904
暗号ストリームに別のハードウェア識別子群および時間スタンプを付加
906
変更暗号ストリームを販売者に送る

【図１０】


11
13
ネットワーク
25
CPU
10
CPU
10
RAM
14
ROM
16
I/Oアダプタ
18
通信アダプタ
20
12
15
ユーザインターフェースアダプタ
19
ディスプレイアダプタ
21
23
22
17
24

フロントページの続き

(56)参考文献 米国特許出願公開第２００５／００５５３１７（ＵＳ，Ａ１）
林 良一（外４名），個人情報を保護しつつ活用する方法に関する一方式，情報処理学会研究報告，日本，社団法人情報処理学会，２００４年 1月１６日，Ｖｏｌ．２００４，Ｎｏ．２，ｐ．９－ｐ．１６

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20-21/24
G06Q 30/06
H04L 9/32