

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-123633

(P2002-123633A)

(43)公開日 平成14年4月26日 (2002.4.26)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 17/60	1 4 0	G 0 6 F 17/60	1 4 0 5 B 0 1 7
	Z E C		Z E C 5 B 0 4 9
	2 1 0		2 1 0 5 B 0 5 5
	3 1 0		3 1 0 E
	4 0 2		4 0 2

審査請求 未請求 請求項の数27 O L (全 37 頁) 最終頁に続く

(21)出願番号 特願2000-316358(P2000-316358)

(22)出願日 平成12年10月17日(2000.10.17)

(71)出願人 591234204

株式会社ローレルインテリジェントシステムズ
神奈川県横浜市青葉区美しが丘5丁目35番地の2

(72)発明者 鳥飼 将迪

神奈川県横浜市青葉区美しが丘5丁目35番地の2 株式会社ローレルインテリジェントシステムズ内

(74)代理人 100064746

弁理士 深見 久郎 (外2名)

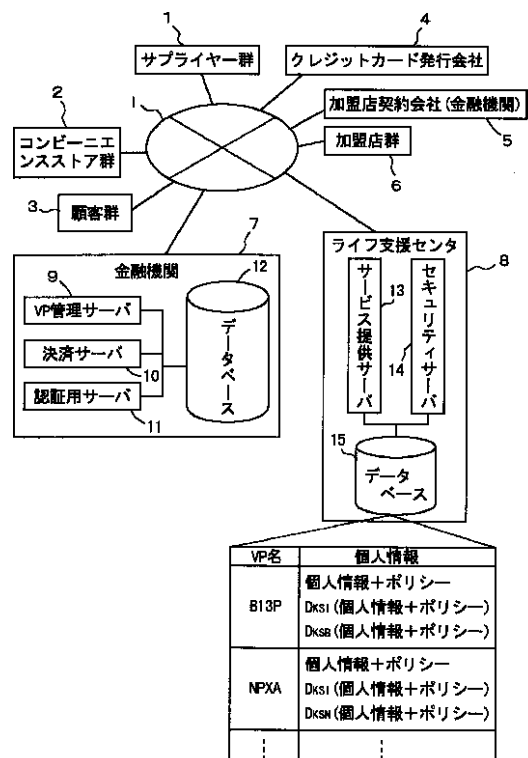
最終頁に続く

(54)【発明の名称】 個人情報保護方法、個人情報保護システム、処理装置および記録媒体

(57)【要約】

【課題】 ネットワーク上で行動するユーザの個人情報を保護しながらも業者側での十分な個人情報の収集に伴うサービスの提供が行ないやすく、しかもネットワーク上で自由に行動できるようにする。

【解決手段】 現実世界での実在人物(ユーザ)がネットワーク上で行動する際に、仮想人物(バーチャルパーソン)になりすまして該バーチャルパーソンとして行動できるようにするための所定のバーチャルパーソンを誕生させて金融機関7のデータベース12に登録させておき、そのバーチャルパーソンになりすましてユーザ(リアルパーソン)がネットワーク上で行動できるようにした。



【特許請求の範囲】

【請求項1】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、

前記実在人物と前記仮想人物との対応関係を特定可能な情報を守秘義務のある所定機関に登録する登録ステップ

とを含むことを特徴とする、個人情報保護方法。

【請求項2】 前記所定機関は、金融機関であることを特徴とする、請求項1に記載の個人情報保護方法。

【請求項3】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、

前記仮想人物用の電子証明書を発行する電子証明書発行ステップとを含むことを特徴とする、個人情報保護方法。

【請求項4】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、

前記仮想人物の住所を、前記実在人物とは異なった住所に設定するための住所設定ステップとを含むことを特徴とする、個人情報保護方法。

【請求項5】 前記仮想人物の住所は、所定のコンビニエンスストアの住所であることを特徴とする、請求項4に記載の個人情報保護方法。

【請求項6】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、

前記仮想人物用のクレジット番号を発行するクレジット番号発行ステップとを含み、

前記クレジット番号発行ステップにより発行されたクレジット番号を利用して前記仮想人物としてクレジットによる支払を可能にしたことを特徴とする、個人情報保護方法。

【請求項7】 コンピュータシステムを利用して、ネッ

トワーク上での個人情報を保護する個人情報保護方法であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、

前記仮想人物用の銀行口座を開設するための処理を行なう口座開設処理ステップとを含み、

前記口座開設処理ステップによって開設された銀行口座内の資金を利用して前記仮想人物として決済ができるようにしたことを特徴とする、個人情報保護方法。

【請求項8】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップを含み、

前記実在人物としてネットワーク上で行動する場合と前記仮想人物としてネットワーク上で行動する場合とで、サイト側がユーザを識別するために送信してくる識別データの受付制限を異ならせることができるようにしたことを特徴とする、個人情報保護方法。

【請求項9】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる処理を行なう仮想人物誕生処理手段と、

前記実在人物と前記仮想人物との対応関係を特定可能な情報を守秘義務のある所定機関において登録する処理を行なうための登録処理手段とを含むことを特徴とする、個人情報保護システム。

【請求項10】 前記所定機関は、金融機関であることを特徴とする、請求項9に記載の個人情報保護システム。

【請求項11】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる処理を行なう仮想人物誕生処理手段と、

前記仮想人物用の電子証明書を発行するための処理を行なう電子証明書発行処理手段とを含むことを特徴とする、個人情報保護システム。

【請求項12】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる処理を行なう仮想人物誕生処理手段と、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段と、前記仮想人物の住所を、前記実在人物とは異なる住所に設定するための処理を行なう住所設定手段とを含むことを特徴とする、個人情報保護システム。

【請求項13】 前記仮想人物の住所は、所定のコンビニエンスストアの住所であることを特徴とする、請求項12に記載の個人情報保護システム。

【請求項14】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段と、前記仮想人物用のクレジット番号を発行するための処理を行なうクレジット番号発行処理手段とを含み、該クレジット番号発行処理手段により発行されたクレジット番号を利用して前記仮想人物としてクレジットによる支払ができるようにしたことを特徴とする、個人情報保護システム。

【請求項15】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段と、前記仮想人物用の銀行口座を開設するための処理を行なう口座開設処理手段とを含み、該口座開設処理手段によって開設された口座内の資金を利用して前記仮想人物として決済ができるようにしたことを特徴とする、個人情報保護システム。

【請求項16】 コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段を含み、前記実在人物としてネットワーク上で行動する場合と前記仮想人物としてネットワーク上で行動する場合とで、サイト側がユーザを識別するために送信してくる識別データの受付制限を異ならせることができるようにしたことを特徴とする、個人情報保護システム。

【請求項17】 ネットワーク上での個人情報の保護に用いられる処理装置であって、

現実世界での実在人物がネットワーク上で行動する際

に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる要求を受付ける要求受付手段と、該要求受付手段により要求が受け付けられたことを条件として、所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段と、該仮想人物誕生処理手段より誕生した仮想人物と該仮想人物に対応する前記実在人物との対応関係を特定可能な情報をデータベースとして記憶させるための処理を行なう対応関係記憶処理手段とを含むことを特徴とする、処理装置。

【請求項18】 ネットワーク上での個人情報を保護するための処理装置であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物の公開鍵の入力を受付けて、該入力された公開鍵をデータベースに記憶させるための処理を行なう公開鍵記憶処理手段と、前記記憶された公開鍵に対応する前記仮想人物用の電子証明書を作成して発行する処理を行なうための電子証明書作成発行処理手段とを含み、

該電子証明書作成発行処理手段は、前記実在人物と前記仮想人物との対応関係を特定可能な情報が守秘義務のある所定機関に登録されている登録済の前記仮想人物であることを条件として、電子証明書の作成発行所処理を行なうことを特徴とする、処理装置。

【請求項19】 ネットワーク上での個人情報を保護するための処理装置であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物に発行されたクレジット番号を利用してクレジット支払による購入要求があった場合に、支払の承認処理を行なうための支払承認処理手段と、

該支払承認処理手段により承認されたクレジットによる支払の要求をクレジットカード発行会社に出すための処理を行なう支払要求処理手段とを含み、前記支払承認処理手段は、前記仮想人物用に発行された電子証明書を確認した上で、支払の承認を行なうことを特徴とする、処理装置。

【請求項20】 ネットワーク上での個人情報を保護するための処理装置であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物用に開設された銀行口座内の資金を決済に用いるために引落し引落し要求を受付けるための処理を行なう引落し要求受付処理手段と、

該引落し要求受付処理手段により引落し要求が受け付けられた場合に、該当する前記仮想人物に相当する銀行口座

を割出して該銀行口座内の資金から引落し要求金額に相当する資金を引落すための処理を行なう引落し処理手段とを含んでいることを特徴とする、処理装置。

【請求項 2 1】 ネットワーク上での個人情報保護するための処理装置であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物の住所であって、前記実在人物とは異なる住所に前記処理装置が設置されており、

該処理装置が設置されている住所を自己の住所としている前記仮想人物を特定可能な情報をデータベースに記憶させるための処理を行なう記憶処理手段と、

該記憶処理手段に記憶されている仮想人物が購入した商品であって前記処理装置が設置されている住所に配達されてきた商品を預かったことを特定可能な情報をデータベースに記憶させるための処理を行なう預かり情報記憶処理手段と、

前記預かった商品の引渡し要求があった場合に、当該引渡し要求を出した仮想人物が前記データベースに記憶されている仮想人物であることを確認し、かつ、商品を預かっている仮想人物であることを確認したことを条件として、該当する商品の引渡しの許可を出すための処理を行なう引渡し許可処理手段とを含むことを特徴とする、処理装置。

【請求項 2 2】 ネットワーク上での個人情報保護するためのプログラムを記録している記録媒体であって、コンピュータに、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための要求操作があったか否かを判定する誕生要求判定手段と、

該誕生要求判定手段により誕生要求があった旨の判定がなされた場合に、前記仮想人物の出生依頼要求を所定機関に送信するための処理を行なう出生要求送信手段と、前記仮想人物の出生要求を行なった前記実在人物を特定可能な情報であって前記仮想人物の出生に必要な情報を前記所定機関へ送信するための処理を行なう所定情報送信手段と、

して機能させるためのプログラムが記憶されていることを特徴とする、コンピュータ読取可能な記録媒体。

【請求項 2 3】 ネットワーク上での個人情報保護するための処理装置であって、

該処理装置は、ユーザの端末に対して情報のやり取りが可能に構成されるとともに、ユーザに携帯される携帯型の処理装置であり、前記ユーザとしての実在人物がネットワーク上で所定の仮想人物になりすまして該仮想人物として行動する際に使用され、

サイト側がユーザを識別するために送信してくる識別デ

ータが前記端末に対し送信されてきた場合に該識別データを当該端末の代わりに記憶可能に構成されていることを特徴とする、処理装置。

【請求項 2 4】 ユーザが前記端末を通してサイトにアクセスした際に、必要に応じて前記記憶している識別データを前記サイトに送信できるように前記記憶している識別データを出力することを特徴とする、請求項 2 3 に記載の処理装置。

10 【請求項 2 5】 前記ユーザの端末に対し情報の入出力を可能にするための入出力部と、該入出力部から前記識別データが入力されてきた場合に該識別データを記憶する識別データ記憶手段とをさらに含むことを特徴とする、請求項 2 3 または請求項 2 4 に記載の処理装置。

【請求項 2 6】 記憶している識別データの出力指令が入力されてきた場合に、記憶している識別データを外部出力することを特徴とする、請求項 2 3 ~ 請求項 2 5 のいずれかに記載の処理装置。

20 【請求項 2 7】 前記仮想人物に関する情報を記憶しており、

前記仮想人物に関する情報の出力指令が入力されてきた場合に、記憶している前記仮想人物に関する情報を外部出力することを特徴とする、請求項 2 3 ~ 請求項 2 6 のいずれかに記載の処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報保護する個人情報保護方法、個人情報保護システム、記録媒体および処理装置に関する。

30 【0002】

【従来の技術】従来において、ユーザがたとえばインターネット等を通してサイトにアクセスして、たとえばショッピング等のネットワーク上での何らかの行動を起す際に、当該ユーザの住所氏名や年齢等の個人情報の送信をサイト側から要求される場合がある。

40 【0003】その際に、従来においては、サイト側がユーザに対しプライバシーポリシーを提示し、個人情報の収集目的、収集した個人情報の取扱い等を明示し、ユーザ側の許可を受けた上で個人情報の送信を行なってもらうように構成されたものがあった。

【0004】

【発明が解決しようとする課題】一方、この種の従来の個人情報保護方法においては、ネットワーク上で行動するユーザが本人自身の名前で行動しているために、個人情報の収集も本人の名前がわかる状態で収集されることとなるために、サイト側への個人情報の提供に関してはいきおい消極的となってしまう、サイト側にしてみれば、個人情報が集まりにくいという状況になる。その結果、顧客の個人情報を収集してその顧客にマッチする商品や情報を選択して顧客に情報提供を行なおうとして

も、十分な個人情報が集まらないために、十分なサービスができないという不都合が生ずる。

【0005】一方、サイトにアクセスしてきたユーザの個人情報を収集する方法として、従来、識別データの一例のクッキー(cookie)をサイト側が利用して、ユーザがどのような種類のサイトにアクセスしたかを追跡して情報収集する方法があった。これは、サイトにアクセスしてきたユーザの端末(パーソナルコンピュータ)に対しクッキーという識別データを送信して記憶させ、次のアクセス時にそのクッキーを手掛かりにユーザの端末(パーソナルコンピュータ)を特定してどのような種類のサイトにアクセスするかを追跡して情報収集するものである。

【0006】しかし、このようなたとえば追跡型のクッキーが記録された端末からユーザが自己の氏名や住所を送信した場合には、クッキーとユーザの氏名とが対応付けられて登録されるおそれがあり、以降クッキーを手掛かりにユーザの氏名や住所等まで特定されてしまい、プライバシー上問題が生ずるおそれがあるという欠点があった。

【0007】そこで、ユーザが端末を通してサイトにアクセスする場合に、個人的に作成した匿名を使って行動することが考えられる。しかし、匿名によりたとえばショッピング等の行動を起した場合には、購入した商品の配達先が特定できなくなるために購入した商品を入手することができないという新たな欠点が生ずる。しかも、匿名の場合には電子証明書が発行されないために、匿名としてネットワーク上で行動するには極めて大きな制限が課せられることとなり、自由に活動することができないという欠点が生ずる。

【0008】本発明は、係る実情に鑑み考え出されたものであり、その目的は、ネットワーク上で行動するユーザの個人情報を保護することができながらも業者側での十分な個人情報の収集に伴うサービスの提供が行ないやすく、しかもネットワーク上で自由に行動できるようにすることである。

【0009】

【課題を解決するための手段】請求項1に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、前記実在人物と前記仮想人物との対応関係を特定可能な情報を守秘義務のある所定機関に登録する登録ステップとを含むことを特徴とする。

【0010】請求項2に記載の本発明は、請求項1に記載の発明の構成に加えて、前記所定機関は、金融機関であることを特徴とする。

【0011】請求項3に記載の本発明は、コンピュータ

システムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、前記仮想人物用の電子証明書を発行する電子証明書発行ステップとを含むことを特徴とする。

【0012】請求項4に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、前記仮想人物の住所を、前記実在人物とは異なった住所に設定するための住所設定ステップとを含むことを特徴とする。

【0013】請求項5に記載の本発明は、請求項4に記載の発明の構成に加えて、前記仮想人物の住所は、所定のコンビニエンスストアの住所であることを特徴とする。

【0014】請求項6に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、前記仮想人物用のクレジット番号を発行するクレジット番号発行ステップとを含み、前記クレジット番号発行ステップにより発行されたクレジット番号を利用して前記仮想人物としてクレジットによる支払を可能にしたことを特徴とする。

【0015】請求項7に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップと、前記仮想人物用の銀行口座を開設するための処理を行なう口座開設処理ステップとを含み、前記口座開設処理ステップによって開設された銀行口座内の資金を利用して前記仮想人物として決済ができるようにしたことを特徴とする。

【0016】請求項8に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップを含み、前記実在人物としてネットワーク上で行動する場合と前記仮想人物としてネットワーク上で行動する場合と

で、サイト側がユーザを識別するために送信してくる識別データの受付制限を異ならせることができるようにしたことを特徴とする。

【0017】請求項9に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる処理を行なう仮想人物誕生処理手段と、前記実在人物と前記仮想人物との対応関係を特定可能な情報を守秘義務のある所定機関において登録する処理を行なうための登録処理手段とを含むことを特徴とする。

【0018】請求項10に記載の本発明は、請求項9に記載の発明の構成に加えて、前記所定機関は、金融機関であることを特徴とする。

【0019】請求項11に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる処理を行なう仮想人物誕生処理手段と、前記仮想人物用の電子証明書を発行するための処理を行なう電子証明書発行処理手段とを含むことを特徴とする。

【0020】請求項12に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段と、前記仮想人物の住所を、前記実在人物とは異なる住所に設定するための処理を行なう住所設定手段とを含むことを特徴とする。

【0021】請求項13に記載の本発明は、請求項12に記載の発明の構成に加えて、前記仮想人物の住所は、所定のコンビニエンスストアの住所であることを特徴とする。

【0022】請求項14に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段と、前記仮想人物用のクレジット番号を発行するための処理を行なうクレジット番号発行処理手段とを含み、該クレジット番号発行処理手段により発行されたクレジット番号を利用して前記仮想人物としてクレジットによる支払ができるようにしたことを特徴とする。

【0023】請求項15に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段と、前記仮想人物用の銀行口座を開設するための処理を行なう口座開設処理手段とを含み、該口座開設処理手段によって開設された口座内の資金を利用して前記仮想人物として決済ができるようにしたことを特徴とする。

【0024】請求項16に記載の本発明は、コンピュータシステムを利用して、ネットワーク上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段を含み、前記実在人物としてネットワーク上で行動する場合と前記仮想人物としてネットワーク上で行動する場合とで、サイト側がユーザを識別するために送信してくる識別データの受付制限を異ならせることができるようにしたことを特徴とする。

【0025】請求項17に記載の本発明は、ネットワーク上での個人情報の保護に用いられる処理装置であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる要求を受付ける要求受付手段と、該要求受付手段により要求が受け付けられたことを条件として、所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段と、該仮想人物誕生処理手段より誕生した仮想人物と該仮想人物に対応する前記実在人物との対応関係を特定可能な情報をデータベースとして記憶させるための処理を行なう対応関係記憶処理手段とを含むことを特徴とする。

【0026】請求項18に記載の本発明は、ネットワーク上での個人情報を保護するための処理装置であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物の公開鍵の入力を受付けて、該入力された公開鍵をデータベースに記憶させるための処理を行なう公開鍵記憶処理手段と、前記記憶された公開鍵に対応する前記仮想人物用の電子証明書を作成して発行する処理を行なうための電子証明書作成発行処理手段とを含み、該電子証明書作成発行処理手段は、前記実在人物と前記仮想人物との対応関係を特定可能な情報が守秘義務のある所定機関に登録されている登録済の前記仮想人物であることを条件として、電子証明書の作成発行所処理を行なうことを特徴とする。

【0027】請求項19に記載の本発明は、ネットワーク上での個人情報を保護するための処理装置であって、

現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物に発行されたクレジット番号を利用してクレジット支払による購入要求があった場合に、支払の承認処理を行なうための支払承認処理手段と、該支払承認処理手段により承認されたクレジットによる支払の要求をクレジットカード発行会社に出すための処理を行なう支払要求処理手段とを含み、前記支払承認処理手段は、前記仮想人物用に発行された電子証明書を確認した上で、支払の承認を行なうことを特徴とする。

【0028】請求項20に記載の本発明は、ネットワーク上での個人情報を保護するための処理装置であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物用に開設された銀行口座内の資金を決済に用いるために引落し引落し要求を受け付けるための処理を行なう引落し要求受付処理手段と、該引落し要求受付処理手段により引落し要求が受け付けられた場合に、該当する前記仮想人物に相当する銀行口座を割出して該銀行口座内の資金から引落し要求金額に相当する資金を引落すための処理を行なう引落し処理手段とを含んでいることを特徴とする。

【0029】請求項21に記載の本発明は、ネットワーク上での個人情報を保護するための処理装置であって、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物の住所であって、前記実在人物とは異なる住所に前記処理装置が設置されており、該処理装置が設置されている住所を自己の住所としている前記仮想人物を特定可能な情報をデータベースに記憶させるための処理を行なう記憶処理手段と、該記憶処理手段に記憶されている仮想人物が購入した商品であって前記処理装置が設置されている住所に配達されてきた商品を預かったことを特定可能な情報をデータベースに記憶させるための処理を行なう預かり情報記憶処理手段と、前記預かった商品の引渡し要求があった場合に、当該引渡し要求を出した仮想人物が前記データベースに記憶されている仮想人物であることを確認し、かつ、商品を預かっている仮想人物であることを確認したことを条件として、該当する商品の引渡しの許可を出すための処理を行なう引渡し許可処理手段とを含むことを特徴とする。

【0030】請求項22に記載の本発明は、ネットワーク上での個人情報を保護するためのプログラムを記録している記録媒体であって、コンピュータに、現実世界での実在人物がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための要求操作があったか否かを判定する誕生要求判定手段と、該誕生要求

判定手段により誕生要求があった旨の判定がなされた場合に、前記仮想人物の出生依頼要求を所定機関へ送信するための処理を行なう出生要求送信手段と、前記仮想人物の出生要求を行なった前記実在人物を特定可能な情報であって前記仮想人物の出生に必要な情報を前記所定機関へ送信するための処理を行なう所定情報送信手段と、して機能させるためのプログラムが記憶されていることを特徴とする。

【0031】請求項23に記載の本発明は、ネットワーク上での個人情報を保護するための処理装置であって、該処理装置は、ユーザの端末に対して情報のやり取りが可能に構成されているとともに、ユーザに携帯される携帯型の処理装置であり、前記ユーザとしての実在人物がネットワーク上で所定の仮想人物になりすまして該仮想人物として行動する際に使用され、サイト側がユーザを識別するために送信してくる識別データが前記端末に対し送信されてきた場合に該識別データを当該端末の代わりに記憶可能に構成されていることを特徴とする。

【0032】請求項24に記載の本発明は、請求項23に記載の発明の構成に加えて、ユーザが前記端末を通してサイトにアクセスした際に、必要に応じて前記記憶している識別データを前記サイトに送信できるように前記記憶している識別データを出力することを特徴とする。

【0033】請求項25に記載の本発明は、請求項23または請求項24に記載の発明の構成に加えて、前記ユーザの端末に対し情報の入出力を可能にするための入出力部と、該入出力部から前記識別データが入力されてきた場合に該識別データを記憶する識別データ記憶手段とをさらに含むことを特徴とする。

【0034】請求項26に記載の本発明は、請求項23～請求項25のいずれかに記載の発明の構成に加えて、記憶している識別データの出力指令が入力されてきた場合に、記憶している識別データを外部出力することを特徴とする。

【0035】請求項27に記載の本発明は、請求項23～請求項26のいずれかに記載の発明の構成に加えて、前記仮想人物に関する情報を記憶しており、前記仮想人物に関する情報の出力指令が入力されてきた場合に、記憶している前記仮想人物に関する情報を外部出力することを特徴とする。

【0036】

【発明の実施の形態】次に、本発明の実施の形態を図面に基づいて詳細に説明する。図1は、個人情報保護システムの全体の概略を示す構成図である。インターネットIを通じて、サプライヤ群1、コンビニエンスストア群2、顧客群3、クレジットカード発行会社4、加盟店契約会社(金融機関)5、加盟店群6、金融機関7、ライフ支援センター8等が接続されている。サプライヤ群1とは、商品メーカー等であり、商品や情報を提供する機関のことである。クレジットカード発行会社4とは、た

例えばSET (Secure Electronic Transaction) により決済を行なう場合のイシューとしての機能を発揮するカード発行会社である。加盟店契約会社5は、電子モール等を構成する加盟店群6が契約している金融機関等からなる会社であり、SETにおけるアクワイアラとして機能する機関である。

【0037】加盟店群6とは、電子モール等における商店ばかりでなく、ニュース情報の提供や各種コンテンツの販売、あるいはユーザ(消費者)の消費支援サービスを行なういわゆるニューミドルマン等も含まれる。この加盟店群6の一例がライフ支援センター8である。このライフ支援センター8は、後述するように、ユーザの個人情報収集し、その個人情報に基づきユーザにふさわしい夢、人生設計、職種、趣味等を推薦して、それらを実現するために必要となる各種商品や情報を提供してくれる加盟店(ニューミドルマンを含む)を推薦するサービスを行なう機関である。

【0038】このライフ支援センター8には、サービス提供サーバ13とセキュリティサーバ14とがデータベース15に接続されており、前述した夢、人生設計、職種等の推薦サービスをサービス提供サーバ13が行ない、そのサービス提供に必要な個人情報の収集の際のセキュリティ管理をセキュリティサーバ14が行なう。そして、収集された個人情報がデータベース15に記憶されている。

【0039】データベース15に記憶されている情報は、仮想人物としてのバーチャルパーソン(以下単に「VP」という)の氏名に対応付けて、そのVPの個人情報とプライバシーポリシーと、両情報をライフ支援センターの秘密鍵KS1で復号化したライフ支援センターの署名と、両情報をVPの秘密鍵KSで復号化したVPの署名とを有している。

【0040】ここに、VPとは、現実世界には実在しないネットワーク上で行動する仮想の人物のことであり、現実世界での実在人物であるリアルパーソン(以下単に「RP」という)がネットワーク上で行動する際に、VPになりすましてそのVPとして行動できるようにするために誕生させた仮想人物のことであり。

【0041】このVPを管理するためのVP管理サーバ9が金融機関7に設置されている。VP管理サーバ9は、後に詳しく説明するように、RPからVPの出生依頼があれば、VPの氏名や住所等の所定情報を決定してVPを誕生させ、そのVPのデータをデータベース12に記憶させておく機能を有している。また、このVP管理サーバ9は、VP用の電子証明書を作成して発行する機能も有している。

【0042】金融機関7に設置されている認証用サーバ11は、RP用の電子証明書を作成して発行する機能を有するものである。金融機関7に設置されている決済サーバ10は、RPによる電子マネーやデビットカードを

使用しての決済ばかりでなく、VPとして電子マネーやデビットカードを使用しての決済を行なうための処理を行なう機能も有している。

【0043】図2は、金融機関7に設置されているデータベース12に記憶されているデータを説明するための図である。データベース12には、RP用のデータとVP用のデータとが記憶されている。RP用のデータは、RPの氏名、住所、認証鍵KN、公開鍵KP、口座番号等から構成されている。このRPに対応させてVPの氏名、住所、公開鍵KP、口座番号、Eメールアドレス等のデータが記憶されている。

【0044】この図2の場合には、太郎という氏名のRPのVPは、B13Pという氏名である。したがって、RPとしての太郎がネットワーク上でVPになりすまして行動する場合には、B13Pという氏名のVPになりすますこととなる。また、VP用の公開鍵、銀行口座番号、Eメールアドレス(電子メールアドレス)が決定されてデータベース12に記憶される。よって、RPがVPとしてネットワーク上で行動する場合には、このVPの氏名、住所、公開鍵、口座番号、Eメールアドレスを利用して行動することとなる。

【0045】その結果、ネットワーク上でVPとして行動した場合には、VPに関する情報が収集されることはあっても、RPに関する情報が意に反して収集されてプライバシーが侵害されることが防止できながらも、VPとしての口座番号を利用してVPとして決済を行なうことができる。さらに、VPの住所は、後述するように、RPの希望するまたはRPの住所に近いコンビニエンスストアの住所であるために、VPとして電子ショッピングをした場合の商品の配達先も確定でき、配達された商品をRPがVPになりすましてコンビニエンスストアにまで出向いて商品を引取ることが可能となる。

【0046】図2に示すように、RP次郎の場合には、NPXAとPNYCとの2人のVPを有している。次郎は、ネットワーク上で行動する場合に、この2人のVPを使い分けて行動することができる。たとえば、仕事関係でネットワーク上で行動する場合には、NPXAを使用し、仕事以外の私的にネットワーク上で行動する場合には、PNYCのVPを使用する等の使い分けが可能となる。その結果、次郎は、後述するVP用IC端末19Vを2種類所有し、NPXA用のVP用IC端末とPNYC用のVP用IC端末とを所有することとなる。

【0047】なお図2に示された「認証鍵」とは、RPが所定のシステムにアクセスする際に本人認証用に用いる鍵であり、これについては後述する。

【0048】データベース12に記憶されているRPとVPとの各種データは、暗号化した状態でデータベース12に格納しておいてもよい。そうすれば、万一データが盗まれたとしても、解読できないために、セキュリティ上の信頼性が向上する。一方、たとえばVPがネット

10

20

30

40

50

ワーク上で目に余る不正行為（たとえば刑法に違反する行為）を行なった場合には、所定機関（たとえば警察等）からの要請等に応じて、そのVPをデータベース12から検索してそのVPに対応するRPを割出し、RPの住所氏名等を要請のあった所定機関（たとえば警察等）に提供するようにしてもよい。

【0049】図3(a)は、コンビニエンスストアの構成を示す図である。コンビニエンスストア2には、データベース17に接続されたサーバ16が設置されている。データベース17には、当該コンビニエンスストア2に住所を持つVPの氏名と、それら各氏名に対応して、商品預かり情報、Eメールアドレス、顧客管理情報等が記憶されている。

【0050】サーバ16は、後述するように、コンビニエンスストア2にVPとして商品を引取りにきた顧客が、当該コンビニエンスストア2に登録されているVPであるか否かを確認し、そのVPに対し商品を預かっている場合にはその商品をVPに引渡すための処理を行なう。

【0051】図3(b)は、顧客群3の顧客に用いられる端末の一例のパーソナルコンピュータ30を示す正面図である。このパーソナルコンピュータ30は、インターネットに接続可能に構成されている。図中19RはRP用IC端末であり、19VはVP用IC端末である。ユーザがRPとしてインターネットIに接続してネットワーク上で活動する場合にはRP用IC端末19Rをパーソナルコンピュータ30のUSB(Universal Serial Bus)ポートに差込む。一方、ユーザがVPとしてインターネットIに接続してネットワーク上で活動する場合には、VP用IC端末19Vをパーソナルコンピュータ30のUSBポート18に差込む。

【0052】一方、ユーザは、RP用IC端末19RやVP用IC端末19Vをパーソナルコンピュータ30に接続して動作させるためには、事前に専用のアプリケーションソフトをインストールしておく必要がある。そのアプリケーションソフトが記録された記録媒体の一例のCD-ROM31をパーソナルコンピュータ30に挿入して、アプリケーションソフトをインストールする。このCD-ROM31に記録されているプログラムのフローチャートは、後述する図10～図14、図16～図18に基づいて後述する。

【0053】図4は、VP用IC端末を説明するための説明図である。VP用IC端末19Vは、前述したように、パーソナルコンピュータ30のUSBポート18に對し着脱自在に構成されており、そのUSBポート18に差込むことにより、パーソナルコンピュータ30との情報がやり取りできるようになり、使用可能な状態となる。

【0054】VP用IC端末19V内には、LSIチップ20が組込まれている。このLSIチップ20には、

制御中枢としてのCPU24、CPU24の動作プログラムが記憶されているROM25、CPU24のワークエリアとしてのRAM22、電気的に記憶データを消去可能なEEPROM26、コプロセッサ23、外部とのデータの入出力を行なうためのI/Oポート21等が設けられており、それらがバスにより接続されている。

【0055】EEPROM26には、電子マネー用のプログラムであるモンデックス(リロード金額データを含む)、その他の各種アプリケーションソフト、VP用に発行された電子証明書、暗証番号、クッキーデータが記憶されている。

【0056】さらに、VP用IC端末19Vは、VPのユーザエージェントとしての機能を有しており、ユーザエージェント用知識データとして、デビットカード情報、クレジットカード情報、VPの氏名、住所、VPのEメールアドレス、VPの公開鍵KPと秘密鍵KS、RPの認証鍵KN、VPの年齢、職業等、VPの各種嗜好情報、VPの家族構成、...等の各種知識データが記憶されている。

【0057】RP用IC端末19Rの場合も、図4に示したVP用IC端末19Vとほぼ同様の構成を有している。相違点といえば、EEPROM26に記録されているユーザエージェント用知識データの内容が相違する。具体的には、VPの氏名、住所の代わりにRPの氏名、住所、VPのEメールアドレスの代わりにRPのEメールアドレス、VPの公開鍵や秘密鍵の代わりにRPの公開鍵、秘密鍵、VPの年齢や職業等の代わりにRPの年齢や職業等、VPの各種嗜好情報の代わりにRPの各種嗜好情報、VPの家族構成の代わりにRPの家族構成となる。

【0058】なお、VPの家族構成は、VPに対応するRPの家族がVPを誕生させている場合には、その誕生しているVPの名前や住所や年齢等のデータから構成されている。つまり、RPの家族に対応するVPの家族すなわちバーチャル家族のデータがこのVPの家族構成の記憶領域に記憶されることとなる。

【0059】図5は、図1に示したVP管理サーバ9の処理動作を示すフローチャートである。ステップS(以下単にSという)1により、VPの出生依頼があったか否かの判断がなされ、あるまで待機する。顧客(ユーザ)がパーソナルコンピュータ30を操作してVPの出生依頼を行なえば、S1aに進み、正当機関である旨の証明処理がなされる。この証明処理は、金融機関7がVPの管理をする正当な機関であることを証明するための処理であり、他人が金融機関7になりすます不正行為を防止するための処理である。この処理については、図9(b)に基づいて後述する。次にS2へ進み、RPの氏名、住所の入力要求をパーソナルコンピュータ30へ送信する。次にS3へ進み、RPの氏名、住所の返信がパーソナルコンピュータ30からあったか否かの判断がな

され、あるまで待機する。

【0060】ユーザであるRPがパーソナルコンピュータ30から自分の氏名、住所を入力して送信すれば、S3によりYESの判断がなされてS4へ進み、乱数Rを生成してチャレンジデータとしてパーソナルコンピュータ30へ送信する処理がなされる。ユーザがVPの出生依頼を行なう場合には、パーソナルコンピュータ30のUSBポート18にVP用IC端末19Vを差込んでおく。その状態で、VP管理サーバ9から乱数Rが送信されてくれば、その乱数をVP用IC端末19Vへ入力する。すると、後述するように、VP用IC端末19V内において入力された乱数RをRPの認証鍵KNを用いて暗号化する処理がなされ、その暗号結果がパーソナルコンピュータ30へ出力される。パーソナルコンピュータ30では、その出力されてきた暗号化データであるレスポンスデータIをVP管理サーバ9へ送信する。すると、S5によりYESの判断がなされてS6へ進み、RPの認証鍵KNを用いて、受信したレスポンスデータIを復号化する処理すなわち $D_{KN}(I)$ を算出する処理がなされる。次にS7へ進み、S4により生成した乱数 $R = D_{KN}(I)$ であるか否かの判断がなされる。

【0061】VPの出生依頼者が金融機関7のデータベース12に記憶されている正規のRPである場合には、 $R = D_{KN}(I)$ となるために、制御がS9へ進むが、データベース12に記憶されているRPに他人がなりすましてVPの出生依頼を行なった場合には、 $R = D_{KN}(I)$ とはならないために、制御がS8へ進み、アクセス拒絶の旨がパーソナルコンピュータ30へ送信されてS1へ戻る。

【0062】一方、S7によりYESの判断がなされた場合には、S9へ進み、希望のコンビニエンスストアの入力があつたか否かの判断がなされる。VPの出生依頼を行なったRPは、誕生してくるVPの住所となるコンビニエンスストアについて特に希望するコンビニエンスストアがあれば、パーソナルコンピュータ30に入力してVP管理サーバ9へ送信する。その場合には、S9によりYESの判断がなされてS10へ進み、その入力されてきたコンビニエンスストアの情報を記憶した後S12へ進む。一方、希望するコンビニエンスストアの入力がなかった場合にはS11へ進み、RPの住所に近いコンビニエンスストアを検索してそのコンビニエンスストアを記憶した後S12へ進む。

【0063】S12では、VPの氏名、VPの住所であるコンビニエンスストアの住所、VPのEメールアドレス等を決定する。次にS13へ進み、VPの公開鍵の送信要求をパーソナルコンピュータ30へ送信する。そして、S14へ進み、公開鍵KPの返信があつたか否かの判断がなされ、あるまで待機する。VPの公開鍵の送信要求を受けたパーソナルコンピュータ30は、接続されているVP用IC端末19Vへ公開鍵出力要求を出力す

る。すると、後述するように、VP用IC端末19Vは、記憶しているVP用の公開鍵KPをパーソナルコンピュータ30へ出力する。パーソナルコンピュータ30では、その出力されてきたVP用の公開鍵KPをVP管理サーバ9へ返信する。すると、S14よりYESの判断がなされてS15へ進み、RPに対応付けて、VPの氏名、住所、公開鍵KP、Eメールアドレスをデータベース12へ記憶させる処理がなされる。

【0064】次にS16へ進み、VPの電子証明書を作成して発行する処理がなされる。次にS17へ進み、RPに、VPの氏名、コンビニエンスストアの住所、コンビニエンスストアの名称、Eメールアドレス、電子証明書を記憶したCD-ROMを郵送するための処理がなされる。次にS18へ進み、S12で決定された住所のコンビニエンスストアにVPの氏名、Eメールアドレス、当該金融機関7の名称を送信する処理がなされる。次にS19へ進み、正当機関である旨の証明処理がなされる。この正当機関である旨の証明処理は、前述したS1aと同じ処理である。次にS1へ戻る。

【0065】図6は、図1に示した認証用サーバ11の処理動作を示すフローチャートである。まずS25により、RPから電子証明書の発行依頼があつたか否かの判断がなされ、あるまで待機する。ユーザであるRPがパーソナルコンピュータ30からRPの電子証明書の発行依頼要求を認証用サーバ11へ送信すれば、制御がS26へ進み、RPの住所、氏名、公開鍵の送信要求をパーソナルコンピュータ30へ送信する処理がなされる。次にS27へ進み、パーソナルコンピュータからRPの住所、氏名、公開鍵の返信があるか否かの判断がなされ、あるまで待機する。そして、返信があつた段階で制御がS28へ進み、RPの電子証明書を作成してパーソナルコンピュータ30へ送信する処理がなされる。次にS29へ進み、RPの住所、氏名、公開鍵KPをデータベースに記憶する処理がなされてS25へ戻る。

【0066】図7～図9は、図1の決済サーバ10の処理動作を示すフローチャートである。S35により、RPの銀行口座番号の作成依頼があつたか否かの判断がなされ、ない場合にはS39へ進み、VPの銀行口座番号の作成依頼があつたか否かの判断がなされ、ない場合にはS40へ進み、デビットカードの発行依頼があつたか否かの判断がなされ、ない場合にはS41へ進み、決済要求があつたか否かの判断がなされ、ない場合にはS35へ戻る。

【0067】このS35～S41のループの巡回途中で、ユーザが金融機関7へ出向き、RPの銀行口座の開設依頼を行なってRPの銀行口座番号の作成依頼が入力されれば、制御がS36へ進み、RPの住所、氏名等の入力要求がなされ、入力があれば制御がS38へ進み、RPの銀行口座を作成して、データベース12に記憶するとともにRPに通知する処理がなされてS35へ戻

る。

【0068】ユーザが金融機関7へ出向き、VPの銀行口座の開設依頼を行なってVPの銀行口座番号の作成依頼要求が入力されれば、S42へ進み、VPの住所、氏名等、RPの住所、氏名等の入力要求がなされる。ユーザは、これら情報を手動でキーボードから入力するか、または、決済サーバ10にRP用IC端末19RやVP用IC端末19Vを接続してこれらデータを自動入力する。データが入力されれば、制御がS44へ進み、RPとVPの対応が適正であるか否かが、データベース12を10 検索することにより確認される。

【0069】RPとVPの対応が適正でない場合にはS51へ進み、対応が不適正である旨を報知してS35へ戻る。一方、RPとVPとの対応が適正な場合にはS45へ進み、VPの銀行口座を作成して、データベース12に記憶するとともに、VPに対応するRPにその銀行口座を郵送する処理がなされた後S35へ戻る。

【0070】ユーザが金融機関7へ出向き、デビットカードの発行要求の依頼を行なってデビットカードの発行要求の入力があれば、S40によりYESの判断がなされてS46へ進み、口座番号と氏名と暗証番号の入力要求がなされる。ユーザがRP用のデビットカードの発行を要求する場合には、RPの銀行口座番号と氏名と暗証番号を入力する。一方、ユーザがVP用のデビットカードの発行要求を希望する場合には、VPの銀行口座番号とVPの氏名とVPの暗証番号とを入力する。これらのデータの10 入力は、RP用IC端末19RまたはVP用IC端末19Vを決済サーバ10へ接続して自動的に入力する。

【0071】これらデータの10 入力が行なわれれば制御がS48へ進み、入力データをデータベース12へ記憶するとともに、デビットカードを発行する処理がなされる。次にS49へ進み、発行されたデビットカードの記憶データをRP用IC端末またはVP用IC端末へ伝送する処理がなされてS35へ戻る。

【0072】決済サーバ10に決済要求が送信されてくれば、S41によりYESの判断がなされてS50へ進み、決済処理がなされた後S35へ戻る。

【0073】図8は、図7に示したS50の決済処理のサブルーチンプログラムを示すフローチャートである。決済要求には、銀行口座内の資金を一部RP用IC端末19RまたはVP用IC端末19Vに引落す引落し要求と、デビットカードを使用しての決済要求と、クレジットカードを使用して決済を行なった場合のクレジットカード発行会社からのクレジット使用金額の引落し要求とがある。まずS55よりIC端末19Rまたは19Vへの引落し要求があったか否かの判断がなされ、ない場合にはS57へ進み、デビットカードを使用しての決済要求があったか否かの判断がなされ、ない場合にはS58へ進み、クレジットカード発行会社からの引落し要求が

あったか否かの判断がなされ、ない場合にはS59によりその他の処理がなされてこのサブルーチンプログラムが終了する。

【0074】ユーザがパーソナルコンピュータ30等からRP用IC端末19RまたはVP用IC端末19Vへ資金の一部引落し要求を決済サーバ10へ送信した場合には、S55によりYESの判断がなされてS56へ進み、正当機関証明処理がなされた後S60へ進む。S60では、氏名の入力要求をパーソナルコンピュータ30等へ送信する処理がなされる。その要求を受けたパーソナルコンピュータ30では、接続されているIC端末19Rまたは19Vに対し氏名の出力要求を伝送する。すると、接続されているIC端末19Rまたは19Vから氏名がパーソナルコンピュータ30へ伝送され、その伝送されてきた氏名をパーソナルコンピュータ30が決済サーバ10へ伝送する。すると、S61によりYESの判断がなされてS62へ進み、乱数Rを生成してチャレンジデータとしてパーソナルコンピュータ30へ送信する処理がなされる。

【0075】その乱数Rを受けたパーソナルコンピュータ30は、後述するように、接続されているIC端末19Rまたは19Vに対し乱数Rを伝送する。乱数Rを受取ったIC端末がRP用IC端末19Rの場合には、記憶している認証鍵KNを用いてRを暗号化してレスポンスデータIを生成し、それをパーソナルコンピュータ30へ出力する。パーソナルコンピュータ30では、その出力されてきたレスポンスデータIを決済サーバ10へ送信する。一方、乱数Rを受取ったIC端末がVP用IC端末19Vの場合には、受取った乱数Rを記憶している公開鍵KPを用いて暗号化してレスポンスデータIを生成し、パーソナルコンピュータ30へ出力する。パーソナルコンピュータ30では、その出力されてきたレスポンスデータIを決済サーバ10へ送信する。

【0076】レスポンスデータIが送信されてくれば、S63によりYESの判断がなされてS64に進み、S60に応じて入力された氏名がRPのものであるか否かが判別され、RPの場合にはS65へ進み、RPの認証鍵KNをデータベース12から検索してその認証鍵KNを用いて受信したレスポンスデータIを復号化する処理すなわち $D_{KN}(I)$ を生成する処理がなされる。次にS66へ進み、 $R = D_{KN}(I)$ であるか否かの判断がなされる。IC端末への引落し要求を行なったユーザがデータベース12に登録されている適正なユーザである場合には、 $R = D_{KN}(I)$ となるはずであるが、データベース12に登録されているユーザになりすまして銀行口座の資金の一部を引落しするという不正行為が行われた場合には、Rと $D_{KN}(I)$ とが一致しない状態となる。その場合には制御がS79へ進み、不適正である旨をパーソナルコンピュータ30へ返信する処理がなされてサブルーチンプログラムが終了する。

【0077】一方、 $R = D_{KN} (I)$ の場合には制御がS67へ進み、引落し額の入力要求をパーソナルコンピュータ30へ送信する処理がなされ、引落し額がパーソナルコンピュータ30から送信されてくれば、制御がS69へ進み、RPの口座から引落し額Gを減算してGをパーソナルコンピュータ30へ送信する処理がなされてサブルーチンプログラムが終了する。

【0078】一方、入力された氏名がVPのものであった場合にはS64によりNOの判断がなされて制御が図9のS85へ進む。S85では、VPの公開鍵KPをデータベース12から検索してその公開鍵KPを用いて受信したレスポンスデータIを復号化する処理すなわち $D_{KP} (I)$ を生成する処理がなされる。次にS86へ進み、 $R = D_{KP} (I)$ であるか否かの判断がなされる。引落し要求を行なっているものがデータベース12に登録されているVPになりすまして引落すという不正行為を行なっている場合には、S86によりNOの判断がなされてS79へ進み、不適正である旨がパーソナルコンピュータ30へ返信されることとなる。一方、S86によりYESの判断がなされた場合にはS87へ進み、引落し額Gの入力要求をパーソナルコンピュータ30へ送信する処理がなされ、パーソナルコンピュータ30から引落し額Gの送信があれば、S89へ進み、VPの銀行口座からGを減算してGをパーソナルコンピュータ30へ送信する処理がなされた後サブルーチンプログラムが終了する。

【0079】ユーザがデビットカードを使用しての決済を行なうべくデビットカード使用操作を行なった場合には、デビットカード使用要求が決済サーバ10へ送信され、S57によりYESの判断がなされてS56へ進み、正当機関証明処理がなされる。次にS70へ進み、暗証番号とカード情報入力要求がユーザのパーソナルコンピュータ30へ送信される。デビットカードの暗証番号とデビットカード情報とがパーソナルコンピュータ30から決済サーバ10へ送信されてくれば制御がS72へ進み、その送信されてきたデータが適正であるか否かの判断がなされ、不適正であればS79へ進む。

【0080】一方、適正である場合にはS73へ進み、使用額Gの入力を待つ。ユーザが使用額Gを入力してそれが決済サーバ10へ送信されてくれば制御がS74へ進み、該当する口座を検索してGを減算するとともにGをユーザのパーソナルコンピュータ30に送信する処理がなされる。

【0081】ユーザが後述するようにクレジットカードによるSETを用いた決済を行なった場合には、クレジットカード発行会社4(図1, 図15参照)からクレジット支払金額の引落し要求が決済サーバ10へ送信される。その引落し要求が送信されてくればS58によりYESの判断がなされてS56の正当機関証明処理がなされた後S75へ進み、ユーザの氏名、口座番号の入力を

待つ。クレジットカード発行会社4からユーザの氏名と口座番号とが送信されてくれば制御がS76へ進み、その入力されたデータが適正であるか否かをデータベース12を検索して判別する。不適正の場合にはS79へ進むが、適正な場合にはS77へ進み、引落し額Gの入力を待機する。クレジットカード発行会社4から引落し額Gすなわちクレジット支払額と手数料との合計金額が送信されてくれば制御がS78へ進み、口座からGを減算してクレジットカード発行会社の口座Gに加算する処理すなわち資金の移動処理がなされる。

【0082】S58によりNOの判断がなされた場合にはS59へ進み、その他の処理が行なわれる。

【0083】図9(b)は、前述したS1a, S19, S56に示された正当機関証明処理のサブルーチンプログラムを示すフローチャートである。まずS90により、当該機関の電子証明書を送信する処理がなされる。この電子証明書を受信した側においては、乱数Rを生成してその乱数Rを送信する。すると、S91によりYESの判断がなされてS92へ進み、その受信した乱数Rを当該機関の秘密鍵KSで暗号化する処理すなわち $L = E_{KS} (R)$ を算出する処理がなされ、その算出されたLを返信する処理がなされる。

【0084】このLを受信した受信側においては、既に受信している電子証明書内の当該機関の公開鍵KPを利用してLを復号化することによりRを得ることができる。そのRと送信したRとがイコールであるか否かをチェックすることにより、正当機関であるか否かをチェックすることが可能となる。これについては後述する。

【0085】図10~図14, 図16~図18は、パーソナルコンピュータ30の動作を説明するためのフローチャートである。S95により、IC端末使用モードであるか否かの判断がなされる。パーソナルコンピュータ30は、RP用IC端末19RまたはVP用IC端末19Vのうちのいずれか少なくとも一方をUSBポート18に接続していなければ動作しないIC端末使用モードと、IC端末を接続していなくても動作可能なIC端末未使用モードとに切り換えることが可能に構成されている。そして、IC端末使用モードでない場合にはS96へ進み、その他の処理がなされるが、IC端末使用モードになっている場合には、S97へ進み、VP用IC端末19Vが接続されているか否かの判断がなされ、接続されていない場合にS98へ進み、RP用IC端末19Rが接続されているか否かの判断がなされ、接続されていない場合すなわち両IC端末ともに接続されていない場合には、制御がS99へ進み、IC端末未接続の警告表示がなされた後S95へ戻る。

【0086】一方、VP用IC端末19Vが接続されている場合には、制御がS100へ進み、VP用のクッキー処理がなされる。この処理については、図11(a)に基づいて後述する。次に制御はS101へ進み、VP

出生依頼処理がなされる。この処理については図12に基づいて後述する。次にS102へ進み、VP用入力処理がなされる。この処理については図14(a)に基づいて後述する。次にS103へ進みVP用決済処理がなされる。この処理については図16に基づいて後述する。

【0087】一方、パーソナルコンピュータ30のUSBポート18にRP用IC端末19Rが接続されている場合には、S98によりYESの判断がなされてS104へ進み、RP用のクッキー処理がなされる。この処理については図11(b)に基づいて後述する。次にS105へ進み、電子証明書発行要求処理がなされる。この処理については図13(b)に基づいて後述する。次にS106へ進み、RP用入力処理がなされる。この処理については図14(b)に基づいて後述する。次にS107へ進み、RP用決済処理がなされる。この処理については、VP用決済処理と類似した制御処理であり、図示を省略する。

【0088】図11(a)は、S100に示されたVP用のクッキー処理のサブルーチンプログラムを示すフローチャートである。S110により、暗証番号が適正である旨のチェックが済んでいるか否かの判断がなされる。チェック済みである場合にはS117へ進むが、まだチェック済みでない場合にはS111へ進み、暗証番号の入力要求を表示する。ユーザがパーソナルコンピュータ30のキーボードからVP用IC端末19Vの暗証番号を入力すれば、制御がS113へ進み、入力された暗証番号をVP用IC端末19Vへ伝送する処理がなされ、VP用IC端末から適否の返信があるまで待機する(S114)。暗証番号が入力されたVP用IC端末19Vでは、後述するように、記憶している暗証番号と入力された暗証番号とを照合して一致するか否かの判断を行ない、一致する場合には適正である旨の返信を行ない、一致しない場合には不適正である旨の返信を行なう。適正である旨が返信されてきた場合には、S115によりYESの判断がなされるが、不適正である旨が返信されてきた場合には制御がS116へ進み、不適正である旨の報知(表示)がパーソナルコンピュータ30によりなされる。

【0089】適正である場合にのみ暗証番号チェック済み状態となり、制御がS117へ進み、パーソナルコンピュータ30にクッキーのデータが記録されているか否かの判断がなされる。記録されていない場合にはS119へ進むが、記録されている場合にはS118へ進み、その記録されているクッキーのデータをVP用IC端末19Vへ伝送した後そのクッキーの記録を消去する処理がなされる。VP用IC端末19Vは、伝送されてきたクッキーデータを記憶する処理を行なう。その結果、パーソナルコンピュータ30に記録されているクッキーデータがVP用IC端末19Vへ移し替えられることとな

る。

【0090】次にS119へ進み、サイトへのアクセス操作があったか否かの判断がなされ、ない場合にはS120に進み、その他の処理がなされてこのサブルーチンプログラムが終了する。一方、サイトへのアクセス操作があった場合にはS121へ進み、VP用IC端末19Vからクッキーデータを呼出し、クッキーとともにサイトへアクセスする処理がなされる。次にS122へ進み、サイトからクッキーデータが送信されてきたか否かの判断がなされ、送信されてきた場合にはS123へ進み、その送信されてきたクッキーデータをVP用IC端末19Vへ伝送して記憶させる処理がなされる。

【0091】このVP用のクッキー処理が行なわれた結果、パーソナルコンピュータ30にはクッキーデータが全く記録されず、既にパーソナルコンピュータ30に記憶されていたクッキーデータとサイトから送られてきたすべてのクッキーデータとがVP用IC端末19Vの方に記憶されることとなる。そしてサイトへアクセスする場合には、そのVP用IC端末19Vに記憶されているすべてのクッキーデータとともにサイトへアクセスすることとなる。その結果、サイト側においては、クッキーを思う存分活用してユーザ(顧客)のデータを収集することができる。しかも、そのクッキーデータは、パーソナルコンピュータ30を特定する識別情報ではなくVP用IC端末19Vを特定する識別情報となり、VP用IC端末19Vは一個人に所有されるものであるために、パーソナルコンピュータ30に比べてより一層個人を正確に特定し得るクッキーデータとなり、サイト側が正確な個人データを収集することができる。さらに、VP用IC端末19Vを使用している場合には、VPの氏名や住所等がサイト側に収集されることはあっても、RPの氏名や住所等がサイト側に収集されることがないために、ユーザ側においてもプライバシーを保護することが可能となる。

【0092】図11(b)は、S104に示されたRP用のクッキー処理のサブルーチンプログラムを示すフローチャートである。S125により、暗証番号のチェック済みであるか否かの判断がなされ、暗証番号が適正な旨のチェックが既に行なわれている場合にはS125によりYESの判断がなされてS132へ進む。一方、適正な暗証番号である旨のチェックが済んでいない場合にはS126へ進み、暗証番号の入力要求がなされ、RP用IC端末19Rの暗証番号をユーザがキーボードから入力すれば、S128へ進み、入力された暗証番号とRP用IC端末へ伝送する処理がなされる。そしてRP用IC端末19Rから暗証番号の適否の返信があるまで待機する(S129)。

【0093】RP用IC端末19Rから暗証番号の適否の判定結果が返信されてくれば、S130へ進み、適正である旨の返信結果であるか否かの判断がなされ、適正

でない場合にはS 1 3 1へ進み、不適正である旨の報知（表示）がなされる。一方、適正である旨の返信であった場合には、S 1 3 2へ進み、パーソナルコンピュータ30にクッキーの記録があるか否かが判断がなされ、ある場合にS 1 3 3へ進み、クッキーの記録がある旨を警告表示してこのサブルーチンプログラムが終了する。その結果、RP用IC端末19Rを接続して使用している場合には、パーソナルコンピュータ30にクッキーの記録があれば警告表示がなされてたとえばサイトへのアクセス等の動作が行なわれなくなる。ゆえに、RP用IC端末19Rを使用してユーザがRPとしてサイト等へアクセスする場合には、そのパーソナルコンピュータ30にクッキーの記録がないことが条件として可能となる。これにより、RPの氏名や住所等がクッキーを通してサイト側に収集されなくなり、ユーザのプライバシーが侵害されてしまうという不都合を防止することができる。

【0094】クッキーの記録がない場合にはS 1 3 2によりNOの判断がなされてS 1 3 4へ進み、サイトへのアクセス操作があったか否かの判断がなされ、ない場合にはS 1 3 7のその他の処理が行なわれる。一方、サイトへのアクセス操作があった場合にはS 1 3 5へ進み、サイトからクッキーが送信されてきたか否かの判断がなされる。サイトからクッキーが送信されてきた場合には、S 1 3 6へ進み、送信されてきたクッキーを拒絶する処理がなされる。その結果、RP用IC端末19Rをパソコン30のUSBポート18へ接続して使用している場合には、サイト側から送信されてきたクッキーをすべて拒絶し、そのクッキーがパソコン30に記録されてしまうことが防止できる。

【0095】その結果、RP用IC端末19Rを使用してユーザがRPとしてネットワーク上で行動する場合には、クッキーデータが全く記録されていないパーソナルコンピュータ30を使用して行動することとなり、クッキーを手掛かりのユーザの本名であるRPの氏名や住所等を収集されることがなく、ユーザのプライバシーが守られる。

【0096】図12はS 1 0 1に示されたVP出生依頼処理のサブルーチンプログラムを示すフローチャートである。このVP出生依頼は、PVを新たに誕生させるための依頼をVP管理サーバ9へ出すための処理である。S 1 4 0により、暗証番号のチェック済みであるか否かの判断がなされ、適正な暗証番号である旨のチェックが済んでいる場合にはS 1 4 1へ進むが、適正な暗証番号のチェックが未だ済んでいない場合にはこのサブルーチンプログラムが終了する。適正な暗証番号である旨のチェックが済んでいる場合にはS 1 4 1へ進みV出生要求の操作があったか否かの判断がなされる。ユーザがパーソナルコンピュータ30のキーボードを操作してVP出生要求の操作を行なえば、制御がS 1 4 2へ進み、VP

出生依頼要求を金融機関7のVP管理サーバ9へ送信する処理がなされる。次にS 1 4 3へ進み、正当機関チェック処理がなされる。この正当機関チェック処理は、相手側の機関（この場合には金融機関7）が正当な機関であるか否かをチェックするものであり、金融機関7になりすまして対応する不正行為を防止するためのものであり、図13(a)にそのサブルーチンプログラムが示されている。

【0097】先に、図13(a)に基づいて正当機関チェック処理のサブルーチンプログラムを説明する。この正当機関チェック処理は、図9(b)に示された正当機関証明処理に対応するチェック側のプログラムである。まずS 1 6 0により、電子証明書を受信したか否かの判断を行ない、受信するまで待機する。正当機関証明処理では、図9に示されているように、S 9 0により電子証明書が送信される。この電子証明書が送信されてくれば、制御がS 1 6 1へ進み、乱数Rを生成して送信する処理がなされる。すると、機関側では、図9に示すようにS 9 2により、当該機関の秘密鍵SKを用いて受信した乱数Rを暗号化してLを算出して送信する処理が行なわれる。このRの暗号化データLをパーソナルコンピュータ30が受信すれば、制御がS 1 6 3へ進み、受信した電子証明書内の公開鍵KPを用いてLを復号化する処理すなわち $D_{KP}(L)$ を算出する処理が行なわれる。

【0098】そして、図12のS 1 4 4へ進み、 $R = D_{KP}(L)$ であるか否かの判断がなされる。正当な機関である場合には、 $R = D_{KP}(L)$ となるはずであり、その場合にはS 1 4 6へ進むが、他人が金融機関7になりすましている場合には、S 1 4 4によりNOの判断がなされ、S 1 4 5へ進み、正当機関でない旨の警告表示がパーソナルコンピュータ30によりなされてこのサブルーチンプログラムが終了する。

【0099】正当機関であることが確認された場合には、S 1 4 6へ進み、RPの氏名、住所の入力要求を受信したか否かの判断がなされ、受信するまで待機する。VP管理サーバ9では、前述したように、VP出生依頼要求を受信すれば、RPの氏名、住所の入力要求を送信するのであり(S 2参照)、そのRPの氏名、住所の入力要求をパーソナルコンピュータ30が受信すれば、S 1 4 6によりYESの判断がなされて制御がS 1 4 7へ進む。

【0100】S 1 4 7では、RPの氏名、住所の入力指示をパーソナルコンピュータ30のディスプレイに表示する処理がなされ、入力があるまで待機する(S 1 4 8)。入力があった段階でS 1 4 9へ進み、その入力データを金融機関7のVP管理サーバ9へ送信する処理がなされる。

【0101】次にS 1 5 0へ進み、本人証明処理が行なわれる。この本人証明処理は、VP出生依頼を行なったユーザが本人自身であるか否かを証明するための処理で

あり、図17(a)にそのサブルーチンプログラムが示されている。ここで、図17(a)に基づいて、その本人証明書のサブルーチンプログラムを説明する。

【0102】この本人証明処理は、前述したS4、S62等に基づいて乱数Rが送信されてきた場合にその乱数に基づいて本人証明を行なうためのものである。まずS125により、乱数Rを受信したか否かの判断がなされ、受信するまで待機する。乱数Rを受信した場合にはS216へ進み、その受信した乱数RをIC端末19Rまたは19Vへ送信する処理がなされる。IC端末では、後述するように、記憶している認証鍵KNまたは公開鍵KPを用いて乱数Rを暗号化してレスポンスデータIを生成して出力する処理が行われる。そのレスポンスデータIが出力されてくれば、S217によりYESの判断がなされてS218へ進み、そのIをVP管理サーバ9へ送信する処理がなされる。

【0103】図12に示すVP出生依頼処理を行なう場合には、パーソナルコンピュータ30のUSBポート18にVP用IC端末19Vを接続している。そして、VP出生依頼処理の際の本人証明処理では、VP用IC端末19Vに記憶されているRPの認証鍵KNを用いて乱数Rを暗号化する処理がなされる。これについては、後述する。

【0104】その結果、図12のS150のVP出生依頼処理の際の本人証明では、RPであることの証明がなされる。

【0105】次にS151へ進み、アクセス拒絶を受信したか否かの判断がなされ、アクセス拒絶を受信した場合にS152へ進み、アクセス拒絶の表示が行なわれる。一方、アクセスが許容された場合にはS153へ進み、VP出生依頼を行なったユーザが希望するコンビニエンスストアの入力があるか否かの判断がなされる。出生したVPの住所が、コンビニエンスストアの住所となるために、ユーザは、自己の希望するコンビニエンスストアがある場合には、そのコンビニエンスストアを特定する情報をパーソナルコンピュータ30のキーボードから入力する。入力があれば、S154により、その希望のコンビニエンスストアのデータがVP管理サーバ9へ送信される。希望のコンビニエンスストアの入力がなかった場合には、前述したように、RPの住所に最も近いコンビニエンスストアの住所が出生したVPの住所となる。

【0106】次にS155へ進み、VPの公開鍵の送信要求があったか否かの判断がなされ、あるまで待機する。VP管理サーバ9では、前述したように、VPの出生依頼があった場合に、VPの公開鍵の送信要求を出す(S13参照)。その送信要求をパーソナルコンピュータ30が受ければ、制御がS156へ進み、VP用IC端末19Vへ公開鍵出力要求を出す。すると、VP用IC端末19Vが、記憶しているVPの公開鍵KPを出力

する。その出力があれば、制御がS158へ進み、その出力された公開鍵KPを金融機関7のVP管理サーバ9へ送信する。

【0107】図13(b)は、S105に示された電子証明書発行要求処理のサブルーチンプログラムを示すフローチャートである。S165により、適正な暗証番号である旨のチェックが済んでいるか否かの判断がなされ、未だに済んでいない場合にはこのサブルーチンプログラムが終了する。一方、適正な暗証番号である旨のチェックが済んでいる場合にはS166へ進み、RP用電子証明書の発行依頼操作があったか否かの判断がなされる。ユーザがパーソナルコンピュータ30のキーボードを操作して発行依頼を行なった場合には、制御がS167へ進み、RPの住所、氏名の入力指示が表示される。ユーザがキーボードより入力すれば、制御がS169へ進み、RP用IC端末19Rから公開鍵KPを呼出す処理がなされる。この電子証明書発行要求処理を行なう場合には、ユーザは、パーソナルコンピュータ30のUSBポート18に自己のRP用IC端末19Rを接続しておく必要がある。そして、S169の処理が行なわれた場合には、その接続されているRP用IC端末19Rが記憶しているRP用の公開鍵KPがパーソナルコンピュータ30に出力され、S170により、その出力されてきた公開鍵KPと入力されたRPの住所、氏名とが金融機関7の認証用サーバ11へ送信される。

【0108】図14(a)はS102に示されたVP用入力処理のサブルーチンプログラムを示し、図14(b)はS106に示されたRP用入力処理のサブルーチンプログラムを示すフローチャートである。

【0109】VP用入力処理が行なわれる場合には、パーソナルコンピュータ30のUSBポート18にVP用IC端末19Vを接続しておく必要がある。S175により、適正な暗証番号である旨のチェックが終了しているか否かの判断がなされ、適正な暗証番号のチェックが未だなされていない場合にはこのサブルーチンプログラムが終了する。適正な暗証番号のチェック済の場合には、S176へ進み、VP用入力操作があったか否かの判断がなされる。前述したように、金融機関7のVP管理サーバ9によりVPの出生処理が行なわれた場合には、誕生したVPの氏名、住所(コンビニエンスストアの住所)、コンビニエンスストアの名称、Eメールアドレス、電子証明書が記憶されたCD-ROMが郵送されてくるのであり、そのCD-ROMをユーザがパーソナルコンピュータ30に挿入すれば、S176によりYESの判断がなされてS178へ進み、そのCD-ROMの記録データが読み込まれて接続されているVP用IC端末19Vへ伝送される。

【0110】ユーザがパーソナルコンピュータ30のキーボードからVP用ユーザエージェントの知識データの

されてS179へ進み、入力された知識データをVP用IC端末19Vへ伝送する処理がなされる。

【0111】ユーザが金融機関7の自己の口座から資金を一部引落しすれば、その引落し額Gがパーソナルコンピュータ30へ送信されてくる(S69参照)。その引落し額Gがパーソナルコンピュータ30に入力されれば、S180によりYESの判断がなされてS181へ進み、引落し額GをVP用IC端末19Vへ転送してリロード金額として加算記憶させる処理がなされる。

【0112】RP用入力処理が行なわれる場合には、パーソナルコンピュータ30のUSBポート18にRP用IC端末19Rを接続しておく必要がある。まずS185により、適正な暗証番号のチェックが済んでいるか否かの判断がなされ、済んでいる場合にはS186へ進み、RPの電子証明書を受信したか否かの判断がなされる。ユーザがRPの電子証明書の発行依頼を認証用サーバに対し行なえば、前述したように、RPの電子証明書が作成されてパーソナルコンピュータ30に送信されてくる(S28参照)。その電子証明書が送信されてくれば、S186によりYESの判断がなされてS187へ進み、受信した電子証明書をRP用IC端末19Rへ伝送して、RP用IC端末へ記憶させる処理がなされる。

【0113】ユーザがパーソナルコンピュータ30のキーボードを操作して、RP用ユーザエージェントの知識データの入力操作を行なえば、S188によりYESの判断がなされてS189へ進み、その入力された知識データをRP用IC端末19Rへ伝送する処理がなされ、RP用IC端末19Rがその入力された知識データを記憶する。

【0114】ユーザが決済サーバ10に対し自己の口座内の資金の一部を引落す引落し要求を行なった場合には、前述したように、引落し金額であるGが決済サーバ10からユーザのパーソナルコンピュータ30へ送信される。すると、S190によりYESの判断がなされてS191へ進み、引落し額GをRP用IC端末19Rへ伝送し、リロード金額としてGを加算更新する処理が行なわれる。

【0115】図15は、ユーザ(RPとVPが存在する)がクレジットカードの支払を行なってSETに従った決済が行なわれる場合の全体概略システムを示す図である。まず、カード会員がクレジットカードの発行手続を行なえば、クレジットカード発行会社4に設置されているサーバが、クレジットカード発行の申込みがあったことを判別して、当該カード会員に対しクレジットカード番号を発行する。その際に、カード会員がVP用のクレジットカードの発行を要求した場合には、クレジットカード発行会社4のサーバは、そのVPの氏名や住所等のデータを入力してもらい、そのデータに基づいて金融機関などに登録されているVPか否かを金融機関7に問合せる。そして、金融機関7のデータベース12に記憶され

ている正規のVPであることが確認されたことを条件として、クレジットカード発行会社4のサーバは、そのVPに対しクレジット番号を発行する処理を行なう。

【0116】つまり、クレジットカード発行会社4のサーバは、仮想人物用のクレジット番号を発行するクレジット番号発行ステップを含んでいる。また、仮想人物用のクレジット番号を発行するクレジット番号発行手段を含んでいる。さらに、このクレジット番号発行ステップまたはクレジット番号発行手段は、前述したように、クレジット番号発行対象となる仮想人物が前記所定機関に登録されている正規の仮想人物であることが確認されたことを条件として、前記クレジット番号を発行する。クレジットカード発行会社4によって発行されたクレジットカード(RP用とVP用の2種類存在する)を所持するユーザは、SETによる取引をするための会員の登録要求を認証用サーバ11に出す。認証用サーバ11は、そのユーザがクレジットカード発行会社4のクレジット会員であるか否かの認証要求をクレジットカード発行会社4に出す。クレジットカード発行会社4からクレジット会員の認証の回答が認証用サーバ11に返信されてくれば、認証用サーバ11は、SET用の電子証明書を作成してカード会員に送る。

【0117】電子モール等の加盟店6がSETによる取引を可能にするためには、まず、SETによる取引のための会員登録要求を認証用サーバ11に出す。認証用サーバ11では、加盟店6が契約している加盟店契約会社(アクアイアラ)5に、当該加盟店6が正当な契約会社であるか否かの認証要求を送信する。加盟店契約会社5から正当な加盟店である旨の回答が返信されてくれば、認証用サーバ11は、その加盟店6のためのSET用の電子証明書を作成して加盟店6に発行する。

【0118】この状態で、カード会員が加盟店6により電子ショッピングを行なってSETにより取引を行なう場合には、まず商品やサービス等の購入要求をカード会員が加盟店6へ送信する。加盟店6では、その購入要求を承認してよいか否かの承認要求を支払承認部33からペイメントゲートウェイ27を介してクレジットカード発行会社4へ送信する。クレジットカード発行会社4から承認の回答がペイメントゲートウェイ27を介して加盟店6に返信されてくれば、加盟店6は、購入を受理した旨をカード会員に送信する。また加盟店6は、支払要求部34から支払要求をペイメントゲートウェイ27に送信する。ペイメントゲートウェイ27は、その支払要求に応じた決済要求をクレジットカード発行会社4へ送信するとともに、支払回答を加盟店6へ返信する。

【0119】カード会員と加盟店6との間では、商品やサービスの購入取引を行なう際に、互いの電子証明書を送信して、正当な本人である旨の確認が行なわれる。

【0120】クレジットカード発行会社4が、ユーザとしてのRPにクレジットカードを発行した場合には、そ

のクレジットカード番号等のカード情報が当該ユーザのRP用IC端末19Rに入力されて記憶される。一方、ユーザがVPとしてクレジットカード発行会社4からクレジットカードの発行を受ける際には、VP用に発行された電子証明書をクレジットカード発行会社4に送信し、金融機関7による身分の証明を行なってもらう必要がある。その上で、クレジットカード発行会社4がクレジットカードを発行した場合には、そのクレジットカードのカード番号等のカード情報が当該ユーザのVP用IC端末19Vに入力されて記憶される。

【0121】前述したSET用の電子証明書の発行も、RP用とVP用との2種類のケースに分けて発行される。そしてそれぞれ発行されたSET用の電子証明書が、それぞれのIC端末19Rまたは19Vに入力されて記憶される。

【0122】図16は、S103に示したVP用決済処理のサブルーチンプログラムを示すフローチャートである。まずS195により、適正な暗証番号である旨のチェックが終了しているか否かの判断がなされ、終了していなければこのサブルーチンプログラムが終了し、適正な暗証番号のチェック済の場合にはS196へ進む。

【0123】このVP用決済処理は、金融機関7のユーザの銀行口座内の資金の一部を引落してVP用IC端末19Vへリロードする処理と、デビットカードを使用して決済を行なう処理と、クレジットカードを使用して決済を行なう処理と、VP用IC端末19Vへリロードされているリロード金額を使用して決済を行なう場合とを有している。

【0124】ユーザが自己の銀行口座内の資金の一部引落してVP用IC端末へリロードする操作を行えば、S197により、その引落し要求が金融機関7の決済サーバ10へ送信される。次にS198へ進み、正当機関チェック処理(図13(a)参照)が行なわれる。

【0125】次にS199へ進み、 $R = D_{KP}(L)$ である否かの判断がなされ、正当機関でない場合にはS119によりNOの判断がなされてS200へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合には、 $R = D_{KP}(L)$ となるために、制御がS201へ進み、氏名の入力要求があったか否かの判断がなされ、あるまで待機する。前述したように、決済サーバ10は、IC端末への引落し要求があった場合には、氏名の入力要求を送信する(S60参照)。この氏名の入力要求が送信されてくれば、S201によりYESの判断がなされてS202へ進み、VP用IC端末19VからVPの氏名を呼出して決済サーバ10へ送信する処理がなされる。次にS203へ進み、本人証明処理(図17(a)参照)がなされる。

【0126】次にS204へ進み、引落し額の入力要求があったか否かの判断がなされ、なければS205へ進み、不適正な旨の返信があったか否かの判断がなされ、

なければS204へ戻る。この204, 205のループの巡回途中で、決済サーバ10がユーザの正当性が確認できないと判断した場合には不適正である旨の返信を行なう(S79参照)。その結果、S205によりYESの判断がなされてS207へ進み、不適正である旨がパーソナルコンピュータのディスプレイにより表示される。一方、決済サーバ10が本人認証の結果正当な本人であると判断した場合には引落し額の入力要求をパーソナルコンピュータ30へ送信する(S87参照)。すると、S204によりYESの判断がなされてS206へ進む。

【0127】S206では、引落し額の入力指示をパーソナルコンピュータ30のディスプレイに表示させる処理がなされる。ユーザがキーボードから引落し額を入力すれば、S208によりYESの判断がなされてS209へ進み、その入力された引落し額Gを決済サーバ10へ送信する処理がなされる。決済サーバ10では、引落し額Gを受信すれば、VPの口座からGを減算してGを送信する処理がなされる(S89参照)。その結果、S210によりYESの判断がなされてS211へ進み、引落し額GをVP用IC端末19Vへ送信してGをリロード金額に加算更新する処理がなされる。

【0128】S196により、NOの判断がなされた場合には、図17(b)のS220へ進み、デビットカードの使用操作があったか否かの判断がなされる。デビットカードの使用操作があった場合には、S235へ進み、デビットカード使用要求を決済サーバ10へ送信する処理がなされる。次にS221へ進み、正当機関チェック処理(図13(a)参照)がなされる。そしてS222へ進み、 $R = D_{KP}(L)$ であるか否かの判断がなされる。正当機関でない場合には、NOの判断がなされてS223へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合には制御がS224へ進み、デビットカードの暗証番号とカード情報の入力要求があったか否かの判断がなされ、あるまで待機する。決済サーバ10は、デビットカードの使用要求があった場合には、暗証番号とカード情報の入力要求をパーソナルコンピュータ30へ送信する(S70参照)。その送信を受信すれば、制御がS225へ進み、暗証番号の入力指示がパーソナルコンピュータ30のディスプレイに表示される。ユーザがデビットカードの暗証番号をキーボードから入力すれば、S226によりYESの判断がなされてS227へ進み、VP用ICカード19Vからカード情報を読み出し暗証番号とともに決済サーバ10へ送信する処理がなされる。

【0129】次にS228へ進み、不適正である旨の返信があったか否かの判断がなされる。暗証番号とカード情報とを受信した決済サーバ10は、適正か否かの判断を行ない(S72)、適正でない場合には不適正である旨の返信を行なう(S79参照)。不適正である旨が返

10

20

30

40

50

信されてくれば、S 2 2 8によりYESの判断がなされてS 2 2 9へ進み、不適正である旨の表示がなされる。一方、不適正である旨の返信が送られてこなければ、制御がS 2 3 0へ進み、使用金額の入力指示がパーソナルコンピュータのディスプレイに表示される。ユーザが使用金額をキーボードから入力すれば、S 2 3 1によりYESの判断がなされてS 2 3 2へ進み、入力された使用金額Gを決済サーバ10へ送信する処理がなされる。

【0130】使用金額Gを受信した決済サーバ10は、前述したように、ユーザに該当する銀行口座を検索して使用金額Gを減算するとともに、その使用金額Gをパーソナルコンピュータ30に返信する処理を行なう(S 7 4)。

【0131】その結果、S 2 3 3によりYESの判断がなされてS 2 3 4へ進み、決済が完了した旨の表示をパーソナルコンピュータ30のディスプレイに表示させる処理がなされる。

【0132】S 2 2 0によりNOの判断がなされた場合には、制御がS 2 3 8へ進む。S 2 3 8では、クレジットカードの使用操作があったか否かの判断がなされる。ユーザがパーソナルコンピュータ30のキーボードを操作してクレジットカードの使用を入力すれば、制御がS 2 3 7へ進み、クレジットカードによる決済要求を加盟店6へ送信する処理がなされる。この加盟店は、ユーザが商品やサービスを購入しようとしている商店である。次に制御がS 2 3 9へ進み、正当機関チェック処理がなされる。この正当機関チェック処理は、図13(a)に示したものである。この正当機関チェック処理に合せ、加盟店6は、当該加盟店の電子証明書を顧客のパーソナルコンピュータ30へ送信し、次に乱数Rを受信すれば、その乱数を自己の秘密鍵KSを用いて暗号化し、その暗号結果Lを顧客のパーソナルコンピュータ30へ送信する。

【0133】制御がS 2 4 0へ進み、 $R = D_{KS}(L)$ であるか否かの判断がなされる。正当な販売店(加盟店)でない場合には、S 2 4 0によりNOの判断がなされて、S 2 4 1へ進み、正当な販売店でない旨の警告表示がなされる。一方、正当な販売店(加盟店)である場合には、S 2 4 2へ進み、オーダ情報OIと支払指示PIとが作成される。オーダ情報OIとは、商品やサービス等の購入対象物や購入個数等を特定するための情報である。支払指示PIは、たとえばクレジットカード番号何々のクレジットカードを利用してクレジットの支払を行なう旨の指示等である。

【0134】次にS 2 4 3へ進み、オーダ情報OIと支払指示PIのメッセージダイジェストを連結した二重ダイジェストMDを算出する処理がなされる。次にS 2 4 4へ進み、二重ダイジェストMDをVP用IC端末19Vへ伝送して署名指示を出すとともに、VP用電子証明書の出力要求を行なう。すると、パーソナルコンピュー

タ30に接続されているVP用IC端末19Vが、後述するように、入力されたMDを秘密鍵KSを用いて復号化していわゆる二重署名を生成してパーソナルコンピュータ30に出力するとともに、記憶しているVP用の電子証明書をパーソナルコンピュータ30に出力する。それら出力があれば、S 2 4 5によりYESの判断がなされてS 2 4 6へ進み、オーダ情報OIと支払指示PIと出力されてきた署名としての $D_{KS}(MD)$ とVP用電子証明書とを加盟店6へ送信する処理がなされる。加盟店6では、それら情報を確認した上で、ユーザの購入要求を受理する購入受理の回答をユーザのパーソナルコンピュータ30へ送信する。すると、S 2 4 7によりYESの判断がなされてS 2 4 8へ進み、取引が完了した旨の表示が行なわれる。

【0135】S 2 3 8によりNOの判断がなされた場合にS 2 4 9へ進み、リロード金額の使用操作があったか否かの判断がなされる。ユーザが、VP用IC端末19Vに蓄えられているリロード金額を使用する旨のキーボード操作を行えば、制御がS 2 5 0へ進み、使用金額の入力指示がパーソナルコンピュータ30のディスプレイに表示される。ユーザが使用金額をキーボードから入力すれば、S 2 5 1によりYESの判断がなされてS 2 5 2へ進み、入力された使用金額Gの引落し要求をVP用IC端末19Vへ伝送する処理がなされる。

【0136】VP用IC端末19Vでは、後述するように、引落し要求を受ければ、その使用金額Gだけリロード金額を減算更新し、引落しが完了した旨の信号をパーソナルコンピュータ30へ返信する。すると、S 2 5 2aによりYESの判断がなされてS 2 5 2bへ進み、Gの支払処理がなされる。

【0137】なお、RP用決済処理は、以上説明したVP用決済処理とほとんど同じ内容の処理であるために、図示および説明の繰返しを省略する。

【0138】図19(a)は、VP用IC端末19Vの処理を示すフローチャートであり、図19(b)は、RP用IC端末19Rの処理動作を示すフローチャートである。

【0139】図19(a)を参照し、VP用IC端末19Vは、S 2 5 3により、暗証番号チェック処理を行なう。次にS 2 5 4へ進み、クッキー処理を行なう。次にS 2 5 5へ進み、本人証明処理を行なう。次にS 2 5 6へ進み、データ入力処理を行なう。次にS 2 5 7へ進み、ユーザエージェント動作処理を行なう。次にS 2 5 8へ進み、リロード金額の使用処理を行なう。次にS 2 5 9へ進み、署名処理を行なう。

【0140】図19(b)を参照して、RP用IC端末19Rは、S 2 6 0により、暗証番号チェック処理を行ない、S 2 6 2により、本人証明処理を行ない、S 2 6 3により、データ入力処理を行ない、S 2 6 4により、ユーザエージェント動作処理を行ない、S 2 6 5によ

10

20

30

40

50

り、リロード金額の使用処理を行なう。次にS266へ進み、署名処理を行なう。

【0141】図20(a)は、S253, S260に示された暗証番号チェック処理のサブルーチンプログラムを示すフローチャートである。S268により、暗証番号が入力されたか否かの判断がなされ、入力されていない場合にはそのままサブルーチンプログラムが終了する。一方、暗証番号が入力されれば、S269へ進み、入力された暗証番号を記憶している暗証番号と照合する処理がなされる。次にS270へ進み、照合の結果一致するかどうかの判断がなされ、一致しない場合にはS271へ進み、不適正な旨をパーソナルコンピュータ30へ送信する処理がなされる。一方、一致する場合にはS272へ進み、適正な旨の返信を行なう。

【0142】図20(b)は、S254に示されたクッキー処理(VP用)のサブルーチンプログラムを示すフローチャートである。S275により、クッキーの入力があるか否かの判断がなされる。パーソナルコンピュータ30にVP用IC端末19Vが接続された時点で、そのパーソナルコンピュータ30にクッキーの記録があった場合には、前述したように、その記録されているクッキーデータがVP用IC端末19Vへ伝送される(S118参照)。また、パーソナルコンピュータ30によりサイトへアクセスしてそのサイトからクッキーが送信されてきた場合にも、その送信されてきたクッキーデータをVP用IC端末19Vへ伝送する(S123参照)。VP用IC端末19Vでは、S118やS123によってクッキーが伝送されてくれば、S275によりYESの判断がなされてS276へ進み、その入力されたクッキーデータをクッキー記憶領域に記憶する処理を行なう。

【0143】一方、S275によりNOの判断がなされた場合には、S277へ進み、クッキーの呼出があるか否かの判断がなされる。パーソナルコンピュータ30によりサイトへアクセスする場合には、VP用IC端末19Vからクッキーを呼出し、そのクッキーとともにサイトへアクセスする(S121参照)。そのクッキーの呼出処理が行なわれれば、S277によりYESの判断がなされてS278へ進み、クッキー記憶領域に記憶しているクッキーデータをパーソナルコンピュータ30に出力する処理がなされる。

【0144】図20(c)は、S255に示された本人証明処理(VP用)のサブルーチンプログラムを示すフローチャートである。S280により、乱数Rの入力があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。乱数Rの入力があった場合にS281へ進み、VP出生依頼時であるか否かの判断がなされる。VP出生依頼時の場合には、S6, S151で説明したように、RPの認証鍵KNを用いてRPが正当な本人であることを証明する必要がある。そのた

めに、VP出生依頼時の場合にはS283進み、入力された乱数RをRPの認証鍵KNで暗号化してIを生成する処理すなわち $I = E_{KN}(R)$ の算出処理を行なう。そして、と284により、その算出されたIをパーソナルコンピュータ30へ出力する処理がなされる。

【0145】一方、VP出生依頼時でない場合には、S281によりNOの判断がなされてS282へ進み、VPは正当な本人であることを証明するべく、VPの秘密鍵KSを用いて入力された乱数Rを暗号化してIを算出する処理、すなわち、 $I = E_{SK}(R)$ を算出する処理を行なう。そしてS248により、その算出されたIをパーソナルコンピュータ30へ出力する処理がなされる。

【0146】図20(d)は、S262に示された本人証明処理(RP用)のサブルーチンプログラムを示すフローチャートである。S287により、乱数Rが入力されたか否かの判断がなされ、入力されていなければこのサブルーチンプログラムが終了する。一方、入力された場合には、制御がS288へ進み、RP用IC端末19Rに記憶されている認証鍵KNを用いて入力されたRを暗号化してIを算出する処理、すなわち、 $I = E_{KN}(R)$ の算出処理が行なわれる。次にS289へ進み、その算出されたIをパーソナルコンピュータ30へ出力する処理がなされる。

【0147】図21(a)は、S256, S263に示されたデータ入力処理のサブルーチンプログラムを示すフローチャートである。S293により、データ入力があったか否かの判断がなされる。入力されるデータとしては、前述したように、VP管理サーバ9によって誕生したVPに関するデータが記録されているCD-ROMの記録データ、ユーザエージェントの知識データ(S179, S189参照)、引落し額G(S181, S191参照)等がある。これらのデータが入力されれば、制御がS294へ進み、入力データに対応する記憶領域に入力データを記憶させる処理がなされる。

【0148】図21(b)は、S257, S264に示されたユーザエージェント動作処理のサブルーチンプログラムを示すフローチャートである。S295により、公開鍵出力要求があったか否かの判断がなされる。公開鍵の出力要求があった場合には、S298に進み、記憶している公開鍵KPを出力する処理がなされる。S295によりNOの判断がなされた場合にS296へ進み、デビットカード情報の出力要求があったか否かの判断がなされる。あった場合にはS299へ進み、記憶しているデビットカード情報を出力する処理がなされる。

【0149】S296によりNOの判断がなされた場合にはS297へ進み、クレジットカード情報の出力要求があったか否かの判断がなされる。あった場合にはS300へ進み、記憶しているクレジットカード情報を出力する処理がなされる。次にS301へ進み、その他の動作処理が行なわれる。このその他の動作処理は、図22

10

20

30

40

50

に基づいて後述する。

【0150】図21(c)は、S258, S265に示されたりロード金額の使用処理のサブルーチンプログラムを示すフローチャートである。S302により、引落し額Gの引落し要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。あった場合には、S303へ進み、記憶しているリロード金額がGを減算する処理がなされ、S304へ進み、引落し完了信号を返信する処理がなされる。

【0151】図21(d)は、S259, S266により示された署名処理のサブルーチンプログラムを示すフローチャートである。S370により、メッセージダイジェストMDの入力があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。一方、S244等によってMDがIC端末へ伝送されてくれば、S370によりYESの判断がなされS371へ進み、その入力されたメッセージダイジェストMDを秘密鍵KSで復号化して電子署名を生成する処理がなされる。次にS372へ進み、その電子署名D_{es}(MD)を出力する処理がなされる。

【0152】図22は、S301に記載されたその他の動作処理のサブルーチンプログラムを示すフローチャートである。S305により、個人情報の送信要求を受けた否かの判断がなされる。この個人情報とは、図4に示されたユーザエージェント用知識データのことであり、たとえば年齢や職業や各種嗜好情報や家族構成等の個人情報のことである。ユーザが加盟店6やライフ支援センター8やその他各種サイトにアクセスした場合に、サイト側から個人情報を要求される場合がある。個人情報の要求を受けた場合には、制御がS306へ進み、プライバシーポリシーを受信したか否かの判断がなされる。サイト側が、個人情報を要求する場合には、その個人情報の収集目的や利用範囲等を明示したプライバシーポリシーをユーザ側に送信する。そのプライバシーポリシーを受信すれば、制御がS307へ進み、個人情報を送信して良いか否かの判断がなされる。

【0153】この判断は、予めユーザがIC端末19Rまたは19Vに、どのような場合に個人情報を送信して良いか否かを入力設定し、その入力設定データに基づいて判断がなされる。送信要求対象となる個人情報の種類やプライバシーポリシーの内容に基づいて、S307によりYESの判断がなされた場合には、S310へ進み、プライバシーポリシーと個人情報とをまとめてIC端末19Rまたは19Vの秘密鍵KSにより復号化して電子署名を生成する処理がなされる。次にS310へ進み、要求されている個人情報と電子署名とをサイト側に送信する処理がなされる。

【0154】次に制御がS313へ進み、個人情報の送信要求を送信してきたサイトの種類に応じてVPの性格を変化させる処理がなされる。VP用IC端末19Vに

は、ユーザエージェントとしてのプログラムが記憶されているとともに、ユーザがアクセスするサイトの種類に応じてVPの性格を変化させるという、ゲームソフトの分野でよく用いられているプログラムが記憶されている。たとえば、ユーザがVPとして学術的なサイトに頻りにアクセスした場合には、VPの性格が理知的で学者肌の性格となる。一方、ユーザが風俗関係のサイトに頻りにアクセスした場合には、VPの性格が、ふしだらでブロークンな性格となる。

10 【0155】S307によりNOの判断がなされた場合には、S308へ進み、要求されている個人情報が出力できないか否かの判断がなされ、出力できないと判断された場合にはS311へ進み、送信拒絶の旨をサイトに送信する処理がなされた後S313へ進む。

20 【0156】IC端末19Rおよび19Vに記憶されているユーザエージェントでは、送信できるかまたは送信できないかの判断がつかない場合には、制御がS309へ進み、出力要求を受けた個人情報とプライバシーポリシーとをパーソナルコンピュータ30のディスプレイに出力して、ユーザ自身に送信の可否を求め処理がなされる。それを見たユーザは、送信して良いか否かをキーボードから入力する。送信して良い旨の入力があった場合にはS312によりYESの判断がなされてS310へ進むが、送信してはならない入力があった場合には、S312によりNOの判断がなされてS311へ進む。

30 【0157】S305によりNOの判断がなされた場合には、S314へ進み、ユーザであるRPから会話要求があったか否かの判断がなされる。ユーザが、VP(VPのユーザエージェント)と会話したい場合には、会話を要求する旨の操作をキーボードから入力する。すると、S314によりYESの判断がなされてS314aへ進み、VPの現在の正確を反映させながら会話することが可能となる。

【0158】図23, 図24は、コンビニエンスストア2のサーバ16の処理動作を説明するためのフローチャートである。S315により、VPの氏名, Eメールアドレス, 金融機関の名称を受信したか否かの判断がなされ、受信していない場合にS316へ進み、VPが購入した商品を預かったか否かの判断がなされ、預かっていない場合にS317へ進み、商品の引取り操作があったか否かの判断がなされ、ない場合にはS318へ進み、その他の処理を行なった後S315へ戻る。

40 【0159】このS315~S318のループの巡回途中で、決済サーバ10が誕生したVPの氏名, Eメールアドレス, 当該金融機関の名称をコンビニエンスストア2へ送信した場合には(S318参照)、S315によりYESの判断がなされてS319へ進み、正当機関チェック処理がなされた後、S320へ進む。

50 【0160】S320では、R=D_{KP}(L)であるか否かの判断がなされ、正当機関でない場合にはNOの判断

がなされてS321へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合にはS320によりYESの判断がなされてS322へ進み、受信データをデータベース17へ登録する処理がなされる。

【0161】ユーザがVPとしてたとえば電子ショッピング等を行なってそのVPの住所であるコンビニエンスストアに購入商品が配達されてコンビニエンスストア2がその商品を預かった場合には、S316によりYESの判断がなされてS316aへ進み、該当するVPの商品預かり情報のアドレス領域に商品を預かった旨の情報を記憶させる処理がなされる。その際に、当該商品の決済が済んでいるか否かの情報も併せて記憶させる。次に制御がS323へ進み、当該VPのEメールアドレスを割出し、そのEメールアドレスへ商品を預かった旨のメールを送信する処理がなされる。VPは、そのEメールを見ることにより、コンビニエンスストアに購入商品が配達されたことを知ることができ、その商品を引取るためにそのコンビニエンスストアに出向く。

【0162】ユーザがVPとしてコンビニエンスストアに出向き、配達された商品を引取るための操作を行なえば、S317によりYESの判断がなされる。そして制御がS324へ進み、VP用IC端末19Vの差込指示が表示される。それを見たユーザは、自己のVP用IC端末19Vをサーバ19のUSBポートへ差込んで接続する。すると、S325によりYESの判断がなされてS326へ進み、暗証番号チェック処理がなされる。ユーザは、サーバ16に設けられているキーボードからVP用の暗証番号を入力する。暗証番号が一致して適正であることを条件として、制御がS327へ進み、接続されているVP用IC端末19VからVP用の氏名を呼出してそれに基づいてデータベース17を検索する処理がなされる。そして、該当するVPの商品預かり情報のアドレス領域に、商品預かり情報が記録されているか否かの判断がS328によりなされる。商品預かり情報がなければS329へ進み、預かり商品がない旨が表示される。一方、商品預かり情報がある場合にはS330へ進み、電子証明書書の出力要求がVP用IC端末19Vに対しなされる。VP用IC端末19Vは、それを受けて、記憶している電子証明書書をサーバ16に出力する。すると、S331によりYESの判断がなされてS332へ進み、出力されてきた電子証明書書の公開鍵KPを読み出し、S333により、本人チェック処理がなされる。

【0163】次にS334へ進み、 $R = D_{\text{sp}}(I)$ であるか否かの判断がなされる。正当でないなりすましのVPである場合には、S334によりNOの判断がなされてS335へ進み、不適正である旨が表示される。一方、適正なVPであった場合には、制御がS336へ進み、預かり商品番号を表示し、S337により、その商品に関し決済済みであるか否かの判断がなされ、決済済みの場合にはS339へ進むが、決済済みでない場合に

はS338へ進み、決済処理が行なわれる。

【0164】S339では、商品の引渡し完了したか否かの判断がなされる。コンビニエンスストア2の店員は、S336により表示された預かり商品番号を見て、該当する番号の商品を探し出し、顧客にその商品を引渡した後、商品引渡し完了操作を行なう。すると、S339によりYESの判断がなされてS340へ進み、データベース17の商品預かり情報のアドレス領域を更新し、商品預かりなしの状態にした後、S315へ戻る。

10 【0165】S326の暗証番号チェック処理は、図24(a)に示されている。S345により、暗証番号の入力指示が表示され、ユーザが入力すればS347へ進み、その入力された暗証番号をサーバ16に接続されているVP用IC端末19Vへ伝送し、その暗証番号の適否の判定結果がVP用IC端末19Vから返送されてくれば、S349へ進む。S349では、適正な判定結果か否かが判別され、不適正であればS350により不適正の表示を行なってS315へ戻るが、適正であればこのサブルーチンが終了して、制御がS327へ進む。

20 【0166】S333の本人チェック処理は、図24(b)に示されている。S355により、乱数Rを生成してVP用IC端末へ伝送する処理がなされ、チャレンジデータRに対するレスポンスデータIがVP用IC端末から返送されてくるまで待機する。Iが返送されてくれば、このサブルーチンが終了する。

【0167】S338の決済処理は、図24(c)に示されている。S359により、預かり商品の価格を表示する処理がなされ、S360へ進み、入金があるか否かの判断がなされる。ない場合にはS362へ進み、リロード金額による支払操作があったか否かの判断がなされ、ない場合にはS360へ戻る。そして、ユーザが現金による支払を行なってコンビニエンスストアの店員が入金があった旨の操作を行なえば、S360によりYESの判断がなされてS361へ進み、商品販売会社の口座へ入金処理を行なってこのサブルーチンプログラムが終了する。

【0168】一方、ユーザがVP用IC端末19に記憶されているリロード金額を使用して支払操作を行なうべくその旨の操作がなされれば、S362によりYESの判断がなされてS363へ進み、価格Gの引渡し要求をVP用IC端末19Vへ伝送する処理がなされる。そしてS364へ進み、VP用IC端末19Vから引渡し完了信号が出力されてきたか否かの判断がなされ、出力されてくるまで待機する。そして、引渡し完了信号を受信すれば、S364によりYESの判断がなされてS361へ進む。

【0169】図25(a)は、ライフ支援センター8のサービス提供サーバ13の処理動作を示すフローチャートであり、図25(b)は、ライフ支援センター8のセキュリティサーバ14の処理動作を示すフローチャート

である。

【0170】図25(a)を参照して、S365により、クッキーを利用して個人情報を収集する処理がなされ、S366により、アクセスしてきた顧客から直接個人情報を収集する処理がなされ、S367により、収集した個人情報に基づき、当該顧客にふさわしい夢、人生設計、職種、趣味等を推薦して、それらの実現に有意義な加盟店(ニューミドルマン)を紹介する処理がなされる。

【0171】紹介した加盟店(ニューミドルマン)にユーザがアクセスした際には、当該加盟店(ニューミドルマン)が当該ユーザに商品やサービスを推薦する際に必要となる当該ユーザの個人情報をサービス提供サーバ13が当該加盟店(ニューミドルマン)へ提供する。

【0172】S366の顧客からの直接個人情報を収集する具体例としては、まず、顧客の性格や、顧客の欲望(金銭欲か名誉欲か、自己実現欲が高いか否か等)の夢を推薦するのに必要な個人情報を入力してもらう。次にその入力情報に基づいて、データベース15に既に記憶されているVPとしてのユーザの中から性格や欲望等が共通するVPを割出して、そのVPの夢を検索して顧客(ユーザとしてのVP)に推薦する。ユーザは、その推薦されたものの中に希望するものがあれば、それを選択するが、なければ、推薦されたものを参考にしながら自己にふさわしい夢を考え出してユーザ自身が入力する。

【0173】このユーザの選んだ夢が、たとえば「技術と法律を生かせる分野で独立開業すること」であったとすると、サービス提供サーバ13は、技術と法律を生かして独立開業ができる職業として、弁理士等のように条件を満たす職業をリストアップして推薦するとともに、独立開業のために必要な人生設計のプランを作成して推薦する。この人生設計のプランに際して、まず家族のデータを入力してもらって家族全員のライフプランを作成し、次に年収を入力してもらって、その年収等から、生活資金のプランを作成し、次に家族構成や家族の年齢等を入力してもらって、この入力情報に基づいて子供資金計画を作成し、次にマイホーム資金計画を作成し、次にイベント資金計画を作成する。さらに、保険や投資信託等の推薦も行なう。

【0174】さらに、サービス提供サーバ13は、前述した弁理士等の職種を推薦することに伴って、それに必要となる文献や教育機関等を推薦する。その際には、法律や技術の専門書の推薦を行なっている加盟店(ニューミドルマン)を推薦する。

【0175】次に、サービス提供サーバ13は、たとえば弁理士という職種でかつユーザと同じような性格や欲望を持つVPを割出し、そのVPの趣味やレジャーの個人情報を検索して多い順に当該ユーザに推薦する。

【0176】そのユーザの趣味やレジャーが確定すれば、その確定した趣味に必要なとなる用品やガイドブック

等を推薦する加盟店(ニューミドルマン)を推薦する。

【0177】従来の商品等の推薦サービスシステムでは、ユーザが具体的商品について評価した点数やユーザの購買履歴データをもとに、そのデータとマッチする顧客データを割出し、その割出された顧客が高い得点を付けた商品や過去に購入した商品を推薦するというものであった。すなわち、具体的商品データに基づいて具体的商品データを推薦するという方法であった。

【0178】しかし、このサービス提供サーバ13では、上位概念(たとえば夢)の顧客データからだんだん下位概念(具体的商品ニーズ)の顧客データまで誘導し、その商品ニーズが決まれば、その商品ニーズにマッチする最終的な商品の推薦を行なう加盟店(ニューミドルマン)を推薦するというものであり、上位概念から下位概念への誘導型推薦方式である。これにより、より適切な推薦ができるとともに、ユーザ(顧客)の上位概念から下位概念への総合的な顧客情報を収集することができる。

【0179】さらに、推薦した加盟店(ニューミドルマン)が具体的な商品や情報を推薦する際に、その顧客のたとえば夢や職種や趣味等の上位概念レベルでの顧客情報と一致するVPをサービス提供サーバ13が検索し、そのVPを加盟店(ニューミドルマン)に提供し、提供されたVPでかつその加盟店(ニューミドルマン)のデータベースに登録されているVPを加盟店が選び出し、そのVPが高得点を付けた商品や購入した商品を当該顧客(ユーザ)に推薦するようにすれば、より有意義な具体的商品の推薦が可能となる。

【0180】次に、S368では、準オーダーメイド仲介サービスが行なわれる。この準オーダーメイド仲介サービスとは、ライフ支援センター8のデータベース15に記憶されている顧客(ユーザとしてのVP)の中から、共通する個人情報を有するもの同士をグループ化して分類し、そのあるグループに属するVPを共通のニーズを有する顧客群ととらえ、そのあるグループ内の顧客群が共同である商品やサービスに対する希望や理想を出し合い、その希望や理想に適合するサービスや商品をサブライヤ1にオーダーメイドで作成させるというサービスである。1人の顧客(ユーザ)がある商品について希望や理想を出し、その希望や理想にマッチする商品をサブライヤが作成するという完全オーダーメイド方式に比べて、作成された商品やサービスが複数のユーザに購入される分、コストを下げることができるという利点を有する。

【0181】図25(b)を参照して、ライフ支援センター8のセキュリティサーバ14は、S340により、個人情報収集の際、プライバシーポリシーを当該ユーザ(顧客)に提示する処理を行なう。次にS341により、プライバシーポリシーの合意を条件に、双方で電子署名を付したデータをデータベース15に格納する処理

がなされる。そしてS342により、その他のセキュリティ処理がなされる。

【0182】S341に従って収集された個人情報は、図1のデータベース15の格納情報を示す表のように、顧客（ユーザとしてのVP）の氏名ごとに分類されて、個人情報とそれに対応するプライバシーポリシーと、それらがライフ支援センター8の秘密鍵KS1で復号化された電子署名と、個人情報とプライバシーポリシーとが当該VPの秘密鍵KSDによって復号化された電子署名とが格納される。

【0183】このように個人情報を収集して格納することにより、この個人情報がたとえば他の業者に流通して渡ったとしても、その個人情報をチェックすることにより、その個人情報に含まれているプライバシーポリシーが守られた流通がなされているのか否か、そのプライバシーポリシーが守られた個人情報の利用がなされているか否かが、チェック可能となる。一方、個人情報に含まれているプライバシーポリシーを改ざんした場合には、その個人情報に含まれているライフ支援センター8の電子署名およびその個人情報の情報主であるVPの電子署名の整合性が崩れるために、改ざんしたことが容易に判別し得る。これによって、個人情報の不正な売買や不正な使用等を極力防止することができ。

【0184】次に、以上説明した実施の形態における特徴点や変形例等を以下に列挙する。

(1) 図1に示すように、本実施の形態では、金融機関7に、VP管理機能と、決済機能と、認証用機能とを設けたが、金融機関7から、VP管理機能を分離独立させ、金融機関以外の他の守秘義務を有する機関にVP管理機能を肩代わりさせてもよい。その肩代わりする機関としては、官公庁等の公共的機関であってもよい。さらに、RPやVPに電子証明書を発行する電子証明書発行機能を、金融機関7から分離独立させ、専門の認証局に肩代わりさせてもよい。

【0185】また、本実施の形態では、コンビニエンスストアの住所をVPの住所としているが、その代わりに、たとえば郵便局や物流業者における荷物の集配場等をVPの住所としてもよい。またVPの住所となる専用の施設を新たに設立してもよい。

【0186】VPを誕生させる処理は、本実施の形態では、所定機関の一例としての金融機関7が行なっているが、本発明はこれに限らず、たとえば、ユーザ自身が自己の端末（パーソナルコンピュータ30）によりVPを誕生（出生）させ、その誕生させたVPの氏名、住所、公開鍵、口座番号、Eメールアドレス等のVP用情報を、金融機関7等の所定機関に登録するようにしてもよい。

【0187】また、誕生したVPは、必ずしも所定機関に登録させなくてもよい。

(2) 図2に示すように、本実施の形態では、1人の

RPが複数のVPを有することができるようにしているが、1人のRPが1人のVPしか有することができないように構成してもよい。

【0188】本発明でいう「人物」、「個人」の用語は、自然人に限らず法人をも含む広い概念である。本発明でいう仮想人物（VP）の氏名とは、換言すれば実在人物（RP）の匿名であり、仮想人物の氏名と実在人物の匿名とは同じ概念である。したがって、仮想人物の住所やEメールアドレスや電子証明書は、実在人物が匿名でネットワーク上で行動する場合の住所、Eメールアドレス、電子証明書ということになる。

【0189】また、処理装置の一例としてのIC端末19Rまたは19Vを、ICカードや携帯電話あるいはPHS（personal handy-phone system）やPDA（personal digital assistant）等の携帯型端末で構成してもよい。これら携帯型端末で構成する場合には、VP用の携帯型端末とRP用の携帯型端末との2種類のものを用意してもよいが、VP用モードあるいはRP用モードに切換可能に構成し、1種類の携帯型端末で事足りるように構成してもよい。

【0190】図3（b）に示したCD-ROM31によるアプリケーションソフトのインストールに代えて、当該アプリケーションソフトのサプライヤからインターネット経由で当該アプリケーションソフトをパーソナルコンピュータ30へダウンロードするように構成してもよい。

【0191】（3）本実施の形態で、図5に示したように、VPの誕生時にそのVPの電子証明書が自動的に作成されて発行されるように構成したが、その代わりに、ユーザからの電子証明書の発行依頼があつて初めてVPの電子証明書の作成発行を行なうようにしてもよい。

【0192】図8等に示したように、本実施の形態では、RPの本人認証を行なう場合には、RPの認証鍵KNを用いるようにしたが、RPが電子証明書の発行を受けている場合には、その電子証明書内の公開鍵を用いてRPの本人認証を行なうようにしてもよい。

【0193】（4）本実施の形態では、図11に示したように、RP用IC端末19Rが接続されている場合には、送信されてきたすべてのクッキーを拒絶するようにしたが、クッキーの種類等に応じて一部受付けるようにユーザが設定できるようにしてもよい。たとえば、追跡型クッキーだけ拒絶して、その他のクッキーは受付けるように設定可能となるように構成してもよい。

【0194】さらに、VP用IC端末19Vが接続されている場合には、すべてのクッキーをVP用IC端末19Vに記憶させるように構成したが、その代わりに、たとえば追跡型クッキーのみVP用IC端末19Vの方に記憶させ、それ以外のクッキーはパーソナルコンピュータ30側に記憶させる等の、ユーザによる調整設定が可

能となるように構成してもよい。

【0195】(5) 前述したVP用IC端末19VとRP用IC端末19Rとは、ユーザエージェント用プログラムとユーザエージェント知識データとが記憶されており、ユーザエージェントとしての機能を有している。

【0196】前述した正当機関証明処理，正当機関チェック処理，本人証明処理，S4～S7等の本人チェック処理により，本人であることの確認を行なつてなりすましを防止するための本人認証手段が構成されている。

【0197】S13～S16により，バーチャルパーソン（仮想人物）用の電子証明書を作成して発行する仮想人物用電子証明書発行手段が構成されている。S25～S28により，現実世界に実在するリアルパーソン（実在人物）用の電子証明書を作成して発行する実在人物用電子証明書発行手段が構成されている。

【0198】S39～S45により，仮想人物（バーチャルパーソン）用の銀行口座を作成するための処理を行なう銀行口座作成処理手段が構成されている。

【0199】S40～S49により，実在人物（リアルパーソン）または仮想人物（バーチャルパーソン）用のデビットカードを発行するための処理を行なうデビットカード発行処理手段が構成されている。S55～S69により，仮想人物（バーチャルパーソン）に携帯される処理装置（VP用IC端末19V）に対し，該仮想人物（バーチャルパーソン）の銀行口座内の資金の一部を引落してリロードするための処理を行なう資金引落し処理手段が構成されている。

【0200】S57～S74により，仮想人物（バーチャルパーソン）のデビットカードを使用して決済を行なうための処理を行なうデビットカード用決済処理手段が構成されている。S57～S78により，仮想人物（バーチャルパーソン）のクレジットカードを使用しての決済を行なうための処理を行なうクレジットカード用決済処理手段が構成されている。このクレジットカード用決済処理手段は，SecureElectronic Transaction（SET）に準拠して決済を行なう。

【0201】(6) S117，S118により，既に記録されているクッキーデータを仮想人物（バーチャルパーソン）に携帯される処理装置（VP用IC端末19V）に移し替えて記憶させる処理を行なうクッキーデータ移し替え処理手段が構成されている。S122，S123により，クッキーデータが送信されてきた場合に，該クッキーデータを仮想人物（バーチャルパーソン）が携帯する処理装置（VP用IC端末19V）に転送して記憶させるための処理を行なうクッキーデータ転送処理手段が構成されている。

【0202】S132，S133により，ユーザが実在人物（リアルパーソン）として端末を通してネットワーク上で行動する際に，当該端末にクッキーが記録されている場合に，その旨の報知を行なうクッキー記録報知手

段が構成されている。S135，S136により，ユーザが実在人物（リアルパーソン）として端末を通してネットワーク上で行動する際に，クッキーが前記端末に送られてきた場合に，当該クッキーを拒絶可能とするための処理を行なうクッキー拒絶手段が構成されている。このクッキー拒絶手段は，すべてのクッキーを拒絶してもよいが，たとえば追跡型クッキーのみを拒絶できる等のように，ユーザ側において調整設定可能に構成してもよい。

10 【0203】さらに，本実施の形態では，図11に示したように，クッキーの受付を制限または拒絶するようにしたが，それに代えてまたはそれに加えて，ユーザがサイト側に再アクセスした際に，既に記憶しているクッキーを当該サイト側へ送信することを禁止または制限するように制御してもよい。すなわち，本発明における個人情報保護システムにおいては，実在人物としてネットワーク上で行動する場合と仮想人物としてネットワーク上で行動する場合とで，サイト側がユーザを識別するために送信してきた識別データであつて既に記憶されている識別データを前記サイト側へ送信する際の送信制限を異

20 ならせることができるようにしてもよい。
【0204】(7) S140～S158により，ユーザが自己の仮想人物（バーチャルパーソン）の出生依頼を行なう処理を行なうための出生依頼処理手段が構成されている。S9～S12により，出生させる仮想人物（バーチャルパーソン）の住所であつて出生依頼者である実在人物（リアルパーソン）の住所とは異なった住所を決定するための処理を行なう住所決定処理手段が構成されている。この住所決定処理手段は，コンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定する。また，この住所決定処理手段は，出生依頼者である実在人物（リアルパーソン）の希望するコンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定可能である。また，この住所決定処理手段は，出生依頼者である実在人物（リアルパーソン）の住所に近いコンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定することが可能である。

30 【0205】S305～S312により，ユーザに携帯される前記処理装置（RP用IC端末19R，VP用IC端末19V）に設けられ，当該処理装置の所有者であるユーザの実在人物（リアルパーソン）としての個人情報または仮想人物（バーチャルパーソン）としての個人情報の送信要求を受けた場合に，記憶している個人情報の中から該当する個人情報を選び出して出力する処理が可能で個人情報自動出力手段が構成されている。この個人情報自動出力手段は，送信要求の対象となっている個人情報が送信してよいものであるか否かを自動的に判別するための処理を行なう自動判別処理手段（S307，308，310，311）を含んでいる。この自動判別

処理手段は、どの種類の個人情報を出力してよいかをユーザが事前に入力設定でき、その入力設定に従って自動判別を行なう。またこの自動判別処理手段は、自動判別できない場合には、要求対象となっている個人情報と送信されてきたプライバシーポリシーとを出力してユーザに対し送信の許否を求めるための処理を行なう（S309）。

【0206】S313により、ユーザに携帯される仮想人物（バーチャルパーソン）用の処理装置に設けられ、当該処理装置の使用状況に応じて当該処理装置によって形成される仮想人物の性格を変化させる仮想人物性格変化形成手段が構成されている。この仮想人物性格変化形成手段は、ユーザが仮想人物（バーチャルパーソン）としてアクセスしたサイトの種類に応じて性格を変化させる。

【0207】S314, S314aにより、ユーザが仮想人物（バーチャルパーソン）と会話を要求した場合に、前記性格変化形成手段により形成された現在の性格を反映して仮想人物（バーチャルパーソン）との会話を現実させる処理を行なう性格反映型会話実現処理手段が構成されている。

【0208】コンビニエンスストア2により、仮想人物（バーチャルパーソン）がネットワーク上で購入した商品が配達されてきた場合に当該商品を預る商品預り場が構成されている。データベース17により、前記商品預り場で商品を預る対象となる仮想人物（バーチャルパーソン）を登録しておくバーチャルパーソン登録手段が構成されている。このバーチャルパーソン登録手段は、仮想人物（バーチャルパーソン）ごとに分類して、商品を預っているか否かを特定するための預り特定情報が記憶される。さらに、当該商品の決済が済んでいるか否かを特定するための決済特定情報が記憶される。また、前記仮想人物（バーチャルパーソン）ごとに分類して当該仮想人物（バーチャルパーソン）のEメールアドレスを記憶している。

【0209】S323により、前記商品預り場に設けられ、商品を預っている仮想人物（バーチャルパーソン）のEメールアドレスに対し商品を預った旨のEメールを送信するための処理を行なうEメール送信処理手段が構成されている。S317～S340により、前記商品預り場に設けられ、ユーザが仮想人物（バーチャルパーソン）として商品を引取りにきた場合に、当該ユーザに対し該当する商品を引渡すための処理を行なう商品引渡し処理手段が構成されている。この商品引渡し処理手段は、引取りにきたユーザの仮想人物（バーチャルパーソン）が本人であることを確認できたことを条件として引渡し処理を行なう。前記商品引き渡し処理手段は、引き渡す商品が決済済みであるか否かを判別し、決済済みでない場合には決済が行なわれたことを条件として商品の引渡し処理を行なう。

【0210】(8) 前記ライフ支援センター8のサービス提供サーバ13により、ユーザの個人情報を収集して、該個人情報に基づいて当該ユーザのライフを支援するライフ支援手段が構成されている。このライフ支援手段は、ユーザの人生の根幹をなす上位の事項（たとえばユーザの夢や人生設計）を推薦し、次にそれよりも下位の事項（たとえば職種や進路等）を推薦し、次にさらに下位の事項（たとえば趣味等）を推薦する等のように、上位から下位への順に推薦処理を行なう。さらに、ライフ支援処理手段は、推薦した事項に関連する消費支援業者（ニューミドルマン等の加盟店）を推薦する処理を行なう。その推薦の際に、収集した当該ユーザの個人情報を前記推薦した消費支援業者に提供する。

【0211】S340により、ユーザの個人情報を収集する際に当該ユーザに対しプライバシーポリシーを提示するプライバシーポリシー提示手段が構成されている。S341により、前記プライバシーポリシー提示手段により提示されたプライバシーポリシーへの合意をユーザから得られたことを条件に、当該ユーザの個人情報を収集して格納する個人情報収集格納手段が構成されている。この個人情報収集格納手段は、当該ユーザの個人情報と、当該ユーザに提示した前記プライバシーポリシーと、前記個人情報と前記プライバシーポリシーとに対して、個人情報収集業者側の電子署名と前記ユーザ側の電子署名を併せてワンセットの情報として格納する。

【0212】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0213】

【課題を解決するための手段の具体例】次に、課題を解決するための各種手段と実施の形態との対応関係を以下に示す。

【0214】(1) ネットワーク（インターネットI）上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップ（S1～S12）と、前記実在人物と前記仮想人物との対応関係を特定可能な情報を守秘義務のある所定機関（金融機関7）に登録する登録ステップ（S15）とを含むことを特徴とする、個人情報保護方法。

【0215】(2) 前記所定機関は、金融機関7であることを特徴とする、個人情報保護方法。

【0216】(3) ネットワーク（インターネットI）上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物（リアルパーソン）がネットワー

ク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップ（S1～S12）と、前記仮想人物用の電子証明書を発行する電子証明書発行ステップ（S16）とを含むことを特徴とする、個人情報保護方法。

【0217】（4） ネットワーク（インターネットI）上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップ（S1～S12）と、前記仮想人物の住所を、前記実在人物とは異なった住所（コンビニエンスストアの住所）に設定するための住所設定ステップ（S9～S12）とを含むことを特徴とする、個人情報保護方法。

【0218】（5） 前記仮想人物の住所は、所定のコンビニエンスストアの住所である。

（6） ネットワーク（インターネットI）上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップ（S1～S12）と、前記仮想人物用のクレジット番号を発行するクレジット番号発行ステップ（クレジットカード発行会社4による発行ステップ）とを含み、前記クレジット番号発行ステップにより発行されたクレジット番号を利用して前記仮想人物としてクレジットによる支払を可能にした（S56, S58, S59, S75～S78）。

【0219】（7） ネットワーク（インターネットI）上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップ（S1～S12）と、前記仮想人物用の銀行口座を開設するための処理を行なう口座開設処理ステップ（S39, S42～S45）と、前記口座開設処理ステップによって開設された銀行口座内の資金を利用して前記仮想人物として決済ができるようにした（S55～S57, S60～S74）。

【0220】（8） ネットワーク（インターネットI）上での個人情報を保護する個人情報保護方法であって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる仮想人物誕生ステップ（S1～S12）を含み、前記実在人物としてネットワーク上で行動する場合と前記仮想人物としてネッ

トワーク上で行動する場合とで、サイト側がユーザを識別するために送信してくる識別データ（クッキー）の受付制限を異ならせることができるようにした（S110～S123, S125～S137）。

【0221】（9） ネットワーク（インターネットI）上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる処理を行なう仮想人物誕生処理手段（S1～S12）と、前記実在人物と前記仮想人物との対応関係を特定可能な情報を守秘義務のある所定機関において登録する処理を行なう登録処理手段（S15）を含むことを特徴とする、個人情報保護システム。

【0222】（10） 前記所定機関は、金融機関7である。

（11） ネットワーク（インターネットI）上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる処理を行なう仮想人物誕生処理手段（S1～S12）と、前記仮想人物用の電子証明書を発行するための処理を行なう電子証明書発行処理手段（S16）とを含む。

【0223】（12） ネットワーク（インターネットI）上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段（S1～S12）と、前記仮想人物の住所を、前記実在人物とは異なる住所に設定するための処理を行なう住所設定手段（S9～S12）とを含む。

【0224】（13） 前記仮想人物の住所は、所定のコンビニエンスストアの住所である（S9～S11）。

【0225】（14） ネットワーク（インターネットI）上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段（S1～S12）と、前記仮想人物用のクレジット番号を発行するための処理を行なうクレジット番号発行処理手段（カード発行会社4）とを含み、該クレジット番号発行処理手段により発行されたクレジット番号を利用して前記仮想人物としてクレジットによる支払ができるようにした（S58, S

56, S75~S78)。

【0226】(15) ネットワーク(インターネットI)上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物(リアルパーソン)がネットワーク上で行動する際に、仮想人物(バーチャルパーソン)になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる処理を行なう仮想人物誕生処理手段(S1~S12)と、前記仮想人物用の銀行口座を開設するための処理を行なう口座開設処理手段(S39, S42~S45)とを含み、該口座開設処理手段によって開設された口座内の資金を利用して前記仮想人物として決済ができるようにした(S55~S57, S60~S74)。

【0227】(16) ネットワーク(インターネットI)上での個人情報を保護する個人情報保護システムであって、現実世界での実在人物(リアルパーソン)がネットワーク上で行動する際に、仮想人物(バーチャルパーソン)になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段(S1~S12)を含み、前記実在人物としてネットワーク上で行動する場合と前記仮想人物としてネットワーク上で行動する場合とで、サイト側がユーザを識別するために送信してくる識別データ(クッキー)の受付制限を異ならせることができるようにした(S110~S123, S125~S137)。

【0228】(17) ネットワーク(インターネットI)上での個人情報の保護に用いられる処理装置(VP管理サーバ9)であって、現実世界での実在人物(リアルパーソン)がネットワーク上で行動する際に、仮想人物(バーチャルパーソン)になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させる要求を受付ける要求受付手段(S1)と、該要求受付手段により要求が受け付けられたことを条件として(S1によりYESの判断がなされたことを条件として)、仮想人物を誕生させるための処理を行なう仮想人物誕生処理手段(S1a~S12)と、該仮想人物誕生処理手段により誕生した仮想人物と該仮想人物に対応する前記実在人物との対応関係を特定可能な情報をデータベースとして記憶させるための処理を行なう対応関係記憶処理手段(S15)とを含む。

【0229】(18) ネットワーク(インターネットI)上での個人情報を保護するための処理装置(VP管理サーバ9)であって、現実世界での実在人物(リアルパーソン)がネットワーク上で行動する際に、仮想人物(バーチャルパーソン)になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物の公開鍵(KB)の入力を受付けて(S14)、該入力された公開鍵をデータベースに記憶させるための処理を行なう公開鍵記憶処理手段(S15)と、前記記憶され

た公開鍵に対応する前記仮想人物用の電子証明書を作成して発行する処理を行なうための電子証明書作成発行処理手段(S16)とを含み、該電子証明書作成発行処理手段は、前記実在人物と前記仮想人物との対応関係を特定可能な情報が守秘義務のある所定機関(金融機関7)に登録されている登録済みの前記仮想人物であることを条件として(S7によりYESの判断がなされたことを条件として)、電子証明書の作成発行処理を行なう(S16の処理を行なう)。

10 【0230】(19) ネットワーク(インターネットI)上での個人情報を保護するための処理装置(加盟店6のサーバ)であって、現実世界での実在人物(リアルパーソン)がネットワーク上で行動する際に、仮想人物(バーチャルパーソン)になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物に発行されたクレジット番号を利用してクレジット支払による購入要求があった場合に、支払の承認処理を行なうための支払承認処理手段(支払承認部33)と、該支払承認処理手段により承認されたクレジットによる支払の要求をクレジットカード発行会社4に出すための処理を行なう支払要求処理手段(支払要求部33)とを含み、前記支払承認処理手段は、前記仮想人物用に発行された電子証明書を確認した上で、支払の承認を行なう。

20 【0231】(20) ネットワーク(インターネットI)上での個人情報を保護するための処理装置(決済サーバ10)であって、現実世界での実在人物(リアルパーソン)がネットワーク上で行動する際に、仮想人物(バーチャルパーソン)になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物用に開設された銀行口座内の資金を決済に用いるために引落し引落し要求を受付けるための処理を行なう引落し要求受付処理手段(S55)と、該引落し要求受付処理手段により引落し要求が受け付けられた場合に、該当する前記仮想人物に相当する銀行口座を割出して該銀行口座内の資金から引落し要求金額(G)に相当する資金を引落すための処理を行なう引落し処理手段(S69)とを含んでいる。

30 【0232】(21) ネットワーク(インターネットI)上での個人情報を保護するための処理装置(サーバ16)であって、現実世界での実在人物(リアルパーソン)がネットワーク上で行動する際に、仮想人物(バーチャルパーソン)になりすまして該仮想人物として行動できるようにするために誕生した所定の仮想人物の住所であって、前記実在人物とは異なる住所(コンビニエンスストア2の住所)に前記処理装置が設置されており、該処理装置が設置されている住所を自己の住所としている前記仮想人物を特定可能な情報をデータベース17に記憶させるための処理を行なう記憶処理手段(S32)と、該記憶処理手段に記憶されている仮想人物が購入した商品であって前記処理装置が設置されている住所

に配達されてきた商品を預かったことを特定可能な情報をデータベースに記憶させるための処理を行なう預り情報記憶処理手段（S316a）と、前記預った商品の引渡し要求があった場合に（S317によりYESの判断がなされた場合に）、当該引渡し要求を出した仮想人物が前記データベースに記憶されている仮想人物であることを確認し（S327）、かつ、商品を扱っている仮想人物であることを確認したことを条件として（S328によりYESの判断がなされたことを条件として）、該当する商品の受渡しの許可を出すための処理を行なう受渡し許可処理手段（S336）とを含む。

【0233】（22） ネットワーク（インターネットI）上での個人情報を保護するためのプログラムを記録している記録媒体（CD-ROM31）であって、コンピュータ（パーソナルコンピュータ30）に、現実世界での実在人物（リアルパーソン）がネットワーク上で行動する際に、仮想人物（バーチャルパーソン）になりすまして該仮想人物として行動できるようにするための所定の仮想人物を誕生させるための要求操作があったか否かを判定する誕生要求判定手段（S141）と、該誕生要求判定手段により誕生要求があった旨の判定がなされた場合に、前記仮想人物の出生依頼要求を所定機関（金融機関7）に送信するための処理を行なう出生要求送信手段（S142）と、前記仮想人物の出生要求を行なう前記実在人物を特定可能な情報であって前記仮想人物の出生に必要な情報を前記所定機関へ送信するための処理を行なう所定情報送信手段（S147～S149）と、して機能させるためのプログラムが記憶されていることを特徴とする、コンピュータ読取可能な記録媒体。

【0234】（23） ネットワーク（インターネットI）上での個人情報を保護するための処理装置（VP用IC端末19V）であって、該処理装置は、ユーザの端末（パーソナルコンピュータ30）に対して情報のやり取りが可能に構成されるとともに（USBポート18を介して情報のやり取りが可能に構成されているとともに）、ユーザに携帯される携帯型の処理装置であり、現実世界での実在人物（リアルパーソン）である前記ユーザがネットワーク上で所定の仮想人物になりすまして該仮想人物として行動する際に使用され、サイト側がユーザを識別するために送信してくる識別データ（クッキー）が前記端末に対し送信されてきた場合に該識別データを当該端末の代わりに記憶可能に構成されている（S276）。

【0235】（24） さらに、前記端末（パーソナルコンピュータ30）によってユーザがサイトにアクセスした際に、必要に応じて記憶している前記識別データ（クッキーデータ）を出力して該識別データを前記サイトに送信できるように構成されている（S278）。

【0236】（25） 前記処理装置（VP用IC端末19V）は、前記ユーザの端末に対し情報の入出力を可

能にするための入出力部（I/Oポート21）と、前記ユーザの端末から前記識別情報が入力されてきた場合に（S275によりYESの判断がなされた場合に）、該入力された識別情報を記憶する識別情報記憶手段（S276）とをさらに含む。

【0237】（26） 前記処理装置（VP用IC端末19V）は、前記ユーザの端末から前記識別情報の出力指令が入力されてきた場合に（S277によりYESの判断がなされた場合に）、記憶している前記識別情報を外部出力する識別情報外部出力手段（S278）をさらに含む。

【0238】（27） 前記処理装置（VP用IC端末19V）は、前記仮想人物に関する情報（VPの氏名、住所、VPのEメールアドレス、VPの公開鍵と秘密鍵、VPの年齢、職業等）を記憶しており、前記VPに関する情報の出力指令が入力されてきた場合に（S295、S305等によりYESの判断がなされた場合に）、前記記憶している仮想人物に関する情報を外部出力する情報外部出力手段（S298、S310等）をさらに含む。

【0239】本発明は、前述した（1）～（27）のみに限定されるものではなく、（1）～（27）の中から任意に2つ以上選択したものの組合せも、本発明の解決手段である。

【0240】

【課題を解決するための手段の具体例の効果】仮想人物誕生ステップにより仮想人物が誕生し、実在人物がネットワーク上で行動する場合にはその仮想人物になりすまして行動することができ、仮想人物の個人情報が流出することがあっても実在人物の個人情報を流出することを防止することができ、ユーザのプライバシーを保護することが可能となる。しかも、前記実在人物と前記仮想人物との対応関係を特定可能な情報が守秘義務のある所定機関に登録されるために、たとえば仮想人物がネットワーク上で目に余る不正行為を行なった場合に、前記所定機関がその仮想人物を手掛かりにそれに対応する実在人物を特定することができ、ネットワーク上での仮想人物の不正行為を抑止する効果も期待し得る。

【0241】前記所定機関が金融機関である場合には、仮想人物として金融機関を利用して決済を行なう場合に、当該金融機関がその仮想人物を手掛かりに実在人物を割出すことも可能であるために、仮想人物であっても安心して決済を行なわせることが容易となる。

【0242】仮想人物用の電子証明書が発行されるために、その仮想人物がネットワーク上で行動する際にその発行された電子証明書を提示することによりある程度の身元保証機能を期待することができ、仮想人物ということで身元が不明であることに起因してネットワーク上での行動範囲が規制されてしまう不都合を極力防止することができる。

10

20

30

40

50

【0243】仮想人物の住所を、実在人物とは異なった住所に設定するために、その仮想人物がネットワーク上で商品等を購入した場合に、その購入商品の配達先を実在人物とは異なる住所にすることができ、仮想人物への商品の配達に際してその配達先の住所を手掛かりに実在人物が見破られてしまう不都合を極力防止することができる。

【0244】仮想人物の住所を所定のコンビニエンスストアの住所にした場合には、コンビニエンスストアが広く全国に分散配置されている関係上、購入商品等の引取りに出向く際に便利である。

【0245】仮想人物用のクレジット番号が発行されて、そのクレジット番号を利用して仮想人物がクレジットによる支払が可能となるために、仮想人物がネットワーク上でクレジット決済を行なう際に実在人物のクレジット番号を使用することなく仮想人物用のクレジット番号を使用することができ、実在人物用のクレジット番号を手掛かりに実在人物が見破られてしまう不都合を極力防止することができる。

【0246】仮想人物用の銀行口座が開設されてその銀行口座内の資金を利用して仮想人物が決済をすることができるために、仮想人物が決済を行なう際に実在人物の銀行口座ではなく仮想人物用の銀行口座を利用することができ、実在人物用の銀行口座を手掛かりに実在人物が見破られてしまう不都合を極力防止することができる。

【0247】実在人物としてネットワーク上で行動する場合と仮想人物としてネットワーク上で行動する場合とで、サイト側がユーザを識別するために送信して識別データの受付制限を異ならせることができるために、比較的識別データに対し寛容にすることができる仮想人物としてネットワーク上で行動する場合には識別データの受付制限を緩和して、業者側の個人情報の収集に極力協力して、収集した個人情報に基づいた業者側のサービス提供を極力受けることができるようにするとともに、実在人物として行動する場合には識別データの受付制限を厳しくすることにより、実在人物としての個人情報が漏洩してしまう不都合を極力防止することができる。

【0248】仮想人物用の電子証明書を作成して発行する際に、実在人物と仮想人物との対応関係を特定可能な情報が守秘義務のある所定機関に登録されている登録済みの仮想人物であることを条件として、電子証明書の作成発行処理がなされるために、その電子証明書を仮想人物が提示した際には、当該仮想人物は守秘義務のある所定機関に登録されていることを確認することができ、電子証明書を通じて信頼性のある仮想人物であることを証明することができる。

【0249】仮想人物の住所であって実在人物とは異なる住所に設置された処理装置により、当該処理装置が設置されている住所を自己の住所としている仮想人物を特定可能な情報がデータベースに記憶され、預った商品の

引渡し要求があった場合に、引渡し要求を出した仮想人物が前記データベースに記憶されている仮想人物であることを確認し、かつ、商品を預かっている仮想人物であることを確認したことを条件として、該当する商品の引渡しの許可を出す処理がなされるために、商品の引渡しに際し仮想人物が本当に本人であることを確認して極力間違いなく商品を引き渡すことが可能となり、商品引渡しの信頼性が向上する。

【0250】仮想人物の誕生要求があったか否かを判定する誕生要求判定手段と、仮想人物の出生依頼要求を送信するための出生要求送信手段と、実在人物を特定可能な情報であって前記仮想人物の出生に必要となる情報を所定機関へ送信するための所定情報送信手段として機能させるためのプログラムが記憶されているコンピュータ読取可能な記録媒体をコンピュータに読取らせることにより、前述した各種手段の機能を発揮することができ、仮想人物を出生させて実在人物がその仮想人物になりすましてネットワーク上で行動することが可能となる。

【0251】サイト側がユーザを識別するために送信する識別データがユーザの端末に対し送信されてきた場合にその識別データを当該ユーザの端末の代わりにユーザが携帯している処理装置に記憶可能となるために、ユーザの端末の方は極力識別データが記録されない状態にすることができ、そのユーザの端末を利用してユーザが実在人物として行動する際に既にその端末に記憶されている識別データに基づいて実在人物としての個人情報が漏洩してしまう不都合を極力防止することができる。

【0252】さらに、ユーザがユーザの端末を通して仮想人物としてサイトにアクセスした際に、必要に応じて前記処理装置に記憶されている識別データをそのサイトに送信することができるために、仮想人物としてネットワーク上で行動する際には、積極的に識別データを業者側に提供して積極的に仮想人物の個人情報を提供し、その見返りとしての業者側における各種サービスを受けることが可能となる。

【図面の簡単な説明】

【図1】 個人情報保護システムの全体構成を示す概略システム図である。

【図2】 金融機関に設置されたデータベースに記憶されている各種データを示す説明図である。

【図3】 (a)はコンビニエンスストアに設置されているデータベースに記憶されている各種情報を説明するための説明図であり、(b)はユーザの端末の一例としてのパーソナルコンピュータの正面図である。

【図4】 ユーザに携帯されるV P用IC端末の回路を示すブロック図および記憶情報の内訳を示す図である。

【図5】 V P管理サーバの処理動作を示すフローチャートである。

【図6】 認証用サーバの処理動作を示すフローチャートである。

【図7】 決済サーバの処理動作を示すフローチャートである。

【図8】 決済処理のサブルーチンプログラムを示すフローチャートである。

【図9】 (a)は決済処理のサブルーチンの一部を示し、(b)は正当機関証明処理のサブルーチンを示すフローチャートである。

【図10】 パーソナルコンピュータの処理動作を示すフローチャートである。

【図11】 (a)はVP用クッキー処理のサブルーチンを示すフローチャートであり、(b)はRP用のクッキー処理を示すフローチャートである。

【図12】 VP出生依頼処理のサブルーチンを示すフローチャートである。

【図13】 (a)は正当機関チェック処理のサブルーチンを示すフローチャートであり、(b)は電子証明書発行要求処理のサブルーチンを示すフローチャートである。

【図14】 (a)はVP用入力処理のサブルーチンを示すフローチャートであり、(b)はRP用入力処理のサブルーチンを示すフローチャートである。

【図15】 SETによる決済処理の概要を説明するための説明図である。

【図16】 VP用決済処理のサブルーチンを示すフローチャートである。

【図17】 (a)は本人証明処理のサブルーチンの示すフローチャートであり、(b)はVP用決済処理のサブルーチンの一部を示すフローチャートである。

【図18】 VP用決済処理のサブルーチンの一部を示すフローチャートである。

【図19】 (a)はVP用IC端末の処理を示すフローチャートであり、(b)はRP用IC端末の処理を示すフローチャートである。

【図20】 (a)は暗証番号チェック処理のサブルーチンを示すフローチャートであり、(b)はクッキー処

理のサブルーチンを示すフローチャートであり、(c)は本人証明処理(VP用)のサブルーチンを示すフローチャートであり、(d)は本人証明処理(RP用)のサブルーチンを示すフローチャートである。

【図21】 (a)はデータ入力処理のサブルーチンを示すフローチャートであり、(b)はユーザエージェント動作処理のサブルーチンを示すフローチャートであり、(c)はリロード金額の使用処理を示すフローチャートであり、(d)は署名処理のサブルーチンを示すフローチャートである。

【図22】 その他の動作処理のサブルーチンを示すフローチャートである。

【図23】 コンビニエンスストアのサーバ処理を示すフローチャートである。

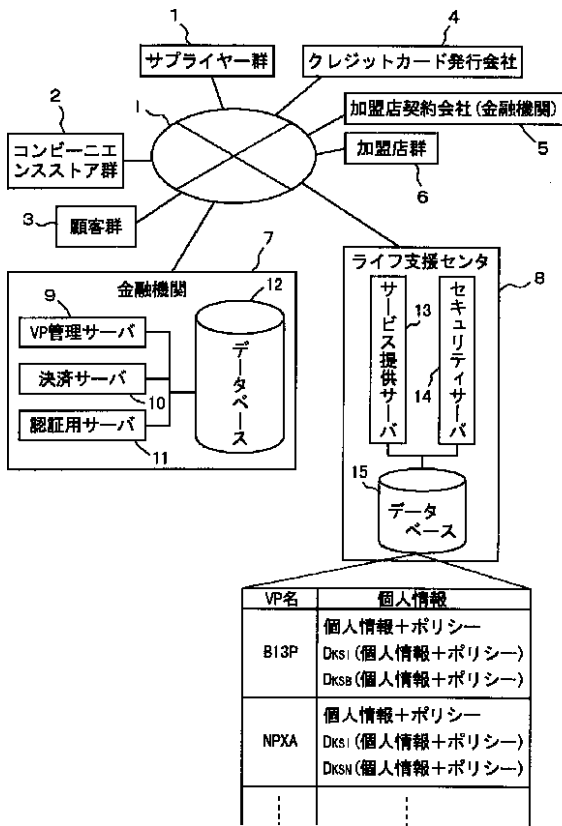
【図24】 (a)は暗証番号チェック処理のサブルーチンを示すフローチャートであり、(b)は本人チェック処理のサブルーチンを示すフローチャートであり、(c)は決済処理のサブルーチンを示すフローチャートである。

【図25】 (a)はライフ支援センターのサービス提供サーバの処理を示すフローチャートであり、(b)はライフ支援センターのセキュリティサーバの処理を示すフローチャートである。

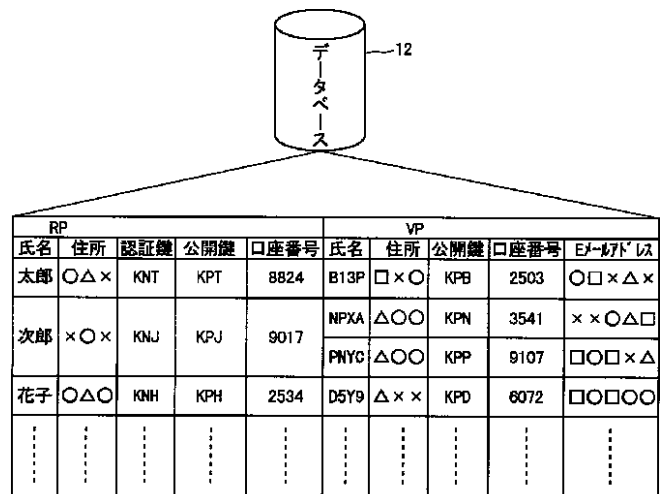
【符号の説明】

Iはインターネット、1はサプライヤ群、7は金融機関、4はクレジットカード発行会社、5は加盟店契約会社、6は加盟店群、2はコンビニエンスストア群、9はVP管理サーバ、10は決済サーバ、11は認証用サーバ、8はライフ支援センター、13はサービス提供サーバ、14はセキュリティサーバ、12、15はデータベース、30はパーソナルコンピュータ、31はCD-ROM、19RはRP用IC端末、19VはVP用IC端末、20はLSIチップ、24はCPU、25はROM、23はコプロセッサ、22はRAM、26はEEPROM、33は支払承認部、34は支払要求部である。

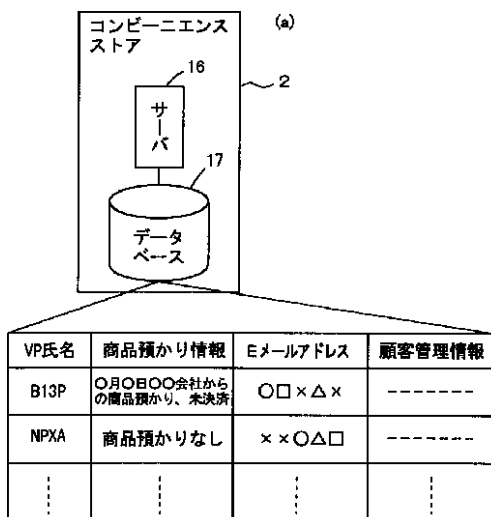
【図1】



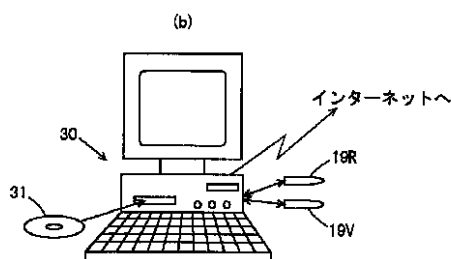
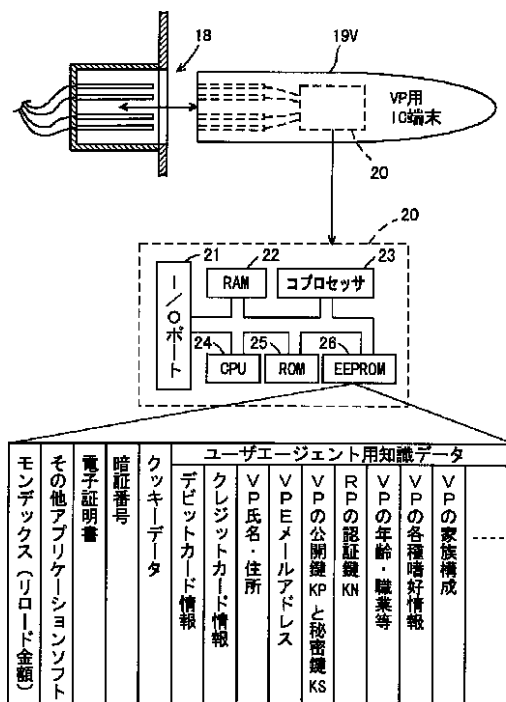
【図2】



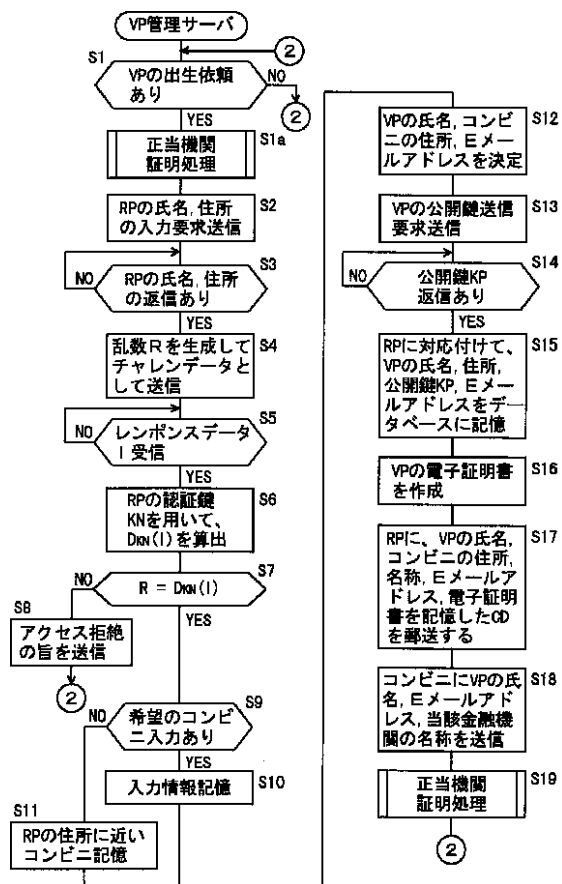
【図3】



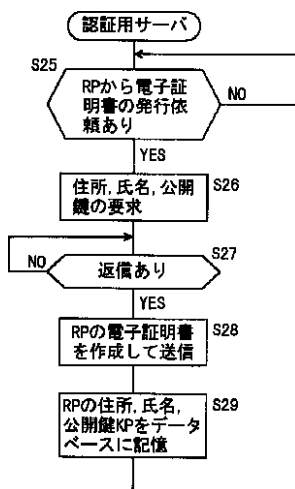
【図4】



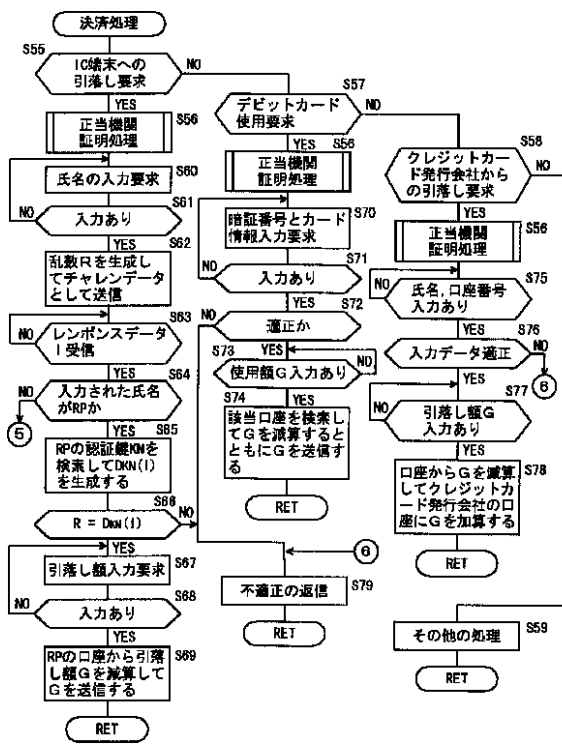
【図5】



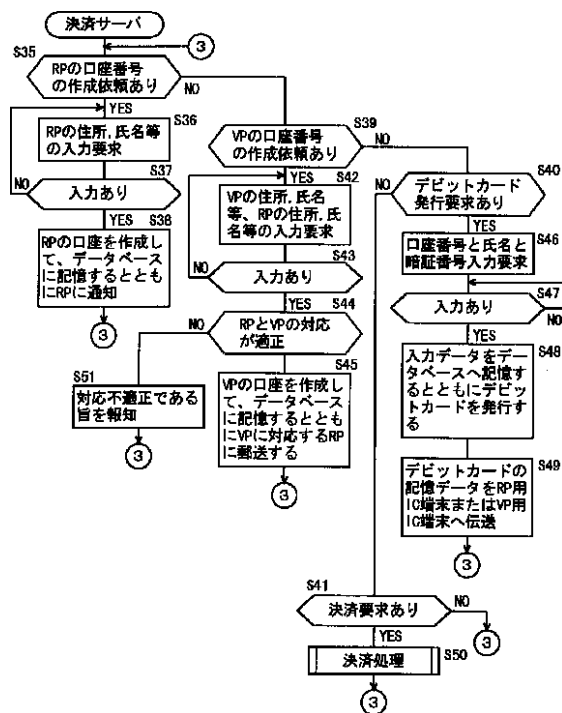
【図6】



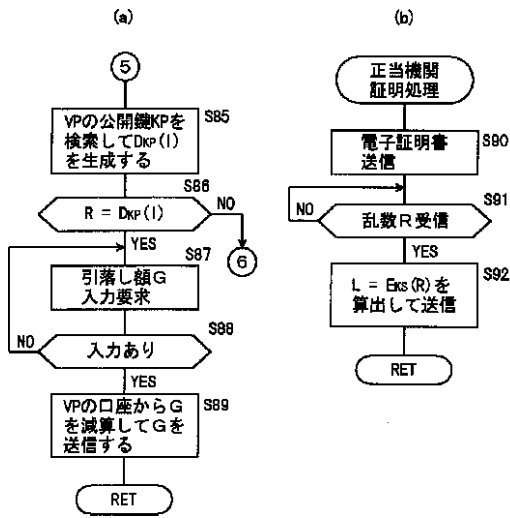
【図8】



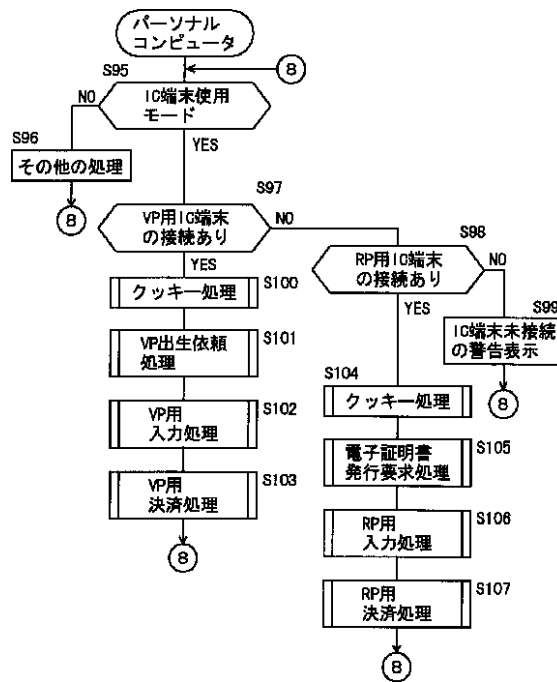
【図7】



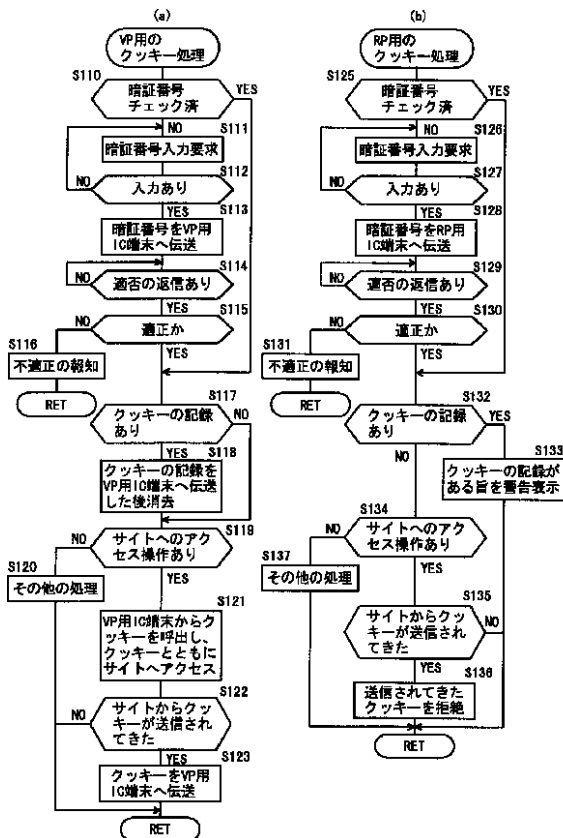
【図9】



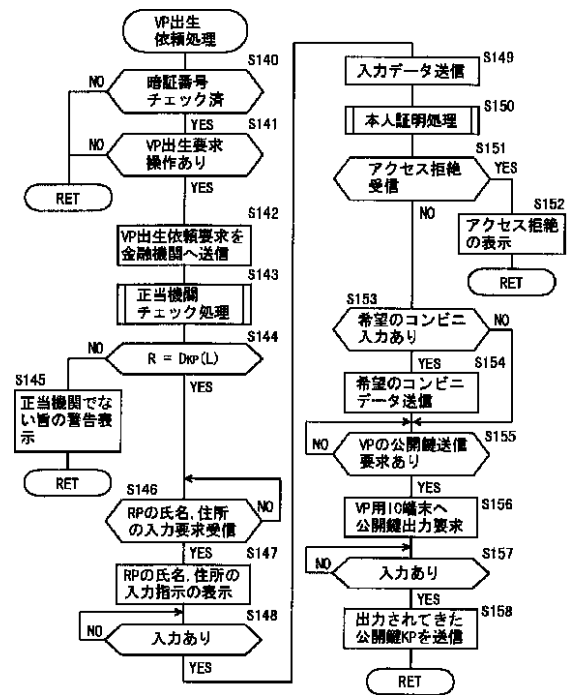
【図10】



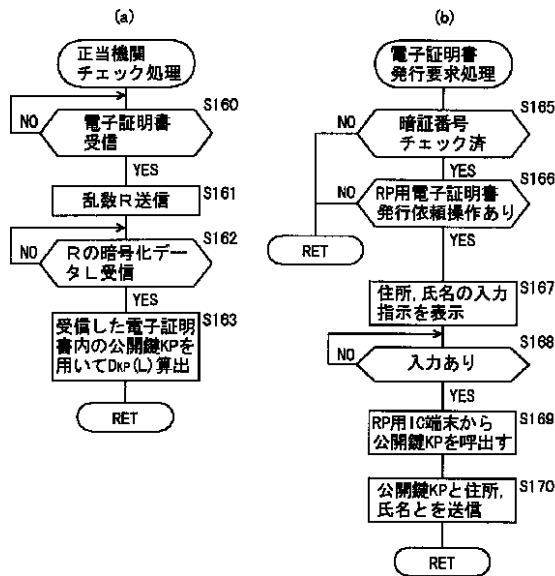
【図11】



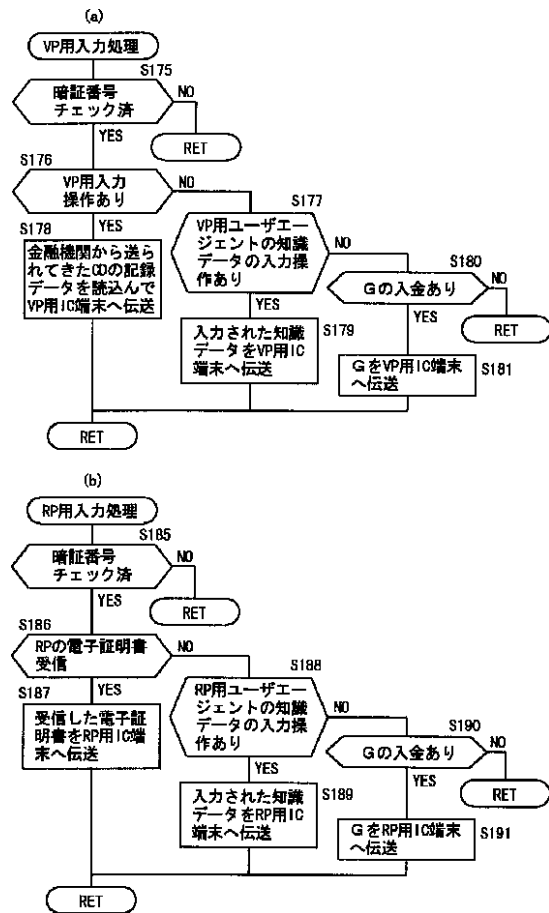
【図12】



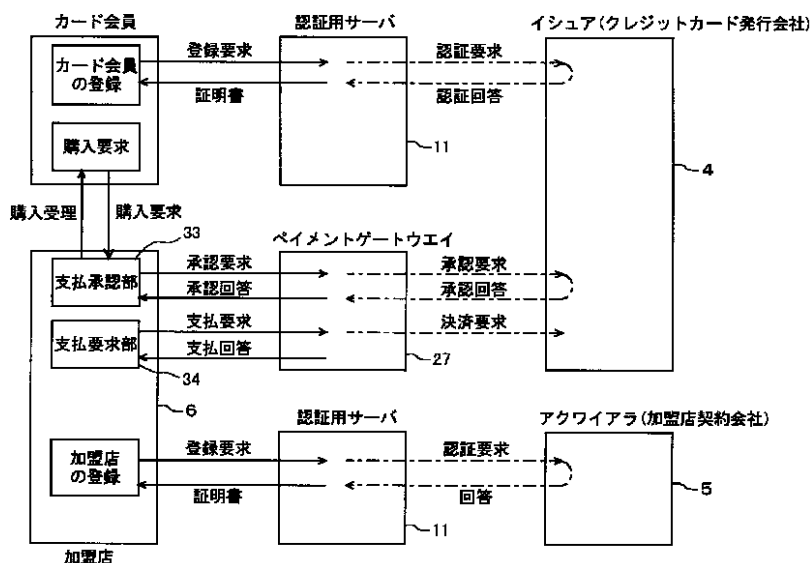
【図13】



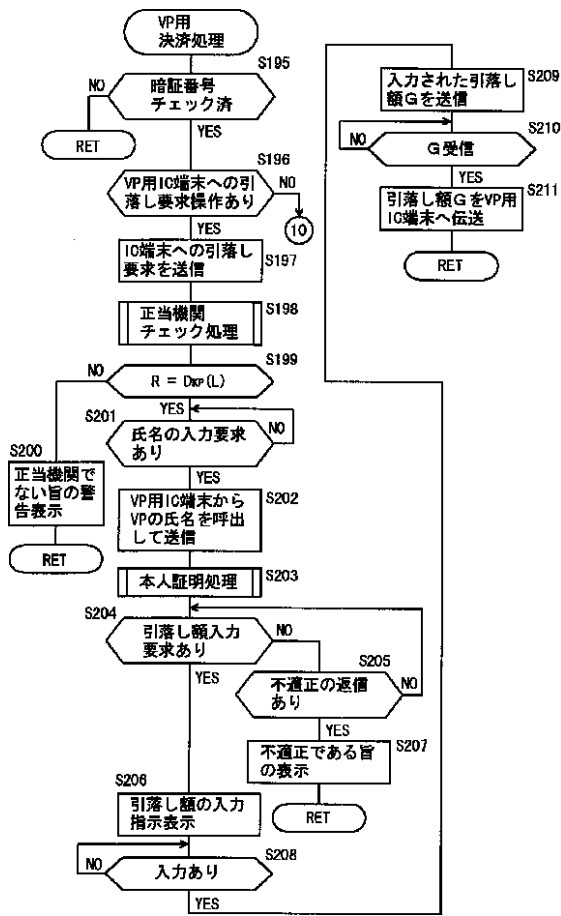
【図14】



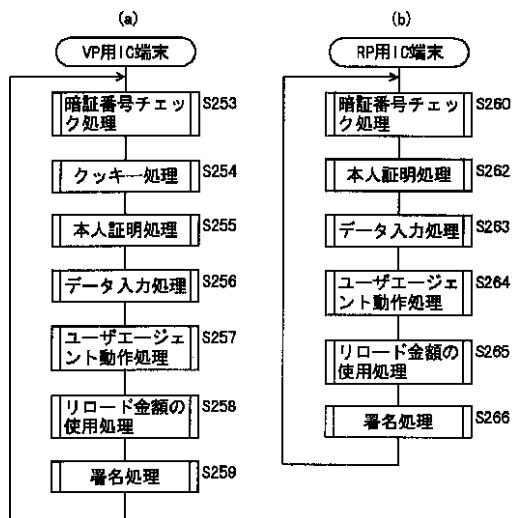
【図15】



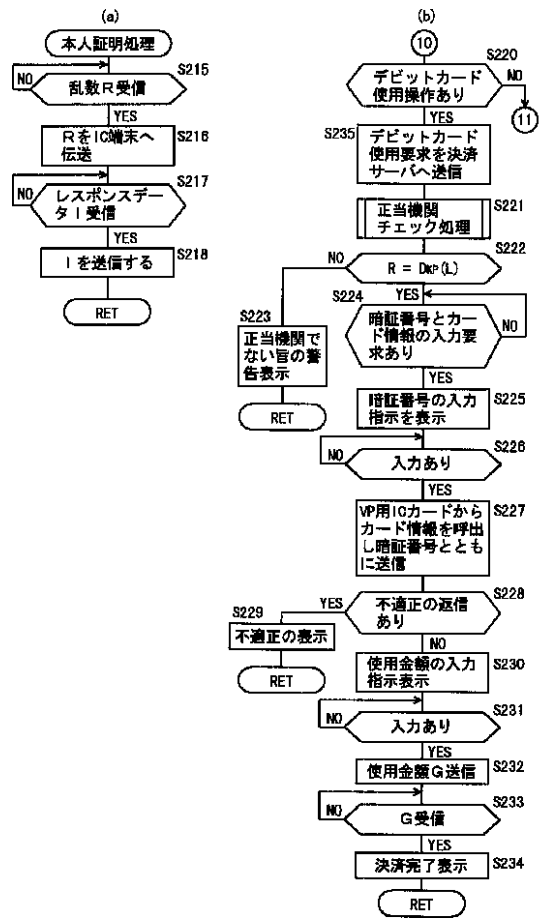
【図16】



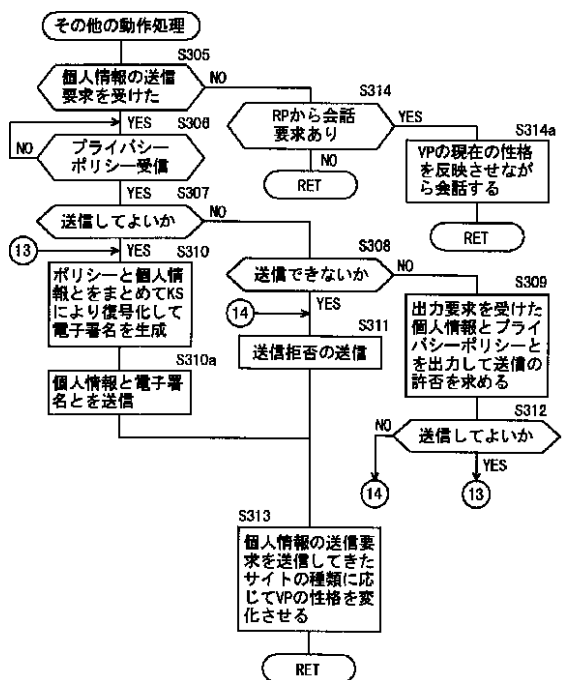
【図19】



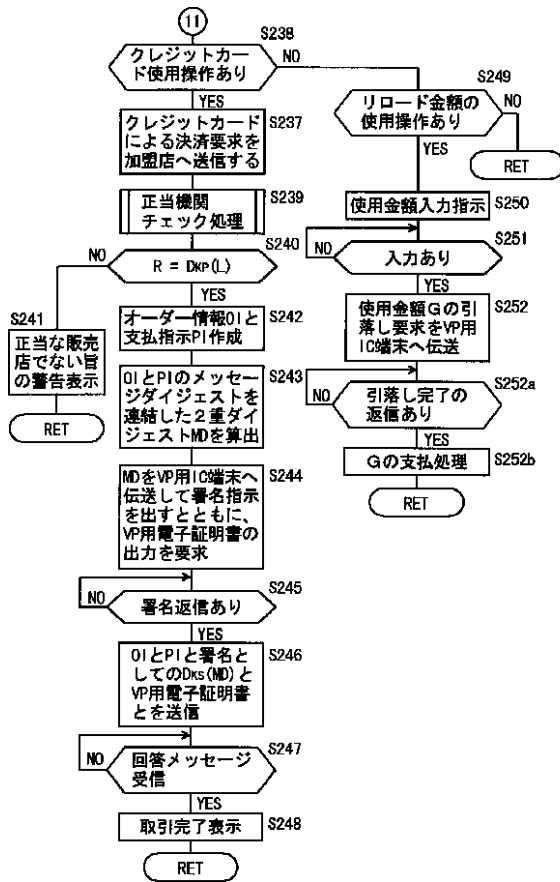
【図17】



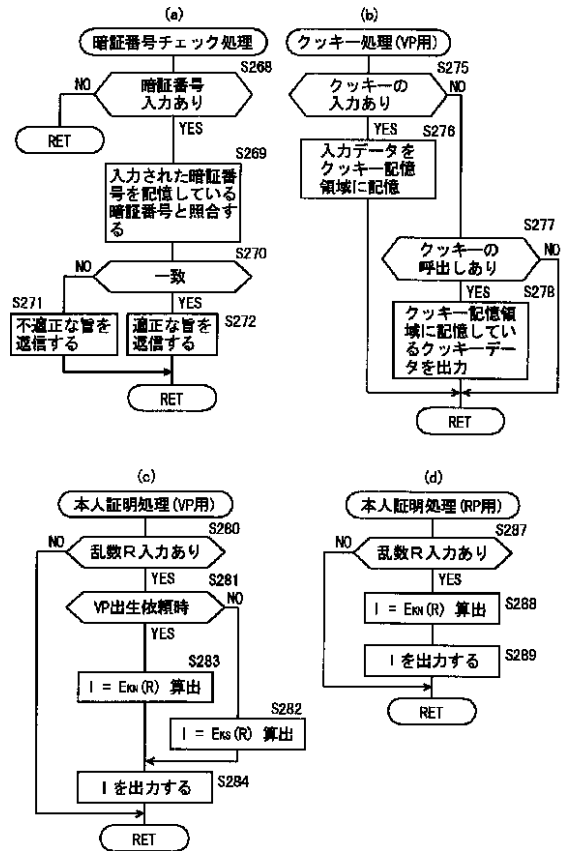
【図22】



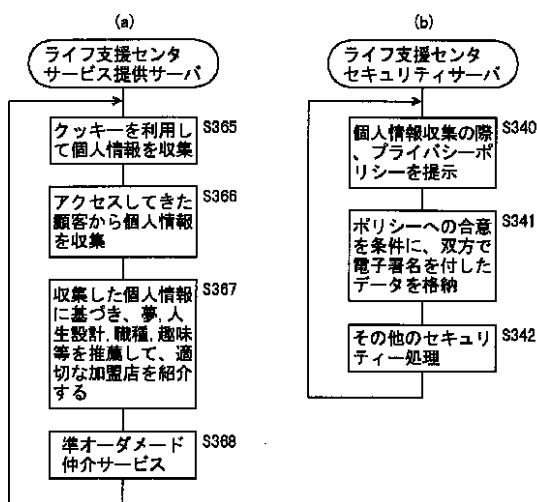
【図18】



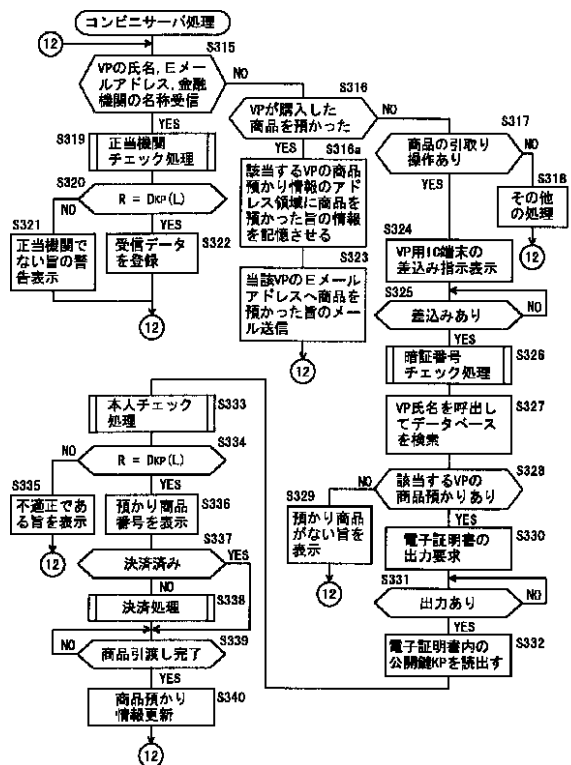
【図20】



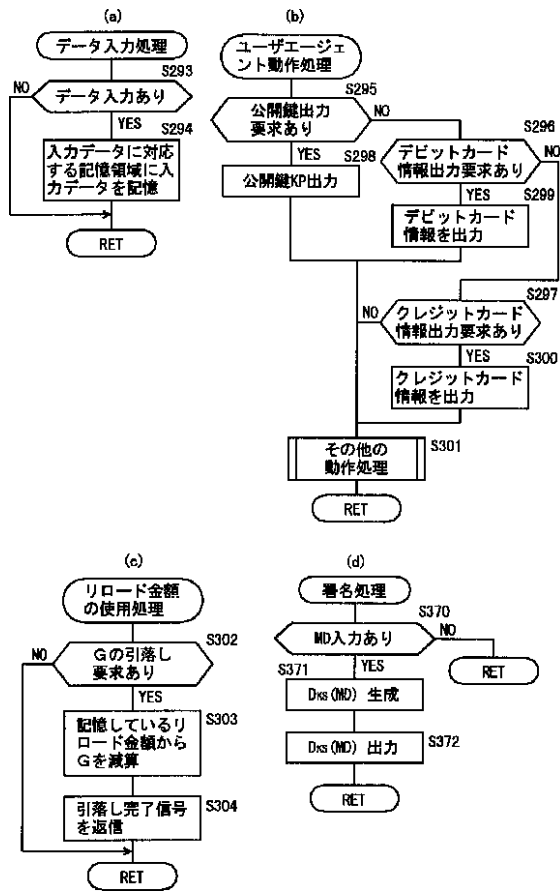
【図25】



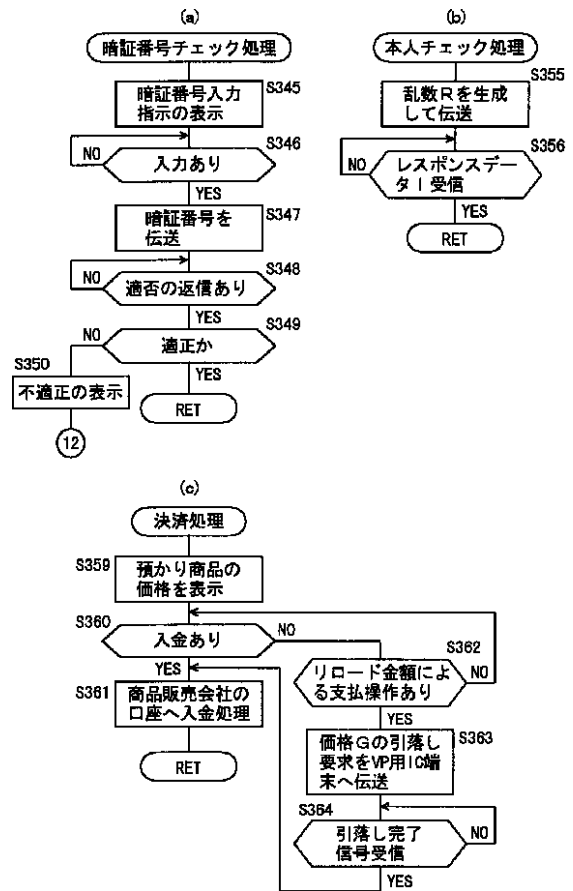
【図23】



【図21】



【図24】



フロントページの続き

(51) Int.Cl. ⁷	識別記号	F I	テマコード ⁸ (参考)
G 0 6 F 17/60	4 0 4	G 0 6 F 17/60	4 0 4
	5 1 2		5 1 2
12/14	3 2 0	12/14	3 2 0 A

(72)発明者 藤井 幹雄
 神奈川県横浜市青葉区美しが丘5丁目35番地の2 株式会社ローレルインテリジェントシステムズ内

(72)発明者 塚本 豊
 神奈川県横浜市青葉区美しが丘5丁目35番地の2 株式会社ローレルインテリジェントシステムズ内
 Fターム(参考) 5B017 AA03 BB00 CA16
 5B049 AA06 BB11 BB46 CC05 FF01
 GG00
 5B055 CB10 CC00