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

特許第5142237号
(P5142237)

(45)発行日　平成25年2月13日(2013.2.13)　(24)登録日　平成24年11月30日(2012.11.30)

(51)Int.Cl.		F I		
G06Q 50/26	(2012.01)	G06F	17/60	140
G06Q 40/02	(2012.01)	G06F	17/60	210
G06Q 30/06	(2012.01)	G06F	17/60	310E
G06Q 20/24	(2012.01)	G06F	17/60	402
G06Q 20/26	(2012.01)	G06F	17/60	404

請求項の数 23　(全 56 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)
(65)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)
審査請求日　平成19年9月4日 (2007.9.4)
審判番号　不服2011-6226 (P2011-6226/J1)
審判請求日　平成23年3月22日 (2011.3.22)

(73)特許権者　593187342
塚本　豊
京都府京都市下京区松原通東洞院東入本燈籠町１１番地　デリード烏丸東５０４号室
(74)代理人　110001195
特許業務法人深見特許事務所
(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
(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

最終頁に続く

(54)【発明の名称】個人情報保護システム、処理装置および記録媒体

(57)【特許請求の範囲】
【請求項１】
ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる前記仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、
前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務のある所定機関において登録し、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出し可能に登録する登録処理手段と、
前記ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当

該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信し、かつ、前記ユーザが前記実在人物としてサイトにアクセスする際に、当該サイトから前記第２識別データが以前送信されてきていたとしても当該第２識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第１識別データが以前送信されてきていた場合には当該第１識別データを当該サイトへ送信する送信制御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システム。

【請求項３】

ネットワークに接続された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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、

前記実在人物用の電子証明書とは異なる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、

前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務のある所定機関において登録する処理を行ない、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出し可能に登録するための登録処理手段とを含み、

前記電子証明書発行処理手段は、前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとが前記所定機関に登録されていることを条件として、電子証明書の発行処理を行なうことを特徴とする、個人情報保護システム。

【請求項４】

前記電子証明書は、前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて登録している守秘義務のある所定機関により発行され、前記仮想人物が当該所定機関において登録されていることの証明に用いられるものである、請求項３に記載の個人情報保護システム。

【請求項５】

前記実在人物が前記仮想人物としてネットワーク上で行動した際に購入した商品の配達先の住所を、前記実在人物とは異なる住所であって現実世界に現存する場所であって前記実在人物が商品を引き取りに行く場所の住所に設定するための処理を行なう住所設定手段をさらに含むことを特徴とする、請求項１～請求項４のいずれかに記載の個人情報保護システム。

【請求項６】

前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段をさらに含むことを特徴とする、請求項５に記載の個人情報保護システム。

【請求項７】

前記仮想人物としてネットワーク上で行動した際に購入した商品の配達先の住所は、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５または請求項６に記載の個人情報保護システム。

【請求項８】
ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、
前記実在人物のクレジット番号とは異なる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９】
ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、
前記実在人物の銀行口座とは異なる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１０】
ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、
前記ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイト

にアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信し、かつ、前記ユーザが前記実在人物としてサイトにアクセスする際に、当該サイトから前記第２識別データが以前送信されてきていたとしても当該第２識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第１識別データが以前送信されてきていた場合には当該第１識別データを当該サイトへ送信する送信制御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１１】

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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記実在人物がネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための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付けられたことを条件として、前記仮想人物用特定データを生成する仮想人物用特定データ生成手段と、

前記実在人物の電子メールアドレスとは異なる前記仮想人物用の電子メールアドレスを設定するメールアドレス設定手段と、

前記仮想人物用特定データ生成手段により生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務を守りながら記憶させるための処理を行ない、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出すことができる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１２】

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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、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、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするために生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データと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い、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出し可能に登録するための登録処理手段と、

前記実在人物の電子証明書を用いて当該実在人物の本人認証を行う本人認証手段と、

前記実在人物用の電子証明書とは異な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、前記本人認証手段による実在人物の本人認証が行われ、かつ、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処理を行なうことを特徴とする、処理装置。

【請求項１３】

ネットワーク上での個人情報を保護するための個人情報保護システムであって、

現実世界での実在人物を特定するための実在人物用特定データと、該実在人物用特定データは異なる仮想人物を特定するための仮想人物用特定データとを、守秘義務のある所定機関において対応付けて登録する登録処理手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段とを含み、
前記登録処理手段は、１人の実在人物に対して複数種類の仮想人物用特定データを対応付けて登録し、
前記提示手段は、前記実在人物であるユーザが前記複数種類の仮想人物用特定データを使分けて使用できるように該複数種類の仮想人物用特定データを選択的に提示する、個人情報保護システム。
【請求項１４】
前記登録処理手段が登録している前記仮想人物用特定データは、当該仮想人物を識別するためのコードを含み、
前記提示手段は、ユーザによる予め設定された規制の範囲内で当該ユーザの個人情報を提示する、請求項１３に記載の個人情報保護システム。
【請求項１５】
前記実在人物が前記仮想人物としてネットワーク上で行動した際に購入した商品の配達先の住所を、前記実在人物とは異なる住所であって現実世界に現存する場所であって前記実在人物が商品を引き取りに行く場所の住所に設定するための処理を行なう住所設定手段をさらに含むことを特徴とする、請求項１３または請求項１４に記載の個人情報保護システム。
【請求項１６】
前記仮想人物としてネットワーク上で行動した際に購入した商品の配達先の住所は、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１５に記載の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を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、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、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して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、前記実在人物とは異なる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を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、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、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して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、前記実在人物とは異なる銀行口座内の資金を決済に用いるために引落す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１９】
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を特定するための実在人物用特定データとは異なるデータであってユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための要求操作があったか否かを判定する要求判定手段と、
該要求判定手段により要求があった旨の判定がなされた場合に、前記仮想人物用特定データの生成要求を所定機関に送信するための処理を行なう生成要求送信手段と、
前記仮想人物用特定データの生成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用特定データの生成に必要となる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、
ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信する送信制御手段と、
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２０】
ユーザに所持されて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を特定するための実在人物用特定データとは異なるデータであってユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための要求操作があったか否かを判定する要求判定手段と、
該要求判定手段により要求があった旨の判定がなされた場合に、前記仮想人物用特定データの生成要求を所定機関に送信するための処理を行なう生成要求送信手段と、
前記仮想人物用特定データの生成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用特定データの生成に必要となる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、
ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信する送信制御手段とを含む、処理装置。
【請求項２１】
ネットワークに接続された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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、
前記実在人物用の電子証明書とは異なる前記仮想人物用の電子証明書を発行するための電子証明書発行手段と、
前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務のある所定機関において登録し、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出すことができるための登録手段とを含み、
前記電子証明書発行手段では、前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとが前記所定機関に登録されていることを条件として、電子証明書の発行が行なわれることを特徴とする、個人情報保護システム。

【請求項２２】
ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、
前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務のある所定機関において登録し、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出し可能に登録する登録処理手段と、
前記ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信する送信制御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２３】
ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動

できるようにするための仮想人物用特定データ生成手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、
前記ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信する送信制御手段とを含むことを特徴とする、個人情報保護システム。
【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を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。
【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。
【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い、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、次回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。

【００１７】

【課題を解決するための手段】

請求項１に記載の本発明は、ネットワークに接続された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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる前記仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、

前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務のある所定機関において登録し、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出し可能に登録する登録処理手段と、

前記ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信し、かつ、前記ユーザが前記実在人物としてサイトにアクセスする際に、当該サイトから前記第２識別データが以前送信されてきていたとしても当該第２識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第１識別データが以前送信されてきていた場合には当該第１識別データを当該サイトへ送信する送信制御手段とを含むことを特徴とする。

【００１８】

請求項２に記載の本発明は、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３に記載の本発明は、ネットワークに接続された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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、

前記実在人物用の電子証明書とは異なる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、
前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務のある所定機関において登録する処理を行ない、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出し可能に登録するための登録処理手段とを含み、
前記電子証明書発行処理手段は、前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとが前記所定機関に登録されていることを条件として、電子証明書の発行処理を行なうことを特徴とする。
請求項４に記載の本発明は、請求項３に記載の発明の構成に加えて、前記電子証明書は、前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて登録している守秘義務のある所定機関により発行され、前記仮想人物が当該所定機関において登録されていることの証明に用いられるものである。
【００２０】
請求項５に記載の本発明は、請求項１～請求項４のいずれかに記載の発明の構成に加えて、前記実在人物が前記仮想人物としてネットワーク上で行動した際に購入した商品の配達先の住所を、前記実在人物とは異なる住所であって現実世界に現存する場所であって前記実在人物が商品を引き取りに行く場所の住所に設定するための処理を行なう住所設定手段とをさらに含むことを特徴とする。
請求項６に記載の本発明は、請求項５に記載の発明の構成に加えて、前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段をさらに含むことを特徴とする。
【００２１】
請求項７に記載の本発明は、請求項５または請求項６に記載の発明の構成に加えて、前記仮想人物としてネットワーク上で行動した際に購入した商品の配達先の住所は、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８に記載の本発明は、ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、
前記実在人物のクレジット番号とは異なる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９に記載の本発明は、ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、

前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、

前記実在人物の銀行口座とは異なる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１０に記載の本発明は、ネットワークに接続された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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、

前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、

前記ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信し、かつ、前記ユーザが前記実在人物としてサイトにアクセスする際に、当該サイトから前記第２識別データが以前送信されてきていたとしても当該第２識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第１識別データが以前送信されてきていた場合には当該第１識別データを当該サイトへ送信する送信制御手段とを含むことを特徴とする。

【００２５】

請求項１１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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記実在人物がネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための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付けられたことを条件として、前記仮想人物用特定データを生成する仮想人物用特定データ生成手段と、

前記実在人物の電子メールアドレスとは異なる前記仮想人物用の電子メールアドレスを

設定するメールアドレス設定手段と、
前記仮想人物用特定データ生成手段により生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務を守りながら記憶させるための処理を行ない、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出すことができる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１２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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、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、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするために生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データと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い、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出し可能に登録するための登録処理手段と、
前記実在人物の電子証明書を用いて当該実在人物の本人認証を行う本人認証手段と、
前記実在人物用の電子証明書とは異な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、前記本人認証手段による実在人物の本人認証が行われ、かつ、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処理を行なうことを特徴とする。
請求項１３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個人情報保護システムであって、
現実世界での実在人物を特定するための実在人物用特定データと、該実在人物用特定データは異なる仮想人物を特定するための仮想人物用特定データとを、守秘義務のある所定機関において対応付けて登録する登録処理手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段とを含み、
前記登録処理手段は、１人の実在人物に対して複数種類の仮想人物用特定データを対応付けて登録し、
前記提示手段は、前記実在人物であるユーザが前記複数種類の仮想人物用特定データを使分けて使用できるように該複数種類の仮想人物用特定データを選択的に提示する。
請求項１４に記載の本発明は、請求項１３に記載の発明の構成に加えて、前記登録処理手段が登録している前記仮想人物用特定データは、当該仮想人物を識別するためのコードを含み、
前記提示手段は、ユーザによる予め設定された規制の範囲内で当該ユーザの個人情報を提示する。
【００２７】
請求項１５に記載の本発明は、請求項１３または請求項１４に記載の発明の構成に加えて、前記実在人物が前記仮想人物としてネットワーク上で行動した際に購入した商品の配達先の住所を、前記実在人物とは異なる住所であって現実世界に現存する場所であって前記実在人物が商品を引き取りに行く場所の住所に設定するための処理を行なう住所設定手段をさらに含むことを特徴とする。

請求項１６に記載の本発明は、請求項１５に記載の発明の構成に加えて、前記仮想人物としてネットワーク上で行動した際に購入した商品の配達先の住所は、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１７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を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、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、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して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、前記実在人物とは異なる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を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、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、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して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、前記実在人物とは異なる銀行口座内の資金を決済に用いるために引落す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。

【００３０】

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を特定するための実在人物用特定データとは異なるデータであってユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための要求操作があったか否かを判定する要求判定手段と、

該要求判定手段により要求があった旨の判定がなされた場合に、前記仮想人物用特定データの生成要求を所定機関に送信するための処理を行なう生成要求送信手段と、

前記仮想人物用特定データの生成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用特定データの生成に必要となる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、

ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信する送信

制御手段と、
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。
請求項２０に記載の本発明は、ユーザに所持されて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を特定するための実在人物用特定データとは異なるデータであってユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための要求操作があったか否かを判定する要求判定手段と、
該要求判定手段により要求があった旨の判定がなされた場合に、前記仮想人物用特定データの生成要求を所定機関に送信するための処理を行なう生成要求送信手段と、
前記仮想人物用特定データの生成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用特定データの生成に必要となる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、
ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信する送信制御手段とを含む。
【００３５】
請求項２１に記載の本発明は、ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、
前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、
前記実在人物用の電子証明書とは異なる前記仮想人物用の電子証明書を発行するための電子証明書発行手段と、
前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務のある所定機関において登録し、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出すことができるための登録手段とを含み、
前記電子証明書発行手段では、前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとが前記所定機関に登録されていることを条件として、電子証明書の発行が行なわれることを特徴とする。
請求項２２に記載の本発明は、ネットワークに接続された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、
ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、
該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在

人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、

前記生成された前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとを対応付けて守秘義務のある所定機関において登録し、前記実在人物が仮想人物としてネットワーク上で行動し不正行為を行なった場合に、当該仮想人物に対応する前記実在人物を割出し可能に登録する登録処理手段と、

前記ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信する送信制御手段とを含むことを特徴とする。

請求項２３に記載の本発明は、ネットワークに接続された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、

ユーザが匿名を用いて仮想人物としてネットワーク上で行動する際の仮想人物生成依頼をユーザの端末から受信する依頼受信手段と、

該依頼受信手段が依頼を受信した場合に、現実世界での実在人物を特定するための実在人物用特定データとは異なる仮想人物を特定するための仮想人物用特定データを生成し、前記ユーザがネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示して仮想人物として行動できるようにするための仮想人物用特定データ生成手段と、

前記実在人物であるユーザが前記仮想人物としてネットワーク上で行動する際に、ユーザの個人情報の要求に応じて、前記実在人物用特定データの代わりに前記仮想人物用特定データを提示する提示手段と、

前記ユーザの端末からユーザが前記実在人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第１識別データと前記仮想人物としてサイトにアクセスした際に当該サイト側がユーザを識別するために送信してきた第２識別データとを区別して、前記識別データを記憶し、前記ユーザが前記仮想人物としてサイトにアクセスする際に、当該サイトから前記第１識別データが以前送信されてきていたとしても当該第１識別データの当該サイトへの送信を阻止するとともに、当該サイトから前記第２識別データが以前送信されてきていた場合には当該第２識別データを当該サイトへ送信する送信制御手段とを含むことを特徴とする。

【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、サプライア群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。サプライア群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、たとえばＳＥＴ（Secure Electronic Transaction）により決済を行なう場合のイシュア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、ユーザの個人情報を収集し、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となる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る。

【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に対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３

０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っ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の返信があっ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っ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、返信があった段階で制御が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っ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っ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要求があったか否かの判断がなされ、ない場合にはＳ４１へ進み、決済要求があっ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に進み、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に比べてより一層一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Ｓ１３１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、Ｓ１３２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の判断がなされ、ある場合にＳ１３３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Ｓ１３２によりＮＯの判断がなされてＳ１３４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Ｓ１３７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Ｓ１３５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、Ｓ１３６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Ｓ１０１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。Ｓ１４０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Ｓ１４１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Ｓ１４１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Ｓ１４２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Ｓ１４３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Ｓ１６０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、Ｓ９０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Ｓ１６１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Ｓ９２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Ｓ１６３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Ｓ１４４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Ｓ１４６へ進むが、他人が金融機関７になしすましている場合には、Ｓ１４４によりＮＯの判断がなされ、Ｓ１４５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、Ｓ１４６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（Ｓ２参照）、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、Ｓ１４６によりＹＥＳの判断がなされて制御がＳ１４７へ進む。

【０１００】

Ｓ１４７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（Ｓ１４８）。入力があった段階でＳ１４９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Ｓ１５０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入力操作を行なえば、Ｓ１７７によりＹＥＳの判断がなされて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からクレジットカードの会員である旨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を一部引落してＶＰ用ＩＣ端末へリロードする操作を行なえば、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信されてくれば、Ｓ２２８によりＹＥＳの判断がなされてＳ２２９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Ｓ２３０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、Ｓ２３１によりＹＥＳの判断がなされてＳ２３２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（Ｓ７４）。

【０１３１】

その結果、Ｓ２３３によりＹＥＳの判断がなされてＳ２３４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】

Ｓ２２０によりＮＯの判断がなされた場合には、制御がＳ２３８へ進む。Ｓ２３８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Ｓ２３７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Ｓ２３９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て、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Ｓ２４０へ進み、$R = D_{KP}(L)$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、Ｓ２４０によりＮＯの判断がなされて、Ｓ２４１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、Ｓ２４２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Ｓ２４３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Ｓ２４４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、Ｓ２４５によりＹＥＳの判断がなされてＳ２４６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、Ｓ２４７によりＹＥＳの判断がなされてＳ２４８へ進み、取引が完了した旨の表示が行なわれる。

【０１３５】

Ｓ２３８によりＮＯの判断がなされた場合にＳ２４９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なえば、制御がＳ２５０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、Ｓ２５１によりＹＥＳの判断がなされてＳ２５２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、Ｓ２５２ａによりＹＥＳの判断がなされてＳ２５２ｂ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、Ｓ２５３により、暗証番号チェック処理を行なう。次にＳ２５４へ進み、クッキー処理を行なう。次にＳ２５５へ進み、本人証明処理を行なう。次にＳ２５６へ進み、データ入力処理を行なう。次にＳ２５７へ進み、ユーザエージェント動作処理を行なう。次にＳ２５８へ進み、リロード金額の使用処理を行なう。次にＳ２５９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、Ｓ２６０により、暗証番号チェック処理を行ない、Ｓ２６２により、本人証明処理を行ない、Ｓ２６３により、データ入力処理を行ない、Ｓ２６４により、ユーザエージェント動作処理を行ない、Ｓ２６５により、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こ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否かの判断がなされ、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に基づいて後述する。
【０１５０】
図２１（ｃ）は、Ｓ２５８，Ｓ２６５に示されたリ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_{KS}（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繁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繁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。
【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。

【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許否を求める処理がなされる。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。
【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）と会話がしたい場合には、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を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。
【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（Ｓ１８参照）、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。
【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内の公開鍵ＫＰを読出し、Ｓ３３３により、本人チェック処理がなされる。

【０１６３】

次にＳ３３４へ進み、$R = D_{KP}(I)$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、商品の引渡しが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。

【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。

【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の引落し要求を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から引落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、引落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、技術と法律を生かせ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、準オーダーメード仲介サービスが行なわれる。この準オーダーメー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プライヤ１にオーダーメー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プライヤが作成するという完全オーダーメード方式に比べて、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等が、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かできる。

【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って初めて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Ｉ

Ｃ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っ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、Secure Electronic 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。

【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っ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）の住所であっ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。

【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な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）との会話を実現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，Ｓ５６，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）。

【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。

【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す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。

【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（Ｓ３２２）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落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となる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ているとともに（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】
　仮想人物用特定データ生成手段により仮想人物用特定データが生成され、ユーザがネットワーク上で行動する場合には実在人物用特定データの代わりに仮想人物用特定データを提示してその仮想人物と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、前記仮想人物用特定データと該仮想人物用特定データに対応する前記実在人物用特定データとが対応付けられて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。
【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ようにした場合には、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ＶＰ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】　ＶＰ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。

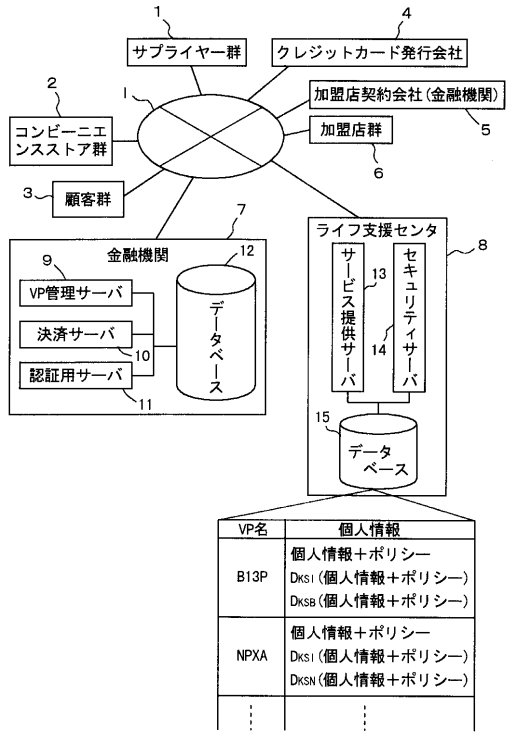
【図１９】　（ａ）はＶＰ用ＩＣ端末の処理を示すフローチャートであり、（ｂ）はＲＰ用ＩＣ端末の処理を示すフローチャートである。

【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。

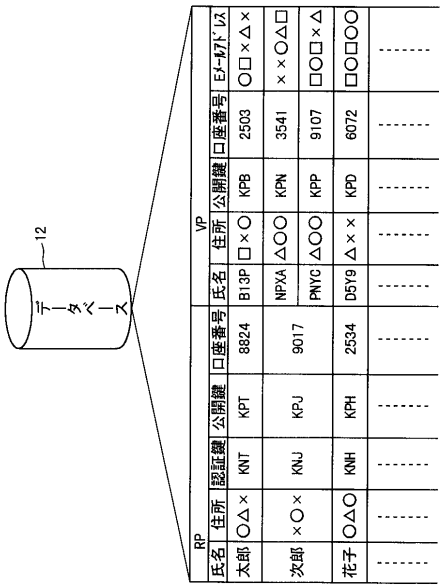
【図２１】　（ａ）はデータ入力処理のサブルーチンを示すフローチャートであり、（ｂ）はユーザエージェント動作処理のサブルーチンを示すフローチャートであり、（ｃ）はリロード金額の使用処理を示すフローチャートであり、（ｄ）は署名処理のサブルーチンを示すフローチャートである。

【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。

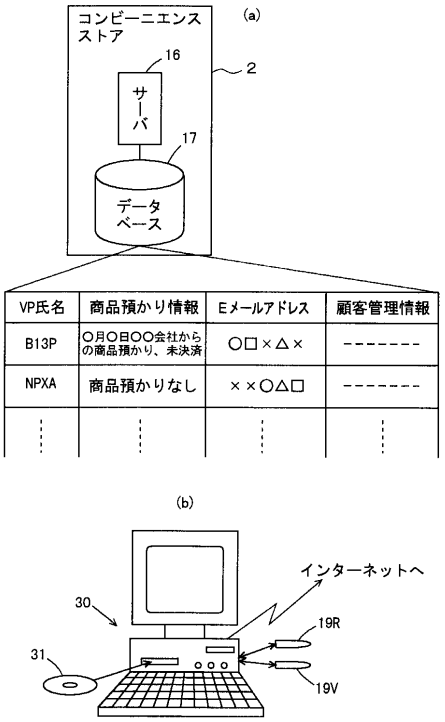
【図１】



【図２】



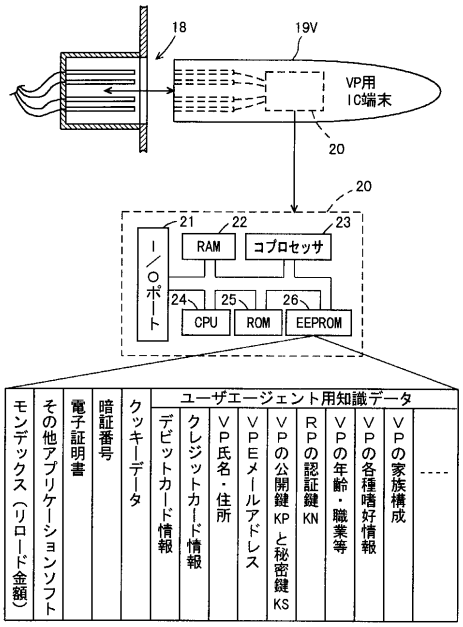
【図３】


コンビーニエンスストア
(a)
16
サーバ
2
17
データベース
VP氏名
商品預かり情報
Eメールアドレス
顧客管理情報
B13P
○月○日○○会社からの商品預かり、未決済
○□×△×

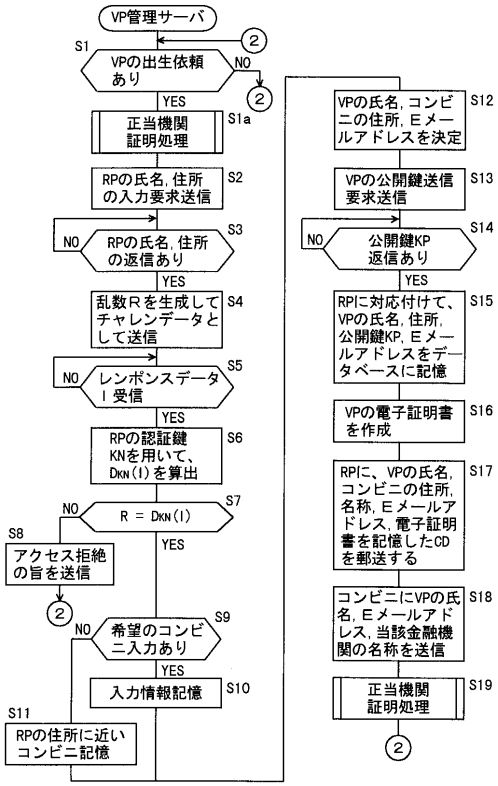
NPXA
商品預かりなし
××○△□

(b)
インターネットへ
30
19R
31
19V

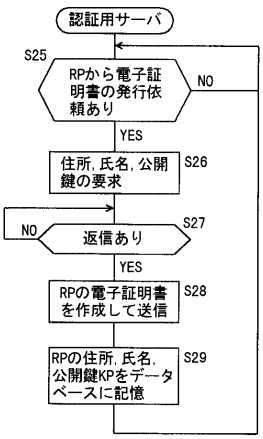
【図４】


18
19V
VP用IC端末
20
20
21
22
23
I/Oポート
RAM
コプロセッサ
24
25
26
CPU
ROM
EEPROM
ユーザエージェント用知識データ
モンデックス（リロード金額）
その他アプリケーションソフト
電子証明書
暗証番号
クッキーデータ
デビットカード情報
クレジットカード情報
VP氏名・住所
VPE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

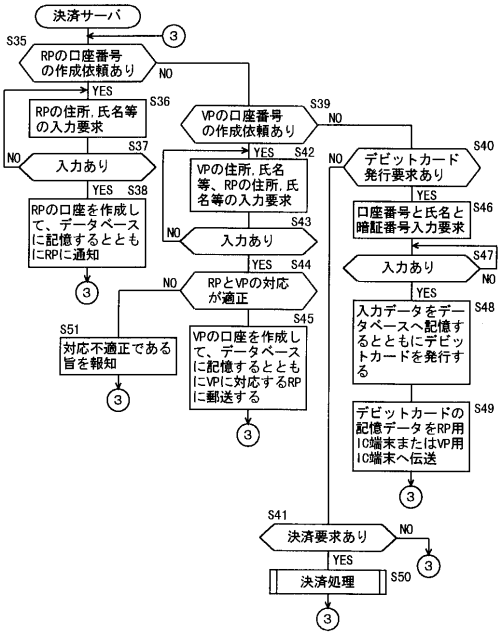
【図５】


VP管理サーバ
S1
VPの出生依頼あり
NO
YES
S1a
正当機関証明処理
S2
RPの氏名,住所の入力要求送信
S3
NO
RPの氏名,住所の返信あり
YES
S4
乱数Rを生成してチャレンジデータとして送信
S5
NO
レンポンスデータI受信
YES
S6
RPの認証鍵KNを用いて、DKN(I)を算出
S7
NO
R = DKN(I)
YES
S8
アクセス拒絶の旨を送信
S9
NO
希望のコンビニ入力あり
YES
S10
入力情報記憶
S11
RPの住所に近いコンビニ記憶
S12
VPの氏名,コンビニの住所,Eメールアドレスを決定
S13
VPの公開鍵送信要求送信
S14
NO
公開鍵KP返信あり
YES
S15
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に記憶
S16
VPの電子証明書を作成
S17
RPに、VPの氏名,コンビニの住所,名称,Eメールアドレス,電子証明書を記憶したCDを郵送する
S18
コンビニにVPの氏名,Eメールアドレス,当該金融機関の名称を送信
S19
正当機関証明処理

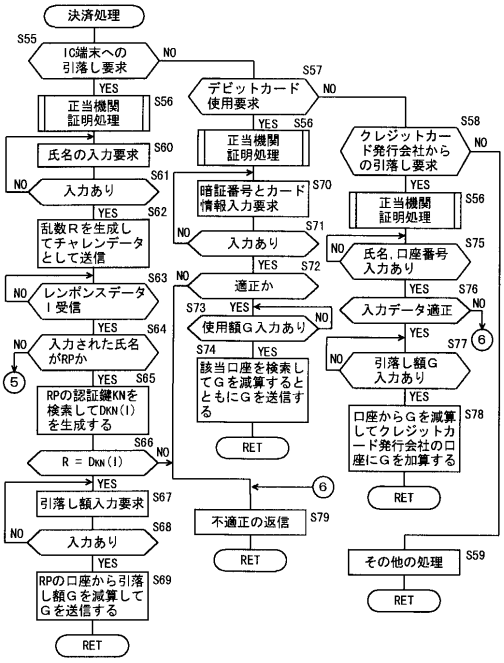
【図６】


認証用サーバ
S25
RPから電子証明書の発行依頼あり
NO
YES
S26
住所,氏名,公開鍵の要求
S27
NO
返信あり
YES
S28
RPの電子証明書を作成して送信
S29
RPの住所,氏名,公開鍵KPをデータベースに記憶

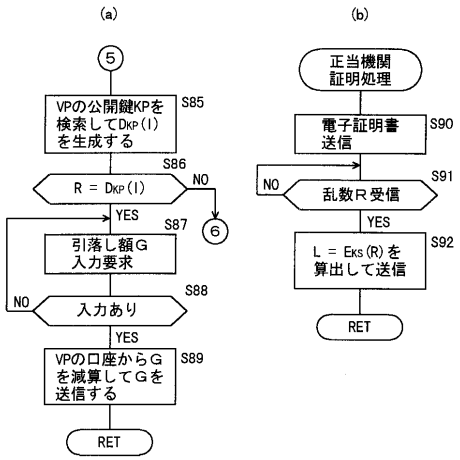
【図７】


決済サーバ
RPの口座番号の作成依頼あり
RPの住所,氏名等の入力要求
入力あり
RPの口座を作成して、データベースに記憶するとともにRPに通知
VPの口座番号の作成依頼あり
VPの住所,氏名等、RPの住所,氏名等の入力要求
入力あり
RPとVPの対応が適正
対応不適正である旨を報知
VPの口座を作成して、データベースに記憶するとともにVPに対応するRPに郵送する
デビットカード発行要求あり
口座番号と氏名と暗証番号入力要求
入力あり
入力データをデータベースへ記憶するとともにデビットカードを発行する
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
決済要求あり
決済処理
S35
S36
S37
S38
S39
S40
S41
S42
S43
S44
S45
S46
S47
S48
S49
S50
S51

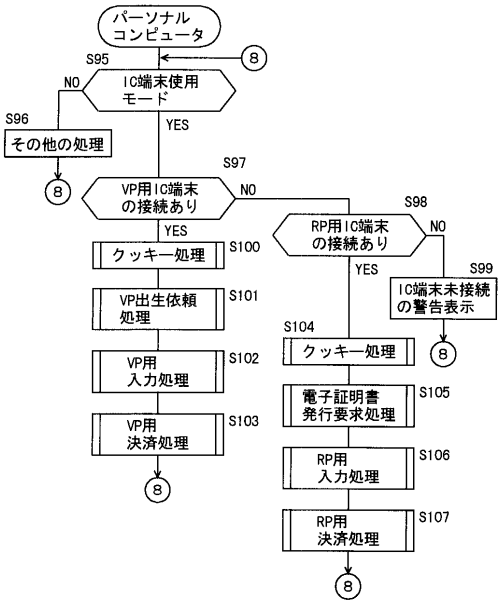
【図８】


決済処理
IC端末への引落し要求
正当機関証明処理
氏名の入力要求
入力あり
乱数Rを生成してチャレンジデータとして送信
レンポンスデータ I 受信
入力された氏名がRPか
RPの認証鍵KNを検索してDKN(I)を生成する
R = DKN(I)
引落し額入力要求
入力あり
RPの口座から引落し額Gを減算してGを送信する
RET
デビットカード使用要求
正当機関証明処理
暗証番号とカード情報入力要求
入力あり
適正か
使用額G入力あり
該当口座を検索してGを減算するとともにGを送信する
RET
不適正の返信
RET
クレジットカード発行会社からの引落し要求
正当機関証明処理
氏名,口座番号入力あり
入力データ適正
引落し額G入力あり
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にGを加算する
RET
その他の処理
RET
S55
S56
S57
S58
S59
S60
S61
S62
S63
S64
S65
S66
S67
S68
S69
S70
S71
S72
S73
S74
S75
S76
S77
S78
S79

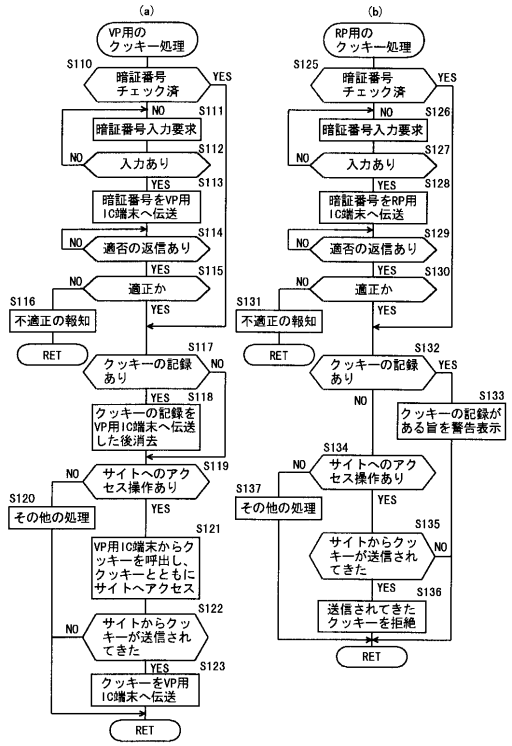
【図９】


(a)
(b)
VPの公開鍵KPを検索してDKP(I)を生成する
R = DKP(I)
引落し額G入力要求
入力あり
VPの口座からGを減算してGを送信する
RET
正当機関証明処理
電子証明書送信
乱数R受信
L = EKS(R)を算出して送信
RET
S85
S86
S87
S88
S89
S90
S91
S92

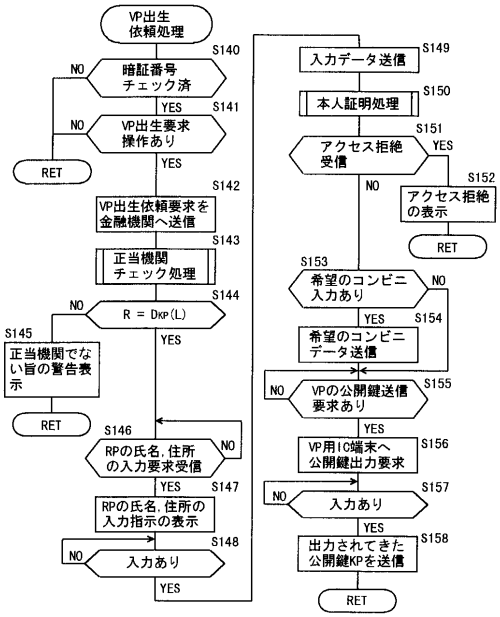
【図１０】


パーソナルコンピュータ
IC端末使用モード
その他の処理
VP用IC端末の接続あり
クッキー処理
VP出生依頼処理
VP用入力処理
VP用決済処理
RP用IC端末の接続あり
IC端末未接続の警告表示
クッキー処理
電子証明書発行要求処理
RP用入力処理
RP用決済処理
S95
S96
S97
S98
S99
S100
S101
S102
S103
S104
S105
S106
S107

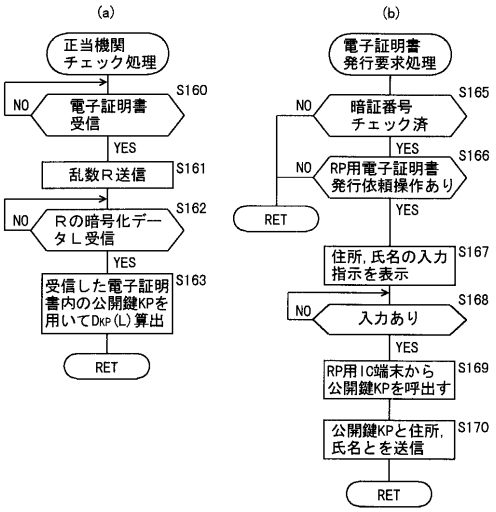
【図１１】



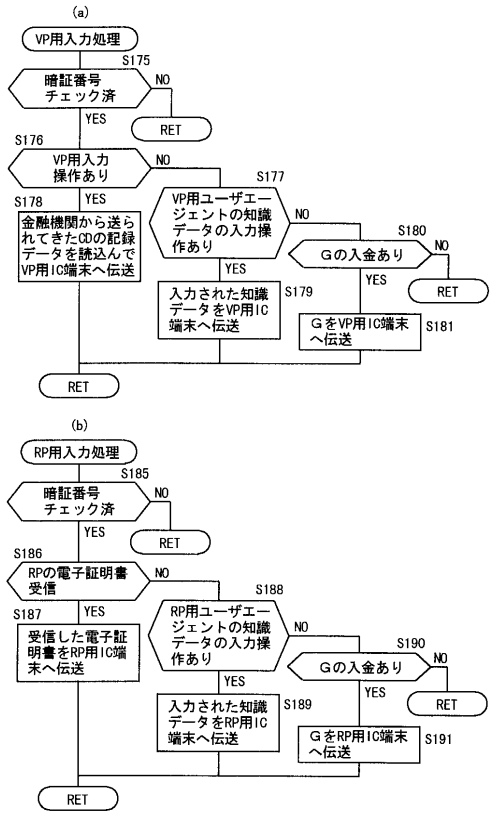
【図１２】



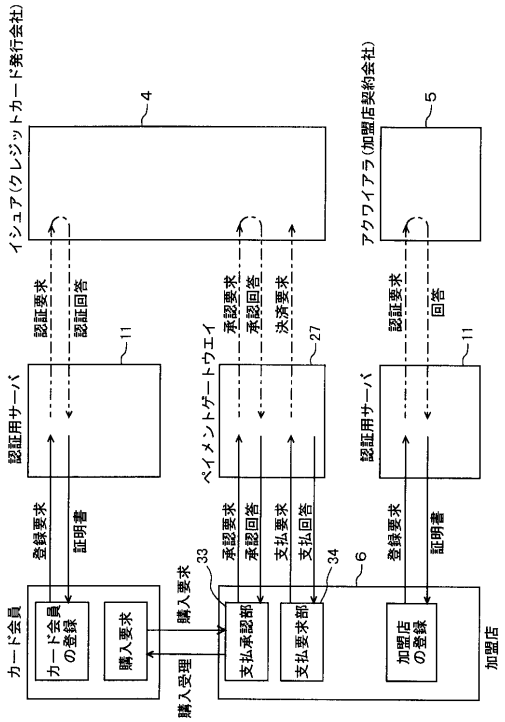
【図１３】



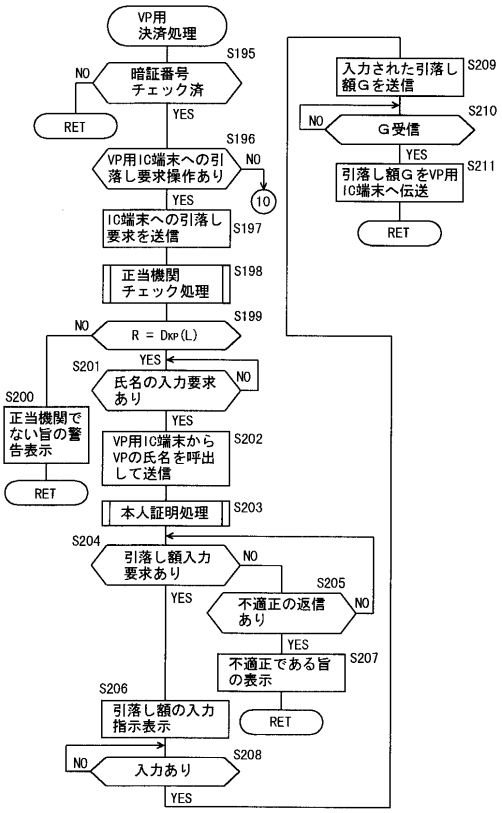
【図１４】



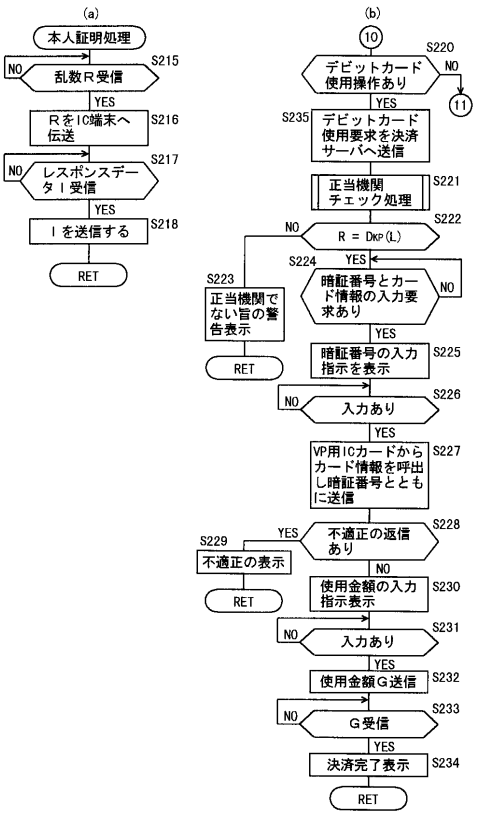
【図１５】



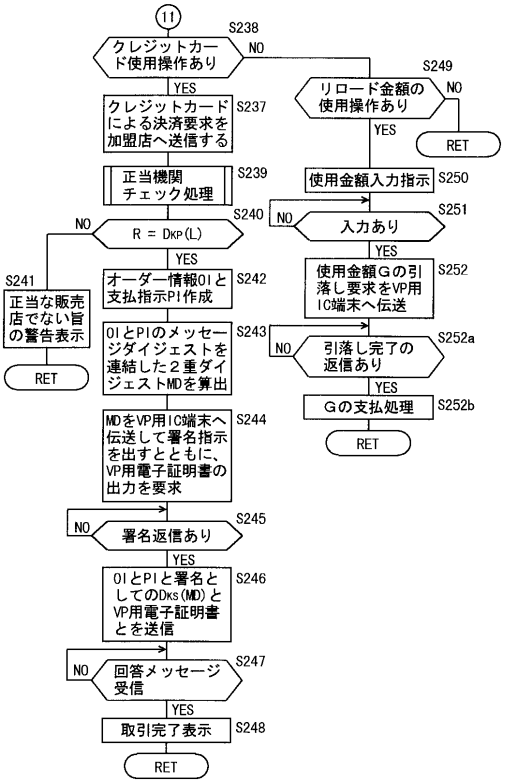
【図１６】



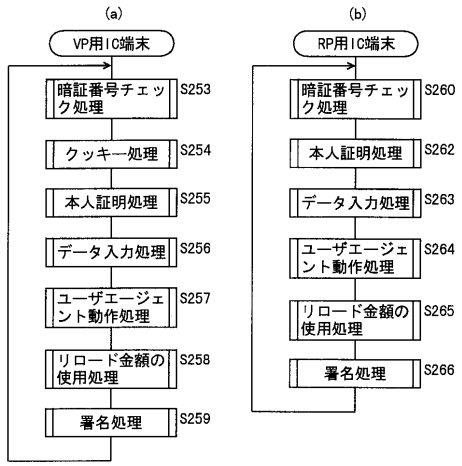
【図１７】



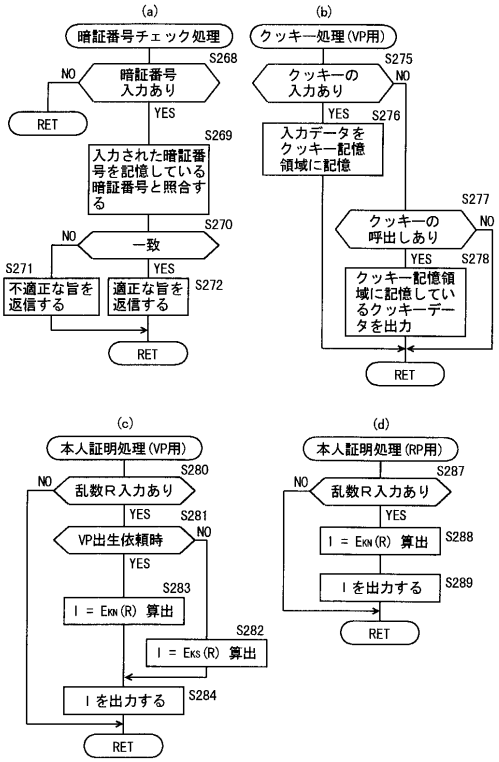
【図１８】



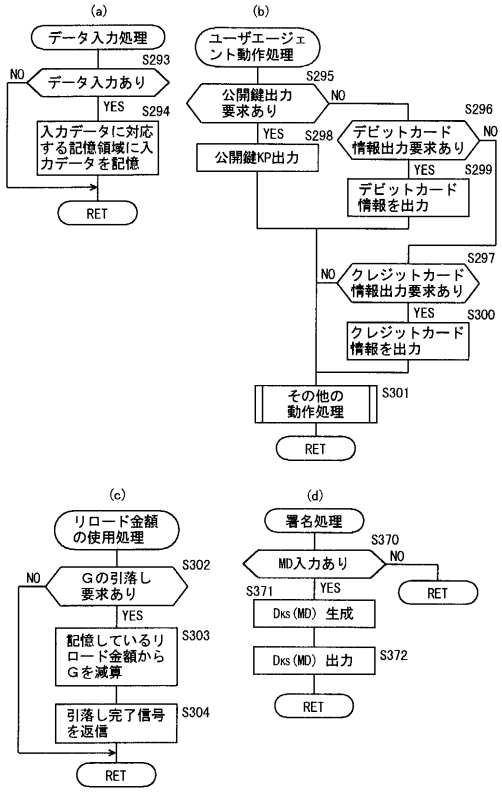
【図１９】



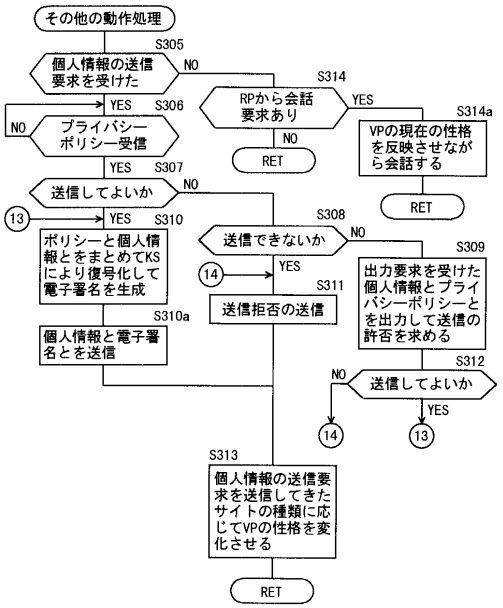
【図２０】



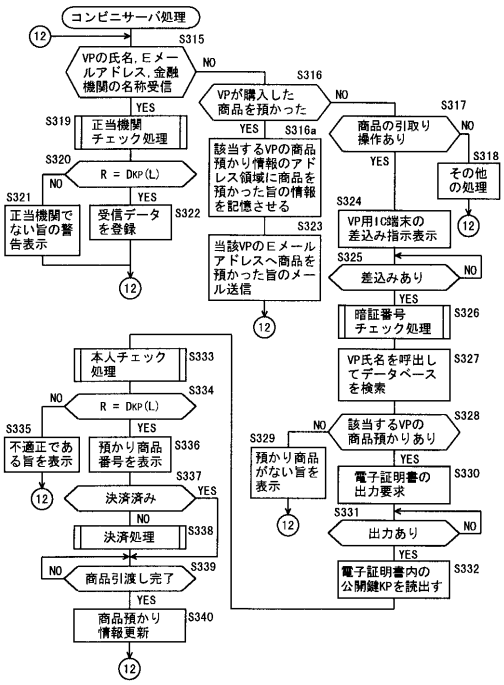
【図２１】



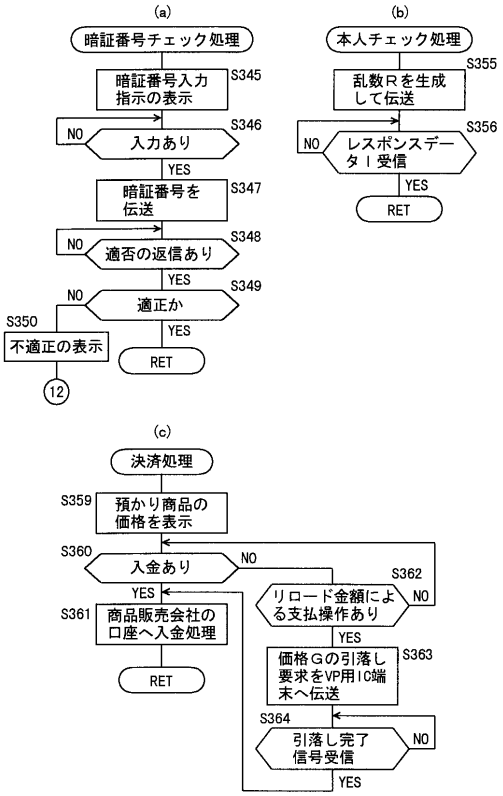
【図２２】



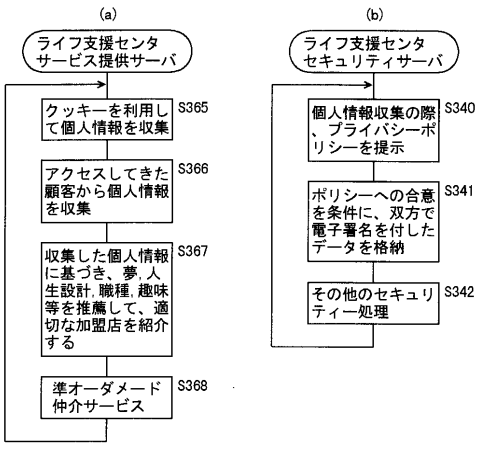
【図２３】


コンビニサーバ処理
12
S315
VPの氏名, Eメールアドレス, 金融機関の名称受信
NO
S316
VPが購入した商品を預かった
NO
S317
商品の引取り操作あり
NO
S318
その他の処理
YES
S319
正当機関チェック処理
S320
R = DKP(L)
NO
S321
正当機関でない旨の警告表示
YES
S322
受信データを登録
YES
S316a
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
S323
当該VPのEメールアドレスへ商品を預かった旨のメール送信
12
S324
VP用IC端末の差込み指示表示
12
S325
差込みあり
NO
YES
S326
暗証番号チェック処理
S327
VP氏名を呼出してデータベースを検索
S328
該当するVPの商品預かりあり
NO
S329
預かり商品がない旨を表示
12
YES
S330
電子証明書の出力要求
S331
出力あり
NO
YES
S332
電子証明書内の公開鍵KPを読出す
S333
本人チェック処理
S334
R = DKP(L)
NO
S335
不適正である旨を表示
YES
S336
預かり商品番号を表示
S337
決済済み
YES
12
NO
S338
決済処理
S339
商品引渡し完了
NO
YES
S340
商品預かり情報更新
12

【図２４】


(a)
暗証番号チェック処理
S345
暗証番号入力指示の表示
S346
NO
入力あり
YES
S347
暗証番号を伝送
S348
NO
適否の返信あり
YES
S349
NO
適正か
YES
S350
不適正の表示
RET
12
(b)
本人チェック処理
S355
乱数Rを生成して伝送
S356
NO
レスポンスデータ！受信
YES
RET
(c)
決済処理
S359
預かり商品の価格を表示
S360
入金あり
NO
YES
S361
商品販売会社の口座へ入金処理
RET
S362
リロード金額による支払操作あり
NO
YES
S363
価格Gの引落し要求をVP用IC端末へ伝送
S364
引落し完了信号受信
NO
YES

【図２５】


(a)
ライフ支援センタ
サービス提供サーバ
S365
クッキーを利用して個人情報を収集
S366
アクセスしてきた顧客から個人情報を収集
S367
収集した個人情報に基づき、夢, 人生設計, 職種, 趣味等を推薦して、適切な加盟店を紹介する
S368
準オーダメード仲介サービス
(b)
ライフ支援センタ
セキュリティサーバ
S340
個人情報収集の際、プライバシーポリシーを提示
S341
ポリシーへの合意を条件に、双方で電子署名を付したデータを格納
S342
その他のセキュリティー処理

フロントページの続き

(51)Int.Cl.		FI		
G06Q 10/00	*(2012.01)*	G06F	17/60	512
G06Q 50/00	*(2012.01)*	G06F	17/60	ZEC

(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

合議体
審判長　清田　健一
審判官　須田　勝巳
審判官　石川　正二

(56)参考文献　特開平１０－０４０２９５（ＪＰ，Ａ）
特開２０００－０５７３７４（ＪＰ，Ａ）
特開２０００－２５１００６（ＪＰ，Ａ）
国際公開第００／１４６４８（WO，Ａ１）
特開平１０－２８５１５３（ＪＰ，Ａ）
特開平０９－１６７２２０（ＪＰ，Ａ）
特開平１１－３０６２６３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06Q10/00-50/00