(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5158662号
(P5158662)
(45)発行日　平成25年3月6日(2013.3.6)　(24)登録日　平成24年12月21日(2012.12.21)

(51)Int.Cl.　F I
G06Q 50/26 (2012.01)　G06F 17/60 １４０
G06F 13/00 (2006.01)　G06F 13/00 ６１０Q

請求項の数 10　(全 75 頁)

(21)出願番号　特願2001-258259(P2001-258259)
(22)出願日　平成13年8月28日(2001.8.28)
(65)公開番号　特開2003-67524(P2003-67524A)
(43)公開日　平成15年3月7日(2003.3.7)
審査請求日　平成20年8月27日(2008.8.27)
審判番号　不服2011-20937(P2011-20937/J1)
審判請求日　平成23年9月28日(2011.9.28)

(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　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

最終頁に続く

(54)【発明の名称】個人情報保護装置

(57)【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装置であって、
現実世界での実在人物を特定して識別するための実在人物用識別データとは異なる仮想人物を識別するための仮想人物用識別データを生成する仮想人物用識別データ生成手段と、
該仮想人物用識別データ生成手段により生成された前記仮想人物用識別データと前記実在人物用識別データ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してウェブサイトにアクセスする際に、ユーザを特定する情報の要求に応じて、当該ユーザに対応する前記仮想人物用識別データを当該ウェブサイトの業者に提供する提供手段と、
複数の前記ユーザの各々の行動履歴情報を各ユーザの個人情報として記憶する個人情報記憶手段と、
該個人情報記憶手段に記憶されている個人情報を提供するための制御を行なう個人情報提供制御手段とを含み、
前記仮想人物用識別データ生成手段が生成する前記仮想人物用識別データは、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の当該仮想人物を識別するための識別データであって、前記ウェブサイトの業者が前記実在人物を特定できな

い識別データであり、
前記仮想人物用識別データ生成手段は、１人のユーザが第１ウェブサイトに対しアクセスする毎に繰り返して用いる当該第１ウェブサイト専用の第１の仮想人物用識別データを生成するとともに、当該１人のユーザが第２ウェブサイトに対しアクセスする毎に繰り返して用いる当該第２ウェブサイト専用の第２の仮想人物用識別データを生成し、
前記登録手段は、各ユーザ毎に、前記実在人物用識別データと前記第１の仮想人物用識別データと前記第２の仮想人物用識別データとの対応関係を特定可能な情報を登録し、
前記提供手段は、前記仮想人物用識別データ生成手段により生成された前記第１の仮想人物用識別データを前記第１ウェブサイトの業者に提供するとともに、前記仮想人物用識別データ生成手段により生成された前記第２の仮想人物用識別データを前記第２ウェブサイトの業者に提供することにより、前記仮想人物用識別データを使分けて提供し、
前記個人情報提供制御手段は、
ユーザの個人情報を前記第１ウェブサイトに提供する際に、当該個人情報の前記第１ウェブサイトの業者への提供を許諾してよいか否かを判定する許諾判定手段を含み、さらに、
該許諾判定手段により許諾してよいと判定された場合に、当該個人情報に対応するユーザの前記第１ウェブサイト以外のウェブサイトでの行動履歴情報を前記第１ウェブサイトの業者に提供する、個人情報保護装置。
【請求項２】
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装置であって、
現実世界での実在人物を特定して識別するための実在人物用識別データとは異なる仮想人物を識別するための仮想人物用識別データを生成する仮想人物用識別データ生成手段と、
該仮想人物用識別データ生成手段により生成された前記仮想人物用識別データと前記実在人物用識別データ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してウェブサイトにアクセスする際に、ユーザを特定する情報の要求に応じて、当該ユーザに対応する前記仮想人物用識別データを当該ウェブサイトの業者に提供する提供手段と、
複数の前記ユーザの各々の個人情報を記憶する個人情報記憶手段と、
該個人情報記憶手段に記憶されている個人情報を提供するための制御を行なう個人情報提供制御手段とを含み、
前記仮想人物用識別データ生成手段が生成する前記仮想人物用識別データは、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の当該仮想人物を識別するための識別データであって、前記ウェブサイトの業者が前記実在人物を特定できない識別データであり、
前記仮想人物用識別データ生成手段は、１人のユーザが第１ウェブサイトに対しアクセスする毎に繰り返して用いる当該第１ウェブサイト専用の第１の仮想人物用識別データを生成するとともに、当該１人のユーザが第２ウェブサイトに対しアクセスする毎に繰り返して用いる当該第２ウェブサイト専用の第２の仮想人物用識別データを生成し、
前記登録手段は、各ユーザ毎に、前記実在人物用識別データと前記第１の仮想人物用識別データと前記第２の仮想人物用識別データとの対応関係を特定可能な情報を登録し、
前記提供手段は、前記仮想人物用識別データ生成手段により生成された前記第１の仮想人物用識別データを前記第１ウェブサイトの業者に提供するとともに、前記仮想人物用識別データ生成手段により生成された前記第２の仮想人物用識別データを前記第２ウェブサイトの業者に提供することにより、前記仮想人物用識別データを使分けて提供し、
前記個人情報提供制御手段は、１人のユーザの個人情報を前記第１ウェブサイトの業者または前記第２ウェブサイトの業者に提供する際に、当該１人のユーザにより前記第１ウェブサイトと前記第２ウェブサイトとで個別に設定されている許諾条件に従って個人情報

を提供する、個人情報保護装置。
【請求項３】
前記登録手段は、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前記対応関係を特定可能な情報を用いて割出すことが可能となるように前記登録する処理を行なう、請求項１または請求項２に記載の個人情報保護装置。
【請求項４】
前記第１ウェブサイトの業者から仮想人物用識別データの通知を受付て当該仮想人物用識別データに対応するユーザの他のウェブサイトでの行動履歴情報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受付けられた前記仮想人物用識別データが前記第１ウェブサイトに使用されている仮想人物用識別データであるか否かを判定して前記ユーザの個人情報の流通状態を監視する監視手段とを含む、請求項１～請求項３のいずれかに記載の個人情報保護装置。
【請求項５】
前記仮想人物用識別データは、ユーザが前記ウェブサイト毎に使い分ける匿名としてのコードデータを含む、請求項１～請求項４のいずれかに記載の個人情報保護装置。
【請求項６】
前記ユーザが前記匿名を用いてネットワーク上で行動する際に使用する前記匿名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をさらに含む、請求項５に記載の個人情報保護装置。
【請求項７】
前記電子証明書は、前記実在人物用識別データと前記仮想人物用識別データとの対応関係を特定可能な情報を登録している守秘義務のある所定機関により発行され、前記匿名を用いるユーザが当該所定機関において登録されているユーザであることを証明するものである、請求項６に記載の個人情報保護装置。
【請求項８】
前記匿名としてのコードデータは、当該匿名を用いるウェブサイトの名称を、当該匿名を用いるユーザが使用できる鍵で暗号化または復号化したものである、請求項５～請求項７のいずれかに記載の個人情報保護装置。
【請求項９】
複数の前記ユーザの個人情報の中に、当該個人情報からユーザ本人が特定される特定個人情報が含まれているか否か判定する特定個人情報判定手段と、
該特定個人情報判定手段により特定個人情報が含まれていると判定された場合に、当該特定個人情報を加工処理してユーザ本人を特定できないようにする個人情報加工手段をさらに含み、
前記提供手段は、前記個人情報加工手段により加工処理された後の個人情報を提供する、請求項１～請求項８のいずれかに記載の個人情報保護装置。
【請求項１０】
ユーザが実在人物としてウェブサイトにアクセスして前記実在人物用識別データを提供した当該ウェブサイト側からユーザを識別するために送信してきた第１クッキーを受付けた後、同じウェブサイトに同じユーザが仮想人物としてアクセスして前記仮想人物用識別データを提供した当該ウェブサイト側からユーザを識別するために送信してきた第２クッキーを受付けたときに、前記第１クッキーと前記第２クッキーとを区別して記憶し、以降同じユーザが前記仮想人物として同じ前記ウェブサイトにアクセスする際に、前記第１クッキーの当該ウェブサイトへの送信を阻止するとともに、前記第２クッキーを当該ウェブサイトへ送信する送信制御手段をさらに含む、請求項１～請求項９のいずれかに記載の個人情報保護装置。
【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を保護する個人情報保護装置に関する。
【０００２】
【従来の技術】
従来において、ユーザがネットワーク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こす際に、当該ユーザの住所氏名や年齢あるいは嗜好情報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】
このような場合において、個人のプライバシーを維持したまま、安心できる状態で安全に正しく権限を与えられた情報転送を行なうものとして、特開平１１－２５０１６５号公報に記載のものがあった。この特許文献に記載のものは、第１のデータ記憶はユーザーに関する静的身元確認データを含む。第２のデータ記憶はユーザーに関する適度に動的な個人データを含む。第３のデータ記憶は、ユーザーに関する動的実態的人口統計学的情報データを含む。上記のシステムで電子ウォレット（財布）を使用して、データの選択された部分をダウンロードしてユーザーに使用させることができる。データは、フォームを埋めたり、ユーザーにサービスを提供したり、ユーザーの匿名性を維持したまま店主が選択的に販売対象となるユーザーを定めることができるように使用することができる。
【０００４】
【発明が解決しようとする課題】
本発明の目的は、ユーザとそのユーザが用いる識別情報（たとえばサイト毎に使い分けられるユーザの匿名）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し、たとえばユーザと業者側との間において、ユーザと前記識別情報との対応関係をめぐるトラブルが発生した場合に、所定機関に登録されている対応関係の情報を参照することを可能とすることである。また、同一人物に関するネットワーク上の行動履歴データをサイト側に提供して、その行動履歴データに基づいたよりカスタマイズされたユーザ好みの情報やサービスをユーザ側に提供しやすくすることである。
【０００８】
【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装置であって、
現実世界での実在人物を特定して識別するための実在人物用識別データとは異なる仮想人物を識別するための仮想人物用識別データを生成する仮想人物用識別データ生成手段と、
該仮想人物用識別データ生成手段により生成された前記仮想人物用識別データと前記実在人物用識別データ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してウェブサイトにアクセスする際に、ユーザを特定する情報の要求に応じて、当該ユーザに対応する前記仮想人物用識別データを当該ウェブサイトの業者に提供する提供手段と、
複数の前記ユーザの各々の行動履歴情報を各ユーザの個人情報として記憶する個人情報記憶手段と、
該個人情報記憶手段に記憶されている個人情報を提供するための制御を行なう個人情報提供制御手段とを含み、
前記仮想人物用識別データ生成手段が生成する前記仮想人物用識別データは、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の当該仮想人物を識別するための識別データであって、前記ウェブサイトの業者が前記実在人物を特定できない識別データであり、
前記仮想人物用識別データ生成手段は、１人のユーザが第１ウェブサイトに対しアクセスする毎に繰り返して用いる当該第１ウェブサイト専用の第１の仮想人物用識別データを

生成するとともに、当該１人のユーザが第２ウェブサイトに対しアクセスする毎に繰り返して用いる当該第２ウェブサイト専用の第２の仮想人物用識別データを生成し、
前記登録手段は、各ユーザ毎に、前記実在人物用識別データと前記第１の仮想人物用識別データと前記第２の仮想人物用識別データとの対応関係を特定可能な情報を登録し、
前記提供手段は、前記仮想人物用識別データ生成手段により生成された前記第１の仮想人物用識別データを前記第１ウェブサイトの業者に提供するとともに、前記仮想人物用識別データ生成手段により生成された前記第２の仮想人物用識別データを前記第２ウェブサイトの業者に提供することにより、前記仮想人物用識別データを使分けて提供し、
前記個人情報提供制御手段は、
ユーザの個人情報を前記第１ウェブサイトに提供する際に、当該個人情報の前記第１ウェブサイトの業者への提供を許諾してよいか否かを判定する許諾判定手段を含み、さらに、
該許諾判定手段により許諾してよいと判定された場合に、当該個人情報に対応するユーザの前記第１ウェブサイト以外のウェブサイトでの行動履歴情報を前記第１ウェブサイトの業者に提供する。
【０００９】
請求項２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装置であって、
現実世界での実在人物を特定して識別するための実在人物用識別データとは異なる仮想人物を識別するための仮想人物用識別データを生成する仮想人物用識別データ生成手段と、
該仮想人物用識別データ生成手段により生成された前記仮想人物用識別データと前記実在人物用識別データ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してウェブサイトにアクセスする際に、ユーザを特定する情報の要求に応じて、当該ユーザに対応する前記仮想人物用識別データを当該ウェブサイトの業者に提供する提供手段と、
複数の前記ユーザの各々の個人情報を記憶する個人情報記憶手段と、
該個人情報記憶手段に記憶されている個人情報を提供するための制御を行なう個人情報提供制御手段とを含み、
前記仮想人物用識別データ生成手段が生成する前記仮想人物用識別データは、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の当該仮想人物を識別するための識別データであって、前記ウェブサイトの業者が前記実在人物を特定できない識別データであり、
前記仮想人物用識別データ生成手段は、１人のユーザが第１ウェブサイトに対しアクセスする毎に繰り返して用いる当該第１ウェブサイト専用の第１の仮想人物用識別データを生成するとともに、当該１人のユーザが第２ウェブサイトに対しアクセスする毎に繰り返して用いる当該第２ウェブサイト専用の第２の仮想人物用識別データを生成し、
前記登録手段は、各ユーザ毎に、前記実在人物用識別データと前記第１の仮想人物用識別データと前記第２の仮想人物用識別データとの対応関係を特定可能な情報を登録し、
前記提供手段は、前記仮想人物用識別データ生成手段により生成された前記第１の仮想人物用識別データを前記第１ウェブサイトの業者に提供するとともに、前記仮想人物用識別データ生成手段により生成された前記第２の仮想人物用識別データを前記第２ウェブサイトの業者に提供することにより、前記仮想人物用識別データを使分けて提供し、
前記個人情報提供制御手段は、１人のユーザの個人情報を前記第１ウェブサイトの業者または前記第２ウェブサイトの業者に提供する際に、当該１人のユーザにより前記第１ウェブサイトと前記第２ウェブサイトとで個別に設定されている許諾条件に従って個人情報を提供する。
【００１０】
請求項３に記載の本発明は、請求項１または請求項２に記載の発明の構成に加えて、前

記登録手段は、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前記対応関係を特定可能な情報を用いて割出すことが可能となるように前記登録する処理を行なう。

【００１１】

請求項４に記載の本発明は、請求項１～請求項３のいずれかに記載の発明の構成に加えて、前記第１ウェブサイトの業者から仮想人物用識別データの通知を受付て当該仮想人物用識別データに対応するユーザの他のウェブサイトでの行動履歴情報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受付けられた前記仮想人物用識別データが前記第１ウェブサイトに使用されている仮想人物用識別データであるか否かを判定して前記ユーザの個人情報の流通状態を監視する監視手段とを含む。

【００１４】

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、前記仮想人物用識別データは、ユーザが前記ウェブサイト毎に使い分ける匿名としてのコードデータを含む。

【００１５】

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、前記ユーザが前記匿名を用いてネットワーク上で行動する際に使用する前記匿名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をさらに含む。

【００１６】

請求項７に記載の本発明は、請求項６に記載の発明の構成に加えて、前記電子証明書は、前記実在人物用識別データと前記仮想人物用識別データとの対応関係を特定可能な情報を登録している守秘義務のある所定機関により発行され、前記匿名を用いるユーザが当該所定機関において登録されているユーザであることを証明するものである。

【００２７】

請求項８に記載の本発明は、請求項５～請求項７のいずれかに記載の発明の構成に加えて、前記匿名としてのコードデータは、当該匿名を用いるウェブサイトの名称を、当該匿名を用いるユーザが使用できる鍵で暗号化または復号化したものである。

請求項９に記載の本発明は、請求項１～請求項８のいずれかに記載の発明の構成に加えて、複数の前記ユーザの個人情報の中に、当該個人情報からユーザ本人が特定される特定個人情報が含まれているか否か判定する特定個人情報判定手段と、

該特定個人情報判定手段により特定個人情報が含まれていると判定された場合に、当該特定個人情報を加工処理してユーザ本人を特定できないようにする個人情報加工手段をさらに含み、

前記提供手段は、前記個人情報加工手段により加工処理された後の個人情報を提供する。

請求項１０に記載の本発明は、請求項１～請求項９のいずれかに記載の発明の構成に加えて、ユーザが実在人物としてウェブサイトにアクセスして前記実在人物用識別データを提供した当該ウェブサイト側からユーザを識別するために送信してきた第１クッキーを受付けた後、同じウェブサイトに同じユーザが仮想人物としてアクセスして前記仮想人物用識別データを提供した当該ウェブサイト側からユーザを識別するために送信してきた第２クッキーを受付けたときに、前記第１クッキーと前記第２クッキーとを区別して記憶し、以降同じユーザが前記仮想人物として同じ前記ウェブサイトにアクセスする際に、前記第１クッキーの当該ウェブサイトへの送信を阻止するとともに、前記第２クッキーを当該ウェブサイトへ送信する送信制御手段をさらに含む。

【００３３】

【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、ブロードバンドを利用したネットワークシステムを示し、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。広域・大容量中継網４３を通じて、クレジットカード発行会社群４、加盟店契約

会社群５、受信局４２、加盟店群６、サプライヤ群１、ＮＭ群（ニューミドルマン群）４８、電子行政群４９、ＸＭＬストア５０、コンテンツプロバイダ群５１、信号５２、携帯電話網５４に接続されたゲートウェイ５３、インターネットＩ、ユーザ宅４７、認証局群４６、コンビニエンスストア群２、会社群４５、データセンタ４４、放送局４１、金融機関群７等が、情報の送受信ができるように構成されている。なお、図中４０は衛星（サテライト）であり、放送局４１からの放送電波を中継して受信局４２に電波を送るためのものである。

【００３４】

クレジットカード発行会社群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。加盟店契約会社群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におけるアクアイアラとして機能する機関である。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。ＮＭ群４８とは、サプライヤ群１と消費者（自然人または法人）との仲立ちを行ない、たとえば消費者のショッピング等の消費行動の支援を行なうサービス業者のことである。従来の問屋や商社等の中間業者が、サプライヤ群の販売支援を行なうのに対し、このＮＭ群４８は、消費者の購入支援（消費行動支援）を行なう点で相違する。ＮＭ群４８の具体例としては、消費者の嗜好情報や購買履歴情報やＷｅｂサイトへのアクセス履歴情報をデータベースとして蓄積し、その蓄積されている消費者のプロフィール情報（個人情報）に基づいてその消費者にマッチする商品情報等を推薦して、消費者の消費行動を助けるサービス業者が当てはまる。

【００３５】

電子行政群４９は、たとえば市役所や税務署あるいは中央官庁等の行政を電子化したものである。ＸＭＬストア５０とは、ＸＭＬによる統一されたデータ構造によってデータを格納するとともに、必要に応じてデータの要求者に所定のデータを提供するデータベースのことである。ＸＭＬストア５０には、ユーザの各種個人情報やユーザエージェント（エージェント用知識データを含む）を格納している。金融機関群７やユーザからＸＭＬストア５０にアクセスがあった場合には、本人認証を行なってセキュリティを保ったうえで、必要なデータを提供できるように構成されている。コンテンツプロバイダ群５１とは、映像、文字、音等の種々のコンテンツをネットワークを通じて提供する業者群のことである。交通整理を行なうための信号機５２も、広域・大容量中継網４３に接続され、遠隔制御できるように構成されている。

【００３６】

携帯電話網４５に接続されている基地局５５に対し、ブラウザフォン（次世代携帯電話）３０の電波が送信され、基地局５５，携帯電話網４５，ゲートウェイ５３，広域・大容量中継網４３を介して、金融機関群７，加盟店群６，ＮＭ群４８，電子行政群４９，ＸＭＬストア５０，コンテンツプロバイダ群５１等にアクセスできるように構成されている。また車両５６も同様に、基地局５５，携帯電話網５４，ゲートウェイ５３，広域・大容量中継網５４を介して、各種サービス業者や各種機関にアクセスできるように構成されている。

【００３７】

認証局群４６とは、電子証明書の発行希望者に対して本人認証をしたうえで電子証明書を発行する機関である。データセンタ４４は、放送局４１から電波により配信される各種データを格納，管理する機関のことである。加盟店群６，サプライヤ群１，ＮＭ群４８，電子行政群４９，コンテンツプロバイダ群５１等にユーザが所定の情報の送信を依頼した場合に、大容量のデータを送信する際には、それら各機関やサービス業者の配信するデータを一旦データセンタ４４に格納しておき、所定の日時が来たときに放送局４１から電波を通じてそのデータを配信し、受信局４２で受信したデータを所定のユーザに広域・大容量中継網４３を通じて配信する。

【００３８】

なお、図１中二重線で示した部分は、無線ＬＡＮ，ＣＡＴＶ，衛星，ｘＤＳＬ（digital subscriber line），ＦＴＴＨ（fiber to the home）などである。

【００３９】

本実施の形態では、認証局群４６ばかりでなく、金融機関群７も、電子証明書を発行する。図１中、１９はユーザに携帯されるＩＣ端末であり、後述するようにユーザのプロフィール情報（個人情報）等が格納されている。

【００４０】

図２（ａ）は、図１に示した会社群４５の一例を示し、図２（ｂ）は、図１に示したユーザ宅４７の一例を示している。

【００４１】

会社４５内には、社内ＬＡＮが構築されており、パーソナルコンピュータ５７，自動販売機５８，サーバ５９，データベース６０，ノート型パーソナルコンピュータ６２，ファクシミリ６１が情報のやり取りができるように接続されている。

【００４２】

ブラウザフォン３０は、パーソナルコンピュータ５７，自動販売機５８，サーバ５９，他のブラウザフォン３０に対し、ブルートゥース（Bluetooth）を使用して直接送受信できるように構成されている。前述したデータセンタ４４は、配信しようとするコンテンツ等の情報のうちセキュリティを要求される情報に関しては暗号化して格納しており、その暗号化情報を配信するときには暗号化された情報のままで放送局４１から電波により配信される。一方、ＩＣ端末１９は、個人情報の他にそのＩＣ端末１９の所持者であるユーザの本人認証用の鍵や暗号アルゴリズム等のセキュリティ機能が備えられている。前述した放送局４１から配信されてきて広域・大容量中継網４３等を経由して会社４５内の社内ＬＡＮに伝送されてきた暗号化情報は、このＩＣ端末１９に記憶されている鍵およびアルゴリズムによって復号化できるように構成されている。

【００４３】

さらに、ブラウザフォン３０にこのＩＣ端末１９を接続することにより、送られてきた情報をブラウザフォン３０で受けてその暗号化情報をＩＣ端末１９により復号化して平文等の元の情報にして表示することができる。ブラウザフォン３０にＩＣ端末１９を接続した場合には、さらに通話を暗号化して送受信することができる。暗号化された通話をブラウザフォン３０が受信すれば、ＩＣ端末１９によりリアルタイムで復号化してもとの通話に戻してその通話をスピーカから流すことができるように構成されている。

【００４４】

ファクシミリ６１にＩＣ端末１９を接続することにより、ファクシミリ６１による送受信データを暗号化することができる。そして暗号化されたデータをファクシミリ６１が受信すれば、ＩＣ端末１９によりそれを復号化して平文等の元のデータに戻してプリントアウトできる。

【００４５】

図２（ｂ）のユーザ宅４７のＲＡＮには、セットボックス６３、テレビ６７、パーソナルコンピュータ６８、照明６４、冷蔵庫６９、エアコンディショナ６５、電話６６、電子錠７０等が接続されている。

【００４６】

図２に示す、パーソナルコンピュータ５７、自動販売機５８、サーバ５９、ファクシミリ６１、ノート型パーソナルコンピュータ６２、セットボックス６３、テレビ６７、パーソナルコンピュータ６８、照明器具６４、冷蔵庫６９、エアコンディショナ６５、電話６６、電子錠７０等は、それぞれＵＲＬが割振られており、外部から広域・大容量中継網４３等を経由してそのＵＲＬ（Uniform Resource Locator）にアクセスすることによりそれぞれの装置にアクセスできるように構成されている。それぞれの装置にアクセスし、その装置の現在の状態等をチェックしたり、外部から遠隔操作できる。たとえば、電子錠７０にアクセスして施錠されていない場合には遠隔操作によって施錠したり、エアコンディショナ６５にアクセスして、ユーザがユーザ宅４７に帰宅する１０分ほど前に、エアコンディ

ショナ６５が作動するようにセットしたり等ができる。
【００４７】
図３は、金融機関７を説明するための説明図である。金融機関７には、ＶＰ管理サーバ９、決済サーバ１０、認証用サーバ１１、データベース１２ａ，１２ｂが備えられている。ＶＰ管理サーバ９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）を管理するためのサーバである。ＶＰとは、現実世界に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。
【００４８】
ＶＰ管理サーバ９は、後述するように、ＲＰからＶＰの出生依頼があれば、その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１２ａ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。ＶＰが売買や決済等の法律行為を行なう場合に、この電子証明書を相手方に送信することにより、仮想人物でありながら独立して法律行為を行なうことが可能となる。
【００４９】
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。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。
【００５０】
データベース１２ａは、ＲＰやＶＰに関するデータを格納するものである。データベース１２ｂは、広域・大容量中継網４３やインターネットＩに接続されているサイト（業者）を管理するためのデータを格納している。
【００５１】
図３に示すように、データベース１２ａには、ＲＰ用のデータとして、ＲＰの氏名、住所、認証鍵ＫＮ、公開鍵ＫＴ、口座番号等が記憶されている。認証鍵とは、ＲＰが金融機関７にアクセスしてきた場合に共通鍵暗号方式により本人認証を行なうための鍵である。公開鍵とは、公開鍵暗号方式に用いられる鍵であり、秘密鍵とペアとなっている鍵である。口座番号は、当該金融機関７においてＲＰが開設している口座番号のことである。
【００５２】
トラップ情報とは、サイト（業者）側が個人情報を収集してそれを不正に流通させた場合に、それを行なった犯人を割出すためにトラップ（罠）を仕掛けるための情報である。たとえば、ＶＰが自己の個人情報をあるサイト（第１譲渡先）に譲渡する際に、その第１譲渡先特有の氏名を用いる。すなわち、ＶＰが自己の氏名を複数種類有し、サイト（業者）ごとに使い分ける。このようなＶＰ氏名を、便宜上トラップ型ＶＰ氏名という。このようにすれば、ダイレクトメールやＥメールが業者側から送られてきた場合には、そのメールの宛名がトラップ型ＶＰ氏名となっているはずである。その送ってきたサイト（業者）が、トラップ型ＶＰ氏名から割出される第１譲渡先とは異なりかつ譲渡した自己の個人情報の開示許容範囲（流通許容範囲）を超えたサイト（業者）であった場合には、その個人情報が第１譲渡先によって不正に開示（流通）されたこととなる。このように、不正流通（不正開示）を行なった第１譲渡先を、トラップ型ＶＰ氏名から割出すことができる。
【００５３】
なお、図３では、次郎が第２トラップ情報、第３トラップ情報、第２個人情報、第３個人情報、２つの情報を有している。次郎が、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ために、これら２種類のＶＰ情報を金融機関７に登録している。ＶＰの住所とは、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２の住所である。その結果、ＶＰとして電子ショッピングをした場合の商品の配達先が、そのＶＰの住所であるコンビニエンスストア２に配達されることとなる。ＲＰ

は、その配達されてきた商品をＶＰになりすましてコンビニエンスストア２にまで出向いて商品を引取ることが可能となる。このようにすれば、住所を手がかりにＶＰとＲＰとの対応関係が見破られてしまう不都合が防止できる。

【００５４】

図３に示したトラップ情報の詳細は、図４に示されている。第１トラップ情報、第２トラップ情報、…の各トラップ情報は、サイト名ごとに、氏名（トラップ型ＶＰ氏名）、公開鍵、Ｅメールアドレス、バーチャル口座番号、バーチャルクレジット番号を含んでいる。たとえば、サイト名（業者名）ＡＢＣにＶＰがアクセスする際には、ＶＰの本名であるＢ１３Ｐを用い、ＶＰの秘密鍵ＫＳＢとペアの公開鍵ＫＰＢ'を用い、ＶＰの本当のＥメールアドレスである○□×△×を用い、ＶＰの本当の口座番号である２５０３を用い、ＶＰの本当のクレジット番号である３２８８を用いる。

【００５５】

一方、サイト名（業者名）ＭＴＴにアクセスする場合には、ＶＰの本名をそのＶＰの秘密鍵で１回暗号化したＥ（Ｂ１３Ｐ）を、トラップ型ＶＰ氏名として用いる。秘密鍵としては、ＶＰの本当の秘密鍵ＫＳＢをＶＰの本当の秘密鍵ＫＳＢで１回暗号化したE_{KSB}（ＫＳＢ）を用いる。この秘密鍵E_{KSB}（ＫＳＢ）に対する公開鍵ＫＰＢがデータベース１２ａに格納されている。Ｅメールアドレスとしては、金融機関７がトラップ型ＶＰのために開設しているＥメールアドレス△△△△△を用いる。口座番号としては、ＶＰの本当の口座番号をＶＰの本当の秘密鍵で１回暗号化したＥ（２５０３）をバーチャル口座番号として用いる。クレジット番号は、ＶＰの本当のクレジット番号をＶＰの本当の秘密鍵で１回暗号化したＥ（３２８８）を用いる。

【００５６】

さらに、サイト名（業者名）ＭＥＣにアクセスする場合には、ＶＰの秘密鍵でＶＰの本名を２回暗号化したE^2（Ｂ１３Ｐ）をトラップ型ＶＰ氏名として用いる。

【００５７】

ＶＰがトラップ型ＶＰ氏名E^2（Ｂ１３Ｐ）を用いてネットワーク上で行動する場合には、秘密鍵ＫＳＢを秘密鍵ＫＳＢで２回暗号化した２回暗号化秘密鍵E^2_{KSB}（ＫＳＢ）を用いる。その２回暗号化秘密鍵とペアになっている公開鍵がＫＰＢ″である。Ｅメールアドレスは、金融機関７がトラップ型ＶＰ用のＥメールアドレスとして開設している△△△△△を用いる。バーチャル口座番号は、ＶＰの本当の口座番号を秘密鍵で２回暗号化したE^2（２５０３）を用いる。クレジット番号は、ＶＰの本当のクレジット番号をＶＰの秘密鍵で２回暗号化したバーチャルクレジット番号E^2（３２８８）を用いる。

【００５８】

このように、サイト名ごとに、トラップ情報の暗号回数が異なる。サイト側（業者側）に提供した個人情報というものは、ネットワーク上を流通した後最終的にはその個人情報主にＥメールやダイレクトメールの形で返ってくる。この個人情報の帰還ループを利用してトラップを仕掛けて個人情報の不正流通を行なった犯人を追跡できるようにするのが、このトラップ情報の狙いである。すなわち、ユーザをネット上で追跡するトラッキング型クッキーの逆を行なうものである。

【００５９】

図５は、図３に示したＶＰの個人情報を説明する図である。第１個人情報、第２個人情報、第３個人情報、…の各個人情報は、個人情報Ａ、個人情報Ｂ、…の複数種類の個人情報が集まって構成されている。たとえば、個人情報Ａは、ＶＰの年齢，性別，職業，年収等であり、個人情報Ｂは、ＶＰの嗜好に関する情報である。

【００６０】

図５に示すように、各個人情報は，金融機関７の秘密鍵ＫＳによるデジタル署名が付されている。たとえば，第１個人情報の個人情報Ａは、○○△の個人情報自体に対しデジタル署名であるD_{KS}（○○△）が付されている。

【００６１】

このデータベース１２ａに格納されている各個人情報は、後述するように、金融機関７が

その真偽をチェックして正しいもののみをデータベース１２ａに格納し、正しいことを認証するためのデジタル署名が付される。

【００６２】

図６は、金融機関７のデータベース１２ｂに格納されている情報を示す図である。データベース１２ｂには、サイト名（業者名）ごとに、その業者が個人情報を不正入手した値と、個人情報を不正流出（不正流通）した値と、それら両値から割出される悪い順位とが記憶されている。

【００６３】

後述するように、あるサイト名（業者名）ＭＴＴが、個人情報を不正に入手すればその不正入手値が「１」加算更新され、個人情報を不正に流通すれば、その不正流通値が「１」加算更新される。そして悪い順位は、不正入手値＋２×不正流出値の計算式で値を出し、その値が大きいほど悪い順位が上位となる。前記計算式の値が一番大きければ悪い順位が一番となる。

【００６４】

図７は、ＸＭＬストア５０の構成を示す図である。ＸＭＬストア５０には、データベース７２とそれを制御するサーバ７１とが設置されている。サーバ７１は、ＸＭＬストア５０にアクセスしてきた者を、本人認証してアクセス制御する機能も備えている。

【００６５】

データベース７２には、ＸＭＬで表現されたデータが格納されている。そのデータの中身は、ＶＰ情報として、ＶＰの氏名であるたとえばＢ１３Ｐ、ＶＰユーザエージェント（知識データを含む）、サイト別情報として、サイト名たとえばＡＢＣ、そのサイトにアクセスしたＶＰに発行された電子証明書、そのＶＰの個人情報と当該サイトのプライバシーポリシーとそれら両情報に対し当該ＶＰが付したデジタル署名D_{KSB}（個人情報＋ポリシー）と当該サイトＡＢＣが付したデジタル署名D_{KSA}（個人情報＋ポリシー）と、トラップ情報としての暗号化回数「０」と、当該ＶＰのＥメールアドレスである○□×△×が含まれている。さらに、ＶＰがサイト名ＭＴＴにアクセスした場合には、そのサイト名ＭＴＴにアクセスしたトラップ型ＶＰに対し発行された電子証明書と、そのサイトにトラップ型ＶＰが提供した個人情報とそのサイトのプライバシーポリシーとそれら両情報に対する当該トラップ型ＶＰのデジタル署名と当該サイトのデジタル署名と、トラップ情報としての暗号回数「１」とＥメールアドレスとが含まれている。

【００６６】

さらに、氏名がＮＰＸＡの他のＶＰの情報も、前述と同様の項目がデータベース７２に記憶される。このデータベース７２には、非常に多くのＶＰごとに、前述した項目でデータが記憶されている。

【００６７】

なお、サイト名ＡＢＣについては、図４で説明したように、トラップ情報として１回も暗号化していない情報を用いているために、データベース７２に格納されている暗号回数も「０」となっている。サイト名ＭＴＴについて言えば、図４で説明したように、トラップ情報として１回暗号化した情報を用いているために、データベース７２に記憶されている暗号化回数も「１」となっている。

【００６８】

前述したＶＰユーザエージェントとは、ユーザであるＶＰのために動作する自立型ソフトウェアのことである。このＶＰユーザエージェントは、ネットワークを通して移動できるようにモバイルエージェントで構成されている。

【００６９】

なお、図３～図７に示した各データは、暗号化した状態で各データベース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（トラップ型ＶＰを含む）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１２ａ等から検索し

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。

【００７０】

図８は、コンビニエンスストア２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７５と、それに接続されたサーバ７４と、そのサーバに接続された端末７３とが設置されている。データベース７５には、当該コンビニエンスストアに住所を持つＶＰ（トラップ型ＶＰを含む）の氏名と、それら各氏名に対応して、商品の預かり情報、Ｅメールアドレス、顧客管理情報等が記憶されている。

【００７１】

当該コンビニエンスストア２にＢ１３ＰのＶＰが購入した商品が配達されれば、データベース７５のＢ１３Ｐの記憶領域に、商品預かり情報として「ＡＢＣ会社からの商品預かり，未決済」が格納される。この未決済とは、Ｂ１３Ｐがネットを通じて商品を購入したもののまだ支払を行なっていない状態のことである。

【００７２】

データベース７５のＥメールアドレスの欄には、各ＶＰに対応してＥメールアドレスが格納されている。Ｂ１３Ｐの場合には、トラップ型ＶＰでないために、当該ＶＰの本当のＥメールアドレスである○□×△×が格納されている。

【００７３】

トラップ型ＶＰであるＥ（Ｂ１３Ｐ）も同様に、商品預かり情報としてたとえば「ＭＴＴ会社からの商品預かり，決済済」が格納される。なお、Ｅ（Ｂ１３Ｐ）は、トラップ型ＶＰであるために、Ｅメールアドレスは、金融機関７のトラップ型ＶＰのために開設されているＥメールアドレスが格納される。

【００７４】

サーバ７４は、後述するように、コンビニエンスストア２にＶＰ（トラップ型ＶＰを含む）として商品を引取りに来た顧客が、当該コンビニエンスストア２に登録されているＶＰ（トラップ型ＶＰを含む）に対し商品を預かっている場合にはその商品をＶＰ（トラップ型ＶＰを含む）に引渡すための処理を行なう。

【００７５】

コンビニエンスストア２は、商品の預かりサービスばかりでなくＶＰ用のダイレクトメールの預かりサービスも行なう。ＶＰはコンビニエンスストア２が住所でありＶＰ宛のダイレクトメールはコンビニエンスストア２に郵送されるためである。

【００７６】

図９は、ユーザに用いられる端末の一例のブラウザフォン３０を示す正面図である。ブラウザフォン３０には、マイクロコンピュータ１９９が備えられている。このマイクロコンピュータ１９９には、ＣＰＵ（Central Processing Unit）１９７と、Ｉ／Ｏポート１９８と、ＲＯＭ１９５と、ＥＥＰＲＯＭ１９４と、ＲＡＭ１９６とが備えられている。このブラウザフォン３０は、ＵＳＢ（Universal Serial Bus）ポートを備えており、ＵＳＢポートに対し、ＩＣ端末１９Ｒまたは１９Ｖまたは１９Ｉが差込み可能に構成されている。ＩＣ端末１９Ｒは、ＲＰ用のＩＣ端末である。ＩＣ端末１９Ｖは、ＶＰ用のＩＣ端末である。ＩＣ端末１９Ｉは、後述するように金融機関が発行したＶＰ用のデータやプログラムが格納されてユーザにまで配達されてくるものであり、その配達されてきたＩＣ端末１９ＩをブラウザフォンのＵＳＢポートに指込むことにより、ＩＣ端末１９Ｉに記憶されているデータやソフトウェアがブラウザフォン３０に記憶されることとなる。

【００７７】

図１０は、ＶＰ用ＩＣ端末１９Ｖ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、ブラウザフォン３０のＵＳＢポート１８に対し着脱自在に構成されており、ＵＳＢポート１８に差込むことにより、ブラウザフォン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。

【００７８】

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２

０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。

【００７９】

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。

【００８０】

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。

【００８１】

ＲＰ用ＩＣ端末１９Ｒの場合も、図１０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。

【００８２】

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。

【００８３】

図１１は、図１０に示したクッキーデータの詳細を示す図である。クッキーデータの記憶領域には、ＶＰ氏名ごとに、そのＶＰ氏名を用いてアクセスしたサイト（業者）側から送られてきたクッキーが格納される。ＶＰが本名Ｂ１３Ｐを用いてサイトにアクセスする場合には、既にトラップ型ＶＰを用いてアクセスしたサイト以外のサイトは、どのサイトでもアクセスできる。その結果、本名Ｂ１３Ｐに限り多くのサイトからのクッキーデータが記憶されている。

【００８４】

図１２は、図３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る。顧客（ユーザ）がブラウザフォン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２４（ｂ）に基づいて後述する。次にＳ２へ進み、ＲＰの氏名，住所の入力要求をブラウザフォン３０へ送信する。次にＳ３へ進み、ＲＰの氏名，住所の返信がブラウザフォン３０からあったか否かの判断がなされ、あるまで待機する。

【００８５】

ユーザであるＲＰがブラウザフォン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ブラウザフォン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、ブラウザフォン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、その暗号結果がブラウザフォン３０へ出力される。ブラウザフォン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DKN（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＝DKN（Ｉ）であるか否かの判断がなされる。

【００８６】

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＝DKN（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＝DKN（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ブラウザフォン３０へ送信されてＳ１へ戻る。

【００８７】

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、ブラウザフォン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。

【００８８】

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ブラウザフォン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ブラウザフォン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をブラウザフォン３０へ出力する。ブラウザフォン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。

【００８９】

次にＳ１６へ進み、ＶＰの電子証明書を作成してＸＭＬストア５０に登録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ＩＣ端末１９Ｉ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。

【００９０】

本発明でいう「匿名用の電子証明書」とは、ユーザと当該ユーザが用いる匿名（ＶＰ氏名）との対応関係を特定可能な情報を登録している守秘義務のある所定機関（金融機関７）により発行され、前記匿名を用いるユーザが当該所定機関に登録されているユーザであることを証明する証明書を含む概念である。よって、本人確認に用いる一般的なデジタルＩＤばかりでなく、前記所定機関が前記匿名を用いるユーザに対し当該ユーザは当該所定機関に登録されているユーザであることを証明する電子的な証明書をすべて含む概念である。たとえば、ユーザが用いる匿名とその匿名が前記所定機関に登録されているメッセージとに対し、前記所定機関によるデジタル署名が施されただけの、簡単な証明書を含む概念

である。

【００９１】

Ｓ１によりＮＯの判断がなされた場合にはＳ１３（ａ）のＳ４００へ進む。Ｓ４００では、個人情報の登録処理が行なわれ、次にＳ４０１によりトラップ情報の登録処理が行なわれ、Ｓ４０２により個人情報の確認処理が行なわれ、Ｓ４０３により個人情報の照合，流通チェック処理が行なわれ、Ｓ４０４により個人情報の販売代行処理が行なわれ、Ｓ４０５によりメール転送，流通チェック処理が行なわれ、Ｓ４０６により他のトラップ型ＶＰのアクセス履歴の提供処理が行なわれ、Ｓ４０７により信頼度ランキング情報の集計，提供処理が行なわれてＳ１へ戻る。ユーザから個人情報の提供を受けたサイト（業者）側では、提供してもらった個人情報が本当に正しい内容であるか否かを確認したいというニーズがある。そこで、金融機関７のＶＰ管理サーバ９は、ユーザから個人情報を受付けてその個人情報が正しい個人情報かどうかをチェックし、正しい個人情報のみをデータベース１２ａに登録する。その処理をＳ４００により行なう。

【００９２】

一方、ネットワーク上でＶＰの利用が盛んになった場合には、ＲＰとＶＰとの両方の詳しい個人情報を収集した業者が、両個人情報をしらみつぶしにマッチングして、両個人情報が一致するＲＰ氏名とＶＰ氏名とを割出し、ＶＰに対応するＲＰを予測してしまうという不都合が生ずる恐れがある。そこで、個人情報をデータベース１２ａに登録する場合には、勤務先名や所属部署名あるいは役職等のＲＰが特定されてしまうような個人情報を排除（または変更）して、登録する必要がある。そのような処理を、Ｓ４００により行なう。

【００９３】

一方、個人情報主であるユーザは、自己の個人情報が正しい内容で流通しているか否かを監視し、間違っていれば正しい内容に修正したいというニーズがある。そこで、データベース１２ｂに登録されている自己の個人情報の真偽をユーザがチェックできるように、Ｓ４０２により、個人情報の確認処理が行なわれる。

【００９４】

さらに、ユーザが自己の個人情報の公開範囲（流通範囲）を限定した上でその個人情報を業者側（サイト側）に提供した場合に、その公開範囲（流通範囲）が守られているか否かを監視したいというニーズがある。個人情報の提供を受けた業者側は、前述したようにその個人情報が正しい情報であるか否かを確認したいというニーズがある。そこで、サイト側（業者側）が所有している個人情報を正しい個人情報が登録されているデータベース１２ａの個人情報と照合できるようにする一方、その照合対象となった業者側所有の個人情報の流通許容範囲をチェックして正しく流通されているか否かをチェックできるように、Ｓ４０３の処理が行なわれる。

【００９５】

ユーザは、個人情報を提供する見返りとして、何らかのサービスあるいは金銭を入手したいというニーズがある。そこで、Ｓ４０４により、個人情報の販売代行が行なわれる。図４に基づいて説明したように、トラップ型ＶＰは、Ｅメールアドレスを金融機関７のトラップ型ＶＰ用として開設しているアドレスにしているため、そのトラップ型ＶＰに宛てたＥメールは金融機関７のトラップ型ＶＰ用に開設されたＥメールアドレス宛に送られる。そこで、その送られてきたＥメールを対応するＶＰのＥメールアドレスに転送する必要がある。その処理を、Ｓ４０５により行なう。その際に、業者側から送られてくるＥメールの宛名はトラップ型ＶＰとなっているために、そのトラップ型ＶＰに対応するサイトを割出し（図４参照）、その割出されたサイトからのＥメールでなかった場合には当該トラップ型ＶＰの個人情報の流通許容範囲内のサイトからのＥメールか否かをチェックし、流通チェックを行なうことも、Ｓ４０５により行なわれる。

【００９６】

図４に基づいて説明したように、トラップ型ＶＰ氏名をサイト別に使い分ける場合には、ユーザ側において、それら氏名毎に分離してサイト側からのクッキーが記録されるように交通整理を行なう必要がある。同一のクッキーが複数のトラップ型ＶＰにまたがって共通

に付着されている場合には、その複数のトラップ型ＶＰは同一人物のＶＰであることが見破られてしまうためである。

【００９７】

このような交通整理を行なった場合には、業者側（サイト側）は、ある１つのトラップ型ＶＰについてのアクセス履歴情報や商品購入履歴情報を収集することはできるが、同一のＶＰでありながら他のトラップ型ＶＰ氏名使用時におけるアクセス履歴や商品購入履歴情報は収集できなくなる。つまり、業者側（サイト側）は、あるＶＰについてその一部の履歴情報しか収集できなくなるという不都合が生ずる。

【００９８】

そこで、業者側（サイト側）から要請があった場合に、他のトラップ型ＶＰのアクセス履歴を提供し得る処理が、Ｓ４０６により行なわれる。

【００９９】

ユーザが自己の個人情報をサイト側（業者側）に提供する際には、その業者がプライバシー保護に関してどの程度信用できる業者であるか否か確認したいというニーズがある。そこで、Ｓ４０７により、信頼度ランキング情報の集計を行なってその集計結果を提供する処理が行なわれる。

【０１００】

図１３の（ｂ）は、Ｓ４００の個人情報の登録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。この個人情報の登録処理は、ユーザがＶＰとして個人情報を登録する際の処理である。

【０１０１】

乱数Ｒを受信したブラウザフォン３０は、そのブラウザフォン３０に接続されているＶＰ用ＩＣ端末１９Ｖに記憶されているＶＰ用の秘密鍵を用いて乱数Ｒを１回暗号化してレスポンスデータＩを生成する。そしてそのレスポンスデータＩを金融機関７のＶＰ用管理サーバ９へ送信する。

【０１０２】

Ｓ４１０により、ユーザ側から個人情報の登録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。登録要求があった場合にはＳ４１１へ進み、正当機関証明処理がなされる。次に制御がＳ４１２へ進み、ＶＰの氏名の入力要求がなされ、Ｓ４１３により入力があったか否かの判断がなされる。入力があった場合には制御がＳ４１４へ進み、乱数Ｒを生成してチャレンジデータとして登録要求を行なったユーザ側に送信する処理がなされる。Ｓ４１５へ進み、ユーザ側からレスポンスデータＩ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。受信した段階でＳ４１６へ進み、ＶＰの公開鍵ＫＰをデータベース１２ａから検索して、受信したレスポンスデータＩを公開鍵ＫＰで暗号化したD_{kp}（Ｉ）を生成する処理がなされる。

【０１０３】

次に制御がＳ４１７へ進み、チャレンジデータＲとD_{kp}（Ｉ）が等しいか否かの判断がなされる。等しくなければユーザの本人認証ができなかったこととなりＳ４２２へ進み、登録拒否の処理がなされる。Ｓ４１７によりＹＥＳの判断がなされた場合には制御がＳ４１８へ進み、登録要求を出したユーザに対し登録を希望する個人情報の入力要求を出す処理がなされる。次にＳ４１９へ進み、入力があったか否かの判断がなされ、入力があるまで待機する。入力があった段階で制御がＳ４２０へ進み、登録対象の個人情報の真偽チェックを行なう。

【０１０４】

この真偽チェックは、たとえば、ＸＭＬストア５０にアクセスして該当するユーザの個人情報が登録されている場合にそれと照合チェックしたり、電子行政群４９に含まれる市役所等にアクセスしてそこに登録されている個人情報と照合チェックしたりして行なわれる。このような機械検索による照合チェックだけでは不十分な場合には、金融機関７の調査員が裏取り調査を行なって真偽チェックを行なう。

【０１０５】

次に制御がＳ４２１へ進み、真偽チェックの結果正しいか否かの判断がなされ、正しくない場合にはＳ４２２へ進み登録拒否の処理がなされる一方、正しい場合にはＳ４２３へ進み、ＲＰが特定される個人情報か否かの判断がなされる。登録しようとしているＶＰの個人情報の中に、たとえば勤務先名や所属部署名あるいは役職等のＲＰが特定されてしまうような個人情報が存在する場合に、それをそのまま登録してしまうと、その登録情報からどのＶＰがどのＲＰに対応するかを第三者に予測されてしまう恐れがある。このデータベース１２ａに登録される個人情報は、Ｓ４０３やＳ４０４によりサイト側（業者側）が知り得る状態となる。その結果、サイト側（業者側）に、ＲＰとＶＰとの対応関係が予測される恐れが生ずる。

【０１０６】

そこで、Ｓ４２３により、ＲＰが特定される個人情報か否かの判断がなされ、予測される個人情報でなければＳ４２５へ進むが、予測される恐れのある個人情報の場合にはＳ４２４へ進み、その個人情報を加工する処理がなされた後Ｓ４２５へ進む。たとえば、勤務先名がＭＥＣであった場合には、それをたとえば「某大手電気メーカー」に加工したり、役職がたとえば専務であった場合には、たとえば「重役」に加工したりする。

【０１０７】

Ｓ４２５では、個人情報に当該金融機関のデジタル署名を付してユーザ名別に登録する処理がなされる。その結果、図５に示すようなデータがデータベース１２ａに登録される。

【０１０８】

図１４は、Ｓ４０１に示されたトラップ情報の登録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。Ｓ４３０により、正当機関証明処理がなされ、Ｓ４３１により、ＶＰ氏名の入力要求がトラップ情報の登録依頼をしてきたＶＰに出される。次にＳ４３２へ進み、その登録依頼をしてきたＶＰが自己のＶＰ氏名を入力したか否かの判断がなされ、入力するまでＳ４３１の要求が出される。次に制御がＳ４３３へ進み、乱数Ｒを生成してチャレンジデータとして登録依頼者であるＶＰに送信する処理がなされる。Ｓ４３４により、レスポンスデータＩを受信したか否かの判断がなされる。

【０１０９】

送信されてきたチャレンジデータＲを受信した登録依頼者であるＶＰがそのチャレンジデータＲを自己の秘密鍵で暗号化してレスポンスデータＩを生成し、金融機関７のＶＰ管理サーバ９へ送信する。すると、制御がＳ４３５へ進み、登録依頼をしてきたＶＰの公開鍵ＫＰをデータベース１２ａから検索し、受信したレスポンスデータＩをその公開鍵ＫＰで復号化する処理を行なう。そしてＳ４３６により、チャレンジデータ$R = D_{kp}(I)$であるか否かの判断がなされ、イコールでない場合には認証の結果そのＶＰが本人と確定できないということであり、Ｓ４３７により登録拒否の通知がそのＶＰになされる。一方、Ｓ４３６によりＹＥＳの判断がなされて認証の結果ＶＰが本人であることが確認できた場合には、制御がＳ４３８へ進み、トラップ情報の送信要求をそのＶＰへ送信する処理がなされる。

【０１１０】

ＶＰから登録してもらいたいトラップ情報が送信されてきたか否かがＳ４３９によりなされ、送信されてくるまで待機する。送信されてきた段階で制御がＳ４４０へ進み、送信されてきたトラップ情報をデータベース１２ａに記憶させる処理がなされる。このトラップ情報は、登録依頼者であるＶＰに対応した記憶領域に記憶される。次に制御がＳ４４１へ進み、そのトラップ情報に対する電子署名を金融機関７が生成して、その電子証明書をＸＭＬストア５０へ登録する処理がなされる。その結果、図７に基づいて説明したように、ＸＭＬストア５０のデータベース７２に電子証明書が格納される。

【０１１１】

この電子証明書は、ＸＭＬストア５０に格納する代わりに登録依頼を行なってきたＶＰのＩＣ端末１９Ｖに格納してもよい。しかし、トラップ情報は、前述したように、そのＶＰがアクセスしたＷｅｂサイト毎に異なり、その結果電子証明書もＷｅｂサイト毎に異なることとなり、多数の電子証明書をＩＣ端末１９Ｖに格納するとなると、記憶容量の問題が

生ずる。ゆえに、本実施の形態では、その記憶容量の問題を克服するために、ＸＭＬストア５０へ登録する。なお、ＩＣ端末１９Ｖの記憶容量が非常に大きなものであれば、金融機関７が発行した電子証明書のすべてまたはその大半をこのＩＣ端末１９Ｖに記憶させてもよい。

【０１１２】

図１５は、Ｓ４０２に示された個人情報の確認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。金融機関７のデータベース１２ａに登録されている自己の個人情報をユーザが確認したい場合には、ユーザがＲＰとして金融機関７のＶＰ管理サーバ９へ確認要求を送信する。その確認要求の送信があればＳ４５０によりＹＥＳの判断がなされ、Ｓ４５１～Ｓ４５８により、前述したものと同様の本人認証処理がなされる。なお、Ｓ４５２による氏名の入力要求とは、ユーザのＲＰの氏名の入力要求である。本人認証の結果ユーザが本人であることが確認された場合にはＳ４５７によりＹＥＳの判断がなされて制御がＳ４５９へ進む。

【０１１３】

Ｓ４５９では、個人情報の確認要求であったか否かの判断がなされる。この個人情報の確認処理のサブルーチンプログラムは、ユーザから自己の個人情報の変更要求があった場合も対処できるように構成されている。そのユーザからの個人情報の変更要求の場合には、Ｓ４５９によりＮＯの判断がなされるが、個人情報の確認要求であった場合にはＳ４５９によりＹＥＳの判断がなされて制御がＳ４６０へ進み、入力されたＲＰ氏名に対応する個人情報をそのユーザに送信する処理がなされる。

【０１１４】

送信されてきた個人情報を確認したユーザは、その個人情報の中に間違った個人情報がある場合、あるいは、転職や引越し等を行なって個人情報が変更された場合には、自己の個人情報の変更要求を金融機関７のＶＰ管理サーバ９へ送信する。すると、Ｓ４５０ａによりＹＥＳの判断がなされて制御がＳ４５１へ進み、Ｓ４５１～Ｓ４５８の認証処理が行なわれる。そして認証の結果本人であることが確認された場合にはＳ４５７によりＹＥＳの判断がなされてＳ４５９へ進み、個人情報の確認要求であったか否かの判断がなされる。この場合には、個人情報の変更要求であるために、制御がＳ４５９ａへ進み、変更したい個人情報（変更情報）の送信要求がそのユーザに対してなされる。

【０１１５】

ユーザは、自己の個人情報中のどの箇所をどのように変更したいかという変更情報を金融機関７のＶＰ管理サーバ９へ送信する。すると、Ｓ４５９ｂによりＹＥＳの判断がなされてＳ４６１により、その送信されてきた変更情報が正しいか否かの真偽チェックがなされる。次にＳ４６２により、そのチェックの結果をユーザに返信する処理がなされる。次にＳ４６３により、チェックの結果正しいか否かの判断がなされ、正しくなければ個人情報の変更を行なうことなくそのままこのサブルーチンプログラムが終了するが、正しい場合にはＳ４６４へ進み、データベース１２ａ中の個人情報の該当箇所を変更する処理がなされる。

【０１１６】

図１６は、Ｓ４０３により示された個人情報の照合，流通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。Ｓ４６５により、照合依頼があったか否かの判断がなされる。たとえば、Ｗｅｂサイト側において、アクセスしてきたユーザの住所、氏名、年齢、性別、年収、嗜好情報等の、個人情報を収集した場合に、その個人情報が本当に正しい個人情報であるか否かを金融機関７において照合できるようにしたのが、このサブルーチンプログラムである。そのようなサイト側（業者側）から照合依頼があれば、制御がＳ４６６へ進み、金融機関７側の電子証明書をサイト側（業者側）へ送信し、Ｓ４６７により、そのサイト側（業者側）の電子証明書の送信を要求する処理がなされる。その業者側から自己の電子証明書が送信されてくればＳ４６８によりＹＥＳの判断がなされて制御がＳ４６９へ進み、照合したいユーザの氏名をその照合依頼者に要求する処理がなされる。照合依頼者であるサイト側（業者側）が照合したいユーザの氏名を送信してくれば、

制御がＳ４７３へ進み、照合したい個人情報の送信要求が依頼者側に出される。依頼者側が照合したい個人情報を金融機関７側に送信してくれば、制御がＳ４７１へ進む。

【０１１７】

Ｓ４７１では、送信されてきた依頼者の電子証明書の業者名（サイト名）と送信されてきた照合対象となるユーザ名とが合致するか否かをトラップ情報に基づいてチェックする処理がなされる。依頼者の電子証明書には、当該依頼者の業者名（サイト名）が記載されている。図４に基づいて説明したように、ＶＰは、Ｗｅｂサイトへアクセスする際に、ＶＰの本名を使う場合もあればトラップ型ＶＰを使う場合もある。つまり、ＶＰは、アクセスするサイト毎に氏名を使い分けているのである。よって、たとえば、図４のＭＴＴから個人情報の照合依頼があった場合には、Ｓ４７０により受信したユーザ氏名は本来Ｅ（Ｂ１３Ｐ）の筈である。このように、サイト名とそれに用いられているＶＰ氏名とが一致するか否かがＳ４７２により判断され、一致する場合にはＳ４７３へ進むが、一致しない場合には図１７のＳ４９４へ進む。

【０１１８】

Ｓ４９４では、ＸＭＬストアの該当個人情報を検索して、プライバシーポリシーに定められている流通許容範囲内に依頼者が含まれているか否かをチェックする処理がなされる。業者名（サイト名）とユーザ名とが一致しなければ、即個人情報の不正流通がなされたと判断すべきではなく、ＶＰがサイト側に個人情報を提供する際にある一定の流通許容範囲内においては他の業者にその個人情報を流通（開示）させてもよいことを承諾している場合が考えられる。この流通許容範囲は、サイト側が用意しているプライバシーポリシーに記述されている。そこで、Ｓ４９４により、ＸＭＬストアの該当個人情報を検索して、そこに格納されているプライバシーポリシーに定められている流通許容範囲内に依頼者が含まれているか否かをチェックするのである。たとえば、依頼者ＭＴＴから送られてきてユーザ名がＢ１３Ｐであり（図４参照）、そのユーザ名からそれに対応するサイト名ＡＢＣを割出すことができる。

【０１１９】

その割出されたサイト名ＡＢＣに基づいてＸＭＬストア５０のデータベース７２を検索し、サイト名ＡＢＣに付随して格納されている「ポリシー」を検索する（図７参照）。このプライバシーポリシーは、ＷｅｂサイトＡＢＣが個人情報を収集する際にユーザ側に提示したものであり、そのプライバシーポリシーには、収集した個人情報の流通許容範囲が記述されている。その流通許容範囲内に照合依頼者であるＭＴＴが含まれているか否かが、Ｓ４９４によっりチェックされる。含まれている場合にはＳ４９４ａによりＹＥＳの判断がなされてＳ４７５へ進むが、含まれていない場合には、その個人情報が不正に流通されたということになり、Ｓ４９５以降の処理がなされる。

【０１２０】

Ｓ４９５では、依頼者名に対応させて個人情報の不正入手値を「１」加算更新する処理がなされる。前述した例では、依頼者ＭＴＴがＶＰ氏名Ｂ１３Ｐを送信してきたということは、サイト（業者）ＡＢＣからＶＰ氏名Ｂ１３Ｐの個人情報を不正に入手したということである。よって、Ｓ４９５により、不正入手値を「１」加算更新する処理がなされる。この不正入手値は、データベース１２ｂに格納される（図６参照）。

【０１２１】

次に制御がＳ４９６へ進み、送信されてきたユーザ名に対応するサイト名（業者名）を割出し、そのサイト名（業者名）に対応させて個人情報の不正流出値を「１」加算更新する処理がなされる。前述した例では、送られてきたユーザ名Ｂ１３Ｐに対応するサイト名（業者名）ＡＢＣを割出し、そのサイト名（業者名）ＡＢＣに対応させて個人情報の不正流出値を「１」加算更新する。つまり、サイト（業者）ＡＢＣは、ＶＰ氏名Ｂ１３Ｐの個人情報をＭＴＴに不正に流出させたのであり、そのため、不正流出値を「１」加算更新するのである。この不正流出値も、データベース１２ｂに格納される（図６参照）。

【０１２２】

次に制御がＳ４９７へ進み、個人情報の不正があった旨およびその詳細データを該当する

ユーザに通知する処理がなされる。

【０１２３】

一方、依頼者の電子証明書に記載されている業者名と送られてきたユーザ名とが合致する場合には、制御がＳ４７５へ進み、依頼者から送信されてきた個人情報をデータベース１２ａの該当するユーザの個人情報（図５参照）と照合する処理がなされる。次にＳ４７６により、照合対象となっているユーザのユーザエージェントをＸＭＬストアから呼出す処理がなされる。次にＳ４７７により、そのユーザエージェントに照合結果を知らせ、依頼者に返信してよいか否かを尋ねる処理がなされる。ユーザエージェントからの返答があれば、制御がＳ４７９へ進み、依頼者に返信してよい旨の返答であった場合には、制御がＳ４８６へ進み、照合結果、正しい個人情報にデジタル署名を付す処理がなされる。このデジタル署名は、正しい個人情報である旨を金融機関７が確認したことを表わすものである。次にＳ４８７により、そのデジタル署名を付した個人情報を依頼者に返信して、それ以外は誤りである旨を依頼者に通知する処理がなされる。なお、依頼者から送信されてきた個人情報に相当するユーザの個人情報がデータベース１２ａになかった場合には、照合できないために、その照合できなかった個人情報について照合できなかった旨を依頼者に返信する。

【０１２４】

一方、ユーザエージェントからの返答の結果がＯＫでなかった場合には制御がＳ４８０へ進み、依頼者への返信の条件としてその依頼者（業者）から見返りを要求するという内容の返答がユーザエージェントからなされたか否かの判断がなされる。ユーザエージェントは、ＯＫの返答と見返り要求の返答と依頼者への返信を拒否する返答との３種類の返答を行なう。依頼者への返信を拒否する返答であった場合には、制御がＳ４８１へ進み、回答拒否を依頼者に返信する処理がなされる。

【０１２５】

見返りを要求する返答であった場合には、制御がＳ４８２へ進み、出された見返り要求を依頼者に返信する処理がなされる。次にＳ４８３により、依頼者からの返答があったか否かの判断がなされ、返答があるまで待機する。返答があった段階でＳ４８４により、交渉が成立したか否かの判断がなされる。交渉不成立の場合には制御がＳ４８１へ進み、回答を拒否する旨を依頼者に返信する処理がなされる。交渉が成立したと判断される場合にはＳ４８５へ進み、交渉が成立した旨をユーザに通知する処理がなされる。それと同時に、金融機関７のＶＰ管理サーバ９は、交渉によって決定された見返り内容を記憶しておく。次に、制御がＳ４８６へ進む。

【０１２６】

図１７の（ｂ）は、Ｓ４０４により示された個人情報の販売代行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。Ｓ４９８により、個人情報の購入要求があったか否かの判断がなされる。業者側から金融機関７のＶＰ管理サーバ９に個人情報の購入要求があれば、制御がＳ４９９へ進み、金融機関７の電子証明書をその購入要求者に送信する処理がなされる。次にＳ５００により、購入要求者の電子証明書の送信をその購入要求者に要求する処理がなされる。購入要求者から電子証明書の送信があれば制御がＳ５０２へ進み、購入対象のユーザ名を購入要求者に要求する処理がなされる。購入要求者から購入対象のユーザ名の送信があれば、制御がＳ５０４へ進み、送信されてきたユーザ名のユーザエージェントをＸＭＬストア５０から呼出す処理がなされる。

【０１２７】

次にＳ５０５により、そのユーザエージェントと購入依頼者とで直接交渉させる処理がなされる。この交渉は、購入要求者に対し個人情報を提供してもよいか否か、また提供するにあたってはどの程度の見返りを要求するか、またその見返り内容は金銭の支払かあるいはサービスの提供か等の交渉である。Ｓ５０６により、交渉が成立したか否かの判断がなされ、不成立の場合には、Ｓ５０７により、販売を拒否する旨を依頼者（購入要求者）に返信する処理がなされる。交渉が成立していると判断された場合には、制御がＳ５０８へ進み、ユーザ名，購入依頼者名，見返り等の販売条件，個人情報の開示許容範囲（流通許

容範囲）を含むプライバシーポリシーに対し、ユーザ，依頼者（購入要求者），金融機関７のそれぞれのデジタル署名を付して記憶する処理がなされる。次にＳ５０９により、販売が決定された金融機関７のデジタル署名を付して依頼者に返信する処理がなされる。

【０１２８】

金融機関７のデータベース１２ａに格納されている個人情報は、その金融機関によって真偽チェックがなされて正しい個人情報のみが格納されており、その正しい個人情報を業者に提供する場合やその正しい個人情報との照合結果を業者に提供する場合には、Ｓ４８６、Ｓ５０９により金融機関７のデジタル署名が付される。よって、業者が所有する個人情報のうち金融機関７のデジタル署名が付されていない個人情報については、誤りの可能性のある個人情報であり、金融機関７のデジタル署名が付されている個人情報は正しい個人情報であることが、一目瞭然でわかる。

【０１２９】

図１８は、Ｓ４０５に示されたメール転送，流通チェック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。Ｓ５１４により、サイト（業者）からメールが送られてきたか否かの判断がなされる。図４等に基づいて説明したように、ＶＰが、本名を用いてサイトにアクセスした場合にはＶＰ自身のＥメールアドレスをそのサイト側に通知するが、トラップ型ＶＰ氏名を用いてサイトにアクセスした場合には、金融機関７のトラップ型ＶＰ用として開設されているＥメールアドレスをそのサイト側に提供する。その結果、そのサイトからのＥメールは、金融機関７のトラップ型ＶＰ用に開設されたＥメールアドレスで送られてくることとなる。

【０１３０】

金融機関７では、そのトラップ型ＶＰ用に開設したＥメールアドレスに送信されてきたメールがある場合には、ＶＰ管理用サーバ９は、Ｓ５１４により、ＹＥＳの判断を行なう。その結果、制御がＳ５１５へ進み、その送られてきたＥメールに含まれている宛名に対応するサイト名（業者名）をデータベース１２ａから割出す処理を行なう。データベース１２ａは、図４に基づいて説明したように、ＶＰの氏名とそのＶＰがアクセスしたサイト名とが対応付けられて記憶されている。この対応関係を利用して、メールの宛名から対応するサイト名（業者名）を割出す処理がなされる。

【０１３１】

次にＳ５１６により、割出されたサイト名とＥメールを送ったサイト名とが一致するか否かの判断がなされる。本来なら一致する筈であるが、個人情報が不正に流通された場合には、その不正流通された個人情報を不正入手したサイトがその個人情報主にＥメールを送る場合がある。その場合には、割出されたサイト名とメールを送ったサイト名とが一致しない状態となる。

【０１３２】

割出されたサイト名とメールを送ったサイト名とが一致しない場合に、即座に個人情報が不正流通されたとは断定できない。サイト側に個人情報を提供する際に、ある一定の流通許容範囲内においては流通させてもよいと個人情報主であるユーザから承諾を得ている場合がある。よって、図１７のＳ４９４，Ｓ４９４ａで説明したのと同様に、Ｓ５２２に制御が進み、ＸＭＬストアの該当個人情報を検索して、ポリシーに定められている流通許容範囲内にＥメール送信者が含まれるか否かチェックする処理がなされ、Ｓ５２３により、含まれると判断された場合には制御がＳ５１７へ進むが、含まれないと判断された場合には制御がＳ５１９へ進む。

【０１３３】

Ｓ５１９では、Ｅメールを送ったサイト名に対応させて個人情報の不正入手値を「１」加算更新する処理がなされ、Ｓ５２０により、Ｓ５１５によって割出されたサイト名に対応させて個人情報の不正流出値を「１」加算更新する処理がなされる。次にＳ５２１により、個人情報の不正があった旨およびその詳細データを該当するユーザへ通知する処理がなされる。

【０１３４】

一方、個人情報が不正流通されていないと判断された場合には制御がＳ５１７へ進み、Ｅメールの宛名に対応するユーザのメールアドレスを割出す処理がなされ、Ｓ５１８により、その割出されたアドレスにＥメールを転送する処理がなされる。

【０１３５】

図１９は、Ｓ４０６に示された他のトラップ型ＶＰのアクセス履歴の提供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。前述したように、ＶＰがトラップ型ＶＰとしてサイトにアクセスした場合には、そのサイト側から送られてくるクッキーはそのトラップ型ＶＰのみに対応してＶＰをＩＣ端末１９Ｖに記憶される（図１１参照）。よって、トラップ型ＶＰとしてアクセスを受けたサイト側では、そのトラップ型ＶＰのみのアクセス履歴や購買履歴しか収集できず、そのトラップ型ＶＰが他のトラップ型ＶＰとしてまたはＶＰの本名を用いてネットワーク上で行動したその行動履歴（アクセス履歴等）は、何ら集計できない。このような場合において、そのサイト側から他のトラップ型ＶＰ（本名を用いたＶＰを含む）のアクセス履歴等のネットワーク上の行動履歴のデータを提供してもらいたいという依頼が、金融機関７にあった場合には、Ｓ５３０によりＹＥＳの判断がなされて制御がＳ５３１へ進み、金融機関７の電子証明書を送信する処理がなされる。

【０１３６】

次にＳ５３２により、依頼者の電子証明書の送信をその依頼者に要求する処理がなされる。電子証明書がその依頼者から送信されてきた段階でＳ５３３によりＹＥＳの判断がなされて制御がＳ５３４へ進み、提供してもらいたいユーザの氏名を依頼者に対し要求する処理がなされる。次にＳ５３５へ進み、依頼者からユーザの氏名の送信があったか否かの判断がなされ、あった場合にＳ５３６へ進み、ユーザの許可証の送信をその依頼者に要求する処理がなされる。ユーザは、トラップ型ＶＰとしてサイトにアクセスして個人情報を提供する際に、他のトラップ型ＶＰ（本名を用いたＶＰを含む）のアクセス履歴等のネットワーク上の行動履歴データも提供してよい旨の承諾を行なう場合がある。

【０１３７】

つまり、図４を参照して、たとえばＶＰがトラップ型ＶＰであるE^2（Ｂ１３Ｐ）としてサイトＭＥＣにアクセスして個人情報を提供した際に、他のトラップ型ＶＰであるＥ（Ｂ１３Ｐ）が本名Ｂ１３Ｐを用いたＶＰのアクセス履歴等のネットワーク上の行動履歴データも併せてそのサイトＭＥＣに提供してもよいことを承諾する場合がある。その場合には、ユーザは、その旨を示す電子的な許可証をそのサイトに送信する。この許可証は、ユーザのデジタル署名が付されている。Ｓ５３６の要求に応じてサイトがその許可証を送信すれば、Ｓ５３７によりＹＥＳの判断がなされ、Ｓ５３９によりその許可証が適正であるか否かの判断がなされる。適正でない場合にはＳ５４５により、アクセス履歴の提供を拒否する通知が依頼者に送信されるが、適正である場合にはＳ５４０により、送信されてきたユーザ氏名に対応する他のトラップ型ＶＰ（本名を用いたＶＰを含む）のアクセス履歴等のネットワーク上での行動履歴データを割出してその依頼者に送信する処理がなされる。

【０１３８】

一方、依頼者であるサイト側がユーザの許可証を持っていない場合には、許可証なしの返信を金融機関７に送信する。すると、Ｓ５３８によりＹＥＳの判断がなされて制御がＳ５４１へ進み、当該ユーザのユーザエージェントをＸＭＬストア５０から呼出す処理がなされ、Ｓ５４２により、そのユーザエージェントと依頼者であるサイト側とを直接交渉させる処理がなされる。

【０１３９】

次にＳ５４３により、交渉が成立したか否かの判断がなされる。交渉不成立の場合にはＳ５４５によりアクセス履歴の提供を拒否する通知が依頼者側に送信される。一方、交渉成立の場合には制御がＳ５４４へ進み、個人情報主であるユーザが無条件で許諾したか否かの判断がなされる。無条件で許諾した場合には、制御がＳ５４０へ進み、アクセス履歴等の行動履歴データを依頼者側に送信する処理がなされる。一方、ユーザが条件付きの許諾を行なった場合には、制御がＳ５４６へ進み、その条件を記憶する処理がなされた後、Ｓ５４０へ進む。Ｓ５４６による条件を記憶する際には、交渉の当事者であるユーザおよび

依頼者の名前と決定された条件とを個人情報の開示許容範囲（流通許容範囲）を含む依頼者側のプライバシーポリシーとに対し、交渉の当事者，金融機関７のそれぞれのデジタル署名を付して記憶する。

【０１４０】

図２０は、Ｓ４０７により示された信頼度ランキング情報の集計，提供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。このサブルーチンプログラムは、データベース１２ｂの記憶データに基づいてＶＰ管理サーバ９が動作するためのものである。Ｓ５５０により、各サイト（業者）毎に、Ｊ＝不正入手値＋不正流出値×２　を算出する処理がなされる。これは、個人情報を不正に入手した者よりも個人情報を不正に流出（流通）させた者の方が、悪質であり罪が重たいために、×２を行なっているのである。

【０１４１】

次にＳ５５１により、算出されたＪが大きい順に悪い順位を算出して各サイト（業者）毎にデータベース１２ｂに記憶させる処理がなされる。次にＳ５５２により、順位の公表要求があったか否かの判断がなされる。個人情報主であるユーザあるいは業者等から順位の公表要求が金融機関７のＶＰ管理サーバ９にあった場合には、制御がＳ５５３へ進み、その要求者に対し順位データを送信する処理がなされる。

【０１４２】

図２１は、図３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がブラウザフォン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ブラウザフォン３０へ送信する処理がなされる。次にＳ２７へ進み、ブラウザフォン３０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ブラウザフォン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１２ａに記憶する処理がなされてＳ２５へ戻る。

【０１４３】

図２２～図２４は、図３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。

【０１４４】

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１２ａ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。

【０１４５】

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１２ａを検索することにより確認される。

【０１４６】

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１２ａ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。
【０１４７】
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。
【０１４８】
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１２ａ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。
【０１４９】
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。
【０１５０】
図２３は、図２２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Ｓ５５４へ進み、クレジットカード発行会社からの問合せ処理が行なわれた後、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。
【０１５１】
ユーザがブラウザフォン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、氏名の入力要求をブラウザフォン３０等へ送信する処理がなされる。その要求を受けたブラウザフォン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から氏名がブラウザフォン３０へ伝送され、その伝送されてきた氏名をブラウザフォン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ブラウザフォン３０へ送信する処理がなされる。
【０１５２】
その乱数Ｒを受けたブラウザフォン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、それをブラウザフォン３０へ出力する。ブラウザフォン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、ブラウザフォン３０へ出力する。ブラウザフォン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。
【０１５３】
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DKN（Ｉ）を生成する処理がなされる。次にＳ６６へ進み、Ｒ＝DKN（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＝DKN（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DKN（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、不適正である旨をブラウザフォン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。

【０１５４】

一方、Ｒ＝DKN（Ｉ）の場合には制御がＳ６７へ進み、引落し額の入力要求をブラウザフォン３０へ送信する処理がなされ、引落し額がブラウザフォン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をブラウザフォン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。

【０１５５】

一方、ユーザがＶＰとしてＶＰ用ＩＣ端末１９Ｖへの引落しを行なう場合には、ＶＰの本名を用いる。入力された氏名がＶＰの本名であった場合には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DKP（Ｉ）を生成する処理がなされる。次にＳ８６へ進み、Ｒ＝DKP（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、不適正である旨がブラウザフォン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の入力要求をブラウザフォン３０へ送信する処理がなされ、ブラウザフォン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をブラウザフォン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。

【０１５６】

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ブラウザフォン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ブラウザフォン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。

【０１５７】

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をユーザのブラウザフォン３０に送信する処理がなされる。

【０１５８】

ユーザがＲＰまたはＶＰの本名を用いて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。

【０１５９】

Ｓ５８によりＮＯの判断がなされた場合にはＳ５５４によるクレジット発行会社４からの問合せ処理が行なわれた後Ｓ５９へ進み、その他の処理が行なわれる。

【０１６０】

図２４（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＝EKS（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。

【０１６１】

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。

【０１６２】

図２５は、Ｓ５５４に示されたクレジットカード会社からの問合せ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。前述したように、ＶＰがトラップ型ＶＰとしてサイトにアクセスして電子ショッピング等を行なってクレジット決済を行なった場合には、ＶＰ本人のクレジット番号が用いられるのではなく、そのＶＰ本人のクレジット番号を何回か秘密鍵で暗号化した暗号化クレジット番号が用いられることとなる。たとえば、図４に示すように、トラップ型ＶＰ氏名Ｅ（Ｂ１３Ｐ）としてサイトＭＰＰにアクセスしたＶＰは、電子ショッピング等を行なってクレジット決済をする際には、バーチャルクレジット番号Ｅ（３２８８）を用いる。ＶＰは、クレジットカード発行会社４に対し３２８８のクレジット番号は登録しているが、Ｅ（３２８８）の暗号化クレジット番号までは登録していない。よって、Ｅ（３２８８）のバーチャルクレジット番号がクレジット決済に伴ってクレジットカード発行会社４に送信されてきた場合には、クレジットカード発行会社４は、そのＥ（３２８８）のバーチャルクレジット番号を自社で検索して真偽を確かめることはできない。

【０１６３】

そこで、そのような場合に、クレジットカード発行会社は、金融機関７にそのバーチャルクレジット番号が正しいか否かの照会を行なってもらうのである。

【０１６４】

クレジットカード発行会社からの問合せがあれば制御はＳ５６１へ進み、Ｓ５６１～Ｓ５６８の前述したものと同様の認証処理が行なわれる。認証の結果本人が確認されればＳ５６７によりＹＥＳの判断がなされてＳ５６９へ進み、照会対象データの入力要求がクレジットカード発行会社に送信される。この照会対象データとは、前述したバーチャルクレジット番号とトラップ型ＶＰ氏名とを含む。このトラップ型ＶＰ氏名をも入力されることにより、そのトラップ型ＶＰ氏名とバーチャルクレジット番号とが対応しているか否か等も照会できる。

【０１６５】

照会対象データがクレジットカード発行会社から送信されてくれば制御はＳ５７１へ進み、データベース１２ａを検索してその送信されてきた照会対象データと照合する処理がなされる。次にＳ５７２により、照合結果送られてきた照会対象データが適正であるか否かの判断がなされ、適正な場合にＳ５７３により、適正な旨をクレジットカード発行会社へ返信し、照合結果適正でない場合にはＳ５７４により、不適正な旨がクレジットカード発行会社に返信される。Ｓ５７３による適正な旨を返信する際には、Ｓ５７０により入力された照会対象データに対し適正な旨を表わす金融機関７側のデジタル署名を付し、そのデ

ジタル署名付きデータが問合せをしたクレジットカード発行会社４へ返信されることとなる。

【０１６６】

図２６～図３１，図３３～図３６は、ブラウザフォン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。ブラウザフォン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未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は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、制御はＳ９９へ進み、ＩＣ端末未使用の警告表示がなされた後Ｓ９５へ戻る。

【０１６７】

一方、ＶＰ用ＩＣ端末１９Ｖが接続されている場合には、制御は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２７に基づいて後述する。ブラウザフォン３０は、サイト側から送られてきたクッキーデータを記憶するための記憶領域を有していない。ゆえに、サイト側から送られてきたクッキーデータであって記憶する必要のあるものは、すべてＶＰ用ＩＣ端末１９ＶまたはＲＰ用ＩＣ端末１９Ｒに記憶される。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２９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３１（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３３に基づいて説明する。

【０１６８】

次に制御がＳ５８０へ進み、個人情報の登録処理がなされる。この個人情報の登録処理は、図１３（ｂ）に示したＶＰ管理サーバ９の登録処理に対応するブラウザフォン３０側の処理である。まずＶＰとしての本人認証処理を行ない、ＶＰ管理サーバ９が本人認証の確認を行なったことを条件として、ＶＰの個人情報を金融機関７のＶＰ管理サーバ９へ送信してデータベース１２ａに登録してもらう処理を行なう。

【０１６９】

次に制御がＳ５８２へ進み、個人情報の確認処理がなされる。この処理は、金融機関７のＶＰ管理サーバ９により図１５に示された確認処理に対応してブラウザフォン３０によりなされる処理である。まずＶＰとしての本人認証がなされ、次に、データベース１２ａに格納されている自分の個人情報の確認を行なう処理がなされる。一方、確認の結果誤りがある場合あるいは引越しや転職等によって個人情報に変更があった場合には、このＳ５８２により、その変更情報が、金融機関７のＶＰ管理サーバ９へ送信される。

【０１７０】

次に制御がＳ５８３へ進み、ＶＰ用Ｗｅｂブラウザ，メール処理がなされる。この処理は、図３６（ａ）に基づいて後述する。次に制御がＳ５８５へ進み、住所，氏名，Ｅメールアドレスの送信処理が行なわれる。一方、ブラウザフォン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２８（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３０（ｂ）に基づいて後述する。次に制御が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３１（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。次に制御がＳ５８４へ進み、偽ＲＰアクセス処理がなされる。この偽ＲＰアクセス処理は、図３６（ｂ）に基づいて後述する。

【０１７１】

図２７は、Ｓ１０２により示された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Ｓ１２０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。ユーザがブラウザフォン３０のキーボード７７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）がブラウザフォン３０によりなされる。

【０１７２】

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Ｓ１１９へ進み、Ｗｅｂ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Ｓ５９０へ進み、そのサイトにトラップ型ＶＰを既に使用しているか否かを、ＶＰ用ＩＣ端末１９Ｖに問う処理がなされる。ＶＰ用ＩＣ端末１９Ｖは、図１１に基づいて説明したように、クッキーデータの記憶領域に、アクセスしたサイト名とそれに用いたＶＰ氏名とを記憶している。ＶＰ用ＩＣ端末では、ブラウザフォン３０から問合せがあったサイトにトラップ型ＶＰを使用しているか否かを、このクッキーデータ記憶領域を検索して割出す。そしてその回答をブラウザフォン３０へ返信する。すると、制御はＳ５９２へ進み、その回答がトラップ型ＶＰを使用済みという内容であるか否かの判断がなされる。使用済みであるとの回答内容であった場合には、制御はＳ５９３へ進み、使用しているトラップ型ＶＰとそれに対応するクッキーとをＶＰ用ＩＣ端末のクッキーデータ記憶領域から呼出し、その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。

【０１７３】

次に制御がＳ５９４へ進み、アクセスした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、送信されてき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。一方、クッキーデータとともにサイトへアクセスしたとしても、そのサイトの別のページをアクセスした際にさらに別のクッキーがサイト側から送られてくる場合がある。そのようなクッキーが送られてきた場合には、Ｓ５９４によりＹＥＳの判断がなされて制御がＳ５９５へ進み、トラップ型ＶＰ氏名と送られてきたクッキーデータとをＶＰ用ＩＣ端末へ転送する処理がなされる。ＶＰ用ＩＣ端末では、伝送されてきたクッキーデータを伝送されてきたトラップ型ＶＰ氏名に対応させて記憶させる処理が行なわれる。

【０１７４】

Ｓ５９２により、トラップ型ＶＰがまだ使用されていないサイトであると判断された場合には、制御がＳ５９６へ進み、トラップ型ＶＰの使用の有無をユーザに尋ねる処理が行なわれる。具体的には、ブラウザフォン３０の表示部７６に、「トラップ型ＶＰを使用しますか？」の表示を行なう。

【０１７５】

次にＳ５９７により、使用する旨の操作がキーボード７７から入力されたか否かの判断がなされる。使用しない旨の操作が行なわれた場合には制御がＳ１２１へ進むが、使用する旨の操作が行なわれた場合には、制御がＳ５９８へ進み、ＶＰ用ＩＣ端末１９Ｖへ新たなトラップ型ＶＰの生成を要求する処理がなされる。このＳ５９８の処理は、Ｓ１１９によりアクセス操作がされたサイト名とトラップ型ＶＰの生成を要求する指令とを、ＶＰ用ＩＣ端末１９Ｖへ伝送するものである。

【０１７６】

ＶＰ用ＩＣ端末では、その要求を受ければ、クッキーデータ領域に記憶されているＶＰ氏名の最後のもの（図１１ではＥ[3]（Ｂ１３Ｐ）が何回暗号化されているかを判別し（図１１では３回）、その暗号化回数よりも１つ多い暗号化回数（図１１では４回）ＶＰ氏名の本名（Ｂ１３Ｐ）を暗号化して新たなトラップ型ＶＰ氏名Ｅ[4]（Ｂ１３Ｐ）を生成する。そしてその生成された新たなトラップ型ＶＰをブラウザフォン３０へ出力する。すると、Ｓ５９９によりＹＥＳの判断がなされてＳ６００へ進み、ＶＰ用ＩＣ端末から送られてきたトラップ型ＶＰの氏名を用いてサイトへアクセスする処理がなされる。よって、サイト側から氏名を要求されれば、その新たなトラップ型ＶＰ氏名Ｅ[4]（Ｂ１３Ｐ）を伝送する。ただし、住所はＢ１３Ｐの住所すなわち、ＶＰ本人のコンビニエンスストアの住所を伝送する。またＥメールアドレスは、金融機関７がトラップ型ＶＰ用として開設しているＥメールアドレスである△△△△△を伝送する。

【０１７７】

次に制御がＳ５８１へ進み、トラップ情報の登録処理がなされる。このトラップ情報の登録処理は、Ｓ５９８に従って新たなトラップ型ＶＰが生成されたために、その新たに生成されたトラップ型ＶＰをデータベース１２ａに登録してもらうために金融機関７のＶＰ管理サーバ９へ送信するための処理である。この処理は、たとえば後述するＳ１４３～Ｓ１４５，Ｓ１５０～Ｓ１５２，Ｓ１６０～Ｓ１６３と同様のセキュリティのためのチェック処理を行ない、その後新たに生成されたトラップ型ＶＰのデータすなわちトラップ型ＶＰ氏名，そのトラップ型ＶＰ氏名を用いるサイト名，公開鍵，バーチャル口座番号，バーチャルクレジット番号を送信する処理である。

【０１７８】

次に制御がＳ６０１へ進み、サイト側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。送信されてきた場合には制御がＳ６０２へ進み、そのサイトに使用しているトラップ型ＶＰ氏名と送られてきたクッキーデータとをＶＰ用ＩＣ端末へ伝送する処理がなされる。ＶＰ用ＩＣ端末では、その伝送されてきたクッキーデータを伝送されてきたトラップ型ＶＰ氏名に対応する領域に記憶させる処理を行なう。

【０１７９】

Ｓ５９７により、トラップ型ＶＰを使用しない旨の操作がなされたと判断された場合には制御がＳ１２１へ進み、ＶＰ用ＩＣ端末からＶＰ用のクッキーすなわちＶＰの本名（図１１ではＢ１３Ｐ）に対応して記憶されているクッキー（図１１ではａｂｃ，ｈｉｊ，ａｍｚ，ｒａｋ…）を呼出し、それら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。

【０１８０】

この場合には、そのアクセスしたサイトでは、ＶＰ本名を用いることとなる。次に制御がＳ１２２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。サイト側からクッキーが送信されてくれば、制御がＳ１２３へ進み、その送信されてきたクッキーをＶＰ用ＩＣ端末１９Ｖへ伝送する処理がなされる。ＶＰ用ＩＣ端末１９Ｖでは、クッキーデータが単独で伝送されてくれば、自動的にＶＰ本名に対応する記憶領域にその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。

【０１８１】

図２８（ａ）は、Ｓ５８５により示された住所，氏名，Ｅメールアドレスの送信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。Ｓ７００により、サイト側から住所，氏名，Ｅメールアドレスの送信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。あった場合には制御がＳ７０１へ進み、そのサイトに使用しているＶＰの氏名，住所，Ｅメールアドレスを送信する処理がなされる。たとえば図１１に示す例の場合には、サイトＭＴＴに使用しているＶＰ氏名はＥ（Ｂ１３Ｐ）であるために、この氏名Ｅ（Ｂ１３Ｐ）を送信する。住所は、Ｂ１３Ｐの住所すなわち□△○である（図３参照）。Ｅメールアドレスは、金融機関７がトラップ型ＶＰ用として開設しているＥメールアドレス△△△△△が送信される。

【０１８２】

このＶＰ用のクッキー処理と住所，氏名，Ｅメールアドレスの送信処理とが行なわれた結果、あるサイトにトラップ型ＶＰとしてアクセスした場合には以降そのサイトにアクセスした際自動的に前回のトラップ型ＶＰ氏名が用いられて前回のトラップ型ＶＰとしてアクセスする状態となる。またサイト側から送られてくるクッキーデータも、そのサイトに対応するトラップ型ＶＰ氏名に付着する状態となる。具体的には、図１１を参照して、サイトＭＴＴにトラップ型ＶＰ氏名Ｅ（Ｂ１３Ｐ）を使用して一旦アクセスすれば、それ以降においては、ＭＴＴにアクセスする場合には必ずこのトラップ型ＶＰ氏名Ｅ（Ｂ１３Ｐ）が用いられ、その際には、前回ＭＴＴから送られてきたクッキーｍｔｔとともにＭＴＴにアクセスすることとなる。一方、ＶＰがその本名Ｂ１３Ｐを用いてＭＴＴにアクセスすることはできない。このようなアクセスを行なおうとした場合には、Ｓ５９２によりＹＥＳの判断がなされてＳ５９３により、自動的にＥ（Ｂ１３Ｐ）としてＭＴＴにアクセスする状態となる。

【０１８３】

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。

【０１８４】

しかも、トラップ型ＶＰ氏名を利用することにより、前述したように、個人情報の不正流出等をチェックすることが可能となる。

【０１８５】

図２８（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）。

【０１８６】

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、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（この場合にはトラッキング型クッキー）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（トラッキング型クッキー）をすべて拒絶し、そのクッキーがＲＰ用ＩＣ端末１９Ｒに記録されてしまうことが防止できる。

【０１８７】

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、トラッキング型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。

【０１８８】

図２９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。ユーザがブラウザフォン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３０（ａ）にそのサブルーチンプログラムが示されている。

【０１８９】

先に、図３０（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２４（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２４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２４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をブラウザフォン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DKP（Ｌ）を算出する処理が行なわれる。

【０１９０】

そして、図２９のＳ１４４へ進み、Ｒ＝DKP（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＝DKP（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ブラウザフォン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。

【０１９１】

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，住所の入力要求をブラウザフォン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。

【０１９２】

Ｓ１４７では、ＲＰの氏名，住所の入力指示をブラウザフォン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。

【０１９３】

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３４（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３４（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。

【０１９４】

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。

【０１９５】

図２９に示すＶＰ出生依頼処理を行なう場合には、ブラウザフォン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。

【０１９６】

その結果、図２９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。

【０１９７】

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２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２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２がある場合には、そのコンビニエンスストア２を特定する情報をブラウザフォン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２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２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２の住所が出生したＶＰの住所となる。

【０１９８】

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（Ｓ３０参照）。その送信要求をブラウザフォン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。

【０１９９】

図３０（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。ユーザがブラウザフォン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、ブラウザフォン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がブラウザフォン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。

【０２００】

図３１（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３１（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。

【０２０１】

ＶＰ用入力処理が行なわれる場合には、ブラウザフォン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２の住所），コンビニエンスストア２の名称，Ｅメールアドレス，電子証明書が記憶されたＩＣ端末１９Ｉが郵送されてくるのであり、そのＩＣ端末１９Ｉをユーザがブラウザフォン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ＩＣ端末１９Ｉ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。

【０２０２】

ユーザがブラウザフォン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。

【０２０３】

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がブラウザフォン３０へ送信されてくる（Ｓ６９参照）。その引落し額Ｇがブラウザフォン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。

【０２０４】

ＲＰ用入力処理が行なわれる場合には、ブラウザフォン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ブラウザフォン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。

【０２０５】

ユーザがブラウザフォン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。

【０２０６】

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からユーザのブラウザフォン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。

【０２０７】

図３２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。

【０２０８】

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。

【０２０９】

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。

【０２１０】

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。

【０２１１】

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。

【０２１２】

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。

【０２１３】

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。

【０２１４】

図３３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。

【０２１５】

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。

【０２１６】

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３０（ａ）参照）が行なわれる。

【０２１７】

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３４（ａ）参照）がなされる。

【０２１８】

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ブラウザフォン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。

【０２１９】

Ｓ２０６では、引落し額の入力指示をブラウザフォン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。

【０２２０】

Ｓ１９６により、ＮＯの判断がなされた場合には、図３４（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３０（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ブラウザフォン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ブラウザフォン３０の表示部７６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。

【０２２１】

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。

【０２２２】

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をブラウザフォン３０に返信する処理を行なう（Ｓ７４）。

【０２２３】

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ブラウザフォン３０の表示部７６に表示させる処理がなされる。

【０２２４】

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。ユーザがブラウザフォン３０のキーボード７７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３０（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ブラウザフォン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を顧客のブラウザフォン３０へ送信する。

【０２２５】

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。

【０２２６】

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とクレジットカードを使用するＶＰ氏名とを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。

【０２２７】

クレジットカードを使用するＶＰ氏名と署名指示と電子証明書の出力要求を受けたＶＰ用ＩＣ端末１９Ｖは、入力されたＶＰ氏名をクッキーデータ記憶領域と照合してそのＶＰ氏名がＶＰの本名Ｂ１３Ｐ（図１１参照）を何回暗号化したものかを割出す。そしてその回数だけ秘密鍵を秘密鍵で暗号化して、その暗号化秘密鍵（ＫＳ）を用いて入力されたＭＤを復号化していわゆる二重署名を生成する。この二重署名を便宜上$D_{(KS)}$（ＭＤ）と表現する。ＶＰ用ＩＣ端末１９Ｖは、その$D_{(KS)}$（ＭＤ）をブラウザフォン３０へ出力する。

【０２２８】

Ｓ２４４に従って入力されたＶＰ氏名がＶＰの本名Ｂ１３Ｐであった場合には、ＶＰ用ＩＣ端末１９Ｖは、その本名に対する電子証明書を格納しているために、その格納している電子証明書をブラウザフォン３０へ出力する。一方、Ｓ２４４に従って入力されたＶＰ氏

名がトラップ型ＶＰ氏名であった場合には、ＶＰ用ＩＣ端末１９Ｖがそのトラップ型ＶＰ氏名用の電子証明書を格納していない。そのトラップ型ＶＰ氏名用の電子証明書は、前述したようにＸＭＬストア５０に格納されている。よって、その場合には、ＶＰ用ＩＣ端末１９Ｖは、ＸＭＬストア５０に電子証明書を取寄せる旨の指示をブラウザフォン３０へ出力する。

【０２２９】

Ｓ２４４の要求をＶＰ用ＩＣ端末１９Ｖへ出力した後、ＶＰ用ＩＣ端末１９Ｖから何らかの返信があれば、Ｓ２４５によりＹＥＳの判断がなされてＳ６０５へ制御が進む。Ｓ６０５では、ＸＭＬストア５０への電子証明書の取り寄せ指示であったか否かの判断がなされ、取り寄せ指示でなかった場合にはＳ２４６へ進むが、取り寄せ指示であった場合には制御がＳ６０６へ進む。Ｓ６０６では、ＸＭＬストア５０へアクセスしてトラップ型ＶＰ氏名に対応する電子証明書を検索して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ブラウザフォン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。

【０２３０】

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ブラウザフォン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。

【０２３１】

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ブラウザフォン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。

【０２３２】

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。

【０２３３】

図３６（ａ）は、Ｓ５８に示したＶＰ用Ｗｅｂブラウザ，メール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。Ｓ６０７により、サイトへのアクセス要求があったか否かの判断がなされる。ない場合にはメールの送信要求があったか否かの判断がなされる。ない場合にはこのサブルーチンプログラムが終了する。

【０２３４】

ユーザがブラウザフォン３０のキーボード７７を操作してサイトへアクセスする操作を行なった場合にはＳ６０７によりＹＥＳの判断がなされて制御がＳ６０８へ進む。Ｓ６０８では、ブルートゥース（Bluetooth）が使用できる端末が近くにあるか否かの判断がなされる。ブルートゥースは、１０メートル程度の近距離無線通信インターフェイスのコード名であり、ブラウザフォン３０に標準装備されている。このＳ６０８により、１０メートル四方に広域・大容量中継網４３に接続されてブルートゥースが使用できる端末がない場合には、制御がＳ６１２へ進み、アクセスできない旨をブラウザフォン３０の表示部７６に表示する処理がなされる。一方、ブルートゥースが使用できる端末がある場合にはＳ６０９へ進み、ブルートゥースを用いてその端末経由でサイトにアクセスする処理がなされる。

【０２３５】

このように、ブラウザフォン３０にＶＰ用ＩＣ端末１９Ｖを接続してＶＰとしてブラウザフォン３０からサイトにアクセスする場合には、携帯電話用の基地局５５，携帯電話網４

５，ゲートウェイ５３経由でサイトにアクセスするのでなく、広域・大容量中継網に接続された端末経由でアクセスする。その理由は、ブラウザフォン３０が発信している電波を手掛かりにその現在位置が割出されるおそれがあるためである。ブラウザフォン３０の場合には、ブラウザフォン３０同士の通話を実現するために、ブラウザフォン３０が位置する一番近い基地局５５を割出してその基地局５５から通話電波を発信するようにしているために、ブラウザフォン３０の位置情報が特定できるように構成されている。このような位置がある程度割出し可能なブラウザフォン３０を利用して、ＲＰとしてそのブラウザフォン３０を利用したり、あるいはＶＰとしてサイトにアクセスしたりした場合には、あるＲＰとあるＶＰとが常に同じ位置に存在することが統計上突き止められてしまい、そのＲＰとそのＶＰとは同一人物ではないかと、見破られてしまうおそれがある。

【０２３６】

そこで、ＶＰとしてブラウザフォン３０を利用してネットワーク上で行動する場合には、携帯電話網５４を利用することなくブルートゥースを利用して広域・大容量中継網４３に接続されている端末経由でネットワーク内に入り込むようにしているのである。

【０２３７】

一方、ユーザがブラウザフォン３０のキーボード７７を操作してＥメールの送受信要求を行なった場合には、Ｓ６１０によりＹＥＳの判断がなされて制御がＳ６１１へ進み、ブルートゥースが使用できる端末が近くにあるか否かの判断がなされる。ない場合にはＳ６１１ａに進み、Ｅメールの送受信ができない旨を表示部７６に表示させる制御を行なった後、このサブルーチンプログラムが終了する。一方、近くにブルートゥースが使用できる端末があった場合には制御がＳ６１３へ進み、ブルートゥースを用いてその端末経由でＥメールの送受信を行なう処理がなされる。

【０２３８】

図３６（ｂ）は、Ｓ５８４に示された偽ＲＰアクセス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。ユーザがＶＰとしてネットワーク上で行動することが多くなれば、ＲＰとＶＰとの両方の詳しい個人情報を収集した業者が、両個人情報を虱潰しにマッチングチェックして、両個人情報が一致するＲＰ氏名とＶＰ氏名とを割出し、ＶＰに対応するＲＰの名前を予測してしまうという不都合が生ずるおそれがある。その１つの解決方法として、ＲＰの個人情報の信頼性を低下させることが考えられる。その偽ＲＰアクセス処理は、ＲＰの氏名を名乗ってランダムにサイトを次から次へとアクセスして渡り歩く動作を自動的に行なうものである。

【０２３９】

Ｓ６５０により偽ＲＰアクセス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。ユーザがブラウザフォン３０のキーボード７７を操作して偽ＲＰアクセス要求を行なえば、制御がＳ６５１へ進み、乱数Ｒを発生させる処理がなされる。次にＳ６５２により、その乱数ＲからＵＲＬ（Uniform Resource Locator）を作成する処理がなされる。次にＳ６５３により、そのＵＲＬへアクセスを試みる処理がなされる。次にＳ６５４により、そのアクセスが成功したか否かの判断がなされる。このＵＲＬは乱数によってランダムに生成されたものであるために、そのＵＲＬに必ず該当するサイトがあるとは限らない。よって、該当するサイトがなければＳ６５４によりＮＯの判断がなされて制御が再びＳ６５１へ戻り、Ｓ６５１～Ｓ６５３の処理を繰返す。

【０２４０】

このＳ５６１～Ｓ５６４のループを巡回することによって、ランダムに生成されたＵＲＬに該当するサイトがあった場合には、Ｓ６５４によりＹＥＳの判断がなされてＳ６５５へ進み、アクセスしようとしているサイトが予め設定されたアクセス許容範囲内のものであるか否かの判断がなされる。ユーザは、たとえば、ＲＰ用ＩＣ端末１９Ｒに格納されているユーザエージェントに対し、アクセスを行なってもよい許容範囲を入力設定しておく。たとえば風俗営業関連のサイト以外を許容する等のように、アクセス許容範囲を入力設定しておく。Ｓ６５５では、ブラウザフォン３０に接続されているＲＰ用ＩＣ端末１９Ｒに格納されているユーザエージェントに対し、アクセスしようとしているサイトがその予め

入力設定されたアクセス許容範囲内のものであるか否かを問合せる処理を行なう。アクセス許容範囲内でない場合には制御が再びＳ６５１へ戻り、再度乱数によるＵＲＬの生成およびそのＵＲＬへのアクセスが試みられる。

【０２４１】

Ｓ６５５によりアクセス許容範囲内であると判断された場合には、制御がＳ６６２へ進み、ＲＰ用ＩＣ端末１９Ｒからクッキーを呼出して、その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。

【０２４２】

次に制御がＳ６５６へ進み、そのサイトにアクセスするとともにそのサイト内でランダムに行動し、かつ、極力ＲＰの住所，氏名および偽の嗜好情報等をそのサイト側に提供する処理がなされる。この処理は、ブラウザフォン３０に接続されているＲＰ用ＩＣ端末１９Ｒ内のユーザエージェントと協働で行なわれる。次に制御がＳ６６０へ進み、サイト側からクッキーの送信があったか否かの判断がなされる。ない場合にはＳ６５７へ制御が進むが、あった場合にはＳ６６１へ制御が進み、その送信されてきたクッキーをＲＰ用ＩＣ端末１９Ｒに記憶させる処理がなされた後Ｓ６５７へ進む。

【０２４３】

次にＳ６５７により、そのサイトのアクセスを終了させる処理がなされ、Ｓ６５８により、所定時間経過したか否かの判断がなされ、未だ所定時間経過していない場合には再びＳ６５１へ戻るが、所定時間経過したと判断された場合にはこのサブルーチンプログラムが終了する。

【０２４４】

図３７（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。次にＳ６１５により、トラップ型ＶＰ処理がなされる。この処理は、図４１に基づいて後述する。

【０２４５】

図３７（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。

【０２４６】

図３８（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、不適正な旨をブラウザフォン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。

【０２４７】

図３８（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。ブラウザフォン３０にＶＰ用ＩＣ端末１９Ｖが接続された時点で、そのブラウザフォン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、ブラウザフォン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ＶＰ氏名に対応するクッキー記憶領域に記憶する処理を行なう。

【０２４８】

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。ブラウザフォン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、ＶＰ氏名に対応するクッキー記憶領域に記憶しているクッキーデータと必要に応じてトラップ型ＶＰ氏名とをブラウザフォン３０に出力する処理がなされる。

【０２４９】

図３８（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をブラウザフォン３０へ出力する処理がなされる。

【０２５０】

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をブラウザフォン３０へ出力する処理がなされる。

【０２５１】

図３８（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をブラウザフォン３０へ出力する処理がなされる。

【０２５２】

図３９（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。

【０２５３】

図３９（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。

【０２５４】
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４０に基づいて後述する。
【０２５５】
図３９（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。
【０２５６】
図３９（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ＤKS（ＭＤ）を出力する処理がなされる。
【０２５７】
図３９（ｅ）は、Ｓ２５９により示されたＶＰ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。Ｓ９９９により、メッセージダイジェストＭＤとＶＰ氏名との入力がブラウザフォン３０から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。
【０２５８】
ＭＤとＶＰ氏名との入力があった場合には制御がＳ９９８へ進み、その入力されたＶＰ氏名から秘密鍵（ＫＳ）を生成する処理がなされる。具体的には、ＶＰ用ＩＣ端末１９Ｖは、入力されたＶＰ氏名に基づいてクッキーデータ記憶領域を検索してその入力されたＶＰ氏名が本名Ｂ１３Ｐ（図１１参照）を何回暗号化したものであるかを割出す。その割出された暗号化回数だけＶＰの秘密鍵をＶＰの秘密鍵で暗号化して秘密鍵（ＫＳ）を生成する。
【０２５９】
次に制御がＳ９９７へ進み、その秘密鍵（ＫＳ）を用いてメッセージダイジェストＭＤを復号化して二重署名を生成する処理がなされる。次に制御がＳ９９８へ進み、その二重署名$D_{(KS)}$（ＭＤ）をブラウザフォン３０へ出力する処理がなされる。
【０２６０】
図４０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１０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。なお、ＶＰの住所、氏名、Ｅメールアドレスに関しては、Ｓ７００，Ｓ７０１で処理する。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。
【０２６１】
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。

【０２６２】

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。

【０２６３】

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。

【０２６４】

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ブラウザフォン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。

【０２６５】

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。

【０２６６】

図４１は、Ｓ６１５により示されたトラップ型ＶＰ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。Ｓ６２０により、新たなトラップ型ＶＰの生成要求があったか否かの判断がなされ、ない場合にはＳ６２３へ進み、トラップ型ＶＰが使用済みであるか否かの問合せ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。

【０２６７】

ブラウザフォン３０がＳ５９８に従ってＶＰ用ＩＣ端末１９Ｖに新たなトラップ型ＶＰの生成要求を出した場合には、Ｓ６２０によりＹＥＳの判断がなされて制御がＳ６２１へ進む。Ｓ６２１では、ＶＰ用ＩＣ端末１９Ｖのクッキーデータ領域の最後のＶＰ氏名の暗号回数ｎを「１」加算して、ＶＰの本名をｎ＋１回秘密鍵で暗号化して新たなトラップ型ＶＰ氏名を生成する処理がなされる。たとえば図１１の場合には、クッキーデータ領域の最後のＶＰ氏名E^3（Ｂ１３Ｐ）の暗号回数が３回であり、これに「１」加算して暗号回数４にし、ＶＰの本名Ｂ１３Ｐを４回暗号化して新たなトラップ型ＶＰ氏名E^4（Ｂ１３Ｐ）を生成する処理がなされる。

【０２６８】

次にＳ６２２へ進み、その生成されたトラップ型ＶＰを、ブラウザフォン３０へ出力するとともに、クッキーデータ領域における最後のＶＰ氏名の次の空き領域に記憶させる処理がなされる。

【０２６９】
Ｓ５９０に従ってブラウザフォン３０がＶＰ用ＩＣ端末１９Ｖに対し今アクセスしようとしているサイトにトラップ型ＶＰが既に使用されているか否かの問合せを行なった場合には、Ｓ６２３によりＹＥＳの判断がなされて制御がＳ６２４へ進む。この問合せの際にはブラウザフォン３０はＶＰ用ＩＣ端末１９Ｖに対し、今アクセスしようとしているサイト名も併せて伝送する。Ｓ６２４では、クッキーデータ領域（図１１参照）を検索する処理がなされる。制御がＳ６２５へ進み、伝送されてきたサイト名に対しトラップ型ＶＰ氏名が使用済みであるか否かの判断がなされる。たとえばブラウザフォン３０から伝送されてきたサイト名がＭＥＣであった場合には、図１１を参照して、トラップ型ＶＰ氏名E^2（Ｂ１３Ｐ）が使用済みであることがわかる。

【０２７０】
トラップ型ＶＰ氏名が使用済みであると判断された場合には制御がＳ６２６へ進み、使用済みである旨をブラウザフォン３０へ出力するとともに、Ｓ６２７により、使用されているトラップ型ＶＰとそれに対応するクッキーデータとをブラウザフォン３０へ出力する処理がなされる。たとえば、図１１の場合には、伝送されてきたサイト名がＭＥＣであった場合には、トラップ型ＶＰとしてE^2（Ｂ１３Ｐ）がブラウザフォン３０へ出力されるとともに、クッキーデータｍｅｃがブラウザフォン３０へ出力される。

【０２７１】
図１１のクッキーデータ領域を検索した結果、ブラウザフォン３０から伝送されてきたサイト名に対しトラップ型ＶＰが未だ使用されていない場合にはＳ６２５によりＮＯの判断がなされて制御がＳ６２８へ進み、未使用の旨をブラウザフォン３０へ出力する処理がなされる。

【０２７２】
図４２，図４３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。

【０２７３】
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。

【０２７４】
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。

【０２７５】
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２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。

【０２７６】

ユーザがＶＰとしてコンビニエンスストア２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を端末７３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、端末７３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。

【０２７７】

差込まれているＶＰ用ＩＣ端末１９Ｖは、前述したように、ＶＰ本名に対する電子証明書は格納しているものの、トラップ型ＶＰに対する電子証明書は格納しておらず、そのトラップ型ＶＰに対する電子証明書はＸＭＬストア５０に格納されている。ＶＰ本名を用いて電子ショッピング等を行なってその購入商品がコンビニエンスストア２へ届けられた場合には、Ｓ３２７に従って呼出されたＶＰ氏名はＶＰの本名となる。その場合には、Ｓ３３０の要求に従ってＶＰ用ＩＣ端末１９Ｖは電子証明書を出力することができる。その場合にＳ３３１によりＹＥＳの判断がなされて制御がＳ３３２へ進む。一方、トラップ型ＶＰ氏名を用いて電子ショッピングを行ないその購入商品がコンビニエンスストア２へ届けられた場合には、その商品をトラップ型ＶＰとしてコンビニエンスストア２へ引取りに行くこととなる。その場合には、Ｓ３２７によってＶＰ用ＩＣ端末１９Ｖから呼出されるＶＰ氏名は、トラップ型ＶＰ氏名となる。その結果、そのトラップ型ＶＰ氏名に対応する電子証明書の出力要求がＳ３３０からＶＰ用ＩＣ端末１９Ｖに対し出される。その場合には、ＶＰ用ＩＣ端末１９Ｖは、ＸＭＬストア５０から電子証明書を取り寄せる旨の指示を出力する。

【０２７８】

その出力があれば、制御がＳ６３１へ進み、ＸＭＬストア５０へアクセスして該当する電子証明書を取り寄せる処理がなされた後制御がＳ３３２へ進む。

【０２７９】

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。

【０２８０】

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。

【０２８１】

Ｓ３２６の暗証番号チェック処理は、図４３（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。

【０２８２】

Ｓ３３３の本人チェック処理は、図４３（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。

【０２８３】

Ｓ３３８の決済処理は、図４３（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。

【０２８４】

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。

【０２８５】

次に、別実施の形態を説明する。この別実施の形態は、ブラウザフォン３０やユーザのパーソナルコンピュータ等のユーザ側端末およびＩＣ端末１９およびＷｅｂサイトによって、個人情報保護のシステムが完結する簡易型システムである。前述した実施の形態との相違は、トラップ型ＶＰのＥメールアドレスがＶＰ本名のＥメールアドレスと同じである。よって、トラップ型ＶＰ宛のＥメールを金融機関７が転送する必要がない。またトラップ型ＶＰの氏名は、そのトラップ型ＶＰがアクセスするサイトの名称を、ＶＰ本名に用いられる秘密鍵で暗号化したものを用いる。トラップ型ＶＰの口座番号やクレジット番号も、ＶＰが本名として用いる口座番号，クレジット番号と同じものを用いる。

【０２８６】

図４４（ａ）は、ＶＰ用ＩＣ端末１９ＶのＥＥＰＲＯＭ２６のクッキー記憶領域に格納されている情報を示す図である。このクッキー記憶領域には、ＶＰ氏名として、ＶＰの本名Ｂ１３Ｐのみが記憶され、トラップ型ＶＰ氏名は何ら記憶されない。トラップ型ＶＰの氏名は、トラップ型ＶＰとしてアクセスしたサイトを本名のＶＰの秘密鍵ＫＳＢで暗号化したものを用いる。この暗号化回数は１回に限らず２回以上の或る定められた回数であってもよい。よって、トラップ型ＶＰがアクセスしたサイト名のみを記憶させることにより、そのサイト名に対応するトラップ型ＶＰの氏名は、わざわざ記憶させなくとも、E_{KSB}（サイト名）の演算式に従って必要に応じてその都度算出することができる。トラップ型ＶＰの秘密鍵は、トラップ型ＶＰに対応するサイト名を本名のＶＰの秘密鍵ＫＳＢで復号化したものを用いる。よって、トラップ型ＶＰに対応させて逐一公開鍵や秘密鍵をＶＰ用ＩＣ端末１９Ｖに記憶させる必要はなく、秘密鍵＝D_{KSB}（サイト名）の演算式に従って必要に応じてその都度算出することができる。よって、ＸＭＬストア５０の「暗号回数」の記憶が不要となる。

【０２８７】

図４４（ｂ）は、トラップ型ＶＰ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。このサブルーチンプログラムは、図４１に示したトラップ型ＶＰ処理の別実施の形

態である。Ｓ９６０により、新たなトラップ型ＶＰの生成要求がブラウザフォン３０からあったか否かの判断がなされ、あった場合には制御がＳ９５９へ進み、アクセスするサイトの名称の入力要求がブラウザフォン３０へ出される。ブラウザフォン３０からアクセスするサイトの名称が伝送されてくれば、制御がＳ９５７へ進み、その伝送されてきたサイト名をＶＰの本名Ｂ１３Ｐの秘密鍵ＫＳＢで暗号化して、新たなトラップ型ＶＰ氏名であるE_{KSB}（サイト名）を算出する処理がなされる。次に制御がＳ９５６へ進み、その算出した新たなトラップ型ＶＰ氏名をブラウザフォン３０へ出力する処理がなされ、Ｓ９５４により、入力されたサイト名をクッキー記憶領域に記憶させる処理がなされる。

【０２８８】

Ｓ９５３～Ｓ９４８は、図４１に示したＳ６２３～Ｓ６２８と同じ制御のために、説明の繰返しを省略する。

【０２８９】

図４４（ｃ）は、ＶＰ用ＩＣ端末１９Ｖによって行なわれる個人情報流通チェック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。Ｓ９７０により、Ｅメールの受信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。トラップ型ＶＰ宛のＥメールの受信があれば、ブラウザフォン３０は、そのＥメールデータをＶＰ用ＩＣ端末へ入力する。すると制御がＳ９６９へ進み、その入力されたＥメールの宛名をＶＰの本名に用いられる公開鍵ＫＰＢで復号化するD_{KPB}（宛名）の演算を行ない、その演算結果がＥメールの送信者名と一致するか否かの判断がなされる。

【０２９０】

Ｅメールの宛名はトラップ型ＶＰ氏名となっており、そのトラップ型ＶＰ氏名は、そのトラップ型ＶＰがアクセスしたサイト名をＶＰの秘密鍵ＫＳＢで暗号化したものを用いている。よって、トラップ型ＶＰがその氏名を用いてアクセスしたサイトからそのトラップ型ＶＰ宛にＥメールが送信された場合には、Ｓ９６９によりＹＥＳの判断がなされる筈である。その場合には、Ｓ９６８により、適正である旨がブラウザフォン３０へ出力され、ブラウザフォン３０の表示部７６によりその旨が表示される。一方、トラップ型ＶＰがその氏名を用いてアクセスしたサイト以外のサイトからそのトラップ型ＶＰ氏名をＥメールの宛名としてＥメールが送信されてくれば、Ｓ９６９によりＮＯの判断がなされ、制御がＳ９６７へ進む。Ｓ９６７では、Ｅメールの宛名を本名のＶＰの公開鍵ＫＰＢで復号化する処理がなされる。その結果、Ｅメールの宛名であるトラップ型ＶＰ氏名が公開鍵ＫＰＢで復号化されて平文のサイト名が算出されることとなる。このサイト名は、Ｅメールの宛名に用いられているＶＰ氏名としてアクセスしたサイト名のことであり、アクセスしたサイトが個人情報をＥメールの送信者に不正流通したことが考えられる。よって、Ｓ９６７により、D_{KPB}（宛名）が不正流通し、送信者名の業者が不正入手した旨をブラウザフォン３０へ出力する。ブラウザフォン３０では、その旨を表示部７６により表示させる。

【０２９１】

なお、Ｓ９６９によりＮＯの判断がなされた場合に、前述した図１７のＳ４９４とＳ４９４ａとの処理を行なった後、Ｓ４９４ａによりＮＯの判断がなされた場合にのみＳ９６７へ進むようにしてもよい。

【０２９２】

次に、以上説明した実施の形態における変形例や特徴点等を以下に列挙する。

（１）　前述したように、ブラウザフォン（携帯電話）３０やＰＨＳ（Personal Handy-phone System）等の最寄の基地局に対し電波で送受信する携帯型送受信機の場合には、最寄の基地局を特定するために携帯型送受信機の現在地がある程度割出されるようになっている。このような携帯型送受信機を用いてＶＰとしてサイトにアクセスする等のネットワーク上での行動を行なう場合には、そのＶＰとして携帯型送受信機を利用している最中に位置がある程度特定されてしまうおそれがある。その結果、あるＶＰはあるＲＰと常に同じ場所に位置するという統計上の結果が割出されてしまい、ＶＰとＲＰとの関連が見破られてしまうおそれがある。

【０２９３】

そこで、次のような手段を採用する。
ユーザに携帯され最寄の基地局との間で電波による送受信を行なって該基地局を通してネットワーク内に進入可能な携帯型送受信機であって、
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仮想人物用処理機能（Ｓ１００～Ｓ１０３，Ｓ５８０，Ｓ５８２～Ｓ５８５）が備えられており、
該仮想人物用処理機能を用いてユーザが仮想人物としてネットワーク内に進入する場合に、ネットワークに接続された端末に対し直接無線通信（ブルートゥース）を行ない、前記基地局からの進入ルートではなく前記端末からネットワーク内に進入する処理を行なうための仮想人物用別ルート進入手段（Ｓ６０７～Ｓ６１３）を備えている、携帯型送受信機（ブラウザフォン３０等）。
【０２９４】
このような手段を採用した結果、ユーザは、仮想人物としてネットワーク内に進入する際には、仮想人物用別ルート進入手段を利用して、基地局からの進入ルートではなく別ルートによる進入が可能となり、その結果、仮想人物の位置が特定されてしまう不都合を極力防止することができる。
【０２９５】
このような効果を奏する手段として、次のようなものを採用してもよい。
ユーザに携帯され、最寄の基地局に対し電波により送受信を行なってネットワーク内に進入可能な携帯型送受信機（ブラウザフォン３０等）に備えられているプロセッサ（ＣＰＵ１９７）を動作させるプログラムであって、
前記プロセッサに、
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処理を行なう仮想人物処理手段（Ｓ１００～Ｓ１０３，Ｓ５８０，Ｓ５８２～Ｓ５８５）と、
該仮想人物処理手段によりユーザが仮想人物としてネットワーク内に進入する際に、該ネットワークに接続されている端末に対し直接無線通信を行なって、前記基地局からの進入ルートではなく前記端末からネットワーク内に進入する仮想人物用別ルート進入手段（Ｓ６０７～Ｓ６１３）と、
として機能させるプログラム。
【０２９６】
（２）　ユーザの個人情報を利用する業者側は、提供してもらいたい個人情報が本当に正しい内容であるか否かを確認したいというニーズがある。
【０２９７】
そこで、以下のような手段を採用する。
所定機関にユーザから個人情報の登録要請があった場合に、その個人情報の真偽チェックを行なうための処理を行なう真偽チェック処理手段（Ｓ４２０）と、
該真偽チェック処理手段による処理の結果、正しいと判断される個人情報に対し前記所定機関のデジタル署名を施すデジタル署名手段（Ｓ４２５）と、
該デジタル署名が施された前記個人情報を当該個人情報のユーザが特定可能な態様で格納する個人情報格納手段（Ｓ４２５，データベース１２ａ）と、
あるユーザ名を指定しての依頼者からの要請に応じて、該ユーザ名に対応する個人情報を前記個人情報格納手段から検索する検索手段とを含む、個人情報システム。
【０２９８】
この個人情報システムは、以下の手段をさらに含んでもよい。
前記依頼者が所有する個人情報の真偽のチェックを依頼してきた場合に、該チェック対象となる前記依頼者の所有する個人情報に対応する個人情報を前記個人情報格納手段から検索し、該検索された個人情報と前記依頼者の個人情報とを照合して真偽チェックを行なう真偽チェック手段（Ｓ４７１，Ｓ４７２）、

該真偽チェック手段による真偽の結果を前記依頼者に通知する結果通知手段（Ｓ４８７）、
前記真偽チェック手段のチェックの結果と前記依頼者の個人情報が正しい内容であった場合に該個人情報に対し前記所定機関のデジタル署名を施すデジタル署名手段（Ｓ４８６）、
前記真偽チェック手段による真偽チェックの結果を前記依頼者に通知してよいか否かを真偽チェック対象となっている個人情報に対応するユーザに尋ねるための処理を行なう手段（Ｓ４７６，Ｓ４７７）、
前記個人情報格納手段に格納されている個人情報の購入要求が依頼者からあった場合に、該購入の対価をめぐる交渉を行なうための処理を行なう交渉処理手段（Ｓ５０４～Ｓ５０６）、
該交渉処理手段による交渉の結果交渉が成立した場合に、購入対象の個人情報を当該個人情報に対する前記所定機関のデジタル署名とともに購入依頼者に送信する送信手段（Ｓ５０９）、
前記交渉処理手段の結果交渉が成立した場合にその成立した条件に対し、購入対象の個人情報に対応するユーザ、前記購入依頼者、前記所定機関のそれぞれのデジタル署名を付して記憶しておく記憶手段（Ｓ５０８）。

【０２９９】

（３）　ユーザがＶＰとしてネットワーク上で行動することが多くなれば、ＲＰとＶＰとの両方の詳しい個人情報を収集した業者が、両個人情報を虱潰しにマッチングチェックして、両個人情報が一致するＲＰ氏名とＶＰ氏名とを割出し、ＶＰに対応するＲＰの名前を予測してしまうという不都合が生ずるおそれがある。そこで、次のような解決手段を採用する。

【０３００】

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した個人情報保護方法に用いられる個人情報保護装置であって、
前記実在人物の要求に応じて、該実在人物が意図しないサイトにアクセスするアクセス手段（Ｓ６５１～Ｓ６６２）を含む、個人情報保護装置。

【０３０１】

このような手段を採用した結果、実在人物が意図しないサイトへのアクセスが自動的に行なわれることとなり、当該実在人物の個人情報の信頼性を低下させることができる。その結果、実在人物と仮想人物との両個人情報のマッチングチェックの結果の信頼性を低下させることができる。

【０３０２】

この個人情報保護装置は、さらに以下の手段を含んでもよい。
前記アクセス手段によりアクセスしたサイト内で、前記実在人物が意図しない行動を行なう行動手段（Ｓ６５６）、
前記アクセス手段によりアクセスしたサイトに対し、前記実在人物の実名（太郎）を提供する処理を行なう個人情報提供処理手段（Ｓ６５６）、
前記アクセス手段によりアクセスしたサイトからユーザを識別するために送信されてきた識別データ（クッキー）を受付けて記憶させるための処理を行なうクッキー受付処理手段（Ｓ６６０，Ｓ６６１）、
前記アクセス手段に備えられ、アクセスするサイトがユーザによって予め設定されたアクセス許容範囲内のものか否かを判別してアクセス許容範囲内でない場合にはアクセスしないアクセス禁止手段（Ｓ６５５）、
なお、この個人情報保護装置は、前述した実施の形態では、ユーザ側端末（ブラウザフォン３０等）により構成されているが、本発明はこれに限らず、たとえばユーザ側の依頼に応じて偽ＲＰアクセス処理サービスを行なう所定のサービス機関を設置し、そのサービス機関に対しユーザ側からの要求があった場合に、前述したアクセス手段、行動手段、等の

動作を行なうようにしてもよい。さらに、実在人物の嗜好情報とは異なる嗜好情報をサイト側に提供してもよい。

【０３０３】

（４）　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「匿名」とは、仮想人物（ＶＰ）の氏名のことであり、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。

【０３０４】

本発明でいう「個人情報保護装置」は、装置単体ばかりでなく、複数の装置がある目的を達成するために協働するように構築されたシステムをも含む広い概念である。

【０３０５】

（５）　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所定機関にＶＰ管理機能を肩代わりさせてもよい。その肩代わりする所定機関としては、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。

【０３０６】

また、本実施の形態では、コンビニエンスストア２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置してもよい。

【０３０７】

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（ブラウザフォン３０等）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。

【０３０８】

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。

（６）　処理装置の一例としてのＩＣ端末１９Ｒまたは１９Ｖは、ＩＣカードや携帯電話あるいはＰＨＳ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用モードに切換え可能に構成し、１種類の携帯型端末で事足りるように構成してもよい。

【０３０９】

図９に示したＩＣ端末１９Ｉ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ネットワーク経由で当該アプリケーションソフトをブラウザフォン３０等へダウンロードするように構成してもよい。

【０３１０】

（７）　本実施の形態では、図１２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。

【０３１１】

図２３等に示すように、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。

【０３１２】

（８）　ブラウザフォン３０に代えて、パーソナルコンピュータを用いてもよい。

【０３１３】
トラップ型ＶＰ用に金融機関７が開設したＥメールアドレス△△△△△は、１種類のみのＥメールアドレスではなく、複数種類用意し、トラップ型ＶＰ氏名毎に使い分けるようにしてもよい。Ｓ６２０～Ｓ６２２またはＳ９６０～Ｓ９５６により、新たな匿名（トラップ型ＶＰ氏名）の生成要求があった場合に、今までに使われていない匿名を生成する新匿名生成手段が構成されている。Ｓ４３１～Ｓ４４１またはＳ９５４により、前記新匿名生成手段により生成された匿名の登録を行なう匿名登録機関（金融機関７またはＥＥＰＲＯＭ２６）に対し新たに生成された匿名の登録依頼があった場合に、該匿名を登録する匿名登録手段が構成されている。
【０３１４】
前述したＳ４５０～Ｓ４６０により、ユーザの個人情報を登録している登録機関に対しユーザから自己の個人情報の確認要求があった場合に、当該ユーザの本人認証を行なう本人認証手段（Ｓ４５２～Ｓ４５８）による本人認証の結果本人であることが確認されたことを条件として、当該ユーザに対応する個人情報を当該ユーザに送信する個人情報送信手段が構成されている。
【０３１５】
図４４（ａ）で示したトラップ型ＶＰ氏名は、サイト名をＶＰの秘密鍵ＫＳＢで複合化したものであってもよい。
【０３１６】
つまり、Ｓ９５７により、D_{KSB}（サイト名）の演算を行なってトラップ型ＶＰ氏名を生成してもよい。その場合には、Ｓ９６９により、E_{KPB}（Ｅメールの宛名）＝送信者名の演算式による判別を行なうこととなる。Ｓ９６７では、E_{KPB}（Ｅメールの宛名）が不正流出し、送信者名の業者が不正入手した旨を出力するという処理になる。
【０３１７】
前述したＳ９５７により、ユーザがネットワークを通してアクセスするサイトに対し、当該サイトの名称を当該ユーザが使用できる鍵（秘密鍵ＫＳＢ）により暗号化または復号化して生成した匿名を生成する匿名生成手段が構成されている。
【０３１８】
ユーザがネットワークを通してアクセスし自己の個人情報を提供したサイトを特定するために用いる識別情報を特定可能な情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメールを送る場合には該メールに含まれることとなる識別情報として、前述した実施の形態では匿名（トラップ型ＶＰ氏名）を用いたが、その代わりにまたはそれに加えて、サイト毎に使い分ける複数のＥメールアドレスやダイレクトメール用の住所(私書箱等)を用いてもよい。
【０３１９】
（９）　ネットワーク（広域・大容量中継網４３）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。
【０３２０】
（１０）　前記所定機関は、金融機関７である。
（１１）　ネットワーク（広域・大容量中継網４３）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。

【０３２１】

（１２）　ネットワーク（広域・大容量中継網４３）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。

【０３２２】

（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）。

【０３２３】

（１４）　ネットワーク（広域・大容量中継網４３）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）。

【０３２４】

（１５）　ネットワーク（広域・大容量中継網４３）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）。

【０３２５】

（１６）　ネットワーク（広域・大容量中継網４３）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）。

【０３２６】

（１７）　ネットワーク（広域・大容量中継網４３）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。

【０３２７】

（１８）　ネットワーク（広域・大容量中継網４３）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）。

【０３２８】

（１９）　ネットワーク（広域・大容量中継網４３）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。

【０３２９】

（２０）　ネットワーク（広域・大容量中継網４３）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。

【０３３０】

（２１）　ネットワーク（広域・大容量中継網４３）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。

【０３３１】

（２２）　ネットワーク（広域・大容量中継網４３）上での個人情報を保護するためのプログラムまたは該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、または該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。

【０３３２】

（２３）　ネットワーク（広域・大容量中継網４３）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）。

【０３３３】

（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）。

【０３３４】

（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。

【０３３５】

（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。

【０３３６】

（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。

【０３３７】

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。

【０３３８】

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。

【０３３９】

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。

【０３４０】

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。

【０３４１】

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。

【０３４２】

（２８）　本実施の形態では、図２８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。

【０３４３】

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。

【０３４４】

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）。

【０３４５】

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。

【０３４６】

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。

【０３４７】

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。

【０３４８】

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。

【０３４９】

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。

【０３５０】

【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。

【０３５１】

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

ユーザがネットワーク（広域・大容量中継網４３）を通してアクセスし自己の個人情報を提供するサイトを特定するために用いる識別情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメール（Ｅメール，ダイレクトメール）を送る場合に該メールに含まれることとなる識別情報（匿名としてのトラップ型ＶＰ氏名，図４４（ａ）のE_{KSB}（サイト名）,サイト毎に使い分けるＥメールアドレスやダイレクトメール用の住所）をプロセッサ（ＣＰＵ２４）を利用して生成する識別情報生成ステップ（Ｓ６２０とＳ６２１またはＳ９６０～Ｓ９５６）と、

該識別情報生成ステップにより生成された識別情報を用いてユーザがサイトにアクセスして個人情報を提供する個人情報提供ステップ（Ｓ５９３，Ｓ６００，Ｓ７００，Ｓ７０１）と、

該個人情報提供ステップにより提供された前記個人情報を入手した者が該個人情報主であるユーザに対し送ったメールに含まれている前記識別情報に基づいて特定される前記サイトと前記メールの送り主とが一致するか否かを判定して前記ユーザの個人情報の流通状態を監視する監視ステップ（Ｓ５１６またはＳ９６９）とを含む個人情報保護方法。

【０３５２】

（２）　前記識別情報は、サイト毎に使い分けるユーザの匿名（図１１，図４４（ａ）に示すトラップ型ＶＰ氏名）である。

【０３５３】

（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装置であって、

ユーザがネットワーク（広域・大容量中継網４３）を通してアクセスし自己の個人情報を提供したサイトを特定するために用いる識別情報を特定可能な情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメールを送る場合には該メールに含まれることとなる識別情報を特定可能な情報（匿名としてのトラップ型ＶＰ氏名,図４４（ａ）のＫＳＢとサイト名,サイト毎に使い分けるＥメールアドレスやダイレクトメール用の住所）を格納する識別情報格納手段（データベース１２ａ，ＥＥＰＲＯＭ２６）と、

前記個人情報を入手した者がその個人情報主であるユーザに対し送ったメール（Ｅメール，ダイレクトメール）に含まれている前記識別情報に基づいて特定される前記サイトと前記メールの送り主とが一致するか否かを判定して前記ユーザの個人情報の流通状態を監視する監視手段（Ｓ５１６，Ｓ５２２，Ｓ５２３）とを含む個人情報保護装置。

【０３５４】

（４）　前記監視手段は、前記識別情報に基づいて特定される前記サイトに前記ユーザが自己の個人情報を提供した際に承諾した当該個人情報の流通許容範囲内（ＸＭＬストア５０のデータベース７２に格納されているプライバシーポリシーによって特定される流通許容範囲内）に前記メールの送り主が含まれていない場合に不適正である旨の判定（Ｓ５２３によるＮＯの判定）を行なう。

【０３５５】

（５）　コンピュータシステムを利用して、ネットワーク（広域・大容量中継網４３）上での個人情報を保護する個人情報保護装置であって、

ユーザがネットワークを通してアクセスし自己の個人情報を提供したサイトを特定するた

めに用いる識別情報を特定可能な情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメール（Ｅメール，ダイレクトメール）を送る場合には該メールに含まれることとなる識別情報を特定可能な情報（匿名としてのトラップ型ＶＰ氏名，図４４（ａ）のＫＳＢとサイト名,サイト毎に使い分けるＥメールアドレスやダイレクトメール用の住所）を格納する識別情報格納手段（Ｓ６２２，ＥＥＰＲＯＭ２６）と、
ユーザがネットワークを通してサイトにアクセスする際に、当該サイトを特定するために用いる識別情報が既に前記識別情報格納手段に格納されている場合には、当該格納されている識別情報を前記サイトに対して用いるための処理を行なう識別情報使用制御手段（Ｓ６２３～Ｓ６２８）とを含む、個人情報保護装置。

【０３５６】

（６）　ユーザと当該ユーザが用いる前記識別情報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）において登録する処理を行なうための登録処理手段（Ｓ４４０）を、前記個人情報保護装置がさらに含む。

【０３５７】

（７）　前記識別情報は、ユーザが前記サイト毎に使い分ける匿名（トラップ型ＶＰ氏名）である（図１１参照）。

【０３５８】

（８）　前記個人情報保護装置は、前記ユーザが前記匿名を用いてネットワーク上で行動する際に使用する前記匿名用の電子証明書を発行する処理を行なうための電子証明書発行処理手段（Ｓ４４１）をさらに含んでいる。

【０３５９】

（９）　前記電子証明書は、ユーザと当該ユーザが用いる前記識別情報との対応関係を特定可能な情報を登録している守秘義務のある所定機関（金融機関７）により発行され、前記匿名を用いるユーザが当該所定機関において登録されているユーザであることを証明するものである。

【０３６０】

（１０）　前記ユーザが前記匿名を用いてネットワーク上で行動する際の住所を、前記ユーザの住所とは異なる住所（コンビニエンスストア２の住所）に設定する処理を行なう住所設定手段（Ｓ１１，Ｓ１２）を、前記個人情報保護装置がさらに含んでいる。

【０３６１】

（１１）　前記住所設定手段は、所定のコンビニエンスストアの住所を設定する（Ｓ１１，Ｓ１２参照）。

【０３６２】

（１２）　前記個人情報保護装置は、前記ユーザが前記匿名を用いてネットワーク上で行動するべくサイトにアクセスする場合には、ユーザが実名（たとえば太郎）を用いてネットワーク上で行動した際にサイト側からユーザを識別するために送信されてきた識別データ（クッキー）を、アクセスするサイトに送信しないようにするための処理を行なう識別データ制御処理手段（Ｓ５９０～Ｓ６０２）をさらに含む。

【０３６３】

（１３）　前記識別データ制御処理手段は、
前記匿名を用いてアクセスしたサイト（たとえばＭＴＴ，ＭＥＣ等）から送られてきた前記識別データ（クッキー）のみを当該匿名専用の識別データとして格納する匿名対応識別データ格納手段（Ｓ５９５，Ｓ２７６，ＥＥＰＲＯＭ２６のクッキーデータ記憶領域（図１１参照））と、
以降ユーザが前記匿名を用いて当該匿名により特定される前記サイトにアクセスする場合に、前記匿名対応識別データ格納手段を検索して当該匿名に対応する識別データを割出し、該識別データを前記サイトへ送信する識別データ検索送信手段（Ｓ６２３～Ｓ６２８）とを含んでいる。

【０３６４】

（１４）　前記個人情報保護装置は、

ユーザが前記匿名を用いてネットワーク上で行動した場合の行動履歴（どのサイトにアクセスしたか等のアクセス履歴等）をどの匿名を用いて行動したかを特定できる態様で格納する行動履歴データ格納手段（データベース１２ａ（図４参照））と、
ユーザが前記匿名を用いてアクセスしたサイト側から、前記ユーザの他の匿名を用いてのネットワーク上での行動履歴データの提供を求められた場合に、前記行動履歴データ格納手段を検索して前記他の匿名を用いての行動履歴データを前記サイトへ提供するための処理を行なう行動履歴データ提供処理手段（Ｓ５３０～Ｓ５４６）とをさらに含む。
【０３６５】
（１５）　前記個人情報保護装置は、前記行動履歴データ提供処理手段に対し匿名を通知して該匿名を用いたユーザの他の匿名を用いてのネットワーク上での行動履歴データの提供を要求された場合に（ユーザの氏名が送信されてきてＳ５３５によりＹＥＳの判断がなされた場合に）、該要求者と前記通知された匿名に基づいて特定される前記サイトとが一致するか否かを判定して前記ユーザの個人情報の流通状態を監視する監視手段（Ｓ５４８）をさらに含む。。
【０３６６】
（１６）　前記個人情報保護装置は、あるユーザによって使用された複数種類の匿名のための共通のクレジット番号（ＶＰ本名のクレジット番号）を各匿名から割出し可能な態様で格納するための処理を行なうクレジット番号格納処理手段（Ｓ４３８～Ｓ４４０）と、
ユーザが前記匿名を用いてネットワーク上でクレジット決済を行なった場合に、クレジット会社からの当該匿名に対応するクレジット番号の有無の問合せを受付け、前記クレジット番号登録処理手段により登録されたクレジット番号を検索して前記問合せのあった匿名に対するクレジット番号の有無を判別し、その判別結果を前記クレジット会社に通知するための処理を行なう通知手段（Ｓ５６０～Ｓ５７４）とを含んでいる。
【０３６７】
（１７）　前記個人情報保護装置は、ユーザが前記匿名によりネットワーク上で行動する際の当該匿名宛の電子メールを受付け、該電子メールを当該匿名に対応するユーザが閲覧可能な電子メールアドレスに転送する、匿名宛電子メール転送手段（Ｓ５１４～Ｓ５２２）をさらに含む。
【０３６８】
（１８）　前記個人情報保護装置は、前記匿名宛電子メール転送手段が受付けた前記電子メールの宛名である匿名に基づいて特定される前記サイトと前記受付けた電子メールの送り主とが一致するか否かを判定して前記ユーザの個人情報の流通状態を監視する監視手段をさらに含む。
【０３６９】
（１９）　前記監視手段は、複数のユーザに対し適正であるか否かの判定サービスを行なう所定機関（金融機関７）に設置され、該所定機関には、前記監視手段による監視結果を集計してサイト毎の個人情報に関する信頼度を算出する信頼度算出手段（Ｓ５５０，Ｓ５５１）と、
該信頼度算出手段により算出された信頼度情報を提供する信頼度情報提供手段（Ｓ５５３）とが備えられている。
【０３７０】
（２０）　前記匿名は、当該匿名を用いるサイトの名称を、当該匿名を用いるユーザが使用できる鍵（秘密鍵）で暗号化または復号化したものである。
【０３７１】
（２１）　ネットワーク（広域・大容量中継網４３）上での個人情報を保護するためのプログラムであって、
プロセッサ（ＣＰＵ２４）に、
ユーザがネットワークを通してアクセスし自己の個人情報を提供したサイトを特定するために用いる識別情報を特定可能な情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメール（Ｅメール，ダイレクトメール）を送る場合には該メールに含

まれることとなる識別情報を特定可能な情報（トラップ型ＶＰ氏名,図４４（ａ）に示すＫＳＢとサイト名,サイト毎に使い分けるＥメールアドレスやダイレクトメール用の住所）をメモリ（ＥＥＰＲＯＭ２６）に記憶させる識別情報記憶手段（Ｓ６２２）と、
ユーザがネットワークを通してサイトにアクセスする際に、当該サイトを特定するために用いる識別情報が既に前記メモリに記憶されている場合には、当該記憶されている識別情報を前記サイトに対し用いるための処理を行なう識別情報使用制御手段（Ｓ６２５～Ｓ６２７）と、
して機能させるためのプログラム。

【０３７２】

（２２）　前記識別情報は、ユーザがサイト毎に使い分ける匿名（トラップ型ＶＰ氏名）であり、
プロセッサに、さらに、
前記ユーザが前記匿名を用いてネットワーク上で行動するべくサイトにアクセスする場合には、ユーザが実名（たとえば太郎）を用いてネットワーク上で行動した際にサイト側からユーザを識別するために送信されてきた識別データ（クッキー）を、アクセスするサイトに送信しないようにする処理を行なう識別データ制御処理手段（Ｓ６２３～Ｓ６２８）として機能させる。

【０３７３】

（２３）　前記識別データ制御処理手段は、
前記匿名を用いてアクセスしたサイトから送られてきた前記識別データ（クッキー）のみを当該匿名専用の識別データとしてメモリに記憶させる匿名対応識別データ記憶手段（Ｓ６２２）と、
以降ユーザが前記匿名を用いて当該匿名により特定される前記サイトにアクセスする場合に、前記メモリを検索して当該匿名に対応して格納されている識別データを割出し、該識別データを前記サイトへ送信するための処理を行なう識別データ検索送信処理手段（Ｓ６２５～Ｓ６２７）とを含む。

【０３７４】

（２４）　ネットワーク（広域・大容量中継網４３）上で個人情報を保護するためのプログラムであって、
プロセッサ（ＣＰＵ２４）に、
ユーザがネットワークを通してアクセスするサイトに対し、当該サイトの名称を当該ユーザが使用できる鍵（秘密鍵ＫＳＢ）により暗号化または復号化して生成した匿名（トラップ型ＶＰ氏名）を使用し、匿名宛の電子メールを受信した場合に、当該電子メールの宛名である匿名を鍵（公開鍵ＫＰＢ）により復号化または暗号化して平文のサイトの名称に戻す変換手段（Ｓ９６９）と、
して機能させるためのプログラム。

【０３７５】

（２５）　プロセッサ（ＣＰＵ２４）に、さらに、
前記変換手段により変換されたサイトの名称と前記受信した電子メールの送り主の名称とが一致するか否かを判定して前記ユーザの個人情報の流通状態を監視する監視手段（Ｓ９６９、Ｓ９６８）として機能させる、プログラム。

【０３７６】

本発明は、前述した（１）～（２５）のみに限定されるものではなく、（１）～（２５）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。

【０３７７】

【課題を解決するための手段の具体例の効果】

ユーザの個人情報を入手した者がその個人情報主であるユーザに対し送ったメールに含まれている識別情報に基づいて、当該個人情報を提供したサイトが特定され、そのサイトと前記メールの送り主とが一致するか否かが判別されるようにした場合には、個人情報の提供を受けたサイトが他の業者にその個人情報を流通させてその個人情報を受取った業者

から当該個人情報のユーザに対しメールが送られた場合に、そのメールに含まれている識別情報に基づいて特定されるサイトとそのメールの送り主である業者の名前とが一致しないこととなる。その結果、ユーザの個人情報の第１譲渡先のサイトから他の業者にその個人情報が譲ったことが判別可能となる。

【０３７８】

前記識別情報がサイト毎に使い分けられるユーザの匿名の場合には、個人情報を入手した業者がユーザを特定するのにその匿名を用い、その匿名からは当該ユーザの個人情報の第１譲渡先であるサイト名が特定できる。

【０３７９】

識別情報に基づいて特定されるサイトにユーザが自己の個人情報を提供した際に承諾した当該個人情報の流通許容範囲内にメールの送り主が含まれていない場合に不適正である旨の判定が行なわれるようにした場合には、個人情報の譲渡時のユーザの個人情報流通許容範囲の承諾をも考慮した適否判定が可能となる。

【０３８０】

ユーザがネットワークを通してサイトにアクセスする際に、当該サイトを特定するために用いる識別情報が既に用いられている場合に、その識別情報を前記サイトに対して用いるための処理が行なわれるために、同じサイトに対して複数種類の識別情報を用いる無駄を省くことができる。

【０３８１】

ユーザとそのユーザが用いる前記識別情報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た場合には、たとえばユーザと業者側との間において、ユーザと前記識別情報との対応関係をめぐるトラブルが発生した場合に、所定機関に登録されている対応関係の情報を参照することが可能となる。

【０３８２】

前記匿名用の電子証明書が発行された場合には、ユーザがたとえば売買を行なう際に相手側にその電子証明書を提示して匿名として売買を行なうことが可能となり、ユーザが匿名を用いて法律行為を行なうことが可能となる。

【０３８３】

ユーザが匿名を用いてネットワーク上で行動する際の住所が、当該ユーザの住所とは異なる住所に設定されれば、その住所を手掛かりにある匿名とあるユーザとが同一人物であることを突き止められてしまう不都合を極力防止することができる。

【０３８４】

ユーザが匿名を用いてネットワーク上で行動する際の住所がコンビニエンスストアの住所であれば、匿名を用いてたとえば電子ショッピング等を行なった場合の商品の届出先がそのコンビニエンスストアとなり、ユーザが匿名としてその商品を引取りに行く際の利便性が向上する。

【０３８５】

ユーザが匿名を用いてネットワーク上で行動するべくサイトにアクセスする場合には、ユーザが実名を用いてネットワーク上で行動した際にサイト側からユーザを識別するために送信されてきた識別データを、アクセスするサイトに送信しないようにするための処理が行なわれた場合には、その識別データを手掛かりにある匿名とあるユーザとが同一人物であること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。

【０３８６】

匿名を用いてアクセスしたサイトから送られてきた前記識別データのみが当該匿名専用の識別データとして格納され、以降ユーザが前記匿名を用いて当該匿名により特定されるサイトにアクセスする場合に、その匿名に対応する識別データが前記サイトへ送信されるようにした場合には、識別情報を手掛かりにある匿名と他の匿名とが同一人物であること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。

【０３８７】

その際に、ユーザが匿名を用いてアクセスしたサイト側から、ユーザの他の匿名を用いて

の行動履歴データを前記サイトへ提供できるようにした場合には、識別データを手掛かりにある匿名と他の匿名とが同一人物であることを見破られる不都合を防止できながらも、同一人物に関するネットワーク上の行動履歴データをサイト側に提供して、その行動履歴データに基づいたよりカスタマイズされたユーザ好みの情報やサービスをユーザ側に提供しやすくなる。

【０３８８】

ユーザが匿名を用いてネットワーク上でクレジット決済を行なった場合に、クレジット会社から当該匿名に対応するクレジット番号の有無の問合せを受け、その匿名のための共通のクレジット番号が検索されて、問合せのあった匿名に対応するクレジット番号の有無が判別され、その判別結果がクレジット会社に通知されるために、複数種類の匿名のための共通のクレジット番号までクレジット会社に登録しておく必要がなくなり、その共通のクレジット番号を手掛かりにある匿名と他の匿名とが同一人物であることを見破られる不都合が極力防止できる。

【０３８９】

ユーザが匿名によりネットワーク上で行動する際の当該匿名宛の電子メールが受付けられてその電子メールが当該匿名に対応するユーザが閲覧可能な電子メールアドレスに転送されるために、電子メールアドレスを手掛かりにある匿名と他の匿名とが同一人物であることを見破られる不都合を極力防止することができる。

【０３９０】

その匿名宛の電子メールの転送の際に、その電子メールの宛名である匿名に基づいて特定されるサイトとその電子メールの送り主とが一致するか否かを判定してユーザの個人情報の流通状態が監視されるために、電子メールの転送時に自動的に監視がなされてユーザの利便性が向上する。

【０３９１】

信頼度算出手段により算出されたサイト毎の個人情報に関する信頼度が提供されれば、ユーザがサイトに対し個人情報を提供する際の判断基準となり、ユーザの利便性が向上する。

【０３９２】

ユーザが使用できる鍵でサイトの名称を暗号化または復号化したものを、当該サイトに用いる匿名にした場合には、業者側から送られてきたメールの宛名である匿名を、鍵により復号化または暗号化することによってサイト名に変換することができる。

【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】　（ａ）は会社の概略構成を示し、（ｂ）はユーザ宅の概略構成を示す図である。

【図３】　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４】　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５】　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６】　金融機関に設置されている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７】　ＸＭＬストアの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８】　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る。

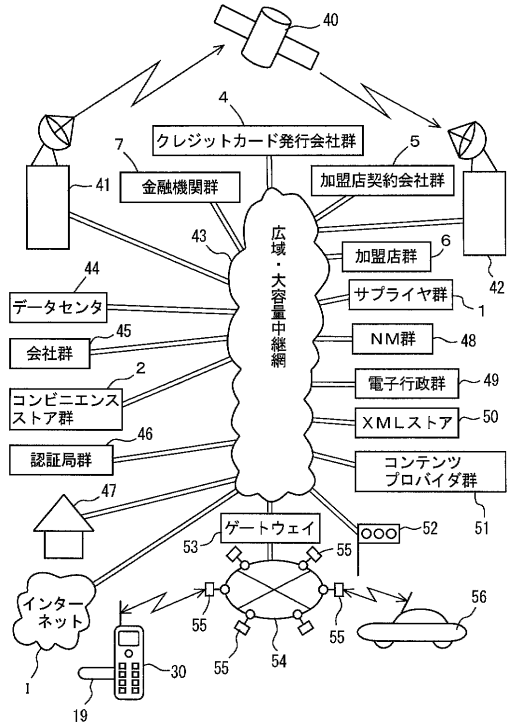
【図９】　ユーザ端末の一例としてのブラウザフォンを示す正面図である。

【図１０】　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。

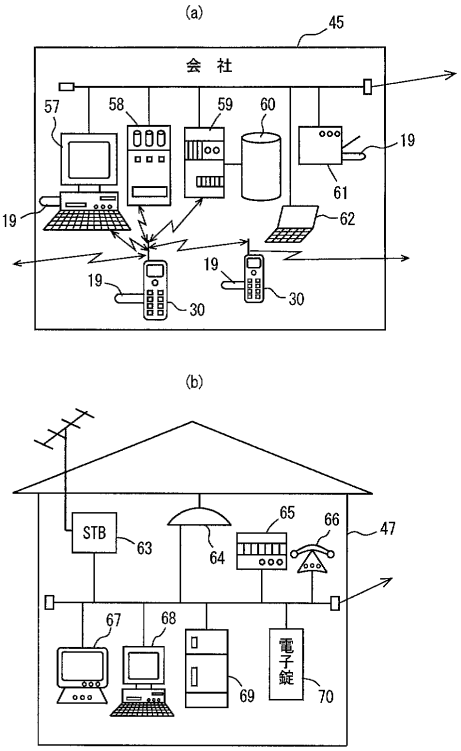
【図１１】　ＶＰ用ＩＣ端末のクッキーデータ記憶領域に記憶されているクッキーデータの内訳を示す図である。
【図１２】　ＶＰ管理サーバの処理動作を示すフローチャートである。
【図１３】　（ａ）はＶＰ管理サーバの処理動作を示すフローチャートであり、（ｂ）は個人情報の登録処理のサブルーチンプログラムを示すフローチャートである。
【図１４】　トラップ情報の登録処理のサブルーチンプログラムを示すフローチャートである。
【図１５】　個人情報の確認処理のサブルーチンプログラムを示すフローチャートである。
【図１６】　個人情報の照合，流通チェックのサブルーチンプログラムを示すフローチャートである。
【図１７】　（ａ）は個人情報の照合，流通チェックのサブルーチンプログラムを示すフローチャートであり、（ｂ）は個人情報の販売代行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１８】　メール転送，流通チェック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１９】　他のトラップ型ＶＰのアクセス履歴の提供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２０】　信頼度ランキング情報の集計，提供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２１】　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２２】　決済サーバの処理動作を示すフローチャートである。
【図２３】　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２４】　（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プログラムを示すフローチャートである。
【図２５】　クレジットカード発行会社からの問合せ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２６】　ブラウザフォンの処理動作を示すフローチャートである。
【図２７】　ＶＰ用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。
【図２８】　（ａ）は住所，氏名，Ｅメールアドレスの送信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り、（ｂ）は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。
【図２９】　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。
【図３０】　（ａ）は正当機関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り、（ｂ）は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。
【図３１】　（ａ）はＶＰ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り、（ｂ）は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。
【図３２】　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３３】　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。
【図３４】　（ａ）は本人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り、（ｂ）はＶＰ用決済処理のサブルーチンプログラムの一部を示すフローチャートである。
【図３５】　ＶＰ用決済処理のサブルーチンプログラムの一部を示すフローチャートである。
【図３６】　（ａ）はＶＰ用Ｗｅｂブラウザ，メール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り、（ｂ）は偽ＲＰアクセス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３７】　（ａ）はＶＰ用ＩＣ端末の処理動作を示すフローチャートであり、（ｂ）は

ＲＰ用ＩＣ端末の処理動作を示すフローチャートである。
【図３８】　（ａ）は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り、（ｂ）はクッキー処理（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り、（ｃ）は本人証明処理（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り、（ｄ）は本人証明処理（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。
【図３９】　（ａ）は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り、（ｂ）は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り、（ｃ）は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り、（ｄ）はＲＰ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り、（ｅ）はＶＰ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。
【図４０】　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。
【図４１】　トラップ型ＶＰ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４２】　コンビニサーバの処理動作を示すフローチャートである。
【図４３】　（ａ）は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り、（ｂ）は本人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り、（ｃ）は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４４】　別実施の形態を示し、（ａ）は、ＶＰ用ＩＣ端末に記憶されているトラップ情報であり、（ｂ）は、トラップ型ＶＰ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り、（ｃ）は、ＶＰ用ＩＣ端末の制御動作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、４３は広域・大容量中継網、１はサプライヤ群、４はクレジットカード発行会社群、７は金融機関群、５は加盟店契約会社群、５０はＸＭＬストア、２はコンビニエンスストア群、４５は会社群、３０はブラウザフォン、５４は携帯電話網、５５は基地局、４７はユーザ宅、９はＶＰ管理サーバ、１０は決済サーバ、１１は認証用サーバ、１２ａ，１２ｂはデータベース、７２はデータベース、７５はデータベース、１９ＶはＶＰ用ＩＣ端末、１９ＲはＲＰ用ＩＣ端末、１８はＵＳＢポート、２６はＥＥＰＲＯＭ、３３は支払承認部、３４は支払要求部である。

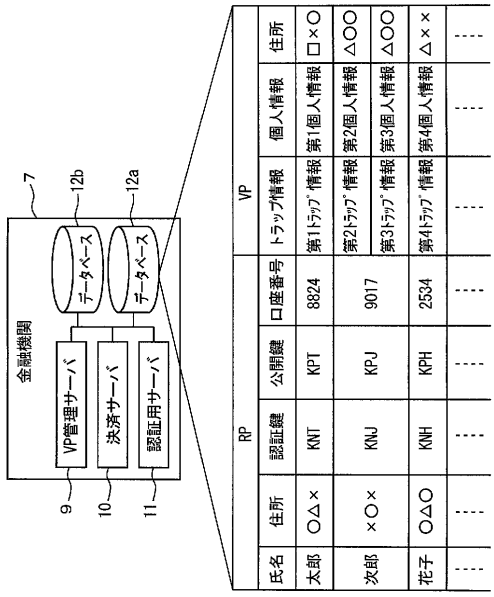
【図１】



【図２】



【図３】



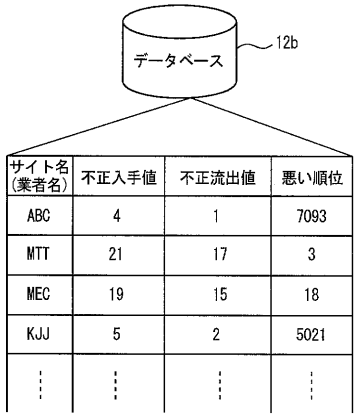
【図４】

第1トラップ情報	サイト名	ABC	MTT	MEC	--------
	氏名	B13P	E(B13P)	E^2(B13P)	--------
	公開鍵	KPB	KPB′	KPB″	--------
	Eメールアドレス	○□×△×	△△△△△	△△△△△	--------
	バーチャル口座番号	2503	E(2503)	E^2(2503)	--------
	バーチャルシビット番号	9145	E(9145)	E^2(9145)	--------
第2トラップ情報	サイト名	AMZ	RAK	ASK	--------
	氏名	NPXA	E(NPXA)	E^2(NPXA)	--------
	公開鍵	KPN	KPN′	KPN″	--------
	Eメールアドレス	××○△□	△△△△△	△△△△△	--------
	バーチャル口座番号	3541	E(3541)	E^2(3541)	--------
	バーチャルシビット番号	3288	E(3288)	E^2(3288)	--------
⋮	⋮	⋮	⋮	⋮	

【図５】

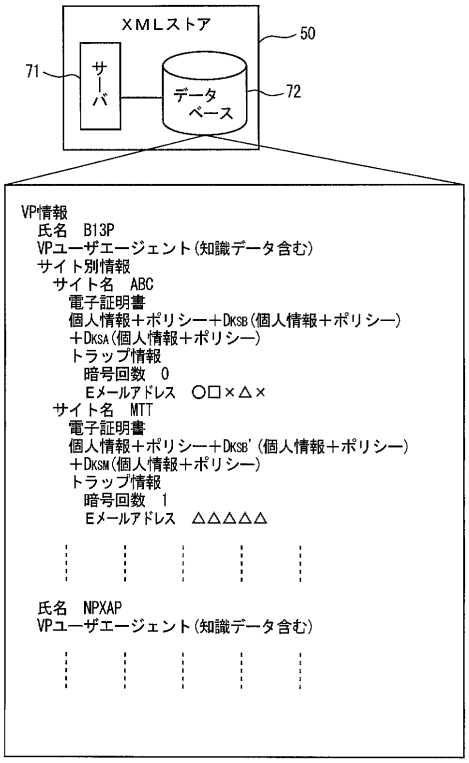
	個人情報A	個人情報B	-------
第１個人情報	○○△+Dks(○○△)	××△+Dks(××△)	-------
第２個人情報	△○○+Dks(△○○)	△×××+Dks(△××)	-------
第３個人情報	○△○+Dks(○△○)	×△×+Dks(×△×)	-------
第４個人情報	△○△+Dks(△○△)	△×△+Dks(△×△)	-------
⋮	⋮	⋮	

【図６】

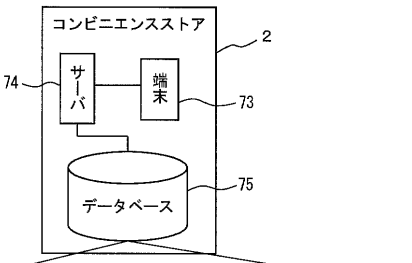


サイト名（業者名）	不正入手値	不正流出値	悪い順位
ABC	4	1	7093
MTT	21	17	3
MEC	19	15	18
KJJ	5	2	5021
⋮	⋮	⋮	⋮

【図７】

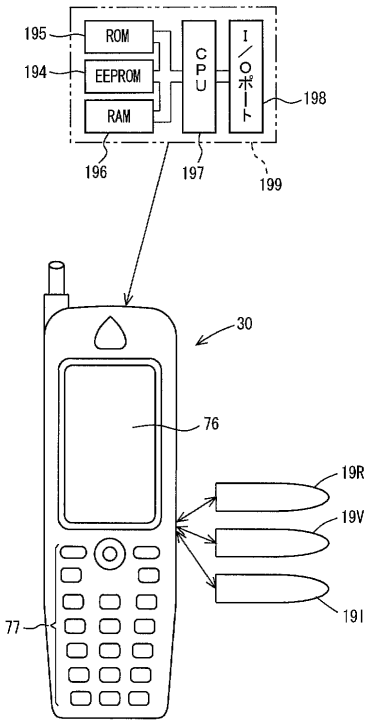


【図８】

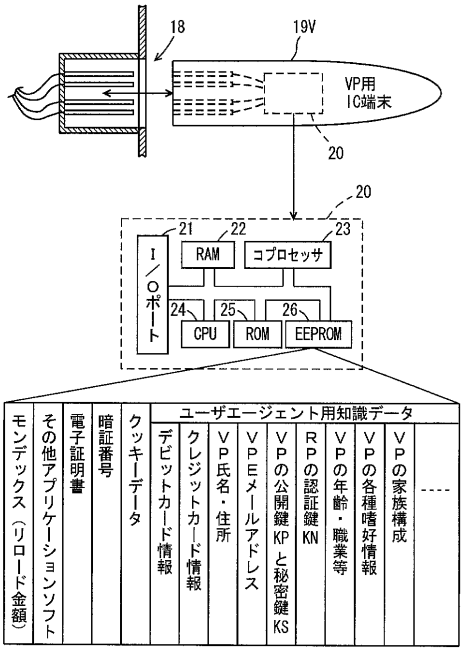


VP氏名	商品預かり情報	Eメールアドレス	顧客管理情報
B13P	ABC会社からの商品預かり,未決済	○□×△×	----------
E(B13P)	MTT会社からの商品預かり,決済済	△△△△△	----------
E^2(NPXA)	MEC会社からの商品預かり,未決済	△△△△△	----------
⋮	⋮	⋮	⋮

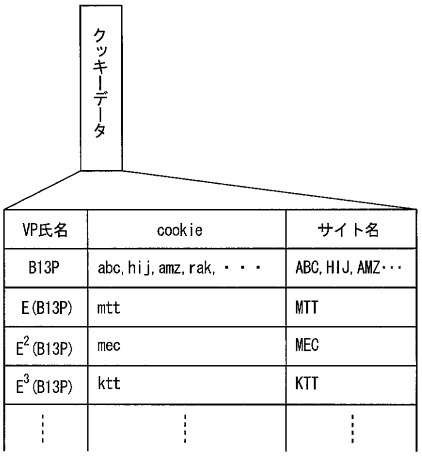
【図９】



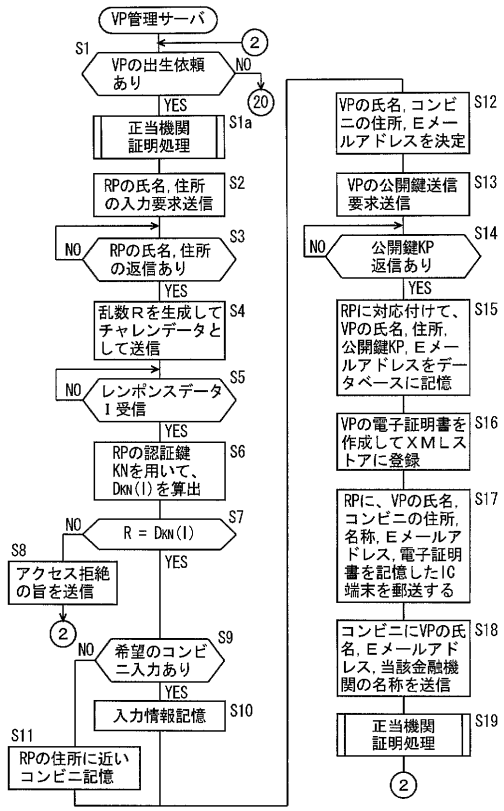
【図１０】



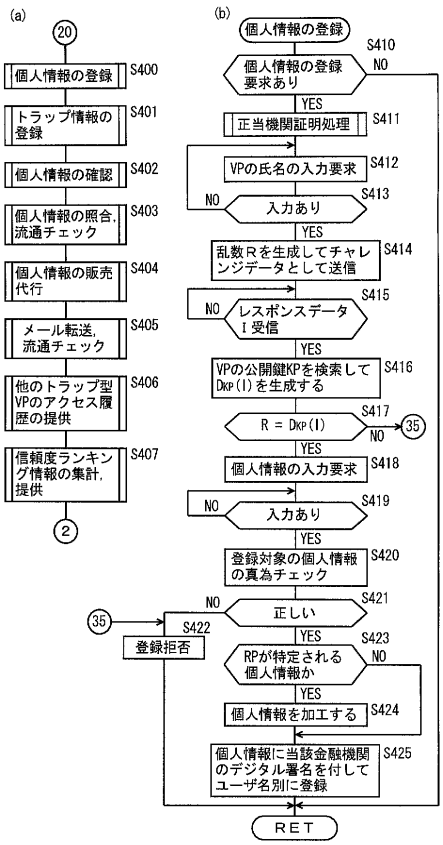
【図１１】



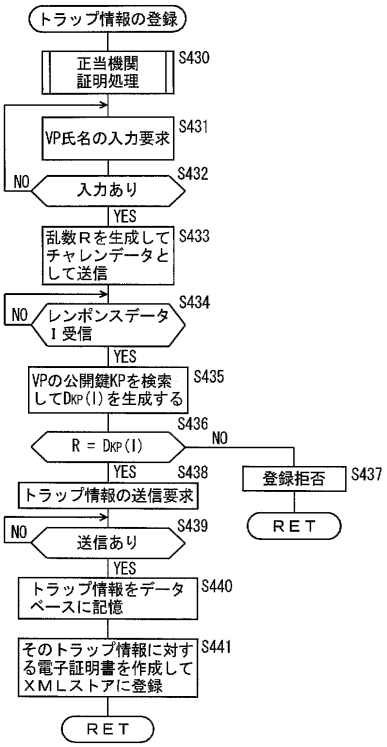
【図１２】



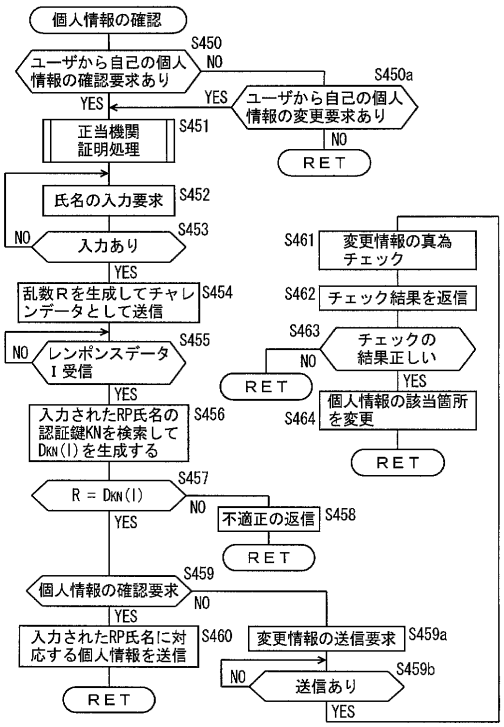
【図１３】



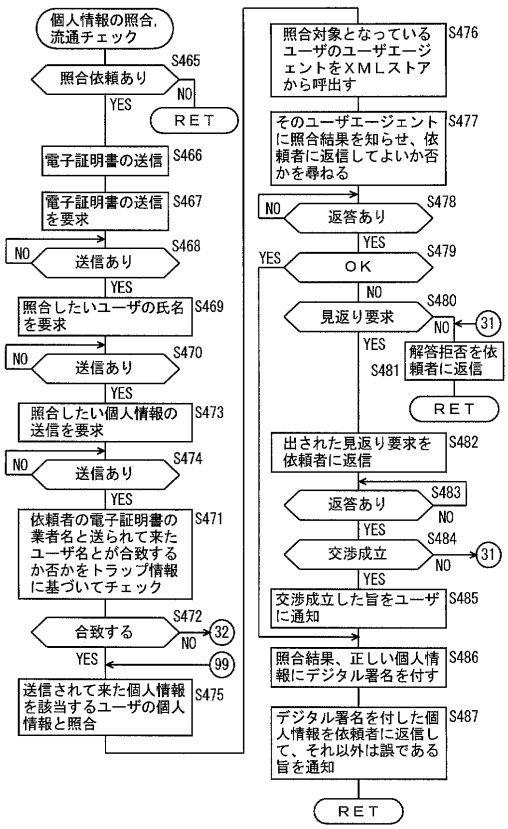
【図１４】



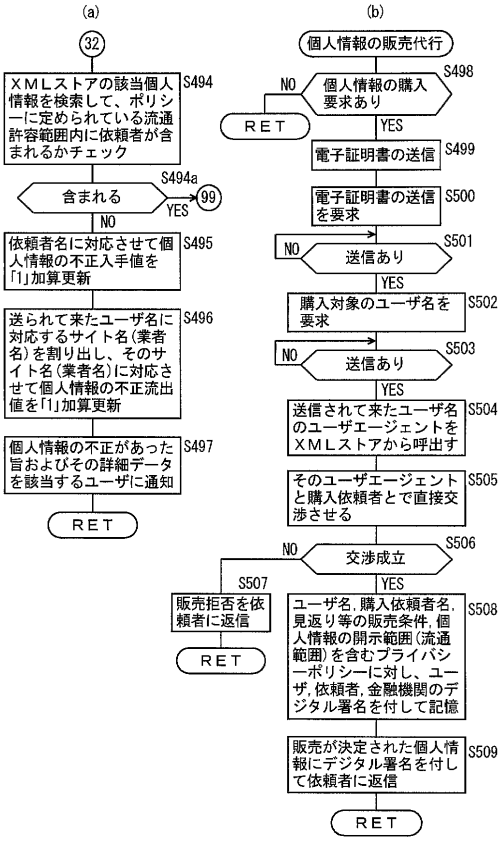
【図１５】



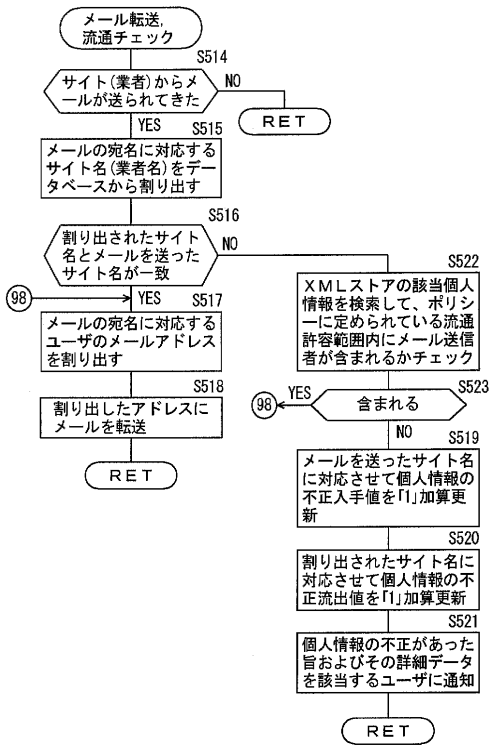
【図１６】



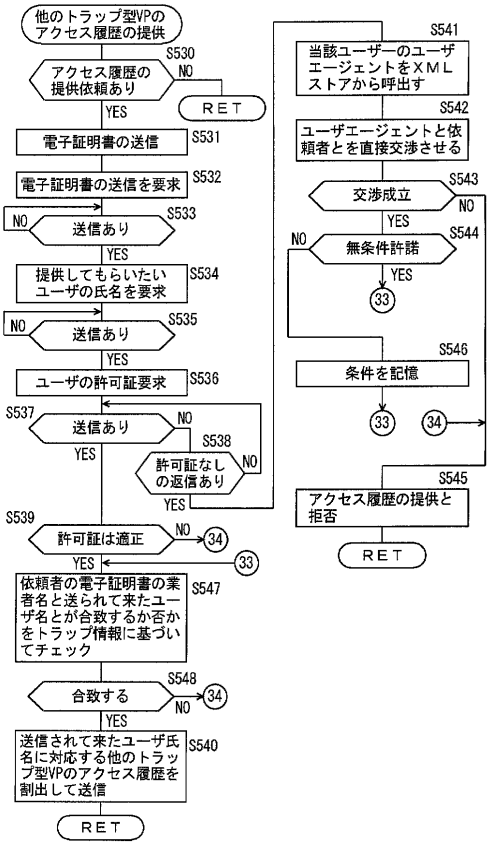
【図１７】



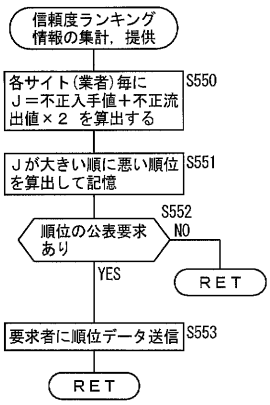
【図１８】



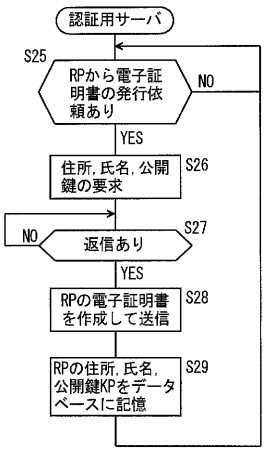
【図１９】



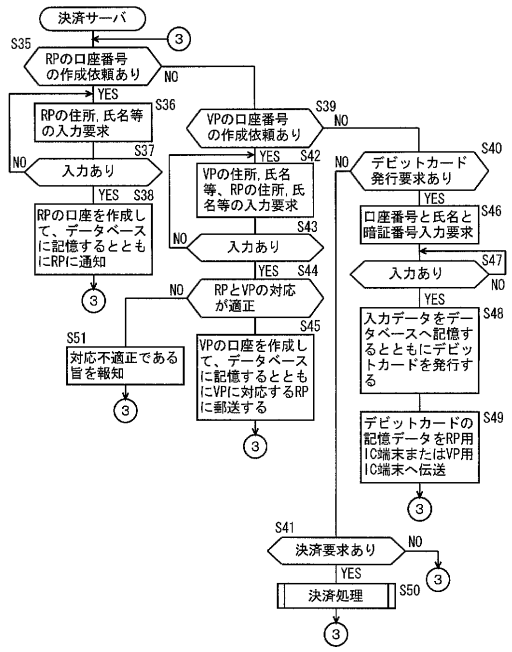
【図２０】



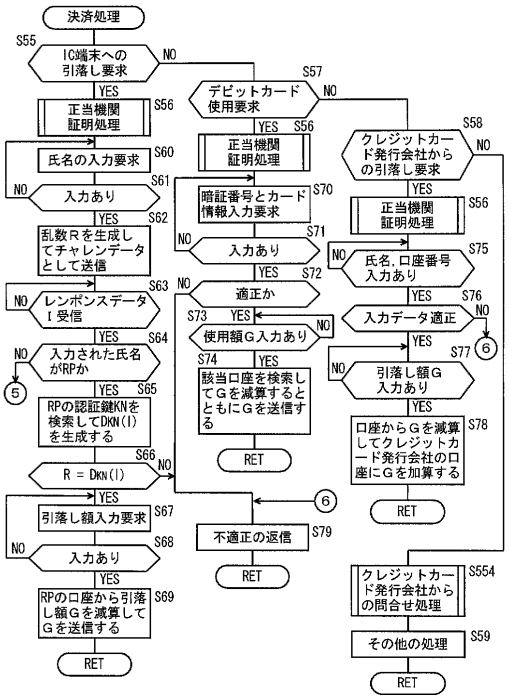
【図２１】



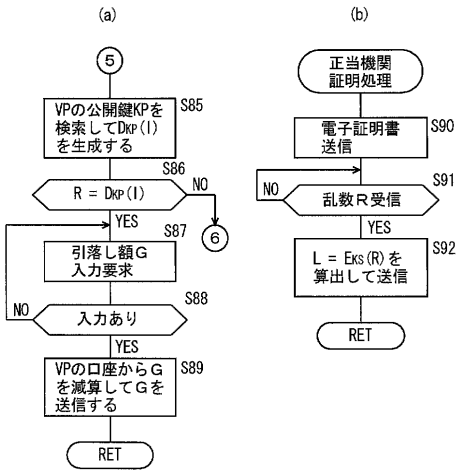
【図２２】



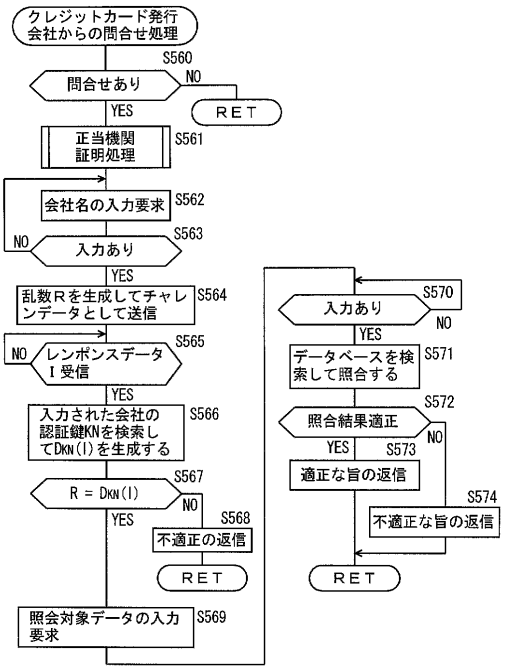
【図２３】



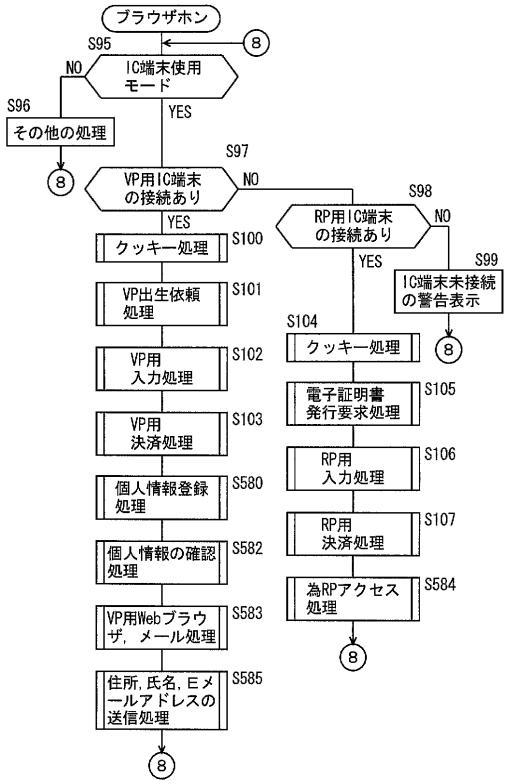
【図２４】



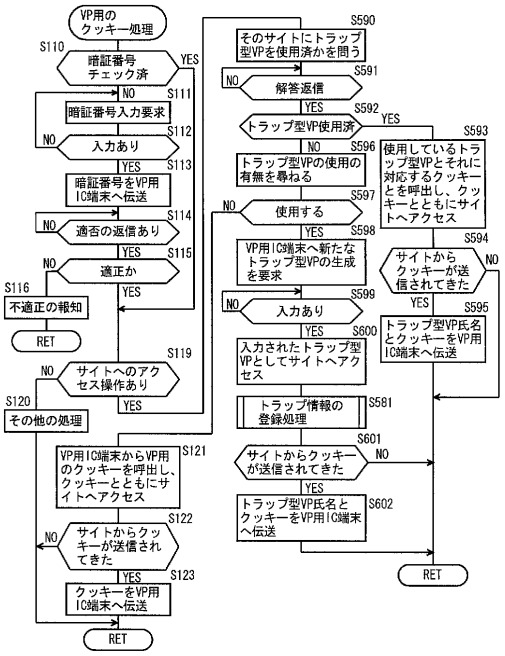
【図２５】



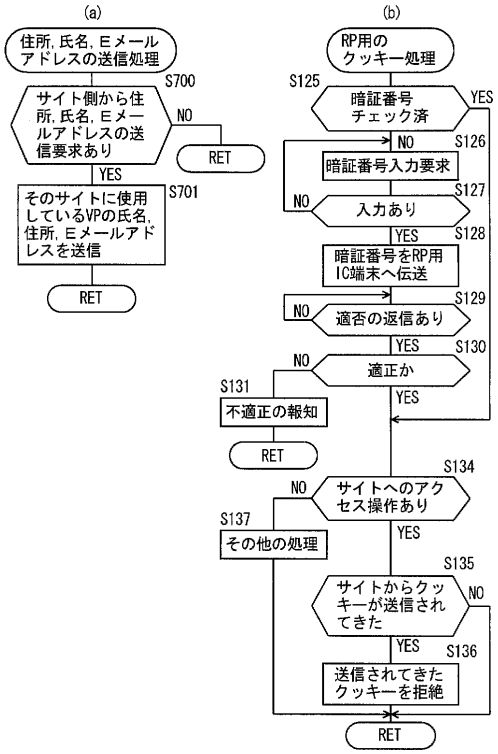
【図２６】



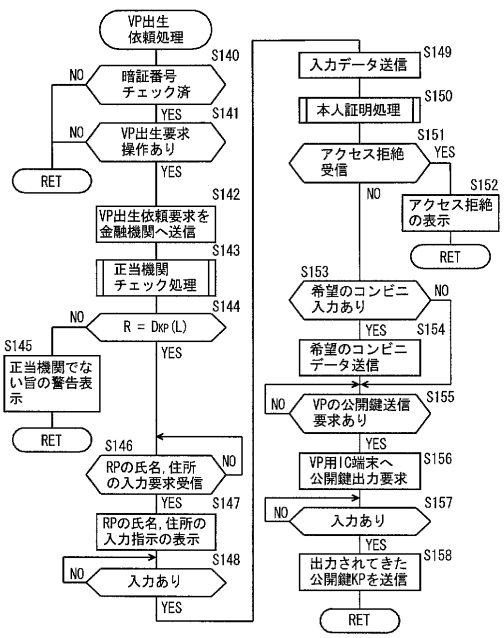
【図２７】



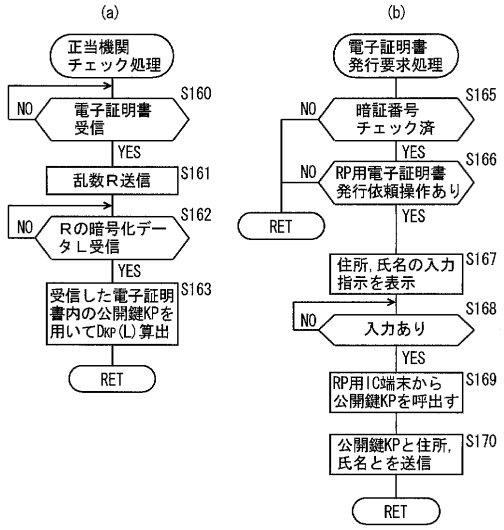
【図２８】



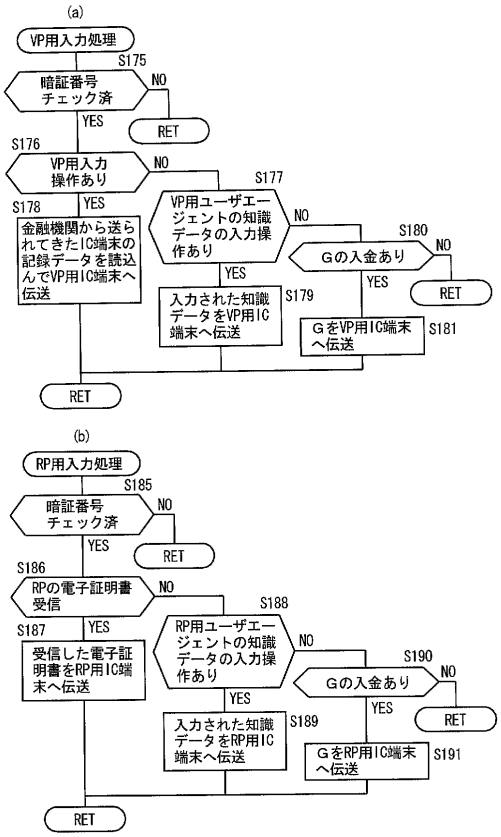
【図２９】



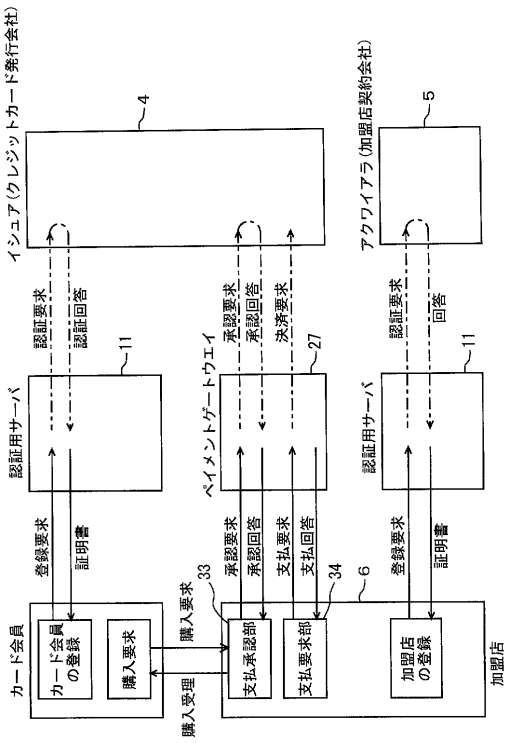
【図３０】



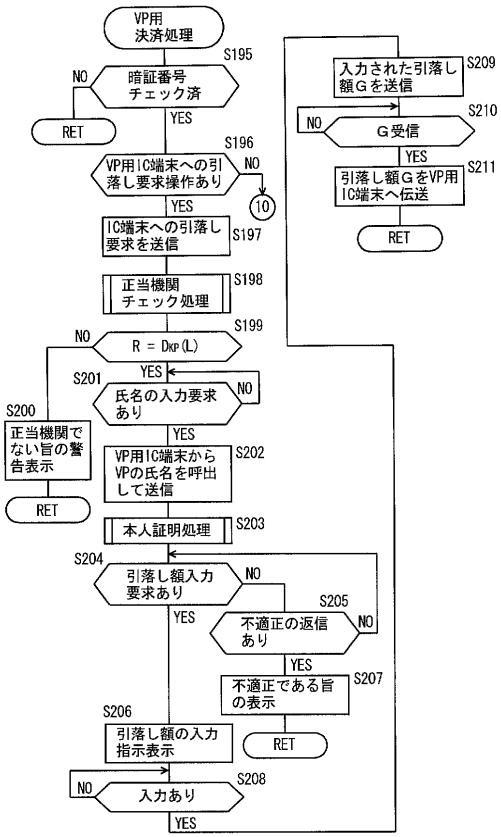
【図３１】



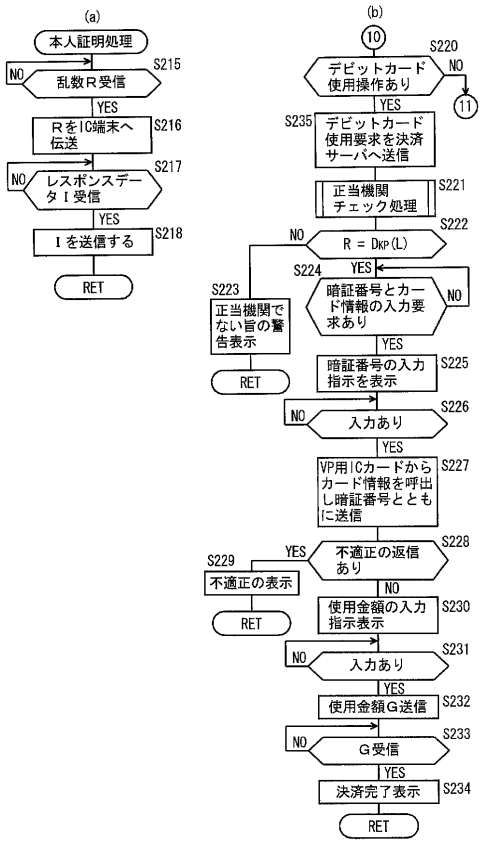
【図３２】



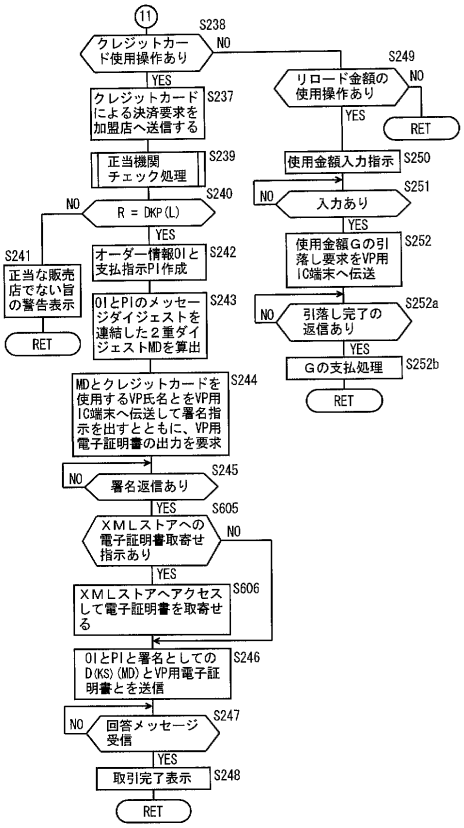
【図３３】



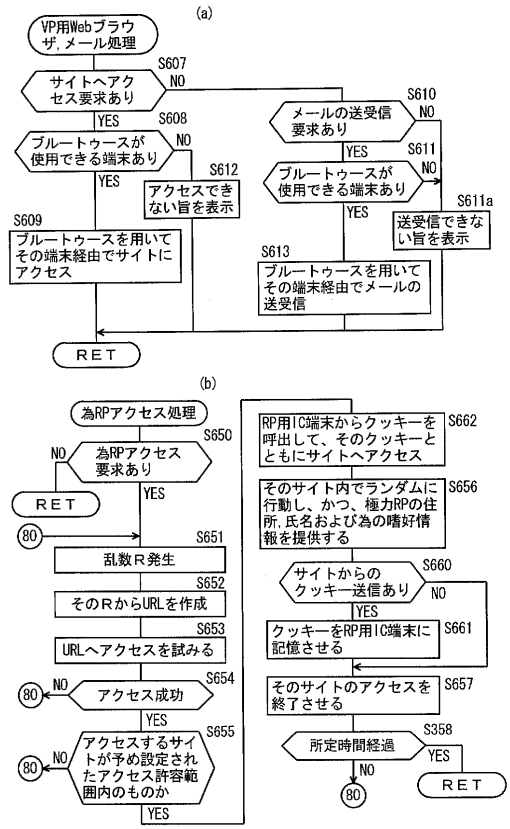
【図３４】



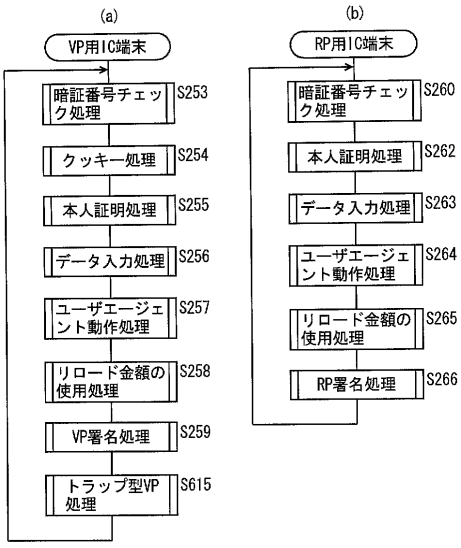
【図３５】



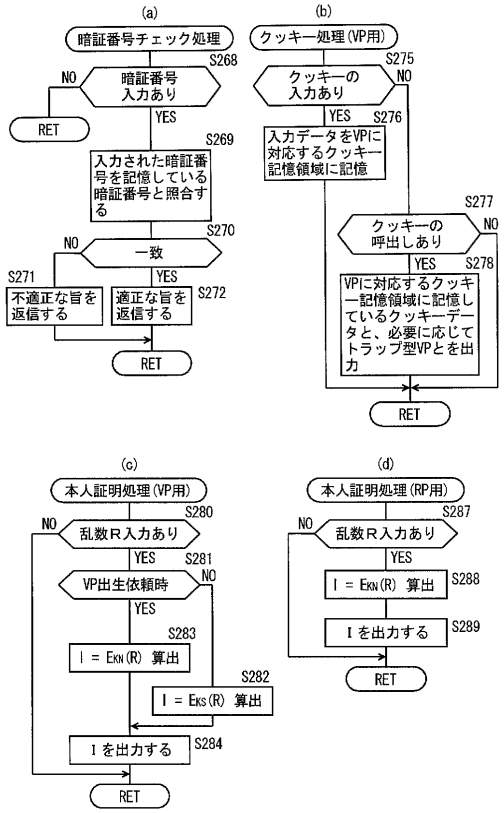
【図３６】



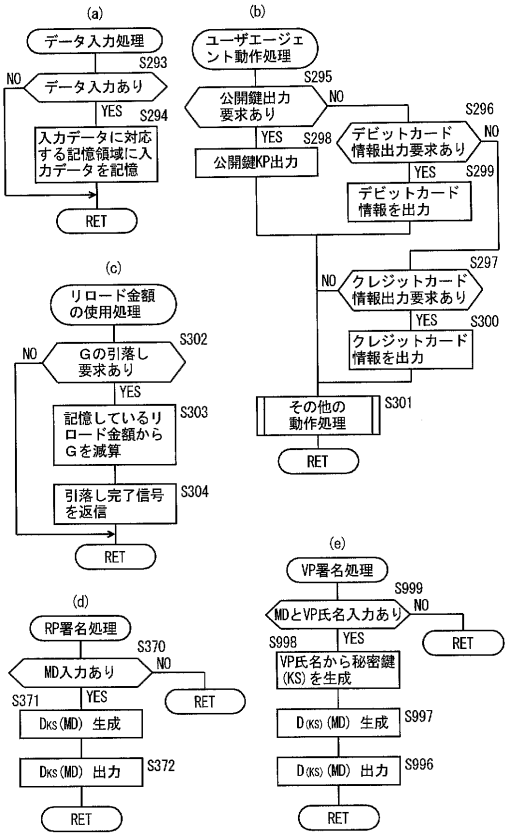
【図３７】



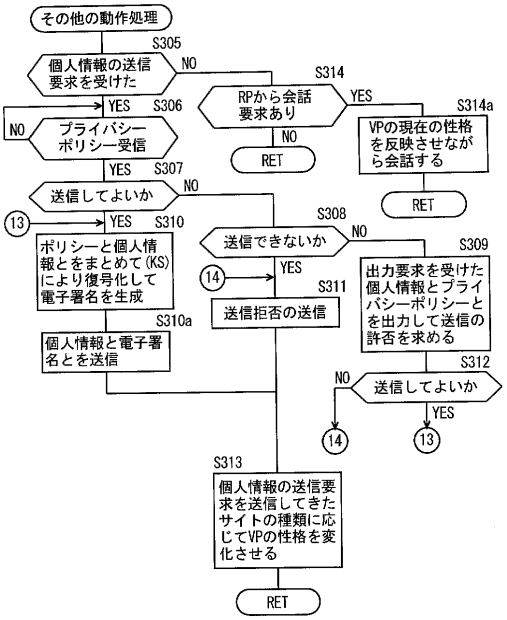
【図３８】



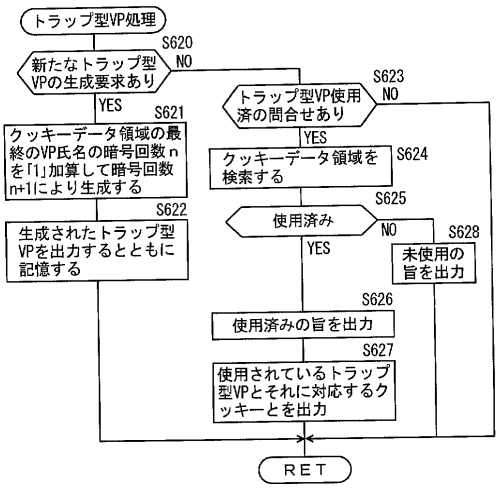
【図３９】



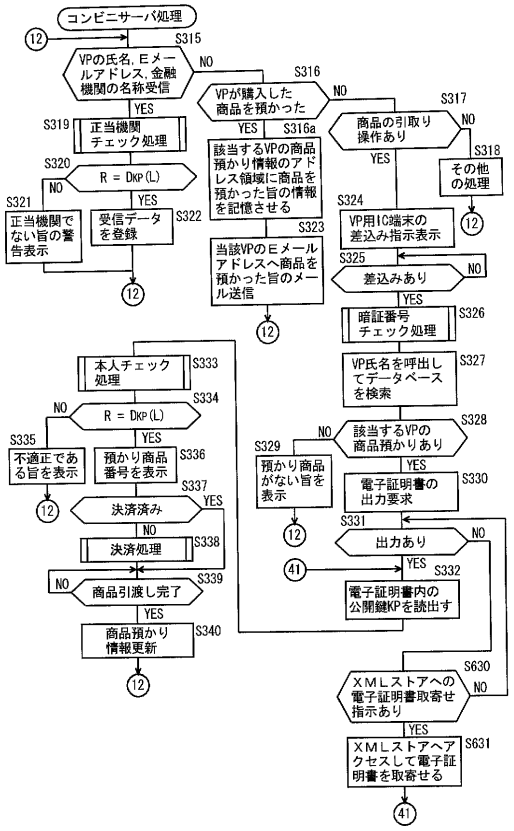
【図４０】



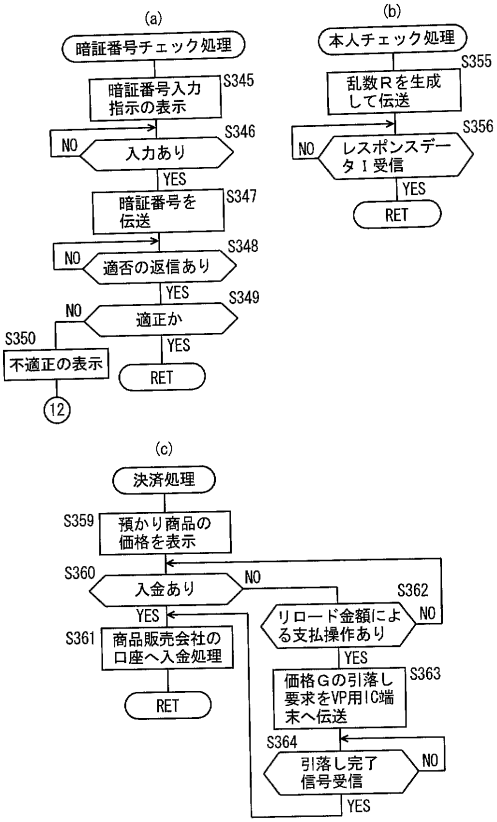
【図４１】



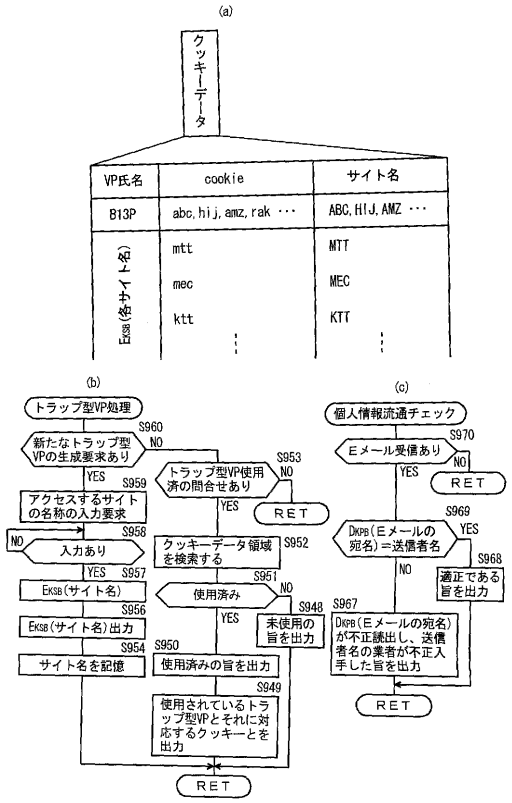
【図４２】


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
YES
S316
VPが購入した商品を預かった
NO
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
S317
商品の引取り操作あり
NO
YES
S318
その他の処理
S319
正当機関チェック処理
S320
R = DKP(L)
NO
YES
S321
正当機関でない旨の警告表示
S322
受信データを登録
S324
VP用IC端末の差込み指示表示
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
YES
S329
預かり商品がない旨を表示
S330
電子証明書の出力要求
S331
出力あり
NO
YES
41
S332
電子証明書内の公開鍵KPを読出す
S630
XMLストアへの電子証明書取寄せ指示あり
NO
YES
S631
XMLストアへアクセスして電子証明書を取寄せる
41
S333
本人チェック処理
S334
R = DKP(L)
NO
YES
S335
不適正である旨を表示
S336
預かり商品番号を表示
S337
決済済み
YES
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

【図４３】


(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I受信
YES
RET
(c)
決済処理
S359
預かり商品の価格を表示
S360
NO
入金あり
YES
S361
商品販売会社の口座へ入金処理
RET
S362
NO
リロード金額による支払操作あり
YES
S363
価格Gの引落し要求をVP用IC端末へ伝送
S364
NO
引落し完了信号受信
YES

【図４４】


(a)
クッキーデータ
VP氏名
cookie
サイト名
B13P
abc, hij, amz, rak ・・・
ABC, HIJ, AMZ ・・・
EKSB(各サイト名)
mtt
MTT
mec
MEC
ktt
KTT
(b)
トラップ型VP処理
S960
新たなトラップ型VPの生成要求あり
NO
YES
S959
アクセスするサイトの名称の入力要求
S958
NO
入力あり
YES
S957
EKSB(サイト名)
S956
EKSB(サイト名)出力
S954
サイト名を記憶
S953
トラップ型VP使用済の問合せあり
NO
YES
RET
S952
クッキーデータ領域を検索する
S951
使用済み
NO
YES
S948
未使用の旨を出力
S950
使用済みの旨を出力
S949
使用されているトラップ型VPとそれに対応するクッキーとを出力
RET
(c)
個人情報流通チェック
S970
Eメール受信あり
NO
YES
RET
S969
DKPB(Eメールの宛名)＝送信者名
YES
NO
S968
適正である旨を出力
S967
DKPB(Eメールの宛名)が不正読出し、送信者名の業者が不正入手した旨を出力
RET

フロントページの続き

合議体
審判長　清田　健一
審判官　石川　正二
審判官　須田　勝巳

(58)調査した分野(Int.Cl., ＤＢ名)
G06F17/60