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

特許第4588529号
(P4588529)

(45)発行日　平成22年12月1日(2010.12.1)　(24)登録日　平成22年9月17日(2010.9.17)

(51)Int.Cl.　　F I
*G06Q 50/00 (2006.01)*　　G06F 17/60 140
*G06F 21/20 (2006.01)*　　G06F 15/00 330A

請求項の数 2　(全 15 頁)

(21)出願番号　特願2005-147788(P2005-147788)
(22)出願日　平成17年5月20日(2005.5.20)
(65)公開番号　特開2006-323728(P2006-323728A)
(43)公開日　平成18年11月30日(2006.11.30)
審査請求日　平成20年1月15日(2008.1.15)

(73)特許権者　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100101465
弁理士　青山　正和
(74)代理人　100108453
弁理士　村山　靖彦
(72)発明者　飯野　徹
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　岩崎　公寛
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
最終頁に続く

(54)【発明の名称】サービスシステムおよび最適サービス提供方法

(57)【特許請求の範囲】
【請求項１】
通信路で接続された、サービス提供サーバと証明書管理サーバと端末とからなり、前記端末はユーザが所有し、該端末を介してユーザにサービスを提供するサービスシステムにおいて、
前記端末は、
前記ユーザの個人情報を記述した個人情報証明書と、
前記個人情報証明書に記述されている個人情報の項目名を前記サービス提供サーバに通知する証明書管理手段と、
前記サービスの実施に必要な個人情報を、前記サービスの実施に必要かつ十分であり、前記サービスの実施に即した具体的な情報に変換する最適化モジュールおよび、前記個人情報証明書の正当性を確認するとともに、前記最適化モジュールの入力となる個人情報を前記個人情報証明書から抽出する証明書検証モジュールを実行する実行手段と、
前記最適化モジュールの変換結果を前記ユーザに表示し、前記ユーザの指示に従い該実行結果の内容を変更して、前記サービス提供サーバへ出力する実行結果確認手段と
を備え、
前記サービス提供サーバは、
前記最適化モジュールの入力項目である個人情報の項目名と、前記最適化モジュールとの対応付けを記憶する記憶手段と、
前記証明書管理手段から通知される前記項目名のうち、前記サービスを実施するのに必

要な個人情報の項目名を抽出して出力する項目選択手段と、
前記記憶手段が記憶する対応付けを参照して、前記項目選択手段から受けた項目名の個人情報をその入力項目とする前記最適化モジュールを特定し、前記端末にダウンロードする最適化モジュール管理手段と、
前記実行結果確認手段の出力を受けて、前記サービスを実施するサービス実施手段とを備え、
前記証明書管理サーバは、
前記項目選択手段が出力した項目名の個人情報を前記個人情報証明書から抽出する前記証明書検証モジュールを、前記端末にダウンロードする証明書検証モジュール管理手段を備えることを特徴とするサービスシステム。

【請求項２】
通信路で接続された、サービス提供サーバと証明書管理サーバと端末とからなり、前記端末はユーザが所有し、該ユーザの個人情報証明書を備え、前記端末を介して前記ユーザに前記個人情報証明書の内容に応じたサービスを提供するサービスシステムにおける最適サービス提供方法において、
前記端末が、前記個人情報証明書に記述されている個人情報の項目名を前記サービス提供サーバに通知する第１の過程と、
前記サービス提供サーバが、前記第１の過程から受けた項目名のうち、前記サービスを実施するのに必要な項目の項目名を、抽出する第２の過程と、
前記証明書管理サーバが、第２の過程が出力した項目名を受けて、該項目名の個人情報を前記個人情報証明書から抽出する証明書検証モジュールを前記端末にダウンロードする第３の過程と、
前記端末が、前記証明書検証モジュールを実行して、前記個人情報証明書の正当性を確認するとともに、前記個人情報証明書から個人情報を抽出する第４の過程と、
前記サービス提供サーバが、前記第２の過程が出力した項目名を受けて、記憶手段が記憶する対応付けであって、前記最適化モジュールの入力項目である個人情報の項目名と、前記最適化モジュールとの対応付けを参照して、該項目名の個人情報をその入力項目とする最適化モジュールを特定し、前記端末にダウンロードする第５の過程と、
前記端末が、前記最適化モジュールを実行して、第４の過程で抽出された個人情報を、前記サービスの実施に必要かつ十分であり、前記サービスの実施に即した具体的な情報に変換する第６の過程と、
前記端末が、前記第６の過程の変換結果をユーザに表示し、前記ユーザの指示に従い内容を変更して、前記サービス提供サーバへ出力する第７の過程と、
前記サービス提供サーバが、第７の過程の出力を受けて、前記サービスを実施する第８の過程と
を備えることを特徴とする最適サービス提供方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークなどを介して提供するサービスの内容を個人情報に基づいて最適化して提供するサービスシステムおよび最適サービス提供方法に関する。

【背景技術】
【０００２】
個人情報には、氏名、住所、性別、生年月日、Ｅｍａｉｌアドレス、電話番号、身体的特徴（身長、体重、血液型）、趣味・嗜好、家族構成など様々なものがある。これらの個人情報を利用して、個々のユーザに応じたサービスを、ネットワークを介したサーバにより提供する従来のシステムでは、端末側のＩＣカードや携帯電話などのＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ：公開鍵暗号基盤）機能を持つトークンに個人情報をクライアント証明書として保持し、サービスを利用する際に、どのサービスであっても、このクライアント証明書をサービス提供者に提示している。サービスにより、

必要な個人情報は変わってくるため、どのサービスでも共通の証明書を用いているということは、あるサービスにとっては不要な項目についても、そのサービス提供者に開示していることを意味する。これは、個人情報の保護という観点から見ると好ましくないうえ、そのサービス提供者にとっては、余計なリスクを保持していることになる。

そこで、特許文献１では、開示する個人情報の項目を限定するために、区分情報と呼ぶ、いくつかの個人情報の項目についての組み合わせを設定し、端末側に各区分情報に対応した個人情報を格納したクライアント証明書を保持しておく。サービス提供者は、サービス提供に必要な個人情報を含むクライアント証明書を、端末側に対して区分情報で指定して取得することで、できる限り不要な個人情報の取得を避けるようになっている。また、特許文献２では、グループ署名を用いることで秘密情報の漏洩防止を行っている。

【特許文献１】特開２００３－３４５９３０号公報
【特許文献２】特開２００４－３２０５６２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】

しかしながら、特許文献１に示すシステムにあっては、各区分情報ごとにクライアント証明書を保持しなければならず、どのようなサービスにでも対応できるように、予め全ての組合わせについてクライアント証明書を用意しておくのは、現実的でないという問題がある。また、区分情報自体は、サービス提供者が指定した情報をサーバに送付するため、利用者自身で個人情報の送出可否を判断していない点で問題がある。また、特許文献２に示すシステムにあっては、耐タンパ装置がないと、利用が出来なくなってしまうという問題がある。

【０００４】

本発明は、このような事情に鑑みてなされたもので、その目的は、クライアント証明書を多数用意する必要がなく、耐タンパ装置が不要であり、サービス内容に沿って個人情報をサービス提供者に開示することで、不要な開示を抑えることができる、サービスシステムおよび最適サービス提供方法を提供することにある。

【課題を解決するための手段】
【０００５】

この発明は上述した課題を解決するためになされたもので、本発明の一態様は、通信路で接続された、サービス提供サーバと証明書管理サーバと端末とからなり、前記端末はユーザが所有し、該端末を介してユーザにサービスを提供するサービスシステムにおいて、前記端末は、前記ユーザの個人情報を記述した個人情報証明書と、前記サービスの実施に必要な個人情報を、前記サービスの実施に必要かつ十分であり、前記サービスの実施に即した具体的な情報に変換する最適化モジュールおよび、前記個人情報証明書の正当性を確認するとともに、前記最適化モジュールの入力となる個人情報を前記個人情報証明書から抽出する証明書検証モジュールを実行する実行手段と、前記最適化モジュールの変換結果を前記ユーザに表示し、前記ユーザの指示に従い該実行結果の内容を変更して、前記サービス提供サーバへ出力する実行結果確認手段とを備え、前記サービス提供サーバは、前記最適化モジュールを、前記端末にダウンロードする最適化モジュール管理手段と、前記実行結果確認手段の出力を受けて、前記サービスを実施するサービス実施手段とを備え、前記証明書管理サーバは、前記証明書検証モジュールを、前記端末にダウンロードする証明書検証モジュール管理手段を備えることを特徴とするサービスシステムである。

【０００６】

また、本発明の一態様は、上述のサービスシステムであって、前記端末は、前記個人情報証明書に記述されている個人情報の項目名を前記サービス提供サーバに通知する証明書管理手段を備え、前記サービス提供サーバは、前記最適化モジュールの入力項目である個人情報の項目名と、前記最適化モジュールとの対応付けを記憶する記憶手段と、前記証明書管理手段から通知される前記項目名のうち、前記サービスを実施するのに必要な個人情報の項目名を抽出して出力する項目選択手段とを備え、前記最適化モジュール管理手段は

、前記記憶手段が記憶する対応付けを参照して、前記項目選択手段から受けた項目名の個人情報をその入力項目とする前記最適化モジュールを特定し、前記端末にダウンロードし、前記証明書検証モジュール管理手段は、前記項目選択手段が出力した項目名の個人情報を前記個人情報証明書から抽出する証明書検証モジュールを、前記端末にダウンロードすることを特徴とする。

【０００７】

本発明の一態様は、通信路で接続された、サービス提供サーバと証明書管理サーバと端末とからなり、前記端末はユーザが所有し、該ユーザの個人情報証明書を備え、前記端末を介して前記ユーザに前記個人情報証明書の内容に応じたサービスを提供するサービスシステムにおける最適サービス提供方法において、前記証明書管理サーバが、前記端末にて実行される証明書検証モジュールを前記端末にダウンロードする第１の過程と、前記端末が、前記証明書検証モジュールを実行して、前記個人情報証明書の正当性を確認するとともに、前記個人情報証明書から前記サービスの実施に必要な個人情報を抽出して、出力する第２の過程と、前記サービス提供サーバが、前記端末にて実行される最適化モジュールを前記端末にダウンロードする第３の過程と、前記端末が、前記最適化モジュールを実行して、第２の過程により出力された個人情報を、前記サービスの実施に必要かつ十分であり、前記サービスの実施に即した具体的な情報に変換する第４の過程と、前記端末が、前記第４の過程の変換結果をユーザに表示し、前記ユーザの指示に従い内容を変更して、前記サービス提供サーバへ出力する第５の過程と、前記サービス提供サーバが、第５の過程の出力を受けて、前記サービスを実施する第６の過程とを備えることを特徴とする最適サービス提供方法である。

【０００８】

また、本発明の一態様は、通信路で接続された、サービス提供サーバと証明書管理サーバと端末とからなり、前記端末はユーザが所有し、該ユーザの個人情報証明書を備え、前記端末を介して前記ユーザに前記個人情報証明書の内容に応じたサービスを提供するサービスシステムにおける最適サービス提供方法において、前記端末が、前記個人情報証明書に記述されている個人情報の項目名を前記サービス提供サーバに通知する第１の過程と、前記サービス提供サーバが、前記第１の過程から受けた項目名のうち、前記サービスを実施するのに必要な項目の項目名を、抽出する第２の過程と、前記証明書管理サーバが、第２の過程が出力した項目名を受けて、該項目名の個人情報を前記個人情報証明書から抽出する証明書検証モジュールを前記端末にダウンロードする第３の過程と、前記端末が、前記証明書検証モジュールを実行して、前記個人情報証明書の正当性を確認するとともに、前記個人情報証明書から個人情報を抽出する第４の過程と、前記サービス提供サーバが、前記第２の過程が出力した項目名を受けて、記憶手段が記憶する対応付けであって、前記最適化モジュールの入力項目である個人情報の項目名と、前記最適化モジュールとの対応付けを参照して、該項目名の個人情報をその入力項目とする最適化モジュールを特定し、前記端末にダウンロードする第５の過程と、前記端末が、前記最適化モジュールを実行して、第４の過程で抽出された個人情報を、前記サービスの実施に必要かつ十分であり、前記サービスの実施に即した具体的な情報に変換する第６の過程と、前記端末が、前記第６の過程の変換結果をユーザに表示し、前記ユーザの指示に従い内容を変更して、前記サービス提供サーバへ出力する第７の過程と、前記サービス提供サーバが、第７の過程の出力を受けて、前記サービスを実施する第８の過程とを備えることを特徴とする最適サービス提供方法である。

【発明の効果】

【０００９】

この発明によれば、個人情報を扱う最適化モジュールをサービス提供サーバから端末にダウンロードして実行し、サービスの共通部分のみをサービス提供サーバで実施するため、サーバの負荷を軽減し、かつ、ユーザのプライバシーを確保しながらも個人情報に依存したサービスを実施することができる。

また、請求項２に記載の発明によれば、最適化モジュールを、ユーザが個人情報証明書

に記載した項目に従ったものとするので、個々のユーザの開示の意思に沿って、個人情報を利用するサービスを実施することができる。

【発明を実施するための最良の形態】

【００１０】

以下、図面を参照して、本発明の実施の形態について説明する。図１は、この発明の一実施形態による電子ショッピングサービスを提供するサービスシステムの構成を示す概略ブロック図である。図２は本実施形態における各装置が保持するデータを示す図である。１００は、ユーザが所有し、電子ショッピングサービスを利用するために使用する携帯端末であり、商品・個人情報選択手段１０１、モジュール実行手段１０２および証明書管理手段１０３からなる。モジュール実行手段１０２は、最適化モジュール１３０および証明書検証モジュール１４０をダウンロードして、実行するための環境である。商品・個人情報選択手段１０１は、モジュール実行手段１０２にて最適化モジュール１３０を実行した結果をユーザに表示し、選択・確認させる機能である。証明書管理手段１０３は、ユーザの個人情報が記述された個人情報証明書１０４をダウンロードして格納し、必要に応じて個人情報証明書１０４の更新要求を証明書管理サーバ１２０に行う機能である。また、証明書管理手段１０３は、格納している個人情報証明書１０４に記述されている個人情報の項目名を出力する機能を持つ。なお、個人情報証明書１０４には、これを格納している携帯端末１００の所有ユーザの個人情報が記述されている。

【００１１】

また、携帯端末１００は、その内部にデータとして、図２に示すモバイルＩＤ２００、モジュール実行モード２０１、個人情報証明書更新フラグ２０２、保存最適化モジュールリスト２０３を保持している。モバイルＩＤ２００は、携帯端末１００に固有のＩＤであり、携帯端末１００の製造時に付与される。なお、モバイルＩＤ２００は、携帯端末１００またはユーザに紐付けられたＩＤ情報であり、例えば個人情報証明書１０４とは別のユーザの証明書に記載されているＩＤ情報でもよい。モジュール実行モード２０１は、モジュール実行手段１０２にて証明書検証モジュール１４０および最適化モジュール１３０を実行する際に、携帯端末１００のネットワーク１５０への接続状態のオンライン／オフラインを管理するためのフラグである。個人情報証明書更新フラグ２０２は、個人情報証明書１０４の有効期限切れや不正が検出された場合に立てられるフラグであり、証明書管理手段１０３が個人情報証明書１０４の更新に成功すると、クリアされる。保存最適化モジュールリスト２０３は、最適化モジュール１３０を削除せずに、携帯端末１００内に保存する際に、これを管理するためにモジュール名、記録場所などが記録されるリストである。

【００１２】

証明書検証モジュール１４０は、証明書管理サーバ１２０から携帯端末１００へダウンロードされ、モジュール実行手段１０２にて動作するモジュールであり、内部にデータとして、図２に示す失効個人情報証明書番号リスト２２２、個人情報証明書検証用証明書２２３、個人情報証明書検証日時２４０、出力個人情報項目名２４１および、証明書管理サーバＵＲＬ２１１を保持する。失効個人情報証明書番号リスト２２２は、不正利用などにより失効された個人情報証明書の個人情報証明書番号が記載されているリストであり、証明書検証モジュール１４０のダウンロード時の最新の状態を証明書管理サーバ１２０より取得し、記載する。個人情報証明書検証用証明書２２３は、証明書管理サーバ１２０の証明書であり、証明書管理サーバ１２０が発行した個人情報証明書を検証するための公開鍵が記載されている。個人情報証明書検証日時２４０は、証明書検証モジュール１４０をダウンロードする際の日時が書込まれており、個人情報証明書１０４の有効期限を確認する際に、現在日時として使用される。出力個人情報項目名２４１は、証明書検証モジュール１４０が個人情報証明書１０４から取得して出力すべき個人情報の項目名である。証明書管理サーバＵＲＬ２１１は、証明書管理サーバ１２０のネットワーク１５０での位置を表すＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）である。証明書検証モジュール１４０は、個人情報証明書検証日時２４０を使用して個人情報証明書１０４の有

効期限を確認し、失効個人情報証明書番号リスト２２２に該個人情報証明書１０４の個人情報証明書番号が記載されていないこと、すなわち、該個人情報証明書１０４が失効されていないことを確認し、個人情報証明書検証用証明書２２３に記載されている公開鍵を用いて、該個人情報証明書１０４が改ざんされておらず正当なものであることを確認し、さらに、該個人情報証明書１０４から出力個人情報項目名２４１に記載されている項目の個人情報を抽出して出力する。

【００１３】

最適化モジュール１３０は、サービス提供サーバ１１０から携帯端末１００へダウンロードされ、証明書検証モジュール１４０と同様にモジュール実行手段１０２上にて動作するモジュールであり、その内部にデータとして、図２に示す、比較パラメータ２３１、必須出力情報２３２、サービス提供サーバＵＲＬ２３３および、商品情報２３４を保持する。比較パラメータ２３１は、身長や胸囲などの個人情報から洋服のサイズなどの商品選定のための情報に変換する際の閾値などのパラメータである。必須出力情報２３２は、サービス事業者がサービスを実施するのに最低限必要な情報項目のリストである。サービス提供サーバＵＲＬ２３３は、サービス提供サーバ１１０のネットワーク１５０での位置を表すＵＲＬである。商品情報２３４は、ユーザが購入を指示した商品に関する商品名称、商品番号である。最適化モジュール１３０は、前述の証明書検証モジュール１４０が出力した個人情報を受けて、比較パラメータ２３１に基づき、商品情報２３４に記載された商品のサイズなどの商品選定のための情報の作成と、サービス提供に必要な個人情報の抽出を行い、これらの情報をサービス提供サーバＵＲＬ２３３に宛てて送信する。

【００１４】

サービス提供サーバ１１０は、携帯端末１００を所有するユーザに電子ショッピングサービスを提供するサーバであり、個人情報項目選択・通知手段１１１、最適化モジュール管理手段１１２およびサービス実施手段１１３からなる。個人情報項目選択・通知１１１は、携帯端末１００から受けた個人情報項目名のうち、当該サービス提供者が利用する項目の項目名を抽出し、利用する個人情報の項目名として出力する。最適化モジュール管理手段１１２は、個人情報項目選択・通知手段１１１より、利用する個人情報の項目名を受けると、該項目を入力として動作する最適化モジュール１３０を携帯端末１００へダウンロードする。サービス実施手段１１３は、携帯端末１００にダウンロードされ、実行されている最適化モジュール１３０と通信し、電子ショッピングサービスを提供する。

また、サービス提供サーバ１１０は、その内部にデータとして、図２に示す、個人情報項目－最適化モジュール対応リスト２１０、証明書管理サーバＵＲＬ２１１、保存最適化モジュールリスト２１２を保持する。個人情報項目－最適化モジュール対応リスト２１０は、最適化モジュール１３０の入力項目である個人情報の項目名と最適化モジュール名の対応表である。保存最適化モジュールリスト２１２は、実行後に即座に消去されずに携帯端末１００内に保存されている最適化モジュール１３０のダウンロード先の携帯端末１００のモバイルＩＤ、最適化モジュール１３０の名称、ダウンロードした日時を格納しているリストである。

【００１５】

証明書管理サーバ１２０は、個人情報証明書１０４の管理を行うサーバであり、証明書検証モジュール管理手段１２１および証明書発行手段１２２からなる。証明書検証モジュール管理手段１２１は、利用する個人情報の項目名の指定を受けて、証明書検証モジュール１４０を生成し、携帯端末１００へダウンロードする。証明書発行手段１２２は、署名された個人情報証明書１０４の携帯端末１００への発行と、有効期限切れなどの場合にモバイルＩＤ２００と暗証番号を確認した携帯端末１００からの要求に応じて個人情報証明書１０４の更新を行う。

また、証明書管理サーバ１２０は、その内部にデータとして、図２に示す発行済み個人情報証明書リスト２２０、個人情報証明書発行用秘密鍵２２１、失効個人情報証明書番号リスト２２２、個人情報証明書検証用証明書２２３を保持する。発行済み個人情報証明書リスト２２０には、証明書管理サーバ１２０で発行した個人情報証明書１０４の発行先携

帯端末１００のモバイルＩＤ２００と個人情報証明書１０４の有効期限と、その通し番号である個人情報証明書番号を格納している。個人情報証明書発行用秘密鍵２２１は、個人情報証明書１０４に付加されている署名を作成する際に使用する秘密鍵である。

ネットワーク１５０は、携帯端末１００、サービス提供サーバ１１０、証明書管理サーバ１２０を接続するネットワークである。

【００１６】

個人情報証明書１０４は、ユーザがこのサービスと契約する際に、銀行口座やクレジットカードによる本人確認とあわせて、証明書管理サーバ１２０が、ユーザの提示した個人情報に有効期限、個人情報証明書番号および、個人情報証明書発行用秘密鍵による署名を付加して発行し、携帯端末１００にダウンロードする。なお、発行する際に、証明書管理サーバ１２０は、発行済み個人情報証明書リスト２２０に、ダウンロード先となるユーザが購入した携帯端末１００のモバイルＩＤ２００と、発行した個人情報証明書１０４に記載した有効期限、個人情報証明書番号、暗証番号を記録する。なお、暗証番号対してハッシュ関数などを適用したデータを暗証番号の代わりに記録してもよい。

【００１７】

次に、図３に示すシーケンス図を用いてこのサービスシステムの動作を説明する。図３のシーケンスは、携帯端末１００がＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）システムのブラウザ機能を持ち、サービス提供サーバ１１０がＷＷＷシステムのサーバ機能を持ち、電子ショッピングサービスにて販売している商品の一覧を、当該機能により発信しており、ユーザが携帯端末１００のブラウザ機能を操作して、当該電子ショッピングサービスにて販売している商品の一覧をサービス提供サーバ１１０から取得して表示し、これらの中から例えばＴシャツを買うことを決め、購入の入力をした状態から始まっている。ユーザがこの購入の入力を携帯端末１００にすると、証明書管理手段１０３は、格納している個人情報証明書１０４に記述されている項目名を全て、例えば、

“氏名、生年月日、血液型、身長、体重、住所、電話番号、クレジットカード番号”・・・（１）

というように、個人情報項目選択・通知手段１１１へ通知する（Ｓ１０）。個人情報項目選択・通知手段１１１は、証明書管理手段１０３より（１）に示した項目名を受けると、受けた項目名の中から当該電子ショッピングサービスのＴシャツ購入で用いる個人情報の項目名である

“氏名、身長、体重、住所、電話番号、クレジットカード番号”・・・（２）

を最適化モジュール管理手段１１２へ出力する（Ｓ１１）と共に、証明書管理サーバ１２０のＵＲＬを証明書管理サーバＵＲＬ２１１より取得して、証明書検証モジュール管理手段１２１へネットワーク１５０を介して通知する（Ｓ１２）。証明書検証モジュール管理手段１２１は、個人情報項目選択・通知手段１１１から（２）に示した項目名を受けると、これらの項目名を出力個人情報項目名２４１に格納し、現在日時を個人情報証明書検証日時２４０に格納し、証明書管理サーバ１２０が保持する失効個人情報証明書番号リスト２２２を証明書検証モジュール１４０に格納した後、この証明書検証モジュール１４０を携帯端末１００のモジュール実行手段１０２へダウンロードする（Ｓ１３）。

【００１８】

モジュール実行手段１０２は、証明書検証モジュール管理手段１２１から、証明書検証モジュール１４０を受けると、これを実行する。すなわち、まずネットワーク１５０との接続を切り、モジュール実行モード２０１にオフラインを登録した後、個人情報証明書１０４の正当性について、次の３点を確認する。１点目は、証明書検証モジュール１４０の個人情報証明書検証日時２４０が個人情報証明書１０４の有効期限を越えていないこと。２点目は、署名の正当性、すなわち、個人情報証明書１０４が偽造されたものや、改ざんされたものでないことを確認することであり、これは、証明書検証モジュール１４０の個人情報証明書検証用証明書２２３から個人情報証明書発行用秘密鍵２２１と対になる公開鍵を取り出し、個人情報証明書１０４の署名が正しいこと、つまり、該個人情報証明書１０４の記載に対して個人情報証明書発行用秘密鍵２２１にて署名が作成されていることを

確認することで行う。３点目は、該個人情報証明書１０４が失効されていないことであり、これは、該個人情報証明書１０４の個人情報証明書番号が、証明書検証モジュール１４０の失効個人情報証明書番号リストにないことで確認する。次に、出力個人情報項目名２４１に格納されている各項目名の個人情報を個人情報証明書１０４から取り出して、例えば、

“氏名：山田太郎、身長：１７２ｃｍ、体重：６５Ｋｇ、住所：東京都ＸＸＸ、電話番号：０３－ＸＸＸＸ、クレジットカード番号：１２３４ＸＸＸＸ”・・・（３）

を得る（Ｓ１４）。

【００１９】

ここで、前述の個人情報証明書１０４の正当性確認で失敗した場合は、モジュール実行手段１０２は、個人情報証明書更新フラグ２０２を立てて、証明書管理手段１０３へ、証明書更新要求を発行する（Ｓ１５）。証明書管理手段１０３は、個人情報証明書更新フラグ２０２を参照して証明書更新要求を受けると、ユーザに（１）に示した個人情報および携帯端末１００購入時に登録した暗証番号を入力させる。なお、暗証番号の代わりに携帯端末１００や携帯端末１００の装着するＩＣチップのＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）で本人認証をしてもよく、バイオメトリクス個人認証方法で代用してもよい。証明書管理手段１０３は、ユーザの入力した個人情報および暗証番号を受けると、ネットワーク１５０との接続を行い、証明書検証モジュール１４０の証明書管理サーバＵＲＬ２１１を参照して、証明書管理サーバ１２０の証明書発行手段１２２へ、携帯端末１００のモバイルＩＤ２００、入力された個人情報および暗証番号とともに個人情報証明書発行要求を通知する（Ｓ１６）。証明書発行手段１２２は、携帯端末１００から受けたモバイルＩＤ２００と暗証番号の整合性を発行済み個人情報証明書リスト２２０にて確認した後、携帯端末１００から受けた個人情報を元に当該ユーザの個人情報証明書１０４を作成して、携帯端末１００の証明書管理手段１０３へ、ダウンロードする（Ｓ１７）。証明書管理手段１０３は、新しい個人情報証明書１０４をダウンロードされると、個人情報証明書更新フラグ２０２をクリアし、あとは、個人情報証明書１０４の正当性を確認した場合と同様にＳ１４からのシーケンスを実施する。

【００２０】

一方、最適化モジュール管理手段１１２は、個人情報項目選択・通知手段１１１から、利用する個人情報の項目名として、（２）に示した項目名を受ける（Ｓ１１）と、個人情報項目－最適化モジュール対応リスト２１０から（２）に示した項目と入力となる個人情報項目が一致する最適化モジュール１３０を探し出して、商品情報２３４としてＴシャツ、比較パラメータ２３１としてＴシャツのサイズの閾値（ここでは、例えば、身長１６５～１７５ｃｍかつ体重５０～６５Ｋｇであれば、“サイズ：Ｍ”）を格納し、これをモジュール実行手段１０２へダウンロードする（Ｓ１８）。モジュール実行手段１０２は、証明書検証モジュール管理手段１２１から、最適化モジュール１３０を受け、前述した証明書検証モジュール１４０の実行が終わると、これを実行して、まず図４に示すステップＳａ１０１を実行し、証明書検証モジュール１４０の実行結果である（３）に示した個人情報から１項目を取り込む。ここでは、１項目目の“氏名：山田太郎”を取込んだとする。ステップＳａ１０２では、全個人情報の取り込みが終了していないので条件が成立せず、ステップＳａ１０３に移る。ステップＳａ１０３では、商品配達に氏名は必要であり、サービス提供サーバ１１０に直接出力する項目なので、条件が成立して、ステップＳａ１０８に移る。ステップＳａ１０８では、氏名は代用する個人情報ではないので条件が成立せず、ステップＳａ１０９に移る。ここで、代用する個人情報とは、例えば、ユーザが電話番号の開示を拒否して代用の連絡先としてメールアドレスを開示する場合のメールアドレスに当たる情報を指している。

【００２１】

ステップＳａ１０９では、“氏名：山田太郎”を個人情報リストに追加する。次に、ステップＳａ１０１に戻って、（３）に示した個人情報から、２項目目の“身長１７２ｃｍ”を取込む。ステップＳａ１０２では、１項目目と同様に全個人情報の取込みは終了して

いないので条件が成立せず、ステップＳａ１０３に移る。ステップＳａ１０３では、身長は直接出力しない項目なので条件が成立せずに、ステップＳａ１０４で比較用パラメータ算出として、Ｔシャツのサイズの選択を行う。このステップＳａ１０４では、比較パラメータ２３１を参照して、身長１６５～１７５ｃｍかつ体重５０～６５Ｋｇであれば、“サイズ：Ｍ”であるとする。身長はサイズＭの範囲内であるが、体重はまだ取込んでいないので、ステップＳａ１０５で他項目として“体重”が必要という条件が成立し、再度、ステップＳａ１０１を実行し、“体重：６５Ｋｇ”を取込む。ステップＳａ１０２、Ｓａ１０３と、身長を取込んだ場合と同様にし、ステップＳａ１０４では、“身長：１７２ｃｍ、体重６５：Ｋｇ”より、“サイズ：Ｍ”を選択する。すると、次のステップＳａ１０５では、サイズの選択に他の項目は不要なので、条件が成立せず、ステップＳａ１０６に移って、商品情報２３４の“Ｔシャツ”と“サイズ：Ｍ”を商品情報リストに追加する。あとは、氏名の場合と同様にして、（３）に示した情報を、住所、電話番号、クレジットカード番号と取込んでいき、個人情報リストに追加する。ここで、個人情報リストと商品情報リストは次のようになっている。

個人情報リスト；“氏名：山田太郎、住所：東京都ＸＸＸ、電話番号：０３－ＸＸＸＸ、クレジットカード番号：１２３４ＸＸＸＸ”・・・（４）

商品情報リスト；“商品：Ｔシャツ、サイズ：Ｍ”・・・（５）

【００２２】

（３）に示した個人情報を全て取込むと、ステップＳａ１０２で、全個人情報取込み終了の条件が成立するので、図５のステップＳａ１１１に移る。ステップＳａ１１１では、（５）に示した商品情報リストの変更可否を確認する。当該最適化モジュール１３０にてパラメータを設定した項目があれば、変更可能であるとして、ステップＳａ１１２に移る。ここでは、当該最適化モジュール１３０が個人情報である身長および体重に基づきＴシャツのサイズを選択したので、変更可能であるとして、ステップＳａ１１２に移る。ステップＳａ１１２では、商品・個人情報選択手段１０１に、（５）に示した商品情報リストである“商品：Ｔシャツ、サイズ：Ｍ”を出力する（Ｓ１９）。商品・個人情報選択手段１０１は、モジュール実行手段１０２から、“商品：Ｔシャツ、サイズ：Ｍ”を受けると、これを携帯端末の画面に表示する。ユーザは、これを確認し、自分の好みにより、任意のサイズに変更する。ここでは、変更せずにそのままにしたとして、説明する。商品・個人情報選択手段１０１は、そのまま“商品：Ｔシャツ、サイズ：Ｍ”をモジュール実行手段１０２に返す。

【００２３】

モジュール実行手段１０２は、商品・個人情報選択手段１０１の応答を受けると、次のステップＳａ１１３に移り、商品情報リスト“商品：Ｔシャツ、サイズ：Ｍ”を再び、商品・個人情報選択手段１０１に出力する（Ｓ２０）。商品・個人情報選択手段１０１は、モジュール実行手段１０２から、商品情報リスト“商品：Ｔシャツ、サイズ：Ｍ”を受けると、これを携帯端末の画面に表示する。なお、ここでは、商品を一つだけ購入したため、ほぼ同様のことを２回繰り返しているが、複数の商品を購入しようとしていた場合などは、１回目は、それぞれの商品について最適化モジュール１３０の選択結果についてユーザに確認を求めており、２回目は最終確認として、それらを全て購入するかをユーザに確認している。ここでは、購入するものはＴシャツを１枚のみなので、そのまま購入することを選択したとして説明する。商品・個人情報選択手段１０１は、そのまま“商品：Ｔシャツ、サイズ：Ｍ”をモジュール実行手段１０２に返す。なお、ここでは、商品ごとに最適化モジュール１３０があるという前提だが、例えば同じ種類の商品には一つで代用してもよく、また商品のなかでも、高額のものにならって、低額の物の確認を省略してもよい。

【００２４】

モジュール実行手段１０２は、商品・個人情報選択手段１０１の応答を受けると、次のステップＳａ１１４に移り、（４）に示した個人情報リストを、商品・個人情報選択手段１０１に出力する（Ｓ２１）。商品・個人情報選択手段１０１は、モジュール実行手段１

０２から、個人情報リストを受けるとこれを携帯端末１００の画面に表示する。ユーザは、これらの個人情報のうち、サービス提供者に開示しても良い項目を選択する。ここでは、全ての項目を開示して良いと選択したとして説明し、ユーザがサービス実施に必要な項目の開示を拒否した場合については、後に詳述する。ユーザが全ての項目を選択すると、商品・個人情報選択手段１０１は、（４）に示した個人情報リストをそのままモジュール実行手段１０２へ返す。モジュール実行手段１０２は、商品・個人情報選択手段１０１の応答を受けると、ステップＳａ１１５に移り、送信内容である（４）の個人情報リストおよび（５）の商品情報リストで、最適化モジュール１３０内に保持しているデータである必須出力情報２３２と比較して、購入に必要な情報が揃っていることを確認する。

【００２５】

ここでは、情報が揃っているので、ステップＳａ１１６の条件は成立し、次のステップＳａ１１７に移り、モジュール実行モード２０１をオンラインに設定した後、ネットワーク１５０と接続する。ステップＳａ１１７では、次にサービス提供サーバＵＲＬ２３３を参照して、サービス提供サーバ１１０のサービス実施手段１１３へ、ステップＳａ１１５にて確認した個人情報リスト（４）および商品情報リスト（５）を送信する（Ｓ２２）。サービス実施手段１１３は、モジュール実行手段１０２から（４）および（５）を受けると、（５）の商品情報リストで指定された商品の（４）の個人情報リストで指定された顧客への販売処理（決済処理、配達手配など）を行う。販売処理が正常に終了すると、サービス実施手段１１３は、モジュール実行手段１０２に、正常終了とモジュール削除の通知を送信する。モジュール実行手段１０２は、ステップＳａ１１８で、サービス実施手段１１３から正常終了とモジュール削除の通知を受けると、ステップＳａ１１９の条件が成立しているので、ステップＳａ１２０に移り、実行中であった最適化モジュール１３０を終了および削除する。

【００２６】

なお、商品を配達するようなサービスではなく、情報を継続的に提供するようなサービスや情報を提供するまでに時間を要するサービスなどの場合には、サービス実施手段１１３は、保存最適化モジュールリスト２１２に、携帯端末１００のモバイルＩＤ２００、最適化モジュール１３０のモジュール名およびダウンロード日時を登録するとともに、正常終了とモジュール保存を携帯端末１００のモジュール実行手段１０２に通知する。すると、ステップＳａ１１９では、応答はモジュール削除ではないので、条件が成立せず、ステップＳａ１２１移り、保存最適化モジュールリスト２０３に登録するとともに、最適化モジュール１３０を保存しておき（Ｓａ１２１）、後にユーザがサービスを利用するときに、保存最適化モジュールリスト２１２を参照して、これを起動する。

【００２７】

ここで、最適化モジュール１３０にて、個人情報をサービス実施に即した情報に変換する例として、身長および体重から、Ｔシャツのサイズを得る例を挙げたが、この他に生年月日や年齢、職業から、未成年者の購入制限やシルバー割引、学生割引を行うようにしても良い。

また、最適化モジュール１３０および証明書検証モジュール１４０を携帯端末１００にネットワーク１５０を介してダウンロードするようにしたが、携帯端末１００が備える赤外線通信や近距離無線通信などのローカル通信を用いても良く、この場合は、コマンドを受けて動作する汎用的なアプリケーションを予め携帯端末１００内にダウンロードしておき、最適化モジュール１３０および証明書検証モジュール１４０をダウンロードする代わりに、コマンドやパラメータを携帯端末１００へ送信することで、同様の機能を実現しても良い。

また、個人情報証明書１０４は携帯端末１００内に格納するとしたが、携帯端末１００に装着するＩＣチップを用意し、これに格納してもよい。この場合、証明書検証モジュール１４０は、携帯端末１００ではなく、このＩＣチップにて実行するようにしても良い。

さらに、証明書検証モジュール１４０および最適化モジュール１３０の正当性を検証する仕組みを、携帯端末１００もしくはＩＣチップに入れても良い。

【００２８】
このように、携帯端末１００には、１つの個人情報証明書１０４を保持しておくだけで、格納している個人情報およびサービス内容に応じた最適化モジュール１３０をダウンロードして実行するため、様々なサービスに対応することができる上、ユーザは、毎回情報を入力する必要がないので、携帯端末を用いたサービスに適している。また、サービス提供者に対して、個人情報を直接開示するのではなく、最適化モジュール１３０がオフライン中に携帯端末１００にて動作し、個人情報をサービス実施に即した情報に変換してサービス提供サーバ１１０に送信するため、例え、サービス提供者にて個人情報の漏洩が起こったとしても、漏洩する情報を最小限に抑えることができる。このため、個人情報として、例えば個人の病気の情報などに応じて処方箋を出すというような、プライバシー性の高い個人情報を活用したサービスも実現可能である。
また、最適化モジュール管理手段１１２は、最適化モジュール１３０を、個人情報証明書１０４に記載されている項目に基づき作成するため、ユーザにより異なった項目を個人情報証明書１０４に記載していたとしても、これらに対応することができる。
【００２９】
ステップＳａ１１４の説明にて、ユーザが全ての個人情報リストの開示を選択したとして説明し、サービスの実施に必要な項目の開示を拒否した場合については後に詳述するとしたが、このような場合について説明する。例えば、ユーザがサービス提供者には住所の開示を拒否したが、配達業者であれば開示しても良いと考えた場合の概略を、図６のフロー図を用いて説明する。この図で、１６０は、予めユーザのＩＤと住所が登録されており、ＩＤの通知を受けることで配達の手配が可能な配達業者サーバである。
【００３０】
ユーザがサービス提供者には住所の開示を拒否、すなわち、ステップＳｂ２００にて、住所の開示が拒否されるため、携帯端末１００の商品・個人情報選択手段１０１はユーザの指示に従い、住所を除いた個人情報リストを生成して、
“氏名：山田太郎、電話番号：０３－ＸＸＸＸ、クレジットカード番号：１２３４ＸＸＸＸ”・・・（６）
とし、これを、ステップＳｂ２０２にて、サービス提供サーバ１１０に送信する。すると、サービス提供サーバ１１０では、これを受けると、ステップＳｂ２０３にて（６）に示した個人情報リストに、サービス実施に必要な項目が全て揃っているか、確認する。ここでは、項目として住所が不足しているため、その場合の制約事項および代用サービスとして、他の配達業者を利用可能なことを、ステップＳｂ２０５で送信する。携帯端末１００は、これを受けて、制約事項を表示するので、ユーザはこれの確認を行い（Ｓｂ２０６）、さらに、サービス提供者に住所を開示せずにサービスを受ける方法として、他の配達業者の利用を可能なことと、この配達事業者を利用するために事前に住所などと共に登録してあった自身のＩＤ（代用可能ＩＤ）が携帯端末１００に表示されるので、これを確認する。
【００３１】
次に、ユーザが、代用可能ＩＤを配達業者サーバ１６０へ送信（Ｓｂ２０９）、かつ、代用可能ＩＤはサービス提供者には非公開（Ｓｂ２１２）を選択すると、携帯端末１００と配達業者サーバ１６０の間で、相互認証と鍵交換を行う（Ｓｂ２１５）。さらに、配達業者サーバ１６０では、代用可能ＩＤをサービス提供サーバ１１０経由で受け取ることを許可する署名を生成して、携帯端末１００に送信する（Ｓｂ２１６）。携帯端末１００は、この署名を受けると、さきほど配達業者サーバ１６０と交換した鍵で、自身の代用可能ＩＤを暗号化し、さきの署名とともに、サービス提供サーバ１１０に送信する（Ｓｂ２１７）。サービス提供サーバ１１０は、この署名と、暗号化された代用可能ＩＤを受けると、署名を検証した後、暗号化されたままの代用可能ＩＤを配達業者サーバ１６０に送信する。ここで、サービス提供サーバ１１０は、鍵を持っていないため、代用可能ＩＤの暗号を解くことはできない。配達業者サーバ１６０は、これを受けると携帯端末１００と交換した鍵でこれを復号化して、代用可能ＩＤを得て、事前に登録してあった住所に基づき配

達を行う。また、このことをサービス提供サーバ１１０に通知する（Ｓｂ２１９）。これを受けて、サービス提供サーバ１１０は、商品の販売処理を続ける（Ｓｂ２２０）。

【図面の簡単な説明】

【００３２】

【図１】この発明の一実施形態による電子ショッピングサービスのサービスシステムの構成を示すブロック図である。

【図２】本実施形態における各装置が保持するデータを示す図である。

【図３】本実施形態における商品購入時のシーケンスを示すシーケンス図である。

【図４】本実施形態における最適化モジュール１３０のフローチャート（その１）である。

【図５】本実施形態における最適化モジュール１３０のフローチャート（その２）である。

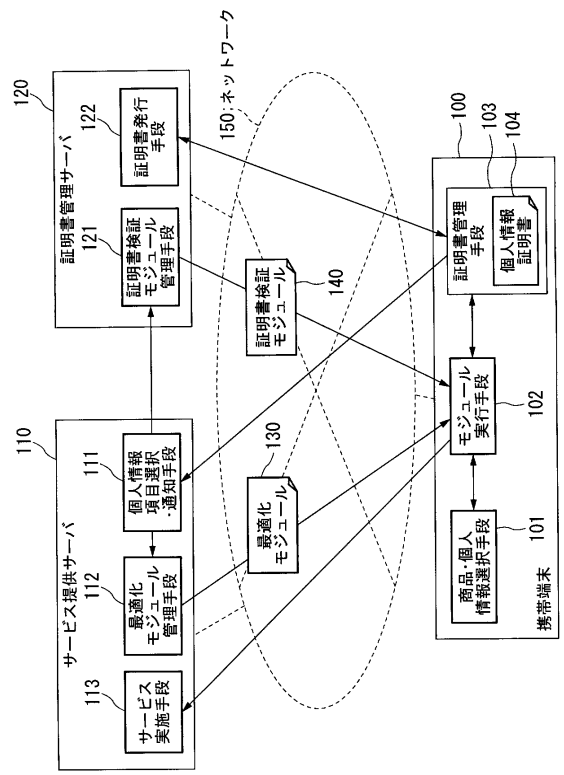
【図６】本実施形態における配達事業者のみに住所などを開示する場合を説明する図である。

【符号の説明】

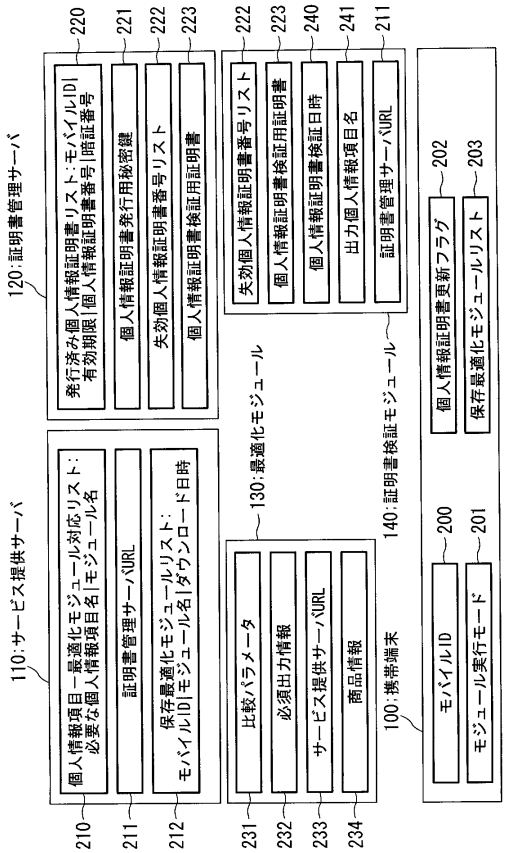
【００３３】

１００…携帯端末
１０１…商品・個人情報選択手段
１０２…モジュール実行手段
１０３…証明書管理手段
１０４…個人情報証明書
１１０…サービス提供サーバ
１１１…個人情報項目選択・通知手段
１１２…最適化モジュール管理手段
１１３…サービス実施手段
１２０…証明書管理サーバ
１２１…証明書検証モジュール管理手段
１２２…証明書発行手段
１３０…最適化モジュール
１４０…証明書検証モジュール
１５０…ネットワーク
１６０…配達業者サーバ
２００…モバイルＩＤ
２０１…モジュール実行モード
２０２…個人情報証明書更新フラグ
２０３…保存した最適化モジュールリスト
２１０…個人情報項目－最適化モジュール対応リスト
２１１…証明書管理サーバＵＲＬ
２１２…保存最適化モジュールリスト
２２０…発行済み個人情報証明書リスト
２２１…個人情報証明書発行秘密鍵
２２２…失効個人情報証明書番号リスト
２２３…個人情報証明書検証用証明書
２３１…比較パラメータ
２３２…必須出力情報
２３３…サービス提供サーバＵＲＬ
２３４…商品情報
２４０…個人情報証明書検証日時
２４１…出力個人情報項目名

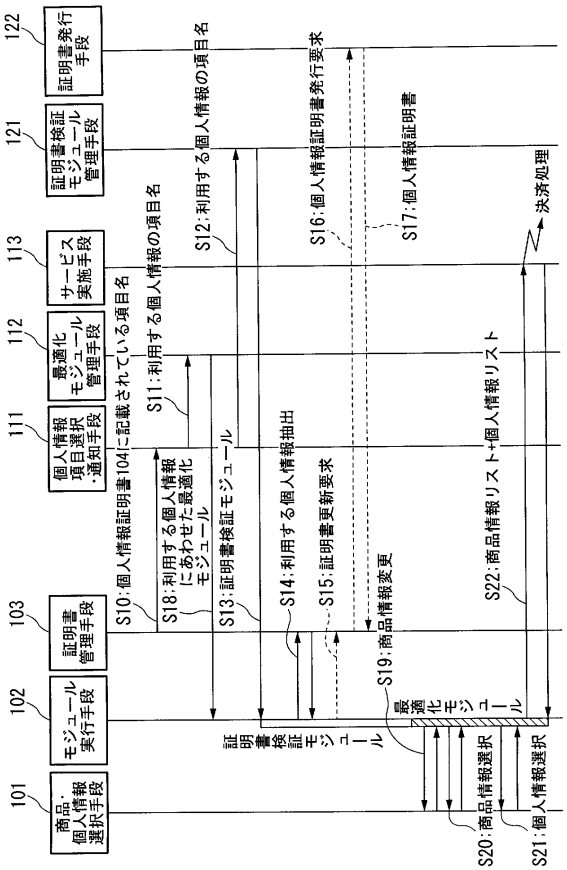
【図１】


120
証明書管理サーバ
121
証明書検証モジュール管理手段
122
証明書発行手段
150:ネットワーク
110
サービス提供サーバ
111
個人情報項目選択・通知手段
112
最適化モジュール管理手段
113
サービス実施手段
130
最適化モジュール
140
証明書検証モジュール
100
証明書管理手段
103
個人情報証明書
104
102
モジュール実行手段
101
商品・個人情報選択手段
携帯端末

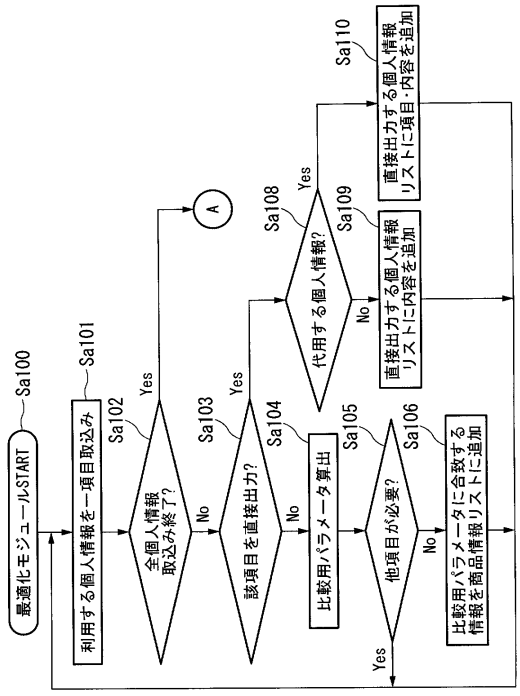
【図２】


120:証明書管理サーバ
発行済み個人情報証明書リスト:モバイルID|有効期限|個人情報証明書番号|暗証番号
220
個人情報証明書発行用秘密鍵
221
失効個人情報証明書番号リスト
222
個人情報証明書検証用証明書
223
110:サービス提供サーバ
個人情報項目－最適化モジュール対応リスト:必要な個人情報項目名|モジュール名
210
証明書管理サーバURL
211
保存最適化モジュールリスト:モバイルID|モジュール名|ダウンロード日時
212
130:最適化モジュール
比較パラメータ
231
必須出力情報
232
サービス提供サーバURL
233
商品情報
234
失効個人情報証明書番号リスト
222
個人情報証明書検証用証明書
223
個人情報証明書検証日時
240
出力個人情報項目名
241
証明書管理サーバURL
211
140:証明書検証モジュール
100:携帯端末
モバイルID
200
モジュール実行モード
201
個人情報証明書更新フラグ
202
保存最適化モジュールリスト
203

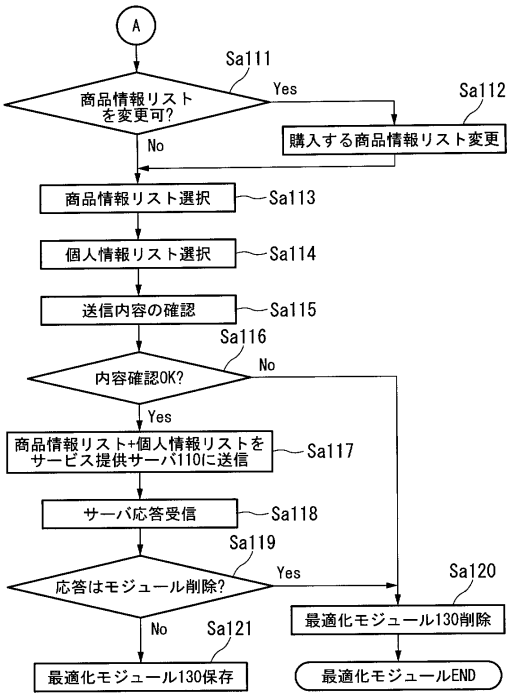
【図３】


101
商品・個人情報選択手段
102
モジュール実行手段
103
証明書管理手段
111
個人情報項目選択・通知手段
112
最適化モジュール管理手段
113
サービス実施手段
121
証明書検証モジュール管理手段
122
証明書発行手段
S10:個人情報証明書104に記載されている項目名
S11:利用する個人情報の項目名
S12:利用する個人情報の項目名
S13:証明書検証モジュール
S14:利用する個人情報抽出
S15:証明書更新要求
S16:個人情報証明書発行要求
S17:個人情報証明書
S18:利用する個人情報にあわせた最適化モジュール
S19:商品情報変更
S20:商品情報選択
S21:個人情報選択
S22:商品情報リスト+個人情報リスト
決済処理
証明書検証モジュール
最適化モジュール

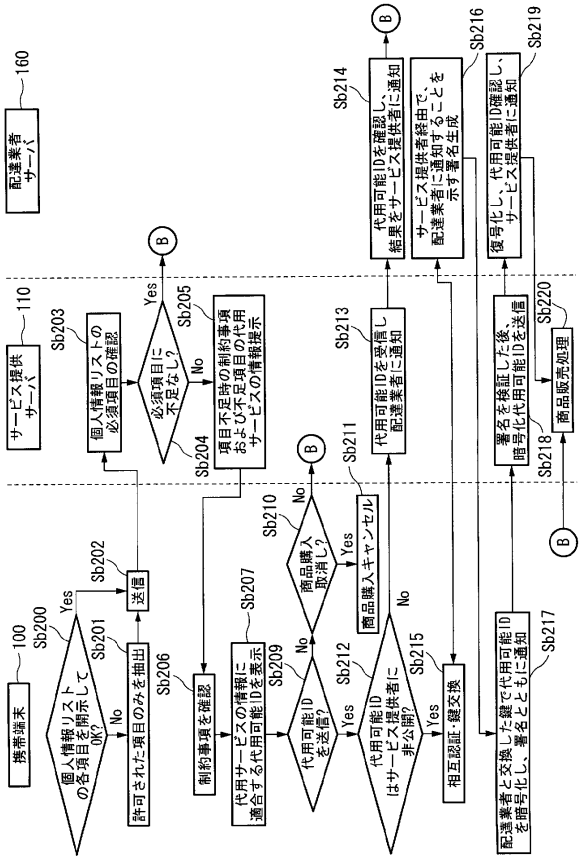
【図４】


最適化モジュールSTART
Sa100
利用する個人情報を一項目取込み
Sa101
全個人情報取込み終了?
Sa102
Yes
No
A
該項目を直接出力?
Sa103
Yes
No
比較用パラメータ算出
Sa104
他項目が必要?
Sa105
Yes
No
比較用パラメータに合致する情報を商品情報リストに追加
Sa106
代用する個人情報?
Sa108
Yes
No
直接出力する個人情報リストに内容を追加
Sa109
直接出力する個人情報リストに項目・内容を追加
Sa110

【図５】


A
Sa111
商品情報リストを変更可?
Yes
Sa112
購入する商品情報リスト変更
No
商品情報リスト選択
Sa113
個人情報リスト選択
Sa114
送信内容の確認
Sa115
Sa116
内容確認OK?
No
Yes
商品情報リスト+個人情報リストをサービス提供サーバ110に送信
Sa117
サーバ応答受信
Sa118
Sa119
応答はモジュール削除?
Yes
Sa120
最適化モジュール130削除
No
Sa121
最適化モジュール130保存
最適化モジュールEND

【図６】


160
配達業者サーバ
110
サービス提供サーバ
100
携帯端末
Sb200
個人情報リストの各項目を開示してOK?
Yes
No
Sb201
許可された項目のみを抽出
Sb202
送信
Sb203
個人情報リストの必須項目の確認
Sb204
必須項目に不足なし?
Yes
No
Sb205
項目不足時の制約事項および不足項目の代用サービスの情報提示
Sb206
制約事項を確認
Sb207
代用サービスの情報に適合する代用可能IDを表示
Sb209
代用可能IDを送信?
No
Yes
Sb210
商品購入取消し?
No
Yes
Sb211
商品購入キャンセル
Sb212
代用可能IDはサービス提供者に非公開?
No
Yes
Sb213
代用可能IDを受信し配達業者に通知
Sb214
代用可能IDを確認し、結果をサービス提供者に通知
Sb215
相互認証・鍵交換
Sb216
サービス提供者経由で、配達業者に通知することを示す署名生成
Sb217
配達業者と交換した鍵で代用可能IDを暗号化し、署名とともに通知
Sb218
署名を検証した後、暗号化代用可能IDを送信
Sb219
復号化し、代用可能ID確認し、サービス提供者に通知
Sb220
商品販売処理
B

フロントページの続き

審査官　山崎　誠也

(56)参考文献　特開２００３－３３８８１６（ＪＰ，Ａ）
国際公開第２００４／０５３７５９（WO，Ａ１）
特開２００４－０１３６１１（ＪＰ，Ａ）
特開２００２－０４１４６７（ＪＰ，Ａ）
特開２００３－０８５４９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－５０／００