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

特許第3922482号

(P3922482)

(45)発行日　平成19年5月30日(2007.5.30)　(24)登録日　平成19年3月2日(2007.3.2)

(51)Int.Cl.		F I		
G06Q 30/00	(2006.01)	G06F	17/60	302E
G06Q 10/00	(2006.01)	G06F	17/60	330
G06F 21/00	(2006.01)	G06F	17/60	512
		G06F	15/00	330Z

請求項の数 13　(全 23 頁)

(21)出願番号　特願平9-280154
(22)出願日　平成9年10月14日(1997.10.14)
(65)公開番号　特開平11-120238
(43)公開日　平成11年4月30日(1999.4.30)
審査請求日　平成16年4月28日(2004.4.28)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　板橋　達夫
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　吉田　公義
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　田川　泰宏

最終頁に続く

(54)【発明の名称】情報処理装置および方法

(57)【特許請求の範囲】

【請求項１】

ユーザの情報処理装置および情報提供者の情報処理装置とネットワークを介して接続される情報処理装置において、

前記ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶する記憶手段と、

前記複数のユーザのうちの所定ユーザの情報処理装置から前記情報提供者の情報処理装置に対して前記情報処理装置自身および前記ネットワークを介してアクセスがあった場合であって、そのアクセスの応答として、前記情報提供者の情報処理装置から前記所定ユーザの前記個人情報の取得の要求が項目毎にあったとき、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定する判定手段と、

前記所定ユーザの前記個人情報の提供回数を計測し、その提供回数が閾値以上となった場合、他の手段の処理とは独立して、前記所定ユーザの情報処理装置に対して、前記個人情報の提供の可否を問い合わせ、その回答を得て、前記提供回数を０にリセットするまでの一連の処理を繰り返す問い合わせ手段と、

前記判定手段の判定結果と前記問い合わせ手段が前回得た回答に基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、

前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止する提供手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記個人情報の複数の前記項目のうち、前記情報提供者の情報処理装置への提供が禁止される項目は、さらに、前記情報提供者の情報処理装置への提供を禁止する第３の属性を有し、
前記提供手段は、さらに、前記要求項目の中に前記第３の属性の項目が存在するか否かに基づいて、前記提供有無の判定をする
ことを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記問い合わせ手段は、前記個人情報の提供の可否に関する回答のためのユーザインタフェースの画像データを作成し、前記所定ユーザの情報処理装置に伝送する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記所定ユーザを認証する認証手段をさらに備える
ことを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記記憶手段に個人情報が記憶されているユーザから同時に複数のアクセスがあったとき、それを検知する検知手段をさらに備える
ことを特徴とする請求項１に記載の情報処理装置。
【請求項６】
前記検知手段は、同一のユーザから同時に複数のアクセスがあったとき、それを前記所定ユーザに通知する
ことを特徴とする請求項５に記載の情報処理装置。
【請求項７】
前記検知手段は、同一のユーザから同時に複数のアクセスがあったとき、それをログファイルに記録する
ことを特徴とする請求項５に記載の情報処理装置。
【請求項８】
前記検知手段は、同一のユーザから同時に複数のアクセスがあったとき、後からのアクセスを拒絶する
ことを特徴とする請求項５に記載の情報処理装置。
【請求項９】
前記個人情報に対する不正なアクセスを検出する検出手段をさらに備える
ことを特徴とする請求項１の情報処理装置。
【請求項１０】
前記個人情報は、OPSまたはP3Pに準拠する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項１１】
ユーザの情報処理装置および情報提供者の情報処理装置とネットワークを介して接続される情報処理装置の情報処理方法において、
前記情報処理装置は、
前記ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶するデータベースと、
処理を実行する処理実行部と
を備え、
前記処理実行部が実行するステップとして、

前記複数のユーザのうちの所定ユーザの情報処理装置から前記情報提供者の情報処理装置に対して前記情報処理装置自身および前記ネットワークを介してアクセスがあった場合であって、そのアクセスの応答として、前記情報提供者の情報処理装置から前記所定ユーザの前記個人情報の取得の要求が項目毎にあったとき、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記データベースに記憶されている記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定する判定ステップと、

前記所定ユーザの前記個人情報の提供回数を計測し、その提供回数が閾値以上となった場合、他のステップの処理とは独立して、前記所定ユーザの情報処理装置に対して、前記個人情報の提供の可否を問い合わせ、その回答を得て、前記提供回数を０にリセットするまでの一連の処理を繰り返す問い合わせステップと、

前記判定ステップの処理による判定結果と前記問い合わせステップの前回の前記一連の処理により得られた回答に基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記データベースに記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止する提供ステップと

を含むことを特徴とする情報処理方法。

【請求項１２】

ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶する記憶手段を有するサーバおよびネットワークを介して、情報提供者の情報処理装置に対して接続される所定ユーザの情報処理装置において、

前記サーバおよび前記ネットワークを介して前記情報提供者の情報処理装置にアクセスするアクセス手段と、

前記アクセス手段による前記アクセスの応答として、前記情報提供者の情報処理装置から前記所定ユーザの前記個人情報の取得の要求が項目毎に前記サーバに対してあり、前記サーバが、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定し、その判定結果と、前記所定ユーザから事前に得ている前記個人情報の提供の可否の回答結果とに基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止するまでの一連の処理を実行すべく、前記一連の処理とは独立して、前記所定ユーザの前記個人情報の提供回数が閾値以上となったことをトリガとして、前記サーバから、前記所定ユーザの情報処理装置自身に対して、前記個人情報の提供の可否が問い合わされたとき、前記所定ユーザから前記回答結果を取得する取得手段と、

前記取得手段により所得された前記回答結果に基づいて、前記サーバに対して、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目の前記情報提供者の情報処理装置への提供の可否を通知することで、前記サーバから次の前記問い合わせがあるまでの間、前記提供の可否を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項１３】

ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶する記憶手段を有するサーバを介して、情報提供者の情報処理装置に対して接続される所定ユーザの情報処理装置の情報処理方法において、

前記情報処理装置は、

前記サーバとの通信を制御する通信制御部と、

前記ユーザに対するユーザインタフェースと

を備え、
前記情報処理装置が実行するステップとして、
前記通信制御部が、前記サーバを介して前記情報提供者の情報処理装置にアクセスするアクセスステップと、
前記アクセスステップの処理による前記アクセスの応答として、前記情報提供者の情報処理装置から前記所定ユーザの前記個人情報の取得の要求が項目毎に前記サーバに対してあり、前記サーバが、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定し、その判定結果と、前記所定ユーザから事前に得ている前記個人情報の提供の可否の回答結果とに基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止するまでの一連の処理を実行すべく、前記一連の処理とは独立して、前記所定ユーザの前記個人情報の提供回数が閾値以上となったことをトリガとして、前記サーバから、前記所定ユーザの情報処理装置自身の前記通信制御部に対して、前記個人情報の提供の可否が問い合わされたとき、前記ユーザインタフェースが、前記所定ユーザから前記回答結果を取得する取得ステップと、
前記取得ステップの処理により所得された前記回答結果に基づいて、前記通信制御部が、前記サーバに対して、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目の前記情報提供者の情報処理装置への提供の可否を通知することで、前記サーバから次の前記問い合わせがあるまでの間、前記提供の可否を制御する制御ステップと
を含むことを特徴とする情報処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、情報処理装置および方法に関し、特に、ネットワーク上にある個人情報を利用して、任意の位置から、簡便な端末装置で、情報提供業者から情報の提供をうけることができるようにした情報処理装置および方法に関する。
【０００２】
【従来の技術】
最近、いわゆるインターネットが普及し、インターネットを介して各種の情報の提供を受けることができるようになってきた。なお、ここで、提供される情報の中には、商品を購入するサービスや、その他の各種のサービスの提供も含まれる。
【０００３】
例えば、ユーザは、インターネットを介して所定のサービス提供者にアクセスし、そのサービス提供者が提供するホームページを介して、所定の商品を購入するような場合、ユーザの氏名、年齢、住所、電話番号、クレジットカードの番号といった個人情報を入力し、情報提供者に提示する必要がある。複数の情報提供者にアクセスし、複数の商品を購入するような場合、ユーザは、その都度、各情報提供者に対して個人情報を入力し、提供する必要がある。通常、このようにしてサービス提供者に対して提供する個人情報は同一の情報であり、ユーザは、同一の情報を繰り返し入力する必要があり、不便である。また、個人情報を誤って入力してしまうおそれもある。
【０００４】
そこで、例えば、OPS(Open Profiling Standard)においては、各ユーザのパーソナルコンピュータ上に、アプリケーションプログラムとして、各ユーザの個人情報を予め記録したプロファイルと、このプロファイルをユーザに代わって、情報提供者に、必要に応じて提供するユーザエージェントとを設けるようにしている。この場合、ユーザエージェントが、プロファイルに予め記録されている個人情報を、ユーザに代わって情報提供者に提供するので、ユーザは、個人情報を、その都度入力する必要がなくなる。

【０００５】
【発明が解決しようとする課題】
しかしながら、このような従来のシステムにおいては、各ユーザが、独自にアプリケーションプログラムとしてのユーザエージェントを用意しなくてはならず、通信プロトコル、その他フォーマットなどが改訂された場合には、その都度、新たなバージョンのアプリケーションプログラムを用意する必要があり、ユーザにとって大きな負担となる課題があった。
【０００６】
さらにまた、例えば、ユーザが携帯用の端末装置を所持して、外出先から、情報提供者にアクセスするような場合、携帯用の端末装置は、家庭に配置されているパーソナルコンピュータなどに較べて、携帯性とコストを重視する観点から、十分な機能を有していない場合が多く、従って、パーソナルコンピュータからアクセスする場合と同一の環境下で、端末装置から情報提供者にアクセスすることができない課題があった。
【０００７】
このため、例えば、書換可能なメモリを用意し、このメモリを適宜変更することで、新たな機能を拡張、追加することも可能であるが、そのようにすると、装置の構成が複雑となる課題があった。
【０００８】
本発明は、このような状況に鑑みてなされたものであり、簡単かつ安価に、また、任意の位置から、常に同一の環境下で、情報の提供を受けることができるようにするものである。
【０００９】
【課題を解決するための手段】
本発明の第１の情報処理装置は、ユーザの情報処理装置および情報提供者の情報処理装置とネットワークを介して接続される情報処理装置であって、前記ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶する記憶手段と、前記複数のユーザのうちの所定ユーザの情報処理装置から前記情報提供者の情報処理装置に対して前記情報処理装置自身および前記ネットワークを介してアクセスがあった場合であって、そのアクセスの応答として、前記情報提供者の情報処理装置から前記所定ユーザの前記個人情報の取得の要求が項目毎にあったとき、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定する判定手段と、前記所定ユーザの前記個人情報の提供回数を計測し、その提供回数が閾値以上となった場合、他の手段の処理とは独立して、前記所定ユーザの情報処理装置に対して、前記個人情報の提供の可否を問い合わせ、その回答を得て、前記提供回数を０にリセットするまでの一連の処理を繰り返す問い合わせ手段と、前記判定手段の判定結果と前記問い合わせ手段が前回得た回答に基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止する提供手段とを備えることを特徴とする。
【００１０】
本発明の第１の情報処理方法は、ユーザの情報処理装置および情報提供者の情報処理装置とネットワークを介して接続される情報処理装置の情報処理方法であって、前記情報処理装置は、前記ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶するデータベースと、処理を実行する処理実行部とを備え、前記処理実行部が実行するステップとして、前記複数のユーザのうちの所定ユーザの情報処理装置から前記情報提供者の情報処理装置に対して前記情報処理装置自身および前記ネットワークを

介してアクセスがあった場合であって、そのアクセスの応答として、前記情報提供者の情報処理装置から前記所定ユーザの前記個人情報の取得の要求が項目毎にあったとき、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記データベースに記憶されている記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定する判定ステップと、前記所定ユーザの前記個人情報の提供回数を計測し、その提供回数が閾値以上となった場合、他のステップの処理とは独立して、前記所定ユーザの情報処理装置に対して、前記個人情報の提供の可否を問い合わせ、その回答を得て、前記提供回数を０にリセットするまでの一連の処理を繰り返す問い合わせステップと、前記判定ステップの処理による判定結果と前記問い合わせステップの前回の前記一連の処理により得られた回答に基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記データベースに記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止する提供ステップとを含むことを特徴とする。

【００１２】

本発明の第２の情報処理装置は、ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶する記憶手段を有するサーバおよびネットワークを介して、情報提供者の情報処理装置に対して接続される所定ユーザの情報処理装置であって、前記サーバおよび前記ネットワークを介して前記情報提供者の情報処理装置にアクセスするアクセス手段と、前記アクセス手段による前記アクセスの応答として、前記情報提供者の情報処理装置から前記所定ユーザの前記個人情報の取得の要求が項目毎に前記サーバに対してあり、前記サーバが、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定し、その判定結果と、前記所定ユーザから事前に得ている前記個人情報の提供の可否の回答結果とに基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止するまでの一連の処理を実行すべく、前記一連の処理とは独立して、前記所定ユーザの前記個人情報の提供回数が閾値以上となったことをトリガとして、前記サーバから、前記所定ユーザの情報処理装置自身に対して、前記個人情報の提供の可否が問い合わされたとき、前記所定ユーザから前記回答結果を取得する取得手段と、前記取得手段により所得された前記回答結果に基づいて、前記サーバから次の前記問い合わせがあるまでの間、前記サーバに対して、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目の前記情報提供者の情報処理装置への提供の可否を制御する制御手段とを備えることを特徴とする。

【００１３】

本発明の第２の情報処理方法は、ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶する記憶手段を有するサーバを介して、情報提供者の情報処理装置に対して接続される所定ユーザの情報処理装置の情報処理方法であって、前記情報処理装置は、前記サーバとの通信を制御する通信制御部と、前記ユーザに対するユーザインタフェースとを備え、前記情報処理装置が実行するステップとして、前記通信制御部が、前記サーバを介して前記情報提供者の情報処理装置にアクセスするアクセスステップと、前記アクセスステップの処理による前記アクセスの応答として、前記情報提供者の情報処理装置から前記所定ユーザの前記個人情報の取得の要求が項目毎に前記サーバに対してあり、前記サーバが、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定

し、その判定結果と、前記所定ユーザから事前に得ている前記個人情報の提供の可否の回答結果とに基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止するまでの一連の処理を実行すべく、前記一連の処理とは独立して、前記所定ユーザの前記個人情報の提供回数が閾値以上となったことをトリガとして、前記サーバから、前記所定ユーザの情報処理装置自身の前記通信制御部に対して、前記個人情報の提供の可否が問い合わされたとき、前記ユーザインタフェースが、前記所定ユーザから前記回答結果を取得する取得ステップと、前記取得ステップの処理により所得された前記回答結果に基づいて、前記通信制御部が、前記サーバに対して、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目の前記情報提供者の情報処理装置への提供の可否を通知することで、前記サーバから次の前記問い合わせがあるまでの間、前記提供の可否を制御する制御ステップとを含むことを特徴とする。

【００１５】

本発明の第１の情報処理装置および方法においては、ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報が、複数のユーザ毎に記憶されており、複数のユーザのうちの所定ユーザの情報処理装置から情報提供者の情報処理装置に対してアクセスがあった場合であって、そのアクセスの応答として、情報提供者の情報処理装置から所定ユーザの個人情報の取得の要求が項目毎にあったとき、情報提供者の情報処理装置から取得が要求された要求項目の中に第１の属性の項目が存在するか否かに基づいて、記憶されている所定ユーザの個人情報の提供に対する所定ユーザの許可の必要性が判定され、その判定結果と、所定ユーザの情報処理装置に対して、個人情報の提供の可否の前回の問い合わせの際に得られた回答とに基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無が判定され、提供すると判定された場合、記憶されている前記所定ユーザの前記個人情報の要求項目が情報提供者の情報処理装置に提供され、提供しないと判定された場合、要求項目の提供が禁止される。また、このような一連の処理とは独立して、前記所定ユーザの前記個人情報の提供回数が計測され、その提供回数が閾値以上となった場合、前記所定ユーザの情報処理装置に対して、前記個人情報の提供の可否の問い合わせが行われ、その回答が得られると、前記提供回数が０にリセットされる、という一連の処理が繰り返される。

【００１６】

本発明の第２の情報処理装置および方法においては、ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶する記憶手段を有するサーバおよびネットワークを介して、情報提供者の情報処理装置に対して接続される所定ユーザの第２の情報処理装置により、次のような処理が実行される。即ち、サーバおよびネットワークを介して情報提供者の情報処理装置にアクセスされ、そのアクセスの応答として、情報提供者の情報処理装置から所定ユーザの個人情報の取得の要求が項目毎にサーバに対してあり、前記サーバが、前記情報提供者の情報処理装置から取得が要求された要求項目の中に前記第１の属性の項目が存在するか否かに基づいて、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定し、その判定結果と、前記所定ユーザから事前に得ている前記個人情報の提供の可否の回答結果とに基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止するまでの一連の処理を実行すべく、前記一連の処理とは独立して、前記所定ユーザの前記個人情報の提供回数が閾値以上となったことをトリガとして、前記サーバから、前記所定ユーザの情報処理装置自身に対して、前記個人情報の提供の可否が問い合わされたとき、前記所定ユーザから前記回答結果が取得され、その回答に基

づいて、サーバに対して、記憶手段に記憶されている所定ユーザの個人情報の要求項目の情報提供者の情報処理装置への提供の可否が通知されることで、その提供の可否が制御される。

【００１７】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１８】

請求項１に記載の情報処理装置は、複数のユーザの個人情報を記憶する記憶手段（例えば、図１のユーザプロファイルデータベース１１０）と、ユーザの情報処理装置（例えば、図１の端末装置１０１）からアクセスがあった場合であって、情報提供者の情報処理装置（例えば、図１のサービス提供装置１１４）から要求があったとき、ユーザの情報処理装置に代わって、記憶手段に記憶されている個人情報を情報提供者の情報処理装置に提供する提供手段（例えば、図１のプロキシ装置１０９）とを備えることを特徴とする。

【００１９】

請求項２に記載の情報処理装置は、記憶手段に記憶されている個人情報の提供に対するユーザの許可の必要性を判定する判定手段（例えば、図８のステップＳ７１）と、判定手段の判定結果に対応して、ユーザの情報処理装置に対して、個人情報の提供の可否を問い合わせ、その回答を得る問い合わせ手段（例えば、図８のステップＳ７２）とをさらに備え、提供手段は、問い合わせ手段が取得した回答に対応して、記憶手段に記憶されている個人情報を、情報提供者の情報処理装置に提供することを特徴とする。

【００２０】

請求項４に記載の情報処理装置は、ユーザを認証する認証手段（例えば、図２のステップＳ１）をさらに備えることを特徴とする。

【００２１】

請求項５に記載の情報処理装置は、記憶手段に個人情報が記憶されているユーザから同時に複数のアクセスがあったとき、それを検知する検知手段（例えば、図１１のステップＳ１３１）をさらに備えることを特徴とする。

【００２２】

請求項９に記載の情報処理装置は、個人情報に対する不正なアクセスを検出する検出手段（例えば、図１１のステップＳ１３２）をさらに備えることを特徴とする。

【００２３】

請求項１３に記載の情報処理装置は、サーバを介して情報提供者の情報処理装置にアクセスするアクセス手段（例えば、図４のステップＳ２１）と、情報提供者の情報処理装置から要求があったとき、サーバが、ユーザに代わって、記憶手段に記憶されている個人情報を情報提供者の情報処理装置に提供することを制御する制御手段（例えば、図４のステップＳ２７）とを備えることを特徴とする。

【００２４】

以下、本発明に係る情報処理装置について、図面を参照しつつ詳細に説明する。図１は本発明の情報処理装置を適用したネットワークシステムの全体構成を図示したものである。図１に示すように、本発明の情報処理装置を適用した端末装置１０１は、PHS(Personal Handy-Phone System)を内蔵しており、そのユーザが家庭に有するパーソナルコンピュータ１０６と同等の機能を有している。

【００２５】

また、端末装置１０１は、誤り訂正機能を備えたデータ伝送規格としてPIAFS(PHS Internet Access Forum Standard)規格、隣接２地点間での認証付きの同期ディジタル通信機能PPP(Point to Point Protocol)、蓄積伝送用のSMTP(Simple Mail Transfer Protocol)に準拠し、トランスポート層をTCP(Transfer Control Protocol)に依存しないプロトコル、お

よび、リアルタイムのインタラクションをサポートするHTTP(Hypertext transfer Protocol)に準拠し、トランスポート層をTCPに依存しないプロトコルの各アプリケーションプロトコル、から構成される通信プロトコルスタックを有している。さらに、端末装置１０１は、ユーザの意志を確実にサーバ１００に通知し、かつ、サーバ１００からの通知を確実にユーザに伝えるために必要十分なユーザインタフェースとして、例えばビットマップディスプレイ装置、タッチパネル、およびスピーカ装置（いずれも図示せず）を備えている。

【００２６】

サーバ１００は、有線(PIAFS)インタフェース１０５，１０８を介して電話回線１０４に、また、有線インタフェース１１２を介してインターネット１１３に、それぞれ接続される一連のコンピュータ群として構成される。有線インタフェース１０８は、ISDN(Integrated Service Digital Network)ターミナルアダプタ装置で、ISDNレイヤ３プロトコルまでの機能を提供する。一方、有線インタフェース１０５は、誤り訂正機能を備えたデータ伝送規格としてPIAFS規格プロトコル機能を有線インタフェース１０８の制御の元で提供する。有線インタフェース１１２はIP(Internet Protocol)ルータ装置であり、インターネットプロトコル(IP)のパケットルーティング機能を提供する。

【００２７】

一連のコンピュータ群は少なくともプロキシ装置１０９、複数のユーザの個人情報を記憶するユーザプロファイルデータベース１１０、および、P3P(Platform for Privacy Preference Project)のユーザエージェント(UA)１１１を、コンピュータプログラムとして有し、個人情報提供の代行サービスとしての機能を実現する。以上に加え、サーバ１００の基本機能として、有線インタフェース１０５の提供する通信インタフェースの上位レイヤであるPPPプロトコル、HTTPプロトコル、SMTPプロトコルの処理機能、有線インタフェース（IPルータ）１１２の提供する通信インタフェースの上位レイヤであるTCP・UDP(User Datagram Protocol)、および関連のインターネットプロトコル群の処理機能が実装されている。また、サーバ１００には、それ自体を管理するためのデータおよびユーザインタフェースも備えられている。

【００２８】

端末装置１０１とサーバ１００は、以下に述べる手順で通信を確立する。まず、端末装置１０１は、内蔵する無線インタフェースとしてのPHSにより基地局１０３に接続されている。ここで、基地局１０３としては、公衆の基地局CS(Cell Station)だけでなく、自営基地局HS(Home Station)を利用することも可能である。端末装置１０１が通信を開始すべく発呼動作を行うと、通常のPHSの手順により基地局１０３へ発呼要求が送られ、電話回線１０４を経由し、所望の通信先であるサーバ１００の有線（PIAFS）インタフェース１０５へ着信要求が通知され、呼が確立する。その後、PIAFSの規格に準拠し、誤り訂正機能を備えたデータ伝送セッションが確立され、PPPの認証を経て、端末装置１０１とサーバ１００のプロキシ装置１０９との間にデータ送受信のセッションが確立する。なお、サーバ１００側から端末装置１０１へ向けての呼の確立も可能であり、その場合も、前述の手順と同様に、各通信プロトコルの規格に定められた標準の動作により呼が確立されてゆく。

【００２９】

以上のようにして確立された端末装置１０１とサーバ１００のプロキシ装置１０９との間のデータ送受信のセッションを用いて、相互にHTTPまたはSMTPに準拠した、簡便なアプリケーションプロトコルを利用して、端末装置１０１のユーザと、ネットワークを経由して個人情報を利用するサービス提供装置１１４や、インターネット１１３を介して各種のサービスを提供するサービス提供装置１１６との間での通信の準備が確立する。

【００３０】

一方、サーバ１００とインターネット１１３とは常時リンクが確立した状態とされ、サーバ１００は、インターネット１１３を介して、サービス提供装置１１４、またはサービス提供装置１１６との間で、パケットの送受信を常時行うことができるようになされている

。
【００３１】
端末装置１０１とサーバ１００による個人情報提供機能は、端末装置１０１、サーバ１００、並びにサービス提供装置１１４、またはサービス提供装置１１６の間の通信が可能な状態、もしくはその変形状態として、端末装置１０１とサーバ１００との間の通信が、一時的に切断されている状態のときに利用が可能である。
【００３２】
サーバ１００のプロキシ装置１０９は、端末装置１０１との間において、SMTP/HTTPといった簡略化されたプロトコルにより通信を行うとともに、インターネット１１３を経由して、顧客データベース１１５を有するサービス提供装置１１４や、顧客データベース１１７を有するサービス提供装置１１６との間で、TCP/IPのプロトコルで通信を行う。プロキシ装置１０９は、ユーザエージェント装置１１１と協調して、随時、個人情報管理のためのユーザインタフェースを作成し、端末装置１０１に提供することで、ユーザの意志を確認するとともに、ユーザに対して情報を出力する機能を有する。このプロキシ装置１０９がインターネット１１３側で必要とされる個人情報管理プロトコル（例えばP3PやOPS）を有するので、端末装置１０１は、これらのプロトコルとは独立に、ユーザインタフェースを提供するための簡便なプロトコルのみでサーバ１００と接続可能である。
【００３３】
サーバ１００のユーザプロファイルデータベース装置１１０は、個人情報提供サービスの核となる各ユーザのプライベートなデータ（個人情報）が格納されているデータベースであり、ユーザ自身がオーナとしてのアクセス権限を持ち、適用する個人情報管理規格（本実施の形態の場合はOPS規格）に定められる形で厳重なアクセス管理が施される。
【００３４】
サーバ１００のユーザエージェント装置１１１は、適用する個人情報管理規格（OPS規格）に定められる形でサービス提供装置１１４と通信を行うための装置であり、サービス提供装置１１４に対しては、ネットワークに接続される通常のパーソナルコンピュータがOPSに対応する場合と同一のインタフェースを提供する。
【００３５】
ユーザエージェント装置１１１は、OPSセッションの開始時、プロキシ装置１０９より通信ポートを提供され、サービス提供装置１１４との通信を開始する。この際、後述のユーザインタフェース提供時の処理低減を目的に、ユーザエージェント装置１１１、プロキシ装置１０９ともに相手を認識するための識別子を持ち合うことも可能である。ユーザエージェント装置１１１は、OPSセッション実行時、ユーザプロファイルデータベース１１０へのデータの書き込み、読み出し、もしくはその両方を行う。また、ユーザエージェント装置１１１は、OPSセッション実行に当たり、データのオーナである端末装置１０１のユーザに、通知もしくは判断を仰ぐ必要がある場合には、プロキシ装置１０９に対して、ユーザインタフェースの作成代行を要求する。
【００３６】
プロキシ装置１０９によるユーザインタフェースの作成には、サービス提供装置１１４より送られてきたHTML(Hypertext Markup Language)等により記述されたフォームを流用する場合と、OPSセッションには存在しないユーザインタフェース画面を新規に作成する場合がある。前者の場合は、OPSプロトコルにより送られてきたユーザインタフェース画面がプロキシ装置１０９に転送され、プロキシ装置１０９から端末装置１０１へ、前述の通信路を使いHTTPインタフェースなどを用い転送され、端末装置１０１のディスプレイに表示される。HTMLのフォーム機能等を使い応答が可能な構成になっている場合、端末装置１０１より入力されるユーザのフィードバック（回答）も、プロキシ装置１０９経由でユーザエージェント装置１１１に戻り、インターネット１１３を通じてサービス提供装置１１４へ転送される。
【００３７】
一方、後者、すなわち、情報利用サービス提供装置１１４が作成したものではなく、ユー

ザの指示を求めたり、ユーザへ通知を行うために、サーバ１００が独自にユーザインタフェースを必要とする場合は、ユーザエージェント装置１１１が自らの識別子とユーザインタフェースを構成するために必要な情報をプロキシ装置１０９へ通知する。このとき、プロキシ装置１０９は、そのユーザインタフェース作成機能を呼び出し、ユーザインタフェースを作成し、作成したユーザインタフェースを端末装置１０１に通知する。また、ユーザの応答がある場合、データは一旦、プロキシ装置１０９で解釈され、対応する内部情報形式に翻訳された上で、ユーザエージェント装置１１１へと通知される。

【００３８】

このように、プロキシ装置１０９がユーザインタフェース作成機能を受け持つことで、端末装置１０１の簡略化とユーザエージェント装置１１１の一般化という目的が両立されているが、端末装置１０１、もしくはユーザエージェント装置１１１に、ユーザインタフェースの作成実行機能を持たせる実装形態も可能である。

【００３９】

次に、代表的な情報交換シーケンスを例に、端末装置１０１、プロキシ装置１０９、ユーザエージェント装置１１１、サービス提供装置１１４の間における通信の流れを説明する。

【００４０】

ユーザエージェント装置１１１は、常に作成されているわけではなく、端末装置１０１が、サーバ１００に対してアクセスしてきたとき作成される。図２は、その場合の処理例を表している。

【００４１】

最初に、ステップＳ１において、プロキシ装置１０９は、端末装置１０１がアクセスしてきたとき、ユーザの認証処理を実行する。例えば、プロキシ装置１０９は、端末装置１０１から、ユーザに割り当てられているＩＤやパスワードの入力を受け、そのＩＤとパスワードが、ユーザプロファイルデータベース１１０に個人情報が記憶されているユーザのＩＤとパスワードに対応するものであるか否かを判定する。プロキシ装置１０９は、ステップＳ２において、認証結果を判定し、ステップＳ１で端末装置１０１から入力されたＩＤとパスワードが、ユーザプロファイルデータベース１１０に記憶されているＩＤとパスワードに対応しないものと判定された場合、ステップＳ７に進み、端末装置１０１に対してエラーのメッセージを伝送し、処理を終了する。すなわち、この場合には、端末装置１０１からのサーバ１００に対するアクセスが拒絶される。

【００４２】

ステップＳ２において、端末装置１０１から入力されたＩＤとパスワードが、ユーザプロファイルデータベース１１０に記憶されているものと対応すると判定された場合、ステップＳ３に進み、プロキシ装置１０９は、そのユーザに対応するユーザエージェント装置１１１を生成する。次に、ステップＳ４に進み、プロキシ装置１０９は、ユーザに対応するユーザエージェント装置１１１を作成することができたか否かを判定し、作成することができた場合には、ステップＳ５に進み、そのユーザとの間のセッションが成立したことを記憶するために、内蔵するセッションテーブルに、そのユーザを登録する。これに対して、ステップＳ４において、例えば、メモリの容量不足、過負荷などの理由により、ユーザエージェント装置１１１を作成することができなかったと判定された場合には、ステップＳ６に進み、プロキシ装置１０９は、端末装置１０１に対してエラーのメッセージを転送し、処理を終了する。

【００４３】

次に図３のタイミングチャートを参照して、個人情報管理（OPS）を利用しないで、サービス提供装置１１４から、例えば、HTTPプロトコルを利用したWebサービスの提供を受ける場合の動作を説明する。

【００４４】

最初に、ステップＳ１１において、TCP/IP通信スタックを持たない端末装置１０１は、プロキシ装置１０９へGet要求を出す。プロキシ装置１０９はステップＳ１２で、同一内容

のGet要求を、TCP/IPプロトコル上のパケットとして、有線インタフェース（IPルータ）１１２、インターネット１１３を経由して、サービス提供装置１１４へ通知する。サービス提供装置１１４は要求に従い、ステップＳ１３で、データをプロキシ装置１０９へ、TCP/IPパケットとして返送する。プロキシ装置１０９はこの結果を、ステップＳ１４で、端末装置１０１へと通知することで、最初のGet要求が完了する。

【００４５】

次に、ユーザが、個人情報管理機構(OPS)を利用したサービスの提供を受ける場合の処理について、図４のタイミングチャートを参照して説明する。ここでは、Webを使って抽選に応募するものとする。端末装置１０１は、ステップＳ２１において、Post要求をプロキシ装置１０９に出力する。プロキシ装置１０９は、この要求をステップＳ２２で、サービス提供装置１１４に伝送する。サービス提供装置１１４は、抽選の応募に必要な情報を端末装置１０１に提供する前に、ユーザの個人情報を得るために、ステップＳ２３において、OPSのREADリクエストをプロキシ装置１０９に出力する。プロキシ装置１０９は、サービス提供装置１１４からのリクエストが、通常のHTTPではなく、OPSセッションの一部であるか否か（個人情報の提供を要求するものであるか否か）を認識し、YESであると認識した場合には、ユーザエージェント装置１１１に対してセッションの開始とREADリクエストを通知する。

【００４６】

ユーザエージェント装置１１１は、プロキシ装置１０９からのREADリクエストにより要求された個人情報を、端末装置１０１に代わってサービス提供装置１１４に返送する前に、ステップＳ２５において、そのユーザの個人情報のオーナである端末装置１０１のユーザに対して、サービス提供装置１１４から伝送してきた、確認のためのユーザインタフェースをプロキシ装置１０９に転送する。このユーザインタフェースのデータは、ステップＳ２６において、プロキシ装置１０９から端末装置１０１に転送される。これにより、端末装置１０１のディスプレイには、例えば、図５に示すようなユーザインタフェースの画面が表示される。

【００４７】

同図に示すように、このユーザインタフェースにおいては、サーバ１００が、端末装置１０１に代わってユーザの個人情報をサービス提供装置１１４に提供することに同意するとき操作されるボタン（YESボタン）と、拒絶するとき操作されるボタン（NOボタン）が表示されている。ユーザは、自分自身の個人情報をサービス提供装置１１４に対して提供することに同意する場合にはYESボタンを、また、同意しない場合にはNOボタンを、それぞれ操作する。

【００４８】

ユーザが、このようにしてボタンを操作すると、その操作に対応する制御データが、ステップＳ２７において、端末装置１０１からプロキシ装置１０９に転送される。プロキシ装置１０９は、この制御データをステップＳ２８において、さらにユーザエージェント装置１１１に転送する。ユーザエージェント装置１１１は、サービス提供装置１１４に、ユーザが個人情報を提供することを拒絶する制御データが入力された場合には、ユーザプロファイルデータベース１１０に記憶されているユーザの個人情報の提供を拒絶する。これに対して、個人情報の提供が同意されている場合には、ユーザエージェント装置１１１は、ユーザプロファイルデータベース１１０から、そのユーザに対応する個人情報のうち、サービス提供装置１１４から要求されているものを読み出し、ステップＳ２９において、これをプロキシ装置１０９に転送する。プロキシ装置１０９は、このユーザエージェント装置１１１から転送を受けた個人情報を、ステップＳ３０において、サービス提供装置１１４に転送する。

【００４９】

ステップＳ３０でサービス提供装置１１４に伝送された個人情報は、ユーザプロファイルデータベース１１０にユーザが予め登録しておいたものである（この登録は、例えば、家庭に配置されているパーソナルコンピュータ１０６により行われる）。従って、ユーザは

、個人情報をアクセス時に入力する必要がないので、誤入力も防止される。
【００５０】
なお、図５に示したユーザインタフェースは、サービス提供装置１１４から伝送されてきたものをそのまま利用することも可能であるが、ユーザエージェント装置１１１、またはプロキシ装置１０９において、ユーザインタフェース画面情報を再構築することも可能である。この場合の処理については、図９のフローチャートを参照して後述する。
【００５１】
以上のように、通常のOPSセッションでは、個人情報の提供に関し、ユーザへの通知は必要ないが、次に、ユーザエージェント装置１１１の判断で、OPSセッションとは別に、ユーザインタフェースを作成してユーザへ通知を行う例について、図６のタイミングチャートを参照して説明する。図６の例においては、ユーザインタフェースによる毎回の確認作業を省略し、内蔵するカウンタ（図示せず）でアクセス回数をカウントし、そのカウント値COUNTが予め設定してある一定回数に達したとき、ユーザに対する確認作業を行うものとする。
【００５２】
最初に、ステップＳ４１において、端末装置１０１は、プロキシ装置１０９に対して、Post要求を出力する。プロキシ装置１０９は、このPost要求をステップＳ４２において、サービス提供装置１１４に転送する。サービス提供装置１１４は、この要求に対応して、ステップＳ４３において、OPSの個人情報のREAD要求を出力する。プロキシ装置１０９は、ステップＳ４４において、このREAD要求に対応して、セッションの開始とREAD要求を、ユーザエージェント装置１１１に通知する。個人情報をサービス提供装置１１４に提供することに対して、端末装置１０１から毎回承諾を得る必要がないので、ステップＳ４５において、ユーザエージェント装置１１１は、ユーザプロファイルデータベース１１０に記憶されている個人情報のうち、サービス提供装置１１４から要求された事項を読み出し、これをプロキシ装置１０９に出力する。プロキシ装置１０９は、ステップＳ４６において、この個人情報を、サービス提供装置１１４に出力する。
【００５３】
すなわち、以上の処理は、図４のステップＳ２１乃至ステップＳ３０の処理のうち、ステップＳ２５乃至ステップＳ２８に示したユーザの確認処理を省略した処理となっている。
【００５４】
ユーザエージェント装置１１１は、以上のようにして、ユーザプロファイルデータベース１１０から個人情報を読み出すたびに、その読み出した回数を１ずつインクリメントし、そのユーザの個人情報を読み出した回数をカウンタのカウント値COUNTに保持している。そして、そのカウント値COUNTが、予め設定してある所定の回数（例えば１０回）に達したとき、ユーザエージェント装置１１１は、ステップＳ４７において、サービス提供装置１１４との間のOPSセッションとは無関係に、自らユーザインタフェースを作成し、プロキシ装置１０９に出力する。プロキシ装置１０９は、ステップＳ４８において、このユーザインタフェースを端末装置１０１に転送する。これにより、端末装置１０１のディスプレイに、例えば、図７に示すように、個人情報を読み出した回数が、予め設定した所定の回数（いまの場合１０回）に達したことが表示される。
【００５５】
ステップＳ４７において、ユーザエージェント装置１１１が、プロキシ装置１０９に対して通知を行うためのインタフェースは、一般のパーソナルコンピュータにおけるユーザエージェント装置と、ユーザインタフェース装置との間のインタフェースと同一のものを利用することができる。これにより、ソフトウェア機構の共有化を図ることができる。
【００５６】
プロキシ装置１０９は、ユーザエージェント装置１１１から受け取ったユーザインタフェースをHTMLフォーマットに変換し、HTTPによりステップＳ４８において、端末装置１０１へ転送する。
【００５７】

ユーザは、図７に示すようなユーザインタフェースの画面を見て、個人情報の提供を許諾するか、または拒否するかの選択を行い、YESボタンまたはNOボタンを操作する。この操作は、ステップＳ４９において、端末装置１０１からプロキシ装置１０９に、HTTPプロトコルにより通知される。プロキシ装置１０９は、さらに、この通知をステップＳ５０において、内部インタフェースを介して、ユーザエージェント装置１１１に通知する。通知を受け取ったユーザエージェント装置１１１は、サービス提供装置１１４に対する個人情報の提供回数を計数するカウンタのカウント値COUNTを０にリセットし、処理を終了させる。

【００５８】

以上のようにして、プロキシ装置１０９は、サービス提供装置１１４からのREAD要求が、ユーザの確認を必要とするものであるのか、必要としないものであるかを判定する必要がある。図８は、この判定処理の詳細を表している。

【００５９】

すなわち、ステップＳ７１において、プロキシ装置１０９は、サービス提供装置１１４から伝送されてきたREAD要求が、OPS関連ヘッダを有するものであるか否かを判定する。OPS関連ヘッダを有しないものである場合には、ステップＳ７５に進み、プロキシ装置１０９は、サービス提供装置１１４からのデータを端末装置１０１に転送する。このようにして、例えば、図３のステップＳ１３において、サービス提供装置１１４から伝送されてきたデータが、ステップＳ１４において、プロキシ装置１０９から端末装置１０１にそのまま転送される。

【００６０】

一方、ステップＳ７１において、サービス提供装置１１４からのデータが、OPS関連ヘッダを有するものであると判定された場合、ステップＳ７２に進み、プロキシ装置１０９は、そのデータをユーザエージェント装置１１１に転送する。このようにして、例えば、図４のステップＳ２４、または図６のステップＳ４４において、セッション開始とREAD要求が、プロキシ装置１０９からユーザエージェント装置１１１に通知される。

【００６１】

次に、ステップＳ７３において、プロキシ装置１０９は、ユーザエージェント装置１１１から必要な情報が転送されてくるまで待機し、転送されてきたとき、ステップＳ７４において、この個人情報をサービス提供装置１１４に転送する。

【００６２】

このようにして、例えば、図４に示すタイミングチャートにおいては、ステップＳ２４において、プロキシ装置１０９からユーザエージェント装置１１１に通知が行われた後、ステップＳ２９において、ユーザエージェント装置１１１からプロキシ装置１０９に個人情報が転送されるまで待機し、転送されてきたとき、プロキシ装置１０９は、ステップＳ３０において、個人情報をサービス提供装置１１４に転送する。

【００６３】

また、同様に、図６のタイムチャートにおいても、プロキシ装置１０９は、ステップＳ４４において、ユーザエージェント装置１１１に対して通知を行った後、ステップＳ４５において、ユーザエージェント装置１１１からプロキシ装置１０９に個人情報が転送されてくるまで待機し、転送されてきたとき、ステップＳ４６において、その個人情報をサービス提供装置１１４に転送する。

【００６４】

次に、図４のステップＳ２５（後述する図１０のステップＳ１１１）において、ユーザエージェント装置１１１が、プロキシ装置１０９にユーザインタフェースを転送してきたとき、プロキシ装置１０９が、このユーザインタフェースに基づいて、端末装置１０１からユーザの確認をとる場合のプロキシ装置１０９の処理ついて、図９のフローチャートを参照して説明する。

【００６５】

ステップＳ８１において、プロキシ装置１０９は、予め用意されているHTMLテンプレート

を初期化し、ステップＳ８２において、READ要求を転送してきたサービス提供装置１１４の識別子とTOE(Term of Exchange)をHTMLテンプレートに記入する。このTOEは、サービス提供装置１１４が個人情報を受け取ったとき、その個人情報をどのように利用するのか（サービス提供装置１１４のサービス提供者だけが利用するのか、あるいは、そのサービス提供者から他のサービス提供者にも提供され、そこでも利用されるのかといったこと）を文字列で表現したものである。図５の表示例では、そのサービス提供者だけが利用するもの（their own use only）とされている。

【００６６】

次に、ステップＳ８３に進み、プロキシ装置１０９は、ユーザに確認すべき項目（サービス提供装置１１４から提供を要求されている個人情報）を１つ抽出し、その属性を読み込む。確認すべき項目が空であるか否か（すべての項目をテンプレートに記入したか否か）をステップＳ８４において判定する。確認項目が空でない場合には、ステップＳ８５に進み、プロキシ装置１０９は、HTMLテンプレートに、その項目の属性に対応する文字列を追加する処理を行う。以上の処理が、ステップＳ８４において、確認項目が空であると判定されるまで繰り返し実行される。このようにして、例えば図５の年齢（age）、年収（annual income）、職業（occupation）などが、テンプレートに追加される。

【００６７】

ステップＳ８４において、確認項目が空になった（確認すべき項目を、テンプレートに全て書き込んだ）と判定された場合、ステップＳ８６に進み、プロキシ装置１０９は、ボタンを追加するなど終了処理を実行し、ステップＳ８７において、そのHTMLを端末装置１０１に出力する。

【００６８】

そして、ステップＳ８８において、プロキシ装置１０９は、ユーザ（端末装置１０１）から応答があるまで待機し、応答があったとき、ステップＳ８９に進み、その応答結果を判定する。応答結果がYESである場合には、ステップＳ９０に進み、応答にYESを設定し、ステップＳ９２において、ユーザエージェント装置１１１に、その応答結果を出力する。ステップＳ８９において、応答結果がNOであると判定された場合には、ステップＳ９１に進み、プロキシ装置１０９は、応答にNOを設定し、ステップＳ９２において、そのNOが設定された応答をユーザエージェント装置１１１に出力する。

【００６９】

次に、ユーザエージェント装置１１１が、プロキシ装置１０９より、例えば、図４のステップＳ２４、または図６のステップＳ４４で、ユーザプロファイルデータベース１１０からの個人情報のREAD要求を受けた場合における詳細な処理を、図１０のフローチャートを参照して説明する。

【００７０】

最初にステップＳ１０１において、ユーザエージェント装置１１１は、内蔵するバッファ１とバッファ２（図示せず）をクリアし、ステップＳ１０２において、個人情報を要求してきたサービス提供装置１１４の識別子とTOEをバッファ２に記入する。次に、ステップＳ１０３において、サービス提供装置１１４から要求されている個人情報の項目を抽出し、その属性を取得する。ステップＳ１０４において取得する対象となっている個人情報の項目が空であるか否かを判定し、空で無ければステップＳ１０５に進み、その個人情報の属性値をチェックする。ステップＳ１０６において、ステップＳ１０５でチェックした個人情報の属性値が、サービス提供装置１１４に提供することを禁止する項目（禁止項目）であることを表しているか否かを判定し、禁止項目を表していない場合には、ステップＳ１０７に進み、その項目（属性に対応する文字列）を応答内容を記憶するバッファ１に記入する。

【００７１】

次に、ステップＳ１０８において、対象となっている項目の属性が自動応答可能（提供する前に、ユーザの確認が不要）であることを表しているか否かを判定する。自動応答可能な項目である場合には、ステップＳ１０３に戻り、次の項目の属性を取得する処理が行わ

れる。例えば、通常、ユーザの氏名、性別などは、自動応答可能な属性の項目とされる。

【００７２】

これに対して、ステップＳ１０８において、いま対象とされている項目が、自動応答の対象ではないと判定された場合、ステップＳ１０９に進み、その項目を確認リストを記憶するバッファ２に記録する。その後、ステップＳ１０３に戻り、それ以降の処理が繰り返し実行される。例えば、ユーザの年齢、年収、職業などは、このようにして、確認リストに登録され、図５に示すように、ユーザに確認が求められる。

【００７３】

ステップＳ１０６において、対象項目が提供を禁止する項目であると判定された場合、ステップＳ１１４に進み、ユーザエージェント装置１１１は、バッファ１とバッファ２をクリアし、ステップＳ１１５において、サービス提供装置１１４に対して、Failedの応答を伝送し、処理を終了する。すなわち、サービス提供装置１１４が、提供を要求してきた個人情報の中に、提供することが禁止されている項目が１つでも入っている場合には、個人情報の保護を優先し、処理を終了させる（サービス提供装置１１４からサービスの提供を受けることを中止する）。

【００７４】

一方、以上のような処理により、サービス提供装置１１４から要求されてきたすべての項目についてのバッファ１、またはバッファ２への書き込みが完了したとステップＳ１０４において判定された場合、ステップＳ１１０に進み、確認リストのバッファ２に確認項目が登録されているか否かが判定される。すなわち、上述したように、自動応答が禁止されている項目（ユーザの確認が必要な項目）は、ステップＳ１０９において、バッファ２の確認リスト中に登録されている。バッファ２の確認リスト中に、所定の項目が登録されている場合には、ステップＳ１１１に進み、ユーザエージェント装置１１１は、そのバッファ２の確認リスト中に登録されている確認項目に関して、ユーザに確認すべき要求をプロキシ装置１０９に出力する。プロキシ装置１０９は、この要求を受けたとき、図９を参照して説明したように、端末装置１０１にユーザインタフェースを転送し、確認処理を行う。確認の結果が得られたとき、プロキシ装置１０９は、その結果をユーザエージェント装置１１１に転送する。

【００７５】

そこで、ユーザエージェント装置１１１は、ステップＳ１１２において、プロキシ装置１０９から応答があるまで待機し、応答があった場合、ステップＳ１１３に進み、その応答結果を判定する。ユーザからの応答結果が、その項目をサービス提供装置１１４に転送することを許可していない場合には、禁止項目が含まれていた場合と同様に、ステップＳ１１４に進み、バッファ１とバッファ２をクリアし、ステップＳ１１５において、サービス提供装置１１４に対してFailedの応答が出力される。

【００７６】

一方、ステップＳ１１３において、ユーザからの応答結果が、確認リスト中の項目をサービス提供装置１１４に提供することを許容していると判定された場合（図５のYESボタンが押された場合）には、ステップＳ１１６に進み、サービス提供装置１１４に対して応答の成功（図５のYESボタンが押されたこと）を示す値と、バッファ１に記録されている項目の内容をプロキシ装置１０９に転送する。上述したように、プロキシ装置１０９は、この項目の転送を受けたとき、これをサービス提供装置１１４に転送する。

【００７７】

一方、ステップＳ１１０において、バッファ２の確認リスト中に確認項目が登録されていないと判定された場合には、ステップＳ１０８において、自動応答が許容されている項目（ユーザに事前に確認する必要がない項目）だけがバッファ１に登録されていることになるので、ステップＳ１１６に進み、バッファ１の内容がプロキシ装置１０９に転送する処理が実行される。

【００７８】

さらに、他のユーザが、不正に所定のユーザの個人情報を利用しようとする場合がある。

そこで、ユーザエージェント装置１１１（またはプロキシ装置１０９）に、不正な個人情報の利用を防止させる機能を付加することができる。図１１は、この場合の、ユーザエージェント装置１１１の処理例を表している。この図１１に示す処理は、所定のユーザから、サーバ１００に対してアクセスが行われ、ユーザエージェント装置１１１が生成された場合に、その処理が開始される。

【００７９】

最初にステップＳ１３１において、そのユーザの同一プロファイル（個人情報）に対して、同時にアクセスすることが不可能な２以上の別の場所（例えば遠隔地）よりアクセスがあったか否かを判定する。そのようなアクセスがあったと判定された場合には、ステップＳ１３４に進み、そのようなアクセスがあったことをユーザエージェント装置１１１のログファイルに記録する。そして、ステップＳ１３５において、ユーザエージェント装置１１１は、時間的に後から行われたアクセスを拒絶する。そして、ステップＳ１３６において、先にアクセスが行われているユーザの端末装置１０１に対して（あるいは、そのアクセスが行われたアクセスポイントを管理するキャリア（アクセス管理者）に対して）、その個人情報に対する他のアクセスがあった旨を、プロキシ装置１０９を介して通知させる。その後、ステップＳ１３１に戻り、それ以降の処理が繰り返し実行される。

【００８０】

ステップＳ１３１において、同一プロファイルに対する他のアクセスがなされていないと判定された場合には、ステップＳ１３２に進み、その他の不正なアクセスの有無が判定され、不正なアクセスが存在しない場合には、ステップＳ１３３に進み、いま、セッションが確立しているアクセスの終了が指令されたか否かが判定され、終了が指令されていない場合には、ステップＳ１３１に戻り、それ以降の処理が繰り返し実行される。ステップＳ１３３において、アクセスの終了が指令されていると判定された場合、処理は終了される。

【００８１】

ステップＳ１３２において、他の不正なアクセスがあったと判定された場合には、ステップＳ１３７に進み、その旨がログファイルに記録された後、ステップＳ１３６に進み、その旨がユーザまたはキャリアに通知される。これにより、不正なユーザを即座に特定することができる。

【００８２】

図１２は、ユーザプロファイルデータベース１１０に記憶されているプロファイルの構成例を表している。このプロファイルのフォーマットは、OPSのフォーマットに対応している。各ユーザのプロファイルには、GUID(Globally Unique ID)が記録されている。このGUIDは、一人のユーザのプロファイルに対して、単一不変のものである。

【００８３】

VCARDは、電子名刺とも称され、ユーザの国、郵便番号、年齢、性、好みのスクリーン名、氏名、写真、誕生日、住所、電話番号、電子メールアドレス、肩書き、職務などが登録されている。このVCARDは、ユーザのみが、その内部のデータを書き込み可能である。

【００８４】

トップレベルセクションＡ，Ｂなどには、さらにサブセクションが設けられている。これらのセクションに、適宜必要な個人情報が登録されている。

【００８５】

なお、OPSのフォーマットに限らず、例えば、P3Pのフォーマットでプロファイルを構成してもよい。

【００８６】

以上のような機能は、本来、パーソナルコンピュータのような十分な資源と拡張性を期待できない携帯機器としての端末装置１０１や、セットトップ機器等での利用を前提としているが、通常のパーソナルコンピュータ１０６から利用することも可能である。この場合、パーソナルコンピュータ１０６とサーバ１００の間で、トランスポート層以下の通信スタックが違うものの、アプリケーションレベルでの通信は同一のものが利用可能である。

このような使用形態の一番のメリットは、端末装置１０１と家庭のパーソナルコンピュータ１０６で、同一のユーザプロファイルデータベース１１０を共有でき、そのプロファイルデータがいずれの機器から更新された場合でも、また、次回いずれの機器からアクセスした場合でも、確実にその反映が利用可能であると言う点である。

【００８７】

このように、代行サービスを行うサーバ１００を利用することで、ユーザインタフェースのみを実装した簡便な端末装置でも、インターネットのようなオープンな環境で、個人のプライバシーに関するデータを含むやり取りを行うことが可能になる。また、サーバ１００がネットワーク側の機能拡張に対応するため、ユーザは簡便な端末装置を利用しつづけながら、新しい機能を利用することが可能になる。

【００８８】

なお、上記したような処理を行うコンピュータプログラムをユーザに伝送する伝送媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【００８９】

【発明の効果】

以上の如く、本発明の第１の情報処理装置および方法によれば、ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報が、複数のユーザ毎に記憶されており、複数のユーザのうちの所定ユーザの情報処理装置から情報提供者の情報処理装置に対してアクセスがあった場合であって、そのアクセスの応答として、情報提供者の情報処理装置から所定ユーザの個人情報の取得の要求が項目毎にあったとき、情報提供者の情報処理装置から取得が要求された要求項目の中に第１の属性の項目が存在するか否かに基づいて、記憶されている所定ユーザの個人情報の提供に対する所定ユーザの許可の必要性が判定され、その判定結果と、所定ユーザの情報処理装置に対して、個人情報の提供の可否の前回の問い合わせの際に得られた回答とに基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無が判定され、提供すると判定された場合、記憶されている前記所定ユーザの前記個人情報の要求項目が情報提供者の情報処理装置に提供され、提供しないと判定された場合、要求項目の提供が禁止される。これにより、情報提供者に対して、誤りがなく、かつ正当な個人情報を確実に伝送することができ、もって、情報提供者は、提供する情報に対して、確実に課金処理を行うことが可能となる。また、ユーザは、任意の移動位置から、同一の環境下で、確実に個人情報を情報提供者に提供することが可能となる。さらに、機能拡張や、不具合の修正などに起因して、情報提供者と間の通信形態が変化したような場合においても、ユーザの情報処理装置を変更する必要性がなくなり、ユーザの負担を軽減することができる。

さらに、上述した一連の処理とは独立して、前記所定ユーザの前記個人情報の提供回数が計測され、その提供回数が閾値以上となった場合、前記所定ユーザの情報処理装置に対して、前記個人情報の提供の可否の問い合わせが行われ、その回答が得られると、前記提供回数が０にリセットされる、という一連の処理が繰り返される。これにより、上述した一連の処理が実行される度に、前記個人情報の提供の可否の問い合わせを行うといったことは不要となる。

【００９０】

また、本発明の第２の情報処理装置および方法によれば、ユーザの個人情報として、そのユーザへの確認が必要な第１の属性または確認が不要な第２の属性をそれぞれ個別に有する1以上の項目を含む個人情報を、複数のユーザ毎に記憶する記憶手段を有するサーバおよびネットワークを介して、情報提供者の情報処理装置に対して接続される所定ユーザの第２の情報処理装置により、次のような処理が実行される。即ち、サーバおよびネットワークを介して情報提供者の情報処理装置にアクセスされ、そのアクセスの応答として、情報提供者の情報処理装置から所定ユーザの個人情報の取得の要求が項目毎にサーバに対してあり、前記サーバが、前記情報提供者の情報処理装置から取得が要求された要求項目

の中に前記第１の属性の項目が存在するか否かに基づいて、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の提供に対する前記所定ユーザの許可の必要性を判定し、その判定結果と、前記所定ユーザから事前に得ている前記個人情報の提供の可否の回答結果とに基づいて、前記所定ユーザの前記個人情報の前記情報提供者への提供有無を判定し、提供すると判定した場合、前記記憶手段に記憶されている前記所定ユーザの前記個人情報の前記要求項目を前記情報提供者の情報処理装置に提供し、提供しないと判定した場合、前記要求項目の提供を禁止するまでの一連の処理を実行すべく、前記一連の処理とは独立して、前記所定ユーザの前記個人情報の提供回数が閾値以上となったことをトリガとして、前記サーバから、前記所定ユーザの情報処理装置自身に対して、前記個人情報の提供の可否が問い合わされたとき、前記所定ユーザから前記回答結果が取得され、その回答に基づいて、サーバに対して、記憶手段に記憶されている所定ユーザの個人情報の要求項目の情報提供者の情報処理装置への提供の可否が通知されることで、その提供の可否が制御される。これにより、安価な装置で、任意の位置から、誤ることなく、確実に、自分自身の個人情報を必要に応じて、情報提供者に提供することが可能となる。さらにまた、ユーザは、アクセスの度に、前記個人情報の提供の可否の問い合わせに対する回答を行う必要がなくなる。

【図面の簡単な説明】

【図１】本発明の情報処理装置を適用したネットワークシステムの構成例を示す図である。

【図２】図１の端末装置１０１とサーバ１００のアクセス開始時の動作を説明するフローチャートである。

【図３】図１の端末装置１０１、プロキシ装置１０９、ユーザエージェント装置１１１およびサービス提供装置１１４の動作を説明するタイミングチャートである。

【図４】図１の端末装置１０１、プロキシ装置１０９、ユーザエージェント装置１１１およびサービス提供装置１１４の動作を説明するタイミングチャートである。

【図５】図４のステップＳ２６における端末装置１０１の表示例を示す図である。

【図６】図１の端末装置１０１、プロキシ装置１０９、ユーザエージェント装置１１１およびサービス提供装置１１４の動作を説明するタイミングチャートである。

【図７】図６のステップＳ４８における端末装置１０１の表示例を示す図である。

【図８】図１のプロキシ装置１０９の他の動作を説明するフローチャートである。

【図９】図１のプロキシ装置１０９のさらに他の動作を説明するフローチャートである。

【図１０】図１のユーザエージェント装置１１１の動作を説明するフローチャートである。

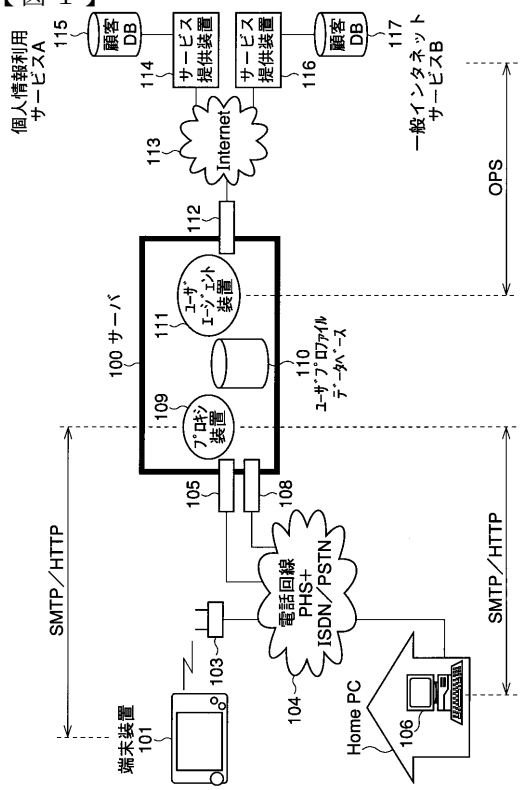
【図１１】図１のプロキシ装置１０９の他の動作を説明するフローチャートである。

【図１２】図１のユーザプロファイルデータベース１１０のプロファイルの構成例を示す図である。

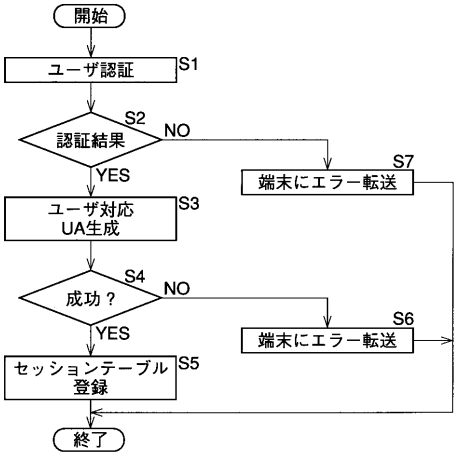
【符号の説明】

１００　サーバ，　１０１　端末装置，　１０３　基地局，　１０４　電話回線，　１０５，１０８　有線インタフェース，　１０９　プロキシ装置，　１１０　ユーザプロファイルデータベース，　１１１　ユーザエージェント装置，　１１４，１１６　サービス提供装置

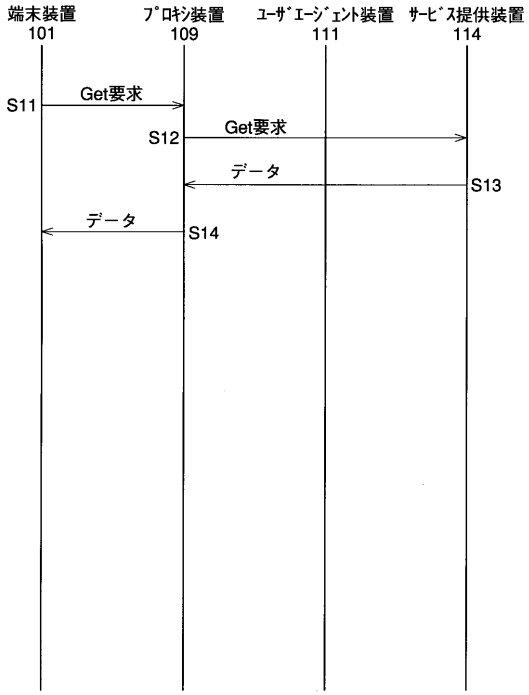
【図１】


個人情報利用サービスA
115
顧客DB
114
サービス提供装置
116
サービス提供装置
117
顧客DB
一般インタネットサービスB
113
Internet
OPS
112
100 サーバ
ユーザエージェント装置
111
ユーザプロファイルデータベース
110
プロキシ装置
109
105
108
SMTP／HTTP
SMTP／HTTP
電話回線 PHS+ ISDN／PSTN
103
104
Home PC
106
端末装置
101

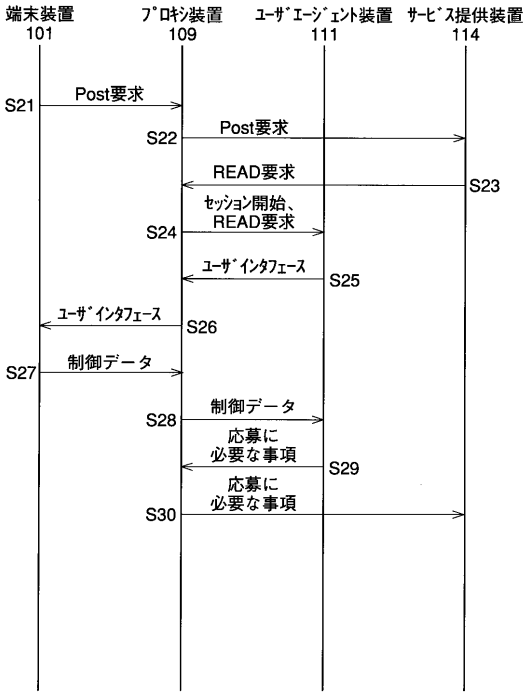
【図２】


開始
ユーザ認証
S1
S2
認証結果
NO
YES
S7
端末にエラー転送
ユーザ対応 UA生成
S3
S4
成功？
NO
YES
S6
端末にエラー転送
セッションテーブル登録
S5
終了

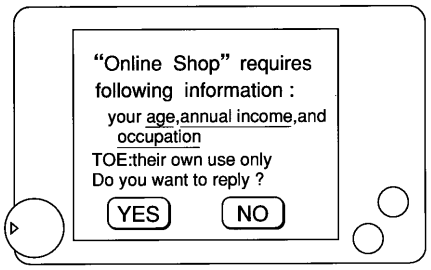
【図３】


端末装置 101
プロキシ装置 109
ユーザエージェント装置 111
サービス提供装置 114
S11
Get要求
S12
Get要求
データ
S13
データ
S14

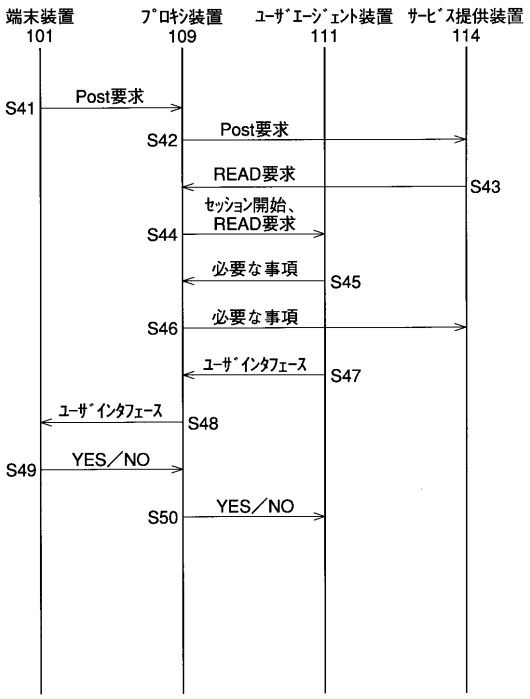
【図４】


端末装置 101
プロキシ装置 109
ユーザエージェント装置 111
サービス提供装置 114
S21
Post要求
S22
Post要求
READ要求
S23
セッション開始、READ要求
S24
ユーザインタフェース
S25
ユーザインタフェース
S26
S27
制御データ
制御データ
S28
応募に必要な事項
S29
応募に必要な事項
S30

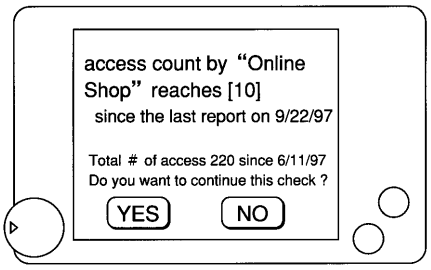
【図５】


"Online Shop" requires
following information :
your age,annual income,and
occupation
TOE:their own use only
Do you want to reply ?
YES
NO

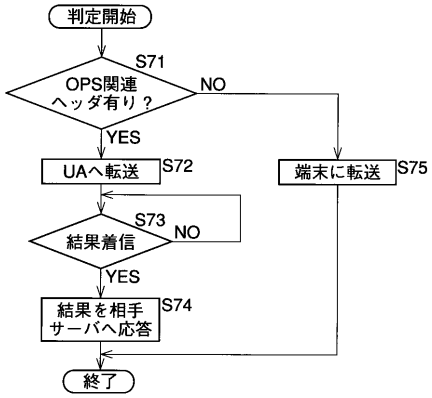
【図６】


端末装置
101
ﾌﾟﾛｷｼ装置
109
ﾕｰｻﾞｴｰｼﾞｪﾝﾄ装置
111
ｻｰﾋﾞｽ提供装置
114
S41
Post要求
S42
Post要求
READ要求
S43
ｾｯｼｮﾝ開始、
READ要求
S44
必要な事項
S45
S46
必要な事項
ﾕｰｻﾞｲﾝﾀﾌｪｰｽ
S47
ﾕｰｻﾞｲﾝﾀﾌｪｰｽ
S48
S49
YES／NO
S50
YES／NO

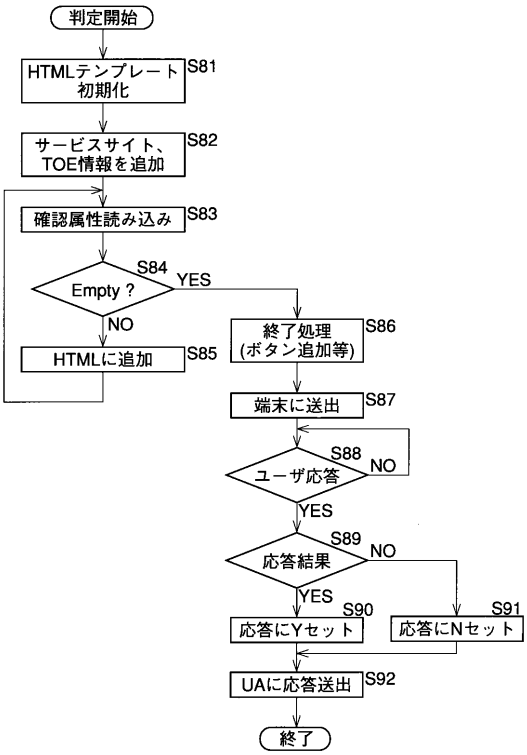
【図７】


access count by "Online
Shop" reaches [10]
since the last report on 9/22/97
Total # of access 220 since 6/11/97
Do you want to continue this check ?
YES
NO

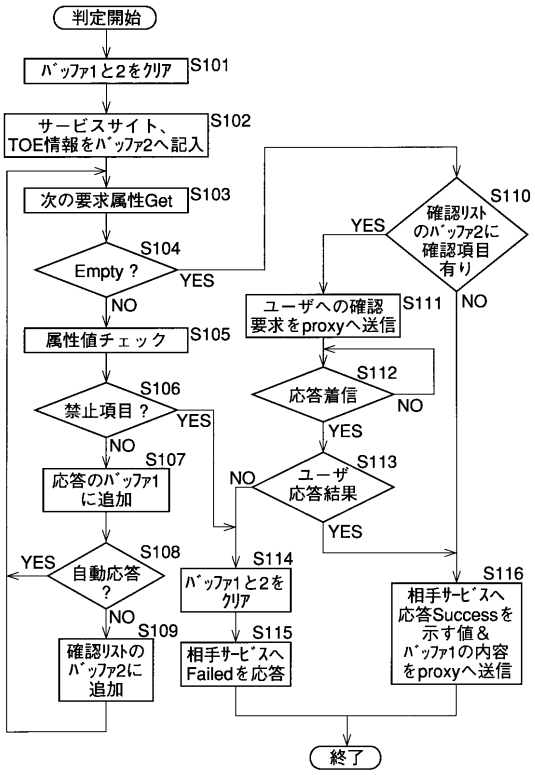
【図８】


判定開始
S71
OPS関連
ヘッダ有り？
NO
YES
UAへ転送
S72
端末に転送
S75
S73
結果着信
NO
YES
結果を相手
サーバへ応答
S74
終了

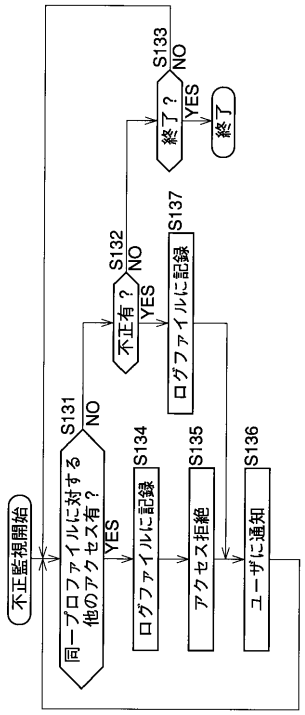
【図９】



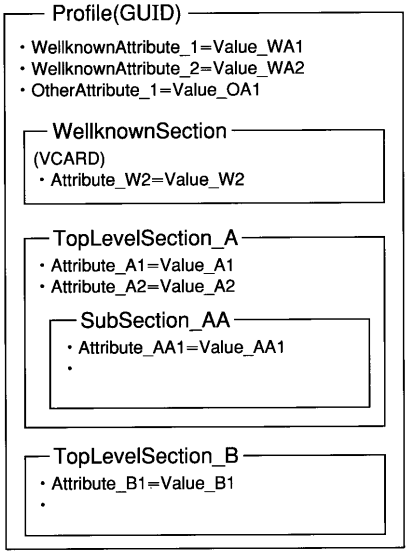
【図１０】



【図１１】



【図１２】



フロントページの続き

(56)参考文献 特開平０９－２０４４４５（ＪＰ，Ａ）
特開平０８－０２３３１５（ＪＰ，Ａ）
特開平０８－０７２９９７（ＪＰ，Ａ）
特開平０７－０９３６６５（ＪＰ，Ａ）
特開平０９－２１２５４８（ＪＰ，Ａ）
特開平０９－１７９９１２（ＪＰ，Ａ）
特開平０９－１６７１８５（ＪＰ，Ａ）
特開平０９－１３４３８９（ＪＰ，Ａ）
特開平０９－０１６６８２（ＪＰ，Ａ）
特開平０９－１１４７８３（ＪＰ，Ａ）
特開平０９－１１４８９１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06Q 30/00
G06F 21/00
G06Q 10/00