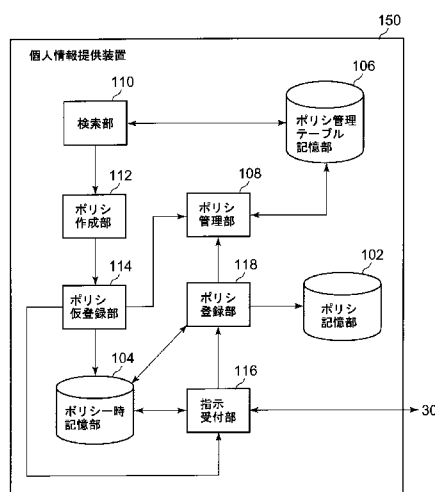


(43) 国際公開日
2010 年 6 月 17 日(17.06.2010)

- 〔続葉有〕

[图4]

[illegible]



GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, 添付公開書類:

NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ,
CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN,
TD, TG).

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

個人情報交換システム、個人情報提供装置、そのデータ処理方法、およびそのコンピュータプログラム

技術分野

[0001] 本発明は、個人情報交換システム、個人情報提供装置、そのデータ処理方法、およびそのコンピュータプログラムに関し、特に、プライバシーポリシーに従って個人情報を交換または提供する個人情報交換システム、個人情報提供装置、そのデータ処理方法、およびそのコンピュータプログラムに関する。

背景技術

[0002] この種の技術として、Liberty Alliance Projectにて策定された、ネットワーク上の各事業者間でユーザに関する情報を連携するための標準技術仕様 I D - W S F (Identity Web Services Framework) がある (図 2 3 参照)。I D - W S F を利用した個人情報交換システムの一例が、非特許文献 1 に記載されている。

[0003] 非特許文献 1 に記載された個人情報交換システムは、ウェブサービスプロバイダ (以後、「W S P」という。) 1 とウェブサービスコンシューマ (以後、「W S C」という。) 2 とディスカバリーサービス (以後、「D S」と略す) 3 とユーザエージェント (利用者端末のソフトウェア) 4 がネットワークを介して接続し、構成する。このような構成を有する非特許文献 1 に記載された個人情報交換システムの典型的な動作として、D S 3 を利用して個人情報を検索、要求、応答する手順を説明する。図 2 3 では、前提として、W S P 1 はユーザエージェント 4 を操作する利用者に関する情報を個人情報 5 として保有し、事前処理として D S 3 にアクセス情報 6 を設定する (ステップ S 0)。これにより、D S 3 は利用者の個人情報を保有する W S P 1 にアクセスすることができる。

[0004] 図 2 3 において、ユーザエージェント 4 を通じて、利用者は、W S C 2 の

利用制限のあるサービスを利用するために、WS C 2にアクセスする（ステップS 1）。WS C 2は、利用者の個人情報にアクセスするための情報を取得するために、DS 3に対してアクセス情報要求証明書要求メッセージを送付する（ステップS 2）。DS 3では、要求に応じてアクセストークンを発行し（ステップS 3）、WS C 2は、アクセス情報6とアクセストークンを取得する（ステップS 4）。WS C 2は取得したアクセス情報を元に、WSP 1に個人情報5の要求メッセージを送付する（ステップS 5）。WSP 1は要求を受け付けると認可判定を行い（ステップS 6）、その結果に基づきWS C 2に個人情報5を送付する（ステップS 7）。この認可判定において、アクセスルール等の情報を用いて、アクセスの可否を決定する。そして、WS C 2からユーザエージェント4にサービスが転記される（ステップS 8）。

[0005] 以上のように、非特許文献1に記載された個人情報交換システムでは、利用者の個人情報要求に応じて、WSP 1がポリシー等の認可判断を行うことで、個人情報の交換が可能になる。

[0006] また、ルールに基づいた情報処理装置の一例が、特許文献1に記載されている。図24に示すように、この情報処理装置10は、アクション動作部12と、誤動作判別部13と、フィードバック学習部14と、ルール修正部15と、ルール格納部16とから構成されている。

[0007] このような構成を有するルールに基づいた情報処理装置10はつぎのように動作する。

すなわち、ルール格納部16が保有するルールに基づきアクション動作部12が、当該ルールに対応する情報処理を行う。アクション動作部12の処理結果に基づき、誤動作判別部13は情報処理に対する応答が肯定的か否定的かを判定する。フィードバック学習部14が、判定結果を利用して当該情報処理に対応するルールを評価する。そして、ルール修正部15が、評価に基づきルール格納部16において保管されているルールを修正する。

[0008] 上記文献記載の事例が示すように、エンティティ間で利用者の個人情報を

交換する際には、ユーザの同意を確認し、その結果をポリシーとして保存する。ポリシーを変更する際には、その変更結果を既存のポリシーに反映させる。別のエンティティが、個人情報を管理しているエンティティにアクセスする際には、変更結果が反映されたポリシーを利用してアクセス可否の判断を行う。

[0009] また、特許文献2に記載のアクセス権管理方法は、個人のプライベート情報および該情報の開示のためのポリシーをサーバに一括保存および管理し、該情報の開示要求に対して該ポリシーに従って開示の可否を決定する。

先行技術文献

特許文献

[0010] 特許文献1：特開2008-123332号公報

特許文献2：特開2002-324194号公報

非特許文献

[0011] 非特許文献1：リバティアライアンスプロジェクト（Liberty Alliance Project）、“リバティ アイデンティティ ウェブサービス フレームワーク（Liberty Identity Web Services Framework（ID-WSF））V2.0”、[online]、2007年7月9日、[平成20年7月1日検索]、インターネット、＜URL http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates＞

発明の概要

発明が解決しようとする課題

[0012] 上述した方式においてはユーザ自身が個人情報へのアクセス可否に関するポリシー（プライバシーポリシー）を設定する場合、個人情報を送付する装置ごとにポリシーを設定する必要があった。そのため、WSCが多ければ多いほどポリシーの設定が増え、個人情報の送付先装置に応じてユーザ自身の同意に基づいたポリシーを設定することは非効率であるという問題点があった。

[0013] 装置ごとにポリシーを設定する理由は、プライバシー保護やコンプライアンス

の観点から利用目的や利用範囲等をユーザが確認をする必要があるからである。しかしながら、上述したように個人情報の送付先装置ごとに全てのポリシーをユーザ自身が設定することは、ユーザに大きな負担を強いることとなる。

[0014] 本発明の目的は、上述した課題を解決する個人情報交換システム、個人情報提供装置、そのデータ処理方法、およびそのコンピュータプログラムを提供することにある。

課題を解決するための手段

[0015] 本発明による個人情報提供装置は、ユーザの個人情報を取得する個人情報取得装置毎かつユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶装置と、ポリシー記憶装置にプライバシーポリシーが記憶されているかを識別する識別情報を、個人情報取得装置毎かつユーザ毎にポリシー管理テーブルに記録して管理するポリシー管理手段と、ポリシー管理テーブルを参照し、個人情報取得装置およびユーザに該当するプライバシーポリシーの識別情報を検索する検索手段と、該当するプライバシーポリシーの識別情報が見つからなかったとき、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成するポリシー作成手段と、作成されたプライバシーポリシーをポリシー記憶装置に記憶し、その識別情報をポリシー管理手段に通知してポリシー管理テーブルに記録させるポリシー登録手段とを備える。

[0016] 本発明による個人情報交換システムは、個人情報を記憶する個人情報記憶装置と、上記個人情報提供装置と、ユーザの個人情報を個人情報提供装置に要求して取得する個人情報取得装置と、ユーザのユーザ端末装置とを備え、個人情報提供装置は、個人情報取得装置からの個人情報の要求に応じて、ユーザ端末装置のユーザに個人情報のプライバシーポリシーの適用の認否を確認し、ユーザからの指示をユーザ端末装置から受け付け、承認されたプライバシーポリシーに従って、個人情報記憶装置から取得したユーザの個人情報を個人情報取得装置に提供する。

[0017] 本発明によるデータ処理方法は、個人情報提供装置のデータ処理方法であ

って、個人情報提供装置は、ユーザの個人情報を取得する個人情報取得装置毎かつユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶装置を備え、ポリシー記憶装置にプライバシーポリシーが記憶されているかを識別する識別情報を、個人情報取得装置毎かつユーザ毎にポリシー管理テーブルに記録して管理し、ポリシー管理テーブルを参照し、個人情報取得装置およびユーザに該当するプライバシーポリシーの識別情報を検索し、該当するプライバシーポリシーの識別情報が見つからなかったとき、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成し、作成されたプライバシーポリシーをポリシー記憶装置に記憶し、その識別情報をポリシー管理テーブルに記録する。

[0018] 本発明によるコンピュータプログラムは、コンピュータに個人情報提供装置を実現させるためのコンピュータプログラムであって、ユーザの個人情報を取得する個人情報取得装置毎かつユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶装置を備えたコンピュータに、ポリシー記憶装置にプライバシーポリシーが記憶されているかを識別する識別情報を、個人情報取得装置毎かつユーザ毎にポリシー管理テーブルに記録して管理するポリシー管理手順、ポリシー管理テーブルを参照し、個人情報取得装置およびユーザに該当するプライバシーポリシーの識別情報を検索する検索手順、該当するプライバシーポリシーの識別情報が見つからなかったとき、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成するポリシー作成手順、および、作成されたプライバシーポリシーをポリシー記憶装置に記憶し、その識別情報をポリシー管理テーブルに記録するポリシー登録手順を実行させるためのものである。

[0019] なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

[0020] また、本発明の各種の構成要素は、必ずしも個々に独立した存在である必要はなく、複数の構成要素が一個の部材として形成されていること、一つの

構成要素が複数の部材で形成されていること、ある構成要素が他の構成要素の一部であること、ある構成要素の一部と他の構成要素の一部とが重複していること等でもよい。

[0021] また、本発明のデータ処理方法およびコンピュータプログラムには複数の手順を順番に記載してあるが、その記載の順番は複数の手順を実行する順番を限定するものではない。このため、本発明のデータ処理方法およびコンピュータプログラムを実施するときには、その複数の手順の順番は内容的に支障しない範囲で変更することができる。

[0022] さらに、本発明のデータ処理方法およびコンピュータプログラムの複数の手順は個々に相違するタイミングで実行されることに限定されない。このため、ある手順の実行中に他の手順が発生すること、ある手順の実行タイミングと他の手順の実行タイミングとの一部ないし全部が重複していること等でもよい。

発明の効果

[0023] 本発明によれば、プライバシーポリシーを登録するユーザ操作の手間を省く個人情報交換システム、個人情報提供装置、そのデータ処理方法、およびそのコンピュータプログラムが提供される。

図面の簡単な説明

[0024] [図1]本発明の実施の形態に係る個人情報交換システムの構成を示すブロック図である。

[図2]図1に示す個人情報交換システムの個人情報提供装置の構成を示す機能ブロック図である。

[図3]図1に示す個人情報交換システムの個人情報提供装置の動作の一例を示すフローチャートである。

[図4]本発明の実施の形態に係る個人情報交換システムの個人情報提供装置の構成を示す機能ブロック図である。

[図5]図4に示す個人情報提供装置の動作の一例を示すフローチャートである。

[図6]本発明の実施の形態に係る個人情報交換システムの個人情報提供装置の構成を示す機能ブロック図である。

[図7]図6に示す個人情報提供装置のポリシー修正処理の流れの一例を示すフローチャートである。

[図8]本発明の実施の形態に係る個人情報交換システムの個人情報提供装置の構成を示す機能ブロック図である。

[図9]本発明の実施の形態に係る個人情報交換システムの個人情報提供装置の構成を示す機能ブロック図である。

[図10]図9に示す個人情報交換システムの個人情報取得装置と個人情報提供装置の動作の一例を示すフローチャートである。

[図11]図10に示すプライバシーポリシー検索処理の流れの一例を示すフローチャートである。

[図12]本発明の実施の形態に係る個人情報交換システムの構成を示すブロック図である。

[図13]図12に示す個人情報交換システムの個人情報取得および提供装置の構成を示す機能ブロック図である。

[図14]図12に示す個人情報交換システムの動作の一例を示すフローチャートである。

[図15]本発明の実施例を説明するための構成とメッセージの流れを示す図である。

[図16]本発明の実施例における個人情報提供装置のポリシー管理テーブル記憶部が保有する情報の一例である。

[図17]本発明の実施例における個人情報提供装置のポリシー管理テーブル記憶部が保有する情報の一例である。

[図18]本発明の実施例における個人情報提供装置のポリシー管理テーブル記憶部が保有する情報の一例である。

[図19]本発明の実施例を説明するための構成とメッセージの流れを示す図である。

[図20]本発明の実施例における個人情報提供装置のポリシー管理テーブル記憶部が保有する情報の一例である。

[図21]本発明の実施例における個人情報取得および提供装置のポリシー管理テーブル記憶部が保有する情報の一例である。

[図22]本発明の実施例における個人情報取得および提供装置のポリシー管理テーブル記憶部が保有する情報の一例である。

[図23]非特許文献 1 に記載された技術における個人情報の交換を実現するメッセージの流れ図である。

[図24]特許文献 1 に記載された技術における情報処理装置の構成を示すブロック図である。

発明を実施するための形態

[0025] 以下、本発明の実施の形態について、図面を用いて説明する。尚、すべての図面において、同様な構成要素には同様の符号を付し、適宜説明を省略する。

[0026] (第 1 の実施の形態)

図 1 は、本発明の実施の形態に係る個人情報交換システム 1000 の構成を示すブロック図である。

本実施形態の個人情報交換システム 1000 は、個人情報を記憶する個人情報記憶装置 90 と、個人情報提供装置 100 と、ユーザの個人情報を個人情報提供装置 100 に要求して取得する個人情報取得装置（図 1 では、複数の個人情報取得装置 20a、…、20n、以後、特に区別しない場合は、「個人情報取得装置 20」と示す）と、ユーザのユーザ端末装置 50 とを備える。個人情報提供装置 100 は、個人情報取得装置 20 からの個人情報の要求に応じて、ユーザの個人情報を提供するものである。個人情報提供装置 100 は、個人情報取得装置 20 に対して、ユーザ端末装置 50 のユーザに個人情報のプライバシーポリシーの適用の認否を確認し、ユーザからの指示をユーザ端末装置 50 から受け付ける。ユーザによって承認されたプライバシーポリシーに従って、ユーザの個人情報の提供の可否を判断した上で、個人情報記憶

装置 90 から取得した個人情報を個人情報取得装置 20 に提供する。

[0027] 具体的には、本実施形態の個人情報交換システム 1000 は、個人情報を他の装置に提供する個人情報提供装置 100 と、個人情報を他の装置から取得する複数の個人情報取得装置 20a ~ 20n と、ユーザが個人情報取得装置 20 にアクセスするために利用するユーザ端末装置 50 がネットワーク 30 を介して接続されている。

[0028] 個人情報記憶装置 90 は、ユーザの個人情報を保管する。本実施形態では、個人情報記憶装置 90 は、個人情報提供装置 100 に接続され、個人情報提供装置 100 が個人情報記憶装置 90 にアクセスして各個人情報取得装置 20 の要求に応じ、かつプライバシーポリシーに従って個人情報を提供する。図 1 では、個人情報記憶装置 90 は、個人情報提供装置 100 に接続された外部の記憶装置として構成されているが、これに限定されず、たとえば、個人情報提供装置 100 に含まれる記憶装置であってもよい。

[0029] 図 2 は、本発明の実施の形態に係る個人情報交換システム 1000 の個人情報提供装置 100 の構成を示す機能ブロック図である。

本実施形態の個人情報提供装置 100 は、ユーザの個人情報を取得する個人情報取得装置毎かつユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶装置（ポリシー記憶部 102）と、ポリシー記憶部 102 にプライバシーポリシーが記憶されているかを識別する識別情報を、個人情報取得装置 20 毎かつユーザ毎にポリシー管理テーブル（ポリシー管理テーブル記憶部 106）に記録して管理するポリシー管理部 108 と、ポリシー管理テーブル記憶部 106 を参照し、個人情報取得装置 20 およびユーザに該当するプライバシーポリシーの識別情報を検索する検索部 110 と、該当するプライバシーポリシーの識別情報が見つからなかったとき、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成するポリシー作成部 112 と、作成されたプライバシーポリシーをポリシー記憶部 102 に記憶し、その識別情報をポリシー管理部 108 に通知してポリシー管理テーブル記憶部 106 に記録させるポリシー登録部 118 とを備える。

- [0030] 本実施形態において、プライバシーポリシーとは、個人情報提供装置 100 が個人情報取得装置 20 からの個人情報要求に対する応答の可否を判断する基準となる情報である。この個人情報へのアクセス可否の判断の基準は個人情報取得装置 20 ごとに異なる。そのため、個人情報提供装置 100 は複数のプライバシーポリシーを保管する。また、プライバシーポリシーはユーザごとにも異なる。
- [0031] 本実施形態の個人情報提供装置 100 は、たとえば、図示しない CPU (Central Processing Unit) やメモリ、ハードディスク、および通信装置を備え、キーボードやマウス等の入力装置やディスプレイやプリンタ等の出力装置と接続されるサーバコンピュータにより実現することができる。そして、CPU が、ハードディスクに記憶されるプログラムをメモリに読み出して実行することにより、上記ユニット 108、110、112、118 の各機能を実現することができる。なお、以下の各図において、本発明の本質に関わらない部分の構成については省略してあり、図示されていない。
- [0032] また、個人情報提供装置 100 の各構成要素は、任意のコンピュータの CPU、メモリ、メモリにロードされた本図の構成要素を実現するプログラム、そのプログラムを格納するハードディスクなどの記憶ユニット、ネットワーク接続用インタフェースを中心にハードウェアとソフトウェアの任意の組合せによって実現される。そして、その実現方法、装置にはいろいろな変形例があることは、当業者には理解されるところである。以下説明する各図は、ハードウェア単位の構成ではなく、機能単位のブロックを示している。
- [0033] 図 3 は、本実施形態の個人情報提供装置 100 の動作の一例を示すフローチャートである。本実施形態のコンピュータプログラムは、コンピュータに個人情報提供装置 100 を実現させるためのコンピュータプログラムであって、コンピュータは、ユーザの個人情報を取得する個人情報取得装置 20 毎かつユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶部 102 を備え、コンピュータに、ポリシー記憶部 102 にプライバシーポリシーが記憶されているかを識別する識別情報を、個人情報取得装置 20 毎かつユーザ毎に

ポリシー管理テーブル記憶部 106 に記録して管理するポリシー管理手順（ステップ S 23）、ポリシー管理テーブル記憶部 106 を参照し、個人情報取得装置 20 およびユーザに該当するプライバシーポリシーの識別情報を検索する検索手順（ステップ S 11）、該当するプライバシーポリシーの識別情報が見つからなかったとき（ステップ S 13 の YES）、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成するポリシー作成手順（ステップ S 15）、作成されたプライバシーポリシーをポリシー記憶部 102 に記憶し（ステップ S 17）、その識別情報をポリシー管理テーブル記憶部 106 に記録するポリシー登録手順（ステップ S 23）、を実行させるように記述されている。

[0034] 図 2 に示すように、詳細には、本実施形態の個人情報提供装置 100 は、ポリシー記憶部 102 と、ポリシー管理テーブル記憶部 106 と、ポリシー管理部 108 と、検索部 110 と、ポリシー作成部 112 と、ポリシー登録部 118 とを備えている。

[0035] ポリシー記憶部 102 は、個人情報取得装置 20 毎かつユーザ毎の個人情報のプライバシーポリシーを記憶する。本実施形態において、ポリシー記憶部 102 には、ユーザによって承認された、承認済みのプライバシーポリシーが記憶される。

[0036] ポリシー管理テーブル記憶部 106 は、ユーザの個人情報を記憶する個人情報記憶装置 90 の個人情報への個人情報取得装置 20 からのアクセスの可否の判断基準となるプライバシーポリシーの記憶場所など、プライバシーポリシーの記憶場所が特定できる識別情報を、ユーザ毎かつ個人情報取得装置 20 毎に記憶する。

[0037] ポリシー管理部 108 は、プライバシーポリシーの記憶場所など、プライバシーポリシーの記憶場所が特定できる識別情報を、ユーザ毎かつ個人情報取得装置 20 毎にポリシー管理テーブル記憶部 106 に記録して管理する。

[0038] 検索部 110 は、ポリシー管理テーブル記憶部 106 を参照し、アクセス可否を判断するために必要となるプライバシーポリシーの保管場所を検索する。図

2では、検索部110への検索指示が図示されていないが、たとえば、後述するように、個人情報取得装置20が個人情報を要求してきたときに、個人情報取得装置20への個人情報の提供の可否を判断するために、検索部110により該当するプライバシーポリシーが探索される。あるいは、予めユーザや管理者によって指定されたユーザの個人情報を提供する可能性のある個人情報取得装置20について、まとめて検索を行い、各個人情報取得装置20についてプライバシーポリシーを作成しておくこともできる。したがって、検索部110への制御は、個人情報の要求やプライバシーポリシーの作成指示などをトリガとすることができる。

[0039] ポリシ作成部112は、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを作成する。本実施形態では、検索部110で、該当するプライバシーポリシーの記憶場所の情報が見つからなかったとき、新規にプライバシーポリシーを自動的に作成する。ここで、デフォルトのプライバシーポリシーは、ユーザ等によって予め設定され、メモリ（不図示）に記憶されているものとする。

[0040] 本実施形態の個人情報提供装置100において、ポリシ作成部112は、デフォルトのプライバシーポリシーとして、ポリシ記憶部102に記憶されているプライバシーポリシーに基づいて、プライバシーポリシーを自動的に作成してもよい。

[0041] たとえば、ポリシ作成部112は、他の個人情報取得装置20に対して既に登録されているユーザのプライバシーポリシーを複製して新規のプライバシーポリシーを作成することができる。ユーザに対応する複数のプライバシーポリシーが登録済みの場合は、登録や更新日時が新しい順や予め定めた優先順位で選択されたプライバシーポリシーを原本として複製してもよい。

[0042] ポリシ登録部118は、ポリシ作成部112により自動的に作成されたプライバシーポリシーをポリシ記憶部102に記憶し、その記憶場所の情報をポリシ管理部108に通知してポリシ管理テーブル記憶部106に記録させる。

[0043] 上述のような構成において、本実施の形態の個人情報提供装置100のデ

ータ処理方法を以下に説明する。以下、図 1～図 3 を用いて説明する。

本実施形態のデータ処理方法は、個人情報提供装置 100 のデータ処理方法であって、個人情報提供装置 100 は、ユーザの個人情報を取得する個人情報取得装置 20 毎かつユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶部 102 を備え、ポリシー記憶部 102 にプライバシーポリシーが記憶されているかを識別する識別情報を、個人情報取得装置 20 毎かつユーザ毎にポリシー管理テーブル記憶部 106 に記録して管理し（ステップ S 23）、ポリシー管理テーブル記憶部 106 を参照し、個人情報取得装置 20 およびユーザに該当するプライバシーポリシーの識別情報を検索し（ステップ S 11）、該当するプライバシーポリシーの識別情報が見つからなかったとき（ステップ S 13 の YES）、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成し（ステップ S 15）、作成されたプライバシーポリシーをポリシー記憶部 102 に記憶し（ステップ S 17）、その識別情報をポリシー管理テーブル記憶部 106 に記録する（ステップ S 23）。

[0044] このように構成された個人情報提供装置 100 の動作について、以下に説明する。以下、図 1～図 3 を用いて説明する。

本実施形態の個人情報提供装置 100 は、以下の動作によりプライバシーポリシーを管理する。たとえば、個人情報取得装置 20 からの個人情報の要求を受信した際などに、要求の可否を判断するプライバシーポリシーが必要となる。

[0045] そこで、まず、検索部 110 により、ポリシー管理テーブル記憶部 106 を参照し、プライバシーポリシーの位置や状態に関する情報を取得する（ステップ S 11）。上述したように、ポリシー管理テーブル記憶部 106 には、ユーザの個人情報を記憶する個人情報記憶装置 90 の個人情報への個人情報取得装置 20 からのアクセスの可否の判断基準となるプライバシーポリシーの記憶場所など、プライバシーポリシーの記憶場所が特定できる識別情報が、ユーザ毎かつ個人情報取得装置 20 毎に記憶されている。

[0046] 検索したユーザの個人情報取得装置 20 に適用するプライバシーポリシーがポリシー記憶部 102 に記憶されていることが識別情報から判別された場合には

（ステップS 1 3のN O）、そのプライバシーポリシーをアクセス可否判断に利用することとなり、その識別情報、すなわちプライバシーポリシーの記憶場所を取得して本処理を終了する。

[0047] 一方、ポリシー記憶部 1 0 2に該当するプライバシーポリシーが存在しない場合には（ステップS 1 3のY E S）、ポリシー作成部 1 1 2が、デフォルトのプライバシーポリシーに基づいて、新たなポリシーを生成し（ステップS 1 5）、ポリシー登録部 1 1 8により、生成されたプライバシーポリシーがポリシー記憶部 1 0 2に登録される（ステップS 1 7）。

[0048] そして、ポリシー登録部 1 1 8からポリシー管理部 1 0 8に、プライバシーポリシーを記憶した場所の情報を通知して、ポリシー管理テーブル記憶部 1 0 6に登録される（ステップS 2 3）。これにより、ポリシー管理部 1 0 8に要求エンティティに対するポリシーが存在することが通知され、アクセス可否判断に利用させることとなる。

[0049] 以上、説明したように、本実施形態の個人情報提供装置 1 0 0によれば、個人情報取得装置 2 0 毎、かつ、ユーザ毎に設定する必要があるプライバシーポリシーを管理でき、必要なプライバシーポリシーが存在しないときに、デフォルトのプライバシーポリシーに基づいて、自動的に作成することができるので、ユーザのプライバシーポリシーの設定処理の操作の手間を大幅に省くことができる。個人情報取得装置 2 0 が多数の場合でも、装置ごとにポリシーを設定する手間を省け、また、ユーザが予め設定したデフォルトのポリシーに基づいて作成されるので、ユーザが同意したものとして利用することができる。

[0050] （第 2 の実施の形態）

図 4 は、本実施形態の個人情報提供装置 1 5 0の構成を示す機能ブロック図である。本実施形態の個人情報提供装置 1 5 0は、上記実施形態の個人情報提供装置 1 0 0とは、ポリシー作成部 1 1 2で作成されたポリシーを一旦仮登録し、ユーザの承認を得てから正式に登録する点で相違する。本実施形態の個人情報交換システム（不図示）は、図 1 の個人情報提供装置 1 0 0に替えて、個人情報提供装置 1 5 0を備える。以下、図 1 の個人情報提供装置 1 0

0を個人情報提供装置150と読み替えて、図1および図4を参照しながら説明する。

[0051] 本実施形態の個人情報提供装置150において、ユーザが未承認のプライバシーポリシーを一時的に記憶するポリシー時記憶装置（ポリシー時記憶部104）と、ポリシー作成部112により作成されたプライバシーポリシーを未承認のプライバシーポリシーとしてポリシー時記憶部104に一時的に記憶し、その識別情報をポリシー管理部108に通知してポリシー管理テーブル記憶部106に記録させるポリシー仮登録部114と、ポリシー時記憶部104に仮登録された未承認のプライバシーポリシーをユーザに提示し、プライバシーポリシーの適用の認否を確認し、指示をユーザから受け付ける指示受付部116とをさらに備え、ポリシー登録部118は、ポリシー時記憶部104に仮登録された未承認のプライバシーポリシーがユーザにより承認されたとき、承認済みプライバシーポリシーとしてポリシー記憶部102に記憶し、その識別情報をポリシー管理部108に通知してポリシー管理テーブル記憶部106に記録させる。

[0052] また、本実施形態の個人情報提供装置150において、ポリシー管理部108が、個人情報取得装置200毎かつユーザ毎にポリシー管理テーブル記憶部106に記録して管理する識別情報は、ポリシー記憶部102またはポリシー時記憶部104のいずれにプライバシーポリシーが記憶されているかを識別する情報を含み、指示受付部116は、検索された識別情報に基づいて、該当するプライバシーポリシーがポリシー時記憶部104に記憶されていることを判定し、ポリシー時記憶部104に仮登録された未承認のプライバシーポリシーをユーザに提示し、プライバシーポリシーの適用の認否を確認し、指示をユーザから受け付けることもできる。

[0053] 具体的には、本実施形態の個人情報提供装置150は、図2の個人情報提供装置100の構成に加え、ポリシー時記憶部104と、ポリシー仮登録部114と、指示受付部116とをさらに備えている。

[0054] ポリシー時記憶部104は、ユーザに承認されていない、未承認のプライバシーポリシーを一時的に記憶する。

なお、本実施形態では、ポリシ記憶部 102 およびポリシー時記憶部 104 は、異なる記憶部としているが、これは論理的なものであり、物理的には、同じ記憶装置内で、ことなる領域やあるいは、承認済か未承認かが識別できる情報を関連付けて記憶できれば、特に領域を分ける必要もない。すなわち、ポリシ管理テーブル記憶部 106 において、プライバシーポリシの記憶場所と、そのプライバシーポリシが承認済みか未承認であることを識別するための情報を関連付けて管理できればよい。

[0055] ポリシ仮登録部 114 は、ポリシ作成部 112 が自動的に作成した未承認のプライバシーポリシをポリシー時記憶部 104 に一時的に記憶し、その記憶場所の情報をポリシ管理部 108 に通知してポリシ管理テーブル記憶部 106 に記録させる。

[0056] 指示受付部 116 は、ポリシー時記憶部 104 に仮登録された未承認のプライバシーポリシをユーザに提示し、このプライバシーポリシに関するユーザの同意を求め、認否の指示をユーザから受け付ける。ここでいう、ユーザとは、個人情報の主体者である。また、図示されていないが、指示受付部 116 は、ネットワーク 30 を介してユーザ端末装置 50 と接続され、ユーザ端末装置 50 の表示装置（不図示）に操作画面を提示することができる。そして、ユーザが操作部（不図示）を操作して入力や指示を行い、ユーザ端末装置 50 におけるユーザによる入力や指示が指示受付部 116 にネットワーク 30 を介して受け付ける。

[0057] ユーザ端末装置 50 にてユーザに操作させるタイミングは、様々な状況が考えられる。たとえば、個人情報取得装置 20 に対してユーザ端末装置 50 からサービスの利用を申請した場合などに、個人情報取得装置 20 から個人情報提供装置 150 に対してユーザの個人情報を問い合わせることが考えられる。その場合は、ユーザ端末装置 50 から個人情報取得装置 20 に対してサービス利用を申請しているサイトから、個人情報提供装置 150、たとえば、インターネットプロバイダなどのサイトのページに移行し、ユーザ端末装置 50 に操作画面を表示させて、ユーザに同意を求めることができる。

[0058] あるいは、ユーザがサービスの利用を申請した後で個人情報取得装置 20 で承認に時間を要する場合、別途、後から、個人情報取得装置 20 から個人情報提供装置 150 に対してユーザの個人情報を問い合わせることも考えられる。その場合は、個人情報提供装置 150 からユーザの連絡先として予め個人情報取得装置 20 に登録されていたメールアドレスなどに、プライバシーポリシーの設定に関するサイトの URL アドレスを記載したメールを送信してもよい。ユーザは、ユーザ端末装置 50 でメールを受信し、メールに記載された URL アドレスのサイトにアクセスすることで、プライバシーポリシーに関する設定画面をユーザ端末装置 50 に表示できる。これにより、ユーザ端末装置 50 から、プライバシーポリシーに対するユーザの認否の回答を得ることが可能となる。

[0059] 本実施形態において、ポリシー登録部 118 は、ユーザにより承認された仮登録されたプライバシーポリシーをポリシー記憶部 102 に記憶し、その記憶場所の情報をポリシー管理部 108 に通知してポリシー管理テーブル記憶部 106 に記録させる。

[0060] 本実施形態において、個人情報提供装置 150 の CPU（不図示）が、コンピュータプログラムを実行することにより、上記ユニット 108～118 の各機能を実現することができる。

図 5 は、本実施形態の個人情報提供装置 150 の動作の一例を示すフローチャートである。本実施形態のコンピュータプログラムは、コンピュータに、ポリシー作成手順（ステップ S 15）により作成されたプライバシーポリシーを未承認のプライバシーポリシーとしてポリシー一時記憶部 104 に一時的に記憶し、その識別情報をポリシー管理テーブル記憶部 106 に記録させるポリシー仮登録手順（ステップ S 18）、ポリシー一時記憶部 104 に仮登録された未承認のプライバシーポリシーをユーザに提示し、プライバシーポリシーの適用の認否を確認し、指示をユーザから受け付ける指示受付手順（ステップ S 19）、ポリシー一時記憶部 104 に仮登録された未承認のプライバシーポリシーがユーザにより承認されたとき、承認済みプライバシーポリシーとしてポリシー記憶部 102 に

記憶する手順（ステップS 2 1）、その識別情報をポリシー管理テーブル記憶部 1 0 6 に記録する手順（ステップS 2 3）、をさらに実行させるように記述されている。

[0061] また、本実施形態のコンピュータプログラムにおいて、ポリシー管理手順（ステップS 2 3）において、個人情報取得装置 2 0 毎かつユーザ毎にポリシー管理テーブル記憶部 1 0 6 に記録して管理する識別情報は、ポリシー記憶部 1 0 2 またはポリシー時記憶部 1 0 4 のいずれにプライバシーポリシーが記憶されているかを識別する情報を含み、コンピュータに、検索された識別情報に基づいて、該当するプライバシーポリシーがポリシー時記憶部 1 0 4 に記憶されていることを判定し（不図示）、ポリシー時記憶部 1 0 4 に仮登録された未承認のプライバシーポリシーをユーザに提示し、プライバシーポリシーの適用の認否を確認し、指示をユーザから受け付ける手順（ステップS 1 9）、を実行させるように記述されてもよい。

[0062] 上述のような構成において、本実施の形態の個人情報提供装置 1 5 0 のデータ処理方法を以下に説明する。以下、図 4 および図 5 を用いて説明する。

本実施形態の個人情報提供装置 1 5 0 のデータ処理方法において、作成されたプライバシーポリシーを未承認のプライバシーポリシーとしてポリシー時記憶部 1 0 4 に一時的に記憶し、その識別情報をポリシー管理テーブル記憶部 1 0 6 に記録し（ステップS 1 8）、ポリシー時記憶部 1 0 4 に仮登録された未承認のプライバシーポリシーをユーザに提示し、プライバシーポリシーの適用の認否を確認し、指示をユーザから受け付け（ステップS 1 9）、ポリシー時記憶部 1 0 4 に仮登録された未承認のプライバシーポリシーがユーザにより承認されたとき、承認済みプライバシーポリシーとしてポリシー記憶部 1 0 2 に記憶し、その識別情報をポリシー管理テーブル記憶部 1 0 6 に記録する。

[0063] また、本実施形態の個人情報提供装置 1 5 0 のデータ処理方法において、個人情報取得装置 2 0 毎かつユーザ毎にポリシー管理テーブル記憶部 1 0 6 に記録して管理する識別情報は、ポリシー記憶部 1 0 2 またはポリシー時記憶部 1 0 4 のいずれにプライバシーポリシーが記憶されているかを識別する情報を含

み、検索された識別情報に基づいて、該当するプライバシーポリシーがポリシー時記憶部 104 に記憶されていることを判定し（不図示）、ポリシー時記憶部 104 に仮登録された未承認のプライバシーポリシーをユーザに提示し、プライバシーポリシーの適用の認否を確認し、指示をユーザから受け付けてもよい（ステップ S 19）。

[0064] このように構成された個人情報提供装置 150 の動作について、以下に説明する。以下、図 1、図 4、図 5 を用いて説明する。

本実施形態の個人情報提供装置 150 は、上記実施形態の個人情報提供装置 100 の図 3 のフローチャートと同様なステップ S 11～S 15、S 23 に加え、図 5 のステップ S 18～S 25 をさらに含む。

[0065] ステップ S 15 で、ポリシー作成部 112 により新たなポリシーが生成された後、ポリシー仮登録部 114 により、ポリシー作成部 112 により作成された新規のプライバシーポリシーがポリシー時記憶部 104 に一時的に保存される（ステップ S 18）。

[0066] そして、指示受付部 116 により、ユーザ端末装置 50 に未承認のプライバシーポリシーを提示し、このプライバシーポリシーに関するユーザの同意を求める。そして、指示受付部 116 が、ユーザ端末装置 50 からプライバシーポリシー設定に関するユーザの同意を受け付けた場合には（ステップ S 19 の YES）、ポリシー登録部 118 により、ポリシー時記憶部 104 に仮登録されていたプライバシーポリシーがポリシー記憶部 102 に登録される（ステップ S 21）。このとき、ポリシー時記憶部 104 に仮登録されていたプライバシーポリシーは削除する。

[0067] そして、ポリシー登録部 118 からポリシー管理部 108 に、プライバシーポリシーを記憶した場所の情報を通知して、ポリシー管理テーブル記憶部 106 に記録される（ステップ S 23）。これにより、ポリシー管理部 108 に要求エンティティに対するポリシーが存在することが通知され、アクセス可否判断に利用させることとなる。

[0068] また、ユーザへの問い合わせに対し、ユーザから同意が得られなかった場

合（ステップS 1 9のNO）、指示受付部 1 1 6は、ポリシー仮登録部 1 1 4に、ポリシー時記憶部 1 0 4に仮登録されていたプライバシーポリシーを削除させる（ステップS 2 5）。そして、ポリシー管理部 1 0 8に要求エンティティに対するプライバシーポリシーが存在しないことが通知され、アクセス可否判断に利用させることとなる。

[0069] 以上、説明したように、本実施形態の個人情報提供装置 1 5 0によれば、上記実施形態の個人情報提供装置 1 0 0と同様な効果を奏するとともに、新規に作成されたプライバシーポリシーは、ユーザの承認を得てから適用することができる。

[0070] また、プライバシーポリシーを設定する際には必ずユーザに確認を取るので、ユーザの意図に反したプライバシーポリシーを、個人情報を提供する装置が適用することを防ぐことができるので、ユーザの意図に基づいて個人情報をエンティティ間で交換できる。

[0071] （第 3 の実施の形態）

図 6 は、本実施形態の個人情報提供装置 2 0 0の構成を示す機能ブロック図である。本実施形態の個人情報提供装置 2 0 0は、上記実施形態の個人情報提供装置 1 0 0および個人情報提供装置 1 5 0とは、ユーザからプライバシーポリシーの変更や設定を受け付ける点で相違する。以下、図 6 の個人情報提供装置 2 0 0は、個人情報提供装置 1 5 0の構成に、ポリシー修正部 2 0 2をさらに備えた構成を例に説明する。

[0072] 本実施形態の個人情報提供装置 2 0 0は、上記実施形態の個人情報提供装置 1 5 0の構成に加え、ポリシー記憶部 1 0 2に記憶されているプライバシーポリシーの修正指示をユーザから受け付け、受け付けた修正指示に基づいて、プライバシーポリシーを修正するポリシー修正部 2 0 2をさらに備える。

[0073] さらに、本実施形態の個人情報提供装置 2 0 0において、ポリシー修正部 2 0 2は、指示受付部 1 1 6が受け付けた指示でユーザにより否認されたプライバシーポリシーの修正指示をユーザから受け付け、受け付けた修正指示に基づいて、プライバシーポリシーを修正し、ポリシー仮登録部 1 1 4は、修正されたプ

ライバシポリシをポリシー時記憶部 104 に一時的に記憶し、その識別情報をポリシ管理部 108 に通知してポリシ管理テーブル記憶部 106 に記録させる。

[0074] なお、個人情報提供装置 200 が、個人情報提供装置 100 の構成にポリシ修正部 202 を追加した構成の場合、ポリシ登録部 118 は、修正されたプライバシポリシをポリシ記憶部 102 に記憶し、その識別情報をポリシ管理部 108 に通知してポリシ管理テーブル記憶部 106 に記録させる。

[0075] このように構成された個人情報提供装置 200 では、上記実施形態の個人情報提供装置 150 の図 5 のステップ S19 の NO の場合、プライバシポリシを削除する替わりに、ユーザの意図する内容に修正することができる。

[0076] すなわち、ユーザ同意を取得する段階で、ユーザが独自のポリシを設定でき、指示受付部 116 が設定内容を受け付け、ポリシ修正部 202 が設定内容に従って、プライバシポリシを修正する。このプライバシポリシのユーザによる設定は、ユーザのユーザ端末装置 50 に対して、個人情報提供装置 200 から設定用画面がネットワーク 30 を介して提供され、ユーザ端末装置 50 でユーザが操作を行うことで実現できる。ユーザ端末装置 50 上の設定画面を介して入力された設定内容は、ネットワーク 30 を介して個人情報提供装置 200 に送信され、指示受付部 116 が受け付ける。

[0077] この修正されたプライバシポリシは、ポリシ仮登録部 114 によりポリシー時記憶部 104 に一時的に仮登録される。そして、ポリシ管理部 108 に通知され、ポリシ管理テーブル記憶部 106 に記録される。

[0078] ここで、ポリシー時記憶部 104 に仮登録されたプライバシポリシが存在するが、このプライバシポリシは未だユーザの同意を得ていないので、上述した新規のプライバシポリシの仮登録時と同様に、指示受付部 116 により、仮登録されたプライバシポリシに関するユーザ同意をユーザ端末装置 50 に求め、ユーザからの指示を受け付ける。ユーザが同意した場合には、ポリシ登録部 118 により、ポリシー時記憶部 104 に一時的に記憶されていたプライバシポリシをポリシ記憶部 102 に登録する。そして、ポリシ登録部

１１８は、ポリシー管理部１０８に通知し、ポリシー管理テーブル記憶部１０６に記録させる。

[0079] 一方、ユーザが同意しない場合には、ポリシー時記憶部１０４のプライバシーポリシーを削除し、そして、ポリシー管理部１０８に要求エンティティに対するプライバシーポリシーが存在しないことが通知され、アクセス可否判断に利用されることとなる。また、図示していないが、ユーザは、この設定の承認を保留することもでき、後で承認するようにしてもよい。

[0080] 図７は、本実施形態の個人情報提供装置２００のポリシー修正処理の詳細な処理の流れの一例を示すフローチャートである。以下、図６および図７を用いて説明する。本実施形態において、個人情報提供装置２００のＣＰＵが、コンピュータプログラムを実行することにより、上記ユニット１０８～１１８、および２０２の各機能を実現することができる。本実施形態のコンピュータプログラムは、コンピュータに、上記実施形態の個人情報提供装置１５０のコンピュータプログラムの手順（図５におけるステップＳ１１～Ｓ２５）に加え、ポリシー修正処理において、指示受付手順（図５におけるステップＳ１９）で受け付けた指示でユーザにより否認された（図５におけるステップＳ１９のＮＯ）プライバシーポリシーの修正指示をユーザから受け付け、受け付けた修正指示に基づいて、プライバシーポリシーを修正するポリシー修正手順（ステップＳ４０１）、修正されたプライバシーポリシーをポリシー時記憶部１０４に一時的に記憶し、その識別情報をポリシー管理テーブル記憶部１０６に記録する手順（ステップＳ４０３）、を実行させるように記述されている。

[0081] 上述のような構成において、本実施の形態の個人情報提供装置２００のデータ処理方法を以下に説明する。以下、図６および図７を用いて説明する。

本実施形態の個人情報提供装置２００のデータ処理方法は、受け付けた指示でユーザにより否認された（図５におけるステップＳ１９のＮＯ）プライバシーポリシーの修正指示をユーザから受け付け、受け付けた修正指示に基づいて、プライバシーポリシーを修正し（ステップＳ４０１）、修正されたプライバシーポリシーをポリシー時記憶部１０４に一時的に記憶し、その識別情報をポリ

シ管理テーブル記憶部 106 に記録する（ステップ S 403）。

[0082] このように構成された本実施形態の個人情報提供装置 200 の動作について、以下に説明する。以下、図 6 および図 7 を用いて説明する。

まず、指示受付部 116 で、ユーザが独自に設定または修正したプライバシーポリシーの設定内容を受け付け、ポリシー修正部 202 により、設定内容に従って、プライバシーポリシーが修正される（ステップ S 401）。

[0083] そして、修正されたプライバシーポリシーは、ポリシー仮登録部 114 によりポリシー時記憶部 104 に一時的に仮登録される（ステップ S 403）。

ここで、ポリシー時記憶部 104 に仮登録されたプライバシーポリシーが存在するが、このプライバシーポリシーは未だユーザの同意を得ていないので、上述した新規のプライバシーポリシーの仮登録時と同様に、指示受付部 116 により、仮登録されたプライバシーポリシーに関するユーザ同意をユーザ端末装置 50 に求め、ユーザからの指示を受け付ける（ステップ S 405）。ユーザが同意した場合には（ステップ S 405 の YES）、ポリシー登録部 118 により、ポリシー時記憶部 104 に一時的に記憶されていたプライバシーポリシーをポリシー記憶部 102 に登録する（ステップ S 407）。そして、ポリシー登録部 118 は、ポリシー管理部 108 に通知し、ポリシー管理テーブル記憶部 106 に記録させる（ステップ S 409）。これにより、ポリシー管理部 108 に要求エンティティに対するポリシーが存在することが通知され（ステップ S 411）、アクセス可否判断に利用されることとなる。

[0084] 一方、ステップ S 405 におけるユーザへの問い合わせに対し、ユーザから同意が得られなかった場合（ステップ S 405 の NO）、指示受付部 116 は、ポリシー仮登録部 114 に、ポリシー時記憶部 104 に仮登録されていたプライバシーポリシーを削除させる（ステップ S 413）。そして、ポリシー管理部 108 に要求エンティティに対するプライバシーポリシーが存在しないことが通知され、アクセス可否判断に利用させることとなる。もし、ユーザが修正したプライバシーポリシーの承認を保留する指示をした場合は、ポリシー時記憶部 104 に仮登録されたプライバシーポリシーは削除せず、ポリシー管理部 10

8に通知し、ポリシー管理テーブル記憶部106に、該当するプライバシーポリシーの記憶場所を記録させる。

[0085] 以上、説明したように、本実施形態の個人情報提供装置200によれば、ユーザの負担を最小限にしつつも、適切なプライバシーポリシーがユーザによって設定できる。そして、ユーザによって設定されたプライバシーポリシーを、ユーザが指定した他の個人情報取得装置20に反映できる。これにより、ユーザは、一度の操作で他の個人情報取得装置20のプライバシーポリシーも設定でき、ユーザの操作の負担を大幅に軽減できる。

[0086] また、ユーザが設定するプライバシーポリシーの内容を当該装置がすでに管理している当該ユーザに関する他のプライバシーポリシーに反映できる。さらに、プライバシーポリシーの変更結果を反映させる際には確実にユーザの同意に関する処理を受け付けることができる。

[0087] (第4の実施の形態)

図8は、本実施形態の個人情報提供装置300の構成を示す機能ブロック図である。本実施形態の個人情報提供装置300は、上記実施形態の個人情報提供装置200とは、ポリシー修正部202で修正したプライバシーポリシーの適用を承認する個人情報取得装置20(図1参照)を指定する点で相違する。

[0088] すなわち、ユーザ自身が個人情報へのアクセス可否を判断するためのポリシー(プライバシーポリシー)を設定する場合、個人情報を配布する装置ごとにプライバシーポリシーを設定する必要があるが、装置が多ければ多いほどプライバシーポリシーを設定する操作が増えるため、プライバシーポリシーを全ての装置向けに設定することは非効率である。

[0089] このため、本実施形態の個人情報提供装置300では、ユーザがプライバシーポリシーを設定した場合、その変更内容を当該ユーザが設定した他のプライバシーポリシーにも反映させるように修正する。修正したプライバシーポリシーを適用する場合には、一度ユーザの確認をとり、ユーザが修正したプライバシーポリシーの適用を同意した場合にのみ、修正ポリシーを適用することにより、ユー

ザは一度ポリシ変更操作するだけで全てのプライバシーポリシにその変更操作の内容を反映させる。

[0090] 本実施形態の個人情報提供装置 300 は、修正されて仮登録されたプライバシーポリシの適用を承認する個人情報取得装置 20 の指定をユーザから受け付ける指定受付部 302 をさらに備え、ポリシ登録部 118 は、ユーザの指定に基づき、適用を承認された個人情報取得装置 20 の承認済みプライバシーポリシとして、修正されて仮登録されたプライバシーポリシをポリシ記憶部 102 に記憶し、その識別情報をポリシ管理部 108 に通知してポリシ管理テーブル記憶部 106 に記録させる。

[0091] また、本実施形態の個人情報提供装置 300 が、図 1 の個人情報提供装置 100 の変形態様の場合、指定受付部 302 は、ポリシ修正部 202 により修正されたプライバシーポリシを自動的に適用する個人情報取得装置 20 の指定をユーザから受け付けてもよく、ポリシ登録部 118 は、ポリシ修正部 202 により修正されたプライバシーポリシを、指定受付部 302 が受け付けた指定に従い、指定された個人情報取得装置 20 のプライバシーポリシとして自動的に適用することができる。

[0092] なお、本実施形態では、図 6 の実施形態の個人情報提供装置 200 の構成に、指定受付部 302 などを追加する構成としたが、これに限定されない。図 2 または図 4 の個人情報提供装置の構成に指定受付部 302 などを追加する構成としてもよい。すなわち、個人情報提供装置において、新規登録されたプライバシーポリシの登録内容を反映させる個人情報取得装置 20 を指定することもできる。

[0093] 本実施形態において、個人情報提供装置 300 の CPU が、コンピュータプログラムを実行することにより、上記ユニット 108 ~ 118、202、302 の各機能を実現することができる。本実施形態のコンピュータプログラムは、コンピュータに、上記実施形態の個人情報提供装置 150 のコンピュータプログラムの手順（図 5 におけるステップ S11 ~ S25）に加え、修正されて仮登録されたプライバシーポリシの適用を承認する個人情報取得装

置 20 の指定をユーザから受け付ける指定受付手順（図示せず）をさらに実行させ、ポリシー登録手順（図示せず）において、ユーザの指定に基づき、適用を承認された個人情報取得装置 20 の承認済みプライバシーポリシーとして、修正されて仮登録されたプライバシーポリシーをポリシー記憶部 102 に記憶し、その識別情報をポリシー管理テーブル記憶部 106 に記録する手順（図示せず）をさらに実行させるように記述されている。

[0094] 上述のような構成において、本実施の形態の個人情報提供装置 300 のデータ処理方法を以下に説明する。

本実施形態の個人情報提供装置 300 のデータ処理方法は、修正されて仮登録されたプライバシーポリシーの適用を承認する個人情報取得装置 20 の指定をユーザから受け付け、ユーザの指定に基づき、適用を承認された個人情報取得装置 20 の承認済みプライバシーポリシーとして、修正されて仮登録されたプライバシーポリシーをポリシー記憶部 102 に記憶し、その識別情報をポリシー管理テーブル記憶部 106 に記録する。

[0095] 以上、説明したように、本実施形態の個人情報提供装置 300 によれば、既にプライバシーポリシーが登録されている個人情報取得装置 20 を含む他の個人情報取得装置 20 の中から修正または設定を反映させる個人情報取得装置 20 をユーザが指定することができ、指定に従って、ポリシー修正部 202 で修正または設定されたプライバシーポリシーを指定された他の個人情報取得装置 20 のプライバシーポリシーにも反映させ、登録することができる。

[0096] すなわち、個人情報を提供する個人情報提供装置 300 は、ユーザの個人情報を保護するために、個人情報取得装置 20 ごとに個人情報へのアクセス可否を判断する必要がある、個人情報取得装置 20 に依存しない単一プライバシーポリシーによるアクセス可否ができないため、個人情報を個人情報取得装置 20 ごとにポリシーを設定する必要がある、個人情報取得装置 20 が多ければ多いほどポリシーの設定が増え、個人情報の送付先の個人情報取得装置 20 に応じてユーザ自身の同意に基づいたポリシーを設定することは非効率であった。したがって、当該個人情報提供装置 300 が他の装置（個人情報取得装

置 20) に対して設定しているアクセス可否判断に関するポリシー（プライバシーポリシー）をシステムが自律的に変更し、変更結果を新たなポリシーとして保存するとユーザの同意を得ているか否か判断することが求められていた。

[0097] 本実施形態の個人情報提供装置 300 では、ユーザがプライバシーポリシーを新たに設定したり、変更した際には、その変更内容を他のプライバシーポリシーに伝播することができるため、全てのプライバシーポリシーをユーザが全て設定する必要がなくなり、プライバシーポリシーを登録するユーザ操作の手間を省くことができる。

[0098] また、指定された個人情報取得装置 20 向けに設定されたプライバシーポリシーは、仮登録として保留しておいてもよい。すなわち、別途、後から実際に個人情報取得装置 20 に個人情報を提供することになった時点で、個別に、あるいは、部分的に、または全体的に承認手続きを行い、登録することもできる。

[0099] （第 5 の実施の形態）

図 9 は、本実施形態の個人情報提供装置 400 の構成を示す機能ブロック図である。本実施形態の個人情報提供装置 400 は、上記実施形態の個人情報提供装置 300 とは、個人情報取得装置 20 から個人情報の要求を受け付け、該当するプライバシーポリシーを取得し、要求した個人情報のアクセス可否を判断し、プライバシーポリシーが存在しない場合は、アクセスを禁止する点で相違する。

[0100] 本実施形態の個人情報提供装置 400 は、個人情報取得装置 20 からユーザの個人情報の要求を受け付け、検索部 110 に個人情報取得装置 20 およびユーザに該当するプライバシーポリシーの識別情報を検索させる要求受付部 402 と、検索部 110 により検索されたプライバシーポリシーの識別情報に基づき、ポリシー記憶部 102 からプライバシーポリシーを取得する取得部 404 と、取得したプライバシーポリシーに従って、要求に応じられるか否かを判断する判断部 406 と、要求に応じられると判断した場合に、要求した個人情報取得装置 20 に、個人情報を記憶する個人情報記憶装置 90 から取得した個人情報

報を提供する提供部４０８とをさらに備える。図９では、個人情報記憶装置９０は個人情報提供装置４００に含まれる構成として記載されているが、他の上記実施形態と同様に個人情報提供装置４００に接続された構成であってもよく、特に限定されない。

[0101] 詳細には、個人情報提供装置４００は、上記実施形態の構成に加え、要求受付部４０２と、取得部４０４と、判断部４０６と、提供部４０８とを備える。

なお、本実施形態では、図８の実施形態の個人情報提供装置３００の構成に、要求受付部４０２などを追加する構成としたが、これに限定されない。図２、図４、図６の個人情報提供装置１００、個人情報提供装置１５０、個人情報提供装置２００の構成に要求受付部４０２などを追加する構成としてもよい。

[0102] 要求受付部４０２は、個人情報取得装置２０ａ～２０ｎのいずれかの装置からユーザの個人情報の要求を受け付け、検索部１１０に個人情報取得装置２０およびユーザに該当するプライバシーポリシーの識別情報を検索させる。取得部４０４は、検索部１１０により検索されたプライバシーポリシーの識別情報に基づき、ポリシー記憶部１０２からプライバシーポリシーを取得する。この取得したプライバシーポリシーにより、個人情報取得装置２０のアクセス可否が判断されることとなる。

[0103] 判断部４０６は、取得したプライバシーポリシーに従って、要求に応じられるか否か、すなわち、個人情報へのアクセス可否を判断する。提供部４０８は、要求に応じられると判断した場合に、要求した個人情報取得装置２０に、個人情報を記憶する個人情報記憶装置９０から取得した個人情報を提供する。本実施形態では、個人情報を含む応答メッセージを作成し、作成されたメッセージを、個人情報取得装置２０ａ～２０ｎのうち情報を要求したいいずれかの装置へネットワーク３０を介して送信する。

[0104] 一方、判断部４０６で個人情報記憶装置９０の個人情報へのアクセスが認められなかった個人情報取得装置２０に対しては、提供部４０８は、エラー

を通知するメッセージを作成し、作成されたメッセージを、個人情報取得装置 20a ~ 20n のうち情報を要求したいいずれかの装置へネットワーク 30 を介して送信する。

[0105] 本実施形態において、個人情報提供装置 400 の CPU が、コンピュータプログラムを実行することにより、上記ユニット 402 ~ 408 の各機能を実現することができる。

図 10 は、本実施形態の個人情報交換システム 1000 の個人情報取得装置 20 と個人情報提供装置 400 の動作の一例を示すフローチャートである。以下、図 9 および図 10 を用いて説明する。

[0106] 本実施形態のコンピュータプログラムは、コンピュータに、個人情報取得装置 20 からユーザの個人情報の要求を受け付け、個人情報取得装置 20 およびユーザに該当するプライバシーポリシーの識別情報を検索させる要求受付手順（ステップ S201）、検索されたプライバシーポリシーの識別情報に基づき、ポリシー記憶部 102 からプライバシーポリシーを取得する取得手順（ステップ S203）、取得したプライバシーポリシーに従って、要求に応じられるか否かを判断する判断手順（ステップ S205）、要求に応じられると判断した場合に（ステップ S205 の YES）、要求した個人情報取得装置 20 に、個人情報を記憶する個人情報記憶装置 90 から取得した個人情報を提供する提供手順（ステップ S207、S209、S213）、をさらに実行させるように記述されている。

[0107] また、上述のような構成において、本実施の形態の個人情報提供装置 400 のデータ処理方法を以下に説明する。以下、図 9 および図 10 を用いて説明する。

[0108] 本実施形態の個人情報提供装置 400 のデータ処理方法は、個人情報取得装置 20 からユーザの個人情報の要求を受け付け（ステップ S201）、要求を受け付けた個人情報取得装置 20 およびユーザに該当するプライバシーポリシーの識別情報を検索し（ステップ S203）、検索されたプライバシーポリシーの識別情報に基づき、ポリシー記憶装置からプライバシーポリシーを取得し（ス

ステップS203)、取得したプライバシーポリシーに従って、要求に応じられるか否かを判断し(ステップS205)、要求に応じられると判断した場合に、要求した個人情報取得装置20に、個人情報を記憶する個人情報記憶装置90から取得した個人情報を提供する(ステップS207、S209、S213)。

[0109] このように構成された本実施形態の個人情報交換システムの動作について、以下に説明する。以下、図9～図11を用いて説明する。

まず、図10を用いて装置間で行われる処理の流れを説明する。個人情報取得装置20a～20nのいずれか(以下、個人情報取得装置20xとする)が個人情報提供装置400に対して個人情報を要求するメッセージをネットワーク30を介して送付する(ステップS101)。そして、個人情報提供装置400が要求メッセージをネットワーク30を介して受信し(ステップS201)、要求メッセージに対する応答メッセージを個人情報取得装置20xに送付することで応答する。ただし、この処理は、個人情報提供装置400が以前に行っていた処理の内容によって異なる。

[0110] そして、個人情報提供装置400において、要求受付部402で受信した要求に呼応して、検索部110による要求された個人情報のプライバシーポリシーの検索処理に移行する(ステップS203)。このステップS203プライバシーポリシー検索処理の詳細については、後述する。

[0111] そして、ステップS203の検索処理では、検索部110からプライバシーポリシーの記憶場所が出力され、取得部404により記憶場所に基づき取得部404によりポリシー記憶部102から取得されたプライバシーポリシーが出力される。そして、判断部406により、得られたプライバシーポリシーの内容に基づき、個人情報へのアクセスの可否が判断される(ステップS205)。

[0112] ステップS205における可否判断において、個人情報へのアクセスが認められた場合には(ステップS205のYES)、提供部408は、個人情報記憶装置90から必要な個人情報を取得する(ステップS207)。そして、提供部408により、個人情報取得装置20xに個人情報を返信するた

めの返信メッセージが作成される（ステップS 2 0 9）。

[0113] 一方、ステップS 2 0 5における可否判断の結果、個人情報の送付が認められない場合には（ステップS 2 0 5のNO）、提供部4 0 8により、個人情報取得装置2 0 xに対して返信するエラーメッセージが作成される（ステップS 2 1 1）。そして、提供部4 0 8により、ステップS 2 0 9またはS 2 1 1で作成された返信メッセージが個人情報取得装置2 0 xにネットワーク3 0を介して送信される（ステップS 2 1 3）。個人情報取得装置2 0 xは、個人情報提供装置4 0 0から返信メッセージをネットワーク3 0を介して受信する（ステップS 1 0 3）。

[0114] 次に、ステップS 2 0 3のプライバシーポリシー検索処理の詳細について、図1 1および図9を用いて説明する。本処理は、個人情報取得装置2 0 xがユーザの個人情報へアクセスできるか否かを判定するために使用するプライバシーポリシーを、検索部1 1 0が取得する処理である。

[0115] まず、個人情報提供装置4 0 0において、検索部1 1 0により、ポリシー管理テーブル記憶部1 0 6に保持されている情報が取得される（ステップS 3 0 1）。この情報は、プライバシーポリシーがどこで管理されているか、という情報を含む。次に、検索部1 1 0は、ポリシーが保管されている状況に応じて、次に行う処理を決定する（ステップS 3 0 3）。

[0116] すなわち、プライバシーポリシーが、ポリシー記憶部1 0 2にのみ登録されていると判断した場合（ステップS 3 0 3のポリシー記憶部にあり）、検索部1 1 0は、取得したプライバシーポリシーの記憶場所に基づき、ポリシー記憶部1 0 2からプライバシーポリシーを取得し、提供部4 0 8に提示し（ステップS 3 3 1）、本処理を終了する。

[0117] また、要求メッセージを送付した個人情報取得装置2 0 x向けのプライバシーポリシーが存在しないと判断した場合（ステップS 3 0 3のポリシーなし）、ポリシー作成部1 1 2により、個人情報取得装置2 0 xにユーザの個人情報を提示するための新規のプライバシーポリシーが作成される（ステップS 3 1 1）。作成されたプライバシーポリシーは、ポリシー仮登録部1 1 4によりポリシー時

記憶部 104 に仮登録される（ステップ S 313）。

[0118] そして、指示受付部 116 が、ステップ S 311 で作成された個人情報へのアクセスに関するプライバシーポリシーを、個人情報の主体者であるユーザに対して提示し、このプライバシーポリシーでよいかをユーザに問い合わせる（ステップ S 315）。新規プライバシーポリシーにユーザが同意しない場合には（ステップ S 315 の NO）、ユーザにプライバシーポリシーを規定させることとなる。指示受付部 116 は、ユーザにプライバシーポリシーを修正して再設定するか否かを確認し（ステップ S 371）、ユーザが修正を選択した場合（ステップ S 371 の YES）、ユーザによるプライバシーポリシーの修正処理に移行する（ステップ S 391）。この修正処理は、図 7 に示した上記実施形態の個人情報提供装置 200 のポリシー修正処理で説明した処理と同様であり、詳細な説明は省略する。

[0119] 一方、修正を選択しなかった場合（ステップ S 371 の NO）、指示受付部 116 は、ポリシー仮登録部 114 に、ポリシー時記憶部 104 に仮登録されていたプライバシーポリシーを削除させる（ステップ S 373）。そして、ポリシー仮登録部 114 からポリシー管理部 108 に、プライバシーポリシーがないことが通知され、ポリシー管理テーブル記憶部 106 に記録され（ステップ S 375）、本処理を終了する。これにより、ポリシー管理部 108 に要求エンティティに対するプライバシーポリシーが存在しないことが通知され（ステップ S 377）、アクセス可否判断に利用させることとなる。

[0120] なお、本実施形態では、修正を選択しなかった場合に、仮登録されたプライバシーポリシーをポリシー時記憶部 104 から削除する場合について説明しているが、これに限定されない。ユーザに仮登録されたプライバシーポリシーを削除せず、そのまま仮登録のまま処理を終了してもよい。この場合、一旦、プライバシーポリシーの同意を保留しておき、次の機会に、上記ステップ S 303 からステップ S 351 に移行することで、ユーザに仮登録されたプライバシーポリシーに同意するかどうかを確認できる。

[0121] 一方、ステップ S 315 で、個人情報取得装置 20x に関する新規プライ

バシポリシーにユーザが同意した場合（ステップS 3 1 5のYES）、この個人情報取得装置20xに関する新規プライバシーポリシーを反映させる他の個人情報取得装置20（ここで、個人情報取得装置20yとする。個人情報取得装置20yとしては複数の装置が指定できる）の指定を指定受付部302が受け付ける。そして、ポリシー登録部118により、ポリシー時記憶部104に仮登録されていたプライバシーポリシーが指定された個人情報取得装置20x、20yに対するプライバシーポリシーとして、ポリシー記憶部102に登録される（ステップS 3 1 7）。このとき、ポリシー時記憶部104に仮登録されていたプライバシーポリシーは削除される。

[0122] このようにして、ユーザはステップS 3 1 5の一度の操作処理によって、個人情報取得装置20xだけでなく、他の個人情報取得装置20yのポリシーにも新規ポリシーの設定を反映できることとなる。この同意のステップS 3 1 5では、一部のプライバシーポリシーのみ同意し、残りは保留として、次の機会に、上記ステップS 3 0 3からステップS 3 5 1に移行することで、ユーザに仮登録されたプライバシーポリシーに同意するかどうかを確認できる。

[0123] そして、ポリシー登録部118からポリシー管理部108に、プライバシーポリシーを記憶した場所の情報を通知して、ポリシー管理テーブル記憶部106に登録される（ステップS 3 1 9）。これにより、ポリシー管理部108に要求エンティティに対するポリシーが存在することが通知され（ステップS 3 2 1）、アクセス可否判断に利用されることとなる。

[0124] また、ステップS 3 0 3の判定において、受信した要求メッセージを送付元の個人情報取得装置20x向けプライバシーポリシーがポリシー時記憶部104にて保管されていると判断した場合（ステップS 3 0 3のポリシー時記憶部にあり）、検索部110は、取得したプライバシーポリシーの記憶場所に基づき、ポリシー時記憶部104から当該プライバシーポリシーを取得する（ステップS 3 5 1）。

[0125] そして、指示受付部116により、プライバシーポリシーがユーザのユーザ端末装置50に提示され、このプライバシーポリシーを個人情報へのアクセス可否

に用いることに同意するか否かをユーザに問い合わせる（ステップS 3 5 3）。

[0126] ユーザが同意した場合（ステップS 3 5 3のYES）、この個人情報取得装置20xに関するプライバシーポリシーを反映させる他の個人情報取得装置20yの指定を指定受付部302が受け付ける。そして、ポリシー登録部118により、ポリシー時記憶部104に仮登録されていたプライバシーポリシーが指定された個人情報取得装置20x、20yに対するプライバシーポリシーとして、ポリシー記憶部102に登録される（ステップS 3 5 5）。このとき、ポリシー時記憶部104に仮登録されていたプライバシーポリシーは削除される。

このようにして、ユーザはステップS 3 5 3の一度の操作処理によって、個人情報取得装置20xだけでなく、他の個人情報取得装置20yのポリシーにもプライバシーポリシーの設定を反映できることとなる。

[0127] そして、ポリシー登録部118からポリシー管理部108に、プライバシーポリシーを記憶した場所の情報を通知して、ポリシー管理テーブル記憶部106に登録される（ステップS 3 5 7）。これにより、ポリシー管理部108に要求エンティティに対するポリシーが存在することが通知され、アクセス可否判断に利用させることとなる。そして、個人情報取得装置20x、20y向けのプライバシーポリシーが存在することが通知され（ステップS 3 5 9）、アクセス可否判断に利用されることとなる。

[0128] 一方、ステップS 3 5 3の判定で、ユーザが同意しない場合（ステップS 3 5 3のNO）、ユーザにプライバシーポリシーを規定させることとなる。この後の処理は、上述したステップS 3 7 1以降の処理と同様になるので、詳細な説明は省略する。

[0129] 以上、説明したように、本実施形態の個人情報提供装置400によれば、ユーザが自身で設定したプライバシーポリシーを当該ユーザに関する他のプライバシーポリシーにも反映させることができ、ユーザはプライバシーポリシーの設定や変更の回数を減らすことができる。

[0130] また、本実施形態の個人情報提供装置400によれば、さらに、変更した

プライバシーポリシーをすぐに更新するのではなく、ユーザの確認が取れた場合にのみポリシー記憶部 102 に登録するというように構成されているため、ユーザの意図に反した個人情報の開示を防ぐことができる。また、複数の装置のうち、現時点で必要なプライバシーポリシーのみ承認し、他は保留とすることもでき、必要なときに必要なものについてのみ確認をすることが可能となる。

[0131] (第 6 の実施の形態)

図 12 は、本発明の実施の形態の個人情報交換システム 1100 の構成を示すプログラム図である。本実施形態の個人情報交換システム 1100 は、上記実施形態の個人情報交換システム 1000 とは、上記実施形態の個人情報提供装置 400 の構成に、さらに、個人情報取得装置 20 の機能を追加した個人情報取得および提供装置 500 を含む点で相違する。

[0132] 図 13 は、本実施形態の個人情報交換システム 1100 の個人情報取得および提供装置 500 の構成を示す機能ブロック図である。なお、本図において、図 9 の個人情報提供装置 400 と同様な構成はすべて省略してある。また、図 12 および図 13 では、個人情報取得および提供装置 500 に接続される個人情報記憶装置 92 は、個人情報提供装置 400 の個人情報記憶装置 90 と異なる構成としているが、これに限定されない。個人情報提供装置 400 と同じ個人情報記憶装置 90 の情報を提供する構成としてもよい。また、本実施形態の個人情報記憶装置 92 は、個人情報取得および提供装置 500 に接続された外部の記憶装置として構成されているが、これに限定されず、たとえば、個人情報取得および提供装置 500 に含まれる記憶装置であってもよい。

[0133] 本実施形態の個人情報取得および提供装置 500 は、上記実施形態の個人情報提供装置 400 の構成に加え、他の個人情報取得装置 20 に、ユーザの個人情報を要求する要求部（個人情報要求生成部 502 および要求送信部 504）と、他の個人情報提供装置から、ユーザの個人情報を受け取る受取部（個人情報受信部 506）とをさらに備える。具体的には、本実施形態の個

個人情報取得および提供装置 500 は、個人情報要求生成部 502 と、要求送信部 504 と、個人情報受信部 506 とを備える。

[0134] 個人情報要求生成部 502 は、個人情報提供装置 400 に対して送付する個人情報の要求メッセージを作成する。要求送信部 504 は、個人情報要求生成部 502 が生成したメッセージを個人情報提供装置 400 にネットワーク 30 を介して送信する。個人情報受信部 506 は、個人情報提供装置 400 より個人情報をネットワーク 30 を介して受信し、個人情報記憶装置 92 に登録する。

[0135] 本実施形態において、個人情報取得および提供装置 500 の CPU が、コンピュータプログラムを実行することにより、上記ユニット 502 ~ 506 の各機能を実現することができる。

[0136] 図 14 は、本実施形態の個人情報交換システム 1100 の動作の一例を示すフローチャートである。本実施形態のコンピュータプログラムは、コンピュータに、個人情報提供装置 400 に、ユーザの個人情報を要求する要求手順（ステップ S1201）、個人情報提供装置 400 から、ユーザの個人情報を受け取る受取手順（ステップ S1203）、をさらに実行させるように記述されている。

[0137] また、上述のような構成において、本実施の形態の個人情報交換システム 1100 の個人情報取得および提供装置 500 のデータ処理方法を以下に説明する。以下、図 13 および図 14 を用いて説明する。

[0138] 本実施形態の個人情報取得および提供装置 500 のデータ処理方法は、個人情報提供装置 400 に、ユーザの個人情報を要求し（ステップ S1201）、個人情報提供装置 400 から、ユーザの個人情報を受け取る（ステップ S1203）。

[0139] このように構成された本実施形態の個人情報取得および提供装置 500 の動作について以下に説明する。以下、図 13 および図 14 を用いて説明する。

まず、個人情報取得および提供装置 500 の個人情報要求生成部 502 が

個人情報を要求するメッセージを作成し、要求送信部 504 が個人情報提供装置 400 に送付する（ステップ S 1201）。そして、個人情報提供装置 400 において、要求受付部 402（図 9 参照）が要求を受信し（ステップ S 1401）、検索部 110（図 9 参照）によりプライバシーポリシーによる送付可否判定ののち、提供部 408（図 9 参照）がメッセージに基づき個人情報を個人情報取得および提供装置 500 に送付する（ステップ S 1403）。個人情報提供装置 400 における個人情報の検索などの処理の詳細については、上記実施形態で説明したので省略する。個人情報提供装置 400 での送信処理が、個人情報取得装置 20 となっていたが、個人情報取得および提供装置 500 に変わった点のみ相違する。

[0140] そして、個人情報取得および提供装置 500 において、個人情報受信部 506 が個人情報提供装置 400 から個人情報をネットワーク 30 を介して受信し（ステップ S 1203）、個人情報記憶装置 92 に記憶する（ステップ S 1205）。その後、個人情報取得装置 20x が必要に応じて、個人情報取得および提供装置 500 に個人情報の要求を送信する（ステップ S 1101）。

[0141] 個人情報取得および提供装置 500 では、個人情報取得装置 20x からの要求に応じて（ステップ S 1207）、個人情報を準備し、上記実施形態の個人情報提供装置 400 で説明したように、図 9 の提供部 408 がネットワーク 30 を介して個人情報取得装置 20x に個人情報を送信する（ステップ S 1209）。この個人情報の送信処理は、上記実施形態の個人情報提供装置 400 と同様であるので、ここでは詳細な説明は省略する。個人情報取得装置 20x は、個人情報取得および提供装置 500 から個人情報を受信する（ステップ S 1103）。あるいは、個人情報提供装置 400 で説明した処理と同様に、個人情報取得および提供装置 500 における個人情報へのアクセス可否判定において、個人情報の提供が不可と判定された場合には、その旨を個人情報取得装置 20x に通知するメッセージを送信する。

[0142] 以上、説明したように、本実施形態の個人情報交換システム 1100 によ

れば、個人情報を取得した装置が個人情報を提供する装置として動作するように構成されているため、ユーザが個人情報をそれぞれの装置に登録する手間を省くことができ、ユーザ処理を簡略化できる。また、個人情報提供装置が集中的に個人情報を管理する必要がなくなるため、個人情報が複数の装置が管理している分散環境に適用することができる。

[0143] 以上、図面を参照して本発明の実施形態について述べたが、これらは本発明の例示であり、上記以外の様々な構成を採用することもできる。

[0144] たとえば、上記実施形態の個人情報提供装置 100 において、ポリシー登録部 118 は、修正されたプライバシーポリシーを他の個人情報取得装置 20 のプライバシーポリシーとして自動的に適用し、他の個人情報取得装置 20 のプライバシーポリシーとして修正されたプライバシーポリシーをポリシー記憶部 102 に記憶し、その識別情報をポリシー管理部 108 に通知してポリシー管理テーブル記憶部 106 に記録させることもできる。

[0145] この構成によれば、修正されたプライバシーポリシーを自動的に他の個人情報取得装置 20 のプライバシーポリシーにも適用できることとなる。

実施例

[0146] (実施例 1)

以下、本発明の個人情報交換システムの実施例を図 15～図 18 を用いて説明する。なお、本実施形態では、上記実施形態の個人情報交換システム 1000 の個人情報提供装置 400 の実施例として説明するものであり、図 1、図 9 も用いて説明する。

[0147] 図 15 に示すように、インターネット上でユーザ情報を管理し、他の装置に提供する情報提供装置 400 として振舞うインターネットサービスプロバイダ (ISP) 606 と、個人情報取得装置 20 (図 1 参照) として振舞う旅行ポータルサイト 602 と、個人情報取得装置 20 として振舞うレンタカーサイト 604 と、ネットワーク 30 (図 1 参照) を介してサービスを受領するユーザ端末装置 600 (図 1 に示すユーザ端末装置 50 に相当) から構成される。本実施例では、ユーザはユーザ端末装置 600 を介して旅行ポー

タルサイト602とレンタカーサイト604が提供するサービスを利用する。そのサービスを利用する際に、ISP606が保有する個人情報を利用する。

[0148] 例えば、旅行ポータルサイト602やレンタカーサイト604はISP606が保有する個人情報を利用してユーザの連絡先である住所や電話番号を取得する。本実施例では、ISP606はレンタカーサイト604に対するプライバシーポリシーをあらかじめ保有しているが、旅行ポータルサイト602にはプライバシーポリシーを設定していないものとする。この状況で、旅行ポータルサイト602とレンタカーサイト604は個人情報を取得する。

[0149] まず、ユーザ（ユーザID：0001とする）は、ユーザ端末装置600を介して旅行ポータルサイト602のサービスにアクセスし、旅行の予約手続きをする（図15におけるステップS501）。このときに、旅行ポータルサイト602は連絡先住所情報が必要になり、この情報をISP606に要求する（ステップS503）。ISP606において、要求受付部402（図9参照）が要求を受け取ると、検索部110（図9参照）が、ポリシー管理テーブル記憶部106（図9参照）を確認する。

[0150] このとき、ポリシー管理テーブル記憶部106は、例えば、図16に示すようなプライバシーポリシーをユーザ毎に管理している。図16に示すように、ISP606が旅行ポータルサイト602向けの当該ユーザ（ID：0001）に関するプライバシーポリシーを設定していない場合には、ポリシー作成部112（図9参照）により新たなプライバシーポリシーが作成され、ユーザ端末装置600を介してユーザに通知される（ステップS505）。ユーザはプライバシーポリシーの通知を受けると、それを受け入れるか、ユーザ自身でポリシーを設定するかを決定し、結果をISP606へ通知する（ステップS507）。

[0151] ここでは、ユーザは自身でプライバシーポリシーを設定したものとする。すると、ISP606のポリシー登録部118（図9参照）はユーザが設定したポリシーをポリシー記憶部102（図9参照）に登録する。さらに必要に応じて、

他の装置に対するプライバシーポリシーを、指定受付部 302（図 9 参照）により受け付けた指定に従って変更する。なお、ここでは、他の装置にも設定したプライバシーポリシーを反映される指示をユーザが行ったものとする。そして、この他の装置に対するプライバシーポリシーの変更については、ユーザによるプライバシーポリシーの同意の確認はこの時点では行われていないものとする。したがって、他の装置に関するプライバシーポリシーは、ポリシー時記憶部 104 に一時的に保管され、仮登録された状況のままとなる。ポリシー管理部 108 により、ポリシー管理テーブル記憶部 106 のプライバシーポリシーの記憶場所に関する情報が変更される（ステップ S509）。

[0152] ポリシー時記憶部 104（図 9 参照）に登録される情報は、新たなプライバシーポリシーであり、その構造は、ポリシー記憶部 102（図 9 参照）に記憶されるプライバシーポリシーと同じ構造をする。また、更新されたポリシーの状態を管理するポリシー管理テーブル記憶部 106（図 9 参照）に記憶される情報は、例えば、図 17 に示す情報であり、図 16 から更新されていることがわかる。

[0153] 次に、ISP 606 はユーザが設定したプライバシーポリシーに基づいて旅行ポータルサイト 602 からの個人情報要求に対する応答を送付するか否かを判断し、送付可能と判断した場合には個人情報を送付する（ステップ S511）。個人情報を取得した旅行ポータルサイト 602 は、サービスをユーザ端末装置 600 に提供する（ステップ S513）。

[0154] 次に、ユーザはユーザ端末装置 600 を介してレンタカーサイト 604 にアクセスする（ステップ S515）。このレンタカーサイト 604 はユーザにサービスを提供するために必要となる個人情報を ISP 606 に要求する（ステップ S517）。ISP 606 において、要求受付部 402（図 9 参照）が個人情報の要求をレンタカーサイト 604 から取得すると、検索部 110（図 9 参照）を介してプライバシーポリシーを検索する。

[0155] この段階では、図 17 に示すとおり、レンタカーサイト 604 向けのプライバシーポリシーはポリシー時記憶部 104（図 9 参照）にあるので、そのプラ

イバシポリシーを取得する。このポリシーは、上述したように、変更内容に関するユーザ確認が取れていないため、指示受付部 116（図 9 参照）によりユーザ端末装置 600 を介してユーザ同意を求める（ステップ S519）。

[0156] ここで、ユーザが同意すると、変更したプライバシーポリシーをポリシー記憶部 102（図 9 参照）に登録し、ポリシー管理テーブル記憶部 106 を図 18 のように変更する（ステップ S521）。その後、プライバシーポリシーに基づいて個人情報をレンタカーサイト 604 に送付できるか否かを判断し、送付できると判断した場合には、個人情報を送付する（ステップ S523）。レンタカーサイト 604 は個人情報を受け取ると、個人情報を利用してサービスをユーザ端末装置 600 に返す（ステップ S525）。

[0157] （実施例 2）

次に、本発明の他の実施例を、図 19～図 22 を参照して説明する。本実施例は上記実施形態の個人情報交換システム 1100 に対応するものである。以下、図 9、図 12 も用いて説明する。

[0158] 本実施例は、図 19 に示すように、インターネット上でユーザ情報を管理し他の装置に提供する個人情報提供装置 400（図 12 参照）として振舞うインターネットサービスプロバイダ（ISP）704 と、個人情報取得・提供装置 500（図 12 参照）として振舞うショッピングサイト 702 と、個人情報取得装置 20（図 12 参照）として振舞う運送業者端末装置 706 と、ネットワークを介してサービスを受領するユーザ端末装置 700（図 12 に示すユーザ端末装置 50 に相当）から構成される。

[0159] 本実施例では、ユーザはユーザ端末装置 700 を介してショッピングサイト 702 にアクセスし、ISP 704 の個人情報を利用してサイト上で買い物をし、その商品配達を運送業者端末装置 706 に依頼するという処理を示している。本実施例では、ISP 704 はショッピングサイト 702 に対するプライバシーポリシーをあらかじめ保有しており、ショッピングサイト 702 は運送業者端末装置 706 に対するプライバシーポリシーを保有していないものとする。この状況で、ショッピングサイト 702 は ISP 704 より個人情報

報を取得し、運送業者端末装置 706 はショッピングサイト 702 より個人情報取得する。

[0160] まず、ユーザ（ユーザ ID：0001 とする）はユーザ端末装置 700 を介してショッピングサイト 702 のサービスにアクセスし、商品を購入する（図 19 におけるステップ S601）。このときに、ショッピングサイト 702 は連絡先住所情報が必要になり、要求送信部 504（図 13 参照）がこの情報を ISP 704 に要求する（ステップ S603）。ISP 704 において、要求受付部 402（図 9 参照）が要求を受け取ると、検索部 110（図 9 参照）を利用して、ポリシー管理テーブル記憶部 106（図 9 参照）を確認する。このとき、ポリシー管理テーブル記憶部 106 は、例えば、図 20 に示すようなプライバシーポリシーを管理している。

[0161] 図 20 に示すとおり、ISP 704 がショッピングサイト 702 向けの当該ユーザに関するプライバシーポリシーを保有しているので、ISP 704 はユーザが設定したプライバシーポリシーに基づいてショッピングサイト 702 からの個人情報要求に対する応答を送付するか否かを判断し、送付可能と判断した場合には個人情報を送付する（ステップ S605）。ショッピングサイト 702 の個人情報受信部 506（図 13 参照）は、個人情報を取得した後、サービスをユーザ端末装置 700 に提供する（ステップ S607）。

[0162] 次に、ユーザはユーザ端末装置 700 を介して運送業者端末装置 706 にアクセスし、商品配達を依頼する（ステップ S609）。この運送業者端末装置 706 はユーザにサービスを提供するために必要となる送り先住所などの個人情報をショッピングサイト 702 に要求する（ステップ S611）。ショッピングサイト 702 において、要求受付部 402（図 9 参照）が個人情報の要求を運送業者端末装置 706 から取得すると、検索部 110（図 9 参照）を介してプライバシーポリシーを検索する。この段階では、図 21 に示すとおり、ショッピングサイト 702 のポリシー管理テーブル記憶部 106 には、ユーザ（ID：0001）の運送業者端末装置 706 向けのプライバシーポリシーが存在しないため、新たにプライバシーポリシーを作成し、ユーザに確認を

取る（ステップS 6 1 3）。

[0163] ユーザが新たなプライバシーポリシーに基づいて個人情報を提供することを同意した場合には、ショッピングサイト702において、当該ポリシーをポリシー記憶部102（図9参照）に登録し、ポリシー管理テーブル記憶部106の情報を図22に示すとおりに変更する（ステップS 6 1 5）。その後、プライバシーポリシーに基づいて個人情報を運送業者端末装置706に送付できるか否かを判断し、送付できると判断した場合には、個人情報を送付する（ステップS 6 1 7）。運送業者端末装置706が個人情報を受け取ると、ユーザ端末装置700に配送要求の受付が終了したことを通知する（ステップS 6 1 9）。

[0164] 本発明によれば、個人情報を管理する装置や個人情報を利用する装置がプライバシーポリシーを設定するためのプログラムといった用途に適用できる。また、個人情報を集中的に管理するポータルサービスにおけるプライバシーポリシーのプロビジョニングといった用途にも適用可能である。

[0165] 以上、実施形態および実施例を参照して本願発明を説明したが、本願発明は上記実施形態および実施例に限定されるものではない。本願発明の構成や詳細には、本願発明の範囲内で当業者が理解し得る様々な変更をすることができる。

[0166] この出願は、2008年12月8日に提出された日本特許出願2008-311966を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

[0167] 1000 個人情報交換システム
20 個人情報取得装置
30 ネットワーク
50 ユーザ端末装置
90 個人情報記憶装置
100 個人情報提供装置

- 1 0 2 ポリシ記憶部
- 1 0 4 ポリシー時記憶部
- 1 0 6 ポリシ管理テーブル記憶部
- 1 0 8 ポリシ管理部
- 1 1 0 検索部
- 1 1 2 ポリシ作成部
- 1 1 4 ポリシ仮登録部
- 1 1 6 指示受付部
- 1 1 8 ポリシ登録部
- 1 5 0 個人情報提供装置
- 2 0 0 個人情報提供装置
- 2 0 2 ポリシ修正部
- 3 0 0 個人情報提供装置
- 3 0 2 指定受付部
- 4 0 0 個人情報提供装置
- 4 0 2 要求受付部
- 4 0 4 取得部
- 4 0 6 判断部
- 4 0 8 提供部
- 1 1 0 0 個人情報交換システム
- 5 0 0 個人情報取得および提供装置
- 9 2 個人情報記憶装置
- 5 0 2 個人情報要求生成部
- 5 0 4 要求送信部
- 5 0 6 個人情報受信部
- 6 0 0 ユーザ端末装置
- 6 0 2 旅行ポータルサイト
- 6 0 4 レンタカーサイト

- 700 ユーザ端末装置
- 702 ショッピングサイト
- 706 運送業者端末装置

請求の範囲

- [請求項1] ユーザの個人情報を取得する個人情報取得装置毎かつ前記ユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶装置と、
前記ポリシー記憶装置に前記プライバシーポリシーが記憶されているかを識別する識別情報を、前記個人情報取得装置毎かつ前記ユーザ毎にポリシー管理テーブルに記録して管理するポリシー管理手段と、
前記ポリシー管理テーブルを参照し、前記個人情報取得装置および前記ユーザに該当するプライバシーポリシーの前記識別情報を検索する検索手段と、
該当する前記プライバシーポリシーの前記識別情報が見つからなかったとき、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成するポリシー作成手段と、
作成された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理手段に通知して前記ポリシー管理テーブルに記録させるポリシー登録手段とを備える個人情報提供装置。
- [請求項2] 前記ポリシー作成手段は、前記デフォルトのプライバシーポリシーとして、前記ポリシー記憶装置に記憶されている前記プライバシーポリシーに基づいて、前記プライバシーポリシーを自動的に作成する
請求項1に記載の個人情報提供装置。
- [請求項3] 前記ポリシー記憶装置に記憶されている前記プライバシーポリシーの修正指示を前記ユーザから受け付け、受け付けた前記修正指示に基づいて、前記プライバシーポリシーを修正するポリシー修正手段をさらに備え、
前記ポリシー登録手段は、修正された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理手段に通知して前記ポリシー管理テーブルに記録させる
請求項1または請求項2に記載の個人情報提供装置。
- [請求項4] 前記ポリシー登録手段は、修正された前記プライバシーポリシーを他の個人情報取得装置の前記プライバシーポリシーとして自動的に適用し、前記

他の個人情報取得装置のプライバシーポリシーとして修正された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理手段に通知して前記ポリシー管理テーブルに記録させる

請求項 3 に記載の個人情報提供装置。

[請求項5] 修正された前記プライバシーポリシーを自動的に適用する個人情報取得装置の指定を前記ユーザから受け付ける指定受付手段をさらに備え、

前記ポリシー登録手段は、修正された前記プライバシーポリシーを前記指定受付手段が受け付けた前記指定に従い、指定された前記個人情報取得装置の前記プライバシーポリシーとして自動的に適用する

請求項 4 に記載の個人情報提供装置。

[請求項6] 前記ユーザが未承認のプライバシーポリシーを一時的に記憶するポリシー一時記憶装置と、

前記ポリシー作成手段により作成された前記プライバシーポリシーを前記未承認のプライバシーポリシーとして前記ポリシー一時記憶装置に一時的に記憶し、その識別情報を前記ポリシー管理手段に通知して前記ポリシー管理テーブルに記録させるポリシー仮登録手段と、

前記ポリシー一時記憶装置に仮登録された前記未承認のプライバシーポリシーを前記ユーザに提示し、前記プライバシーポリシーの適用の認否を確認し、指示を前記ユーザから受け付ける指示受付手段とをさらに備え、

前記ポリシー登録手段は、前記ポリシー一時記憶装置に仮登録された前記未承認のプライバシーポリシーが前記ユーザにより承認されたとき、承認済みプライバシーポリシーとして前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理手段に通知して前記ポリシー管理テーブルに記録させる

請求項 1 から請求項 5 のうちのいずれか 1 項に記載の個人情報提供装置。

[請求項7] 前記ポリシー管理手段が、前記個人情報取得装置毎かつ前記ユーザ毎

に前記ポリシー管理テーブルに記録して管理する前記識別情報は、前記ポリシー記憶装置または前記ポリシー時記憶装置のいずれに前記プライバシーポリシーが記憶されているかを識別する情報を含み、

前記指示受付手段は、検索された前記識別情報に基づいて、該当する前記プライバシーポリシーが前記ポリシー時記憶装置に記憶されていることを判定し、前記ポリシー時記憶装置に仮登録された前記未承認のプライバシーポリシーを前記ユーザに提示し、前記プライバシーポリシーの適用の認否を確認し、指示を前記ユーザから受け付ける

請求項 6 に記載の個人情報提供装置。

[請求項 8]

前記指示受付手段が受け付けた前記指示で前記ユーザにより否認された前記プライバシーポリシーの修正指示を前記ユーザから受け付け、受け付けた前記修正指示に基づいて、前記プライバシーポリシーを修正するポリシー修正手段をさらに備え、

前記ポリシー仮登録手段は、修正された前記プライバシーポリシーを前記ポリシー時記憶装置に一時的に記憶し、その識別情報を前記ポリシー管理手段に通知して前記ポリシー管理テーブルに記録させる

請求項 7 に記載の個人情報提供装置。

[請求項 9]

修正されて仮登録された前記プライバシーポリシーの適用を承認する個人情報取得装置の指定を前記ユーザから受け付ける指定受付手段をさらに備え、

前記ポリシー登録手段は、前記ユーザの前記指定に基づき、適用を承認された前記個人情報取得装置の前記承認済みプライバシーポリシーとして、前記修正されて仮登録された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理手段に通知して前記ポリシー管理テーブルに記録させる

請求項 8 に記載の個人情報提供装置。

[請求項 10]

前記個人情報取得装置からユーザの個人情報の要求を受け付け、前記検索手段に前記個人情報取得装置および前記ユーザに該当するプラ

イバシポリシの前記識別情報を検索させる要求受付手段と、

前記検索手段により検索された前記プライバシーポリシの識別情報に基づき、前記ポリシ記憶装置から前記プライバシーポリシを取得する取得手段と、

取得した前記プライバシーポリシに従って、前記要求に応じられるか否かを判断する判断手段と、

前記要求に応じられると判断した場合に、前記要求した前記個人情報取得装置に、個人情報を記憶する個人情報記憶装置から取得した前記個人情報を提供する提供手段とをさらに備える

請求項 1 から請求項 9 のうちのいずれかに 1 項に記載の個人情報提供装置。

[請求項11] 他の個人情報提供装置に、ユーザの個人情報を要求する要求手段と、

前記他の個人情報提供装置から、前記ユーザの個人情報を受け取る受取手段とをさらに備える

請求項 1 から請求項 10 のうちのいずれか 1 項に記載の個人情報提供装置。

[請求項12] 個人情報を記憶する個人情報記憶装置と、

請求項 1 から請求項 11 のうちのいずれか 1 項に記載の個人情報提供装置と、

ユーザの個人情報を前記個人情報提供装置に要求して取得する個人情報取得装置と、

前記ユーザのユーザ端末装置とを備え、

前記個人情報提供装置は、前記個人情報取得装置からの前記個人情報の前記要求に応じて、前記ユーザ端末装置の前記ユーザに前記個人情報のプライバシーポリシの適用の認否を確認し、前記ユーザからの指示を前記ユーザ端末装置から受け付け、承認された前記プライバシーポリシに従って、前記個人情報記憶装置から取得した前記ユーザの前記

個人情報をも前記個人情報取得装置に提供する
個人情報交換システム。

[請求項13] ユーザの個人情報を取得する個人情報取得装置毎かつ前記ユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶装置を備えた個人情報提供装置のデータ処理方法であって、

前記ポリシー記憶装置に前記プライバシーポリシーが記憶されているかを識別する識別情報を、前記個人情報取得装置毎かつ前記ユーザ毎にポリシー管理テーブルに記録して管理し、

前記ポリシー管理テーブルを参照し、前記個人情報取得装置および前記ユーザに該当するプライバシーポリシーの前記識別情報を検索し、

該当する前記プライバシーポリシーの前記識別情報が見つからなかったとき、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成し、

作成された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理テーブルに記録する

個人情報提供装置のデータ処理方法。

[請求項14] 前記デフォルトのプライバシーポリシーとして、前記ポリシー記憶装置に記憶されている前記プライバシーポリシーに基づいて、前記プライバシーポリシーを自動的に作成する

請求項13に記載の個人情報提供装置のデータ処理方法。

[請求項15] 前記ポリシー記憶装置に記憶されている前記プライバシーポリシーの修正指示を前記ユーザから受け付け、受け付けた前記修正指示に基づいて、前記プライバシーポリシーを修正し、

修正された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理テーブルに記録する

請求項13または請求項14に記載の個人情報提供装置のデータ処理方法。

[請求項16] 修正された前記プライバシーポリシーを他の個人情報取得装置の前記プ

ライバシポリシとして自動的に適用し、前記他の個人情報取得装置のプライバシポリシとして修正された前記プライバシポリシを前記ポリシ記憶装置に記憶し、その識別情報を前記ポリシ管理テーブルに記録する

請求項 1 5 に記載の個人情報提供装置のデータ処理方法。

[請求項17] 修正された前記プライバシポリシを自動的に適用する個人情報取得装置の指定を前記ユーザから受け付け、

修正された前記プライバシポリシを、受け付けた前記指定に従い、指定された前記個人情報提供装置の前記プライバシポリシとして自動的に適用する

請求項 1 6 に記載の個人情報提供装置のデータ処理方法。

[請求項18] 前記ユーザが未承認のプライバシポリシを一時的に記憶するポリシ一時記憶装置をさらに備えた個人情報提供装置のデータ処理方法であって、

作成された前記プライバシポリシを前記未承認のプライバシポリシとして前記ポリシ一時記憶装置に一時的に記憶し、その識別情報を前記ポリシ管理テーブルに記録し、

前記ポリシ一時記憶装置に仮登録された前記未承認のプライバシポリシを前記ユーザに提示し、前記プライバシポリシの適用の認否を確認し、指示を前記ユーザから受け付け、

前記ポリシ一時記憶装置に仮登録された前記未承認のプライバシポリシが前記ユーザにより承認されたとき、承認済みプライバシポリシとして前記ポリシ記憶装置に記憶し、その識別情報を前記ポリシ管理テーブルに記録する

請求項 1 3 から請求項 1 7 のうちのいずれか 1 項に記載の個人情報提供装置のデータ処理方法。

[請求項19] 前記個人情報取得装置毎かつ前記ユーザ毎に前記ポリシ管理テーブルに記録して管理する前記識別情報は、前記ポリシ記憶装置または前

記ポリシー時記憶装置のいずれに前記プライバシーポリシーが記憶されているかを識別する情報を含み、

検索された前記識別情報に基づいて、該当する前記プライバシーポリシーが前記ポリシー時記憶装置に記憶されていることを判定し、前記ポリシー時記憶装置に仮登録された前記未承認のプライバシーポリシーを前記ユーザに提示し、前記プライバシーポリシーの適用の認否を確認し、指示を前記ユーザから受け付ける

請求項 18 に記載の個人情報提供装置のデータ処理方法。

[請求項20]

受け付けた前記指示で前記ユーザにより否認された前記プライバシーポリシーの修正指示を前記ユーザから受け付け、受け付けた前記修正指示に基づいて、前記プライバシーポリシーを修正し、

修正された前記プライバシーポリシーを前記ポリシー時記憶装置に一時的に記憶し、その識別情報を前記ポリシー管理テーブルに記録する

請求項 19 に記載の個人情報提供装置のデータ処理方法。

[請求項21]

修正されて仮登録された前記プライバシーポリシーの適用を承認する個人情報取得装置の指定を前記ユーザから受け付け、

前記ユーザの前記指定に基づき、適用を承認された前記個人情報取得装置の前記承認済みプライバシーポリシーとして、前記修正されて仮登録された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理テーブルに記録する

請求項 20 に記載の個人情報提供装置のデータ処理方法。

[請求項22]

前記個人情報取得装置からユーザの個人情報の要求を受け付け、

前記要求を受け付けた前記個人情報取得装置および前記ユーザに該当するプライバシーポリシーの前記識別情報を検索し、

検索された前記プライバシーポリシーの識別情報に基づき、前記ポリシー記憶装置から前記プライバシーポリシーを取得し、

取得した前記プライバシーポリシーに従って、前記要求に応じられる可否かを判断し、

前記要求に応じられると判断した場合に、前記要求した前記個人情報取得装置に、個人情報を記憶する個人情報記憶装置から取得した前記個人情報を提供する

請求項 1 3 から請求項 2 1 のうちのいずれか 1 項に記載の個人情報提供装置のデータ処理方法。

[請求項23] 他の個人情報提供装置に、ユーザの個人情報を要求し、
前記他の個人情報提供装置から、前記ユーザの個人情報を受け取る
請求項 1 3 から請求項 2 2 のうちのいずれか 1 項に記載の個人情報提供装置のデータ処理方法。

[請求項24] コンピュータに個人情報提供装置を実現させるためのコンピュータプログラムであって、

ユーザの個人情報を取得する個人情報取得装置毎かつ前記ユーザ毎に設定されるプライバシーポリシーを記憶するポリシー記憶装置を備えたコンピュータに、

前記ポリシー記憶装置に前記プライバシーポリシーが記憶されているかを識別する識別情報を、前記個人情報取得装置毎かつ前記ユーザ毎にポリシー管理テーブルに記録して管理するポリシー管理手順、

前記ポリシー管理テーブルを参照し、前記個人情報取得装置および前記ユーザに該当するプライバシーポリシーの前記識別情報を検索する検索手順、

該当する前記プライバシーポリシーの前記識別情報が見つからなかったとき、デフォルトのプライバシーポリシーに基づいて、新規にプライバシーポリシーを自動的に作成するポリシー作成手順、および

作成された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理テーブルに記録するポリシー登録手順を実行させるためのコンピュータプログラム。

[請求項25] コンピュータに、前記ポリシー作成手順において、前記デフォルトのプライバシーポリシーとして、前記ポリシー記憶装置に記憶されている前記

プライバシーポリシーに基づいて、前記プライバシーポリシーを自動的に作成する手順を実行させるための請求項 24 に記載のコンピュータプログラム。

[請求項26]

コンピュータに、

前記ポリシー記憶装置に記憶されている前記プライバシーポリシーの修正指示を前記ユーザから受け付け、受け付けた前記修正指示に基づいて、前記プライバシーポリシーを修正するポリシー修正手順を実行させ、

前記ポリシー登録手順において、修正された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、前記ポリシー管理手順において、その識別情報を前記ポリシー管理テーブルに記録する手順をさらに実行させるための請求項 24 または請求項 25 に記載のコンピュータプログラム。

[請求項27]

コンピュータに、

前記ポリシー登録手順において、修正された前記プライバシーポリシーを他の個人情報取得装置の前記プライバシーポリシーとして自動的に適用し、前記他の個人情報取得装置のプライバシーポリシーとして修正された前記プライバシーポリシーを前記ポリシー記憶装置に記憶させ、前記ポリシー管理手順において、その識別情報を前記ポリシー管理テーブルに記録する手順を実行させるための請求項 26 に記載のコンピュータプログラム。

[請求項28]

コンピュータに、

修正された前記プライバシーポリシーを自動的に適用する個人情報取得装置の指定を前記ユーザから受け付ける指定受付手順を実行させ、

前記ポリシー登録手順において、修正された前記プライバシーポリシーを前記指定受付手順で受け付けた前記指定に従い、指定された前記個人情報取得装置の前記プライバシーポリシーとして自動的に適用する手順を実行させるための請求項 27 に記載のコンピュータプログラム。

[請求項29]

前記ユーザが未承認のプライバシーポリシーを一時的に記憶するポリシー

一時記憶装置をさらに備えたコンピュータに、

前記ポリシー作成手順により作成された前記プライバシーポリシーを前記未承認のプライバシーポリシーとして前記ポリシー時記憶装置に一時的に記憶させ、

前記ポリシー管理手順において、その識別情報を前記ポリシー管理テーブルに記録させるポリシー仮登録手順を実行させ、

前記ポリシー時記憶装置に仮登録された前記未承認のプライバシーポリシーを前記ユーザに提示し、前記プライバシーポリシーの適用の認否を確認し、指示を前記ユーザから受け付ける指示受付手順を実行させ、

前記ポリシー登録手順において、前記ポリシー時記憶装置に仮登録された前記未承認のプライバシーポリシーが前記ユーザにより承認されたとき、承認済みプライバシーポリシーとして前記ポリシー記憶装置に記憶する手順を実行させ、

前記ポリシー管理手順において、その識別情報を前記ポリシー管理テーブルに記録する手順を実行させるための請求項24から請求項28のうちのいずれか1項に記載のコンピュータプログラム。

[請求項30]

前記ポリシー管理手順において、前記個人情報取得装置毎かつ前記ユーザ毎に前記ポリシー管理テーブルに記録して管理される前記識別情報は、前記ポリシー記憶装置または前記ポリシー時記憶装置のいずれに前記プライバシーポリシーが記憶されているかを識別する情報を含み、

コンピュータに、

前記指示受付手順において、検索された前記識別情報に基づいて、該当する前記プライバシーポリシーが前記ポリシー時記憶装置に記憶されていることを判定し、前記ポリシー時記憶装置に仮登録された前記未承認のプライバシーポリシーを前記ユーザに提示し、前記プライバシーポリシーの適用の認否を確認し、指示を前記ユーザから受け付ける手順を実行させるための請求項29に記載のコンピュータプログラム。

[請求項31]

コンピュータに、

前記指示受付手順で受け付けた前記指示で前記ユーザにより否認された前記プライバシーポリシーの修正指示を前記ユーザから受け付け、受け付けた前記修正指示に基づいて、前記プライバシーポリシーを修正するポリシー修正手順を実行させ、

前記ポリシー仮登録手順において、修正された前記プライバシーポリシーを前記ポリシー時記憶装置に一時的に記憶し、その識別情報を前記ポリシー管理テーブルに記録する手順を実行させるための請求項 30 に記載のコンピュータプログラム。

[請求項32]

コンピュータに、

修正されて仮登録された前記プライバシーポリシーの適用を承認する個人情報取得装置の指定を前記ユーザから受け付ける指定受付手順を実行させ、

前記ポリシー登録手順において、前記ユーザの前記指定に基づき、適用を承認された前記個人情報取得装置の前記承認済みプライバシーポリシーとして、前記修正されて仮登録された前記プライバシーポリシーを前記ポリシー記憶装置に記憶し、その識別情報を前記ポリシー管理テーブルに記録する手順を実行させるための請求項 31 に記載のコンピュータプログラム。

[請求項33]

コンピュータに、

前記個人情報取得装置からユーザの個人情報の要求を受け付け、前記個人情報取得装置および前記ユーザに該当するプライバシーポリシーの前記識別情報を検索させる要求受付手順、

検索された前記プライバシーポリシーの識別情報に基づき、前記ポリシー記憶装置から前記プライバシーポリシーを取得する取得手順、

取得した前記プライバシーポリシーに従って、前記要求に応じられるか否かを判断する判断手順、および

前記要求に応じられると判断した場合に、前記要求した前記個人情報取得装置に、個人情報を記憶する個人情報記憶装置から取得した前

記個人情報を提供する提供手順をさらに実行させるための請求項 2 4 から請求項 3 2 のうちのいずれか 1 項に記載のコンピュータプログラム。

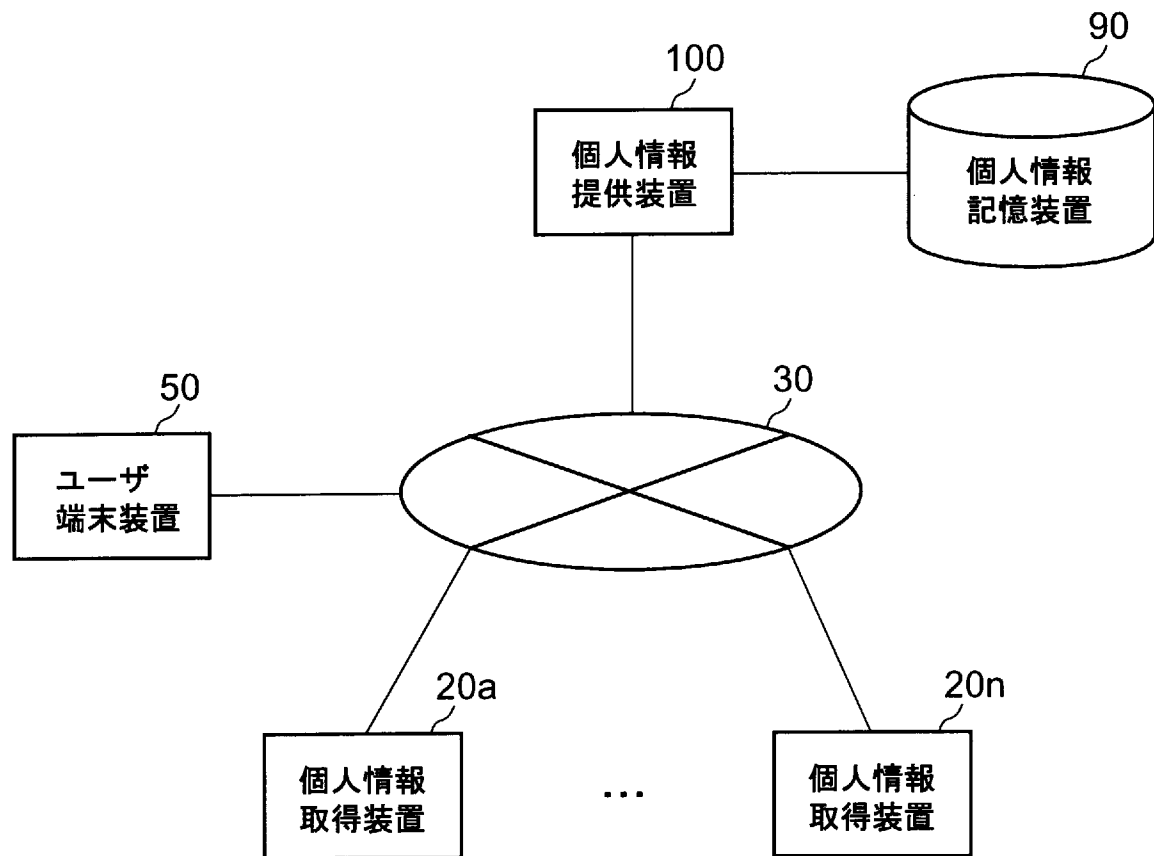
[請求項34]

コンピュータに、

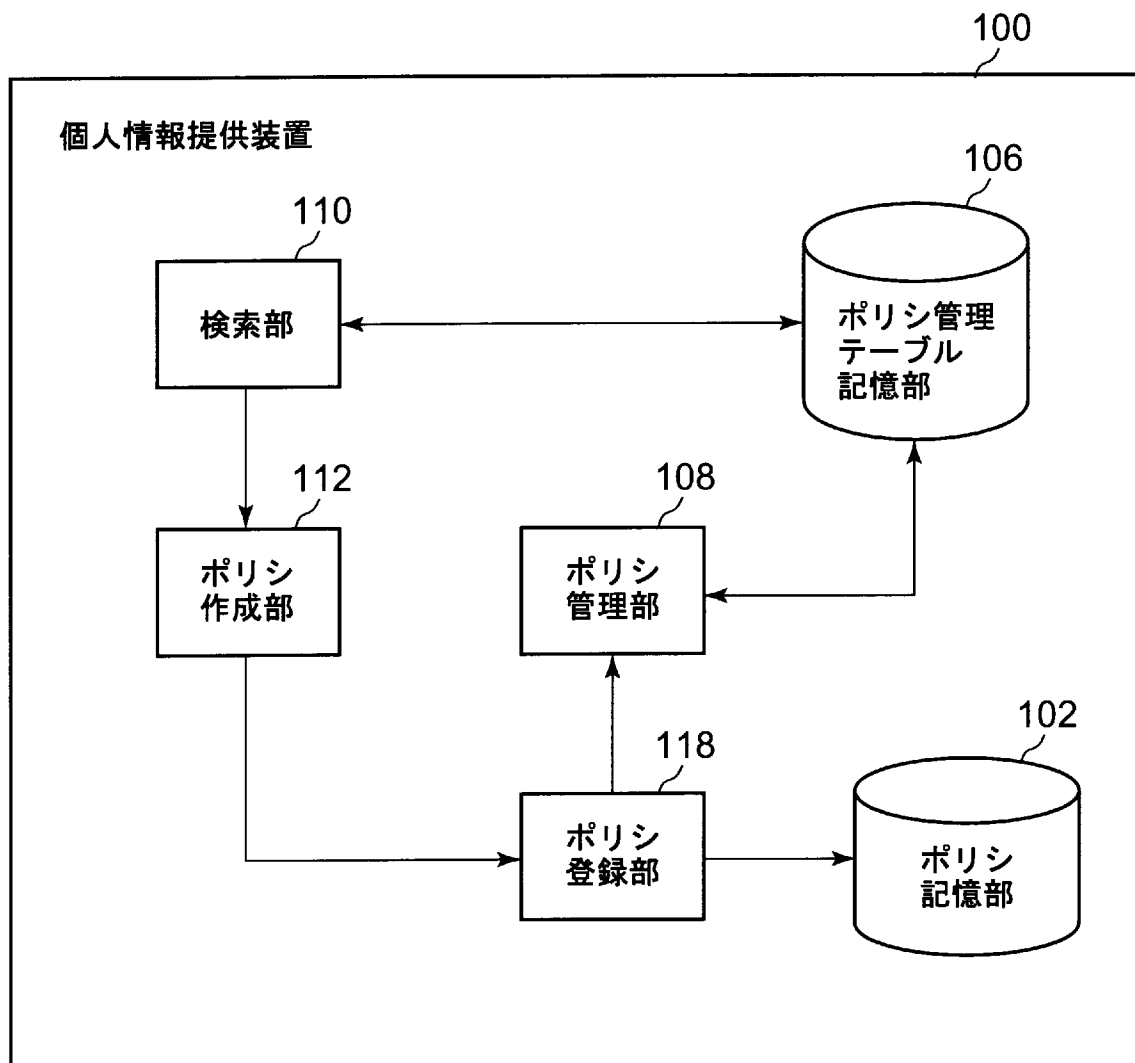
他の個人情報提供装置に、ユーザの個人情報を要求する要求手順、および

前記他の個人情報提供装置から、前記ユーザの個人情報を受け取る受取手順をさらに実行させるための請求項 2 4 から請求項 3 3 のうちのいずれか 1 項に記載のコンピュータプログラム。

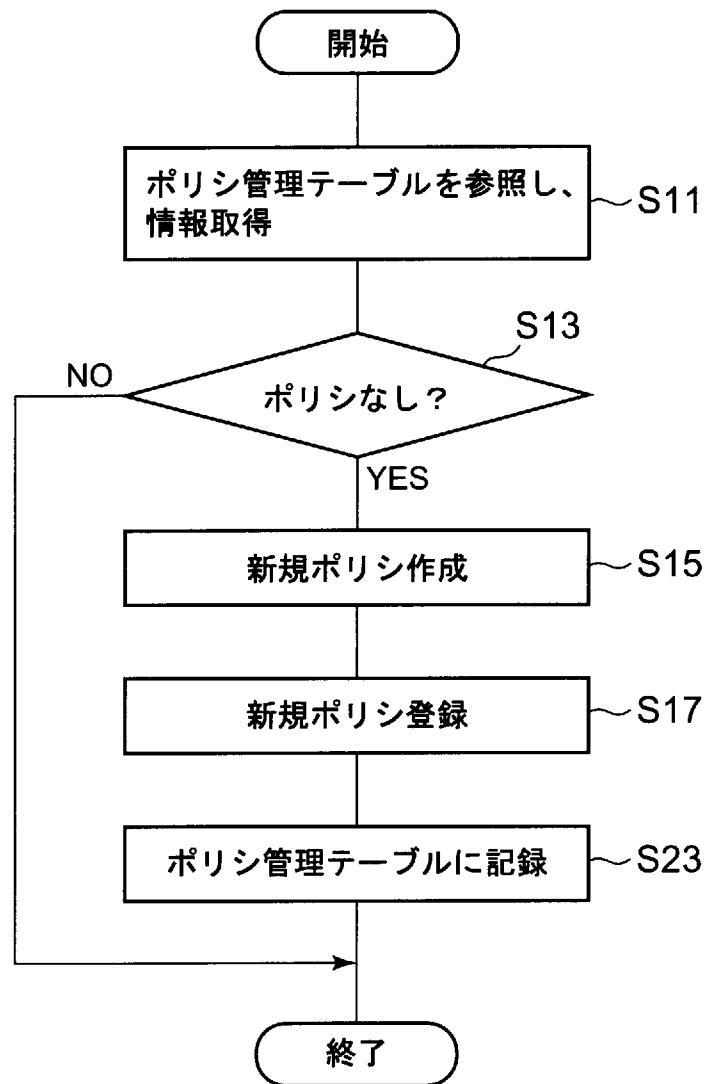
[図1]

1000 個人情報交換システム

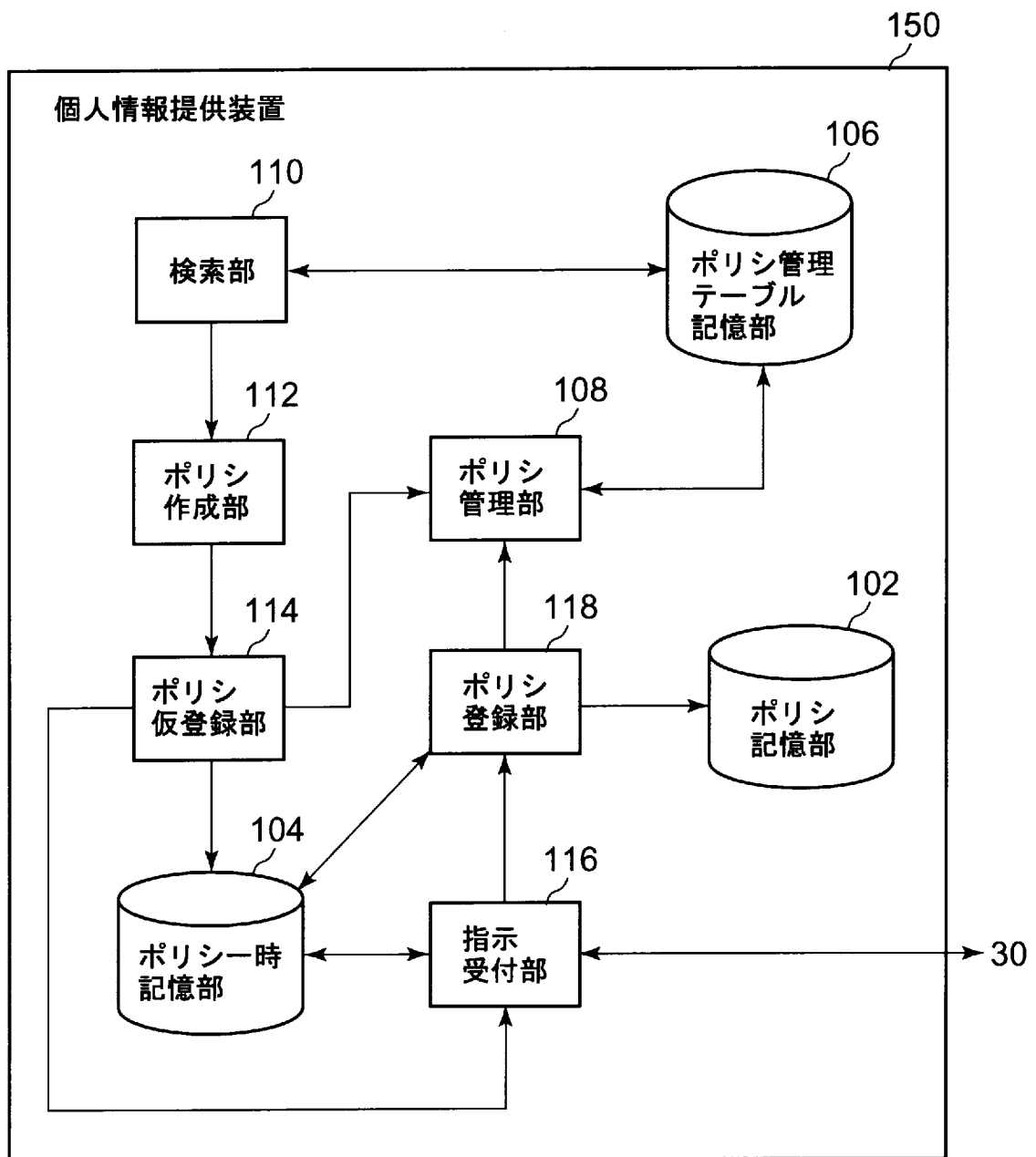
[図2]



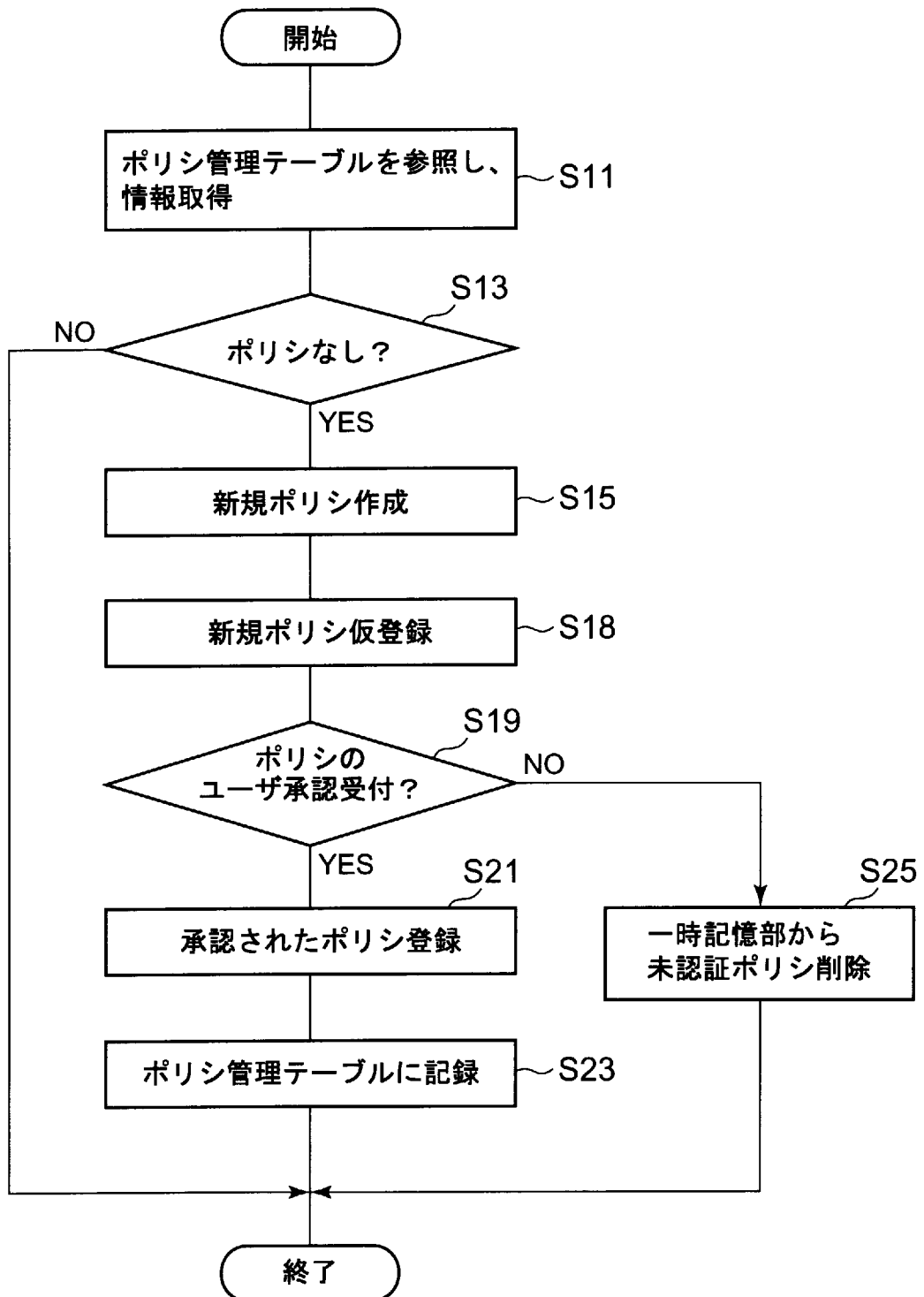
[図3]



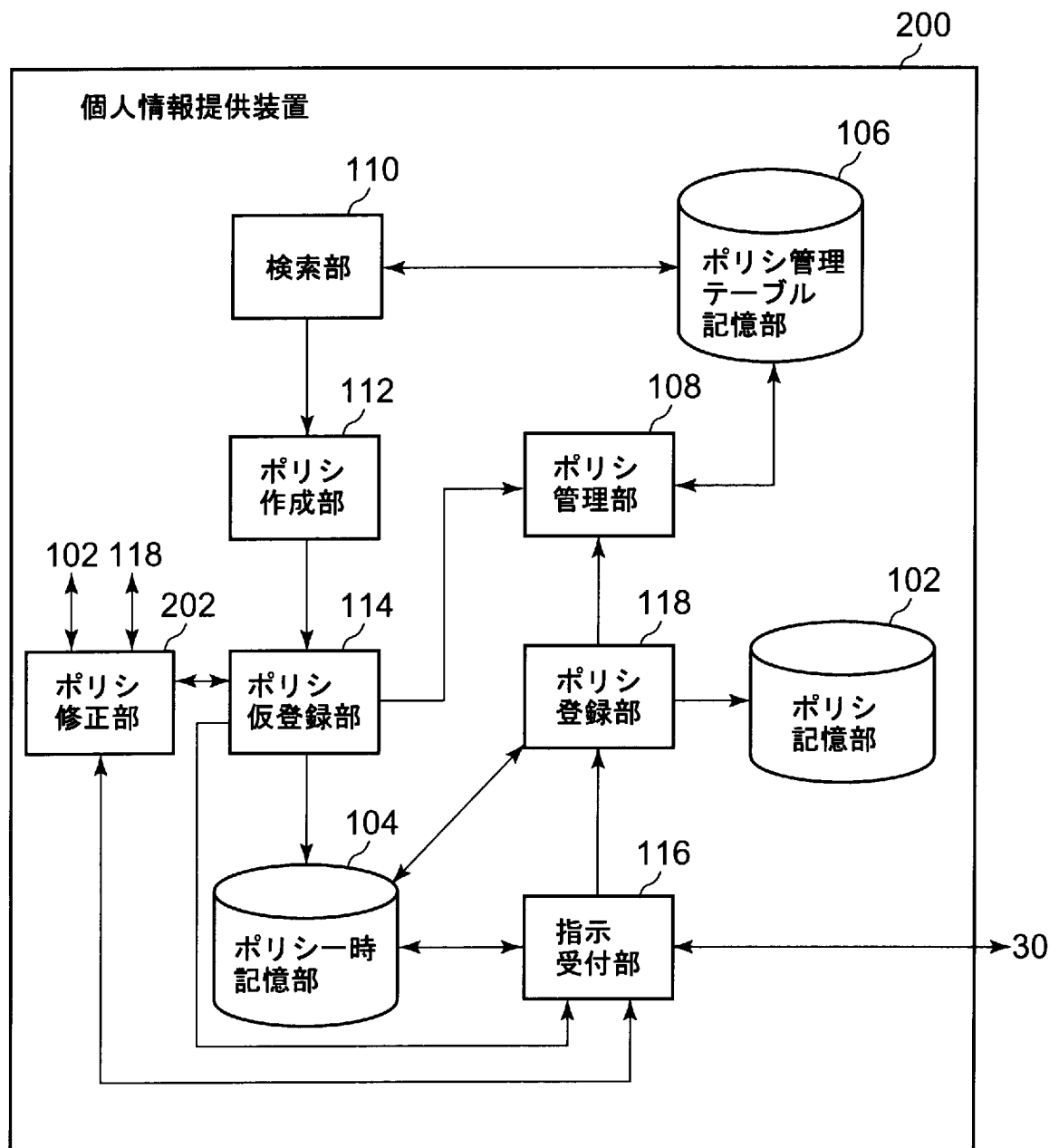
[図4]



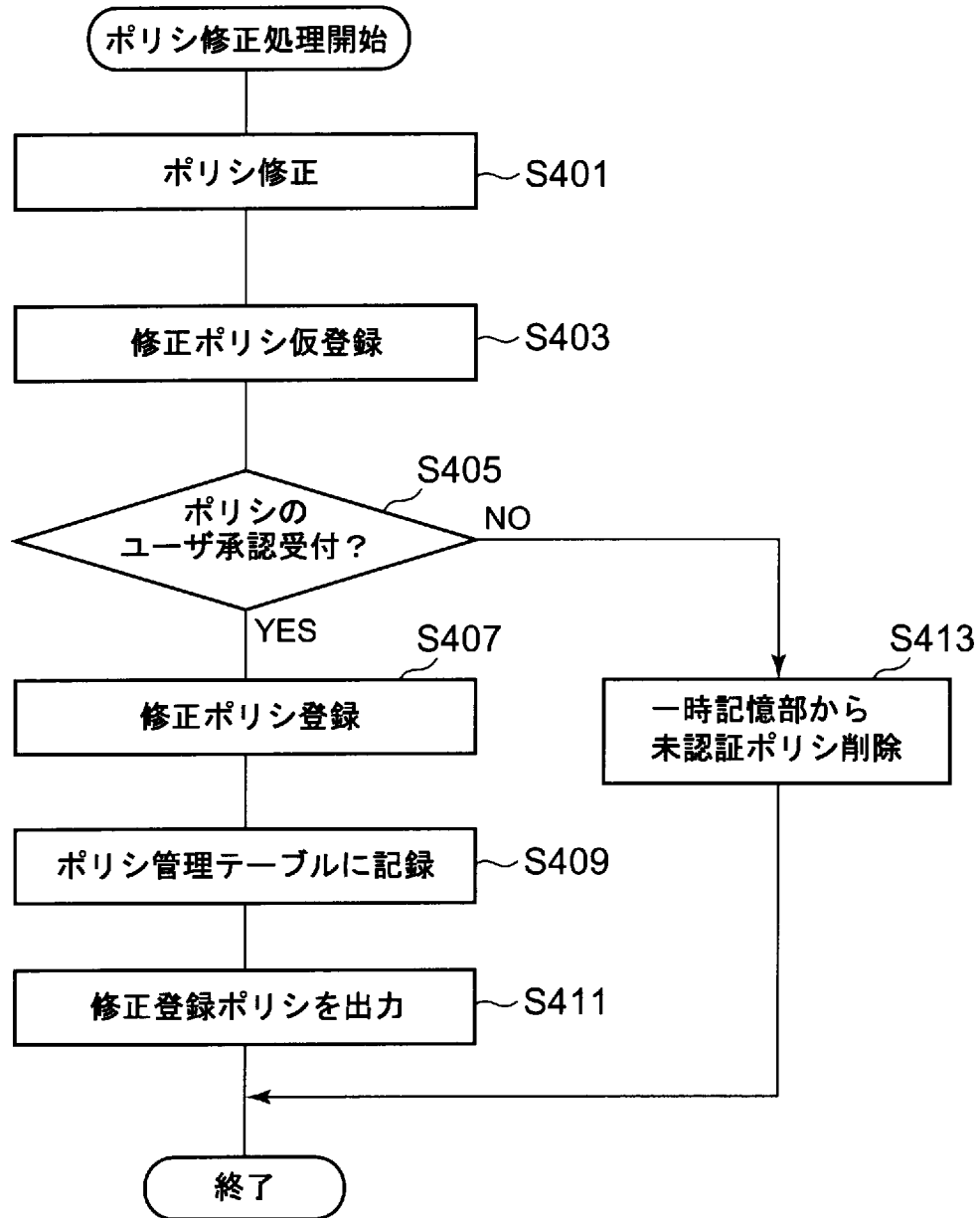
[図5]



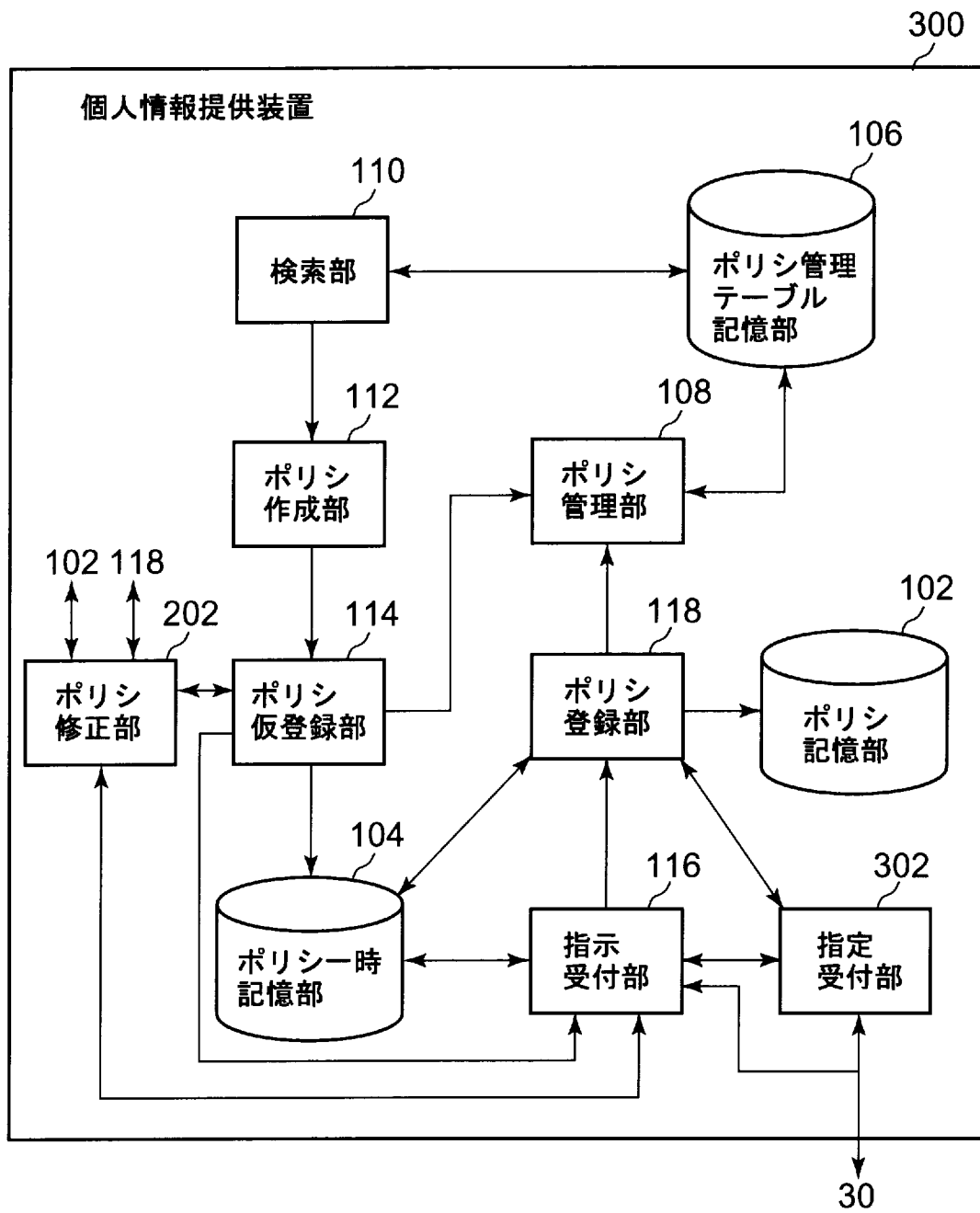
[図6]



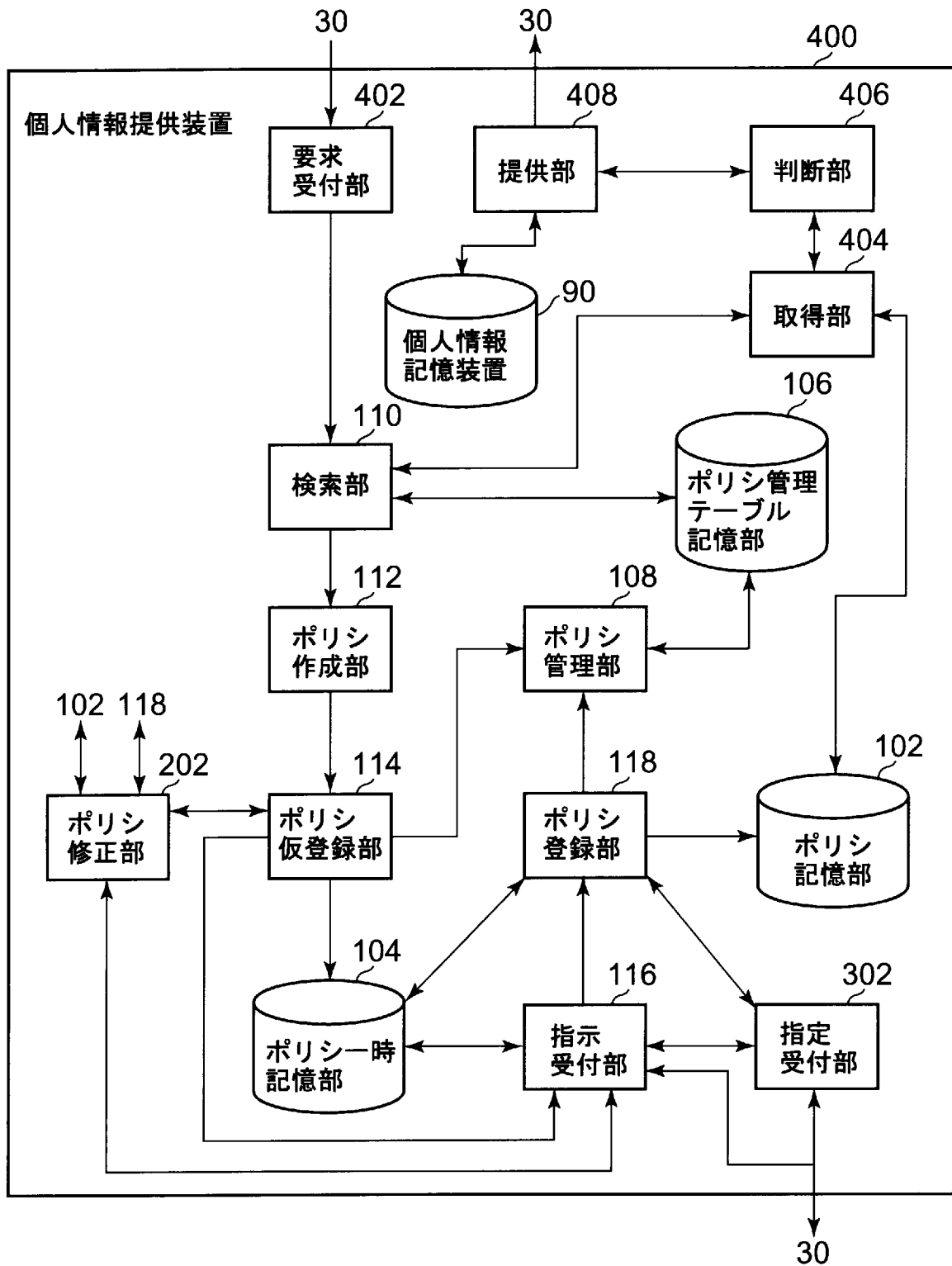
[図7]



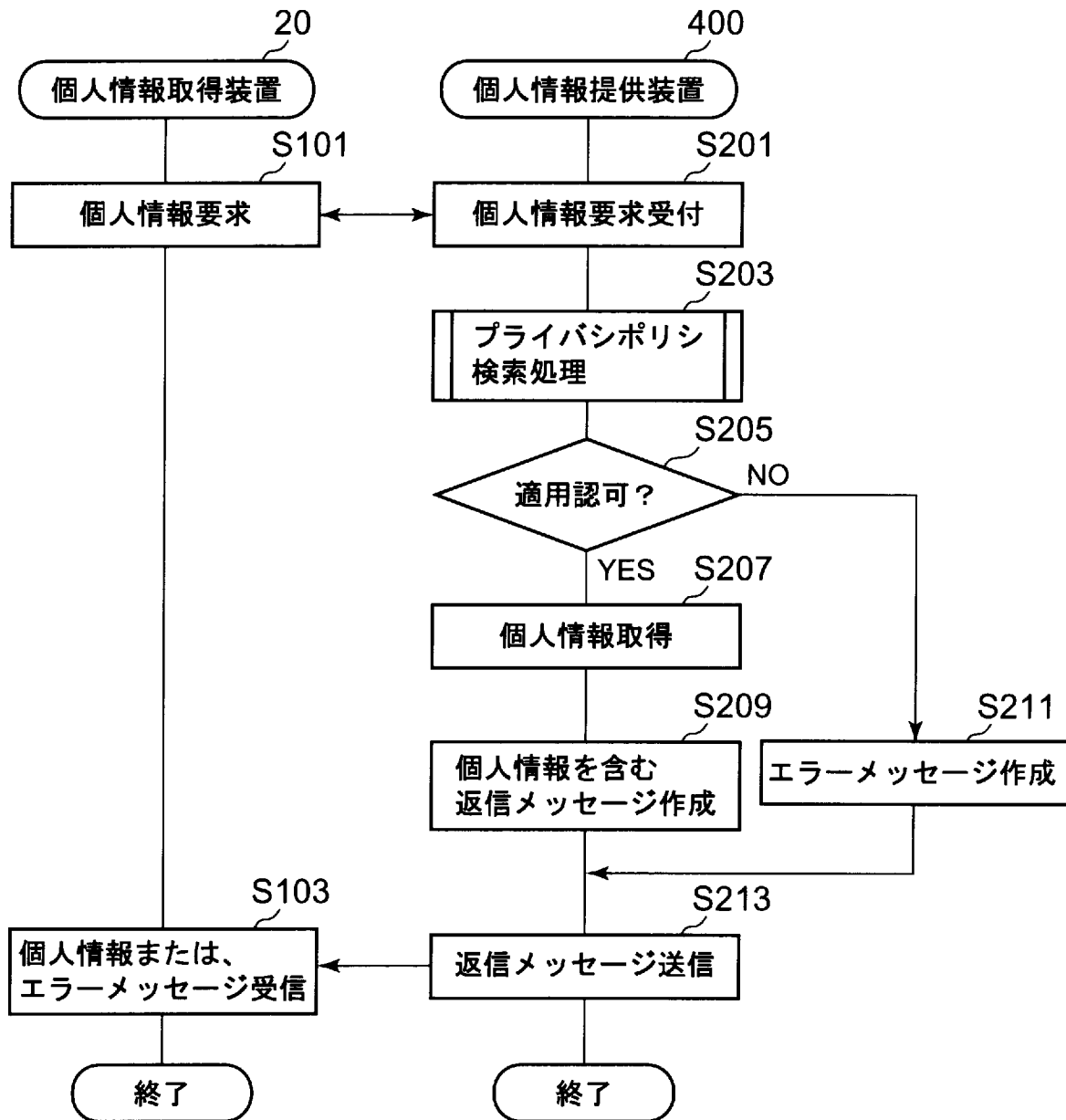
[図8]



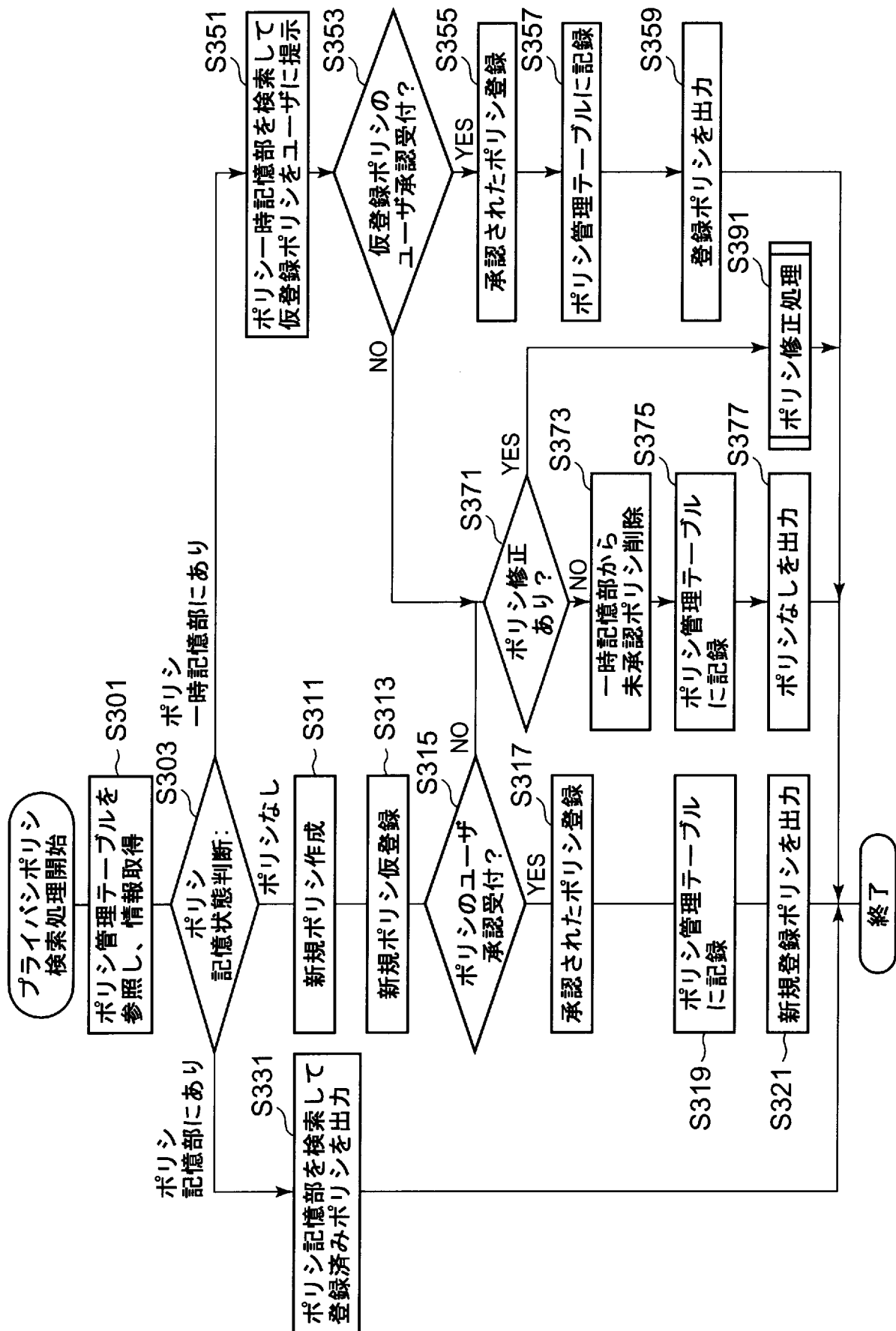
[図9]



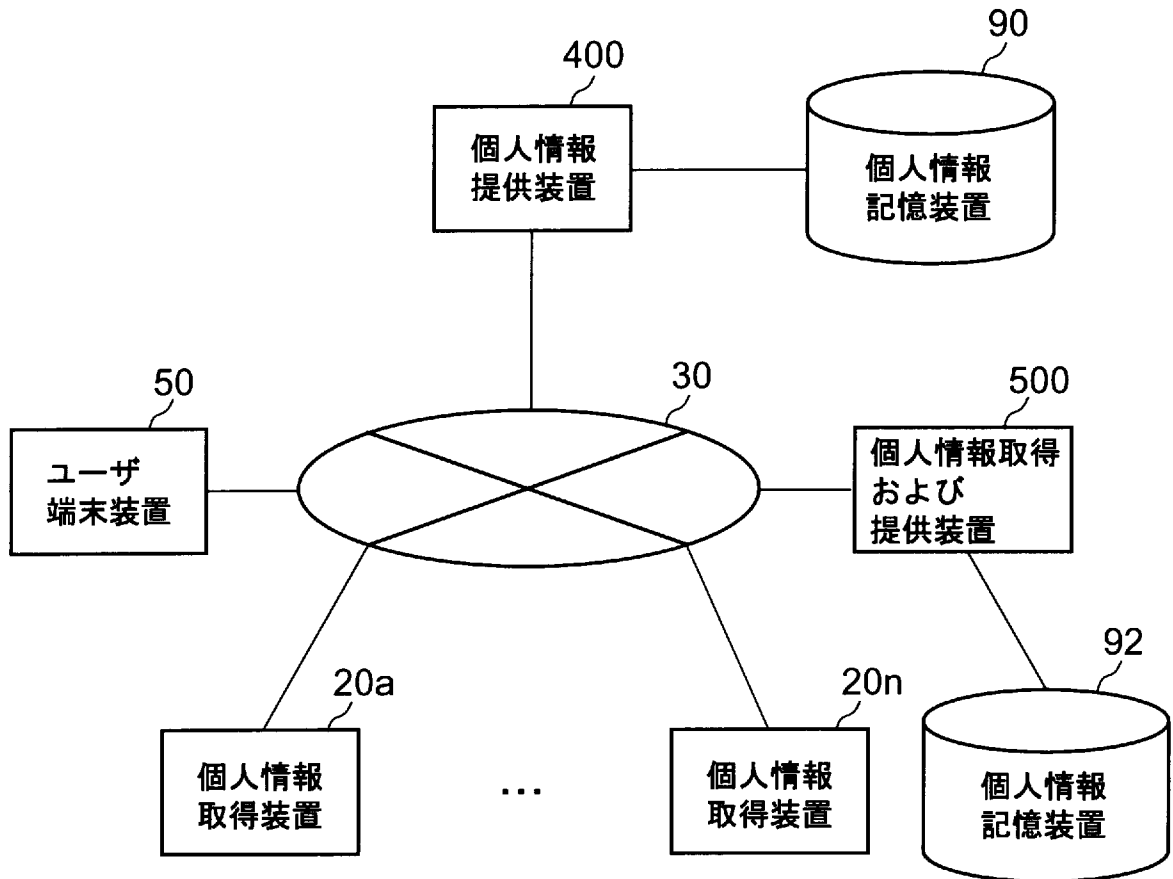
[図10]



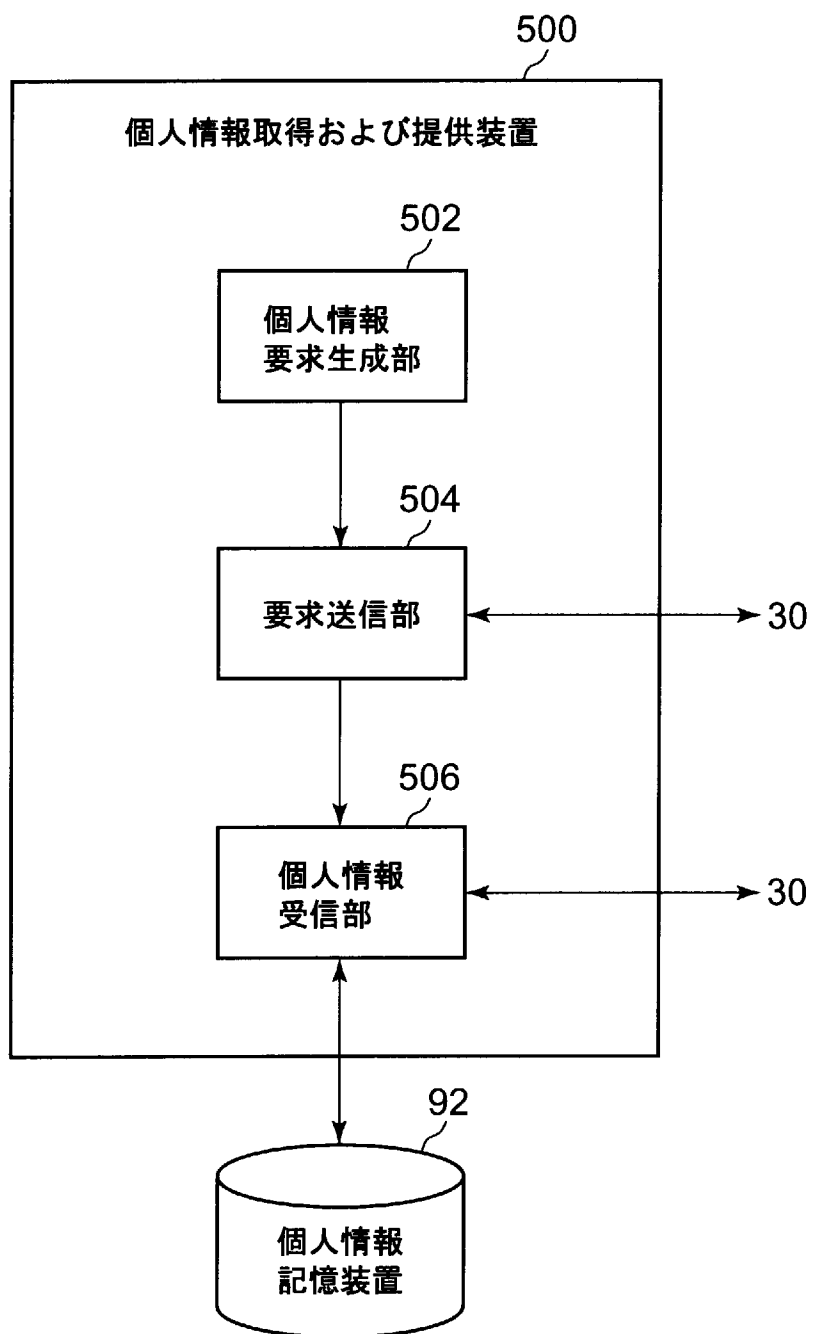
[図11]



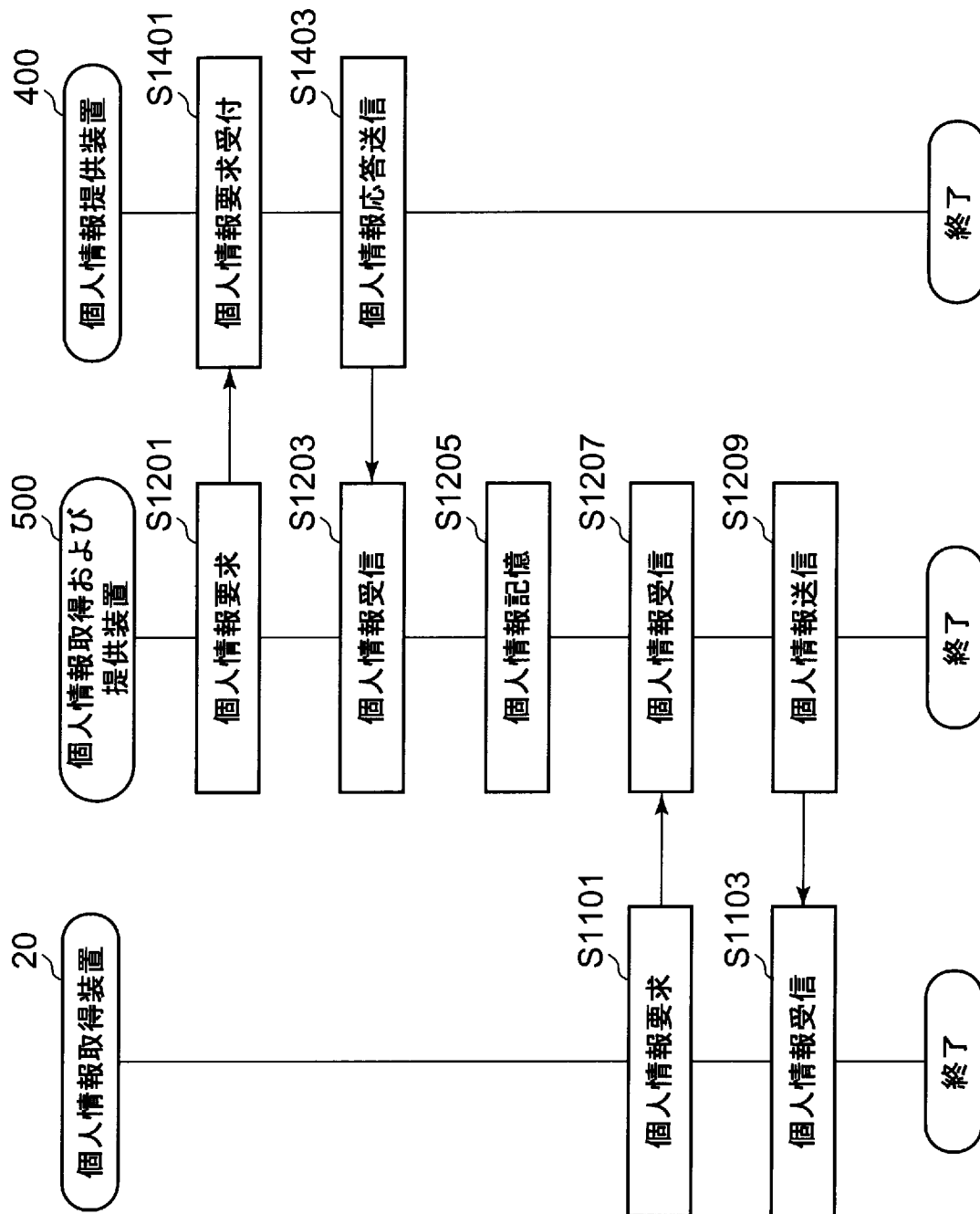
[図12]

1100 個人情報交換システム

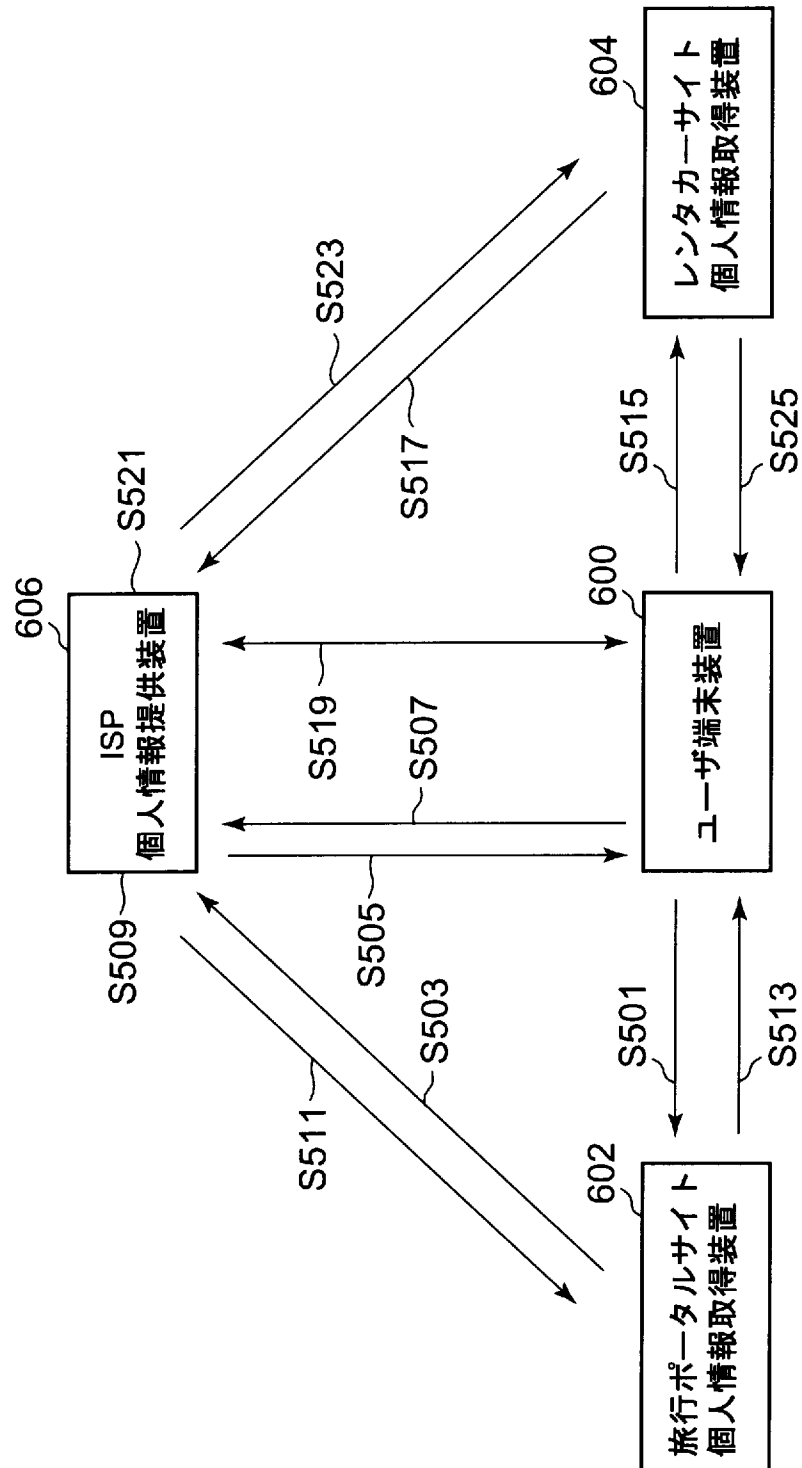
[図13]



[図14]



[図15]



[図16]

106

ユーザID	送信相手プロバイダ	ポリシー記憶場所
ID: 0001	レンタカーサイト http://rent-car.com	ポリシー記憶部
ID: 0001	ショッピングサイト http://shopping	ポリシー記憶部
ID: 0002	旅行ポータル http://travel.com	ポリシー記憶部
⋮	⋮	⋮

[図17]

106

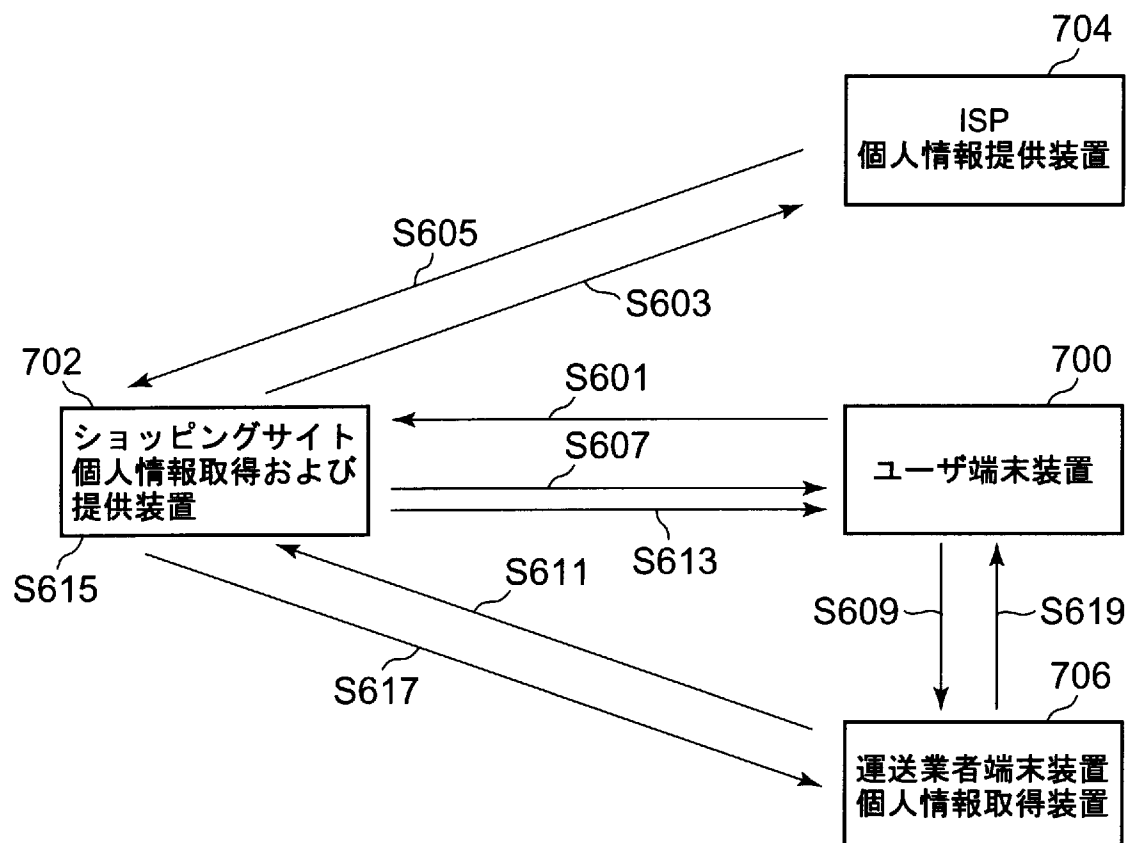
ユーザID	送信相手プロバイダ	ポリシー記憶場所
ID: 0001	レンタカーサイト http://rent-car.com	ポリシー時記憶部
ID: 0001	ショッピングサイト http://shopping.com	ポリシー時記憶部
ID: 0001	旅行ポータル http://travel.com	ポリシー記憶部
ID: 0002	旅行ポータル http://travel.com	ポリシー記憶部
⋮	⋮	⋮

[図18]

106

ユーザID	送信相手プロバイダ	ポリシー記憶場所
ID: 0001	レンタカーサイト http://rent-car.com	ポリシー記憶部
ID: 0001	ショッピングサイト http://shopping	ポリシー時記憶部
ID: 0001	旅行ポータル http://travel.com	ポリシー記憶部
ID: 0002	旅行ポータル http://travel.com	ポリシー記憶部
⋮	⋮	⋮

[図19]



[図20]

106

ユーザID	送信相手プロバイダ	ポリシー記憶場所
ID: 0001	ショッピングサイト http://shopping.com	ポリシー記憶部
ID: 0002	旅行ポータル http://travel.com	ポリシー記憶部
⋮	⋮	⋮

[図21]

106

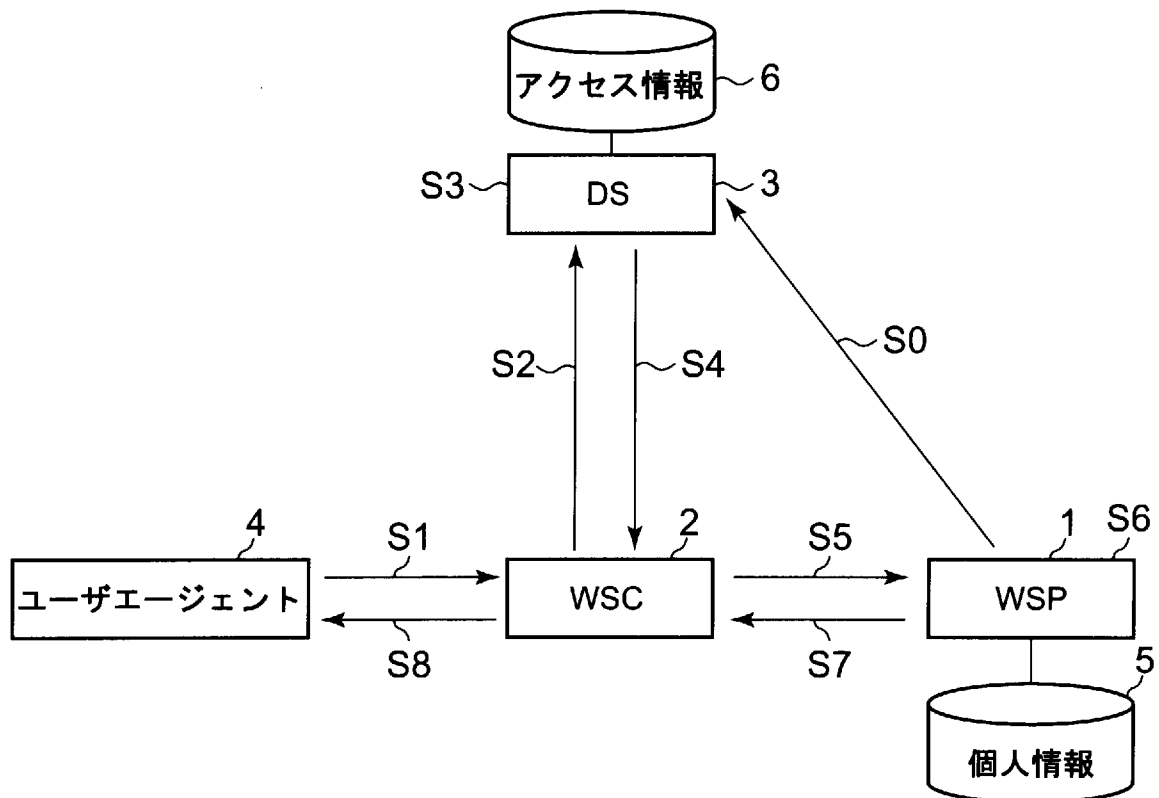
ユーザID	送信相手プロバイダ	ポリシー記憶場所
ID: 0001	ISP http://ISP.com	ポリシー記憶部
ID: 0002	運送業者 http://travel.com	ポリシー記憶部
⋮	⋮	⋮

[図22]

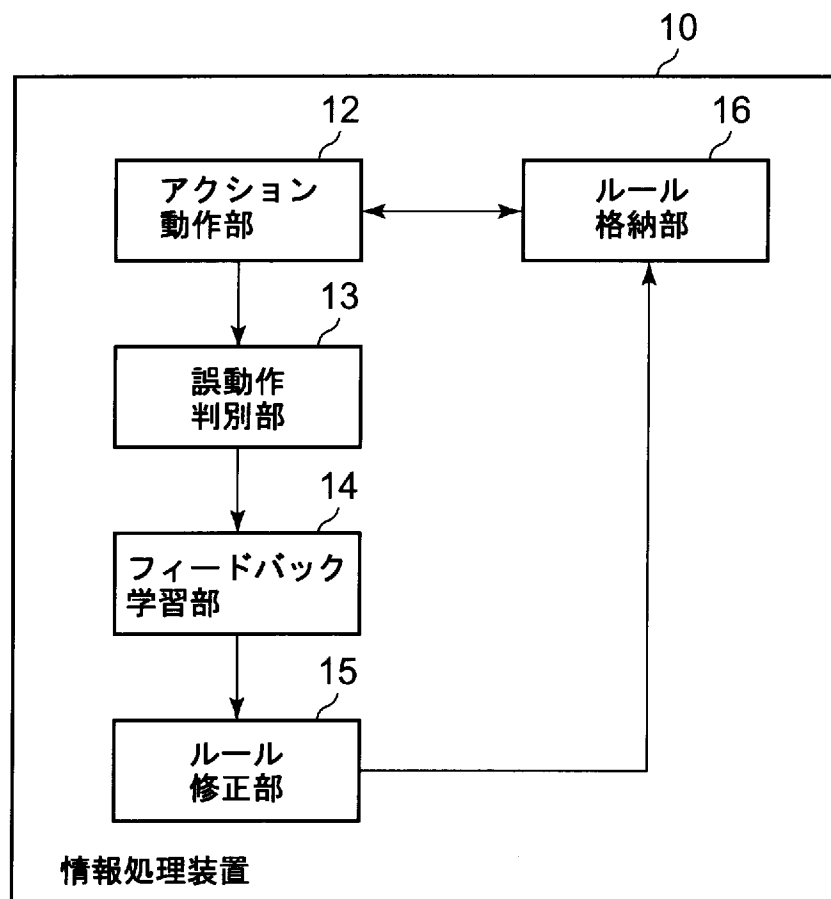
106

ユーザID	送信相手プロバイダ	ポリシー記憶場所
ID: 0001	ISP http://ISP.com	ポリシー記憶部
ID: 0001	運送業者 http://travel.com	ポリシー記憶部
ID: 0002	運送業者 http://travel.com	ポリシー記憶部
⋮	⋮	⋮

[図23]



[図24]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/006518

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/24 (2006.01) i, G06Q30/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/24, G06Q30/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2010

Kokai Jitsuyo Shinan Koho 1971-2010 Toroku Jitsuyo Shinan Koho 1994-2010

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2005-284353 A (Hitachi, Ltd.), 13 October 2005 (13.10.2005), abstract; paragraphs [0035] to [0038]; fig. 4, 10 to 12 (Family: none)	1-34
Y	JP 2004-192353 A (Nippon Telegraph And Telephone Corp.), 08 July 2004 (08.07.2004), abstract; paragraphs [0006] to [0013]; fig. 1, 7 (Family: none)	1-34
Y	JP 05-189442 A (Hitachi, Ltd.), 30 July 1993 (30.07.1993), entire text; all drawings (Family: none)	1-34

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
04 February, 2010 (04.02.10)Date of mailing of the international search report
16 February, 2010 (16.02.10)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/006518

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 09-062559 A (Fujitsu Ltd.), 07 March 1997 (07.03.1997), entire text; all drawings (Family: none)	1-34
Y	JP 2003-058709 A (American Family Life Assurance Company of Columbus), 28 February 2003 (28.02.2003), paragraphs [0019], [0086] (Family: none)	1-34
Y	WO 2007/148562 A1 (NEC Corp.), 27 December 2007 (27.12.2007), entire text; all drawings & US 2009/0276825 A1 & EP 2031540 A1	1-34
A	JP 2005-339308 A (Hitachi, Ltd.), 08 December 2005 (08.12.2005), entire text; all drawings (Family: none)	1-34
A	JP 2006-309737 A (NTT Communications Corp.), 09 November 2006 (09.11.2006), entire text; all drawings (Family: none)	1-34

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. G06F21/24(2006.01)i, G06Q30/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (I P C))

Int.Cl. G06F21/24, G06Q30/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 0 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 0 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 0 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2005-284353 A (株式会社日立製作所) 2005. 10. 13, 要約、段落 [0035]-[0038]、図 4、10-12 (ファミリーなし)	1-34
Y	JP 2004-192353 A (日本電信電話株式会社) 2004. 07. 08, 要約、段 落[0006]-[0013]、図 1、7 (ファミリーなし)	1-34
Y	JP 05-189442 A (株式会社日立製作所) 1993. 07. 30, 全文、全図 (フ ァミリーなし)	1-34

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

0 4 . 0 2 . 2 0 1 0

国際調査報告の発送日

1 6 . 0 2 . 2 0 1 0

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官 (権限のある職員)

岸 野 徹

5 S

3 9 8 3

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 09-062559 A (富士通株式会社) 1997. 03. 07, 全文、全図 (ファミリーなし)	1-34
Y	JP 2003-058709 A (アメリカン ファミリー ライフ アシュアランス カンパニー オブ コロンバス) 2003. 02. 28, 段落[0019]、[0086] (ファミリーなし)	1-34
Y	WO 2007/148562 A1 (日本電気株式会社) 2007. 12. 27, 全文、全図 & US 2009/0276825 A1 & EP 2031540 A1	1-34
A	JP 2005-339308 A (株式会社日立製作所) 2005. 12. 08, 全文、全図 (ファミリーなし)	1-34
A	JP 2006-309737 A (エヌ・ティ・ティ・コミュニケーションズ株式会社) 2006. 11. 09, 全文、全図 (ファミリーなし)	1-34