

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02012/046670

発行日 平成26年2月24日 (2014. 2. 24)

(43) 国際公開日 平成24年4月12日 (2012. 4. 12)

(51) Int.Cl.	F I	テーマコード (参考)
G06Q 50/10 (2012.01)	G06Q 50/10 100	
G06Q 30/06 (2012.01)	G06Q 30/06 190	
G06Q 30/02 (2012.01)	G06Q 30/02 132	
G06F 21/60 (2013.01)	G06F 21/24 160C	

審査請求 未請求 予備審査請求 未請求 (全 52 頁)

出願番号 特願2012-537687 (P2012-537687)	(71) 出願人 000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(21) 国際出願番号 PCT/JP2011/072695	
(22) 国際出願日 平成23年9月26日 (2011. 9. 26)	
(31) 優先権主張番号 特願2010-225741 (P2010-225741)	(74) 代理人 100109313 弁理士 机 昌彦
(32) 優先日 平成22年10月5日 (2010. 10. 5)	(74) 代理人 100124154 弁理士 下坂 直樹
(33) 優先権主張国 日本国 (JP)	(72) 発明者 島山 誠 東京都港区芝五丁目7番1号 日本電気株式会社内

最終頁に続く

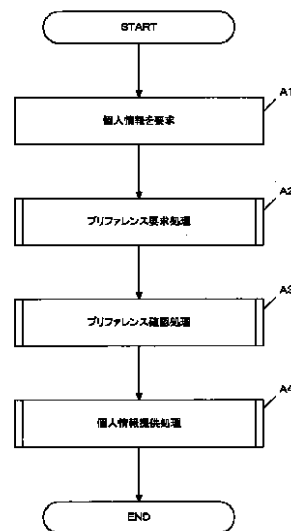
(54) 【発明の名称】 個人情報送受信システム、個人情報送受信方法、個人情報提供装置、プリファレンス管理装置、およびコンピュータ・プログラム

(57) 【要約】

個人情報を保有する装置数が増大した場合であっても、その個人情報の開示に関するプリファレンスを個々の装置に設定するユーザの負担軽減が可能な個人情報送受信システム等が開示される。

係る個人情報送受信システムにおいて、個人情報取得装置は、個人情報を個人情報提供装置に送信する。個人情報提供装置は、個人情報の開示に関するプリファレンスをプリファレンス管理装置に要求する。プリファレンス管理装置は、要求されたプリファレンスと、プリファレンス格納部に格納しておいた過去のプリファレンスとに基づいて生成した確認用プリファレンスを提示する。ユーザ端末は、提示されたプリファレンスを確認し、確認したプリファレンスを個人情報提供装置に送信する。個人情報提供装置は、受信したプリファレンスに基づいて、個人情報を個人情報取得装置に開示可能であると判断した場合に、その個人情報を、個人情報取得装置に送信する。

図10



A1 Request personal information
A2 Preference request processing
A3 Preference confirmation processing
A4 Personal information provision processing

【特許請求の範囲】**【請求項 1】**

個人情報取得装置と、個人情報提供装置と、プリファレンス管理装置と、ユーザ端末とを備え、

前記個人情報取得装置は、

前記ユーザ端末に対するサービス提供に必要な個人情報の要求を表す個人情報要求メッセージを、前記個人情報提供装置に送信する個人情報要求手段と、

前記個人情報を前記個人情報提供装置から受信する個人情報受信手段と、
を有し、

前記個人情報提供装置は、

前記個人情報を格納する個人情報格納手段と、

前記個人情報取得装置から前記個人情報要求メッセージを受信する個人情報要求受信手段と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、前記プリファレンス管理装置に送信するプリファレンス要求手段と、

前記プリファレンスを前記プリファレンス管理装置から受信するプリファレンス受信手段と、

前記プリファレンス受信手段によって受信されたプリファレンスに基づいて、前記個人情報を、前記個人情報取得装置に開示可能か否かを判断する開示可否判断手段と、

前記開示可否判断手段によって開示可能であると判断された場合に、前記個人情報を、前記個人情報格納手段から読み出すと共に、前記個人情報取得装置に送信する個人情報送信手段と、

を有し、

前記プリファレンス管理装置は、

前記ユーザ端末によって過去に設定されたプリファレンスを格納するプリファレンス格納手段と、

前記個人情報提供装置から前記プリファレンス要求メッセージを受信するプリファレンス要求受信手段と、

前記プリファレンス格納手段に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成する確認用プリファレンス生成手段と、

前記確認用プリファレンスを、前記ユーザ端末に提示し、提示した確認用プリファレンスに基づいて設定されたプリファレンスを前記ユーザ端末から受信するプリファレンス確認手段と、

前記プリファレンス確認手段によって受信された前記プリファレンスを前記個人情報提供装置に送信するプリファレンス送信手段と、

を有し、

前記ユーザ端末は、

前記プリファレンス管理装置から提示される前記確認用プリファレンスに基づいて、前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを設定し、設定したプリファレンスを、前記プリファレンス管理装置に送信するプリファレンス設定手段、

を有することを特徴とする個人情報送受信システム。

【請求項 2】

前記プリファレンス管理装置において、前記確認用プリファレンス生成手段は、

前記プリファレンス格納手段に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づいて、前記確認用プリファレンスを生成する

ことを特徴とする請求項 1 に記載の個人情報送受信システム。

10

20

30

40

50

【請求項 3】

前記プリファレンス管理装置は、

前記個人情報提供装置および前記個人情報取得装置の個人情報の取り扱いに関する取扱情報を格納する取扱情報格納手段と、

前記プリファレンス格納手段に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる提供元の個人情報提供装置および開示先の個人情報取得装置に類似する提供元および開示先に関する類似プリファレンスを、前記取扱情報格納手段に格納された各装置の取扱情報に基づいて抽出し、抽出した類似プリファレンスに基づいて、前記確認用プリファレンスを推定することによって生成する確認用プリファレンス推定手段と、

をさらに有することを特徴とする請求項 1 または請求項 2 に記載の個人情報送受信システム。

10

【請求項 4】

前記プリファレンス管理装置において、前記確認用プリファレンス推定手段は、

前記取扱情報格納手段に基づいて前記個人情報提供装置および前記個人情報取得装置を分類し、前記プリファレンス要求メッセージに含まれる提供元の個人情報提供装置と同一の分類に属する個人情報提供装置から、前記プリファレンス要求メッセージに含まれる開示先の個人情報取得装置と同一の分類に属する個人情報取得装置に対して、前記個人情報の開示に関して過去に設定されたプリファレンスを、前記類似プリファレンスとして抽出する

20

ことを特徴とする請求項 3 に記載の個人情報送受信システム。

【請求項 5】

前記プリファレンス管理装置において、前記確認用プリファレンス推定手段は、

前記プリファレンス格納手段に格納されたプリファレンスに基づいて、該各プリファレンスに含まれる個人情報の種類に対する評価値を算出するとともに、前記プリファレンス要求メッセージに含まれる個人情報の種類に対する評価値を算出することにより、前記プリファレンス要求メッセージに含まれる個人情報の評価値から、所定範囲内の評価値を有する種類の個人情報の開示に関するプリファレンスを、前記類似プリファレンスとして抽出する

ことを特徴とする請求項 3 または請求項 4 に記載の個人情報送受信システム。

30

【請求項 6】

前記個人情報提供装置は、

前記プリファレンス管理装置を表す情報を格納するプリファレンス管理装置情報格納手段と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関するプリファレンスの要求先となるプリファレンス管理装置を、前記プリファレンス管理装置情報格納手段に基づいて決定するプリファレンス要求先決定手段と、

をさらに備え、

前記プリファレンス要求手段は、

前記プリファレンス要求先決定手段によって決定されたプリファレンス管理装置に対して、前記プリファレンス要求メッセージを送信する

40

ことを特徴とする請求項 1 から請求項 5 のいずれかに記載の個人情報送受信システム。

【請求項 7】

前記個人情報提供装置は、

前記プリファレンス管理装置から取得したプリファレンスを保管するプリファレンス保管手段と、

前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを、前記プリファレンス保管手段を検索することによって取得するプリファレンス取得手段と、

をさらに備え、

50

前記開示可否判断手段は、
前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスが前記プリファレンス保管手段に保管されている場合、前記プリファレンス取得手段によって取得されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する

ことを特徴とする請求項 1 から請求項 6 のいずれかに記載の個人情報送受信システム。

【請求項 8】

前記ユーザ端末は、

前記個人情報の開示に関して過去に設定したプリファレンスの変更内容を前記プリファレンス管理装置に送信するプリファレンス変更内容設定手段をさらに備え、

10

前記プリファレンス管理装置は、

前記変更内容を前記ユーザ端末から取得する変更内容取得手段と、

前記変更内容取得手段によって取得された変更内容に基づいて、前記プリファレンス格納手段に格納されたプリファレンスを更新するプリファレンス更新手段と、

前記プリファレンス更新手段によって更新されたプリファレンスに関連する個人情報提供装置および個人情報取得装置を特定し、特定した個人情報提供装置および個人情報取得装置に対するプリファレンス変更通知を生成するプリファレンス変更通知生成手段と、

前記プリファレンス変更通知生成手段によって特定された個人情報提供装置および個人情報取得装置に対して、前記プリファレンス変更通知をそれぞれ送信するプリファレンス変更通知送信手段と、をさらに備える

20

ことを特徴とする請求項 1 から請求項 7 のいずれかに記載の個人情報送受信システム。

【請求項 9】

個人情報取得装置と、個人情報提供装置と、プリファレンス管理装置と、ユーザ端末とを用いて、

前記個人情報取得装置は、

前記ユーザ端末に対するサービス提供に必要な個人情報の要求を表す個人情報要求メッセージを、前記個人情報提供装置に送信し、

前記個人情報提供装置は、

前記個人情報を個人情報格納手段に予め格納しておき、

前記個人情報取得装置から前記個人情報要求メッセージを受信し、

30

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、前記プリファレンス管理装置に送信し、

前記プリファレンス管理装置は、

前記ユーザ端末によって過去に設定されたプリファレンスをプリファレンス格納手段に格納しておき、

前記個人情報提供装置から前記プリファレンス要求メッセージを受信し、

前記プリファレンス格納手段に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成し、

40

前記確認用プリファレンスを前記ユーザ端末に提示し、

前記ユーザ端末は、

前記プリファレンス管理装置から提示される前記確認用プリファレンスに基づいて、前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを設定し、

設定したプリファレンスを前記プリファレンス管理装置に送信し、

前記プリファレンス管理装置は、

設定されたプリファレンスを前記ユーザ端末から受信し、

受信された前記プリファレンスを前記個人情報提供装置に送信し、

前記個人情報提供装置は、

50

前記プリファレンスを前記プリファレンス管理装置から受信し、
受信されたプリファレンスに基づいて、前記個人情報前記個人情報取得装置に開示可能か否かを判断し、

開示可能であると判断された場合に、前記個人情報を前記個人情報格納手段から読み出すと共に、前記個人情報取得装置に送信し、

前記個人情報取得装置は、
前記個人情報を前記個人情報提供装置から受信する、
ことを特徴とする個人情報送受信方法。

【請求項 10】

前記プリファレンス管理装置は、
前記プリファレンス格納手段に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づいて、前記確認用プリファレンスを生成することを特徴とする請求項 9 に記載の個人情報送受信方法。

【請求項 11】

個人情報を格納する個人情報格納手段と、
前記個人情報の要求を表す個人情報要求メッセージを、個人情報取得装置から受信する個人情報要求受信手段と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、プリファレンス管理装置に送信するプリファレンス要求手段と、

前記プリファレンスを前記プリファレンス管理装置から受信するプリファレンス受信手段と、

前記プリファレンス受信手段によって受信されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する開示可否判断手段と、

前記開示可否判断手段によって開示可能であると判断された場合に、前記個人情報を前記個人情報格納手段から読み出すと共に、前記個人情報取得装置に送信する個人情報送信手段と、

を備えたことを特徴とする個人情報提供装置。

【請求項 12】

前記プリファレンス管理装置から取得したプリファレンスを保管するプリファレンス保管手段と、

前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを、前記プリファレンス保管手段を検索することによって取得するプリファレンス取得手段と、
をさらに備え、

前記開示可否判断手段は、
前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスが前記プリファレンス保管手段に保管されている場合、前記プリファレンス取得手段によって取得されたプリファレンスに基づいて、前記個人情報を、前記個人情報取得装置に開示可能か否かを判断することを特徴とする請求項 11 に記載の個人情報提供装置。

【請求項 13】

ユーザ端末によって過去に設定された、個人情報提供装置から個人情報取得装置に対する個人情報の開示に関する規定を表すプリファレンスを格納するプリファレンス格納手段と、

前記プリファレンスの要求を表すプリファレンス要求メッセージを、前記個人情報提供装置から受信するプリファレンス要求受信手段と、

前記プリファレンス格納手段に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成する確認用プリファレンス生成手段と、

10

20

30

40

50

前記確認用プリファレンスを前記ユーザ端末に提示し、提示した確認用プリファレンスに基づいて設定されたプリファレンスを、前記ユーザ端末から受信するプリファレンス確認手段と、

前記プリファレンス確認手段によって受信された前記プリファレンスを、前記個人情報提供装置に送信するプリファレンス送信手段と、
を備えたことを特徴とするプリファレンス管理装置。

【請求項 14】

前記確認用プリファレンス生成手段は、
前記プリファレンス格納手段に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づいて、前記確認用プリファレンスを生成することを特徴とする請求項 13 に記載のプリファレンス管理装置。

10

【請求項 15】

個人情報を個人情報格納装置に格納する個人情報格納機能と、
前記個人情報の要求を表す個人情報要求メッセージを、個人情報取得装置から受信する個人情報要求受信機能と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、プリファレンス管理装置に送信するプリファレンス要求機能と、

前記プリファレンスを前記プリファレンス管理装置から受信するプリファレンス受信機能と、

20

前記プリファレンス受信機能によって受信したプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する開示可否判断機能と、

前記開示可否判断機能によって開示可能であると判断された場合に、前記個人情報を個人情報格納装置から読み出すと共に、前記個人情報取得装置に送信する個人情報送信機能と、
をコンピュータ装置に実行させることを特徴とするコンピュータ・プログラム。

【請求項 16】

前記プリファレンス管理装置から取得したプリファレンスを、プリファレンス保管装置に保管するプリファレンス保管機能と、

30

前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを、前記プリファレンス保管装置を検索することによって取得するプリファレンス取得機能と、をさらに前記コンピュータ装置に実行させ、

前記開示可否判断機能によって、前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスが前記プリファレンス保管装置に保管されていると判断された場合に、前記プリファレンス取得機能によって取得されたプリファレンスに基づいて、前記個人情報を、前記個人情報取得装置に開示可能か否かを判断することを特徴とする請求項 15 に記載のコンピュータ・プログラム。

【請求項 17】

ユーザ端末によって過去に設定された、個人情報提供装置から個人情報取得装置に対する個人情報の開示に関する規定を表すプリファレンスを、プリファレンス格納装置に格納するプリファレンス格納機能と、

40

前記個人情報提供装置から、前記プリファレンス要求メッセージを受信するプリファレンス要求受信機能と、

前記プリファレンス格納装置に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成する確認用プリファレンス生成機能と、

前記確認用プリファレンスを前記ユーザ端末に提示し、提示した確認用プリファレンスに基づいて設定されたプリファレンスを、前記ユーザ端末から受信するプリファレンス確認機能と、

50

前記プリファレンス確認機能によって受信された前記プリファレンスを、前記個人情報提供装置に送信するプリファレンス送信機能と、
をコンピュータ装置に実行させることを特徴とするコンピュータ・プログラム。

【請求項18】

前記確認用プリファレンス生成機能は、前記プリファレンス格納装置に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づいて、前記確認用プリファレンスを生成することを特徴とする請求項17に記載のコンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、個人情報を通信ネットワークを介して送受信する技術分野に関する。特に、本発明は、個人情報の開示に関するユーザプリファレンスに基づいて、その個人情報を、通信ネットワークを介して、複数の装置間において送受信する技術分野に関する。

【背景技術】

【0002】

個人情報の開示に関するユーザプリファレンスに基づき、その個人情報を、通信ネットワーク（以下、単に「ネットワーク」と略称する）を介して、複数の装置間において送受信する個人情報送受信システムが知られている。ここで、個人情報の送受信に関するユーザプリファレンスとは、その個人情報を保有する装置から他の装置へ、当該個人情報を提供 20
する際の条件、提供の可否等を表す情報（データ）である。このユーザプリファレンスは、一般に、そのユーザプリファレンスによって特定可能なユーザによって規定された情報である。以下、本願においては、個人情報の開示に関するユーザプリファレンスを、単に「プリファレンス」と記載する場合がある。

例えば、プリファレンスは、個人情報の種類ごとに、使用目的や開示範囲が規定された情報を含んでいる。また、プリファレンスは、個人情報の主体であるユーザによって作成される場合もあれば、個人情報を利用してサービスを提供する事業者によって作成される場合もある。ユーザ以外によって作成されたプリファレンスは、そのユーザに許諾されること 30
によって有効となる。

非特許文献1は、このような個人情報送受信システムの一例を開示する。図33は、関連技術としての非特許文献1に開示された個人情報送受信システムの構成図である。図33に示すように、非特許文献1に記載された個人情報送受信システムは、ウェブサービスプロバイダ（以下、WSPという）と、ウェブサービスコンシューマ（以下、WSCという）と、ユーザエージェントとを備える。WSPは、エンドユーザの個人情報を保有している。WSCは、エンドユーザの個人情報を利用したサービスを、ユーザエージェントを介してエンドユーザに提供する。ユーザエージェントは、一般的なウェブブラウザ等によって構成されており、アクセス先をリダイレクトする機能を有する。WSPは、エンドユーザによって同意された場合にのみWSCに個人情報を提供する。 40

この非特許文献1に記載された個人情報送受信システムは、次のように動作する。まず、ユーザエージェントは、WSCにアクセスすることにより、サービスの提供を要求する（ステップZ1）。次に、WSCは、WSPに対して個人情報を要求するメッセージを送信する（ステップZ2）。要求メッセージを受信したWSPは、個人情報をWSCに提供することに関するエンドユーザによる許諾確認（許諾確認処理）が済んでいるか否かを判断する。ここで、エンドユーザによる許諾確認が未だ済んでいない場合に、WSPは、エンドユーザの許諾確認が必要であることが記載されたメッセージを、WSCに対して送信する（ステップZ3）。このメッセージは、ステップZ2における要求メッセージに対するWSCへの応答メッセージである。この応答メッセージは、エンドユーザによる許諾確認が必要であることを示すメッセージと、WSPの許諾確認用URL（Uniform Resource Locator）とを含む。 50

応答メッセージを受信したWSCは、その応答メッセージに含まれるWSPの許諾確認

50

用URLにアクセスするように、ユーザエージェントをリダイレクトする(ステップZ4)。このリダイレクトによって許諾確認用URLにアクセスされたWSPは、ユーザエージェントに対して、個人情報をWSCへ提供してよいか否かを確認する(ステップZ5)。その後、WSPは、ユーザエージェントをWSCにリダイレクトする(ステップZ6)。ユーザエージェントによって再度アクセスされたWSCは、WSPに対して、個人情報を要求するメッセージを再度送信する(ステップZ7)。このとき、上述したステップZ5において個人情報をWSCに提供することを許諾する情報を取得していれば、WSPは、個人情報を含むメッセージをWSCへ提供する(ステップZ8)。個人情報を取得したWSCは、取得した情報に基づくサービスを、ユーザエージェントに提供する(ステップZ9)。

10

このように、非特許文献1に記載された個人情報送受信システムでは、個人情報を保有するWSPがユーザエージェントと直接通信することにより、個人情報の開示に関するプリファレンスを取得して個人情報をWSCに提供する。

また、特許文献1は、他の個人情報送受信システムを開示する。図34は、他の関連技術としての特許文献1に開示された個人情報送受信システムの構成図である。図34に示すように、この特許文献1に記載された個人情報送受信システムは、ウェブサーバと、顧客端末とがネットワークを介して接続された構成を備える。

この特許文献1に記載された個人情報送受信システムは、次のように動作する。まずウェブサーバは、顧客に発行した仮ID(ID:識別子、識別情報)を顧客端末に対して送信する。次に、顧客端末は、仮IDを用いてウェブサーバにログインする。次に、ウェブサーバは、プライバシーポリシーとして予め定められている各項目を、顧客端末に提示する。そして、顧客端末は、エンドユーザの操作に応じて、プライバシーポリシーの各項目に対する同意または不同意を表す情報を、ウェブサーバに送信する。ウェブサーバは、受信した情報に基づいてこの仮IDを登録可能であると判断した場合、仮IDと、各項目に対する同意または不同意を表す情報とを、そのエンドユーザに関するプロフィールとして登録すると共に、そのエンドユーザに対して、本IDを配布する。

20

このように、特許文献1に記載された個人情報送受信システムでは、ウェブサーバが顧客端末から、プライバシーポリシーの各項目に対する同意または不同意を表すプリファレンスを直接取得することにより、顧客の同意に基づくサービス提供を実現する。

即ち、非特許文献1および特許文献1に記載された個人情報送受信システムでは、個人情報を保有する装置が、その個人情報の主体であるユーザ(エンドユーザ)の操作する端末と直接通信することにより、個人情報の開示に関するプリファレンスを取得する。

30

【先行技術文献】

【特許文献】

【0003】

【特許文献1】特開2006-99407号公報

【非特許文献】

【0004】

【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)、“リバティアイディーダブルエスエフインタラクティブサービススペシフィケーション(Liberty ID-WSF Interaction Service Specification)”[online]、2006年7月30日、[平成22年7月15日検索]、インターネット、<URL <http://www.projectliberty.org/liberty/content/download/3461/23009/file/liberty-id-wsf-interaction-svc-v2.0-original.pdf>>

40

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、非特許文献1および特許文献1に記載された個人情報送受信システムで

50

は、複数の装置が個人情報を保有する場合、ユーザは、複数の装置に対して、それぞれプリファレンスの設定または許諾を行う必要がある。このため、非特許文献1および特許文献1に記載された個人情報送受信システムでは、個人情報を保有する装置数が増大すると、プリファレンスを設定するユーザの負担が増大するという課題がある。

具体的には、非特許文献1および特許文献1に記載された個人情報送受信システムにおいて、ユーザは、個人情報を保有する複数の装置を対象として、個人情報の種類別に、情報開示の可否判断を登録する必要がある。個人情報の開示可否を判断するために、ユーザは、個人情報を保有する各装置の個人情報の取り扱いに関する詳細を把握する必要がある。したがって、個人情報を保有する装置数の増大に伴い、ユーザが把握しなければならない情報が増大し、開示可否の判断におけるユーザ負担が増大する。

例えば、非特許文献1に記載された個人情報送受信システムでは、ユーザは、WSPごとに開示可否の判断を行う必要がある。したがって、WSP数の増大により、ユーザが把握すべき各WSPの情報も増大し、ユーザ負担が増大する。

また、特許文献1に記載された個人情報送受信システムにおいても、ユーザは、ウェブサーバ毎に、プライバシーポリシーに記載された各項目に対する同意を判断する必要がある。したがって、ウェブサーバ数の増大に伴い、ユーザ負担が増大する。

さらに、個人情報を保有する複数の装置に対してプリファレンスを設定する場合、ユーザにとって、装置間でプリファレンスを矛盾しないよう設定することは負担である。なぜなら、係る複数の装置に対してプリファレンスを設定する場合、ユーザにとって終始一貫した判断基準に基づき各装置にプリファレンスを設定することは人間の特性に起因して難しいからである。このため、ユーザは、異なる装置が個別に保有する同一種類の個人情報に対して、個人情報の開示許可を与えてしまう場合がある。例えば、ユーザは、プロバイダAに対してプロバイダBへの住所情報を提供することを禁止する一方で、プロバイダCに対してはプロバイダBへの住所情報の提供を許可するかもしれない。このような場合、当該ユーザに関するプリファレンスは、プロバイダAとプロバイダBとの間で矛盾する。しかも、ユーザは、矛盾したプリファレンスを設定していることを確認することが難しい。

このように、非特許文献1および特許文献1に記載された個人情報送受信システムを採用する場合、特定のユーザに関する個人情報を保有する装置数が増大するのに伴い、複数の装置間でプリファレンスを矛盾しないよう設定するユーザ負担が増大する。

本発明は、上述の課題を解決するためになされた。本発明は、個人情報を保有する装置数が増大した場合であっても、その個人情報の開示に関するプリファレンスを個々の装置に設定するユーザの負担軽減が可能な個人情報送受信システム等を提供することを主たる目的とする。

【課題を解決するための手段】

【0006】

上記目的（課題）を解決する一つの見地として、本発明に係る個人情報送受信システムは、個人情報取得装置と、個人情報提供装置と、プリファレンス管理装置と、ユーザ端末とを備える。そして、この個人情報送受信システムにおいて、

前記個人情報取得装置は、

前記ユーザ端末に対するサービス提供に必要な個人情報の要求を表す個人情報要求メッセージを、前記個人情報提供装置に送信する個人情報要求手段と、

前記個人情報を前記個人情報提供装置から受信する個人情報受信手段と、
を有し、

前記個人情報提供装置は、

前記個人情報を格納する個人情報格納手段と、

前記個人情報取得装置から前記個人情報要求メッセージを受信する個人情報要求受信手段と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、前記プリファレンス管理

10

20

30

40

50

装置に送信するプリファレンス要求手段と、

前記プリファレンスを前記プリファレンス管理装置から受信するプリファレンス受信手段と、

前記プリファレンス受信手段によって受信されたプリファレンスに基づいて、前記個人情報情報を、前記個人情報取得装置に開示可能か否かを判断する開示可否判断手段と、

前記開示可否判断手段によって開示可能であると判断された場合に、前記個人情報情報を、前記個人情報格納手段から読み出すと共に、前記個人情報取得装置に送信する個人情報送信手段と、

を有し、

前記プリファレンス管理装置は、

前記ユーザ端末によって過去に設定されたプリファレンスを格納するプリファレンス格納手段と、

前記個人情報提供装置から前記プリファレンス要求メッセージを受信するプリファレンス要求受信手段と、

前記プリファレンス格納手段に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成する確認用プリファレンス生成手段と、

前記確認用プリファレンスを、前記ユーザ端末に提示し、提示した確認用プリファレンスに基づいて設定されたプリファレンスを前記ユーザ端末から受信するプリファレンス確認手段と、

前記プリファレンス確認手段によって受信された前記プリファレンスを前記個人情報提供装置に送信するプリファレンス送信手段と、

を有し、

前記ユーザ端末は、

前記プリファレンス管理装置から提示される前記確認用プリファレンスに基づいて、前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを設定し、設定したプリファレンスを、前記プリファレンス管理装置に送信するプリファレンス設定手段、

を有する。

また、上記目的を解決する他の見地として、本発明に係る個人情報送受信方法は、個人情報取得装置と、個人情報提供装置と、プリファレンス管理装置と、ユーザ端末とを用いる。即ち、係る個人情報送受信方法において、

前記個人情報取得装置は、

前記ユーザ端末に対するサービス提供に必要な個人情報の要求を表す個人情報要求メッセージを、前記個人情報提供装置に送信し、

前記個人情報提供装置は、

前記個人情報を個人情報格納手段に予め格納しておき、

前記個人情報取得手段から前記個人情報要求メッセージを受信し、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、前記プリファレンス管理装置に送信し、

前記プリファレンス管理装置は、

前記ユーザ端末によって過去に設定されたプリファレンスをプリファレンス格納手段に格納しておき、

前記個人情報提供装置から前記プリファレンス要求メッセージを受信し、

前記プリファレンス格納手段に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成し、

前記確認用プリファレンスを前記ユーザ端末に提示し、

前記ユーザ端末は、

10

20

30

40

50

前記プリファレンス管理装置から提示される前記確認用プリファレンスに基づいて、前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを設定し、

設定したプリファレンスを前記プリファレンス管理装置に送信し、

前記プリファレンス管理装置は、

設定されたプリファレンスを前記ユーザ端末から受信し、

受信された前記プリファレンスを前記個人情報提供装置に送信し、

前記個人情報提供装置は、

前記プリファレンスを前記プリファレンス管理装置から受信し、

受信されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断し、

開示可能であると判断された場合に、前記個人情報を前記個人情報格納手段から読み出すと共に、前記個人情報取得装置に送信し、

前記個人情報取得装置は、

前記個人情報を前記個人情報提供装置から受信する。

また、上述した目的を解決する更なる見地として、本発明に係る個人情報提供装置は、個人情報を格納する個人情報格納手段と、

前記個人情報の要求を表す個人情報要求メッセージを、個人情報取得装置から受信する個人情報要求受信手段と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、プリファレンス管理装置に送信するプリファレンス要求手段と、

前記プリファレンスを前記プリファレンス管理装置から受信するプリファレンス受信手段と、

前記プリファレンス受信手段によって受信されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する開示可否判断手段と、

前記開示可否判断手段によって開示可能であると判断された場合に、前記個人情報を前記個人情報格納手段から読み出すと共に、前記個人情報取得装置に送信する個人情報送信手段と、

を備える。

また、上述した目的を解決する更なる見地として、本発明に係るプリファレンス管理装置は、

ユーザ端末によって過去に設定された、個人情報提供装置から個人情報取得装置に対する個人情報の開示に関する規定を表すプリファレンスを格納するプリファレンス格納手段と、

前記プリファレンスの要求を表すプリファレンス要求メッセージを、前記個人情報提供装置から受信するプリファレンス要求受信手段と、

前記プリファレンス格納手段に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成する確認用プリファレンス生成手段と、

前記確認用プリファレンスを前記ユーザ端末に提示し、提示した確認用プリファレンスに基づいて設定されたプリファレンスを、前記ユーザ端末から受信するプリファレンス確認手段と、

前記プリファレンス確認手段によって受信された前記プリファレンスを、前記個人情報提供装置に送信するプリファレンス送信手段と、
を備える。

尚、上述した目的は、上述した構成を備える個人情報提供装置、あるいはプリファレンス管理装置の機能を、コンピュータによって実現するコンピュータ・プログラム、及びそのコンピュータ・プログラムが格納されたコンピュータ読み取り可能な記憶媒体によっても達成される。

10

20

30

40

50

【発明の効果】

【0007】

本発明によれば、個人情報保有する装置数が増大しても、その個人情報の開示に関するプリファレンスを設定するユーザの負担を軽減することができる個人情報送受信システム等を提供することができる。

【図面の簡単な説明】

【0008】

【図1】本発明の第1の実施形態としての個人情報送受信システムの構成図である。

【図2】本発明の第1の実施形態における個人情報提供装置のハードウェア構成図である。

10

【図3】本発明の第1の実施形態における個人情報取得装置のハードウェア構成図である。

【図4】本発明の第1の実施形態におけるプリファレンス管理装置のハードウェア構成図である。

【図5】本発明の第1の実施形態におけるユーザ端末のハードウェア構成図である。

【図6】本発明の第1の実施形態における個人情報提供装置の機能ブロック図である。

【図7】本発明の第1の実施形態における個人情報取得装置の機能ブロック図である。

【図8】本発明の第1の実施形態におけるプリファレンス管理装置の機能ブロック図である。

【図9】本発明の第1の実施形態におけるユーザ端末の機能ブロック図である。

20

【図10】本発明の第1の実施形態としての個人情報送受信システムの個人情報送受信動作の概略を説明するフローチャートである。

【図11】本発明の第1の実施形態としての個人情報送受信システムのプリファレンス要求処理を説明するフローチャートである。

【図12】本発明の第1の実施形態としての個人情報送受信システムのプリファレンス確認処理を説明するフローチャートである。

【図13】本発明の第1の実施形態としての個人情報送受信システムの個人情報提供処理を説明するフローチャートである。

【図14】本発明の第2の実施形態としての個人情報送受信システムの構成図である。

【図15】本発明の第2の実施形態における個人情報提供装置の機能ブロック図である。

30

【図16】本発明の第2の実施形態としての個人情報送受信システムにおけるプリファレンス要求処理を説明するフローチャートである。

【図17】本発明の第3の実施形態としての個人情報送受信システムの構成図である。

【図18】本発明の第3の実施形態における個人情報提供装置の機能ブロック図である。

【図19】本発明の第3の実施形態としての個人情報送受信システムにおけるプリファレンス要求処理を説明するフローチャートである。

【図20】本発明の第4の実施形態としての個人情報送受信システムの構成図である。

【図21】本発明の第4の実施形態におけるユーザ端末の機能ブロック図である。

【図22】本発明の第4の実施形態におけるプリファレンス管理装置の機能ブロック図である。

40

【図23】本発明の第4の実施形態としての個人情報送受信システムのプリファレンス変更処理を説明するフローチャートである。

【図24】本発明の第5の実施形態としての個人情報送受信システムの構成図である。

【図25】本発明の第5の実施形態におけるプリファレンス管理装置の機能ブロック図である。

【図26】本発明の第5の実施形態としての個人情報送受信システムの個人情報取得処理を説明するフローチャートである。

【図27】本発明の第5の実施形態としての個人情報送受信システムのプリファレンス確認処理を説明するフローチャートである。

【図28】本発明の第5の実施形態としての個人情報送受信システムの確認用プリファレ

50

ンス推定処理を説明するフローチャートである。

【図 29】本発明の第 6 の実施形態としての携帯電話端末用ショッピングポータルシステムの構成図である。

【図 30】本発明の第 6 の実施形態としての携帯電話端末用ショッピングポータルシステムの動作を説明するシーケンス図である。

【図 31】本発明の第 7 の実施形態としての A S P 基盤システムの構成図である。

【図 32】本発明の第 7 の実施形態としての A S P 基盤システムの動作を説明するシーケンス図である。

【図 33】関連技術の個人情報送受信システムの構成図である。

【図 34】他の関連技術の個人情報送受信システムの構成図である。

【発明を実施するための形態】

【0009】

以下、本発明の実施形態について、図面を参照して詳細に説明する。

(第 1 の実施形態)

本発明の第 1 の実施形態としての個人情報送受信システム 1 の構成を図 1 に示す。図 1 において、個人情報送受信システム 1 は、個人情報提供装置 10 と、個人情報取得装置 20 と、プリファレンス管理装置 30 と、ユーザ端末 40 とを備えている。また、これらの装置は、インターネット、LAN (Local Area Network)、公衆回線網、無線通信網またはこれらの組合せ等によって構成されるネットワーク 9 を介して互いに通信可能に接続されている。

個人情報提供装置 10 は、ユーザの個人情報を管理する装置である。また、個人情報提供装置 10 は、個人情報を他の装置に提供する際の開示条件が規定されたプリファレンスを、プリファレンス管理装置 30 から取得する。また、個人情報提供装置 10 は、取得したプリファレンスに基づいて、個人情報取得装置 20 に対して個人情報を提供する。

個人情報取得装置 20 は、ユーザの個人情報に基づくサービスを提供する装置である。また、個人情報取得装置 20 は、ユーザ端末 40 からのサービスの提供要求に応じて、必要となる個人情報を個人情報提供装置 10 から取得する。また、個人情報取得装置 20 は、取得した個人情報に基づいて、ユーザ端末 40 に対してサービスを提供する。

プリファレンス管理装置 30 は、ユーザの個人情報の開示条件を既定したプリファレンスを管理する装置である。また、プリファレンス管理装置 30 は、個人情報提供装置 10 に対して、個人情報提供装置 10 による個人情報取得装置 20 に対する個人情報の開示条件を既定したプリファレンスを提供する。

ユーザ端末 40 は、個人情報の主体となるユーザによって操作される端末である。また、ユーザ端末 40 は、個人情報取得装置 20 に対して、ユーザの個人情報に基づくサービスの提供を要求する。

なお、図 1 には、説明の便宜上から、各装置をそれぞれ 1 つずつ示しているが、本発明における各装置の数を限定するものではない。

次に、個人情報送受信システム 1 を構成する各装置のハードウェア構成を図 2 ~ 図 5 に示す。

図 2 において、情報提供装置 10 は、ハードウェア資源として、CPU (Central Processing Unit) 1001 と、RAM (Random Access Memory) 1002 と、ROM (Read Only Memory) 1003 と、ハードディスク等の記憶装置 1004 と、ネットワークインタフェース 1005 とを備えたコンピュータである。

図 3 において、情報取得装置 20 は、ハードウェア資源として、CPU 2001 と、RAM 2002 と、ROM 2003 と、ハードディスク等の記憶装置 2004 と、ネットワークインタフェース 2005 とを備えたコンピュータである。

図 4 において、プリファレンス管理装置 30 は、ハードウェア資源として、CPU 3001 と、RAM 3002 と、ROM 3003 と、ハードディスク等の記憶装置 3004 と、ネットワークインタフェース 3005 とを備えたコンピュータである。

10

20

30

40

50

図5において、ユーザ端末40は、ハードウェア資源として、CPU4001と、RAM4002と、ROM4003と、ハードディスク等の記憶装置4004と、ネットワークインタフェース4005と、入力装置4006と、表示装置4007とを備えたコンピュータである。

次に、個人情報送受信システム1の機能ブロック構成を図6～図9に示す。

図6において、個人情報提供装置10は、個人情報格納部101と、個人情報要求受信部102と、プリファレンス要求部103と、プリファレンス受信部104と、開示可否判断部105と、個人情報送信部106と、を備える。

ここで、個人情報提供装置10に関して、図2に示したハードウェア資源と、図6に示した機能ブロックとの関係を述べる。個人情報格納部101は、記憶装置1004によって構成されている。また、個人情報要求受信部102と、プリファレンス要求部103と、プリファレンス受信部104と、個人情報送信部106とは、記憶装置1004またはROM1003に格納されたコンピュータ・プログラム(ソフトウェア・プログラム)を、RAM1002に読み込んで実行するCPU1001、および、ネットワークインタフェース1005によって構成される。また、開示可否判断部105は、記憶装置1004またはROM1003に格納されたコンピュータ・プログラムをRAM1002に読み込んで実行するCPU1001によって構成される。

図7において、個人情報取得装置20は、個人情報要求部201と、個人情報受信部202と、を備える。ここで、個人情報取得装置20に関して、図3に示したハードウェア資源と、図7に示した機能ブロックとの関係を述べる。個人情報要求部201および個人情報受信部202は、記憶装置2004またはROM2003に格納されたコンピュータ・プログラムをRAM2002に読み込んで実行するCPU2001、および、ネットワークインタフェース2005によって構成される。

図8において、プリファレンス管理装置30は、プリファレンス格納部301と、プリファレンス要求受信部302と、確認用プリファレンス生成部303と、プリファレンス確認部304と、プリファレンス送信部305と、を備える。ここで、プリファレンス管理装置30に関して、図4に示したハードウェア資源と、図8に示した機能ブロックとの関係を述べる。プリファレンス格納部301は、記憶装置3004によって構成される。また、プリファレンス要求受信部302と、プリファレンス確認部304と、プリファレンス送信部305とは、記憶装置3004またはROM3003に格納されたコンピュータ・プログラムをRAM3002に読み込んで実行するCPU3001、および、ネットワークインタフェース3005によって構成される。また、確認用プリファレンス生成部303は、記憶装置3004またはROM3003に格納されたコンピュータ・プログラムをRAM3002に読み込んで実行するCPU3001によって構成される。

図9において、ユーザ端末40は、プリファレンス設定部401を備える。ここで、ユーザ端末40に関して、図5に示したハードウェア資源と、図9に示した機能ブロックとの関係を述べる。プリファレンス設定部401は、記憶装置4004またはROM4003に格納されたコンピュータ・プログラムをRAM4002に読み込んで実行するCPU4001、ネットワークインタフェース4005、入力装置4006、および、表示装置4007によって構成される。

なお、各装置の機能ブロックを構成するハードウェア構成は上述の構成に限定されない。

次に、個人情報提供装置10の各機能ブロックについて、図6を用いて説明する。個人情報格納部101は、個人情報を格納している。例えば、個人情報格納部101は、個人情報の主体となるユーザを識別するユーザIDと、その個人情報の種類と、その個人情報の内容とを関連付けた(紐付けした)情報を、個人情報として格納していてもよい。ここで、個人情報の種類とは、氏名、住所、電話番号、クレジットカード番号等といった、個人の属性を表す情報の種類をいう。

個人情報要求受信部102は、個人情報取得装置20から、個人情報要求メッセージRM1を受信する。例えば、個人情報要求メッセージRM1には、要求される個人情報の主

10

20

30

40

50

体であるユーザID、その個人情報の種類、個人情報取得装置20がその個人情報を利用する目的や利用範囲等を表す利用条件、および、要求元の個人情報取得装置20を識別する装置IDをそれぞれ表す情報が含まれていてもよい。

プリファレンス要求部103は、個人情報要求メッセージRM1の受信に応じて、要求された個人情報の開示条件を規定するプリファレンスを要求するプリファレンス要求メッセージRM2を、プリファレンス管理装置30に対して送信する。例えば、プリファレンス要求メッセージRM2には、要求されている個人情報の主体となるユーザID、その個人情報の種類、個人情報取得装置20におけるその個人情報の利用条件、自装置から他の装置への当該個人情報の開示条件、要求元の個人情報取得装置20の装置ID、および、自装置である個人情報提供装置10を識別する装置IDをそれぞれ表す情報が含まれてい

10

てもよい。ここで、自装置から他の装置への個人情報の開示条件とは、例えば、個人情報提供装置10から個人情報取得装置20に対して個人情報を提供する際に利用する通信プロトコル等であってもよい。

プリファレンス受信部104は、プリファレンス管理装置30からプリファレンスを取得する。例えば、プリファレンスには、ユーザID、個人情報の種類、その個人情報の取り扱い条件、個人情報提供装置10の装置ID、個人情報取得装置20の装置ID、ユーザの許諾確認の結果（開示許可または開示不許可）、および、有効期間等が含まれてい

てもよい。ここで、個人情報の取り扱い条件には、例えば、個人情報取得装置20における個人情報の利用目的、保有期間、第三者への提供の有無、管理方法等を表す情報が含まれてい

20

てもよい。また、個人情報の取り扱い条件には、例えば、個人情報を開示する際に利用する通信プロトコルとして「SSL(Secure Socket Layer)通信を用いて個人情報を送信する」等の条件が含まれていてもよい。

開示可否判断部105は、プリファレンス受信部104によって受信されたプリファレンスに基づいて、個人情報取得装置20から要求された個人情報を、個人情報取得装置20に対して開示可能か否かを判断する。具体的には、開示可否判断部105は、取得されたプリファレンスに、開示許可を表す情報が含まれるか否かに基づいて、要求された個人情報を開示可能か否かを判断する。さらに、開示可否判断部105は、取得されたプリファレンスに含まれる個人情報の取り扱い条件と、個人情報要求メッセージRM1に含まれる利用条件とを比較することにより、要求された個人情報を開示可能か否かを判断してもよい。さらに、開示可否判断部105は、取得されたプリファレンスに含まれる有効期間を検証することにより、要求された個人情報を開示可能か否かを判断してもよい。

30

個人情報送信部106は、開示可否判断部105によって開示可能であると判断された場合に、該当する個人情報を、要求元の個人情報取得装置20に送信する。

次に、個人情報取得装置20の各機能ブロックについて、図7を用いて説明する。

個人情報要求部201は、ユーザ端末40から要求されるサービス提供に必要な個人情報の提供を要求する個人情報要求メッセージRM1を、個人情報提供装置10に送信する。例えば、個人情報取得装置20が、サービス提供のためにユーザAのメールアドレスを必要とし、取得する個人情報の利用条件として「製品に関する情報提供を利用目的」としている場合を想定する。この場合、個人情報要求部201は、個人情報要求メッセージRM1に、「ユーザID：A、個人情報の種類：メールアドレス、利用条件：製品に関する情報提供を利用目的とする、個人情報取得装置の装置ID：0001」を含めて個人情報提供装置10に送信する。

40

個人情報受信部202は、個人情報提供装置10から個人情報を受信する。

次に、プリファレンス管理装置30の各機能ブロックについて、図8を用いて説明する。

プリファレンス格納部301は、ユーザ端末40によって現在までに設定されたプリファレンスを格納している。例えば、プリファレンス格納部301は、ユーザID、個人情

50

報の種類、その個人情報の取り扱い条件、個人情報取得装置20の装置ID、個人情報提供装置10の装置ID、ユーザの許諾確認の結果（開示許可または開示不許可）、および、有効期間等を含むプリファレンスを格納していてもよい。

プリファレンス要求受信部302は、個人情報提供装置10からプリファレンス要求メッセージRM2を受信する。

確認用プリファレンス生成部303は、プリファレンス格納部301に格納された過去のプリファレンスと、個人情報提供装置10から受信するプリファレンス要求メッセージRM2とに基づいて、ユーザ端末40に提示する確認用プリファレンスCPを生成する。例えば、確認用プリファレンス生成部303は、プリファレンス格納部301に格納されたプリファレンスのうち、プリファレンス要求メッセージRM2に含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づいて、確認用プリファレンスCPを生成してもよい。

10

この場合、具体的には、確認用プリファレンス生成部303は、プリファレンス要求メッセージRM2に含まれるユーザIDおよび個人情報の種類とそれぞれ同一のユーザIDおよび個人情報の種類を含むプリファレンスを、プリファレンス格納部301から検索する。そして、該当するプリファレンスが検索された場合、確認用プリファレンス生成部303は、検索された過去のプリファレンスに、プリファレンス要求メッセージRM2に含まれる個人情報提供装置10の装置IDおよび個人情報取得装置20の装置IDを適用したプリファレンスを、確認用プリファレンスCPとして生成する。

換言すると、例えば、確認用プリファレンス生成部303は、要求されている個人情報の主体となるユーザと同一のユーザによって、要求されている個人情報の種類と同一種類の個人情報に関して、要求元の個人情報取得装置20以外の個人情報取得装置20に対する開示条件が規定されたプリファレンスに基づいて、確認用プリファレンスCPを生成してもよい。

20

さらに、確認用プリファレンス生成部303は、プリファレンス要求メッセージRM2に含まれる内容をそのまま反映させた確認用プリファレンスCPを生成してもよい。

プリファレンス確認部304は、上述した確認用プリファレンスCPをユーザ端末40に提示し、提示した確認用プリファレンスCPに基づいて設定されたプリファレンスを、ユーザ端末40から受信する。なお、ここで、プリファレンス確認部304は、提示した確認用プリファレンスCPに対する同意または不同意のみが設定されたプリファレンスを受信してもよい。また、プリファレンス確認部304は、提示した確認用プリファレンスCPの一部または全部がカスタマイズされて設定されたプリファレンスを受信してもよい。

30

例えば、確認用プリファレンス生成部303によって、過去のプリファレンスに基づく確認用プリファレンスCPとして、確認用プリファレンスA、および、プリファレンス要求メッセージRM2に含まれる内容をそのまま反映させた確認用プリファレンスBが生成されている場合を想定する。この場合、プリファレンス確認部304は、2つの確認用プリファレンスAおよびBをユーザ端末40に送信することにより提示する。そして、この場合、プリファレンス確認部304は、確認用プリファレンスAおよびBのいずれかがユーザによって許諾されたことを表す情報、あるいは、確認用プリファレンスAまたはBの一部または全部に対するカスタマイズ内容を表す情報を、ユーザ端末40から取得する。

40

ここで、確認用プリファレンスAが許諾されたことを表す情報を取得した場合、プリファレンス確認部304は、過去のプリファレンスに基づく確認用プリファレンスAに、開示許可を表す情報を付加したものを、設定済みのプリファレンスとして取得したことになる。

あるいは、確認用プリファレンスBが許諾されたことを表す情報を取得した場合、プリファレンス確認部304は、プリファレンス要求メッセージRM2の内容をそのまま反映した確認用プリファレンスBに、開示許可を表す情報を付加した情報セットを、設定済みのプリファレンスとして取得したことになる。

あるいは、カスタマイズ内容を表す情報を取得した場合、プリファレンス確認部304

50

は、確認用プリファレンス A および確認用プリファレンス B の内容に、カスタマイズ内容を適用した情報セットを、設定済みのプリファレンスとして取得したことになる。

また、プリファレンス確認部 304 は、受信した設定済みのプリファレンスを、プリファレンス格納部 301 に格納する。

プリファレンス送信部 305 は、プリファレンス確認部 304 によって受信された設定済みのプリファレンスを、個人情報提供装置 10 に送信する。

なお、プリファレンス送信部 305 は、プリファレンスを要求した個人情報提供装置 10 から、個人情報の要求元である個人情報取得装置 20 に対して、個人情報を提供可能であると判断できる場合にのみ、プリファレンスを個人情報提供装置 10 に送信するようにしてもよい。この場合、プリファレンス送信部 305 は、該当する個人情報提供装置 10 から該当する個人情報取得装置 20 に対して個人情報を提供可能ではないと判断した場合、エラー通知メッセージを送信してもよい。

次に、ユーザ端末 40 の各機能ブロックについて、図 9 を用いて説明する。プリファレンス設定部 401 は、プリファレンス管理装置 30 から提示される上述した確認用プリファレンス CP に基づいて、個人情報提供装置 10 から個人情報取得装置 20 への個人情報の提供に関するプリファレンスを設定する。そして、プリファレンス設定部 401 は、設定したプリファレンスを、プリファレンス管理装置 30 に送信する。

具体的には、プリファレンス設定部 401 は、プリファレンス管理装置 30 から提示される上述した確認用プリファレンス CP を表示装置 4007 に表示する。そして、プリファレンス設定部 401 は、入力装置 4006 を介して、確認用プリファレンス CP に基づく設定内容を取得する。確認用プリファレンス CP に基づく設定内容とは、例えば、複数の確認用プリファレンス CP のいずれが許諾されたかを表す情報や、確認用プリファレンス CP の一部または全部がカスタマイズされた内容を表す情報である。そして、プリファレンス設定部 401 は、入力装置 4006 を介して取得した設定内容を、プリファレンス管理装置 30 に送信する。

以上のような構成を有する個人情報送受信システム 1 の動作について、図 10 ~ 図 13 に示すフローチャートを参照して説明する。

図 10 は、個人情報送受信システム 1 の個人情報送受信動作の概略を説明するフローチャートである。図 10 において、まず、個人情報取得装置 20 は、個人情報提供装置 10 に対して、個人情報要求メッセージ RM1 を送信する (ステップ A1)。

次に、個人情報要求メッセージ RM1 を受信した個人情報提供装置 10 は、その個人情報要求メッセージ RM1 に応じたプリファレンスを要求するためのプリファレンス要求メッセージ RM2 を、プリファレンス管理装置 30 に対して送信する (ステップ A2)。係るステップ A2 におけるプリファレンス要求処理の詳細については、図 11 を参照して後述する。

次に、プリファレンス要求メッセージ RM2 を受信したプリファレンス管理装置 30 は、ユーザ端末 40 に対して、確認用プリファレンス CP の確認を行うことにより、設定済みのプリファレンスを取得する。そして、プリファレンス管理装置 30 は、取得したプリファレンスを個人情報提供装置 10 に対して送信する (ステップ A3)。係るステップ A3 におけるプリファレンス確認処理の詳細については、図 12 を参照して後述する。

次に、プリファレンスを取得した個人情報提供装置 10 は、取得したプリファレンスの内容に基づいて、該当する個人情報を個人情報取得装置 20 に対して提供可能であると判断できる場合、個人情報格納部 101 に格納している個人情報の中から、該当する個人情報を、個人情報取得装置 20 に対して送信する (ステップ A4)。係るステップ A4 における個人情報提供処理の詳細については、図 13 を参照して後述する。

以上で、個人情報送受信システム 1 の個人情報送受信動作の概略の説明を終了する。

次に、ステップ A2 における個人情報提供装置 10 のプリファレンス要求処理について、図 11 に示すフローチャートを用いて説明する。図 11 に示すプリファレンス要求処理は、個人情報提供装置 10 の CPU 1001 が図 2 に示すハードウェア資源を利用してコンピュータ・プログラムを実行することによって実現する処理手順を表す。

10

20

30

40

50

まず、個人情報提供装置 10 において、個人情報要求受信部 102 は、個人情報要求メッセージ R M 1 を個人情報取得装置 20 から受信する（ステップ B 1）。この個人情報要求メッセージ R M 1 には、例えば、要求されている個人情報の主体であるユーザ ID、その個人情報の種類、その個人情報の利用目的や利用範囲等の利用条件、および、要求元の個人情報取得装置 20 の装置 ID 等が含まれていてもよい。

次に、プリファレンス要求部 103 は、ステップ S B 1 にて受信した個人情報要求メッセージ R M 1 に基づいてプリファレンス要求メッセージ R M 2 を作成し、作成したプリファレンス要求メッセージ R M 2 を、プリファレンス管理装置 30 に対して送信する（ステップ B 2）。このプリファレンス要求メッセージ R M 2 には、例えば、個人情報要求メッセージ R M 1 に含まれていた各種の情報に加えて、個人情報提供装置 10 から個人情報取得装置 20 に対して個人情報を開示する開示条件、および、個人情報提供装置 10 の装置 ID 等が含まれていてもよい。

以上で、図 10 のステップ A 2 におけるプリファレンス要求処理の説明を終了する。

次に、ステップ A 3 におけるプリファレンス管理装置 30 のプリファレンス確認処理について、図 12 に示すフローチャートを用いて説明する。図 12 に示すプリファレンス確認処理は、プリファレンス管理装置 30 の CPU 3001 が図 4 に示すハードウェア資源を利用してコンピュータ・プログラムを実行することによって実現する処理手順を表す。

まず、プリファレンス管理装置 30 において、プリファレンス要求受信部 302 は、プリファレンス要求メッセージ R M 2 を、個人情報提供装置 10 から受信する（ステップ C 1）。このプリファレンス要求メッセージ R M 2 には、上述のように、例えば、要求される個人情報の主体であるユーザ ID、個人情報提供装置 10 および個人情報取得装置 20 における利用条件や開示条件、個人情報提供装置 10 の装置 ID、および、個人情報取得装置 20 の装置 ID 等が記載されている。

次に、確認用プリファレンス生成部 303 は、プリファレンス格納部 301 に格納されている過去のプリファレンスと、プリファレンス要求メッセージ R M 2 とに基づいて、確認用プリファレンス C P を生成する（ステップ C 2）。例えば、確認用プリファレンス生成部 303 は、プリファレンス要求メッセージ R M 2 に含まれていたユーザ ID および個人情報の種類と同一のユーザ ID および個人情報の種類を含むプリファレンスに基づいて、確認用プリファレンス C P を生成する。さらに、確認用プリファレンス生成部 303 は、プリファレンス要求メッセージ R M 2 の内容をそのまま反映した確認用プリファレンス C P を生成してもよい。

なお、該当する過去のプリファレンスがプリファレンス格納部 301 に格納されていない場合、確認用プリファレンス生成部 303 は、プリファレンス要求メッセージ R M 2 の内容をそのまま反映した確認用プリファレンス C P のみを生成してもよい。

次に、プリファレンス確認部 304 は、ユーザ端末 40 に対して、確認用プリファレンス C P を提示する（ステップ C 3）。次に、プリファレンス確認部 304 は、ステップ C 3 で提示した確認用プリファレンス C P に基づいて設定されたプリファレンスを、ユーザ端末 40 から受信する（ステップ C 4）。このとき、プリファレンス確認部 304 は、例えば、ステップ C 3 で提示した確認用プリファレンス C P のいずれかに対する許諾を表す情報、または、確認用プリファレンス C P がカスタマイズされた設定内容等を取得し、取得した内容を、確認用プリファレンス C P に適用することにより、設定済みのプリファレンスとしてもよい。

なお、確認用プリファレンス C P のいずれもが許諾されず、カスタマイズもされない場合、確認用プリファレンス生成部 303 が、利用条件および開示条件をより厳しくした確認用プリファレンス C P を再生成し、プリファレンス確認部 304 が、再生成された確認用プリファレンス C P を用いて、ユーザ端末 40 に対する再確認処理を行ってもよい。

また、プリファレンス確認部 304 は、確認用プリファレンス C P のいずれもが許諾されず、カスタマイズもされない場合、設定済みのプリファレンスを受信できなかったこととする。

設定済みのプリファレンスを受信した場合（ステップ C 5 で Yes）、プリファレンス

10

20

30

40

50

確認部 304 は、受信したプリファレンスを、プリファレンス格納部 301 に登録する（ステップ C6）。そして、プリファレンス送信部 305 は、受信したプリファレンスを含めた応答メッセージを作成する（ステップ C7）。

一方、設定済みのプリファレンスを受信できなかった場合（ステップ C5 で No）、プリファレンス送信部 305 は、エラー通知を含む応答メッセージを生成する（ステップ C8）。次に、プリファレンス送信部 305 は、ステップ C7 またはステップ C8 で生成した応答メッセージを、個人情報提供装置 10 に対して送信する（ステップ C9）。

以上で、ステップ A3 におけるプリファレンス確認処理の説明を終了する。

次に、ステップ A4 における個人情報提供装置 10 の個人情報提供処理について、図 13 に示すフローチャートを用いて説明する。図 13 に示す個人情報提供処理は、個人情報提供装置 10 の CPU 1001 が図 2 に示すハードウェア資源を利用してコンピュータ・プログラムを実行することによって実現する処理手順を表す。

まず、個人情報提供装置 10 において、プリファレンス受信部 104 は、プリファレンス管理装置 30 より応答メッセージを取得する（ステップ D1）。次に、開示可否判断部 105 は、取得した応答メッセージに含まれるプリファレンスを検証する（ステップ D2）。

例えば、開示可否判断部 105 は、以下の事項等を検証する。

- 応答メッセージにプリファレンスが含まれているか否か、
- 応答メッセージに含まれるプリファレンスに含まれる取り扱い条件を個人情報要求メッセージ RM1 に含まれる利用条件が満たすか否か、
- 開示許可を表す情報が含まれているか否か、および、
- プリファレンスに含まれる有効期間。

次に、開示可否判断部 105 は、検証結果に基づいて、個人情報提供装置 10 から個人情報取得装置 20 に個人情報を提供できるか否かを判断する（ステップ D3）。個人情報を提供可能と判断された場合、個人情報送信部 106 は、個人情報格納部 101 から該当する個人情報を取得する（ステップ D4）。次に、個人情報送信部 106 は、ステップ D4 で取得された個人情報を含む応答メッセージを生成する（ステップ D5）。

一方、ステップ D3 において、個人情報提供装置 10 から個人情報取得装置 20 に個人情報を提供できないと判断した場合、個人情報送信部 106 は、エラー通知を含む応答メッセージを生成する（ステップ D6）。

次に、個人情報送信部 106 は、ステップ D5 または D6 で作成した応答メッセージを、個人情報取得装置 20 へ送信する（ステップ D7）。

以上で、ステップ A4 における個人情報提供処理の説明を終了する。

なお、図 12 のステップ C5 において、プリファレンス管理装置 30 は、プリファレンスを受信したと判断した場合、さらに、受信されたプリファレンスに基づいて個人情報提供装置 10 から個人情報取得装置 20 に対して個人情報を提供可能か否かを判断するようにしてもよい。これにより、プリファレンス管理装置 30 および個人情報提供装置 10 が、それぞれステップ C5 およびステップ D3 において開示可否判断処理を行うことになり、開示可否判断の確実性を向上することができる。

また、図 12 のステップ C2 において、プリファレンス管理装置 30 は、プリファレンス要求メッセージ RM2 に含まれる情報が許諾されていることを表すプリファレンスが、プリファレンス格納部 301 に格納されていた場合、ステップ C2 ~ C6 の処理を省略してもよい。この場合、プリファレンス管理装置 30 は、該当するプリファレンスをプリファレンス格納部 301 から取得し、取得したプリファレンスについて、ステップ C7 ~ C8 を実行する。これにより、ユーザ端末 40 に対してプリファレンスを確認する処理を省略することができる。

次に、本発明の第 1 の実施形態の効果について述べる。

第 1 の実施形態に係る個人情報送受信システムは、個人情報を保有する装置数が増大しても、個人情報の開示に関するプリファレンスを設定するユーザの負担を軽減（最小限に抑制）することができる。

10

20

30

40

50

その理由は、プリファレンス管理装置 30 が、個人情報提供装置 10 から個人情報取得装置 20 に対する個人情報の開示に関するプリファレンスをユーザ端末 40 から取得し、個人情報提供装置 10 が、プリファレンス管理装置 30 によってユーザ端末 40 から取得されたプリファレンスに基づいて、個人情報取得装置 20 に個人情報を提供するためである。

すなわち、第 1 の実施形態としての個人情報送受信システムでは、プリファレンス管理装置 30 がプリファレンスを集中管理するので、ユーザは、個人情報を保有する装置ごとに個人情報の開示に関するプリファレンスを設定する必要がない。よって、本実施形態よれば、個人情報の開示に関するプリファレンスを設定するユーザの負担を軽減することができる。

また、本実施形態に係る上記の効果を楽しむ更なる理由は、プリファレンス管理装置 30 の確認用プリファレンス生成部 303 が、プリファレンス格納部 301 に格納された過去のプリファレンスに基づいて、確認用プリファレンス CP を生成し、生成した確認用プリファレンス CP をユーザ端末 40 に提示するからである。このため、ユーザは、過去に設定したプリファレンスを容易に確認することができ、個人情報を保有する複数の装置における個人情報の開示に関して、複数のプリファレンスを矛盾しないように設定することが容易となるからである。

(第 2 の実施形態)

次に、上述した本発明の第 1 の実施形態を基礎とする第 2 の実施形態について、図面を参照して詳細に説明する。なお、本実施形態の説明において参照する各図面において、本発明の第 1 の実施形態と同一の構成および同様に動作するステップには同一の符号を付して、本実施形態における詳細な説明を省略する。

まず、第 2 の実施形態としての個人情報送受信システム 2 の構成を図 14 に示す。図 14 において、個人情報送受信システム 2 は、第 1 の実施形態における個人情報送受信システム 1 と比較して、個人情報提供装置 10 に替えて個人情報提供装置 50 を備える点が異なる。本実施形態において、個人情報提供装置 50 は、図 2 に示す個人情報提供装置 10 と同様なハードウェア資源を備えることとする。

個人情報提供装置 50 の機能ブロックの構成を図 15 に示す。図 15 において、個人情報提供装置 50 は、第 1 の実施形態における個人情報提供装置 10 と比較して、プリファレンス管理装置情報格納部 507 と、プリファレンス要求先決定部 508 とをさらに備える点が異なる。

プリファレンス管理装置情報格納部 507 は、プリファレンス管理装置 30 を表す情報を格納している。例えば、プリファレンス管理装置情報格納部 507 は、個人情報の主体であるユーザを識別するユーザ ID と、そのユーザ ID のユーザによって設定されるプリファレンスを管理するプリファレンス管理装置 30 を識別する装置 ID と、プリファレンス要求メッセージ RM2 の送付先の URL とを関連付けた情報を格納していてもよい。

プリファレンス要求先決定部 508 は、個人情報要求受信部 102 によって受信した個人情報要求メッセージ RM1 に応じたプリファレンス要求メッセージ RM2 の送信先となるプリファレンス管理装置 30 を、プリファレンス管理装置情報格納部 507 に基づいて決定する。例えば、プリファレンス要求先決定部 508 は、個人情報要求メッセージ RM1 に含まれるユーザ ID に関連付けられた装置 ID のプリファレンス管理装置 30 をプリファレンス要求メッセージ RM2 の送信先として決定してもよい。

以上のように構成された個人情報送受信システム 2 のプリファレンス要求処理について、図 16 を参照して説明する。図 16 に示すプリファレンス要求処理は、個人情報提供装置 50 の CPU 1001 が図 2 に示すハードウェア資源を利用してコンピュータ・プログラムを実行することによって実現する処理手順を表す。なお、個人情報送受信システム 2 の個人情報送受信動作の概略、プリファレンス確認処理、および、個人情報提供処理については、図 10、図 12、図 13 を参照して上述した第 1 の実施形態としての個人情報送受信システム 1 と同様であるため、本実施形態における説明を省略する。

図 16 において、まず、個人情報提供装置 50 の個人情報要求受信部 102 は、個人情

10

20

30

40

50

報要求メッセージ R M 1 を個人情報取得装置 2 0 から受信する (ステップ B 1)。次に、プリファレンス要求先決定部 5 0 8 は、プリファレンス管理装置情報格納部 5 0 7 を参照して、ステップ B 1 で受信した個人情報要求メッセージ R M 1 に応じたプリファレンス要求メッセージ R M 2 を送信すべきプリファレンス管理装置 3 0 を決定する (ステップ K 1)。

例えば、プリファレンス要求先決定部 5 0 8 は、個人情報要求メッセージ R M 1 に記載されているユーザ ID に関連付けられたプリファレンス管理装置 3 0 の装置 ID および送付先 URL を取得する。

次に、プリファレンス要求部 1 0 3 は、プリファレンス要求メッセージ R M 2 を作成し、ステップ B 2 で決定した要求先に対して送信する (ステップ B 2)。

以上で、プリファレンス要求処理の説明を終了する。

次に、本発明の第 2 の実施形態の効果について述べる。

第 2 の実施形態に係る個人情報送受信システム 2 は、個人情報の開示に関するプリファレンスを設定するユーザの負担を、さらに軽減することができる。その理由は、個人情報提供装置 5 0 が、プリファレンス管理装置 3 0 に関する情報を格納しておき、格納しておいた情報に基づいて、個人情報要求メッセージ R M 1 に応じたプリファレンスの要求先を決定するからである。これにより、本実施形態に係る個人情報送受信システム 2 は、複数のプリファレンス管理装置 3 0 が管理するプリファレンスの中から、ユーザ端末 4 0 に提示する確認用プリファレンス CP を生成する際に、参照するプリファレンスとしてより適したものを選択することができるからである。

(第 3 の実施形態)

次に、上述した第 1 及び第 2 の実施形態を基礎とする第 3 の実施形態について、図面を参照して詳細に説明する。なお、本実施形態の説明において参照する各図面において、第 1 及び第 2 の実施形態と同一の構成および同様に動作するステップには同一の符号を付して本実施形態における詳細な説明を省略する。

まず、第 3 の実施形態に係る個人情報送受信システム 3 の構成を図 1 7 に示す。図 1 7 において、個人情報送受信システム 3 は、第 2 の実施形態における個人情報送受信システム 2 と比較して、個人情報提供装置 5 0 に替えて個人情報提供装置 6 0 を備える点異なる。本実施形態において、個人情報提供装置 6 0 は、図 2 に示す個人情報提供装置 1 0 と同様なハードウェア資源を備えることとする。

個人情報提供装置 6 0 の機能ブロックの構成を図 1 8 に示す。図 1 8 において、個人情報提供装置 6 0 は、第 1 及び第 2 の実施形態における個人情報提供装置 5 0 と比較して、プリファレンス要求部 1 0 3 に替えてプリファレンス要求部 6 0 3 と、開示可否判断部 1 0 5 に替えて開示可否判断部 6 0 5 とを備え、更に、プリファレンス保管部 6 0 9 と、プリファレンス取得部 6 1 0 とを備える点異なる。

プリファレンス保管部 6 0 9 は、プリファレンス受信部 1 0 4 によってプリファレンス管理装置 3 0 から取得したプリファレンスを保管する。プリファレンス取得部 6 1 0 は、個人情報要求メッセージ R M 1 によって要求される個人情報を個人情報提供装置 6 0 から個人情報取得装置 2 0 に提供することに関するプリファレンスが、プリファレンス保管部 6 0 9 に保管されている場合、プリファレンス保管部 6 0 9 に保管されているプリファレンスを取得する。

例えば、プリファレンス取得部 6 1 0 は、個人情報要求メッセージ R M 1 に含まれるユーザ ID、個人情報の種類、利用条件、個人情報取得装置 2 0 の装置 ID 等と同一の情報を含むプリファレンスが、プリファレンス保管部 6 0 9 に保管されているか否かを判断する。そして、プリファレンス取得部 6 1 0 は、個人情報要求メッセージ R M 1 に含まれる各種情報と同一の情報を含むプリファレンスが、プリファレンス保管部 6 0 9 に保管されている場合、そのプリファレンスを取得する。

また、プリファレンス取得部 6 1 0 は、個人情報要求メッセージ R M 1 に含まれる各種情報と同一の情報を含むプリファレンスが、プリファレンス保管部 6 0 9 に保管されていない場合、プリファレンス要求メッセージ R M 2 の送信が必要であることをプリファレン

10

20

30

40

50

ス要求部 603 に通知する。

プリファレンス要求部 603 は、プリファレンス要求メッセージ R M 2 の送信が必要であることがプリファレンス取得部 610 から通知された場合、上述した第 2 の実施形態におけるプリファレンス要求部 103 と同様に、プリファレンス要求メッセージ R M 2 をプリファレンス管理装置 30 に送信する。プリファレンス要求部 603 は、プリファレンス要求メッセージ R M 2 の送信が必要であることが通知されない場合、プリファレンス要求メッセージ R M 2 を送信しない。

開示可否判断部 605 は、プリファレンス取得部 610 によってプリファレンス保管部 609 からプリファレンスが取得された場合に、そのプリファレンスを検証する。例えば、開示可否判断部 605 は、プリファレンス保管部 609 から取得されたプリファレンスの有効期間を確認し、そのプリファレンスが有効であるか否かを判断することにより検証を行ってもよい。また、開示可否判断部 605 は、プリファレンス取得部 610 によってプリファレンス保管部 609 から取得したプリファレンスが有効でない場合、プリファレンス要求メッセージ R M 2 の送信が必要であることをプリファレンス要求部 603 に通知する。

以上のように構成された個人情報送受信システム 3 のプリファレンス要求動作について、図 19 を参照して説明する。図 19 に示すプリファレンス要求処理は、個人情報提供装置 60 の CPU 1001 が図 2 に示すハードウェア資源を利用してコンピュータ・プログラムを実行することによって実現する処理手順を表す。なお、個人情報送受信システム 3 の個人情報送受信動作の概略、プリファレンス確認処理、および、個人情報提供処理については、図 10、図 12、図 13 を参照して説明した第 1 の実施形態に係る個人情報送受信システム 1 と同様であるため、本実施形態における説明を省略する。

図 19 において、まず、個人情報提供装置 60 の個人情報要求受信部 102 は、個人情報要求メッセージ R M 1 を受信する (ステップ B 1)。次に、プリファレンス取得部 610 は、ステップ B 1 で受信した個人情報要求メッセージ R M 1 によって要求される個人情報を個人情報提供装置 60 から個人情報取得装置 20 に提供することに関するプリファレンスを、プリファレンス保管部 609 から検索する (ステップ E 1)。

例えば、プリファレンス取得部 610 は、ステップ B 1 で取得した個人情報要求メッセージ R M 1 に記載されているユーザ ID、個人情報の種類、利用条件、個人情報取得装置 20 の装置 ID と同一の情報が含まれるプリファレンスを検索する。すなわち、プリファレンス取得部 610 は、個人情報要求メッセージ R M 1 に含まれる内容に基づく個人情報の開示が、該当するユーザによって過去に許諾されていたことを表すプリファレンスを、プリファレンス保管部 609 から検索する。

ここで、該当するプリファレンスが検索されなかった場合 (ステップ E 2 で No)、プリファレンス要求先決定部 508 は、プリファレンス管理装置情報格納部 507 に基づいて、プリファレンスの要求先となるプリファレンス管理装置 30 を決定する (ステップ K 1)。そして、プリファレンス要求部 603 は、プリファレンス要求メッセージ R M 2 を、ステップ K 1 で決定したプリファレンス管理装置 30 へ送信する (ステップ B 2)。一方、該当するプリファレンスが検索された場合 (ステップ E 2 で Yes)、プリファレンス取得部 610 は、検索されたプリファレンスを取得する (ステップ E 3)。

次に、開示可否判断部 605 は、ステップ E 3 で取得したプリファレンスを検証することにより (ステップ E 4)、このプリファレンスに基づいて個人情報提供装置 10 から個人情報取得装置 20 に個人情報を提供可能であるか否かを判断する (ステップ E 5)。提供可能でないと判断された場合、個人情報提供装置 60 は、ステップ K 1 およびステップ B 2 の処理を行うことにより、プリファレンス要求メッセージ R M 2 を送信する。

一方、ステップ E 5 において、提供可能であると判断された場合、個人情報提供装置 60 のプリファレンス要求処理は終了し、図 13 に示した個人情報提供処理のステップ D 4 以降に処理が進められる。

以上で、プリファレンス要求処理の説明を終了する。

次に、本発明の第 3 の実施形態の効果について述べる。

10

20

30

40

50

第3の実施形態に係る個人情報送受信システム3は、第1及び第2の実施形態と同様に、個人情報を保有する装置数が増大してもプリファレンスを設定する際のユーザの負担を軽減することができる。更に、本実施形態によれば、プリファレンス管理装置30に対して、プリファレンスを要求する個人情報提供装置60の負荷を軽減することができる。その理由は、個人情報提供装置60が、プリファレンス管理装置30から過去に取得したプリファレンスを保管しておき、保管したプリファレンスに基づいて提供可能な個人情報を個人情報取得装置から要求された場合には、プリファレンス管理装置30にプリファレンス要求メッセージRM2を送信しないからである。

(第4の実施形態)

次に、上述した第1の実施形態を基礎とする第4の実施形態について、図面を参照して詳細に説明する。なお、本実施形態の説明において参照する各図面において、本発明の第1の実施形態と同一の構成および同様に動作するステップには同一の符号を付して本実施形態における詳細な説明を省略する。

まず、本発明の第4の実施形態としての個人情報送受信システム4の構成を図20に示す。図20において、個人情報送受信システム4は、本発明の第1の実施形態としての個人情報送受信システム1と比較して、プリファレンス管理装置30に替えてプリファレンス管理装置70と、ユーザ端末40に替えてユーザ端末80とを備える点異なる。

ユーザ端末80の機能ブロックの構成を図21に示す。図21において、ユーザ端末80は、本発明の第1の実施形態におけるユーザ端末40と比較して、プリファレンス変更内容設定部802をさらに備える点異なる。

ここで、ユーザ端末80は、図5に示すユーザ端末40と同様なハードウェア資源を備えることとする。プリファレンス変更内容設定部802は、記憶装置4004またはROM4003に格納されたコンピュータ・プログラムをRAM4002に読み込んで実行するCPU4001、ネットワークインタフェース4005、入力装置4006、および、表示装置4007によって構成される。なお、プリファレンス変更内容設定部802を構成するハードウェア構成は上述の構成に限定されない。

プリファレンス変更内容設定部802は、設定済みのプリファレンスに対する変更内容を設定し、設定変更されたプリファレンスをプリファレンス管理装置70に送信する。例えば、プリファレンス変更内容設定部802は、入力装置4006を介して指定されたユーザIDを含むプリファレンスの一覧をプリファレンス管理装置70から取得し、取得したプリファレンスの一覧を表示装置4007に表示する。そして、プリファレンス変更内容設定部802は、入力装置4006を介して一覧から選択されたプリファレンスの内容をプリファレンス管理装置70から取得し、取得した内容を表示装置4007に表示する。そして、この場合、プリファレンス変更内容設定部802は、表示したプリファレンスに対する変更内容を入力装置4006を介して取得し、取得した変更内容をプリファレンス管理装置70に送信する。

例えば、過去に「ユーザID：A、個人情報の種類：メールアドレス、個人情報の取り扱い条件：ショッピングポータル登録店舗サイトのみに開示する、個人情報取得装置：ID0001、個人情報提供装置：ID0002」というプリファレンスが設定されていた場合を想定する。

この場合、変更内容設定部802は、例えば、このプリファレンスの個人情報の取り扱い条件を「ショッピングポータル登録店舗のうち音楽コンテンツを扱うサイトのみに開示する」といった変更内容を入力装置4006を介して取得する。あるいは、変更内容設定部802は、取り扱い条件を「開示不可」とする変更内容を取得する場合もある。そして、変更内容設定部802は、取得した変更内容をプリファレンス管理装置70に送信する。

プリファレンス管理装置70の機能ブロックの構成を図22に示す。図22において、プリファレンス管理装置70は、第1の実施形態におけるプリファレンス管理装置30と比較して、変更内容取得部706と、プリファレンス更新部707と、変更通知生成部708と、変更通知送信部709とをさらに備える点異なる。

10

20

30

40

50

ここで、プリファレンス管理装置 70 は、図 4 に示すプリファレンス管理装置 30 と同様なハードウェア資源を備えることとする。変更内容取得部 706 および変更通知送信部 709 は、記憶装置 3004 または ROM 3003 に記憶されたコンピュータ・プログラムを RAM 3002 に読み込んで実行する CPU 3001、および、ネットワークインタフェース 3005 によって構成される。また、プリファレンス更新部 707 および変更通知生成部 708 は、記憶装置 3004 または ROM 3003 に記憶されたコンピュータ・プログラムを RAM 3002 に読み込んで実行する CPU 3001 によって構成される。なお、プリファレンス管理装置 70 の各機能ブロックを構成するハードウェア構成は上述の構成に限定されない。

変更内容取得部 706 は、過去に設定されたプリファレンスに対する変更内容を、ユーザ端末 80 から取得する。変更内容は、例えば、上述のように、プリファレンスの取り扱い条件に対する変更や、有効期間の変更等であってもよい。

プリファレンス更新部 707 は、変更内容取得部 706 によって取得された変更内容に基づいて、プリファレンス格納部 301 に格納されたプリファレンスを更新する。

プリファレンス変更通知生成部 708 は、プリファレンス更新部 707 によって更新されたプリファレンスに関連する個人情報提供装置 10 および個人情報取得装置 20 を特定し、特定した個人情報提供装置 10 および個人情報取得装置 20 に対するプリファレンス変更通知を生成する。例えば、プリファレンス変更通知生成部 708 は、更新前のプリファレンスを過去に送信した個人情報提供装置 10、および、更新前のプリファレンスに記載された開示先の個人情報取得装置 20 を、変更通知先として特定する。なお、プリファレンス変更通知生成部 708 は、更新により取り扱い条件が厳しくなった場合にのみ変更通知を生成し、緩くなった場合には変更通知を生成しなくてもよい。

プリファレンス変更通知送信部 709 は、プリファレンス変更通知生成部 708 によって特定された個人情報提供装置 10 および個人情報取得装置 20 に対して、プリファレンス変更通知をそれぞれ送信する。

以上のように構成された個人情報送受信システム 4 のプリファレンス更新動作について、図 23 を参照して説明する。なお、個人情報送受信システム 4 の個人情報送受信動作の概略、プリファレンス要求処理、プリファレンス確認処理、および、個人情報提供処理については、図 10 ~ 図 13 を参照して説明した本発明の第 1 の実施形態としての個人情報送受信システム 1 と同様であるため、本実施形態における説明を省略する。

図 23 において、まず、プリファレンス管理装置 70 の変更内容取得部 706 は、ユーザ端末 80 の変更内容設定部 802 からプリファレンスの変更内容を取得する（ステップ F1）。次に、プリファレンス更新部 707 は、変更内容に基づいて、プリファレンス格納部 301 に格納されたプリファレンスを更新する（ステップ F2）。

次に、プリファレンス変更通知生成部 708 は、ステップ F1 で取得された変更内容に基づいて、他の装置に対してプリファレンスの変更を通知する必要があるか否かを判断する（ステップ F3）。例えば、プリファレンス変更通知生成部 708 は、ステップ F1 で取得された変更内容に含まれる個人情報の取り扱い条件が、更新前のプリファレンスに含まれる取り扱い条件より厳しい場合、他の装置に対してプリファレンスの変更を通知する必要があると判断する。

ステップ F3 において、プリファレンスを変更する必要があると判断した場合、個人情報送受信システム 4 は、プリファレンス更新処理を終了する。一方、ステップ F3 において、プリファレンスを変更する必要があると判断した場合、プリファレンス変更通知生成部 708 は、プリファレンス変更通知を送付する装置を決定する（ステップ F4）。

例えば、プリファレンス変更通知生成部 708 は、更新前のプリファレンスを過去に送信した個人情報提供装置 10 や、更新前のプリファレンスにおいて個人情報の提供先として規定された個人情報取得装置 20 等を、プリファレンス変更通知を送付する装置として決定する。

次に、プリファレンス変更通知生成部 708 は、プリファレンス変更通知メッセージを生成する（ステップ F5）。例えば、プリファレンス変更通知メッセージには、ステップ

10

20

30

40

50

F 1 で取得した変更内容と、更新前のプリファレンスとが含まれていてもよい。

次に、変更通知送信部 7 0 9 は、プリファレンス変更通知メッセージを、ステップ F 4 にて決定した装置にそれぞれ送信する（ステップ F 6）。

以上で、個人情報送受信システム 4 は、プリファレンス更新処理を終了する。

次に、本発明の第 4 の実施形態の効果について述べる。

第 4 の実施形態に係る個人情報送受信システム 4 は、個人情報を保有する装置数が増大しても、個人情報の開示に関するプリファレンスを更新する際のユーザの負担を軽減することができる。その理由は、プリファレンス管理装置 7 0 がプリファレンスの変更内容を取得した場合、プリファレンス格納部 3 0 1 に格納されたプリファレンスを更新するとともに、該当するプリファレンスに関連する他の装置（個人情報提供装置 1 0 や個人情報取得装置 2 0）に対して、変更通知を送付するからである。このため、本実施形態によれば、ユーザは、個人情報を保有する装置ごとにプリファレンスの更新を行う必要がない。さらに、本実施形態によれば、プリファレンスが更新されても、個人情報提供装置 1 0 および個人情報取得装置 2 0 は、一貫したプリファレンスに基づいて個人情報を送受信することができる。

10

（第 5 の実施形態）

次に、上述した第 1 の実施形態を基礎とする第 5 の実施形態について、図面を参照して詳細に説明する。なお、本実施形態の説明において参照する各図面において、第 1 の実施形態と同一の構成および同様に動作するステップには同一の符号を付して本実施形態における詳細な説明を省略する。

20

まず、第 5 の実施形態に係る個人情報送受信システム 5 の構成を図 2 4 に示す。図 2 4 において、個人情報送受信システム 5 は、第 1 の実施形態における個人情報送受信システム 1 と比較して、プリファレンス管理装置 3 0 に替えてプリファレンス管理装置 9 0 を備える点異なる。

プリファレンス管理装置 9 0 の機能ブロックの構成を図 2 5 に示す。図 2 5 において、プリファレンス管理装置 9 0 は、第 1 の実施形態におけるプリファレンス管理装置 3 0 と比較して、連携装置情報格納部 9 1 0 と、取扱情報格納部 9 1 1 と、取扱情報取得部 9 1 2 と、確認用プリファレンス推定部 9 1 3 と、をさらに備える点異なる。

ここで、ファレンス管理装置 9 0 は、図 4 に示すファレンス管理装置 3 0 と同様なハードウェア資源を備えることとする。連携装置情報格納部 9 1 0 および取扱情報格納部 9 1 1 は、記憶装置 3 0 0 4 によって構成される。また、取扱情報取得部 9 1 2 および確認用プリファレンス推定部 9 1 3 は、コンピュータ・プログラムを R A M 3 0 0 2 に読み込んで実行する C P U 3 0 0 1、および、ネットワークインタフェース 3 0 0 5 によって構成される。なお、プリファレンス管理装置 9 0 の各機能ブロックを構成するハードウェア構成は上述の構成に限定されない。

30

連携装置情報格納部 9 1 0 は、プリファレンス管理装置 9 0 が連携する連携装置に関する情報を格納する。ここで、連携装置とは、例えば、プリファレンス管理装置 9 0 からのプリファレンス提供先としてあらかじめ登録された個人情報提供装置 1 0 であってもよい。また、連携装置とは、例えば、プリファレンス管理装置 9 0 によって管理されるプリファレンスによって個人情報の開示先として許可される個人情報取得装置 2 0 であってもよい。また、連携装置に関する情報には、例えば、これらの個人情報提供装置 1 0 または個人情報取得装置 2 0 の装置 I D、および、装置の U R L 等が含まれていてもよい。

40

連携装置情報格納部 9 1 0 は、あらかじめ登録されることにより連携装置に関する情報を格納してもよい。あるいは、連携装置情報格納部 9 1 0 は、プリファレンス要求メッセージ R M 2 に含まれる個人情報提供装置 1 0 および個人情報取得装置 2 0 に関する情報を連携装置情報として格納してもよい。あるいは、ユーザ端末 4 0 からプリファレンスを受信するのに応じて、受信したプリファレンスに記載された個人情報提供装置 1 0 および個人情報取得装置 2 0 に関する情報を連携装置情報として格納してもよい。

取扱情報格納部 9 1 1 は、上述した連携装置が公開している個人情報の取り扱いに関する取扱情報を、連携装置別に格納する。ここで、取扱情報とは、例えば、プライバシーポ

50

リシーヤ、サービス提供条件等であってもよい。

取扱情報取得部 9 1 2 は、連携装置情報格納部 9 1 0 に登録された 1 つ以上の連携装置にアクセスし、個々の連携装置の取扱情報を取得する。そして、取扱情報取得部 9 1 2 は、取得した各連携装置の取扱情報を、取扱情報格納部 9 1 1 に格納する。

確認用プリファレンス推定部 9 1 3 は、プリファレンス要求メッセージ R M 2 に含まれる個人情報取得装置 2 0 および個人情報提供装置 1 0 に類似した個人情報取得装置 2 0 および個人情報提供装置 1 0 を含む類似プリファレンスを、取扱情報格納部 9 1 1 に基づいて抽出する。そして確認用プリファレンス推定部 9 1 3 は、抽出した類似プリファレンスに基づいて、確認用プリファレンス C P を推定する。

具体的には、確認用プリファレンス推定部 9 1 3 は、取扱情報格納部 9 1 1 に基づいて、プリファレンス格納部 3 0 1 に格納されたプリファレンスに含まれる個人情報提供装置 1 0 および個人情報取得装置 2 0 を、複数のグループに分類する。

そして、確認用プリファレンス推定部 9 1 3 は、プリファレンス要求メッセージ R M 2 に含まれる個人情報提供装置 1 0 および個人情報取得装置 2 0 の属するグループを、取扱情報格納部 9 1 1 に基づいて判定する。さらに、確認用プリファレンス推定部 9 1 3 は、プリファレンス要求メッセージ R M 2 に含まれる個人情報提供装置 1 0 と同一グループに属する個人情報提供装置 1 0 から、プリファレンス要求メッセージ R M 2 に含まれる個人情報取得装置 2 0 と同一グループに属する個人情報取得装置 2 0 に対して、個人情報を提供する際に過去に設定されたプリファレンスを、類似プリファレンスとして抽出する。

また、確認用プリファレンス推定部 9 1 3 は、プリファレンス格納部 3 0 1 に格納されているプリファレンスに基づいて、各プリファレンスに含まれる個人情報の種類別の評価値を算出する。ここで、個人情報の種類別の評価値とは、例えば、ある種類の個人情報の開示がユーザによって許可される度合いを表す秘匿度等であってもよい。

さらに、確認用プリファレンス推定部 9 1 3 は、プリファレンス要求メッセージ R M 2 によって要求されている個人情報の種類別の評価値を算出する。そして、確認用プリファレンス推定部 9 1 3 は、要求されている個人情報の種類別の評価値の中から、所定範囲内の評価値が関連付けされている、特定の種類の個人情報を含むプリファレンスを、類似プリファレンスとしてさらに抽出する。

例えば、確認用プリファレンス推定部 9 1 3 は、1 つの個人情報提供装置 1 0 から、ある種類の個人情報が開示された個人情報取得装置 2 0 の装置数等の開示状況に基づいて、その種類に対する評価値を算出してもよい。確認用プリファレンス推定部 9 1 3 は、このような開示状況に関する情報を、プリファレンス格納部 3 0 1 に格納されたプリファレンスに含まれる個人情報の種類、個人情報提供装置 1 0 の装置 I D、および、個人情報取得装置 2 0 の装置 I D を集計することにより求めてもよい。

なお、確認用プリファレンス推定部 9 1 3 は、プリファレンス要求メッセージ R M 2 に含まれる情報に基づいて、個人情報の種類別の評価値を算出してもよい。この場合、個人情報提供装置 1 0 のプリファレンス要求部 1 0 3 は、自装置における各種の個人情報の開示状況を、プリファレンス要求メッセージ R M 2 に含めて送信するように構成する。

また、確認用プリファレンス推定部 9 1 3 は、個人情報提供装置 1 0 および個人情報取得装置 2 0 の分類および個人情報の種類に対する評価値に基づいて、類似プリファレンスを抽出してもよい。そして、確認用プリファレンス推定部 9 1 3 は、類似プリファレンスに基づいて、ユーザに提示する確認用プリファレンス C P を推定することにより生成する。

例えば、プリファレンス要求メッセージ R M 2 によって、装置 I D 0 0 0 1 の個人情報提供装置 1 0 から装置 I D 0 0 0 2 の個人情報取得装置 2 0 に対してクレジットカード番号を提供する際のプリファレンスが要求されている場合を想定する。このとき、確認用プリファレンス推定部 9 1 3 は、装置 I D 0 0 0 1 の個人情報提供装置 1 0 と同一のグループ A に含まれる個人情報提供装置 1 0 から、装置 I D 0 0 0 2 の個人情報取得装置 2 0 と同一のグループ B に含まれる個人情報取得装置 2 0 に対して、クレジットカード番号の評価値 5 以上の評価値を有する種類の個人情報の開示が許可されているプリファレンスを、

10

20

30

40

50

類似プリファレンスとして抽出する。

そして、この場合、確認用プリファレンス推定部 9 1 3 は、類似プリファレンスの取扱条件を集計する。このとき、「第三者への提供は不可」という取扱条件が最も多かったと想定する。この場合、確認用プリファレンス推定部 9 1 3 は、確認用プリファレンス CP として、「装置 ID 0 0 0 1 の個人情報提供装置 1 0 から装置 ID 0 0 0 2 の個人情報取得装置 2 0 に対してクレジットカード番号を提供する際、第三者への提供を不可であることを取扱条件として開示に同意する」といった内容の確認用プリファレンス CP を推定する。

以上のように構成された個人情報送受信システム 5 の取扱情報取得処理、プリファレンス確認処理、および、プリファレンス推定処理について、図 2 6 ~ 図 2 8 を参照して説明する。なお、個人情報送受信システム 5 の個人情報送受信動作の概略、プリファレンス要求処理、および、個人情報提供処理については、図 1 0、図 1 1、図 1 3 を参照して説明した第 1 の実施形態における個人情報送受信システム 1 と同様であるため、本実施形態における説明を省略する。

まず、個人情報送受信システム 5 の取扱情報取得処理について、図 2 6 を参照して説明する。なお、プリファレンス管理装置 9 0 は、この取扱情報取得処理を、後述するプリファレンス確認処理の実行前にあらかじめ実行しておく。

まず、連携装置情報格納部 9 1 0 は、連携装置情報を格納する（ステップ G 1）。例えば、連携装置情報格納部 9 1 0 は、プリファレンス管理装置 9 0 の管理者によって登録された連携装置情報を格納してもよい。また、連携装置情報には、各連携装置を識別する装置 ID や、装置の URL 等が含まれていてもよい。

次に、取扱情報取得部 9 1 2 は、連携装置情報格納部 9 1 0 に登録された各連携装置について、取扱情報を取得する（ステップ G 2）。例えば、取得する取扱情報には、各装置が開示しているプライバシーポリシーや、サービス提供条件等が含まれていてもよい。なお、取扱情報取得部 9 1 2 は、このような取扱情報として、例えば、各装置によってウェブサイトに掲載されている情報を取得してもよい。

次に、取扱情報格納部 9 1 1 は、取扱情報取得部 9 1 2 によって取得された情報を格納する（ステップ G 3）。

以上で、プリファレンス管理装置 9 0 は、取扱情報取得処理を終了する。

次に、個人情報送受信システム 5 のプリファレンス確認処理の詳細について説明する。

図 2 7 において、プリファレンス管理装置 9 0 のプリファレンス確認処理は、図 1 2 を用いて説明した第 1 の実施形態におけるプリファレンス管理装置 3 0 のプリファレンス確認処理と比較して、ステップ C 2 の代わりに、ステップ I 1 およびステップ I 2 を実行する点が異なる。

ステップ C 1 が実行された後、確認用プリファレンス推定部 9 1 3 は、ステップ C 1 で受信したプリファレンス要求メッセージ RM 2 に含まれる個人情報提供装置 1 0 および個人情報取得装置 2 0 に関する取扱情報を、取扱情報格納部 9 1 1 から取得する（ステップ I 1）。

次に、確認用プリファレンス推定部 9 1 3 は、ステップ I 1 で取得した取扱情報に基づいて、プリファレンス格納部 3 0 1 に格納されたプリファレンスのうち、ステップ C 1 で受信したプリファレンス要求メッセージ RM 2 によって要求されるプリファレンスに類似する類似プリファレンスを抽出する。そして、確認用プリファレンス推定部 9 1 3 は、抽出した類似プリファレンスに基づいて、確認用プリファレンス CP を推定する（ステップ I 2）。

以降、プリファレンス管理装置 9 0 は、ステップ C 3 ~ C 9 まで第 1 の実施形態におけるプリファレンス管理装置 3 0 と同様に動作することにより、ユーザ端末 4 0 から取得したプリファレンスを、個人情報提供装置 1 0 に送信する。

ここで、ステップ I 2 における確認用プリファレンス推定処理の詳細について、図 2 8 を参照して説明する。まず、確認用プリファレンス推定部 9 1 3 は、取扱情報格納部 9 1 1 に格納された各連携装置の取扱情報に基づいて、連携装置の分類を行う（ステップ J 1

10

20

30

40

50

)。例えば、確認用プリファレンス推定部 9 1 3 は、各連携装置の取扱情報に含まれる項目およびその内容に関して、類似度または距離を算出し、算出した類似度または距離の大きさに基づいて、連携装置の分類を行ってもよい。また、類似度または距離に基づいて分類を行う技術としては、パターン認識、ベイズ推論、ニューラルネットワーク等、既存の技術を用いればよい。

次に、確認用プリファレンス推定部 9 1 3 は、ステップ J 1 で行った分類に基づいて、プリファレンス要求メッセージ R M 2 に含まれる装置 I D の個人情報提供装置 1 0 および個人情報取得装置 2 0 がそれぞれ属する分類を取得する(ステップ J 2)。

次に、確認用プリファレンス推定部 9 1 3 は、プリファレンス格納部 3 0 1 に格納されたプリファレンスに含まれる個人情報の種類別の評価値を算出する(ステップ J 3)。次に、確認用プリファレンス推定部 9 1 3 は、プリファレンス要求メッセージ R M 2 に含まれる個人情報の種類の評価値を算出する(ステップ J 4)。

例えば、ステップ J 2 および J 3 において、確認用プリファレンス推定部 9 1 3 は、上述したように、該当する種類の個人情報の開示状況に基づいて算出される秘匿度を、個人情報の評価値として算出してもよい。

次に、ステップ J 2 およびステップ J 4 で取得した、プリファレンス要求メッセージ R M 2 に含まれる個人情報提供装置 1 0 および個人情報取得装置 2 0 がそれぞれ属する分類、および、プリファレンス要求メッセージ R M 2 に含まれる種類の個人情報の評価値に基づいて、確認用プリファレンス推定部 9 1 3 は、プリファレンス格納部 3 0 1 から類似プリファレンスを抽出する。そして、確認用プリファレンス推定部 9 1 3 は、類似プリファレンスに基づいて、ユーザ端末 4 0 へ提示する確認用プリファレンス C P を推定する(ステップ J 5)。

例えば、確認用プリファレンス推定部 9 1 3 は、下記の事項を類似プリファレンスとして、プリファレンス格納部 3 0 1 から抽出する。

- プリファレンス要求メッセージ R M 2 に含まれる個人情報提供装置 1 0 および個人情報取得装置 2 0 がそれぞれ属する分類 A および分類 B に対して、同一の分類 A に含まれる個人情報提供装置 1 0、

- 同一の分類 B に含まれる個人情報取得装置 2 0、および、

- プリファレンス要求メッセージ R M 2 に含まれる個人情報の種類「クレジットカード番号」の評価値「5」以上の評価値を持つ種類の個人情報を含むプリファレンス。

そして、この場合、確認用プリファレンス推定部 9 1 3 は、抽出した類似プリファレンスの中で最も多い取扱条件の「第三者への提供不可」を適用した確認用プリファレンス C P を生成する。

以上で、プリファレンス管理装置 9 0 は、確認用プリファレンス推定処理を終了する。

なお、確認用プリファレンス推定処理において、ステップ J 1 における連携装置の分類処理、および、ステップ J 3 における個人情報の種類別の評価値の算出処理は、あらかじめ実行しておいてもよい。

次に、本発明の第 5 の実施形態の効果について述べる。

第 5 の実施形態に係る個人情報送受信システムによれば、該当するユーザによって過去に設定されたプリファレンスが無い場合であっても、プリファレンスを設定するユーザの負担をさらに軽減することができる。その理由は、確認用プリファレンス推定部 3 0 3 が、個人情報提供装置 1 0 および個人情報取得装置 2 0 の個人情報取扱情報に基づいて、要求されているプリファレンスに類似する類似プリファレンスを抽出し、抽出した類似プリファレンスに基づいて、ユーザ端末に提示する確認用プリファレンス C P を推定するからである。

また、本実施形態に係る上記の効果を楽しむ更なる理由は、確認用プリファレンス推定部 9 1 3 が、個人情報の種類に対する評価値を算出することにより、要求されているプリファレンスが対象とする個人情報の種類に対する評価値の中から、所定範囲内の評価値が関連付けされている、特定の種類の個人情報を対象とした類似プリファレンスを抽出し、抽出したプリファレンスに基づいて、ユーザ端末に提示する確認用プリファレンス C

Pを推定するからである。

(第6の実施形態)

次に、上述した第1の実施形態を基礎とする第6の実施形態について説明する。本実施形態は、本発明の第1の実施形態としての個人情報送受信システム1を、携帯電話端末用のショッピングポータルシステムに適用した例である。

本発明の第6の実施形態としての携帯電話端末用ショッピングポータルシステム6の構成を、図29に示す。図29において、携帯電話端末用ショッピングポータルシステム6は、個人情報提供装置10に相当するショッピングポータル61と、個人情報取得装置20に相当するコンテンツプロバイダ62と、プリファレンス管理装置30としてのモバイルキャリア63と、ユーザ端末40としての携帯電話端末64とを備える。また、これらの各装置は、ネットワーク9を介して通信可能に接続されている。

なお、図29に示す携帯電話端末用ショッピングポータルシステム6の構成は、説明の便宜上から、ショッピングポータル61、コンテンツプロバイダ62、モバイルキャリア63および携帯電話端末64をそれぞれ1つ有する構成である。但し、本発明は、係る構成には限定されず、これらの装置が適宜複数備えられたシステム構成であってもよい。

ショッピングポータル61は、個人情報を保有し、保有している個人情報をコンテンツプロバイダ62からの要求に応じて提供する。また、ショッピングポータル61は、コンテンツプロバイダ62に個人情報を送信する際に必要となるプリファレンスを、モバイルキャリア63に要求する。ここで、プリファレンス要求メッセージRM2には、個人情報の提供先となるコンテンツプロバイダ62の装置ID、および、提供する個人情報の種類等が記載される。

コンテンツプロバイダ62は、携帯電話端末64からコンテンツ要求を取得し、携帯電話端末64に対してコンテンツを提供する。このとき、コンテンツプロバイダ62は、携帯電話端末64にコンテンツを提供してよいか否かを判断するために、ユーザの個人情報を必要とする。そこで、コンテンツプロバイダ62は、該当するユーザの個人情報をショッピングポータル61に対して要求する。

モバイルキャリア63は、プリファレンスを要求するメッセージをショッピングポータル61から取得し、携帯電話端末64より取得したプリファレンスを提供する。このとき、モバイルキャリア63は、携帯端末94からプリファレンスを取得するため、携帯電話94に対して、確認用プリファレンスCPを送信し、この確認用プリファレンスCPに対する設定内容を取得する。

携帯電話端末64は、コンテンツプロバイダ62にアクセスしコンテンツを要求する。また、携帯電話端末64は、モバイルキャリア63から送信される確認用プリファレンスCPに対する設定内容をモバイルキャリア63に送信する。

以上のように構成された携帯電話端末用ショッピングポータルシステム6の動作について、図29および図30を参照して説明する。

まず、携帯電話端末64は、コンテンツプロバイダ62にコンテンツを要求する(ステップL1)。次に、コンテンツプロバイダ62は、このコンテンツを携帯電話端末64に提供してよいか否かを確認するために必要となる個人情報を、ショッピングポータル61に要求する(ステップL2)。

次に、個人情報要求メッセージRM1を受信したショッピングポータル61は、この個人情報をコンテンツプロバイダ62に提供してよいか否かを判断するために必要となるプリファレンスを、モバイルキャリア63に要求する(ステップL3)。

次に、プリファレンス要求メッセージRM2を受信したモバイルキャリア63は、ショッピングポータル61からコンテンツプロバイダ62に対してこの個人情報を送受信してよいか否かを規定する確認用プリファレンスCPを生成する。(ステップL4)。

このとき、モバイルキャリア63は、該当するユーザによって過去に設定されたプリファレンスや、要求されるプリファレンスに類似する類似プリファレンスに基づいて、確認用プリファレンスCPを生成する。

次に、モバイルキャリア63は、携帯電話端末64に対して、ステップL4で生成した

10

20

30

40

50

確認用プリファレンスCPとステップL3で取得したプリファレンス要求内容を提示する(ステップL5)。

このように、過去に設定済みのプリファレンスや類似するプリファレンスに基づいて生成した確認用プリファレンスCPを携帯電話端末64に提示することにより、モバイルキャリア63は、プリファレンスを設定するユーザ負担を軽減することができる。

次に、携帯電話端末64は、確認用プリファレンスCPに対するユーザの設定内容を表す情報を、モバイルキャリア63に送信する(ステップL6)。

なお、ステップL5およびL6の処理は、モバイルキャリア63および携帯電話端末64の間の直接通信により行われる。直接通信を行う技術としては、例えば、携帯電話端末64に搭載されたウェブブラウザアプリケーションのリダイレクト機能や、電子メールの送受信等が適用可能である。

次に、モバイルキャリア63は、取得した設定結果を確認用プリファレンスCPに適用することによって設定されたプリファレンスを、ショッピングポータル61へ提供する(ステップL7)。

次に、ショッピングポータル61は、取得したプリファレンスをもとに、個人情報コンテンツプロバイダ62に提供可能か否かを判断する。そして、ショッピングポータル61は、提供可能であると判断すれば、個人情報をコンテンツプロバイダ62に提供する(ステップL8)。

次に、個人情報を取得したコンテンツプロバイダ62は、取得した個人情報に基づいて、コンテンツを携帯電話端末64に提供可能か否かを判断する。そして、コンテンツプロバイダ62は、提供可能であると判断すれば、コンテンツを携帯電話端末64へ提供する(ステップL9)。

以上で、携帯電話端末用ショッピングポータルシステム6は動作を終了する。

次に、本発明の第6の実施形態の効果について述べる。

第6の実施形態に係る携帯電話端末用ショッピングポータルシステム6は、個人情報を保有するショッピングポータル数およびコンテンツプロバイダ数が増大しても、個人情報の開示に関する条件や開示の可否を規定するプリファレンスを設定するユーザの負担を軽減することができる。その理由は、モバイルキャリア63が、ショッピングポータル61からコンテンツプロバイダ62に対する個人情報の開示に関するプリファレンスを携帯電話端末64から取得し、ショッピングポータル61が、モバイルキャリア63によって取得されたプリファレンスに基づいてコンテンツプロバイダ62に個人情報を提供するためである。

すなわち、第6の実施形態に係る携帯電話端末用ショッピングポータルシステム6では、モバイルキャリア63がプリファレンスを集中管理するので、携帯電話端末64のユーザは、個人情報を保有するショッピングポータルやコンテンツプロバイダごとに個人情報の開示に関するプリファレンスを設定する必要がないからである。

(第7の実施形態)

次に、上述した第1の実施形態を基礎とする第7の実施形態について説明する。本実施形態では、第1の実施形態に係る個人情報送受信システム1を、ASP(Application Service Provider)基盤システムに適用した例について説明する。

本発明の第6の実施形態としてのASP基盤システム7の構成を、図31に示す。図31において、ASP基盤システム7は、ASPサーバ装置71と、ユーザ端末72とを備えている。また、サーバ装置71とユーザ端末72とはネットワーク9を介して通信可能に接続されている。ASPサーバ装置71とユーザ端末72とは、コンピュータによって実現可能である。即ち、ASPサーバ装置71のハードウェア資源には、図2乃至図4に示したコンピュータ(情報処理装置)を採用することができる。ユーザ端末72のハードウェア資源には、図5に示したコンピュータ(情報処理装置)を採用することができる。

ASPサーバ装置71は、ユーザ管理部711と、個人情報管理部712と、アプリケーション部713Aおよび713B(以下、総称してアプリケーション部713ともいう

10

20

30

40

50

)とを備える。

ここで、ユーザ管理部 7 1 1 は、A S Pサーバ装置 7 1を構成するコンピュータの記憶装置 (1 0 0 4 等) に格納され、A S Pサーバ装置 7 1をプリファレンス管理装置 3 0として動作させるコンピュータ・プログラムをR A M (1 0 0 2 等) に読み込んで実行するC P U (1 0 0 1 等)、記憶装置 (1 0 0 4 等)、およびネットワークインタフェース (1 0 0 5 等) によって構成される。

また、個人情報管理部 7 1 2 は、A S Pサーバ装置 7 1を構成するコンピュータの記憶装置に格納され、A S Pサーバ装置 7 1を個人情報提供装置 1 0として動作させるコンピュータ・プログラムをR A M (1 0 0 2 等) に読み込んで実行するC P U (1 0 0 4 等) および記憶装置 (1 0 0 4 等) によって構成される。

10

また、アプリケーション部 7 1 3 は、A S P基盤システム 7 にサービスの運営を委託する事業者によってA S Pサーバ装置 7 1を構成するコンピュータに登録されているコンピュータ・プログラムをR A M (1 0 0 2 等) に読み込んで実行するC P U (1 0 0 4 等)、記憶装置 (1 0 0 4 等)、およびネットワークインタフェース (1 0 0 5 等) によって構成される。

なお、図 3 1 には、一例として、2つのアプリケーション部 7 1 3 (7 1 3 A , 7 1 3 B) を示しているが、本実施形態に係るA S P基盤システム 7 におけるA S Pサーバ装置 7 1が備えるアプリケーション部の数を限定するものではない。

ユーザ管理部 7 1 1 は、ユーザ端末 7 2 によって設定されたプリファレンスを格納している。また、ユーザ管理部 7 1 1 は、ユーザ端末 7 2 によって設定されたプリファレンスを、個人情報管理部 7 1 2 に提供する。個人情報管理部 7 1 2 は、個人情報を格納している。また、個人情報管理部 7 1 2 は、ユーザ管理部 7 1 1 にプリファレンスを要求することにより取得し、取得したプリファレンスに基づいて、個人情報をアプリケーション部 7 1 3 に提供する。

20

アプリケーション部 7 1 3 A および 7 1 3 B は、サービス提供部 7 1 4 A および 7 1 4 B (以下、総称してサービス提供部 7 1 4 ともいう) と、個人情報送受信部 7 1 5 A および 7 1 5 B (以下、総称して個人情報送受信部 7 1 5 ともいう) とを含む。サービス提供部 7 1 4 は、ユーザ端末 7 2 に対して個人情報に基づくサービスを提供する。

個人情報送受信部 7 1 5 は、上述した第 1 の実施形態における個人情報取得装置 2 0 および個人情報提供装置 1 0 の一実施形態を構成する。すなわち、個人情報送受信部 7 1 5 は、第 1 の実施形態における個人情報要求部 2 0 1、個人情報受信部 2 0 2、個人情報格納部 1 0 1、個人情報要求受信部 1 0 2、プリファレンス要求部 1 0 3、プリファレンス受信部 1 0 4、開示可否判断部 1 0 5 および個人情報送信部 1 0 6 を含む。

30

個人情報送受信部 7 1 5 の個人情報要求部 2 0 1 は、サービス提供部 7 1 4 によるサービス提供に必要となる個人情報を、個人情報提供装置 1 0 としての個人情報管理部 7 1 2 または他のアプリケーション部 7 1 3 の個人情報送受信部 7 1 5 に対して要求する。このように、個人情報送受信部 7 1 5 の個人情報要求部 2 0 1 は、必要に応じて複数の個人情報提供装置 1 0 に個人情報を要求する。

個人情報送受信部 7 1 5 の個人情報受信部 2 0 2 は、取得した個人情報をサービス提供部 7 1 4 に出力するとともに、個人情報格納部 1 0 1 に格納する。個人情報送受信部 7 1 5 の個人情報要求受信部 1 0 2 は、他のアプリケーション部 7 1 3 の個人情報送受信部 7 1 5 からの個人情報要求メッセージ R M 1 を受信する。個人情報送受信部 7 1 5 のプリファレンス要求部 1 0 3 は、ユーザ管理部 7 1 1 に対してプリファレンス要求メッセージ R M 2 を送信する。そして、個人情報送受信部 7 1 5 のプリファレンス受信部 1 0 4 は、ユーザ管理部 7 1 1 からプリファレンスを取得する。

40

以上のように構成されたA S P基盤システム 7 の動作について、図 3 1 および図 3 2 を参照して説明する。

まず、ユーザ端末 7 2 は、アプリケーション部 7 1 3 A のサービス提供部 7 1 4 A に対してサービス提供を要求する (ステップ M 1)。次に、サービス提供部 7 1 4 A は、サービスの提供に個人情報を必要とするため、個人情報送受信部 7 1 5 A に個人情報を要求す

50

る（ステップM2）。

次に、個人情報送受信部715Aは、複数の装置に個人情報を要求する（ステップM3-1、M3-2）。例えば、個人情報送受信部715Aは、他の事業者によって登録されたアプリケーション部713Bの個人情報送受信部715Bと、ASP基盤システム7によって提供される個人情報管理部712とに個人情報要求メッセージRM1を送信する。

次に、個人情報送受信部715Bおよび個人情報管理部712は、要求された個人情報の送受信に関するプリファレンス要求メッセージRM2を、ユーザ管理部711にそれぞれ送信する（ステップM4-1、M4-2）。

次に、ユーザ管理部711は、プリファレンス格納部301に格納された過去のプリファレンスを参照することにより、ユーザ端末72に確認用プリファレンスCPを提示する（ステップM5）。

次に、ユーザ管理部711は、ユーザ端末72から、確認用プリファレンスCPに基づいて設定されたプリファレンスを取得する（ステップM6）。

次に、ユーザ管理部711は、取得したプリファレンスを、個人情報送受信部715Bおよび個人情報管理部712に提供する（ステップM7-1、M7-2）。

次に、プリファレンスを取得した個人情報管理部712および個人情報管理部712は、プリファレンスの内容を確認し、個人情報送受信部715Aに個人情報を提供する（ステップM8-1、M8-2）。

次に、個人情報を取得した個人情報送受信部715Aは、サービス提供部714Aに個人情報を提供する（ステップM9）。

次に、サービス提供部714Aは、取得した個人情報に基づくサービスを、ユーザ端末72に対して提供する（ステップM10）。

以上で、ASP基盤システム7は動作を終了する。

なお、ユーザ管理部711は、ステップM6において、エンドユーザによるプリファレンスの設定内容を取得するだけでなく、ASP基盤システム7またはアプリケーション部713の管理者によるプリファレンスの設定内容を取得してもよい。管理者によるプリファレンスの設定内容を取得する場合、ユーザ管理部711は、取得した設定内容に基づくプリファレンスを、ユーザによる個別のプリファレンスが取得できない場合に適用するプリファレンスとして、プリファレンス格納部301に格納してもよい。

次に、本発明の第7の実施形態の効果について述べる。

第7の実施形態に係るASP基盤システム7は、個人情報を保有するアプリケーション部の数が増大しても、個人情報の送受信に関するプリファレンスを設定するユーザ負担を軽減することができる。その理由は、ユーザ管理部711が、個人情報管理部712および各アプリケーション部（713A、713B）から他のアプリケーション部に対する個人情報の開示に関するプリファレンスを取得し、個人情報管理部712および各アプリケーション部が、ユーザ管理部711によって取得されたプリファレンスに基づいて、他のアプリケーション部に個人情報を提供するためである。

すなわち、第7の実施形態に係るASP基盤システム7では、ユーザ管理部711がプリファレンスを集中管理するので、個人情報を送受信するアプリケーション部の数が増大しても、ユーザは、アプリケーション部毎に個人情報に関するプリファレンスを設定する必要はない。

なお、上述した本発明の各実施形態において、各フローチャートを参照して説明したプリファレンス要求処理（図11、図16、図19）、プリファレンス確認処理（図12、図27）および個人情報提供処理（図13）等の各種の処理は、コンピュータ・プログラムとして個人情報提供装置（10等）およびプリファレンス管理装置（30等）の不揮発性の記憶媒体（記憶装置1004等）に格納しておき、係るコンピュータ・プログラムをCPU（1001など）に読み出して実行することにより、これらの処理の機能を実現することができる。そして、このような場合において、本発明は、係るコンピュータ・プログラムのコード或いは記憶媒体によっても構成されると捉えることができる。

また、上述した各実施形態は、適宜組み合わせられて実施されることが可能である。また、

10

20

30

40

50

本発明は、上述した各実施形態に限定されず、様々な態様で実施されることが可能である。

尚、上記の各実施形態の一部又は全部は、以下の付記のようにも記載されうるが、係る以下の付記には限定されない。

(付記 1)

個人情報取得装置と、個人情報提供装置と、プリファレンス管理装置と、ユーザ端末とを備え、

前記個人情報取得装置は、

前記ユーザ端末に対するサービス提供に必要な個人情報の要求を表す個人情報要求メッセージを、前記個人情報提供装置に送信する個人情報要求部と、

前記個人情報を前記個人情報提供装置から受信する個人情報受信部と、

前記個人情報提供装置は、

前記個人情報を格納した個人情報格納部と、

前記個人情報取得装置から前記個人情報要求メッセージを受信する個人情報要求受信部と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、前記プリファレンス管理装置に送信するプリファレンス要求部と、

前記プリファレンスを前記プリファレンス管理装置から受信するプリファレンス受信部と、

前記プリファレンス受信部によって受信されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する開示可否判断部と、

前記開示可否判断部によって開示可能であると判断された場合に、前記個人情報を前記個人情報取得装置に送信する個人情報送信部と、

を有し、

前記プリファレンス管理装置は、

前記ユーザ端末によって過去に設定されたプリファレンスを格納するプリファレンス格納部と、

前記個人情報提供装置から前記プリファレンス要求メッセージを受信するプリファレンス要求受信部と、

前記プリファレンス格納部に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成する確認用プリファレンス生成部と、

前記確認用プリファレンスを前記ユーザ端末に提示し、提示した確認用プリファレンスに基づいて設定されたプリファレンスを前記ユーザ端末から受信するプリファレンス確認部と、

前記プリファレンス確認部によって受信された前記プリファレンスを前記個人情報提供装置に送信するプリファレンス送信部と、

を有し、

前記ユーザ端末は、

前記プリファレンス管理装置から提示される前記確認用プリファレンスに基づいて、前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを設定し、設定したプリファレンスを前記プリファレンス管理装置に送信するプリファレンス設定部、

を有することを特徴とする個人情報送受信システム。

(付記 2)

前記プリファレンス管理装置の前記確認用プリファレンス生成部は、

前記プリファレンス格納部に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づい

10

20

30

40

50

て、前記確認用プリファレンスを生成することを特徴とする付記 1 に記載の個人情報送受信システム。

(付記 3)

前記プリファレンス管理装置は、

前記個人情報提供装置および前記個人情報取得装置の個人情報の取り扱いに関する取扱情報を格納する取扱情報格納部と、

前記プリファレンス格納部に格納されたプリファレンスのうち、前記プリファレンス要求メッセージ R M 2 に含まれる提供元の個人情報提供装置および開示先の個人情報取得装置に類似する提供元および開示先に関する類似プリファレンスを、前記取扱情報格納部に格納された各装置の取扱情報に基づいて抽出し、抽出した類似プリファレンスに基づいて

10

、前記確認用プリファレンスを推定することにより生成する確認用プリファレンス推定部と、

をさらに有することを特徴とする付記 1 または付記 2 に記載の個人情報送受信システム。

(付記 4)

前記プリファレンス管理装置の前記確認用プリファレンス推定部は、

前記取扱情報格納部に基づいて前記個人情報提供装置および前記個人情報取得装置を分類し、前記プリファレンス要求メッセージに含まれる提供元の個人情報提供装置と同一の分類に属する個人情報提供装置から、前記プリファレンス要求メッセージに含まれる開示先の個人情報取得装置と同一の分類に属する個人情報取得装置に対して、前記個人情報の開示に関して過去に設定されたプリファレンスを、前記類似プリファレンスとして抽出する

20

ことを特徴とする付記 3 に記載の個人情報送受信システム。

(付記 5)

前記プリファレンス管理装置の前記確認用プリファレンス推定部は、

前記プリファレンス格納部に格納されたプリファレンスに基づいて、各プリファレンスに含まれる個人情報の種類に対する評価値を算出するとともに、前記プリファレンス要求メッセージに含まれる個人情報の種類に対する評価値を算出することにより、前記プリファレンス要求メッセージに含まれる個人情報の評価値から所定範囲内の評価値を有する種類の個人情報の開示に関するプリファレンスを、前記類似プリファレンスとして抽出することを特徴とする付記 3 または付記 4 に記載の個人情報送受信システム。

30

(付記 6)

前記個人情報提供装置は、

前記プリファレンス管理装置を表す情報を格納するプリファレンス管理装置情報格納部と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関するプリファレンスの要求先となるプリファレンス管理装置を、前記プリファレンス管理装置情報格納部に基づいて決定するプリファレンス要求先決定部と、

をさらに備え、

前記プリファレンス要求部は、

前記プリファレンス要求先決定部によって決定されたプリファレンス管理装置に対して、前記プリファレンス要求メッセージを送信する

40

ことを特徴とする付記 1 から付記 5 のいずれかに記載の個人情報送受信システム。

(付記 7)

前記個人情報提供装置は、

前記プリファレンス管理装置から取得したプリファレンスを保管するプリファレンス保管部と、

前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを、前記プリファレンス保管部から検索することにより取得するプリファレンス取得部と、

をさらに備え、

前記開示可否判断部は、

50

前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスが前記プリファレンス保管部に保管されている場合、前記プリファレンス取得部によって取得されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する

ことを特徴とする付記 1 から付記 6 のいずれかに記載の個人情報送受信システム。

(付記 8)

前記ユーザ端末は、

前記個人情報の開示に関して過去に設定したプリファレンスの変更内容を前記プリファレンス管理装置に送信するプリファレンス変更内容設定部をさらに備え、

前記プリファレンス管理装置は、

前記変更内容を前記ユーザ端末から取得する変更内容取得部と、

前記変更内容取得部によって取得された変更内容に基づいて前記プリファレンス格納部に格納されたプリファレンスを更新するプリファレンス更新部と、

前記プリファレンス更新部によって更新されたプリファレンスに関連する個人情報提供装置および個人情報取得装置を特定し、特定した個人情報提供装置および個人情報取得装置に対するプリファレンス変更通知を生成するプリファレンス変更通知生成部と、

前記プリファレンス変更通知生成部によって特定された個人情報提供装置および個人情報取得装置に対して、前記プリファレンス変更通知をそれぞれ送信するプリファレンス変更通知送信部と、をさらに備える

ことを特徴とする付記 1 から付記 7 のいずれかに記載の個人情報送受信システム。

(付記 9)

個人情報取得装置と、個人情報提供装置と、プリファレンス管理装置と、ユーザ端末とを用いて、

前記個人情報取得装置は、

前記ユーザ端末に対するサービス提供に必要な個人情報の要求を表す個人情報要求メッセージを、前記個人情報提供装置に送信し、

前記個人情報提供装置は、

前記個人情報を個人情報格納部に格納しておき、

前記個人情報取得装置から前記個人情報要求メッセージを受信し、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、前記プリファレンス管理装置に送信し、

前記プリファレンス管理装置は、

前記ユーザ端末によって過去に設定されたプリファレンスをプリファレンス格納部に格納しておき、

前記個人情報提供装置から前記プリファレンス要求メッセージを受信し、

前記プリファレンス格納部に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成し、

前記確認用プリファレンスを前記ユーザ端末に提示し、

前記ユーザ端末は、

前記プリファレンス管理装置から提示される前記確認用プリファレンスに基づいて、前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを設定し、

設定したプリファレンスを前記プリファレンス管理装置に送信し、

前記プリファレンス管理装置は、

設定されたプリファレンスを前記ユーザ端末から受信し、

受信された前記プリファレンスを前記個人情報提供装置に送信し、

前記個人情報提供装置は、

前記プリファレンスを前記プリファレンス管理装置から受信し、

10

20

30

40

50

受信されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断し、

開示可能であると判断された場合に、前記個人情報を前記個人情報取得装置に送信し、前記個人情報取得装置は、前記個人情報を前記個人情報提供装置から受信する、ことを特徴とする個人情報送受信方法。

(付記 10)

前記プリファレンス管理装置は、前記プリファレンス格納部に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づいて、前記確認用プリファレンスを生成することを特徴とする付記 9 に記載の個人情報送受信方法。

10

(付記 11)

個人情報を格納した個人情報格納部と、前記個人情報の要求を表す個人情報要求メッセージを個人情報取得装置から受信する個人情報要求受信部と、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、プリファレンス管理装置に送信するプリファレンス要求部と、

前記プリファレンスを前記プリファレンス管理装置から受信するプリファレンス受信部と、

20

前記プリファレンス受信部によって受信されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する開示可否判断部と、

前記開示可否判断部によって開示可能であると判断された場合に、前記個人情報を前記個人情報取得装置に送信する個人情報送信部と、を備えたことを特徴とする個人情報提供装置。

(付記 12)

前記プリファレンス管理装置から取得したプリファレンスを保管するプリファレンス保管部と、

前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを、前記プリファレンス保管部から検索することにより取得するプリファレンス取得部と、をさらに備え、

30

前記開示可否判断部は、

前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスが前記プリファレンス保管部に保管されている場合、前記プリファレンス取得部によって取得されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する

ことを特徴とする付記 11 に記載の個人情報提供装置。

(付記 13)

ユーザ端末によって過去に設定された、個人情報提供装置から個人情報取得装置に対する個人情報の開示に関する規定を表すプリファレンスを格納するプリファレンス格納部と、

40

前記プリファレンスの要求を表すプリファレンス要求メッセージを、前記個人情報提供装置から受信するプリファレンス要求受信部と、

前記プリファレンス格納部に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成する確認用プリファレンス生成部と、

前記確認用プリファレンスを前記ユーザ端末に提示し、提示した確認用プリファレンスに基づいて設定されたプリファレンスを前記ユーザ端末から受信するプリファレンス確認部と、

50

前記プリファレンス確認部によって受信された前記プリファレンスを前記個人情報提供装置に送信するプリファレンス送信部と、
を備えたことを特徴とするプリファレンス管理装置。

(付記 14)

前記確認用プリファレンス生成部は、
前記プリファレンス格納部に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づいて、前記確認用プリファレンスを生成することを特徴とする付記 13 に記載のプリファレンス管理装置。

(付記 15)

個人情報を個人情報格納部に格納する個人情報格納ステップと、
前記個人情報の要求を表す個人情報要求メッセージを個人情報取得装置から受信する個人情報要求受信ステップと、

前記個人情報要求メッセージの受信に応じて、前記個人情報の開示に関する規定を表すプリファレンスの要求を表すプリファレンス要求メッセージを、プリファレンス管理装置に送信するプリファレンス要求ステップと、

前記プリファレンスを前記プリファレンス管理装置から受信するプリファレンス受信ステップと、

前記プリファレンス受信ステップで受信されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断する開示可否判断ステップと、

前記開示可否判断ステップで開示可能であると判断された場合に、前記個人情報を前記個人情報取得装置に送信する個人情報送信ステップと、
をコンピュータ装置に実行させることを特徴とするコンピュータ・プログラム。

(付記 16)

前記プリファレンス管理装置から取得したプリファレンスをプリファレンス保管部に保管しておくプリファレンス保管ステップと、

前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスを、前記プリファレンス保管部から検索することにより取得するプリファレンス取得ステップと、
をさらに前記コンピュータ装置に実行させ、

前記開示可否判断ステップにおいて、前記個人情報提供装置から前記個人情報取得装置に対する前記個人情報の開示に関するプリファレンスが前記プリファレンス保管部に保管されている場合、前記プリファレンス取得ステップで取得されたプリファレンスに基づいて、前記個人情報を前記個人情報取得装置に開示可能か否かを判断することを特徴とする付記 15 に記載のコンピュータ・プログラム。

(付記 17)

ユーザ端末によって過去に設定された、個人情報提供装置から個人情報取得装置に対する個人情報の開示に関する規定を表すプリファレンスをプリファレンス格納部に格納しておくプリファレンス格納ステップと、

前記個人情報提供装置から前記プリファレンス要求メッセージを受信するプリファレンス要求受信ステップと、

前記プリファレンス格納部に格納された過去のプリファレンスと、前記プリファレンス要求メッセージとに基づいて、前記ユーザ端末に提示する確認用プリファレンスを生成する確認用プリファレンス生成ステップと、

前記確認用プリファレンスを前記ユーザ端末に提示し、提示した確認用プリファレンスに基づいて設定されたプリファレンスを前記ユーザ端末から受信するプリファレンス確認ステップと、

前記プリファレンス確認ステップで受信された前記プリファレンスを前記個人情報提供装置に送信するプリファレンス送信ステップと、
をコンピュータ装置に実行させることを特徴とするコンピュータ・プログラム。

(付記 18)

10

20

30

40

50

前記確認用プリファレンス生成ステップにおいて、前記プリファレンス格納部に格納されたプリファレンスのうち、前記プリファレンス要求メッセージに含まれる情報の少なくとも一部と同一の情報を含むプリファレンスに基づいて、前記確認用プリファレンスを生成する

ことを特徴とする付記 17 に記載のコンピュータ・プログラム。

以上、上述した実施形態を模範的な例として本発明を説明した。しかしながら、本発明は、上述した実施形態には限定されない。即ち、本発明は、本発明の範囲内において、当業者が理解し得る様々な態様を適用することができる。

この出願は、2010年10月5日に提出された日本出願特願2010-225741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。

10

【符号の説明】

【0010】

1、2、3、4、5 個人情報送受信システム

6 携帯電話端末用ショッピングポータルシステム

7 ASP基盤システム

9 ネットワーク

10、50、60 個人情報提供装置

20 個人情報取得装置

30、70、90 プリファレンス管理装置

40、80 ユーザ端末

20

61 ショッピングポータル

62 コンテンツプロバイダ

63 モバイルキャリア

64 携帯電話端末

71 ASPサーバ装置

72 ユーザ端末

101 個人情報格納部

102 個人情報要求受信部

103、603 プリファレンス要求部

104 プリファレンス受信部

30

105、605 開示可否判断部

106 個人情報送信部

201 個人情報要求部

202 個人情報受信部

301 プリファレンス格納部

302 プリファレンス要求受信部

303 確認用プリファレンス生成部

304 プリファレンス確認部

305 プリファレンス送信部

401 プリファレンス設定部

40

507 プリファレンス管理装置情報格納部

508 プリファレンス要求先決定部

609 プリファレンス保管部

610 プリファレンス取得部

706 変更内容取得部

707 プリファレンス更新部

708 変更通知生成部

709 変更通知送信部

711 ユーザ管理部

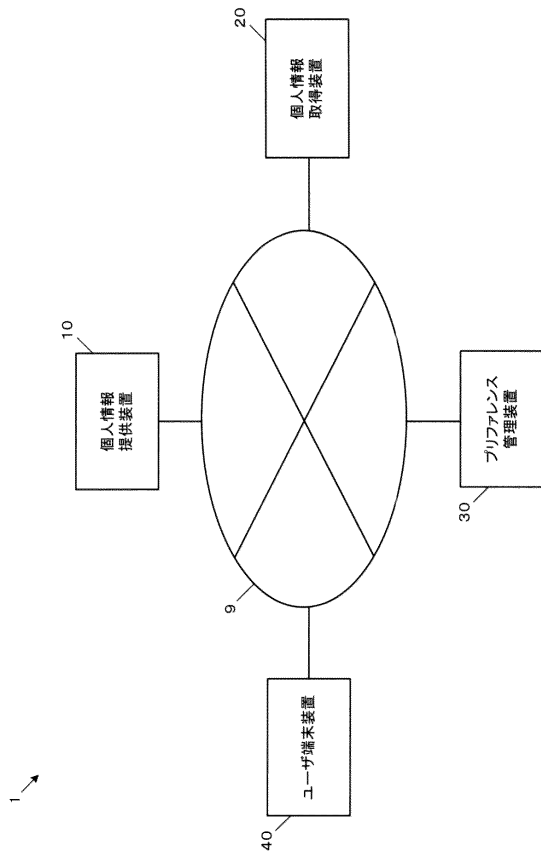
712 個人情報管理部

50

- 7 1 3 アプリケーション部
- 7 1 4 サービス提供部
- 7 1 5 個人情報送受信部
- 8 0 2 変更内容設定部
- 9 1 0 連携装置情報格納部
- 9 1 1 取扱情報格納部
- 9 1 2 取扱情報取得部
- 9 1 3 確認用プリファレンス推定部

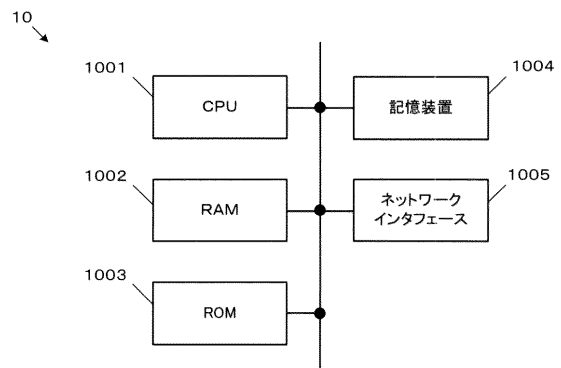
【 図 1 】

図1



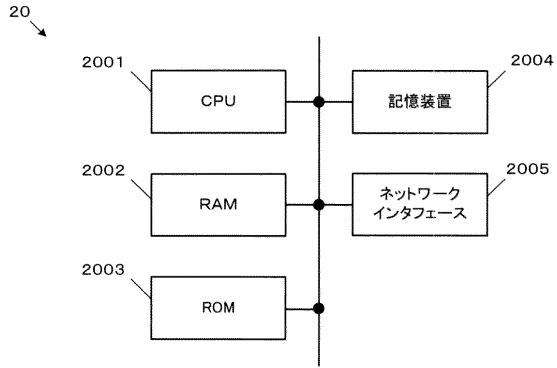
【 図 2 】

図2



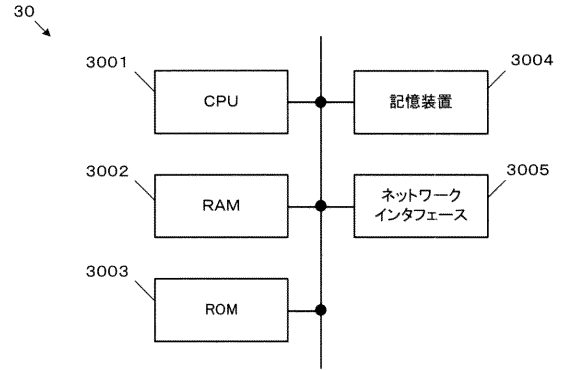
【 図 3 】

図3



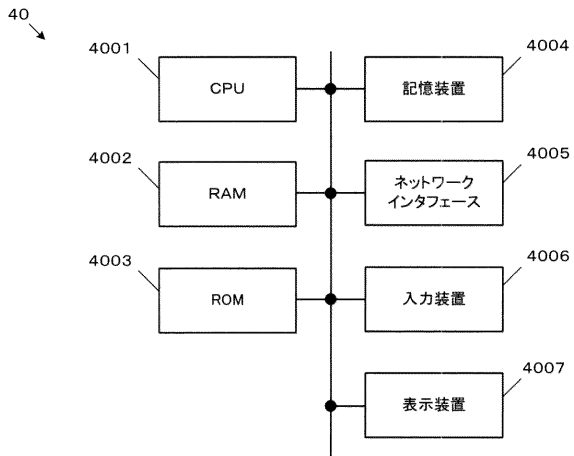
【 図 4 】

図4



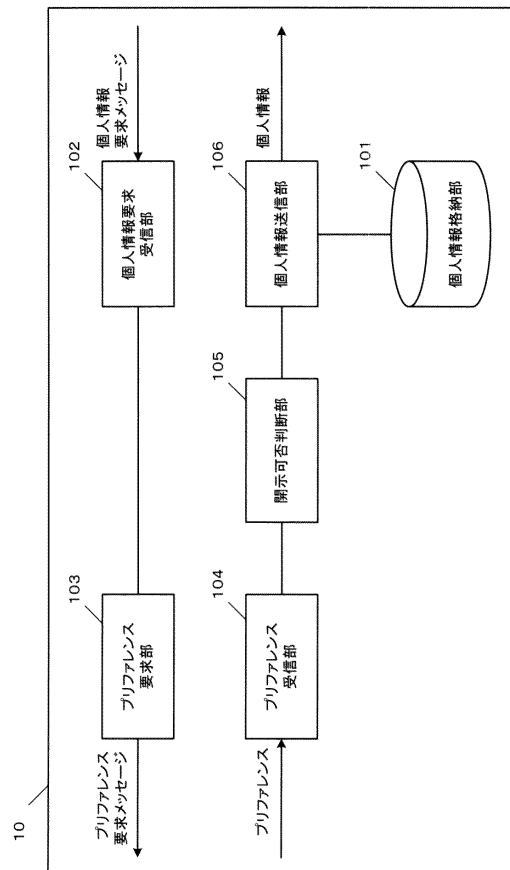
【 図 5 】

図5



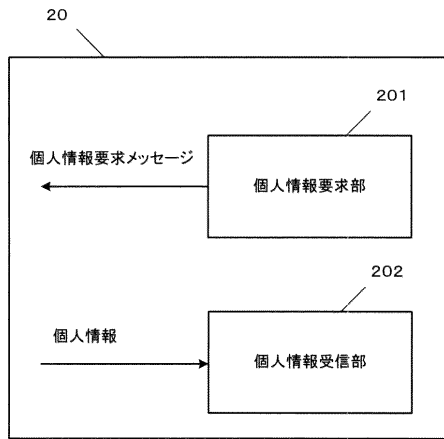
【 図 6 】

図6



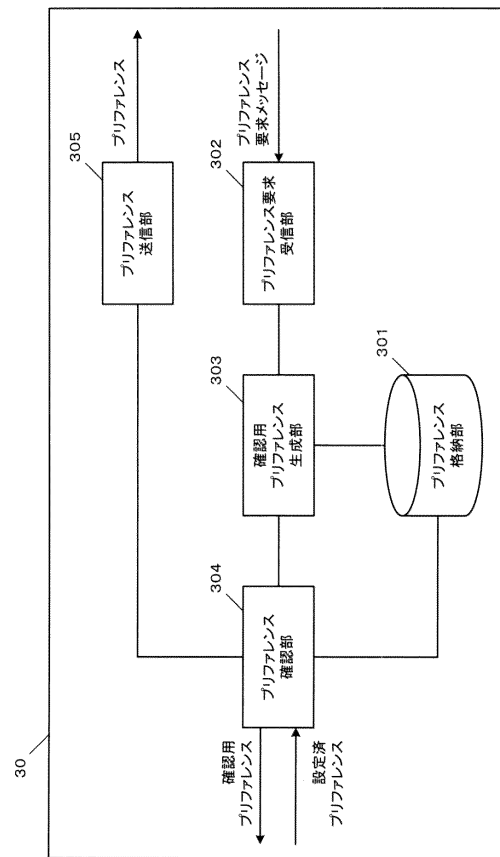
【 図 7 】

図7



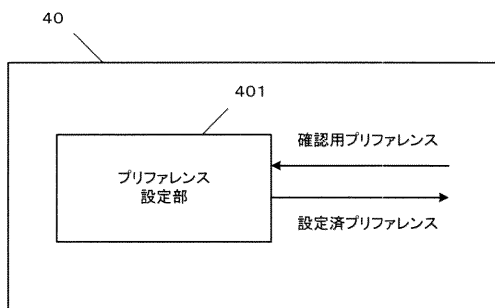
【 図 8 】

図8



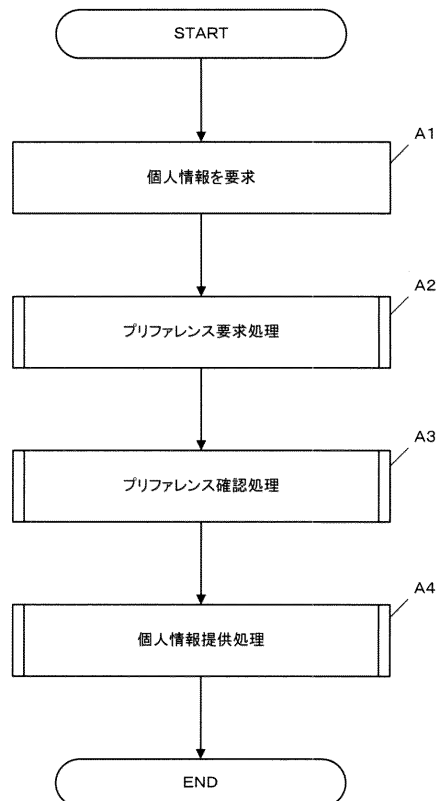
【 図 9 】

図9



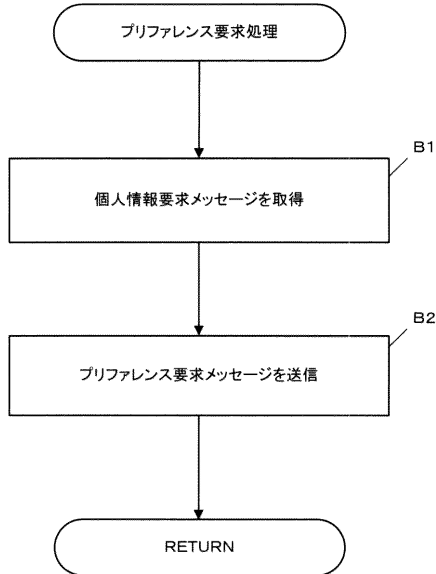
【 図 10 】

図10



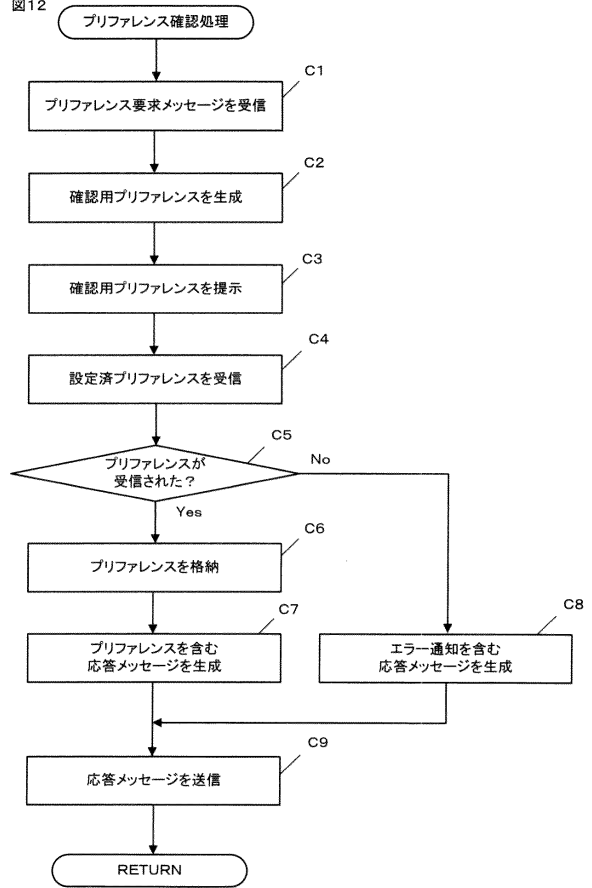
【 図 1 1 】

図11



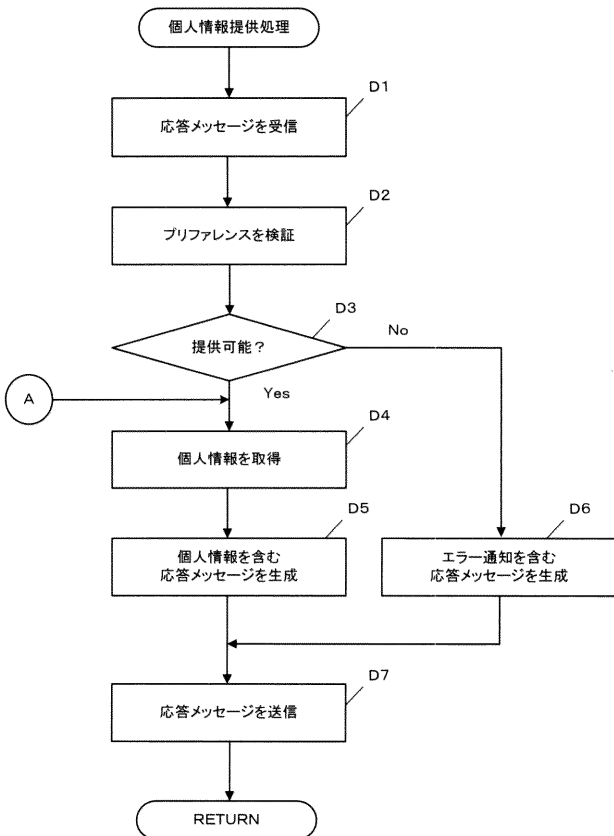
【 図 1 2 】

図12



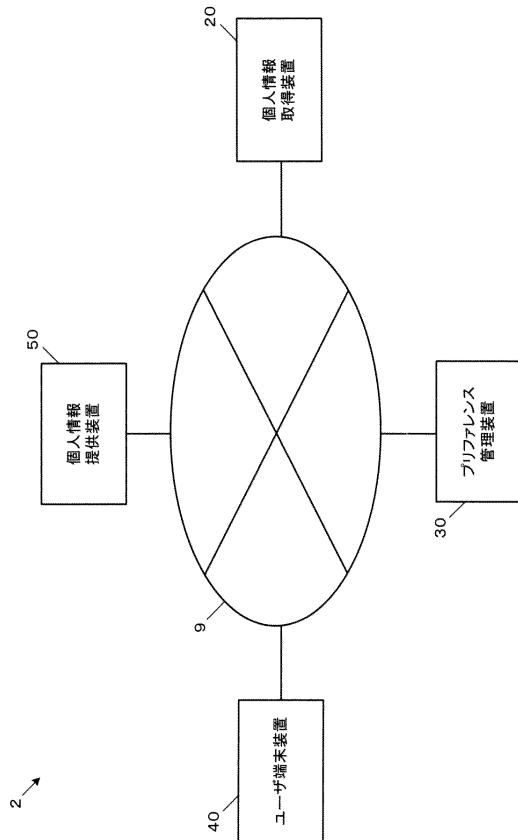
【 図 1 3 】

図13



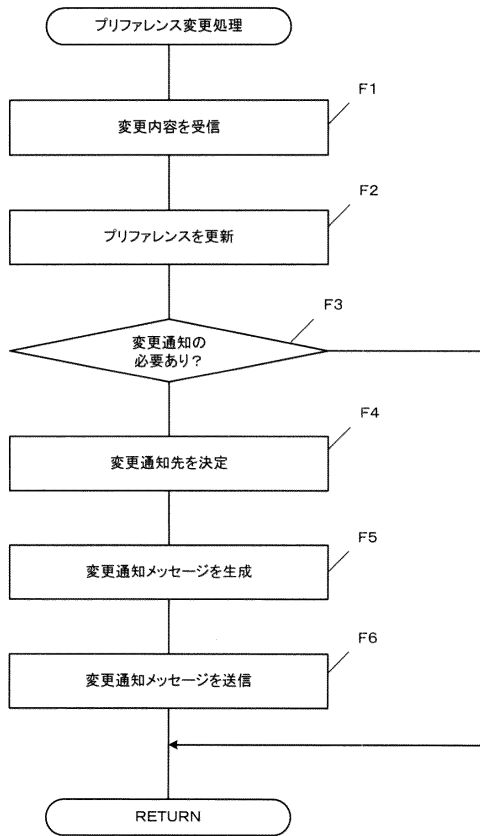
【 図 1 4 】

図14



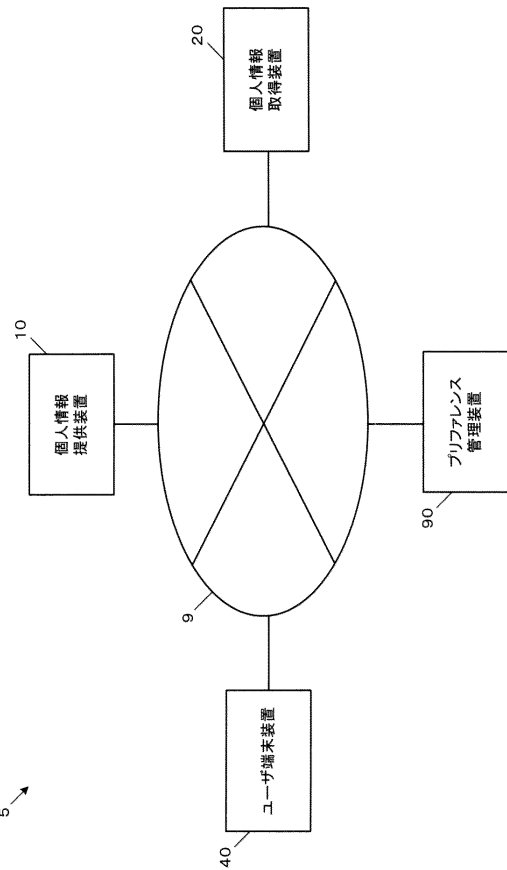
【図23】

図23



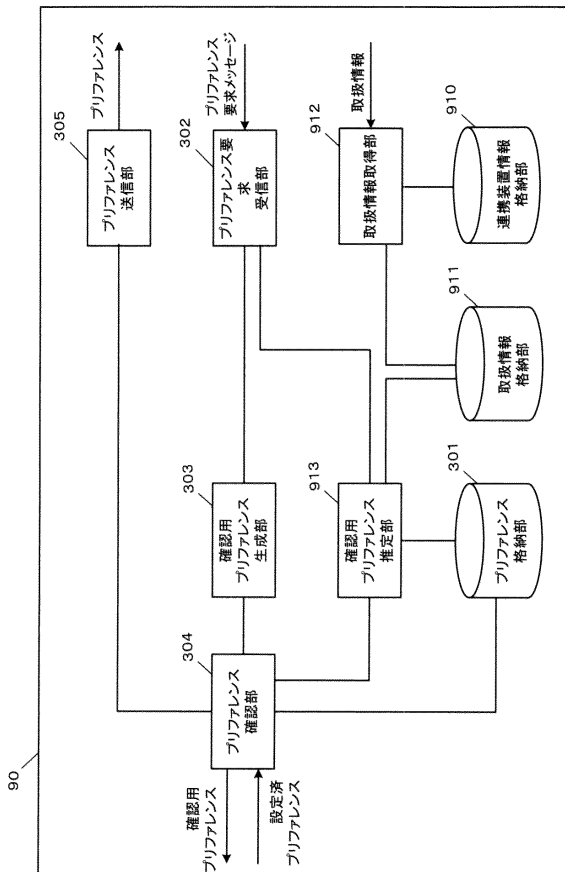
【図24】

図24



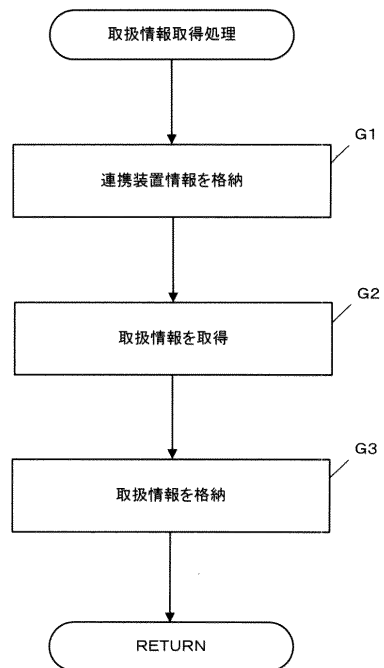
【図25】

図25



【図26】

図26



【図27】

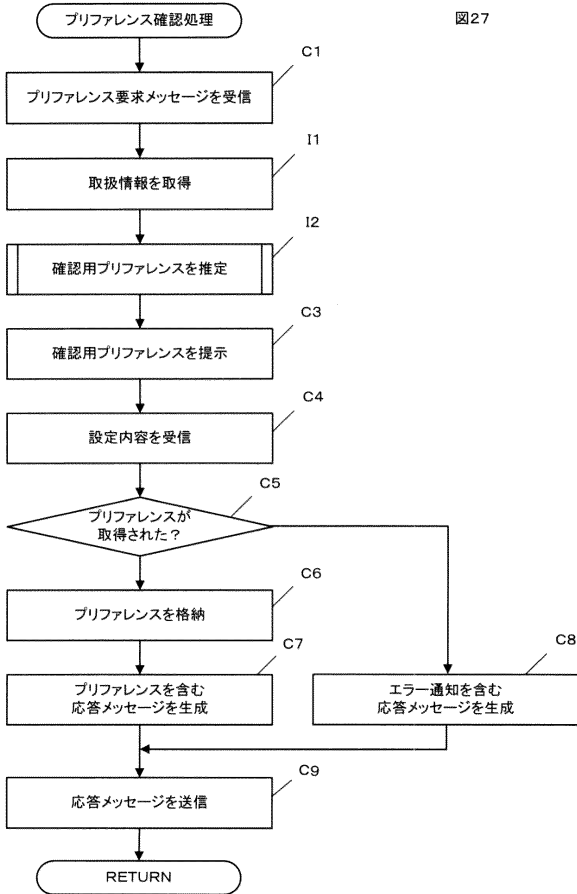


図27

【図28】

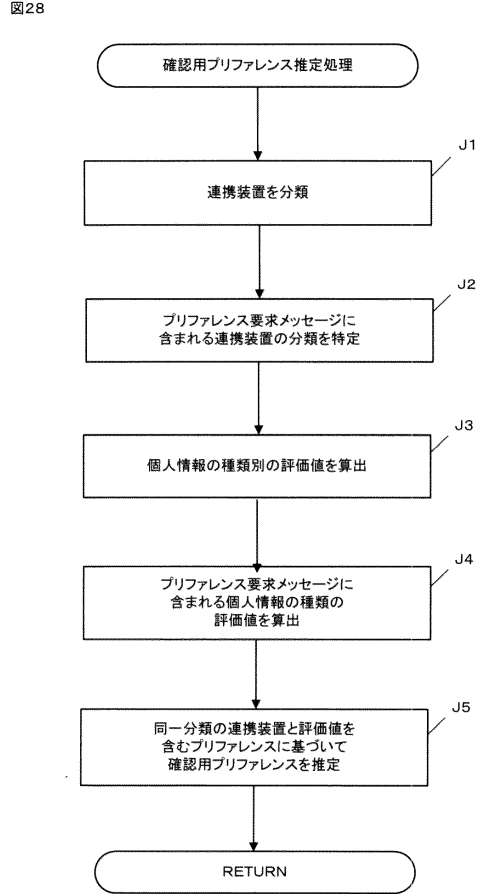


図28

【図29】

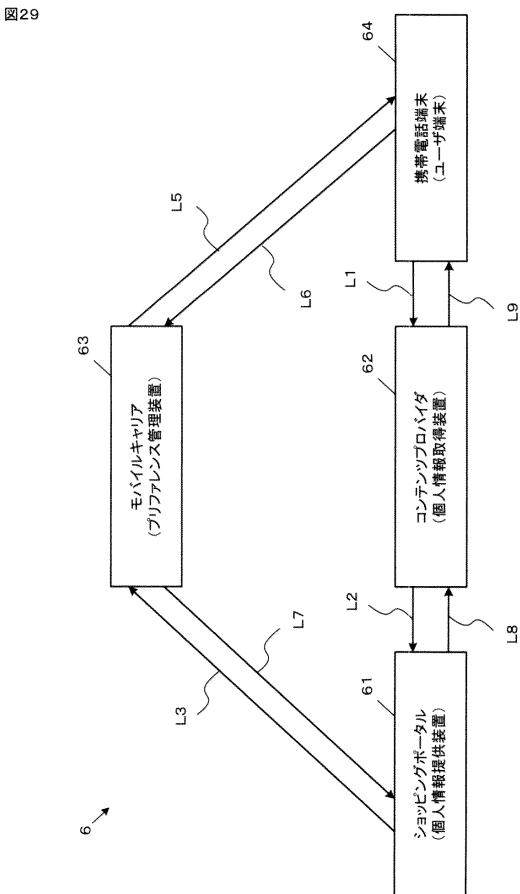


図29

【図30】

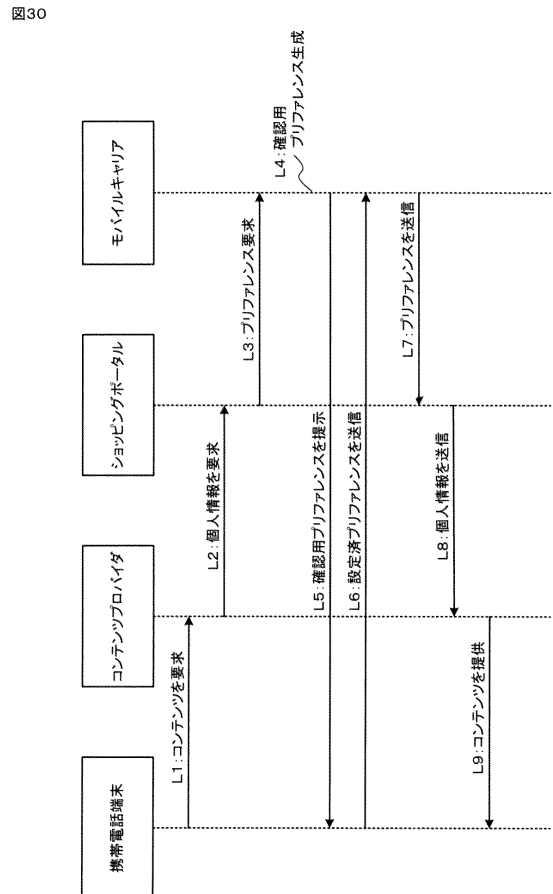
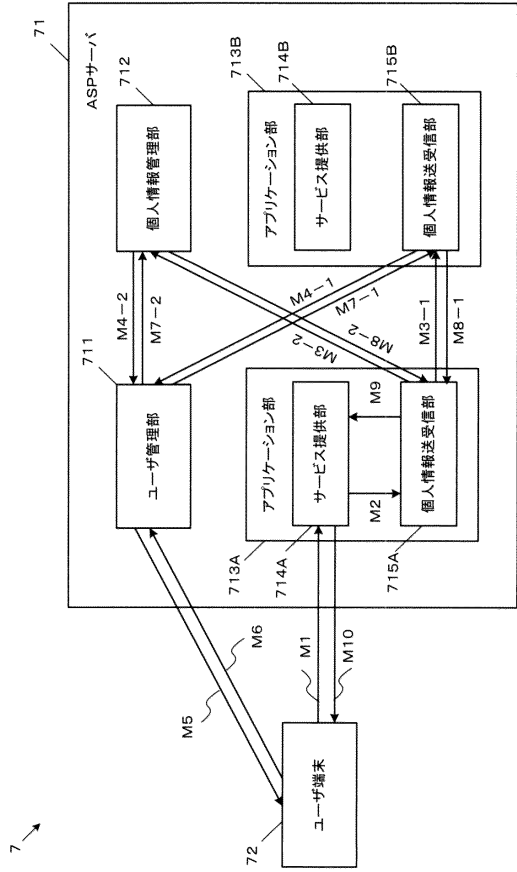


図30

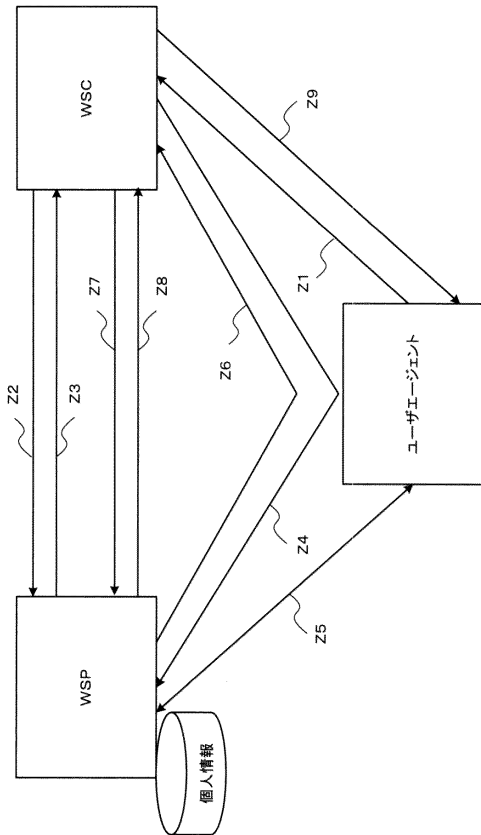
【 図 3 1 】

図31



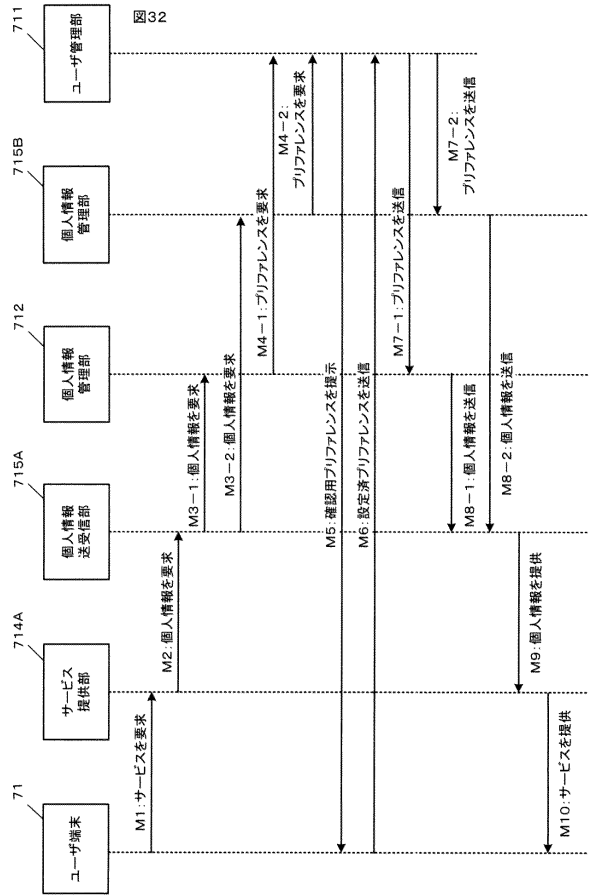
【 図 3 3 】

図33



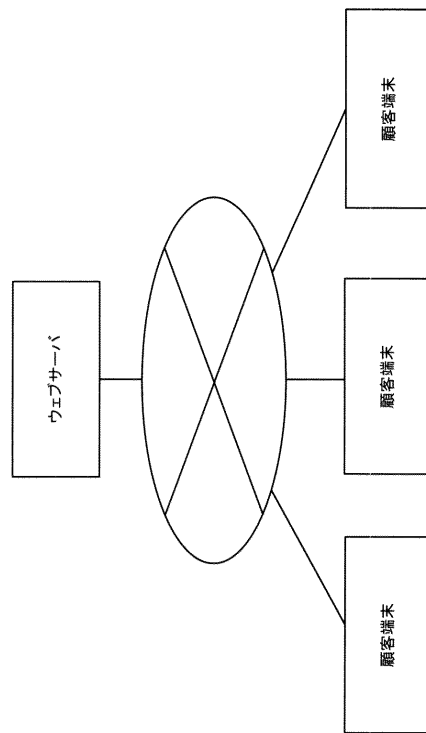
【 図 3 2 】

図32



【 図 3 4 】

図34



【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2011/072695
A. CLASSIFICATION OF SUBJECT MATTER G06Q50/10 (2012.01) i, G06F21/24 (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) G06Q50/00, G06F21/24 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 1996-2011 Kokai Jitsuyo Shinan Koho 1971-2011 Toroku Jitsuyo Shinan Koho 1994-2011 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.
X A	JP 2006-031578 A (Nippon Telegraph and Telephone Corp.), 02 February 2006 (02.02.2006), entire text; all drawings (Family: none)	11, 12, 15, 16 1-10, 13, 14, 17, 18
A	JP 2009-258826 A (NEC Corp.), 05 November 2009 (05.11.2009), entire text; all drawings (Family: none)	1-18
A	JP 2009-199573 A (Nippon Telegraph and Telephone Corp.), 03 September 2009 (03.09.2009), entire text; all drawings (Family: none)	1-18
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> 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 27 December, 2011 (27.12.11)		Date of mailing of the international search report 17 January, 2012 (17.01.12)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/072695

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2009/110277 A1 (NEC Corp.), 11 September 2009 (11.09.2009), entire text; all drawings (Family: none)	1-18
A	JP 2010-092110 A (Fujitsu Ltd.), 22 April 2010 (22.04.2010), entire text; all drawings & US 2010/0088743 A1 & EP 2172869 A2 & KR 10-2010-0038141 A & CN 101714227 A	1-18
A	JP 2004-192353 A (Nippon Telegraph and Telephone Corp.), 08 July 2004 (08.07.2004), entire text; all drawings (Family: none)	1-18

国際調査報告		国際出願番号 PCT/JP2011/072695									
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G06Q50/10(2012.01)i, G06F21/24(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 (IPC)) Int.Cl. G06Q50/00, G06F21/24											
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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2011年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2011年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2011年</td> </tr> </table>				日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2011年	日本国実用新案登録公報	1996-2011年	日本国登録実用新案公報	1994-2011年
日本国実用新案公報	1922-1996年										
日本国公開実用新案公報	1971-2011年										
日本国実用新案登録公報	1996-2011年										
日本国登録実用新案公報	1994-2011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									
X A	JP 2006-031578 A (日本電信電話株式会社) 2006.02.02, 全文, 全図 (ファミリーなし)	11, 12, 15, 16 1-10, 13, 14, 17, 18									
A	JP 2009-258826 A (日本電気株式会社) 2009.11.05, 全文, 全図 (ファミリーなし)	1-18									
A	JP 2009-199573 A (日本電信電話株式会社) 2009.09.03, 全文, 全図 (ファミリーなし)	1-18									
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> 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		の日の後に公表された文献									
「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		「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									
「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		「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									
「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)		「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									
「O」口頭による開示、使用、展示等に言及する文献		「&」同一パテントファミリー文献									
「P」国際出願日前で、かつ優先権の主張の基礎となる出願											
国際調査を完了した日 27.12.2011		国際調査報告の発送日 17.01.2012									
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 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) 唐橋 拓史	5L 3575								
		電話番号 03-3581-1101 内線	3562								

国際調査報告		国際出願番号 PCT/J P 2 0 1 1 / 0 7 2 6 9 5
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
A	WO 2009/110277 A1 (日本電気株式会社) 2009. 09. 11, 全文, 全図 (ファミリーなし)	1-18
A	JP 2010-092110 A (富士通株式会社) 2010. 04. 22, 全文, 全図 & US 2010/0088743 A1 & EP 2172869 A2 & KR 10-2010-0038141 A & CN 101714227 A	1-18
A	JP 2004-192353 A (日本電信電話株式会社) 2004. 07. 08, 全文, 全 図 (ファミリーなし)	1-18

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, T J, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, R O, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, H U, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI , NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN

(注) この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。