(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-20643
(P2013-20643A)
(43)公開日　平成25年1月31日(2013.1.31)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/60	(2013.01)	G06F	21/24	160C	5B084
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104
G06Q 50/26	(2012.01)	G06F	17/60	140	
G06F 21/33	(2013.01)	G06F	21/20	133	
G06F 21/62	(2013.01)	G06F	21/24	160B	

審査請求 有　請求項の数 8　ＯＬ　（全 19 頁）　最終頁に続く

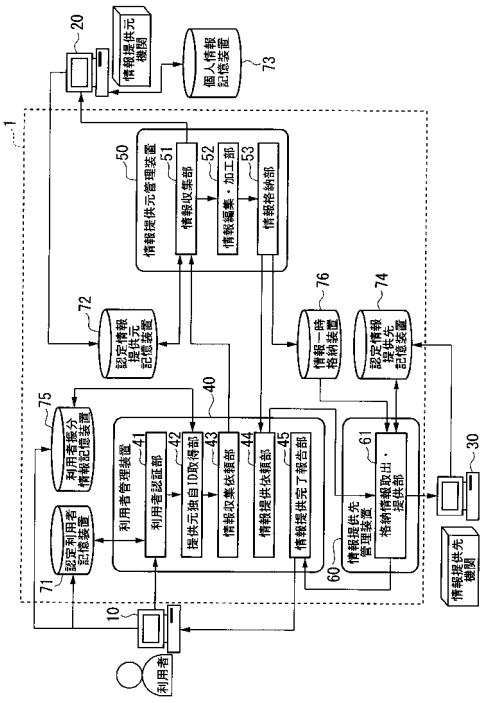
(21)出願番号　特願2012-221660 (P2012-221660)
(22)出願日　平成24年10月3日 (2012.10.3)
(62)分割の表示　特願2008-327684 (P2008-327684)の分割
原出願日　平成20年12月24日 (2008.12.24)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100108453
弁理士　村山　靖彦
(72)発明者　新倉　陽子
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　湊　章枝
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

最終頁に続く

(54)【発明の名称】個人情報提供装置、および個人情報提供方法

(57)【要約】
【課題】個人情報保有機関から第三者機関へ個人情報の送信を、その個人情報の本人の意思に基づいて行うことを可能とする。
【解決手段】個人情報提供装置が、利用者端末から送信される情報取得依頼に応じて、情報提供元装置の識別情報が示す情報提供元装置から、当該情報提供元装置の識別情報に対応付けられた利用者識別情報に対応する個人情報を読み出し、読み出した当該個人情報を、情報一時格納部に記憶させ、利用者端末から送信される情報提供依頼に応じて、情報一時格納部に記憶された個人情報を読み出し、読み出した当該個人情報を、利用者識別情報に対応する情報提供先装置の識別情報が示す情報提供先装置に送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
利用者を識別する利用者識別情報に対応付けられた前記利用者の個人情報がそれぞれに記憶された複数の情報提供元装置と、前記個人情報の提供を受ける複数の情報提供先装置と、前記利用者の利用者端末とネットワークを介して接続される個人情報提供装置であって、
前記個人情報を一時的に記憶する情報一時格納部と、
前記利用者端末から送信される情報取得依頼に応じて、前記情報提供元装置の識別情報が示す前記情報提供元装置から、当該情報提供元装置の識別情報に対応付けられた前記利用者識別情報に対応する前記個人情報を読み出し、読み出した当該個人情報を、前記情報一時格納部に記憶させる情報提供元管理部と、
前記利用者端末から送信される情報提供依頼に応じて、前記情報一時格納部に記憶された前記個人情報を読み出し、読み出した当該個人情報を、前記利用者識別情報に対応する前記情報提供先装置の識別情報が示す前記情報提供先装置に送信する情報提供部と、
を備えることを特徴とする個人情報提供装置。
【請求項２】
前記利用者端末から、前記複数の情報提供元装置のうち、前記個人情報の送信を依頼する前記情報提供元装置の識別情報を受信する情報提供元識別情報受信部と、
前記利用者端末から送信される情報提供先機関リストの伝送依頼に応じて、前記情報提供先装置の識別情報が情報提供先リストとして記憶されている情報提供先記憶部から読み出した前記情報提供先リストを前記利用者端末に送信し、前記送信した前記情報提供先リストの中から選択された前記情報提供先装置の識別情報を前記利用者端末から受信する情報提供先識別情報受信部と、
前記利用者を識別する利用者識別情報と、前記情報提供元識別情報受信部が受信した前記情報提供元装置の識別情報と、前記情報提供先識別情報受信部が受信した前記情報提供先装置の識別情報とが対応付けられた利用者振分情報が記憶される利用者振分情報記憶部と、
を備え、
前記情報提供元管理部は、
前記利用者端末から送信される情報取得依頼に応じて、前記利用者振分情報記憶部に記憶された前記利用者振分情報に基づいて、前記情報提供元装置の識別情報が示す前記情報提供元装置から、当該情報提供元装置の識別情報に対応付けられた前記利用者識別情報に対応する前記個人情報を読み出し、読み出した当該個人情報を、前記情報一時格納部に記憶させ、
前記情報提供部は、
前記利用者端末から送信される情報提供依頼に応じて、前記利用者振分情報記憶部に記憶された前記利用者振分情報に基づいて、前記情報一時格納部に記憶された前記個人情報を読み出し、読み出した当該個人情報を、前記利用者識別情報に対応する前記情報提供先装置の識別情報が示す前記情報提供先装置に送信する
ことを特徴とする請求項１に記載の個人情報提供装置。
【請求項３】
前記情報提供元識別情報受信部は、
前記利用者端末から送信される情報提供元機関リストの伝送依頼に応じて、前記情報提供元装置の識別情報が情報提供元リストとして記憶されている情報提供元記憶部から読み出した前記情報提供元リストを前記利用者端末に送信し、前記送信した前記情報提供元リストの中から選択された前記情報提供元装置の識別情報を前記利用者端末から受信することにより、前記利用者端末から、前記複数の情報提供元装置のうち、前記個人情報の送信を依頼する前記情報提供元装置の識別情報を受信する
ことを特徴とする請求項２に記載の個人情報提供装置。
【請求項４】

前記情報提供元装置から利用登録申込フォームを受信し、前記受信した利用登録申込フォームを前記利用者端末に送信し、前記利用者端末から送信された入力済み利用登録申込フォームを前記利用者端末から受信し、前記受信した入力済み利用登録申込フォームに入力された情報の形式的なチェックを行い、不正な入力がないか否かを判定する管理部、
を備え、
前記利用者振分情報記憶部には、前記管理部により不正な入力がないと判定された場合、前記利用者識別情報と前記情報提供元装置の識別情報とを対応付けた前記利用者振分情報が記憶される、
ことを特徴とする請求項２または請求項３に記載の個人情報提供装置。
【請求項５】
前記利用者振分情報記憶部は、前記利用者識別情報と、前記情報提供元装置の識別情報とに対応付けて、前記情報提供元装置において前記利用者の個人情報を識別する情報提供元独自識別情報を記憶し、
前記情報提供元管理部は、前記利用者振分情報記憶部に記憶されている前記情報提供元独自識別情報に基づいて、前記情報提供元装置から前記個人情報を読み出す
ことを特徴とする請求項１から請求項４のいずれか１項に記載の個人情報提供装置。
【請求項６】
前記情報一時格納部は、
予め定められた期間を過ぎた場合と、定められた情報提供先装置に前記個人情報が送信された場合と、定められた回数の前記個人情報の読み出しがあった場合と、前記利用者端末から前記個人情報を削除する依頼を受信した場合とのうち少なくともいずれかの場合に、自身に記憶された前記個人情報を削除する
ことを特徴とする請求項１から請求項５のいずれか１項に記載の個人情報提供装置。
【請求項７】
前記利用者端末と、前記情報提供元装置と、前記情報提供先装置とのそれぞれに対応する電子証明書を予め生成して発行する電子署名生成部をさらに備え、
前記利用者端末と、前記情報提供元装置と、前記情報提供先装置とのいずれかの装置と前記ネットワークを介して通信する際には、前記電子証明書に基づく認証判定処理を行い、認証しない場合には、当該装置と通信を行わない
ことを特徴とする請求項１から請求項６のいずれか１項に記載の個人情報提供装置。
【請求項８】
利用者を識別する利用者識別情報に対応付けられた前記利用者の個人情報がそれぞれに記憶された複数の情報提供元装置と、前記個人情報の提供を受ける複数の情報提供先装置と、前記利用者の利用者端末とネットワークを介して接続される個人情報提供装置の個人情報提供方法であって、
前記利用者端末から送信される情報取得依頼に応じて、前記情報提供元装置の識別情報が示す前記情報提供元装置から、当該情報提供元装置の識別情報に対応付けられた前記利用者識別情報に対応する前記個人情報を読み出し、読み出した当該個人情報を、情報一時格納部に記憶させ、
前記利用者端末から送信される情報提供依頼に応じて、前記情報一時格納部に記憶された前記個人情報を読み出し、読み出した当該個人情報を、前記利用者識別情報に対応する前記情報提供先装置の識別情報が示す前記情報提供先装置に送信する
ことを特徴とする個人情報提供方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、個人情報の提供を行う個人情報提供装置、および個人情報提供方法に関する。
【背景技術】
【０００２】

従来、官的機関、公的機関などに保有された公的な個人情報を、その個人情報の本人が第三者機関に提出しようとする場合、一般的に、その個人は個人情報を保有する機関に対して自身の個人情報の証明書の発行を申請し、紙媒体として発行された個人情報を第三者機関に提出する。例えば、引越しをして運転免許証の住所変更を行う際には、市区町村役所の窓口等で紙媒体の住民票を取得し、第三者機関である警察等に持参している。このような公的機関で発行された住民票は、個人の身分証明のために例えば銀行などの第三者機関に持参されることもある。

ところで、特許文献１には、このような個人情報を、その個人情報へのアクセス回数、期間、期限などの制限を示す開示利用規定とともにカプセル化した情報を生成して管理することで、個人情報が転々と流通した場合に、その開示利用規定に基づいた開示が行われるように制御する技術が示されている。特許文献２には、所定の認証機関により高い信頼性が認証された第三者機関によって運用される個人情報管理支援装置が、クレジットカード会社のような複数の契約企業の個人情報管理システムに記憶される個人情報へのアクセスを仲介する技術が示されている。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００３－３４５９３１号公報

【特許文献２】特開２００４－３４８７００号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

しかしながら、ある個人情報保有機関に保有された個人情報を第三者機関に提出する際、個人情報保有機関において紙媒体の個人情報の発行を受け、第三者機関に持参するのは個人にとって面倒である。そこで、情報通信ネットワークを介して個人情報保有機関から第三者機関へ個人情報を送信することが考えられるが、この際には、その個人情報の情報提供元の個人情報保有機関や情報提供先の第三者機関が本人の意思に基づいて決定され、漏洩やなりすましなどの脅威なく安全に行われることが望ましい。上述の特許文献に記載された技術は、このような特定の個人情報保有機関から他の特定の第三者機関への個人情報を送信するものではない。

【０００５】

本発明は、このような状況に鑑みてなされたもので、個人情報保有機関から第三者機関へ個人情報の送信を、その個人情報の本人の意思に基づいて行うことを可能とする個人情報提供装置、および個人情報提供方法を提供する。

【課題を解決するための手段】

【０００６】

上述した課題を解決するために、本発明は、利用者を識別する利用者識別情報に対応付けられた前記利用者の個人情報がそれぞれに記憶された複数の情報提供元装置と、前記個人情報の提供を受ける複数の情報提供先装置と、前記利用者の利用者端末とネットワークを介して接続される個人情報提供装置であって、前記個人情報を一時的に記憶する情報一時格納部と、前記利用者端末から送信される情報取得依頼に応じて、前記情報提供元装置の識別情報が示す前記情報提供元装置から、当該情報提供元装置の識別情報に対応付けられた前記利用者識別情報に対応する前記個人情報を読み出し、読み出した当該個人情報を、前記情報一時格納部に記憶させる情報提供元管理部と、前記利用者端末から送信される情報提供依頼に応じて、前記情報一時格納部に記憶された前記個人情報を読み出し、読み出した当該個人情報を、前記利用者識別情報に対応する前記情報提供先装置の識別情報が示す前記情報提供先装置に送信する情報提供部と、を備えることを特徴とする。

【０００７】

また、本発明は、前記利用者端末から、前記複数の情報提供元装置のうち、前記個人情報の送信を依頼する前記情報提供元装置の識別情報を受信する情報提供元識別情報受信部

と、前記利用者端末から送信される情報提供先機関リストの伝送依頼に応じて、前記情報提供先装置の識別情報が情報提供先リストとして記憶されている情報提供先記憶部から読み出した前記情報提供先リストを前記利用者端末に送信し、前記送信した前記情報提供先リストの中から選択された前記情報提供先装置の識別情報を前記利用者端末から受信する情報提供先識別情報受信部と、前記利用者を識別する利用者識別情報と、前記情報提供元識別情報受信部が受信した前記情報提供元装置の識別情報と、前記情報提供先識別情報受信部が受信した前記情報提供先装置の識別情報とが対応付けられた利用者振分情報が記憶される利用者振分情報記憶部と、を備え、前記情報提供元管理部は、前記利用者端末から送信される情報取得依頼に応じて、前記利用者振分情報記憶部に記憶された前記利用者振分情報に基づいて、前記情報提供元装置の識別情報が示す前記情報提供元装置から、当該情報提供元装置の識別情報に対応付けられた前記利用者識別情報に対応する前記個人情報を読み出し、読み出した当該個人情報を、前記情報一時格納部に記憶させ、前記情報提供部は、前記利用者端末から送信される情報提供依頼に応じて、前記利用者振分情報記憶部に記憶された前記利用者振分情報に基づいて、前記情報一時格納部に記憶された前記個人情報を読み出し、読み出した当該個人情報を、前記利用者識別情報に対応する前記情報提供先装置の識別情報が示す前記情報提供先装置に送信することを特徴とする。

【０００８】

また、本発明は、前記情報提供元識別情報受信部は、前記利用者端末から送信される情報提供元機関リストの伝送依頼に応じて、前記情報提供元装置の識別情報が情報提供元リストとして記憶されている情報提供元記憶部から読み出した前記情報提供元リストを前記利用者端末に送信し、前記送信した前記情報提供元リストの中から選択された前記情報提供元装置の識別情報を前記利用者端末から受信することにより、前記利用者端末から、前記複数の情報提供元装置のうち、前記個人情報の送信を依頼する前記情報提供元装置の識別情報を受信することを特徴とする。

【０００９】

また、本発明は、前記情報提供元装置から利用登録申込フォームを受信し、前記受信した利用登録申込フォームを前記利用者端末に送信し、前記利用者端末から送信された入力済み利用登録申込フォームを前記利用者端末から受信し、前記受信した入力済み利用登録申込フォームに入力された情報の形式的なチェックを行い、不正な入力がないか否かを判定する管理部、を備え、前記利用者振分情報記憶部には、前記管理部により不正な入力がないと判定された場合、前記利用者識別情報と前記情報提供元装置の識別情報とを対応付けた前記利用者振分情報が記憶される、ことを特徴とする。

【００１０】

また、本発明は、前記利用者振分情報記憶部は、前記利用者識別情報と、前記情報提供元装置の識別情報とに対応付けて、前記情報提供元装置において前記利用者の個人情報を識別する情報提供元独自識別情報を記憶し、前記情報提供元管理部は、前記利用者振分情報記憶部に記憶されている前記情報提供元独自識別情報に基づいて、前記情報提供元装置から前記個人情報を読み出すことを特徴とする。

【００１１】

また、本発明は、前記情報一時格納部は、予め定められた期間を過ぎた場合と、定められた情報提供先装置に前記個人情報が送信された場合と、定められた回数の前記個人情報の読み出しがあった場合と、前記利用者端末から前記個人情報を削除する依頼を受信した場合とのうち少なくともいずれかの場合に、自身に記憶された前記個人情報を削除することを特徴とする。

【００１２】

また、本発明は、前記利用者端末と、前記情報提供元装置と、前記情報提供先装置とのそれぞれに対応する電子証明書を予め生成して発行する電子署名生成部をさらに備え、前記利用者端末と、前記情報提供元装置と、前記情報提供先装置とのいずれかの装置と前記ネットワークを介して通信する際には、前記電子証明書に基づく認証判定処理を行い、認証しない場合には、当該装置と通信を行わないことを特徴とする。

【００１３】
また、本発明は、利用者を識別する利用者識別情報に対応付けられた前記利用者の個人情報がそれぞれに記憶された複数の情報提供元装置と、前記個人情報の提供を受ける複数の情報提供先装置と、前記利用者の利用者端末とネットワークを介して接続される個人情報提供装置の個人情報提供方法であって、前記利用者端末から送信される情報取得依頼に応じて、前記情報提供元装置の識別情報が示す前記情報提供元装置から、当該情報提供元装置の識別情報に対応付けられた前記利用者識別情報に対応する前記個人情報を読み出し、読み出した当該個人情報を、情報一時格納部に記憶させ、前記利用者端末から送信される情報提供依頼に応じて、前記情報一時格納部に記憶された前記個人情報を読み出し、読み出した当該個人情報を、前記利用者識別情報に対応する前記情報提供先装置の識別情報が示す前記情報提供先装置に送信することを特徴とする。
【発明の効果】
【００１４】
以上説明したように、本発明によれば、個人情報提供装置が、利用者端末から送信される情報取得依頼に応じて、情報提供元装置の識別情報が示す情報提供元装置から、当該情報提供元装置の識別情報に対応付けられた利用者識別情報に対応する個人情報を読み出し、読み出した当該個人情報を、情報一時格納部に記憶させ、利用者端末から送信される情報提供依頼に応じて、情報一時格納部に記憶された個人情報を読み出し、読み出した当該個人情報を、利用者識別情報に対応する情報提供先装置の識別情報が示す情報提供先装置に送信するようにしたので、個人情報保有機関から第三者機関へ個人情報の送信を、その個人情報の本人の意思に基づいて行うことが可能となる。
【図面の簡単な説明】
【００１５】
【図１】本発明の一実施形態による個人情報提供システムの構成を示すブロック図である。
【図２】本発明の一実施形態による個人情報記憶装置に記憶されるデータ例を示す図である。
【図３】本発明の一実施形態による利用者振分情報記憶装置に記憶されるデータ例を示す図である。
【図４】本発明の一実施形態による情報提供元装置の事前登録処理の例を示す図である。
【図５】本発明の一実施形態による情報提供先装置の事前登録処理の例を示す図である。
【図６】本発明の一実施形態による利用者端末の事前登録処理の例を示す図である。
【図７】本発明の一実施形態による利用者端末により情報提供元装置が選択される動作例を示す図である。
【図８】本発明の一実施形態による利用者端末により情報提供先装置が選択される動作例を示す図である。
【図９】本発明の一実施形態により個人情報が取得される動作例を示す図である。
【図１０】本発明の一実施形態により個人情報が送信される動作例を示す図である。
【発明を実施するための形態】
【００１６】
以下、本発明の一実施形態について、図面を参照して説明する。
図１は、本実施形態による個人情報提供システム１の構成を示すブロック図である。個人情報提供システム１は、利用者管理装置４０と、情報提供元管理装置５０と、情報提供先管理装置６０と、認定利用者記憶装置７１と、認定情報提供元記憶装置７２と、個人情報記憶装置７３と、認定情報提供先記憶装置７４と、利用者振分情報記憶装置７５と、情報一時格納装置７６とを備えている。また、個人情報提供システム１は、ネットワークを介して利用者端末１０と、情報提供元装置２０と、情報提供先装置３０と接続されている。ここで、利用者端末１０と、情報提供元装置２０と、情報提供先装置３０とはコンピュータ装置でありそれぞれ１台を図示して説明するが、個人情報提供システム１は、これらと同様の構成を備えるそれぞれ複数台のコンピュータ装置に接続されても良い。

【００１７】
利用者端末１０は、情報提供元管理装置５０に対応する個人情報記憶装置７３に個人情報が記憶された利用者によって利用されるコンピュータ端末である。利用者端末１０は、ネットワークを介して利用者管理装置４０、情報提供先管理装置６０と接続されており情報通信が可能である。利用者端末１０は、予め備えたインターネットブラウザの機能により他のコンピュータ装置と通信を行う。利用者端末１０は、具体的には、ＰＣ（パーソナルコンピュータ）、ＰＤＡ（Personal Digital Assistant）、携帯電話端末などの、入力部、出力部、制御部、演算部、記憶部を備えたコンピュータ機器が適用される。ここで、出力部には、表示部、音声出力部などが適用される。
【００１８】
情報提供元装置２０は、利用者の個人情報を保有する情報提供元機関に利用されるコンピュータ装置である。情報提供元機関は、国や自治体、警察、医療保険者などの官的、公的な個人情報保有機関である。情報提供元装置２０は、個人情報記憶装置７３に接続される。個人情報記憶装置７３には、情報提供元装置２０に対応する情報提供元機関に保有される個人情報が予め記憶される。図２は、個人情報記憶装置７３に記憶される個人情報のデータ例を示す図である。個人情報記憶装置７３には、情報提供元独自ＩＤに対応付けられて個人情報が記憶される。情報提供元独自ＩＤは、複数の情報提供元機関のうち特定の情報提供元機関が独自に利用者を識別する識別情報である。個人情報は、個人を特定する情報、或いは、個人の属性、特性等の情報であり、例えば、氏名、年齢、住所地、職業、保有資産、所得、勤務先、本籍地、家族構成、通院歴、保険、年金、健診結果などに関する情報である。情報提供元装置２０は、自身が個人情報を保有する利用者の利用者端末１０から、個人情報提供システム１を利用した個人情報の送信についての利用依頼を受信すると、その利用者端末１０に対して利用登録フォームを送信して、個人情報提供システム１を利用することの利用者本人の意思を確認する。利用登録フォームは、例えば、本人確認を行うことが可能な利用者の識別情報などの入力項目を備えている。利用者端末１０から情報入力済みの利用登録フォームを受信した情報提供元装置２０の情報提供元機関は、利用登録フォームに入力された情報に基づいて利用者の審査を行い、個人情報の本人が利用登録を希望していると認定する。
【００１９】
情報提供先装置３０は、個人情報記憶装置７３に記憶された個人情報の情報提供先となる情報提供先機関に利用されるコンピュータ装置である。情報提供先機関は、自治体や警察などの官的、公的な機関でも良いし、銀行や不動産会社などの民間企業でも良いし、学校などの教育機関などでも良い。
【００２０】
利用者管理装置４０と、情報提供元管理装置５０と、情報提供先管理装置６０とは、所定の認定機関によって管理される。この認定機関は、官的、公的機関によって個人情報を扱うことを認定された機関であり、情報提供元装置２０を利用する情報提供元機関と、情報提供先装置３０を利用する情報提供先機関と、利用者端末１０を利用する利用者とのそれぞれについて、個人情報提供システム１を利用することを許可するか否かについての認定審査を行う。ここで、情報提供元機関や情報提供先機関の認定審査とは、例えば、その機関が法律や慣習等に照らし、漏洩等の脅威に対して適切な個人情報の取り扱いを行っているか否か等の条件が予め定められた審査基準を満たすか否かを審査することであり、審査基準を満たす場合には、認定機関は審査対象の情報提供元機関または情報提供先機関を認定する。利用者の認定審査とは、その利用者に対応する個人情報が、確かにその利用者本人の個人情報であるか否かを審査することであり、確かにその利用者本人の個人情報であるとされる場合には、利用者を認定する。ここで、情報提供元機関、情報提供先機関、利用者を認定する認定機関は、それぞれ異なる認定機関であっても良いが、官的、公的機関によって個人情報を扱うことを認定された機関であることが望ましい。
【００２１】
利用者管理装置４０は、認定機関により管理され、個人情報提供システム１が備える各

コンピュータ装置および利用者端末１０と通信を行うコンピュータ装置であり、利用者認証部４１と、提供元独自ＩＤ取得部４２と、情報収集依頼部４３と、情報提供依頼部４４と、情報提供完了報告部４５とを備えている。

利用者認証部４１は、利用者端末１０と通信を行う際、予め利用者端末１０の利用者に対して発行された電子証明書に基づいて利用者の認証判定処理を行う。電子証明書は、ＰＫＩ（Public Key Infrastructure）に基づいて利用者に発行された情報であり、利用者を識別する利用者ＩＤの正当性を判定する情報である。このような電子証明書は、利用者ＩＤとともにＩＣカードなどに記憶され、認定された利用者に予め発送されるようにしても良い。認証判定処理において、利用者認証部４１は、利用者ＩＤとともに利用者端末１０から送信される電子証明書が、利用者ＩＤに基づいて生成された情報であるか否かを予め定められたアルゴリズムにより判定する。利用者認証部４１は、電子証明書が利用者ＩＤに基づいて生成されたと判定した場合には、その利用者ＩＤは正当であると判定し、利用者ＩＤと電子証明書とを送信した利用者端末１０を認証する。利用者認証部４１は、電子証明書が利用者ＩＤに基づいて生成されていないと判定した場合には、その利用者ＩＤは正当でないと判定し、利用者ＩＤと電子証明書とを送信した利用者端末１０を認証しない。

【００２２】

提供元独自ＩＤ取得部４２は、利用者端末１０から送信される利用者ＩＤと、個人情報の送信を依頼する情報提供元機関を識別する情報提供元機関ＩＤとを受信し、利用者ＩＤと情報提供元機関ＩＤとに対応する情報提供元独自ＩＤを利用者振分情報記憶装置７５から読み出す。図３は、利用者振分情報記憶装置７５に記憶された情報提供元機関の利用者振分情報のデータ例を示す図である。利用者振分情報記憶装置７５には、利用者ＩＤと、情報提供元機関ＩＤと、情報提供元独自ＩＤとが対応付けられて記憶される。利用者ＩＤは、情報提供元機関の別に関わらず利用者管理装置４０によって利用者を識別する識別情報である。情報提供元機関ＩＤは、複数の情報提供元機関のうちで特定の情報提供元機関を識別する識別情報である。情報提供元独自ＩＤは、複数の情報提供元機関のうちの特定の情報提供元機関が独自に利用者を識別する識別情報である。

【００２３】

情報収集依頼部４３は、提供元独自ＩＤ取得部４２が利用者振分情報記憶装置７５から読み出した情報提供元独自ＩＤに対応する個人情報の提供依頼を情報提供元管理装置５０に送信する。

情報提供依頼部４４は、利用者端末１０から送信される情報提供依頼に基づいて、情報提供先管理装置６０に情報提供先装置３０への個人情報の提供依頼を送信する。

情報提供完了報告部４５は、情報提供依頼部４４によって情報提供先装置３０に個人情報の提供依頼が送信された後、情報提供先装置３０から個人情報の提供が完了したことを示す完了通知を受信すると、利用者端末１０に完了通知を転送する。

【００２４】

情報提供元管理装置５０は、認定機関により管理され、個人情報提供システム１が備える各コンピュータ装置および情報提供元装置２０と通信を行うコンピュータ装置である。情報提供元管理装置５０は、情報提供元装置２０と通信を行う際には、予め情報提供元装置２０に送信された電子証明書に基づく認証判定処理を行い、認証した場合に通信を行い、認証しない場合には通信を行わない。情報提供元管理装置５０は、情報収集部５１と、情報編集・加工部５２と、情報格納部５３とを備えている。

【００２５】

情報収集部５１は、利用者管理装置４０から送信される個人情報の提供依頼を受信すると、情報提供元装置２０に個人情報の提供依頼を送信し、情報提供元装置２０から返信される個人情報を受信する。

情報編集・加工部５２は、情報収集部５１が受信した個人情報に対して、改ざん防止などのための暗号化や電子署名を付与する処理等を行い、発行証明書を生成する。これにより、個人情報が情報提供先機関に提供された後に改ざんされることを防ぐことが可能であ

る。
情報格納部５３は、情報収集部５１が取得した個人情報と情報編集・加工部５２によって生成された発行証明書とを情報一時格納装置７６に送信する。
【００２６】
情報提供先管理装置６０は、認定機関により管理され、個人情報提供システム１が備える各コンピュータ装置および情報提供先装置３０と通信を行うコンピュータ装置である。情報提供先管理装置６０は、情報提供先装置３０と通信を行う際には、予め情報提供先装置３０に送信された電子証明書に基づく認証判定処理を行い、認証した場合に通信を行い、認証しない場合には通信を行わない。情報提供先管理装置６０は、格納情報取出・提供部６１を備えている。格納情報取出・提供部６１は、利用者管理装置４０から送信される個人情報の提供依頼に応じて、情報一時格納装置７６格納された個人情報を、情報提供先装置３０に送信する。
【００２７】
認定利用者記憶装置７１には、認定機関によって正当性が認定された利用者の利用者情報が記憶される。利用者情報は、利用者を識別する利用者ＩＤや、当該利用者を認証するためのパスワードなどの情報が含まれても良い。
認定情報提供元記憶装置７２には、認定機関によって正当性が認定された複数の情報提供元機関の識別情報がリスト化された情報提供元機関リストが記憶される。
個人情報記憶装置７３には、上述したような個人情報が記憶される。
認定情報提供先記憶装置７４には、認定機関によって正当性が認定された複数の情報提供先機関の識別情報がリスト化された情報提供先機関リストが記憶される。
【００２８】
利用者振分情報記憶装置７５には、上述したような情報提供元の利用者振分情報（情報提供元）の他に、利用者ＩＤと、利用者端末１０から依頼された個人情報の情報提供先を識別する情報提供先ＩＤとを対応付けた情報提供先の利用者振分情報（情報提供先）が記憶される。
【００２９】
情報一時格納装置７６には、情報提供元管理装置５０によって情報提供元装置２０を介して個人情報記憶装置７３から読み出された個人情報が記憶される。このように個人情報提供システム１によって提供される個人情報は、情報一時格納装置７６に格納されるため、例えば複数の情報提供先装置３０に対して個人情報を提供するような場合に、情報提供元装置２０から個人情報を複数回読み出すことなく、情報一時格納装置７６に記憶された個人情報を複数の情報提供先装置３０に提供できる。このため、個人情報記憶装置７３から個人情報を読み出す回数を減らし、またネットワークや情報提供元装置２０の処理負荷を下げるとともに漏洩のリスクを軽減することができる。また、情報一時格納装置７６に記憶された個人情報は、記憶された後に定められた条件を満たすと判定されると情報一時格納装置７６によって削除される。定められた条件とは、例えば、記憶された後に予め定められた期間を過ぎた場合や、定められた情報提供先機関の情報提供先装置３０に送信された場合、定められた回数の個人情報の読み出しがあった場合、利用者端末１０から個人情報を削除する明示の依頼を受けた場合などである。
【００３０】
次に、図面を参照して、本発明による個人情報提供システム１によって、認定情報提供元記憶装置７２に記憶される個人情報が情報提供先装置３０に送信される動作例を説明する。
図４は、情報提供元装置２０から個人情報提供システム１への事前登録処理を示す図である。まず、情報提供元装置２０は、情報提供元管理装置５０に認定依頼を送信する（ステップＳ１）。情報提供元管理装置５０が、情報提供元装置２０から送信された認定依頼を受信すると、認定機関は、情報提供元機関の認定審査を行う。認定機関が、情報提供元装置２０の情報提供元機関を認定し、認定したことを示す情報が情報提供元管理装置５０に入力されると（ステップＳ２）、情報提供元管理装置５０は、認定情報提供元記憶装置

７２に情報提供元装置２０の登録依頼を行う（ステップＳ３）。認定情報提供元記憶装置７２は、情報提供元管理装置５０から情報提供元装置２０の登録依頼を受信すると、情報提供元装置２０を識別する情報提供元ＩＤを自身の記憶領域に情報提供元リストとして記憶する（ステップＳ４）。

【００３１】

認定情報提供元記憶装置７２は、情報提供元ＩＤを記憶すると、登録完了通知を情報提供元管理装置５０に送信する（ステップＳ５）。情報提供元管理装置５０は、認定情報提供元記憶装置７２から送信された登録完了通知を受信すると、情報提供元機関の正当性を証明する電子証明書を発行し（ステップＳ６）、情報提供元装置２０に送信して、認定完了通知を送信する（ステップＳ７）。

【００３２】

図５は、情報提供先装置３０から個人情報提供システム１への事前登録処理を示す図である。情報提供先装置３０から個人情報提供システム１への事前登録処理は、図４を用いて説明した情報提供元装置２０から個人情報提供システム１への事前登録処理と同様である。事前登録処理により、情報提供先装置３０は認定機関により認定され、認定された情報提供先機関を識別する情報提供先ＩＤは情報提供先リストとして認定情報提供先記憶装置７４に記憶される。また、認定された情報提供先機関には、その正当性を証明する電子証明書が発行され、情報提供先管理装置６０に送信される。

【００３３】

図６は、利用者端末１０から個人情報提供システム１への事前登録処理を示す図である。利用者端末１０から個人情報提供システム１への事前登録処理は、図４を用いて説明した情報提供元装置２０から個人情報提供システム１への事前登録処理と同様である。事前登録処理により、利用者端末１０は認定機関により認定され、認定された利用者を識別する利用者ＩＤは認定利用者記憶装置７１に記憶される。また、認定された利用者には、その正当性を証明する電子証明書が発行され、利用者ＩＤとともに利用者端末１０に送信される。

【００３４】

図７は、利用者の意思に基づき、利用者の個人情報を保有する情報提供元機関の情報提供元管理装置５０に、個人情報提供システム１を用いて個人情報を送信するための登録が行われる処理動作例を示す図である。

まず、利用者端末１０は、正当性が認定され、利用可能な情報提供元機関の紹介要求を利用者管理装置４０に送信する（ステップＳ３０）。この際、利用者管理装置４０は、ステップＳ２４、２５において利用者端末１０に送信した利用者ＩＤや電子証明書に基づいて、利用者端末１０の認証判定処理を行う（ステップＳ３１）。利用者管理装置４０は、利用者端末１０の認証判定処理において利用者端末１０を認証すると、認定情報提供元記憶装置７２に、利用可能な情報提供元機関リストの伝送依頼を送信する（ステップＳ３２）。認定情報提供元記憶装置７２は、利用者管理装置４０からの情報提供元機関リストの伝送依頼に応じて、ステップＳ４で記憶した情報提供元機関リストを、利用者管理装置４０に送信する（ステップＳ３３）。

【００３５】

利用者管理装置４０は、認定情報提供元記憶装置７２から受信した情報提供元機関リストを、利用者端末１０に転送する（ステップＳ３４）。利用者端末１０は、利用者管理装置４０から受信した情報提供元機関リストを自身の表示部に表示させる（ステップＳ３５）。利用者端末１０の利用者は、利用者端末１０に表示された情報提供元リストを閲覧し、情報提供元リストに示される情報提供元機関のうち、自身の個人情報を個人情報提供システム１によって送信することを許可する情報提供元機関を選択し、利用者端末１０に入力する。利用者端末１０は、利用者に選択された情報提供元機関に対応する情報提供元機関ＩＤを、利用者管理装置４０に送信する（ステップＳ３６）。利用者管理装置４０は、ステップＳ３１と同様に、利用者端末１０の認証判定処理を行い（ステップＳ３７）、利用者端末１０を認証すると、情報提供元管理装置５０に対して利用登録申込フォームの送

信依頼を送信する（ステップＳ３８）。

【００３６】

情報提供元管理装置５０は、利用者管理装置４０から利用登録申込フォームの送信依頼を受信すると、情報提供元装置２０から、利用者登録申込フォームを読み出し（ステップＳ３９、ステップＳ４０）、利用者管理装置４０に送信する（ステップＳ４１）。利用者端末１０は、利用者管理装置４０が情報提供元管理装置５０から受信した利用者登録申込フォームを受信し、表示部に表示させる（ステップＳ４２）。利用者端末１０の利用者は、利用者端末１０の表示部に表示された利用者申込フォームに示される項目に対応する情報を利用者端末１０に入力する。利用者端末１０は、利用者に情報が入力された入力済みの利用者申込フォームを、利用者管理装置４０に送信する（ステップＳ４３）。利用者管理装置４０は、利用者端末１０から送信された入力済み利用者申込フォームを受信すると、ステップＳ３１と同様に利用者の認証判定処理を行うとともに、入力済み利用者申込フォームに入力された情報の形式的なチェックを行い、不正な入力がないか否かを判定する（ステップＳ４４）。ここで、形式的なチェックとは、例えば入力された文字の文字数などが予め定められた制限文字数以内であるか否かなどの判定処理である。

【００３７】

利用者管理装置４０は、利用者端末１０の認証を行い、入力済み利用者申込フォームに不正な入力がないと判定すると、入力済み利用者申込フォームを情報提供元管理装置５０に送信する（ステップＳ４５）。情報提供元管理装置５０は、利用者管理装置４０から受信する入力済み利用者申込フォームを情報提供元装置２０に転送する（ステップＳ４６）。情報提供元装置２０が入力済み利用者申込フォームを受信すると、情報提供元機関は、入力済み利用者申込フォームに入力された情報に基づいて、利用者の審査を行う。情報提供元装置２０に、利用者による個人情報提供システム１の利用を承認することを示す利用情報が入力されると、情報提供元装置２０は、利用者を識別する利用者ＩＤと、利用者ＩＤに対応する自身の情報提供元情報機関を識別する情報提供元独自ＩＤとを対応付けた利用登録承認情報を生成し（ステップＳ４７）、情報提供元管理装置５０に送信する（ステップＳ４８）。

【００３８】

情報提供元管理装置５０は、情報提供元装置２０から送信された利用登録承認情報を利用者管理装置４０に送信する（ステップＳ４９）。利用者管理装置４０が、情報提供元管理装置５０から送信された利用登録承認情報を利用者振分情報記憶装置７５に転送する（ステップＳ５０）と、利用者振分情報記憶装置７５は、利用者ＩＤと情報提供元独自ＩＤとを対応付けた利用者振分情報（情報提供元）を自身の記憶領域に記憶する（ステップＳ５１）。利用者振分情報記憶装置７５は、利用者振分情報の記憶が完了したことを示す登録完通知を利用者管理装置４０に送信する（ステップＳ５２）。利用者管理装置４０は、登録完了通知を利用者端末１０に転送する（ステップＳ５３）。これにより、利用者端末１０の利用者の意思に基づいて、その利用者の個人情報を、個人情報提供システム１を介して情報提供元装置２０が受信することを示す情報が、利用者振分情報記憶装置７５や情報提供元装置２０に記憶される。

【００３９】

図８は、利用者の意思に基づき、利用者の個人情報を保有する情報提供先機関の情報提供先管理装置６０に、個人情報提供システム１を用いて個人情報を利用するための登録が行われる処理動作例を示す図である。

まず、利用者端末１０は、正当性が認定され、利用可能な情報提供元機関の紹介要求を利用者管理装置４０に送信する（ステップＳ６０）。この際、利用者管理装置４０は、ステップＳ３１と同様の認証判定処理を行う（ステップＳ６１）。利用者管理装置４０は、利用者端末１０の認証判定処理において利用者端末１０を認証すると、認定情報提供先記憶装置７４に、利用可能な情報提供先機関リストの伝送依頼を送信する（ステップＳ６２）。認定情報提供先記憶装置７４は、利用者管理装置４０からの情報提供先機関リストの伝送依頼に応じて、ステップＳ１３で記憶した情報提供先機関リストを、利用者管理装置

４０に送信する（ステップＳ６３）。

【００４０】

利用者管理装置４０は、認定情報提供先記憶装置７４から受信した情報提供先機関リストを、利用者端末１０に転送する（ステップＳ６４）。利用者端末１０は、利用者管理装置４０から受信した情報提供先機関リストを自身の表示部に表示させる（ステップＳ６５）。利用者端末１０の利用者は、利用者端末１０に表示された情報提供先機関リストを閲覧し、情報提供先機関リストに示される情報提供先機関のうち、自身の個人情報を個人情報提供システム１を介して受信することを依頼する情報提供先機関を選択し、利用者端末１０に入力する。利用者端末１０は、利用者に選択された情報提供先機関に対応する情報提供先ＩＤを、利用者管理装置４０に送信する（ステップＳ６６）。利用者管理装置４０は、ステップＳ３１と同様に、利用者端末１０の認証判定処理を行う（ステップＳ６７）。利用者管理装置４０が、利用者端末１０を認証すると、利用者端末１０の利用者ＩＤと利用者に選択された情報提供先ＩＤとを、利用者振分情報記憶装置７５に送信する（ステップＳ６８）。利用者振分情報記憶装置７５は、利用者管理装置４０から送信された利用者ＩＤと情報提供元独自ＩＤとを対応付けた利用者振分情報（情報提供先）を自身の記憶領域に記憶する（ステップＳ６９）。利用者振分情報記憶装置７５は、利用者振分情報の記憶が完了したことを示す登録完通知を利用者管理装置４０に送信する（ステップＳ７０）。

【００４１】

利用者管理装置４０は、利用者振分情報記憶装置７５から送信された登録完了通知を受信すると、情報提供先管理装置６０に、情報提供先装置３０への利用者情報の通知依頼を送信する（ステップＳ７１）。情報提供先管理装置６０は、利用者管理装置４０から情報提供先装置３０への通知依頼を受信すると、情報提供先装置３０に接続用証明書を要求する（ステップＳ７２）。情報提供先装置３０が、情報提供先管理装置６０に接続用証明書を送信すると（ステップＳ７３）、情報提供先管理装置６０は、受信した接続用証明書の認証を行い（ステップＳ７４）、情報提供先管理装置６０に対応する到達管理情報を生成して（ステップＳ７５）、情報提供先装置３０に送信する（ステップＳ７６）。情報提供先装置３０は、利用者ＩＤを含む利用者情報を記憶し（ステップＳ７７）、情報提供先管理装置６０に到達通知を送信する（ステップＳ７８）。情報提供先管理装置６０は、利用者管理装置４０に対して情報提供先への利用者情報通知の完了通知を送信する（ステップＳ７９）。利用者管理装置４０は、認定情報提供先記憶装置７４から受信した完了通知を利用者端末１０に転送する（ステップＳ８０）。これにより、利用者端末１０の利用者の意思に基づいて、その利用者の個人情報を、個人情報提供システム１を介して情報提供先装置３０が受信することを示す情報が、利用者振分情報記憶装置７５や情報提供先装置３０に記憶される。

【００４２】

図９は、情報提供元機関が保有し個人情報記憶装置７３に記憶される個人情報を、その個人情報の本人が利用する利用者端末１０に送信する個人情報提供システム１の動作例を示す図である。

まず、利用者端末１０は、利用者管理装置４０に、情報提供元装置２０に記憶された自身の個人情報の取得依頼を送信する（ステップＳ９０）。ここで、取得依頼には、個人情報の取得対象となる個人の利用者ＩＤと、個人情報を保有する情報提供元機関の情報提供元ＩＤとが含まれる。利用者管理装置４０は、利用者端末１０の認証判定処理を行う（ステップＳ９１）。利用者管理装置４０の利用者認証部４１が利用者端末１０を認証すると、提供元独自ＩＤ取得部４２は、利用者端末１０の利用者ＩＤに対応する情報提供元独自ＩＤの取得依頼を利用者振分情報記憶装置７５に送信する（ステップＳ９２）。利用者振分情報記憶装置７５は、ステップＳ５１で記憶した利用者振分情報から、取得依頼に含まれる利用者ＩＤと情報提供元機関ＩＤとに対応する情報提供元独自ＩＤを読み出し、利用者管理装置４０に送信する（ステップＳ９３）。

【００４３】

利用者管理装置４０が、情報提供元管理装置５０から送信された情報提供元独自ＩＤを受信すると、利用者管理装置４０の情報収集依頼部４３は、情報提供元管理装置５０に対して情報提供元独自ＩＤに対応する個人情報の提供依頼を送信する（ステップＳ９４）。情報提供元管理装置５０の情報収集部５１は、個人情報の提供依頼を情報提供元装置２０に送信する（ステップＳ９５）。情報提供元装置２０は、情報提供元独自ＩＤに対応する個人情報を、個人情報記憶装置７３から読み出し、情報提供元管理装置５０に送信する（ステップＳ９７）。情報提供元管理装置５０の情報編集・加工部５２は、情報提供元装置２０から送信された個人情報を受信すると、情報提供元装置２０の認証判定処理を行い、２０を認証すると、改ざん防止のために、読み出した個人情報に電子署名などを付与した発行証明書を生成する（ステップＳ９８）。情報提供元管理装置５０は、情報提供元装置２０から読み出した個人情報と、生成した発行証明書との情報を、情報一時格納装置７６に送信する（ステップＳ９９）。情報一時格納装置７６は、情報提供元管理装置５０から受信した情報を、自身の記憶領域に記憶させる（ステップＳ１００）と、情報提供元管理装置５０に情報格納の完了通知を送信する（ステップＳ１０１）。情報提供元管理装置５０が、情報格納の完了通知を利用者管理装置４０に転送する（ステップＳ１０２）と、利用者管理装置４０は、情報格納の完了通知を利用者端末１０に転送する（ステップＳ１０３）。

【００４４】

利用者端末１０は、利用者管理装置４０から完了通知を受信すると、利用者管理装置４０に個人情報の閲覧要求を送信する（ステップＳ１０４）。利用者管理装置４０は、利用者端末１０の認証判定処理を行い（ステップＳ１０５）、認証すると、情報一時格納装置７６に個人情報の伝送依頼を送信する（ステップＳ１０６）。情報一時格納装置７６は、個人情報の伝送依頼に応じて、ステップＳ１００で記憶した個人情報を読み出し（ステップＳ１０７）、利用者管理装置４０に送信する（ステップＳ１０８）。利用者管理装置４０は、情報一時格納装置７６から受信した個人情報を、利用者端末１０に送信する（ステップＳ１０９）。利用者端末１０は、利用者管理装置４０から送信された個人情報を表示部に表示させる（ステップＳ１１０）。これにより、個人情報記憶装置７３に記憶される個人情報が、電子証明書等により正当性が証明された利用者端末１０にのみ送信される。

【００４５】

図１０は、ステップＳ１００で情報一時格納装置７６に記憶された利用者の個人情報が、利用者の指定する情報提供先装置３０に送信される動作例を示す図である。

利用者端末１０は、情報提供先装置３０への個人情報の提供依頼を利用者管理装置４０に送信する（ステップＳ４０）。利用者管理装置４０は、利用者端末１０の認証判定処理を行い、認証すると、利用者振分情報記憶装置７５に情報提供先装置３０の利用登録の有無の照会を行う。利用者振分情報記憶装置７５は、ステップＳ６９において記憶した利用者振分情報（情報提供先）を読み出し、利用者端末１０の利用者ＩＤと情報提供先装置３０の情報提供先ＩＤとが対応付けられているか否かを判定し、対応付けられていれば、利用者管理装置４０に情報提供可を示す通知を送信する（ステップＳ１２３）。利用者管理装置４０は、情報提供先管理装置６０に情報提供依頼を送信する（ステップＳ１２４）。情報提供先管理装置６０は、利用者管理装置４０から情報提供依頼を受信すると、情報提供先装置３０に情報提供の通知を行う（ステップＳ１２５）。情報提供先装置３０が、接続用証明書を情報提供先管理装置６０に送信すると（ステップＳ１２６）、情報提供先管理装置６０は、情報提供先装置３０の認証判定処理を行う（ステップＳ１２７）。

【００４６】

情報提供先管理装置６０は、利用者端末１０に対応する個人情報の伝送依頼を情報一時格納装置７６に送信する（ステップＳ１２８）。情報一時格納装置７６は、ステップＳ１００で記憶された利用者端末１０に対応する個人情報を読み出し（ステップＳ１２９）、情報提供先管理装置６０に送信する（ステップＳ１３０）。情報提供先管理装置６０は、情報一時格納装置７６から送信された個人情報に到達管理情報を付加し（ステップＳ１３１）、情報提供先装置３０に送信する（ステップＳ１３２）。情報提供先装置３０は、情

報提供先管理装置６０から送信された個人情報を受信すると、情報提供先装置３０が個人情報を受信したことを示す到達通知を情報提供先管理装置６０に送信する（ステップＳ１３３）。到達通知には、例えば情報提供先装置３０の情報提供先ＩＤや、３０が個人情報を受信した日時などが含まれる。

【００４７】

情報提供先管理装置６０は、情報提供先装置３０から送信された到達通知を、情報一時格納装置７６に転送する（ステップＳ１３４）。情報一時格納装置７６は、情報提供先管理装置６０から送信された到達通知を記憶し（ステップＳ１３５）、情報提供先管理装置６０に完了通知を送信する（ステップＳ１３６）。情報提供先管理装置６０は、情報一時格納装置７６から送信された完了通知を、利用者管理装置４０に送信する（ステップＳ１３７）。利用者管理装置４０は、情報提供先管理装置６０から送信された完了通知を利用者端末１０に転送する（ステップＳ１３８）。

【００４８】

なお、本実施形態では、個人情報提供システム１が、利用者管理装置４０、情報提供元管理装置５０、情報提供先管理装置６０、認定利用者記憶装置７１、認定情報提供元記憶装置７２、個人情報記憶装置７３、認定情報提供先記憶装置７４、利用者振分情報記憶装置７５、情報一時格納装置７６の各装置を備えることとしたが、これらの物理的な装置構成は上述の例に限定されるものではなく、ネットワークの回線容量や規模、各ハードウェアの性能、接続される利用者端末や情報提供元装置や情報提供先装置の数、扱う個人情報のデータ量などの環境に応じて適切な装置構成をとることとして良い。利用者管理装置４０や情報提供元管理装置５０や情報提供先管理装置６０が備える各部についても、上述の構成に限るものではなく、例えば上述の個人情報提供システム１が備える全ての装置が備える各機能部を単一の装置が備えるように構成することもできる。

【００４９】

以上説明したように、本発明によれば、複数の個人情報保有機関のうち、信頼できると認定された個人情報保有機関から、信頼できると認定された第三者機関に対して、個人情報の提供を希望する本人の意思に基づいて、電子証明書による認証などを介して、原本性、真正性のある個人情報を電子情報としてネットワーク経由で提供することが可能となる。ここで、個人情報提供システムは、外部の利用者端末１０や情報提供元装置２０や情報提供先装置３０と通信を行う際に電子証明書による認証判定処理を行うため、第三者が不正に本人になりすまして情報を取得するリスクを軽減することが可能である。また、情報提供元装置２０、情報提供先装置３０は認定機関により認定された機関であるため、利用者はより安心して個人情報を提供することができる。さらに、利用者管理装置４０、情報提供元管理装置５０、情報提供先管理装置６０のそれぞれの処理動作についての動作ログを記憶し、解析することで、不正利用等を発見することが可能である。

このように、本発明によれば、セキュアな個人情報の流通の仕組みを構築することができ、個人情報を活用した各種サービスを、効率的、効果的かつ安全に行うことが可能となる。

【００５０】

なお、本発明における処理部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより個人情報の提供を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、ホームページ提供環境（あるいは表示環境）を備えたＷＷＷシステムも含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持してい

るものも含むものとする。

【００５１】

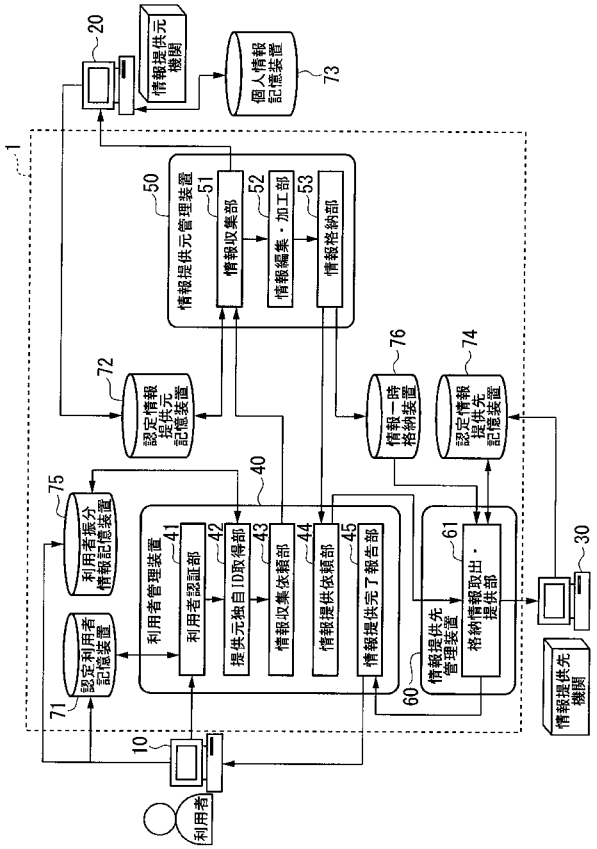
また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【符号の説明】

【００５２】

１　個人情報提供システム
１０　利用者端末
２０　情報提供元装置
３０　情報提供先装置
４０　利用者管理装置
４１　利用者認証部
４２　提供元独自ＩＤ取得部
４３　情報収集依頼部
４４　情報提供依頼部
４５　情報提供完了報告部
５０　情報提供元管理装置
５１　情報収集部
５２　情報編集・加工部
５３　情報格納部
６０　情報提供先管理装置
６１　格納情報取出・提供部
７１　認定利用者記憶装置
７２　認定情報提供元記憶装置
７３　個人情報記憶装置
７４　認定情報提供先記憶装置
７５　利用者振分情報記憶装置
７６　情報一時格納装置

【図１】



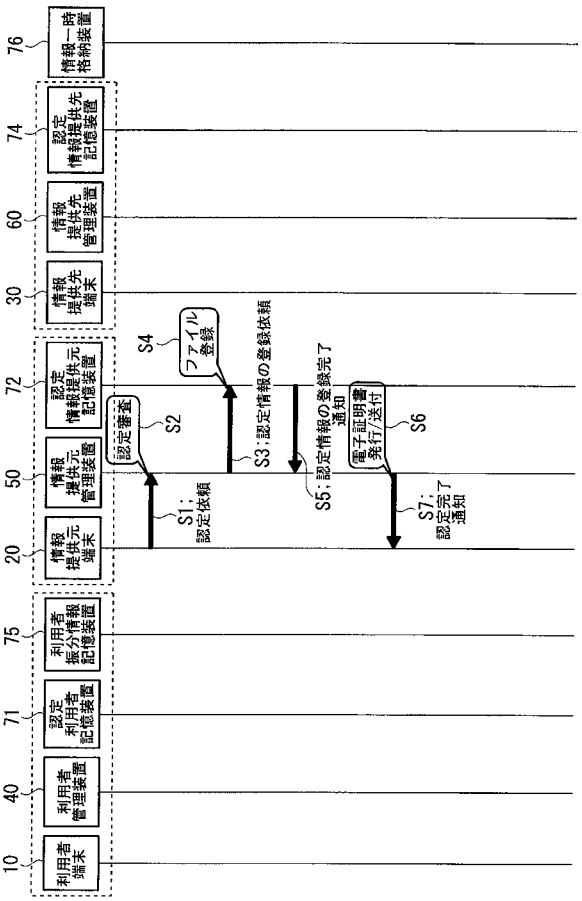
【図２】

情報提供元独自ID	個人情報
A1	…
A2	…
A3	…
…	…

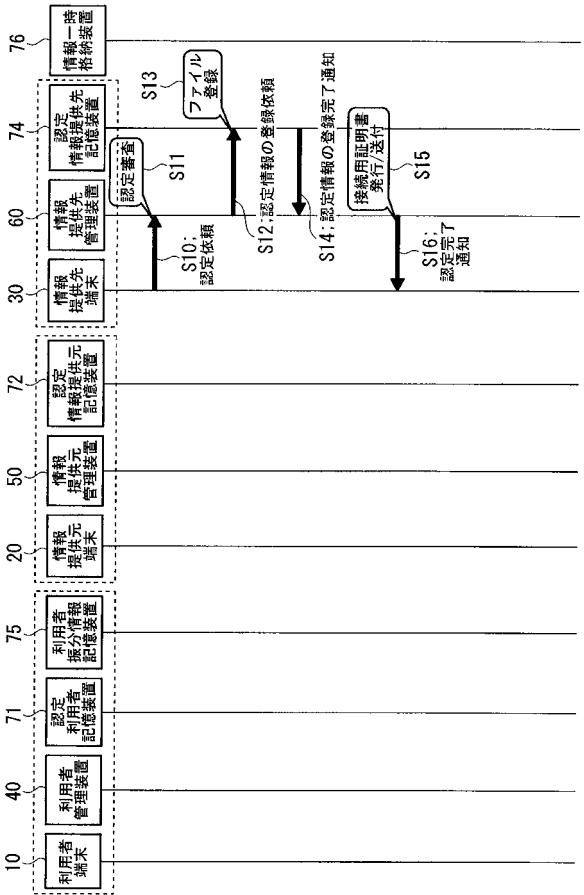
【図３】

利用者ID	情報提供元機関ID	情報提供元独自ID
1	A	A1
1	B	B1
1	C	C1
2	C	C2
…	…	…

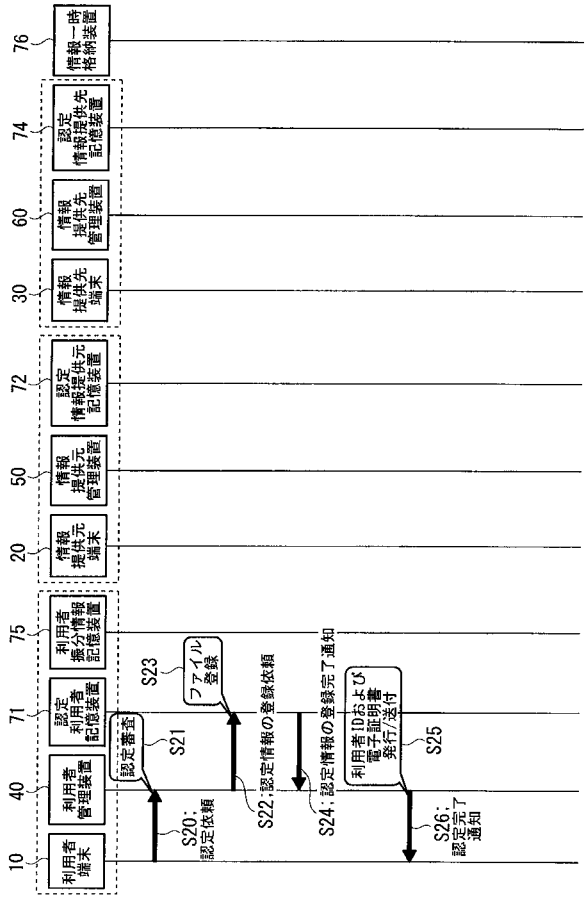
【図４】



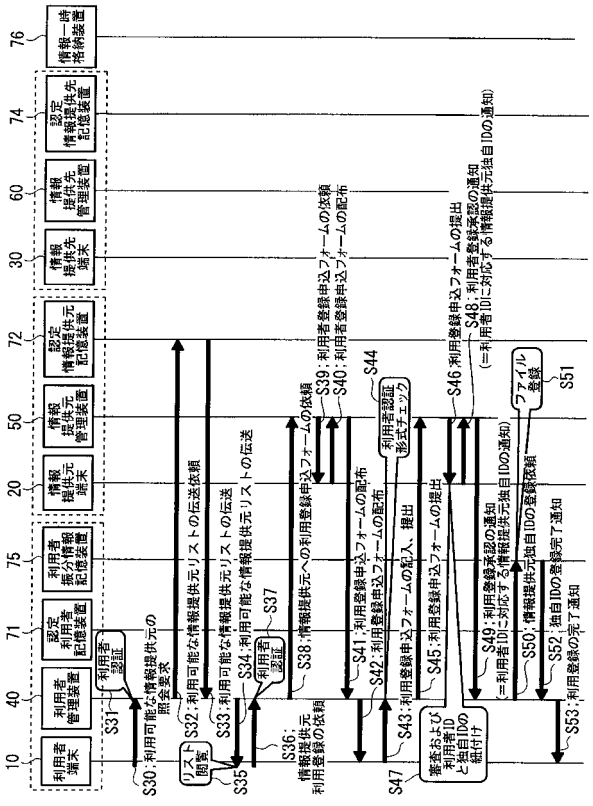
【図５】



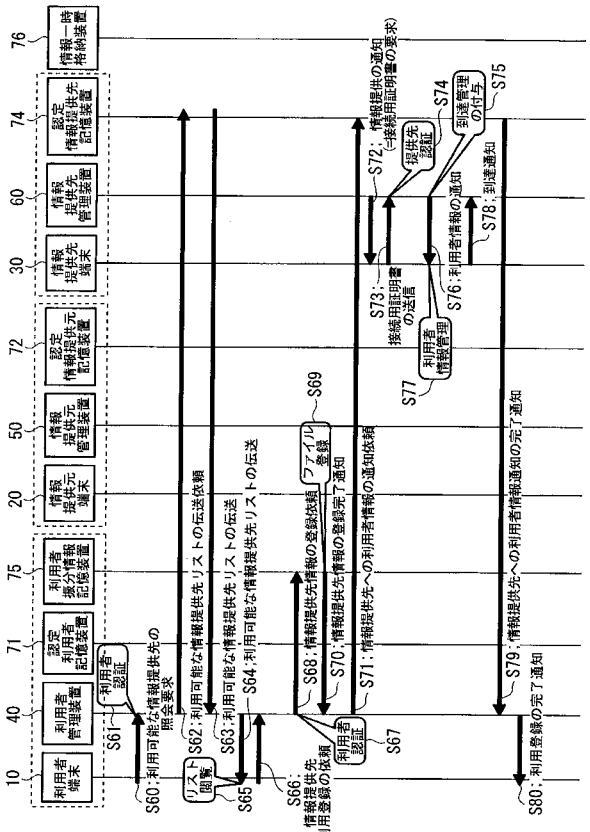
【図６】


利用者端末
利用者管理装置
認定利用者記憶装置
利用者振分情報記憶装置
情報提供元端末
情報提供元管理装置
認定情報提供元記憶装置
情報提供先端末
情報提供先管理装置
認定情報提供先記憶装置
情報一時格納装置
S20;認定依頼
S21
認定審査
S22;認定情報の登録依頼
S23
ファイル登録
S24;認定情報の登録完了通知
S25
利用者IDおよび電子証明書発行/送付
S26;認定完了通知

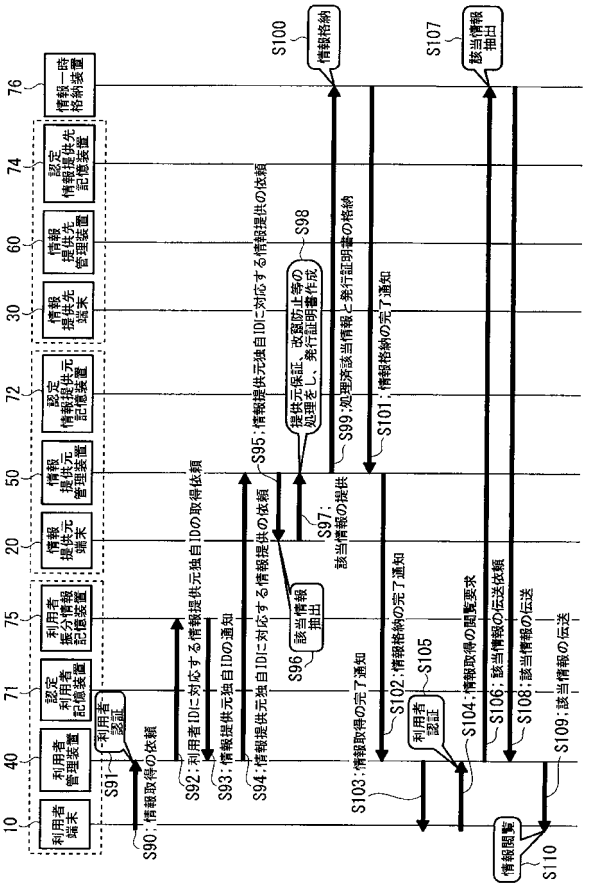
【図７】


利用者端末
利用者管理装置
認定利用者記憶装置
利用者振分情報記憶装置
情報提供元端末
情報提供元管理装置
認定情報提供元記憶装置
情報提供先端末
情報提供先管理装置
認定情報提供先記憶装置
情報一時格納装置
S30;利用可能な情報提供元の照会要求
S31
利用者認証
S32;利用可能な情報提供元リストの伝送依頼
S33;利用可能な情報提供元リストの伝送
S34;利用可能な情報提供先リストの伝送
S35
リスト閲覧
S36;情報提供先利用登録の依頼
S37
利用者認証
S38;情報提供元への利用登録申込フォームの依頼
S39;利用者登録申込フォームの依頼
S40;利用者登録申込フォームの配布
S41;利用登録申込フォームの配布
S42;利用登録申込フォームの配布
S43;利用登録申込フォームの記入、提出
S44
利用者認証
形式チェック
S45;利用登録申込フォームの提出
S46;利用登録申込フォームの提出
S47
審査および利用者IDと独自IDの紐付け
S48;利用者登録審査の通知
(=利用者IDに対応する情報提供元独自IDの通知)
S49;利用登録承認の通知
(=利用者IDに対応する情報提供元独自IDの通知)
S50;情報提供元独自IDの登録依頼
ファイル登録
S51
S52;独自IDの登録完了通知
S53;利用登録の完了通知

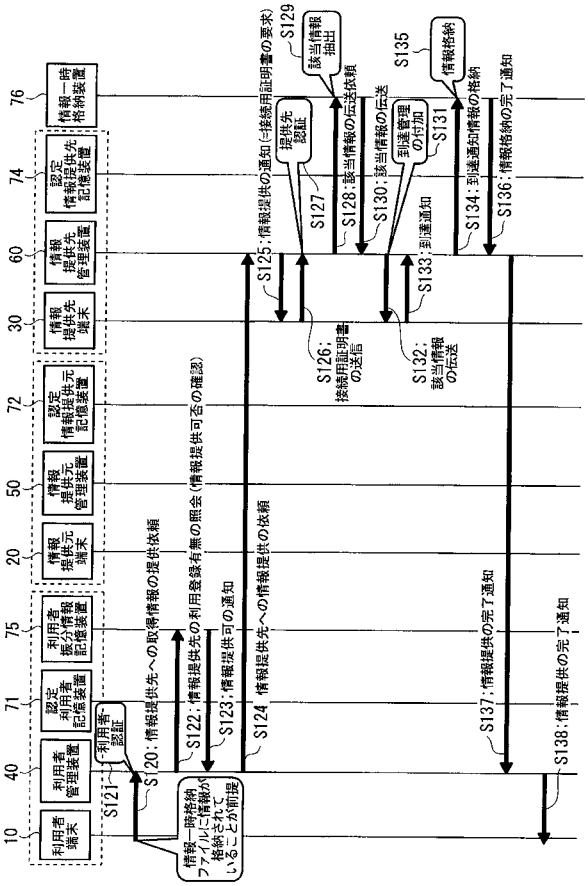
【図８】


利用者端末
利用者管理装置
認定利用者記憶装置
利用者振分情報記憶装置
情報提供元端末
情報提供元管理装置
認定情報提供元記憶装置
情報提供先端末
情報提供先管理装置
認定情報提供先記憶装置
情報一時格納装置
S60;利用可能な情報提供先の照会要求
S61
利用者認証
S62;利用可能な情報提供先リストの伝送依頼
S63;利用可能な情報提供先リストの伝送
S64;利用可能な情報提供先リストの伝送
リスト閲覧
S65
S66;情報提供先利用登録の依頼
利用者認証
S67
S68;情報提供先情報の登録依頼
S69
ファイル登録
S70;情報提供先情報の登録完了通知
S71;情報提供先への利用者情報の通知依頼
S72;情報提供の通知
(=接続用証明書の要求)
提供先認証
S73;接続用証明書の送信
S74
到達管理の付与
S75
S76;利用者情報の通知
S77
利用者情報登録
S78;到達通知
S79;情報提供先への利用者情報通知の完了通知
S80;利用登録の完了通知

【図９】


利用者端末
利用者管理装置
認定利用者記憶装置
利用者振分情報記憶装置
情報提供元端末
情報提供元管理装置
認定情報提供元記憶装置
情報提供先端末
情報提供先管理装置
認定情報提供先記憶装置
情報一時格納装置
S90;情報取得の依頼
S91
利用者認証
S92;利用者IDに対応する情報提供元独自IDの取得依頼
S93;情報提供元独自IDの通知
S94;情報提供元独自IDに対応する情報提供の依頼
S95;情報提供元独自IDに対応する情報提供の依頼
S96
該当情報抽出
S97;該当情報の提供
提出元保証、改竄防止等の処理をし、発行証明書作成
S98
S99;処理済該当情報に発行証明書の格納
S100
情報格納
S101;情報格納の完了通知
S102;情報格納の完了通知
S103;情報取得の完了通知
S104;情報取得の照会要求
S105
利用者認証
S106;該当情報の伝送依頼
S107
該当情報抽出
S108;該当情報の伝送
S109;該当情報の伝送
情報照会
S110

【図１０】


利用者端末
利用者管理装置
認定利用者記憶装置
利用者振分情報記憶装置
情報提供元端末
情報提供元管理装置
認定情報提供元記憶装置
情報提供先端末
情報提供先管理装置
認定情報提供先記憶装置
情報一時格納装置
10
40
71
75
20
50
72
30
60
74
76
S120：情報提供先への取得情報の提供依頼
S121：利用者認証
S122：情報提供先の利用登録有無の照会（情報提供可否の確認）
S123：情報提供可の通知
S124 情報提供先への情報提供の依頼
S125：情報提供の通知（=接続用証明書の要求）
S126：接続用証明書の送信
S127
S128：該当情報の伝送依頼
S129
S130：該当情報の伝送
S131
S132：該当情報の伝送
S133：到達通知
S134：到達通知情報の格納
S135
S136：情報格納の完了通知
S137：情報提供の完了通知
S138：情報提供の完了通知
情報一時格納ファイルに情報が格納されていることが前提
利用者認証
提供先認証
該当情報抽出
到達管理の付加
情報格納

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
Ｇ０６Ｆ　13/00	*(2006.01)*	Ｇ０６Ｆ	21/24　１６５Ａ	
		Ｇ０６Ｆ	13/00　５４０Ａ	

(72)発明者　吉村　美和子
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

Ｆターム(参考) 5B084 AA01 AA02 AA12 AA26 AA30 AB18 AB20 AB30 AB32 AB33
AB36 AB39 BB16 CA03 CB09 CD22 CD23 DC02 DC03 DC04
5J104 AA07 KA01 KA02 KA04 NA05 NA38 PA07