明　細　書

発明の名称 ：

文書生成装置、通信端末、中継端末および文書生成システム

技術分野

[0001] 本発明は、個人情報を管理するための技術、に関する。

背景技術

[0002] 近年、「デジタル・トランスフォーメーション（DX: Digital transformation）」に対する関心が急速に高まりつつある。企業の視点から見たデジタル・トランスフォーメーションとは、ネットワーク技術を活用することで社会のニーズを機敏に捉えつつ、自己のビジネスモデルを柔軟に変革することでビジネスに勝ち抜くことを意味する。

[0003] しかし、企業で採用されている既存の業務システムの多くは事業部門ごとに過度に最適化されていることが多く、こういったレガシーシステムが全社横断的なデータ活用を妨げている。レガシーシステムがむしろ企業の重荷になりかねないという危機感が存在する。

先行技術文献

特許文献

[0004] 特許文献1：特許第５３６０１５７号公報

発明の概要

発明が解決しようとする課題

[0005] また、企業が大量の情報を収集してこれを囲い込むことで独自のサービスを提供するというビジネス戦略の行き詰まりや弊害も指摘されている。まず、巨大なデジタル・プラットフォーマーの情報支配に対する根強い反発感情がある。デジタル・プラットフォーマーは、膨大な個人情報を収集し、これを独占的に活用することで優位性を確保する。個人は、デジタル・プラットフォーマーと個別交渉する力を持たず、個人情報の活用に関する各種規約を一方的に変更されるリスクにさらされる。このような問題認識の高まりによ

り、各国は個人情報利用について規制を強めつつある。ＥＵの一般データ保護規則（GDPR：General Data Protection Regulation）はその代表例である。

[0006] エネルギーの問題もある。モノとインターネットがつながるＩｏＴ時代になるとデータ管理のために膨大な電力需要が発生すると予測されている。２０１６年における世界の年間電力消費量は約２３，０００ＴＷＨといわれているが、２０４０年にはこれが１０倍以上になるともいわれる。ＩｏＴデバイスが激増し、膨大なＩｏＴデバイスがクラウドを前提として動くことで通信ネットワークおよびデータセンターの電力消費量が押し上げられるためである。

[0007] 本発明は、上記課題認識に鑑みて完成された発明であり、その主たる目的は、個人を基点としたデータ管理技術、を提案することにある。

課題を解決するための手段

[0008] 本発明のある態様における文書生成装置は、外部端末から、タグを付与されたデータを受信する受信部と、所定形式の文書に必要なタグを示す第１フィルタを参照し、受信されたデータに付与されるタグが第１フィルタに適合するか否かを判定する検査部と、第１フィルタに適合するデータに基づいて文書を生成する文書生成部と、を備える。

[0009] 本発明のある態様における通信端末は、文書生成装置と接続される。

この通信端末は、データとタグを対応づけて格納するデータ格納部と、ユーザからの入力にしたがって、外部に送信可能なデータのタグを示す第２フィルタを設定するフィルタ設定部と、第２フィルタを参照し、第２フィルタに含まれるタグを付与されたデータを選んで文書生成装置に送信する送信部と、を備える。

送信部は、文書生成装置から不足タグを通知されたあとに不足タグが第２フィルタに再設定されたとき、不足タグに対応するデータを文書生成装置に送信する。

[0010] 本発明の別の態様における通信端末は、複数のサーバそれぞれからタグを

付与されたデータを受信する受信部と、受信されたデータとタグを対応づけて、内蔵記憶装置に保存するデータ管理部と、を備える。

データ管理部は、第１のサーバから第１のタグを付与された第１のデータを受信し、かつ、第２のサーバから第２のタグを付与された第１のデータを受信したときには、第１のデータに対して第１のタグおよび第２のタグを対応づけて保存する。

[0011] 本発明のある態様における中継端末は、文書生成装置と接続される。

中継端末は、ユーザからデータの入力を受け付ける入力部と、文書生成装置から第１のフィルタを受信する受信部と、ユーザが保有する情報担体から、タグを付与されたデータを読み取るデータ取得部と、読み取られたデータに付与されるタグが第１フィルタに適合するか否かを判定する検査部と、読み取られたデータのうち、第１フィルタに適合するデータを選んで文書生成装置に送信する送信部と、を備える。

送信部は、文書生成装置から不足タグを通知されたあとに不足タグに対応するデータが入力されたとき、更に、不足タグに対応するデータを文書生成装置に追加送信する。

[0012] 本発明のある態様における文書生成システムは、通信端末と文書生成装置を含む。

通信端末は、データとタグを対応づけて格納するデータ格納部と、ユーザからの入力にしたがって、外部に送信可能なデータのタグを示す第２フィルタを設定するフィルタ設定部と、第２フィルタを参照し、文書生成装置にアクセスしたとき第２フィルタに含まれるタグを付与されたデータを選んで文書生成装置に送信する送信部と、を備える。

文書生成装置は、通信端末から、タグを付与されたデータを受信する受信部と、所定形式の文書に必要なタグを示す第１フィルタを参照し、受信されたデータに付与されるタグが第１フィルタに適合するか否かを判定する検査部と、第１フィルタに適合するデータに基づいて文書を生成する文書生成部と、第１フィルタに含まれる複数のタグのうち、一部のタグに対応づけられ

るデータが不足しているとき、不足タグを通知する通知部と、を備える。

通信端末の送信部は、文書生成装置から不足タグを通知されたあとに不足タグが第２フィルタに再設定されたとき、不足タグに対応するデータを文書生成装置に送信する。

文書生成装置の文書生成部は、不足タグに対応するデータが受信されたとき、受信されたデータを含めて文書を生成する。

発明の効果

[0013] 本発明によれば、個人を中心としたデータ管理を実現しやすくなる。

図面の簡単な説明

[0014] [図1]ＤＩエンジンの連携を説明するための概念図である。

[図2]官公庁、企業、個人によるデータ交換の概念図である。

[図3]文書生成システムのハードウェア構成図である。

[図4]文書生成装置の機能ブロック図である。

[図5]ユーザ端末の機能ブロック図である。

[図6]複数のファイルサーバに分散する個人情報をユーザ端末に集約する方法を説明するための模式図である。

[図7]第２フィルタによる出力制御を説明するための模式図である。

[図8]文書生成装置が発行する公文書の形式の一例である。

[図9]文書定義テーブルのデータ構造図である。

[図10]発行履歴情報のデータ構造図である。

[図11]第１フィルタによる入力制御を説明するための模式図である。

[図12]第２実施形態における文書生成装置の公文書発行過程を示すフローチャートである。

[図13]ユーザ端末が不足タグを通知されたときの処理過程を示すフローチャートである。

[図14]データ補充画面の画面図である。

[図15]公文書の真正確認時の処理過程を示すシーケンス図である。

[図16]第３実施形態における文書生成システムのハードウェア構成図である

。

[図17]中継端末の機能ブロック図である。

[図18]第３実施形態における個人情報の入出力制御を説明するための模式図である。

[図19]第３実施形態における中継端末の公文書発行過程を示すフローチャートである。

発明を実施するための形態

[0015] 既存の業務システムは、事業部門ごと、企業ごとに構築され、特定業務に最適化されているものが多い。巨大で複雑、更に、長い運用に耐えてきた歴史のある業務システムの中には抜本的な改修や拡張が難しくなっているものもある。同様の理由から、複数の業務システムを連携あるいは統合させることも難しい場合がある。

[0016] また、単一企業のサービス提供システムが巨大化し、いわゆるビッグデータを独占することは「監視社会」を招くリスクがある。更に、膨大な数のＩｏＴ機器から膨大なデータをサーバ群（クラウド）に吸い上げることは、通信にともなう負荷と電力消費を増大させる。特に、データ収集頻度が高くなるほどこういった問題は顕在化しやすい。

[0017] 本実施形態においては、個人に対応づけられるＤＩエンジン（Digital Intelligence Engine）により個人情報を管理する。詳細は後述するが、企業などのサービス提供者が個人情報をいったん収集し、ユーザ（サービス享受者）がサービス提供者のシステムにアクセスしてサービスを受けるのではなく、ユーザがＤＩエンジンにより個人情報を個別的に管理し、サービス提供者がユーザの個人情報からサービスに必要な一部の個人情報をもらうことでサービスを提供する。

[0018] ＤＩエンジンは、ＭＰＵ（Micro-Processor Unit）を搭載するチップとして実装される（以下、「ＤＩチップ」とよぶ）。ＤＩチップは、ＭＰＵと揮発性メモリおよび不揮発性メモリを含み、不揮発性メモリには個人情報が記憶される。ＤＩエンジンは、狭義には、ＤＩチップのＭＰＵで実行される軽

量のアプリケーション・ソフトウェアであり、広義には、ＤＩチップ全体が発揮する機能の総称である。本実施形態においては、特に断らない限りは、ＤＩエンジンとは後者の意味であるとする。

[0019] ＤＩチップはユーザとともに移動する。ＤＩチップは、たとえば、ユーザが保有するスマートフォンあるいはユーザが保有するカードなどに内蔵されることが望ましい。ＤＩエンジンは、データの保存機能と出力機能のほか、ユーザに対するコンシェルジュ機能を備えることが望ましい。

[0020] ＤＩエンジンはユーザの個人情報を格納する。個人情報はＤＩエンジンに暗号化されて保存されており、サーバは個人情報を自由に収集することはできない。サーバが一部の個人情報を格納してもよいが、個人情報を自由かつ制限なく格納できるのはあくまでもＤＩエンジンである。サーバは、サービスの提供にあたってはＤＩエンジンが許可した範囲でＤＩエンジンから一部の個人情報をもらう。

[0021] たとえば、サーバＳ１は、ユーザＰ１のＤＩエンジンから個人情報の一部Ｘ１をもらう。別のサーバＳ２は、ユーザＰ１のＤＩエンジンから個人情報の一部Ｘ２をもらう。個人情報Ｘ１および個人情報Ｘ２はまったく別の内容かもしれないし、一部が共通することもある。個人情報Ｘ１および個人情報Ｘ２の共通部分ＸＣがあれば、共通部分ＸＣをキーとしてサーバＳ１およびサーバＳ２は連携することもできる。

[0022] サービス提供側ではなく、サービス享受側のユーザに「データ主権」がある。ＤＩエンジンはユーザ本人が許可した個人情報しか出力しないためプライバシーを守りやすい。ＤＩエンジンは個人情報を暗号化してＤＩチップに保存する。サービス提供側は、際限なく膨大な個人情報をいったん集めた上でサービスを提供するのではなく、ＤＩエンジンから必要な個人情報を適宜もらうことでサービスを提供する。

[0023] ＤＩチップのアプリケーション・ソフトウェアは軽量・省サイズのソフトウェアである。現段階では、０．２ＭＢ以内に収まる程度になると想定されている。コンシェルジュ機能を有する場合でも、基本的には、ＤＩエンジン

が格納する個人情報をベースとして各種の処理を行うので処理負荷は小さい。クラウド・コンピューティングを前提としないため、通信負荷は低く、電力消費も抑制できる。

[0024] 図１は、ＤＩエンジンの連携を説明するための概念図である。

ＤＩエンジンは、個人のデータを集める。ユーザ自身がＤＩエンジンに個人情報を登録してもよいし、ＤＩエンジンはスマートフォンなどの外部機器から個人情報を収集してもよい。たとえば、ユーザＰ２のＤＩエンジンは、このユーザＰ２が「埼玉出身」の「井原真実」で、２０２０年１０月５日に「トマト」を食べたという個人情報を格納している。ユーザＰ２は、トマトを食べるときにスマートフォンでトマトを撮影する。ＤＩエンジンは、スマートフォンがトマトを撮影したとき、このユーザＰ２がトマトを食べたと判断してもよい。あるいは、ユーザＰ２自身が個人情報をＤＩエンジンに登録してもよい。ＤＩエンジンへの個人情報の登録方法は任意である。

[0025] 複数のＤＩエンジンが個人情報を相互交換することで全体としての個人情報管理システムが形成される。たとえば、ユーザＰ１は、「男性」「独身」という一部の個人情報のみを出力可能（公開可能）に設定してもよい。ユーザＰ２は、ユーザＰ１（ＤＩエンジン）と通信したとき、ユーザＰ１が独身の男性であることを知ることができる。一方、ユーザＰ１が「年収５００万円」という年収情報を非公開としていた場合、年収情報はユーザＰ２には通知されない。ユーザＰ１は、年収情報をユーザＰ３には公開するかもしれない。各ユーザは相手に合わせて公開可能な個人情報を設定できる。

[0026] ＤＩエンジンによって、情報は物理的に可搬される。ユーザＰ１のＤＩエンジンがユーザＰ２のＤＩエンジンに個人情報を提供することで、ユーザＰ２のＤＩエンジンはユーザＰ１およびユーザＰ２の関係性にあった提案を行うことができる。たとえば、ユーザＰ１とユーザＰ２が初対面であっても、共通の話題を提案できる。上記例の場合、ユーザＰ１はユーザＰ２が埼玉出身だと知ることができれば埼玉県の話から話のきっかけを掴むことができる。ＤＩエンジンが個人情報を格納するため、データセンターの情報管理負担

も軽減されると考えられる。

[0027] ＤＩエンジンは、自らが保有する膨大な個人情報のうち、外部に提供してもよい個人情報を絞ることができる。また、他者から供給される個人情報のうち、受け取りたい個人情報の種類を絞ることもできる。以下においては、サーバ（中央）にデータを収集して活用する従来型の情報管理システムを「中央管理型システム」、ＤＩエンジンがデータを格納し、ＤＩエンジンから供給されるデータに基づいて各種処理を実行する情報管理システムを「分散管理型システム」とよぶ。

[0028] 中央管理型システムの場合、あるサービスを提供する企業Ｃ１は、自社のデータベースＤＢ１に独自にデータを収集する。一方、別のサービスを提供する企業Ｃ２も、自社のデータベースＤＢ２に独自にデータを収集する。それぞれが独自かつ貪欲にデータ収集を行うので、データベースＤＢ１に格納されるデータとデータベースＤＢ２に格納されるデータの多くは重複する。この結果、同一データが多数のデータベースに重複保存されることになる。データベースのフォーマットも各社各様であるため拡張性に乏しく、複数のデータベースを連携させづらくなる。

[0029] 一方、分散管理型システムにおいては、ＤＩエンジンからもらう個人情報に基づいて連携する方式であるため、企業はきちんと要件定義されたデータベースをもつ必要がなくなる。企業は必要なデータを、ＤＩエンジンからユーザ承認のもとで受け取ることでサービスを提供する。大量の個人情報を常に確保していく必要がなくなる。

[0030] たとえば、図１に示すように、ＤＩエンジンが格納する個人情報は多種多様である。ユーザＰ１のＤＩエンジンには「年収」に関する個人情報が含まれているがユーザＰ２のＤＩエンジンには「年収」情報は含まれていない。ＤＩエンジンは、項目（例：年収）とデータ（例：５００万円）のペアを雑多に格納する。また、ユーザＰ２の「食べたもの：トマト」と「日時：２０２０年１０月５日」のように複数の個人情報につながりをもたせることもできる。ユーザＰ１は、ユーザＰ２が最近食べたものを知りたいときであって

、ユーザＰ２が「２０２０年１０月５日にトマトを食べた」という情報を提供しても構わないと考えているならば、ユーザＰ１はユーザＰ２が２０２０年１０月５日にトマトを食べたことを知ることができる。もし、ユーザＰ１が料理人であれば、ユーザＰ１のＤＩエンジンは、この情報をもとに「ユーザＰ２はトマトを食べることができる」、あるいは、「ユーザＰ２はトマトが好きなのかもしれない」と判断できる。この結果、ユーザＰ１のＤＩエンジンは、ユーザＰ２に対してトマト料理を提供すべきと判断するかもしれない。

[0031] 本実施形態における情報管理システムによれば、個人情報をＤＩエンジンで管理することにより、データベースにおける同一データの重複格納を抑制できる。また、オペレータがデータベースに個人情報を登録するときの入力ミス、コピーミスを減らすこともできる。サービス提供者は、ＤＩエンジンから必要に応じて個人情報を得て、必要に応じて処理するためである。また、ＤＩエンジンで個人情報を管理することにより、大規模な情報漏洩を生じるリスクが小さくなる。

[0032] 従来の中央管理型システムにおいては、大量の個人情報を統計処理することにより個人に対して適切なサービスを提案することで商機を捉えることに主眼を置いている。たとえば、あるユーザが商品Ａを購入したとき、商品Ａを購入した人は商品Ｂを購入することが多いという統計情報に基づいてこのユーザに商品Ｂを提案する。

[0033] これに対して、本実施形態における分散管理型システムは、ＤＩエンジンから得た個人情報を分析することで個人の価値観にあったサービスを提供できる。たとえば、あるユーザがお店に入ったとき、このユーザがトイレットペーパーを買ってからしばらく時間が経っていることがわかれば、ＤＩエンジンはトイレットペーパーの購入を提案してもよい。

[0034] また、新型コロナウイルス（重症急性呼吸器症候群コロナウイルス２）について、「３７．５度以上の発熱が４日以上」続くことが受診の目安とされている。しかし、個人によって平熱温度はさまざまであるため、平熱温度が

もともと高いユーザについては３７．５度以上に基準値を設定することが望ましいと考えられる。ＤＩエンジンは、ユーザの体温を検出し、独自の基準値に基づいて受診要否を判定してもよい。

[0035] ＤＩエンジンはＤＭＳ（Data Management System）として情報管理のキーとなる。また、各ユーザが利用する二次電池などの電源を管理するのがＢＭＳ（Battery Management System）である。ＤＭＳとＢＭＳにより、個人の情報とエネルギーを管理する。更に、多数のＤＭＳ，ＢＭＳから得た情報に基づいてＥＭＳ（Energy Management System）が構成される。

[0036] ＤＩエンジンに搭載されるＭＰＵには、それほどの処理能力は求められない。ＭＰＵは、ローパフォーマンスのＣＰＵ（Central Processing Unit）でもよいし、ＧＰＵ（Graphics Processing Unit）でもいい。ＭＰＵは、ＦＰＧＡ（Field-Programmable Gate Array）であってもよい。

[0037] ＤＩエンジンをデータベースに搭載してもよい。従来の中央管理型システムにおいては、大量のデータを格納するデータベースを設計するときにデータ構造に関する厳密な要件定義を必要としていた。この結果として、データベースの統合や変更に際しては多くの工数がかかっていた。本実施形態における分散管理型システムの応用例として、データベースにＤＩエンジンを搭載してもよい。まず、登録したいデータをデータベース（ＤＩエンジン）に入力する。ＤＩエンジンは、データをデータベースにそのまま記憶させる。データベースからのデータ取得要求があったときには、ＤＩエンジンはデータベース内から所望のデータを検索して出力する。ＤＩエンジンは、データの使用頻度に応じて各データに重み付けを行う。具体的には、使用頻度の高いデータ、たとえば、氏名などのデータの優先度を高めることにより、データの検索性を高めることができる。このような制御方法によれば、データ構造に関する要件定義を行わなくても、データベースの実際に使用状態に応じてデータの重要性（格付）を設定することにより、データの入力容易性と取得容易性の双方を高めることができる。

[0038] このほか、ＤＩエンジンは、学術文献やＳＮＳ（Social Networking Servi

ce）、ニュース記事などに含まれる言葉を収集し、そのつながりを作る機能をもたせてもよい。たとえば、ワードＷ１の近傍（たとえば同一文、同一段落）にワードＷ２が出現するとき、ワードＷ１とワードＷ２は関連性があるとする。関連の強さを分析することにより、情報のつながりを可視化できる。Word2Vecのような既知技術の応用により関連の強さを判定してもよい。

[0039] また、ＤＩエンジンから得られる限定された個人情報を統計分析することも考えられる。たとえば、「雨の日に商品Ａを買った」という個人情報が繰り返し取得されたときには、雨の日には商品Ａが売れるという知見が得られる。あるいは、ユーザＰ１が、過去の雨の日に商品Ａを買ったという個人情報があれば、店舗のＰＯＳ端末は、このユーザＰ１が雨の日に来店したときには商品Ａを薦めてもよい。同様にして、万引きをする人は最初に商品Ｂを買ってから万引きを実行することが多いという情報が得られれば、商品Ｂを選んだ人を優先的にマークするという対応が可能である。

[0040] お薬手帳の持参を忘れる患者も多い。このため、医師が処方箋を書くときに薬の飲み合わせをきちんと確認できないというリスクがある。ＤＩエンジンは、ユーザがいつどんな薬を飲んだか、あるいは、処方されたかという個人情報を格納している。医師は、ＤＩエンジンから薬歴に関する情報のみを取得するだけでも、いっそう適切に処方箋を出すことが可能となる。また、ＤＩエンジンからユーザの体調に関する個人情報を得られれば、体調に合わせて薬の種類や量を変更することも可能となる。

[0041] 企業によって、あるいは、部署によって同じ概念を異なる用語で表すことがある。たとえば、部署Ｅ１ではある概念Ｘを用語Ｙ１と呼び、別の部署Ｅ２では同じ概念Ｘを用語Ｙ２と呼ぶとする。この場合、部署Ｅ１と部署Ｅ２のコミュニケーションに齟齬をきたす可能性がある。ここで、部署Ｅ１のユーザのＤＩエンジンから、用語Ｙ１と関連づけられる用語群Ｇ１を抽出し、部署Ｅ２のユーザのＤＩエンジンから、用語Ｙ２と関連づけられる用語群Ｇ１を抽出する。用語群Ｇ１と用語群Ｇ２が類似しているとき、双方のＤＩエンジンは用語Ｙ１と用語Ｙ２が同一または類似の概念に対応していると認識

できる。

[0042] まず、ＤＩエンジンによる個人情報の管理のあと、家族などの小さな単位で個人情報の一部を管理またはバックアップすることが考えられる。たとえば、ＤＩエンジンが格納する情報量をＭ１とすると、ユーザは家族で運用するエッジサーバに一部の個人情報をバックアップさせる。エッジサーバに格納する個人情報の情報量はＭ１×０．１程度であってもよい。このような制御方法によれば、ユーザはＤＩエンジンで個人情報を管理しつつ、家族で共有可能な一部の個人情報をエッジサーバに提供する。

[0043] 家族が所有する自動車（エッジサーバの一種）に各員が個人情報の一部を提供することにより、自動車はユーザに合わせて運転のアシスト方法を変更してもよい。

[0044] 更に、個人情報の一部はマンションや学校、職場などのコミュニティに共有情報として提供されてもよい。この場合にも、個人情報を制限なく提供するのではなく、コミュニティにおいて必要かつ有用な情報、たとえば、氏名、性別、住所などに限定して個人情報を提供するとしてもよい。このように、個人がＤＩエンジンで個人情報を管理しつつ、家族や会社、地域、国家などに個人情報を限定的に提供していくことにより、データ管理の主権性を守りつつ、コミュニティから得られる利便性を享受しやすくなる。

[0045] 図２は、官公庁、企業、個人によるデータ交換の概念図である。

たとえば、官公庁はマイナンバーのデータベースＤＢ１と住基ネット（住民基本台帳ネットワークシステム）のデータベースＤＢ２をもっているとする。この２つＤＢを統合するため、官公庁のＤＩエンジンにデータベースＤＢ１のデータ群とデータベースＤＢ２のデータ群をまとめて投入する。ここで、データベースＤＢ１には個人情報として「氏名」「住所」「マイナンバー」「年齢」「職業」が対応づけて登録されているとする。また、データベースＤＢ２には個人情報として「氏名」「住所」「住基番号」「性別」「出生地」「パスポートの有無」が対応づけて登録されているとする。２つのデータベースにおいて、「氏名」「住所」が共通するため、この２つのデータ

「氏名」「住所」をキーすることにより、２種類のデータベースを統合できる。たとえば、「氏名：佐藤一郎」「住所：京都府京都市北区上賀茂本山」という２種類のデータに対応する「マイナンバー」「年齢」「職業」を特定するとともに、同じ２種類のデータに対応づけられる「性別」「住基番号」「出生地」「パスポートの有無」を特定する。「氏名：佐藤一郎」「住所：京都府京都市北区上賀茂本山」に対して「マイナンバー」「年齢」「職業」「性別」「住基番号」「出生地」「パスポートの有無」を対応づければ、ユーザＰ１（氏名：佐藤一郎）についてデータベースＤＢ１とデータベースＤＢ２のデータを統合できる。他のユーザについても同様である。

[0046] また、ユーザＰ１は、自治体から住民票を取得したいときには、ＤＩエンジンから住民票取得に必要な個人情報（例：氏名と住所）を官公庁に提供する。官公庁は、限定された個人情報を受け取ることにより、住民票を作成し、ユーザＰ１の携帯端末に住民票データを送信すればよい。住民票発行業務を担当する自治体は、住民票発行に必要なデータ以外のデータ、たとえば、ユーザの職歴などを管理する必要がない。自治体は、サービスのために保存しておくべき公式データのみを管理し、サービスに必要なその他の情報は、適宜、住民のＤＩエンジンから取得すればよい。

[0047] また、企業も、顧客のＤＩエンジンから提供される個人情報に基づいて商品情報あるいは広告を顧客に送信してもよい。複数の企業がひとりの顧客に対してサービスを提供する場合にもＤＩエンジンを通した連携が可能である。たとえば、ユーザＰ１が「自動車によく乗る」という情報を提供するとき、自動車メーカーは新車を提案してもよいし、市役所は市内のドライブスポットを提案してもよい。ユーザＰ１が提案されたドライブスポットに興味をもったときには、ドライブスポット近辺のお店からユーザＰ１に広告を送信してもよい。お店は、ユーザＰ１の素姓を知る必要はない。

[0048] 以下においては、個人情報の集約および活用方法について第１実施形態から第３実施形態に分けて説明する。

第１実施形態においては、複数のファイルサーバに分散されている個人情

報（データ）を、ユーザ端末（通信端末）に集約する方法について説明する。

第２実施形態においてはインターネットとの接続機能を有するユーザ端末に保存される個人情報を利用して公文書を発行する方法について説明する。

第３実施形態においてはインターネットとの接続機能を有さないバッジ（情報担体）に保存される個人情報を利用して公文書を発行する方法について説明する。

以下、第１実施形態から第３実施形態をまとめていうときや、特に区別しないときには「本実施形態」とよぶ。

[0049] ［第１実施形態］

図３は、文書生成システム２００のハードウェア構成図である。

文書生成システム２００は、文書生成装置１００と、複数のファイルサーバ１０４とユーザ端末３００を含む。文書生成装置１００、ファイルサーバ１０４およびユーザ端末３００はインターネット１０２を介して接続される。ユーザ端末３００は、ユーザが保有する通信端末であり、ラップトップＰＣ（Personal Computer）、タブレットＰＣ、スマートフォンなどが想定される。このほか、ユーザ端末３００はスマートウォッチ（腕時計型携帯情報端末）などのいわゆるウェアラブル端末であってもよい。本実施形態におけるユーザ端末３００はスマートフォンであるとして説明する。ユーザ端末３００はＤＩエンジンを搭載する。ユーザ端末３００はＤＩチップを搭載してもよいし、ＤＩエンジンとしての機能を実現するアプリケーション・ソフトウェアをユーザ端末３００にインストールしてもよい。

[0050] ファイルサーバ１０４は、公的機関等により運用されるデータベースであり、ユーザの個人情報を管理する。ファイルサーバ１０４の運営者としては、地方自治体、官公庁、企業、教育機関、金融機関などが想定される。各機関は、それぞれ独自の形式にてユーザの個人情報を管理する。

[0051] 文書生成装置１００は、公文書を作成・発行する装置である。本実施形態における文書生成装置１００は行政機関により運用される。文書生成装置１

００は、住民票、図書カード、戸籍謄本、運転免許証、登記事項証明書等の各種公文書を発行する。

[0052] ユーザは、あらかじめユーザＩＤおよびパスワードを文書生成装置１００に登録しておく。文書生成装置１００は、ユーザＩＤとパスワードに基づいてユーザの本人確認を行う。

[0053] 図４は、文書生成装置１００の機能ブロック図である。

文書生成装置１００の各構成要素は、ＣＰＵ（Central Processing Unit）および各種コプロセッサ（co-processor）などの演算器、メモリやストレージといった記憶装置、それらを連結する有線または無線の通信線を含むハードウェアと、記憶装置に格納され、演算器に処理命令を供給するソフトウェアによって実現される。コンピュータプログラムは、デバイスドライバ、オペレーティングシステム、それらの上位層に位置する各種アプリケーションプログラム、また、これらのプログラムに共通機能を提供するライブラリによって構成されてもよい。

以下に説明する各ブロックは、ハードウェア単位の構成ではなく、機能単位のブロックを示している。図５のユーザ端末３００、図７の中継端末４００についても同様である。

[0054] 文書生成装置１００は、通信部１１０、データ処理部１１２およびデータ格納部１１４を含む。

通信部１１０は、インターネット１０２を介してユーザ端末３００、中継端末４００（後述）およびファイルサーバ１０４との通信処理を担当する。データ格納部１１４は各種情報を格納する。データ処理部１１２は、通信部１１０により取得されたデータおよびデータ格納部１１４に格納されているデータに基づいて各種処理を実行する。データ処理部１１２は、通信部１１０およびデータ格納部１１４のインタフェースとしても機能する。

[0055] 通信部１１０は、ユーザ端末３００等の外部装置に各種情報を送信する送信部１１８と、外部装置から各種情報を受信する受信部１１６を含む。

送信部１１８は、文書発行に必要なデータが欠落しているときにユーザ端

末３００に不足しているデータを通知する通知部１２０を含む。

[0056] データ処理部１１２は、検査部１２２、証明部１２４、文書生成部１２６およびフィルタ設定部１２８を含む。

検査部１２２は、第１フィルタ（後述）に基づいて、ユーザ端末３００等の外部装置から受信したデータの受入可否を判定する。証明部１２４は、外部からの問い合わせに際して、公文書の真正性を確認する。文書生成部１２６は公文書を生成する。フィルタ設定部１２８は、公文書の種類に応じて第１フィルタを設定する。

[0057] 図５は、ユーザ端末３００の機能ブロック図である。

ユーザ端末３００は、ユーザインタフェース処理部３０２、通信部３０４、データ処理部３０６およびデータ格納部３０８を含む。ユーザインタフェース処理部３０２は、ユーザからの操作を受け付けるほか、画像表示や音声出力など、ユーザインタフェースに関する処理を担当する。通信部３０４は、無線の通信ネットワークを介して文書生成装置１００、ファイルサーバ１０４等との通信処理を担当する。データ格納部３０８は各種情報を格納する。データ処理部３０６は、ユーザインタフェース処理部３０２と通信部３０４により取得されたデータおよびデータ格納部３０８に格納されているデータに基づいて各種処理を実行する。データ処理部３０６は、ユーザインタフェース処理部３０２、通信部３０４およびデータ格納部３０８のインタフェースとしても機能する。

[0058] ユーザインタフェース処理部３０２は、入力部３１０および出力部３１２を含む。入力部３１０は、ユーザからの各種操作を受け付ける。出力部３１２は、画像、音声等により各種情報を出力する。

[0059] 通信部３０４は、文書生成装置１００等の外部装置に各種情報を送信する送信部３１４と、外部装置から各種情報を受信する受信部３１６を含む。

[0060] データ処理部３０６は、フィルタ設定部３１８とデータ管理部３２０を含む。フィルタ設定部３１８は、第２フィルタ（後述）を設定することにより、データ格納部３０８に格納されている個人情報の出力可能範囲を制御する

。データ管理部３２０は、データ格納部３０８にある個人情報を管理する。データ管理部３２０は、データ格納部３０８に保存するデータの暗号化、データ格納部３０８から読み出すデータの復号も行う。

[0061] 図６は、複数のファイルサーバ１０４に分散する個人情報をユーザ端末３００に集約する方法を説明するための模式図である。

ユーザの個人情報は、ユーザ端末３００等において管理されているものもあれば、ファイルサーバ１０４において管理されているものもある。ユーザは、各ファイルサーバ１０４に分散されているさまざまな個人情報をユーザ端末３００に集約させることができる。

[0062] ファイルサーバ１０４ａは公的機関Ａにより運営され、ファイルサーバ１０４ｂは別の公的機関Ｂにより運営されているとする。公的機関Ａ、Ｂはそれぞれ独自にファイルサーバ１０４ａ、ファイルサーバ１０４ｂを運営しているため、双方のデータ管理の方法には統一性がない。

[0063] ファイルサーバ１０４ａにおけるユーザＰＸに関する個人情報は、「項目」と「データ」の組み合わせとして管理されている。以下において、「データ」とは、項目に対応づけられる個人情報の一部を意味するものとする。また、データの集合体を意味するときには「個人情報」とよぶ。

[0064] ファイルサーバ１０４ａにおいては「項目ＴＡ：データＤ１」「項目ＴＢ：データＤ２」「項目ＴＣ：データＤ３」「項目ＴＤ：データＤ４」という４種類のデータが項目とともに管理されている。項目としては、「名前」「性別」「婚姻歴」「出生地」「住所」「金融資産」などが想定される。

[0065] ファイルサーバ１０４ｂにおいてもユーザＰＸに関する個人情報が項目とデータの組み合わせとして管理されている。ファイルサーバ１０４ｂにおいては「項目ＴＡ：データＤ１」「項目ＴＥ：データＤ２」「項目ＴＣ：データＤ３」「項目ＴＦ：データＤ５」という４種類のデータが項目とともに管理されている。

[0066] ユーザ端末３００は、データとタグを対応づけて、個人情報を管理する。「タグ」はデータの属性を定義する概念であり、本実施形態におけるタグに

は「項目名」が該当する。ユーザ端末３００の送信部３１４はファイルサーバ１０４ａにデータ取得要求（ダウンロード要求）を送信し、受信部３１６はユーザＰＸの個人情報をファイルサーバ１０４ａからダウンロードする。たとえば、「項目ＴＡ：データＤ１」が取得されたとき、データ管理部３２０は「データＤ１」と「タグＴＡ」を対応づけてデータ格納部３０８に登録する。以下、タグＴＡを付与されたデータＤ１のことを「データＤ１（ＴＡ）」のように表記する。

[0067] 同様にして、ユーザ端末３００はファイルサーバ１０４ｂからもユーザＰＸの個人情報をダウンロードする。「項目ＴＡ：データＤ１」はファイルサーバ１０４ａ、ファイルサーバ１０４ｂの双方から取得される重複したデータである。この場合、データ管理部３２０はデータＤ１（ＴＡ）を１つだけデータ格納部３０８に登録する。

[0068] ユーザ端末３００は、ファイルサーバ１０４ａから「項目ＴＢ：データＤ２」を受信したとき、データＤ２にタグＴＢを対応づけ、データＤ２（ＴＢ）として保存する。続いて、ファイルサーバ１０４ｂから「項目ＴＥ：データＤ２」を受信したときには、データＤ２にタグＴＥも対応づけられる。すなわち、データ管理部３２０は、データＤ２（ＴＢ、ＴＥ）をデータ格納部３０８に登録することになる。たとえば、ＴＢは「住所（address）」、ＴＥは「場所（place）」であり、ファイルサーバ１０４ａおよびファイルサーバ１０４ｂでは同じデータＤ２を異なる項目名で管理していることがある。この場合、データ管理部３２０は、単一のデータＤ２に対してＴＢタグ（住所）とＴＥタグ（場所）の２つを対応づける。

[0069] ファイルサーバ１０４ａが有する「項目ＴＣ：データＤ３」はファイルサーバ１０４ｂにも保有されている。ファイルサーバ１０４ａが有する「項目ＴＤ：データＤ４」はファイルサーバ１０４ｂには保有されておらず、ファイルサーバ１０４ｂが有する「項目ＴＦ：データＤ５」はファイルサーバ１０４ａには保有されていない。ユーザ端末３００はファイルサーバ１０４ａ、ファイルサーバ１０４ｂの双方にアクセスすることで、ファイルサーバ１

０４ａだけが管理するデータも、ファイルサーバ１０４ｂだけが管理するデータもユーザ端末３００に集めることができる。

[0070] ［第２実施形態］

第２実施形態においては、ＤＩエンジンを搭載するユーザ端末３００から文書生成装置１００に個人情報を選択的に送信し、文書生成装置１００は受信した個人情報に基づいて各種の公文書を生成する。公文書は電子データとして文書生成装置１００からユーザ端末３００に送信される。

[0071] 図７は、第２フィルタ３３０による出力制御を説明するための模式図である。

ユーザ端末３００は、個人情報の出力可能範囲を第２フィルタ３３０により制御する。一方、文書生成装置１００においては個人情報の入力可能範囲を第１フィルタにより制御する。第１フィルタについては図１１に関連して後述する。第２フィルタ３３０においては、データの出力を許可するタグ（以下、「許可タグ」とよぶ）と許可しないタグ（以下、「禁止タグ」とよぶ）が設定される。図７に示す第２フィルタ３３０においては、許可タグはタグＴＡ，ＴＣ，ＴＤ，ＴＥの４つであり、禁止タグはＴＢ，ＴＦの２つである。ユーザＰＸは、ユーザ端末３００において第２フィルタ３３０の許可タグおよび禁止タグを指定する。フィルタ設定部３１８はユーザＰＸからの指定にしたがって第２フィルタ３３０を設定する。送信部３１４は、データ格納部３０８に格納されるさまざまなデータの出力可否を第２フィルタ３３０にしたがって判定する。

[0072] データＤ１（ＴＡ）のタグＴＡは許可タグであるため、送信部３１４はデータＤ１（ＴＡ）を文書生成装置１００など外部装置へ送信する。データＤ２（ＴＢ，ＴＥ）のタグＴＢは禁止タグであるが、タグＴＥは許可タグであるため、送信部３１４はデータＤ２（ＴＢ，ＴＥ）も送信許可する。このように、送信部３１４は１つのデータに複数のタグが対応づけられている場合、複数のタグのいずれか１つが許可タグであれば送信を許可する。

[0073] タグＴＣは許可タグであるため、送信部３１４はデータＤ３（ＴＣ）の送

信を許可する。同様に、タグＴＤも許可タグであるため、送信部３１４はデータＤ４（ＴＤ）も送信する。一方、タグＴＦは禁止タグであるため、データＤ５（ＴＦ）はユーザ端末３００から外部に出力されない。このように、ユーザＰＸは第２フィルタ３３０を設定することにより、データ格納部３０８に格納されているさまざまな個人情報のうち「外部に出してもよいデータ」と「外部に出してはいけないデータ」を制御できる。

[0074] 図８は、文書生成装置１００が発行する公文書１３０の形式の一例である。

文書生成装置１００は、上述したように、住民票、運転免許証などさまざまな公文書１３０を発行する。公文書１３０ごとに、必要とするデータとそのレイアウト、デザインなどがあらかじめ決められている。図８に示す公文書１３０は住民票であり、さまざまな大きさの５種類の記入欄１３２が設定されている。以下においては、ユーザＰＸが図８に示す公文書１３０の発行を受ける場面を想定して説明する。

[0075] ５種類の記入欄１３２にはそれぞれ、タグＴＡ，ＴＢ，ＴＣ，ＴＦ，ＴＧが対応づけられている。すなわち、公文書１３０を発行するためには、これらのタグに対応づけられるデータをユーザＰＸは文書生成装置１００に提供する必要がある。

[0076] 文書生成部１２６は、公文書１３０を発行するとき、発行日時を発行日欄１３６に記載する。また、公文書１３０を発行するとき、文書生成部１２６は発行した公文書１３０を識別するための文書ＩＤを生成する。公文書１３０には、文書ＩＤおよび発行日時を含む二次元コード１３４も記載される。文書生成部１２６は、文書生成装置１００のＵＲＩ（Uniform Resource Identifier）を二次元コード１３４に含めてもよい。

[0077] 図９は、文書定義テーブル１４０のデータ構造図である。

文書定義テーブル１４０は、文書生成装置１００のデータ格納部１１４に格納される。文書定義テーブル１４０は、文書タイプごとに必要なタグ（項目）を定義するファイルである。文書タイプとは公文書１３０の種類を示す

。文書タイプによって記載すべき個人情報は異なる。たとえば、住民票と図書カードでは、記載すべきデータの種類および量が異なる。

[0078] 文書タイプＦ１の公文書１３０（以下、「公文書１３０（Ｆ１）」のように表記する）はタグＴＡ，ＴＢ，ＴＣ，ＴＤを付与されるデータを必要とする。公文書１３０が必要とするタグには「必須タグ」と「任意タグ」がある。以下、必須タグに対応するデータを「必須データ」、任意タグに対応するデータを「任意データ」とよぶ。また、公文書１３０の作成に必要としないタグを「不要タグ」、不要タグに対応するデータを「不要データ」とよぶ。

[0079] 上述した４つのタグＴＡ，ＴＢ，ＴＣ，ＴＤは、いずれも公文書１３０（Ｆ１）の必須タグである。文書生成部１２６は、ユーザＰＸからこれら４つの必須タグに対応する必須データが提供されれば、公文書１３０（Ｆ１）を生成できる。

[0080] 公文書１３０（Ｆ３）の必須タグはタグＴＡ，ＴＥ，ＴＫであり、タグＴＨは任意タグである。文書生成部１２６は必須タグＴＡ，ＴＥ，ＴＫに対応する必須データを取得できれば公文書１３０（Ｆ３）を生成する。任意データ（ＴＨ）も提供されたときには、文書生成部１２６は任意データ（ＴＨ）も公文書１３０（Ｆ３）に記載する。任意データ（ＴＨ）を取得できなかったときには、文書生成部１２６は任意データ（ＴＨ）を含まない公文書１３０（Ｆ３）を発行する。

[0081] 図１０は、発行履歴情報１５０のデータ構造図である。

発行履歴情報１５０も、文書生成装置１００のデータ格納部１１４に格納される。上述したように、文書生成部１２６はユーザからの求めに応じて公文書１３０を発行するとき、文書ＩＤを生成し、発行日時を記録する。文書生成部１２６は、文書ＩＤおよび発行日時を含む二次元コード１３４を公文書１３０に記載するとともに、発行履歴情報１５０にも登録する。たとえば、文書ＩＤ＝Ｋ０１の公文書１３０は、文書タイプは「Ｆ１」であり、「２０２１年７月２１日の１４時３５分」に発行されている。以下、文書ＩＤおよび発行日時をまとめて「発行情報」とよぶ。

[0082] 図１１は、第１フィルタ１６０による入力制御を説明するための模式図である。

上述したように、ユーザ端末３００は、個人情報の出力可能範囲を第２フィルタ３３０により制御する。文書生成装置１００においては個人情報の入力可能範囲を第１フィルタ１６０により制御する。すなわち、ユーザ端末３００に格納される個人情報のうち第２フィルタ３３０により出力許可されるデータのみが文書生成装置１００に送信され、ユーザ端末３００から送信されるデータのうち第１フィルタ１６０により入力許可されるデータだけが文書生成装置１００により処理対象として受け入れられる。

[0083] ユーザＰＸは、文書生成装置１００に対して公文書１３０（Ｆ２）の発行を要求したとする。図９に示したように公文書１３０（Ｆ２）は５種類の必須タグＴＡ，ＴＢ，ＴＣ，ＴＦ，ＴＧを有する。なお、公文書１３０（Ｆ２）は、図８に示した公文書１３０に対応する。

[0084] 文書生成装置１００のフィルタ設定部１２８は、ユーザＰＸのユーザ端末３００から公文書１３０（Ｆ２）の発行要求が受信されたとき、第１フィルタ１６０の許可タグと禁止タグを文書定義テーブル１４０に基づいて設定する。具体的には、必須タグおよび任意タグは許可タグとして設定され、不要タグは禁止タグとして設定される。公文書１３０（Ｆ２）の場合、タグＴＡ，ＴＢ，ＴＣ，ＴＦ，ＴＧが許可タグとなっており、タグＴＤ，ＴＥは禁止タグとなっている。

[0085] ユーザＰＸのユーザ端末３００からは、第２フィルタ３３０を通して、データＤ１（ＴＡ），データＤ２（ＴＢ，ＴＥ）、データＤ３（Ｔ３）、データＤ４（ＴＤ）が文書生成装置１００に送信されている（図７も参照）。

[0086] 文書生成装置１００の検査部１２２は、これら４種類のデータの受入可否を第１フィルタ１６０に基づいて判定する。タグＴＡ，ＴＢ，ＴＣは許可タグなので、検査部１２２はデータＤ１（ＴＡ）、データＤ２（ＴＢ，ＴＥ）、データＤ３（ＴＣ）を受け入れる。データＤ２（ＴＢ，ＴＥ）は、出力時の第２フィルタ３３０においてタグＴＢは禁止タグ、タグＴＥは許可タグと

なっていたのでタグＴＥに基づいて出力されている。一方、入力時の第１フィルタ１６０においてタグＴＢは許可タグ、タグＴＥは禁止タグとなっているので、データＤ２（ＴＢ，ＴＥ）はタグＴＢに基づいて受信されている。このように複数のタグを有するデータは、出力許可および入力許可されやすくなる。

[0087] タグＴＤが禁止タグであるため、検査部１２２はデータＤ４（ＴＤ）を受け入れない。検査部１２２はデータＤ４（ＴＤ）をいったん受信したあとはこのデータＤ４（ＴＤ）をローカルメモリから削除する。検査部１２２はデータＤ４（ＴＤ）をローカルストレージにも残さない。したがって、公文書１３０（Ｆ２）の生成に際して不要データが文書生成装置１００に残ることはない。ユーザＰＸは第２フィルタ３３０により出力可能な個人情報の範囲を定義しつつ、文書生成装置１００は不必要な個人情報を取得・保存しないことを保証するため、ユーザ端末３００から文書生成装置１００に提供される情報量を必要最小限に絞ることができる。

[0088] 許可タグＴＦに対応する必須データＤ５（ＴＦ）はユーザ端末３００に保存されている（図７参照）。ユーザＰＸは第２フィルタ３３０においてタグＴＦを禁止タグに設定していたため、文書生成装置１００には必須データＤ５（ＴＦ）が送信されていない。

[0089] 許可タグＴＧに対応する必須データはユーザ端末３００に保存されていない。ユーザＰＸは、公文書１３０（Ｆ２）を発行してもらうためには、許可タグＴＦ，ＴＧに対応する必須データも文書生成装置１００に提供する必要がある。以下、公文書１３０を生成するのに必要でありながら、ユーザ端末３００から提供されていないデータに対応するタグのことを「不足タグ」とよぶ。また、不足タグに対応するデータのことを「不足データ」とよぶ。すなわち、不足データとは、必須データのうち、ユーザ端末３００から文書生成装置１００に提供されていないデータである。図１１の例では、タグＴＦ，ＴＧは公文書１３０（Ｆ２）の不足タグとなっている。

[0090] 詳細は後述するが、不足タグＴＦについては、ユーザＰＸは必須データＤ

５（ＴＦ）が出力されるように第２フィルタ３３０を調整する必要がある。具体的には、ユーザＰＸは不足タグＴＦを許可タグに設定する。一方、不足タグＴＧについては、ユーザＰＸは不足タグＴＧに対応するデータ（個人情報）を手動入力する必要がある。

[0091] なお、文書生成装置１００のフィルタ設定部１２８は任意タグについても、第１フィルタ１６０において許可タグに設定する。たとえば、公文書１３０（Ｆ３）の場合、ユーザは任意タグＴＨを第１フィルタ１６０の許可タグに設定する。文書生成部１２６は、任意データ（ＴＨ）が得られなくても公文書１３０（Ｆ３）を生成できるので、この場合には任意タグＴＨを不足タグには設定しない。

[0092] 以下、タグおよびデータに関する用語をまとめる。

必須データ：公文書１３０を生成するために必要なデータ。

任意データ：公文書１３０に記載可能であるが、提供されなければ公文書１３０に記載されないデータ。

不要データ：公文書１３０に使用されないデータ。

不足データ：公文書１３０の必須データのうち、ユーザから提供されていないデータ。

必須タグ：必須データに対応するタグ。

任意タグ：任意データに対応するタグ。

不要タグ：不要データに対応するタグ。

不足タグ：不足データに対応するタグ。

許可タグ：第２フィルタ３３０または第１フィルタ１６０において、通過を許可されるタグ。第１フィルタ１６０においては必須タグおよび任意タグが許可タグとされる。

禁止タグ：第２フィルタ３３０または第１フィルタ１６０において、通過を禁止されるタグ。第１フィルタ１６０においては不要タグが禁止タグとされる。

[0093] 第２フィルタ３３０の許可タグ、禁止タグ、第１フィルタ１６０の許可タ

グ、禁止タグによって、個人情報に含まれる各種データが文書生成装置１００に受け入れられるかが決まる。

以下、

タグＴ１：第２フィルタ３３０および第１フィルタ１６０の双方において許可タグとなっている。

タグＴ２：第２フィルタ３３０において許可タグ、第１フィルタ１６０において禁止タグとなっている。

タグＴ３：第２フィルタ３３０において禁止タグ、第１フィルタ１６０において許可タグとなっている。

タグＴ４：第２フィルタ３３０において禁止タグ、第１フィルタ１６０において禁止タグとなっている。

とする。

データ（Ｔ１）：第２フィルタ３３０を通過して、ユーザ端末３００から文書生成装置１００に送信される。第１フィルタ１６０も通過して、文書生成装置１００により処理対象として受け入れられる。

データ（Ｔ２）：第２フィルタ３３０を通過して、ユーザ端末３００から文書生成装置１００に送信される。第１フィルタ１６０を通過できないので文書生成装置１００にいったん受信されても即時にローカルメモリ（受信メモリ）から削除される。

データ（Ｔ３）：第２フィルタ３３０を通過できないので、文書生成装置１００から出力されることはない。

データ（Ｔ４）：第２フィルタ３３０を通過できないので、文書生成装置１００から出力されることはない。

すなわち、タグＴ１を有するデータのみが、文書生成装置１００の処理対象となる。

[0094] 図１２は、第２実施形態における文書生成装置１００の公文書発行過程を示すフローチャートである。

ユーザは、まず、ユーザＩＤおよびパスワードとともに文書タイプを指定

する発行要求を送信する。発行要求と同時に、ユーザ端末３００は、第２フィルタ３３０にしたがって個人情報の一部を文書生成装置１００に送信する。図１２に示す処理は、発行要求および個人情報の一部が文書生成装置１００に受信されたあとに開始される。

[0095] 文書生成装置１００のフィルタ設定部１２８は、文書タイプに応じて第１フィルタ１６０を設定する（Ｓ１０）。検査部１２２は、ユーザ端末３００から受信した各種データに不要データがないかを検査する（Ｓ１２）。図１１に示した例の場合、データＤ４（ＴＤ）は不要データである。不要データがあれば（Ｓ１２のＹ）、検査部１２２は不要データをローカルメモリ（受信メモリ）から削除する（Ｓ１４）。不要データがなければ（Ｓ１２のＮ）、Ｓ１４の処理はスキップされる。

[0096] 次に、検査部１２２は、不足データがないかを検査する（Ｓ１６）。不足データがあるときには（Ｓ１６のＮ）、通知部１２０は不足タグをユーザ端末３００に通知する（Ｓ２４）。不足タグの通知を受けた場合、ユーザ端末３００は不足タグに対応するデータを改めて文書生成装置１００に送信する必要がある。ユーザ端末３００の不足タグ通知への対応方法については後述する。

[0097] 不足データがないときには（Ｓ１６のＹ）、すなわち、公文書１３０の必須データがすべてそろったときには、文書生成部１２６は公文書１３０を生成する（Ｓ１８）。具体的には、文書生成部１２６は公文書１３０の記入欄１３２に、ユーザＰＸから受信した必須データまたは任意データを記入し、二次元コード１３４および発行日欄１３６を追記することで公文書１３０を生成する。文書生成部１２６は、発行情報（文書ＩＤと発行日時）を発行履歴情報１５０に登録する（Ｓ２０）。

[0098] 送信部１１８は、生成された公文書１３０を電子データ、たとえば、ＰＤＦ（Portable Document Format）ファイルとしてユーザ端末３００に送信する（Ｓ２２）。なお、文書生成部１２６は、公文書１３０を付属のプリンタによって印刷し、ユーザＰＸの住所に郵便発送するように手配をしてもよい

。

[0099] 以上のように、文書生成装置１００は公文書１３０の作成に必要な範囲で個人情報を取得し、記入欄１３２に必須データまたは任意データを記載することで公文書１３０を生成する。また、公文書１３０の作成後は、検査部１２２はユーザ端末３００から受信したデータをすべてローカルメモリおよびローカルストレージから削除する。同様に、公文書１３０の送信後は、文書生成部１２６は公文書１３０自体もローカルメモリおよびローカルストレージから削除する。このような制御方法によれば、文書生成装置１００は、公文書１３０を生成するときだけ個人情報を取得し、その後は個人情報を保存しないのでユーザＰＸの個人情報が文書生成装置１００から漏洩するリスクを最小化できる。

[0100] 図１３は、ユーザ端末３００が不足タグを通知されたときの処理過程を示すフローチャートである。

不足タグが存在するとき、すなわち、公文書１３０の必須データが不足しているときには、文書生成装置１００の通知部１２０はユーザ端末３００に不足タグを通知する。ここでは、図１１の例示にしたがってタグＴＦ，ＴＧが不足タグとして通知されたとする。

[0101] 不足データ、すなわち、未提供の必須データがユーザ端末３００のデータ格納部３０８に格納されているときには（Ｓ３０のＹ）、ユーザＰＸは第２フィルタ３３０を調整する（Ｓ３２）。たとえば、不足データＤ５（ＴＦ）はデータ格納部３０８に存在するので（図７参照）、ユーザＰＸは第２フィルタ３３０においてタグＴＦを許可タグに設定変更すればよい。不足データがデータ格納部３０８に格納されていないときには（Ｓ３０のＮ）、Ｓ３２の処理はスキップされる。

[0102] 第１フィルタ１６０の調整後も未出力の不足データが残っている場合には（Ｓ３４のＹ）、いいかえれば、未保有の不足データがあるときには、ユーザＰＸは新たにデータを入力する（Ｓ３６）。このとき、ユーザ端末３００の出力部３１２は後述のデータ補充画面３４０からタグＴＧに対応するデー

タをユーザに入力させる。あるいは、出力部３１２は「タグＴＧに対応するデータを入力してください」と表示するとともにデータ入力画面を表示させてもよい。タグＴＧが、たとえば「生年月日」であれば、出力部３１２は生年月日を入力するためのデータ入力画面を表示させればよい。不足タグＴＧに対応するデータはデータ格納部３０８には存在しないので、ユーザＰＸは不足タグＴＧに対応するデータＤＸをユーザ端末３００に入力する（Ｓ３６）。ユーザ端末３００の入力部３１０は、データＤＸの入力を受け付ける。また、ユーザ端末３００のデータ管理部３２０は、新規入力したデータＤＸにタグＴＧを対応づけてデータ格納部３０８にデータＤＸ（ＴＧ）として登録する（Ｓ３８）。不足データがなければ（Ｓ３４のＮ）、Ｓ３６，Ｓ３８の処理はスキップされる。

[0103] 公文書１３０の不足データがすべて補充されたあと、送信部３１４は不足データを文書生成装置１００に追加送信する（Ｓ４０）。不足タグがタグＴＦ，ＴＧのときには、送信部３１４はデータＤ５（ＴＦ）とデータＤＸ（ＴＧ）を送信する。以上の処理過程を経て、文書生成装置１００は公文書１３０の必須データを取得する。

[0104] なお、データ格納部３０８にデータＤＸ（ＴＩ）が登録されていたとする。ここで、ユーザＸが不足タグ（ＴＧ）に対応してデータＤＸを入力した場合には、データ管理部３２０は、タグＴＩがすでに対応づけられているデータＤＸに新たにタグＴＧも対応づける。データＤＸの入力後、データＤＸはタグＴＧ，ＴＩの双方に対応可能なデータＸ（ＴＧ，ＴＩ）として管理される。

[0105] 図１４は、データ補充画面３４０の画面図である。

文書生成装置１００から不足タグを通知されたとき、ユーザ端末３００の出力部３１２はデータ補充画面３４０を表示させる。ここでは不足タグＴＦ，ＴＧが通知されたとする。出力部３１２は、不足タグＴＦの隣りにフィルタ調整ボタン３４２、不足タグＴＧの隣りにデータ入力ボタン３４４を表示させる。

[0106] より具体的には、不足データ（ＴＦ）がデータ格納部３０８に存在するときには、出力部３１２は第２フィルタ３３０を調整するためのフィルタ調整ボタン３４２をタグＴＦに対応する位置に表示させる。ユーザＰＸがフィルタ調整ボタン３４２をタッチしたとき、フィルタ設定部３１８は第２フィルタ３３０においてタグＴＦを禁止タグから許可タグに変更する（図１３のＳ３２）。第２フィルタ３３０の設定変更により、不足データＤ５（ＴＦ）は文書生成装置１００へ送信可能となる。

[0107] 不足データ（ＴＧ）がデータ格納部３０８に存在しないときには、出力部３１２はデータ入力するためのデータ入力ボタン３４４をタグＴＧに対応する位置に表示させる。ユーザがデータ入力ボタン３４４をタッチしたとき、出力部３１２はデータ入力画面（不図示）を表示させる。ユーザがこのデータ入力画面でデータＤＸを入力したとき、データ管理部３２０はデータＤＸとタグＴＧを対応づけてデータ格納部３０８に登録する。また、不足データＤＸ（ＴＧ）は文書生成装置１００への送信が可能となる。

[0108] 図１５は、公文書１３０の真正確認時の処理過程を示すシーケンス図である。

ここでは、ユーザＰＸから公文書１３０Ｘを提示されたユーザＰＹが、この公文書１３０Ｘの真正性を確認する場面を想定して説明する。ユーザＰＹは、自らのユーザ端末３００を用いて公文書１３０Ｘの二次元コード１３４を読み取る（Ｓ５０）。ユーザ端末３００の送信部３１４は、二次元コード１３４に含まれる発行情報（文書ＩＤおよび発行日時）を文書生成装置１００に送信する（Ｓ５２）。

[0109] 文書生成装置１００の証明部１２４は、受信した発行情報が発行履歴情報１５０に登録されていれば公文書１３０Ｘは本物であると判定する。一方、発行履歴情報１５０に登録されていなければ、証明部１２４は、公文書１３０は文書生成装置１００から発行されていない偽文書であると判定する（Ｓ５４）。送信部１１８は判定結果をユーザ端末３００に送信する（Ｓ５６）。

[0110] ユーザＰＸから公文書１３０Ｘを提示されたユーザＰＹは、二次元コード１３４に含まれる発行情報に基づいて文書生成装置１００に問い合わせることで、公文書１３０Ｘの真偽を簡易に確認できる。

[0111] ［第３実施形態］

第３実施形態においては、ユーザバッジ３５０から中継端末４００を介して文書生成装置１００に個人情報を選択的に送信し、文書生成装置１００は受信した個人情報に基づいて各種の公文書１３０を生成する。公文書１３０は電子データとして文書生成装置１００から中継端末４００に送信される。

[0112] 第３実施形態においては、ユーザバッジ３５０に個人情報が記録される。ユーザバッジ３５０はＤＩエンジンを搭載するが、ユーザインタフェース機能とインターネット接続機能を有していない点においてユーザ端末３００と異なる。ユーザバッジ３５０は個人情報と第２フィルタ３３０を含む。ユーザバッジ３５０はＮＦＣ（Near Field Communication）、Bluetooth（登録商標）など、インターネット１０２を介さない近距離無線通信によりデータの送受信が可能である。

[0113] ユーザＰＸは、ユーザ端末３００からユーザバッジ３５０に個人情報および第２フィルタ３３０をコピーすることもできる。たとえば、ユーザ端末３００にユーザバッジ３５０のバッジＩＤを登録しておけば、ユーザ端末３００の送信部３１４は登録済みのユーザバッジ３５０に対してのみ、個人情報と第２フィルタ３３０を書き込むことができる。

[0114] ユーザバッジ３５０は、バッジ型の情報担体である。情報担体は、このほかにも、カード型であってもよい。指輪、リストバンド、メガネなどさまざまな装身具に情報担体（ＤＩエンジン）としての機能をもたせてもよい。

[0115] 図１６は、第３実施形態における文書生成システム２１０のハードウェア構成図である。

文書生成システム２１０においては、文書生成装置１００と中継端末４００は有線または無線により接続される。ユーザバッジ３５０はインターネット１０２を介した通信機能を備えていないため、第３実施形態においては、

ユーザバッジ３５０は中継端末４００を経由して文書生成装置１００にデータを送信する。

[0116] 中継端末４００は、一般の店舗に設置される。中継端末４００にはプリンタ４０６が接続される。中継端末４００はタッチパネル付きのモニタ４０２と近距離無線通信によるデータの読み書きが可能なリーダ／ライタ４０４を備える。ユーザＰＸは、ユーザバッジ３５０をリーダ／ライタ４０４にかざすことで中継端末４００に個人情報を読み取らせる。中継端末４００はユーザバッジ３５０から読み取った個人情報を文書生成装置１００に送信し、文書生成装置１００は公文書１３０を生成してその電子データを中継端末４００に送信する。中継端末４００は公文書１３０をプリンタ４０６から印刷する。

[0117] 図１７は、中継端末４００の機能ブロック図である。

中継端末４００は、ユーザインタフェース処理部４１０、通信部４１２、リーダ／ライタ処理部４１４、データ処理部４１６およびデータ格納部４１８を含む。ユーザインタフェース処理部４１０は、ユーザからの操作を受け付けるほか、画像表示や音声出力など、ユーザインタフェースに関する処理を担当する。通信部４１２は、無線の通信ネットワークを介して文書生成装置１００との通信処理を担当する。リーダ／ライタ処理部４１４はリーダ／ライタ４０４によりユーザバッジ３５０とのデータ送受を行う。データ格納部４１８は各種情報を格納する。データ処理部４１６は、ユーザインタフェース処理部４１０、通信部４１２およびリーダ／ライタ処理部４１４により取得されたデータおよびデータ格納部４１８に格納されているデータに基づいて各種処理を実行する。データ処理部４１６は、ユーザインタフェース処理部４１０、通信部４１２、リーダ／ライタ処理部４１４およびデータ格納部４１８のインタフェースとしても機能する。

[0118] ユーザインタフェース処理部４１０は、入力部４２０および出力部４２２を含む。入力部４２０は、タッチパネルを介してユーザからの各種操作を受け付ける。出力部４２２は、画像、音声等により各種情報を出力する。

[0119] 通信部４１２は、文書生成装置１００に各種情報を送信する受信部４２４と、文書生成装置１００から各種情報を受信する送信部４２６を含む。送信部４２６は、文書生成装置１００から第１フィルタ１６０を受信する。

[0120] リーダ／ライタ処理部４１４は、ユーザバッジ３５０からデータを読み取るデータ取得部４２８と、ユーザバッジ３５０にデータを書き込むデータ書込部４３０を含む。

[0121] データ処理部４１６は、検査部４３２、フィルタ設定部４３４、データ登録部４３６および印刷制御部４３８を含む。

検査部４３２は、第１フィルタ１６０に基づいて、ユーザバッジ３５０から取得したデータのうち文書生成装置１００に送信すべきデータを選択する。フィルタ設定部４３４は、文書生成装置１００から受信した第１フィルタ１６０を設定する。また、フィルタ設定部４３４は、ユーザからの指示により第２フィルタ３３０の許可タグおよび禁止タグを設定変更することもできる。データ登録部４３６は、ユーザバッジ３５０へのデータの登録を実行する。印刷制御部４３８はプリンタ４０６を制御する。

[0122] なお、ユーザバッジ３５０のＤＩエンジンは、書き込まれるデータを暗号化して内蔵するローカルストレージに保存し、ローカルストレージからデータを出力するときには暗号化されているデータを復号する。

[0123] 図１８は、第３実施形態における個人情報の入出力制御を説明するための模式図である。

ユーザバッジ３５０は、各種の個人情報と第２フィルタ３３０を格納する。図６と同様、ユーザバッジ３５０は、データＤ１（ＴＡ）、データＤ２（ＴＢ，ＴＥ）、データＤ３（ＴＣ）、データＤ４（ＴＤ）およびデータＤ５（ＴＦ）を内蔵しているとする。また、図７と同様、第２フィルタ３３０においてはタグＴＡ，ＴＣ，ＴＤ，ＴＥが許可タグであり、タグＴＢ，ＴＦは禁止タグであるとする。

[0124] 第２フィルタ３３０により、ユーザバッジ３５０からはデータＤ１（ＴＡ）、データＤ２（ＴＢ，ＴＥ）、データＤ３（ＴＣ）、データＤ４（ＴＤ）

が出力されるが、データＤ５（ＴＦ）は出力されない。上述したように、ユーザバッジ３５０のＤＩエンジンはデータ出力時に復号処理を実行する。

[0125] ユーザＸは、モニタ４０２においてユーザＩＤ、パスワードおよび発行したい公文書１３０の文書タイプ（例：住民票）を入力する。中継端末４００の送信部４２６は、文書タイプを文書生成装置１００に通知する。文書生成装置１００のフィルタ設定部１２８は、文書タイプに対応する第１フィルタ１６０を設定し、第１フィルタ１６０を中継端末４００に送信する。ここでは文書タイプ（Ｆ２）が指定され、図１１に示す第１フィルタ１６０が送信されたとする。すなわち、第１フィルタ１６０においてはタグＴＡ，ＴＢ，ＴＣ，ＴＦ，ＴＧが許可タグ、タグＴＤ，ＴＥが禁止タグとして設定される。

[0126] 中継端末４００のフィルタ設定部４３４は、文書生成装置１００から受信した第１フィルタ１６０を設定する。検査部４３２は第１フィルタ１６０にしたがってユーザバッジ３５０から出力されたデータの受入可否を判定する。

[0127] フィルタ設定部４３４は、第１フィルタ１６０にしたがって、データＤ１（ＴＡ）、データＤ２（ＴＢ，ＴＥ）、データＤ３（ＴＣ）を受け入れるが、データＤ４（ＴＤ）は受け入れを拒否する。フィルタ設定部４３４は、いったん受け取ったデータＤ４（ＴＤ）をローカルメモリから削除する。

[0128] 検査部４３２は、第１フィルタ１６０および受信したデータを参照し、不足タグＴＦ，ＴＧを特定する。このとき、出力部４２２は図１４に示したデータ補充画面３４０と同様の画面をモニタ４０２に表示させる。ユーザＰＸはフィルタ調整ボタン３４２をタッチすることによりタグＴＦを第２フィルタ３３０の許可タグに設定できる。このとき、フィルタ設定部４３４はデータ書込部４３０を介してユーザバッジ３５０の第２フィルタ３３０の設定を変更し、データ取得部４２８は不足データＤ５（ＴＦ）をユーザバッジ３５０から取得する。送信部４２６は不足データＤ５（ＴＦ）を文書生成装置１００に送信する。

[0129] ユーザＰＸはデータ入力ボタン３４４をタッチすることにより、タグＴＧに対応するデータＤＸを入力できる。送信部４２６は不足データＤＸ（ＴＧ）を文書生成装置１００に送信する。また、データ登録部４３６はデータＤＸ（ＴＧ）を、データ書込部４３０を介してユーザバッジ３５０に書き込む。

[0130] なお、ユーザＰＸは、データＤＸ（ＴＧ）をユーザバッジ３５０に書き込むとき、第２フィルタ３３０においてタグＴＧを許可タグとするか禁止タグとするかを指定できてもよい。フィルタ設定部３１８は、ユーザＰＸからの指示にしたがって第２フィルタ３３０のタグＴＧについて設定を追加する。

[0131] 図１９は、第３実施形態における中継端末４００の公文書発行過程を示すフローチャートである。

ユーザは、まず、ユーザＩＤおよびパスワードとともに文書タイプを指定する発行要求を中継端末４００に入力する。中継端末４００は文書生成装置１００に文書タイプを通知し、文書生成装置１００のフィルタ設定部１２８は文書タイプに対応する第１フィルタ１６０を中継端末４００に送信する。また、文書生成装置１００は、第１フィルタ１６０の許可タグそれぞれについて、必須タグおよび任意タグのいずれであるかも通知する。以上の準備が完了したあと、図１９に示す処理が開始される。

[0132] 中継端末４００のフィルタ設定部４３４は、第１フィルタ１６０を設定する（Ｓ６０）。検査部４３２は、ユーザバッジ３５０から受信した各種データに不要データ、すなわち、第１フィルタ１６０の禁止タグに対応づけられているデータがないかを検査する（Ｓ６２）。不要データがあれば（Ｓ１２のＹ）、検査部４３２はこの不要データをローカルメモリから削除する（Ｓ６４）。不要データがなければ（Ｓ６２のＮ）、Ｓ６４の処理はスキップされる。

[0133] 次に、検査部４３２は、不足データ、すなわち、必須タグに対応するデータに不足がないかを検査する（Ｓ６６）。必須データに不足がなければ（Ｓ６６のＹ）、送信部４２６はユーザバッジ３５０から受信したデータのうち

、公文書１３０の作成に必要な必須データをすべて文書生成装置１００に送信する（Ｓ６８）。なお、任意データも取得されているときには、送信部４２６は任意データも文書生成装置１００に送信する。

[0134] 文書生成装置１００の文書生成部１２６は公文書１３０を作成し、文書生成装置１００の送信部１１８は中継端末４００に公文書１３０（電子データ）を送信する。中継端末４００の受信部４２４は公文書１３０を受信する（Ｓ７０）。印刷制御部４３８は、プリンタ４０６を制御して公文書１３０を印刷する（Ｓ７２）。このような制御方法により、ユーザＰＸはユーザバッジ３５０を中継端末４００のリーダ／ライタ４０４にかざすだけで、所望の公文書１３０を店舗にて受け取ることができる。

[0135] 一方、必須データに不足があれば（Ｓ６６のＮ）、出力部４２２は不足データの補充を促す（Ｓ７４）。上述したように、ユーザＰＸは第２フィルタ３３０の調整またはデータの新規入力をすることにより不足データを補充する。

[0136] ［総括］

以上、実施形態に基づいて、文書生成システム２００、２１０を説明した。

ユーザは複数のファイルサーバ１０４にアクセスすることによりユーザ端末３００に個人情報を集約できる。さまざまなファイルサーバ１０４に分散されている個人情報をユーザ端末３００に集める方式なので、ユーザ端末３００に個人情報を手動で登録するよりも登録負担が大幅に軽減される。

[0137] 図６に関連して説明したように、同じデータＤ２が、ファイルサーバ１０４ａとファイルサーバ１０４ｂでは別々の項目名にて取り扱われていることもある。この場合、ユーザ端末３００は、データＤ２に２つの項目名をタグＴＢ，ＴＥとして対応づけるので、データＤ２はさまざまな第１フィルタ１６０、第２フィルタ３３０に基づく通過検査に対応しやすくなる。

[0138] たとえば、ユーザは、自分の居住地に関する情報を出力許可したいとする。この場合、ユーザはタグＴＢ（住所）を第２フィルタ３３０の許可タグに

設定してもよいし、タグＴＥ（場所）を許可タグに設定してもよい。ユーザは「居住地に関する情報」から連想されるタグＴＢを許可タグとすれば、改めてタグＴＥ（場所）も許可タグに設定する必要はない。このため、類似した名前のタグが多数生成された場合であっても、ユーザは１つのタグを許可タグとして選ぶだけで関連するタグも実質的に許可タグとできるため、タグが多様化しても管理しやすくなる。

[0139] さまざまな機関により運営される多数の文書生成装置１００を想定した場合、文書生成装置１００によって許可タグの名称が統一されるとは限らない。たとえば、文書生成装置１００ａでは「居住地に関する情報」についてタグＴＢ（住所）が対応づけられ、文書生成装置１００ｂでは「居住地に関する情報」についてタグＴＥ（場所）が対応づけられるかもしれない。この場合、上述したように１つのデータに対して複数のタグを対応づけることで、データ管理に柔軟性をもたせることができる。

[0140] ユーザは、第２フィルタ３３０を設定することにより、外部に出力してよい個人情報の範囲を定義できる。ユーザ端末３００あるいはユーザバッジ３５０に個人情報を無制限に蓄積した上で、個人情報の出力可能範囲を設定する方式であるため、ユーザ端末３００等に個人情報を集約しつつも過度な情報流出を招かないように制御できる。

[0141] ユーザは、ユーザ端末３００から文書生成装置１００にアクセスすることにより、あるいは、ユーザバッジ３５０を中継端末４００にかざすことにより、いつでもどこでも文書生成装置１００による公文書発行サービスを受けることができる。いいかえれば、ユーザは２４時間年中無休にて、公的機関により身分証明をしてもらうことができる。

[0142] 文書生成装置１００は、公文書１３０の文書タイプごとに第１フィルタ１６０を設定する。文書生成装置１００あるいは中継端末４００は、公文書１３０の作成に不必要なデータをローカルメモリおよびローカルストレージから削除するため、文書生成装置１００等は不必要なデータを収集しなくなる。更に、文書生成装置１００等は、公文書１３０の発行後は受信した個人情

報をすべてローカルメモリあるいはローカルストレージから削除することで、いっそう厳格な情報管理が可能となる。

[0143] 第１フィルタ１６０および第２フィルタ３３０のダブルフィルタにより、公文書１３０の作成に必要なデータが揃わないときには、ユーザは第２フィルタ３３０の調整により不足データを追加補充できる。いいかえれば、ユーザは不足タグに応じて第２フィルタ３３０を調整するだけで、文書生成装置１００に必要最小限の範囲にてデータを追加送信できる。また、ユーザが不足タグに対応して新規データを入力したときには、ユーザ端末３００あるいはユーザバッジ３５０において不足タグと新規データが対応づけて登録される。

[0144] ユーザが不足タグに応じてデータを新規入力するごとに、個人情報はいっそう充実し、次回からは同じデータを入力する必要はなくなるので利便性も向上する。更に、新規入力したデータＤＸがすでに別のタグＴ１に対応づけられているときには、データＤＸに不足タグＴ２が追加で対応づけられる。この結果、次回からはタグＴ１，Ｔ２のいずれについても同一データＤＸで対応できるので、そのデータＤＸの適用範囲が拡大される。このように、文書生成装置１００の文書発行サービスを利用することでデータ管理の柔軟性も高くなる。

[0145] 文書生成装置１００は、公文書１３０を発行するとき、発行履歴情報１５０に発行情報を登録する。このため、ユーザは、公文書１３０の二次元コード１３４を読み取って文書生成装置１００に問い合わせることにより、公文書１３０が真文書か偽文書であるかを直ぐに確認できる。

[0146] ユーザは、ユーザ端末３００の個人情報を第２フィルタ３３０とともにユーザバッジ３５０に移動または複製できる。ユーザは、ユーザ端末３００よりも軽量かつ携行しやすいユーザバッジ３５０を持ち歩くことにより、手軽に身分証明サービスを受けることができる。ユーザバッジ３５０のＤＩエンジンは、ユーザバッジ３５０の紛失に備えて個人情報を暗号化して保存する。中継端末４００は、ユーザＩＤとパスワードによる本人認証が成功しなか

ったときには、リーダ／ライタ４０４からのデータの受け入れを拒否してもよい。

[0147] なお、本発明は上記実施形態や変形例に限定されるものではなく、要旨を逸脱しない範囲で構成要素を変形して具体化することができる。上記実施形態や変形例に開示されている複数の構成要素を適宜組み合わせることにより種々の発明を形成してもよい。また、上記実施形態や変形例に示される全構成要素からいくつかの構成要素を削除してもよい。

[0148] ［変形例］

本実施形態においては、文書生成装置１００は公的機関により運営され、ユーザは文書生成装置１００から住民票などの公文書１３０の発行サービスを受ける場面を想定して説明した。文書生成装置１００は、公文書１３０以外にもさまざまな文書を発行してもよい。たとえば、発行対象となる文書としては、企業のポイントカード、荷物の宛名シート、年賀状、投資報告書、作業報告書、領収書、医療カルテ、伝票などが考えられる。また、文書生成装置１００が生成する「文書」は、静止画像、動画ファイル、音声ファイル等のテキスト以外の形式にて情報を含む電子データであってもよい。

[0149] 文書生成装置１００は、文書の作成に必要なデータをすべてユーザから取得する必要はない。文書に含まれる必須データまたは任意データの一部は文書生成装置１００にあらかじめ保存されているデータであってもよいし、文書生成装置１００が他のファイルサーバ１０４から取得してもよい。

[0150] 文書生成装置１００または中継端末４００は、第１フィルタ１６０をユーザに提示してもよい。たとえば、文書生成装置１００の送信部１１８は、第１フィルタ１６０をユーザ端末３００あるいは中継端末４００に送信し、第１フィルタ１６０において設定される許可タグをリスト表示させてもよい。ユーザは、文書作成前に、第１フィルタ１６０（許可タグのリスト）を参照し、文書ごとに必須タグと任意タグを確認してもよい。

[0151] 第２フィルタ３３０は複数であってもよい。ユーザは複数の第２フィルタ３３０から適宜いずれかの第２フィルタ３３０を選択してもよい。たとえば

、ユーザはデータの出力先に応じて第２フィルタ３３０を選択してもよい。

[0152] ユーザはデータの出力先に応じて複数の第２フィルタ３３０を組み合わせてもよい。たとえば、データの出力先Ｙ１に対しては、ユーザは、第２フィルタ３３０Ａを使用し、データの出力先Ｙ２に対しては、ユーザは、第２フィルタ３３０Ａと第２フィルタ３３０Ｂを使用してもよい。この場合、ユーザ端末３００の送信部３１４は、第２フィルタ３３０Ａおよび第２フィルタ３３０Ｂの双方において許可タグとして設定されているデータのみを出力するとしてもよい。このような制御方法によれば、出力先に応じて個人情報の出力範囲制限の強さを第２フィルタ３３０の使用枚数によって制御できる。

[0153] 本実施形態においては、二次元コード１３４は発行情報として文書ＩＤと発行日時を含むとして説明した。変形例として、二次元コード１３４には文書ＩＤと発行日時のハッシュ値を含めてもよい。ハッシュ値とすることで二次元コード１３４からは文書ＩＤ等を直接読み取ることができなくなるため二次元コード１３４の改ざんによる文書偽造がいっそう難しくなる。また、発行情報は文書ＩＤと発行日時に限らず、さまざまな情報を含んでもよい。たとえば、公文書１３０の発行を要求したユーザのユーザＩＤ、公文書１３０を発行した文書生成装置１００の装置ＩＤなどが発行情報の一部に含まれてもよい。

[0154] ファイルサーバ１０４は、多数のユーザのユーザ端末３００に個人情報をダウンロードさせる。ファイルサーバ１０４は、ユーザ端末３００にダウンロードされた個人情報をローカルストレージから削除してもよい。たとえば、ファイルサーバ１０４ａからユーザＰＸにより個人情報（ＰＸ）がダウンロードされたときには、ファイルサーバ１０４ａのデータ管理部（図示せず）は個人情報（ＰＸ）を一定期間の経過後にローカルストレージから削除してもよい。このような制御方法によれば、ファイルサーバ１０４からユーザ端末３００へのデータの移行が少しずつ促進される。ユーザによるダウンロードが進むほど、ファイルサーバ１０４が管理すべきデータが減っていく。このため、ファイルサーバ１０４からユーザ端末３００に個人情報をダウン

ロードしたあとは、ユーザはファイルサーバ１０４からの個人情報の漏洩を心配する必要がなくなる。

[0155] 本実施形態においては、任意データが入力されなかったときには、文書生成装置１００はその任意データを含まない公文書１３０を生成するとして説明した。変形例として、任意データが受信されなかったときには、検査部１２２は不足タグとして任意タグを通知してもよい。ユーザは、通知を受けたあと、ユーザ端末３００または中継端末４００において任意データを入力する。ユーザが任意データを入力したときには文書生成装置１００は任意データを含む公文書１３０を生成する。一方、ユーザが任意データの入力を拒否したときには文書生成装置１００は任意データを含まない公文書１３０を生成してもよい。

[0156] ユーザバッジ３５０に第２フィルタ３３０を登録するとして説明したが、中継端末４００はユーザバッジ３５０から第２フィルタ３３０を読み出してもよい。すなわち、中継端末４００は第１フィルタ１６０および第２フィルタ３３０を取得し、検査部４３２は第１フィルタ１６０および第２フィルタ３３０の双方に基づいて、ユーザバッジ３５０にある個人情報のうち文書生成装置１００に提供可能な個人情報を選んでもよい。

[0157] 本実施形態においては、ユーザはユーザＩＤとパスワードにより文書生成装置１００にアクセスすることで本人確認をするとして説明した。このほかにもｅＫＹＣ（electronic Know Your Customer）認証により文書生成装置１００はユーザの本人確認を行ってもよい。

請求の範囲

[請求項1] 外部端末から、タグを付与されたデータを受信する受信部と、

所定形式の文書に必要なタグを示す第１フィルタを参照し、前記受信されたデータに付与されるタグが前記第１フィルタに適合するか否かを判定する検査部と、

前記第１フィルタに適合するデータに基づいて文書を生成する文書生成部と、を備える、文書生成装置。

[請求項2] 前記検査部は、前記第１フィルタに適合しないデータをローカルメモリから削除する、請求項１に記載の文書生成装置。

[請求項3] 前記第１フィルタに含まれる複数のタグのうち、一部のタグに対応づけられるデータが不足しているとき、不足しているデータのタグである不足タグを通知する通知部、を更に備え、

前記文書生成部は、前記不足タグに対応するデータが新たに受信されたとき、前記受信されたデータを含めて文書を生成する、請求項１に記載の文書生成装置。

[請求項4] 前記検査部は、受信されたデータに複数のタグが付与されているときには、前記複数のタグのいずれかが前記第１フィルタに含まれるタグと適合するか否かを判定し、

前記文書生成部は、前記複数のタグのいずれかが前記第１フィルタに適合したとき前記受信されたデータを含めて文書を生成する、請求項１に記載の文書生成装置。

[請求項5] 前記外部端末に、前記生成された文書のファイルデータを送信する送信部、を更に備え、

前記文書生成部は、前記外部端末から提供されるデータに基づいて公文書を生成する、請求項１に記載の文書生成装置。

[請求項6] 文書の真正性を確認する証明部、を更に備え、

前記文書生成部は、文書生成時に文書ＩＤおよび発行日時を文書に付与するとともに、文書ＩＤおよび発行日時を対応づけて発行履歴情

報として登録し、

前記証明部は、前記外部端末から文書ＩＤおよび発行日時を含む確認要求がなされたときには、前記確認要求に含まれる文書ＩＤおよび発行日時が前記発行履歴情報に登録されているとき、前記外部端末に対して文書が真正であることを通知する、請求項１に記載の文書生成装置。

[請求項7] 請求項３に記載の文書生成装置と接続され、

データとタグを対応づけて格納するデータ格納部と、

ユーザからの入力にしたがって、外部に送信可能なデータのタグを示す第２フィルタを設定するフィルタ設定部と、

前記第２フィルタを参照し、前記第２フィルタに含まれるタグを付与されたデータを選んで前記文書生成装置に送信する送信部と、を備え、

前記送信部は、前記文書生成装置から不足タグを通知されたあとに前記不足タグが前記第２フィルタに再設定されたとき、前記不足タグに対応するデータを前記文書生成装置に送信する、通信端末。

[請求項8] データの入力を受け付ける入力部と、

前記データ格納部のデータおよびタグを管理するデータ管理部と、を更に備え、

前記送信部は、前記文書生成装置からの不足タグの通知に対応して新たにデータが入力されたときには、前記入力されたデータに前記不足タグを付与して前記文書生成装置に送信し、

前記データ管理部は、前記入力されたデータと前記不足タグを対応づけて前記データ格納部に保存する、請求項７に記載の通信端末。

[請求項9] 前記データ管理部は、前記入力されたデータと同一のデータに対して既に第１のタグが付与されているときには、前記データに対して更に前記不足タグを第２のタグとして追加で対応づける、請求項８に記載の通信端末。

[請求項10] 複数のサーバそれぞれからタグを付与されたデータを受信する受信部と、

前記受信されたデータとタグを対応づけて、内蔵記憶装置に保存するデータ管理部と、を備え、

前記データ管理部は、第１のサーバから第１のタグを付与された第１のデータを受信し、かつ、第２のサーバから第２のタグを付与された第１のデータを受信したときには、前記第１のデータに対して前記第１のタグおよび前記第２のタグを対応づけて保存する、通信端末。

[請求項11] ユーザからの入力にしたがって、外部に送信可能なデータのタグを示す第２フィルタを設定するフィルタ設定部と、

前記第２フィルタを参照し、前記第２フィルタに含まれるタグを付与されたデータを選んで外部装置に送信する送信部と、を更に備え、

前記送信部は、前記第１のデータに対応づけられる前記第１のタグまたは前記第２のタグのいずれかが前記第２フィルタにおいて設定されているとき、前記第１のデータを送信対象とする、請求項１０に記載の通信端末。

[請求項12] 請求項３に記載の文書生成装置と接続され、

ユーザからデータの入力を受け付ける入力部と、

前記文書生成装置から前記第１のフィルタを受信する受信部と、

ユーザが保有する情報担体から、タグを付与されたデータを読み取るデータ取得部と、

前記読み取られたデータに付与されるタグが前記第１フィルタに適合するか否かを判定する検査部と、

前記読み取られたデータのうち、前記第１フィルタに適合するデータを選んで前記文書生成装置に送信する送信部と、を備え、

前記送信部は、前記文書生成装置から不足タグを通知されたあとに前記不足タグに対応するデータが入力されたとき、更に、前記不足タグに対応するデータを前記文書生成装置に追加送信する、中継端末。

[請求項13] 前記情報担体にデータを書き込むデータ登録部、を更に備え、

前記データ登録部は、前記不足タグに対応してデータが入力されたとき、前記入力されたデータを前記不足タグとともに前記情報担体に書き込む、請求項１２に記載の中継端末。

[請求項14] 前記情報担体には、外部に出力可能なデータのタグを示す第２フィルタがあらかじめ登録されており、

ユーザからの入力にしたがって前記情報担体の前記第２フィルタを設定変更するフィルタ設定部、を更に備える請求項１２に記載の中継端末。

[請求項15] 通信端末と文書生成装置を含み、

前記通信端末は、

データとタグを対応づけて格納するデータ格納部と、

ユーザからの入力にしたがって、外部に送信可能なデータのタグを示す第２フィルタを設定するフィルタ設定部と、

前記第２フィルタを参照し、前記文書生成装置にアクセスしたとき前記第２フィルタに含まれるタグを付与されたデータを選んで前記文書生成装置に送信する送信部と、を備え、

前記文書生成装置は、

前記通信端末から、タグを付与されたデータを受信する受信部と、

所定形式の文書に必要なタグを示す第１フィルタを参照し、前記受信されたデータに付与されるタグが前記第１フィルタに適合するか否かを判定する検査部と、

前記第１フィルタに適合するデータに基づいて文書を生成する文書生成部と、

前記第１フィルタに含まれる複数のタグのうち、一部のタグに対応づけられるデータが不足しているとき、不足タグを通知する通知部と、を備え、

前記通信端末の前記送信部は、前記文書生成装置から不足タグを通

知されたあとに前記不足タグが前記第２フィルタに再設定されたとき、前記不足タグに対応するデータを前記文書生成装置に送信し、

前記文書生成装置の前記文書生成部は、前記不足タグに対応するデータが受信されたとき、前記受信されたデータを含めて文書を生成する、文書生成システム。

[請求項16] 外部端末から、タグを付与されたデータを受信する機能と、

所定形式の文書に必要なタグを示す第１フィルタを参照し、前記受信されたデータに付与されるタグが前記第１フィルタに適合するか否かを判定する機能と、

前記第１フィルタに適合するデータに基づいて文書を生成する機能と、をコンピュータに発揮させるプログラム。

[請求項17] データとタグを対応づけて格納する機能と、

ユーザからの入力にしたがって、外部に送信可能なデータのタグを示す第２フィルタを設定する機能と、

前記第２フィルタを参照し、前記第２フィルタに含まれるタグを付与されたデータを選んで文書生成装置に送信する機能と、

前記文書生成装置から不足タグを通知されたあとに前記不足タグが前記第２フィルタに再設定されたとき、前記不足タグに対応するデータを前記文書生成装置に送信する機能と、をコンピュータに発揮させるプログラム。

[請求項18] 複数のサーバそれぞれからタグを付与されたデータを受信する機能と、

前記受信されたデータとタグを対応づけて、内蔵記憶装置に保存する機能と、

第１のサーバから第１のタグを付与された第１のデータを受信し、かつ、第２のサーバから第２のタグを付与された第１のデータを受信したときには、前記第１のデータに対して前記第１のタグおよび前記第２のタグを対応づけて保存する機能と、をコンピュータに発揮させ

るプログラム。

[請求項19] ユーザからデータの入力を受け付ける機能と、

文書生成装置から第１のフィルタを受信する機能と、

ユーザが保有する情報担体から、タグを付与されたデータを読み取る機能と、

前記読み取られたデータに付与されるタグが前記第１フィルタに適合するか否かを判定する機能と、

前記読み取られたデータのうち、前記第１フィルタに適合するデータを選んで前記文書生成装置に送信する機能と、

前記文書生成装置から不足タグを通知されたあとに前記不足タグに対応するデータが入力されたとき、更に、前記不足タグに対応するデータを前記文書生成装置に追加送信する機能と、をコンピュータに発揮させるプログラム。