(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6100781号
(P6100781)
(45)発行日　平成29年3月22日(2017.3.22)　(24)登録日　平成29年3月3日(2017.3.3)

(51)Int.Cl.　F I
G06Q 50/10 (2012.01)　G06Q 50/10

請求項の数 6　(全 12 頁)

(21)出願番号	特願2014-527649 (P2014-527649)
(86)(22)出願日	平成24年8月30日 (2012.8.30)
(65)公表番号	特表2014-531069 (P2014-531069A)
(43)公表日	平成26年11月20日 (2014.11.20)
(86)国際出願番号	PCT/EP2012/066837
(87)国際公開番号	WO2013/030260
(87)国際公開日	平成25年3月7日 (2013.3.7)
審査請求日	平成27年6月26日 (2015.6.26)
(31)優先権主張番号	61/530,416
(32)優先日	平成23年9月2日 (2011.9.2)
(33)優先権主張国	米国(US)
(31)優先権主張番号	11191213.5
(32)優先日	平成23年11月29日 (2011.11.29)
(33)優先権主張国	欧州特許庁(EP)

(73)特許権者　504344495
ナグラビジョン　エス　アー
スイス　ＣＨ－１０３３　シュゾー－シュール－ローザンヌ，ルート　ドゥ　ジュネーヴ　２２－２４
(74)代理人　100085372
弁理士　須田　正義
(72)発明者　ニコラ，クリストフ
スイス　ＣＨ－１１６２　サン－プレクス，シェマン　ドゥ　ス－ザレン　１５

審査官　木方　庸輔

最終頁に続く

(54)【発明の名称】ユーザの個人データへのアクセスを制御する方法

(57)【特許請求の範囲】
【請求項１】
信頼できるセンター（ＴＣ）により、ユーザ（ＵＴ１，ＵＴ２）の個人データへのアクセスを制御する方法であって、
前記信頼できるセンター（ＴＣ）は、少なくとも１つのデータベース（ＴＤＢ）を有し、特定のあるユーザ用に、個人データと、前記個人データに関連するアクセス条件とのための記憶場所を有し、前記方法は、
・ユーザが、その個人データを前記信頼できるセンター（ＴＣ）の前記データベース（ＴＤＢ）中に読み込ませ、かつ前記個人データにアクセス条件を割り当てる工程であって、前記個人データは、２つの異なるアクセス条件を有する少なくとも２つのカテゴリーに分けられ、各カテゴリーはユーザ値に関連付けられる、工程と、
・第三者（ＴＰＷＳ）が、前記信頼できるセンター（ＴＣ）に、複数のユーザ（ＵＴ）の前記個人データへのアクセスを要求する工程であって、前記要求は検索基準を有する、工程と、
・前記検索基準に合う第１ユーザセットを決定するために、前記信頼できるセンター（ＴＣ）が、前記複数のユーザの前記個人データに関する前記検索基準を実行する工程とを含み、
前記データベース（ＴＤＢ）が、少なくとも１つのカウンターを有する管理データを更に有し、
・前記検索基準に合う前記第１ユーザセットの量を示す情報と、前記第１ユーザセットの

各ユーザの前記ユーザ値の合計を前記第三者（ＴＰＷＳ）に戻す工程と、
・前記第三者（ＴＰＷＳ）が、前記合計の全て又は一部分を承認する工程であって、これにより、前記第１セットの全て又は一部分を含みうる第２ユーザセットを定義する工程と、
・前記合計が抽出されたユーザの累積値を網羅する前記第２ユーザセットの前記個人データを戻す工程と、
・前記第２ユーザセットの前記カウンターを、彼らの各個人データの値の内容で更新する工程と
を更に含むことを特徴とする方法。
【請求項２】
前記検索基準に合う前記第１ユーザセットの量を示す前記情報を前記第三者（ＴＰＷＳ）に戻す工程が、
・同じユーザ値を有する前記第１ユーザセットの全てのユーザをグループ化する工程と、
・前記第三者（ＴＰＷＳ）に、グループ毎のユーザの量を送信する工程と
を含む請求項１記載の方法。
【請求項３】
信頼できるセンター（ＴＣ）により、ユーザの個人データへのアクセスを制御する方法であって、
前記信頼できるセンターは、少なくとも１つのデータベース（ＴＤＢ）を有し、特定のあるユーザ（ＵＴ）用に、個人データと、前記個人データに関連するアクセス条件とのための記憶場所を有し、前記方法は、
・ユーザが、その個人データを前記信頼できるセンター（ＴＣ）の前記データベース（ＴＤＢ）中に読み込ませ、かつ前記個人データにアクセス条件を割り当てる工程を含み、
前記データベース（ＴＤＢ）が、少なくとも１つのカウンターを有する管理データを更に有し、前記個人データは、２つの異なるアクセス条件を有する少なくとも２つのカテゴリーに分けられ、各カテゴリーはユーザ値に関連付けられ、本方法は、
・第三者（ＴＰＷＳ）が、前記信頼できるセンター（ＴＣ）に、複数のユーザの前記個人データへのアクセスを要求する工程であって、前記要求は検索基準及び第三者の値を有する、工程と、
・前記ユーザ値が前記第三者の値以下であるとの前記検索基準に合う第１ユーザセットを決定するために、前記信頼できるセンター（ＴＣ）が、前記複数のユーザの前記個人データに関する前記検索基準を実行する工程と、
・前記第１ユーザセットの前記個人データを戻す工程と、
・前記第１ユーザセットの前記カウンターを、彼らの各個人データの値の内容で更新する工程と
を更に含むことを特徴とする方法。
【請求項４】
前記第三者（ＴＰＷＳ）は、その要求と共に限界値を送信し、第２ユーザセットは、前記第２ユーザセットの各ユーザのユーザ値の合計が前記限界値を上回らないように、前記第１ユーザセットから選択される請求項３記載の方法。
【請求項５】
前記第三者（ＴＰＷＳ）の要求は、フィルタリングデータを有し、前記個人データを送信する工程は、前記第三者（ＴＰＷＳ）のウェブサイトに前記個人データを送信する工程の前に、前記フィルタリングデータに応じて前記個人データをフィルタリングする工程を含む
請求項１～４のいずれか１項に記載の方法。
【請求項６】
・少なくとも個人データのいくつかを検証する工程と、
・前記個人データの検証が成功した場合に、異なるユーザ値を割り当てる工程と
を含む

請求項１～５のいずれか１項に記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
通信網の発達に伴い、これらの通信網のユーザは、ますます、個人データをサービスプロバイダへ引き渡すよう求められ、この種の個人データがデータベースに供給される。
【０００２】
コンピュータ環境の重要性及び性能が向上するに従って、平均的なユーザは、そのプライバシーの必要性をあまり気にかけようとしない劣悪な品質のコンピュータエンジンにますますイライラさせられている。
【背景技術】
【０００３】
個人の日常生活の一部である様々な接続システムに対して個人が与える個人データに対して高い評価を行う第三者もある。このような第三者が行いうる利用は、市場調査から、目標を定めた宣伝、データマイニングなどに渡っている。
【０００４】
現在までに、
１）ユーザがその個人データを完全に制御し続けることができる、
２）この種のデータを引き渡す不釣り合いなリスクを採ることはないと、ユーザを説得する、
３）さらに可能な工程として、ユーザの信頼のおかげで投稿された個人データを、前記ユーザにとって直接的な利益となるように、公式に貨幣化する
ような枠組み又は構造は存在していない。
【０００５】
データベースの品質は、個人の不信感により悪影響を受けうる。例えば、国勢調査の場合には、自由思想を持つユーザが、このようなデータを提供するように彼らに要求している政府機関を信用していないという理由だけで、偽のデータを提供することにより反体制的行動をとることがある。
【０００６】
提供されたデータが明らかに射程範囲外のデータであれば、この結果フローを削除することは比較的容易で自動的に行うことができる。これは、例えば、単に、１人のユーザが提供した回答同士を単に照合することにより行うことができる。しかし、この自由思想を持つ人がより洗練されていて、自動的な照合を出し抜く方法を知っている場合には、真実のデータを得るために、かつ、集められたデータベースの良い品質の結果を得るためにできうることはほとんどない。
【０００７】
従って、ユーザが、自身のデータに関して完全にかつ継続的に制御することができ、平均的な個人の信頼を得るように設計されていて、この種の個人が心を開いて、この種のシステムの信頼できるユーザになるように促すシステムの必要性が存在する。
【０００８】
この問題は、特に若者の間でのソーシャルネットワークの人気の高まりにより、深刻な問題になっている。多くのこのようなソーシャルネットワークの管理者は、これらの若者に経験がないことによるいずれの将来の不利益、対、この種のソーシャルネットワークの訪問者が陥る可能性がある理解力の問題についてほとんど考慮しない傾向にある。
【０００９】
例えば、不用心なある若者が、考え直せば又は数年後にはアクセスを限定したいと考えるような映像を、ソーシャルネットワークがホスティングする個人的な保管部に投稿することがありえる。このような画像は、例えば、個人的なパーティ（このパーティで、アル

コールや、より一般的に言えば意識状態を変えるような物質を摂取又は吸入していた）で撮ったビデオや写真でありえる。

【００１０】

前記不用心な若者が卒業して、求職する際に、ソーシャルネットワークが無制限な又は十分に制限されていない視聴者にアクセスを許していたという事実が、上述の映像により描写されるような前記生き様への手がかりとなり、所望の仕事を見つける上での不利益となりうる。

【００１１】

前記若者が政治活動を志す場合、反動はより厳しくなりえ、若い人としての過去の生活の証拠が、マスコミにより、広く公衆とりわけあまり寛容ではない年配の公衆に示され、その人がすでに成長していて、若者であったころの過去の挙動について後悔していたとしても、この当該人物の信頼性を低めてしまいうる。手が届かないデータベースに、若者の投稿の抜粋を継続的に保存しておくことは、従って、彼らの職業上の未来又は政治的な未来にとって非常に有害となりうる。

【００１２】

ソーシャルネットワークの管理者は、データの所有権の問題を知ると、所定のソーシャルネットワークの個人の会員に適用する法的条項を変更して、彼らの組織を時々過剰に守る傾向があるという事実により、この問題はより深刻となる。

【００１３】

このような場合、この種の個人の会員の利益を考慮することはないので、前記利益を非常に損なう結果となりうる。例えば、法的な条件は、個人の個人的な保管部に投稿されたいずれの及び全てのデータの所有権を主張して、事前通知なく変えられる。

【００１４】

この種の法的条項の変更についての情報が加入者に伝えられるとしても、多数の若いユーザはこれに反応することなく、従って暗黙のうちにこの種の変更を受け入れる可能性が高い。そして、これに反応して、自分の不利益になるデータの削除を要求する人がいる場合さえも、彼らは、前記ソーシャルネットワーク相手にコスト高となる訴訟になる見込みに直面し、成功については不確実である。このような訴訟での個人に対するコストを、被告としてのソーシャルネットワークに対してしばしば不釣り合いに与えられる資源と比べると、そもそもこの個人がこの種の訴訟を始めることを阻む可能性があり、この個人の側にストレスが生じる。

【００１５】

個人がその信頼性、個人的な生活又は職業上の将来を低められ、傷つけられ又は妥協させられた件数は上昇し、マスコミがこのような案件を取り上げる件数も増え、その結果、公衆が知ることになる件数も上昇する。

【００１６】

このような件数が急上昇するに従って、上述の事実の結果、ソーシャルネットワークに対する反逆が広く公衆においてますます増えている。しかし、ソーシャルネットワークは、若い公衆の間では流行していて、勢いがある。これにより、将来の社会生活のために彼らが受ける危険性を必ずしも自覚しない野心的な人物にとって、ソーシャルネットワークは不可避となる。

【発明の概要】

【００１７】

提案するのは、信頼できるセンター（ＴＣ）により、ユーザ（ＵＴ１，ＵＴ２）の個人データへのアクセスを制御する方法であって、信頼できるセンター（ＴＣ）は、少なくとも１つのデータベース（ＴＤＢ）を有し、特定のあるユーザ用に、個人データと、個人データに関連するアクセス条件とのための記憶場所を有し、この方法は、

・ユーザが、その個人データを信頼できるセンター（ＴＣ）のデータベース（ＴＤＢ）中に読み込ませ、かつ前記個人データにアクセス条件を割り当てる工程であって、前記個人データは、２つの異なるアクセス条件を有する少なくとも２つのカテゴリーに分けられ、

各カテゴリーはユーザ値に関連付けられる、工程と、
・第三者（ＴＰＷＳ）が、信頼できるセンター（ＴＣ）に、複数のユーザ（ＵＴ）の個人データへのアクセスを要求する工程であって、前記要求は検索基準を有する工程と、
・検索基準に合う第１ユーザセットを決定するために、信頼できるセンター（ＴＣ）が、複数のユーザの個人データに関する検索基準を実行する工程とを含み、
前記データベース（ＴＤＢ）が、少なくとも１つのカウンターを有する管理データを更に有し、
・検索基準に合う第１ユーザセットの量を示す情報と、第１セットの各ユーザのユーザ値の合計を第三者（ＴＰＷＳ）に戻す工程と、
・第三者が、合計の全て又は一部分を承認する工程であって、これにより、第１セットの全て又は一部分を含みうる第２ユーザセットを定義する工程と、
・合計が抽出されたユーザの累積値を網羅する第２ユーザセットの個人データを戻す工程と、
・第２ユーザセットのカウンターを、彼らの各個人データの値の内容で更新する工程と
を更に含む。

【図面の簡単な説明】
【００１８】
本発明は、添付の図面により、より理解されるであろう。
【図１】インターネットに接続された信頼できるセンターを備えたシステムを示す図である。
【図２】信頼できるセンターがプロキシの役割を果たしているシステムを示す図である。
【発明を実施するための形態】
【００１９】
本発明の本質は、一般公衆の少なくとも一部分に開かれていて、信頼できるセンターＴＣへの加入システムにある。このシステムでは、定義されたシステム特徴により、加入会員の個人データがこのシステムに供給されると、加入会員は完全にその個人データを制御し続けることができると促される。従って、加入会員は、信頼できるセンターに真実のデータを提供するように促される。
【００２０】
このように定義された信頼できるセンターＴＣの特徴の本質は、前記提供されたデータの処理における品質の最低限の基準にありうる。例えば、既存のシステムは、あるインターネットユーザが、イタリアのホテルのサイトを閲覧しているという事実を突き止めて、即座にそのユーザにディスカウント価格の旅行を提案することができる。この種の提案は、押し付けがましく、望まれない宣伝であると認識されうる。品質の最低限の基準の本質とは、各個人のユーザについて、どの程度までこの種の自動的な提案を生成し表示しうるのかについて定義することでありえる。
【００２１】
別の定義されたシステム特徴の本質は、個人のユーザのデータの履歴を正真正銘にかつ信頼性をもって消去することができる可能性を提供することにもある。
【００２２】
本発明の特別なある実施形態では、あるシステム特徴は、加入するユーザに対して完全な透明性を提供するように設計されている。
【００２３】
本発明の特別なある実施形態では、システムは、加入するユーザに対して、このユーザがシステムに供給するデータのタイプについて、異なるレベルの制御を提供する。
【００２４】
第１の例として、制御のレベルの第１カテゴリーが、ユーザのスポーツの好みに割り当てられている。この種の好みに関するデータの本質は、スポーツにおけるユーザの個人的

な評価にありうる。例えば、あるユーザＡは、フットボールよりもバスケットボールが好きで、テニスよりもフットボールが好きで、ウィンドサーフィンよりもテニスが好きであるとシステムに知らせうる。このような好みのデータの本質は、ある所定のスポーツにおける競合する様々なチームに関する個人的な評価にもありうる。別の例として、あるユーザＢは、あるレベルの所有権と制御とで、あるバスケットボールチームよりも、別のバスケットボールチームの方が好きであるという情報を開示しうる。

【００２５】

第２の例として、制御の第２カテゴリー又はレベルが、ユーザの趣味に割り当てられている。

【００２６】

第３の例として、制御の第２レベルが、ユーザの政治的な指向に割り当てられている。従って、政治的な指向に関するデータは、ユーザにより、スポーツの好み又は趣味よりもより繊細であるとして考えられることがありえ、外部の非ユーザのアクセスに対して、より制限的な保護レベルが許可されうる。

【００２７】

第４の例として、制御の第３レベルが、ユーザの性的な好み、指向又は趣味に割り当てられている。

【００２８】

更なる例として、ある制御レベルが、ユーザの投資家としてのプロファイルの特徴に割り当てられている。この種の特徴は、金銭的な保守性、リスク許容度、代替スキームへの投資の傾向、投資の選択におけるフェアトレードを好む傾向、自然保護を好む傾向などでありえる。

【００２９】

本発明のある特別な実施形態によれば、システムは、上述のように異なるタイプのデータに関して異なる制御レベルを提供する。

【００３０】

この制御は、様々な方法で行われうる。即ち、

ａ）直接的に、明確な選択により、

ｂ）間接的に、例えばアクセスルールを定義することにより、

ｃ）プロキシにより、即ち、信頼できる第三者に制御レベルを外注することにより、

行われうる。

【００３１】

各カテゴリーについて、ユーザは、前記カテゴリーのこの情報の値を表すユーザ値を定義することができる。この値を書き込む様々な方法が適用可能である。

・ユーザは、自由にこの値を定義することができる。

・システムが予め定義された値を提案し、ユーザが１つを選択する。

・値は、システムにより自動的に追加され、ユーザは単にこれを承認する。

【００３２】

ユーザが個人データのある特定のカテゴリーを共有しないと決めうる点が留意に値する。

【００３３】

実際、あるカテゴリーが第三者の検索基準に合う場合、第三者に送り返されるのはそのカテゴリーではなく、ユーザ識別である。所定のカテゴリーについて、例えばスポーツについて、ユーザは、識別のいずれの部分が送られるかを決めることもできる。ユーザは、電子メールアドレス、名前、所在地、ツイッターアカウント又はフェースブックアカウント、即ち、第三者がサービス又は品物を前記ユーザに提案することができるのに使用可能な情報を選択することができる。

【００３４】

上述の方法は、より抽象的なレベルで、かつ匿名的に使用可能である。第三者は、ある特定の検索基準のヒット数のみに興味があることもありうる。例えば、ある会社は、特定

の場所でスポーツ店を開店する前に、この将来の店の近隣の地理的領域にいるスポーツ関連の常連客になる人の数に関する情報を得るために、信頼できるセンターに要求することができる。この場合、信頼できるセンターは、ユーザの識別を送り返すことはない。

【００３５】

この場合、個人データの各カテゴリーは、実際２つのユーザ値を持つことができ、１つは、ユーザの識別にアクセスするための値で、もう１つは単にこの匿名の検索に参加するための値である。

【００３６】

この検索の結果は、多数のヒットを与えうる。これが、本方法が最適化特徴を提案する理由である。この場合、ユーザ値は様々な内容を有しうるが、即ち、あるユーザについては０．１セントのユーザ値、そして別のユーザについて０．２セントのユーザ値であり、信頼できるセンターは、同じ金額を有するユーザをグループ化することにより、第三者に送信されるデータを編成する。信頼できるセンターは、情報を金額で表し、例えば、（検索基準を満たすユーザのうちで）１２００人のユーザを０．１セントで、かつ、２３００人のユーザを０．２セントで提示する。その後、第三者は、さらなる検索基準を追加して検索を洗練することを決め、かつ信頼できるセンターに要求を返す、又は、第１ユーザセットとして提案された取引を受け入れることができる。

【００３７】

第三者から送られる検索基準中、後者は限界値を含みうる。この値は、信頼できるセンターから第三者に何個のヒットが戻されるかを定義している。この限界値は、この限界値が到達するまでに生じるユーザ値に相当する。

【００３８】

個人データが正確な場合、その個人データに対する興味がより高いことは周知である。これが、信頼できるセンターがユーザの助けを借りて又はこれを借りずに、個人データの様々な検証を行うことができる理由である。ユーザは、そのデータの正当性が立証されることに興味を持つことができ、これにより、各カテゴリーに対してより高い価値を認めることができる。検証は、年齢、性、住所及びこれ以外の個人データに焦点を合わせている。好みの色や休暇の行き先などについて検証するのはより難しい。

【００３９】

ユーザプロファイルが信頼できるセンターにより検証されると、この信頼できるセンターは、ユーザ値を上げることができる。第三者は、検索基準中に、正当性が立証された（かつ通常より多く支払う）ユーザ又は全てのユーザへアクセスする可能性を含ませることができる。

【００４０】

図２中、実施形態は、信頼できるセンターＴＣがプロキシの役割を果たす場合を図示している。様々なユーザＵＴ１・ＵＴ２は、まず信頼できるセンターＴＣに接続し、このセンターから、第三者のウェブサイトＴＰＷＳ１・ＴＰＷＳ２にアクセスする。この場合、ユーザがまず信頼できるセンターＴＣを通じて第三者ウェブサイトＴＰＷＳに接続する。この際に、ＴＣの機能は透明であり、ユーザの識別及び認証は、より後の段階で行われる。

【００４１】

別の実施形態では、プロキシは、ＴＰＷＳにアクセスする前に、ユーザを認証する。

【００４２】

その後、ＴＰＷＳはユーザの識別を要求し、この要求はＴＣに渡される。ＴＣはユーザの個人データの（全体及び一部）がこのＴＰＷＳにとってアクセス可能であるか否かをチェック可能である。アクセス可能の場合は、個人データはＴＰＷＳに送り返される。その上、ユーザは前記ＴＰＷＳの固有の識別子によって識別可能であり、この識別子はユーザがこのＴＰＷＳに接続する際に常に同じであるが、前記ＴＰＷＳには固有である。

【００４３】

本発明のある特別な実施形態では、システムは、データに適用される様々な暗号化特徴

を介して、データの様々な制御レベルを提供する。

【００４４】

本発明を実行する第１の方法によれば、ユーザは、このユーザの端末ＵＴを介して信頼できるセンターＴＣに接続し、ユーザと信頼できるセンターとの間の安全な通信のおかげで、そのユーザの個人データを読み込ませる。

【００４５】

上述のように、個人データは、カテゴリーに分けられ、各カテゴリーは特別なアクセス権に割り当てられる。このアクセス権中では、いくつかのデータが、これらのデータにアクセスすることを許可されている第三者として定義されることも可能である。この第三者のウェブサイトがこのカテゴリーのデータにアクセス可能である場合、この設定は、ユーザが繰り返し見る第三者ウェブサイト（例えば、フェイスブック（Ｆａｃｅｂｏｏｋ（登録商標））、ツイッター（Ｔｗｉｔｔｅｒ（登録商標））、リンクトイン（Ｌｉｎｋｅｄｌｎ（登録商標））のリストの形態でも可能である。個人データは、写真、動画のテキストでもありうる。

【００４６】

これ以外にも、個人データを活用するための規則を定義すること、例えば、個人データが第三者に移転される際の金銭的対価を定義することなどが可能である。個人データの各カテゴリーについて、特定の金額が定義可能である。

【００４７】

第三者のウェブサイトＴＰＷＳは、信頼できるデータベースＴＤＢ中に登録することができる。プロファイルや、活動のタイプ（例えば、スポーツの活動、情報など）についての記述が定義可能である。この第三者は、この第三者が興味を有するユーザのタイプについて（例えば、若い男性又はペットを飼っている人など）定義することができる。

【００４８】

このウェブサービスは、このウェブサービスが興味を持つカテゴリーに合うユーザの個人データにアクセスするための対価を定義することもできる。この対価は、ユーザの全記録に関連づけられるか、あるいは、ユーザのデータカテゴリーによって分けられるかのいずれかである。

【００４９】

第２工程において、ユーザが第三者ウェブサイトＴＰＷＳにアクセスし、自身を識別するように誘われる。第三者ウェブサイトが個人データを得るためには、この第三者ウェブサイトは、信頼できるセンターに対して安全にリンクし始め、ユーザの身元及び第三者ウェブサイトの識別子を送信する。

【００５０】

その後、信頼できるセンターは、このリンクを通じてユーザを認証し、ユーザの認証情報を要求する。これはパスワードの形態でもありえるが、又は、（ワンタイムパスワードを生成する個人的なカードを用いた）ワンタイムパスワードなどを関与させたより安全な操作に基づきえる。ユーザが認証されると、信頼できるセンターは、第三者のウェブサイトの識別子を用いて、個人データへのアクセス条件をチェックする。この検証を考慮して，個人データは第三者のウェブサイトに戻される（又は、戻されない）。

【００５１】

信頼できるセンターへの要求は、フィルタリング情報も含みうる。第三者のウェブサイトは（データの記述子を使って）個人データの一部のみに興味を持つこともありうるし、あるいは、データのサイズのタイプも限定しうる。個人データが５００メガバイトの動画を含む場合、第三者のウェブサイトは要求するデータの最大サイズを特定することも可能である。サイズの代わりに又はサイズに加えて、第三者のウェブサイトは、それが興味を有するデータのタイプ、例えば、好みや、写真などについて特定することもできる。

【００５２】

ユーザを特定するために、第三者は、信頼できるセンターから固有の識別子を受け取りうる。この識別子は、一方ではユーザを識別するが、他方では第三者にとって固有のもの

である。この場合、第三者は、現在そのサービスにアクセスしているユーザの個人データを、ユーザの真の身元を知ることなく受け取る。

【００５３】

認証プロセスの間に、第三者は、興味のあるカテゴリーを追加して、信頼できるセンターに送信することもできる。信頼できるセンターは、その後、今認証されたユーザが、第三者により識別されたカテゴリーに合うかどうかを検証し、これに合う場合、このユーザの個人データが第三者に送信されうる。金銭的対価がユーザにより定義されていて、かつそれがこの第三者により受け入れられた場合には、第三者から提供された振り込みが、ユーザの口座になされる。その後、ユーザのカウンターは１つ値を上げる。

【００５４】

上述したように、信頼できるセンターは、プロキシの役割を果たしうる。この信頼できるセンターのデータベースは、個人データを有し、このプロキシは、まずユーザを識別する。一旦識別すると、信頼できるセンターは、ユーザの端末とウェブサイトとの間の通信を監視しうる。ユーザがなんらかの個人データ（例えば、電話番号）を遮断していた場合で、電話番号が要求されている場合には、信頼できるセンターは、ユーザに警告を与えうる。プロキシモードの場合には、その目標は、ユーザからウェブサイトに送信されるだろう個人データをつかむことである。個人データを要求するサイトを遮断することは困難であるが、知っているデータ（即ち、ユーザが信頼できるセンターに与えたデータ）を遮断することは容易である。このモードの場合、プロキシは、ＤＬＰ（データ消失防止）装置として作用する。

【００５５】

より軽いバージョンでは、小さなソフトウェアアプリケーションをユーザのコンピュータ中に読み込ませ、信頼できるセンター用のユーザの識別を記憶することが可能である。ユーザが、信頼できるセンターでそれ自身がアカウントを持っている第三者のウェブサイトにアクセスすると、ユーザはその個人データへのアクセスを第三者に対して（通常、対価を受けて）権限を与える。この権限を与えるのは、第三者のウェブページにおける信頼できるセンターのロゴをクリックする形態で行われうる。ユーザの匿名性を保つために、第三者はユーザのアプリケーションにこの第三者の識別子（ＩＤＴＰ）を与える。ユーザのアプリケーションは、ユーザの識別子（ＩＤＵ）、非対称の一対の鍵の秘密鍵である個人的な鍵（ＫＵｐｒ）、及び、信頼できるセンターの公開鍵である信頼できるセンターの鍵（ＫＴｐｕ）を保存する。

【００５６】

ユーザのアプリケーションは、２つの暗号を生成する。第１の暗号（ＩＤＵ）$_{KTpu}$は、信頼できるセンターの鍵ＫＴｐｕでユーザの識別子ＩＤＵを暗号化することにより得られ、第２の暗号（ＩＤＴＰ）$_{KuPr}$は、第三者の識別子ＩＤＴＰを個人的な鍵ＫＵｐｒで暗号化することにより得られる。この第２の暗号は、第三者にとって、ユーザがすでにこの第三者を訪れたか否かをチェックすることができるための固有の識別子を表している点に留意されたい。すでに訪れていた場合には、前回の訪問時に収集されたデータ及びこのユーザの可能な個人データを用いて、ウェブの提案の提示を個人向けにすることができる。

【００５７】

第２の暗号が新規の場合には、これは、このユーザがこの第三者に初めて接続することを意味する。この第三者は信頼できるセンターにアクセスして、第１の暗号及び自身の識別を送信することができる。信頼できるセンターはこの第１の暗号を復号化して、どのユーザに関するのかを決定する。信頼できるセンターは、ユーザが送信に権限を与え、対価規則が満たされる場合に、第三者に前記ユーザの個人データを戻すことができる。

【００５８】

個人的な鍵は、非対称の鍵ではなく対称的な秘密鍵でありうる。

【００５９】

本発明のある実施形態によれば、個人データを信頼できるセンターで初期化している間、あるいは、これ以降のある段階において、ユーザは、電子証明書又は非対称の一対の鍵

形式での暗号材料を受け取ることができる。この暗号材料は、ユーザの機器（例えば、ラップトップ、スマートフォンやタブレットなど）に保存される。この材料は、第三者のウェブサイトで実行される認証工程で用いられる。この第三者のウェブサイトが信頼できるセンターとの接続を開始した後に、ユーザと信頼できるセンターとの間で交換されるデータは、暗号材料を用いて暗号化される。その結果、第三者のウェブサイトは、認証方法に干渉することができず、交換されたデータを理解することができない。

【００６０】

別の実施形態によれば、第三者のウェブサイトは、ユーザの個人データを得るための要求を送ることができる。この要求中で、このウェブサイトは、個人データにアクセスするための対価及び検索基準に関する提案を定義することができる。その後、信頼できるセンターは、そのデータベースを検索し尽くし、その検索基準に合うユーザのデータを見つける。あるユーザが見つかれば、このセンターは、これらのデータへのアクセス条件リンクがこれらのデータの送信を許可することを検証する。この検証は、一般的なアクセス条件を考慮することができ、例えば、このカテゴリーが第三者にアクセス可能であるか、あるいは、この第三者がこれらのデータへのアクセスを明らかに許可されているか否かを考慮することができる。

【００６１】

双方の場合で、ユーザは、そのデータにアクセスするための金銭的基準を定義することができ、信頼できるセンターは、ユーザの期待と第三者の提案とを比較する。これらが一致すれば、ユーザの個人データは、第三者に転送され、第三者により提案された対価が与えられる。

【００６２】

本発明のこの特別な実施形態では、このシステムは、ユーザに対して、所定の条件下での、このユーザの個人データのある部分の通信（これは、この種の通信に対してユーザに補償する準備がある第三者に対して行われる）を貨幣化する可能性を提供する。

【００６３】

この種の所定の条件は、上述の制御のレベルの影響下にある個人データを第三者に再販する許可又は許可の拒否を含むことができる。

【００６４】

本発明の方法を実行するために、信頼できるセンターは、処理能力と保存能力と通信手段とを有する。信頼できるセンターは好ましくは、インターネットに接続され、ユーザは、その個人データを投稿することができる。処理能力は、個人データを保護及び編成し、第三者が要求した検索を行うことを担当する。

【図１】

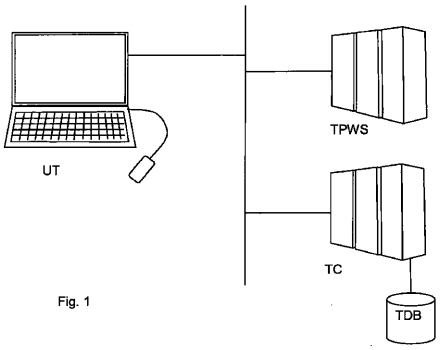

Fig. 1

【図２】

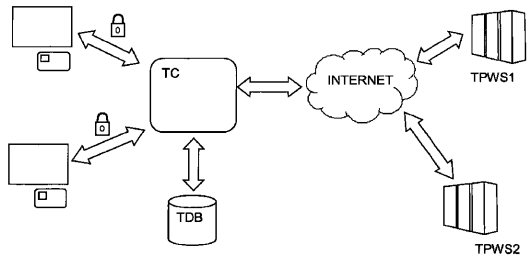

Fig. 2

フロントページの続き

(56)参考文献 特開２００１－２９０９５６（ＪＰ，Ａ）
特開２００５－２０２５７７（ＪＰ，Ａ）
特表２０１３－５１２５２５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ １０／００ － ９９／００