修士論文

サービス提供者による個人の識別を回避する機構の提案

門脇真之佑

主指導教員 知念 賢一

北陸先端科学技術大学院大学
先端科学技術研究科
（情報科学）

令和３年２月

Abstract

インターネットの普及により様々な情報が交換されるようになった。この様々な情報の中には個人情報も含まれている。またインターネットをの利用を前提としたSNSや通販のようなサービスは社会生活に不可欠なものとなっている。個人がサービスを利用する際交換される情報の中には個人情報が含まれていることもある。そのためサービス提供者はこの個人情報をサービスを利用するたびに収集することができる。そして一度収集されてしまった情報は利用者がコントロールできないので、将来においてもサービス提供者の元に残ってしまう可能性が高い。個人情報の収集を防ぐために個人情報とサービスを利用するための取引情報を切り離す方法も考えられるが、多くの情報がサービス提供者の元に収集されてしまうと個人情報が再識別されてしまう。このような問題の解決策として個人情報を匿名加工して匿名加工情報に変換する方法がある。この匿名加工情報とは個人が特定されないように個人情報を加工した情報のことである。匿名加工情報から個人情報を復元することはできない。匿名加工情報から個人を識別することを再識別という。

本研究では個人情報を匿名加工情報情報に変換する匿名加工システムを使って個人が特定されない様にサービスを利用するための機構を提案した。この匿名加工システムには４つの機能がある。１つ目の機能は個人情報の項目に入っているデータを匿名加工情報に変換する。指定されれば匿名加工せずに個人情報をサービスに渡すこともできる。２つ目は１つ目で作られた匿名加工情報のレコードを他のサービス利用者が自由に使用できる機能である。３つ目はサービス利用者の個人情報に基づかない匿名加工情報を増やすことができる機能である。４つ目は匿名加工システムがサービス提供者と関係なくサービスを利用する機能である。これらの機能を使って匿名加工システムは個人サービス提供者と個人情報の関係性を希薄化させる。また匿名加工システムを複数利用することも提案する。複数の匿名加工システムを水平と垂直に重層的に配置することで、一つと場合と比べてサービス提供者と個人情報の関係性を希薄化させる。

上記の匿名加工システムとサービス利用者の中継をする匿名加工ポリシー管理システムも提案する。匿名加工ポリシー管理システムはサービス利用者の個人情報をID管理するものである。このIDとはここでは個人を識別するための番号や記号のことである。ID管理にはセパレートモデル・フラットモデル・セクトラルモデルの３種類がある。本研究ではセクトラルモデルによってID管理することを提案している。またこの匿名加工ポリシー管理システムは各サービスに対してどの個人情報が利用するために必須あるのか記録されている。

使いたいサービスを選択してそのサービスを利用するために必要な情報を、匿名加工ポリシー管理システムと匿名加工システムを通して入力される。またこの匿名加工ポリシー管理システムは利用者と一対一の関係である。匿名加工ポリシー管理システムから匿名加工システムに対しては、個人情報のレコードと選択したサービスと匿名加工の加工方針が渡される。匿名加工システムは匿名加工が可能

である個人情報を匿名加工する。その後、次の匿名加工システムに個人情報のレコード・サービス利用者選択したサービスの情報・サービスで必要とされる個人情報のレコードを渡す。最後尾の匿名加工システムがサービスに個人情報を与える。このように匿名加工ポリシー管理システムと匿名加工システムサービスを組み合わせることで利用者と個人情報の関係を希薄化させる。

　なお匿名加工システムと匿名加工ポリシー管理システムを使ってもサービスを利用する際に必要な個人情報があるという問題が残る。しかしこの問題は決済代行サービスや駅前などに設置されている誰でも利用できる宅配ボックスなどを使用することで回避できる。

目 次

図 目 次

表 目 次

第1章　はじめに

1.1　背景

インターネットの普及により様々な情報が交換されるようになった。この様々な情報の中には個人情報も含まれている。この個人情報には氏名・年齢・住所・連絡先のような電話帳に載るような情報だけではなく、思想信条や趣味嗜好といったような他人には知られたくないようなプライベートな情報も含まれている。またインターネットをの利用を前提としたSNSや通販のようなサービスは、今日では社会インフラとなっており社会生活に不可欠なものとなったいる。

個人がサービスを利用する際交換される情報の中には個人情報が含まれていることもある。そのためサービス提供者はこの個人情報をサービスを利用するされるたびに収集することができる。そして一度収集されてしまった情報はすべて削除させることが難しいので、将来においてもサービス提供者の元に残ってしまう可能性が高い。個人情報を収集されないための対策として個人情報とサービスを利用するための取引情報を切り離す方法も考えられるが、多くの情報がサービス提供者の元に収集されてしまうと個人情報が再識別されてしまう。

サービスを利用している個人と収集されてしまった個人情報の関係性が明白になってしまうと、その情報をもとにダイレクトメールが届くようになったりするだけではなく本人になりすまして買い物をされてしまったり、さらに悪いと犯罪に巻き込まれてしまう危険性もある。

1.2　目的

本研究の目的はサービスを利用しても個人が知られたくない個人情報等の情報をサービス提供者に知らせないようにすることである。そのために個人情報を特定の個人だと特定されないように情報を加工してサービスを利用する。この加工した情報のことを匿名加工情報という。匿名加工は一度だけでなく何度もそれをおこなうことで個人との関係性を希薄日させる。またそのサービスを利用するために必要な個人情報を管理するためのシステムも提案する。

1.3　本論文の構成

本論文の構成は 7 つの章から構成されている。2 章では匿名加工の方法について説明する。3 章では ID の管理モデルに関して説明する。4 章では 2 章で説明した匿名加工を使った匿名加工システムの提案をおこなう。5 章では 3 章で説明した ID 管理モデルを使って匿名加工ポリシー管理システムを提案をおこなう。6 章では 4 章と 5 章で提案したシステムを通販サイトを利用した際にどう作用するのかを考察する。7 章で本研究についてのまとめをおこない、今後の展望についても述べる。

第2章　匿名加工情報

2.1　匿名加工情報ができた背景

通信技術の発達にともない個人情報が多く集まるようになった。そのためビックデータと呼ばれる巨大なデータセットが収集できるようになり、行政や企業などがそれぞれの活動にこのビッグデータを活用するようになっていった。しかしビッグデータには個人情報が含まれるため、プライバシー保護にも配慮しながら活用する方法が必要となっていた。この章では Computer Security Symposium の [1][2][3][4][5] 予稿集を参考にした。

2.2　匿名加工情報

匿名加工情報とは、個人が特定されないように個人情報を加工した情報のことで、この匿名加工情報から個人情報を復元することができないものである。個人情報の分類と匿名加工情報の加工方法に関しては柏市役所の個人情報の取扱項目の具体例 [6] と個人情報保護委員会個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）[7] を参考にした（表 2.1、表 2.2、表 2.3、表 2.4、図 2.1）。

2.3　法律と倫理

2.3.1　匿名加工情報に関する法律

個人情報の保護に関する法律の第 4 条・第 8 条・第 60 条に基づいて個人情報の保護に関する法律についてのガイドラインが個人情報保護委員会より出されておりこれに準じて匿名加工がなされている。また 2.3 では三菱総合研究所の匿名加工情報・個人情報の適正な利活用の在り方に関する動向調査報告書 [8] と野村総合研究所パーソナルデータの適正な利活用の在り方に関する動向調査（平成３０年度）報告書 [9] を参考にした。

表 2.1: 個人情報の分類表 (1)

分類	項目	例示
基本的項目	氏名	氏名、通称名、芸名、旧姓、ペンネーム等
	性別	男・女
	生年月日	生年月日、干支、年齢、年代
	住所	住所、郵便番号、居所、居住区域名、住所歴、転居先、住宅付近図、住所登録日
	国籍・本籍	本籍、本籍所在地、国籍、外国人であることの表示、戸籍編製・除籍年月日
	連絡先	電話番号、FAX番号、メールアドレス、連絡先等
	識別番号	整理番号、受験番号、免許番号、許可番号、被保険者番号、ＩＤ番号等の個人に付されている番号
	個人番号	番号法に基づき付された個人番号
	その他	死亡日時又は場所，顔写真，指紋，声紋，印鑑（印影），市民となった日等の住所以外の居 住に関すること，言語
家庭環境	家族状況	続柄、家族構成、扶養関係、同居・別居の別、父子・母子家庭、世帯主との関係、生い立ち
	親族関係	養子縁組、離縁、認知、血族・姻族関係、相続人の有無（相続人氏名含む）、里親・里子
	婚姻	婚姻の事実・時期、婚姻期間、離婚の事実・時期・理由等、内縁関係
	住居状況	住居の間取り、住居の状況（自家・借家の別、戸建て・マンション・アパートの別、コンクリー ト、木造の別等）、家具等の状況等
	趣味・嗜好	旅行・読書等の趣味、色彩・インテリア等の好み、飲酒・喫煙等
	その他	その他 食生活の内容等衣食住に関すること、家庭生活に係る癖

表 2.2: 個人情報の分類表 (2)

分類	項目	例示
社会生活	職業・職歴	勤務先に係る情報、所属、就職・退職年月日、在職期間、配置転換、解雇・停職等の処分、勤務内容
	学業・学歴	卒業・在学校名、退学・休学・停学等、入学・卒業年度、在学年度、クラブ活動、専攻科目等、学校での生活状況に関すること
	職業上の地位	役職名、職位・職名、昇格・降格
	資格・免許	資格、免許等の有無、種類等、講習会の修了も含む。
	成績・評価	学業成績、勤務成績・評価、各種試験の結果・成績等、叙位叙勲、表彰、反則金、補導歴、違反歴等
	支援措置・保護	支援措置情報、に関する情報（法定後見人等に関することを含む）
	社会活動	各種団体の加入・活動に係る情報、各種行事等への参加状況、団体等における地位
	その他	交友関係、行政指導に関すること、訴訟内容等、冠婚葬祭、選挙権に関すること
経済的事項	収入・支出状況	給与所得・譲渡所得等の金額，年収，月収等，控除内容，支出の種類・内容，奨学金，補 助金，補償金 資産内容
	資産内容	資産内容、不動産・動産の所在・評価額、有価証券の所有状況、債権・債務額、預金の 額、絵画・骨董品・彫刻等の保有状況、住居情報（ただし資産価値に関する情報に限る ）
	課税・納税状況	課税・納税内容、各種税の納税額、負担金の納付状況、滞納状況等、減免状況
	取引状況等	金融機関の口座、取引相手、取引額等、貸付状況
	公的扶助・社会手当	生活保護・各種手当の受給の有無、受給内容等、災害給付金
	その他	破産関係、財産管理人の有無、保険・年金に関すること等

表 2.3: 個人情報の分類表 (3)

分類	項目	例示
心身的事項	健康・身体状況	健康診断結果、血圧、検査名、検査結果、機能回復訓練記録等、妊娠の有無、胎児の状況（母親情報）、身体測定結果、身長、体重、体力測定結果、運動能力、血液型、容姿
	傷病歴	傷病名、傷病の程度・原因、病歴、治療の内容（カルテ）、看護記録等
	障害	障害の有無、障害の種類・部位・程度、補装具の有無等、手帳関係
	介護	介護度、介護サービスの内容、介護認定の有無及び内容、ケースワークの所見
	診断書	診断書、医師の意見書等
	その他	性格、長所・短所、精神的な悩み、身体的な悩み、心身に関する癖、行動、出産関係、死亡 の原因
思想信条等	思想・信条	人格そのものあるいは精神作用の基礎に関わる個人情報（政治に関するものは除く）、 思想、信条、世界観、人生観、倫理観等、主義・主張
	支持政党	人格そのものあるいは精神作用の基礎に関わる個人情報（政治に関するもの）、 支持政党名、所属する政治団体名、政治的信条、政治的理念、政治活動経歴
	宗教	畏敬崇拝する心情あるいは行為に係る個人情報 信仰する宗教・宗派、嫌いな宗教、家の宗教、宗教的慣習、所属する宗教法人名、信仰状況
	犯罪歴等	犯罪の経歴が過去にあったことを示す個人情報 、刑罰に処せられた事実に関する個人情報（過料に関する個人情報は除く） 、少年の保護事件に係る保護処分の執行等に係る個人情報 個人の前科、逮捕歴、勾留歴、犯罪歴、執行猶予、起訴猶予、仮釈放、刑罰の有無 （過料は除く）
	その他	過去において不当な社会的差別の原因となった事実やその取扱いを誤ると不当な差別を助長するおそれのある個人情報 、人種・民族・門地・同和問題に関する情報（地域改善対策特定事業に係る国の財政上の 特別措置に関する法律（昭和６２年法律第２２号）、第２条第１項に規定する対象地域の同和関係者であるという事実に係る個人情報

表 2.4: 匿名加工情報の加工方法

名称	手法
ソート	加工対象となる個人情報データベース等に含まれる個人情報のレコ ードを一定の規則に従い並べ替える
シャッフル	加工対象となる個人情報データベース等に含まれる個人情報のレコ ードの並び順を(確率的に)変える
仮 ID 化	加工対象となる個人情報データベース等に含まれる個人情報におい て ID に該当する項目を仮 ID となる項目に置き換える
項目削除	加工対象となる個人情報データベース等に含まれる個人情報の項目を削除する
レコード削除	加工対象となる個人情報データベース等に含まれる個人情報のレコードを削除する
セル削除	加工対象となる個人情報データベース等に含まれる個人情報の特定のセルを削除する
一般化	加工対象となる情報に含まれる記述等について、上位概念若しくは数値に置き換える
トップ(ボトム)コーディング	加工対象となる個人情報データベース等に含まれる数値に対して、特 に大きい又は小さい数値をまとめる
レコード一部抽出(サンプリング)	加工対象となる個人情報データベース等に含まれる個人情報の一部 のレコードを抽出する
項目一部抽出	加工対象となる個人情報データベース等に含まれる個人情報の項目の一部を重複しない形で抽出する
ミクロアグリゲーション	加工対象となる個人情報データベース等を構成する個人情報をグループ化した後、グループの代表的な記述等に置き換える
丸め(ラウンディング)	加工対象となる個人情報データベース等に含まれる数値に対して、四捨五入などして得られた数値に置き換える
データ交換(スワッピング)	加工対象となる個人情報データベース等を構成する個人情報相互に 含まれる記述等を(確率的に)入れ替える
ノイズ(誤差)付加	一定の(確率)分布に従って発生したランダムな数値等を付加する
擬似データ生成	人工的な合成データを作成し、これを加工対象となる個人情報データ ベース等に含ませる

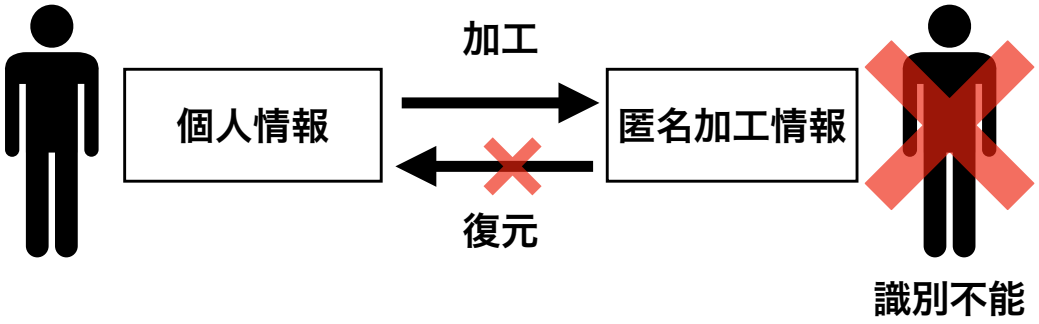

図 2.1: 匿名加工の概念図

2.3.2 匿名加工情報の作成者の義務

匿名加工情報の作成者は以下の全ての項目を義務として負う。また匿名加工情報を取り扱う者は以下の（４）・（５）・（６）の項目を義務として負う。

（１）適正加工義務

匿名加工情報を作成するときは、委員会規則で定める基準に従った匿名加工をする。

（２）加工方法等安全管理措置

匿名加工情報を作成したときは、加工の際に削除した情報や加工方法について、委員会規則で定める基準に従った安全管理措置を講じる。

（３）作成時公表義務

匿名加工情報を作成したときは、委員会規則で定めるところにより、匿名加工情報に含まれる個人に関する情報の項目を公表する。

（４）提供時公表義務

匿名加工情報を作成して第三者提供するときは、委員会規則で定めるところにより、あらかじめ、匿名加工情報に含まれる個人に関する情報の項目と提供の方

法を公表し、受領者に匿名加工情報であることを明示する。

（５）識別行為禁止

匿名加工情報を作成して自ら取り扱う際には、匿名加工情報の作成に用いられた個人情報に係る本人を識別するために、匿名加工情報を他の情報と照合してはならない。

（６）安全管理措置等

匿名加工情報を作成したときは、(a) 安全管理措置、(b) 苦情処理その他の適正な取り扱いを確保するための措置、(c) その内容の公表について、努力義務を負う。

2.3.3　適正加工義務

匿名加工情報の作成者の義務の適正加工義務については具体的には以下のような措置が求められている。

（１）特定の個人を識別することができる記述等の削除。

氏名や住所、生年月日などの個人が識別できる記述等を削除したり、他の記述に置き換える必要がある。

（２）個人識別符号の記述等の削除。

個人識別符号とはDNAや虹彩、声紋などの生態情報をデジタルデータに変換したものや、マイナンバーなどの対象を識別する符号のことで削除したり、他の記述に置き換える必要がある。

（３）情報を相互に連結する符号の削除。

個人情報を分散管理しようとするときに付されているID等で削除したり、他の記述に置き換える必要がある。

（４）特異な記述等の削除。

珍しい事実に関する記述または他の個人と著しく差異がある記述等で削除したり、他の記述に置き換える必要がある。

（５）個人情報とデータベースにある他の個人情報との差を考慮した措置。

（１）から（４）のような匿名加工をしても大量の匿名加工情報が集まると同じ符号を合わせていくことで再識別されてしまうため、このことを考えた処置が必要となる。

2.3.4　個人情報と匿名加工情報

匿名加工情報は個人が特定されないように加工されているため個人情報ではない。そのため個人情報とは異なり第三者提供をする際に同意は必要ない。また目的外の利用をする際にも同意を必要としない。このことが根拠となりビッグデータが市場で取引されるようになっている。

第3章　ID管理モデル

3.1　ID管理モデルが必要である背景

IDとはここでは個人を識別するための番号や記号のことである。このIDを使って日本の行政では社会保障や税など管理をしている。このようなIDがあることのメリットとして、税と社会保障のバランスを適切にしたり、行政に申請をしなくても行政側から国民に必要と思われる提案が届くようになったりしている。また行政側としても事務を効率化することができる。

このIDの管理方法にはフラットモデル・セパレートモデル・セクトラルモデルの３種類がありそれぞれにメリット・デメリットがある。この章では森 亮二 [10][11]、石井 夏生 [12][13] 利、安達和夫 [14]、高崎 晴夫 [15] の論文などを参考にした。

3.2　ID管理モデルの分類

3.2.1　セパレートモデル

行政のサービス別に異なる番号や記号を使用しているモデルである。国民はそれぞれの分野ごとに異なる番号や記号を管理しなくてはならない。また行政間で連携してデータを活用することも難しい。しかし連携できないためにIDが流出してもその影響が限定的である。このような特徴のため国民の利便性の向上や、行政の業務の簡略化が難しい。現在の日本の行政で使われているモデルはこのセパレートモデルである（図 3.1）。

3.2.2　フラットモデル

共通のIDによって各サービスを管理しているモデル。行政間での連携がしやすいため国民が手続きを簡素化しやすい。しかしIDが流出した場合の影響範囲も広い。またIDが流出した場合はすべてのサービスに対してIDをつけ直す必要がある（図 3.2）。

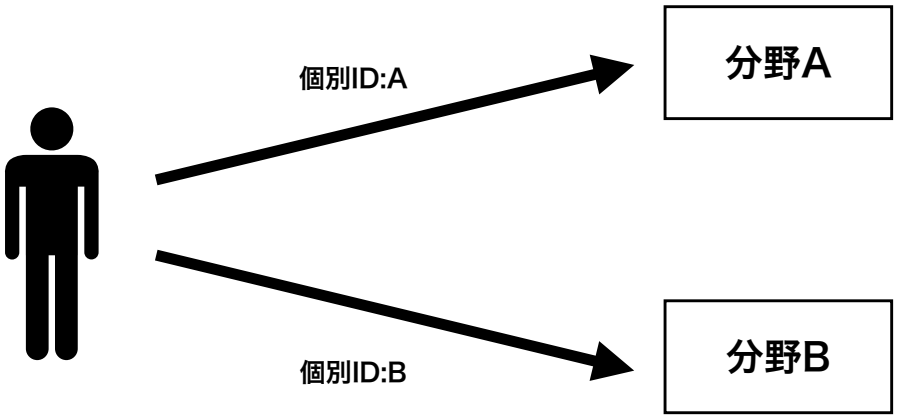

図 3.1: セパレートモデルの概念図

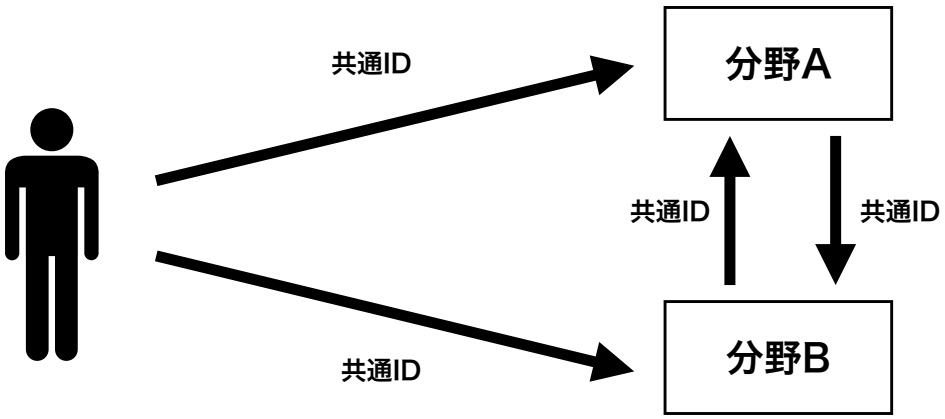

図 3.2: フラットモデルの概念図

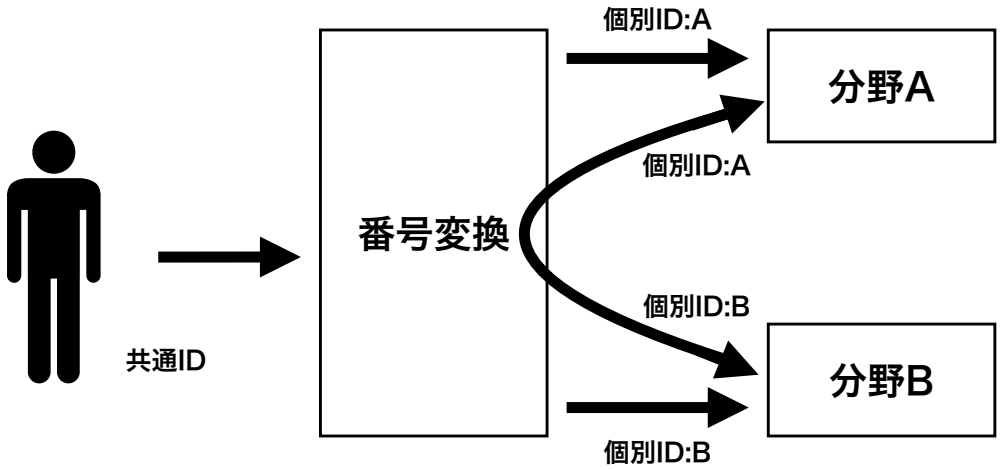

図 3.3: セクトラルモデルの概念図

3.2.3　セクトラルモデル

各サービスではそれぞれ異なる ID により個人情報を管理するが、国民は 1 つの ID でサービスを利用できる。行政間での連携がしやすいため国民が手続きを簡素化しやすい。また行政側で ID が流出してもその影響が限定的である。このセクトラルモデルはセパレートモデルとフラットモデルのメリットを生かしつつデメリットを減らしているモデルである（図 3.3)。

3.3　トラストサービス

コロナ騒動もあり社会の中で行政手続きの IT 化が必須のものとなってきている。しかしそのためには成りすましや改ざんなどをされないように対策する必要がある。行政の IT 化に必要なものとして ID 管理とトラストサービスがある。トラストサービスとはデータの真正性やデータ流通基盤の信頼性を確保する仕組みのことである。具体的には下記の通りである。

（1）電子署名

電子データについて本人が作成したことを証明するもの。

（2）タイムスタンプ

電子データがある時刻に存在しそれが改ざんされていなことを証明するもの。

（3）ｅスタンプ

電子データがある法人によって発行されたことを証明するもの。

（4）ウェブサイト認証

ウェブサイトの管理主体を証明するもの。

（5）ｅデリバリー

送受信者の証明と送受信したデータの完全性を証明するもの。

3.4　ID 管理モデルの課題

ID 管理モデルを導入する際には 2 つ課題がある。1 つ目がプライバシーの問題である。日本でも住基ネットなどを導入しようとした際に反対運動や裁判などが起こりプライバシー侵害への懸念された。また今まで行政が知り得なかった情報を新たに知られる点も問題とされていた。セクトラルモデルやトラストサービスの実現などで対策していく必要がある。

２つ目は ID 管理モデルを導入する際のコストの問題である。導入することで税と社会保障のバランスを適切にしたり、行政に申請をしなくても行政側から国民に必要と思われる提案が届くようになったりするメリットはある。しかしこのメリットを上回る費用が掛かってしまうと導入する意味がなくなる。実際にイギリスでは ID カードスキームを導入しようとした際に費用対効果が認められないとして廃止された

第4章　匿名加工システムの提案

4.1　匿名加工

個人情報の項目に入っているデータを匿名加工し匿名加工情報とすることで、サービス提供者に取られてしまう個人情報を減らすことができる。しかしサービスによっては匿名加工すると利用できないサービスもある。例えば宅配サービスはであれば届けて欲しい住所を入力しなければ届かないし、クレジットカードで支払いがしたければクレジットカード番号やその暗証番号などを入力しなければいけない。このようなデータに関しては図の様に匿名加工されずに個人情報の項目が個人からサービス提供者に提供される必要がある（図 4.1、図 4.2）。

4.2　匿名会加工システム

4.2.1　個人情報の項目の入れ替え

作られた匿名加工情報 A を使って毎回同じ個人 A がサービスを利用すると、サービス提供者に個人情報が収集されてしまい個人が特定されてしまう恐れがある。これを防ぐために最初に匿名加工情報 A を作った時とは異なるサービス利用者 B が利用することでサービス利用者 A と匿名加工情報 A の関係性を希薄化する（図 4.3、図 4.4）。

4.2.2　匿名加工情報の追加

匿名加工情報は最初にサービス利用者の個人情報を元にして生成していた。しかしそれだけではなくサービス利用者がいなくても匿名加工情報を任意に生成して匿名加工システムの匿名加工情報群を増やすことで、サービス提供者に対してサービス利用者と個人情報の関係性を希薄化させる（図 4.5）。

4.2.3　匿名加工情報のダミー

4.2.2 で説明した匿名加工情報はあくまでサービス利用者がこの匿名加工情報を使用してサービスを受けるために使われるものであった。しかし匿名加工情報の

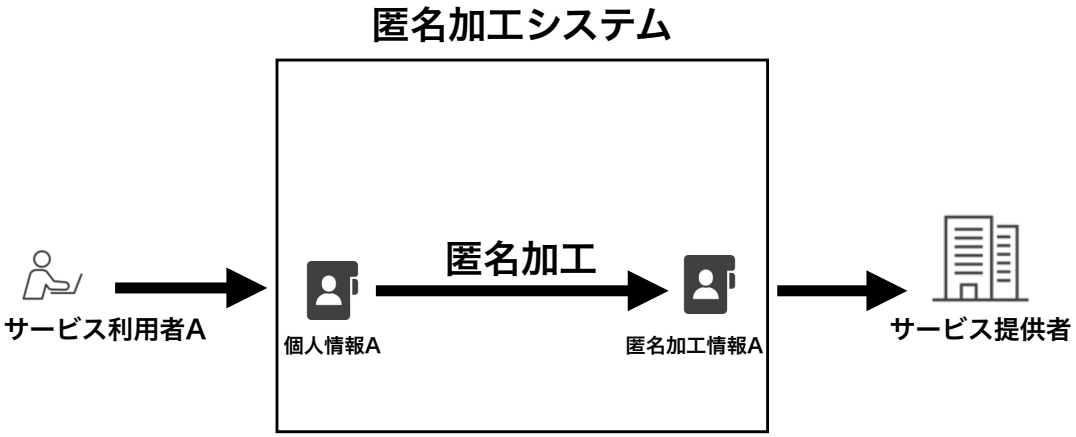

図 4.1: 匿名加工システムの概念図

サービス利用者	名前	住所	電話番号
個人情報A	山田　太郎	Y県N市OO町	×××ー△△△ー□□□□

匿名加工　匿名加工　匿名加工

サービス利用者	名前	住所	電話番号
匿名加工情報A	鈴木　一郎	Y県N市OO町	□□□ー▶▶▶ー××××

図 4.2: 匿名加工の能否の概念図

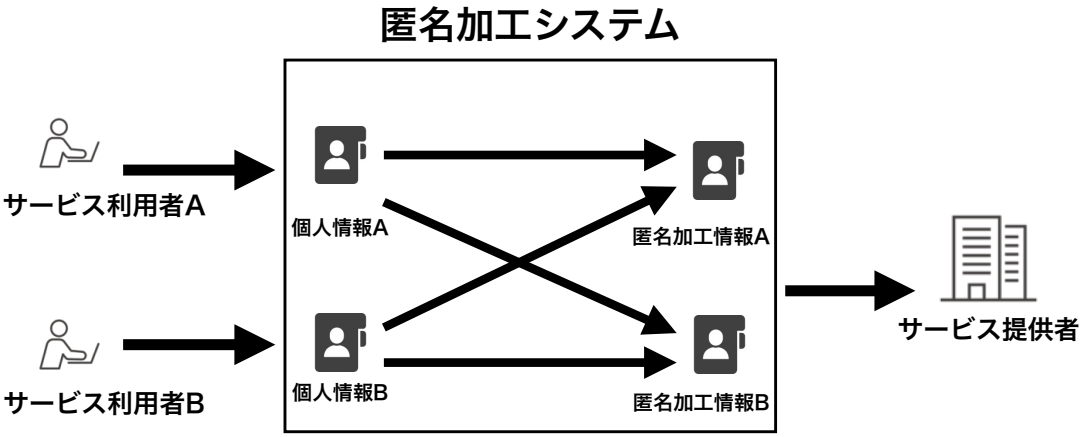

図 4.3: 匿名加工情報の項目の入れ替えの概念図

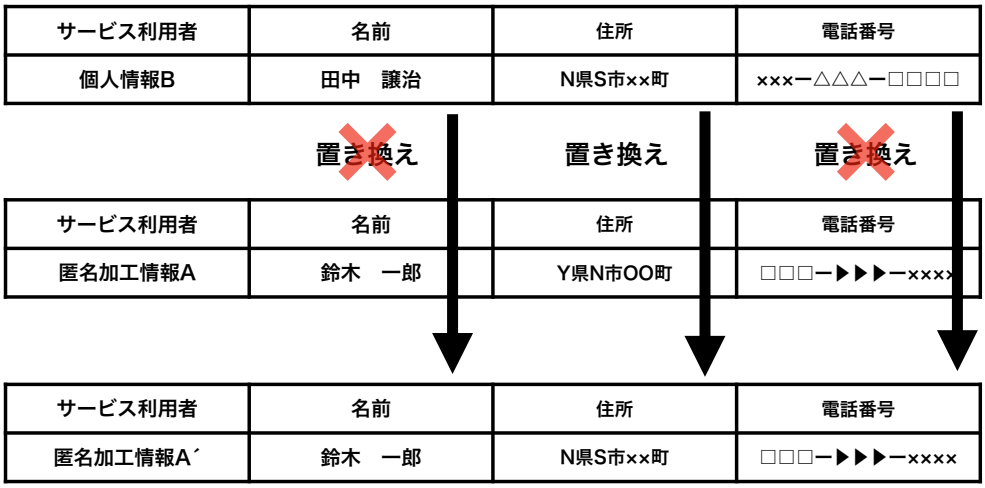

図 4.4: 項目の入れ替えの能否の概念図

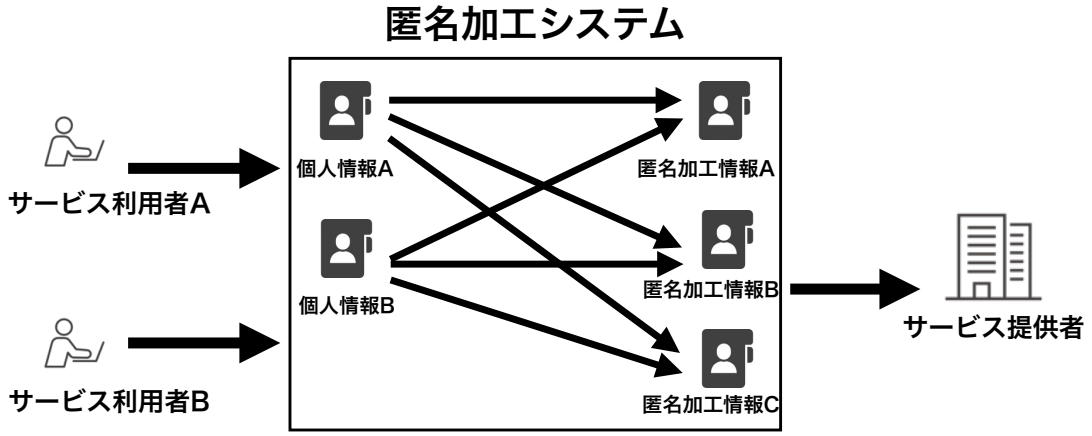

図 4.5: 匿名加工情報の追加の概念図

ダミーはサービス利用者に関係せずにサービスを利用するものである。これによってサービス提供者の中に存在しない個人情報を増やすことでサービス提供者が持っている個人情報を希薄化させる（図 4.6）。

4.2.4　専門的に利用される匿名加工情報

サービス利用者たちが同じようなサービスの利用方法をする場合、それぞれがバラバラに匿名加工情報を使ってサービスを利用するのではなく同じようなサービスの利用方法をするための専用の匿名加工情報を用意する。サービス提供者に集まる情報が画一的になるためサービス利用者と個人情報の関係性を希薄化させられる（図 4.7）。

4.3　匿名加工システムの配置

4.3.1　匿名加工システムの垂直方向の配置

これまで匿名加工システムが 1 つだけあり、それがサービス提供者に対してやりとりをしているものを紹介してきた。ここからは匿名加工システムを 1 つではなく複数用意してサービス提供者とやりとりすることを提案する。匿名加工システムを複数用意しそれぞれが 4.2.1 から 4.2.4 で提案してきた仕組みを持っているものとする。

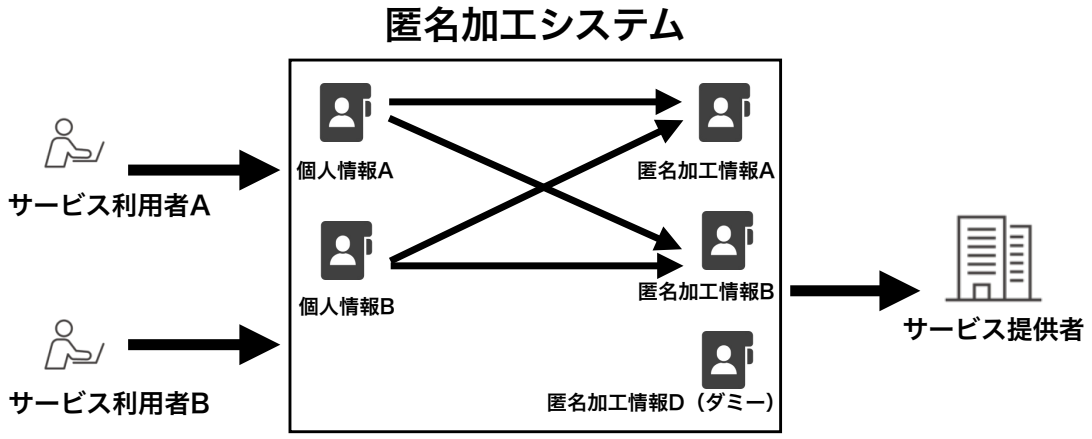

図 4.6: 匿名加工情報のダミーの概念図

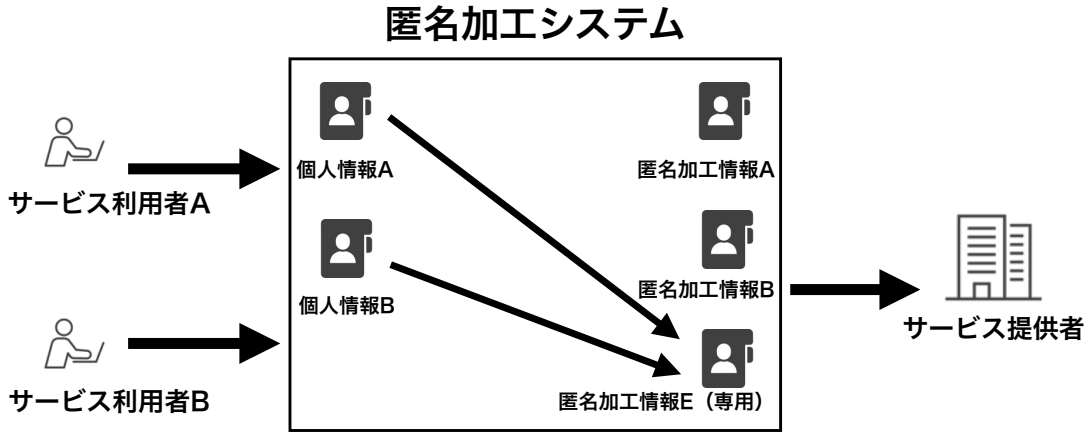

図 4.7: 専門的に利用される匿名加工情報の概念図

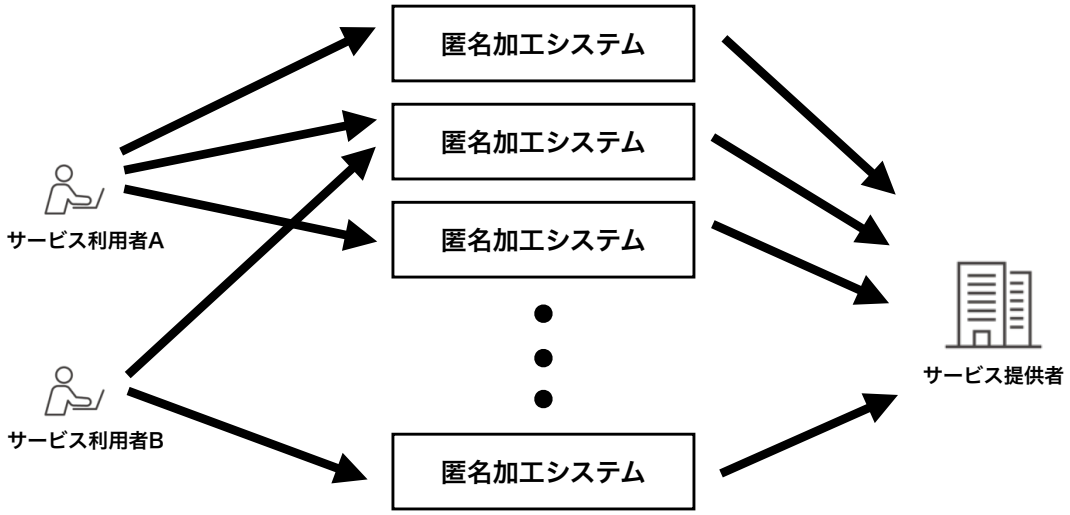

図 4.8: 匿名加工システムの縦方向の配置の概念図

垂直に並べられている匿名加工システムをサービス利用者がサービス提供者とやりとりするたびにランダムに利用する。毎回同じ匿名加工システムを使わないことでサービス提供者にサービス利用者と個人情報の関係性を希薄化することができる（図 4.8）。

4.3.2 匿名加工システムの水平方向の配置

4.3.1 では垂直に複数の匿名加工システムを配置することを考えた。ここではそれを水平にも並べ重層化することを提案する。多重化することで 4.2 でサービス提供者が認識できるサービス利用者と個人情報の関係性を希薄化させたものを、さらに希薄化させる（図 4.9）。

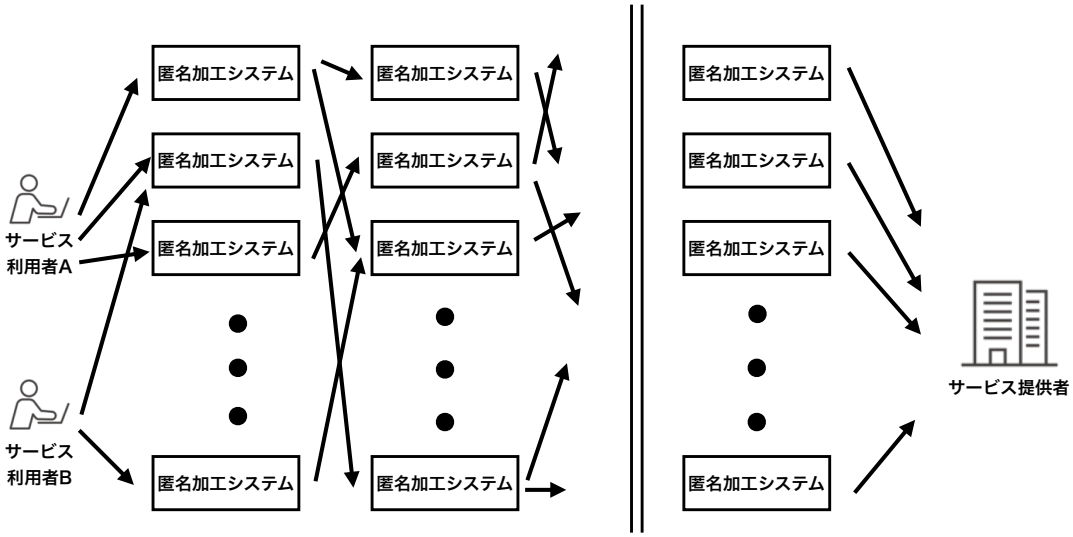

図 4.9: 概念図:匿名加工システムの横方向の配置の概念図

第5章　個人情報のID管理

ここでは第3章のID管理モデルで説明したセクトラルモデルを匿名加工システムに加えることでサービス提供者が個人情報を毎回サービスを利用するごとに入力せずに済むための仕組みの提案をする。

5.1　セクトラルモデルによる個人情報のID管理

ID管理のモデルは第3章で述べたようにセパレートモデル・フラットモデル・セクトラルモデルの3種類があった。まずセパレートモデルで個人情報のID管理をする場合を考える。セパレートモデルの場合は各サービスに対してそれぞれ異なるIDを割り振り管理しなくてはいけない。IDが流出した際の影響範囲は限定的だが、個人情報を変更する際などに全てのIDに対して書き換えなくてはいけないため手間がかかてしまう。

次にフラットモデルで個人情報のID管理をする場合を考える。フラットモデルは共通IDを利用するため手間はセパレートモデルと比べて少なく済む。しかし共通IDが流出した場合、影響範囲が大きくなってしまうという問題点がある。

最後にセクトラルモデルで個人情報のID管理をする場合を考える。セクトラルモデルではセパレートモデルとフラットモデルのメリットを生かしつつデメリットを減らすことができる。よって個人情報のID管理にはセクトラルモデルを採用する（図5.1）。

5.2　匿名加工ポリシー管理システム

個人情報をセクトラルモデルでID管理するために匿名加工ポリシー管理システムについて述べていく。この匿名加工ポリシー管理システムは第2章の個人情報の分類の表で示した個人情報を保存しておくものである。このシステムはサービス利用者が直接やりとりをするもので、サービス利用者が入力した個人情報を匿名加工システムに渡している。

匿名加工ポリシー管理システムのメリットとしては、一度このシステムに入力さえしてしまえば、新しくサービスを利用する際にもこの匿名加工ポリシー管理システムを使えば新たに入力する必要がなくなる。またサービス提供者が引っ越

図 5.1: 匿名加工ポリシー管理システムの概念図

しなどで個人情報の更新が必要になった時も全てのサービスに対して個人情報を書き換える必要がなくなる（図 5.2)。

5.3　匿名加工ポリシー管理システムとサービスの関係性

5.2 では匿名加工ポリシー管理システムについて述べてきた。ここでは匿名加工ポリシー管理システムとサービスの関係性との関係性について述べていく。4.2 の匿名加工で述べた通りサービスごとに必要な個人情報と、匿名加工情報に置き換えてもサービスを利用する際に問題にならない個人情報がある。必要な個人情報とそうでない個人情報のレコードである匿名加工ポリシーを匿名加工ポリシー管理システムの個人情報のテーブルの中に追加する。サービス利用者が利用したいサービスを選択すると匿名加工ポリシー管理システムがこの匿名加工のポリシーを匿名加工システムに渡す。

またサービスがアップデートされると必要となる個人情報が変わってしまう恐れがあるのでサービスに関するレコードは更新される必要がある。このようにすることでサービス利用者がサービスに対しておこなう個人情報の更新の手間を省くことができる。

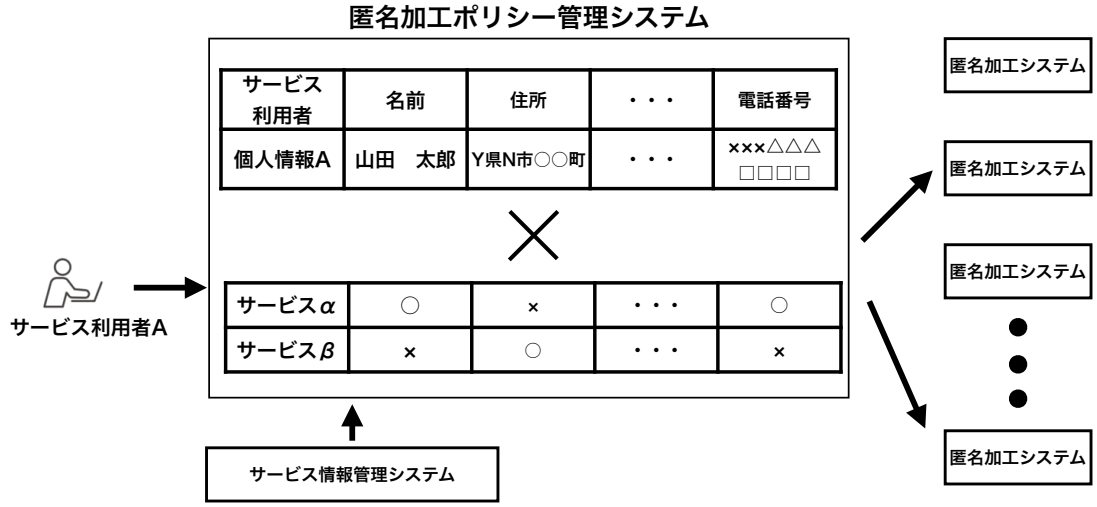

図 5.2: 匿名加工ポリシー管理システムとサービスとの関係性の概要図

5.4 匿名加工ポリシー管理システムと匿名加工システムの関係性

サービス利用者がサービスを利用するために匿名加工ポリシー管理システムにアクセスする際には、共通 ID を使ってアクセスする。そして使いたいサービスを選択してそのサービスを利用するために必要な情報を、匿名加工ポリシー管理システムと匿名加工システムを通して入力される。またこの匿名加工ポリシー管理システムは利用者に一対一の関係で与えられている。

匿名加工ポリシー管理システムから匿名加工システムに対しては、個人情報のレコードと一緒にサービス利用者が選択したサービスの情報と、匿名加工のポリシーが渡される。匿名加工システムは匿名加工が可能である個人情報を匿名加工する。その後、次の匿名加工システムに個人情報のレコード・サービス利用者選択したサービスの情報・匿名加工のポリシーを渡す。

サービス提供者に一番近い匿名加工システムがサービス利用者が選択したサービスに対して、匿名加工された個人情報を入力する。このような一連の流れによってサービス利用者と個人情報の関係を希薄化させながらサービスを利用できるようにする（図 5.3）。

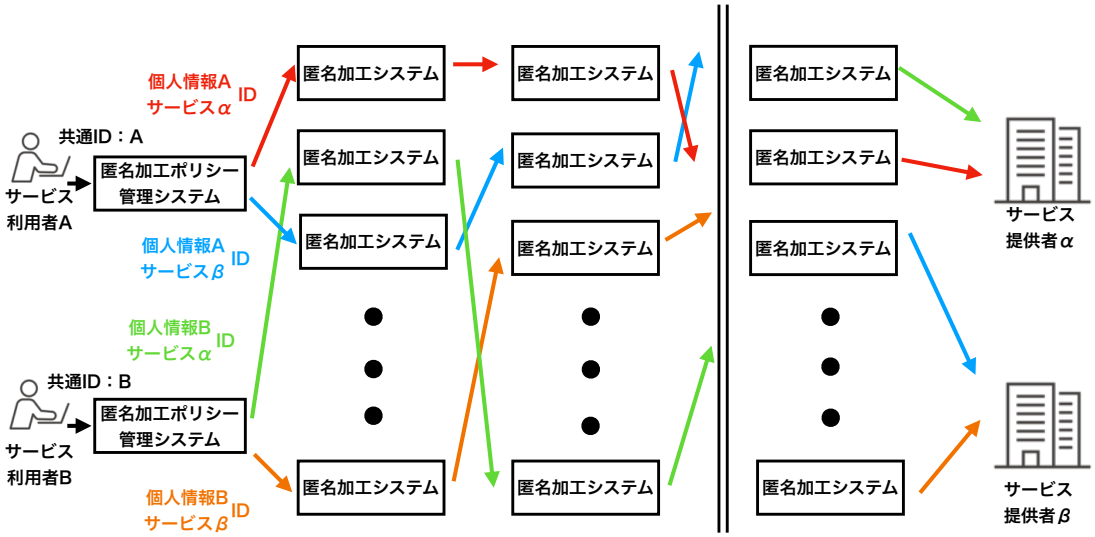

図 5.3: 提案機構の全体図

第6章　システムの複合体以外の個人を識別させない機構の提案

第４章や第５章で説明してきた匿名加工ポリシー管理システムや匿名加工システムなどを通販サイトで使った場合どのように動作するのかをこの章ではシミュレーションしていく。

6.1　顧客情報の入力

通販サイトにアカウント（会員情報）を作成するための流れを述べていく。まず利用したい通販サイトにアクセスする。次に通販サイトにアカウントを個人情報を登録する。この時にメールアドレスが実在するかどうか確認する作業が必要であったり、ボットがWEBページを不正に利用していないかどうか確認される場合がある。そして登録が完了する。

私が提案してきた機構はこのアカウントの作成時に使われるものである。クレジットカードを使いたいのであればクレジットカードの名義の名前とクレジット番号と有効期限を、自宅に荷物を届けたいのであれば自宅の住所を匿名加工することなく登録しなくてはいけない。しかしどれ以外のサービスを利用するために必須でない個人情報には匿名加工情報を登録しなくてはいけない（図 6.1）。

登録確認の回避

同じアカウントをサービスを利用するたびに使用するとサービス利用者と個人情報の関係性がサービス提供者に知られることとなってしまうので、毎回異なるアカウントからサービスを利用する必要がある。しかしアカウントを作成する際に登録の確認作業が入ってしまうと、毎回異なるアカウントを使用することが難しくなってしまう。

この問題の対策としては私が提案した機構を使用するサービス利用者向けにサービスそれぞれに複数のアカウントを用意する方法がある。事前に用意されたアカウントにログインするために必要なメールアドレスやパスワードなどをサービス利用者が事前に知ることができようにし、このアカウントの登録情報を本機構で書き換えサービスを利用する。そしてサービスの利用が終了したらアカウントを

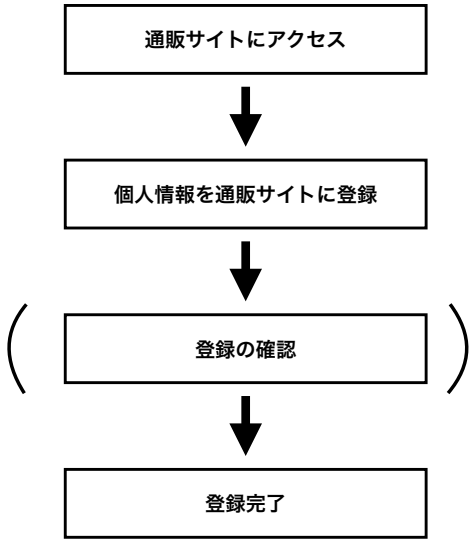

図 6.1: 個人情報入力のフローチャート

最初の状態に戻す。このようにすることで登録確認の問題は回避することができる（図 6.2)。

6.2　サービス利用時の金の流れ

6.1 ではアカウントの登録して通販サイトのサービスを利用できるようにするまでの動作をシミュレーションしてきた。ここでは通販サイトのサービスを利用した際の金の流れについてシミュレーションする。

まず初めにクレジットで支払いする場合についてシミュレーションする。サービス利用者が通販サイトでサービスを利用する際にクレジットカードの名義の名前・クレジット番号・有効期限・セキュリティコードを入力する。通販サイトは入力されたクレジットカードの情報を元にクレジットカード会社に支払いを要求し、クレジットカード会社はサービス利用者の代わりに代金を支払う。後日クレジットカード会社はサービス利用者の口座から立て替えて支払った代金を銀行口座から引き落とす。クレジットでの支払いではクレジットカードの名義の名前・クレジット番号・有効期限・セキュリティコードがサービス提供者である通販サイトの運営者に知られてしまう。

次に代引きで支払いする場合についてシミュレーションする。サービス利用者が通販サイトでサービスを利用する際に支払い方法に代引きを指定すると、商品を届ける運送会社に対して通販サイトの運営者が代引きを依頼する。運送会社がサービス利用者に商品を届けた際に代金を支払わせる。そのご運送会社が通販サ

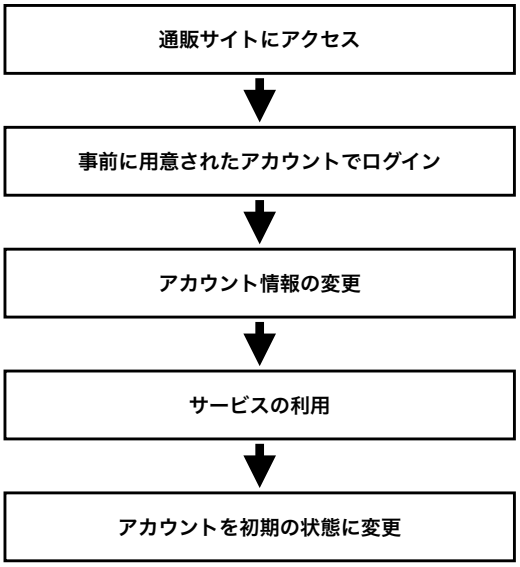

図 6.2: 事前に用意されたアカウントを使用する際のフローチャート

イトの運営者に代金を送金する。代引きを利用するとサービス利用者が受け取る場所が通販サイトの運営者に知られてしまう。

さらに銀行振り込みで支払いする場合についてシミュレーションする。サービス利用者が通販サイトでサービスを利用する際に銀行振り込みを選択すると、通販サイトからサービス利用者に銀行の店名・預金種類・口座番号が伝えられる。サービス利用者は口座に関する情報を元に振り込み人名義や連絡先などを加えて銀行などで振り込みする。振り込み人名義や連絡先を個人情報とは関係性が低いもので銀行振り込みすればサービス提供者に個人情報を伝えないで済むが、毎回どこかで振り込む手間がかかってしまう（図 6.3、図 6.4）。

支払いでの問題の回避

上記で説明した日払い方法の問題点を解決する方法として決済代行サービスを利用してクレジット支払いをするという方法がある。決済サービスを利用するためにはまずクレジットカード情報を決済代行サービスに登録する。その決済代行サービスのアカウントを使って通販サイトでサービスを利用する。そうすることでクレジット番号・有効期限・セキュリティコードを通販サイトの運営者に伝えないで済むようになる。

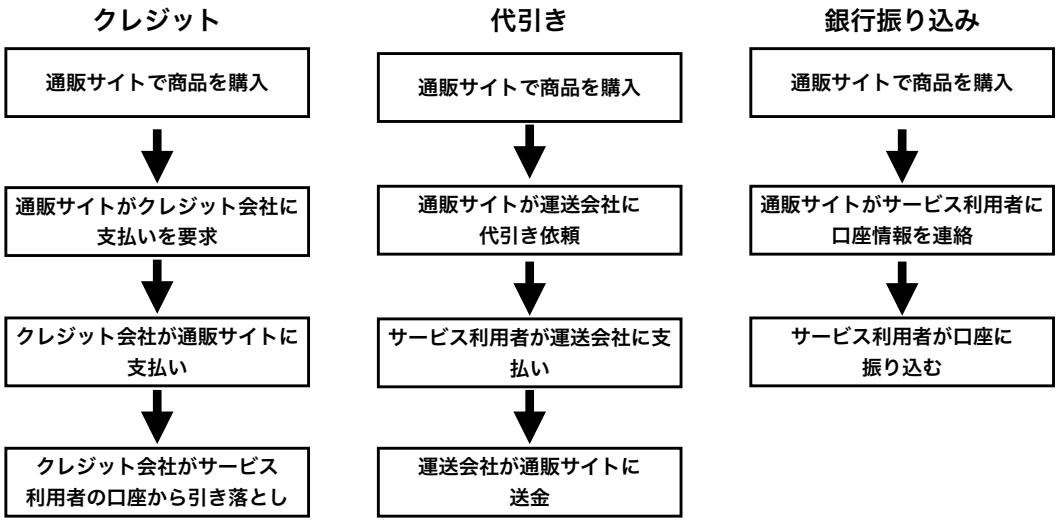

図 6.3: 代金支払いのフローチャート (1)

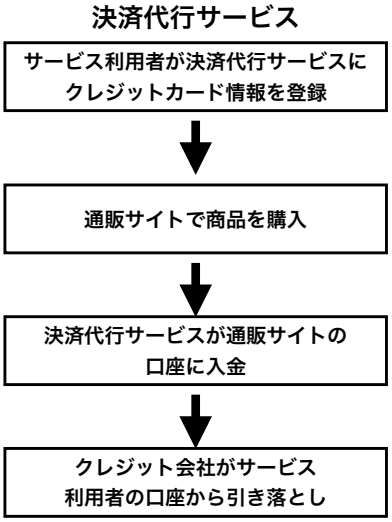

図 6.4: 代金支払いのフローチャート (2)

6.3　サービス利用時の物の流れ

ここでは通販サイトのサービスを利用した際の物の流れについてシミュレーションする。通販サイトで購入した商品は運送会社を通じて指定した住所に届けられる。この時自宅など個人との関係性がわかる場所を指定してしまうとサービス提供者にサービス利用者と個人情報の関係性がわかってしまう。

この問題を回避する方法として、駅前や運送会社などに設置されている宅配ボックスを配送先にしたり、コンビニなどで荷物を受け取るという方法がある。両方ともサービス利用者とその住所を直接関連させることはできないが、毎回同じ受け取流場所を使ってしてしまうと受け取る場所の地域とサービス利用者の関係性がわかってしまうため受け取り場所を不便でない範囲で変更する必要がある。

第7章　おわりに

7.1　まとめ

本研究では解決したい問題が３つあった。１つ目がサービス提供者に個人情報を含む多くの情報が収集されていることと、収集された情報を元にサービス利用者と個人の関係性が明らかにされてしまうことが問題であった。次に２つ目は１つ目の問題を解決するための提案では個人情報をサービスを使うたびに入力する必要があり、あまりにも手間が増えるため現実的ではないことが問題であった。そして３つ目は２つ目の解決策だけではサービスを利用する際に必要となってしまう個人情報があることであった。

１つ目の問題を解決するために個人情報を匿名化して個人が特定されにくい情報に変えてサービスを利用することを提案した。また個人情報をただ匿名化させるだけでなく、匿名加工情報を増やしたりサービス提供者とは関係ないダミー情報を送ったりする匿名加工システムを提案した。さらにこの匿名加工システムを重層的に配置することでサービス利用者と個人情報の関係性を希薄化させる仕組みを提案した。２つ目の問題を解決するためにこの匿名加工システムを使用する際に個人情報を自動で入力する匿名加工ポリシー管理システムを提案した。このシステムは各サービスに対してどの個人情報が利用するために必須の情報であるのかも記録されており、その情報をもとに匿名加工システムに個人情報を匿名化させるものであった。３つ目の問題は決済代行サービスや駅前などに設置されている誰でも利用できる宅配ボックスなどを使用することで回避することを提案した。

7.2　今後の展望

匿名加工システムの課題

サービスを利用するためには匿名加工することができない情報がある点が課題である。またサービス提供者に匿名加工システムを使用していることが知られてしまうと、サービスの利用を停止させられてしまう恐れがある。

匿名加工ポリシー管理システムの課題

個人情報を一箇所で集中管理しているため、このシステムが攻撃されるとすべての個人情報が流出してしまう恐れがある。

マイナンバーが導入され各種サービスに使用された場合の課題

マイナンバーが本格的に導入されていくと行政だけではなく民間のサービスでも本人確認が容易になっていってしまう。そのため今まで以上にサービス提供者が個人情報とサービス利用者の関係性を理解しやすくなる環境が作られてしまう。

中央銀行が発行する通貨が仮想通貨になった場合の課題

中央銀行が発行する仮想通貨が一般的に使用されるようになると取引を追跡されるようになり、通貨の取引履歴から個人情報が知られてしまう恐れがある。

謝辞

本研究をおこなえるまでに多くの方々に大変お世話になりました。本研究の締めくくりに感謝の意を述べていきたいと思います。母校である小樽商科大学の深田秀実せんには、文系の学部卒でも情報科学に関して勉強できる環境を探して欲しいという無理難題をお願いし、多岐にわたる選択肢を示していただいただきました。このことがなければ JAIST に入学することはなかったと思います。

入試合格後右も左もわからない中入学前に配属研究室を探して大学構内をさまよっていた私を、知念賢一特任准教授は研究室案内していただき配属の内定をいただきました。入学後は大学での勉強のみならず骨折などの多くのトラブルにまで巻き込んでしまいながら、それでも快く指導していまいただきました。また篠田陽一教授には情報科学に疎い学生であった私を、ゼミなどの発表で本研究の完成まで導いていただきました。研究室の学生には歳の離れた学生であったにもかかわらず受け入れていただきました。

学外においては、三味線の師匠である柳原達宏氏に多くの面でお世話になりました。また両親には怪我をして大変だったにもかかわらず石川県で勉強することを認めて物心両面で支えていただきました。ここまで本研究を進めるにあたって上に記述しきれていない多くの方々にもお世話になりました。皆様ありがとうございました。

関連図書

[1] 長谷川聡, 正木彰伍, 岡田莉奈. 大規模データを実用的な速度で処理可能な匿名化ライブラリの設計と実装評価. In *Computer Security Symposium 2017*, pp. 1824–1828, October 2017.

[2] 金沢史明, 岸野徹. 特許出願からみた匿名化関連技術の技術動向—平成 29 年度特許出願技術動向調査より—. In *Computer Security Symposium 2018*, pp. 906–912, October 2017.

[3] 山岡裕司, 前田若菜. 自己情報コントロールと権限分散を両立するパーソナルデータ流通方式の提案. In *Computer Security Symposium 2018*, pp. 920–926, October 2017.

[4] 小栗秀暢. 匿名データの安全性指標としての再識別率とその活用方式の提案. In *Computer Security Symposium 2018*, pp. 927–934, October 2017.

[5] 藤村明子, 間形文彦, 千田浩司, 諸橋玄武, 高橋克己. 新たな個人情報保護法における匿名加工情報の基準に関する一考察. In *Computer Security Symposium 2015*, pp. 1143–1150, October 2015.

[6] 柏市オフィシャルウェブサイト. 個人情報の取扱項目の具体例, 2014. `http://www.city.kashiwa.lg.jp/soshiki/030100/p034475_d/fil/gutai.pdf`.

[7] 個人情報保護委員会. 個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）, November 2017. `http://www.city.kashiwa.lg.jp/soshiki/030100/p034475_d/fil/gutai.pdf`.

[8] 株式会社三菱総合研究所 社会 ICT イノベーション本部. 匿名加工情報・個人情報の適正な利活用の在り方に関する動向調査報告書, March 2018. `https://www.ppc.go.jp/files/pdf/tokumeikakou_report.pdf`.

[9] 株式会社野村総合研究所. パーソナルデータの適正な利活用の在り方に関する動向調査（平成３０年度）報告書, March 2020. `https://www.ppc.go.jp/files/pdf/houkokusho_201903.pdf`.

[10] 森亮二. パーソナルデータの利活用における技術および各国法制度の動向：3. 日本の個人情報保護法改正の状況. 情報処理.vol55.no12, pp. 1342–1349, October 2017.

[11] 森亮二. 匿名加工情報とは何か, July 2017. https://www.soumu.go.jp/main_content/000487916.pdf.

[12] 石井夏生利. パーソナルデータの利活用における技術および各国法制度の動向：2. アメリカのプライバシー保護に関する動向. 情報処理.vol55.no12, pp. 1346–1352, October 2014.

[13] 石井夏生利. 国民ＩＤとプライバシー・個人情報保護に関する法的論点整理, October 2010. https://www.kantei.go.jp/jp/singi/it2/denshigyousei/dai2/siryou4_2.pdf.

[14] 安達和夫. 海外における個人識別番号と情報連携, October 2010. https://www.kantei.go.jp/jp/singi/it2/denshigyousei/dai2/siryou4_1.pdf.

[15] 高崎晴夫. パーソナルデータの利活用における技術および各国法制度の動向：1. 個人情報保護にかかわる法制度をめぐる EU の状況. 情報処理.vol55.no12, pp. 1347–1345, October 2014.