【論文】

自己情報記録・公開アプリ開発の展望
―公開鍵暗号法を用いた一方向特定加工情報の提案―

京都光華女子大学　　臼井　義比古

1. はじめに

情報化社会が大きく発展した現代社会において、個人が日常的に記録するデータは、個人的な利用のみならず、秘匿性が十分担保できれば、社会的に極めて有用なデータとなりうる。その情報共有社会システム実現のためには、データ発出人が確実に秘匿され、かつ発出人の正当性が確認され、いつでも発出人(以下本人と記述する)による削除可能なシステムの構築が不可欠である。

現在データの流通は、ウエブアクセスの個人関連情報や、ウェアラブルデバイスからの、例えば個人の体温や、体重などの個人関連情報の扱いを中心に進められており、個人情報保護法案なども関連の個人情報の侵害を懸念してあわせて検討・推進されている。筆者は現在これらとモデルが違う 2-2 で後述する Twkel のようなアプリを用いて、個人情報や個人関連情報の交換も個人情報保護法の範疇を守りながら、複数人数分のデータは個人での利用以上に社会的知見が多く得られる可能性が高いことを根拠に、一方向特定加工情報を提案し、個人情報の安全性を守りながらネットワーク上での個人情報の制御ができることを提案したい。また Cookie モデルや、ウェアラブルモデルとのモデルの違いはあるが、一方向特定加工情報モデルを配慮した法制度が整えば、今回作成中の Twkel のようなアプリのデータ公開機能の実現は可能であると考える。

すなわち、個人の生活情報などの公開と交換の価値を評価し、個人情報に抵触するかどうかの調査を行い、抵触するのであれば技術的対応と法律改正の点で検討を加える必要があると考える。特に問題なのは、個人情報の扱いについて法令の規定があり、第三者へのデータの提供と、本人許諾目的外の利用が制限されている点である。今回は、個人情報保護法案や弁護士の解釈などの調査を行い、今回計画しているアプリ Twkel(仮称)の作成に必要なデータ交換方法の案を作成し、Twkel の今後の展望について報告する。

2．個人の生活情報のネットワーク上の流通の価値とクリアするべき法律的上の問題点について

個人の生活や情報は、個人のデータのままでも、疾病の生活習慣的素因として捉えることができる可能性があるが、複数集まると、健康情報として、さらには、研究材料として、より公共の福祉を増進するように用いることができる可能性がある。

たとえば、生活習慣情報と疾病の関連の分析がすすみ、AI などによる、生活診断に使える可能性もでてくると考えている。もちろん、無用なデータやシステムとなってしまう可能性はあるが、この報告では、まず、様々なデータの記録をつけ、流通させることの価値と、それを行うのにクリアするべき個人情報保護法の問題について議論したい。

2-1 古文書に記載された地震の記録

記録者が想定していたかどうか不明の情報の利用の評価の一つの例として、古文書に記載された、地震の記録の解読プロジェクトが行われた例をあげる。

古文書には過去に起こった地震の情報などがあるとして、京都大学古地震研究会(京都大学古地震研究会 2019)によって始められたプロジェクト「みんなで翻刻」がある(みんなで翻刻)。このプロジェクトでは、古文書・古記録・古典籍などの江戸時代以前に筆記・出版された資料を読み、地震や大災害という周期の長い自然現象の研究に役立てることが計画されている。一つの成果として、「市民参加型オンラインプロジェクト『みんなで翻刻』東京大学地震研究所蔵の古京都大学、東京大学、国立歴史民俗博物館文書のうち 495 点をすべて解読！」という記者発表が 2019 年 3 月 19 日付けでから行われている(京都大学・東京大学・国立歴史民俗博物館、2019)。

京都大学古地震研究会は、「地震や自然災害の理解には、経験（観察、観測）が欠かせません。まれにしか起きない自然現象なので、文字史料から得られる過去の経験が決定的に重要なのです」とこのような情報の重要性について言及している。

また古地震研究会のホームページ(2017 頃)によると、「理学研究科，文学研究科，防災研究所，生存圏研究所，図書館 および佛教大学の教職員と学生さん」が参加しており、様々な方面から興味を持たれていることがわかる。

推察になるが、記録を書いた人物は、これらの記録が上述のような多様な方面から利用されることを想定していなかったと思われる。

このように、後の時代に現代のデータがいかに使われるかは不明であるが、データをつけて残しておいた場合に、後に有効に使われる可能性はある。近年の、めざましいデータの保存コストの低減から、後日役にたつ可能性がでてくることを期待し、データの蓄積を始めるのがよいと思慮する。

2-2 Twkel で行いたいデータ記録と交換

本件に関わるアプリ「Twkel」は日本語の「記録をつける」の「つける」を世界中で発音できるように命名したものである。体温や食事時間や運動量などの個人の生活データを可視化の機能などを持たせ、筆者が開発に着手、現在開発中である。

Twkel には様々な形式のデータの蓄積と確認のための簡単な表示を行う機能をもたせ、その後、データの公開・交換に関しての機能を追加していく予定であるが、データの公開交換に関しては、受け取った側でデータの起源を区別できるようにしたいと考えている。

例えば、ある個人に関する健康データは月日がたてば増える。そして、データ交換網を、追加や差分で流通することになる。同一人物のデータが増えた場合は、同じ人物のデータとして扱うのが、データの有効性を高めると考えられる。

また、個人情報を含んだ情報は収集時に利用を明示する必要があるが、Twkel は単にデータを収集し、収集したデータがどのような目的に使われえるかを検討することが目的であるので、目的の公表無しで取集を行いたいと考えている。

個人関連情報は扱いがデリケートで、情報流通後に削除をしたくなる可能性があるが、これにも対応したい。いったん流通したデータを後日消去できる機能を持ったほうが、ユーザが安心してデータを流

すことができ、収集できるデータが増える可能性が高くなり、より高度な知見が得られやすいと考えられる。

2-3 これまで開発されてきたデータ記録アプリの概要と現行法の制約

これまで開発されてきたデータ記録アプリは相当の数が存在しており、App Store や Google Play などで検索することができる(App Store での検索結果例えば「記録」などで検索)(Google Play で例えば「記録」で検索)。これらのアプリには記録するデータが固定のものもあるが、データ形式を自由に設定できるものもある。

曽根・谷口・河合・大平(2018)によりデータベースに記録する汎用アプリも報告されているが、検索を行った範囲では、これらのアプリで記録されたデータをネットワーク上で公開、交換する機能のものを見つけることができなかった。データを一時的にサーバに記録し、診断を受けられるものや、メールや LINE でデータを送信する機能を持つものは存在していた。

Twkel はデータの利用目的を探すのが目的の一つであり、収集の目的が明示できないという制約がある。一方、個人情報を収集する場合には収集の内容と目的を本人にわかりやすく通知する必要があり、今回計画中の、目的不詳の収集と転送では、各社ストアのプライバシーポリシー(Apple、2021)(Google、2021)に違反となる可能性も高い。このため、Twkel のような実装を行ったアプリが見つけられなかった可能性は高い。

2-4 個人情報収集の法律的問題

個人情報保護法は、個人を特定可能な情報(以下個人情報)や個人に関連する情報を本人が制御する権利を保護する法律である。個人情報の交換で個人の利益が損なわれないように、2003 年に制定され、2017 年と 2020 年に改正された。(2020 年改正の同法の全面施行は 2022 年 4 月 1 日)。

2003 年の制定後、AI やビックデータが一般にも広がり、個人情報の保護内容が社会の実情に沿うように改正された。2017 年の法改正で匿名加工情報が追加され、2020 年の改正では仮名加工情報が追加されることになった。これらに分類されるデータは、第三者への提供が容易にできるものや、社内でより柔軟な目的のために利用することができるものがあり、以下で説明する。

2-4-1 個人情報の保護について

ここで、個人情報とは個人を特定できる情報とする。また、個人関連情報とは個人に関連する情報から、個人情報を除いたものとする。

基本的に個人情報保護法では、個人関連情報と個人情報を組みあわせたものは、本人が制御できるものであり、本人の許諾なく第三者への提供はできず、情報収集時の許可を取った目的外の利用はできない(Web Lawyers、2020)。

2-4-2 匿名加工情報

2017 年の個人情報保護法改正で追加された個人情報の分類で、ビックデータなどに対応するために作成された。個人を特定可能な情報(氏名など、それだけで個人を特定できる情報だけではなく、他の

情報とあわせて特定可能な情報を含む)を削除し、個人関連情報のみにすることで、企業間での「自由な流通・利活用」させることを容易にしたものである(板倉、2021)。また「匿名加工情報に加工することで、当初は全く想定していなかった利用目的への利活用が可能」となった(Web Lawyers、2020)。

しかしながら、匿名加工情報はデータ内に個人を特定可能な要素がないため、同一人物のデータが複数あった場合などに同一人物のものと判断できない、あるいは、異なる時期に作成された同一人物のデータを連結できないという問題がある。連結できるような情報をつけてしまうと、匿名加工情報ではなくなる。

また、本人がデータの削除を求めた場合でも、本人のデータかどうかがわからず削除できないという問題もある。加工元のデータからは削除可能であるが、企業内であってもいったん匿名加工情報として流通させてしまうと削除は不可能である。

さらに、他の情報と照らしあわせても、個人が特定できないようにする必要があり、例えば、年齢が 110 歳以上という情報が含まれると、個人が特定しやすくなってしまうため、匿名加工情報として扱える情報が制限されるという問題もある。

2-4-3 仮名加工情報

2020 年公布の個人情報保護法改正で追加された情報の分類である。仮名加工情報は匿名加工情報と同様に、直接的に個人を特定可能な情報は切り離す必要があるが、匿名加工情報と異なり、例えば年齢が 110 歳などの情報を含んでいて他の情報との照合を行うことで本人が特定可能となってもよい。さらに、もとの個人情報を復元することができないことが要件とはされておらず(Web Lawyers、2020)、個人情報へのリンクを残してもよい。

仮名加工情報は、匿名加工情報と比較して利用目的が柔軟になり、企業内におけるビッグデータの利活用を目的としているが(板倉、2021)、前述のように情報を照合して個人が特定可能になるので、企業間の融通のハードルは高くなっている(水町、2021)(板倉、2021)。

目的外の利用は、法律上は不可だが、利用目的の変更制限がかからず、事実上目的外の利用が可能という意見がある(Web Lawyers、2020) (水町、2021)。

2-4-4 加工情報のまとめ

表 1 に匿名加工情報と仮名加工情報の概要をまとめる。各項目は様々な条件付きの可否であるが、詳細は省いて一般的な可否を表示した。これらの情報源は各弁護士のホームページであり、各弁護士のホームページには各職の意見であることが付記されている。

匿名加工情報や仮名加工情報に分類されない一般的な個人情報は、基本的に本人の合意がなければ、第三者に提供することができず、目的外の利用を行うこともできないので、比較の対象として「下記以外の個人情報」として 1 段目に書いた。

表中で「データの整合性」とあるのは、複数回にわたって提供されるデータから、同一人物からのものであるかどうかを特定できるかどうかで、仮名加工情報では、照合情報とのリンクのキーを使うことで特定可能である。「削除可能」は、流通したデータが後日本人の依頼で削除できるかどうかを示す。仮名加工情報では、個人を特定可能な照合情報を持っているかどうかで異なるため「○/×」と記した。

前者が個人を特定可能な照合情報を持っている場合である。

表 1　匿名加工情報と仮名加工情報の概要

	第三者提供	目的外利用	データの整合性	削除可能
下記以外の個人情報	×	×	○	○
匿名加工情報	○	○	×	×
仮名加工情報	×	○	○/×	○/×

3. 一方向特定加工情報の提案

表 1 を見るとわかるように、第三者提供や目的外利用やデータの追加時のデータの整合性の担保や後日の本人希望による削除をすべて可能とすることができず、目的に応じて選択する必要がでてくる。

3-1 一方向特定加工情報

そこで、本報告では一方向特定加工情報を提案する。一方向特定加工情報は、公開鍵暗号法をもちいて、匿名加工された個人関連情報と同情報のハッシュを秘密鍵で署名したものである。本人が秘密鍵を保持しておいて、秘密鍵を用いて追加のデータを送信すれば、同じデータ元であることが証明できる。この機能をもちいると、データの追加や削除や変更がデータを作成した本人から自由に行うことができる。

つまり、流通しているデータ単体からも、仮名加工情報の照合情報に該当する追加情報とあわせても本人の特定はできないが、本人が持つ秘密鍵があれば、公開鍵を比較して、同一人の起源の情報であることが示せる。たとえば、本人が複数回に分割してデータを流通させた場合、添付された公開鍵と匿名の証明書をもちいて同一起源のデータであることが確認できるため、統合ができる(ただし、データのハッシュは統合できないので、統合結果の再送はできない)。また、たとえば、データ流通事業者に対して、秘密鍵を用いて削除依頼をだした場合、データ流通業者は個人データの本人からの削除依頼であることが確認できる。同様に、個人データの利用目的の制限なども、本人側から行うことが可能になる。ただし、データを保持する側が操作に応じた場合に限る。

このように一方向特定加工情報は、公開鍵暗号法の能力の範囲で、匿名加工情報と同じ匿名性を持ち、公開鍵をキーとしてデータベースに登録でき、同一人のデータであることがわかるという範囲で仮名性をもつ。

3-2 一方向特定加工情報の問題点

3-2-1 法改正の必要性

一方向特定加工情報はデータの起源である本人からみて匿名ではないので、現在の個人情報保護法では、匿名加工情報として扱うことはできない。また、仮名加工情報としては扱えるが、先にも述べたように、仮名加工情報を第三者に提供するときは、第三者への移転の可否を本人に確認する必要があり、第三者提供は実質的に難しいと考えられているため、ネットワーク上の流通をしやすくするためには、仮名加工情報としては考えないほうがよい。

つまり、一方向特定加工情報は第三者が照合情報を持たないため、これらの制約を外した新たな加工情報として考えるのが妥当と考える。そのためには法の改正が必要となる。

3-2-2 第一中継者の存在

一方向特定加工情報は、本人から見て最初の中継者(第一中継者)には個人情報が漏れる可能性がある。したがって、第一中継者には、法的な制限を設け、次以降の中継者より、厳しい制約を設ける必要がある。流通する一方向特定加工情報に第一中継者の ID に相当するデータを付加することにより、データの利用者は、本人に対して連絡を行うことが可能となる。

また、第一中継者が、データ中継事業を行えなくなっても、本人は異なる中継者に接続して、個人関連情報の削除を行うことができる。秘密鍵を保管しておけば、本人であることが証明できる。ただし、他の中継者に接続した時点で個人情報が漏れる可能性はある。これらの点については法改正などを含めて、検討する必要がある。

3-2-3 照合による個人特定可能問題

患者数が少ない特殊な病気などの事由で個人が特定できてしまう場合がある。個人が特定可能な特殊な情報は、本人の同意を得て公のものとして、敬意をもってそれらを扱うしかないと考えている。とはいうものの、なにがしらかの策があれば、それにこしたものはなく、今後の検討課題としたい。

3-3 流通モデルの違い

一方向特定加工情報は、秘密鍵を本人が持つことで情報の追加や削除のコントロールを行うため、アプリなどでは対応できるが、インターネットのアクセス時に利用される Cookie モデルを用いて取得される個人情報などでは対応ができない。つまり、秘密鍵が使えるインターフェースを持てる場合に利用が限定される。

また、複数の第一データ中継者に対して同じ公開鍵秘密鍵ペアを用いると、秘匿性が劣化するという問題がある。

さらに、ウェアラブルデバイスを用いて作成された個人関連情報を一方向特定加工情報にして流通させる場合は Cookie モデルほど多くの第一中継者を介さないとは思われるが、アプリごとに第一中継者が異なり、秘匿性が落ちることと、秘密鍵と公開鍵のペアを使い分けたとしても、同じデータを複数の第一中継者に送ることで、データの内容から同一人であることが知られてしまう可能性が高くなることに注意が必要である。

4. データ流通業界との協力

2−1 で述べたように、単純に情報を「つけ」蓄積交換することには価値がある可能性があり、Twkel の開発を今後も行っていきたい。また、3 で提案した一方向特定加工情報を用いると、Twkel で行いたい第三者への提供や目的外利用やデータの整合性の保持や後日の削除が行えることを示した。しかしながら、これらの実現にはいくつかの問題があり、解決方法を以下で議論したい。

4-1 Twkel モデルと法改正の必要性

個人情報を交換する場合、個人情報保護法に触れないようにする必要があるが、現在の個人情報保護法では、2-4-4 で述べたように、第三者への受け渡しが難しい仮名加工情報が使うか、情報源が全く区別できず重複が起こる可能性がある匿名加工情報を使うことになり、十分ではない。 それに加え、目的を示さず個人情報を収集し、自由に第三者に提供し、それでいてデータが同一人物の個人情報であることがわかるようにしたいとも考えており、条件は厳しい。

これらを満足するには、一方向特定加工情報などのような、加工情報が必要である。それを実現するには、法律を変えるだけの根拠を示し、実績を積む必要がある。このために、個人情報を流通させたい業界や地域と連携して、Twkel モデルが可能になるような法改正ができるように、議論を行っていく必要があると考えている。

4-2 法改正の動きとデータ交換社会の動向

個人情報保護法は、社会の変化に対応し、個人の権利や安全性の保護と公共の利益の境界の変化を探り、必要な法令を制定していく必要から、3 年ごとに改正が行われていくことになっている。

眞野(2020)によると、現在、データ交換に関して IEEE で P3800 というデータ流通に関する委員会が立ち上げられ、データ交換技術の標準化が行われている。データ流通関連の取り組みへの参加を検討中である。

5. まとめ

目的を定めず。日常的に数値などのデータをつける（記録する）ことで、その後にデータが、個人的あるいは社会的に利用される可能性があることの一例をあげた。データの流通は、ウエブアクセスの個人関連情報や、ウェアラブルデバイスからの個人関連情報の扱いを中心に進められており、個人情報保護法案なども関連の個人情報の侵害を懸念してすすめられているが、これらとモデルが違う Twkel のようなアプリをもちいた個人情報や個人関連情報の交換も、個人情報保護法の範疇で守られるように行動をする必要がある。

この報告では一方向特定加工情報を提案し、個人情報の安全性を守りながらネットワーク上での個人情報の制御ができることを示した。また Cookie モデルや、ウェアラブルモデルとのモデルの違いを指摘し、Twkel のような一方向特定加工情報モデルを配慮した法制度が整えば、今回作成中のアプリのデータ公開機能の実現は可能であることが示せた。

参考文献

板倉陽一郎(2021)「個人情報保護法改正によるデータ流通への影響 2017 年改正，2020 年改正及び 2021 年改正法案」https://www.jftc.go.jp/cprc/conference/index_files/kentou21040701.pdf

京都大学・東京大学・国立歴史民俗博物館(2019)記者発表、https://www.kyoto-u.ac.jp/sites/default/files/embed/jaresearchevents_newsdepartmentrigakunews2018documents190319_101.pdf(2021/12/19

閲覧)
京都大学古地震研究会、https://kozisin.info/(2021/12/19 閲覧)
古地震研究会「過去の合宿」http://www1.rcep.dpri.kyoto-u.ac.jp/~kano/kozisin/#!index.md(2021/12/19 閲覧)
個人情報保護法(2020)
曽根良昭・谷口啓子・河合雅弘・大平栄二(2018)「介護老人保健施設における健康管理データの収集及び表示汎用アプリの開発」『美作大学短期大学地域生活科学研究所所報』(14)、4-5、(2018-01)
眞野浩 (2020)「IEEE P3800 の概要と狙い」『IEEE P3800 Data Trading System の標準化 基礎と概要』データ 流通推進協議会、https://data-trading.org/openseminar/(2021/12/16 閲覧)
みんなで翻刻、https://honkoku.org/ (2021/12/19 閲覧)
水町雅子(2021)(2021.12 改訂)「個人情報保護法改正 2020 年のポイント解説」http://www.miyauchi-law.com/f/200325pii2020kaiseigaiyou.pdf(2021/12/19 閲覧)
Apple (2021)「App Store での App のプライバシーに関する詳細情報の表示」『App Store』https://developer.apple.com/jp/app-store/app-privacy-details/(2021/12/19 閲覧)
Google (2021) 望ましくないソフトウェアのポリシー」『Google について』https://www.google.com/about/unwanted-software-policy.html(2021/12/19 閲覧)
Web Lawyers (2020)「個人情報保護法改正で変わる！仮名加工情報と匿名加工情報の利活用を弁護士が解説」『Web Lawyers コラム』https://web-lawyers.net/anonymously_processed_information/(2021/12/23 閲覧)

Prospect of the Construction of Disclosure System of One's Personal Data:

Proposal of the One Way Detectable Information Using Public Key Cryptography

Yoshihiko USUI

Twkel, a smartphone application software which is currently under development, enables us to memorize the structural data of our daily activities such as body temperatures, weights, and so on. Twkel is also designed to transfer personal data through the Internet. This is because the collected personal data of so many people may help produce some important knowledge, for example, in terms of our health, even though we don't understand the value of their personal data. This kind of data trading system is not constructed yet, because the Personal Data Protection Law prohibits free transportation of the personal data without the permission from its sender. In this paper, we will introduce the data mining project where the data had not been originally intended to be used for that purpose, to show the potential of our data accumulation application software Twkel. In addition to this, we propose the One Way Detectably Modified Personal Information model to be added to the Personal Data Protection Law. One Way Detectably Modified Personal Information can show whether the sender has the same private key of the original sender without identifying who the original sender really is, using the public key cryptography. In this information model, information can identify the sender by itself, so the data can be merged or deleted on the command from the sender. This helps to produce the effective use of the personal data while keeping the personal information confidential.