川口嘉奈子, (2019), 「プライバシー保護のために必要な「わかりやすさ」とはどのようなものか」,
千葉大学大学院人文公共学府研究プロジェクト報告書第 342 集
『知覚・推論・発話をめぐるアスペクト形成』pp.16-24.

プライバシー保護のために必要な「わかりやすさ」とはどのようなものか

What is it like "the plain explanation to the general public" for their privacy preserving?

川口 嘉奈子
Kanako KAWAGUCHI

アブストラクト

2018 年 5 月に EU の新たなデータ保護規則である General Data Protection Regulation[1]（以下、GDPR）が施行され、日本企業の個人データ保護の取り組みに変更が求められることとなった。GDPR は、ユーザが自身の個人データを必要なだけ守ることができるよう、情報を取り扱う企業が個人データを取扱う際の指針を示したプライバシーポリシーや、利用に際しての同意取得の説明が、明瞭でわかりやすい記述であることを要求している。本稿では、ユーザのプライバシー保護のために、どの程度の「わかりやすさ」が必要とされるかについて考察する。

Abstruct

Businesses in Japan were forced to modify their commitment to personal data preserving due to General Data Protection Regulation (GDPR), which is a new regulation for data preserving of EU and took effect on 25th May 2018. GDPR requests all businesses to provide written information for plain explanations about their privacy policy and procedure of soliciting data subjects for their consent. In this paper, I examine how "plain" explanations the general public need for preserving their privacy by themselves.

0　はじめに　～議論の前提と状況確認～

個人の行動・購買履歴、SNS での発言など、インターネットの存在が当然のものとなっ

[1] GDPR (General Data Protection Regulation: 一般データ保護規則)
https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

た社会生活上で生じる自身由来の情報やデータは、自ら把握できないほど存在し、今この瞬間も増え続けている。

日本では 2017 年 5 月に改正個人情報保護法[2]が施行され、上記のような個人データ[3]の利活用と保護に加え、事業者が国外に個人情報を移動することにかかる規制が盛り込まれた。このこともまた、そもそもの在り様がボーダーレスなインターネットを基盤とする社会において必要な措置であり、規制であると言えるだろう。範囲内から範囲外へと個人データを移送するいわゆる「越境」は、EU 内においては、1995 年に発効した EU データ保護指令の時代から原則として禁止されてきた。そして、2018 年 5 月に施行された EU の新たなデータ保護規則である General Data Protection Regulation（以下、GDPR）でも、その原則は継続されている。

私たちの個人データを、グローバルに展開する企業がネットワークを通じて簡単に取得・所持できる状態が常態化する中で、それらを利活用して利益につなげたいと考えるのは営利団体として自然なことであろう。他方で、私たちは、自分自身についてのデータを、どの企業がどのように取得し、利用しているかについて、あまりにも知らない場合が多い。そうしたデータは自分についてのものであるにもかかわらず、インターネットを介したサービスを利用すれば取られてしまう。ここには何か不正があるのではないかという素朴な直観は、私たちがサービス利用時に行う、データ利活用への「同意」によって、これまで対策されてきた。

GDPR 下では、先に述べた「越境」制限の他に、もう一つ大きな変更点がある。この「同意」についてである。

個人に関するデータを事業者が利用したい場合には、単なる同意ではなく、本人による明確で積極的な「同意(consent)」を取得しなければならなくなった。プライバシーの範囲に照らして不適切、あるいは不確実なデータ利用を避け、個々人の人権を守るためである。詳しくは 1 節で述べるが、例えば、インターネット上のサービスやアプリケーション等を私たちが使用する際、事業者が取得できる個人情報の利用に関して、「同意」取得の過程はかねてより存在するものの、実質を欠いていた。この状況下で、GDPR には、ユーザに「同意」を要求する場合に、「明瞭かつ平易な文言で、理解しやすく、かつ容易にアクセスし得る形で、その他の案件と明らかに区別できる方法によって明示されなければならない」[4]という但し書きが盛り込まれた。本稿で論じたいのは、ユーザ個々人の手で自らのプライバ

[2] 「個人情報の保護に関する法律」 https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000057&openerCode=1

[3] GDPR の保護対象とされる「個人データ」は、「personal data」の訳語である。GDPR における personal data とは、「識別された、または識別されうるデータ主体（data subject）に関するあらゆる情報」と定義されている。また、「識別されうる」とは、氏名、識別番号、所在地データ、オンライン識別子、または身体的・生理的・遺伝子的・精神的・経済的・文化的、社会的固有性などの中からいずれかによって、直接または間接的に識別可能であることを指す。さらなる詳細は GDPR 第 4 条第 1 項を参照のこと。

[4] GDPR 第 7 条第 2 項。

シーを保護することを目指すにあたり、GDPR が求めるような正しい「同意」取得の重要性を全面的に認めつつも、現実問題としてその実現はかなり困難である、ということである。

本稿の構成は以下の通りである。まず１節で、「同意」取得の問題点について概観した後、２節では、プライバシーポリシーの理解度に関するアンケート調査の結果から、記述の工夫と内容理解に関連性がないことを示す。３節では、どういった「わかりやすさ」を達成できれば、ユーザ自身が判断を下す形でのプライバシー保護が実現できるのか、について考察する。

1　同意取得とその問題

今や、「同意する」というボタンをクリックしなければ使いたいサービスを利用できない、という状況に遭遇したことのない人はほとんどいないだろう。その時私たちは、サービスの利用条件や契約について、あるいは、個人データの処理方法に関するプライバシーポリシーに対して「同意」を求められている。同時に膨大な量のテキストが表示される[5]が、画面をフリックして最下部の「同意する」を押すだけで、途中に書かれている文言を読んでいない。これが実質を伴わない「同意」である。

日本の個人情報保護法には、どういう状態になれば「同意」が成立しているとみなされるかについて、条件や定義が明記されていない。しかしながら、GDPR には定義も条件も明記されている。「同意」とは、「自由に与えられ、特定の、情報提供を受けた上での、不明確ではないデータ主体の意思表示」[6]であることとされていて、これらすべてを満たさなければ同意したとはみなされない。すなわち、GDPR 下では、データ主体が自己情報利用の同意請求に際し、何を求められているかを理解し、意思を持って個人が正しく選択し、自らのプライバシーを保護するために行動しなければならないことを意味している。自己責任が要求されがちなインターネット社会に適応し、じゅうぶんに慣れ親しんでいる人、あるいは、プライバシーや個人データの保護について一定の知識や関心がある人々にとっては、当然の要求であるように感じられるかもしれない。だが、最後の「不明確ではないデータ主体の意思表示」のためにユーザの「明白で積極的な行為」が要求される、という条件は、少なくとも現状より大きな負担をユーザに強いることになる。というのも、先ほど述べたような、利用条件などを記した画面の下方に「同意する」ボタンを置くようなタイプの同意取得は、ユーザがよく読まずに同意ボタンを押す可能性が高いため、「明白で積

[5] プライバシーポリシーを読むためにかかる時間が膨大であるという指摘は McDonald & Cranor (2008)、McDonald & Lowenthal (2013)等を参照のこと。こうした論文においては英語圏でのプライバシーポリシーが槍玉に上がっているが、日本語のケースでも状況はまったく同じである。

[6] GDPR 第 4 条第 11 項。

極的な行為」とはみなされないからである。

GDPR 以前の同意取得の方法に問題があったことは恐らく間違いないが、かといって、明示的な同意を逐一求めることにも無理があるという指摘は、Schermer らによって GDPR 策定以前から継続的になされていた[7]。彼らの一連の主張を端的にまとめれば、個人のデータ取得・利用に明示的な同意を義務付けると、データ主体が責任を持って同意しなければならない機会が飛躍的に増大し、さらには、何に同意しているかについてユーザが明確に理解しなければならず、結局のところ、一切を真面目に判断しな（できな）くなるであろうという予測である。

GDPR 施行以前でも、日本人ユーザが同意に際しての書面を無視して同意する理由の上位は、文章が長いことと、難解であることであった[8]。GDPR 以降、個人データの取り扱いについてより詳細な条件が付されることになった今、プライバシーポリシーの文言は長くなる一方[9]であり、一般的なユーザが提示される全てに目を通すようになるとは思われない。また、データ主体から正しく同意を得ているということを立証する責任は事業者の側にあり、同意取得のために書面を事業者側から提示するようなケースでは、「データ主体にとって、理解しやすく利用しやすい形式で、明瞭かつ平易な文言を用いて提供されるべき」[10]とされている。同意の書面が「難解であるから読まない」と言う層は、この変更によって同意のための書面を読むようになるかもしれない。だが、一般的なユーザが、わかりやすいと当人たちが思う形式の書面を読んだ場合と、わかりやすくないと判断した書面を読んだ場合では、プライバシーポリシーの理解度に差がないという調査結果がある。次節ではそれについて論じる。

まとめると、GDPR は、個人データの利用に際し、データ主体による正確かつ明確な同意を必要とする点で、GDPR 以前に守られなかったさまざまな個人データにまつわるプライバシーをデータ主体自身の手で守ることを可能にしたと言える。その意味では、かつての同意取得の問題点を改善しようと動いたと言える反面、同意のために処理しなければならない書面の分量が増え、同意を求められる回数が増えて処理が煩雑になり、とりわけプライバシーや個人情報についての知識が薄い、あるいはプライバシー保護に必要性を感じていないデータ主体にとっては改悪であるとも考えられる。仮に改悪であると感じる層が多数派であるとすると、実質的には、プライバシー保護が促進されたと言うことはできないだろう。

---

[7] Schermer, Custers and van der Hof (2014)において、GDPR 施行に向けた同意取得のあり方について、詳細な検討と提案がなされていた。

[8] この知見はアンケート調査から得られたものである。調査の詳細については、金森他(2017）を参照のこと。

[9] 金森他(2019)の調査によれば、GDPR 施行後、例えば Google のプライバシポリシーは 9388 文字から 24008 文字に増加している。

[10] GDPR 前文第 42 項。

2　プライバシーポリシーの理解度と「わかりやすいと感じること」には相関がない

プライバシーポリシー等の書面を読まずに同意している層が、GDPR 下においては、ある程度読んでから同意しなければならなくなったと仮定すると、そうした文書をデータ主体が「読む」ということを前提にした考察にも意義が生じる。また、「データ主体にとってわかりやすい」表示形式があるとすれば、それを明確にしておくことは重要であると考えられる。

以上のモチベーションに基づき、人々が日々の場面でプライバシーポリシーを読むにあたり、どういった形式のものをわかりやすいと感じるか、また、理解できたと調査主体が感じるかどうかの主観的理解度と、設問を回答することによる客観的理解度について、GDPR 施行後に質問紙調査を実施した[11]。実施方法や対象等、調査の詳細はここでは割愛するが、使用した形式は「通常の文章型」、「項目別にリンクし、自由に参照しながら表示する型」、「表形式で整理した型」、「難解語にハイライトと詳細説明へのリンクを付与した文章型」である。文言の内容はすべて同一で、「通常の文章型」以外の形式は、GDPR 施行に際して事業者が「ユーザにとってわかりやすい」と判断し、変更した形式の代表的なものである。

まず、読み手が「わかりやすい」と感じる形式には有意な差が存在している。表形式が 48.4%でもっとも支持され、項目別型が 26.4%、詳細説明型が 19.5%と続き、通常の文章型をわかりやすいと述べた人は 5.7%であった。次に、プライバシーポリシーを読んで、その内容を自分が理解できたと思うかどうかという主観的理解度は、表示形式の違いにかかわらず結果にほとんど差がなかった。ここからは、表示形式を「わかりやすい」と感じたからといって、内容が理解できたと思うわけではない、という読み手の特性が明らかになる。すなわち、プライバシーポリシーの表示形式を変更することは、主観的理解度には影響を及ぼさない。また、取得または利用される個人データの種類を、文章に書かれた内容から判定させる客観的理解度調査の結果にも、表示形式の違いによる有意な差は見受けられなかった。サンプルプライバシーポリシーを読むにあたっては、「わかりやすい」と思う文章を読んでも、そう思わない文章を読んでも、内容の理解度には関係がない。つまり、プライバシーポリシーや同意にかかる文書の内容が、読解力ではどうにもならない専門的な知識を要求している可能性や、表示形式にかかわらず、調査主体が結局のところ文章を読んでいない可能性などが示唆されるように思われる。

ただし、私たちがプライバシー保護のために真剣に読まなければならない文書は、日頃から使用しているアプリケーションやサービスのプライバシーポリシー等であるはずである。自分の生活に関係のない、アンケート調査で使用するサンプルプライバシーポリシー

[11] この説で議論に上がる質問紙調査の全貌については、金森他(2019)p. 4 以降を参照のこと。同一グループでの共同研究において、プライバシーポリシーの理解にかかわる質問紙調査を 2017 年から継続して行なっている。

を読んで設問に答えるという行為により、自身のプライバシーを守ることに直結したプライバシー理解の度合いを計測できているかどうかという点については、疑問の余地があると考えられる。

以上のことから、GDPR が求めている「わかりやすさ」に関して、表示形式を工夫するというアプローチは、データ主体のプライバシー理解とは関連がなく、自らのプライバシーを正しく守ることができるという目的達成に寄与しないことが明らかになった。結論としては、GDPR 下のデータ主体は、同意のための文章を読み、かつ理解できることが前提になっているものの、この前提が成り立たないようにも観察されるため、「読んで同意を得る」という方法とは異なる手段を提案しておくことに一定の意義があるように思われる。次節では、そのアイデアを提示したい。

3　データ主体が自らプライバシーを守るために必要な「簡単さ」

事業者が収集する個人情報や個人データによるプライバシーの侵害を避けるために、私たち一人一人が自ら保護しようと取り組まなければならないとされる理由は、プライバシーであると感じる範囲は個々人により異なる、というプライバシーの性質のためである。もし、プライバシーが、すべての人間にとって共通のものであるならば、法や制度で定義し、守るべき範囲を示せば現状のような混乱は生じないだろう。プライバシーと同じく、社会、文化、個人に対する相対的性質を持ち、プライバシーとは何かを一言で定義できずに、家族的類似性[12]のような形でしか捉えられない概念は、社会の中にはあまり存在していないように見受けられる。つまり、現状のデータ主体は、サービス利用のために（同意をしているとはいえ）自分のデータを勝手に取られざるを得ないのに、自らプライバシーを守る苦労を背負わされる、という二重苦に陥っている。その上で、インターネット上のサービスを利用したいという気持ちと、このコスト感の折衝の手近な落としどころが、プライバシーポリシー等の文章を読むというコストを支払わずにサービスを利用する、という着地点になっていると推測される。このとき、データ主体のプライバシーが結果的に犠牲になっていることは言うまでもない。人権を尊重する観点から、個々人それぞれに異なるプライバシーを自ら適切に守ることができるように、個人データを扱う事業者が配慮するという GDPR の目的からすれば、本末転倒の状態であろう。

サービスの提供に応じて発生するデータを事業者が利活用することは、社会にとって悪いことばかりではない。ビッグデータを用いた分析は、それ以前には見えていなかった実態を明らかにしたり、長期的な予測を可能にしたりする。また、ディープラーニングや AI の学習にも材料となるデータが必要である。よって、プライバシーに抵触しないものはな

[12] 『哲学探究』の 67 節において、ウィトゲンシュタインは、部分的に共通する特徴をもつものの集合体に名前がついている状態を指して「家族的類似(Familienähnlichkeit)」という概念を導入した。

るべく利用できる方がよい。こうした視点から、個人に関するデータも収集されているが、個人情報保護法や GDPR のような法制度によって、データ主体は保護されている。事業者が個人に関するデータを利用する際、匿名化や仮名化など、個人を特定できない形で利用できる技術と手法が日々更新されていることも、その成果の一つであると言えるだろう。ただし、こうした技術によるデータ加工は、データ主体のためというよりも、事業者が法に触れないために行われている。すなわち、多くのデータ主体は同意のための文言をよく読まずに同意するため、当人が思っている以上の情報を提供しているが、法の効力によってデータ加工が行われているために実質的に波風が立たないという状況である。個人データを扱う事業者が全面的に信頼できるならば、それでもプライバシー保護はできている、と言えるのかもしれない[13]。しかし、そうした事業者のすべてが全面的な信頼に値するかと言われると疑問が残る。だからこそやはり、個々人がそれぞれにプライバシー保護をしようと努力することは重要であると言える。

２節までの議論で、同意取得のための文章（主にプライバシーポリシー）を読まない人が多い、また、仮に読んだとしてもプライバシー概念を理解するとは限らないということが明らかになった。最後に、今後の社会において、ごく普通の人々が自らのプライバシーレベルを反映させたプライバシー保護を可能にするかもしれない手段について概観する。個々人が本当の意味でプライバシーを理解して判断できていると言えるために必要であると現時点で考えられる、同意取得の方法を以下にまとめる。

一つめは、利用したいサービスのプライバシーポリシー等をコンピュータないし AI に読み取らせて、取得・利用される情報の種類を明らかにし、それに応じてデータ主体がサービス利用の可否を判断できるようにしたアプリケーションによる同意取得である[14]。この方法は、データ主体が文章を「読まない」問題を回避することができる。だが、取得されても問題がないと判断した情報の組み合わせによって発生するプライバシー被害の危険性を、データ主体が認識できない可能性は残される。よって、個々人のプライバシー理解を向上させることが次の課題になるだろう。また、事業者が同意取得のために提示する文章は自然言語で記述されているため、コンピュータに自動で読ませるにあたっては、ある程度、処理上の困難が生じると予測される。

二つめは、同意のために文書を提示するのではなく、音声あるいはチャット形式[15]での

---

[13] プライバシーの概要を個々人が理解して保護することは困難なので、事業者（情報を取り扱う企業）が信頼を高めることで、理解の負担を軽減できる可能性については、川口(2017)で論じた。

[14] こうしたタイプの試みは 2006 年頃から見られるようになったが具体的なサービスには至っていない。たとえば、W3C Working Group, “The Platform for Privacy Pref- erences 1.1(P3P1.1) Specification”, November 2006, http://www.w3.org/TR/P3P11/など。今後は AI に読ませる方向性での研究が盛んになると筆者は予測している。ディープラーニングを応用したプライバシーポリシーの読み取りの簡易提示の研究には Harkous, Fawaz, Lebret, Schaub & Shin(2018)などがある

[15] サービス提供者ではなく、ユーザがチャットで質問をして意思決定するタイプのアプリケーションには既存のものが発表されている。たとえば、など。しかしながら、本論からも分かる通り、データ主体が

対話により、取得される情報の種類をデータ主体に提示し、利用の可否を判断させるアプリケーションである。これは、積極的な同意という GDPR の条件をクリアでき、かつ、読む負担も発生しない。２節での議論と齟齬があるかもしれないが、文章よりも動画や音声をわかりやすいと感じる層は多いと考えられる上に、対話形式になれば親しみやすさも増し、企業への信頼度にも好影響を与える可能性もあるように思われる。また、一つめの手法で問題となったプライバシー理解についても、対話形式であれば、その都度侵害事例等を提示しながら説明することも比較的容易であるように思われるため、リスク認知という問題点の解消にも期待が持てる。

以上のように、GDPR が要求するデータ主体のプライバシー保護状態を実現するためには、事業者によるデータ保護のための技術的な取り組みが重要である一方で、データ主体の負担を大幅に軽減するアプリケーション等の手法の開発と、プライバシーそのものについての理解を促進する取り組みが重要である。とりわけ後者については、現実的にどの程度の理解を達成すれば問題が生じないのかということについての考察や調査を進める一方で、本論で提示した「読まない」人を念頭に置いた対策と同様に、「理解を諦めている」人々に対する代替案を立てることも視野に入れる必要があるように思われる。具体的な手法や社会実装に向けての提案は今後の課題にしたい。

文献

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., & Shin, K.G., (2018), "Polisis Automated Analysis and Presentation of Privacy Policies Using Deep Learning," *27th USENIX Security Symposium*, August 15-17, 2018.

McDonald, A. M. & Cranor, L. F., (2008), “The Cost of Reading Privacy Policies," *A Journal of Law and Policy for the Information Society*. (online article)

McDonald, M. & Lowenthal, T., (2013), "Nano-notice: Privacy Disclosure at a Mobile Scale," *Journal of Information Policy*, vol. 3, pp.331-354.

金森祥子, 野島良, 岩井淳, 川口嘉奈子, 佐藤広英, 諏訪博彦, 太幡直也, (2017), “プライバシーポリシーを読まない理由に関する一考察,” *Computer Security Symposium 2017*.(PDF 論文集）

金森祥子, 野島良, 岩井淳, 川口嘉奈子, 佐藤広英, 諏訪博彦, 太幡直也, (2018), “プライバシーポリシー自動解析のための学習データ構築に向けた取り組み,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018) .（PDF 論文集）

金森祥子, 岩井淳, 川口嘉奈子, 佐藤広英, 諏訪博彦, 太幡直也, 盛合志帆, (2019), “GDPR

プライバシーについての専門知識を持たないケースがあるため、事業者の側からの質問に答える形式が望ましいと筆者は考えている。

対応のプライバシーポリシーに関するユーザ評価," 2019 年暗号と情報セキュリティシンポジウム (SCIS2019) .（PDF 論文集）

川口嘉奈子.(2017), "プライバシー保護と信頼," 千葉大学大学院人文社会科学研究科研究プロジェクト報告書, 第 312 集,『合理性の諸問題』, pp.16-26.

大谷卓史 (2015), "インターネットユーザーの個人データ取得と利用の「同意の危機」問題について,"電子情報通信学会技術と社会・倫理研究会研究報告, 2015-CSEC-70, 12 号.

Schermer, B. W., Custers, B., & von der Hof, S., (2014), *The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection*, Ethics and Information Technology, vol.16, pp.171-182.

Wittgenstein, L., (1958), *Ludwig Wittgenstein, Generally Known As Blue and Brown Books, Preliminary Studies for the "Philosophical Investigations,"* Basil Blackwell.

謝辞

本研究は、JSPS 科研費若手研究（B）(15K16692)の助成を受けたものです。

（かわぐち　かなこ／東京医療保健大学　医療保健学部　講師）