データ・プライバシーの再設計：人間とテクノロジーのインタラクションにとっての通知と同意の再構想

出典・凡例

本稿は，World Economic Forum, Redesigning Data Privacy: Reimagining Notice & Consent for human- technology interaction (White Paper, July 2020) の要約である。

原語を付す際には ( ) を用いた。また，重要と思われる箇所には下線を付してある。

エグゼクティヴ・サマリー

- テクノロジーの発展により，人間とテクノロジーの関わり方は変化しつつあるものの，インターフェイスがどのようなものであれわれわれはデータの収集・利活用について同意することを求められることがしばしばある
- しかし，現在の設計では同意は意味のないものとなっており，期待された役割を果たしているとはいえない
- プライバシーの文脈では，通知 (Notice) はある機関がある個人からどのような情報を収集しようとするかを諸個人に伝える主要な手段であり，同意 (Consent) はある個人がデータ収集の諸条件を知り，合意するプロセスであるが，本白書が示すように，現在のこうしたプロセスには多くの問題がある
- 本白書では 2 つの相補的な観点から検討を行う：もし通知と同意が目的にそぐわないとすれば，どのように改善できるか？　また，規約一覧の体制を超えたそれはどのようなものか？

Part A：人間とテクノロジーのインタラクションのためのデータ収集とデータ処理の諸課題

序

- ますます多くの国および地域がデータ保護およびプライバシー・ルールを立法の方式で行っており，そうした法律の多くは，個人に関してどのようなデータの収集および処理が合法となるかという点の条件を定めている
- データの取扱いについて許可を得るための最も古く，かつ最も直截的な方法は，当該データの対象となる個人から許可を得るというものであるが，データ量の増大とデータ処理の複雑化によってこの方法がいまだに適切かという点については疑問が残る
- 現在では，多くの研究者，政策形成者，国民および産業の間で，個人のデータ収集および処理への通知と同意の要件は，もはや人間が合理的に行うのが現実的には不可能であるという点でひろく意見が一致している
- 本白書では，われわれがどのようにして現在のようになったのか，今後われわれがどのようになるのか，また，どのように消費者と企業がデータ収集および処理へのプライバシー規範を改善しうるかについて，具体的に探究する

通知に関わる問題

- 利用規約を提示されると，人びとは反射的に「同意する」を選択しており，彼らはそれを読んでもおらず，理解してもおらず，多くはその目的を誤解している
- まず，そもそも利用規約は長すぎてほとんど全員が読むことができない
- 利用規約は基本的に法律家によって書かれており，多くの人にとって理解が困難である
- 通知が依拠している同意のモデルは，通知の頻度と遍在性に合っていない
- 現在の通知は，個人がそれをすべて読むほどの余裕がないタイミングで判断を迫るものとなっている

同意の重要性

- オンラインでのプライバシーの通知はありきたりで例外的ではない経験になっており，われわれはこれらの経験を医療的手続等のインフォームド・コンセントを要求する例外的な同意と区別している
- Nancy Kim によれば，同意とは「典型的には，次の 3 つの条件の存在ないし不存在に基づく結論づけである——すなわち，同意の意図的な表明，知識，および意欲／自発性という条件である
  - 同意は他方当事者に対し，ことばまたは行為を通じて表現されなければならず，その意思疎通は意図的でなければならない
  - また，同意する当事者はその内容を理解していなければならない
  - さらに，同意は自発的・任意的でなければならない
  - 本白書の文脈で言えば，データ収集に同意する個人は当該収集プラクティスを事前に理解し，強制や操作 (manipulated) を受けておらず自由に同意を行い，明瞭かつ積極的に同意を意思表示できる手段を与えられる状態であるのが望ましい
- Kim によれば，アメリカではデータ収集に関する現在の同意の在り方は契約法に由来するが，契約法では同意者の現実の知識は必要とされないものの，個人の自律への脅威の程度に応じて，同意する事項の知識についての把握能力，情報アクセス，通知が要求されるのに対し，多くのオンラインでの同意においては，個人が完全に読了および理解できる程度の通知が義務づけられることはない

どのようにして現在のようになったか？　通知と同意の前史

- 通知と告知は，20 世紀後半に発展した原則である公正情報慣行原則 (Fair Information Practices) の鍵となる要素である
- もともとの FIP では通知と同意は含まれておらず，そこでは目的の限定，個人に自身のデータへのアクセスを与えるという意味での透明性，データの訂正，諸機関の答責性，という諸原則に焦点を当てていた
- アメリカでは，連邦レベルでのあらゆる個人情報を網羅するプライバシー保護法がないため，FIP がオンライン領域でのデータ収集方法を統制する主要な手段となっている
- ヨーロッパでは，まず 1981 年に個人データの自動処理に係る個人の保護が採択され，その後データ保護指令が成立し，2018 年に一般データ保護規則 (GDPR) に代わった
  - こうした EU 法の発展の基礎にはデータ保護およびプライバシーに関する個別の権利があるが，GDPR では通知と同意は 6 つの法的基礎のうちの一つにすぎないものとされている
- アメリカとヨーロッパではそれぞれ異なるアプローチが採られているが，通知と同意は国際的に一貫した規範となっている
  - GDPR と CCPA の制定によって通知と同意モデルにおける欠陥を修正する必要性・緊急性がさらに高まっている

通知と同意を精査する

- プライバシー法学者のダニエル・ソロヴによれば，同意はほとんどすべてのデータ収集，利活用，および開示を正当化するものとなっており，多くの場面で同意は意味をなしていない
- また，オバマ政権期の大統領科学技術諮問会議 (PCAST) の報告書によれば，通知と同意は基本的にプライバシー保護の負担を個人の側に課しており，「権利」というものによって通常意味されるものと正反対になっている
- プライバシー法制においては設計を考慮しなければならず，その際には合理的行為者像ではなく現実に意思決定を行う人間を想定しなければならない

改革がない場合の問題

1. われわれはスクリーンをもたないテクノロジーの現実を適切に説明することができていない
   - 現在の法制度はスクリーンをもつテクノロジーを前提にしているが，現実にはスクリーンをもたないテクノロジーによっても情報の収集・利活用が行われており，通知と同意はそうしたテクノロジーにはそぐわないものである
2. われわれは企業がプライバシー保護のための革新的な解決策をみつけるのを適切に支援することができていない
   - 多くの機関ではプライバシー保護に関する事項を法律事務所等に委託して確認した上でユーザー・エクスペリエンスの設計を行うが，明確なガイドラインがないためにその課題は難しいものであり続けており，スクリーンをもつテクノロジーから移行することは最小限にとどまっている
3. われわれはデータの二次利用の現実を説明することができていない
   - 目的が代わる二次利用の場合につねに再同意を要求することは現実的ではない
   - そこで，次の 2 つの方法が考えられる
     - 人間の必要性を説明するために通知と同意の方式を根本的に再構築する
     - 通知と同意の方式を別のものによって根本的に置き換える：とくにスクリーンをもたないテクノロジーにおいて求められる
   - いずれにせよ，そうした解決策は人間を念頭に置いて設計されなければならない

Part B：別のアプローチを採るチャンス：なぜわれわれは人間中心の設計が必要なのか

通知と同意の再設計：人間中心の設計アプローチ

- 既存の通知と同意の方式は人間の心理の複雑な現実を考慮していない
  - それが前提としているのはプライバシー・ポリシーを読んで理解できる古典的な合理的個人モデルであるが，行動経済学や社会心理学の研究によれば，人間の選択は多くの非理性的要素によって影響を受けていることが明らかとなっている
- プライバシーに関するプラクティスを再構想する一つの方法は，ユーザーを構成する人びとに関する考え方を変えることである
  - 現在の通知と同意アプローチは経済的合理性を計算する消費者を想定しているが，現実の人間の活動にはさまざまなものがあることから，われわれのアプローチではプライバシーを消費者保護だけでなく人権としてとらえている

- 鍵となる課題は，①包括同意を与えてプライバシーへの支配をすべて委ねることと，②データが利活用されるたびに毎回「ミクロ同意」を要求し，毎回の同意の内容を理解することができないという帰結に至ること，という両極の間に妥協点を見出すことである

人間中心の設計とは何か？

- 人間中心の設計 (human-centred design) とは，アメリカの研究者である Don Norman の寄与によるものであり，HCD とは「ユーザーのニーズと利益に基礎をおく哲学であり，製品を使いやすく，理解しやすくすることに力点を置くものである」
- 人間中心の設計による通知と同意アプローチは，必ずしも適切ではないコンテクストを読むべき義務に依拠するモデルの限界や，データ収集自体に内在する倫理に関する問題を提起する
  - そうであるがゆえに，こうしたメカニズムにより誰が利益を受けるのか，誰が排除され，誰が負担を課されるのか，といった点について批判的な問いを提起することが重要となる

集団的プライバシー

- プライバシーは個人に着目することが多いが，必ずしも個人に限られるものではなく，集団的なものでもありうる
  - たとえば人びとが自身に関する情報を共有すると，家族，友人，同僚，近隣住民の事柄までもが明かされることがある
- 通知と同意の用い方は，利用の具体的な背景的状況および個人よりも幅広い人口の集団的プライバシーにとっての課題によってさらに陰影をつけられる

別の諸モデル：型にはまらずに考えてみる

- 通知と同意の別のモデルは，相対的に世界全体で受け容れやすいものであり，テクノロジー中立（スクリーンの有無を問わないもの）であり，可能なかぎり倫理的に基礎づけられるものでなければならない
  - つまり，収集の目的を尊重することに加え，最も権力をもたない (the least privileged) 人びとのニーズと脆弱性を認識することが必要である

グローバルなテクノロジー中立的アプローチの必要性

- GDPR の諸原則はヨーロッパ以外の諸国においても事実上のグローバル・スタンダードとなっている点から，その採択はデータ保護とプライバシーにとって国際的なゲーム・チェンジャーであった
  - GDPR には既存の通知と同意の枠組みを明確化する通知と同意のメカニズムのためのガイドラインが含まれており，当該サービスにとって不可欠でないかぎり同意をサービスの条件として備え付けてはならないことを明確にしている
- 他方で，アメリカの CCPA はプライバシー・ポリシーの提示とそれへの同意について小さな改善しか要求していない
- われわれは，通知と同意に対する将来の変更は，最大限の程度においてマルチステークホルダーのグローバルな規制アプローチの一部にならなければならないと推奨する

明確な倫理的フレームワークの構築

- GDPR と CCPA に共通するのは，公正情報慣行原則における要素，つまりデータ保護のために個人の支配と人格的自律に主として価値を置いているという点である

- しかし，先述のとおり，データは生活におけるさまざまな側面に影響を与え，個人にとどまらず社会等に影響を与えることも多いことから，このような価値づけには不完全な点がある
- われわれが明らかにしたのは，規制を嚮導する倫理的フレームワークを明らかにする必要性と，テクノロジー・デザインにおいて通常考えられるよりも幅広い価値を考えることの必要性である

同意と社会的正義

- 将来の設計にあたっては社会における最も脆弱な人びとのニーズと懸念を考慮する必要があり，とくにデータ収集による負の影響を認識する必要がある
  - こうした考慮をしなければ，既存の社会的分断を強化し，加速させる危険を負うこととなる

政策形成における業界〔慣行〕の重要性

- 業界規範は政策形成に先行することがしばしばあるため，上記のような難点の解決にとって重要となる
  - 業界を考慮しなければ人びとにとってのプライバシー保護の改善も，ビジネスやより広い社会にとってのイノベーションも改善されずにコンプライアンスの競争を行うこととなってしまうことから，業界は，こうした対話のあらゆる段階において考慮されなければならない

われわれはどのように前進するのか？

- 通知と同意メカニズムはデジタル環境において多くの者にとって重要となることから，通知と同意のモデルはもはや法の領域のみにとどまるものではない
  - それは本来的に人間とテクノロジーの関わり合いの問題であるから，人間とコンピュータの関わり合いに関する問題の専門家および学者や，理想的には公共政策および倫理の専門家および学者を必要とする問題である

Part C：探究すべき諸観念

よりよい手段の特徴は何か？

1. **主体性 対 ユーザビリティ**
   - 既存のメカニズムはユーザー・フレンドリーでないだけでなく，彼らに交渉や撤回を許さないため，消費者に主体性を与えていない
   - 通知と同意のメカニズムのデザインを再構想することは必ずしもユーザーの主体性を取り戻すことになるとは限らないが，将来のそうしたメカニズムは，たとえば同意の条件やオプトインの要件について交渉する力をユーザーに与えるものでなければならない
2. **設計に着目した共同とツール**
   - われわれは，デザイナー，技術開発者，パブリック・セクターなどの利害関係者の交流を奨励することでグローバルな公共的参加に焦点を当てることができる
3. **現実の選択**
   - 選択を撤回する選択を援助すべきである
   - つまり，同意の暫定性，一時性に注意を置く通知と同意の設計を行うべきである

探究すべき 9 つのアイディア

1. **政策立案者のためのデータ可視化ツール**

- プライバシー政策やデータ保護メカニズムの効果は抽象的に議論されることが多く，データ収集の現実の影響を明示する必要があるにもかかわらず，実際には多くの政策形成者や政治家には技術および設計の専門家が欠けているため，規制等の在り方に負の影響を与える可能性がある
- データ可視化の目標は，政策立案者に対して，規制の結果が個人に対してどのように影響するかを例証するために，プロトタイプ，グラフィックおよびビジュアルの例を作るためのツールを与える点にある

2. 害を精査するプロセス

- 通知に関して，アメリカにおける消費者は企業の利益を保護する契約に署名しているのに対し，EU ではデータを収集・処理しようとする企業が適切で合法的な根拠を選ばなければならないとされている (GDPR 6 条 1 項)
- リスク精査は企業にとってよく議論された概念である一方で，潜在的なプライバシーのリスクについてはそうした議論がなされてこなかった
- このリスク精査のプロセスは，GDPR の下での正当な目的を選ぶ場合と近似し，それによればデータ処理者は事前にデータ処理による影響を精査する必要がある

3. デフォルトでの目的制限

- 目的制限とは，個人情報の収集と利活用は当初予定していた目的に限定され，ミッション・クリープは許されないという概念である
- この概念を発展させて，一定の有害な二次利用を違法とすれば，個人にはデータ収集・利活用の選好についてかつてないほどの自律が与えられることとなる

4. 建設的な規制と責任あるイノベーション

- 政府機関は企業に対し，責任ある，また倫理的なデータ収集・利活用を目指すプラクティスを採用するようインセンティヴを与えることができる
- こうした建設的な規制は業界主導の行為指針によっても行われうる

5. スマート・シティにおけるプライバシー・バイ・デザイン

- スマート・シティにおけるインフラの施行にあたり政策立案者は，居住者に対してデータ収集への同意と充分な同意のメカニズムを与え，彼らに選好について交渉する手段を与える必要があるという課題に直面する
- スマート・シティは，設計の正義に着目したプロセス (design justice-focused process) を通じて市民に関わることによって，プライバシーと共存することができる
- また，スマート・シティでは透明性といった原理も必要とされ，居住者は自信の個人情報が収集・処理がいつ，どこで行われるかを知る権利がある

6. 公共空間における追跡への自律

- 公共空間における自由な表現は開かれた社会に不可欠であるが，公的機関および私的機関の双方によってなされる公共空間での監視やデータ収集は萎縮効果を生じさせうる
- こうした問題に対処するために，個人情報の収集および利活用に関する個人の選好を，スマートフォンベースのエージェントやウェアラブル・デバイスに設計に組み込むことがありうる

7. データ・トラスト

- データ・トラスト (Data trusts) は，公正な仕方で個人情報が収集・処理される方法を提供し，データ・トラストは信託された機関によって監督される
- 現在のところ，データ・トラストをどのように定義するかについては一般的コンセンサスはない
  - 英国では「公正，安全，衡平な方法でデータを共有する方法」と定義され，こうしたモデルは実践的にはデータアクセスの技術的なメカニズムだけでなく法的条件および管理プロセスを特定する可能性がある

    - 他の定義では，当該トラストに対して民主的コントロールをもち，その利益に対して持分をもつ構成員のためにデータを管理する相互的機関とされる
    - また，データ・トラストは信託という特定の法的構造を意味することもある
  - さまざまなデータ・トラストのモデルはプライバシーのジャーゴンに精通していない人びとや必ずしもプライバシーの問題に対して自身の決定を行う時間と労力がない人びとのためにある
    - 一つの懸念は，データ・トラストがどのようにして消費者の利益と選択を誠実に代表しうるか，という点についてである
    - 別の懸念はデータの安全性の確保という点についてである

8. アルゴリズムの説明可能性

- 通知に基づいて同意が与えられた場合，通知はその後当該データについてどのようなことが起こるかについてその通知は誠実に説明していることが前提とされているが，「ブラックボックス」のアルゴリズムによってこの前提は崩され，個人に意味のある同意を期待するのは現実ではなくなるかもしれない
- したがって，ブラックボックスのアルゴリズムが適切でない状況やコンテクストを確定することが必要となるだろう

9. パーソナル・ユーザー・エージェント

- データの収集・利活用のたびに同意を求めることは現実的ではないためわれわれの個人としての主体性を損なっているという問題があるが，これを解決する一つの方法は，ソフトウェアベースの仮想エージェントを作り，個人のプライバシーへの選好をやりとりすることで仲介する役割を果たしてもらう，というものである
    - 現実には，こうしたエージェントはユーザーのデバイス上やサードパーティのサービス上において，ユーザーのデジタル・アイデンティティに結びつけることで運用されることとなる
- こうしたアプローチには個人が自身のプライバシーへの選好について事前に同意することが不可欠であり，そうした選好にもとづいてエージェントがプライバシー・ポリシーを処理して同意していくこととなる
- こうしたエージェントの提案は新しいものではなく，すでにさまざまなものが提案されてきたが，スマートフォンやクラウド・サービスの普及によって非常に現実的なものとなっている
    - 自立的エージェントは B2B の場面ではすでにひろく採用されており，研究者はこの概念に証明を与えてきた

結論

——では，どこへ向かうか？

- 通知と同意の枠組みを再設計するためのよりニュアンスに富んだ，多分岐のツールを生み出すには，さらなる研究が必要であり，またマルチステークホルダーにおける共同アプローチによるビジネスの果たす役割も重要となる
- 現在の通知と同意の目的も価値のあるものではあるが，人間とテクノロジーのインタラクションについては有効な同意を行うことができないという点で時代遅れとなっている
- テクノロジーの変化とそれに伴う個人情報収集の増加を考慮すれば，人びとがあらゆる個人情報に有効な同意を行うものと期待するのは合理的ではない
- 人間中心の設計アプローチを採り，スクリーン上の契約書のようなモデルに依拠するのを見直すことで，より適切な目的のデータ収集・処理に向けた別のモデルを提示できる

（松本　有平）