2ZD-03

デジタル時代におけるプロファイリングの課題と規制の方向性

上條英夫†
情報セキュリティ大学院大学

１．はじめに

デジタル化の進展に伴い膨大なパーソナルデータの取得・蓄積が進み、AIの高度化と相まって、個人のプロファイリングが可能になっている。こうしたデジタル技術を活用した新たな利用分野では、民間主導で自主ルールが策定、運用されることが望ましいとされている。本稿では、プロファイリングに関連する各種AIガイドライン、GAFA等プラットフォーマーの対応状況および法規制の動向を確認し、これらから見える課題と規制の方向性を探る。

２．AIに関する各種ガイドライン

AI の適正な利用に向け、日米欧における様々な組織・団体から、AI 原則、AI 活用指針といった形のガイドライン（以下「AI ガイドライン」と総称）が提示されている。各 AI ガイドラインが提示する尊重すべき価値は次表のとおりである。いずれも人間の尊厳やプライバシーの保護、AI のブラックボックス化を防ぐための透明性・アカウンタビリティなど、現代社会を構成する基本的な価値が共通して重視されており、AI の適正な利用に向けて、尊重すべき価値に関する共通の認識ができつつあると考えられる。

AI ガイドライン比較表[1]

ガイドライン名称	アシロマAI原則	倫理指針	人間中心のAI社会原則	倫理的に調整された設計（第1版）	信頼できるAIのための倫理ガイド	AIに関する理事会勧告	AI利活用ガイドライン
組織・団体	Future of Life Institute	人工知能学会	内閣府	IEEE	欧州委員会	OECD	総務省
公表時期	2017/02	2017/02	2019/03	2019/03	2019/04	2019/05	2019/08
人間中心			○		○	○	○
人間の尊厳	○	○	○	○	○	○	○
多様性、包摂	○	○	○		○	○	○
持続可能な社会	○	○	○		○	○	○
国際協力			○		○	○	○
適切な利用				○		○	○
教育・リテラシー			○	○	○	○	○
人間の判断の介在	○	○	○		○	○	○
適正な学習					○	○	○
AI間の連携						○	○
安全性	○	○	○	○	○	○	○
セキュリティ			○	○	○	○	○
プライバシー	○	○	○	○	○	○	○
公平性		○	○		○	○	○
透明性	○	○	○	○	○	○	○
アカウンタビリティ	○	○	○	○	○	○	○

３．プラットフォーマーにおける対応

プラットフォーマーの代表である GAFA の AI 利用に関する指針（以下「AI 利用指針」と総称）の公表状況を確認したところ、Google が 2018 年に“AI at Google: our principles”として公表しているのみで、他は公表していない。このため、AI 利用指針を公表しているマイクロソフト、IBM を加え 3 社について調査した。次図は各社の AI 利用指針を「AI ガイドライン比較表」の項目にならい筆者がまとめたものである。

AI 利用指針比較表

	Google	Microsoft	IBM
AI利用指針名称	AI at Google: our principles	The Future Computed －Artificial Intelligence and its role in society	Everyday Ethics for Artificial Intelligence
公表時期	2018/06	2018/01	2018/09
人間中心	○	○	○
人間の尊厳	○	○	○
多様性、包摂	○	○	○
持続可能な社会	○	○	
国際協力		○	
適切な利用	○	○	○
教育・リテラシー	○	○	○
人間の判断の介在	○	○	○
適正な学習	○	○	○
AI間の連携		○	
安全性	○	○	○
セキュリティ	○	○	○
プライバシー	○	○	○
公平性	○	○	○
透明性	○	○	○
アカウンタビリティ	○	○	○

各社の指針とも AI ガイドラインで尊重すべきとされている項目を概ね網羅しており、調査した 3 社が AI 利用に当たってこうした価値を重視していることが伺える。一方、プラットフォーマーの代表とされる GAFA でさえ AI 利用指針を公表しているのは 1 社のみで、他企業も十分な広がりをみせている状況ではない。また、AI 利用指針を公表していても利用者にはその遵守に関する実態は分からないという課題がある。

次に GAFA 各社プライバシーポリシーのプロファイリングに関する記載についても確認した。Amazon は特にプロファイリングに関する記載はない。Apple は「Apple がアルゴリズムの使用やプロファイリングにより、お客様に大きな影響を与える決定を行うことはない」との記載があるのみである。Google、Facebook は「カスタマイズしたサービス・広告の提供のため」といったプロファイリング実施目的の記載があるが、どのようなアルゴリズムによりどのようなプロファイリングが行われているか、プロファイリングされた結果を確認しプロファイリング自体

† Hideo Kamijo, Institute of Information Security
[1] AI ネットワーク社会推進会議「報告書 2019 別紙 2 AI ガイドライン比較表」を元に筆者加工

を拒否したり、プロファイリングされた結果を訂正したりする方法については記載されていない。各社ともプロファイリングについて十分な開示がなされているとは言い難い。

４．日米欧のプロファイリング規制の動向

続いて日米欧の法規制について概観する。

●欧州：EU 一般データ保護規則(GDPR)

GDPR は特別な規定を設けてプロファイリングに係わる個人の権利を明確化している。「異議申立権（21 条）」では、「当権利が行使された場合、データ管理者は利用者の利益等を上回る正当な理由を示さない限りプロファイリングを中止しなければならない」としている。また、「自動処理のみに基づき重要な決定を下されない権利（22 条）」は、プロファイリングのような自動処理のみに基づいて、本人に法的効果を与える、あるいはそれに類する重大な影響を与える決定を下されない権利である。GDPR はプロファイリング一般についてはオプトアウト方式を採用し、本人に法的効果あるいはそれに類する重大な影響を与えるプロファイリングは厳格なオプトイン方式で規制している。

●米国

現状、連邦レベルでプロファイリングを法的に規制している状況にはないものの、ニューヨーク市で行政が使用するアルゴリズムの公正さを監視するタスクフォースが設置されたり、カリフォルニア州プライバシー権法でプロファイリングの実施に係る権利義務が明記されたりする等の動きがある。

●日本

2015 年の個人情報保護法改正のベースとなった「パーソナルデータの利活用に関する制度改正大綱」において、プロファイリングについて、「継続して検討すべき課題とする」とされたが、その後プロファイリングに関する一般的な法律は制定されていない。

５．課題と規制の方向性

以上見てきたように、プロファイリングは、プライバシーひいては基本的人権や自由、差別防止といった現代社会における基本的な価値に大きなダメージを与え得ることから適正な利用が求められ、各種ガイドラインが提示されるようなってきている。デジタル技術の新たな活用分野では、民間主導で自主ルールが策定・運用されることが望ましいとされるが、自主ルールを公表している企業は限定的であり、公表していてもその遵守に関する実態は外部からは把握できない。現代社会が重視する基本的な価値にプロファイリングが与える影響の大きさ、誤った結果が導出される容易さ、プロファイリング実施状況を外部から把握することの困難さ等を考えると、さらに踏み込んだ実効性のあるルールを早急に整備すべきである。

ルール整備に当たっては、ルールの位置づけに関して大きく 2 つの方向性が考えられる。第 1 は GDPR のようにプロファイリングについて法律で厳格に定め、利用者の権利を明確にするとともに、権利の侵害があった際は罰則を課すという方向性である。第 2 は原則によりガバナンスを効かせるという方向性、すなわちプロファイリングに関してプライバシー保護や透明性等の原則を定めるが、原則の実施方法は基本的に企業の裁量に委ねるという方向性である。プロファイリングにより利用者の権利が侵害された際の影響の大きさを踏まえると、原則によるガバナンスは一般的に企業に対するインセンティブを機能させにくく実効性の確保が容易でない[2]ため、技術革新のスピードに柔軟に対応しにくいといった課題はあるものの、第 1 の法規制による対応が望ましいと考えられる。技術革新のスピードへの柔軟な対応については、たとえば個人情報保護法のように 3 年毎に見直すといったことを明文化することで一定の緩和が可能であろう。また、プロファイリングにおける不可視性の克服、すなわちルールが守られていることの保証に関して、利用者が信頼できる制度の構築という観点も重要なポイントになる。今後こうした課題に対する GDPR 等先行事例における対応等につき調査を進め、考察を深める予定である。

参考文献

[1]AI ネットワーク社会推進会議 「報告書 2019」
[2]山本龍彦 「ビッグデータ社会とプロファイリング」（論究ジュリスト 2016 年夏号）
[3]AI 利用指針
Google: https://ai.google/principles
Microsoft: https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/
IBM: https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf
[4]GAFA プライバシーポリシー
Google: https://policies.google.com/privacy?hl=ja
Apple: https://www.apple.com/jp/legal/privacy/jp/
Facebook: https://ja-jp.facebook.com/privacy/explanation/
Amazon: https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=201909010

[2] 原則によるガバナンスの例としては、強制力が乏しいもの（プライバシーマーク制度、ISMS、環境監査等）から、法的に実施が義務付けられている訳ではないが実態として一定の強制力をもつもの（コーポレートガバナンス・コード、Apple・Google のアプリ審査基準、業界団体による標準・基準等）まで幅があるが、一定の強制力を持たせるには企業が従わざるを得ない環境整備が必要である。