集中管理型AIから分散管理型AIへ

From Centralized AI to Decentralized AI

東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター教授
橋田　浩一

1986 年より 2001 年まで電子技術総合研究所。その間 1988 年から 1992 年まで（財）新世代コンピュータ技術開発機構に出向、2001 年から 2013 年まで産業技術総合研究所。2013 年から現職。専門は自然言語処理、認知科学、サービス科学など。日本認知科学会会長、言語処理学会会長等を歴任。

1 監視する AI

アメリカの GAFA（Google、Apple、Facebook、Amazon）や中国の BAT（百度 Baidu、阿里巴巴集団 Alibaba、騰訊 Tencent）などの巨大なテクノロジー企業が利用者からパーソナルデータ（PD）を無料で集めてターゲティング広告等に使って儲けていると批判されています（これは Apple には当てはまりませんが）。事業者がそのように PD を収集し分析することにより集中管理型 AI（centralized AI; CAI）で消費者の行動を予測し誘導するような経済システムをズボフ（Zuboff, 2019）は**監視資本主義**と呼びます。

監視資本主義においては、消費者がしばしば意図せずに提供した PD を事業者が活用して消費者の行動に介入します。購買の履歴や SNS の投稿などのデータを分析することによって、本人も気付いてないかも知れないいろいろなことが間接的にわかるからです。たとえばアメリカのスーパーマーケットの Target は、無香料の石鹸とかカルシウムやマグネシウムのサプリメントなど 25 種類ほどの商品の購買データから女性が妊娠している確率を計算したり予定日を推測したりするアルゴリズムを開発し、それによってある女性が妊娠していると判断してベビー服やベビーベッドのクーポン券を送ったところ、彼女の父親が「うちの娘はまだ高校生なのに妊娠を勧めてるのか？」と言ってどなり込んで来たそうです（Duhigg, 2012）。土曜日のデートを控えて金曜日にそわそわしている男の子に高価なジャケットを売り付けるというようなこともできそうです。クーポン券を受け取った女の子は自分が妊娠していることを他人に知らせるつもりがないでしょうし、男の子の方も自分がうっかり高いジャケットを買ってしまいそうなくらいそわそわしていることを誰かに明かそうとは思っていないでしょうが、事業者がそういうことを知って消費者の行動に介入するのが監視資本主義です。

購買だけでなく選挙での投票などの行動も介入の対象になります。2016 年 6 月にイギリスの国民投票で EU 離脱（ブレグジット）が決まり、11 月にアメリカの大統領選挙でトランプが当選しましたが、いずれの勝者も選挙コンサルティング会社のケンブリッジ・アナリティカ（CA）を使っていました。大統領選挙に対するロシアによる介入への CA の関与をアメリカ議会が調べていることが 2018 年 5 月に報道されたことに端を発して、CA は不正に取得した有権者の PD を使って投票行動を操ったとして激しく非難され、2018 年に解散しました。PD の不正な取得というのは、Facebook と連携するアプリが Facebook の「友達 API」を使って利用者の友達の情報も集めていたということですが、これはそんな API を提供していた Facebook の落度も大きいですね。Facebook もそう思ったのか、この API によるデータ収集は 2015 年以降できなくなっています。

一方、CA は PD の分析によって有権者を多数のグループに分け、各グループに適したメッセージを送ることによって投票を操作したとされています。その方法はあまり効果がないと考える人も多いようですが、たとえ現在得られるデータを現在の技術で処理して大した効果がないとしても、近い将来得られるデータを近い将来の技術

で処理したら効果が大きいことは十分にあり得ます。また、SNS が普及したせいで極端な意見が広まりやすくなっているのだとしたら、意見の伝播を操作して世論に影響を与えることができそうです。

以上のように監視資本主義の技術的な基盤は PD の集中管理に基づく AI による個人適応(パーソナライゼーション）です。この個人適応は、商品・サービスの提供を各個人に適応させるだけではなく、個人の行動を操作することを含みます。そのために PD を使うのですが、多くの場合、各個人は自分のどんな PD がどうやって取得されどう処理されて自分にどんな介入や操作がなされているのかよくわかりません。個人が自律的に意思決定し行動するという民主主義の前提が脅かされるわけです。

監視資本主義の本来の目的は金儲けですから、個人の自由に基づく民主主義を CAI が脅かすと言っても、それが権威主義政治に直結したりするわけではありません。しかし、監視資本主義によって育まれた CAI を権威主義的な統治に利用することは可能であり、それはすでに中国などで行なわれています。ハイルマン（Heilmann, 2016）は最近の中国の統治体制をデジタル・レーニン主義（digital Leninism）と呼んでいますが、これは、集中管理型のデジタル技術によって社会主義をアップグレードしているという意味です。

たとえば Alibaba の芝麻（ジーマ）信用は、購買や SNS での発言や職業や交友関係などの PD に基づいて各個人を点数で評価するシステムです。その点数が高いとローンの金利が安くなったりホテルのデポジットが免除されたりする一方で、点数が低いと高い買い物ができなくなったりします。芝麻信用を含む 8 つの民間の信用サービスは中国人民銀行の支援の下で 2015 年に始まったのですが、その支援は 2017 年に打ち切られました。それらのサービスがあまりにもうまく行って影響力が強まったため、その力がさらに強まるのを中国政府が好ましく思っていないということでしょう。一方、中国政府が運用する「社会信用システム」は国家のシステムですからその有効範囲はもっと広く、たとえば点数が悪いと飛行機に乗れなかったりします。交通違反を犯すと街頭ビジョンで晒しものになったりすることもあるようです。

父親が子供のために良かれと思って本人の意思によらずに子供に介入・干渉するように、強い立場の者が弱い立場の者のためとして本人の意思を問わずに介入・干渉することをパターナリズムと言います。上記のように国家が個人の行動に介入するのは典型的なパターナリズムですね。大屋（2019）が指摘するように、習近平の戦略はその点でマルクス主義でも毛沢東思想でもなくレーニン主義です。知的に成長した労働者が資本家による搾取に対して革命を起こすというのがマルクスの描いたシナリオだったようですが、労働者が自ずと成長することはないと悟ったレーニンは、エリートが労働者を先導して革命を成就すべきだという「前衛理論」を主張したわけです。それは、農民大衆の意見に正統性の根拠を求める毛沢東思想とも異なります。また、スターリン主義ではなくレーニン主義であるのは、暴力によるあからさまな強権政治ではなくて、デジタル技術によって洗練されたソフトな介入を行なうということでしょう。

しかし、レーニン主義によって中央集権的な体制を確立し維持するには集中管理 AI によるソフトな介入だけでは足りない場合もあります。チベットやウイグルや香港はソフトに介入するだけでなく暴力的に弾圧せざるを得ないわけです。たとえば、中国の正式な国家統計である「中国統計年鑑」（国家統計局，2021）によれば、2017 年から 2019 年にかけて、中国の他の地域では少数民族の人口がだいたい微増しているのに対し、新疆ウイグル自治区だけ少数民族の人口が 1,654 万人から 1,490 万人に約 10% も減っており、何か尋常でないことが起こっているようです（平野，2021）。産児制限なんかでは人口が 2 年で 10% も減るはずがありません。ヒトラーはユダヤ人を絶滅させようとしましたが、それと同じようなことが行なわれているのかも知れません。

ターゲティング広告で自分に合った商品やサービスが簡単にわかるとしたらそれ自体は良いことでしょうし、信用スコアも人々のモラルを高めて社会の効率を良くしている面が確かにありますから一概に悪いとは言えないでしょう。しかしどう考えても虐殺や弾圧はいけません。そして、監視資本主義で使われている CAI が、そのような蛮行のための監視だけでなく蛮行の隠蔽や正当化にも活用されています。さらに、権威主義国家のみならずテロリストや悪徳企業による虐殺や搾取に使われる恐れもあります。

このように CAI にはさまざまなリスクがあります。

ほぼあらゆる技術が使いようによっては弊害を生むわけですが、CAI が他の技術よりやっかいなのは、そのリスクを管理し弊害を防ごうという合意が成り立たないことです。公害などはどの国にとっても望ましくないので各国内での合意に基づいて法律などが整備されることにより減ってきました。また、世界規模の核戦争や温暖化には勝者がなく、全人類が甚大な損害を被るので、それらを回避するために世界全体が協力し合うことが可能と考えられます。しかし、グローバル企業や国家による CAI の活用には勝者があるので、そのリスクを共同で管理することについて世界中の企業や国々が合意することはあり得ません。

個人に介入しその行動を操作する CAI は巨大な利益や権力を生みますが、操作される人々は意思決定の自由を失っているかも知れません。それどころか弾圧されたり虐殺されたりする人々も現にいます。そのようなことが世界中に広がるのは何としても防がなければならないと思いますが、それは可能でしょうか？

2 懐に入る AI

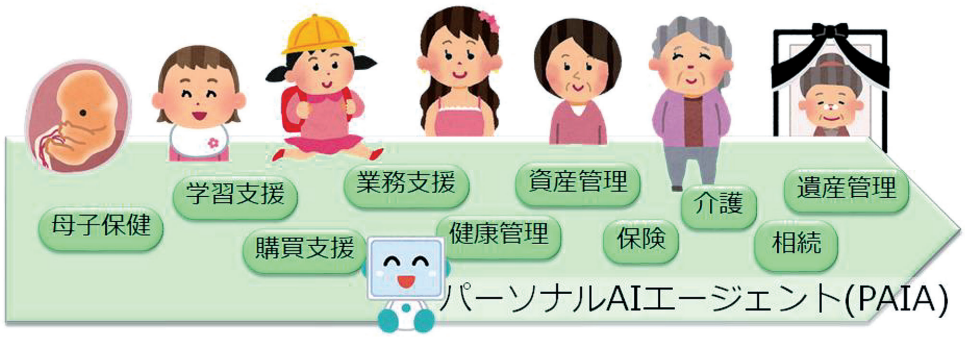
集中管理型 AI（CAI）は企業や国家などの機関が運用し、個人に介入します。CAI が人権を侵す恐れが大きいのは、このように AI の運用者と介入の対象が異なるからです。したがって、その恐れを低減させるには運用者と介入対象を一致させる必要があります。介入の対象はいずれにせよ個人なので、運用者と介入対象が一致するということは、個人が運用する AI が本人に介入するということです。つまり、個人に属する AI（**パーソナル AI エージェント**；PAIA）が本人に介入するということです。

PAIA は利用者本人にとっても AI の提供者にとっても価値が大きいはずです。つまり、本人にとってより大きな価値を生み、したがって市場メカニズムにより、事業者にも CAI より大きな収益をもたらすでしょう。PAIA が CAI よりも付加価値が高いのは、CAI よりも多くの PD をフル活用して利用者本人に介入できるからです。CAI はいくつかの点で個人のことを本人よりも良く理解するでしょうが、PAIA の方が CAI よりもはるかに良く本人のことを理解し、したがって本人の行動に深く介入できるはずです。

PAIA が CAI よりも多くの PD を使うことができるのは、他者より本人の方が多くの PD を取得できるからです。たとえば Google は大量の PD を集めていますが、そのために Chrome ブラウザや Google 検索や YouTube や Google マップやポケモン GO や Google アナリティクスなどいろいろなサービスを駆使しています。Google アナリティクスは Web サイトの利用状況を分析するツールで、日本の自治体なども含むいろいろな機関の Web サイトが無料で使っていますが、そのような Web サイトへのアクセスの履歴は（Chrome 以外のブラウザでアクセスしても）Google に送られます。しかし、そもそも PD は本人に由来するものですから、Google が取得するよりも本人が取得する方が技術的に簡単で倫理的・法律的にも適正です。本人の情報端末やセンサから PD を取得して本人の手もとで保管すれば良いわけです。さらに、たとえ GAFA や BAT でもひとつの企業が取得できる PD はいくらいろいろあると言っても範囲がかなり限られます。たとえば、Amazon ショッピングアプリでの購買のデータは Google にはわかりません。楽天でハチミツを買って Amazon でオムツを買ったら、ハチミツを買ったことを Amazon は知らず、オムツを買ったことを楽天は知りません。センサデータなどを暗号化してクラウドに保存したら他者にはその内容がわかりません。

さらに、利用者本人の行動支援が PAIA の主要な役割ですが、そこではほとんどの場合 PD を他者に開示しないので、PD を安心してフル活用できます。CAI によるサービスでは PD を CAI の運用者に開示しなければならないので、たとえば恥ずかしくて他人に言えない黒歴史みたいな PD は使いにくいわけですが、PAIA による行動支援にはそんな制限がありません。他者に明かせない機微な PD は価値が高いことが多いので、CAI よりも PAIA による行動支援の方がその点でも価値が高いと考えられます。下図のように、PAIA は利用者本人の誕生前から死後にわたる広い意味での人生において、本人の多様な PD を駆使して本人を支援し、また本人の行動変容を促してその人生をより良いものにするための行動の最適化を図ることになるでしょう。

本人に集約された PD をフル活用し、その PD を原則として他者に開示せずプライバシーを守りながら本人を支援することによって、PAIA は CAI よりも個人の



行動に深くキメ細かく介入することができます。一般に、サービス受容者本人の行動に深く介入することによって個人サービス（個人が提供者または受容者として直接関与するサービス）の価値が高まりますから、PAIA による支援は最も価値の高い個人サービスと言えるでしょう。その価値は基本的にはサービス受容者本人にとっての価値ですが、それが高ければ、市場メカニズムにより PAIA を開発・提供する企業の収益も大きいはずです。

PAIA の方が CAI よりも儲かることに気付けば、企業は CAI による監視資本主義的な事業から PAIA による事業に移行するでしょう。たとえば Amazon はこれまで自社のクラウドの中で CAI による推薦の計算を行なった結果を利用者に示して購買を促してきたわけですが、その代わりに Amazon が商品のカタログを作り、利用者の PAIA がそのカタログをダウンロードして利用者端末の中でマッチングを行なった結果を利用者に示す、ということになります。CAI を動かすための情報システムと PAIA を動かすための情報システムはかなり異なるので、その移行は容易ではありませんが、移行によって Amazon の事業は大幅に拡大するでしょう。

企業が CAI から PAIA に移行しても、非民主的な政治体制を指向する国々が CAI を捨てて PAIA を採用することはあまり期待できません。しかしそのような国々は、中国、ロシア、北朝鮮、ミャンマー、ベネズエラなどせいぜい十数か国です。多くの発展途上国にとって民主主義か権威主義かよりも経済の方がはるかに重要ですから、CAI より PAIA の方が儲かるとなれば、わざわざ権威主義を選ぶ理由はないですね。

したがって、CAI が人権や民主主義を脅かす弊害は PAIA の普及によって最小限に止めることができると考えられます。CAI を使わないようにしようという国際的な合意は成り立ちませんが、もっと付加価値が高く民主主義と相性が良いと期待される PAIA によって CAI を置き換えることはできそうだということです。

しかし、さらに少し考えてみると、PAIA が CAI よりも個人の行動に深くキメ細かく介入できるということは、人間の自律性を侵すリスクも PAIA の方が大きいということです。PAIA は利用者本人の PD をフル活用して本人に介入しますから、本人にとって最高のサービスを提供できるだけでなく、本人に対して最悪の害をなすこともできるわけです。多くの技術がそうであるように CAI も PAIA も両刃の剣であり、実は PAIA の方が鋭利な両刃の剣なのです。PAIA のメリットを損なわないような、しかし厳格なガバナンスが必要です。

参考文献

Charles Duhigg（2012）How Companies Learn Your Secrets. *The New York Times Magazine*. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

国家统计局（2021）中国统计年鉴 . http://www.stats.gov.cn/tjsj/ndsj/

Sebastian Heilmann（2016）Leninism Upgraded: Xi Jinping's Authoritarian Innovations. *China Economic Quarterly*, 20（4）15 - 22

平野 聡（2021）これぞ動かぬ証拠〝新疆ジェノサイド〟示した中国統計年鑑. https://wedge.ismedia.jp/articles/-/21994

大屋 雄裕（2019）個人信用スコアの社会的意義 . 情報通信政策研究，2（2），15-26.

Shoshana Zuboff（2019）*The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs. ISBN 9781610395694. OCLC 1049577294.（邦訳：野中 香方子（2021）監視資本主義：人類の未来を賭けた闘い . 東洋経済新聞社）