
研究

予測アルゴリズムに基づく与信管理の功罪—ライフチャンスへの影響とその対策の有効性の検討を中心に—

The merits and demerits of credit risk management based on prediction algorithms: Focusing on the impact on life opportunities and the effectiveness of countermeasures

キーワード：

予測アルゴリズム, ビッグデータ, ライフチャンス, プロファイリング

keyword：

Prediction Algorithms, Big data, Life Opportunities, Profiling

首都大学東京 堀内進之介

Tokyo Metropolitan University Shinnosuke HORIUCHI

要約

ビッグデータを解析する情報処理技術の高度化を背景に、評価対象の動向を合理的な精度で予測するアルゴリズムの開発が進んでいる。金融分野では、FinanceとTechnologyを融合させた〈FinTech〉と総称される企業やサービスが、この技術によって顧客の与信管理を自動化したことで、多くの人びとが金融サービスにアクセス可能になった。治安維持や司法の現場でもビッグデータを解析し、将来、誰が被害者や加害者となる蓋然性が高いかを評価する予測アルゴリズムの導入が進んでおり、犯罪予測や予測的ポリシングが常態化しつつある。予測アルゴリズムは多くの恩恵をもたらしているが、他方では、さまざまな人間活動や決定がビッグデータを基にした予測によって影響を受け始めており、自由な活動や決定を委縮させる可能性が増している。

そこで、本稿では〈ビッグデータによる予測〉の実態を、特に与信管理との関係を中心にケーススタディとして考察する。この考察では、まず個人のライフチャンスへの影響について、いくつかの事例を

原稿受付：2019年3月5日

掲載決定：2019年6月17日

取り上げ、それらに共通すると思われる諸問題を整理・検討する。その上で、それら諸問題に関する個人的および社会的な対策にはどのような課題があるかを明らかにする。そして最後に、諸問題の是正には既存の対策に加え、特に何が検討されるべきか、その論点を提示する。

Abstract

Along with the advance of information processing technology for analyzing big data, development of algorithms for predicting future behaviors of evaluated subjects with reasonable precision is accelerating. With this technology, companies and services collectively called “FinTech,” which integrate finance and technology, have been automating credit risk management for customers, thereby enabling access to financial services for many people. Predictive algorithms for analyzing big data are being introduced into the scenes of public order-maintenance and justice; predictive algorithm-based evaluation of who is likely to become a victim or a perpetrator in the future, as well as crime prediction and predictive policing are gradually becoming a normality. While big data-based predictive algorithms have provided a number of benefits, on the other hand, they have also started to impact various human activities and decisions, and the possibility of diminution of free activities and free decisions is growing.

Therefore, this paper considers the actual situation of prediction that is based on big data, as a case study, especially in relation to credit risk management. Through that consideration, I would like to clarify: firstly, what is the impact of information technology supporting credit risk management on an individual’s life opportunities; secondly, what kinds of measures have been taken against such impact; and thirdly, whether such measures have come to be effective.

1 はじめに

2000年代の初頭には、情報技術の飛躍的な高度化と普及の中で、私たち個々人は生身の身体を喪失し、行動・購買・閲覧などの履歴情報の集合体、すなわちパーソナルデータ（以下、PDという）として把握され、管理されるようになるとの見通し（Deleuze 1992, Lyon 2001）は、すでに現実的なものであった。

この現実には、悲観的に評価されただけではなく、その後の10年足らずの間に肯定的にも語られるようになった。事実、2011年に世界経済フォーラムがまとめたレポートでは、公的機関や民間組織のデータベースに集積された「PDは新しい石油、つまり21世紀の価値ある石油」であると述べられている（World Economic Forum 2011: 5）。そして、さらに10年近くが経過した現在、PDは、政治、経済、文化など多方面での利用が模索されており、それらを分析対象とする技術やサービスは、日常の生活環境を構成する必須の要素になりつつある。

この間の情報技術の高度化によって、たとえば近年のレコメンデーションシステム開発に見られる通り、PDは、諸個人の選好を把握するのみならず、プロファイリング⁽¹⁾を通じて——改正個人情報保護法における要配慮個人情報に該当する——私秘的な事柄を含めた状態や履歴を推知しうる資源として、マーケティングや与信管理のために活用されるに至っている（堀内 2018, 山本 2016）。

このような近年の動向は、Richards and King（2014: 393）によれば、産業革命に匹敵するインパクトを有し、それゆえに〈ビッグデータ革命〉と呼びうるものであるという。そして、彼らは、この革命の下で「デート、ショッピング、医療、投票行動、法執行、テロ対策、サイバーセキュリティを含む、ありとあらゆる人間活動および決定が、ビッグデータによる予測によって影響を受け

始めている」と指摘している。

そこで、本稿では〈ビッグデータによる予測〉の実態を、特に与信管理との関係を中心にケーススタディとして考察する。この考察では、まず個人のライフチャンス⁽²⁾への影響について、いくつかの事例を取り上げ、それらに関連する諸問題を整理・検討する。その上で、それら諸問題に関する個人的および社会的な対策にはどのような課題があるかを明らかにする。そして最後に、諸問題の是正には既存の対策に加え、特に何が検討されるべきか、その論点を提示する。

1.1 考察の目的と関心について

考察を始める前に、補助線を引く意味で、本稿の目的と関心について述べておきたい。本稿は、与信管理との関係を中心に〈ビッグデータによる予測〉が惹起しうる諸問題に対して、後述する既存の個人的および社会的な対策には、どのような課題があるかを明らかにし、何が検討されるべきかを論じることを目的としている。換言すれば、既存の対策の有効性を判断することが目指されている。しかしながら、ここに言う有効性の判断は、既存の対策がどの程度生じた問題を範疇に収めることに成功しているか、あるいは生じた問題にどれほど対処しうるかといったことを直接考察することによって為されるのではない。つまり、既存の対策の、生じた問題それ自体に対する対処能力を吟味するのではない。各国の対策の有効性が、問題それ自体に対する対処能力の意味で理解される場合には、その吟味は、具体的な制度だけでなく、国ごとの法文化や慣習など制度的背景も考慮に入れた分析が必要であろう。けれども、そのような分析によっても把握しがたい問題がある。本稿は、この問題に照準する。では、その問題とは何か。

第二節での指摘を先取りすれば、それは、〈ビッグデータによる予測〉が惹起しうる諸問題の中には、問題に巻き込まれる本人ですら、問題が生じ

ていることを容易には把握できないものがあるということである。与信において、〈ビッグデータによる予測〉やその運用が不当な評価を下しても、本人がその評価が不当であるという事実を知り得ない場合には、いくら既存の対策が生じた問題それ自体に対する対処能力を持ち得ていても、その恩恵に与ろうとする動機そのものが生じ得ない。本稿が、次節での考察を通じて、既存の対策が抱える課題として指摘するのは、この点である。

それゆえ、本稿の関心は、既存の対策の対処能力を吟味するよりも、〈ビッグデータによる予測〉によって、人びとが実生活において、どのような選択肢や機会を得られ、あるいは奪われているのかを考察するという点にある。こうした目的と関心に基づき、第二節では、〈ビッグデータによる予測〉による正と負の影響を考察し、とりわけ負の影響の中心部分、つまり負の影響は、問題の把握自体が容易ではないことを確認する。そして、第三節では、既存の個人的な対策と、社会的な対策が——事例として取り上げるニューヨーク市議会が可決した条例を除いて——負の影響の中心部分に対して有効なものとなっていないことを論じ、一つの参照されるべきモデルとして、上記の条例が十分に機能するためには、さらに何が検討されるべきかを論じる。

2 ライフチャンスへの影響

与信管理は、一般的には、商取引において取引可否や取引の規模を考える際に、取引先の与信状況を評価することを意味する。しかし、Web利用の拡大を背景に、いまではWebサービスの供与者や利用者自身の信頼性 (trustworthiness)⁽³⁾を評価することも与信管理として見なされる。とはいえ、従来の商取引における与信管理と、Webに関連するそれとは次の点で異なっている。すなわち、前者では、基本的に実名の取引先を直接的に評価するのに対して、後者では多くの場合、データ上

の人格 (以下、ペルソナという) を、つまりPDを分析対象として評価が為されるのである。

ところで、後者の意味での与信管理は、前者よりもはるかに難度が高いものであった。というのも、Web上の行為者は、ときに実際の年齢や性別、嗜好などを偽り、オフラインとは異なるWeb上のアイデンティティを構築して、複数のペルソナを使い分けるからである (Kendall 1998, 森尾 2009)。

しかし、近年、①PDの集積としてのビッグデータと、②プロファイリングなどの高度な情報処理技術や、評価対象の動向を予測するアルゴリズムの開発 (以下、これらを与信管理技術という) によって、ペルソナに対する与信管理も合理的な精度で行えるようになってきた。後述するように、2008年以降の金融分野での〈FinTech〉の台頭は、与信管理技術が実現したものである。そして現在、与信管理技術は、Joh (2014: 37) が「警察による捜査に次の劇的変化をもたらさしめるものである」と論じるように、商取引にとどまらず、他分野にも大きな影響を与え始めている。そこで、次節では、与信管理技術が個人のライフチャンスに与える影響について、特に金融と治安維持をケーススタディとして検討する。

2.1 金融分野における与信管理技術

与信管理技術の急速な普及によって、金融分野では産業構造の変革が進んでいる。「金融業は、もともと情報サービス産業の性格を持ち、ITとの親和性が高い分野である」(淵田 2015: 8) が、ICT媒体の普及や与信管理技術の開発によって、金融業界では、FinanceとTechnologyを融合させた〈FinTech〉と総称される企業やサービスが、近年、急速に台頭してきている。

たとえば、世界最大級の投資銀行Goldman Sachs社は、Digital Reasoning社が開発した自然言語処理技術によって、インサイダー取引などの不正行為に当たる行動パターンを発見し、迅速に調査を開始できる仕組みを構築しつつ (八山 2017: 10)、

機械学習機能を持つ取引アルゴリズムを用いた株取引や通貨取引の自動化を進めている (Byrnes 2017: para.7-9)。米国の銀行最大手のJPMorgan Chase社も、商業融資に関する契約内容を自動的に解釈・審査する情報処理システムを導入しているほか (Son 2017)、顧客の過去の取引履歴などを分析し、最適な商品やサービスを即座に提示するレコメンデーションシステムの運用を開始している (Noonan 2017: para.2-3)。

このように既存の金融機関では与信管理技術の導入が進んでいるが、それは専ら日常業務の効率化を目的としたものである。他方、新興の金融機関では、多くの場合、その導入は新規顧客の開拓のために為される。たとえば、1994年にバージニア州に設立されたCapital One社は、与信管理技術を用いた質の高いサービス⁽⁴⁾を提供することで、現在、6500万以上の顧客口座を有する巨大な金融機関に急成長を遂げている (八山 2017: 6)。

与信管理技術が個人のライフチャンスに与える影響を検討する上で、〈FinTech〉が注目に値するのは、それによって、これまで金融サービスを利用できないか、あるいは利用を制限されていた〈金融マイノリティ (the unbanked)〉と呼ぶ人びとも、金融サービスを積極的に利用できるようになったということである。李 (2015) によれば、世界最大の人口を擁し、激しい経済格差のある中国でも、中国最大手の電子商取引企業アリババ・グループを筆頭に〈FinTech〉が登場したことで、低所得者層や若年層などの金融マイノリティが金融サービスを利用できるようになり、その結果、中国ではWeb上の第三者決済や投資理財商品の取扱額が、近年、激増しているという。資金調達や資産運用を必要としながらも、その機会に恵まれなかった人びとからすれば、与信管理技術は多くの便益をもたらすものだと言えよう。

2.2 治安維持に関わる与信管理技術

〈FinTech〉の事例が示す通り、与信管理技術

によって、かつては容易にアクセスできなかった事柄にも、多くの人びとが手軽にアクセスできるようになってきた。しかし、この事実は裏を返せば、以前よりも遥かに広い範囲でかつ多くのデータが、与信管理技術の評価対象になったということでもある。そして現在、このような与信管理技術は、行政分野においても、特に治安維持に関して、積極的に活用され始めている (Joh 2014: 42-55)。

一般に、犯罪予測 (crime prediction) ないしは予測的ポリシング (predictive policing) と呼ばれるものがそれに当たる。これまでも、たとえばニューヨーク市警が導入した戦略管理システム (CompStat) のように、過去の犯罪データを収集・分析することで、犯罪者の標的となる確率の高い〈場所〉を特定する技術は存在した。しかし、Johによると、近年では予測ポリシングは、過去の犯罪データ以外のデータ、たとえば自動車のナンバープレートを識別する監視カメラの履歴データなどを取り込むことで、「犯罪アナリストには為し得ない仕方で、人・物・場所の関連性を明らかにする情報を生成し、警察がリアルタイムにそうした情報にアクセスすることを可能にしている」(Joh 2014: 49)。

実際、シカゴ警察では与信管理技術を用いて、将来、犯罪者や被害者となる蓋然性の高い人びとをリスト (Heat List) にまとめ、その人びとに対して、犯罪リスクを警告したり、職業訓練や住宅供給などの社会的サービスについて告知したりする活動を行っている (Gorner 2013, 山本 2015: 325-326)。また、ある報道によれば、特定の人物が重罪を犯す可能性を、性別、目や肌の色、交通違反や軽犯罪を犯した回数、刺青の有無といった個人情報をもつて分析対象としつつ、合理的な精度をもって予測するアルゴリズムが、すでに開発されているという (Robertson 2013: para.4)。この種の〈人〉を対象とする予測的ポリシングは、飛行機への搭乗者管理に用いる“*No Fly List*” (Zarsky

2013: 1515) や、居住者の市民権管理のための “No Citizenship List”, 移民の労働資格管理を行う “No Work List” および選挙権管理を効率化する “No Vote List” の作成などでも活用が指摘されている (Hu 2016: 1763-1770)。

さらに、この技術は、司法の現場でも活用が始まっている。アメリカの一部の州⁽⁵⁾では、再犯予測システム (COMPAS)⁽⁶⁾が、刑事裁判中の被告人に関する犯罪歴、雇用状況、教育レベル、家族の犯罪歴、信条を含む130以上の情報を分析し、再犯リスクを10段階で評価している。そして、その評価結果は、裁判官が判決の参考として用いている。

これらの事例が示す通り、治安維持に関わる与信管理技術は、分析対象となるデータが増加し、情報処理技術も高度化したことで——米国が入国管理に導入した “Automated Targeting System-Persons: ATS-P” (Zarsky 2013: 1515) や「顔認証技術」のように——犯罪歴のある人物や不審な行動をする人物を集団の中に発見するために活用されるのみならず、犯罪とは縁がないと思われる人びとの中で、あるいは刑事裁判中の被告人の中で、将来、誰が犯罪者や被害者という形で犯罪に関与する可能性があるのかを予測するためにも、活用され始めているのである。

2.3 与信管理技術のライフチャンスへの影響

このような与信管理技術の利用状況を踏まえて、以下では、それが個人のライフチャンスにどのような正ないし負の影響を与えうるかを検討する。

金融分野では、与信管理技術を核とする (FinTech) の台頭によって、低所得者や若年層を含む多様な人びとが、各種の金融サービスを手軽に利用できるようになってきている。治安維持でも、与信管理技術によって犯罪発生率や検挙率が向上したほか、事前の注意喚起が為される等、与信管理技術が個人のライフチャンスに与えるメリットは大きいと言える。これらは概して正の影響だと言えよ

う。しかしながら、これらのメリットのために、与信管理技術を手放しに評価できるかと言えば、決してそうではない。以下で論じるように、事例からは与信管理技術には、少なくとも〈運用における問題〉と〈既存の差別的慣行に起因する問題〉という、二種類の負の影響が生じていることが伺え、それらはライフチャンスに深刻な影響を与える可能性がある。しかるに、以下ではこれらの問題を検討する。

2.3.1 与信管理技術の運用における問題

クレジットカードの信用格付けシステム (credit scoring systems) をはじめとして、与信管理技術を用いた評価システムでは、通常、統計上の中央値や平均スコアが何であるか、どのようなアルゴリズムが用いられているかは、信用調査機関等によって秘匿されている。そのため、評価対象者は、評価を上げる／下げる行動とはどのようなものかを知ることができないのである。このことが、次のような問題を惹起している。

Marwick (2014: 5) によれば、日々の摂取カロリーや睡眠時間を記録するアプリが収集したPDは、アプリ利用者にとっては健康管理のためであっても、そのPDが保険会社の評価システムによって利用される時には、アプリ利用者に知らされないまま、健康保険料が引き上げられる原因の一つになることがあるという。同様に、Citron and Pasquale (2014: 5) は、たとえばジェネリック薬品を購入するといった経済的な節約の努力が、信用調査機関の評価システムによって財政難と誤って評価される場合には、理由を知らされないまま、ローンの金利が上昇する可能性がある指摘している。

これらの問題が生じる原因としては、先述の通り、評価対象者が評価を上げる／下げる行動とはどのようなものかを知り得ないこと、つまり評価システムが不透明であることが挙げられる。評価システムの不透明性により、たとえ誤った評価が

為されていても、評価対象者がその事実を容易には把握し得ず、したがって、それをただす機会も容易には持ち得ない状況が生まれているのである。

問題の所在を把握し得ず、ただす機会を得難い状況はこれだけではない。評価システムが複数存在する場合にも、同様の問題が生じている。たとえば、米国消費者連盟（CFA）および全米信用報告協会（NCRA）が、50万件を超える消費者の信用スコアを調査した結果によれば、消費者の29%がある信用調査機関と別の信用調査機関との間で少なくとも50ポイントも異なる信用スコアを有し、4%は100ポイントの開きがあった。そして、金融機関は、複数の信用調査機関による異なった信用スコアがある場合、リスク回避のために消費者に最も不利な信用スコアを採用する傾向があったと指摘している（Carter et al 2006: 41）。消費者に不利な評価結果を意図的に選択し、それを基に高い金利を設定していた点で、そうした金融機関は、公正・公平を大きく損なうものである。しかし、評価システムの不透明性と同様に、消費者が独力でその事実をつかみ、異議申し立てすることは、問題の所在を知り得ぬゆえに、ほとんど不可能だと思われる。

こうした事例に見られる問題は、評価結果を採用する上での、運用者側の恣意性に起因するものだと言える。不透明性や恣意性に起因するこれらの問題は、何れも評価対象者とは無関連の、評価システムの〈運用上の問題〉である。

2.3.2 既存の差別的慣行に起因する問題

与信管理技術に関わる問題は、信用調査機関や金融機関による恣意的な運用に起因するものほかに、運用者の意図とは無関係に生じる問題もある。そうした問題は、評価システムが依拠するデータに既存の差別的慣行が反映されることによって生じている。その意味では、この問題は、評価対象者と独立したものではなく、関連した問題である。たとえば、信用格付けシステムは、不安定な

就労形態をリスクと見なし、渡り労働者(migratory worker)や低賃金労働者の信用スコアを低く見積もる傾向がある。それゆえ、不安定な就労を強いられる人びとの大多数が人種的マイノリティである場合、信用格付けシステムや運用者に差別的な意図が無くても、結果的に、これらの人びとに差別的効果をもたらすことになるのである（Citron and Pasquale 2014: 13-14）。

同様の問題は、上述のATS-Pや顔認証技術でも生じている。Garvieら（2016: Findings & Scorecard, RACIAL BIAS）が行った調査によれば、米国国土安全保障省（DHS）が入国管理に用いている顔認証システムは、逮捕率の人種格差が反映されたことで、黒人を要注意人物として評価する確率が高くなっていたのである。さらに悪いことに、顔認証システムの予測アルゴリズムは、いったん要注意人物として黒人を評価すると、その人物が無実であっても、要注意人物として評価されたという事実自体を学習し、上述の黒人に対する差別的効果を助長する〈負のスパイラル〉を生じさせる可能性もあったという⁽⁷⁾。

これらの事例からは、与信管理が与信管理技術に基づくようになるにつれ、既存の差別的効果が助長されたり、あるいは、たった一度の失敗によって、その後の個人のライフチャンスに深刻な影響が生じたりする可能性が、現実味を帯びてきていることが伺える。それゆえ、Havard（2011: 260-275）は、こうした事情を踏まえて、信用格付けなどに用いられる予測アルゴリズムは、既存の差別的な慣行を排除するというよりも、それらを意識されない仕方では体系化しつつ、正当化さえしようものであると指摘している。

上記の問題は、〈既存の差別的慣行に起因する問題〉だということができるが、この問題もまた〈運用上の問題〉と同じく、評価対象者には、問題の所在を容易にはつかめず、解決の糸口を見出すのが困難な問題だと言えよう。

3 現状の対策とその課題についての検討

与信管理技術が惹起しうるこれらの問題(以下、与信問題という)に対して、目下、どのような対策が取られており、それらはどの程度有効なのだろうか。この点を検討するに当たり、ここでも、いくつかの事例を取り上げてみたい。その際、本稿が目指すのは、法的な整備が進められている場合、すなわち、社会的な対策が講じられている場合と、それが不完全な場合、個人的な対策を必要とする場合での違いである。以下で検討する論点を先取りして詳述すれば、ここに言う社会的な対策とは、①与信管理技術によって問題が生じた場合、個人が法的に問題を解決するための諸権利の付与および、それらの権利に基づく異議申し立てを踏まえ問題を調査し、必要とあれば制裁を課す枠組みと、②個人の異議申し立てを必ずしも必要とせず、第三者が与信管理技術によるPDの処理を監査する枠組みの二つを意味している。

前者①に関しては、先ごろ施行されたEUデータ保護規則、いわゆるGDPR (European Parliament and Council 2016) を取り上げ、後者②に関しては、2017年にニューヨーク市議会が可決した市当局による差別的なアルゴリズムの使用を禁止する条例 (The New York City Council 2017) を取り上げる。理由の第一は、これらには与信管理技術の弊害に対処するという明確な目的があること、第二は、上記の通り、GDPRとニューヨーク市の条例では、方法論に大きな違いがあることによる。

また、ここに言う個人的な対策とは、上記の社会的な対策の恩恵に与ることなしに、人びとが個別に試みている実践を意味する。こうした実践に関しては、中国の事例を取り上げる。その理由は、中国では、信用格付けシステムの国家単位での導入が進んでいる反面、社会的な対策が不十分⁽⁸⁾であるために、人びとは個別に対策を模索しているからである。

以下では、中国での個人的な対策の現状と、ヨー

ロッパや米国における社会的な対策とを事例に、有効性についての検討を進めることにしたい。

3.1 個人的な対策とその課題

中国では、当局主導の〈社会信用システム〉の導入が進行中である(国务院:2014)。これに先駆けて、アリババ・グループ傘下にある芝麻信用などの民間企業が、信用格付けシステムをサービスとして展開しており、そうしたサービスはすでに生活インフラの一部になっている。当局は、民間企業の実績を取り込む可能性が高く⁽⁹⁾、そのため社会信用システムが惹起しうる問題は、芝麻信用などの民間企業が展開する信用格付けシステムをめぐる問題と、基本的には同様になると考えられる。それゆえ、ここでは、芝麻信用が展開する信用格付けシステムをめぐる問題を取り上げる。

芝麻信用は、第三者決済と電子マネー (Alipay) の運営が主たる業務で、信用格付けシステムはそうした業務に付随するサービスの一つである。芝麻信用では、信用格付けを含むサービスを「信用生活」と呼ぶ(芝麻信用 2015)。信用生活では、アリババ・グループが運営するECプラットフォームを通じて収集されたPDや金融貸出情報などを基に、予測アルゴリズムが①年齢や学歴や職業などの属性(身份特质)、②支払いの能力(履约能力)、③クレジットカードの返済履歴をふくむ信用履歴(信用历史)、④SNSなどでの交流関係(人脈関係)、⑤趣味嗜好や生活での行動(行为偏好)の5つの要素を評価し、個人の社会的な信用度(芝麻分)を350点から950点の範囲で得点化する。そして「芝麻分の得点が高いほど、ユーザーはより効率的でより良いサービスをうることができる」仕組みになっている(芝麻信用 2015)。実際、信用生活では高得点者は多くの特典を享受できる⁽¹⁰⁾。しかし、他方で、たとえば入院によって公共料金の支払に行けず、支払期限を一時的に超過してしまうなど、故意でなくとも過失の累積により得点を失うと、ライフチャンスは大きく制限されるこ

とになる (Josh and Wong 2016)。さらに、信用生活では、評価の項目に交友関係が含まれており、評価基準も不透明であることから、仮に低得点者との交友が評価対象に影響すると臆断されるなら、低得点者は社会的な排除の対象となる可能性がある。それゆえ、中国では、得点の向上がすでに死活問題になっている。実際、中国では、得点を上げるための攻略法がSNS上で盛んに情報交換され、支払期日の厳守は言うに及ばず、本人の信条や価値観に関わりなく積極的に寄付を行うなど、高得点につながると噂される活動が手当たり次第に試されており、PDを意図的に上書きして、高得点を得られるペルソナを構築することが個人的な対策として実践されているのである (山谷剛史 2015)。

しかしながら、このような対策は、評価対象者を品行方正にして「社会全体の誠実性と信用度を向上させる」(国务院 2014: para.1) という、当局の統治目的には適っても、与信問題の根本的な解決に寄与しないことは明らかである。なぜなら、中国で個人的な対策として試みられているのは、既存の評価システムや評価体制を前提とした、高得点をうるための不確かな実践でしかないからである。そうした実践は、運用者側の恣意性に起因する〈運用上の問題〉や〈既存の差別的慣行に起因する問題〉を何ら解決するものではない。その意味で、このような形での攻略法の探求は、むしろ Winnerが〈逆適応〉と呼ぶ過程、すなわち「技術的手段に適合するように、物事が作り変えられていく」過程でしかないだろう (Winner 1986 = 2000: 279)。

中国の事例を鑑みるにしても、あるいは既存の評価システムや評価体制の改革・善用を求める何らかの個人的な働きかけを試みるにしても、上述したように、与信問題はそもそも評価対象者には、問題の所在ですら容易にはつかめない問題である故に、個人的な対策には限界があり、根本解決には寄与しがたいと思われる。その意味では、個人

を超えた社会的な対策が不可欠であると言えよう。それでは、社会的な対策は、どのようなものであるべきだろうか。Citron and Pasquale (2014: 26-27) は、それは、与信管理技術それ自体や運用面での透明性を確保する〈技術的なデュープロセス (technological due process)〉の確立、すなわち、私たちの誰もが自分自身に関するすべてのデータにアクセスでき、理想的には与信管理技術それ自体も公的な検閲に開かれうる手続の整備であるべきだと論じている。確かに、第二節で見た事例からすれば、不当な評価に異議申し立てするにも、問題の所在を知らねばならず、そのためには、評価の手続きが可視化されている必要があるように思われる。

しかしながら、Citronらの提案にも、いくつかの看過できない問題がある。一つ目は、中国の現状が示唆する問題である。現在の中国で、仮に与信管理技術の詳細が公開されれば、どのようなことが起きるだろうか。噂に過ぎない情報であってもそれに基づき試行錯誤をしていることからすれば、与信管理技術の詳細を公開することは、高得点を目指してペルソナを上書きする個人的な対策に拍車をかけ、却って〈逆適応〉を加速させる事態を招くことが予想される。

二つ目は、より普遍的な問題である。それは、技術的なデュープロセスにより、誰もが自分自身に関するデータにアクセスできるようになったとしても、個人単位で、データやアルゴリズムに問題がないかを常に監査するのは負担が大きく、能力の面でも現実的ではないということである⁽¹¹⁾。

以上の点に鑑みれば、与信問題に関しては、手続きの透明性を〈どのように〉確保するだけでなく、それを〈誰に〉与えるかも重要な論点であると言え、社会的な対策を実効性のあるものにする上で、看過できない論点であると思われる。

3.2 社会的な対策とその課題

先ごろヨーロッパで施行されたGDPRも、先述

の論点に関しては同様の問題を抱えている。それはどうということか。GDPRは、私たちをデータ主体 (Data Subject) と規定した上で、「自動処理のみに基づいて重要な決定を下されない権利」⁽¹²⁾ や「いつでもPDの処理に異議を申し立てる権利」を認め、データ主体の基本的権利と自由を保護する考えを打ち出している (European Parliament and Council 2016: Article 21-21)。PDの取得に際して、個人の明示的な同意を必要とすることや、それを撤回しうるデータ主体の権利 (Rights of the data subject) が明確にされていることも特徴の一つであろう。

このようなGDPRが仮に中国でも適用されれば、信用格付けシステムによってライフチャンスを制限された人びとは、その苦境を覆しうる大きな可能性を手に入れることになるだろう。その意味では、GDPRは有効な対策たり得ているように見える。しかしながら、ライフチャンスが制限されるのではなく、むしろ拡大したと感じている人びと、すなわち高得点者に関してはどうであろう。彼ら／彼女らにしても、データ主体としての権利や人格の尊厳が損なわれる可能性は同様である。しかし、そのような高得点者が、信用格付けシステムに異議申し立てを行う蓋然性はいかほどであろう。報道によれば、信用生活ガリリースされてから数か月以内のうちに、高得点であることはステータスシンボルになったという (Botsman 2017: para.15)。こうした実情に鑑みれば、高得点者が異議申し立ての主体となる蓋然性は決して高くないように思われる。さらに、優遇される高得点者にとっても、不当な扱いを受ける低得点者にとっても、評価システムの不透明性や、その運用上の恣意性などにより、異議申し立て自体が得点の低下につながる可能性が残る場合には、GDPRが規定する異議申し立ての権利も机上の空論になりかねない。

以上を要するに、与信問題に対しては、GDPRのような個人的な異議申し立てを法的に可能にす

る社会的な対策には、少なくとも二つの問題があると言える。一つは、問題が生じているか否かさえ容易に把握できない場合には、個人が異議申し立てをする機会や動機を持ち得ない故に、この社会的な対策が法的に諸問題を解決しうるほどに整備されていたとしても、有効に機能し得ない可能性があるということである。もう一つは、個人が異議申し立てできる機会や動機を持ち得るように、与信管理技術に対する技術的なデュープロセスを導入しても、個人がデータやアルゴリズムに問題がないかを監査し続けるのは、負担の面でも、能力の面でも現実的ではないということである。

これらの点を踏まえ、データ主体としての基本的権利や基本的人権を擁護する観点に立つならば、私たち個々人の権利侵害や尊厳毀損の自覚の有無にかかわらず——つまりデータ主体の親告 (Complaint) に基づき不正なPDの処理が調査される仕組みではない形で——与信問題に対処可能な社会的な対策を講じる必要があると言えるのではなかろうか。

そのような社会的な対策、つまりデータ主体の親告を必ずしも必要としない形での対策に関しては、どのようなものが考えられるだろうか。それを考えるには、米国での試みが一つの参照点になるだろう。

ニューヨーク市議会は、2017年12月に市当局による差別的なアルゴリズムの使用を禁止する米国初の条例を可決した。この条例では、タスクフォースが予測アルゴリズムの公平性や妥当性を精査することが規定されている (The New York City Council 2017)。条例の原案では、技術的なデュープロセスの一環として、監査対象となった与信管理技術のソフトウェアコードを一般公開することが含まれていたが、法執行機関や企業の反対もあり、タスクフォースを設置する案へと変更された (Zima 2018: para.14)。この変更は、行政や企業の思惑を反映する妥協の産物であるが、結果的に、個人的な負担を軽減するのにも貢献し

ている。すなわち、与信管理技術の運用者でも、利用者でもなく、機密保持義務を有する第三者機関が分析対象のビッグデータやプログラムコードなどを精査し、問題があれば是正を勧告する仕組みは、評価システムの機密を開示したくない行政や企業の運用者と、監査の負担に耐え切れない利用者の双方に配慮しながら、前者の国家安全保障に関する機密情報や知的財産権を保護しつつ、後者の利益をも保護するものとして、評価できるように思われる。繰り返せば、この仕組みは、評価システムの透明性を〈どのように〉確保するかという論点と、それを〈誰に〉与えるかという論点の双方に貢献するものだと考えられる。

3.3 〈どのように〉、そして〈誰に〉という視座

このように、与信問題に対する、上記の第三者機関を中心とする仕組みを高く評価する意義、そして後述する、この仕組みに対する追加的な論点の意味を、若干ながら先行研究との関係でも確認しておきたい。その際、中心となるのは、やはり透明性を〈誰に〉与えるかという視座である。

これまでも述べたように、与信問題の焦点は、不当な扱いを受ける本人ですら、その事実を容易に把握できないということである。それ故、既存の対策の対処能力を強化する以上に、与信管理技術の透明性をどのように確保するかも議論されてきた。そして同時に、与信問題を生じかねない予測アルゴリズムが秘匿されているのは、「民主的なプロセスからあまりにも遠く離れている」(Citron 2007: 1312) として、その恩恵や弊害を被る評価対象者に、予測アルゴリズムは原則的に開かれるべきであるとも主張されてきた。例えばCitron (2007: 1312) は、予測アルゴリズムの原則的な公開はもちろん、公聴会の開催やオープンソースコードの使用を義務付けるなど、一般市民がその構築に参加できるようにする民主的アプローチも模索すべきだと述べている。透明性と説明責任の確保については、Joh (2014: 41) も同様に、

警察部門が監視能力を拡大する新技術を導入する前に、一般市民がそれを承認するか否かを判断できるように、新技術の詳細を明らかにする積極的な役割を、地方自治体は果たすべきだと論じている。

しかし、こうした主張には、与信管理技術の目的を損なうとの理由で、批判が寄せられている。予測の仕方が明らかになれば、予測が回避され、問題行動が維持ないし助長される可能性があるからである (Harcourt 2007)。実際には、予測アルゴリズムは学習しながら常に更新されていく動的モデルであるから、予測回避は容易ではないが、それでも中国で〈逆適応〉が生じているように、試行錯誤がされる可能性はある。むしろ透明性の確保、つまり民主的アプローチがより深刻な問題となるのは、それが与信問題を助長する場合である。予測アルゴリズムは相関関係を求めるに過ぎないが、透明性の確保によりその内実を知った一般市民は、誤って因果関係として理解し、偏見を科学の名の下に強化することが懸念されるのである (Zarsky 2013: 1560-1563)。

これらの指摘は、透明性を〈誰に〉与えるかという視座の重要性を示している。期待に反して、与信管理技術の内実を、一般市民に開示したり、共同構築したりしようとする民主的な試みは、負荷が高いだけでなく、ときに有害になる可能性がある。しかるに、与信問題それ自体は広く理解されるとしても、与信管理技術の理解や取り扱いは高度な専門知を要すると言える。この点において、Zarsky (2013) の示唆は重要である。彼は、民主的アプローチに基づく透明性の確保は逆説を招く可能性があること、因果関係を特定する試みは避けられるべきこと、さらに、予測アルゴリズムの開発は、監査可能性に照らして人間が理解可能なレベルに留めるように義務付けられるべきであることを論じているからである (Zarsky 2013: 1566)。

ニューヨーク市のタスクフォースは妥協の産物でありながら、しかし、これら先行研究に照らし、とりわけ透明性を〈誰に〉与えるかという

視座において、民主的アプローチの困難を回避している点で、一定程度評価できることが分かるだろう。ただし、この第三者機関による監査の仕組みが、〈どのように〉に関して一層の実効性を持ち、かつ首尾よく機能するには、さらに次の二点を考慮することが不可欠であろう。

その第一は、第三者機関が技術や法の専門家だけでなく、倫理、政策、社会問題などに精通した専門家も含んだものになることである。なぜなら、既存の差別的な慣行に起因するような、評価システムの運用者の意図に還元されない問題に対処するには、運用者の信頼性 (trustworthiness) や技術作動面での信頼性 (reliability) だけではなく、評価システムのベースとなる情報の信頼性 (credibility) を評価することも必須だからである。

その第二は、コストと強制力に関わることである。第三者機関に原則限るとはいえ、透明性をもたらすには、与信管理技術の開発と活用実態に関する広範な調査が必要になり、そのコストは社会が負うものとして相当な額になる可能性がある。しかるに、その軽減のためには、行政機関や民間企業に与信管理技術の開発や活用を明らかにする義務を負わせよう——上述のタスクフォースにはそれが無い——何らかの法的な整備を進めることが必要である。そして、第三者機関の設置も費用を要することから、その負担を意義あるものにするには、実効性と妥当性を重視しつつ、第三者機関による是正要求は、勧告に留まらず法的な強制力を持つべきであるように思われる。

与信問題に対しては、与信管理技術を一般市民に開示するという意味での民主的アプローチの困難が多少なりとも論じられる限りは、〈どのように〉以上に、〈誰に〉という視座も含めた対策が講じられる必要がある。ニューヨーク市の事例のように妥協的かつ偶発的に現れた事例にも学びつつ、上記で示唆したような追加的な論点を吟味しながら、より一層計画的に、第三者機関による監査と是正の仕組みが講じられていくことが期待さ

れる。

4 おわりに

本稿では、与信管理技術の功罪について、特に金融と治安維持に関する具体事例を取り上げながら、与信問題とその対応策の有効性を検討してきた。検討を通じて、与信管理技術は、個人のライフチャンスを拡大する可能性がある反面、評価システムの不透明性や運用者側の恣意性によって、評価対象者が不当に評価される場合があること、そして、評価システムが既存の差別的慣行を反映したデータに依拠している場合があるほか、そのデータに基づく評価を評価システムが更に学習してしまうことで、差別を助長する可能性があることなど、ライフチャンスを制限する可能性もあることを示した。そして、その可能性に対する現状の対策には、いくつかの課題があることを論じた。

すなわち、個人的な対応は、〈適応〉につながる可能性があるほか、監査や異議申し立てにかかわる個人的な負担の大きさに鑑みれば、必ずしも有効とは言えないことを示した。そのため、個人的な異議申し立てを法的に可能にする社会的な対策としてのGDPRも、個人的な負担の大きさに関して同様の問題を抱えていること、そして、何より問題が生じているか否かさえ容易には把握し得ない与信問題に対しては、データ主体の権利を実際に行使しうる可能性が制限される故に、このような社会的な対策は、必ずしも有効なものとはなり得ないことを論じた⁽¹³⁾。それゆえ、本稿では、こうした点に鑑み、与信管理技術から個人のライフチャンスを守り、なおかつ私たちの権利や尊厳を擁護するには、与信問題に対処する法的な強制力を持つ第三者機関が必要であること、そして、与信管理技術の開発や活用の申告を義務付ける法律の整備も必要であることを示した。

このような社会的な対策は、当然、日本にも必要なものである。けれども、日本では、それ以上

の、あるいは以外の対応も必要になると思われる。それはどうしてか。日本では、改正個人情報保護法が与信問題に対応するための法律であると言えるが、個人情報保護委員会が「推知情報にとどまる場合は、要配慮個人情報には該当しない」（個人情報保護委員会 2018: Q3-9）との見解を示しているために、仮に、与信管理技術が要配慮個人情報を推知し、それに基づいて当人を評価しても、実害が及ばないか、あるいは実害を認識し異議申し立てしない限りは、評価対象者が保護されない状況が続いているからである。与信管理技術が高度化を遂げる中で、推知情報と確定情報とを区別することは、いやまデータ主体としての権利や人格の尊厳の保護にとって、深刻な問題を孕むことは明らかである。日本では、この点の是正も焦眉の課題であると言えよう。

与信管理技術が個人のライフチャンスにもたらすメリットを失うことなく、そのデメリットを抑制していくには、与信管理技術の動向を注意深く見定めながら、その実態に見合う社会的な対策を構築していくことが不可欠である。それには、推知情報と確定情報とを区別するというような、情報それ自体の信頼性 (credibility) に関するこれまでの常識を見直すことや、仕様通りに作動することのみを重視する、技術それ自体の信頼性 (reliability) に関する姿勢を問い直すことも、必要不可欠だと言えよう。

注

- (1) プロファイリングとは、「自然人について個人のある側面を評価するため、特に自然人の仕事の実績、経済状況、健康、個人の嗜好、関心、信頼、行動、所在または移動に関する側面を分析または予測するための、PDの利用から成るPDのあらゆる形態の自動処理」のことである (European Parliament and Council 2016: Article 4 Definitions (4))。
- (2) 本稿では、「社会構造によって付与される個人の発展のための可能性」を意味するものとする (Dahrendorf 1979)。
- (3) 本稿における信頼性に関する三つの区別 (trustworthiness, credibility, reliability) は、加藤ほか (2006) を参照したものである。
- (4) 報道によれば、Capital One社は、与信管理技術によって顧客ごとの債務不履行に陥るリスクを割り出し、そのリスクに見合った金利及び使用限度額を設定したクレジットカードサービスを提供することで、新規顧客を増やしつつも、業界平均より60～75%高い不良債権額の抹消に成功している (Tech Industry 2002: Numerical analytics systems)。
- (5) 2016年時点で、「COMPAS」の評価結果を刑事判決の際に活用している州は、アリゾナ州、コロラド州、デラウェア州、ケンタッキー州、ルイジアナ州、オクラホマ州、バージニア州、ワシントン州、ウィスコンシン州である (Angwin et al. 2016)。
- (6) Northpointe社が構築したシステムで、正式名称は「Correctional Offender Management Profiling for Alternative Sanctions」である。
- (7) 山本龍彦は、「負のスパイラル」に陥り、社会的・経済的に排除され続ける者たちが現われ、その者たちによるバーチャルスラムが形成される可能性を指摘している (山本 2016: 40-41)。
- (8) 2017年6月1日に、中国では「中华人民共和国网络安全法」が施行された。この法律では、第22条で、個人情報はサービスの提供者がユーザーから取得の同意を得て収集することを定めている。しかし、第28条では、インターネット事業者は中国当局 (公安機関および国家安全機関) に対し、技術的なサポートを含む協力を与える

よう定められており、第30条では、インターネット上の安全のために、入手した情報を運用する旨が定められているなど、解釈次第では、中国当局がPDや予測アルゴリズムなどを接収しうる余地が残されている。また、本稿が検討の対象としている予測管理技術が惹起しうる諸問題については、この法律では具体的な対策は講じられていない（中国人民代表大会 2016）。

- (9) 当局が、2018年に信用調査機関としての許可書を正式に交付したのは、新設された百行征信用のみである（中国人民銀行 2018）。百行征信用は、当局の直接的な指導下にある業界団体と信用調査業務のパイロット展開を許可された民間企業8社が株主で、業界団体が筆頭株主であるため、当局が信用調査機関としての主導権を掌握したと言える。
- (10) 中国では、公共サービスも含めサービスの大半にはデポジット（事前預託）が必要である。しかし、芝麻分の得点が高いとそれが免除されるほか、ビザの取得や金融商品の金利などでも優遇される（芝麻信用 2015）。
- (11) 監査を個人に任せることが有効でないのは、次のことから明らかである。Solove and Hartzog (2014: 667) によれば、消費者の多くは、PDの取得や利用を行う旨が書かれた「プライバシー・ポリシー」がある場合でも、単に読んでいないか十分には理解していないのである。
- (12) この権利は、プロファイリング自体を規制するものではない。この権利において問題視されているのは、個人を評価する段階で評価を自動化して処理（決定）することであって、推定を行う際のアルゴリズムに基づく処理それ自体ではない。個人の評価が自動処理であるか否かにかかわらず、推

定を行うアルゴリズムの処理の段階で与信問題は生じうる。この可能性を踏まえて、GDPRはこの権利に加えて、「いつでもPDの処理に異議を申し立てる権利」を定めているのである。この点については、高木 (2017: 92)、堀内 (2018: 32) を参照されたい。

- (13) 堀内進之介 (2018: 33) は、人間の認知と意志力に関する体系的な脆弱性の観点から、個人的な対応を前提とするGDPRの問題点を指摘している。

参考文献

- Angwin, J., Larson, J., Mattu, S., and Kirchner, L., 2016, "Machine bias," ProPublica, May 23, 2016, <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>>, accessed 2019-02-24.
- Botsman, R., 2017, "Big data meets Big Brother as China moves to rate its citizens," WIRED, October 21, 2017, <<https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>>, accessed 2019-02-24.
- Byrnes, N., 2017, "As Goldman Embraces Automation, Even the Masters of the Universe Are Threatened," MIT Technology Review, February 7, 2017, <<https://www.technologyreview.com/>>, accessed 2019-02-24.
- Carter, C., E. Renuart, M. Saunders, C.C. Wu, 2006, "The Credit Card Market and Regulation: In Need of Repair," *NORTH CAROLINA BANKING INSTITUTE*, 10(1): 23-56.
- Citron, D.K., & Pasquale, F., 2014, "The Scored Society: Due Process For Automated Predictions", *Washington Law Review*, 89: 1

- 33.
- , 2007, “Technological due process.” *Washington Law Review*, 85: 1249-1313.
- 中国人民代表大会, 2016, “中华人民共和国网络安全法,” <http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm>, accessed 2019-02-24.
- 中国人民銀行, 2018, “设立经营个人征信业务的机构许可信息公示表,” <<http://www.pbc.gov.cn/rmyh/105208/3485339/index.html>>, accessed 2019-02-24.
- Dahrendorf, R., 1979, *Lebenschancen: Anläufe zur sozialen und politischen Theorie*, Frankfurt a.M.: Suhrkamp. (= 吉田博司・田中康夫・加藤秀治郎訳, 1982, 『ライフ・チャンス—「新しい自由主義」の政治社会学』創世記).
- Deleues, G., 1992, *Postscript on the Societies of Control*, MIT Press, 59: 3-7.
- 淵田康之, 2015, 「金融の破壊的イノベーションとFinTech」『野村資本市場クォーターリー』2015 Summer: 5-20.
- Garvie, C., A. Bedoya, J. Frankle, 2016, “THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA,” The Georgetown Law Center for Privacy & Technology, <<https://www.perpetuallineup.org/>>, accessed 2019-02-24.
- European Parliament and Council, 2016, “General Data Protection Regulation,” <<https://gdpr-info.eu/art-4-gdpr/>>, accessed 2019-02-24.
- Gorner, J., 2013, “Chicago police use ‘heat list’ as strategy to prevent violence,” Chicago Tribune, August 21, 2013, <http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list>, accessed 2019-02-24.
- 八山幸司, 2017, 「米国のフィンテックにおける人工知能の活用（フィンテックAI）の現状と課題」『JETRO』: 1-25.
- Harcourt, B.E., 2007, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*, University of Chicago Press.
- Havard, C.J., 2011, “On The Take: The Black Box of Credit Scoring and Mortgage Discrimination,” *Boston University Public Interest Law Journal*, 20(2): 241-287.
- 堀内進之介, 2018, 「情報技術をめぐる今日の課題—PDおよびプロファイリングを中心に」『情報文化学会誌』25(1): 27-34.
- Hu, M., 2016, “Big Data Blacklisting,” *Florida Law Review*, 67(5): 1735-1809.
- Joh, Elizabeth E., 2014, “Policing by Numbers: Big Data and the Fourth Amendment,” *Washington Law Review*, 89(1): 35-68.
- Josh, C., and G. Wong, 2016, “China’s New Tool for Social Control: A Credit Rating for Everything,” The Wall Street Journal, November 28, 2016, <<https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590>>, accessed 2019-02-24.
- 加藤義清・黒崎禎夫・江本浩, 2006, 「情報コンテンツの信頼性とその評価技術」『人工知能学会研究会資料』SIG-SWO-A602-01: 1-10.
- Kendall, L., 1998, “Meaning and Identity in ‘Cyberspace’: The Performance of Gender,” *Class, and Race Online. Symbolic Interaction*, 21(2): 129-153.
- 個人情報保護委員会, 2018, 「『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関するQ&A」, <https://www.ppc.go.jp/files/PDf/180720_APPI_QA.PDf>, accessed 2019-02-24.

- 国务院, 2014, “国务院关于印发社会信用体系建设规划纲要(2014-2020年)的通知,” <http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm>, accessed 2019-02-24.
- 李立荣, 2015, 「急成長する中国のコンシューマー向けインターネットファイナンス」『野村資本市場クォーターリー』2015 Summer: 82-106.
- Lyon, D., 2001, *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press.
- 森尾博昭, 2009, 「インターネットにおけるアイデンティティー社会心理学的視点から」『人工知能学会誌』24(4): 535-543.
- Noonan, L., 2017, “JPMorgan Chase in push to mine customer data,” *Financial Times*, January 30, 2017, <<https://www.ft.com/content/1eaf6436-e4a2-11e6-9645-c9357a75844a>>, accessed 2019-02-24.
- Marwick, A.E. 2014, “How Your Data Are Being Deeply Mined,” N.Y. REV. BOOKS, January 9, 2014, <<http://www.tiara.org/wp-content/uploads/2018/05/Marwick-How-Your-Data-Are-Being-Deeply-Mined.pdf>>, accessed 2019-02-24.
- Richards, N.M. and J.H. King, 2014, “Big Data Ethics,” *Wake Forest Law Review*, 49(2): 393-432.
- Robertson, J., 2013, “How Big Data Could Help Identify the Next Felon—Or Blame the Wrong Guy,” August 15, 2013, <<https://www.bloomberg.com/news/>>, accessed 2019-02-24.
- Solove, D.J. and W. Hartzog, 2014, “The FTC and the New Common Law of Privacy,” *Columbia Law Review*, 114: 583-676.
- Son, H., 2017, “JPMorgan Software Does in Seconds What Took Lawyers 360,000 Hours,” *Bloomberg*, February 28, 2017, <<https://www.bloomberg.com/news/>>, accessed 2019-02-24.
- 高木浩光, 2017, 「個人情報保護から個人データ保護へ—民間部門と公的部門の規定統合に向けた検討(2)」『情報法制研究』2: 75-99.
- Tech Industry, 2002, “The return of artificial intelligence,” *Tech Industry*, June 28, 2002, <<https://www.cnet.com/news/the-return-of-artificial-intelligence/>>, accessed 2019-02-24.
- The New York City Council, 2017, “A Local Law in relation to automated decision systems used by agencies”.
- Winner, L., 1986, *The Whale And the Reactor: A Search for Limits in an Age of High Technology*, Chicago: University of Chicago Press. (= 吉岡斉・若松征男訳, 2000, 『鯨と原子炉—技術の限界を求めて』紀伊国屋書店).
- World Economic Forum, “Personal data: the emergence of a New Asset Class”.
- 山谷剛史, 2015, “中国の社会信用スコア「芝麻信用」で高得点を狙うネットユーザー,” *ZDNet Japan*, 2015年12月15日, <<https://japan.zdnet.com/article/35074894/>>, accessed 2019-02-24.
- 山本龍彦, 2015, 「予測的ポリシングと憲法: 警察によるビッグデータ利用とデータマイニング」『慶應法学』31: 321-345.
- , 2016, 「ビッグデータ社会とプロファイリング」『論究ジュリスト』18(2017): 34-44.
- 芝麻信用, 2015, <<https://www.xin.xin/#/detail/1-2>>, accessed 2019-02-24.
- Zarsky, T.Z., 2013, “Transparent Predictions,” *University of Illinois Law Review*, 4: 1503-1569.
- Zima, E., 2018, “Could New York City’s AI Transparency Bill Be a Model for the Country?,” *Government Technology*,

JANUARY 4, 2018, <<http://www.govtech.com/policy/Could-New-York-City-AI->

Transparency-Bill-Be-a-Model-for-the-Country.htm>, accessed 2019-02-24.