C. Véliz, *Privacy is Power*, Bantam Press, 2020.[1]

第 2 章「我々はどのようにしてここに至ったのか？」

第二章紹介担当者：中村貴行

第二章全体の要約

今日のプライバシーをめぐる状況は 1990 年代と比べて悪化している。以下の三つの要因が少なくともそれに関連している。**第一は、我々のデジタル化された生活から生まれる個人情報が非常に収益性の高いものになりうるということが発見されたこと、第二は、2001 年 9 月 11 日のテロリストによる攻撃、そして第三はプライバシーが時代遅れの価値だという誤った考えである。**

デジタル化された生活の中では、副産物としてデータ上の痕跡が生み出される。それはユーザーに関する情報として利用可能である。Google はその収益性に着目し、ユーザーの個人情報を利用して効果的な広告を表示させるビジネスモデルを確立した。こうしたデータ経済は監視資本主義と呼ばれ、後になって平等、公平、民主主義を侵食するために有害である。

2001 年の同時多発テロ以降、アメリカ政府はテロ対策のために一般市民の広範な監視を始めた。それは官民の協働によってなされ、今も続いている。我々は官民両方の監視から身を守らなければならないし、危機の際にもプライバシーの重要性を忘れてはならない。

プライバシーは時代錯誤の規範であり、進歩の妨げだと批判される。しかし、実際は時代錯誤ではないし、それを守ることは重要である。

---

[1]著者のカリッサ・ヴェリッツは、道徳哲学、政治哲学を専門とし、現在、オックスフォード大学、哲学部、AI 倫理研究所（Institute for Ethics in AI）の准教授を務める。本著作は、専門家のみならず、一般の読者にむけて、監視経済・データ経済の成立によるリベラル・デモクラシーの動揺について警鐘をならし、プライバシー権の重要性を主張する。原著は約 250 ページと膨大であるため、第 2 章、第 3 章、第 4 章、第 5 章、第 6 章の概要を、節ごとに紹介する。なお、紹介にあたっては、三上航志（京都大学大学院文学研究科倫理学専修　研究員）の監修の下、2 章、4 章、6 章は中村貴行（京都大学大学院　修士一年生）、3 章は水野貴文（京都大学文学部　5 回生）、5 章は豊田樹（京都大学文学部　4 回生）が中心となって担当した。

¶1(p. 27)

今日のプライバシーを巡る状況は1990年代のそれよりも大幅に暗いものとなった。20世紀の終わりには、あなたの車はあなたに関する情報を集めることはなかった。今の世界は、少なくとも我々のプライバシーと我々の周りのものに対するコントロールという点に関しては、以前より暗いものである。我々はどのようにしてここに至ったのか？どうして我々は監視社会[2]が根付くことを許したのか？少なくとも三つの要素が我々のプライバシーの侵食において役割を果たした。①我々のデジタル化された生活から生まれる個人情報が非常に収益性の高いものになりうるということの発見、②2001年9月11日のテロリストによる攻撃、③プライバシーは時代遅れの価値だという誤った考えである。

「くずデータを金粉に変える」

本節の要点（¶2-22, pp. 28-35.）：

我々がデジタル技術を使用する際、オンライン上の行動からデータ上の痕跡が副産物として作られる。この「**くずデータ**（data exhaust）」は、当初は商業目的には利用されていなかったが、Googleによって商業目的で利用されるようになった。

Googleの黎明期、創設者であるラリー・ペイジとセルゲイ・ブリンはページランクというアルゴリズムを考案し、検索エンジンを開発した。ページランクはウェブページがどれだけ信頼できるかを評価するために、そのページへのリンクの数と質を測り、その結果に応じて検索結果をランク付けする。他の検索エンジンとは対照的にページランクは、例えば新聞記事を無名のブログよりも上位に表示させることができた。

Googleは当初、広告に依存することが検索エンジンを広告主のために偏ったものとし、それが消費者のニーズからかけ離れたものになることを懸念していた。だが、Googleの成長に応じて収益性が求められるようになり、Googleは検索結果への広告の掲載権を販売し始めた。ユーザーの個人情報を用いる「監視資本主義」の始まりである。

Googleは資金を得ながらも、当時の平均的な広告と比べて広告がユーザーのためになるようにしようとしていたようである。しかし、Googleの広告システムは広告主にとってブラックボックスであったし、ユーザーを広告主という顧客に販売する商品にしてしまった。

[2] 本書においては、「データ経済（data economy）」「監視経済（surveillance economy）」「監視資本主義（surveillance capitalism）」「監視社会（surveillance society）」といった用語が、ほぼ同じ意味として用いられている。これらは、オンライン・オフラインを問わず、個人の行動履歴を監視することで得られる個人データの収集・分析・交換によって成立する経済システムを指す用語である。「導入（introduction）」（pp. 1-5）及び、「導入」注1（p. 213）を参照のこと。

Google は広告会社として成功したが、それは我々のプライバシーを犠牲としたものだった。我々は考えていることを検索しがちであり、Google は我々の検索からそれらをリアルタイムに知ることができる。また、Google は薬物の使用や中絶の検討などの我々が進んで提供することのないような個人的な情報にもアクセスできる。Google は「ターゲティング広告で使用するためのユーザー情報の作成」という特許も申請した。これはユーザーが進んでは提供しないかもしれない情報を推測する方法を含んでいた。**Google はユーザーのウェブサイトとの関わりによって生まれるデータを受け取り、それをサービスの向上に使っていたのが、それをターゲティング広告に使うという明確な目的のためにユーザー情報を作り出し、探し求めるようになったのだ。**

Google は**アドセンス**(AdSense)を導入し、検索結果以外のページにも広告が表示されるようにした。また、**クッキー**（cookie）を使用してユーザーの個人情報にアクセスしたり、ディスプレイ広告を用いたりするようにもなった。ユーザーの個人情報により収益を得る監視経済の発展である。

監視経済が大規模になるまで、我々の多くは無料のサービスに気を取られて、自らが何を譲渡しているのかに注意を払わなかった。今やデジタルプラットフォームは不可欠なものであり、我々はデータ収集から抜け出すことは不可能に思われる。そして Google はこれが競争的優位を保つために意図的になされたと認めている。

こうしたデータ経済は何年も後になって平等、公平、民主主義の侵食につながるので、悪影響が直ちに明らかでない時にもプライバシー権は守られなければならない。事実、監視経済は避けることもできた。しかし、災難がその障害になったのである。

「災難の発生」

本節の要点（¶23-45, pp. 35-43）：

1990 年代の後半には、規制機関はクッキーの使用に懸念を示し始めていた。しかし、**2001 年 9 月 11 日に同時多発テロ事件が発生すると、政府の注意は安全保障に向けられた。これによりプライバシーの保護が棚上げにされるばかりか、むしろテロを防止するために、官民両方による個人情報を利用した監視が正当化された。政府は正当な根拠なく秘密裏に大規模な監視を始めた。**

NSA は PRISM という計画に従って、著名な IT 企業の数々から様々な個人情報を集めていた。NSA は XKEYSCORE というツールを用いて、任意の人物のオンライン上の活動に入りこむことができた。世界の多くのインターネット通信はアメリカ管理下のインフラや技術を通過するため、こうして、NSA は世界中ほとんど全てのユーザーを監視することが可能だった。

嘆かわしいことに、こういった大衆監視はテロリズムを防止するのに役立っていたわけではなかった。テロリズムは稀な出来事であり、大衆監視はむしろ無意味なデータを付

け加えるだけなのだ。それはすぐに巨大なものとなるテック企業と政府に力を与え、一般市民から力を奪っただけだった。

この出来事から引き出されるべき**第一の教訓は、監視社会が官民の協働によって生まれたということだ**。パランティアはその最たる例である。パランティアはビッグデータ解析の企業であり、CIA によって出資され、情報機関との協働のもと構想されたものである。XKEYSCORE の問題点の一つは、例えば特定の時刻のスカイプ通話などの情報を検索した時に得られる結果が多すぎるといったデータ過多であったが、パランティアはこれを改善した。

こうした官民の協働による監視は今なお世界的な規模で存在する。民間企業が個人情報を集めて政府に提供することもあるし、政府が収集したデータを企業に売り渡すこともある。そのため、我々は両方の監視から身を守らねばならないだろう。

この出来事から引き出されるべき**第二の教訓は、危機は市民的自由を脅かすということである**。命を守るという大義名分は強力だったので、危機の最中、諸々の決定は賛否、エビデンス、代替策を慎重に検討することなくなされた。しかし、我々は生きる際のリスクをゼロにすることはできないし、そのような考え方は権威主義に導かれるだけである。**テロリズムやパンデミックと違い、プライバシーの喪失は差し迫った印象を与えない。しかしそれはすぐには明確な被害が出てこないだけで、確かに惨事に繋がるのだ。**

我々がプライバシーがなぜ重要なのかを常に心に留めておけば、我々が危機の際にも個人情報を十分に守ることの見込みはもっと増すだろう。

「何が重要なのか、なぜ重要なのかを忘れる」

本節の要点（¶46-53, pp. 43-46）：

2010 年、Facebook の創立者であるマーク・ザッカーバーグはプライバシーがアナクロニズムであり、もはや社会規範ではないと仄かした。時代錯誤の法律や規則は不公平と進歩の遅延に繋がるため、我々がそれをなくしたいと考えるのはもっともなことだ。しかし、Facebook は 2019 年に「未来はプライベートである」と主張を変更させながらも、そのわずか一ヶ月後に、ある裁判で、ユーザーは Facebook を使うことによって「プライバシーの合理的な期待を否定している」ため「プライバシーの利益」を持たないと主張したのであり、その主張は一貫していない。また、我々がプライバシーが時代遅れでアナクロニズムだと考えるのは、テック企業の利益のためなのであり、プライバシーは全く時代遅れのものではない。

プライバシーは進歩の妨げとして批判されてきた。プライバシーは 2001 年から市民の安全の障害として非難されてきたし、医療の文脈でも障壁とみなされてきた。コロナウイルス・パンデミックに際して、各国において、接触追跡アプリの導入のためにどの程度デ

ータ保護に対する逸脱を許容しうるのか、ということが議論された。

プライバシーという極めて重要な規範を時代遅れのものと勘違いすることは危険である。**プライバシーの歴史は長く、我々はそれを当然のものとみなしがちである。しかし、そのことによって、我々は容易にプライバシーがいかに重要で、なぜ重要なのかを忘れてしまうのだ。**また、オフラインでのプライバシー侵害は不快感や違和感を伴うことが多いが、オンラインのプライバシー侵害は気づきにくい。

次の二つの章は、プライバシーを守る戦いは権力を求める奮闘であり（第3章)、個人情報は有毒である（第4章）という二つの教訓を、我々に思い起こさせるだろう。

第 3 章「プライバシーは力である」

第三章紹介担当者：水野貴文

第三章全体のまとめ

本章ではプライバシーと力の関係が論じられる。Facebook や Google に代表されるようなテック企業は、収集した個人データを基に、アプリケーション、広告、フェイクニュースなどを巧みに利用し、人びとに自らの利益を損なわせるような行動に仕向ける。このような力は「**ソフトな力**」と呼ばれる。また、テック企業は、私たちが抵抗しようと試みても、私たちの知らない間にデータを引き抜こうとする。このような力は「**ハードな力**」と呼ばれる。テック企業はこの両者を用いて、近年ますます全体主義的になっている。テック企業にこのような力を与えないためには、プライバシーが必要なのである。テック企業は、もしあなたが何も悪いことをしていないのであれば、データの提供を拒否する理由は何もないという物語を語る(このような物語を広めることも、ソフトな力の一種である)。しかし、**プライバシーは私たちの悪事を隠すために必要なのではない。そうではなく、他者が私たちのデータを基に力をつけ、私たちに悪事をなすことを防ぐために、とりわけ、私たちの自律の侵害および民主主義の破壊を防ぐために必要なのである**。ケンブリッジ・アナリティカは、データを基に私たちの投票先を推測し、その上で個人に最適化されたコンテンツを送るというデジタル選挙運動を秘密裡に遂行した。こうした選挙戦への干渉に見られるように、悪意をもったテック企業たちによって私たちの民主主義は脅かされている。**テック企業の力は私たちのデータに由来しているため、私たちの自律のコントロールと自治の能力を回復するためにはプライバシーを回復するしかない**。以下で述べるように、プライバシーは集合的な性質をもっているため、プライバシーの回復のためには、社会の成員全員による集合的努力が求められる。つまり、**プライバシーを守ることは、リベラル・デモクラシーを生きる私たちにとって市民的義務**なのである。今こそテック企業に抵抗する時だ！

導入部分

導入部（¶ 1-9. pp. 47-49）の要点：

プライバシーはあなたの最も個人的な諸側面を露わにしてしまう鍵のようなものである。誰かに自分のプライバシーを与え、その人と親密になることは、その人に弱みを共有し、あなたを傷つける力を与え、その特権的地位をその人が決して利用しないと信じることを意味する。しかし多くの企業や人々はあなたの利益を最優先しているわけではない。

企業はあなたの好みに関するデータを損な取引に誘い込むために使うかもしれないのである。**プライバシーは、もしそれが欠けてしまうと他人に力を与えてしまうがために重要なのである。**

自分には隠したり恐れたりするもの、あるいは何か特別なものや大切なものはないから自分のプライバシーは安全だと思うかもしれない。しかしそれは誤りである。あなたにはアプリ、プラットフォーム、広告などに対して注意を向ける能力がある。あなたにはセンシティブ情報がある。あなたには身体がある。あなたにはアイデンティティがある。あなたには個人的つながりがある。あなたにはものを言う力がある。あなたには投票権がある。**あなたは力の源なのだ。**それゆえ個人データを集め、分析する者は、あなたに広告を注視させたり、あなたの行動を推測したりする力を得ることができる。Facebook や Google は、こうしたあなたに影響を与える力を売るために、データを保持しているのであり、**彼らは力のビジネスに従事しているといえる。**

「力」

本節の要点（¶ 10-15, pp. 50-51）：

筆者はこの節で 2 つの「力（power）」の概念、すなわち**ソフトな力**と**ハードな力**を導入する。**前者は「その働きかけがなければ、行ったり考えたりしなかったであろう何かを、誰かにさせる能力」であり、演説、推薦、広告フェイクニュースなどがある。後者は「権力者が、抵抗にも拘わらず自らの意志を強制的に成し遂げる能力」のことである。**デジタル化の時代において力をもつ諸組織、つまりテック企業は、ハードな力を行使することなく、まずはソフトな力によって私たちに強い影響を与えている。以下、本章ではプライバシーと力の関係を探求することで、テック企業が力を集め、行使し、変換するやり方を理解することを目指す。そうすることで、私たちはプライバシー権の侵害によって引き起こされるある種の支配に対して、よりうまく抵抗するための道具やアイデアを得ることができるだろう。

「力と知識」

本節の要点（¶ 16-20, pp. 51-53）：

知識はそれ自体一種の力であるが、フーコーが論じるように、逆に、力は何が知識と見なされるのかを決定する。Google はまずあなたのデータ(≒知識)を集めることで力を獲得する。その力のおかげで、今度は Google が何があなたに関する知識と見なせるのかを決定することができる。さらに、**力は人間の主体のありようを構築し、変容させる。つまり、人びとの欲望でさえ、力の結果でありうるのだ。このような、力が主体を知の対象とし、主体のありようまでも変化させていく過程は、以下のような事例におい**

ても見出すことができる。例えば、人びとをアプリケーションの中毒にするためにドーパミン(人を行動に動機づける神経伝達物質)がどのように作用するのかに関する研究をテック企業が用いるというケースがある。プラットフォームに没頭させるために不定期の報酬を作ったり派手な色を使ったりする、あるいは投稿に対する「いいね」やコメントによってあなたにドーパミンを出させる、といった具合である。

知識に由来する力と力によって定義づけられる知識は、2 者間の知識の非対称性がある場合より一層支配的になる。例えば Facebook があなたについて知るべきすべてのことを知っており、あなたが Facebook について何も知らなかった場合、両者がお互いについて平等に知り合っている場合よりも Facebook は力を得るだろう。

「デジタル化時代における力」

本節の要点（¶ 21-26, pp. 53-55）：

個人データに由来する予測力と影響力はデジタル化時代における典型的な力である。テック企業はそれら 2 つの力を独占している。

伝統的には、独占禁止法に抵触する企業の特徴とは、顧客を失うことなく利益を上げることができる状態であった。しかし Google や Facebook は無料でサービスを提供しているためこれには当てはまらない。とはいえ、**たとえ利益を上げていなくとも、もし企業が顧客を失うことなく彼らに種々の損害を与えることができるならば、独占企業である可能性があると考えるべき**である。

実際、広告によって利益の大半を稼いでいる Google のような企業は、私たちに関するデータを多く持っているという優位性のために、**競合他社の対抗を不可能にしてきた**。

「ハードな力」

本節の要点(¶27-38, pp. 55-58)：

私たちが抵抗しようと試みている場合であっても我々からデータが引き抜かれるとき、テック企業はハードな力を用いていることになる。例えば Google は Google Maps において、あなたが位置履歴の設定をオフにしても、アプリを開いているときは位置データを保存していた。こうした事例は、テック企業は私たちの許可を得ることなく、私たちが知らないうちにデータを奪っているのであり、テック企業によるハードな力の行使といえる。

テック企業のハードな力は昔から存在したが、近年ますます権威主義的になってきている。例えば、中国政府はテック企業と協同して、ビッグデータから人々の信用度を数値化する社会信用システムを設計してきた。人々は日常の些細な違反によってスコアを下げられ、そのスコアが人生の全ての場面における機会の獲得と制限に影響することに

なる。高いスコアを持つ者は公的な場において種々のサービスの恩恵にあずかることができるが、低いスコアの者は公的に辱しめられる。**全体主義社会のひとつの特徴は、力が生活の全ての側面をコントロールするという点であるが、この意味においてテック企業のハードな力は「全体的」であるのだ。**中国ほどでないないものの、リベラル・デモクラシーの西洋社会においても、信用スコアが知らず知らずのうちに計上され、その結果消費者が不利益を被るシステムは存在している。秘密で不透明なスコア化システムは受け入れられない。市民として、私たちには自分たちの生活を支配するルールを知る権利がある。

テック企業がハードな力を及ぼす別の方法は、そもそも破ることができないルールを設定することである。自由な社会では、法が存在していることと執行されることの間にはいくらかの自由度があり、人々は些細なものであるならば処罰されることなく違反することができる。しかし、**テック企業が制定するルールは明文化されず、コンピュータによって自動的にコード化され、強制される。その結果、私たちは例外的にルールに違反する自由が奪われてしまうのである。**

「ソフトな力」

本節の要点（¶ 39-57, pp. 58-64）：

ソフトな力は、ハードな力に比べて強制的でないように見えるため、より受け入れられやすいかもしれないが、テック企業のソフトな力は、私たちの利益になると見せかけて、私たちを操作し、私たちを自らの利益を損う行為に従事させる。例えば、ニュースフィードをスクロールし、あなたの時間を奪い、あなたに頭痛を与えているのは、確かにあなたの指である。しかし、もし Facebook のようなプラットフォームがあなたを誘惑しなければ、あなたが無限にスクロールし続けることはないのである。

技術的方法のほかに、テック企業は私たちにある物語を語ることでソフトな力を行使する。すなわち、あなたが何か悪いことをしたわけではないのなら、テック企業にデータを握られることを拒否する理由はなにもないという物語である。しかし、プライバシーは悪事を隠すためのものではない。プライバシーとは、他者から与えられうる悪事から私たち自身を守るということに関するものであり、また、ある力が私たちについての知識を使ってより一層強大になるという事態を不可能にするために、その力を盲目にするということに関わるものなのである。また、テック企業の力は、デジタル技術が必要で、不可避で、進歩的であるという物語とそれを支持する合理性を喧伝するが、技術の少なくともいくつかは、そうではない。例えば Google 翻訳のアルゴリズムは性差別的であり進歩的ではない。また、グーグルグラスの失敗にみられるように、技術がヒットするかどうかは私たちの協力次第なのである。

テック企業は人々の福利に貢献するような仕方でオンライン世界を設計できるし、す

べきである。データを商品として扱うことはよい製品を作ることとは関係がなく、それは金儲けの手段に過ぎない。組織がデータを集め、使用することに反対すべき理由の1つは、私たちの自律を尊重しない組織が存在するからである。それらの組織は、私たちの自律を損なうような仕方で私たちのデータを好き勝手使うことで、オフラインでは窃盗や強制と呼ばれうる悪事をなしている。それにもかかわらず、彼らは自分たちがしていることを婉曲的に表現し、あたかも好ましいことであるかのように言うのである。物事をその本来の名前で呼び、私たち自身の物語を作らなくてはならない。

「駒のように利用される人たち（pawns)」

本節の要点（¶58-78, pp. 65-71）：

あなたは、データサイエンティストたちがスクリーン上で行うゲームにおける（彼らは時にこれを「人工社会」と呼ぶ)、駒にすぎない。データサイエンティストたちは、可能な限り集めた情報からコンピュータ上で私たちのバーチャルアバターを作り、それらで実験をしている。様々なシミュレーションの末、自分たちの思い通りの結果を作り出す方法を発見できれば、彼らはそれを実際の世界で試してみるのだ。これは**ケンブリッジ・アナリティカ**が政治運動の支援のために実際に使った手法である。彼らはFacebookユーザー27万人を騙し、そこから人々のオンライン上でのつながりを悪用することで、計約8700万人のユーザーからセンシティブデータを集めた。そしてこのセンシティブデータを基に、彼らは史上最も個別化された政治運動を形成したのである。

ケンブリッジ・アナリティカのデータサイエンティストたちの具体的な手順は次の通りである。あなたに関するデータを集めると、まず彼らはあなたをパーソナリティの5大特徴によってスコア化する。次に彼らの予測アルゴリズムをあなたのプロフィールに当てはめ、例えば投票先の確率などを計算する。最後にあなたが多くの時間を過ごすソーシャルメディアのプラットフォームを特定し、あなたに最適化されたコンテンツを見せ、その影響を観察し、改良を重ねるのだ。

ケンブリッジ・アナリティカのデジタル選挙運動には道徳的制約がなく、とりわけ次の2点において危険であった。すなわち(1)人々に異なるコンテンツを見せることで分断を煽り、合理的な意思決定を可能にする共通の経験を破壊したという点、(2)一見したところ選挙運動に見えず、彼らのプロパガンダはニュースや一般人のコンテンツに見えたという点である。ケンブリッジ・アナリティカのみならず、悪意をもったその他の巨大テック企業によって**私たちの民主主義は脅かされている。**彼らの力は私たちのデータに由来しているのである。したがって**私たちの自律のコントロールと自治の能力を取り戻す唯一の方法は、プライバシーを回復することなのだ。**

「プライバシー、自律、自由」

本節の要点（¶ 79-93, pp. 71-75）：

自律とはあなた自身の生活に対して力をもつことである。自律は個人及び社会的福利にとって大変重要であるため、リベラル・デモクラシーにおいては、他者に危害を加えるケースなどを除き基本的には他人の自律に干渉してはならない。

プライバシーが欠如すると、他者があなたの生活に干渉することが容易になってしまう。自分の価値観を自律的に決定するためには、外部の圧力から自由な時間と空間が必要なのである。人々は、オンライン上のコンテンツを通して他者から監視され、自身のなすことが自身にとって悪い帰結をもたらしうると知るとき、自己検閲する傾向にある。このことは、「萎縮効果（chilling effect）」として知られている。

テック企業は今まで私たちの自律を尊重してこなかった。テック企業の利益とあなたや社会にとっての利益の間には対立があるため、いくらテック企業があなたについて熟知しているからといって、彼らの提案があなたの価値観に基づいているとは限らない。また Google のような企業は、スマートフォンやラップトップを通してあなたの行動を部分的に形成しているため、彼らのアドバイスに従わないようにすることは殊の外難しい。**結局のところ、彼らはあなたに選択肢を提示し、それに従うようにナッジし、新たなタイプのソフトな権威主義を作り上げているのだ。**

民主主義国家が成立するためには、あなた 1 人だけでなく社会の成員全員が自律を持っていなくてはならない。それゆえ、私たちの自律と社会の自由を取り戻すためには、**社会の成員全員による集合的な努力によって、プライバシーを守っていかねばならない**のである。

「プライバシーは集合的である」

本節の要点（¶ 94-116, pp. 75-82）：

ケンブリッジ・アナリティカの惨事が示す通り、プライバシーは個人的であると同時に集合的である。すなわち、先の事例においては、1 人のプライバシーを晒すことは、私たち全員を危険に晒すのであった。

プライバシーの集合的な性質を考慮に入れると、いわゆる「個人」データを当人の私有財産として自由に売買できるようにするという発想の危うさがわかる。遺伝子を例に考えてみよう。たとえば Ancestry のような企業にあなたが遺伝子データを提供することで、あなたの家族や子孫に不利益が生じるかもしれない。というのは、あなたの遺伝子の構造の大半は他人と共有されているため、そこから様々な推論が可能だからである。遺伝子データベースは政府に対する反対者の特定や、強制送還目的での移民の国籍の推定などに悪用されうるのだ。また、匿名の DNA サンプルであっても、他のいくつかの

データと組み合わせることでその人物の身元を絞り込むことができる。しかし、遺伝子検査は様々な理由から誤検出の割合が高くなる可能性があり、冤罪につながりうる。遺伝子に限らず、私たちはお互いを脆弱にしうる無数の仕方で結びついている。このようなプライバシーの相互依存状態が示唆するのは、**私たちは誰しも自分のデータを売ることについて道徳的な正当性をもっておらず、私たちの個人データは他人の個人データをも含むため、私たちが自身の個人データを所有する仕方は、財産を所有する仕方とは異なる、ということである**。

プライバシーの集合的性質とは、あなたのプライバシー上の不注意が他者のプライバシー権の侵害を促進するという意味に留まらない。**プライバシーの喪失の数々の諸帰結は、社会の構造を傷つけ、民主主義を危うくするという形で集合的に経験されるのである。**「プライバシーの文化」が奪われ、至る所で監視が行われる「晒の文化」においては、人びとの間の私的な空間や親密なつながりが失われ、人々の不信感や恐怖感が増し、リベラルな社会の基盤が失われてしまう。また、プライバシーが欠如することで、個人データが個別化されたプロパガンダやフェイクニュースのために使用されると、社会の不和と分断が引き起こされてしまう。Facebook のような企業は、異なる人々に候補者に関する異なる情報を提供することで、社会の分極化を引き起こすのだ。

プライバシーが私たちに与える集合的な力は民主主義にとって必要不可欠である。プライバシーは、テック企業や国家ではなく人々に力を与えるのであり、公共財としてのプライバシーを守ることはリベラル・デモクラシーを生きる私たちの市民的義務である。

「なぜリベラル・デモクラシーなのか」

本節の要点（¶115-127, pp. 82-85）：

本節ではリベラル・デモクラシーの必要性が論じられる。最近では民主主義を支持する声は必ずしも多数派ではなく、また 2019 年はエコノミストによる民主主義のグローバルスコアが過去最低であった。そのため、「リベラル・デモクラシーを維持するためにはプライバシーが必要である」と論じるだけでは不十分であり、**「そもそもなぜリベラル・デモクラシーなのか」について改めて説明する必要がある**のだ。

民主主義とは主権が国民に与えられている政府のシステムのことであり、言い換えれば、独裁者ではなく、社会的に対等な者同士が彼ら自身を統治する公平な社会的秩序のことである。なぜ民主主義を守らねばならないのか。簡潔にいえば、民主主義は全ての人の基本的な諸権利を最も適切に守るからである。

たしかに民主主義は完璧な政治形態ではないが、民主主義には他の政治システムにはない次のような長所がある。すなわち、(1)社会の大半の人の利害と意見を考慮に入れるよう政治家に強制できるため、多数の人をほどほどに幸福にでき、(2)そのようにして多

くの情報源と観点を取り入れることで、よい決定をする可能性を高めることができる上、(3) 国内外においてより平和的である傾向にあり、(4) 法の支配によって人々が比較的安心感を享受できる。

こうした社会全体から見る観点ではなく、とりわけ「あなたの」権利を確実なものとするためには、民主主義はリベラルでなければならない。リベラリズムは「多数者の専制」を避け、最小限の制約を除いて市民にできるだけ多くの自由を与えようとする。リベラル・デモクラシーは少数者の諸権利が守られることを確実なものとするのである。

「プライバシーは正義の目隠しである」

本節の要点（¶ 126, pp. 85-86）：

リベラル・デモクラシーの最高の徳の 1 つは平等と正義を強調することである。一方で、データ経済の最大の悪の 1 つは、様々な方法で、私たちの平等を弱らせ差異を大きくする、ということである。私たちは各々のデータに応じて異なる仕方で扱われてしまい、例えば、情報と機会に同じようにアクセスすることができなくなってしまうのである。正義の特徴の 1 つはその不偏性であるが、**プライバシーはシステムに目隠しをすることで、私たちが平等かつ不偏的に扱われることを確実にしてくれるのである。**

「力の非対称性を矯正する」

本節の要点（¶ 127-131, pp. 86-88）：

力の非対称性の原因は知識の非対称性である。最近まで私たちはデジタル領域における巨大テック企業と政治的プロパガンダの働きについてほとんど知らなかったため、彼らの思い通りに操作されてきたのである。私たちは彼らについてもっと知り、逆に私たちについては知られないようにしなくてはならない。

新聞、裁判所、アカデミアは真理、正義、公平を保護するものであるため、健全なリベラル・デモクラシーのためには、それらの独立性を守らねばならない。例えば、巨大テック企業から資金提供を受けるような研究には慎重にならねばならないし、あるいは、内部告発者とその内容を報じるよいジャーナリストを支援してなくてはならない。

私たちが巨大テック企業の魔力から解放されるためには、個人化されたコンテンツが、何の目的のために、そしてどのように設計されたかを理解することが必要なのだ。

「力に抵抗する」

本節の要点（¶ 132-136, pp. 89-90）：

デジタル化時代の諸組織はあまりに多くの力を持っている。しかし、私たちは彼らの

力の基盤となっているデータを取り戻すことができるし、新しいデータの収集に制限をかけることができる。テック企業は私たちのデータから力を得ているのであり、彼らはその基盤の脆弱性に気づいている。私たちが規制をかけたり抵抗したり、あるいはプライバシーを優先する企業が現われたりすることで、彼らは消えうるのである。テック企業に対するこのような抵抗は**テックラッシュ**(techlash)と呼ばれている。

たとえあなたが現在の政府やテック企業が行っていることに疑問をもっていないとしても、彼らの力が制限されることを望むべきである。というのは、次に力を獲得するものがより権威主義的な人物かもしれないからだ。事態がよくない方向に進んでからでは手遅れになるかもしれない。政府やテック企業に力を持たせたままでは危ない。今こそ抵抗の時だ！

第 4 章「有害なデータ」

第四章紹介担当者：中村貴行

第 4 章全体の要約

個人データはデータ主体とそれを管理するものを脆弱にする。それは個人や組織、社会全体を害する。

個人データの誤った管理が社会を毒す主な経路は四つある。第一に、個人データは国家の安全保障を危険に晒すことがある。第二に、それは民主主義を腐敗させるのに使われることがある。第三に、それは晒しの文化と自警（a culture of exposure and vigilantism）を後押ししてリベラルな社会を脅かすことがある。第四に、それは個人の安全を危うくすることがある。

我々は過去から学び、個人データによって個人や組織、社会が毒された歴史を繰り返さないようにしなくてはならない。

導入部

¶1〜¶3, pp. 91-92 の要点：

アスベストと個人データの類似点は多い。両者は安価に入手可能であり、実用的であり、そしてなにより有害である。セキュリティの専門家であるブルース・シュナイアー（Bruce Schneier）の言葉を借りれば、**個人データとは「有毒資産（toxic asset）」**である。

さらに、個人データは、センシティブで、大変悪用されやすく、安全に保つのが難しく、そして多くの者――犯罪者から保険会社や情報機関まで――に渇望されている。この意味で、**データとは脆弱なもの（vulnerable）なのであり、このことは、データ主体とデータを保管するものを、同様に脆弱にしてしまう**のである。

「毒された生活」

本節の要点（¶4-13, pp. 92-95）：

個人データが攻撃されることで個人が被害を被った例は多くある。そのうちの一つは、既婚者の不倫を手助けするマッチングサイトである**アシュレイ・マディソン（Ashley Madison）**に関するものだ。ハッカーの攻撃により、メンバーシップを解約したものを含む 3000 万人のユーザーの個人データ（名前、住所、好み、郵便番号、クレジットカードの番号）が暴露され、多くのユーザーが不眠や失業などの被害を被った。

ハッカーには、不倫をした人々を裁き罰する道徳的な正当性はないし、また、ユーザーの中には、配偶者の認知と同意を得ていた人、ただ登録しただけの人といった、複雑な事情を抱える人々が含まれていたのであり、このような社会的制裁は不倫に対する適切な処罰とは言えない。また、子供や配偶者などは、明らかに非がないにもかかわらず被害を被ったのだ。

また、後ろめたいことがなくても個人データによって被害を被ることはある。そのような例の一つは、なりすましである。ラモナ・マリア・ファギウラ（Ramona Maria Faghiura）は、**なりすまし（identity theft）**の被害にあっていたために、2015 年に無実の罪で拘束され、その結果、不安障害まで患うことになった。なりすましの最も頻発している事例はクレジットカード詐欺であり、ある調査では、92%の人が、なりすましからスパイウェアの標的になることに至るまでの、なんらかの種類のオンラインでのプライバシーの侵害を経験したことがあると答えた。

さらに、なりすましに加えて、**恐喝**の事例も挙げることができる。例えば、2017 年にエストニアにある美容外科の個人データがハックされ、世界 60 か国にわたるその利用者は、個人データと引き換えに、ビットコインで「身代金」を支払うよう恐喝されたのである。

このように、個人データの悪用によって、様々な形で個人は被害を受けうるが、データの災難は政府と企業といった組織をも害しうる。

「毒された組織」

本節の要点（¶ 14-19, pp. 95-97）：

データの脆弱性はそれを保管し分析する組織にも及び、必要以上にデータを溜め込む組織は自らのリスクを生み出している。幸運なことに Facebook はプライバシーの問題を切り抜けてきたが、そのイメージは悪化することになった。また、個人データを悪用したケンブリッジ・アナリティカは業務停止に追い込まれたし、外部のデベロッパーによるユーザーの個人データへのアクセスが可能になっていたと明らかにされた Google+は閉鎖されることになった。さらに、倒産を避けることができたとしても、非常に高い罰金を科される場合もある。例えば、ブリティッシュ・エアウェイズ(British Airways)は、セキュリティ問題のために、GDPR によって 1 億 8300 万ユーロもの罰金を科された。さらに、2015 年に生じた、アメリカ合衆国人事管理局(United States Office of Personnel Management)の情報漏洩は、データの漏洩が、組織の威信を傷つけるだけでなく、国家全体の安全保障を損ねることもあることを示す一例だ。

「毒された社会」

¶20

個人データの誤った管理が社会を毒す主な経路は四つある。個人データは、①国家の安全保障を危険に晒し、②民主主義を腐敗させるのに使われることもあり、③暴露と自警の文化（a culture of exposure and vigilantism）を後押ししてリベラルな社会を脅かし、④個人の安全を危うくする。

「国家安全保障への脅威」

本節の要点（¶21-30, pp. 98-101）：

個人データによって国家の安全保障が危険にさらされた例の一つは、データブローカーである**エキファックス（Equifax）**のデータ流出である。エキファックスは機密情報を暗号化せず保管し、脆弱性の確認された古いバージョンのソフトウェアを使っていた。攻撃者はエキファックスから、1 億 4700 万人のアメリカ人の個人データを盗み出した。これは、歴史上最大の情報流出の一つであるが、この件に関して、アメリカ合衆国は中国軍関係者を起訴した。攻撃の理由としては、中国軍が、スパイとして雇用できる潜在的な標的を特定したかったからといった点が挙げられる。

第二の例は、ゲイ・バイ・トランスの人々に適した**マッチングアプリである Grindr** に関するものである。アメリカ合衆国は、Grindr の株式を保有していた中国の企業 Beijing Kunlun に、アメリカの企業に株式を売却するように圧力をかけた。Kunlun は、北京に拠点を置くエンジニアに、個人的なメッセージを含む数百万のアメリカ人の個人データへのアクセスを与えていた。そのため、米軍やアメリカの情報機関のメンバーのうち何人かがアプリを使用していた場合、中国は彼らを脅迫するのにそのデータを使うことができたし、米軍の動きを推測することができたのである。

第三の例は、**フィットネス会社であるストラヴァ（Strava）**に関するものだ。ストラヴァはすべてのランニングルートをウェブサイト上に公開していたが、これによって、非公開の軍事基地に勤務する軍人のランニングルートから、基地の位置を特定することができたり、特定の軍人を追跡したりすることができたのだ。

これらの事例が示すように、**個人情報にアクセスすることによって、ある国家全体の安全保障を、外国の勢力が脅かすことができる**のだ。

「民主主義への脅威」

本節の要点（¶31-48, pp. 101-108）：

個人データは選挙への干渉にも使われうる。ケンブリッジ・アナリティカの例が示す通り、その方法はマイクロターゲティングである。位置情報、行動データ、心理的属性など

の個人データによって類型化した集団に、特定の政治的主張を示す広告を表示させることによって、その集団の投票に効果的に影響を及ぼすことができる。

確かに、マイクロターゲティングは、限定された効果しか持たず、それゆえ我々は選挙へのその影響を心配する必要はないと指摘する懐疑論者もいる。彼らがいうには、性格的特徴と政治的価値観の相関は必ずしも強いものではないのである。さらに、Facebook の「いいね」の予想に使える力は使用期限があり、何かを「いいねする」ことが今日意味することは、それが一年後に意味することとは異なっているかもしれない。しかし、**マイクロターゲティングは、確かに限定されたものかもしれないが、影響力を持つということは疑いえず、特にこれが数百万単位での人々に向けられるとき、決して無視できない票数となって現れ出る**。アル・ゴアとジョージ・W・ブッシュ間の 2000 年のアメリカ大統領選挙戦は、フロリダのたった 537 票によって勝敗が決定されたのを思い起こそう。Facebook のマイクロターゲティングに基づく選挙広告は、2014 年のスコットランドの住民投票、2015 年のアイルランドの住民投票、2016 年のブレグジットの国民投票、2017 年のドイツ連邦議会選挙、2017 年のアイスランド議会選挙などにおいて用いられた。さらに、こうした選挙への介入の疑惑は、2020 年のアメリカ大統領選挙に関しても生じている。しかし、これらのメッセージが選挙にどんな影響を与えてきたのかについての情報は、Facebook 自身に秘匿されているのであって、我々はこれについて全く知らない。**我々についてのデータを Facebook に一方的に与え続け、選挙に介入することを許容することは、民主主義を毀損する可能性がある**。

個人データに基づいたマイクロターゲティングされた政治広告と旧式の政治広告の違いとは、それぞれの個人に、異なった、そして潜在的に矛盾する情報を見せるという点にある。我々が皆同じ広告を見ているなら、我々はそれについて議論し、ファクトチェックを行い、批判することができる。しかし、**パーソナライズされた広告は、我々の世界の対立と分断をあおり、公共圏を個人が交わることのない現実に砕き、健全な政治的議論ができる見込みを少なくしてしまう**のだ。

「リベラリズムへの脅威」

本節の要点（¶ 49-57, pp. 108-111）：

リベラリズムは公共圏における議論を保証するために、親密圏が堅固であることを要求する。そのためにはプライバシーが重要である。文明的な生活が円滑に送られるためには、健全な程度の寡黙さ（reticence）と秘匿性（concealment）が必要である。もし我々がお互いの心を常に全て読むことができたら、親密圏は縮小してなくなってしまい、公共圏は終わりのない不必要な衝突によって汚されてしまうだろう。**リベラリズムがうまくいくためには、一般市民がある程度の秘密を互いに教え合わないような、慎みの文化（a culture of restraint）が必要なのである**。

ソーシャルメディアはより多くのデータを得るために、人々により多くをシェアするように求める。しかし、秘密、恐れていること、各々のあまり好ましくない部分について全てを教え合うことは、「慎みの文化」ではなく「晒しの文化（a culture of exposure）」につながる。ある程度の慎みを保つのは不誠実ではなく、むしろ互いに対する親切であり、それはリベラリズムにとって重要なのだ。

「個人の安全に対する脅威」

本節の要点（¶ 58-76, pp. 111-116）：

個人データの悪用が個人の安全を脅かした例の一つは、ナチスによるユダヤ人の迫害であり、オランダとフランスの事例は対照的である。オランダの人口記録所の監督官であったヤコブス・ランベルトゥス・レンツ（Jacobus Lambertus Lentz）は、ID カードの携帯システムをナチスに提案し、すべてのオランダの成人は身分証明書を携帯することが求められた。ユダヤ人の携帯するカードには「J」が刻印され、死の宣告が彼らのポケットに入れられた。また、レンツは、人口に関する記録を拡大するために、データを記録、処理するためのパンチカードである、ホレリス機（Hollerith machine）という作表機を導入した。これらの施策により、ナチスがオランダでユダヤ人を追跡することは容易になった。一方、フランスでは、プライバシーを理由に宗教に関する情報を収集していなかった。また、フランス陸軍総司令官であるルネ・カルミーユ（René Carmille）は作表機を手に入れたが、フランス・レジスタンスの最高位の内通者の一人として、ナチスの命令に密かに背いて、データ収集を妨害した。その結果、数十万人の命が、ユダヤ人のデータを収集しないことを選んだたった一人の人間によって、救われた。**このことは、データ収集は人命を奪いうるものである、ということを意味している。オランダにおけるユダヤ人の死亡率は 73%であったのに対し、フランスにおけるユダヤ人の死亡率は 25%であり、大きな差がついた。**

ナチスが記録所へ向かうべきだと知っていたように、今日の悪人はどこで我々のデータを見つければ良いのかを知っている。そして彼らは我々の最もセンシティブなデータを支配下に置くために軍隊をもって侵略する必要さえない。現代においては腕のいいハッカーさえいれば良い。その意味では、リスクはインターネット以前より増大している。

我々は過去の失敗から学ぶべきだ。アスベストは至る所で使われ、取り除くのが困難になった。そして今もなお多くの人々を苦しめている。**同様に、個人データは有害であり、我々は個人データをそのようなものとして規制しなければならない。我々は、アスベストの事例やオランダの事例から教訓を学び、その失敗を繰り返さないようにしよう。**

第 5 章「プラグを抜く」

紹介担当者：豊田樹

第五章全体のまとめ

データ経済はあまりに進行してしまっており、我々のデータが様々な形で利用されてしまっている。このような現状を変えるには様々な点で我々の普段受け入れてしまっているデータ経済を改変する必要がある。その一つは個人化された広告である。テック企業は我々のデータを集めることで個人化した広告を用意するがその効果はその悪影響に見合うものではない。また、個人情報を売買の対象とみなすことやデータの収集をデフォルトに設定することも、われわれ自身を危険な状況に追い込んでしまう。しかし、データ自そのものを集めることだけではなく、個人情報に至ってしまうようなセンシティブな推論も同様に規制されるべきである。

また、データを扱うことにおいて、ビックテックは顧客に信託義務という種類の義務を負う必要がある。というのも、医者や弁護士のように、専門的な技術があり顧客に対して力の差がある際は信託義務が発生するからである。また、同様に重要なのは、サイバーセキュリティを向上させることや、作成から一定期間が過ぎたデータを削除することである。

技術の進歩に個人情報は必要ないかもしれない。これまでの人工知能による成果においてもっとも成功したと考えられるプログラムは個人情報なしで成果を上げたし、新たな抗生物質を探す人工知能も個人情報なしでその成果を上げた。

現在のパンデミックのような事態は通常時では、人々が受け入れないような規制を政府が行う可能性がある。しかしパンデミック対策においても個人情報を用いずに効果を上げることは可能かもしれない。

導入部

導入部の要点（¶ 1-9, pp 117-119.）：

監視経済はかなり進行してしまっている。個人情報は、今や、データ経済から手を引くこと（プラグを抜くこと）が非現実的に聞こえるほど、データ経済の一部になってしまっている。生体情報の歴史的な流出や、ジェノサイド目的での個人データの乱用など、**データ災害（data disaster）**も起きてしまうかもしれない。

人類が災害を避けることができた例も存在する。かつてオゾン層が減少しているということが発覚した際にはフロンの使用や生産に対する反対や代替物の開発により、オゾンも守ることができたし、地球温暖化のペースを遅らせることにも成功した。

このように災害を防ぐことができたのと同様に、プライバシーも守ることができる。本章における勧告のほとんどは、政策立案者へ向けたものであるが、もし、政治家が、我々がプライバシーを気にかけていることを知り、プライバシーを守るための規制をしなければ投票と支援がなくなることを知るならば、彼らを行動させることができる。**我々は、我々が政治家に要求するべきことについて、よく知らなければならない。**

個人化された広告の中止

本節の要点（**¶ 10-32, pp. 119-126.**）：

個人化された広告はデータ経済の悪い側面を生み出しており、それを全面的に禁止することが最もよい解決策であると考えられている。

行動ターゲティング広告は、消費者に対して購入の興味があるものを見せ、広告主が売り上げを高めうる広告のみに費用を払うという特徴を考慮すれば魅力的に思われるが、それによって生み出される悪影響に見合っておらず、その効果も疑わしい。まず、行動ターゲティング広告の効果が疑わしいものであるという研究結果が存在する。つまり、ある研究によると、クッキーを用いた広告による収益の増加はたった 4%（一つの広告につき平均して 0.00008 ドル）にすぎない増加であった。また、ターゲティング広告は非ターゲティング広告に比べて非常に高価である。それに加えて、今日の広告の多く、特にオンラインの広告はせいぜい不愉快であり、最悪の場合忌み嫌われている。

このように、ターゲティング広告はビジネスにおいてあまり効果的ではないかもしれないが、選挙を決定づけることができるかもしれない。Facebook は、実際に、アルゴリズムを変更し、ターゲティング広告を用いることで分断を煽っている。

従って、我々を監視し派手な飛び跳ねる画像で気をそらすような有害な広告を作り出す代わりに、**オンライン広告は、言葉と事実に基づいたものを目指すべきである**と考えることができる。例えば、コンテンツ連動型の広告（contextual advertising）や、情報提供型広告（informative advertising）である。前者は、「靴」と検索した場合に靴の広告を表示し、後者は言葉で情報を提供するタイプのものである。

さらに、**そもそも広告業がデータ経済の大きな部分を占めすぎているので、制限するべき**という主張も存在する。広告に対する支出の割合の増加と幸福度の低下が結びつくという研究結果もある。広告が人々の福利を悪化させないように、広告を制限し、リアルタイム入札も禁止されるべきである。

個人情報の取引の中止

本節の要点（**¶ 33-44, pp. 126-130.**）：

既往歴などの個人情報は売買されたり、搾取されたりするべきではないが、そういっ

た個人情報の悪用の機会は急増している。その一つとしてデータブローカーがある。データブローカーは我々がネットに残すデータの痕跡を収集し、それを必要とする者に売却することで利益を上げている。じっさいに、20 年前、エイミー・ボイヤー（Amy Boyer）は彼女の個人情報と位置情報を Docusearch 社から購入したストーカーによって殺害された。このように利用されるデータは我々の同意なく収集されており、その購入は高価でもない。

こういったデータの利用に対して適切な規制を行うことで、個人情報を通して蓄積される権力が経済的、政治的権力に変化することを防がねばならない。資本主義的な社会であっても一定のものは売られるべきではないということは同意しうるだろう。個人情報もそういったものの一つである。

個人情報の取引はすべてのデータ収集や使用、データの売買を禁止するべき、ということを意味しているわけではなく、適切なやり方であればそれは有効に利用される。また、現在では匿名化されているデータがいつ再識別化されるかわからないので、何が個人情報であるかの厳密な定義が必要である。

デフォルトでの個人情報の収集を停止する

本節の要点（**¶ 45-55, pp. 130-134.**）：

ビッグテックの中には、サービスの利用者の許可なくデータを奪うことで巨大化したものもある。これらの企業のやり方は、消費者の反抗を無視し、しつこく反抗された場合のみそれに対処する。しかし、その時には、すでに我々は、当初は受け入れることのない条件を受け入れてしまっているのである。

われわれが触れるウェブサイトやアプリなどはほぼすべてが我々のデータを収集している。そのデータ収集は我々にリスクを押し付けているのである。現在の法規制の多くはデータの「使用」についてのものであり、データの「収集」についての規制は十分ではない。企業、政府機関、そして、あらゆるウェブサイトやアプリのユーザー設定のデフォルトは、データを収集するべきでない。データ収集についてはオプトアウトよりもオプトインを採用するべきである。

必要なデータは収集されるべきかもしれないが、必要なデータとは、価値あるサービスを提供するために必要不可欠であるデータのとして狭く理解されるべきである。

我々のプライバシーを守りつつデータを収集する方法として「差分プライバシー」が有効かもしれない。差分プライバシーとは、データベースに数学的ノイズを挿入することで、統計的な分析の正確さを損なわずにプライバシーを守ることができる技術である。すべてがこの方法で収集できるとは限らないが、このように、プライバシーを搾取するというよりプライバシーを守る道具の発達に我々はより投資するべきなのである。

秘密裏に行われるセンシティブな推論の中止

本節の要点（**¶ 56-62, pp. 134-136.**）：

前節では、個人情報の収集について論じられたが、ここでは収集に制限がかかってもそれを推論によってすり抜けることが可能であることが指摘される。

例えば、Facebook の「いいね」は性的志向や宗教や政治的見解を推論するのに使用されており、このような直接的に個人情報ではない外的なシグナルが、個人情報に対する推論に使用されている。

こういった推論の懸念点は、個人情報を収集されているということに気づかずに収集されてしまうという点や自分ではコントロールできない外的シグナル（自分の顔やスマートフォンのタイプの方法）から推論されてしまうので、自分を守るためにできることが少ないという点である。また、その推論のアルゴリズムの正確性に問題があるかもしれないにも関わらず、使用され続けるという点も問題である。

適切な場合ではこういった推論も許容されるかもしれないが、たとえそれらが間違っていてもセンシティブな推論は個人情報として扱われるので、個人情報と同程度にきつく制限されなければならない。外的なサインが個人情報の推論に使用されている場合はいつでもデータの主体に同意が求められるべきであるし、彼らは不正確な推論に対して反対し修正する権利を持つべきである。そして、推論されたセンシティブな情報は個人情報としてあつかわれるべきである。

信託義務の履行

本節の要点（**¶ 63-72, pp. 136-139.**）：

信託義務（fiduciary duty）とは、弱い立場にある個人に対して、彼らに仕えることになっている専門家から守るために存在する義務である。例えば、医師や弁護士といった専門家は彼らに依頼する個人の身体上の問題や法律上の問題など、非所に価値の高いものを任されているし、依頼者は彼らに対して非常に弱い立場になってしまう。こうした状況ではそういった専門家は彼らの顧客に忠実であることや配慮の義務を負う。受託者は顧客の利益に最大限適うように行動しなければならない。**個人情報を集める企業などにも同じような義務が存在するかもしれない。**

ビッグテックにも同様の義務が存在するという考えに対しては、「そのような方針は株主に対する信託義務に反する」という批判が行われてきた。しかし、自らの顧客を犠牲にしてまで株主の福利を最大化するべき、という指針は道徳的に疑わしい。これに対しては、ユーザーの利益をつねに株主の利益よりも優先するということを確立する、あるいはユーザーに対する信託義務の違反に十分な罰則を設ける、という選択肢が存在する。

信託義務によってビッグテックの利益とユーザーの利益は一致に向かうかもしれない。

サイバーセキュリティの基準の向上

本節の要点（**¶ 73-83, pp. 139-143.**）：

前節まででプライバシーが守られる際に問題となる点をそれぞれ見てきたが、そもそも我々の用いるアプリやガジェットが安全でない限り、プライバシーは守られないだろう。企業の側からすれば、サイバーセキュリティに投資して得られるものはあまり多くない上に、悪い結果が生まれた場合にも被害を受けるのは顧客である。

2001 年以降、プライバシーは失われたが、その代わりにセキュリティが向上しているわけではなかった。企業や政府が我々を安全に保つためにデータを引き抜くことを許可されたが、その結果インターネットは安全ではなくなってしまったのである。

我々はパンデミックを予想できたのにも関わらず準備を怠っていた。大規模なサイバー攻撃が行われるということも予想されているので、対策を行う必要がある。また、新型コロナウイルスのパンデミックの結果として、サイバー攻撃は急増している。非常に多くの人が安全でない Wi-Fi やデバイスを使って家から仕事をしているので、いわゆる「攻撃対象領域（attack surface）」、つまり侵入可能な場所が増えたのである。サイバーセキュリティを強化するには、システムを切り離すことが重要である。スマートケトルとスマートフォンが接続されていれば、前者を通じてあなたのスマートフォンにアクセスすることが可能かもしれないのであって、このようにあまりに多くのシステムがすべて接続されているということは、サイバー攻撃に対してのリスクを高めることになってしまう。

データの消去

本節の要点（**¶ 84-105, pp. 143-150.**）：

既に生み出されたデータに対して、それらを消去する計画が存在しなければならない。忘れるということは個人にとって重要な能力であるだけでなく、社会にとっても必要なものである。すべてのことを記録し、記憶している社会は不寛容になる傾向がある。現代はこれまでのどの時代よりも多くのことを記憶している。かつては記録を燃やすなどの自発的方法、自然に忘れたり摩耗で失ったりするという非自発的な方法でものごとを忘れていた。現在までは記録を残すことはコストのかかることだった。

デジタル化した現在では、デジタル化、安価なストレージ、簡単な検索（復旧）とグローバルな到達領域の四つの技術的な要素によって記録がデフォルトにされている。

こうして多くのデータを保持することで我々は賢くなり、より良い決断を下すことができるようになってきていると考えたくなるが、何が重要なデータかを選別することが難しくなる。そのことが事実を歪めて、変化の障害になってしまうというリスクを生み出し、広範かつ永続的な記録を危険なものにしてしまう。

我々は個人情報を無期限に保存することをやめるべきである。しかし、社会に対して忘れること、データを消すことを強制することは倫理的に不可能であるという批判も存在する。確かに本を燃やしたり、オンラインの投稿を削除したりするのは権威主義的な政府が行うことであり、民主的な政府はデータを蓄積する。だが、永久にデータを保持することが可能になった我々は、忘れるという自然さをもう一度導入するべきである。

データを削除できなくとも、厳重な補完の下で残しておくことで、データを保持することの利点とプライバシーの保護を両立できるかもしれない。忘れられる権利によって、個人情報の内の公共の利益をもたらさなかったり、目的を欠いていたりするものにアクセスすることを難しくすることが可能であり、このことよって我々を保護できるということが重要である。

個人情報の追跡

本節の要点（**¶ 106-110, pp. 150-152.**）：

個人情報の規制についてのもっとも大きい課題の一つは、データを取り締まることの難しさである。ヨーロッパのデータ保護機関はしばしば人員不足で資金不足なので、有効な取り締まりを行えていない。各人が自分のデータを誰が保有しているかを知ることができないことが非対称性を悪化させている。我々は自分のデータを追跡できないので、今この時も、あるアルゴリズムが我々を信用できないとタグ付けしているかもしれないし、同時に、他のアルゴリズムが（もしかすると見当違いの基準に基づいて）必要としている手術の順番をさらに遅らせることを決定しているかもしれないということに気づけないかもしれない。

データの追跡についての技術的課題は、データについての同意と個人情報のタグ付けによるプライバシーの喪失という二点が少なくとも存在する。前者に関しては、自分のデータから何が推論されるかを知るのは難しいので、そのデータから知られてしまうかもしれないことに関係する人全員に同意を求めることは難しい。また、後者に関しては、個人情報を追跡するために、情報に個人情報をタグ付けすることで、そのことが自分の情報をさらすことになってしまうかもしれない。

政府の監視の抑制

本節の要点（¶ **111-116, pp. 152-154.**）：

政府は市民の安全を守るために大規模な監視を行う必要はなく、対象を絞り、状況に対して適切なものでなければならない。監視を行うのであれば、監視に関連するすべての情報にアクセスできるようにするべきであり、透明性が必要である。監視の詳細は公開されるべきであり、対象は絞って行われなければならない。

データについてのデータであるメタデータは暗号化されず、かなりセンシティブなものなので、プライバシー保護についての課題となっている。権威主義的な政権がメタデータに対してアクセスすることを阻止しなければならない。

監視設備の禁止

本節の要点（¶ **117-118, pp. 154-155.**）：

あまりに危険な監視技術が存在する。**顔認証や歩行、心拍認証などは匿名性を破壊する技術なので禁止が検討されるべきであり、高解像度衛星やドローンも排除されるべきである。**

プライバシーに投資する

本節の要点（¶ **119, p. 155.**）：

ビッグテックに対抗するためには、プライバシーツールの開発だけでなくよりよいデータ管理が必要であり、プライバシー保護機関への全面的援助も必要である。

独禁法を更新する

本節の要点（¶ **120, p. 155.**）：

独禁法の規制はデジタル時代の現実を反映しなければならない。

子供たちを守る

本節の要点（¶ **121-129, pp. 155-158.**）：

子供は特に傷つきやすい立場にあるため、守られるべきである。幼児は、彼らの安全を守るため、という口実で監視されてしまう風潮がある。

子供を特に気にかける理由は、監視は子供の未来を危険にさらしてしまうということと、過剰な監視は精神を破壊することがある、ということである。健全な成長のためには、自分の失敗が記録されないといったことが必要であり、失敗して学ぶことが必要なのである。

子供のケースの難点は、彼らの安全にある程度の監視が必要である、というところにある。学校での監視は卒業後に彼らがさらされるであろう監視に慣れさせるという意味で教育であると主張するものもいるが、そのような権利をないがしろにする教育をうけた人々が大人になって権利を尊重するということは不可能なように思われる。

子供に過度な監視を施すことは、彼らに自己検閲を教えこみ、責任のある大人になるのを妨げていることになるかもしれない。

個人情報は必要ないのだろうか

本節の要点（**¶ 130-137, pp. 158-160.**）：

本節では、イノベーションとデータ蓄積の関係が問題となる。**データ経済を制限することはイノベーションを止めてしまうわけではない。というのも、進歩とは人間の権利を侵害するものであってはならず、権利を守るものでなければならないからである。**

ここでいう進歩を技術的なものに限ったとしても、プライバシーを犠牲にして発展させるべきではない。グーグルのような企業は個人情報から利益を出すのではなく、自身のサービスに対して対価を受け取って利益を出すべきであり、過剰に個人情報を収集するべきではないかもしれない。

さらに、これまでで最も高度な AI が個人情報なしに作り上げられてということは、技術の発展に個人情報の搾取は必要がないということを示しているかもしれない。グーグルの DeepMind によって開発されたアルゴリズムである AlphaZero は、外的なデータを用いず、自らとの対戦を行って十分に能力を発展させた。

医療について

本節の要点（**¶ 138-139, pp160-161.**）：

医療とは、データにまつわる領域の中でも特殊なものである。その三つの理由は、我々にとっての医療の重要性、医療データのセンシティブさ、医療データの匿名化の困難さの三つである。

個人情報に依存しない医療の進歩も可能かもしれない。

医療に関するデジタル技術の展望

本節の要点（**¶ 140-149, pp. 161-164.**）：

デジタル技術が医療の分野で期待を下回る結果しかもたらせなかった実例が二つ存在する。IBM と DeepMind の医療用 AI の例は、医療に AI を適用することの難しさと、それが患者を助けることができないかもしれないことを明らかにした。ある近年のメタ

アナリシスは約 2 万個の研究に注目したが、それらの内のたった 14 個のみが、臨床的環境でそのアルゴリズムを試験するのに十分な方法論的な質を備えていたことを、研究者たちは明らかにした。

さらに、医療に AI 技術を導入することには、誤診断によって患者を傷つけてしまう可能性がある。また、AI などのデジタル技術には故障というリスクも存在する。

医療にデジタル技術を導入するならば、DeepMind と Royal Free が行ったよりも倫理的に行う方法がある。そこには、医学研究に参加する人々のデータの利用や削除について規定しておくことや、患者のデータを用いて行われる取引は患者の利益になることを確実にすることなどが含まれる。

倫理的な医学研究

本節の要点（**¶ 150-153, pp. 164-165.**）：

医療の場において被験者の同意の適切さや保護、補償なしに、彼らを研究に参加させるべきではない。医療に関する実験に参加した人々のデータは、被験者が有利になる仕方で扱われるべきである。

個人情報を用いない医学的進歩

本節の要点（**¶ 154-159, pp165-167.**）：

囲碁の世界で個人情報を用いずに作り上げられた AI である AlphaZero は優れた功績である。これと同じように、**個人情報を用いないで医学的進歩を成し遂げた実例として薬物に耐性を持ち始めたバクテリアに対する抗生物質の発見がある。**

MIT のある研究グループは、数千の薬品と天然化合物の原子的、分子的性質についての情報をコンピュータープログラムに与えて、バクテリアを殺すような分子の種類を同定することができるようにアルゴリズムをトレーニングした。その結果、新しい抗生物質である halicin は強力で、バクテリアがまだ耐性を発達させていない新しい方法で働くということが分かってきている。

危機への警告

本節の要点（**¶ 160-174, pp. 167-173.**）：

この本が執筆されているタイミングもパンデミックが拡大していた。このパンデミック下では、その対策として徹底的な検査ではなく接触追跡アプリが採用された。**この接触追跡アプリはプライバシー的あるいはセキュリティ的なリスクを持ち込むことになる。**

また、ここでアプリという対策が優先されたことの背景には、技術についての魔術的思考、つまりデジタル技術はすべての問題を魔法のように解決してくれるだろうという期待が存在するかもしれない。

パンデミックのような緊急事態は国家の権力を強めるような政策を実施する口実となってしまいがちである。このパンデミックは 9.11 のように特別な措置を受け入れてしまう機会になってしまうかもしれない。危機の間は、大損害をもたらす大災害を止めるために必要なことは何でもしたくなりがちである。**しかし、逼迫した災害を抑制する方法について考えることに加えて、嵐が去った後に残るであろう世界についても考える必要がある。**

今がその時である

本節の要点（**¶ 175, p. 173**）：

今がデータ経済を変革するために行動すべき時である。

第 6 章「あなたができること」

紹介担当者：中村貴行

第六章全体のまとめ

監視資本主義はあなたの協働と同意に依存している。監視資本主義に抵抗し、プライバシーを守る文化を作り出し、社会を変えるためにあなたができることと、その際の注意点について具体的に述べよう。

導入部

導入部のまとめ（¶1-12, pp.175-178）：

社会における変化は、最初は信じられないものであっても、実際に起こる。そして、我々は物事を良い方向に変化させることができる。資本主義が権利を侵害するのならば、我々は資本主義を制約しなければならない。監視資本主義は我々の協働に立脚しているので、我々が監視資本主義との協働をやめれば、我々は社会の仕組みを変えることができる。

それに関係して、以下の 3 点が重要である。第一に、便利さは過大評価されている。便利さによって我々は有意義な努力をしなくなりがちである。第二に、現在のプライバシーを守ることは、未来のプライバシーを守ることにつながる。仮にあなたが現在プライバシーを必要としていないように思えても、あなたは未来においては隠したいことができるかもしれないし、あなたの国家は人権を尊重しなくなるかもしれない。第三に、プライバシーは集団的なものであり、あなただけではなくあなたの愛する人や知人にも関係する。以下ではプライバシーを守るためにあなたができることを挙げよう。

シェアする前によく考えよう

本節のまとめ（¶13, pp. 178-179）：

Facebook などのプラットフォームの情報は、無数の企業や政府に利用される可能性がある。何かを投稿する際は、あなたを害す形で使われうる情報が含まれないかに気をつけよう。そしてそれは想像力を要求する。例えば、指の写真からは指紋の情報が読み取られうるのだ。

他者のプライバシーを尊重しよう

本節のまとめ（¶14-19, pp.179-180）：

他者の写真や音声記録をオンラインに投稿する際には同意を求めよう。
誰かを家に招く時には、あなたが持っているスマートデバイスについて警告しよう。
子供もプライバシーを持つことを心に留めておこう。
興味本位で DNA テストをするのはやめよう。
他者があなたにアクセスを許しているプライベートな情報を晒すと言ってその人を脅すのはやめよう。

プライバシー空間を作り出そう

本節のまとめ（¶20, pp. 180-182）：

パーティや講義、学会などでプライバシーに配慮するルールを定めて、プライバシーを享受できる場所を作り出そう。

「NO」と言おう

本節のまとめ（¶21-22, pp. 181-）：

オンラインで個人データの収集への同意を求められたら、「No」と言おう。「Yes」と言う誘惑は強いが、一つ一つのプライバシー喪失が積み重なって大きな違いを生むのである。「No」と言うのが困難なウェブサイトがあれば、そのサイトを使わず代わりのサイトを使おう。

プライバシーを選ぼう

本節のまとめ（¶23-34, pp. 182-187）：

プライバシーに配慮しない選択肢とプライバシーに配慮した選択肢がある場合は、プライバシーに配慮した選択肢を選ぼう。

- デバイス
  - Alexa や Google Home のようなデジタルアシスタントを買う前によく考えよう。家に置くなら、設定を調べてプライベートな設定にしよう。
  - ノートパソコンやスマートフォンを買うときは、メーカーとの利害の衝突がないかを調べよう（メーカーが個人データを搾取して収入を得ている場合、そのメ

ーカーの製品は買ってはならない)。
  - プライバシーに関する最新のニュースを読もう。Huawei や ZTE のニュースの例がある。
- メッセージアプリ
  - エンドトゥエンドの暗号化を提供しており、プロバイダがあなたのメタデータを悪用したり、メッセージをクラウドに無防備に蓄積したりしないことが確信できることが重要である。
  - Signal はメッセージに有効期限を設けることができるので、有効な選択肢である。Telegram もあなたがいつでもメッセージを消去できるため、言及に値する。しかし、Telegram は暗号化の安全性が Signal に劣るし、メッセージがデフォルトでは暗号化されないという欠点がある。
- E メール
  - プロバイダを選ぶときは、暗号化が簡単かどうかと、プロバイダが拠点としている国がどこかを吟味しよう。チェックする価値のある選択肢には、Protonmail(スイス)、Tunatora(ドイツ)、Runbox(ノルウェー)がある。
  - E メールにはトラッカーが含まれている可能性がある。E メールアドレスはそれを求める会社や個人の全てには渡さないようにしよう。もしくは偽のアドレスを渡そう。
  - 企業に E メールを求められた時に、myemail+企業名+@email.com というアドレスを教えるというテクニックもある。あなたは依然として E メールを受け取れるが、その企業があまりにもうるさくなった時にはそのアドレスを封鎖することができるし、E メールが漏洩しても、どの企業に責任があるのかがわかる。
- 検索エンジン
  - ブラウザのデフォルトの検索エンジンを、不必要なあなたのデータを収集しないようなものに変えよう。プライバシーフレンドリーな選択肢には DuckDuckGo や Qwant が含まれる。
- ブラウザ
  - 異なる活動には異なるブラウザを使おう。サインインしなければならないサイトと、ブラウジングのためのブラウザを分けよう。
  - Brave, Vivaldi, Opera はプライバシーを念頭に置いたブラウザだ。Firefox と Safari も適切なアドオンを使えばそうだろう。

プライバシーのための拡張機能とツールを使おう

本節のまとめ（¶35-41, pp. 187-190）：

アドブロッカーを使うと、広告をなくすことができる。また、この種の広告文化に同意

していないことを示すことにもつながる。Privacy Badger、DuckDuckgo Privacy Essentials は有効だ。

HTTPS Everywhere は Electronic Frontier Foundation によって開発された拡張機能であり、あなたの多くの主要なウェブサイトとのやりとりを暗号化する。

信頼に値しない拡張機能もある。拡張機能を使う前に、手早く検索をかけてそれが安全なものであることを確かめよう。

Tor ブラウザはあなたをオンラインで匿名化する。デメリットは、検索が遅くなってしまうことと、情報機関に目をつけられる可能性があることである。

VPN もあなたの通信をプライベートにするツールの一つである。

設定を変えよう

本節のまとめ（¶ 42-43, p. 190-191）：

あなたが得ようとするプライバシーのレベルに合わせて設定を変更しよう。1 年に 1 回は設定を確認しよう。企業は頻繁に規約を変更するからだ。

電子データをため込まないようにしよう（don’t cyberhoard）

本節のまとめ（¶ 44-45, pp. 190-191）：

デバイスに不要なデータを溜め込まないようにしよう。オンラインにあるデータのバックアップを作成し、それを暗号化されたハードドライブに保存して、そのデータをインターネットから削除するのが良い。

強いパスワードを選択しよう

本節のまとめ（¶ 46, p. 192）：

強いパスワードを使おう。重要なのはパスワードの長さである。

難読化を使おう

本節のまとめ（¶ 47-49, p. 191-193）：

監視とデータ収集を阻害するために、曖昧で混乱するような、ミスリーディングな情報を意図的に付加しよう。真実とは異なる名前、誕生日、e メール、居住地等を教えることを検討しよう。アカウントやガジェットを共有することも有効である。

アナログでいこう

本節のまとめ（¶50, p. 193）：
アナログの製品を活用しよう。

新聞を買おう

本節のまとめ（¶51-52, p. 193-194）：
新聞を買うことで、報道機関の独立を支援しよう。企業や政府の隠していることを報道するには、独立している必要があるからだ。また、ソーシャルメディアのコンテンツは品質が疑わしいだけではなく、トラッキングの危険性もある。

プライバシーを要求しよう

本節のまとめ（¶53-58, p. 194-195）：
企業や政府にプライバシーを尊重するように要求しよう。要求することで、彼らはちゃんと機能しなくてはならなくなる。また、要求することによって彼らに大衆が同意していないことを知らせることになる。
医師などの、あなたと交流しあなたにデータを求める専門家にプライバシーを要求しよう。プライバシーを要求するために、法律などをよく読んであなたの持つ権利について知っておこう。議員とコンタクトを取り、正しい候補に投票しよう。企業のプライバシーポリシーが良くないときは、Trustpilot のようなウェブサイトで悪い評価を下してプライバシーに言及しよう。

彼らに依存してはならない

本節のまとめ（¶59, pp. 195-196）：
一つのテック企業に依存するのは危険である。できるだけ一つのプラットフォームやアプリ依存しないように心がけよう。

あなたはテック業界で働いていますか？

本節のまとめ（¶60-67, 196-198）：
あなたがテック業界で働いているのなら、あなたには製品にプライバシーを最初から織り込む大きな役目がある。テック業界の人々は、どんな風に思い出されたいかについて

考えてみるべきである。民主主義を破壊した人々の一人として思い出されたいのか？それともデータの見通しを修正するのを手助けした人々の一人として思い出されたいのか？

全ての個人は、組織に対して貢献することに対して道徳的責任を持つ。あなたが人々を害する可能性のあるプロジェクトに従事しているかもしれないと考えたなら、雇用者をより倫理的なプロジェクトに向かわせるか、転職を考えても良いかもしれない。

テック企業の従業員は協働して抗議すればより大きな違いを生むことができる。

プライバシーについて憂慮している、アカデミアにいる人や非営利組織を頼ることもできる。Bruce Schneier や Cathy O'Neil、Yves-Alexandre de Montjoye のような人々の著作は参考になる。Electric Frontier Foundation、Privacy International、European Digital Rights、そして noyb は良い情報源だ。

あなたがスタートアップに出資する人になったら、出資する企業が倫理審査を経ることを確実に求めるようにしよう。

ベストを尽くそう

本節のまとめ（¶ 68-72, pp. 198-200）：

プライバシーを守る対策は常にうまくいくわけではないが、ベストを尽くそう。第一に、あなたはあなたのデータをいくらか守ることができるかもしれない。第二に、あなたは他の誰かのデータを守ることができるかもしれない。第三に、プライバシーを守る試みは、社会に対するメッセージとなる。

企業と政府に我々のプライバシーを守るように働きかけるかどうかは我々次第である。そして我々の文化に影響を及ぼすために、あなたが完全を達成する必要はない。

受け入れられないものを拒否しよう

本節のまとめ（¶ 73-76, pp. 200-201）：

世界をより良い場所に変えた人々に共通することは、受け入れられないものを拒否するということである。プライバシーの侵害に無関心であることや、諦めの感情を抱くことは適切ではない。

自分を無力だと思ってはならない。デジタル経済はあなたの協働と同意に依存している。

世界人権宣言は、我々に人権を守り、最後の一線を超えないように警告している。プライバシーは正当な権利である。それを守ろう。