特集／米国の対中国等懸念国規制強化の動向

〈2〉経済安保としてのデータセキュリティ
～米国の最終規則に見る「データの武器化」～

IISE 国際社会経済研究所 特別研究主幹
信州大学　特任教授
海上自衛隊幹部学校　客員研究員
布施　哲

はじめに

「あなたのことを最も知っているのはグーグルかもしれない」。

私たちは日常的にインターネットに接続されたデジタルサービスを利用することで様々なデータを生み出し、それらのデータはデジタル事業者によって取得、活用されている。

IP アドレスや年齢、氏名などの属性情報、検索履歴、購買履歴、「いいね」した回数とトピック、友達とのつながり、位置情報といったデータを分析、利用してデジタル事業者はユーザー個人単位の嗜好や購買欲求を分析、予測してデジタル広告を生成し、ユーザーの行動や認識の変容を日々、促している。

広告ターゲットの解像度は高く、市場やグループ単位ではなく個人単位への働きかけを可能にしている。それを可能にしているのはマイクロ・ターゲティングと呼ばれる手法で、Google や Facebook（メタ社）などの大手インターネットプラットフォーマーの収益源となってきた。

こうしたビジネスの一環として行われてきた個人単位のプロファイリングを可能とするマイクロターゲティングの手法は近年、国家安全保障や諜報の領域において敵対勢力によって利用される（＝武器化される）リスクが議論されるようになっている[1]。

国家安全保障上のキーパーソンをデータを使って特定して脅迫やリクルート対象とすることや、認知戦のターゲットにするといった「データの武器化」の脅威である[2]。こうした流れを受けて国家安全保障の文脈でもデータを保護するデータセキュリティ[3]の議論が台頭しつつある。

さらには AI 時代の到来により、AI の性能を左右するデータは産業競争力や経済安保の観点からも重要な意味を持つようになりつつある。AI 利活用が国力を左右するとも言われる中では AI の性能を左右するデータは戦略物資であり、その保護のあり方を定めたデータセキュリティは経済安保の重要施策として捉えられるべきであろう。

そこで本論ではデータセキュリティを国家安全保障の観点から位置付けて規制を定めた米司法省による最終規則を詳述することで、国家安全保障におけるデータが持つ意味と価値について考察するととも

[1] Kirsten Hazelrig, “Intelligence After Next: Surveillance Technologies Are Imbedded Into The Fabric of Modern Life- The Intelligence Community Must Respond,” MITRE, January 2023. https://www.mitre.org/sites/default/files/2023-01/PR-22-4107-INTELLIGENCE-AFTER-NEXT-14-January-2023.pdf
[2] Ibid.
[3] 本論が対象とするデータは個人情報に加えて、安全保障関連データ、営業データ、技術データ、事業（産業）データとする。データ定義などの詳細は経済産業省『産業データの越境データ管理等に関するマニュアル』令和 7 年 1 月 27 日を参照。

に国家安全保障上のニーズに基づいたデータセキュリティの意義、課題を明らかにする。

そのうえで同規則が残した課題である、データセキュリティが持つ経済安保の側面についても検討し、日本の経済安保政策へのインプリケーションとする。

1. マイクロ・ターゲティングという軍民両用技術

「現代における戦略物資は石油ではなくデータ」[4]だと指摘されて久しい。

この言葉にはデータが取引、交換、所有、奪取が可能な、デジタル経済における価値を裏書きする戦略物資で、かつ貨幣のような存在でもあるとの意味が込められている。

実際、巨大インターネット・プラットフォーマーをはじめとする企業はデジタルサービスを通じて得られたデータを分析、活用することによって顧客が求めるニーズが何かを特定し、顧客の属性や潜在ニーズにフィットした働きかけ（デジタル広告やクーポンの提示、商品ラインナップの改善など）をおこなうことで巨額の売り上げと利益を生み出している[5]。

そうした自社のデジタルサービスを通じて得られた顧客やユーザーに関するデータを分析することで個人単位でターゲットを絞って働きかけをおこない、ユーザーの行動や認識の変容を促す手法をマイクロ・ターゲティングと呼ぶ[6]。マイクロ・ターゲティングはデジタル広告やECサイト、選挙運動などで多用されている。

米の大手スーパーのターゲット社は自社のショッピングサイトで顧客の属性を把握し、購買履歴、検索履歴の変化から顧客のライフスタイルの変化やそれに伴う嗜好の変化を予測して、将来、顧客が必要とするであろう商品のオンライン・クーポンやインターネット広告を表示することで購買行動を促している[7]。

たとえば女性客がオンライン・ストアで無香料のローションや除菌シート、葉酸、亜鉛などのサプリメントを購入すると、自社のアルゴリズムが妊婦だと判定してマタニティグッズのクーポンを表示するといった具合である。ターゲット社では「妊娠予測スコア」の算出の指標となる25の製品を指定しており、該当製品の購入履歴に応じたスコアリングがされているという[8]。

こうしたデータによってユーザーのライフスタイルの変化、嗜好の変化を予測して先回りするサイクルをいかに精度高く高速に実行できるかが企業の市場優位性に直結する時代になっている。

その成功例が若い女性を中心に絶大な支持を集めている中国発のファスト・ファッションECサイトのSHEIN（シーイン）である。ユーザーがどのような商品を検索したか、カートに入れられても購買に結びつかなかった商品は何か、SNS上で人気を集めているデザインや服は何かをAIがリアルタイムで分析している。消費者が求める最新トレンドをいち早く掴んで商品化して、ユーザーの購買行動（あるいは認識）の変容を促すサイクルを高速化させていることが強みとしている。

まさにマイクロ・ターゲティングによってデータは価値を生み出すものとなり、そのサイクルの精度とスピードはAIによってさらに向上している。たとえばFacebookユーザーが押した「いいね」が68回分あれば、アルゴリズムは人間よりも高い精度で

[4] “The World’s Most Valuable Resource is No Longer Oil, but Data,” *The Economist*, May 6, 2017.
[5] 特にメタ（Facebook）のデジタル広告市場における優位性は後述するマイクロ・ターゲティングが基盤となっている。Paul Hitlin, Lee Raine, and Kenneth Olmstead, “Facebook Algorithms and Personal Data” Pew Research Center: Internet, Science and Tech Report, January 16, 2019.
[6] Sasha Issenberg, The Victory Lab: The Secret Science of Winning Campaign, Reprint Edition (New York: Broadway Books, 2013), Justin Hendrix and David Carrol, “Your Own Devices will Give the Next Cambridge Analytica Far More Power to Influence Your Vote,” *MIT Technology Review*, April 2, 2018.
[7] Kashmir Hill, “How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did,” *Forbes*, Updated Aug 11, 2022.
[8] Ibid.

そのユーザーの人種、支持政党、性的嗜好、飲酒の有無などが推定可能だとする分析もある[9]。データが戦略物資と呼ばれる所以はまさにここにある。

2. マイクロ・ターゲティングを使って武器化されるデータ

ビジネスで活用されているマイクロ・ターゲティングは敵対国によって悪用されて国家安全保障上の脅威となることも懸念されている[10]。具体的には個人の弱みを特定して脅迫や強要（スパイ勧誘）をしたり、位置情報の把握による監視や軍施設や秘密施設の位置の特定、サイバー攻撃のための基礎情報の取得などである[11]。

さらにマイクロ・ターゲティングは情報戦や認知戦のツールにもなり得る。ターゲットのデジタル上での行動データから導き出された嗜好にフィットする形で生成したナラティブや偽情報を打ち込んで、投票行動や政治行動、認識を誘導するといったリスクが挙げられる[12]。

民間の商用デジタルサービスのデータが武器化される懸念が意識された事例はフィットネスデータのアプリ Strava をめぐるものだった。Strava はスマートフォンや PC にランニングやサイクリングの経路データを記録するもので、ランニングした時間と経路が「ヒートマップ」という形で地図上に示される。米軍兵士が基地内外をランニングした経路データによって基地内外のアクセス経路の利用パターンが把握されるセキュリティ上のリスクが問題視された[13]。シリアなどに所在する米軍の秘密基地の位置を暴露するケースもあって、米軍当局は兵士に対して派遣中の同サービスの利用を禁止する措置を出している[14]。

BBC が報じたカブールにあったバグラム空軍基地における兵士の行動を表すヒートマップ（Fitness app Strava Lights Up Staff at Military Bases, BBC, January 29, 2018. https://www.bbc.com/news/technology-42853072 より）

---

[9] Craig Silverman and Ryan Mac, "Facebook Gets Rich Off Of Ads That Rip Off Its Users," BuzzFeed News, December 10, 2020. Brittany Kaiser, *Targeted*: *The Cambridge Analytica Whistleblower's Inside Story of How Bid Data*, *Trump and Facebook Broke Democracy and How It Can Happen Again*, (Harper, 2019), p.398.

[10] Jessica Dawson and Katie Matthew, "Data as Ammunition-A New Framework for Information Warfare," *The Cyber Defense Review*, Summer 2024., Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review*, Winter 2021.

[11] Hazelrig, Intelligence, *MITRE*

[12] 2016 年の米大統領選挙において Facebook から得られたユーザーデータが選挙運動悪用された事件では Facebook で得られた個人情報やデータに加えて、購買データ、教会への礼拝の有無、チャリティー活動への参加の有無、航空会社の会員資格の有無、アミューズメントパークへの入園の有無などのデータを合わせて分析することで、選挙区ごとにどの候補をどの程度、支持しているかのプロファイリングをおこなって、そのプロファイリングに応じて政治広告やメッセージを調整する試みがされたとされている。Christpher Wyle, *Mindf*ck*: *Cambridge Analytica and the Plot to Break America* (New York: Random House, 2019).

[13] Matt Burgess, "Strava's Data Lets Anyone See the Names(and Heart Rates) of People Exercising on Military Bases," *Wired UK*, January 30, 2018.

[14] Ibid.