総務省 学術雑誌『情報通信政策研究』 第 9 巻第 2 号
Journal of Information and Communications Policy Vol.9 No.2

調査研究ノート（査読付）

ターゲティング広告配信におけるデータクリーンルームの４機能とその個人情報保護法の下での評価

猪谷 誠一 [1]

要　旨

日本のインターネット広告売上の約半数を占めるディスプレイ広告には、ユーザを識別しての追跡が不可欠である。従来サードパーティクッキーやモバイル広告識別子によって行ってきたユーザの追跡は、近年高まるプライバシー保護の社会的要請によって困難となっている。それに加えて、人々の生活や実店舗のデジタル化が進んだ結果、今やマーケティングデータは識別子や取得主体、取得の文脈等の異なるデータが断片化して並立しており、実務上大きな課題となっている。データクリーンルーム（DCR）はこの断片化したデータを保有者が開示することなく共有し、分析や協業を可能にするものとして近年注目されている技術である。本稿では、ターゲティング広告配信の文脈において、DCR が利用企業に提供する機能を(1)データ拡充、(2)統計・モデル作成、(3)アクティベーション、(4)広告効果測定に分類することを提案する。この４機能について考えられるデータフローを列挙したところ、計 23 パターンが得られた。そこで 23 パターンそれぞれにおいて広告主、パートナー、DCR ベンダに適用される個人情報保護法上の規律を検討した。その結果、DCR によってユーザデータが開示されないことが保証されていたとしても、個人情報保護法上の義務が免じられるケースがないことがわかった。最後に DCR の４機能すべてを提供するためのデータ移転の検討を行い、DCR 参加者いずれもが個人データの第三者提供として DCR 利用に伴うデータ提供を整理する形が適当であることを明らかにした。

キーワード：インターネット広告、個人関連情報、個人情報保護法、第三者提供、データクリーンルーム、統計情報

１．はじめに

現代人の生活には情報が不可欠である。仕事だけでなく家庭生活や余暇や娯楽にも情報、特に電子化された情報が深く入り込んでいる。特に近年の先進国ではスマートフォンの利用の伸びが著しい。2024 年の日本人のスマートフォン平均使用時間は 1 日当たり約 162 分で前年より約 10 分増加した [2]。一方、いわゆる４マスの接触時間はいずれも減少し、差し引き合計するとメディア総接触時間は約 433 分となった。これは 1 日の 30%に相当し、睡眠時間（1 日平均約 462 分）とほぼ等しい。このメディアを介した情報接触を支えているのが広告である。2024 年の日本の広告費は 7 兆 6730 億円で前年比 104.9%を記録した [3]。そのうちマス４媒体の広告費は前年比 100.9%の 2 兆 3363 億円、インターネット広告費は前年比 109.6%の 3 兆 6517 億円であった。

[1] 一般財団法人情報法制研究所上席研究員

[2] 株式会社博報堂ＤＹメディアパートナーズ メディア環境研究所「メディア定点調査 2024」(2024)。

[3] 株式会社電通「日本の広告費 2024」(2024)。

インターネット広告は大きく検索エンジンの検索結果に連動して表示される「検索連動広告」[4]と、ウェブサイトやアプリ上に画像や動画の形式で表示される「ディスプレイ広告」に分けられる[5]。前者は 2024 年日本のインターネット広告売上の約 40%を占める[6]。検索が行われると、検索語と関連するキーワードに関するオークションが開催される。広告主が予めキーワードに対する入札戦略を指定しておくことで、入札金額や広告文、ランディングページ [7]の情報を入札し、一定以上の評価を得た広告が表示される仕組みである[8]。後者はインターネット広告売上の約 54%を占める[9]。ユーザの属性や関心、コンテンツの内容等に基づいて適切な広告を選択してユーザがアクセスした媒体の広告枠に配信を行う。配信にはアドネットワーク、アドエクスチェンジ、DSP（Demand-Side Platform）、SSP （Supply-Side Platform）といった数多くの事業者が介在している [10]。

ディスプレイ広告では、誰にどの程度の頻度や回数でどのクリエイティブ [11]を表示するかを制御し、広告がユーザにどのような行動を喚起したか測定するため、ユーザを識別して追跡する必要がある。ウェブでは主にクッキー、アプリではスマートフォン OS が提供するモバイル広告 ID による追跡が一般的であった。特に広告配信事業者が発行するサードパーティクッキーがその中心的役割を果たしてきた。

しかし近年、プライバシー保護への社会的関心が高まることで追跡のための技術への制約が強化されている。サードパーティクッキーを例にすれば、Apple はウェブブラウザ Safari において 2017 年に制限を開始し 2020 年には完全にブロックするようになった [12]。Firefox は 2018 年に [13]、Microsoft の Edge も 2020 年にサイトをまたいだトラッキングをブロックするようになった [14]。自社収益の多くを広告に依存する Google も Chrome でのサードパーティクッキー廃止計画を 2020 年に発表したものの、3 度にわた

4 「リスティング広告」とも呼ばれる。
5 公正取引委員会「デジタル広告分野の取引実態に関する最終報告書」(2021), 11 頁
6 株式会社電通「2024 年日本の広告費 インターネット広告媒体費 詳細分析」(2025) https://www.dentsu.co.jp/news/release/2025/0312-010858.html 最終アクセス: 2025 年 12 月 18 日以下全て同様。
7 広告をクリックした後に表示される広告主のページのこと。
8 評価はユーザの検索との関連性やランディングページの質なども合わせて行われるため、最も高額な入札を行った広告ばかりが表示されるわけではない。
9 株式会社電通・前掲注(6)。
10 一般財団法人情報法制研究所オンライン広告研究タスクフォース「オーディエンスターゲティング広告における匿名加工情報の利用に関する提言」(2017) https://www.jilis.org/proposal/data/2017-12-18.pdf, 10–14 頁。
11 広告として表示される具体的な画像や動画のこと。
12 John Wilander “Full Third-Party Cookie Blocking and More” (2020) https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
13 Mozilla Corporation “Firefox Focus New to Android, blocks annoying ads and protects your privacy” (2017) https://blog.mozilla.org/press/2017/06/firefox-focus-new-to-android-blocks-annoying-ads-and-protects-your-privacy/
14 Microsoft Edge Team “Safety and privacy in Microsoft Edge” (2020) https://blogs.windows.com/msedgedev/2020/10/26/safety-privacy-cyber-security-awareness-month/

って延期し、2024 年 7 月には廃止計画そのものを廃止した[15]。ただし Google もサードパーティクッキーへの依存を減らすことを模索している[16]。

これに加え、スマートフォンでのアプリ利用拡大、プラットフォーム事業者や EC サイト等クローズドなエコシステム（ウォールド・ガーデン。以下、「WG」という。）の伸長、店舗来店や購入等オフラインデータの充実といった環境変化により、マーケティングデータは識別子や管理主体が異なるものが並立する断片化が著しい。その結果、追跡やターゲティングの精度が低下し、最適化や効果測定が困難となっている。それを解決すべく、異なる主体が保有するデータを適切に統合して分析や配信を行う仕組みが求められている。

データクリーンルーム（以下、「DCR」という。）は、このマーケティングデータの断片化を解決するものとして近年注目されている技術である。世界的なオンライン広告業界団体 Interactive Advertising Bureau (IAB)と Ipsos による広告主、媒体、広告代理店へのオンライン調査によると、203 社の回答企業のうち 2022 年時点で 64%が DCR を利用中と回答している[17]。わが国での DCR の普及の程度は明らかでないが、グローバルな WG だけでなく複数の国内企業が DCR の提供を行っており、今後普及が進むと考えられる。

一方で DCR に関する公的機関やアカデミアによる中立的な検討は世界的に見ても十分とはいえない。数少ない例外が Herbrich や Jindal による論文と米連邦取引委員会(FTC)によるブログである。Herbrich の論文は、DCR を WG 型と中立型に分類し、GDPR に照らしてステークホルダが共同管理者・処理者のいずれに該当するか、処理の根拠は同意と正当な利益のいずれか等の検討をしたものである[18]。Jindal による論文は、DCR について概念やステークホルダの整理、データプライバシーやセキュリティ上の利点、法的・倫理的な課題を総覧している[19]。FTC は、DCR はデフォルトでプライバシーを守ることはできず、トラッキングピクセル同様のプライバシー上の問題を惹き起こすと警告するブログを 2024 年に公開した[20]。当該ブログでは、DCR の利用がプライバ

---

[15] Anthony Chavez “A new path for Privacy Sandbox on the web” (2024) https://privacysandbox.com/news/privacy-sandbox-update/

[16] Google はサードパーティクッキーに代わる新たなターゲティング広告配信技術 Privacy Sandbox の開発を 2019 年以降続けてきたが、2025 年 10 月にプロジェクトの終了を発表した。ITMedia 「Google, 『プライバシーサンドボックス』を実質終了 関連技術のほとんどを廃止へ」 (2025) https://www.itmedia.co.jp/news/articles/2510/19/news019.html

[17] IAB & Ipsos “State of Data 2023: Data Clean Rooms & the Democratization of Data in the Privacy-Centric Ecosystem” (2023) https://www.iab.com/wp-content/uploads/2023/01/IAB_State_of_Data_2023.pdf

[18] Tilman Herbrich “Data Clean Rooms” *Computer Law Review International* vol.23(4) p.109 (2022).

[19] Piyush Jindal “Privacy-Preserving Data Analysis: Implications of Clean Rooms” *International Journal of Management, IT & Engineering* vol.14(6) (2024).

[20] Federal Trade Commission “Data Clean Rooms: Separating Fact from Fiction” (2024) https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/11/data-clean-rooms-separating-fact-fiction

シー上の問題を曖昧にさせることや、データ拡充により個人の識別とトラッキングが容易になること、DCR の利点であるさまざまな制約は DCR ベンダと利用者が適切に設定しなければ機能しないことを指摘している。

これ以外の DCR に関する文書は DCR ベンダや業界団体によるものに限られている。前者は自らが提供する機能の紹介にとどまっている上に、「プライバシーとデータ利活用の両立」を謳うものの、様々な側面を持つプライバシーのうち DCR が対応するのはどれなのか、そしてデータ保護法との関係といった点への言及は見られない [21]。業界団体の文書も総論的なものにとどまるものが多い中 [22]、IAB や IAB Tech Lab によるものは DCR の法的位置づけや限界、制約について触れており注目に値する [23]。前者は DCR の構成をパターン分けした上で、米国のいくつかの州のデータ保護法で規制される個人情報の「販売」に DCR の利用が該当するかを検討している。結果、DCR での処理も個人情報の処理であり、プライバシー強化技術（PETs）を使っても非識別化は保証されないことや、DCR を用いても州法で規制される「販売」に該当する場合があり、法の適用を免れることはできないことを指摘している。後者は DCR に参加するすべての事業者が信頼できる必要があり、それを担保するためにデューデリジェンスが必要なこと、関係者間で後述する ID 単位での突合のために用いる ID やその突合の方法、データのクレンジングや正規化の水準のすり合わせが必要なこと等を指摘している。そして DCR ベンダを選ぶ際には、コストやスピード、連携可能なデータの幅広さといったビジネス的側面だけでなく、候補ベンダが想定しているプライバシー攻撃モデルとそれに対応する PETs の適正さや、越境データ対応といった点も利用組織が注意深く検証することを勧めている。

DCR によるマーケティングデータ断片化の解決は、データ取得時の文脈を越えた利用と表裏一体であり、それに基づく決定がデータ主体への不意打ちになる蓋然性が高い。にもかかわらず、DCR 特にその法的な位置づけを論じた文献は、日本での利用を前提にしたものは目下存在しないし、そもそも DCR によって何が可能になるのかの整理すら

[21] InfoSum “The ultimate guide to Data Clean Rooms 2023 edition” (2023); World Federation of Advertisers “WFA Survey: A Closer Look at Data Clean Rooms” (2023); Kamakshi Sivaramakrishnan & Lena Pennington “Snowflake Data Clean Rooms: Securely Collaborate to Unlock Insights and Value” (2024) https://www.snowflake.com/en/blog/unlock-insights-with-snowflake-data-clean-rooms/ ; Amazon Web Services “AWS Clean Rooms” https://aws.amazon.com/jp/clean-rooms/ ; LiveRamp “Clean Rooms Guide: 12 Essential Strategies for Marketers” https://liveramp.com/data-clean-room-playbook-interactive/

[22] IAB Europe “Data Clean Rooms: A Promising Prospect” (2022) https://iabeurope.eu/data-clean-rooms-a-promising-prospect/ ; The Association of National Advertisers “ANA Releases ‘Ultimate Playbook for Data Clean Rooms’” (2024) https://www.ana.net/content/show/id/pr-2024-10-datacleanrooms

[23] IAB “Data Clean Rooms: A U.S. State Privacy Law Perspective” (2025) https://www.iab.com/wp-content/uploads/2025/04/IAB_Data_Clean_Rooms_A_US_State_Privacy_Law_Perspective_April-2025.pdf; IAB Tech Lab “Data Clean Rooms: Guidance and Recommended Practices” (2023) https://iabtechlab.com/blog/wp-content/uploads/2023/06/Data-Clean-Room-Guidance_Version_1.054.pdf, 24 頁。

存在しない。つまり不意打ちの危険を孕むサービスが法的位置づけも曖昧なまま普及し始めているのが日本の現状といえる。こうした状況を改めるべく、本稿では広告の文脈下における DCR について機能の整理を行い、それぞれの機能に対して個人情報の保護に関する法律 [24]（以下、「個情法」という。）の下でどのような規律が適用されうるか検討する。第２節では本稿のスコープと分析法について触れる。続く第３節で DCR の概要と、その機能が(1)データ拡充、(2)統計・モデル作成、(3)アクティベーション、(4)広告効果測定の４つに分けられることを提案する。第４節では DCR に関係する法として個情法と電気通信事業法を取り上げ、続く分析に必要な個情法上の規律を整理する。第５節では DCR の４機能それぞれについて考えられるデータフローを列挙し、それぞれにどのような規律が適用されるか検討する。第６節では第５節の結果をまとめ、４機能すべてを備えた DCR を可能にする方法を検討する。第７節でまとめを行い、今後の展望に触れる。

２．本稿のスコープと分析法

本稿ではオーディエンスターゲティング広告を代表とした広告領域の利用を前提にDCRの機能分類と法的評価を行う。その理由としては、(1) 執筆時点でDCRのベンダや事業利用例のほとんどが広告に関わるものであり [25]、(1a) 既に幅広い DCR の利用パターンが存在し、他領域での利用パターンは広告領域のそれの亜種として包摂されうること [26]、(1b) 広告領域での用途は仮想的なものではなく市場でニーズがあるものであること、(2) 特にオーディエンスターゲティング広告では、DCR を用いることがデータ主体に配信される広告の変化という形で可視化されるため、プライバシー上の問題として表面化する可能性を多分に孕むことが挙げられる。

データ保護法とDCRとの関係については上記HerbrichやIABが触れてはいるが、その議論を日本にそのまま持ち込むことはできない。GDPR と個情法との間ですら、相互の十分性認定はあるものの、制度の内実に大きな違いがあるためである [27]。DCRとの関係で特に重要な差異は、GDPR の下では処理が適法であればその一連の処理の中で事業者の境界を越えることがあっても特段追加の義務が生じないのに対し [28]、個情法では全体で見れば 1 つの目的のための処理だったとしても、個人データが事業者の境界を越える場合には様々な義務が生じるというものである。結果、GDPR の下での DCR は特定目的の処理の適法化根拠、参加者の管理者／処理者該当性や責任の割当て、当該処理とデータ主体の合理的期待との関係といった論点に焦点が当たり、処理の具体的な実装パターンの違いは結論に必ずしも影響を与えない。一方、個情法の下ではどのようなデー

[24] 平成 15 年法律第 57 号。
[25] たとえば英語版 Wikipedia の Data clean room （2025 年 11 月 27 日時点）に記載されている会社 6 社すべてが DCR を広告関連事業の一環としている。
[26] ５．２．統計・モデル作成参照。
[27] Seiichi Igaya & Osamu Sudoh “Ignored Discrepancies in the Fundamental Concepts of Data Protection Laws in Japan and the EU” *International Data Privacy Law* vol.15(2) p.171 (2025).
[28] 域外移転を伴う場合を除く。

タがどのような位置づけで移転し提供されるのかが議論の中心となる。例えば仮に個人データが移転しても委託やいわゆる「クラウド例外」の場合は義務が生じないなど、一連の処理の中での個々の移転それぞれでの場合分けなくして DCR の法的位置づけを論じることはできない。

なお本稿では、IAB が行った DCR 参加者間でのデータの移転パターンを分析の第一の分類軸とするのではなく、DCR によって可能となる用途の分類を行った上で、それぞれの用途の中で DCR 参加者間データ移転パターンの場合分けを行う形を採用する。その理由は、第一には本稿の貢献のひとつが現在後景に退いている「なんのために DCR を利用するか」を改めて整理した点であるため、それに合わせた議論を行うのが自然だからである。また、用途にまず着目する形の議論は処理ごとに適法化根拠を求める EU での議論と平仄が合うだけでなく、現在個情法の見直し論点の 1 つに、統計情報作成を前提にした個人データの突合に係る規制緩和があり、日本にも処理に着目した規制に向かう兆しも見られるためである。

３．データクリーンルームとは何か

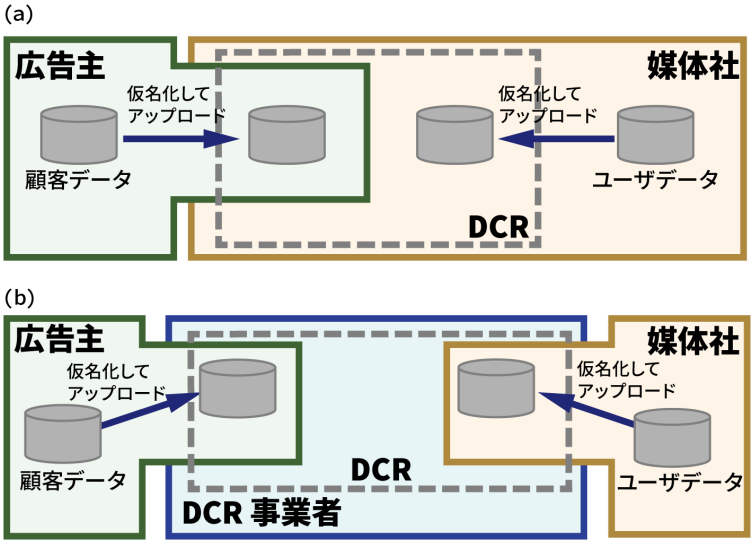
３．１．データクリーンルームの概略

DCR について IAB の技術部門 IAB Tech Lab は「オンライン広告エコシステムのあらゆるステークホルダに安全なデータ共有を可能にするソリューション」と紹介している。そしてそれを利用することで、(1) データに利用目的制限をかける、(2) 組織のプライバシーポリシー遵守を支援する、(3) 媒体のオーディエンス価値を最大化する、(4) 自社データを開示・共有せず価値を引き出す、(5) 分析プロセスの中でデータに変更・操作されないことを保証する、といったことが可能としている [29]。他の DCR ベンダ等も類似したメリットを謳っている [30]。それらを総合すると、DCR とは「参加する組織が自らのデータを開示・共有せずに統合し、分析やデータの利用を可能にする隔離された環境」ということができる。

DCR の嚆矢は 2017 年に Google が発表した Ads Data Hub とされる [31]。Amazon や Meta、TikTok、LINE ヤフーといった WG も自らのユーザのデータとクライアントデータとの統合を謳う DCR を提供している（WG 型 DCR）。それ以外に Habu、LiveRamp、InfoSum、Snowflake といった事業者は、自らユーザデータを持たず、広告主と媒体のデータ連携を支援する DCR サービスを提供している（中立型 DCR）。それぞれの DCR を利用する際のデータの保有のされ方を図 1 に示す。それぞれのデータホルダが自らの個人データを仮名化した上で DCR 領域にアップロードし、統合を実施する者でもデータ内容にアクセスできない領域で統合が行われる点は共通している。

[29] IAB Tech Lab・前掲注(23), 8–9 頁。
[30] Acompany プライバシーテック研究所「世界のデータクリーンルームサービスとは? AWS や Snowflake、Habu などを比較してみた」(2023) https://www.acompany.tech/privacytechlab/data-clean-room-platform ;
[31] InfoSum・前掲注(21), 5 頁。

図１．WG 型 DCR(a)と中立型 DCR(b)でのデータの所在と保有のされ方



３．２．データクリーンルームの機能

ターゲティング広告の配信とは本質的には、広告主が指定したターゲットに対し、ひとりひとりのターゲットに適した広告表現を、媒体が表示することである。これを実現するため、実務では典型的には以下のような手順を踏む。(1) 広告主は広告出稿に先立って、マーケティングデータを収集する。(2) 集めたデータに基づいてターゲットを選定する。ターゲットは識別子により直接選定される場合もあれば、該当非該当を判断する条件や統計モデルによって選定される場合もある。(3) 開発したターゲット選定法を媒体に渡して配信を行わせる。(4) 媒体は広告主に配信の結果を報告する [32]。DCR に関する既存の文書等を総覧すると、上記 4 つすべてのステップに DCR が貢献しうることがわかる。それぞれに係る DCR の機能を (1) データ拡充、(2) 統計・モデル作成、(3) アクティベーション、(4) 広告効果測定と呼ぶこととし、以下それぞれについて概観する。

(1)　データ拡充とは、広告主データセットに媒体やWG（これら広告主ではない側の DCR 一方当事者をまとめて以下「パートナー」という。）のデータを付加することで、精緻な顧客理解を可能とするものへと充実させることを指す。広告主は自らが知らない顧客の側面を知ることができるため、事業戦略や広告ターゲット選定をより精度高く行うことができる。ここで付加されるデータは広告主データの ID にマッチするパートナーデータの ID ごとの情報である。しかし未加工の情報が付加されることは極めて例外的で、その ID が属するセグメントや値の範囲（年齢が 33 歳の場合「30 代」等）といった派生値が付加されるのが一般的である（以下、このデータ拡充のための派生値の作成を以降「処理 Drv」という。）。なお、広告主データセットに存在するがパートナーデータセットには存在しない ID には何もデータが付加されない。

[32] 日本インタラクティブ広告協会『必携インターネット広告 プロが押さえておきたい新常識』(インプレス 2019)。

(2)　統計・モデル作成とは、DCR 内で広告主とパートナー双方の顧客データを統合して擬似シングルソースデータを作成して機械学習や統計分析を行い [33]、他の用途に資する情報を作成することである。出力される情報には主に 2 つの形式がある。1 つは一般的な統計的知見である。変数間の相関や傾向といった知見となっているため、データ主体に直接影響を及ぼす使われ方は稀である。広告以外での DCR の用途のほとんどはこれに含まれる。もう 1 つがターゲット判別モデルで、(3)で述べる間接アクティベーションに用いることを想定した統計モデルの形をしている。こちらはパートナーデータを入力するとターゲットとしての有望度を予測することが主たる目的であり、人間の知見となるとしてもそれは副次的成果にすぎない。なお、DCR 内でのデータ統合に際しては、ID 単位での突合が行われることが現在一般的である。しかし ID 単位での突合を行わない方式も論理的には考えられる。例えば、広告主データセットのみでモデル学習を行った上でパートナーに提供し、パートナーデータセットを用いてそのモデルに追加学習を行うといった形である。

(3)　アクティベーションとは、広告主からの指示の下でパートナーが自らの顧客に対して広告を配信することを指す。広告主の顧客 ID との関係で更に「直接アクティベーション」と「間接アクティベーション」の２つに分けることができる。直接アクティベーションとは、広告主の顧客 ID とマッチするパートナー顧客 ID に対して広告を配信するものである。間接アクティベーションとは、広告主は自ら保有する顧客データ等からターゲットの判別手段を開発してパートナーに提供し [34]、パートナーが自らの顧客データに当該手段を適用してターゲットと推定された顧客に広告を配信するものである。

(4)　広告効果測定とはパートナーにおける配信実績と広告主における流入や購買といった行動の実績を DCR 内で紐づけて擬似シングルソースデータを作成し、これに DCR が提供する分析を加えることで広告配信の成果を検証するものである。DCR 内では ID 単位での突合が行われるが、プライバシー保護のため DCR の分析環境は ID 単位のデータや、セルに含まれる人数が小さい集計結果の出力を行わないようになっている。

４．データクリーンルームに関連する法

４．１．個人情報保護法

DCR との関係で個情法上着目すべき情報は個人データと個人関連情報である。個情法では、保護の対象となる個人情報を生存する個人に関する情報であって、その記述等により特定個人を識別できるものとしている（個情法 2 条 1 項)。そして個人データとは、個人情報を含む情報の集合物であって、特定個人を検索できるよう体系性を持たせた個人情報データベース等に含まれる個々の個人情報を指す（個情法 16 条 3 項)。個人関連情報とは、生存する個人に関する情報であって、個人情報、仮名加工情報、匿名加工情報のいずれにも該当しないものをいう（個情法 2 条 7 項)。

[33] 単一の調査によって取得されたデータを「シングルソースデータ」という。２つのデータセットを ID 単位で突合することによって擬似的にシングルソースデータを作成するため「擬似シングルソースデータ」と呼ぶ。
[34] ここで(2) 統計・モデル作成で得た擬似シングルソースデータを用いて作ったモデルを使っても良い。

個人データの取扱い上 DCR と関係が深い規律は第三者提供に係るものと委託に係るものである。第三者提供に係るものとしては、原則として予め本人の同意を得ること（個情法 27 条 1 項)、受領者は提供される個人データの取得の経緯等の確認（個情法 30 条 1 項)、授受を行った双方が相手方氏名等の記録・保存を行うこと（個情法 29 条 1 項及び 30 条 3 項）がある。ただし、本人同意原則の例外としてオプトアウト方式も認められる（個情法 27 条 2 項)。また、個人データを第三者に提供することが想定される場合には利用目的としてその旨を特定する必要がある [35]。更に、個人データが外国（ただしわが国から十分性認定を受けている国または地域を除く）にある第三者（ただし「相当措置」を講じる体制を整備している者を除く）に提供される場合には当該第三者が存する外国における個人情報保護制度等の情報を本人に提供した上で本人からの同意を得なければならない（個情法 28 条)。以上の第三者提供に係る授受双方に課される規律を以降、「規律[27]」と表す。

委託に係る規律としてはまず委託元は委託先に対し必要かつ適切な監督を行う義務がある（個情法 25 条)。委託先が外国の第三者である場合は個人データの外国第三者への提供に係る規律と同じものが適用される。これらを以降「規律[25]」と表す。また、委託先は自らが独自に取得した個人データまたは個人関連情報を、委託の枠内で、委託された個人データに本人ごとに突合することはできない [36]（これを以降「規律[7-41A]」と表す)。ただしこの突合は、委託元から委託先への第三者提供と整理して委託元が規律[27]に対応した場合または委託先が本人から同意を取得すれば可能である [37]（これを以降「規律[7-41B]」と表す。)。複数の者から個人データの委託を受けている委託先が、それぞれの個人データに含まれる本人ごとに突合することもできない [38]（これを以降「規律[7-43]」と表す。)。

DCR との関係で個人関連情報の取扱い上特に着目すべき規律は、個人関連情報を個人データとして取得するときに係るものである。このとき、受領側は個人関連情報の提供を受けて個人データとして取得することを認める旨の同意を本人から得る必要があり（個情法 31 条 1 項)、提供側はそれを確認せずに当該個人関連情報を提供することはできない（個情法 31 条柱書)。これを以降「規律[31]」と表す。

また、ターゲティング広告一般に係る規律として、「本人から得た情報から、本人に関する行動・関心等の情報を分析する場合 [39]」いわゆるプロファイリングを行う場合には、個情法 17 条 1 項により個人情報の利用目的として特定しなければならない [40]。これを以降「規律[17]」と表す。

---

[35] 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン （通則編)」, 3-1-1。
[36] 個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』に関する Q&A」, Q.7-41。
[37] 同上。
[38] 同上, Q.7-43。
[39] 個人情報保護委員会「個人情報保護法 GL 通則編」・前掲注(35), 33 頁。
[40] 同上。

４．２．電気通信事業法

2022 年 6 月の電気通信事業法改正によって、インターネット広告のトラッキングを可能にするタグや情報収集モジュールに新たな規律が設けられた（電気通信事業法 27 条の 12。外部送信規律）。これはウェブサイトやアプリケーションを利用する際に、ユーザがアクセスしたページに埋め込まれたタグや情報収集モジュールによって、ユーザの端末が第三者のサーバに情報を送信すること（外部送信）を問題視したもので、こうした外部送信に関する情報をユーザが確認できるようにする趣旨の規律である [41]。外部送信規律の対象となるのは例えばソーシャル・ネットワーキング・サービス、検索エンジン、EC モールなど、電気通信役務自体が事業目的となる事業者である。DCR との関係では多くの WG が対象になるであろう。一方、電気通信役務を手段としてのみ利用する事業者は規律の対象とならない。自社 EC サイトの運営者や自らの情報発信のためホームページを運営する企業・個人等が該当するため、広告主には外部送信規律が適用されないと考えられる。外部送信規律が適用された場合には、送信される利用者情報の内容、送信先の氏名または名称、送信される情報の利用目的を通知または公表する必要がある。

外部送信規律は DCR を利用せずともインターネット広告に関わっている事業者であれば広告主を除き広く適用されるため、DCR 特有の問題を論じる本稿では外部送信規律に係る義務についての言及は省くこととする。

５．データクリーンルーム機能ごとの法的評価

DCR の機能ごとの法的評価に際し、広告主、パートナー、DCR をそれぞれ A、P、D と表記する。WG 型 DCR の場合は P と D が同一となる。広告主データセット、パートナーデータセットをそれぞれ a、p と表し、a や p に含まれるデータの内容を明らかにする必要があるときには、丸括弧で囲んで追記する。その際、ID（ハッシュ化等の変換を施したものも含む。以下同様。）は ID、顧客の属性情報（関心や行動も含む）は At と表す。例えば、a(ID)は A の顧客 ID リストであり、p(ID, At)は P の顧客 ID とそれに紐づく属性のリストである。加えて、データセットの保有主体を明らかにする必要がある場合には、データセットの右に上付きで a^A（A が保有している a を表す）や p^D(ID, At)（D が保有している p(ID, At)を表す）のように表記する。また、以下の前提をおく。(1) a や p は、DCR に用いるため A 及び P が自社顧客データセットのうち氏名等の直接識別子を除いて作成して DCR にアップロードしたものである（図 1 参照）。(2) ただし、a や p は元の顧客データとの容易照合性が存在するため、いずれも個人データである。なお紙幅の都合上、以降の分析は中立型 DCR を主に扱い、WG 型 DCR は補足的に触れるに留める。

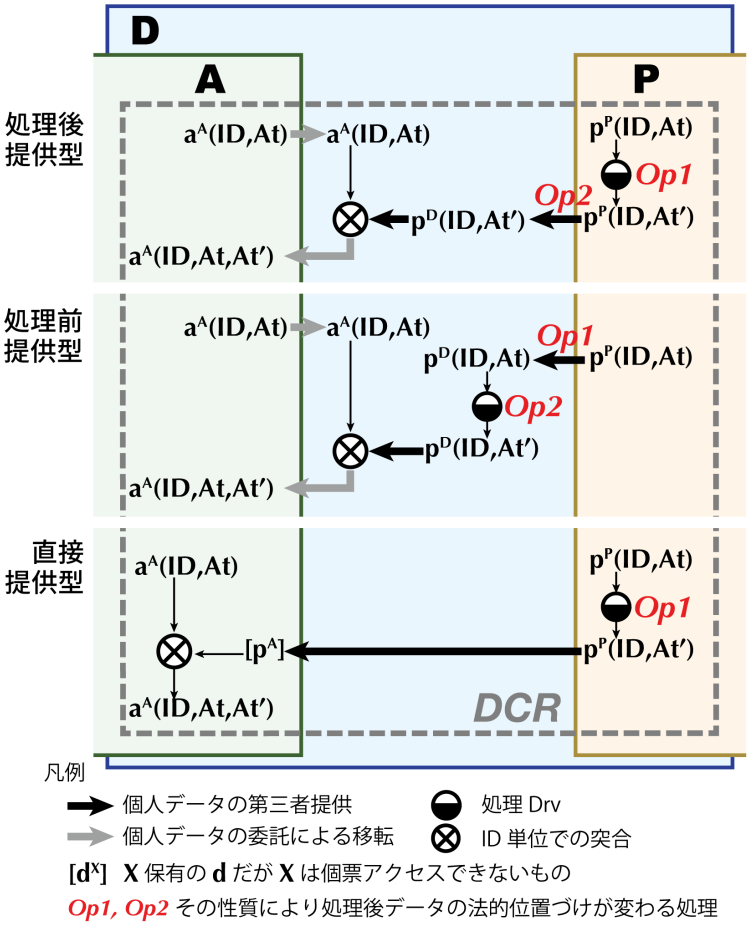
５．１．データ拡充

データ拡充は p(ID,At)に処理 Drv を施して p(ID,At')を作り、a(ID,At)と突合することによって実現される。従って、処理 Drv を行う者（P または D）と突合を行う者（D ま

[41] 総務省総合通信基盤局「外部送信規律について」(2023)
https://www.soumu.go.jp/main_content/000862755.pdf, 3–4 頁。

たは A）によって場合分けする。突合を D が行う場合は、P が処理 Drv を行う「処理後提供型」と D が処理 Drv も行う「処理前提供型」に分かれる [42]。A が突合を行う場合は P が処理 Drv を行う「直接提供型」のみである（図２）[43]。

図２．中立型 DCR を用いたデータ拡充のデータフロー



データ拡充の法的評価のためには、更に処理 Drv と P→D のデータ移転（以下「P→D 移転」という。）における容易照合性によって場合分けが必要である。まず処理後提供型を考える。

イ） 処理 Drv と P→D 移転いずれも容易照合性がある場合…$p^P(ID, At')$と $p^D(ID, At')$いずれも個人データである。したがって P→D 移転に規律[27]が適用される。D 内で行われる $a^A(ID, At)$と $p^D(ID, At')$の照合も個人データの第三者提供となり規律[27]が適用される。

[42] ここでは A は D にデータ拡充の委託を行っていることを前提とするが、委託先の監督を省くために A から D への第三者提供で構成することも可能である。第 6 節参照。
[43] データ拡充では最終的に $a^A(ID)$と ID 単位の照合が行われるため、処理 Drv を個情法 16 条 6 項の匿名加工とすることはできない。

ロ)　処理 Drv のみ容易照合性がある場合…p(ID, At')は P→D 移転によって個人データから個人関連情報となるため P→D 移転には個人データの第三者提供として規律[27]が適用される。D での照合は個人関連情報の個人データとしての取得として D と A に規律[31]が適用される。

ハ)　処理 Drv に容易照合性がない場合…p^{P}(ID, At')が処理 Drv によって個人関連情報になり、D においても個人データとしての取得にならないため、P→D 移転には規律[31]は適用されない。一方で D での照合は個人関連情報の個人データとしての取得として D と A に規律[31]が適用される。

同様に処理前提供型は、

ニ)　P→D 移転と処理 Drv いずれも容易照合性がある場合…p^{D}(ID, At)と p^{D}(ID, At')いずれも個人データである。したがって P→D 移転に規律[27]が適用される。D 内で行われる a^{A}(ID, At)と p^{D}(ID, At')の照合も個人データの第三者提供となり規律[27]が適用される。

ホ)　P→D 移転のみ容易照合性がある場合…P→D 移転は個人データの第三者提供なので P と D に規律[27]が適用される。処理 Drv で p^{D}(ID, At')は個人関連情報になるが、D での照合は個人関連情報の個人データとしての取得として D と A に規律[31]が適用される。

ヘ)　P→D 移転に容易照合性がない場合…提供元基準により P→D 移転は個人データの第三者提供なので規律[27]が適用される。p^{D}(ID, At)は個人関連情報であり、処理 Drv を経ても変わらない。D での照合は個人関連情報の個人データとしての取得として D と A に規律[31]が適用される。

直接提供型は、

ト)　処理 Drv に容易照合性がある場合…p^{P}(ID, At')は個人データなので、a(ID, At)との照合は個人データの第三者提供となり、規律[27]が適用される。

チ)　処理 Drv に容易照合性がない場合…p^{P}(ID, At')は個人関連情報なので、A は個人関連情報を個人データとして取得する形となり、規律[31]が適用される。

以上をまとめると、すべてのパターンにおいて A には個人データの第三者提供または個人関連情報の個人データとしての取得が起きるため、規律[27]または規律[31]が適用されることがわかる。なお、WG 型 DCR の場合は P=D なので、中立型 DCR のパターンすべてが直接提供型に収斂することになる。

５．２．統計・モデル作成

統計・モデル作成への法的評価は、モデル作成に用いるデータによって３つに分かれる。(a) A が a^{A}(At)のみを用いる場合、(b) a(ID, At)と p(ID, At)とを ID 単位で突合した擬似シングルソースデータを用いる場合、(c) ID 単位での突合を行わず、A が a^{A}(At)を用いてモデルを作成し、そのモデルを P に提供して、P が p^{P}(At)を用いて追加学習を行う場合である。ただし、(a)は通常の広告配信のセグメントの作成と変わるところがなく、DCR 固有の論点がないため検討を省く。(c)は a^{A}(At)からのモデル作成は統計情報等の作成に該当するため利用目的に記載の必要はなく、また P への提供にも制限はない。P がそのモデルと p^{P}(At)を使って追加学習を行うことも統計情報等の作成に該当すると評

価でき、(c)の形でモデルを作ることに個人情報保護法による義務が課されることはないと考えられる。そのため以降は(b)に絞って検討する。

まず、D が突合と学習を行うパターンと P または A が行うパターンに分けられる。前者の場合、規律[7-41B]より A→D 移転と P→D 移転の少なくとも１つは個人データの第三者提供である必要がある。したがって次の３パターンがありうる。

- D 内学習・両提供型…両提供が個人データの第三者提供なので A、P、D すべて規律[27]が適用される。
- D 内学習・P 提供型…個人データの第三者提供に関わる P と D に規律[27]が適用され、委託に関わる A と D には規律[25]が適用される。
- D 内学習・A 提供型…個人データの第三者提供に関わる A と D に規律[27]が適用され、委託に関わる P と D には規律[25]が適用される。

後者はいわゆる「クラウド例外」により D は突合・学習環境を用意するが自らはデータを取り扱わない場合である。提供元と提供先が逆転するがいずれの場合でも AP 間で直接個人データの提供が行われるため規律[27]が適用される。学習されたモデルは統計情報なので移転に際して個情法上の規律は適用されない。以上をまとめると図３のようになる[44]。なお、WG 型 DCR では D=P なので「A 内学習型」「P 内学習型」のみが可能で、同様に規律[27]が適用される。

なお 2025 年 9 月現在、個人情報保護法の今後の検討点の１つとして「特定の個人との対応関係が排斥された[...]統計作成等の作成にのみ利用されることが担保されていること等を条件に、本人同意なき個人データ等の第三者提供[...]を可能と」する検討を個人情報保護委員会が行っている[45]。本節で論じている統計やモデルはまさに特定個人との対応関係が排斥された統計情報等に該当するため、今後の法改正によっては本人同意を得ることなく作成できる可能性がある。この改正は、得られた情報が個人への決定に用いられない一般的な統計的知見であれば本人に驚きを与える可能性も低いため進めるべきと筆者は考える。一方で、得られたものが個人への決定を左右する場合には、５．４．で述べる「モデルを介した情報移転」の問題が発生する可能性があるため、決定の理由等を本人が容易に知りうる状態にするといった措置を検討することも考えられる[46]。

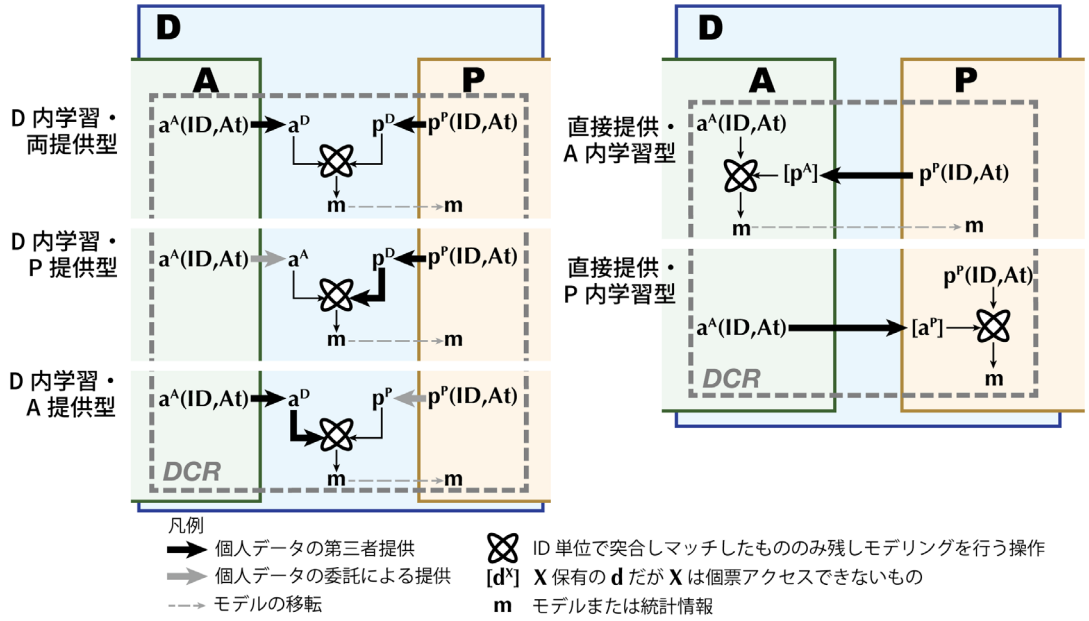
---

[44] 一般の統計的知見を作成する場合であってもデータフローは同じであり、出力されたｍが統計的知見となる。個人との関連性が排斥された統計情報であれば、P に提供するだけでなく、A やその他の第三者に提供できる。

[45] 個人情報保護委員会「個人情報保護法の制度的課題に対する考え方について（個人データ等の取扱いにおける本人関与に係る規律の在り方）」(2025), 1 頁。

[46] Purtova と Leenes は GDPR の個人データの定義が個人に「関する(relating to)」情報であって、個人に「ついての(about)」情報ではないことに着目し、個人についての情報を一切含まないがそうした情報を処理するプログラムも個人データになると論じている。Nadezhda Purtova & Ronald Leenes “Code as personal data: Implications for data protection law and regulation of algorithms” *International Data Privacy Law* vol.13(4) p.245 (2023).

図３．中立型 DCR による統計・モデル作成のデータフロー



５．３．直接アクティベーション

直接アクティベーションのためには a(ID)と p(ID)を照合する必要があり、照合の場は D か P がありうる。前者の場合は規律[7-41B]より A→D 移転と P→D 移転の少なくとも１つは個人データの第三者提供である必要がある。したがって次の３パターンがありうる。

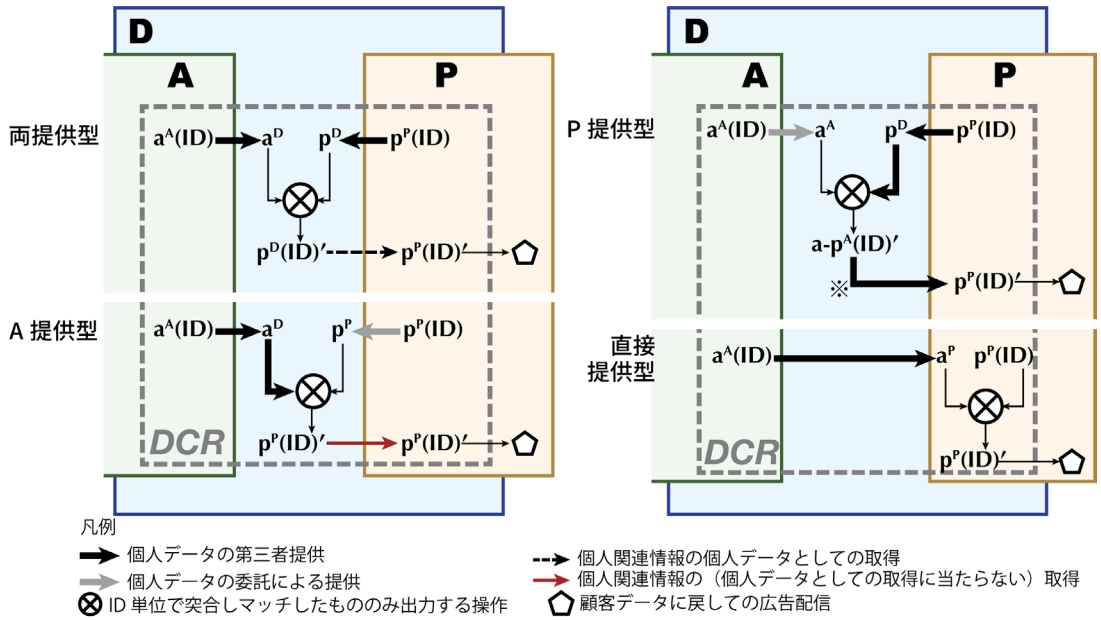
- 両提供型…両提供が個人データの第三者提供なので A、P、D に規律[27]が適用される。一方、突合後の $p^D(ID)'$は個人関連情報で、P に提供されてターゲティング広告配信に使われるのであるから、個人関連情報の個人データとしての取得に該当し、D と P に規律[31]が適用される。
- A 提供型…A→D 移転は個人データの第三者提供なので規律[27]が、P→D 移転は委託に伴う移転なので規律[25]が適用される。突合後の $p^P(ID)'$ は $p^P(ID)$のサブセットでしかなく「委託先で独自に取得した個人関連情報を当該データに付加」されていないため、P に戻す際には規律[31]は適用されないと解することができる [47]。
- P 提供型…A→D 移転は委託に伴う提供なので規律[25]が、P→D 移転は個人データの第三者提供なので規律[27]が適用される。突合後の $a\text{-}p^A(ID)'$は D が取扱ってはいるが委託元である A が保有しているため、ここからマッチした p(ID)を取り出して P に提供することは A から P への個人データの第三者提供となり規律[27]が適用される [48]。

[47] ここでは p(ID)の中からマッチしたものだけを P に返す場合を想定している。p(ID)すべてにマッチしたか否かのフラグを付けて P に返す場合には、委託先独自取得の個人関連情報を当該データに付加に該当することになり規律[31]が適用される。
[48] 突合後データを一旦 A に戻してから P に提供することも論理的には考えられる。しかしこの場合は委託先が独自取得した個人関連情報 $p^D(ID)$を $p^A(ID)$に付加して委託元に戻

後者はクラウド例外による直接提供型で、規律[7-43]により委託では不可能なので、個人データの第三者提供による１パターンに収斂し、A と P に規律[27]が適用される。

以上をまとめて直接アクティベーションが可能なデータフローを図示したものが図４である。委託による提供の場合は D に移転しても主体は提供元のままであることに注意されたい。どのパターンであっても A は第三者提供を行うこととなり規律[27]に対応する必要があるのに加え、D や P にもデータフローの設計ごとに異なる規律が適用されることがわかる。なお、WG 型 DCR の場合は P=D なので直接提供型になり、規律[27]が適用される。

図４．中立型 DCR を用いた直接アクティベーションのデータフロー[49]



５．４．間接アクティベーション

間接アクティベーションでは５．２．で作成され P に提供されたモデル m を P が p(At)に適用してターゲット有望度を推定し、広告配信の可否を決める。これはいわゆるプロファイリングに該当するため規律[17]が適用される。一方これは P によるデータの内部利用に過ぎず、移転や突合に係る規律は適用されない。

ただしここで行われるプロファイリングは、各社が自社保有のデータのみに基づいて行うものとは異なる性質を持つことに注意が必要である。それはモデルが a(At)と p(At)両方に基づいて作られるため、a(At)が持つ情報がモデルに埋め込まれている点である。そのため、ユーザから見れば A しか知らないはずの自分の情報を P が知っているように感じる可能性がある。例えば、次のようなケースが考えられる。「U には幼い子どもがいる。また U は育児雑誌 K を購読しており、K のサイト上で育児に関する情報を得たり、

す形となるため、D と A に追加で規律[31]が適用される。したがって D から A に戻さず、D からマッチした p(ID)を直接 P に提供する形が合理的といえる。

[49] 突合後のデータに付く記号´はマッチしたものだけのデータであることを表す。P 提供型の※は A から P への第三者提供となることに注意。

K 主催の会員向けイベントに参加もしている。一方 U はソーシャル・ネットワーキング・サービス S にアカウントを持っているが、こちらでは子どもの存在を示唆する言動はまったく行っていない。あるとき K が広告主、S が媒体として DCR を通じて、K が開発した商品 I の潜在顧客を判定するモデルを作成したとする。モデルの性能が十分高ければ U は I の潜在顧客と判定され、I の広告が U の閲覧する S 上に表示される。U にとっては、子どもの存在を秘して活動していたはずの S に自身が購読する K が開発した I の広告が表示され、驚きを覚えるであろう。」この問題は異なる文脈のデータに基づいて学習したモデルを使ってプロファイリングを行う場合常に発生しうるもので、DCR 特有の問題ではない。だが DCR によるモデル作成は 2 つのデータセットを本人ごとに突合するため、得られるモデルの性能は一般的なものより高くなると想定される。したがって DCR においてこの「モデルを介した情報移転」の問題は顕著になる懸念がある。

モデルを介した情報移転については、現時点では規律の議論はない。例えば個人情報保護委員会は、統計作成等に限る第三者提供の同意義務の緩和に関して、得られた統計情報等をどのように使うのが適当かについては言及していない [50]。一方、個人情報保護委員会事務局メンバーはこの義務の緩和に関し「統計作成のためと言いながら、裏でターゲティング広告に使うことは許容されない」と発言している [51]。これは少なくとも統計作成を謳いながら実際には統計を作成せず直接アクティベーションを行うことを否定していることは確かである。一方、実際に統計（モデル）を作成し、そのモデルをターゲティング広告の配信に用いる間接アクティベーションまで否定する意図があるのかは明らかではない。しかし、本人にとって見れば、A のみが知るはずの情報に基づいた決定が下されうるという点では直接アクティベーションも間接アクティベーションも変わるところはない。こうした本人の合理的期待を超えるデータに基づく決定に対しては、単なる統計的知見の作成・提供とは別に、決定の根拠となった主な情報の内容や保有者等を本人が容易に知りうる状態にするといった規律もありうる [52]。

５．５．広告効果測定

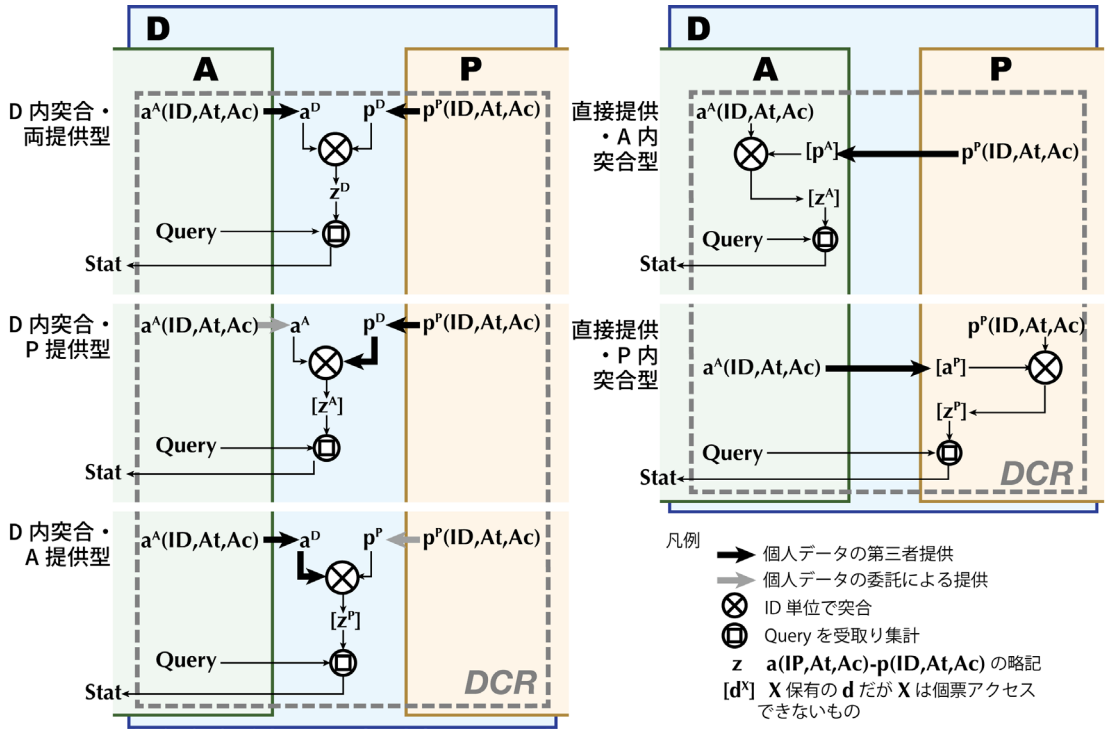
広告を配信したことによる実績データを Ac で表すと、広告効果測定では D において a(ID, At, Ac)と p(ID, At, Ac)とを ID 単位で突合して擬似シングルソースデータを作成し、これに D が提供する環境下で分析を加える形となる。分析の結果は、ID 単位または小サンプル単位の集計は出力されないことが保証されているため、「個人との対応関係が排斥された統計情報」に該当する。したがって広告効果測定の法的評価は５．２．統計・モデル作成で検討したものと実質的に同じになる。すなわち D への移転が双方第

[50] 個人情報保護委員会「制度的課題に関する考え方」・前掲注(45), 1 頁。
[51] 一般社団法人次世代基盤政策研究所「NFI 5 周年記念シンポジウム ～2035 年の次世代基盤政策～」（2025 年 8 月 25 日開催） 「テーマ 2: データ利活用と個人情報保護」小川久仁子氏発言。
[52] この決定理由の説明は、DCR の「自社が保有するデータが外部に開示されない」機能により実務上実現困難な可能性がある。あるデータ主体への決定にどの変数がどれだけ寄与したのか分析するためには、a と p 双方のすべての変数名と値にアクセスできる必要があると考えられ、そのような者は DCR の構成上存在しないからである。

三者提供のもの（両提供型）と第三者提供と委託の組合せ（D 突合・P 提供型及び A 提供型）、そしてクラウド例外による A-P 間直接の第三者提供（直接提供・A 内突合型と P 内突合型）である（図５）。図５からはすべてのパターンで A または P に規律[27]が適用されることがわかる。なお WG 型 DCR では D=P なので「A 内突合型」「P 内突合型」のみが可能で、同様に規律[27]が適用される。

ただし、広告効果測定の場合はモデル作成と違って得られた分析結果がターゲティング広告配信に使われることは想定されないため、現在検討されている統計作成等に限る第三者提供の同意義務の緩和が適用される可能性は、モデル作成よりは高いであろう。

図５．中立型 DCR を用いた広告効果測定のデータフロー



６．データクリーンルームが採用しうる法的構成

前節で DCR の機能ごとに法的評価を加えた結果として、中立型 DCR の場合のデータの移転に伴う義務をまとめたものが表１である。これらからは、DCR の４機能のいずれを提供するかによって、可能な法的構成が限られることがわかる。機能によって対応すべき規律が異なる状態は実務上煩雑であるため、提供する機能すべてをカバーできる構成を採用するのが望ましい。情報の移転を伴わない間接アクティベーションを除く４機能すべてを提供しようとするならば、中立型 DCR であれば、D は a や p を取り扱わないことを保証してすべて A-P 間の第三者提供として整理する直接提供型を採用することとなろう。

表 1. 中立型 DCR における各ステークホルダ間のデータ移転等に適用される規律

機能	パターン	小区分	A	D	P
データ拡充	処理後提供型	イ	[25(A→D)] [27(D→A)]	[25(A→D)] [27(P→D)] [27(D→A)]	[27(P→D)]
		ロ	[25(A→D)] [31(D→A)]	[25(A→D)] [27(P→D)] [31(D→A)]	[27(P→D)]
		ハ	[25(A→D)] [31(D→A)]	[25(A→D)] [31(D→A)]	-
	処理前提供型	ニ	[25(A→D)] [27(D→A)]	[25(A→D)] [27(P→D)] [27(D→A)]	[27(P→D)]
		ホ	[25(A→D)] [31(D→A)]	[25(A→D)] [27(P→D)] [31(D→A)]	[27(P→D)]
		ヘ	[25(A→D)] [31(D→A)]	[25(A→D)] [27(P→D)] [31(D→A)]	[27(P→D)]
	直接提供型	ト	[27(P→A)]	-	[27(P→A)]
		チ	[31(P→A)]	-	[31(P→A)]
統計・モデル作成	D 内学習	両提供型	[27(A→D)]	[27(P→D)] [27(A→D)]	[27(P→D)]
		P 提供型	[25(A→D)]	[27(P→D)] [25(A→D)]	[27(P→D)]
		A 提供型	[27(A→D)]	[25(P→D)] [27(A→D)]	[25(P→D)]
	直接提供	A 内学習型	[27(P→A)]	-	[27(P→A)]
		P 内学習型	[27(A→P)]	-	[27(A→P)]
直接アクティベーション	両提供型		[27(A→D)]	[27(P→D)] [27(A→D)] [31(D→P)]	[27(P→D)] [31(D→P)]
	A 提供型		[27(A→D)]	[25(P→D)] [27(A→D)]	[25(P→D)]
	P 提供型		[25(A→D)] [27(A→P)]	[27(P→D)] [25(A→D)]	[27(P→D)] [27(A→P)]
	直接提供型		[27(A→P)]	-	[27(A→P)]
間接アクティベーション			-	-	[17]
広告効果測定	D 内突合	両提供型	[27(A→D)]	[27(P→D)] [27(A→D)]	[27(P→D)]
		P 提供型	[25(A→D)]	[27(P→D)] [25(A→D)]	[27(P→D)]
		A 提供型	[27(A→D)]	[25(P→D)] [27(A→D)]	[25(P→D)]
	直接提供	A 内突合型	[27(P→A)]	-	[27(P→A)]
		P 内突合型	[27(A→P)]	-	[27(A→P)]

しかしこのパターンでは D がデータを取扱うことができないため、事業形態によっては採用できない場合も考えられる。そのような場合には、取扱う情報が個人情報か個人関連情報かの判断は事業者に任されていることを踏まえ [53]、処理 Drv 及び第三者提供前後での容易照合性を否定できたとしても、得られたデータを個人関連情報ではなく個人データとして取扱うことが考えられる。これにより、表1の[31]をすべて[27]に置き換えることができる。すると、データ拡充を除く 3 機能を両提供型で実現できることがわかる。一般論としては個人データに係る規律は個人関連情報に係る規律に比べて幅広いため、規律[31]ではなく[27]を選択することは対応のコストを高めることにつながり合理的とは言えない。しかし、機能によって対応すべき規律が異なることでステークホルダが負担するコストと比べ、どちらの負担が大きいかは必ずしも明らかではない。更に現在、個人関連情報について「このような[特定の個人に対して何らかの連絡を行うことができる]記述等が含まれる個人関連情報について、個人の権利利益の侵害につながる蓋然性の特に高い行為類型である不適正利用及び不正取得に限って、個人情報と同様の規律を導入すること」[54]の検討が行われている。DCR の利用は「個人の権利利益の侵害につながる蓋然性の特に高い行為類型」と直ちには言えないので、この検討の影響を受けることはないと考えられる。だが、そもそも個人関連情報に関する規律はいわゆる「リクナビ事件」を受けて導入されたものとされ [55]、その導入は弥縫的で理論的一貫性を欠くとの批判がある [56]。上述の特定個人への連絡可能な個人関連情報の規律の検討はまさにその証左といえ、今後個人関連情報に関わる何らかの問題が発生すれば追加で規律が導入される可能性は否定できない [57]。それであれば、予測可能性の高い規律を選択することも実務上ありうる [58]。

---

[53] 個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン（通則編）の一部を改正する告示案』に関する意見募集結果」(2021 年 8 月 2 日公表), 番号 295 及び 374。

[54] 個人情報保護委員会「個人情報保護法の制度的課題に対する考え方(案)について（個人データ等の取扱いの態様の多様化等に伴うリスクに適切に対応した規律の在り方）」(2025), 1 頁。

[55] 石井夏生利・曽我部真裕・森亮二(編)『個人情報保護法コンメンタール第 2 版第 1 巻』(勁草書房 2024), 592 頁 〔森亮二〕。

[56] Igaya & Sudoh 前掲注(27)。

[57] 元来、データ保護規制は高リスクな決定への利用を統制するもので、高リスクな情報を保護するものではなかったことが指摘されている（高木浩光「個人情報保護から個人データ保護へ(9) —法目的に基づく制度見直しの検討—」情報法制研究 vol.16 p.96 (2024)）。近年の機械学習技術の進化は機微な属性の推定を容易にしており、もはや高リスクな情報のみを保護することの限界も指摘されている（Paul Ohm “Broken promises of privacy: Responding to the surprising failure of anonymization” UCLA Law Review vol.57(6) p.1701(2010)）。これらを踏まえると、情報に着目して保護を図るアプローチは合理的ではないよう筆者には思われる。寧ろ本人への決定に用いられる情報は一律保護対象とし、決定の性質に直接着目する方が見通しも良くなるのではないか。

[58] なお、WG 型 DCR では直接アクティベーション、間接アクティベーション及びモデル作成は規律[27]が、データ拡張は規律[27]または[31]が適用される形が可能である。

なお、データ拡充の「処理後提供型」「処理前提供型」では A が D に拡充を委託するため規律[25]が適用されるが、これを第三者提供とすることも考えられる(脚注 42 参照)。より「重い」規律[27]が課されることになるが、パターン(イ)(ニ)の場合、既に D→A 移転に課されている規律[27]への対応と統合できるメリットがある。他の(ロ)(ハ)(ホ)(ヘ)でも前述の個人関連情報の個人データとしての取り扱いを選択することで規律[31]を[27]に置き換えているのであれば同様である。

結局、4 機能すべてを備えた DCR を実現するためには、個人関連情報や委託といった特別な規定を用いず、すべての移転を個人データの第三者提供として整理するのが総合的に見て合理的であることが示唆される。

7．おわりに

本稿では、プライバシー保護と両立する形でマーケティングデータの断片化を解決する技術として普及しはじめている DCR について、広告領域での利用を前提に個情法上の検討を行った。まず、DCR が利用企業に提供する機能を(1)データ拡充、(2)統計・モデル作成、(3)アクティベーション、(4)広告効果測定に分類し、それら 4 機能で考えられるデータフローを列挙し、計 23 パターンを得た。続いて 23 パターンそれぞれにおける広告主、パートナー、DCR ベンダに適用される個情法上の規律をデータ提供に重点を置いて検討した。その結果、DCR によってユーザデータが開示されないことが技術的に保証されていたとしても、関係者のいずれかまたはすべてに規律[27]、[31]、[25]いずれかの規律が適用され、個情法上の規律が免除されるパターンがないことがわかった。また、4 機能すべてを提供する DCR で採用しうる法的構成は、WG 型 DCR の場合は「広告主と DCR 双方を個人情報取扱事業者としてデータの提供を第三者提供とする」パターン、中立型 DCR の場合は、「広告主、パートナー、DCR ベンダすべてを個人情報取扱事業者とし、それぞれの間でのすべてのデータ提供を個人データの第三者提供とする」パターンと「広告主とパートナーを個人情報取扱事業者とし、DCR ベンダはいわゆる『クラウド例外』が適用される状態で、広告主とパートナー間でのデータ提供を第三者提供とする」パターンの 2 つが考えられることを示した。

本稿は DCR について網羅的な場合分けを試みた結果、すべての移転を個人データの第三者提供と整理するのが合理的であるという「愚直な」結論を得た。筆者はこの結論を、いわゆる「デジタル敗戦」の巻き返し策としてデータ連携の必要性が叫ばれる昨今のわが国に示唆を与えるものと考えている。というのも、個情法は必要な連携を妨げるものとしてしばしば名指され[59]、DCR 以上に高度な技術や技巧的な法解釈で義務が適用されない連携を模索する動きが見られるからである。しかし 5．4 で述べた通り、データ主体から見れば、自らの合理的期待を越えたデータ連携が行われ、それに基づく決定が下されることこそが問題であって、法の適用の有無は副次的な問題でしかない。なぜ法が適用されないかの微視的な理由など言うまでもない。そうした技術や技巧に依拠したデータ連携が跋扈し、法がそれを掣肘できないとなれば、企業や法への消費者の信頼

[59] 自由民主党「デジタル・ニッポン 2024 —新たな価値を創造するデータ戦略への視座—」(2024), 22 頁。

が揺らぎ、データ社会の実現は却って遠のくことになろう。翻って本稿の結論は、技巧頼みの方策が実務上も非合理的となることを例示するものである。愚直故に消費者にも理解しやすいため、驚きを与える可能性を下げることにもつながる。DCR についても、こうした愚直な形での実装こそが望ましいのではないか。

加えて、同じデータに基づいて同じ目的の処理を行うにもかかわらず、どの中間データを誰に移転するかという形式的側面によって DCR に係る処理の法的位置づけが変わること自体が適当かには疑問がある。法的位置づけに幅があることによって、ある DCR はすべてを個人データの第三者提供で整理し、別の DCR は個人関連情報に係る規定への対応が必要といった断片化がもたらされうる。そもそもこの遠因は、個情法の規制が事業者を単位にしていること（第２節参照）に加え、個人データや個人関連情報のように、課される義務の異なる複数の保護対象が並立していることにある。EU の GDPR は処理単位で規制が行われている上に保護対象情報は個人データのみであるため、処理を構成する操作や中間データが変わったとしても処理そのものの法的位置づけは変わらない [60]。今後、複数事業者が経常的にデータを連携する事例は DCR に限らず増えると考えられる。個情法の事業者単位の構造が現実にそぐわない場面が増えるのならば、処理単位での規制に移行することも視野に入れる必要がある。

なお、本稿で触れることのできなかった論点としてはまず、諸外国のデータ保護制度の下での DCR 評価との比較がある。もとよりインターネット広告はステークホルダが世界中に分散しながら協力して機能を実現させている。DCR も例外でなく、その多くが外国企業によって開発・提供されている。それらのベンダが前提とする法制度はまちまちであるため、外国で機能提供を可能にするデータフローが日本では適法にならない場合やその逆、更に、ある法域の下では思いもよらない点が別の法域で問題になることが起こりうる。DCR に限らず外国ベンダのソリューションを導入する際にはついて回る問題ではあるが、実務上は重要な問題である。特に欧州司法裁判所による *Meta Platforms Inc* v *Bundeskartellamt* 判決は、収集の文脈の異なる個人データを統合することはデータ主体の合理的期待を超えるため、文脈ごとに同意取得が必要としている [61]。DCR が異なる文脈の個人データを統合することを踏まえると注意深い分析が必要である。更に、WG 型 DCR への適用も考えられるデジタルサービス法や 2025 年 11 月に発表された GDPR 改正を含むデジタルオムニバス案など、DCR を利用する際には各国・地域の様々な法令に目配りが必要と考えられる。

もう１つ本稿で触れることのできなかった論点が、DCR ベンダが採用する PETs が DCR の機能や法制度対応にどのように寄与しているかの検討である。DCR ベンダはプ

[60] GDPR では代わりに共同管理者や処理者としての責任分担の交渉が必要であるが、これは少なくとも「適法に行うには交渉が必要である」ということ自体は関係者に共有されていることを意味する。ある DCR は個人データの第三者提供で、別の DCR は個人関連情報で適法化といった断片化した状態は、DCR 利用組織に無用の対応コストを強い、データ主体に DCR への不信感を与えることにつながる。

[61] 欧州司法裁判所 C-252/21 *Meta Platforms Inc* v *Bundeskartellamt* (2023) ECLI:EU:C:2023:537.

ライバシー保護とデータ共有・協業を両立するため様々な PETs を採用している [62]。しかし IAB Tech Lab が DCR ガイドでも指摘した通り、１つ１つの PET は特定のプライバシー攻撃を防ぐもので、プライバシー上の問題をすべて解決する「銀の弾丸」ではないし、今回の分析からわかるように技術の導入が自動的に法令遵守をもたらすとは限らない。５．４で論じたように DCR にはユーザを驚かせる要素を持つため、法令上の義務に限定することなくプライバシー全般に視野を拡げて PETs を採用した DCR が解決する問題と解決しない問題を見極め、後者については別の手当てを模索する必要があろう。

インターネット広告にはプライバシー上の問題だけでなく、ディスインフォメーションやフィルターバブルを助長しているという批判がある [63]。しかし冒頭に述べた通り、広告は現代人の情報生活を支える不可欠なインフラであり、そのエコシステムにおいてインターネット広告の占める割合は無視できるものではない。そして広告は、人々により優れた商品・サービスの情報を届ける経済の潤滑油としてだけでなく、その収益によりメディアの経営を可能とし、ひいては人々の知る権利を支える機能も担っている。広告モデルに替わるメディア収益モデルは未だ模索中であるため、広告の重要性が下がることは当面考えにくい。だとすれば、インターネット広告に様々な問題があるからといって、そのすべてを捨てることはできない。個々の問題を特定した上で、解決や適正化をする必要がある。そのためには、技術やビジネスの変化のスピードが激しい領域ではあるが、実態に即したきめ細やかな分析を適時に行い、合理的な解決策を模索する不断の努力が今後も求められるだろう。

参考文献

ITMedia 「Google,『プライバシーサンドボックス』を実質終了 関連技術のほとんどを廃止へ」(2025) https://www.itmedia.co.jp/news/articles/2510/19/news019.html

Acompany プライバシーテック研究所 「世界のデータクリーンルームサービスとは？AWS や Snowflake、Habu などを比較してみた」(2023) https://www.acompany.tech/privacytechlab/data-clean-room-platform

Google Cloud「差分プライバシーを利用する」 https://cloud.google.com/bigquery/docs/differential-privacy?hl=ja

[62] 例えば Google や AWS の DCR では差分プライバシーが、TikTok では合成データと TEE が、IAB Tech Lab の DCR をまたいだ直接アクティベーションのためのプロトコル PAIR では可換暗号が使われている。Vini Jaiswal “PrivacyGo Data Clean Room: A new tool for data collaboration” (2024) https://developers.tiktok.com/blog/privacygo-data-clean-room-open-source; IAB Tech Lab “Publisher Advertiser Identity Reconciliation (PAIR)” (2025) https://iabtechlab.com/pair/ ; Amazon Web Services “AWS Clean Rooms Differential Privacy” https://aws.amazon.com/jp/clean-rooms/differential-privacy/ ; Google Cloud「差分プライバシーを利用する」 https://cloud.google.com/bigquery/docs/differential-privacy?hl=ja

[63] 鳥海不二夫・山本龍彦「共同提言『健全な言論プラットフォームに向けて ver2.1 ―情報的健康を、実装へ』」(2024) https://www.kgri.keio.ac.jp/docs/XDignity-WP20241029.pdf

石井夏生利・曽我部真裕・森亮二(編)『個人情報保護法コンメンタール第２版第１巻』(勁草書房 2024)
公正取引委員会「デジタル広告分野の取引実態に関する最終報告書」(2021)
個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編)」
個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』に関する Q&A」
個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン（通則編）の一部を改正する告示案』に関する意見募集結果」(2021 年 8 月 2 日公表)
個人情報保護委員会「個人情報保護法の制度的課題に対する考え方(案)について（個人データ等の取扱いの態様の多様化等に伴うリスクに適切に対応した規律の在り方)」(2025)
個人情報保護委員会「個人情報保護法の制度的課題に対する考え方について（個人データ等の取扱いにおける本人関与に係る規律の在り方)」(2025)
自由民主党「デジタル・ニッポン 2024 ―新たな価値を創造するデータ戦略への視座―」(2024)
一般財団法人情報法制研究所オンライン広告研究タスクフォース「オーディエンスターゲティング広告における匿名加工情報の利用に関する提言」(2017)
https://www.jilis.org/proposal/data/2017-12-18.pdf
総務省総合通信基盤局「外部送信規律について」(2023)
https://www.soumu.go.jp/main_content/000862755.pdf
高木浩光「個人情報保護から個人データ保護へ(9) ―法目的に基づく制度見直しの検討―」情報法制研究 vol.16 p.96 (2024)
株式会社電通「日本の広告費 2024」(2024)
株式会社電通「2024 年日本の広告費 インターネット広告媒体費 詳細分析」(2025)
https://www.dentsu.co.jp/news/release/2025/0312-010858.html
鳥海不二夫・山本龍彦「共同提言『健全な言論プラットフォームに向けて ver2.1 ― 情報的健康を、実装へ』」(2024) https://www.kgri.keio.ac.jp/docs/XDignity-WP20241029.pdf
日本インタラクティブ広告協会『必携インターネット広告 プロが押さえておきたい新常識』(インプレス 2019)
株式会社博報堂ＤＹメディアパートナーズ メディア環境研究所「メディア定点調査 2024」(2024)

Amazon Web Services “AWS Clean Rooms” https://aws.amazon.com/jp/clean-rooms/
Amazon Web Services “AWS Clean Rooms Differential Privacy” https://aws.amazon.com/jp/clean-rooms/differential-privacy/
The Association of National Advertisers “ANA Releases ‘Ultimate Playbook for Data Clean Rooms’” (2024) https://www.ana.net/content/show/id/pr-2024-10-datacleanrooms
Anthony Chavez “A new path for Privacy Sandbox on the web” (2024) https://privacysandbox.com/news/privacy-sandbox-update/

Federal Trade Commission “Data Clean Rooms: Separating Fact from Fiction” (2024) https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/11/data-clean-rooms-separating-fact-fiction

Firefox Corporation “Firefox Focus New to Android, blocks annoying ads and protects your privacy” (2017) https://blog.mozilla.org/press/2017/06/firefox-focus-new-to-android-blocks-annoying-ads-and-protects-your-privacy/

Tilman Herbrich “Data Clean Rooms” *Computer Law Review International* vol.23(4) p.109 (2022)

Seiichi Igaya & Osamu Sudoh “Ignored Discrepancies in the Fundamental Concepts of Data Protection Laws in Japan and the EU” *International Data Privacy Law* vol.15(2) p.171 (2025)

IAB “Data Clean Rooms: A U.S. State Privacy Law Perspective” (2025) https://www.iab.com/wp-content/uploads/2025/04/IAB_Data_Clean_Rooms_A_US_State_Privacy_Law_Perspective_April-2025.pdf

IAB & Ipsos “State of Data 2023: Data Clean Rooms & the Democratization of Data in the Privacy-Centric Ecosystem” (2023) https://www.iab.com/wp-content/uploads/2023/01/IAB_State_of_Data_2023.pdf

IAB Europe “Data Clean Rooms: A Promising Prospect” (2022) https://iabeurope.eu/data-clean-rooms-a-promising-prospect/

IAB Tech Lab “Data Clean Rooms: Guidance and Recommended Practices” (2023) https://iabtechlab.com/blog/wp-content/uploads/2023/06/Data-Clean-Room-Guidance_Version_1.054.pdf

IAB Tech Lab “Publisher Advertiser Identity Reconciliation (PAIR)” (2025) https://iabtechlab.com/pair/

InfoSum “The ultimate guide to Data Clean Rooms 2023 edition” (2023)

Vini Jaiswal “PrivacyGo Data Clean Room: A new tool for data collaboration” (2024) https://developers.tiktok.com/blog/privacygo-data-clean-room-open-source

Piyush Jindal “Privacy-Preserving Data Analysis: Implications of Clean Rooms” *International Journal of Management, IT & Engineering* vol.14(6) (2024).

LiveRamp “Clean Rooms Guide: 12 Essential Strategies for Marketers” https://liveramp.com/data-clean-room-playbook-interactive/

Microsoft Edge Team “Safety and privacy in Microsoft Edge” (2020) https://blogs.windows.com/msedgedev/2020/10/26/safety-privacy-cyber-security-awareness-month/

Paul Ohm “Broken promises of privacy: Responding to the surprising failure of anonymization” UCLA Law Review vol.57(6) p.1701(2010)

Nadezhda Purtova & Ronald Leenes “Code as personal data: Implications for data protection law and regulation of algorithms” *International Data Privacy Law* vol.13(4) p.245 (2023).

Justin Schuh “Building a more private web: A path towards making third party cookies obsolete” (2020) https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

Kamakshi Sivaramakrishnan & Lena Pennington “Snowflake Data Clean Rooms: Securely Collaborate to Unlock Insights and Value” (2024) https://www.snowflake.com/en/blog/unlock-insights-with-snowflake-data-clean-rooms/

John Wilander “Full Third-Party Cookie Blocking and More” (2020) https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

World Federation of Advertisers “WFA Survey: A Closer Look at Data Clean Rooms” (2023)

（掲載決定日：令和 7 年 12 月 16 日）