サステナビリティ課題としての個人データ保護

板津　直孝

▌要　約▐

1. ブラックロックのフィンク CEO は、2020 年 1 月に公表した年頭書簡に、サステナビリティ課題のひとつとして「個人データ保護」を掲げた。個人データ保護は人権保護の社会要素と安全管理措置の観点での企業統治の要素を併せ持ち、投資先企業でも、同課題を強く意識した企業行動が見られる。その象徴的な動きのひとつが、IBM が 2020 年 6 月に先陣を切った、米国大手テクノロジー企業による人権保護に基づいた顔認識技術及び製品の提供の見直しである。
2. 顔認識技術など、ソフトウェアが意思決定を左右する仕組みは、バイアスを除去できていないことが最近の研究で明らかになっている。個人データを含むビッグデータに基づき人工知能（AI）が行う「プロファイリング」を法的にいかに規律していくべきかが、足下では人種差別の観点で社会問題として顕在化している。欧州経済領域（EEA）で 2018 年 5 月に施行された「一般データ保護規則（GDPR）」では、個人に対して、プロファイリングを含む自動処理のみに基づいた意思決定に服さない権利を保障している。
3. 個人データ保護の強化の潮流はまた、欧米間の個人データの越境移転において大きな影響を与えている。欧州連合（EU）司法裁判所は 2020 年 7 月、米国の個人データの保護水準が十分でないとして、欧米間での円滑な個人データの越境移転を可能にする「プライバシー・シールド」を無効とする判決を下した。報道によれば、米国の数千社がビジネスに支障をきたす恐れがあるとしている。
4. 個人データ処理が、自然人の権利及び自由に対して高いリスクをもたらす可能性がある場合には、技術及び製品の開発に先立って、企業はプライバシー・アセスメントを実施する必要がある。企業が、個人データに関連したリスクを軽減し機会を追求するには、データ処理と個人の権利利益の制約の均衡を評価することが重要である。

野村資本市場研究所　関連論文等

・板津直孝「新型コロナウイルス（COVID-19）と個人データ保護－多国籍企業に求められる取り組み－」『野村サステナビリティクォータリー』2020 年夏号。

Ⅰ はじめに

世界最大の資産運用会社であるブラックロックのラリー・フィンク CEO は 2020 年 1 月 14 日、恒例の投資先企業の CEO への年頭書簡を公表した。「金融の根本的な見直し（A Fundamental Reshaping of Finance）」と題した同書簡は、運用受託機関として、今後は投資戦略の中心にサステナビリティを置くという「サステナビリティ宣言」を強く印象付けるものであった。企業が様々なサステナビリティ課題に対してどのような対応をしているかについて、より明確に把握する必要性があるとして、気候変動対応だけでなく、従業員の多様性、サプライチェーンの持続可能性と並び、「個人データ保護」を具体的に挙げている。

個人データ保護は、近年、機関投資家が注目し始めている ESG 課題であり、E（環境）、S（社会）、G（企業統治）の中でも、人権保護の社会要素と安全管理措置の観点での企業統治の要素を併せ持つ。多くの国では、憲法上の基本的人権に位置づけられているプライバシー権の保護を目的として、個人データ保護関連法の施行又は強化が進められており、個人データの安全管理措置の強化を企業に求め始めている。

投資先企業サイドでも、自社製品における個人データ処理から生じる中長期的なリスクを踏まえ、人権保護の観点でサステナビリティ課題を強く意識した企業行動が見られる。その象徴的な動きのひとつが、米国大手テクノロジー企業による顔認識技術[1]の開発及び製品の販売の見直しである。その先陣を切ったのが、IBM である。

IBM のアービンド・クリシュナ CEO は 2020 年 6 月 8 日、米国議会への公開書簡という形で、汎用的な顔認識及び分析のためのソフトウェアを提供しないと発表した[2]。同氏は、「IBMは、集団監視、人種プロファイリング、基本的な人権および自由の侵害など、我々の価値観と、信頼及び透明性の原則（Principles of Trust and Transparency）と一致しない目的のために、他のベンダーが提供する顔認識技術を含む技術の使用に強く反対し、容認しない。我々は今こそ、国内の法執行機関が顔認識技術を採用すべきかどうか、またどのように採用すべきかについて国民的対話を始める時だと考えている」と述べた。同書簡では、人工知能（AI）システムのベンダーとユーザーは、AI が特に法執行機関で使用される場合に、バイアス[3]のテストを受け、そのようなバイアステストが監査され、報告されることを保証する責任を共有しており、また、警察による違法行為に関するより厳格な連邦法の制定を要求している。

IBM に続きアマゾンは 2020 年 6 月 10 日、顔認識システム「レコグニション」の警察への提供を今後 1 年間停止する旨を公表した[4]。その翌日には、マイクロソフトが、人権に基づいて顔認識技術を管理できる連邦法が規定されるまで、顔認識システムの警察への販

1 本稿での Facial Recognition については、顔認証を含めた顔認識として日本語表記している。
2 IBM, “IBM CEO’s Letter to Congress,” 8 June 2020.
3 バイアスは、母集団の不公正な標本抽出や、平均して正確な結果が得られない推定過程から生じる。個人、グループ、信条に対する偏見が生じる。
4 Amazon, “We are implementing a one-year moratorium on police use of Rekognition,” 10 June 2020.

売を停止すると発表した[5]。

顔認識システムを代表とする AI による特定の個人の識別には、人権保護の観点で安全管理措置が強く求められる。自社製品に組み込まれたエラーやバイアスにより、不測の人種差別や人権侵害を引き起こす可能性がある。エラーやバイアスから個人データを保護することは、サステナビリティ課題として、企業及び機関投資家が関心を高めている重要な ESG 要因となっている。現在導入されている AI 製品は、正確性及び説明可能性の点において課題が残されており、欧州経済領域（EEA）では、AI による自動化された意思決定に服さない権利を個人に認めている。

本稿では、情報通信技術（ICT）の進展による個人データのビッグデータ化など、グローバルな個人データ処理が急速に進み、個人データの共有や収集の規模が劇的に拡大している中で、サステナビリティ課題として重視され始めた個人データ保護に焦点を当てる。まず、人権保護の基本理念と強化される個人データ保護関連法に基づく執行の動向を整理し、その上で、企業のサステナビリティに資するプライバシー・アセスメントを考察する。

Ⅱ　デジタル経済における個人データ保護の基本理念

１．自己情報コントロール権を保障する個人データ保護

個人データ保護の強化に対する関心の高まりは、プライバシーの権利が自己情報コントロール権として「積極的プライバシー権」の側面を持つようになってきていることからも伺える。個人データの侵害時などに損害賠償請求等ができるというのが、従来の消極的なプライバシー権だが、これに対して、自己情報コントロール権は、企業等による個人データ処理においてデータ主体[6]が自己に関する情報をコントロールできる、つまり、積極的に個人データの公開や削除などの処理についてデータ主体が決定できるという権利である。

個人データの多くは、プライバシー性を有する。日本でも、プライバシーの権利は新しい人権として日本国憲法第 13 条によって保障された基本的人権である。個人データ保護における自己情報コントロール権は、プライバシー権の重要な構成要素であり、憲法上保護されるべき基本的人権であることから、公権力が自己情報コントロール権を制限する場合には、立法機関たる国会による立法措置が必要になる。

欧州連合（EU）では、基本的人権の確保を目的とした個人データ保護への対応が着実に進められてきた。個人データの保護は、欧州共通の憲法の枠組みの一部を構成し、「人間の尊厳」を基調とする EU 基本権憲章の第 8 条に明記されている。基本権としての人権尊重の精神に根差した「一般データ保護規則（GDPR：General Data Protection Regulation）」は、EU で 2018 年 5 月 25 日に施行された。GDPR では、第 5 条「個人データ処理に関する

[5] The Washington Post, “Microsoft bans police from using its facial-recognition technology,” 11 June 2020.

[6] 特定されたまたは特定可能な自然人は、総称して、データ主体（Data Subject）と定義され、個人データ保護に対する権利に関する諸権利の行使主体を表す。

基本原則」第 1 項(a)において「適法性、公正性、透明性」を掲げており、データ主体に対して、個人データの処理が適法かつ公正であり、透明性が確保されていることを求めている。企業が個人データ保護に対応する企業統治の一環としてプライバシー・ルールを検討する際には、この「適法性、公正性、透明性」の原則を基本理念として、ルールの根本に据えることが必要である。上述した米国大手テクノロジー企業による顔認識技術の開発及び製品の販売の見直しは、地域は異なるものの、まさにこの基本理念に基づいた対応であると言える。

個人データ保護の強化により、データ主体が自身の個人データをより強固にコントロール可能とすることは、デジタル経済における企業への消費者の信頼確保にも繋がる。GDPR では、前文第 7 項において「自然人は自身の個人データのコントロールを有するべきである」としており、自己情報コントロール権を保障する個人の権利を定めている。GDPR では、データ主体に関する具体的な権利が、第 3 章第 12 条から第 23 条において保護されている（図表 1）。

図表 1　GDPR によって保護されているデータ主体の権利

データ主体の権利の概要
「情報提供の透明性」（第 12 条） 管理者は、データ主体に、簡潔で、透明性があり、分かりやすく、容易にアクセスできる方式により、明確かつ平易な文言を用いて、個人データ処理について情報を提供する措置を講じなければならない。
「情報権」（第 13 条・第 14 条） 管理者は、データ主体からの取得、データ主体以外からの取得のそれぞれについて、所定の項目についての情報を提供しなければならない。
「アクセス権」（第 15 条） データ主体は、管理者に対し、データ主体に関する個人データが処理されているか否かの確認をとる権利、及び、個人データ及び所定の情報にアクセスする権利（開示請求権）を有する。
「訂正権」（第 16 条） データ主体は、管理者に対し、過度に遅滞することなく、データ主体に関する不正確な個人データを訂正させる権利を有する。
「削除権」（第 17 条） データ主体は、処理目的との関係で個人データが必要でなくなった場合や、個人データ処理に対する同意を撤回した場合など、所定の要件に該当する際には、データ主体に関する個人データを管理者に削除させる権利（忘れられる権利）を有する。
「処理制限権」（第 18 条） データ主体は、管理者に対し、個人データの正確性に異議を申し立てた場合に、管理者が個人データの正確性を確認する期間内や違法な処理がされた場合などに、個人データの処理を制限する権利を有する。
「個人データの訂正若しくは削除又は処理制限に関する通知義務」（第 19 条） 管理者は、第 16 条から第 18 条に基づく個人データの訂正、削除、処理制限を請求された場合には、個人データの受領者に通知しなければならない。
「データ・ポータビリティ権」（第 20 条） データ主体は、処理が同意又は契約に基づく場合で、かつコンピュータ処理されている場合に、①個人データを管理者に提供させる権利、②ある管理者から他の管理者に個人データを移行する権利、③技術的に実行可能な場合、ある管理者から別の管理者へ直接に個人データを移行させる権利を有する。
「異議申立権」（第 21 条） データ主体は、個人データが公的利益又は公的権限の遂行、又は正当な利益に基づいて処理がされている場合、プロファイリングによる処理も含め、個人データ処理に異議を唱える権利を有する。管理者は、ダイレクトマーケティング目的での個人データ処理に対して異議を申し立てられた場合、その処理を止めなければならない。
「プロファイリングを含む自動処理のみに基づく決定の対象とならない権利」（第 22 条） データ主体は、データ主体に関する法的効果をもたらす、又は、データ主体に対して同様の重大な影響を及ぼすプロファイリングを含む自動処理のみに基づいた決定の対象とならない権利を有する。

（出所）GDPR より野村資本市場研究所作成

データ主体の権利には、情報提供の透明性（第12条）、情報権（第13条・第14条）、アクセス権（第 15 条）、訂正権（第 16 条）、削除権（第 17 条）、処理制限権（第 18 条）、個人データの訂正若しくは削除又は処理制限に関する通知義務（第 19 条）、データ・ポータビリティ権（第20条）、異議申立権（第21条）、プロファイリングを含む自動処理のみに基づく決定の対象とならない権利（第22条）がある。

２．人権侵害のリスクを内在するプロファイリング

データ主体の権利の中でもGDPR第22条は、ビッグデータを利用したAIによる自動化された意思決定を取り入れるビジネスが世界的に拡大していることから、特に注目されている。この「プロファイリング」を法的にいかに規律していくべきかが、世界的な社会問題となっている。プロファイリングとは、犯罪捜査においては行動科学的に分析し犯人の特徴を推論することであるが、現在は、個人に関する決定を下すため、または個人の選好、行動及び態度を分析若しくは予測するための個人データの自動処理を意味する。 GDPR第4条第 4 項では、「自然人に関する一定の個人的側面を評価するために、特に、当該自然人の業績、経済状況、健康、個人的嗜好、興味、信頼性、行動、位置又は移動に関連する側面を分析又は予測するために、個人データの利用から構成されるあらゆる形態による個人データの自動処理」と定義付けている。顔認識技術による特定の個人の自動識別、すなわちプロファイリングから生じる個人データ侵害のリスクは、技術開発及び製品販売を進める企業にとって重要なサステナビリティ課題であり、機関投資家からも今後ますます注目されていくことであろう。

ICT の進展は、個人データを様々な異なる情報源から入手することを可能にしている。インターネット検索、購買履歴、携帯電話、ソーシャルネットワーク、ビデオ監視システム、モノのインターネット（IoT）から収集されたライフスタイルや行動データは、企業が収集する可能性のある個人データの例である。無数のオンライン及びオフラインのデータソースから個人データを収集し統合してビッグデータが構成され、名前、住所、年齢幅、趣味、民族、宗教を含む詳細な個人のプロファイルへの作成に至る。このビッグデータを利用して AI が分析し、人々を異なるグループに分類する。AIによる自動化された意思決定は、人間の関与なしに自動化された手段で行う意思決定であるが、予測するために利用されるデータセットの選択からビッグデータで対処される問題の定義、ビッグデータ分析の結果に基づく意思決定までの、あらゆる段階でエラーやバイアスが組み込まれる可能性を排除できていない。

GDPR 第 22 条で定める「データ主体に関する法的効果をもたらす、又は、データ主体に対して同様の重大な影響を及ぼすプロファイリングを含む自動処理のみに基づいた決定」では、データ主体から異議を申し立てられた場合、管理者は、データ主体の利益・権利・自由よりもデータ処理が優越することや、訴訟上の必要があるなどのやむを得ない適法な根拠を証明しない限り、個人データを処理できなくなる。同条は、個人データが不正確な

結果となる要素を正し、データ主体の権利利益が侵害されることを未然に防ぐことで、データ主体に対する差別的効果を防ぐことを意図している。

３．安全管理措置の強化の必要性が増す電子通信

GDPR とともに、EU のデジタル単一市場戦略を支える重要な法基盤になると位置付けられているのが、「e プライバシー規則（ePrivacy Regulation）案」である。現代社会において、電子通信は、思想や宗教、表現等の基本的な権利の行使にあたって重要な役割を果たしており、電子通信データの秘密が守られることの必要性が増している。同規則案は、GDPR を具体化し補完するものとして電気通信サービス利用者に高いレベルのセキュリティや秘密保護を求めており、2002 年 7 月発効の「e プライバシー指令（ePrivacy Directive）」を置き換えることが予定されている。加盟各国に直接の効力を持つ同規則案は、発効に向けた議論が慎重に進められているが、EU のデジタル・トランスフォーメーション（DX）に対する経済的・社会的影響等が論点になり、採択に向けた道のりは険しいものとなっている。2019 年 11 月 22 日、同規則案は、常駐代表委員会（COREPER ： Comite des Representants Permanents）により否決された[7]。欧州委員会（EC）は 2020 年 7 月末現在、e プライバシー規則の修正案の提出に向けて調整を進めている。

４．個人データの越境移転における保護措置

デジタル経済の進展により、現在では各国の消費者が自宅に居ながらにして、世界中から商品を購入したりサービスを受けたりすることができるようになっている。商品やサービスを提供する非居住者又は外国法人にとって、インターネットを利用した取引においては、物理的な営業拠点がなくても他国の消費者と取引をし、他国での重要な経済活動に従事することが可能になる。個人データは、容易に国境を越えて共有や収集されるようになり、グローバルな個人データ処理が急速に進み、その規模も劇的に拡大している。

各国の個人データ保護関連法において特に意識されるのが、個人データの「越境移転規制」である。越境移転規制とは、個人データ保護に対する法制度が十分に整っていない国へ個人データが移転されることで、個人データの侵害が発生する事態を防止するために個人データの国外移転を規制するものである。

GDPR では、EEA 域外に拠点を置く企業等が EEA 域内で商品やサービスを提供したり個人の行動を監視したりする場合には、EEA 域内の企業等と同様の個人データ保護が適用される。つまり、EEA 域内に拠点を置かなくても、日本から EEA 域内の個人の行動を分析する場合や、EEA 域内の顧客に対して商品又はサービスを提供する場合も、GDPR の規定が適用されるということである。EU の個人データ保護法は制定当初から、国際的な個人データ移転を可能にするいくつかのメカニズムを提供してきた。これらの主な目的は、

[7] EDRi, “ePrivacy: EU Member States push crucial reform on privacy norms close to a dead end,” 22 November 2019.

EEA 域内の個人データが域外に移転されるときに、個人データが GDPR と同等の水準の保護措置と共に域外移転することを保障することにある。

GDPR の下で国際的なデータ移転を可能にするには、原則として、「十分性認定（Adequacy Decision）」が求められる。十分性認定とは、EC が、特定の国や地域が個人データについて十分な保護水準を確保していると決定することをいう。十分性認定を受けることで、EEA 域内での個人データの国外移転に際して、個別の許可や手続きは必要なくなる。EC が EEA と同等の水準にあると認められる個人データ保護制度を世界に求めていることからも、個人データ保護関連法の整備を進めるうえで GDPR を参考にする国々は多い。GDPR は、グローバルなデータフローに対する開放性と、個人に対する高度な保護を兼ね備えており、GDPR を発効した EC は、データフローと個人データ保護の両方を必要とするデータサービスを提供する多国籍企業に対して、グローバルな基準設定機関としての役割を果たしているとも言える。

日本政府もまた、「データ・フリー・フロー・ウィズ・トラスト（DFFT）」のコンセプトを世界に発信している。すなわち、デジタル時代の競争力の源泉であり「21 世紀の石油」と呼ばれているデータは、プライバシーやセキュリティ、知的財産などのデータの安全性を確保しながら、原則として国内外において自由に流通することが必要であると、国際社会に向けて提唱している。

日欧の同調により、日本と EU は 2019 年 1 月 23 日、個人の権利利益を保護する上で、自国と同等の水準にあると認められる個人データ保護に関する制度を有している外国等として、相互に認定した。日本においては、個人情報保護法第 24 条に基づき EEA 協定に規定された国を指定し、EC においても、GDPR 第 45 条に基づく日本の十分性認定を決定した。同枠組みの発行により、日本と EEA 域内での個人データの移転に際して、個別の許可や手続きは必要なくなる。日本企業は、EEA 域内の事業者から個人データの提供を受けたり、委託を受けて個人データを処理したりすることができる。

個人データの保護と円滑なデータフローは、相互に排他的なものではなく、個人データ保護がデータ移転時も確保されることで、個人データを処理する企業への消費者の信頼を高めることと、グローバルなデータフローの促進を両立することが可能になる。企業は、グローバルにデータフローをマネジメントするに当たり、個人データ保護の観点を企業経営に取り入れることで、自社のサービスに対する消費者の信頼を高めることができる。適切な個人データ保護は、グローバルなデジタル経済において、多国籍企業に競争優位性をもたらすことになる。これは企業自身の、サステナビリティに資する取組みにつながると考えられる。こうした企業の取組みは、ESG 投資を拡大している機関投資家によって一層注目されていくと言える。

Ⅲ 強化される個人データ保護関連法に基づく執行の動向

１．新たな問題に直面した欧米間の個人データの越境移転

米国と EU との間では、個人データの越境移転に関して、個人データ保護に配慮した「プライバシー・シールド」が独自のフレームワークとして整備されていた。2015 年 10 月に EU 司法裁判所が無効とした二国間協定である「セーフハーバー」に代わるもので、EU 市民の個人データを EU の個人データ保護関連法に則った形で合法的に米国に移転することが可能となっている。米国には、連邦法において包括的な個人データ保護関連法が制定されていないなどの諸事情から、プライバシー・シールドが、日本と EU との間における十分性認定に相当する。

同制度で米国当局の認可を受けた米国企業は、GDPR に基づく個人データの EEA 域内から米国への移転に関して十分な保護レベルに達している企業とされ、米国と EU との間の国境を越えた個人データの移転は適正に実施されているかに見えた。

ところが、欧州議会は、プライバシー・シールドの枠組みで米国当局の認証を受けた米国企業が大規模な個人データ侵害を発生させたことから、プライバシー・シールドは個人の権利を保護するのに十分ではないと判断した。欧州議会は、GDPR の遵守を確保するために必要な措置をとり、米国が完全に遵守しない限り同制度を停止するよう EC に求める決議を 2018 年 7 月に採択した。

欧州議会が重要視した事案は、フェイスブックにおける個人データ侵害である。個人データ侵害の影響を受けた全世界のユーザー数は、フェイスブックの推計では 8,700 万人に上る。米国の連邦裁判所は 2020 年 4 月 23 日、2019 年 7 月にフェイスブックが連邦取引委員会（FTC）と交わした和解案を正式に承認した[8]。同判決により、フェイスブックは、ユーザーのプライバシー保護に対するアプローチを根本的に変え、50 億ドルの制裁金を支払うことに同意した。フェイスブックはまた、同事案に関連して、FTC との和解の他に、英国データ保護機関（ICO）より 50 万ポンド[9]、及び、米国証券取引委員会（SEC）より 1 億ドル[10]の制裁金をそれぞれ科されている。ICO による制裁金は、GDPR 施行前の EU データ保護指令により英国で制定された 1998 年データ保護法（Data Protection Act 1998）第 55 A 条に基づいている。ICO コミッショナーであるエリザベス・デンハム氏は、これらの違反行為が非常に重大であると考え、旧法に基づく最高金額の制裁金を科したとし、仮にこれが現行法である GDPR の下であったなら、制裁金は極めて高額になっていただろうと述べている。

EC は、上述の欧州議会の採択を受け、プライバシー・シールドに関わる米国との共同レビューを 2018 年 10 月に開始した。

---

8 CNET, “Federal court approves $5B Facebook settlement with FTC over Cambridge Analytica,” 24 April 2020.

9 ICO, “ICO issues maximum £500,000 fine,” 25 October 2018.

10 SEC, “Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data,” 24 July 2019.

２．EU 司法裁判所による無効判決

プライバシー・シールドは商業的な個人データの移転を容認するものであるが、国家安全保障の観点から例外を認めているため、EC は、米国の米国外国諜報活動偵察法（FISA：The Foreign Intelligence Surveillance Act of 1978）の第 702 条[11]と救済メカニズムについても、プライバシー・シールドに基づく個人データの移転を容認するか、評価する必要がある。フェイスブックによる個人データ侵害による欧州議会の採択を受け、EC は商業的側面での評価も開始した一方で、EU 司法裁判所は 2020 年 7 月 16 日、米国行政機関による個人データへのアクセスの観点で、プライバシー・シールドを無効とする判決を下した。

今般の判決は、オーストリアの弁護士であり EEA 域内のフェイスブックユーザーであるマックス・シュレム氏が、アイルランドに拠点を置くフェイスブックの関係会社から米国への個人データの移転の違法性を争って起こした訴訟に関連して下されている。EEA 域内から米国への個人データの移転がプライバシー・シールドに依拠する場合であっても、米国において十分に保護されない懸念があるとして、審理が進められていた。

同裁判所は、行政監察官のメカニズムはデータ主体に対して効果的な行政上または司法上の救済を提供しないと結論付け、プライバシー・シールドは EU 法に規定されているものと本質的に同等な保護水準を提供しておらず無効であるとした[12]。EU 法で要求されているものと実質的に同等の水準のメカニズムとしては、行政監察官の独立性と、米国の諜報機関を拘束する決定権を行政監察官に与える規則の存在の、両方を確保することであるとしている。

この判決は、最終審であり上訴することはできない。多くの米国企業は、プライバシー・シールドにより欧米間での個人データの移転を行っており、新たな対応に迫られる。報道によれば、今回の判決で、米国へ商用データを移転する数千社が日常業務に支障を来す恐れがあるとしている[13]。欧米間で個人データの移転を行う日本企業も、同様に対応が必要である。

EEA 域内から米国へ個人データを移転するには、プライバシー・シールドの他に、データ主体の明示的な同意や標準契約条項（SCC：Standard Contractual Clauses）[14]の締結などがある。個々のデータ主体にリスクについて情報提供した上で明示的な同意を取り付けることは、実務的に困難であることが推察される。

SCC は、個人データ移転元と移転先との間で、十分な保護措置等を内容とする EC が認めたひな形条項による契約の締結であるが、EU 司法裁判所は判決を下すに当たって、契

[11] 第 702 条は、電子通信サービスプロバイダに支援を要請し、米国政府が米国外にいる外国人を対象とした監視を実施し、外国諜報情報を入手することを認めている。

[12] Court of Justice of the European Union, “Judgement of the court,” 16 July 2020.

[13] Bloomberg, “EU Court Blocks Data Pact Amid Fears Over U.S. Surveillance,” 16 July 2020.

[14] SCC は GDPR 施行前の EU データ保護指令に基づく条項であり、GDPR 施行後は標準データ保護条項（SDPC：Standard Data Protection Clauses）に該当する。

約上の性質を有している SCC の有効性は認めつつも、SCC の利用には必要に応じて追加的な保護措置が必要であると付け加えている。判決によると、EU 法では、SCC に依存している個人データの管理者又は処理者は、必要に応じて、個人データの移転先と協力して、SCCの条項によって移転される個人データに追加的な保護を提供することにより、移転先の法律が、EU 法に基づき、SCC に従って移転される個人データの適切な保護を確保しているか否かを確認する必要があるとしている。つまり、SCCに基づいて個人データを米国に移転するには、管理者及び処理者は、EEA 域内で適用される EU 法と同等の水準にある保護措置が個人データに適用されていることを確認する必要がある。しかし、米国での国家安全保障に関する現状のメカニズムでは、行政監察官の独立性と、米国の諜報機関を拘束する決定権を行政監察官に与える規則の存在の両方が確保されない限り、SCCの有効性は実質担保されていない可能性がある。企業としては、米国への移転に伴うリスクを重視するのであれば、EEA 域内での個人データの処理に留めたデータフローを再構築することが有力な選択肢となる。

連邦法上の個人データ保護関連法に関するスタンスや方向性が不透明なトランプ政権は、企業によるサステナビリティ課題への取り組みに影を落としている。EU 司法裁判所による無効判決は、セーフハーバーに続き 2 回目である。無効判決が及ぼす米国企業への影響を考慮し、十分な保護水準を伴ったデータ利活用を整備するためには、米国政府が早急に連邦法上の法整備を進展させることが解決策のひとつである。米国政府が連邦法上の個人データ保護関連法を制定し、EC から十分性認定を受け、さらには日本からも個人情報保護法第 24 条による指定を受けることとなれば、日米欧間の DFFT 構想の実現にも近づくことが期待できよう。

３．個人データ保護関連法に関する米国の現状

米国ではオバマ政権（当時）の下で、2012 年 2 月 23 日、消費者データプライバシーに関する政策文書が公表されていた。ところが政権交代後、米国議会では消費者プライバシー権利法に関する法案が複数提出されているが、連邦法における包括的な個人データ保護関連法は 2020 年 7 月末現在、制定されていない。しかしながら、テクノロジー企業によるユーザーデータの利用等に際しては、米国民のプライバシーがリスクにさらされないようにすることは極めて重要である。

インターネットを通じた商品及びサービスのデジタル化は、世界経済を変革し、国境を越えた個人データの移転は、あらゆる分野のあらゆる規模の企業でビジネスの一部となっている。商業取引が個人データの流れにますます依存するようになるにつれて、データセキュリティと個人データ保護は、「消費者」の信頼の中心的な要素となってきている。

連邦法における包括的な個人データ保護関連法が制定されていない米国の現状において、消費者プライバシー保護の場面で公的機関が法執行を行う根拠としては、連邦取引委員会法（FTC 法：Federal Trade Commission Act）第 5 条がある。FTC 法第 5 条①では、「商取

引における又は商取引に影響を及ぼす不公正若しくは欺瞞的な行為又は慣行は、本法により違法と宣言する」と定められており、連邦取引委員会（FTC：Federal Trade Commission）に広範な権限を付与している。FTC は、FTC 法に基づいて設けられた委員会であり、不公正な競争方法の防止と独占禁止法に違反した企業の調査を主な任務とする。実質的に EU のデータ保護機関に相当し、民間分野における消費者データ処理を監督している。

もっとも、連邦政府機関の動向に一線を画する形で、一部の州政府では消費者データ保護に対して積極的な対応が進められている。カリフォルニア州は2020年1月、「カリフォルニア州消費者プライバシー法（CCPA：California Consumer Privacy Act）」を施行した。CCPA の制定以降、マサチューセッツ州、ニューヨーク州などの 10 州以上で CCPA をモデルとする法案が州議会に提出されており、連邦法上の包括的な消費者データ保護関連法制定の機運にも繋がっている。

CCPA は、憲法上の人権に位置づけられるプライバシー権の保護[15]を主な目的とする法律である。同法は、消費者に、企業が取集した個人情報を知る権利（開示請求権）、個人情報を削除する権利（削除権）、及び個人情報の第三者販売を停止する権利（オプトアウト権）を与えていることが特徴である。

Ⅳ　プライバシー・アセスメントと企業のサステナビリティ

個人のデータに係る権利侵害のリスクを軽減しつつ事業機会を追求する責任があるという認識は、個人の権利保護を備えたデータ利活用の世界的な浸透に従って、政府や企業などの間で共有され始めている。技術革新のスピード、複雑さ、国境を越えた個人データ保護関連法の広範な適用範囲が、企業のこれまで展開してきた人権保護へのアプローチを変革している。グローバルにビジネスを展開する企業に対しては特に、現在設定されているプライバシー・ポリシーやビジネス慣行で、ビジネスの不確実性や予期せぬリスクの可能性に対処できるのかが問われている。

また、顔認識技術をはじめとする技術の進歩とそれが経済に導入され普及していく過程で、人権への影響とリスクの性質が大きく変化してきている。健康データの処理による医療診断、ターゲティング広告から、プロファイリングによる国家安全保障に至るまで、企業に対しては、世界的にビジネスの機会が広がり始めている。その一方で、企業が、データ主体に保障された人権に重大な影響を及ぼす可能性のある製品などを、バイアスを含んだまま市場に解き放つリスクもある。脆弱な人々を差別するアルゴリズムなどは、市場に流通する前に未然に修正されなければならない。企業が、個人データに関連してリスクを軽減し機会を追求するには、データ処理の必要性と、達成させる目的のために取られる手段としての個人の権利利益の制約との間に均衡が保たれているかを評価することが重要である。

2020 年 7 月 21 日付ウォール・ストリート・ジャーナル紙によると、フェイスブックは、

[15] Article 1, Section 1 of the Constitution of the State of California.

同社の主要ソーシャルネットワークであるフェイスブックとインスタグラムを動かすアルゴリズムに、人種的バイアスがないかを調査するために新たな社内チームを設置する[16]。新設された「エクイティ・アンド・インクルージョン・チーム」では、機械学習システムを含む同社のアルゴリズムが、米国の黒人、ヒスパニック、その他のマイノリティのユーザーにどのような影響を与えているか、また、それらの影響を白人のユーザーと比較した場合どうなのかを調査する。ソフトウェアが意思決定を左右する仕組みにはバイアスのあることが、研究で明らかになっているとしている。

前述した GDPR 第 22 条では、データ主体に対して、プロファイリングを含む自動処理にのみに基づく決定の対象とならない権利を定めており、バイアスに対する強固な保護措置を施している。同条に基づけば、企業がアルゴリズムに含まれるバイアスを検出し修正できない限り、最終的な意思決定には、人を介在させることが求められよう。

個人データを処理する企業の中には、製品開発を進める上で人権アセスメントを実施する動きもある。グーグルは、製品の開発にあたり、潜在的な人権への影響を見極めながらリスク防止と軽減を図る目的で人権アセスメントを外部に委託し、顔認識製品分野にもたらされる可能性のある問題を洗い出した。プライバシー、表現の自由、安全性、子どもの権利、差別の禁止などの観点から、人権に与える影響の分析を行なっている。その結果検出された懸念される影響に対処するための方策を、同社は開発の重要な要素として取り入れた。

近年、人権への影響評価や、企業内部及び権利保有者との深い関わりなどに対処するため、事前のリスク評価の一環でプライバシー・アセスメントの取り組みが進められている。大手テクノロジー企業の間では、プライバシーなどの人権に配慮しながら AI や生体認証関連の事業でビッグデータを活用するために、位置情報や、顔や指紋で個人を識別する生体認証に含まれる個人データをどのように保護するかが課題となっている。これは、個人データ保護を備えたデータ利活用の実現に向けた企業の取り組みの一環である。

プライバシー・アセスメントは、個人データ処理の開始に先立ち実施されるリスク評価制度である。米国、カナダ、オーストラリアなどでは、プライバシー影響評価（PIA：Privacy Impact Assessment）が行われてきた。日本のマイナンバー制度においても PIA と類似の制度が導入されている。GDPR では、データ保護影響評価（DPIA：Data Protection Impact Assessment）が PIA に相当する。

GDPR は、新たな技術を用いた個人データ処理が、処理の性質・範囲・状況・目的を考慮すると、自然人の権利及び自由に対して高いリスクをもたらす可能性がある場合には、管理者に対し、処理の開始に先立ち、予定している個人データ処理に関する個人データ保護上の影響評価の実施を義務付けている（第 35 条第 1 項）。

DPIA は、以下のような個人データ処理を予定している場合、特に重要となる。

[16] The Wall Street Journal, “Facebook Creates Teams to Study Racial Bias, After Previously Limiting Such Efforts,” 21 July 2020.

- プロファイリングなどの自動処理に基づいた、自然人に関する個人的側面の体系的かつ広範囲な評価であって、その自動化された意思決定が、自然人に法的効果やそれに類する重大な影響をもたらす場合
- センシティブデータ[17]や有罪判決及び犯罪行為に関する個人データを大規模に処理する場合
- パブリック・スペースで体系的な大規模監視を行う場合

実務においては、EC が公表している DPIA に関するガイドライン[18]が参考になる。

マイクロソフトは、「今が行動の時だ」と題した顔認識技術に関する見解を公表している[19]。何も行動を取らなければ、5 年後には、顔認識サービスが社会的問題を悪化させるような状況に直面する可能性があり、一度そうなってしまえば、課題を解決することは遥かに困難になるとしている。同社にとって、顔認識技術及び製品は、サステナビリティの観点で重要な課題であると言える。

個人データ侵害によって自然人の権利及び自由に対して高いリスクをもたらす可能性は、大手テクノロジー企業に限った話ではない。例えば、ICO は、脆弱なセキュリティ対策に起因する個人データの漏洩などに対して、ブリティッシュ・エアウェイズに 1 億 8,339 万ポンド[20]及びマリオット・インターナショナルに 9,920 万ポンド[21]の制裁金をそれぞれに科すことを両者に通知している。グローバルに顧客データを保有する企業においては、より強固なデータセキュリティが求められる。

個人データは、データ主体との関係において、適法であり、公正であり、透明性のある態様で処理されなければならない。企業が保護を備えたデータ利活用を実現するためには、データ主体の権利を保護し個人データ保護関連法の遵守を確保するための技術的・組織的措置を講じて、同措置が個人データ処理と統合するように設計し、個人データ処理が処理目的に必要な最小限に限定されるように初期設定することが重要である。自然人の権利及び自由に対して高いリスクをもたらす可能性がある場合には、技術及び製品の開発に先立って、プライバシー・アセスメントを実施する必要がある。企業には、実施を予定している個人データ処理が、財務インパクトを及ぼす可能性のある、重要なサステナビリティ課題であるかを確実に識別することが、今まさに求められていると言えよう。

---

17 人種的もしくは民族的な出自、政治的な意見、宗教上もしくは思想上の信条、または、労働組合への加入を明らかにする個人データの処理、ならびに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、または、自然人の性生活もしくは性的指向に関するデータ（GDPR 第 9 条第 1 項）。

18 Article 29 Data Protection Working Party, “Guidelines on Data Protection Impact Assessment（DPIA）and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679,” 4 October 2017.

19 Microsoft, “Facial recognition: It’s time for action,” 6 December 2018.

20 ICO, “Statement in response to an announcement to the London Stock Exchange that the ICO intends to fine British Airways for breaches of data protection law,” 8 July 2019.

21 ICO, “Statement in response to Marriott International, Inc’s filing with the US Securities and Exchange Commission that the Information Commissioner's Office (ICO) intends to fine it for breaches of data protection law” 8 July 2019.