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－

板津　直孝

▌要　約▐

1. 新型のコロナウイルス感染症である COVID-19 は、世界的規模で経済・社会に多大な影響を及ぼしている。多国籍企業にとっては、業績への対応のみならず、グローバルに従業員の健康と安全を確保することが重要となる。同時に、広範なサプライチェーン上で COVID-19 対応措置を講じる上での、個人データの保護が求められている。個人データ保護は人権保護の一部であり、近年、企業に人権尊重の義務を求める考え方が世界的な潮流となってきている。
2. 各国のデータ保護機関及び関連する公的機関は、COVID-19 対応に関連して、相次いで個人データ保護の文脈でのガイダンスや見解を公表している。欧州連合では、個人データ保護を目的とした「一般データ保護規則（GDPR）」が、2018 年 5 月 25 日から適用されている。GDPR は、個人データへの侵害に対して、最大で全世界年間売上高の 4%という巨額な制裁金を企業に科すことで、多国籍企業に対し厳格な規律を求めている。
3. 欧州のみならず、中国、米国そして日本などにおいても、COVID-19 への感染が疑われる場合の、雇用主による従業員の健康データの収集や、コンタクトトレーシングアプリによるユーザーの位置情報や濃厚接触履歴の収集に対する取扱いが公表されている。健康データは、特に、個人データの中でも慎重な取り扱いが求められるセンシティブデータだからである。
4. 企業が人権を尊重し個人データを保護することは、企業による持続可能な開発目標（SDGs）への貢献につながる。COVID-19 対応が契機となり、多国籍企業は、ESG の S（社会）課題における人権保護の重要性を再認識し、サプライチェーン上での個人データ保護に関して具体的な行動を推進する形になっているとも言える。

野村資本市場研究所　関連論文等

・西山賢吾「ESG の社会（S）課題としての「ビジネスと人権」」『金融・資本市場動向レポート』No20-09

Ⅰ はじめに

2019年12月以降、新型コロナウイルス感染症（COVID-19）は短期間で世界的な広がりを見せ、経済・社会に多大な影響を及ぼしている。感染拡大防止への対応は、公衆衛生を確保するという国家の義務を浮き彫りにする一方で、このような事態に際して、企業は業績への対応のみならず、従業員の健康と安全を確保する労働法上の義務を負うことや、広範なサプライチェーン上での感染拡大防止に向けた責任ある行動が求められることも明確にしている。

多国籍企業においては特に、グローバルサプライチェーン上での感染状況やリスクを把握し、事業所内での2次感染防止や事業活動の継続のために、的確な情報に基づいた対応に迫られているが、ここでの情報には個人データが含まれる。また公衆衛生向上の必要性から、プラットフォーム事業者や移動通信事業者は、ユーザーの位置情報やサービス利用履歴を統計的に集計・解析し、地域での人流把握やクラスター早期発見等の感染拡大防止に資する活動が期待されているが、個人データの活用がその中核となっている。

COVID-19 対応措置を講じるうえでの個人データの取扱いに対して、各国のデータ保護機関（DPA：Data Protection Authority）及び関連する公的機関は、相次いで個人データ保護の文脈でのガイダンスや見解を公表している。各国の政府、公的機関及び民間企業が、COVID-19 の抑制と緩和のための措置を講じているが、そこには、様々な種類の個人データの処理が含まれているからである。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、グローバルなデータ処理が急速に進んでおり、データ共有やデータ収集の規模は、劇的に拡大している。多国籍企業については、大規模な個人データの漏洩や不正利用がグローバルリスクとして指摘されている。

個人データは人権の一部であり、その保護には人権保護の考え方である、無差別の原則が適用される。同原則は、国際人権法の最も基本的な原則並びに権利の1つであり、人権条約の中核を成す。市民的及び政治的権利に関する国際規約並びに経済的、社会的及び文化的権利に関する国際規約では、様々な理由に基づく差別を禁止している。このような考え方に基づき、個人データ保護に関する法整備や DPA の設立が各国で進められている。これらの法規制の多くは、人の生命、身体又は財産の保護のために必要がある場合や、公衆衛生の向上のために特に必要がある場合について、特別な取扱いを定めている。その際、公的機関における個人データの取扱いと民間企業におけるそれとは異なる。また、国及び地域ごとに法規制の内容も異なる。

各国・地域が規定する個人データ保護の中には、グローバルにビジネスを行う多国籍企業に影響を及ぼすものもあるため、実際の COVID-19 対応における個人データの取扱いについては、ビジネスを展開する国や地域ごとの個人データ保護関連法の確認が必要である。また、プラットフォーム事業者や移動通信事業者は特に、各国の DPA と連携して人権の保護に取り組むことが重要である。COVID-19 の感染拡大防止に資するデータ提供を政府

機関から要請された場合には、提供するデータの管理者[1]は、当該個人データの本人（データ主体）に対して、その行為が法的根拠に基づいていること等につき説明責任を負っているからである。民主主義社会においては、政府機関によるいかなる個人データ処理も、本質的に、プライバシーとデータ保護の権利に対する干渉となり、正当な目的に関連し、必要でありかつ比例性原則を満たしている場合に限り、正当化され得る。比例性原則とは、達成されるべき目的と、そのために取られる手段としての権利・利益の制約との間に、均衡を要求する考え方である。

本稿では、COVID-19 対応措置を講じる上での、民間企業と政府機関のそれぞれの場合における個人データの具体的な取り扱いについて、各国の DPA 及び関連する公的機関が公表する見解と取扱い事例を整理し、国や地域ごとに異なる個人データ保護関連法とこれらの法規制が多国籍企業に及ぼす影響について考察する。

Ⅱ　COVID-19 に関連した個人データ保護の国際的な動向

１．一般データ保護規則（GDPR）に基づく欧州の動向

１）欧州データ保護会議（EDPB）の議長声明

欧州データ保護会議（EDPB：European Data Protection Board）の議長は、欧州連合（EU）加盟国の DPA による COVID-19 対応に関する文書の公表に続くものとして、2020 年 3 月 16 日、COVID-19 のアウトブレイクに関連した個人データの取扱いに関する声明を発表した[2]。

EU では、個人データの保護という基本的人権の確保を目的とした「一般データ保護規則（GDPR：General Data Protection Regulation）」が、2018 年 5 月 25 日から適用されている。EDPB は、EU 加盟各国の DPA の代表、欧州データ保護監察機関（EDPS）の代表によって構成され、データ保護に関するベストプラクティスの公表などを通じて、EU 域内における GDPR の統一的な適用を促し、DPA の効果的な協力を保証するための会議体である。

この声明では、EU のデータ保護法は、COVID-19 対応措置を妨げるものではないとしつつも、このような例外的な時期においても、企業は政府と同様に、個人データの取扱いを含むパンデミック対策を採用する際には、データ主体の個人データ保護を確保しなければならないことが強調されている。したがって、個人データの合法的な取扱いを保証するために、多くの事項に留意すべきであるとしている。

EDPB は第一に、GDPR は、企業及び公的機関がデータ主体の同意なしに、今般のパンデミックの状況において個人データを処理することを可能にするいくつかの法的

[1] 単独または他者と共同で個人データの処理に関する目的、条件、及び手段を決定する自然人、法人、公的機関、政府機関、又はすべてのその他の団体。（GDPR 第 4 条第 7 項）

[2] EDPB, “Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak,” 16 March 2020.

図表 1　COVID-19 に関連する個人データ処理に法的根拠を与える規定

GDPR	公衆衛生の分野における公共の利益のため、又は重要な利益を保護するため（GDPR 第 6 条「処理の合法性」及び第 9 条「特別な種類の個人データの処理」）、又は他の法的義務を遵守するために、雇用主が個人データの取扱いを必要とする場合に認められる。
e プライバシー指令	同指令を実施する EU 加盟国の国内法は、位置データが匿名化されている場合、又は個人の同意がある場合にのみ、事業者が位置データを使用できる。 匿名データのみを処理することが不可能な場合、公衆衛生の分野における公共の利益の例外に該当することがあることに留意するとともに、EU 加盟国は国の安全と公共の安全を追求する立法措置を導入する必要がある（第 15 条）。

（出所）EDPB, “Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak,” 16 March 2020 より野村資本市場研究所作成

根拠を規定している（図表 1）。

第二に、移動位置データのような電子通信データの処理には、「e プライバシー指令（ePrivacy Directive）」が適用される（図表 1）。同指令は、電気通信サービス利用者に高いレベルのセキュリティーや機密保護を提供することを目的としており、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と位置付けられている。

EDPB は、公的機関に対して、まずは COVID-19 対応措置として「匿名」での位置情報の処理を行い、特定の場所におけるモバイルデバイスの集中に関する地図作成を求めている。匿名化とは、特定の個人を識別することができないように個人データを加工し、当該個人データを復元できないようにすることをいう。データの匿名化により、一定のルールの下で、本人の同意を得ることなく、ユーザーの位置情報やサービス利用履歴を統計的に集計・解析することができる。

匿名化が困難なため、EU 加盟国が e プライバシー指令第 15 条に基づき緊急立法を導入する場合は、必要かつ適切で比例性原則に基づく措置を構成するという条件の下で可能であり、EU 加盟国は、個人に司法救済の権利を与えるなどの適切な保護措置を実施する義務を負う。この点に関し、いくつかの EU 加盟国は、COVID-19 対応措置として緊急立法を採択しており、人流の把握やクラスター早期発見等の感染拡大防止を目的として、特定の場所におけるモバイルデバイスの集中度合いを解析している。

2）スペイン・データ保護機関（AEPD）による報告書

2020 年 3 月 12 日、スペイン・データ保護機関（AEDP：Agencia Española de Protección de Datos）は、データ保護と COVID-19 に関する報告書を公表した[3]。同報告書は、個人データを処理するための法的根拠及び個人データの最小化という、データ保護に関する 2 つの側面を扱っている。個人データの最小化とは、適切で、関連性

[3] AEDP, “Report from the Statement Legal Service (Detached Department of the SLS at the Spanish DPA) on Processing Activities Relating to the Obligation For Controllers from Private Companies and Public Administrations to Report on Workers Suffering from COVID-19,” 12 March 2020.

があり、かつ、処理の目的に限定された個人データのみを処理するという要件である。同報告書は、スペインの国内法と GDPR の両方を考慮し、EDPB の議長声明をより具体的に解説している。

AEPD はデータの管理者に対し、 GDPR には 、COVID-19 への対応措置との関連で個人データを処理する際の法的根拠がいくつかあることを指摘している。ただし、健康データなどの特別な種類のデータが含まれるため、AEPD は、以下の通り、GDPR 第 6 条及び第 9 条が規定する法的根拠の両方を満たす必要があることを強調している（図表 2、3）。

第 6 条(1) (c)では「管理者が従うべき法律」について規定されているが、当該法律は、具体的には、EU 法または EU 加盟国法を指している。EU 加盟国法について AEPD は、特にスペインの労働法に基づく雇用主の労働災害防止義務を例示している。

第 6 条(1) (d)では重要な利益の保護の対象を「データ主体又は他の自然人」としていることから、AEPD は、COVID-19 に感染する可能性のあるすべての人の保護を目的とした個人データの処理を正当化するために、可能な限り幅広い方法で解釈されるべきであると述べている。

図表 2　GDPR 第 6 条に基づく COVID-19 に関する個人データ処理の法的根拠

第 6 条(1) (c)	管理者が従うべき法律上の義務を果たすために、その処理が必要な場合。
第 6 条(1) (d)	データ主体又は他の自然人の重要な利益を保護するために、その処理が必要な場合。
第 6 条(1) (e)	公共の利益のために遂行される業務又は管理者に与えられた職権の行使のためにその処理が必要な場合。

（出所）General Data Protection Regulation (GDPR)より野村資本市場研究所作成

図表 3　GDPR 第 9 条に基づく COVID-19 に関する個人データ処理の法的根拠

第 9 条(2) (b)	EU 法、加盟国法又はデータ主体の基本的権利及び利益に対して適切な保護措置を備えた加盟国法に基づく労働協約によって認可されている限りにおいて、雇用法、社会保障法及び社会保護法の分野において管理者又はデータ主体の義務を履行し、特定の権利を行使する目的で処理が必要な場合。
第 9 条(2) (c)	データ主体が物理的又は法的に同意を与えることができない場合、データ主体又は他の自然人の重要な利益を保護するために処理が必要な場合。
第 9 条(2) (g)	追求される目的に比例し、データ保護の権利の本質を尊重し、データ主体の基本的権利と利益を保護するための適切かつ具体的な措置を備えた EU 法又は加盟国法に基づいて、実質的な公共の利益のために処理が必要な場合。
第 9 条(2) (h)	EU 法、加盟国法又は医療専門家との契約に従い、第 3 項の秘密保持義務に記載されている条件及び保護措置に基づき、従業員の作業能力の評価、医療診断、健康・公的介護・治療・健康又は公的介護システムとサービスの管理のため、予防医学又は職業医学の目的で処理が必要な場合。
第 9 条(2) (i)	データ主体の権利と自由を保護するための適切で具体的な措置、特に職業上の守秘義務を定める EU 法又は加盟国法に基づく、国境を越えた健康への深刻な脅威からの保護や、医療及び医薬品又は医療機器の品質及び安全性に関する高い基準の確保など、公衆衛生の分野における公共の利益のために処理が必要な場合。

（出所）GDPR.EU, “General Data Protection Regulation (GDPR)”より野村資本市場研究所作成

個人データのうち健康データは、 GDPR では特別な種類のデータとして分類されている。そのため、図表 3 の通り第 9 条に含まれる例外のいずれかに該当しない限り、その取扱いは禁止されている。

第 9 条(2) (b)は、雇用主と従業員との関係を定めている。雇用主は、職業上のリスクの防止に関するスペインの国内法である法律 31/1995 に基づいて、従業員の安全と健康を確保する義務を負う。従業員も、法律 31/1995 に基づき、職場の他の従業員の安全を確保する義務を負っていることから、COVID-19 感染者に接触した疑いがある場合には、雇用主に通知しなければならない。その際雇用主は、従業員から受け取った個人データを GDPR に従って処理しなければならない。

AEPD は、管理者が COVID-19 の感染拡大を防止するために必要最低限の、適切かつ関連性のある個人データのみを処理するべく、データ最小化を強調している。この点、GDPR 前文第 54 項では、公共の利益を理由とする健康関連データの処理は、雇用主、保険会社又は銀行などの第三者が、他の目的のために個人データを取り扱う結果となってはならない旨、明確に述べている。

３）ドイツ・データ保護会議（DSK）の声明

ドイツ・データ保護当局の共同調整機関であるドイツ・データ保護会議（DSK：The Conference of German Data Protection Authorities）は、2020 年 3 月 13 日、COVID-19 に関連して、雇用主による従業員の個人データ処理に焦点を当てた声明を公表した[4]。

同声明は、COVID-19 に関連して処理される個人データのほとんどは、健康データであり、特別な種類の個人データに該当することから、GDPR 第 9 条に従って特に保護されるべきだと強調している。健康データの処理は基本的に制限された方法でのみ可能である。処理される個人データの量はその目的の重要性に比例する必要があり、他の基本的な権利との間でバランスのとれたものでなければならない。

その上で、従業員間のウイルスの拡散を可能な限り防止または制限するために、雇用主が従業員及び訪問者の健康データを含む個人データを処理することは、データ保護法に適合するとしている。具体的には、(1) 感染が確認された又は感染している人と接触したか、(2) 該当期間中にロベルト・コッホ研究所（RKI）[5]によりリスク地域として分類された地域を訪れたか、という個人データが含まれる。感染者と接触したことのある人には注意を喚起すべきであるが、接触した可能性のある人に感染者または潜在的感染者の個人データを開示することは、例外的に必要な場合にのみ許可される。

そして、COVID-19 に対処するために処理された個人データは、その目的に合致しなくなった時点、すなわち感染拡大が終息した時点、又は COVID-19 が十分に封じ込められた時点で削除しなければならないことを、DSK は強調している。

---

[4] BfDi, “Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie,” 13 March 2020.

[5] 1891 年に設立された感染症や非感染性疾患のためのドイツ連邦共和国の中央監視研究機関。

４）イタリア・データ保護機関（Garante）の声明

DSK と比較して、イタリア・データ保護機関（Garante：Garante Per La Protezione Dei Dati Personali）は、GDPR における健康データの処理の条件を厳格に解釈している。Garante が 2020 年 3 月 2 日に公表した声明によると、雇用主は、個々の従業員への特定の要請又は許可されていない調査を通じて、従業員及び濃厚接触者における COVID-19 の症状に関する情報、又は職場外の地域に関する情報を、自主的に体系的かつ一般的な方法で収集してはならないことを明確にした[6]。こうした情報の収集は医療当局に委ねるべきであり、雇用主は、法律で特に義務付けられている場合又は所管官庁から要請されている場合を除き、従業員の健康データを自発的に収集すべきではないとした。

Garante は、すべての管理者が、COVID-19 関連対策の全国的な調整を管轄する機関（管轄機関）の要請に対応して、イタリア保健省及び管轄機関から提供される COVID-19 の蔓延を防止するための指示を厳格に遵守することを求めている。

５）フランス・データ保護機関（CNIL）の声明

COVID-19 に関連した健康データの処理について、イタリアの Garante と同様に厳格な解釈を公表した EU 加盟国のデータ保護機関として、フランスの情報処理及び自由に関する全国委員会（CNIL：Commission nationale de l'infromatique et des libertes）が挙げられる[7]。

CNIL が 2020 年 5 月 6 日に公表した声明によると、CNIL は、特に、COVID-19 への感染が疑われる場合の管理を超える健康データの収集に懸念を抱いている。これらのデータは、GDPR と公衆衛生法の規定の両方により、実際には非常に特別な保護の対象となっているからである。

CNIL によれば、雇用主は、従業員から COVID-19 症状に関する情報を体系的で一般化された方法で、又は個別の問い合わせや要求を通じて収集すべきではない。例えば、雇用主が従業員や訪問者に毎日体温チェックを受けさせたり、健康データをアンケートで集めたりすることは適切ではないとしている。CNIL の立場は、この点で、イタリアの Garante が公表した声明と同様に GDPR を厳格に解釈したものである。

その上で、CNIL は、雇用主及び従業員に、COVID-19 に関しては労働法に従って対応措置を講ずべきであるとしている。具体的には、雇用主は、労働法 L. 4121-1 条に従って、従業員の健康と安全に責任を負うため、従業員に個人の感染リスクの報告を求め、関連する情報を保健当局と共有することができる。従業員は、労働法 L.4122-1 条に従って、自身と他の従業員の健康と安全を維持するために、COVID-19 の感染が疑われる場合は、雇用主に通知する必要がある。最終的に、保健当局が健康データを収集し、状況に応じた対策を講じる。COVID-19 の症状に関する情報と特定の人々の最近の動きに関する情報の評価と収集は、これらの公的機関の責任である。

---

6 Garante, “Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati,” 2 March 2020.

7 CNIL, “Coronavirus (COVID-19) : les rappels de la CNIL sur la collecte de données personnelles,” 6 March 2020.

２．中国サイバースペース管理局（CAC）による通知

中国では COVID-19 対応措置として、地方政府と地方公安局（PSB）が、感染者や濃厚接触者の氏名、年齢、住所、公共交通機関の乗車履歴、位置情報などの個人情報を収集している。同国では公衆衛生を目的とした情報収集が広く行われるようになったことで、個人情報の漏洩や不正利用の可能性が懸念事項として浮上した。

中国サイバースペース管理局（CAC：Cyberspace Administration of China）は、2020 年 2 月 9 日、COVID-19 に関連した個人情報の侵害に対する国民の懸念に対応し、個人情報の更なる無許可利用を防止するため、個人情報の効果的な保護及びビッグデータの積極的な活用に関する通知を公布した（図表 4）[8]。

CAC は、関連部門の指導の下で積極的にビッグデータを利用することを推奨しているが、違法に個人情報を収集、利用、公開し、個人情報を大量に流出させる個人情報の侵害に対して、厳しく取り締まるとしている。

図表 4　COVID-19 に関する個人情報保護に関する通知の概要

公衆衛生上の目的で個人情報を収集することができる者の制限
感染症の予防及び治療に関する法律及び公衆衛生上の緊急事態への対応に関する規則に基づき、国務院衛生部の許可を受けた機関以外は、法令に別段の定めがある場合を除き、防疫及び取締り又は疾病の予防及び治療を理由として、本人の同意なく個人情報を収集し、又は利用することはできい。
情報収集の最小化原則の遵守
個人情報の収集は、国家標準[1]である「個人情報安全規範」を参照し、情報収集の最小化原則を遵守する必要がある。収集対象は、原則として、診断を受けて陽性となった者、感染の可能性がある者、濃厚接触者に限られ、特定地域の人々に対する事実上の差別の形成を防ぐため、特定地域のすべての人々を対象としない。
個人情報の利用目的の制限
COVID-19 対応措置のために収集した個人情報は、その他の目的で利用することはできない。COVID-19 対応措置で必要があるもの及びデータ脱感作（Data Desensitization）[2]を経たものを除き、本人の同意なしに、氏名、年齢、身分証明書番号、電話番号、自宅住所などの個人情報を公開してはならない。
個人情報への技術的保護措置
個人情報を収集又は管理する機関は、個人情報のセキュリティー保護に責任を負い、盗難や漏洩を防止するために厳格な管理及び技術的保護措置を講じる。

（注）　1. 国家推奨標準であり、法的拘束力はないが、実務上に重要な参考基準。
2. 特定の種類の個人データに対し一定の規則を通じてデータの変形をし、センシティブデータに係る信頼可能な保護を実現すること。

（出所）CAC, “关于做好个人信息保护利用大数据支撑联防联控工作的通知,” 9 February 2020 より野村資本市場研究所作成

[8] CAC, “关于做好个人信息保护利用大数据支撑联防联控工作的通知, ” 9 February 2020.

３．米国連邦議会の COVID-19 消費者データ保護法案

2018 年 5 月に GDPR が EU で施行され、巨大 ICT 企業（ビッグテック）に対して巨額な制裁金が課されるなど、個人データ保護に関する法整備や執行が各国において進められているが、米国ではこれまで、連邦法においては、GDPR に相当する個人データ保護の法令制定を求める議論の段階というのが実状であった。

しかしながら、テクノロジー企業が COVID-19 の拡大を追跡するためにデータを利用する際、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。前述の通り、GDPR の考え方に基づけば、健康情報や位置情報は特別な種類の個人データを第三者に明らかにする可能性があり、個人データを利用する企業はデータ処理の透明性を確保しなければならない。

米国連邦議会では、COVID-19 の危機的状況にあっても個人データ保護はきわめて重要であり、テクノロジー企業が COVID-19 を追跡する技術革新と米国民のプライバシー保護との適切な均衡を図るように義務付けることを目的として、2020 年 4 月 30 日、「COVID-19 消費者データ保護法案」が提出された[9]。同法案は、公衆衛生上の緊急事態の期間中、COVID-19 の拡大を追跡し制限する取り組みに関連して、健康情報や位置情報の収集と利用を規制するものであり、その概要は図表 5 の通りである。

図表 5　COVID-19 消費者データ保護法案の概要

- 連邦取引委員会（FTC）の管轄下にある企業に対し、COVID-19 の拡大を追跡する目的で、個人の健康、地理的位置、又は近接に関する情報を収集、処理、又は移転する際に、個人に事前通知をし、個人から肯定的な明示の同意を得ることを義務付ける。
- 企業に対して、データがどのように取り扱われ、誰に移転され、どのくらいの期間保持されるかを、収集時点で消費者に開示するように指示する。
- 企業が消費者データの再識別を防止するための技術的及び法的保護措置を確実に採用するために、集計データと非識別データの構成要素について明確な定義を確立する。
- 個人の健康情報、地理的位置情報、又は近接情報の収集、処理、又は移転から個人がオプトアウトできるように企業に義務付ける。
- COVID-19 に関連したデータ収集活動を説明する透明性レポートを企業に公開するように指示する。
- 対象事業体が収集した個人を特定できる情報について、データの最小化とデータセキュリティの要件を確立する。
- COVID-19 の公衆衛生上の緊急事態のために利用されなくなった場合には、個人を特定できるすべての情報を削除又は識別不能にすることを企業に義務付ける。
- 州検事総長に本法を施行する権限を与える。

（注）　同法案では、個人からの同意の撤回について定めている。
（出所）U.S. Senate Committee on Commerce, Science, and Transportation, “Wicker, Thune, Moran, Blackburn Announce Plans to Introduce Data Privacy Bill,” 30 April 2020 より野村資本市場研究所作成

[9] U.S. Senate Committee on Commerce, Science, and Transportation, “A bill to protect the privacy of consumers’ personal health information, proximity data, and geolocation data during the coronavirus public health crisis,” 30 April 2020.

同法案において、米国の個人データ保護の執行に関して、連邦レベルで重要な役割を果たすとされているのが、連邦取引委員会（FTC：Federal Trade Commission）である。FTCは、1914 年に制定された米国連邦取引委員会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、民間分野における個人データ処理を監督している。

具体的に規制の対象となる個人データは、正確な位置情報データ、近接データ及び個人の健康情報である。対象となる個人データを収集、処理又は移転する企業が、(1) COVID-19 の感染、徴候、症状を追跡する、(2)ソーシャル・ディスタンシングに関するガイドライン又はCOVID-19 に関連する他の要請に従った措置をとる、(3) COVID-19 においてコンタクトトレースを実施する際に、同法案の規定が適用される。

４．日本の個人情報の保護に関する法律（個人情報保護法）での取り扱い

日本の個人情報保護委員会事務局は、企業が COVID-19 感染拡大防止を目的として個人データを取り扱う機会が増えていることを踏まえ、2020 年 4 月 2 日、COVID-19 感染拡大防止を目的とした個人データの取扱いを公表した[10]。

日本における個人データ保護法制については、情報化の急速な進展により個人の権利利益の侵害の危険性が高まったことと国際的な法制定の動向等を受けて、「個人情報の保護に関する法律」（個人情報保護法）が、2003 年 5 月に公布され、2005 年 4 月に全面施行された。同法は、2016 年 1 月 1 日より、内閣府の外局として置かれた 3 条委員会[11]である個人情報保護委員会が所管している。

個人情報保護法では、個人情報取扱事業者[12]が保有する個人データについて、原則として、本人に通知等している利用目的とは異なる目的で利用し、又は、本人の同意なく第三者に提供することを規制している。しかしながら COVID-19 感染拡大の状況においては、例外的な対応が必要となる可能性も高まる。その点、同法第 16 条「利用目的による制限」及び第 23 条「第三者提供の制限」では、個人情報取扱事業者が、本人の同意なく、個人データを目的外に利用し、第三者への提供を可能にする場合の、法的根拠が定められている（図表 6）。

COVID-19 対応においては、コンタクトトレーシングアプリの利用が注目されている。具体的には、携帯端末の Bluetooth 等の技術を用いて、当該利用者同士の濃厚接触履歴を作成・保存し、これを手掛かりに、利用者に感染者が出た場合に速やかに当該利用者の濃厚接触者に警告を出すアプリの利用である。個人情報保護委員会は、コンタクトトレーシ

10 個人情報保護委員会事務局「新型コロナウイルス感染症の感染拡大防止を目的とした個人データの取扱について」2020 年 4 月 2 日

11 国家行政組織法第 3 条や内閣府設置法第 64 条の規定に基づいて、府省の外局として置かれる、独立性の高い行政委員会。内閣府では、公正取引委員会・国家公安委員会・個人情報保護委員会がある。

12 個人情報データベース等を事業の用に供している者。

図表 6　第 16 条及び第 23 条に基づく COVID-19 に関する個人データ取扱いの法的根拠

■ 第 16 条第 3 項第 2 号、第 23 条第 1 項第 2 号
人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

■ 第 16 条第 3 項第 3 号、第 23 条第 1 項第 3 号
公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

■ 第 16 条第 3 項第 4 号、第 23 条第 1 項第 4 号
国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（出所）e-Gov「個人情報の保護に関する法律」より野村資本市場研究所作成

ングアプリについては、EDPB と同様に慎重な見解を示しており、個人に十分かつ具体的な内容の情報を伝えた上で、当該個人の任意の同意により行われるべきであるとしている。また、当該アプリに関与する事業者が、国や地方公共団体とも連携し、アプリ運用の透明性の確保や適切な安全管理措置の実施により利用者の信頼を得ていくことが必要不可欠であるとして、個人データに係る個人の権利利益の確保の要請と感染症対策という公共政策上の利用の要請とのバランスに留意した慎重な見解を表明している。これらのアプリは、利用者の PCR 検査結果や行動履歴といった、取扱いを誤れば個人の権利利益を大きく侵害しかねないシステムであるからである。

Ⅲ COVID-19 対応の多国籍企業への示唆

１．企業に求められるサプライチェーン上の個人データへの適切な対応

世界中でビジネスを展開している多国籍企業では、サプライチェーンが世界に広がり、企業活動によって影響を受ける個人が多数存在している。企業が個人データ保護に対して措置を講じる際には、自社の従業員の個人データという狭い範囲ではなく、事業活動を行う上で影響を与える可能性のある第三者も含めて、広範なサプライチェーン上の個人データ保護について配慮することが求められている。

EU 市民の人権などを定めた EU 基本権憲章において、個人データの保護は基本的人権とされており、デジタル時代における人権保護の強化等の観点も踏まえて、GDPR や e プライバシー指令が立法された。GDPR や e プライバシー指令は、個人データやプライバシーの保護に関し厳格に規定しており、デジタル・プラットフォーマーの事業展開にも大きく影響している。欧州委員会より個人データについて十分な保護水準を確保しているという十分性認定を受けている日本をはじめとして、各国で制定が進められている個人データ保護関連法は GDPR を参考としたものが多く、個人データの保護を尊重する土壌は世界

的に広がりを見せている。

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と共に、同権利の侵害は民法の不法行為（民法 709 条）であり民事上の責任を生じさせるという意味で、法律上保護された権利として認められている。個人情報の多くはプライバシー性を有し、企業は、個人情報保護法に限らず民法等関係法令を確認し遵守する必要がある。

人権保護についてはこれまで、主に公的機関により対応が行われてきたが、近年、企業に人権を尊重する義務を求める考え方が世界的な潮流となってきている。個人データ保護はこうした動向のひとつであり、各国の法令にも反映され、多国籍企業に特に大きな影響を及ぼしつつある。

金融資本市場では、投資判断の際に ESG（環境・社会・ガバナンス）課題を組み込む ESG 投資が世界的に活発化している。人権保護は ESG の S 要素であり、企業の対応は、機関投資家が ESG 投資を行う上での判断に取り入れられうる。各国の DPA の取組みとそれに対する企業の対応は、ESG 投資を進める機関投資家にとって、個人データ保護への配慮の観点から企業を評価する上で、今後ますます有用となってくる可能性があると言えよう。

２．多国籍企業が考慮すべき COVID-19 に関連する個人データ保護措置

本稿で紹介した通り、個人データ保護に関連する法令やその解釈は、多国籍企業がビジネスを展開する国や地域によって異なる。GDPR をはじめとする多くの個人データ保護関連法に基づけば、COVID-19 に関連するデータ処理では、特別な種類の個人データに該当する個人の健康データを取扱うケースが想定されるため、より慎重な対応措置が企業に求められる。前述の通り、個人データ侵害に対して、GDPR では、全世界での年間売上高のうち最大で 4%までを企業に科す巨額な制裁金があることも留意すべきである。

具体的には、多国籍企業が、国境を越えてグローバルに従業員の健康と安全を確保したり、コンタクトトレーシングアプリを利用してパンデミック対策を講じる際に、あるいはプラットフォーム事業者や移動通信事業者が、ユーザーの位置情報やサービス利用履歴を利用したりする際には、各国の異なる法令や解釈に向き合う必要がある。これらの企業は、人権保護と無差別の原則に立ち返り、COVID-19 に関連する自社の個人データ保護方針又は透明性レポートを、自社内と影響を及ぼす可能性のある第三者に対して開示することが推奨される。

前述した各国の法令や DPA による解釈を保守的に理解した上で参考にすると、多国籍企業がグローバルな個人データ保護措置を講じる上で、以下のような、幾つかの共通した論点が浮かび上がってくる。これらは、多国籍企業が個人データ保護方針を策定する上で、考慮すべき項目として参考になると言える。

１）個人データの利用目的の明示と本人の同意

個人データの利用目的や、収集されるデータの種類、データ保管の期間などを具体的に特定し、データ主体にわかりやすく明示した上で、有効な同意を得る。企業は、COVID-19 に対する公衆衛生上の保護を目的とした場合のみ個人データを処理し、その行為が公衆衛生上の緊急事態に関する法令や労働法等の法的根拠に基づき、透明性が確保された体制を整備することにより、説明責任をデータ主体に対して果たす。

２）データ保護・バイ・デザイン及びデフォルト

企業は、個人データの処理に当たって、匿名化などの適切な技術的・組織的措置を講じ、データ最小化のようなデータ保護の原則を効果的な方法で実施し、データ主体の権利を保護するために必要な措置を、データ処理と統合した形で設計する。COVID-19 対応措置として可能な限り匿名での位置情報の処理を行い、特定の個人を識別することができないように個人データを加工し、当該個人データを復元できないようにする。匿名化が困難な場合は COVID-19 の拡大を防止するために、適切で、関連性があり、かつ、特定の目的に限定された個人データのみを処理する。企業は、データ保護の初期設定において、特定の各処理目的に必要な個人データだけが処理されることを確保するべく、適切な技術的および組織的措置を講じなければならない。

このような考え方は、GDPR 第 25 条においてデータ保護・バイ・デザイン及びデフォルトとして明記されている。管理者は、データ主体の権利を保護し GDPR の遵守を確保するための技術的・組織的措置を講じて、同措置がデータ処理と統合するように設計し、データ処理行為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（デフォルト）する義務がある。

３）必要性に応じた個人データの消去

企業は、公衆衛生面で有用性がなくなり不要となった個人データを遅滞なく消去し、以後の目的外利用のために個人データを保持してはならない。

４）個人データの安全管理措置

企業は、暗号化などの個人データを保護する適切な安全管理措置を講じ、従業員及び委託先の監督を適切に行うとともに、データ主体からの問い合わせや苦情を受け付ける体制を構築する。

欧州では GDPR に基づき、ビッグテックをはじめとする多くの多国籍企業が個人データの侵害に対して、巨額の制裁金を科される状況になっている。「個人データはタダである」という認識は過去のものであり、米国においても、カリフォルニア州では連邦法に先駆けて「消費者プライバシー法（CCPA：California Consumer Privacy Act）」が 2020 年 1 月 1 日から施行され、企業は個人データ保護の安全管理措置のコストに直面している。日本でも、

個人情報保護法の改正が進められており、個人データ保護の強化は世界的潮流であることは間違いない。

日本政府はまた、「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ー、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。多国籍企業は、DFFT 構想を含めた世界レベルでの個人情報保護ルール・メイキングの現状を踏まえ、サプライチェーンをマネジメントする必要がある。

企業が人権を尊重し個人データを保護することは、企業による持続可能な開発目標（SDGs）への貢献にもつながる。COVID-19 対応により、多国籍企業は、ESG の S 課題における人権保護の重要性を再認識し、サプライチェーン上での個人データ保護に関して具体的な行動を推進する形になっているとも言える。COVID-19 対応を契機として、広範なサプライチェーン上での個人データ保護と責任ある企業行動が、一層求められていくと思われる。