EU一般データ保護規則における クレジットカード情報の取扱い

石井夏生利
筑波大学図書館情報メディア系准教授

要 旨

本稿では、2018年5月25日に適用が開始された欧州連合（EU）の一般データ保護規則（GDPR）について、クレジットカード情報の取扱いに与える影響を整理し、日本の個人情報保護法の今後に向けた示唆を論じる。

国際ブランドのクレジットカードは、世界中の加盟店で利用することができるため、クレジットカード事業者にはGDPRが適用されると解するべきである。

GDPRを適用する際には、「同意」と「契約」の解釈に留意する必要がある。GDPRの同意は、「自由になされた、特定の、情報を提供された」ことを要件とし、同意と契約を混同することは認められていない。二段階の同意確認が明示的同意の有効性を担保する。契約締結・履行の「必要性」は厳格に解釈され、効率性向上のみではその要件を満たさない。

クレジットカード事業と関係の深いプロファイリングについては、特に、データ主体に対する透明性の保障が重視されている。

日本の個人情報保護法を論じる上では、特に、プロファイリングに関する規定の導入是非が論点となる。導入の手法には様々なものがあるが、本質的に、国内法によってプロファイリングを規律する必要性があるのか、という基本から議論を行う必要がある。

【目次】

Ⅰ．はじめに
Ⅱ．クレジットカード事業との関係で問題となり得るGDPRの規定
Ⅲ．欧州データ保護会議の指針
Ⅳ．訪問調査の結果
Ⅴ．検討

Ⅰ．はじめに

本稿では、2018年5月25日に適用が開始された欧州連合（European Union, EU）の一般データ保護規則（General Data Protection Regulation, GDPR）[1]について、クレジットカード情報の取扱いに与える影響を整理し、日本の個人情報保護法[2]の次期改正に向けた示唆を論じる

ことを目的とする。日本国内で活動する事業者は、日本の個人情報保護法を遵守することは当然ながら、域外適用規定の条件を満たすとGDPRの適用を受けることとなる。国際ブランドのクレジットカードは、世界中の加盟店で利用することができるため、EU市民に対するサービス展開では、GDPRを遵守することが求められる。また、日本の個人情報保護法は、いわゆる「十分性」認定との関係で、GDPRとの差分が意識されてきた。同法は施行後3年毎に見直される予定であることから（個人情報の保護に関する法律附則第12条3項）、GDPRの日本法に与える影響も注視しなければならない。

そこで、本稿では、主にクレジットカード事業との関係で問題となり得る規定を中心に取り上げ、規定の内容及び解釈を整理した上で、2018年2月に実施したブリュッセル（ベルギー）及びパリ（フランス）での訪問調査結果をまとめることを通じて、クレジットカード事業者が実施すべき情報の適正な取扱いと、個人情報保護法への今後の示唆を論じる。

Ⅱ．クレジットカード事業との関係で問題となり得るGDPRの規定

1. 域外適用（第3条）

第3条は、「地理的範囲」を定めている。特に2項は、第三国の組織や事業者に適用される規定であり、重要性がある。

「1　本規則は、取扱いがEU内で行われるか否かにかかわらず、EU内で管理者又は取扱者の事業所が活動を行う状況での個人データの取扱いに適用される。
2　本規則は、次に掲げる取扱行為に関連する場合、EU内で設立されていない管理者又は取扱者による、EU内にいるデータ主体の個人データの取扱いに適用される：
(a) データ主体に支払いが要求されるか否かにかかわらず、EU内の当該データ主体へ商品若しくはサービスを提供する場合；又は、
(b) EU内でその活動が行われる限りにおいて、彼らの活動を監視する場合。
3　略」

2項（a）号について、適用の有無を決するためには、管理者又は取扱者が、EU内の1つ以上の加盟国のデータ主体に対し、明らかにサービスを提供しようとしているか否かを確認すべきである。管理者、取扱者又は媒介者のウェブサイト、電子メールアドレス又は他の連絡先に単にアクセスできることや、管理者が設立された第三国で一般に用いられる言語を使用

しているにすぎない場合は、かかる意図は十分に確認できない。

一方で、1つ以上の加盟国内で一般に用いられる言語又は通貨を利用して、かかる言語での商品又はサービスを提供する可能性がある場合や、EU内の消費者又は利用者に言及するといった要素は、管理者による意図を明らかにすることができる（前文第（23）項）。この点について、本調査とは異なる機会にEU関係者に確認したところによると、英語圏である英国の場合は（離脱の問題はあるものの）、英語に加えてポンドでの取引を行えば適用され得るとのことであった。クレジットカード情報は世界的に流通するため、欧州市民に向けたサービスの場面では、2項（a）号に基づきGDPRが適用され、その遵守が求められる。

2. 適法な取扱い（第5条、第6条）

第5条1項（a）号は、「個人データの取扱いに関する諸原則」のうち、データ主体に関して、適法、公正、かつ透明性のある態様において取り扱われることを求めている（「適法性、公正性及び透明性」）。

第6条は「取扱いの適法性」を定めており、1項は、第5条1項（a）号の「適法性」を満たすための要件を明らかにしている。

「1　取扱いは、少なくとも次に掲げる項目の1つが適用される場合に限り、そしてその範囲においてのみ、適法に取り扱われるものとする：
(a) データ主体が、1つ以上の特定の目的のために自己の個人データを取り扱うことに同意を与えた場合；
(b) データ主体が当事者である契約を履行するため、又は、契約締結前にデータ主体の要請に基づく措置を講じるために、取扱いが必要である場合；
(c) 管理者が服する法的義務を遵守するために取扱いが必要である場合；
(d) データ主体又は他の自然人の重大な利益を保護するために取扱いが必要である場合；
(e) 公の利益、又は、管理者に付与された公的権限を行使する際に実施される業務を遂行するために取扱いが必要である場合；
(f) 管理者又は第三者によって追求される適法な利益のために取扱いが必要である場合。ただし、とりわけ、データ主体が児童である場合に、個人データ保護を求めるデータ主体の利益又は基本的権利及び自由が当該利益に優越する場合はこの限りでない。(f) 号前段は、公的機関が職務を遂行する際に実施する取扱いには適用されない。」

前文では、不正防止の場合に、管理者の適法な利益が認められることが示されている（第47項）。

3. 同意（第4条、第7条）

「データ主体の同意」は、「自由になされた、特定の、情報を提供された、かつ、不明瞭ではないデータ主体の意思表示であって、本人が、言明又は明らかに積極的な行動のいずれかによって、自己に関する個人データが取り扱われることへの同意を表明するものをいう」（第4条11項）。

同意には、電子的手段を含む、文書による表明や、口頭での表明などの方法があり、前文では次のように説明されている。

インターネット・ウェブサイトを訪問したときに同意する旨についてボックスにチェックを入れることや、情報社会サービス[3]の技術的設定を選択すること、その他、自己の個人データに関して（管理者又は取扱者から）提案された取扱いに、明確にデータ主体の受諾を示す表明又は行動を含む。そのため、黙っていること、事前にチェックされたボックス又は何もしないことは同意を構成しない（前文第（32）項）。

同意の関連では、GDPR第7条「同意の条件」が重要である。

「1　取扱いが同意に基づく場合、管理者は、データ主体が自身の個人データの取扱いに対して同意したことを証明できなければならない。
2　データ主体の同意が他の事項にも関わる書面において与えられている場合には、その同意の要請は、明瞭かつ平易な文言を用いて、理解しやすくかつ容易にアクセスし得る形で、かかる他の事項と明らかに区別できる態様によって示されなければならない。本規則違反を構成するあらゆる宣言は拘束力がないものとする。
3　データ主体は、いつでも同意を撤回する権利を有する。同意の撤回は、撤回前の同意に基づく取扱いの適法性には影響を与えない。同意付与に先立ち、データ主体はその旨を通知されなければならない。同意付与と同じく同意撤回は容易でなければならない。
4　同意が自由になされているか否かを評価する際、特に、サービス提供を含め、契約の履行が当該契約の履行に必要のない個人データの取扱いに対する同意を条件としているか否かに最大限の考慮を払わなければならない。」

4. 透明性（第12条～第14条）

全体を通じて、GDPRは、透明性を重視している点が重要である。

第12条「データ主体が権利を行使するための情報通知及び手続の透明性」は、管理者に対し、データ主体への情報提供を義務付けている。

管理者は、個人データの取扱いについて、データ主体に対し、特に児童に向けられたあら

ゆる情報に関しては、明瞭かつ平易な文言を用いた、簡潔で、透明で、理解しやすくかつ容易にアクセスし得る形態で、第13条（データ主体から個人データを収集した場合に提供すべき情報）及び第14条（データ主体から個人データを取得しなかった場合に提供すべき情報）に定める情報、並びに、第15条から第22条（アクセス権、訂正権、消去権（「忘れられる権利」）、取扱制限への権利、個人データの訂正等に関する通知義務、データ・ポータビリティの権利、異議申立権、プロファイリングを含む自動処理による個人に関する決定）及び第34条（データ主体への個人データ侵害の連絡）に基づく通知を提供するための適切な措置を講じなければならない。その情報は、電子的手段を含め、書面又は他の手段により提供されなければならない。データ主体の身元を証明できるときには、その求めに応じて情報を口頭で提供することができる（第12条1項）。

管理者は、第15条から第22条に基づくデータ主体の権利行使を容易にしなければならない（第12条2項）。管理者は、データ主体に対し、過度に遅滞することなく、また、請求を受領してから1ヶ月以内に、これらの権利行使を受けて取った行動を伝えなければならない（第12条3項）。上記の情報提供ないし通知、及び、管理者の行為は無料で行われる（第12条5項）。

第13条は、「データ主体から個人データを収集した場合に提供すべき情報」を定めている。データ主体に関する個人データがデータ主体から収集される場合、管理者は、個人データ取得の際に、データ主体に対し、(a) 管理者又は代理人の身元及び連絡先、(b) データ保護責任者の連絡先、(c) 予定する個人データの取扱目的、取扱いの法的根拠、(d) 個人データの取扱いが第6条1項 (f) 号に基づく場合、管理者又は第三者が追求する適法な利益、(e) 個人データの受領者又はその種類、(f) 管理者が個人データを第三国若しくは国際機関に移転する意図を有している事実、及び、欧州委員会による十分性認定の存否に関する事実、又は、第46条（適切な安全保護措置による移転）若しくは第47条（拘束的企業準則）、若しくは第49条1項後段（特定の状況による例外）に定める個人データ移転の場合に、妥当な若しくは適切な保護措置、及び、それらの写しを取得する方法等に関するすべての情報をデータ主体に提供しなければならない（第13条1項）。

管理者は、追加情報として、(a) 個人データの保存期間又は当該期間を決定するための基準、(b) 個人データへのアクセス及び訂正若しくは消去、データ主体に関する取扱いの制限、取扱いへの異議及びデータ・ポータビリティを管理者に求める権利の存在、(c) 個人データの取扱いが第6条1項 (a) 号又は第9条2項 (a) 号に基づく場合[4]に、いつでも同意を撤回する権利の存在、(d) 監督機関への不服申立権、(e) 個人データの提供が制定法ないしは契約上の義務であるか否か、契約締結の必要条件、データ主体への個人データ提供義務の有無、当

該データを提供しないことにより起こり得る結果、(f) プロファイリングを含む、自動処理による個人に関する決定の存在、その場合に、関連する論理についての意味ある情報、当該取扱いがデータ主体に与える結果の重大性及び予測される結果をデータ主体に提供しなければならない（第13条2項)。

第14条は、「データ主体から個人データを取得しなかった場合に提供すべき情報」を定めている。提供すべき情報は第13条とほぼ同内容ではあるが、第14条は、間接的に個人データを取得した場合であるため、追加情報として、個人データの情報源、及び適用可能な場合には、公にアクセスできる情報源からのものか否かを通知することとなっている(第14条2項(f)号)。自動処理による決定について、様々な情報源が用いられてきたために個人データの情報源をデータ主体に提供できない場合には、一般的な情報を提供すべきとされている（前文第(61）項)。

5. データ・ポータビリティ（第20条）

第20条「データ・ポータビリティの権利」は、1995年データ保護指令には存在しなかった新たな権利であり、クラウド・コンピューティングやソーシャル・ネットワーク・サービスの場面などで問題となり得る。この権利は、データ主体において、①管理者に提供した自己に関する個人データについて、構造化され、共通に利用され機械で判読可能な形式により受け取る権利、及び、②当該データを、個人データの提供を受けた管理者に妨害されることなく、他の管理者に移す権利である。この権利を行使できる場面は、(a) 取扱いが第6条1項 (a) 号若しくは第9条2項（a）号による同意に基づく場合又は第6条1項（b）号による契約に基づく場合であり、かつ、(b)取扱いが自動的手段により行われている場合である(第20条1項)。1項の権利を行使する際に、データ主体は、技術的に実行可能であれば、個人データをある管理者から他の管理者に直接に移行させる権利を有する（第20条2項)。

6. プロファイリング（第21条、第22条）

「プロファイリング」とは、「自然人に関するある一定の個人的な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し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的な取扱いをいう」(第4条4項)。

プロファイリングについては、異議申立権（第21条）のほか、プロファイリングに特化した規定として、第22条「プロファイリングを含む、自動処理による個人に関する決定」に関

する規定が置かれている。

第21条「異議申立権」は、データ主体に対し、プロファイリングを含め、第6条1項（e）号又は（f）号に基づく自己に関する個人データの取扱いに対して、何時でも異議を申し立てる権利を与えている。管理者は、データ主体の利益、権利及び自由に優越する取扱いのため、又は、法的主張の確立、行使又は防御のための説得力ある適法な根拠を証明しない限り、個人データを取り扱ってはならない（1項）。後段の証明責任は管理者側が負う（前文（69）項）。

第6条1項は適法な取扱いの条件を列挙しており、(e) 号は、公の利益、又は、管理者が公的権限を行使する場合の取扱い、(f) 号は、管理者又は第三者によって追求される適法な利益のために取扱いが必要である場合である。ダイレクト・マーケティング目的のための個人データの取扱いは、適法な利益のために行うものとみなすことができるとされている（前文(47)項）。

しかし、同条は、ダイレクト・マーケティングのための取扱いに、より厳格な定めを置いている。個人データがかかる目的のために取り扱われる場合、データ主体は、それに関するプロファイリングを含め、当該マーケティングのための自己に関する個人データの取扱いに対し、何時でも異議を申し立てる権利を有する（2項）。この場合、ダイレクト・マーケティング目的のための取扱いは認められない（3項）。1項及び2項に定める権利は、明示的にデータ主体の注意を引く形で、明確に、かつ他の通知とは分離して示されなければならない（4項）。データ主体は、情報社会サービスを利用する状況では、自動的手段を用いて異議申立権を行使することができる（5項）。データ主体は、公益のために取扱いが必要とされる場合を除き、個人データが第89条1項により科学的若しくは歴史的研究目的又は統計目的のために取り扱われる場合にも異議申立権を有する（6項）。

第22条の概要は次の通りである。

まず、データ主体に対し、プロファイリングを含め、自己に関する法的効果をもたらすか、又は、それに類する重大な影響を自己にもたらす、自動的手段による取扱いのみに基づく決定に服さない権利を有している（第22条1項）。この権利は、決定が、（a）データ主体とデータ管理者間の契約締結又は履行に必要である、（b）管理者が服するEU法又は加盟国法によって認められており、また、それが、データ主体の権利及び自由並びに適法な利益を保護するために適切な措置を定めている、（c）データ主体の明確な同意に基づく場合のいずれかに該当するときには適用されない（第22条2項）。

第22条2項に規定されている例外の（a）号及び（c）号に該当する場合、データ管理者は、データ主体の権利及び自由並びに適法な利益を保護するための適切な措置を実施しなければならず、少なくともそれには、管理者側で人を介在させる権利、データ主体が自己の意見を表明する権利、及び決定に異議を唱える権利が含まれる（第22条3項）。

第22条2項の例外に該当する決定は、第9条1項に定める特別な種類の個人データ（いわゆるセンシティブデータ）に基づいてはならない。ただし、第9条2項（a）号の「データ主体が明示的な同意を与えた場合」又は（g）号の「EU法又は加盟国法に基づき、重要な公益を理由とする場合」が適用され、かつ、データ主体の権利及び自由並びに適法な利益を保護するための適切な措置が講じられている場合は、この限りでない（第22条4項）。

第22条の解釈に関しては、前文の中で次のような補足説明がなされている。

第22条1項の「法的効果をもたらすか、又は、それに類する重大な影響」には、オンライン上の貸付申請の自動的拒否又は人間を介在させない採用活動などが該当する。かかる取扱いには「プロファイリング」が含まれる。第22条2項（b）号の「管理者が服するEU法又は加盟国法」には、EU諸機関又は国内の監視機関の規則、標準及び勧告に従って実施される、詐欺及び脱税の監視及び予防目的などが含まれる。

第22条3項との関係では、当該評価後に達した決定の説明を受ける権利も含まれる。ただし、3項に定める措置は、児童と関係するものであってはならない。

データ主体に関して、公正かつ透明な個人データの取扱いを保障するため、個人データが取り扱われる具体的状況及び文脈を考慮に入れ、管理者は、プロファイリングに対する適切な数学的又は統計的手順を用いるべきであり、適切な技術的及び組織的措置を実施すべきである。それは、個人データが不正確な結果となる要素を正し、間違いのリスクを軽減し、データ主体の利益及び権利に関わる潜在的リスクを考慮に入れる方法で、かつ、人種又は民族的出自、政治的意見、宗教又は信念、労働組合への加盟、遺伝若しくは健康状態又は性的嗜好に基づく自然人への差別的効果を防ぐ方法で個人データを確実に保護するためのものである。特別な種類の個人データ（いわゆるセンシティブデータ）に基づく自動処理による決定及びプロファイリングは、特別な条件下でのみ認められるべきである（以上、前文第（71）項）。

7. 共同管理者（第26条）

第26条は、「共同管理者」の定めを置いている。

二者以上の管理者が共同で個人データの取扱いの目的及び手段を決定する場合、かかる管理者は共同管理者となる。彼らは、データ主体の権利行使、並びに、第13条（データ主体から個人データを収集した場合に提供すべき情報）及び第14条（データ主体から個人データを取得しなかった場合に提供すべき情報）に定める情報提供義務について、相互に協定を締結する方法により、透明な態様で、義務遵守のための各責任を決めなければならない。

ただし、管理者の服するEU法又は加盟国法の定めがある場合はこの限りでない。協定は、データ主体のための連絡先を指定することができる（第26条1項）。1項の協定は、データ主

体との関係で、共同管理者の各役割及び関係を適切に反映しなければならず、協定の骨子はデータ主体が入手できなければならない（第26条2項）。データ主体は、1項の協定にかかわらず、各管理者に対して自己の権利を行使することができる（第26条3項）。

管理者及び取扱者の責任は、監督機関による監視及び措置との関係においても明確な割当てを必要とする（前文第（79）項）。

8. 取扱者[5]（第28条）

第28条は「取扱者」を定めている。1項の定めは次の通りである。

「1　管理者の代わりに取扱いが行われる場合、その管理者は、取扱いが本規則の義務を満たし、データ主体の権利を確実に保護する方法で、適切な技術的及び組織的措置を実施することを十分に保障する取扱者のみを用いなければならない。」

取扱者の選任に際しては、特に、専門知識、信頼性及びリソースが考慮される（前文第81項）。

第28条2項は、再委託の制限規定に相当する規定である。

「2　取扱者は、個別的又は一般的な文書による事前許可を管理者から得ることなく、他の取扱者に従事させてはならない。文書による一般的な許可の場合、取扱者は、他の取扱者の追加又は交替に関して、予定されるあらゆる変更を管理者に通知しなければならず、それによって管理者に当該変更への異議を述べる機会を提供する。」

第28条3項は、EU法若しくは加盟国法に基づく契約又は他の法律行為により、管理者との関係で取扱者を拘束するよう義務づけている。この契約及び法律行為には、個人データの取扱いの対象事項及び期間、取扱いの性質及び目的、個人データの類型及びデータ主体の種類、並びに、管理者の義務及び権利を定めることとされているが、同項は、さらに、8項目の事項を定めるよう義務づけている。具体的には、(a) 取扱者が服するEU法又は加盟国法が義務づける場合を除き、第三国又は国際機関への個人データの移転を含め、管理者の文書による指示のみに基づき個人データを取り扱うこと、(b) 守秘義務、(c) 第32条（(個人データの）取扱いの安全性）に基づき義務づけられるすべての措置を講じること、(d) 2項及び4項に定める条件の遵守、(e) データ主体の権利行使に対応するための、適切な技術的及び組織的措置による管理者の支援、(f) 第32条から第36条（(個人データの）取扱いの安全性、監督機関への個人データ侵害通知、データ主体への個人データ侵害の連絡、データ保護影響評価、事前協議）の義務を遵守するための管理者の支援、(g) サービスの提供終了後にすべての個

人データを抹消し又は管理者へ返還すること、及び、EU法又は加盟国法が定める場合を除き、現存の写しを消去すること、(h) 本条の遵守を証明するために必要な全情報を管理者が入手できるようにすること、また、監査人の点検・監査を可能にし、それに貢献することである。(h) 号前段に関しては、取扱者において、指示が本規則又はEU若しくは加盟国のデータ保護規定を侵害するとの意見を有する場合には、直ちに管理者に通知しなければならない。

9. 第三国移転（第44条～第50条）

第5章「第三国又は国際機関への個人データの移転」は、第44条から第50条で構成される。国際データ移転の全体的な構成として、GDPRでは、データ移転を行うための三段階の規律が設けられている。

第1に、原則として、欧州委員会が十分な保護レベルを認定することにより、第三国等へのデータ移転が認められる（第45条）。第2に、欧州委員会が十分性の認定を下していない場合には、適切な安全保護措置を講じることにより、第三国等へのデータ移転が認められる（第46条）。適切な安全保護措置には、拘束的企業準則（Binding Corporate Rules, BCRs）、欧州委員会が採択した標準データ保護条項（標準契約条項、Standard Contract Clauses, SCCs）、行動規範や認証制度が含まれる。第3に、欧州委員会の十分性認定が下されておらず、適切な安全保護手段がない場合には、第49条の「特定の状況による特例」に基づき、第三国等へのデータ移転が認められる。第49条1項は、(a) 十分性認定及び適切な安全措置がないことにより、データ主体が当該移転により被る可能性のあるリスクの通知を受けた後、提案された移転に明示的な同意を与えた場合、(b) 移転が、データ主体と管理者間における契約履行、又は、データ主体の請求により講じられる契約前措置の実施のために、移転が必要な場合、(c) 管理者及び他の自然人又は法人の間で、データ主体の利益において結ばれる、契約の締結又は履行のために、移転が必要な場合などにおいて、個別のデータ移転を認めている。

Ⅲ．欧州データ保護会議の指針

1. 指針の公表状況

GDPRは、長大な上に入り組んだ法であるため、前文及び本文のみでその全容を把握することはできない。そこで、GDPRが適用開始される2018年5月25日までの間は、1995年データ保護法に基づく「個人データの取扱いに係る個人の保護に関する作業部会」（以下「第29条作業部会」という。）[6]が、同日以後は欧州データ保護会議（European Data Protection Board）が、GDPRの解釈に関する指針を公表してきた。2018年7月19日現在で、採択又は承

認されている指針は、次の通りである[7]。

これらのうち、2018年の訪問調査結果でも頻繁に登場した「同意」と「プロファイリング」に関する指針について、それぞれの概要を整理する。

【欧州データ保護会議により採択された指針】

・「規則2016/679第42条及び第43条に基づく認証及び認証基準の特定に関する1/2018指針」2018年5月25日採択
「規則2016/679第49条の例外に関する2/2018指針」 2018年5月25日採択

【欧州データ保護会議が2018年5月25日に承認した第29条作業部会の指針】

・「規則2016/679に基づく個人データ侵害通知に関する指針」（WP250 rev.01） 2017年10月3日採択、2018年2月6日最終改正及び採択
・「データ・ポータビリティ権に関する指針」（WP242 rev.01） 2016年12月13日採択、2017年4月5日最終改正及び採択
・「データ保護責任者（「DPOs」）に関する指針」（WP243 rev.01） 2016年12月13日採択、2017年4月5日最終改正及び採択
・「規則2016/679の目的のための、データ保護影響評価（DPIA）、及び、取扱いが「高いリスクをもたらす可能性」を有するか否かを決定することに関する指針」（WP248 rev.01） 2017年4月4日採択、2017年10月4日最終改正及び採択
・「規則2016/679の目的のための、自動処理による個人に関する決定及びプロファイリングに関する指針」（WP251 rev.01） 2017年10月3日採択、2018年2月6日最終改正及び採択
・「管理者又は取扱者の主たる監督機関を特定するための指針」（WP244 rev.01） 2016年12月13日採択、2017年4月5日最終改正及び採択
・「規則2016/679に基づく同意に関する指針」（WP259 rev.01） 2017年11月28日採択、2018年4月10日最終改正及び採択
・「規則2016/679に基づく透明性に関する指針」（WP260 rev.01） 2017年11月29日採択、2018年4月11日最終改正及び採択

【その他の第29条作業部会指針】

・「規則2016/679の目的のための、制裁金の適用及び設定に関する指針」（WP253） 2017年10月3日採択

2. 同意に関する第29条作業部会指針

「規則2016/679に基づく同意についての指針」（2017年11月28日採択、2018年4月10日最終改正及び採択、WP259 rev.01）[8]は、有効な同意を得るための解釈を示している。構成は、「1. 導入」、「2. GDPR第4条11項に基づく同意」、「3. 有効な同意の要件」、「4. 明示的な同意の取得」、「5. 有効な同意を取得するための追加的条件」、「6. 同意とGDPR第6条に基づく他の適法な根拠との相互関係」、「7. GDPRにおける特定の懸念分野」、「8. 95/46/ECに基づき取得された同意」である。

なかでも、「3. 有効な同意の要件」及び「4. 明示的な同意の取得」が重要である。加えて、「5. 有効な同意を取得するための追加的条件」、「6. 同意とGDPR第6条に基づく他の適法な根拠との相互関係」についても、必要な部分を抜粋要約する。

「3. 有効な同意の要件」

「3. 1　自由」

「自由」は、データ主体の真の選択及びコントロールを意味する。原則として、データ主体が真の選択を持たない場合、同意を強制されたと感じる場合、同意をしなければ否定的な結果を甘受することとなる場合には、同意は有効ではない。同意が交渉の余地のない取引条件の一部として拘束されている場合、データ主体が不利益を被ることなく同意を拒否し又は撤回することのできない場合には、自由とはいえない。

「3. 1. 1　力の不均衡」

前文第（43）項は、公的機関と個人の間には明らかな力の不均衡が存在することが多いため、同意に依拠できる可能性は低いと述べている。力の不均衡は、雇用環境においても生じる。従業員が、同意に何らのプレッシャーを感じることなく、職場のカメラ監視のような監視システムの作動、又は評価書類への記入等、従業員が雇用主から同意の要請を受けて自由に応対できる可能性は低い。雇用主と従業員の関係という性質から、職場でのデータの取扱いの多くは、第6条1項の同意に依拠することはできない。しかし、同意があろうがなかろうが不利な結果をもたらさないような、例外的な場合には、同意に依拠することもできる。

力関係の不均衡は他の場面でも生じる。同意は、データ主体が真の選択を行うことができ、同意をしなくとも、詐欺、脅迫、強制又は重大な負の結果（例えば相当な追加費用）のリスクを生じさせない場合にのみ有効である。

「3. 1. 2　条件」

同意の任意性を評価する上で、第7条4項は重要な役割を果たしている。同条項は、個人情報の取扱目的が、当該個人情報を必要としないサービス契約条項に偽装されたり、それに縛られたりしないよう求めている。GDPRは、同意を求められる個人データの取扱いが、直接又は間接の反対給付とならないよう保障している。個人データの適法な取扱いのための2つの適法な根拠、すなわち同意と契約は、混同されたり曖昧にされてはならない。

拘束性を評価するために、契約の範囲及び契約履行に必要なデータを確定することが重要である。第29条作業部会の意見06/2014[9]に従い、「契約履行のために必要」は、厳格に解釈する必要がある。取扱いは、各データ主体との契約を履行するために必要でなければならず、例えば、オンラインで購入した商品を配達するためにデータ主体の住所を取り扱う場合や、支払いを容易にするためにクレジットカード情報を取り扱う場合がある。雇用の場面では、給与を支払うために給与情報及び口座情報を取り扱う場合に許される。データの取扱いと契約履行の目的との間に、直接的かつ客観的な関連性が必要である。

例えば、銀行が、顧客に対し、第三者がマーケティングを行う目的で支払明細を扱うための同意を求めたとする。この取扱いは、顧客との契約履行や通常の銀行口座サービスの提供のためには必要でない。顧客がこの取扱目的への同意を拒否した場合に、銀行サービスの拒否や銀行口座の閉鎖、又は手数料の増加につながる場合には、同意は自由に与えられ、又は、撤回できるものとはいえない。

第7条4項「同意が自由になされているか否かを評価する際、特に、サービス提供を含め、契約の履行が当該契約の履行に必要のない個人データの取扱いに対する同意を条件としているか否かに最大限の考慮を払わなければならない。」の「最大限の考慮」（utmost account）は、契約/サービスがそれに結びついた個人データの取扱いへの同意を求める場合に、管理者に特に注意を払うよう示唆している。同条項の証明責任は管理者にあるが、同条が適用される場合には、同意が自由に与えられたことの証明が一層難しくなる。

管理者が、追加目的のための個人データの利用への同意を含むサービスと、それと同等のサービスで、データ利用への同意を含まないサービスを提供していたとする。この場合、追加的なデータ利用への同意がなくても契約の締結又は履行を行うことができる限りにおいて、条件付きのサービスには該当しない。

「3. 1. 3　粒度」

同意の粒度について、サービスは、複数の取扱いを伴う可能性がある。その場合、データ主体は、複数の取扱目的へ同意するよりも、どの目的に同意しているかを自由に選択できる

ようにすべきである。

個別に同意を取ることが適切であるにもかかわらず、データ主体による個別同意を許さない場合には、同意は自由に与えられたとは推定されない（前文第（43）項）。同意は、同じ目的のために実施される全ての取扱い行為を含むべきである。取扱いが複数目的を有する場合、同意はそれらの全てに与えられるべきである（前文第（32）項）。

管理者が取扱いのためのいくつかの目的を融合し、各目的への個別同意を求めようとしない場合、任意性が欠如する。

例えば、同じ同意要請の中で、小売業者が顧客に電子メールによるマーケティングを行うためにデータを利用することと、グループ内での他の事業者とも彼らの情報を共有することへの同意を求めたとする。同意は細分化されておらず、別目的のための別の同意がないため、同意は有効ではない。

「3. 1. 4　損害」

管理者は、損害なく同意が撤回できることを証明しなければならず（前文第（42）項）、例えば、管理者は、同意を撤回しても何らの追加費用を要さず、同意撤回に対する明らかな不利益がないことを証明する必要がある。他の損害には、データ主体が同意しない場合の詐欺、脅迫、強制又は重大な不利益結果がある。

「3. 2　特定の」

第6条1項（a）号「データ主体が、一つ以上の特定の目的のために自己の個人データを取り扱うことに同意を与えた場合」のうち、「特定の」とは、「1つ又はそれ以上の」目的との関係で、それぞれに同意を与えることをいう。要約すると、管理者は、「特定の」要素を遵守するために、（i）二次利用に対する保護措置としての目的の特定、（ii）同意要請の粒度、（iii）他の事項に関する情報とデータ取扱行為に対する同意取得に関する情報を明確に区分することが求められる。同条項に依拠する場合には、データ主体は、常に、特定の取扱目的に対して同意しなければならない。管理者が新たな目的でデータを取り扱う場合は、新たに同意を取得する必要がある。

「3. 3　情報を与えられた」

同意を取得するに先立って、データ主体に情報を提供することは、データ主体において、情報を与えられた上での決定を行い、何に同意しているかを理解し、例えば自己の同意を撤回する権利などを行使できるようにするために重要である。

「3. 3. 1 「情報を与えられた」同意のための、内容に関する最低限の要件」

同意を取得するに先立ってデータ主体に提供すべき情報には、最低限、次のものが含まれる。

(i) 管理者の情報
(ii) 同意が求められる各取扱行為の目的
(iii) いかなる（種類の）データが収集され利用されるか
(iv) 同意撤回権の存在
(v) 第22条2項（c）号に基づく自動処理決定のためのデータ利用に関する情報
(vi) 十分性認定及び第46条に定める適切な保護措置が存在しないことによる、データ移転に関する可能性のあるリスク

(i) 及び (iii) について、複数の（共同）管理者に依拠する場合には、これらの組織は全て列挙されるべきである。取扱者は同意要件の一部として列挙される必要はない。しかし、管理者は、第13条及び第14条に従い、受領者又は受領者の種類に関する完全なリストを提供する必要があり、それには取扱者が含まれる。

「3. 3. 2 同意の提供方法」

同意の提供方法には、文書、口頭での陳述、音声又は動画メッセージ等、様々な方法によることが可能であるが、明白で分かりやすい言語を用いることを保障し、法律家ではなく通常人にとって容易に理解できるメッセージであるべきである。法理用語が満載の、冗長で読めないプライバシーポリシーを用いてはならない。同意は明白で、他の事項と区別しなければならず、一般の利用条件の中に同意を紛れ込ませてはならない。

「3. 4 不明瞭ではない意思表示」

同意は、データ主体の声明又は明白な積極的行動によることを求めている。

「明白な積極的行動」とは、特定の取扱いへの意図的な同意を取らなければならないことを意味する。「文書による声明」が最も基準を満たす文意的な方法であるが、現実的でない場合がある。文書による声明は様々な形態及び規模で行うことができる。

現行の契約法を損なうことなく、同意は記録された口頭での声明を通じて行うことができるが、データ主体が同意を表明するに先立ち、情報を入手可能であることに十分留意しなければならない。

管理者は、契約への同意や、一般的なサービス利用条件の受諾と同じ行為を通じて同意を取得できないことを認識しなければならない。一般的な利用条件への包括的な受諾は、個人データの利用に同意するための明白な積極的行動とみなすことはできない。GDPRは、事前

にチェックされたボックスもオプトアウトも認めていない。

例えば、スクリーンのバーのスワイプ、カメラの前で手を振る、スマートフォンを時計周りにまわすか八の字に動かす行為は、明白な情報が与えられている限りでは、同意を示す選択肢となり得る。当該行動が特定の要請への同意を明らかに意味している（例えば、このバーを左にスワイプすると、Yの目的のためのXの取扱いに同意したことになる。確認のためにもう一度行って下さい等）。他方、同意への宣言を含む利用条件を通じて、下にスクロールするかスワイプする行為（スクロールすることで同意を構成することをデータ主体に警告する記述をスクリーン上に示す場合）は、明白かつ積極的行動にはならない。大量の文書をデータ主体が急いでスクロールし、警告を見失う可能性があるため、その行動は十分に明白性を持たないからである。データ主体はクリック疲れを起こしているかもしれず、同意の質問をもはや読まない結果をもたらす。

いずれにせよ、同意は常に、管理者が、同意が求められる個人データを取り扱うに先立って取得されるべきである。GDPRは、第4条11項の文言では述べていないが、同意は取扱行為に先立って行わなければならず、第6条1項の冒頭及び（a）号の「与えた」という文言がこの解釈を支援する。

「4. 明示的な同意の取得」

明示的同意は重大なデータ保護のリスクが生じる場合、すなわち、第9条（特別な種類の個人データの取扱い）、第22条（プロファイリングを含む、自動処理による個人に関する決定）、第49条（特定の状況による例外）の場合に求められる。

「明示的」とは、データ主体が同意の明示的な表明を行うことをいう。文書による声明のほか、文書による声明にデータ主体が署名する場合が当てはまる。

デジタル又はオンラインの文脈では、電子的書式に記入する方法、電子メールを送る方法、データ主体の署名を載せたスキャン文書をアップロードする方法、又は、電子署名を行う方法が該当する。理論的には、口頭での声明も明示的同意になり得るが、声明を記録する場合は有効な明示的同意の全条件を証明することは難しいかもしれない。

データ管理者は、文章が明らかに同意を示している場合、例えば、「私は、自己のデータが取り扱われることをここに同意します」などの場合には、「はい」と「いいえ」のチェックボックスを含む明示的な同意画面を提供することにより、ウェブサイト訪問者から明示的同意を得ることもできる。「私のデータが取り扱われるであろうことは私にとって自明です」という例は認められない。

二段階の同意確認が明示的同意を有効にする方法である。例えば、データ主体が管理者か

ら医療データを含む記録の取扱いを予定していることを通知する電子メールを受け取り、管理者はそのメールの中で特定の目的のための特定の情報群の利用への同意を求める旨を説明する。データ主体がこのデータの利用に同意する場合、管理者は「同意します」との声明を含む電子メールの返信を送るよう依頼する。その返信が送られた後に、同意を確認するために、データ主体がクリックを要する確認リンクを受け取るか、SMSメッセージで確認コードを受け取るという方法である。

「5. 有効な同意を取得するための追加的条件」

「5. 1　同意の証明」

GDPRは管理者の証明方法を正確には述べていないが、問題のデータの取扱行為が続く限り、同意の証明義務は存在する。

GDPRは、同意の持続期間についての期間制限は設けていない。それは状況によるものであって、元々の同意の範囲やデータ主体の期待による。取扱作業が変更されたり、相当程度進展した場合には、同意はもはや有効ではない。

第29条作業部会は、同意が適切な間隔を持って更新されるべきことを最良の実務として推奨する。全ての情報を再提供することで、データ主体は自己のデータの利用方法や権利行使方法について十分に情報提供を受け続けることを保障される。

「5. 2　同意の撤回」

同意の撤回について、第7条3項は、「データ主体は、いつでも同意を撤回する権利を有する。同意の撤回は、撤回前の同意に基づく取扱いの適法性には影響を与えない。同意付与に先立ち、データ主体はその旨を通知しなければならない。同意付与と同じく同意撤回は容易でなければならない。」と定めている。同条項は、同意の付与と撤回を同じ行為を通じて行わなければならないとは述べていない。しかし、同意が電子的手段で1回のマウスのクリックやスワイプ、キーストロークのみで取得された場合には、データ主体は、同等に簡便な方法で同意を撤回できるようにしなければならない。同意がサービス特有のユーザーインターフェイス（例えば、ウェブサイト、アプリ、ログインアカウント、IoTデバイスのインターフェイス又は電子メール等）を通じて取得された場合には、データ主体は同じ電子的インターフェイスを通じて撤回できるべきである。なぜなら、同意を撤回するという理由のみで他のインターフェイスへ移転することは、不当な努力を伴うからである。さらに、データ主体は、損害なく同意を撤回できるべきであり、手数料は無料で、サービスレベルの低下があってはな

らない。例えば、オンラインチケットの購入時にワンクリックで同意したにもかかわらず、撤回の場合には営業時間内にコールセンターに連絡しなければならない場合には、第7条3項を遵守したことにならない。

原則として、同意が撤回された場合には、同意撤回前の適法な全ての取扱行為は適法性を維持するが、管理者は当該取扱行為を止めなければならない。他の適法な根拠がなければ、データは管理者によって削除されなければならない。

事業者は、データ主体が同意を撤回しても、契約履行に基づき取り扱っているデータを削除する必要はない。

データ主体が同意を撤回し、管理者がデータを利用し続けたい場合に、管理者は、黙って（撤回された）同意から他の適法な根拠に移動してはならない。さらに、取扱いの適法な根拠を変更する際は、データ主体に第13条（データ主体から個人データを収集した場合に提供すべき情報）及び第14条（データ主体から個人データを取得しなかった場合に提供すべき情報）に基づき通知を行わなければならない。

「6. 同意とGDPR第6条に基づく他の適法な根拠の相互関係」

第6条に基づく6つの適法な根拠は、目的特定との関係で、取扱いに先立って確定しなければならない。

管理者は、同意から他の適法な根拠に取り替えてはならない。例えば、同意の有効性に問題が生じた場合に、取扱いを正当化するために、適法な法的根拠を遡及的に利用することは認められていない。管理者は、個人データの取扱時に適法な根拠を開示するよう義務づけられることから、何が適法な根拠であるかをあらかじめ決定しておかなければならないからである。

3. プロファイリングに関する指針

「規則2016/679の目的のための、自動処理による個人に関する決定及びプロファイリングに関する指針」（2017年10月3日採択、2018年2月6日最終改正及び採択WP251）[10]は、プロファイリングに関する規定の解釈を公表している。

この指針は、「Ⅰ．導入」及び「Ⅱ．定義」に続き、「Ⅲ．プロファイリング及び自動的決定に関する一般的規定」、「Ⅳ．第22条に定める自動的決定に関する特別な規定」についての説明を加えた後、善良な実務に関する勧告等を別添に掲載している。本稿との関係で特筆すべき事項は、次の通りである。

「Ⅱ．定義」

プロファイリングは統計的推論を行う手続であり、その3つの要素として、自動的であること、個人データに関すること、個人的側面を評価することが挙げられる。第4条4項の定義は、自動的処理「のみ」というよりは、あらゆるプロファイリングに言及している。

自動的決定は、プロファイリングとは異なるが、部分的には重複する。自動的処理のみによる決定は、人の関与なく技術的手段によって決定する能力である。自動的決定はあらゆる種類のデータに基づき行うことができ、例えば、当該個人から直接に提供されるデータ（質問への回答など）、個人に関する観察データ（アプリを介して収集される位置データなど）、既に生成された個人のプロフィールなど、派生又は推測されたデータ（信用評価など）が含まれる。

自動的決定はプロファイリングがなくても行うことができ、プロファイリングは自動的決定がなくても生じ得る。しかし、プロファイリングと自動的決定は必ずしも分離されておらず、自動的手段のみによる決定プロセスとして始まったものが、データの利用方法によっては、プロファイリングに基づくものになり得る。

プロファイリングには、①一般的プロファイリング、②プロファイリングに基づく決定、③プロファイリングを含む自動的処理のみに基づく決定（第22条）の方法がある。特に、②と③の違いは、オンライン上のローン申請の場面で如実に表れる。具体的には、自動的手段のみにより生成されたプロフィールに基づきローンに同意するか否かを人が決定する場合は②に該当し、ローンに同意するか否かをアルゴリズムが決定し、その決定が意味ある人の介入なくして、個人に自動的に届けられる場合は③に該当する。

管理者は、全ての諸原則を満たし、取扱いの適法な根拠を有する限りにおいて、プロファイリングと自動的決定を行うことができる。追加的保護措置及び制限は、第22条1項の場合に適用される。

プロファイリングには、前記のとおり3種類存在するが、法的枠組みは、(1) プロファイリング及び自動的決定に関する一般的な法的枠組、(2) 第22条に定める自動処理のみによる決定の2種類に分けられる。

「Ⅲ．プロファイリング及び自動的決定に関する一般的規定」

プロファイリング及び自動的決定に関する一般的規定には、データ保護諸原則（第5条）、（個人データの）取扱いの適法性（第6条）、特別な種類のデータ（いわゆるセンシティブデータ）（第9条）、情報提供を受ける権利（第13条、第14条）、データ主体の権利（第15条以下）がある。これらのうち、不正防止やマネーロンダリングなどに関連して、プロファイリングを

実施する法的義務が生じ得る（第6条1項（c）号）。これらの中で特に留意すべき点は、以下の通りである。

適法、公正かつ透明な取扱い（第5条1項（a）号）について、プロファイリングの手順は、データ主体には見えないことが多い。それは、個人に関する派生又は推測データ―新たな個人データであって、データ主体自体から直接には提供されていないもの―を生成することによって機能する。個人の理解力には差があり、プロファイリング及び自動的決定手順に関する複雑な技術を理解することを困難と思うかもしれない。そこで、簡潔で、透明で、分かりやすく容易にアクセスできる情報を提供することが重要である（第12条～第14条）。

適法、公正かつ透明な取扱い（第5条1項（a）号）について、プロファイリングは、不公正で差別を生むかもしれない。例えば、人々が雇用や信用や保険の機会を得ることを拒否したり、彼らを過度に危険又は費用のかかる金融商品の標的にしたりする場合がある。例えば、データブローカーが、基礎データに関する消費者の承諾又は認識を得ることなく、プロフィールを金融機関に販売したとする。プロフィールは消費者をカテゴリに分類する（例えばタイトルを「田舎者で滅多に成功しない」、「民族的なセカンドシティの困窮者」、「厳しい始まり：若くて独身の親」）、又は、消費者の経済的脆弱性に着目し、彼らを「採点」する。金融機関は、これらの消費者に対して短期の小口ローン（payday loan）や、他に「従来型ではない」金融サービス（高コストのローンや他に金融上リスクのある商品）を提供する。このような場合は、第5条1項（a）号の要件を満たさない。

取扱いの適法性のうち、契約履行のための「必要性」（第6条1項（b）号）は狭義に解釈されなければならない。例えば、人為的ミスを減らす、顧客の不払いリスクを減らす、決定を短期化し、効率性を向上させるなどの考慮事項のみでは不十分とされている。

これは、取扱いのための第6条（1）項（b）号を満たさないプロファイリングの例である。

ユーザーは、オンライン小売業者からいくつかの商品を購入する。契約を履行するために、小売業者は、支払い目的で、利用者のクレジットカード情報、また、商品を配送するために、利用者の住所を取り扱わなければならない。彼らがウェブサイトへ訪問し、利用者の好みやライフスタイルの選択に関するプロフィールを作成することで、契約が履行されるわけではない。小さく印刷された契約書にプロファイリングが具体的に記載されていても、この事実のみでは契約履行に「必要」であることとはならない。

第6条（1）項（f）号の管理者又は第三者の適法な利益について、第29条作業部会の適法な利益に関する意見[11]は、マーケティング又は広告目的による侵害的なプロファイリングや追跡実務のための法的根拠として、管理者が適法な利益を用いる旨を正当化することは難しいことを示唆している。例えば、複数のウェブサイト、位置、装置、サービス又はデータ仲

介をまたいで個人を追跡することに関わる実務である。

第15条のアクセス権、第16条の訂正権、第17条の消去権は、入力データ（プロフィールを作成するために用いられた個人データ）と、出力データ（プロフィールそれ自体又は個人に割り当てられた「採点」）の双方に適用される。

第21条の異議申立権について、管理者側のやむにやまれぬ（compelling）適法な根拠と、データ主体の異議申立権の根拠を衡量する際には、単に適法な利益が存在する（第6条（1）項（f）号）ことでは足りず、「やむにやまれぬ」利益が優越しなければならない。

「Ⅳ．第22条に定める自動的決定に関する特別な規定」

専ら自動化された個人に関する決定には第22条が適用される。同条の要点は「自動的処理のみに基づく」、「法的効果」、「その人に対する類似の重大な影響」の3点である。同条を要約すると、（i）原則として、法的又はそれに類する重大な効果を有するプロファイリングを含む、完全に自動化された個人に関する決定の禁止、（ii）例外規定、（iii）データ主体の権利及び自由並びに法的利益を保護するための措置である。保護措置には、情報を受ける権利（第13条、第14条に規定する、関連する論理、データ主体に対する重大性及び想定される結果）、人の介入を得る権利及び決定に異議を述べる権利がある。

「自動的処理のみに基づく」とは、決定プロセスに人の介入が存在しないこという。「人の介入」を意味あるものにするためには、決定を変更する権限と能力のある者が実施し、全ての利用可能な入出力データを考慮に入れなければならない。

GDPRは、「法的」又は「類似の重大な」を定義していないが、「法的効果」とは、誰かの法的権利や地位に影響を与えるものをいう。例えば、契約のキャンセル、児童手当又は住宅手当など、法が付与する特定の社会福祉の資格を与えられ又は拒否される、入国又は市民権の拒否がある。「類似の重大な効果」とは、法的効果を生じなくとも、影響の点で同等又は類する重大な影響をもたらす場合をいう。データ主体への高いリスクをもたらす蓋然性のある取扱いについて、管理者は、データ保護影響評価（Data Protection Impact Assessment, DPIA）を実施しなければならない。

前文第（71）項は、「類似の重大な効果」に関する典型的な例として、オンラインクレジット申請の自動拒否や人の介入がないオンライン採用の実務を挙げている。「類似の重大な効果」は、注目に値するに足りる十分な重大性又は重要性を持たなければならない。いいかえると、決定は、当該個人の状況、行動又は選択に重大な影響を及ぼす、データ主体への長期的又は永続的な影響を有する、又は、極論としては、個人の排除又は差別につながるような可能性を必要とする。

貸付の資格（eligibility to credit）のような、人の経済状態に影響を与える決定、保健サービスに影響を与える決定、雇用機会を否定し又は極めて不利にする決定、教育機会に影響を与える決定などはこの類型に入り得るとしても、十分な重大性の基準を正確にはかることは困難である。

「類似の重大な効果」は、自動的決定に関わらない他者の行動によってももたらされる。例えば、クレジットカード会社が、消費者自身の支払い履歴ではなく、従来とは異なる信用基準、例えば、同じ店で購入する同じ地域に住む他の消費者の分析などに基づき、消費者のカードの限度額を引き下げるかもしれない。このことは、他者の行動に基づき誰かの機会が奪われることを意味し得る。他の場合には、これらの性質を利用することが、それがなければ拒否されていたであろう、従来の信用履歴がない者に、信用を拡大するという利点を与えるかもしれない。

第22条2項は、次に掲げる3つの場合に、1項の例外規定を定めている。

(a)　契約の履行や締結に必要な場合

(b)　管理者が服するEU法又は加盟国法によって認められており、また、それが、データ主体の権利及び自由並びに適法な利益を保護するために適切な措置を定めている場合

(c)　データ主体の明示的同意に基づく場合

（a）号の「契約の履行」について、必要性は狭く解釈すべきである。管理者は、よりプライバシーを侵害しない方法を採用できるか否かを考慮に入れ、このプロファイリングが必要であることを示さなければならない。より侵害的ではない手段で同じ目的を達成できる場合には、プロファイリングは「必要」ではない。

（b）号については、詐欺や脱税の防止等、前文第（71）項が定めを置いている。

（c）号の明示的同意について、GDPRは定義を置いていないが、同意は何かしらの他の積極的行動よりも明示的な声明によって特に確実にされなければならない。

第22条との関連で、データ主体は、第13条2項（f）号及び第14条（2）項（g）号[12]に基づき、情報提供を受ける権利を有する。第22条の潜在的リスクに照らし、管理者は、特に透明性の義務に留意すべきである。管理者が第22条1項に定める自動的決定を行う場合、データ主体に対し、この類の活動に従事していること、関連する論理についての意味ある情報、決定の重大性と想定される取扱結果を説明しなければならない。

「『関連する論理』についての意味ある情報」について、管理者は、決定の背景にある理屈又は決定に達する際に依拠した基準に関し、データ主体に伝えるための簡便な方法を見いだすべきであり、利用されるアルゴリズムの複雑な説明や全アルゴリズムの開示を必ずしも行わずに済むようにすべきである。ただし、提供される情報は、テータ主体にとって決定の理

由を理解できるものでなければならない。例えば、次のような例がある。

管理者は、信用評価を用いて個人のローン申請の拒否を行う。評価は信用情報機関から提供され、又は、管理者が保有する情報に基づいて直接に計算されてきたかもしれない。情報源にかかわらず(個人データがデータ主体から直接に収集されなかった場合に、第14条2項(f)号に基づきデータ主体に提供されなければならない情報源に関する情報)、もし、管理者がこの評価に依拠する場合には、データ主体にそのことと理屈を説明できなければならない。管理者は、この手順によって公正かつ責任のある融資決定の助けになると説明する。

管理者は、決定に達する際に考慮した主な特徴、当該情報の情報源及び関連情報の詳細を提供する。このことには、例えば、申請書式にデータ主体が記入した（提供した）情報、延滞を含む過去の口座の動き、詐欺記録情報及び倒産記録のような正式な公的記録が含まれる。

利用される信用評価手法には、公正、効果的かつ不公平とならないよう、定期的に審査されていることをデータ主体に知らせるための情報が含まれる。管理者は、第22条3項の規定に沿って、拒否決定の再検討をデータ主体が請求するための連絡先をデータ主体に提供する。

第15条1項（h）号は、管理者において、特定の決定を説明するのではなく、取扱いにより想定される結果に関する情報をデータ主体に提供すべきであると定めている。アクセス権を行使することにより、データ主体は、プロファイリングを含め、自己に関する決定に気付くことができる。管理者は、データ主体に対し、一般的な情報（特に、決定プロセスの際に考慮された要因、及び、総体的なレベルでの各「重み」に関するもの）を提供すべきであり、それは、データ主体が決定に異議を唱えるために役立つ。

管理者は、第22条の「自動的決定のみに基づく決定に服さない権利」について、2項（a）号及び（c）号の例外が適用される場合であっても、同条3項に基づき、データ主体のためのさらなる保護層として、「少なくとも管理者側で人の介入を得る権利、自己の見解を述べる権利、及び決定を争う権利」を定めている。管理者は、データ主体がこれらの権利を行使するための簡便な方法を提供しなければならない。人の介入が鍵となる要素である。適切な権限及び能力を持つ誰かが、決定を変更するためのあらゆる審査を行わなければならない。審査を行う者は、データ主体が提供したあらゆる追加情報を含め、全ての関連データの徹底的評価を実施すべきである。

第22条2項（b）号は、取扱いを許可する加盟国法に、データ主体を保護する適切な措置を含めるよう義務づけている。このことは、取扱いに関する透明性の必要性を強調する。データ主体は、決定がどのように下されていかなる根拠に基づくかを完全に理解する場合に限り、決定に異議を述べ又は自己の見解を述べることができる。

収集若しくは共有されるデータや、自動的決定プロセスに誤りや偏りが生じると、不正確

な分類、及び、不正確な予測に基づく評価であって、個人に不利な影響を与えるという効果をもたらし得る。

管理者は、あらゆる偏りを確認するために、取り扱うデータセットに基づく評価を頻繁に実施し、相関関係に対する過度な依拠を含め、あらゆる偏見要素に対処するための方法を開発すべきである。アルゴリズムの監査とプロファイリングを含む自動的決定の正確性と関連性に関する定期的審査の仕組みは、他の有用な手段である。

Ⅳ．訪問調査の結果

筆者は、2018年2月13日から21日にかけて、ブリュッセル（ベルギー）及びパリ（フランス）に訪問し、EU関係者からGDPRとクレジットカード情報に関する意見を聴取した。訪問先及び調査結果は、次の通りである。

1. クレジットカード会社〔ブリュッセル〕

(1) 前提

同社における個人のクレジットカード番号（personal account number）の流通は、イシュア銀行から中間業者のネットワークを通じてアクワイアラ銀行へ行き、加盟店へ流通する。同社は、中間業者に位置付けられる。

管理者はイシュア銀行とアクワイアラ銀行であり、同社は両銀行から委託を受ける取扱者の立場で行動する。同社は管理者の指示に基づいて行動するので、「適法な取扱い」（第6条）の根拠は必要ない。

GDPRを遵守するためには、データの流れを把握するためのデータマッピングが非常に重要である。どのような個人情報をどのような目的でどのように集めて分析し、どこにデータを転送し、データのアクセスを許可しているのかという情報を集めることである。データ処理が適正に行われているかの透明性、ガバナンスを効かせるためには、組織がどのようなデータを用いて活動しているか、データの流れを理解することが最も重要である。

同社は、データなしには存続できないので、データ保護に真剣に取り組んでいる。消費者の信頼を裏切り、データ侵害が起きた場合などに、GDPRの制裁金が高いためである。何か起きた時に、きちんとしたステップを踏んだかどうかを証明できるようにする。管理者であるイシュア銀行とアクワイアラ銀行からも問い合わせがかなりある。他の事業者の遵守意識には温度差があるのではないか。

GDPRによって訴訟が起きやすくなった。アメリカほどクラスアクションはできないが、

そのきっかけをGDPRが作った。アメリカでは訴訟に資金を出すファンドを作ってビジネスが展開されている（投資家から資金を募ったり和解金の一部をファンドに組み込むなど）。規制当局から制裁を受けるだけではない。

GDPRが適用開始されると、データ主体からのデータへのアクセス要請が増えるのではないかと予想している。そのためにデータアクセス・ポータルを作っている。

(2) 適法な取扱い（第5条1項、第6条）

GDPRに基づく適法な取扱い（第6条）を行うための根拠には、①同意、②契約の締結・履行のため、③法的義務に基づく場合、④管理者のための適法な利益、がある。

①は、データ分析を行って、マーケティングや製品開発（product development）を行う場合、②は、クレジットカード取引に伴う通常の処理を行う場合、③は、マネーロンダリング対策などの公益に該当する場合（Anti Money Laundering Directiveに公益に該当するとの記載がある）、④は、不正防止などの場合にそれぞれ適用される（不正防止のためのデータの取扱いを公益として扱うには明文が必要であるが、決裁サービス指令Ⅱ（Payment Services Directive Ⅱ）[13]には公益性は明示されていない）。

④を適用する際には個人の権利と組織の利益のバランスを衡量しなければならない。不正防止は、決裁サービス指令Ⅱに定めが置かれている。ヨーロッパ内では、不正防止は法的義務に該当するかもしれないが、不正防止の場合は④の「管理者のための適法な利益」を使う場合が多い。

(3) 管理者と取扱者

同社は、基本は取扱者（processor）として行動するが、管理者として行動する場合もある。例えば、不正な取引の流れを見る場合は、「適法な利益」に該当するものとし、かつ、アメリカにデータを移して分析する場合には、BCRsに基づいて転送する。また、同社は、アナリティクス専門の部署を持っている。オペレーションの改善を行う場合は「適法な利益」に基づき、管理者として行動する。また、顧客から同意を取って、マーケティングのオファーを行う場合（Priceless Specials）がある。この場合も管理者として活動する。消費者と直接に折衝（interact）するのは、主にマーケティングの場面である。

管理者であるか取扱者であるかは、頼まれれば取扱者となり、自ら行う場合に管理者となる点で違いがある。ただし、例えば、不正防止の依頼を受けて分析を行う場合、基本的には指示を受けて行うが、細かい判断を行うときに管理者の要素が入る場面もある。明確には分けられない。1つの処理の中で、管理者であり取扱者である場合がある。

チャリティーのような団体など、本人が団体と既に何らかの関係（existing relationship）があり、本人が組織から情報を受ける合理的期待がある場合には、同意を必要としない例外もある（前文第（165）項、第91条）。マーケティング目的の場合は、そのような例外はないため、同意を取っている。

GDPRの施行によって、取扱者間のデューディリジェンスが大変であった（再委託先の選択と契約の変更）。

（4）GDPRに基づく管理者の義務

第1は、消費者へのプライバシー通知を細かく、かつ簡潔に行うことである。同社は、GDPRに列挙された事項の通知を行うために全ての項目を見直した。GDPRの適用開始に向けてウェブサイトの表記は改定する予定がある。

第2は、適法な取扱いを担保することである。

第3は、第三者に委託するときの適用条項を盛り込むこと、委託先への管理義務を果たすことなどである（第28条）。取扱者は委託に限らず、パートナーとのやりとりにも適用される。

第4は、国際移転の枠組み（十分性、SCCsやBCRs）を遵守することである。ちなみに、同社はBCRsを取得し、プライバシー・シールド[14]にも加盟している。

第5は、個人の権利に対応することである。データの消去、アップデートできない場合の理由説明が求められる。

（5）「同意」と「契約の締結・履行」の違い

法的根拠の中に「同意」と「契約の締結・履行」があり、両者は別のものである。同意は、契約に付随するオプショナルなサービスを提供する場合に使われる。マーケティングは、「契約の締結・履行」には必要ないので、同意が必要である。

全ての場合に同意が必要というわけでもない。クレジットカード取引のために必要ではあるが、そのデータを用いて解析を行い、製品開発をする場合には、「契約履行」ではない。その取扱いが「適法な利益」を超える場合には同意の取得を考えなければならない。

本来的なクレジットカード取引のために行うデータの流通は、「契約締結・履行」に必要な場合なので、同意は必要ない。

事前にチェックボックスにチェックが入っているものは許されておらず、アクティブな同意が必要である。

GDPRに包括同意はなく、個別同意しかない。

信用評価のために銀行が信用調査機関（credit bureau）から情報を取ることについて、リ

スクを取りたくない銀行であれば、本人から同意を取っているのではないか。それがなければ契約ができない旨の説明を付けなければならない。GDPRは、個人情報の提供をサービス提供と引き替えにすることを認めていないが、銀行には信用調査義務があるので、この場合は許されるのではないか。オンラインサービスでマーケティングのオファーを得ることを義務として、その上でサービス加入を許すことは認められていない。ただ、クレジットカードの場合には銀行側にも調査義務があるので、おそらく法律又は金融庁の指針に基づいているのではないか。

GDPRの施行によって、同意のチェックボックスの変更、すなわち、チェックボックスを増やすことと撤回のメカニズムを作ることが一番大変であった。

(6) プロファイリング

プロファイリングを行うための明示的同意（第22条2項（c）号）は、適法な取扱いを行うための同意とは別に取らなければならない。同社では、チェックボックスを2つ設けている。同意を別に取るかどうかは、組織の判断によるが、例えば、個人が自分に対してオファーをもらうことが目的のプログラムがある。その場合、当該個人は、既にオファーの内容が自分に合っているので、自分に対してそれなりに情報分析が行われていると想像しているのではないか。そのような場合には、チェックボックスを1つにする組織もあるかもしれない（ただし、同社は別々にボックスを設けている）。同社には、街単位でオファーを行う（CLOのような）マーケティングサービスもある。

プロファイリングは、第6条で求められる取扱いのための適法な根拠とは別に義務づけられるものである。クレジットカード加入時の契約に基づく自動スクリーニングは「契約締結・履行のために必要」（第22条2項（a）号）に該当しない。契約履行とはサービスを提供することを意味するが、信用リスクを管理することは、それとは異なる。信用リスクの評価は、組織の適法な利益のためであって、それが法的義務でない限り、「契約履行」には当たらない。

どの法的根拠を使うかは、プロファイリングの種類にもよる（第29条作業部会の指針による）。信用情報機関（Credit Bureau）の場合は、同意が必要なプロファイリングの域に入っているのではないか。消費者との接点がないので、銀行を通して同意を取っているかもしれないし、「適法な利益」で行っているかもしれない。

第22条は管理者にも取扱者にも適用されるが、取扱者は管理者の判断に基づいて行動するので、結局は管理者判断となる。同社が管理者となる場合は、明示的同意を取っている。

GDPRの適用があるプロファイリングか否かは場合による（例えば、本人に悪影響を及ぼす場合は、プロファイリングとしてGDPRが適用されるなど）。全てのプロファイリングに同

意が必要というわけではなく、第29条作業部会の文書に基づいて同意の要否を判断する。

(7) 第三国移転

EU域外の第三国に個人データが移転する場合は、BCRsかSCCsを用いなければならないが、それらの手段がない場合は個人の同意を取らなければならない。その場合は、データの取引単位で個別の同意を取ることになる。

「同意」は得るだけでなく、無料で撤回する権利も保障しなければならない（第7条3項）。同意に基づく個人データの移転の場合は難しい話になってしまう。撤回を拒否できない。サービス提供には第三国移転は必須ではない。国内でプロセスを行うという選択肢もあるので、同意に基づく移転は非常に難しいと思う。意識の高い消費者でない限りは撤回しないだろうが、まれにいるのでお勧めではない。クレジットカード取引で同意に基づかせるのは難しく、国内でのみ転送すべき（あるいは、マニュアルで処理して欲しい）という話になってしまう。同意を撤回した数人のためだけにプロセスを変えなければならなくなってしまう。

(8) データ・ポータビリティ

銀行間でアカウント情報を移すことはあり得る。イギリスの銀行では既に行われている。簡単にスイッチできるようになっている。

データ・ポータビリティは、管理者のみを対象としており、取扱者である同社には適用されない。しかし、管理者から転送を指示されることはある。エクセル等のファイルにダウンロードできるよう、対応している。実際に消費者が銀行に行って、取引情報を他に転送して欲しいということはあまり想定できない。リクエストが来る可能性は極めて低いのではないか。

同社が管理者として扱っている情報についても、ポータビリティに対応できるようにしているが、稀だと思われる。消費者オファーを行うマーケティングサービスの場合は、消費者との直接の接点があるので、ポータビリティの要請はあり得ると思う。ただ、どの業態に転送させるのかは謎である。フォーマットは双方向（interactive）でなくてもよく、エクセルを用いて先方で読めれば良い。

データアクセスのみならず、データアクセス・ポータルを用いてポータビリティを行うことができる。

2. クリストファー・クーナー氏[15]〔ブリュッセル〕

(1) GDPR全般について

非常に法的に不安定な状況にある。指令に基づく現行のルールに縛られながら数ヶ月後の

適用開始に向けて準備をしなければならない。徐々に対応を進めている。

GDPRは非常に長くて複雑である。解釈がまだ決まっていないところもあり、裁判所の判断も監督機関による解釈の先行事例もない。投機的な解釈を行う者もある。

GDPRの拘束性から、国内の制度を変えなければならないため、国レベルでは懸念がある。政治的な意味でも緊張があり、EU懐疑派やEU全体の調和に反対する者もいる。各国政府と欧州委員会側の緊張関係もある。

(2) クレジットカード事業者への影響

GDPRは非常に広い規制である。数少ない中小事業者を除けば、一般的には全ての種類の事業者に適用され、クレジットカード事業者への特別な例外はない。

特別な事項としては、前文第47項に「不正防止」を管理者の適法な利益とする説明がある（第6条1項（f）号）。ヨーロッパでは、クレジットカード事業者は、適法な利益の根拠をどこに置くかについて懸念している。

他に重要な規定として、第26条の共同管理者の規定がある。クレジットカードシステムには、システムオペレーター、イシュア銀行、加盟店等、複数の当事者が関与し、違う役割を担っている。多くの場合、彼らは共同管理者となる。第26条は、各管理者の役割や責任について、文書による詳細な取り決めを行うよう義務づけている。クレジットカード事業者は、共同管理者として、その役割を明らかにしなければならないが、多くの場合は共同管理者になるのではないか。しかし、クレジットカードシステムにはこれまで適用されてきたルールがあるため、実態を尊重し、従前の取組を変える必要はない。しかし、既存のシステムによる取組を明文化し、第26条に沿っていることを確認することが重要である。

(3)「同意」と「契約を締結・履行するため」の関係

GDPRは「同意」の要件を厳格化した。これは、特に、GoogleやFacebookにおいて、長くて分かりにくい利用条項に同意するなど、オンライン上のデータ処理について不満の残るケースが多くあったからである。GDPRの文章は、事業者にもっと明確な同意の表明を（得るよう）義務付けた。第7条2項は、同意とそれ以外の事項を明確に区別できるよう義務づけている。前文第43項には、別の取扱いには別の同意を与えるよう求めている。例えば、クレジットカード取引のための取扱いと、マーケティング目的の取扱いがあるが、取扱いの目的が複数ある場合には、各目的に応じて同意を取らなければならない。個別の目的を明確に示し、それぞれについて同意を取らなければならない。

個別の決済について同意を取ることは現実的ではないので、クレジットカード取引のため

にデータをクレジットカードのネットワークで流通させることは、カード保有者が契約を締結するために必要であると解釈できる（第6条1項（b）号）。ただし、この規定は厳格に解釈されている。契約を履行するために本当に「必要」でなければならないが、少なくとも決済取引のためであれば同条項が適用できる。「必要」でなければならないため、例えば新たなサービス提供のためであれば、同条項は適用できない。

「同意」の概念は、GDPRの方が日本よりも厳しい。特定の、情報を与えられた、明白な同意であることが必要であり、黙示的同意は認められない。しかし、同意は常に署名によらなければならないわけではなく、明白な行動を取る方法でも取得可能である（医者にかかって治療を受ける場合など）。

同意を取る単位は目的毎ないしは取扱毎である。複数の目的を示して1つのチェックボックスにチェックをしてもらう方法は許されない。

第7条3項の同意の撤回には例外はない。同意が使われすぎないようにする必要がある。撤回の効力は将来に向かって生じる（遡及効はない）。

(4) 透明性の確保について

第13条（データ主体から個人データを収集した場合に提供すべき情報）と第14条（データ主体から個人データを取得しなかった場合に提供すべき情報）も重要である。これらは管理者に適用され、取扱者には適用されない。

一般的に、取扱者が通知を義務づけられるのは限定的である。取扱者は、第28条に基づきプライバシー通知を行わなければならない場合もあるかもしれない。

第29条作業部会の文書のうち、プロファイリングに関連する論理の通知をどの程度細かく行うかについては、非常に議論がある。自動的決定の技術的論理を説明するのは現実的ではない。欧州データ保護会議が事例を出すであろうが、合理的アプローチが必要であり、微に入り細に入りロジックを示す必要はない。シンプルかつ明確な方法での情報提供を行うべきという機運が高まっている。プロファイリングのメカニズムについて通知をすると営業秘密や他の知的財産と抵触する場合がある。

(5) 越境データ移転

クレジットの決済行為はグローバルに展開されていると思う。複数のコンピュータを経てデータが国境を超えればデータ移転に該当する。

十分性、BCRs、SCCの他に、新たな仕組みとして、認証や行動規範がある。認証や行動規範はまだ実証実験が進められており、まだ明確ではないが、数ヶ月後に欧州データ保護会議

から具体化された文書が出されるであろう。

第49条1項（b）号と第6条1項（b）号の契約締結・履行に「必要」な場合に関する解釈は、どちらも限定的に解釈されるという点で、概ね共通する。単に便利だからという理由では許されない。

(6) プロファイリング

ダイレクトマーケティング目的の場合は、異議申立権の例外はない（第21条）。

第29条作業部会文書に関して、第22条の解釈には不明瞭な点がある。一般的には、その適用範囲は広く、信用情報機関から受け取ったデータも自社がデータ分析を行ったデータも含まれる（派生データ・推測データの箇所）。

第29条作業部会文書のうち、プロファイリングの該当性基準と判断主体について、まだ明確な解釈はできていない。管理者が一定の施策を講じなければならないため（第22条3項）、主に管理者を対象にしている（のではないか）。

第29条作業部会文書のうち、第22条2項（a）号及び（c）号は、第6条と同様に解釈して良いと思うが（本来的な決済のために、クレジット入会審査の目的でのプロファイリングは契約に「必要」であること、それ以外は同意）、厳格に解釈しなければならない。本人の信頼性を評価するための審査は必要であるが、広い範囲の審査は「必要」性を満たさない。契約の「必要性」を満たさない場合は、同意を取る必要があるが、高次元なところに基準を置いておく必要がある。クレジットカード会社は、法的根拠を慎重に吟味しなければならない。

3. 欧州委員会司法・消費者総局[16]〔ブリュッセル〕

(1) 国内法とクレジットカード情報の流通

クレジットカード取引でデータ流通の問題が生じた事例は把握していない。GDPRは指令を引き継いでおり、法的基盤及び主な原則に変更はない。クレジットカード取引との関係で問題になるのは、前文第（47）項の不正防止である。

(2) クレジットカード情報の流通と管理者・取扱者

イシュア銀行がまずは管理者となる。共同管理者の規定（第26条）が適用されると考えられる。管理者と取扱者の関係は、扱われるデータや取扱い方（ビジネスモデル）による。

係属中ではあるが、ショッピングモールに関する事案で管理者と取扱者の位置づけが争われている事案がある[17]（C40/2017）。

(3) 同意

GDPRは、一般的に明示的同意（explicit consent）を要求しているわけではない（センシティブデータと越境移転のみ）。第4条11項の同意は、明確かつ積極的な行動（clear and affirmative action）を求めている。黙って行う（tacit）ものも含まれる。

EUのデータ保護制度（第6条）は、多元的であり、複数の法的根拠（契約＋同意）に依拠しても構わない。しかし、契約と同意は全く別である。

通常のクレジットカードの事業シナリオでは、同意は適切な法的基礎にはならない。契約締結・履行に「必要」であるという規定（第6条1項（b）号）が法的基礎となる。同意は、追加的、選択的な仕組みでしかない。例えば、クレジットカード取引のために収集した個人データをマーケティングやリサーチ、ロイヤルティクラブに加入させるような場合であって、契約とは別に本人から同意を取らなければならない。契約と同意はお互いに依存する関係にはない。

(4) 越境データ移転

第49条1項の解釈のうち、基づく契約締結・履行に必要である（b号）という規定は、第6条同様である。明示的同意（a号）はより高次な同意となる。

第49条は、法的安定性の観点から、大量、体系的、構造的なデータ移転には適用できない。BCRsやSCCは、大量、体系的、構造的なデータ移転を行うクレジットカード会社にとって最も適したツールである（法的確実性）。

(5) プロファイリング

第22条は自動的処理のみに基づく決定に適用される。プロファイリングが個人に関する決定をもたらす場合もそうでない場合もある。

クレジットカードの処理では、カードを発行するための情報を取得し、アルゴリズムに当てはめ、評価を下す。「意味のある人の介入」について、アルゴリズムではどのようなデータが考慮され、何が計算されたかなど、人による意味のある確認が求められている。

オンラインでのクレジットカード申込みや学校への出願などがあるが、自分の評価が正しく行われなかったことを主張できることが重要である。アルゴリズムは、低所得者層地域の居住者であるなどの1つの要素で差別をもたらすこともあるが、実は他の資産がある場合なども考慮するよう主張できることが重要である。

第13条2項（f）号と第14条2項（g）号の透明性を確保することも重要である。人の介入は、能動的に決定を見直させるためのものである。関連する論理について、アルゴリズムを示す

ことは知的財産権に抵触するため、義務づけていない。何が行われ、どのような要素が存在し、結果が何であるかを伝えることが重要である。

4. タンギー・ヴァン・オーバーストラーテン氏[18]〔ブリュッセル〕

(1) 同意

同意には2つの種類がある。1つは明示的な同意であり、特別な種類の個人データ（いわゆるセンシティブデータ）に適用される。もう1つは通常の同意であり、不明瞭でなく（unambiguously）表明（express）されたものでなければならない。これは、完全な形で情報提供を受け、意思を積極的（actively）に表明するというものであり、隠された事項があったり、利用条件に拘束されたりするものであってはならない。

第29条作業部会が同意に関する指針を出しており、タブレット上でスワイプをすることでも同意の表明（express consent）になる。何かをしなければならないが、署名やチェックボックスへのチェックには限られず、顔認証で頷くだけでも良い。

（明示的な）同意に依拠できるのは、ダイレクトマーケティング目的での機微情報の取扱い、プロファイリングを含む自動的決定である。しかし、自動的決定については、契約の締結・履行のためという規定に依拠することもできる。

(2) 契約の締結・履行のための「必要性」

（第6条、第22条、第49条など）クレジットカード取引では契約の必要性に依拠することが通常であるが、「必要性」は厳格に解釈されることに注意しなければならない。

ヨーロッパ人が日本に旅行をしてクレジットカードを使う場合、イシュア銀行はデータをアクワイアラ銀行に移転しなければならない。その場合は契約を履行するために「必要」である。それに対し、クレジットカード会社が、その人物が誰で、何のためにどこで支払いを行ったか等の情報を収集し、パートナーと共有する場合は、「必要」性は満たされない。また、GDPRは、移転が偶発的（occasional）であることも必要であると述べている（前文第（111）項）。これは、一例としてヨーロッパ人が頻繁に日本に行かない場合などに当てはまるであろう。

(3) 越境データ移転

大量構造的データ流通については、同意で正当化することはできない。同意は不定期なものでなければならない。ほとんどの顧客に対して、同意は撤回されるリスクがあるため、同意に依拠することは勧めていない。

支払いのための決済は、（EU域内のみで処理されている場合もあるが）基本的には越境デ

ータ移転に当たる。

十分性を日本が取れば越境移転の問題は解決するが、多国籍企業の場合は、十分性を取っていない国も関与するため、単純ではない。

(4) 同意と契約の違い

GDPRの適用開始までは、一般的な条項の中にデータ保護の規定を入れるような契約が認められていた。しかし、管理者は、契約の中で、一般条項を参照することに加えて、データ保護に特化した文書を添付する形で、プライバシーに関する規定を設けている。どのように取扱いを受け入れるかについては、プライバシーに関する文書の最後に、いくつかの短い重要文章を載せている。管理者、目的、権利、自動的決定プロセス等のチェックボックスを設けている。しかし、それでは負担が大きいので、ダイレクトマーケティング、調査、広告、自動的決定等を行う日本の顧客向けには、6つのチェックボックスを設けた文書を用意している。

同意は、チェックボックス毎に個人のyes/noの判断が異なるため、マネージが難しい。そこで、多国籍企業などは、ダッシュボードを設けており、顧客が、何に同意をしたかを確認できるようにしている。判断を変えるときにはダッシュボードを使って自ら行うことができる。ソフト等で費用がかかるため、全ての企業に勧めることはできない。

GDPRに基づく場合は、個別の目的/取扱い毎に同意を取らなければならない。

同意に過度に依拠することは勧めていない。日本を含め、中国、インド、マレーシア等、アジアの国々は同意に依拠するところが多い。もし越境適用（第3条2項）が適用されるならば、企業は実務を変更しなければならないであろう。越境適用される場合（クレジットカード事業者がEU市民の情報を取り扱う場合）には、SCCsやBCRsなどの移転のソリューションに加えて、まずは適法な取扱い（第6条）を保障するための措置を講じなければならない。ヨーロッパの市場を見た場合には、マスターカードかビザが主流ではないか。

契約締結・履行の「必要」性は厳格に解釈しなければならないが、通常のクレジットカード取引における情報処理は、クリアランスを含めて必要性が認められる。

(5) 管理者・取扱者

マスターカードとビザは基本的には類似するビジネスモデルである。アメックスは異なっており、全てを自己のシステム内でデータを処理している。

（いずれのビジネスモデルも）銀行のみならず、おそらくクレジットカード会社も管理者になるであろう。カード会社が取扱者として活動することについては部分的には賛成するが、

全てのデザインを行っており、銀行は何もデザインしていない場合には、主体はクレジットカード会社ではないか。ただし、管理者と取扱者の区別はさほど重要ではない。GDPRに基づき、取扱者の義務及び保障が増大しているからである。むしろ、管理者になりたがる顧客が多いのではないか。なぜなら、彼らが自ら判断権限を持つ（責任範囲を決められる）からである。顧客は、サービス提供者を管理者にはしたくない。なぜなら、自らデータの権限を持っていたいからである。

クレジットカードビジネスは複数の管理者が関わるため、共同管理者（第26条）の規定が重要性を増している。加えて、取扱者義務が、契約締結義務等（第28条）によって重くなっている。

第13条、第14条の透明性確保は管理者の義務であり、取扱者は管理者のために行動するに過ぎない。そのため、取扱者は、透明性の義務を負わない。

(6) プロファイリング

「プロファイリング」の定義は非常に広い。第29条作業部会は、誰かを特定のカテゴリに入れたらプロファイリングに該当すると述べている。クレジットカードのビジネスでは、ある人物の支払能力等を評価して限度額を設定する。クレジットカードが海外で不正利用された場合などでは、カードをブロックするためにプロファイリングが必要である。

自動処理のみによるプロファイリングを決定プロセスにつなげた場合には、人の介入を保障しなければならない（第22条3項）。しかし、クレジットカード事業では不可能な場面がある。なぜなら、もし、カード加入後にレストラン（NY）で支払おうとした時に、それが他の国外（香港）で不正利用されている可能性を理由にブロックされていたら、支払いをさせて欲しいと思うであろう。しかし、人を相手にするのとは異なり、支払いが自動化されている場合には、人の介入を保障することは難しいであろう（コールセンターに助けを求めることはできるとしても）。既に自動処理されている場合に、人の介入をさせるのは遅きに失する。

しかし、「関連する論理」を伝えることで、第22条3項の遵守は可能である。クレジットカード業界では、「関連する論理」の内容は簡単である。なぜなら、その決定は支払い能力、最近の取引履歴、限度額等と結びついているからである。アルゴリズムは知財に抵触するので説明する必要はない。技術的な情報ではなく、（オーバーストラーテン氏の見解では）いかなる要素を考慮に入れて決定したかという理由を説明すれば良い。健康情報に基づいて保険加入の是非を判断する際にも、考慮に入れた事項は明らかといえる。簡潔で分かりやすく伝える必要はある。「関連する論理」は、決定に至った理由及び結論と同義である。

取扱いがプロファイリングに当たるかどうかを判断する第一時的主体は、管理者である。

GDPRの全ては、管理者が「責任」を果たさなければならないということである（第24条）。指針がGDPRの解釈をサポートしている。

5. Commission Nationale de l'Informatique et des Libertés（CNIL）[19]〔パリ〕

(1) ビジネスモデル

フランスのクレジットカードのビジネスモデルは複雑である。カードの支払いは、個人銀行（イシュア）から加盟店の銀行（アクワイアラ）へ行くわけであるが、その間に国内でデータが流通する場合には、GIECB（Groupements des cartes bancaires）[20]という第三セクターがスキームを動かす。フランス国外のデータ移転の場合）には、純粋なフランスのレイヤー以外の事業者、すなわちビザやマスターカードのスキームが使われる。

GIECBのデータ処理の目的は、1つは技術的な支払いの処理、もう1つは不正行為の管理である。

(2) 取扱いの適法性（第6条）

取引の遂行という意味では、「契約の履行のために取扱いが必要」な場合に該当する（第6条1項（b）号）。（対銀行への）不正行為の管理は、管理者側の適法な利益に該当する。不正行為の管理は、必ずしも第6条1項（a）号に根拠を求めなくても行うことはできるが、（個人データの取扱いの文脈では）管理者側の適法な利益に該当する。

GIECBのスキームの中で、第6条の同意が必要となる場面はない（契約に基づいているから）。問題となった事例もない。マーケティング目的の場合には、同意が必要な場合も考えられるが、標準的な契約で対応できるのではないかと考えている。同意が必要になるかどうかは、どの程度の侵害性があるかどうか。プロファイリングも、どの程度のデータがどの程度分析されるかによる。マーケティングだから自動的に同意が必要というわけではない。

(3) 管理者と取扱者

プレーヤーがたくさんいるため、管理者に該当するか取扱者に該当するかはケースバイケースである。各銀行がカードを発行するが、ビザやマスターカードがついているので、ビザやマスターカードが独自の目的のためにデータを取り扱う場合もある。

これまで「共同管理者」（第26条）という概念はなかった。実際、GDPRが5月25日から適用開始されるが、どのようなステータスにするかはまだ決まっていない。共同管理には疑問がたくさんある。欧州のハーモナイズ化もあるので、どのような立場に立つかは他の加盟国との整合性を取る必要もある。

(4) 越境データ移転

大量・構造的移転には個別の例外（derogation）は使えない（2016年訪問時と同様の回答）。この部分についての解決策は見つかっていない。

BCRs、SCCsが越境データ移転のためのツールだが、これらは今現在の話であって、認証や行動規範などの検討も進められている。認証（certification）を行う団体を認定する組織は、（CNILとは別に）COFRAC[21]（「フランスAccreditation委員会」というように訳すことができる）という団体が行う。フランスには、認証制度が既に存在している。

SCCsには、欧州司法裁判所で問題になっている事案がある[22]。

(5) プロファイリング

クレジットスコアリングがプロファイリングに関係しており、第29条作業部会の指針が出ている。指針はプロファイリングを詳細化しており、狭める形で解釈されているようである。

第22条については、フランスでは、事後に人的介入を可能とする規定は、既に存在している。異議を唱えて観察してもらう仕組みである。

「関連する論理」は、なぜ信用が得られなかったかについての説明が求められる。どのような決定的要素があり、信用が得られなかったのか。アルゴリズムの分析を行って信用評価を行うのは、信用協会のようなところであり、そこが説明をしなければならない。アルゴリズムを示すことは知的財産権の関係から必要ではないし、普通の人が見ても分からない。

(6) その他

フランス国内で、GDPRを補足する法案が審議中であり、4月始め頃に採択される予定である[23]。GDPRの考え方は、1995年の指令から変更ない。

第29条作業部会の同意とプロファイリングに関する指針が重要である。

6. Groupements des cartes bancaires（GIECB）〔パリ〕

(1) 管理者・取扱者

（イシュア銀行、アクワイアラ銀行、GIECB、ビザ、マスターカードなど、多数当事者が関与するクレジットカードビジネスの中で、誰が管理者・取扱者、あるいは共同管理者になるかという質問をしたところ、GIECBの仕組みの話が入り）、GIECBは、不正防止や取引のセキュリティのサービスを行っている。支払いのための取扱いは、STET（GIECBの下部組織）が行っている。

GDPRの適用と評価には時間がかかるので、研究中である。第29条作業部会の指針やCNIL

の解釈を待っているので、包括的に見ていかなければならない。数ヶ月後には考え方は変わっているかもしれない。

データの取扱いは、スキームとは分けて考えなければならない。国内はGIECBのスキーム、海外はビザやマスターカードというようには、完全に分けられていない。フランスで普通カードを持っている場合に、GIECBマークとビザ、マスターカードのマークが付いている。交換手数料委員会（Interchange Commission）のルールによると、カード所有者がスキームを選択できるようになっている。

GIEDBは、管理者となる場合もあれば、取扱者となる場合もある。GIECBが管理者ではないかという考え方もあるが、その論点はまさに現在検討中であり、詳細な回答はできない。究極的には、責任自体は管理者も取扱者も同じであると考えている。

(2) 同意と契約

適法な取扱いについて（第6条)、通常のクレジットカード取引で流通する情報については、適法な利益、法的義務、契約を締結・履行するためといった根拠でかなりの部分がカバーされるので、同意は必要ない。

不正防止、取引の安全性は、契約の締結・履行又は適法な利益のどちらか（又は両方）に該当する。

同意には、通常の同意と明示的同意に分けなければならない。後者は、センシティブデータのような特殊な場合に適用される。

通常の同意はチェックボックスにチェックを入れるようなもので、明示的な同意は、ダブルメール（同意の返事をした者にさらにメールを送り、リンクをクリックさせる等）や署名をしたものが該当する。

総体的には、同意に依拠するべきではない。同意、ことさら明示的同意には実務的な負荷がかかる。

(3) 第三国への越境適用

個人データを越境流通させるクレジットカード業界は、ヨーロッパ市民向けにGDPRの準備をしなければならない。

(4) 第三国等への越境移転

EU域外に個人データを移転する場合、すなわち、日本の事業者がEU市民のデータをストックしたい場合には、明示的同意などの根拠を満たさなければならない。域外に出た場合に

は、データをセンシティブなものとして扱わなければならない。

明示的同意等を定める第49条（特定の状況による例外）（derogation）は制限的な場合にしか使われない。1回限りの突発的な移転に厳しい条件で適用される。クレジットカードのような大量・恒常的な取引には、十分性、BCRs、企業－サプライヤ間のSCCsで対処する。

derogationは厳しく適用されなければならず、本当に契約を締結・履行するために必要な場合や、明示的な同意を必要とする場合がある。

(5) プロファイリング

一般的には、第22条自体は自動審査を禁止しているわけではなく、自動審査による結果に適用され、その中に例外事項がある。

ある個人がカードを保有する場合の審査は、銀行によって異なる。GIECBで管理しているわけではない。

GIECBがプロファイリングを行っているかどうかは答えられない。

第13条と第14条の関連する論理（logic involved）は、CNILが勧告（recommendation）を出している。それによると、プロファイリングにどのような重要性があって行うのか、その場合にどのような結果が生じるかを明示せよと述べている。透明性のプロセスに関しては、イシュア銀行次第である（統一ルールがあるわけではない様子）。1978年のフランス法に基づいて行ってきたので、独自の政策をとってきた。

(6) データ・ポータビリティ

個人が保有するか、個人が指名した第三者に移転できるようにするためには、フォーマットが重要である。明確で分かりやすい電子的フォーマットである。

カード保有者又は移転先銀行のPCで読めるようになれば良いので、エクセルシートで用意すれば良い。

警察の照会に答えるような場合など、法的義務に基づき作成したデータなどは含まれない。個人が同意した場合や、契約の締結・履行を行う場合など、条文上の要件に当てはまるデータだけが対象となる。

(7) GDPRの一般的な影響

抜本的なところでは、どのような個人データを取り扱えるのか、どのように適用されるかという点を評価しなければならない。

利点は、今までは自動的に処理してきたが、改めて個人データ保護の重要性を啓蒙する機

会を得ることになった点である。究極的には、当該データは当該目的のために必要か、という点を企業が問い直す機会となる。

GIECBとしては、データの最小化（data minimization）は行わないが、取引の安全に注力する。

Ⅴ．検討

クレジットカード事業者がGDPRを遵守する関係で注意すべき事項は、①管理者であるのか取扱者であるのか、②適法な取扱いの根拠、③越境移転の枠組、④個人による権利行使への対応、である。

①の解釈は、関係者によって立場が異なっている。個人データの取扱いに関する決定権限を有するか否かは文脈により異なるため、「管理者」や「取扱者」は相対的概念である（第4条7項及び8項）。クレジットカード事業者は、管理者となる場合もあれば、取扱者となる場合もあるが、事業のグランドデザインを描いている場合には、他者から指示を受ける立場ではないため、管理者としてみなすべきと考えられる。また、クレジットカード事業は、システムオペレーター、イシュア銀行、加盟店等、マルチプレーヤーで運用されることから、共同管理者の規定が適用され得る（第26条）。

②については、「同意」ないしは「契約の締結・履行のための必要性」が根拠となり得る（第6条1項（a）号及び（b）号）。クレジットカードの決済目的の場合は「契約履行」のためと解釈し、それ以外は個別同意を求めるという実務運用がなされている。不正防止の場合は、「管理者の追求する適法な利益」が適用される（同条1項（f）号）。ここで注意すべきは、「同意」と「契約」の違いを理解し、契約を根拠とする場合には「必要性」を厳しく解釈しなければならない点である。さらに、「同意」の中にも、通常の同意と明示的同意があり、両者の概念も異なっている。

日本の個人情報保護法では、「本人の同意」とは、本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう（当該本人であることを確認できていることが前提となる。）。「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意にかかる判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない[24]。例えば、本人に対して、一定期間内に回答がない場合には同意したものとみなす旨の電子メールを送り、当該期間を経過した場合に、本人の同意を得たこととすることは困難とされている。他方、「明示の同意」以外に「黙示の同

意」が認められるか否かについては、個別の事案ごとに、具体的に判断することとなる旨が解説されており、黙示の同意は排除されていない。サービスの提供の申込の際に、申込者から申込書・約款等で包括的に同意を得た場合には、有効な同意と解釈されている[25]。

このように、日本では黙示的同意や包括的同意も「同意」に含めることができ、同意に法律上の有効期限もない。利用規約の一部に個人情報の取扱いへの同意を取るための条項を設けても、日本法では同意として有効である。個人情報保護法自体に、オプトアウトのように、同意を擬制して第三者提供を認める仕組みもある。

他方、GDPRの同意は、「自由になされた、特定の、十分に情報を提供された」、自己のデータの取扱いに対する明白なデータ主体の意思表示であって、同意と契約を混同することは認められていない。同意を得るための文言は、他と区別しなければならないなど、同意スキームを用いるためには多くの制約が課せられている（第7条）。

明示的同意は、データ主体の明示的な表明による同意であって、個人による高いレベルでの個人データへコントロールを及ぼすという趣旨で設けられている。手法は既に述べた通りであるが、口頭で取得することは推奨されておらず、二段階の同意確認が有効性を担保する。

さらに、人為的ミスを減らす、顧客の不払いリスクを減らす、決定を短期化し、効率性を向上させるなどといった理由では、契約締結・履行の「必要性」を満たすことができない。この文言は狭義に解釈される。

③については、2018年7月17日の段階で、EUと個人情報保護委員会との対話が終了し、同年秋までに個人データ移転の枠組を運用可能とするための国内手続を進めることとなっているため、EUから日本への個人データ移転には障壁がなくなる見込みが高い[26]。しかし、クレジットカード事業のように、多国籍で大量・構造的にデータを移転させる場合には、BCRsかSCCs、あるいは認証制度若しくは行動規範に基づくことが必要となる。個別移転に適用される明示的同意（第49条1項（a）号）は、大量構造的データ移転には適用されず、偶発的な移転でなければならない（前文第（111）項）。

④については、データの消去、アップデート、それらができない場合の理由を説明できるようにするほか、日本には存在しない権利（データ・ポータビリティやプロファイリング等）に対応しなければならない。特に、プロファイリングは「取扱い」の一種であるため、取扱いに関する義務規定一般に加えて、異議申立権（第21条）、プロファイリングを含む、自動処理のみによる決定に服さない権利（第22条）が適用される。特に、データ主体に対する透明性が重視されており、自動的決定に関する活動に従事していること、関連する論理についての意味ある情報、決定の重大性と想定される取扱結果を説明しなければならない（第13条2項（f）号、第14条2項（g）号）。「関連する論理」は、日本法には馴染みのない用語である

が、要するに、決定に至った理由と結論を意味しており、クレジットカード取引の場合には、支払能力、最近の取引履歴、限度額等を根拠に説明すれば足りる。むしろ、第22条は、例外が適用される場合の保護措置として、人の介入をいかに担保するかという点が課題となる。この点はEU内でも解釈が固まっているわけではないようである。

次に、日本の法制度への示唆を簡単に述べておきたい。2015年の個人情報保護法改正に先だち、2014年6月24日に取りまとめられた「パーソナルデータの利活用に関する制度改正大綱」（高度情報通信ネットワーク社会推進戦略本部）は、プロファイリングを継続的な検討課題に位置づけている。

日本の個人情報保護法制は、プロファイリングに関する規定を有しておらず、導入した場合の影響力の予見は難しい。規律方法としては、プロファイリングが人の差別をもたらさないようにするための基本的責務等を定め、業界のガイドラインで自主的な取組を促す方法、プロファイリング禁止を義務化する方法、プロファイリングを制限するよう努力義務を課す方法などがある。しかし、人の評価を行うためのコンピュータ処理は、ありとあらゆる場面で行われているため、ガイドライン方式で実例を類型化することは容易ではない。プロファイリングを義務規定として設けるのは、個人情報取扱事業者への規律方法に即しているが、AIが広く用いられるようになった社会への波及効果が大きいことから賛成しがたい。また、努力義務として規律を入れることも、法的効果の弱さが懸念される。

そこで、プロファイリングの規律を有するGDPRを参考にせざるを得ないが、仮に設けるとすれば、第29条（訂正等）又は第30条（利用停止等）に続く権利の1つに位置づけることが考えられる。これらの規定は、保有個人データの内容が事実でないとき（訂正等）、目的外利用又は適正取得違反の場合（利用停止等）に適用されることから、プロファイリングにどのような要件を課すのかが問題となる。プロファイリング自体に異議を申し立てるのか、プロファイリングによる決定が差別を生み出すことを制限するのかというように、規律対象をいかに確定するかによっても、権利内容は異なる。第29条作業部会のプロファイリングに関する指針の中でも、GDPRがプライバシーには限定されない新規定を導入した旨に言及されている。差別に対処する場合には、個人情報保護法に位置づける論理的必然性はない。場合によっては、特定分野で規律を設ける方法もあり得る。いずれにせよ、次の個人情報保護法改正が行われる際には、EUとの差分を意識しすぎることなく、本質的に、国内法によってプロファイリングを規律する必要性があるのか、という基本から議論を行う必要がある。

［注］

[1] Regulation（EU）2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC（General Data Protection Regulation）, 2016 O.J.（L 119）1-88.

[2] 個人情報の保護に関する法律（平成15年5月30日法律第57号）。改正法は平成27年9月9日法律第65号。

[3] 情報社会サービスとは、通常は、報酬を伴う、遠隔からの、電子的手段によるサービスであって、サービス利用者が個別に要請するものを意味する（Directive（EU）2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services（OJ L 241, 17.9.2015, p. 1））。ウェブサイトストア、検索エンジン、オンライン広告、動画共有サイト、ブログ、ホスティング、オンデマンドビデオ、オンライン相談、オンラインマーケットプレイス、SNS等が含まれる（Mario Sõrm, *Directive 2000/31/EC, Workshop on the regulatory and practical aspects of electronic commerce*, Feb. 17-18, 2014, at Rabat）。

[4] 第6条1項（a）号は同意、第9条2項（a）号は明示的な同意に基づく取扱いを認めている。

[5]「処理者」と訳されることもある。

[6] 第29条作業部会の正式名称は「個人データの取扱いに係る個人の保護に関する作業部会」といい、1995年データ保護指令に基づく助言機関である。この組織は、監督機関又は各加盟国が指名した代表者、EUの機構等の代表者、欧州委員会の代表者で構成される。GDPRに基づき、2018年5月25日、第29条作業部会は欧州データ保護会議（European Data Protection Board）へと改組され、その権限は大幅に強化されている。

[7] European Data Protection Board, Guidelines, https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en；Article 29 Data Protection Working Party, Guidelines, http://ec.europa.eu/newsroom/article29/news.cfm?item_type＝1360. 指針の翻訳は、個人情報保護委員会が順次公表している（https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/）ほか、日本貿易振興機構（JETRO）が実務ハンドブック等を公表している（https://www.jetro.go.jp/world/europe/eu/gdpr/）。

[8] Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, WP259 rev.01（Adopted on 28 November 2017, last revised and adopted on 10 April 2018）.

[9] Article 29 Data Protection Working Party, *Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP217（Adopted on 9 April 2014）.

[10] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251 rev.01（Adopted on 3 October 2017, last revised and adopted on 6 February 2018）.

[11] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on Apr. 9th, 2014, pp. 59-60.

[12] 第13条2項（f）号と同様、プロファイリングを含む自動的決定に関する通知事項が定められている。

[13] Payment services（PSD 2）- Directive（EU）2015/2366, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

[14] EU-U.S.プライバシー・シールドとは、EUからアメリカへの越境データ集通を適法に行うために、2016年7月12日に採択され、同年8月1日に開始したスキームである。アメリカは、EUとの間で、自主規制に基づくセーフハーバー・プライバシー協定を締結し、2000年からその運用を行ってきた（EUから見ると十分性認定の一種である）。しかし、2013年のPRISM問題を契機にセーフ・ハーバーの見直し論が高まり、その過程で、欧州司法裁判所は、2015年10月6日、セーフ・ハーバーに関する十分性認定を無効と判断する判決を下した。この事態を受け、EUとアメリカは改めて交渉を行い、救済手段や監督の強化などを盛り込んだプライバシー・シールドを採択することとなった。

[15] クリストファー・クーナー氏は、Wilson Sonsini Goodrich & Rosati法律事務所の弁護士であるとともに、ブリュッセル自由大学教授等を務めている。専門は、プライバシー・データ保護法であり、International

Data Privacy Lawの編集代表を務めている。代表的な著書に、Transborder Data Flows and Data Privacy Law（Oxford University Press, 2013）などがある。クーナー弁護士に関する情報は、下記のウェブ・サイト参照。
https://www.wsgr.com/WSGR/DBIndex.aspx?SectionName=attorneys/BIOS/12684.htm
https://www.vub.ac.be/LSTS/members/kuner/

[16] 欧州委員会は、EUの主要機関の1つであり、法案提出やEU法の遵守監視等の責務を担っている。同委員会は複数の部局に分かれているが、データ保護のセクションは、司法・消費者総局の中の、基本的権利及びEUの市民権に関する部門に置かれており、GDPRの責任者はこのセクションに所属している。

[17] Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV.（Case C-40/17）, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CN0040.

[18] リンクレーターズ法律事務所の弁護士。リンクレーターズ法律事務所は、グローバルローファームであり、バンキング、M&A、金融、証券、企業再編等、幅広い業務を行っている。オーバーストラーテン氏は、リンクレーターズ法律事務所の弁護士であり、プライバシー・データ保護部門における、グローバルヘッドを務めている。オーバーストラーテン弁護士に関する情報は、下記のウェブ・サイト参照。
https://www.linklaters.com/ja-jp/find-a-lawyer/tanguy-van-overstraeten

[19] CNILの正式名称は、フランスの「情報処理及び自由に関する国家委員会」であり、「情報技術、データファイル及び市民的自由に関する1978年1月6日の法律第78-17号」の執行を担う独立監視機関である。EU加盟国の中では積極的な法執行を行うことで知られている。GDPRの適用開始により、1978年法は廃止され、CNILは新たにGDPRの法執行を担うこととなる。

[20] GIECBは、1984年に設立された経済利益団体である。各銀行のカードシステムを共通化し、国内のカード保持者がどこでも買い物ができるよう、普遍的な支払いを可能にするためのユニバーサルサービスを提供することを目的とする。加盟企業は約130社であり、国内でカード事業を行っている全ての事業者が対象となる。BNPなどの大手銀行が多い。

[21] https://www.cofrac.fr/.

[22] アイルランドの高等法院は、2017年10月3日、Facebookのデータが米国の監視機関と共有されることに対する不服申立がなされた事件について、欧州司法裁判所への付託決定を下している（http://www.europe-v-facebook.org/sh2/HCJ.pdf）。

[23] GDPRの実施法は、2018年5月14日に成立した。

[24] 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）（平成28年11月、平成29年3月一部改正）24頁。

[25] 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」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ&A（平成29年2月16日、平成29年5月30日更新）Q1-56、Q1-57、Q5-22。

[26] 個人情報保護委員会「日EU間の相互の円滑な個人データ移転を図る枠組み構築に係る最終合意」（2018年7月17日）（https://www.ppc.go.jp/news/press/2018/20180717/）。