《寄　稿》

クレジットカード情報とEUの個人データ保護法制

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、欧州連合（EU）のデータ保護法制における「個人データ」概念にクレジットカード番号が含まれるか否か、それが含まれる場合に、域内及び域外で適法に流通させられる根拠は何かを明らかにするとともに、EUの個人データ保護法制と日本の個人情報保護法の違いを明らかにすることにより、クレジットカード番号を含む決済データ（クレジットカード決済データ）を適切かつ円滑に流通させるための方策を検討した。

EU関係者に行ったインタビューによると、識別された、又は識別されうる自然人（データ主体）に関する全ての情報は「個人データ」であり、口座番号やデビットカード番号などと同様に、クレジットカード番号もその一つである、「同意」は限定的に解釈される、第三国移転のための例外規定は、大量・構造的・反復取引には適用できない、EUから個人データを受けるためには標準契約条項又は拘束的企業準則を用いる必要がある、等の点で一致した。

日本の個人情報保護法の2015年改正法のうち、「個人識別符号」にクレジットカード番号を含めるべきか否かが問題となり、現時点では含まれていない。しかし、仮に今後含まれることとなった場合には、クレジット決済を不可能にしてしまう危険がある。銀行口座番号等、他の金融・信用情報分野の事業者が取り扱う番号との平仄を合わせる必要がある。また、外国にある第三者への提供の制限及び第三者提供に係る記録の作成等についても、クレジットカード会社にとっては遵守に困難を伴うと考えられる。大量・構造的・反復的に決済データを移転し、データの移転先が随時変動するクレジットカード会社に適した規定及び解釈が求められる。

【目次】

Ⅰ．はじめに
Ⅱ．データ保護指令
Ⅲ．GDPR
Ⅳ．訪問調査結果
Ⅴ．日本の個人情報保護法
Ⅵ．クレジットカード情報の適切な流通に向けて

Ⅰ．はじめに

本稿では、欧州連合（European Union, EU）におけるクレジットカード番号の取扱いについて、1995年EUデータ保護指令（以下「データ保護指令」という。）[1]及び2016年EU一般データ保護規則（General Data Protection Regulation, GDPR）（以下「GDPR」という。）[2]の定める「個人データ」概念にクレジットカード番号が含まれるか否か、含まれる場合に、域内及び域外で適法に流通させられる根拠は何かを明らかにすること、並びにこうしたEUの個人データ保護法制と日本の個人情報の保護に関する法律（以下「個人情報保護法」という。）[3]の違いを明らかにすることにより、クレジットカード決済データを適切かつ円滑に流通させるための方策を検討することを目的とする。

本稿では、データ保護指令及びGDPRにおける「個人データ」の範囲、適法な取扱いのための要件、第三国等移転のためのソリューションを紹介し、2016年6月に行った訪問調査の概要を整理した。その上で、日本の個人情報保護法の内容及び解釈との比較を行い、クレジットカード業界にとって懸念されるであろう課題を論じ、その対応策を検討した。

Ⅱ．データ保護指令[4]

1.「個人データ」

データ保護指令は、「個人データ」を「識別された、又は、識別されうる自然人（データ主体）に関するすべての情報をいう；識別されうる自然人とは、とりわけ、個人識別番号、又は、その人の身体的、生理的、精神的、経済的、文化的、若しくは社会的アイデンティティに特有な1つ以上の要素を参照することよって、直接又は間接に識別することができる者をいう。」（第2条（a）号）と定義している。「個人データ」は、日本の個人情報保護法では「個人情報」に相当する。

前文（26）項は、識別性に関して、「保護の諸原則は、識別された又は識別されうる個人に関する全ての情報に適用されなければならないこと、個人が識別されうるか否かの決定には、取扱いに責任を負う者によってであれ、その他の者によってであれ、当該人物を識別するために合理的に用いられる見込みのある全ての手段を考慮すべきこと」[5]という考え方を示している。

2.「個人データ」概念に関する4/2007意見

「個人データ」の概念を分析したものには、データ保護指令に基づく第29条作業部会にお

いて、2007年6月20日に採択した「個人データ概念に関する4/2007意見（WP136）」[6]がある。

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では、第29条作業部会から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。

まず、WP136は、次の5つの一般的な考慮事項を掲げた。

①データ保護指令は、個人データ概念を広範に含んでいる。

②指令の定める諸原則の目的は、個人の保護にある。

③指令の適用範囲はいくつかの活動を適用除外し、関係する状況への適切な法的対応を提供するために法文の中に柔軟性を組み込んでいる。

④データ保護諸原則の範囲は過度に広範とすべきではない。

⑤しかし、個人データ概念の解釈を不当に制限することもまた、回避すべきである。

次に、WP136は、「個人データ」の定義について、19の事例を交えながら、「あらゆる情報」（any information）、「関連する」（relating to）、「識別された又は識別可能な」（an identified or identifiable）、「自然人」（natural person）という4つの要件に基づき整理を行った。特に紙面が割かれたのは、「識別された又は識別可能な」という要件であり、WP136の中では、次のような説明がなされている。

一般用語では、人の集団の中で、その人物が集団の他の全ての構成員から「区別された」（distinguished）ときに、自然人が「識別された」とみなされうる。したがって、その人物がまだ識別されていなかったとしても、それが可能なときに（これが「できる」という接尾辞の意味である）、当該自然人は「識別されうる」。後者は、この要件を決定づける境界となる。識別性は、通常、「識別子」と呼ばれる特定の情報を通じて達成される。データ保護指令第2条の「個人データ」も識別子に言及している。

「直接的」又は「間接的」な識別可能性は、特定の状況に依拠する。非常に一般的な名字は、教室内の生徒を識別するには十分となりうるが、誰かを識別する一国の人口全体から誰かを選び出す（single out）には十分ではない。「黒いスーツを着た男性」のような付属的情報ですら、信号で立っている通行人から誰かを識別できるかもしれない。

「直接的」について、人の氏名が最も共通の識別子である。

「間接的」について、この類型は、「固有の組み合わせ」（unique combinations）と関係する。一見したところでは、利用可能な識別子の範囲では特定人物を選び出せない場合でも、他の

情報（データ管理者が保有するか否かを問わない）と組み合わせることによって、他者と区別され、その人物を「識別できる」可能性がある。

氏名自体は、必ずしも全ての場合に個人を識別するわけではない点に注意すべきである。個人データを登録したコンピュータファイルは、ファイル内の2人の人物の混同を避けるため、登録された人に固有の識別子を割り当てることが通常である。ウェブ通信量監視ツールによって、機械の行動及び機械の背後にいる利用者の行動を識別することが容易となる。個人に氏名や住所を聞かなくとも、社会経済的、心理学的、哲学的又は他の基準によって、この人物を類型化し、ある決定をその人物に帰属させることは可能である。なぜなら、その個人の連絡先（コンピュータ）は、その人物の身元を開示することを必ずしも求めていないことからである。個人を識別する可能性は、その人物の氏名を見つける能力を必ずしも意味しない。個人データの定義は、この事実を反映している。

識別手段について、データ保護指令前文第（26）項は、「個人が識別されうるか否かの決定には、管理者や他のあらゆる者が、当該者を識別するために合理的に実施することが見込まれるあらゆる手段を考慮すべき」[7]と読む際に、「識別可能性」に特に留意している。仮説的に個人を選び出す可能性があるだけでは不十分である。「管理者…あらゆる手段」という上記基準は、問題となる全ての要素を考慮に入れるべきである。識別を行う費用のみならず、目的、取扱方法、管理者が期待する利点、懸念される個人の利益、組織の機能不全（守秘義務違反等）、及び技術的失敗を全て考慮に入れるべきである。他方、この審査は動的なものであり、取扱時点の最新技術及びデータが取り扱われる期間の開発可能性を考慮すべきである。

識別性に関する例に、IP（Internet Protocol）アドレスを挙げることができる。IPアドレスは個人データとなる場合とならない場合があるが、ISP（Internet Service Provider）は、問題のIPアドレスが個人識別性を有するか否かを通常は知ることができず、IPアドレスに結びつくデータを同様に処理することから、ISPにおいて、絶対的な確信をもって、識別可能ではない利用者に対応したデータを区別する立場にある場合を除き、全てのIP情報は、安全を取って、個人データとして取り扱う必要がある。

3. 適法な取扱いのための基準

データ保護指令第2節は、「適法なデータの取扱いの基準」（第7条）を定めている。これは、同指令第6条1項が「加盟国は、個人データが次の条件を満たすように定めなければならない。」と定め、その条件の1つに「(a) 公正かつ適法に取り扱われること」を挙げたことを受けている。すなわち、データ管理者は、第6条に基づき個人データを適法に取り扱わなければならず、そのために第7条の要件を満たす必要がある。

なお、「データ管理者」とは、単独で又は他と共同して、個人データの取扱いの目的及び手段を決定する自然人、法人、公的機関、機関又はその他の団体をいう（第2条（d）号）。個人データの「取扱い」とは、「自動的な手段であるか否かにかかわらず、個人データに対して行われる作業又は一連の作業をいう。この作業とは、収集、記録、編集、蓄積、修正又は変更、復旧、参照、利用、移転による開示、周知又はその他周知を可能なものとすること、整列又は結合、ブロック、消去又は破壊することをいう」（第2条（b）号）。日本の個人情報保護法と比較すると、「データ管理者」は、個人情報取扱事業者及び行政機関等が相当し、「取扱い」は、利用や提供よりもはるかに広い範囲をカバーする。

「第7条

加盟国は、次の条件を満たす場合にのみ、個人データが取り扱われるように定めなければならない。

（a）データ主体が明確に同意を与えた場合、又は

（b）データ主体が当事者となっている契約の履行のために取扱いが必要な場合、又はデータ主体の請求により、契約の締結前に、その段階を踏むために取扱いが必要な場合、又は

（c）～（e）省略

（f）管理者又はデータの開示を受ける第三者若しくは当事者の適法な利益のために取扱いが必要な場合。ただし、これらの利益より、第1条第1項の規定に基づいて保護が必要とされるデータ主体の基本的な権利及び自由に関する利益が優先する場合には、この限りではない。」

（a）号の「同意」について、データ保護指令は、「データ主体が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ことによって、自由になされた特定のかつ十分に情報を提供された上での意思表示をいう。」（第2条（h）号）と定めている。

適法な取扱いのための基準は、下記の第三国移転の例外規定と類似するが、全く別の規定である。本条は、「域内」「域外」の区別なく、データ管理者に該当する者が個人データを取り扱う場合に適用される。

4. 第三国移転

4.1 第三国移転制限とその例外

データ保護指令は、EUの28加盟国及び欧州経済地域（European Economic Area, EEA）の3ヶ国[8]から第三国に対する個人データを移転するための要件として、第25条の原則及び第

26条の例外に関する定めを設けている。第三国移転制限を設けたことで世界的に有名になったのは、第25条の「十分なレベルの保護措置」の定めである。同条1項は、「加盟国は、取り扱われている又は移転後の取扱いが意図されている個人データの第三国への移転は、本指令の他の規定に従って採択された国内規定の遵守を侵すことなく、当該第三国が十分なレベルの保護措置を確保している場合に限って、行うことができることを定めなければならない。」と規定している。

第25条の原則に対し、第26条は、次の通り、十分な保護レベルを保障していない第三国に対する個人データの移転を認めるための特例を定めている[9]。

「第26条　例外

1　加盟国は、第25条の例外として及び特別な場合を規律する国内法に別段の定めがある場合を除き、第25条2項の意味における十分な保護レベルを保障しない第三国に対する個人データの移転又は一群の移転は、次に掲げる条件を満たした場合に行うことができることを定めなければならない。

（a）データ主体が、予定されている移転に対して明確な同意を与えている場合、又は

（b）移転が、データ主体及び管理者間の契約の履行のために、又はデータ主体の請求により、契約締結前の措置の実施のために必要である場合、又は

（c）移転が、データ主体の利益のために、管理者及び第三者間で結ばれる契約の締結又は履行のために必要である場合、又は

（d）～（f）省略

2　加盟国は、1項の規定を損なうことなく、管理者が個人のプライバシー並びに基本的な権利及び自由の保護、また、これらに相当する権利の行使に関して、十分な安全保護措置を示す場合、第25条2項の意味における十分な保護レベルを保障しない第三国への個人データの移転又は一群の移転を許可することができる。このような保護措置は、特に適切な契約条項から帰結することができる。

3　省略

4　欧州委員会が、第31条2項に定めた手続に従い、一定の標準契約条項が、本条第2項によって要求される十分な安全保護措置を提供していると決定する場合、加盟国は、委員会の決定を遵守するために必要な措置を講じなければならない。」

第26条1項（a）号及び（b）号は、第7条（a）号及び（b）号と、第26条1項（c）号は第7条（f）号と文言上類似しているが、各規定は別々に適用される。

後述するインタビュー結果にも登場する重要な仕組みとして、標準契約条項（Standard Contract Clauses, SCC）と拘束的企業準則（Binding Corporate Rules, BCR）がある。これらはGDPRにも取り入れられている。

SCCは、第26条2項及び4項に基づく仕組みであり、十分性の認定を受けていない第三国がこの方法を用いることにより、適法にデータ移転を受けることが可能となる[10]。欧州委員会は、①EU内で設立された管理者からEU外で設立された管理者への移転に関するSCCと、②EU 内で設立された管理者からEU外で設立された取扱者への移転に関するSCCの決定文書を公表している。

①に関する文書は、「95/46/EC指令に基づく第三国への個人データ移転のための標準契約条項に関する2001年6月15日の2001/497/EC委員会決定」[11]、「第三国への個人データ移転のため一群の代替的標準契約条項の導入に関して、2001/497/EC 決定を改正する2004年12月27日の委員会決定」[12]がある。②に関しては、「第三国で設置された取扱者に対する個人データ移転のための標準契約条項に関する、欧州議会及び理事会の95/46/EC指令に基づく2010年2月5日の2010/87/EU委員会決定」[13]がある。②は、個人データの外部委託にも用いられる。

BCRは、主に多国籍企業を対象としており、監督機関により法的に執行可能であること、法令遵守を運用するなど実践的であること等に留意した「国際データ流通に対する拘束的企業準則」を策定し、EU内の監督機関が当該ルールを承認した場合には、多国籍企業間でのデータ流通が認められるという仕組みをいう。SCCは契約に基づく仕組みであるのに対して、BCRは、次のような点にメリットがあるといわれている[14]。

・BCRが対象とするグループ内の全てのデータ流通に対して、データ保護指令第25条及び第26条で述べた原則を遵守させることができる。
・グループ内の個人データ保護関連の実務を統一させる。
・第三国へのデータ移転から生じるリスクを防ぐ。
・移転の度に契約を交わす必要を避ける。
・企業のデータ保護政策を外部に発信する。
・個人データ管理に関して、従業員への内部指針を備える。
・企業が事業を展開する上で、データ保護を欠かせないものにする。

BCRは、第26条2項を根拠としており、第29条作業部会が一連の文書を公表している。

BCRを申請しようとする企業グループは、①適用範囲、②定義、③目的の制限、④データ内容及び均衡性、⑤個人データの取扱いの法的根拠等を含む22項目について、誓約ないしは

説明を行わなければならない。

BCRの申請は、(1) 主管の監督機関の指定、(2) 申請文書の作成・当該監督機関への提出、(3) 監督機関による協力手続の開始、(4) 相互認証参加国がBCRを受領すること等による協力手続の終結、(5) 各国の監督機関が採用したBCRに基づく移転の許可申請という段階を踏んで行われる。

2017年2月2日現在、BCRの手続を完了させた企業は80社を超えており、主管の監督機関は、フランス、英国、オランダが多数を占めている。日本企業では、2016年12月24日、楽天グループがルクセンブルクの監督機関からBCRの承認を受けている[15]。日本企業としては初めての承認である。

4.2 第三国移転制限に関する第29条作業部会意見

上記の文書とは別に、第29条作業部会文書の中には、クレジットカード情報の取扱いに関する事柄を述べた文書が2つ存在する。それらは、「第三国への個人データ移転：EUデータ保護指令第25条及び第26条の適用」[16]と題する作業文書（1998年7月24日採択）、及び、「指令第26条（1）項の共通解釈に関する作業文書」[17]（2005年11月25日採択）である。文書番号に基づき、前者はWP12、後者はWP114と称することとする。各該当部分を訳出すると次の通りである。

［WP12］

1995年データ保護指令第26条1項（b）号及び同項（c）号に付される条件にもかかわらず、これらの例外は影響を有する。例えば、乗客のための航空券予約に必要な個人データ移転、国際的な銀行の業務やクレジットカード決済に必要なデータ移転に、度々適用できる可能性が高い。実際のところ、「データ主体の利益のため」の契約の例外（第26条1項（c）号）は、特に、銀行口座決済の受益者に関するデータの移転を含む。受益者は、データ主体であるが、移転を行う管理者との契約を締結する当事者でない場合が多いであろう[18]。

［WP 114］

第29条作業部会は、反復的、大量又は構造的なものと認められ得る個人データの移転は、可能であれば、また、正確にはそれらが重要な性質を持つことを理由に、特定の法的枠組（すなわち、契約又はBCR等）の範囲内で、実行されるべきであると勧告する。

他方で、同作業部会は、大量又は反復的な移転が、第26条第1項に基づき適法に実施され得ることを認めている。それは、かかる法的枠組への依拠が実際には不可能である場合、データ主体へのリスクが小さく、かつ、第6条から第8条が適切に適用されている場合である。1つの関連する例として、例えば、いまだに日々大規模に行われている国際的な貨幣の移転

による例を挙げることができる[19]。

Ⅲ．GDPR[20]

1.「個人データ」

GDPRは、2012年1月25日の欧州委員会提案から4年以上が経過した2016年4月27日、一般データ保護規則として調印され、同規則は、同年5月4日、EU官報に掲載された。これは、デジタル時代における市民の基本的権利を強化するとともに、デジタル単一市場で規律を単一化することにより企業の事業を促進させるためのEUのデータ保護法改正である。

GDPRの「個人データ」は、「識別され又は識別され得る自然人（「データ主体」）に関連するあらゆる情報をいう。識別され得る自然人とは、とりわけ、氏名、識別番号、位置データ、オンライン識別子などの識別子、又は当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、若しくは社会的アイデンティティに特有な1つ以上の要素を参照することよって、直接又は間接に識別され得る者をいう。」と定義されている（第4条（1）項）。範囲については、データ保護指令と基本的な内容に変更はない。

前文では、識別性及び識別可能性について、概ね次のように説明されている。

自然人を識別し得るか否かを決定するためには、管理者又は他者のいずれかが自然人を直接又は間接に識別するために、例えば選別（singling out）するなど、合理的に利用する可能性の高い全ての手段を考慮に入れるべきである。かかる可能性を確認するためには、取扱いの時点で利用できる技術及び技術的発展を考慮に入れ、識別に要する費用及び総時間など、全ての客観的要素を考慮に入れるべきである。そのため、データ保護諸原則は、匿名情報、特に、識別され又は識別し得る自然人に関係しない情報や、データ主体をもはや識別できない態様に匿名化した個人データには適用すべきではない。したがって、本規則は、統計又は研究目的を含め、かかる匿名情報の取扱いには関係しない（前文（26）項）。

識別可能性の判断及び匿名化データに諸原則が適用されないことに関しては,データ保護指令の前文（26）項にも同旨の説明がある。そのため、識別性の解釈は、第29条作業部会の考え方と同様であると見ることができる。

GDPRの「個人データ」の識別子の例には、氏名、位置データ、オンライン識別子が追加された。オンライン識別子には、IPアドレス、クッキー識別子又はRFIDタグなどがある。自然人は、デバイス、アプリケーション、ツール及びプロトコルから提供されるオンライン識別子と関連付けられ得る。このことは、履歴を残し、特に、固有識別子及びサーバから受け取る他の情報と結びついた時に、自然人のプロフィールを作り出し、彼らを識別するために

利用することができる（前文（30）項）。

2. 適法な取扱いのための基準

GDPR第6条は、「取扱いの適法性」を定めている。データ保護指令と同様、第5条1項は「個人データは、次に掲げる事項を満たさなければならない。」と定め、その（a）号は「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（「適法性、公正性及び透明性」）。」と規定している。第6条はその適法性を満たすための要件を明らかにしたものである。

「第6条　取扱いの適法性

1　取扱いは、次に掲げる少なくとも1つの項目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）～（e）省略

（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。」

EUでは「同意」は非常に厳格に解釈されており、データ保護指令において、「特定の」「情報を与えられた」「自由な」という要件を満たすことが求められてきた。そのため、標準的な契約を事業者ないしは雇用者等があらかじめ用意しており、消費者ないしは従業員側に選択の余地がない場合や、約款の中に同意条項が含まれるような場合には、同意の要件を満たすことは困難である。また、同意は項目を列挙する形で個別に付与することが必要であり、包括的な同意は認められない。

GDPRでは、「データ主体の同意」は、「自由になされた、特定の、十分に情報を提供された、かつ、明示的な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。」と定められている（第4条（11）号）。データ保護指令と比較すると、「自由」、「特定」、

「十分に情報を提供された」という要件に加え、「明示的な同意」が明文化された点で厳格化された。

第6条1項各号のうち、(f) 号は次のように説明されている。

(f) 号は、データ主体が管理者の顧客である場合等、データ主体と管理者間に適切な関係がある場合に存在する。データ主体が、個人データ収集時とその状況において、当該目的のための取扱いが行われ得ることを合理的に予測できるか否かを含め、適法な利益の存在は慎重に評価すべきである。データ主体がさらなる取扱いを合理的に予測しない場合には、データ主体の利益及び基本的権利が優越する。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（前文（47）項)。管理者又は第三者が追求する適法な利益は、営利目的の場合にも認められる[21]。

第7条は「同意の条件」を定めている。これは、データ保護指令には存在しなかった新設規定である。

「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、サービス約款を含め、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。」

GDPR第7条は、「同意の条件」として、管理者の証明責任（1項)、文書上の同意付与の際に他の事項と区別し、データ主体が理解しやすい態様で同意を要請すること（2項)、データ主体の将来に向けた同意撤回権（3項)、同意の任意性を判断する際に、契約履行に同意を条件づけているか否かを確認すること（4項）を定めている。

前文は、同意について紙幅を割いて説明を行っている。

2項について、管理者が事前に策定した同意の宣言は、理事会指令93/13/EEC[22]に従い、明確かつ平易な言語を用いて、理解しやすく容易に入手できる形式で与えられるべきであり、不公正な文言を含むべきではない。十分に情報を与えられた同意を行うために、データ主体は、少なくとも管理者の身元及び意図した個人データの取扱目的を認識すべきである。同意は、データ主体が本心からの自由な選択を行っておらず、又は同意の拒否や撤回ができない場合は、自由に与えられたものとみなすべきではない（前文（42）項)。

上記の理事会指令では、個々に交渉されておらず、当事者間の権利義務に重大な不均衡をもたらすような契約条件である場合や、事前に起草された標準契約などで、消費者が条件内容に影響を与えることができない場合は、不公正とみなされることなどが定められている。

続いて、前文は、自由な同意付与に関して、次のように説明している。

データ主体と管理者間に明確な不均衡がある場合、特に、管理者が公的機関であるために,特別の状況で同意を自由に与えた可能性が低い場合には、個人データを取り扱うための有効な法的根拠とすべきではない。また、同意は、もし個別に行うことが適切であるにもかかわらず、別の個人データ取扱業務で個別の同意を認めない場合、又はサービス提供を含む契約履行の場合に、当該同意がかかる履行に必要でないにもかかわらず、同意に依拠する場合には、自由に与えられなかったとみなされる（前文（43）項)。

3. 第三国等移転

国際データ移転の全体的な構成として、データ保護指令では、同指令第25条で原則、同指令第26条で例外を定めるというシンプルな枠組みであったが、GDPRでは、データ保護移転を行うための三段階の規律が設けられた。

第1に、原則として、欧州委員会が十分な保護レベルを決定することにより、第三国等へのデータ移転が認められる（第45条)。GDPRでは、十分な保護レベルの決定対象に、地域、取扱部門、又は国際機関が含まれること、第三国又は国際機関から他の第三国又は国際機関への転送が含まれることが明らかにされた。

第2に、欧州委員会が十分性の決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、BCRや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、SCC）が含まれる。BCRは、第47条「拘束的企業準則」の中で詳細に定められている。

さらに、GDPRは、第3段階として、欧州委員会の十分性決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「特定の状況による例外」に基づき、第三国等へのデータ移転を認める旨の規定を設けた。

1） 原則

第45条は、「十分性決定に基づく移転」を定めており、これは、データ保護指令第25条を受けた規定である。1項は、「1　第三国又は国際機関への移転は、第三国、当該第三国における地域若しくは一つ以上の取扱部門、又は当該国際機関において、十分なレベルの保護措置を確保していると欧州委員会が決定した場合に行うことができる。当該移転は、さらなる個別の許可を要求してはならない。」と定めており、2項は保護レベルの十分性を評価する際の要素、3項は欧州委員会の十分性決定の採択手続及びその後の見直し、4項は十分性決定後の継続監視、5項は欧州委員会による十分性決定の将来的取消等、6項は十分性決定取消後の協議を定めている。

2） 適切な安全保護措置

①　第46条

第46条は「適切な安全保護措置による移転」を定める。十分性決定が得られていない場合における、第2段階の移転手段である。この手段は、監督機関の許可を要しないものと要するものに分けられる。

1項の定めは次の通りである。

「1　第45条3項に基づく決定が下されていない場合、管理者又は取扱者は、適切な安全保護措置であって、執行可能なデータ主体の権利及びデータ主体のための効果的な法的救済を利用できるという条件に基づくものを提供した場合に限り、第三国又は国際機関に個人データを移転することができる。」

2項は、移転手段として、拘束力ある執行可能な取決め、BCR、標準データ保護条項、行動規範、認証制度を認めている。これらは監督機関の許可を必要としない。執行可能な権利行使及び効果的な法的救済が重要視されている（前文（108）項参照）。

標準データ保護条項については、管理者又は取扱者において、欧州委員会又は監督機関が採択した標準的なデータ保護条項を用いる場合、取扱者と他の取扱者間の契約のように、より広い契約の中に標準的なデータ保護条項を含めることを防止すべきではない。また、欧州委員会又は監督機関が採択した標準契約条項と直接又は間接に矛盾せず、又は、データ主体の基本的権利又は自由を侵さない場合に、他の規定又は保護措置を追加することも防止すべきではない。管理者又は取扱者は、標準保護条項を補足する契約上の取決めを通じて、追加的保護措置を提供するよう奨励されるべきである（前文（109）項）。

3項は、管理者若しくは取扱者と、第三国若しくは国際機関の管理者、取扱者若しくは個人データ受領者の間における契約条項など、監督機関の許可を条件に移転を認める方法を定

める。

② 第47条

GDPRは、第47条においてBCRを明文化している。1項の定めは次の通りである。

「第47条 拘束的企業準則

1 所管の監督機関は、次に掲げる場合、第63条に定める一貫性の仕組みに従い拘束的企業準則を承認しなければならない。

(a) 法的拘束力があり、従業員を含め、企業グループ又は共同経済活動に従事する事業グループに関連する全てのメンバーに適用され、遵守されている、

(b) 自己の個人データの取扱いに関して、データ主体に対して執行可能な権利を明示的に与えている。及び、

(c) 2項に定める義務を満たしている。」

2項は、1項(c)号に基づき、BCRを得るための要件が掲げられている。要件は多岐にわたっているが、要約すると、(a) 企業グループ等に関する構成及び連絡先、(b) 第三国移転に関する情報、(c) 内外での法的拘束力、(d) データ保護諸原則の適用、(e) データ主体の権利及び法的救済、(f) EU外のメンバーがBCRに違反した場合における、加盟国上の管理者又は取扱者の責任、(g) データ主体への情報提供方法、(h) データ保護責任者等の任務、(i) 苦情申立手続、(j) データ保護監査等を含むBCRの遵守確認、(k) 規則変更の報告及び記録、(l) 監督機関との協力、(m) 第三国にある企業グループ等が服する法的義務であって、BCRの保障に実質的な悪影響を及ぼす可能性が高いものを所管の監督機関に報告する仕組み、(n) 職員へのデータ保護訓練である。

3) 特定の状況による例外

第49条は、「特定の状況による例外」を定める。これは第3段階の移転方法であるが、「特定の状況」というように限定されており、1項の文言にも「のみ」と定められている点に注意しなければならない。本条は、大量、構造的、反復的な移転には適用されないと解釈されているため、クレジットカード決済データの流通に適用することは困難といわざるを得ない。

「第49条は 特定の状況による例外

1 第45条3項に定める十分性決定がなされていない場合、又は、拘束的企業準則を含め、第

46条に基づく適切な安全保護措置がない場合、第三国又は国際機関への個人データの移転又は一群の移転は、次に掲げる条件の1つを満たしている場合にのみ行われなければならない。

(a) 十分性決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、

(d) ～ (g) 省略。」

Ⅳ. 訪問調査結果

GDPRの採択により、2018年5月25日の適用開始日からは、加盟国にもGDPRが直接適用される。そのため、データ保護指令に基づく加盟国の国内法は、一部を除いてGDPRに置き換えられるが、同指令に基づく従前の考え方を把握しておくことは、GDPRの解釈を行う上でも重要である。そこで、本節では、2016年6月に筆者が訪問調査を行い、「個人データ」の範囲、適法な取扱いの基準、第三国移転のためのソリューション、WP12及びWP114に関する立場について、各国の監督機関、業界団体、業界の弁護士より聴取した内容を整理した。

なお、クレジットカード事業者がEUのデータ保護法制においていかなる立場に立つかという点は、その企業のビジネスモデルによって異なる。これは、「管理者」(controller) ないしは「取扱者」[23] (processor) となるのは誰か、という論点である。「管理者」とは、個人データの取扱いの目的及び手段を決定する者、「取扱者」とは、管理者のために個人データを取り扱う者をいう。関係者からは、クレジット兼デビットカードの発行者である銀行が管理者になる場合、クレジットカード会社が管理者になる場合、イシュア銀行から委託を受けて個人データを取り扱うため、クレジットカード会社は「管理者」ではなく「取扱者」になる場合についての説明があった。

1. 欧州委員会司法・消費者総局[24]

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、データ保護部門は、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の責任者はこの部門

に所属している。

1） 同意

データ保護指令の段階では、加盟国が指令を国内法化する時に黙示的同意を許容する場合もあり、各国の運用に委ねられてきた。健康情報などのセンシティブ・データは明示的な同意が必要とされる。クレジットカード番号は、センシティブ・データには含まれないため、一般の個人データと同様に扱われる。

誤解しないよう注意すべきことは、GDPRでは同意は全て明示的同意になり、不明確さをなくした点である。

2）「個人データ」

識別可能性は状況による。

多くの場合は、クレジットカード番号は他の情報と結び付いて取り扱われるため、間接的な識別性があり、時には直接的な識別性を持つこともある。

3） 適法な取扱い、第三国移転

管理者は、取扱い全般について法の遵守が必要であり、適法性の根拠が常に求められる（同意や契約はその1つ）。

第三国移転を行うためにはそのための手段が必要であり、まず第1には十分性、第2は適法な安全保護（BCRや標準契約条項など）、第3が例外規定である。第3は最後の手段にすべきであり、第3に含まれる個別の契約や同意は、第2の手段よりも保護レベルが下がる。

4） WP12、WP114

WP12の説明は、カード発行者と加盟店管理会社であるアクワイアラ銀行が契約当事者で、データ主体が受益者となる場合など、クレジットカード取引にも当てはまる。

WP114の解釈は疑問がある。2015年10月6日に欧州司法裁判所が下したセーフ・ハーバー無効判決（以下、当事者の名前を取って「シュレムス判決」という。）[25]により、大量流通が繰り返される事案で、米国とEU間で締結していたセーフ・ハーバーが無効になった[26]。大量の移転には適切な保護措置が必要である。判決が出ると解釈も変更され得る。

事案により判断されるが、データ移転の例外（指令第26条、GDPR49条）の解釈は、厳格に行われる。2013年のコミュニケーションペーパーがある[27]。

2. フランス（CNIL）

フランスでは、情報処理及び自由に関する国家委員会（Commission Nationale de l'Informatique et des Libertés, CNIL）[28]に訪問した。同委員会は、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[29]の執行を担う独立監視機関である。

1） 情報技術、データファイル及び市民的自由に関する1978年法

「個人データ」の定義は第2条、第7条は個人データの適法な取扱いのための条件、第69条は第三国移転制限の例外を定めている。いずれもデータ保護指令に沿った内容である。

2） 解釈

① 識別番号について

フランスの法律の中で、識別番号として特別な規定による保護が必要なのは、国民全てが持っている社会保障番号（Numéro d'Identification au Répertoire, NIR）である。それ以外のクレジットカード番号、銀行カード番号などは、民間事業者が保有している番号であり、NIRほど重要な識別番号とは考えられていない。しかし、銀行カード番号についても個人データとして保護対象となっている。

クレジットカード番号、銀行カード番号、デビットカード番号の間の保護レベルの差はない。クレジットカード番号は裏面のセキュリティ番号が保持者を特定するため、追加的保護が必要とされているが、CNILの保護ではなく、PCIDSS（Payment Card Industry Data Security Standard）の規格に基づくものである。

個人データに該当するか否かは、法律に定めがあり、CNILのような監督機関がそれを解釈する。データを取り扱う事業者の（判断の）自由はない。

② 適法な取扱い、第三国移転

a. 適法な取扱い

前提として、クレジットカード等を使った決済システムの説明をすると、まず、イシュア銀行（カード発行会社）からカードの発行を受けた保持者が買い物をした時に、加盟店が取引をしているアクワイアラ銀行（加盟店管理会社）と、イシュア銀行の間で、銀行間取引が行われるシステムがある（補填を行うシステム）。フランスの特徴は、銀行間取引が経済利益団体（Groupements des cartes bancaires, CB）によって管理されていることである。フランス国外の場合はVisaやMastercardなどの国際ブランド会社が管理する。

フランス人のカード保持者（データ主体）が日本でクレジットカード決済をした場合、決

済データが日本からフランスのアクワイアラ銀行に伝送される場合の情報流通は、VisaやMastercardなどが持つ国際ブランド会社の決済システムによる。EU域内で活動基盤を有している場合は欧州法が適用される（がそれ以外は適用されない）。フランスにはCBがあるため、CNILからの個々のカード会社へのアプローチは薄い。

適法な取扱いを保障する根拠として、「データ主体の同意」と「データ主体が当事者である契約を履行するため」が考えられるが、1つ1つの取引への同意取得は現実問題として困難であるため、データ主体が当事者となっているクレジットカード等の契約を結んでいれば、適法な取扱いの条件を満たすことは可能である。

b.　第三国移転

日本の観光客がフランスで一時的にデビットカードやクレジットカードを使った際に、日本の観光客のイシュア銀行やクレジットカード会社とフランスの加盟店のアクワイアラ銀行との間の取引になる。これは明らかな国際的なデータ移転に該当する。法的には整備できていないことを認めなければならない。電子決済の場合、CBとの間にはこのようなスキームはあったが、カバーできていない。第29条作業部会の会議でもCNILはポジションを明確にしていない。

ネット販売であれ国際的な電子決済システムであれ、データ移転があることはあまり認識されてこなかった。EUの中で潜在的に個人データの移転ではないかという議論はあったが、今までは地球のどこにいても、イシュア銀行とアクワイアラ銀行との間の補填だけで、データの移転はないと考えられていた。SWIFTコードのようなものが登場したため、個人データの移転であることが認識されてきたので、管理するための法的なスキームが必要になっている。今はその問題に直面しているところである。

データ保護指令の第25条、1978年法の第69条で、例外規定を設けている。しかし、移転が構造的、大量、反復的な性格を持っている場合には、適用されない。クレジットカードやデビットカードを用いた取引は、構造的であり、大量であり、反復的であるため、例外規定を適用することはできない。これは欧州全体の統一的な解釈であり、法文で定めているわけではない。例外規定を濫用されないようにするためである。

1978年法の第7条と第69条の違いについて、第69条は移転を可能にする条文であり、第7条とは対象が異なる。第69条は、大量構造的反復的取引には適用されない。第1段階は十分性があるか否か、第2段階は、定型条項（セーフ・ハーバーやBCR）であり、第3段階はさらなる下層レベルとして、例外規定の有無を見る。例外規定をどうしても適用しなければならないのは、例えば一時的にデータ主体が国外にいる場合や、特定の国際協力条約がある場合

などがある。

国際的な資金決済は法的な意味で「個人データ移転」に該当する（支払う側と許可する側）。法的な根拠が明確でない状態で取引が行われている状況では、日本に個人データを移転したフランス側のアクワイアラ銀行の責任になる。データを受け取った日本のイシュア銀行やクレジットカード会社の責任は、今のところはない。第29条作業部会のファイナンシャルマターズの中でもWP12、WP114はあまり認識されて来なかった。確かに日本の銀行やクレジットカード会社にとっては不安になると思われる。今後検討するテーマだと思う。

フランスから日本に電話をかける時ですらデータ移転は発生しているため、それをあえてブロックしないのと同じように、CNILは経済活動や人の移動を法的な理由で止めることはできないと思う。

3） WP12、WP114

第29条作業部会の文書の拘束力を確認したところ、参考にするものでしかなく、拘束力はないとの意見と、それに対して拘束力がないとは言い切れないという意見に分かれた。後者は、監督機関同士で決めた立場であるため、制約的なものではあるという立場である。回答は次の通りである。

WP12は一時的なものであり、銀行の振込みを主な対象としており、国外で出身国にいる家族に一時的な送金をするような場合を想定している。1998年当時の解釈はこれで良いが、今の適用性については懐疑的にならざるを得ない。現在の解釈にはそぐわず、より厳しくなっている。

実務的に資金の発端となっているところ（支払う側）とそれを受け取る側の移転を管理しようとするのは困難であるため、それをあえて行ってこなかったのだろうと思う。これまでは単なる資金フローがあるだけだと思われてきたので、移転に対する要求度が低かった。2011年のテロ事件以降は懸念が出てきている。元々銀行は当局の操業許可を得て開業されているために信頼されており、様々な監査も受けているので安心だと考えられてきた（クレジットカード会社を含む金融機関に同じ義務が課せられている）。

3. フランス（Groupements des cartes bancaires, CB）

経済利益団体であるCBへの訪問調査結果は次の通りである。

1）「個人データ」

クレジットカード番号やデビットカード番号について、フランスの法令は区別していない。

1980年OECDプライバシー・ガイドライン、データ保護指令、欧州評議会第108号条約[30]も区別していない。クレジットやデビットカード番号が直接間接に1人の個人を特定できる場合には、個人データに該当する。「識別番号」に該当するか否かではなく、個人を識別できるか否かによるが、クレジットやデビットカードの場合は間接的に個人を識別できるため、個人データに該当する。

2） 適法な取扱い

クレジットやデビットカードの発行者に関して、CBは国内の事業者を加盟社としており、同意を得ることで適法に流通させられる。国外についてはVisaやMastercardなどの国際ブランド企業が対応しているが、CBの対象事業者ではない。国外（特にアメリカ）にデータを出す場合は、CNILの許可が必要である。セーフ・ハーバー無効判決によって無法地帯となっており、CNILの許可が必要ではあるものの、実態がそれに追いついていない。

3） 国内外流通

CBのひな型には、国内外で流通させるための規定が入っており、契約上の規定が国内外の流通を適法に行うための法的根拠となっている。

4. ベルギー（CPP）

ベルギーでは、プライバシー保護委員会（Commission for the Protection of Privacy, CPP）[31]に訪問した。同委員会は、1992年プライバシー法（1992年12月8日付個人データの取扱いに関するプライバシー保護についての法律）[32]に基づき設置された独立監視機関である。

1） 1992年プライバシー保護法

1992年法は、第1条1項に「個人データ」の定義を置き、第5条で取扱いの適法性の要件を定め、第22条で第三国移転制限の例外規定を置いている。いずれもデータ保護条項に沿った内容である。

2） 解釈

① 個人データ

クレジットカード（又は口座）番号は、1992年法に基づく（固有の）識別番号に該当し、個々の自然人と関係し得る情報を含む。データ保護指令の考え（第29条部会のWP136）をよく参照している。同指令の「個人データ」概念は広い。

個人識別性は、クレジットカード番号が「識別番号」に該当するか否かにとどまらず、「自然人」と「関係する」か否かが重要である。クレジットカード番号は、オンラインでクレジットカードを用いた場合など、自然人と「関係する」ことから、ベルギーのデータ保護法の対象となる。類似の考えは、第29条作業部会のWP136の中でも、「人の集団の中で、その人物が集団の他の全ての構成員から「区別された」ときに、自然人が「識別された」とみなされうる」ことが記されている[33]。

そのため、概念の法的解釈に加え、客観的（統計的）分析により、固有識別番号、氏名又は住所のないデータであっても、人を識別し得る可能性（リスク）が何であるかを算出することもできる。特に重要であるのは、個人の自然人を「選び出す」ための固有識別番号の能力である。銀行口座番号、デビットカード番号、顧客番号等も個人を固有の識別番号である。

個人識別のための第1のアプローチに、直接の識別番号がある。ベルギー人には個々の識別番号が付与されており、生年月日、性別等と組み合わせられて個人を識別する[34]。その番号がなければ行政機関は個人を識別できない。

第2のアプローチは、他の情報との組み合わせによって個人を識別できる場合である[35]。クレジットカード番号を用いて個人を識別するにはさらなる情報が必要であり、それらの情報との組み合わせで、個人データの取扱いを行っているという結論に至る。クレジットカード番号と他の固有番号によって、非常に簡単に個人を識別することができる。ほとんどの場合に、個人に紐付く固有番号があれば、「個人データの取扱い」に当たる。

識別可能性は状況に依存する。個人と紐付くためにどの程度の変数があり、どの程度の要素があるかによる。IPアドレスには固定と変動型があるが、固定型のIPを自然人が使っていれば、容易に「個人データの取扱い」であるということができる。変動型は、グレーゾーンがあり、議論がある（欧州司法裁判所にかかっている案件がある）[36]。状況により、どの程度の識別リスクがあるかを見る。

識別可能性と、上記2007年第29条作業部会文書の選別について、氏名を知ることは必須ではなく、1人を固有に割り出せるか否かによる。選別できる能力はより重要になっており、ビッグデータの文脈での基準になっている[37]。携帯電話などでオンラインショッピングを行う場合に、固有の行動パターンなどで1人の個人であることが分かれば、氏名は必要とされない。第29条作業部会の文書に関しては、加盟国によって意見が異なる。第29条作業部会の文書は、多数意見としての一般的な選別を述べているが、我々の意見は異なり、加盟国の中にも異なる意見を持つ者がいる。第29条作業部会の意見は、いくつかの異なる意見のブレンドであり、白黒をつけるものではない。第29条作業部会の文書への参照は、EUレベルでの背景文書として維持する重要性はあり、全員の意見を代表するものである。

② 適法な取扱い、第三国移転

1992年プライバシー法第5条（取扱いの適法性）と第22条（国際移転の例外）は混乱するかもしれない。EU域内の情報の流通は自由である。第5条と第22条はデータ保護指令に由来するが、範囲が異なる。同じ意味でもない。「同意」は非常に制限的に解釈される。

a. 適法な取扱い

包括的な文言を承諾するだけでは、第5条の「同意」と解釈されない。雇用関係で従業員に選択の余地がない場合は「自由に与えられた」同意ではない。同意には法に基づく3つの条件（「特定の」、「情報を得た」、「自由な」）が必要であり、包括的な契約条件に基づく同意は「特定の」の条件を満たさない。「自由な」とは、撤回可能で、交渉の余地がない固定の一般条件ではないことを意味する。クレジットカード会社には標準的な契約条項があり、顧客には選択の余地がないため「自由」とはいえない。ウェブサイト上の表明に賛同することも「同意」ではない。署名は、特定の範囲及び項目を他と分離した上で（商品やサービスの購入等）行われる場合に限り有効である。クレジットカード会社を含む多くの企業の実務では有効な「同意」を取得できていない場合が多い。同意取得の証明責任は管理者側が負う。

第5条の「契約を履行するために必要な場合」について、クレジットカードによる支払いが唯一又は排他的な選択肢である場合には、「契約履行のために必要」という文言が適用され得る。ただし、この文言もまた厳格に解釈される。データは必ずしも契約履行に必要でない場合もある。例えば電気通信サービスを受けるに伴って請求書を受領するために住所等を提供することは理に適っている。年齢や職業等はマーケティング目的に必要であるとしても契約履行に必要とはいえない。

b. 第三国移転

第5条は包含的な条文であるが、第22条は全く異なる条文で、特定の場面に適用される。EUとEEA地域以外に個人データを移転する場合に適用される。移転するためには法的解決策を得なければならない。第22条は、例えば、委託先の国や、データ保護法のない国などへ移転する際の個々の例外を挙げたものである。

第22条も厳格に解釈される。一般的な契約条件やライセンス契約などでは「同意」の要件を満たさない。

第22条に基づく第三国移転の例外規定は特定されているため、第29条作業部会は、データ保護指令第26条1項について、構造化され、大量の、反復して行われる取引には適用できないと解釈している。SWIFTのようなデータは、構造化された、重要かつ安全なデータであるが、大量のデータであるので、第22条の例外は適用できない。構造化された大量のクレジットカード決済データが国際移転する場合も同様であり、他の法的解決手段（BCRやSCCなど）

を採るべきである。企業は契約履行に必要等の理由でいまだ第22条の例外を適用しているかもしれないが、第29条作業部会の見解とは異なる。

「契約の締結又は履行のために必要」という文言は、例えばEU市民が日本のウェブサイトで品物を購入する際に、クレジットカードが唯一の選択肢であれば、「契約の締結又は履行のために必要」という要件に該当する。しかし、銀行振り込み等の他の選択肢がある場合は、この要件に該当しない。「特定の状況」をGDPRに沿って解釈すべきである。

3) WP12、WP114の有効性

第29条作業部会で10年ほど前に議論した文書（2005年発布）のものはあるが、その後は手続の変更により、業界とは最近はあまり議論していない。

次の2つの事項においていまだ有効である。第1は、例外が狭く解釈されるという点である。第2は、データ保護指令のような「原則」と「例外」ではなく、GDPRでは、EUの現在の実務に即した形で「特定の」状況における例外という別のアプローチが採用されたため、立法者がこれらの文書を狭く解釈しているという点である。

前記のとおり、第29条作業部会文書に拘束力はないが、GDPRが適用開始されることにより、新たに設置されるデータ保護会議の指針及び勧告はより重視されることになるであろう。

5. クレジットカード会社

訪問調査では、EU域内の某クレジットカード会社に訪問し、クレジットカード番号の取扱実務に関するインタビューを行った。

1) 支払処理の際に受領する情報

当社は支払処理を行う際に大半のデータを受領するが、受領するデータ要素は限られている。すなわち、個人のクレジットカード番号、加盟店名及び場所、取引の日付、時間及び合計金額を受領する。当社は、通常はカード保有者の氏名やその他の連絡先情報は受領しない。また、購入した製品やサービスの種類に関する情報も受領しない。この情報はクレジットカードを発行し、カード保有者と直接的な関係を持つイシュア銀行が保管する。

2)「個人データ」

当社がクレジットカード番号の背後にいる人物を知らない場合でも、クレジットカードの番号は個人データとして取り扱っている。GDPRでは、クレジットカード番号は明確に個人データとみなされている。

3） 取扱いの適法性

EU法では個人データの取り扱いに関して6つの法的根拠がある。

第1は同意である。EUでは、「同意」の基準を満たすことは極めて困難である。例えば、消費者は自身の自由意思に基づいて同意を撤回できる必要がある。当社はクレジットカード取引の取扱いにあたって同意を法的根拠として使用しない。例えば、同意はマーケティング活動を実施する場合に使用される。

第2の根拠は契約の履行である。クレジットカード支払いを行う際の取扱時にこの法的根拠を使用する。消費者はイシュア銀行との間でクレジットカードを入手するための契約を締結する必要があり、クレジットカード処理を行うためには、個人データを取り扱う必要がある。この法的根拠を必要とする法人はイシュア銀行（管理者）であり、当社（処理者）ではない。当社はイシュア銀行が依拠する法的根拠に従って主要な処理を実施する。

第3の根拠は、イシュア銀行と当社が自己の法的義務を遵守する場合である。例えば、詐欺やマネーロンダリングへの対策を行う目的で個人データを収集及び使用する場合に該当する。

第4の根拠は、管理者又は第三者が自己の適法な利益を追求する場合である。イシュア銀行及び当社は、消費者に損害が発生せず、その者のプライバシーが侵害されない場合にのみ情報を取り扱うことができる。これは利益のバランスである。GDPRでは、詐欺の監視及び防止、並びに直接のマーケティング目的で必要な個人データの取り扱いは、通常は管理者の適法な利益を根拠に正当化されることを明記している。別の例を挙げると、データ分析のために、それ以上の個人データを利用する場合に匿名化することは、通常は管理者の適法な利益に基づく。個人データの匿名化は個人データの処理形式の1つであるために法的根拠が必要となる。

4） 第三国移転

個人データが物理的にEU外に持ち出される場合には、移転とみなされる。また、EU外（例えば米国）からデータにアクセスする場合にも移転に該当する。スマートフォンやインターネットが存在するため、地方に住んでいる場合であっても、誰でもいつでもデータを移動することができる。国際移転を行うための法的根拠は、個人データを取り扱うための法的根拠とは異なる。

当社は以前にセーフ・ハーバーの承認を受けており、EUから当社のメインデータベースが置かれている米国への個人データの移転は正当化される。現在、当社は、データ移転に関する全ての活動で、EUのSCCを使用しているが、長期的戦略はBCRを使用することである。

BCRは、現在EU及びスイスのデータ保護機関から、多国籍企業にとっての最良のデータ移転の仕組みとみなされている。BCRには個人の保護の強化や、企業にとっての世界規模の範囲を含めた複数の利点がある。当社のBCRによって、EU及びスイスの個人データの自由な流れが促進され、当社のグローバルグループ内の全てのデータ処理を行うことができる。当社のBCRは、EUデータ保護機関が必要とする全ての規制上の承認を受けている。そのため、当社では、近く国際データ移動の法的根拠としてBCRの使用へ移行するつもりである。

SCCは、EUデータ保護法の下で国境間のデータ移転を可能にする手段の1つであるが、過剰に規範的であり、データフローの変化に対応する柔軟性を欠いている場合には、企業にとって実務的な負担が発生する可能性もある。

EUデータ保護法では、会社がデータをEU外に移転するために利用することのできる、個人の同意や契約書の締結のような例外も規定されている。ただし、このような例外は、その他のメカニズム（例：SCCもしくはBCR）が利用できない場合にのみ適用され、大量・反復的なデータ移転には絶対に用いるべきでない。そのため、これらの例外はクレジットカード取引の取り扱いでは適切ではない。

5） WP12、WP114

常に大量のデータを移転する企業は国際データ移転のための適切な保護措置を追加する必要がある。例外を適用できるケースには限度がある。

6. 法律事務所

訪問調査では、EUのデータ保護法制に詳しい弁護士にも訪問調査を行った。

1）「個人データ」

「個人データ」の範囲は非常に広い。識別可能な人と結びつくや否や、個人データの概念に入る。直接間接の識別性がある。識別番号は直ちには個人を識別するものではないが、デビットカードやクレジットカード番号は通常は銀行口座の情報と結び付き、間接的に個人識別が可能になるため、個人データとみなされる。両者に違いはない。カード番号の識別性がないのは、無記名式のプリペイドカードである。

2） 国内流通・第三国移転の適法性

1）のように、クレジットカード番号も銀行口座の情報と結びつき、間接的に個人識別が可能となる。クレジットカード番号は「個人データ」であるため、EEA以外への国際移転には

根拠が必要である。十分性の認定を受けていない国は一定の追加ルールを守らなければならない。EEA地域内での情報流通は、法遵守ができている限りは自由である（諸原則の遵守やセキュリティなどの義務全般）。十分性を受けた国は非常に限られており、それ以外は一定の例外を用いなければならない。例外は法の中に列挙されている。それに加えて、契約（BCRやSCC）の手段がある。

クレジットカードのデータにとっては、最も多くの場合に用いられるのは同意であると思われるが、契約履行のための例外もある。ベルギー人がING銀行からクレジットカードの発行を受けて日本に旅行をし、支払いはホテルで行われた場合には、通常、ING銀行から日本のホテルにクレジットカードのデータは移転する。これは、契約の履行のために必要な場合に該当する。

同意と契約の履行の例外は全く異なる。同意はその1つであり、同意が取れると他の例外は必要ない。もし同意が得られなければ、契約履行のために必要であるという例外を用いることができる。カード保有者が国外で支払いを行う場合が該当する。例外は累積的なものではなく、この場合は同意を得る必要はない。

ベルギー人がベルギーの銀行からクレジットカードの発行を受け、クレジットカードを日本で使った場合には、銀行との間の契約履行のために必要であって、同意は必要ない。クレジットカードの利用が支払いを行えるようにするためであり、クレジットカードのデータの流通は、ベルギーのイシュアから日本の加盟店と取引するアクワイアラ銀行へ流れる。他方、構造によって、クレジットカード会社は米国に情報を流すこともある。なぜなら、米国内に中央化されたDBがあるからである。ベルギーと日本の間で流通させれば足りるものについて米国を介する場合は、契約履行のために必要とはいえないため、その場合は同意等他の理由が必要になる。「取扱い」が、「契約を履行する」ために「必要」であることが求められるのであって、契約があれば良いというものではない。「取扱い」が、「契約を履行する」ために「必要」というのは、裁判所や規制者によって、非常に狭く限定的に解釈されている。

おそらく、国際カードの場合はほとんどの場合が米国を経由する。そのため、他の法的根拠が必要であり、SCCやBCRなどの手当をしなければならない。例えばSWIFTの場合はクレジットカード事業者とは異なるが、EEA域内であれば移転のための法的根拠（transfer solution）は必要ない。クラウドを利用するのか、欧州外で中央化されたデータベースを利用するのか等、データの保存設備次第によって異なる。

（プライバシー・シールドが採択されていない6月時点では）セーフ・ハーバーには依拠できないため、移転は違法になる。企業は、SCCやBCRなど他のソリューションに依拠している。米国の事業者が他のソリューションの手当ができていない場合もあり得る。大手のクラ

ウド事業者などでソリューションの変更を行おうとしているところもある。小規模の事業者には手段がない。EUのデータ保護法は非常に複雑で、全てを実施することは困難であり、グレーゾーンもある。

適法な取扱いの要件（データ保護指令第7条）は、移転の規定とは別である。第7条は取扱いの法的根拠である。取扱いには適法性の要件が必要であり、移転を行うためにはそのためのソリューションが必要である。「移転」は、域内から域外へ、「取扱い」の適法性は、域内域外を問わない。第7条は取扱い全般を対象にした法的根拠を定めている。取扱いの一部として、域内から域外へと移転する場合に、追加的ルールを守らなければならない（それが移転のためのソリューション）。「同意」の要件を満たせば、データ保護指令第7条と第26条の両方をカバーすることはできる。

「同意」は「契約」の形態によっても取得することはできる。実務的には、1本の契約でカバーすることはできる。ただし、通常「同意」は「契約」とは異なる。データの移転等を説明した契約条件を示され、チェックを入れて署名をするのが同意である。

7. 英国

英国では、英国カード協会（The UK Cards Association）[38]に訪問した。

1） 1998年データ保護法

英国の個人情報保護法は、1998年データ保護法である。他国の法令と比べると、附則の中に重要規定を置くなど、やや異なる構成を取っているが、規定内容はEUデータ保護指令に倣っている。同法は、第1条1項で「個人データ」の定めを置き、附則の中で適法な取扱いの要件及び第三国移転制限を定めている。

2） 解釈

① 「個人データ」

「個人データ」は、監督機関である情報コミッショナー事務所（Information Commissioner's Office, ICO）[39]が明確に定義づけている。個人データは、生存する個人を識別できる情報であって、データ管理者（データの所有者）が入手できる情報である。他の情報から個人が識別できる場合であっても、所有されているデータは個人データとしてみなされる。総合的な情報として、ICOが全ての考え得る状況における詳細なガイダンスを発表している[40]。

クレジットカード番号やデビットカード番号は、他のデータ（名前、生年月日等）を関連付けることができ、間接的に識別可能な情報であるため、個人データに該当すると思う。番

号だけでは個人を識別できないであろうが、保管されている他の情報によって個人を識別することができる。

② 適法な取扱い

クレジットカードを発行するときに、データ主体が合意書にサインをする。その合意書の中に同意が含まれており、一定の状況下で情報を共有化することについての同意である。データ主体は、それにより公正かつ適法に扱われることを期待する。業界として、同意条項のひな型は用意していない。規則やガイドラインを策定する団体でもない。

1998年データ保護法の第8原則(EEA以外へのデータ移転に関する十分なレベルの保護)は、データ保護指令に基づく規定であり、主にEEAの中での情報移転と、EEAと同等と考えられる第三国への情報移転を対象とする。第8原則は、取引以外にも、データを処理するために英国から他の国に移転する場合（不正行為対応等）にも適用される。

Ⅴ. 日本の個人情報保護法

1. 個人情報保護法改正

個人情報保護法の改正法は、2015年9月3日に成立し、同年9月9日に公布された。同法の全面施行日は、2017年5月30日である。

個人情報保護法の改正過程では様々な議論が交わされたが[41]、成立した改正法のポイントは次のように整理されている【図表-1】。

【図表-1】個人情報保護法の改正のポイント

定義の明確化等	・個人情報の定義の明確化(身体的特徴等が該当) ・要配慮個人情報(いわゆる機微情報)に関する規定の整備 ・個人情報データベース等から権利利益を害するおそれが少ないものを除外 ・取り扱う個人情報が5,000人分以下の事業者に対しても法を適用
適切な規律の下で個人情報等の有用性を確保	・利用目的の変更を可能とする規定の整備 ・匿名加工情報に関する加工方法や取扱い等の規定の整備 ・個人情報保護指針の作成や届出、公表等の規定の整備
個人情報の流通の適正さを確保	・本人同意を得ない第三者提供(オプトアウト規定)の届出、公表等厳格化 ・トレーサビリティの確保(第三者提供に係る確認及び記録の作成義務) ・不正な利益を図る目的による個人情報データベース等提供罪の新設
個人情報保護委員会の新設及びその権限	・個人情報保護委員会を新設し、現行の主務大臣の権限を一元化
個人情報の取扱いのグローバル化	・国境を越えた適用と外国執行当局への情報提供に関する規定の整備 ・外国にある第三者への個人データの提供に関する規定の整備
請求権	・本人の開示、訂正等、利用停止等の求めは請求権であることを明確化

出所：首相官邸ウェブサイトの「政策会議」のうち、「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」(http://www.kantei.go.jp/jp/singi/it2/pd/pdf/gaiyou.pdf) より。

この中で本稿と関係する部分を挙げると、まず、第1の「定義の明確化等」がある。これは、ビッグデータを利活用したいというニーズと、「個人情報」の範囲の曖昧さ（グレーゾーンの存在）による利活用の阻害を解消するための改正である。消費者にとっても、事業者によって個人情報として保護されるか否かに違いが生じると、自己の情報提供に心理的抑制が働くという点が指摘されていた。そこで、定義の明確化を図るべく、「個人識別符号」が新たに定められ、その範囲は個人情報の保護に関する法律施行令（以下「政令」という。）[42]に委任された（法第2条1項二号、2項）。政令第1条によると、身体的特徴の一部又は行動をデジタル化した情報及び旅券番号、年金番号、運転免許証番号、マイナンバー等が列挙されている。

次は、第3の「個人情報の流通の適正さを確保」である。これは、いわゆる名簿業者の問題が発端となった。2014年7月に発覚したベネッセコーポレーションからの大量漏えい事件により、名簿業者の規制を意図した改正が導入された。ただし、「名簿業者」を定義することが困難であることや、名簿の販売行為を規制することで過度な規制になるとの懸念が生じたことから、①オプトアウトにより個人データを第三者に提供する際の個人情報保護委員会への届出、公表等（法第23条2～4項）、②個人データを第三者に提供する際に、提供者は提供先等の記録を作成・保管し、受領者は個人データ取得の経緯等を確認し、その記録を作成・保管する旨の義務規定を置くことによるトレーサビリティの確保（法25条、26条）、③個人情報データベース等提供・盗用罪（法第83条）の新設によって対応することとなった。クレジットカードの取扱いとの関係では、②が問題となる。

さらに、第5の「個人情報の取扱いのグローバル化」も関係する。これは、国際的なデータ流通に対応するための改正である[43]。外国にある第三者への個人データ提供も新設規定である（法第24条）、個人情報取扱事業者が外国で個人情報を取り扱う場合の域外適用（法第75条）、個人情報保護委員会から外国執行当局への情報提供に関する規定（法第78条）が新設された。

2. 個人情報の範囲

クレジットカード情報と個人情報の範囲を考える上では、①個人情報の識別性、②個人識別符号該当性が問題となる。個人情報保護法第2条は、それぞれについて次のように定めている。

第2条　この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記

録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第2号において同じ。）で作られる記録をいう。第18条第2項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

二　個人識別符号が含まれるもの

2　この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。

一　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

二　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

法第2条1項一号について、個人情報保護委員会の「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）」[44]によると、「「個人に関する情報」とは、氏名、住所、性別、生年月日、顔画像等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない。」と説明されている[45]。クレジットカード会社がクレジットカード契約に基づき加入者から取得する情報は、一号によって個人情報に該当するといえる。

法第2条1項二号及び同条2項について、「個人識別符号」とは、当該情報単体から特定の個人を識別できるものとして政令に定められた文字、番号、記号その他の符号をいい、これに該当するものが含まれる情報は個人情報となる[46]。法第2条2項は2種類の個人識別符号を定めており、具体的には政令に委ねられている。政令によると、法第2条2項一号の個人識別符号は、DNAを構成する塩基配列や顔の骨格、皮膚の色、容貌等、7種類の身体の特徴のいずれかを電子計算機の用に供するために変換した文字、番号、記号その他の符号のうち、「特

定の個人を識別するに足りるものとして個人情報保護委員会規則で定める基準に適合するもの」が該当する（政令第1条一号）。

法第2条2項二号の個人識別符号は、旅券番号、基礎年金番号、運転免許証番号、マイナンバー等、公的に用いられる番号が該当する（政令第1条二号～八号）。より具体的には、個人情報の保護に関する法律施行規則（以下「規則」という。）[47]が定めを置いている（規則第3条及び第4条）。

2017年2月16日、個人情報保護委員会は、「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を公表した[48]。そのQ1-22には「携帯電話番号やクレジットカード番号は個人識別符号に該当しますか。」という項目があり、A1-22によって「携帯電話番号やクレジットカード番号は、様々な契約形態や運用実態があり、およそいかなる場合においても特定の個人を識別することができるとは限らないこと等から、個人識別符号に位置付けておりません。なお、このような番号も、氏名等の他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなる場合には、個人情報に該当します。」との回答が示されている。

「個人識別符号」は、個人に発行されるカードに記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、発行を受ける者ごとに異なるよう割り当てられ又は記載されることにより、発行を受ける者を識別できるものであることから、法第2条1項二号の文言上はクレジットカード番号も入り得る。

しかし、クレジットカード決済は、クレジットカード番号が加盟店からクレジットカード会社（アクワイアラ）、国際ブランド会社、クレジットカード会社（イシュア）等、多段階、複数の事業者を経由して（時には国境を越えて）、クレジットカードの有効性や与信枠の確認等（オーソリゼーション）などが行われることが前提である。クレジットカード番号が単体で個人識別符号に含まれるとなると、個人情報に該当するという強い効果を持つことになり、クレジットカード決済の都度、クレジットカード番号が流通する複数の当事者間で個人情報保護法の規制（第三者提供の際の同意取得等）がかかってしまい、クレジットカード決済を不可能にしてしまうという懸念が指摘されている。

クレジットカード番号、加盟店名及び場所、取引の日付、時間及び合計金額が含まれる決済情報については、特定個人を識別できる可能性が高いと思われるが、そうでない場合は、容易照合性の有無によって識別性が決せられる（第2条1項一号）。前掲のQ&Aによると、クレジットカード番号については、契約形態や運用実態を配慮する形で個人識別符号から除外されているが、この議論は、クレジットカード番号に限らず、関連する金融・信用事業者で横断的に行われるべきである。

決済情報が個人データに該当する場合、クレジットカード会社からすると、外国にある第三者への提供の制限及び第三者提供にかかる記録作成義務等の点で決済情報の流通に支障を来すことが懸念されている。

3. 第三者提供

1） 第三者提供の制限

法第23条1項は、次の通り、第三者提供の制限に関する原則規定を定めている。

「第23条　第三者提供の制限

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二　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。

三　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。

四　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。」

同条2項はオプトアウト、3項は、オプトアウトに関する事項の変更に関する本人への通知及び個人情報保護委員会への届出等、4項は、オプトアウトに関する事項の変更に関する個人情報保護委員会による公表、5項は、委託や共同利用等の場合において「第三者」に該当しない場合、6項は、共同利用に関する事項の変更についての本人への通知等を定めている。

第24条は、「外国にある第三者への提供の制限」を定めている。

「第24条　外国にある第三者への提供の制限

個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下

この条において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。以下この条において同じ。）に個人データを提供する場合には、前条第1項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。」

個人情報取扱事業者は、個人データを外国にある第三者に提供するに当たっては、法第24条に従い、次の①から③までのいずれかに該当する場合を除き、あらかじめ「外国にある第三者への個人データの提供を認める旨の本人の同意」を得る必要がある[49]。

①当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国として個人情報の保護に関する法律施行規則で定める国にある場合

②当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として規則で定める基準に適合する体制を整備している場合

③法第23条1項各号に該当する場合

第23条及び第24条の対象は「個人データ」であるが、クレジットカード会社が会員の個人情報を取り扱う場合は、個人情報データベース等を構成する情報として取り扱っていると考えられる。そのため、事業者の取扱部門が容易照合性を満たさないようにデータベースを別々に保管していても（個人情報保護委員会・前掲Q&AのQ1-15参照）クレジットカード番号が「個人識別符号」に含まれると、第23条及び第24条の義務がかかることとなる。

①について、現時点で個人情報保護委員会が認めている国は存在しない。②については、個人情報保護委員会規則第11条において、「個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第4章第1節の規定の趣旨に沿った措置の実施が確保されていること。」（一号）、「個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。」（二号）と定められている。

一号の「適切かつ合理的な方法」は、個人データの提供先である外国にある第三者が、我が国の個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずることを担保できる方法が求められている[50]。例えば、①外国にある事業者に個人データの取扱いを委託する場合には、提供元及び提供先間の契約、確認書、覚書等、②同一の企業グループ内で個人データを移転する場合には、提供元及び提供先に共通して適用される内規、プライバシーポリ

シー等が該当する。また、提供元の事業者がアジア太平洋経済協力（Asia-Pacific Economic Cooperation, APEC）の越境プライバシールール（Cross Border Privacy Rules, CBPR）システム[51]の認証を取得し、提供先の「外国にある第三者」が当該個人情報取扱事業者に代わって個人情報を取り扱う者である場合にも、「適切かつ合理的な方法」該当する。

一号の「法第4章第1節の規定の趣旨に沿った措置」は、利用目的の特定、利用目的による制限等、法第15条から第29条までに定める個人情報取扱事業者の義務に沿った措置を意味する。

二号は、提供先の外国にある第三者が、APECのCBPRシステムの認証を取得していることが該当する。

しかし、提供元ないしは提供先がCBPRの認証を受けたとしても、そもそもCBPRの参加国は米国、メキシコ、日本、カナダのみであるため、現時点では認証取得の効果は高くない。

クレジットカード会社における決済データの取扱いは、国内のみならず世界中の地域で継続的に行われている。世界各国の提供先との間で、日本の個人情報取扱事業者の義務規定に沿った措置を確保することは現実的ではない。

③の法第23条1項各号について、決済処理に適用できるものはない。

以上から、クレジットカード番号を含む決済データを外国に移転する場合には、あらかじめ「外国にある第三者への個人データの提供を認める旨の本人の同意」を取得しなければならない。この同意は、第23条1項各号に該当する場合以外は、「外国」にある「第三者」への個人データの提供について本人同意を必要とする。これは、オプトアウト、委託、事業承継、共同利用の場合であっても、「外国」にある「第三者」へ個人データを提供することへの本人同意を必要とすることを意味する。決済処理がデータ移転に該当するか否かという点に議論の余地はあるとしても、外国へのデータ移転が日々大量に発生するクレジットカード業界において、このような個別同意を取得することは現実的ではない、ということが懸念されている。

2） 第三者提供に関する記録作成等

法第25条は、「第三者提供に係る記録の作成等」と題し、個人情報取扱事業者に対し、個人データを第三者に提供したときは、個人情報保護委員会規則に基づき、当該個人データを提供した年月日、当該第三者の氏名又は名称等の記録を作成し、その記録を一定期間保存するよう義務づけている（法第25条1項及び3項）[52]。外国にある第三者に提供する場合には、法第23条第1項各号のいずれかに該当すれば記録作成等の義務は生じないが、決済情報は転々流通することを予定しているため、同条各号に該当する場合は考えにくい。

個人情報保護委員会の「個人情報の保護に関する法律についてのガイドライン（第三者提

供時の確認・記録義務編）」[53]によると、外国にある第三者に個人データを提供する場合の記録義務の適用は、次の4つの類型に分けられる。

類型Ⅰ　本人の「同意」を得ている場合

類型Ⅱ　当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国として個人情報の保護に関する法律施行規則で定められた国にある場合

類型Ⅲ　当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として規則に定める基準に適合する体制を整備している場合

類型Ⅳ　法第23条1項各号に該当する場合

【図表-2】各類型と記録義務の適用関係

＜適用表＞

類型の別		記録義務の適用の有無
類型Ⅰ		有（*1）
類型Ⅱ又は類型Ⅲ	「2-1-2　法第 23 条第 5 項各号に掲げる場合」に該当しない場合（*2）	
	「2-1-2　法第 23 条第 5 項各号に掲げる場合」に該当する場合	無
類型Ⅳ		

（*1）記録義務が適用される場合の記録の作成方法、記録事項などについては、国内の第三者に個人データを提供する場合と同様に、「4　記録義務」に従うこととなる。

（*2）具体的には、法第 23 条第 1 項柱書（「本人の同意」）又は法第 23 条第 2 項（オプトアウト）に基づき、第三者提供を行う場合である。

出所：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（第三者提供時の確認・記録義務編）」（https://www.ppc.go.jp/files/pdf/guidelines03.pdf）5頁より。

上記の通り、ⅠからⅣの類型は、クレジットカードデータの取扱実務には適しておらず、提供にかかる記録の作成・保管義務の遵守は容易ではない【図表-2】。個人情報保護委員会規則第12条2項は、提供にかかる記録を都度速やかに作成するよう義務づけている。同条但書きでは、当該第三者に対し個人データを継続的又は反復して提供する場合の一括作成を認めているが、決済データの流通先は、複数国にわたっており、常時変動すると考えられることから、一定期間における継続又は反復提供先を抽出することも困難ではないかと思われる。

第26条は、第三者から個人データの提供を受ける際の確認及び記録作成・保存義務を定めている（法第26条1項及び3項）。確認事項の中には、第三者の氏名又は名称等に加え、当該

第三者による個人データ取得の経緯が含まれる。これについても、大量、反復的であり、かつ、授受の相手が都度変動するクレジットカード取引については、同様の問題が発生する。

ところで、EUのGDPRにも記録作成義務は存在する。GDPR第30条「取扱行為の記録」は、管理者及び取扱者等に対する文書保管義務を定めている。記録すべき情報の中には、「該当する場合には、第三国又は国際機関の特定を含む、第三国又は国際機関への個人データ移転。第49条第1項後段に定める移転の場合には、適切な安全保護措置に関する文書。」が含まれている（GDPR第30条1項（e）号、4項（c）号）。しかし、同条項は、第三国又は国際機関の特定までを要求するにとどまっており、個々の移転を記録することまでは求めていない。

Ⅵ. クレジットカード決済データの適切な流通に向けて

今回の訪問調査では、①クレジットカード番号の個人識別性（識別番号該当性）、②クレジットカード決済データを適法に取り扱うための法的根拠、③クレジットカード決済データを域外（国外）に適法に移転させるための法的根拠等について、関係者にインタビューを行った。

①については、クレジットカード番号の個人識別性を否定する回答はなかった。EUの個人データ保護制度では、識別され、又は識別され得る自然人（データ主体）に関するすべての情報を「個人データ」とし、「識別され得る自然人」について、さらに、識別番号（identification number）をはじめとする様々な要素を参照することよって、直接又は間接に識別され得る者をいうと定義付けている。それにはクレジットカード番号のみならず、口座番号やデビットカードの番号など他の金融、信用情報分野の事業者が取り扱う番号の全てがこれに該当する。この点は、データ保護指令もGDPRも同様である。日本の改正個人情報保護法では、「個人識別符号が含まれるもの」について、容易照合性がなくても「個人情報」該当性を認めることによって定義の明確化を図ったと説明されており、個人識別符号に含まれるか否かが個人情報該当性を決する重要な要素となる。クレジットカード会社が保有する会員情報は個人情報に該当するが、クレジットカード番号が個人識別符号に含まれると、容易照合性を回避しても決済データの全てが個人情報に該当するため、決済処理に与える影響が大きい。今後、仮に個人識別符号にクレジットカード番号を含めることがあったとしても、銀行口座番号等、他の金融・信用情報分野の事業者が取り扱う番号との平仄を合わせる必要がある。同時に、決済情報の流通を妨げないようにする法的手当てが必要である。

EUの個人データ保護法制では、識別番号は参照要素の1つであるため、「クレジットカード番号が識別符号に含まれるか」という観点での直接的な議論は行われていない。ただし、このような法制上の違いはあるものの、識別番号にクレジットカード番号は含まれないとい

う見解は見られず、少なくとも間接的な識別可能性は認められるという回答で一致していたといえる。

②及び③に関しては、文言が類似していることから、解釈も共通的であるとの認識に基づき質問を行ったところ、全く異なる規定であり、別々に解釈されるという回答を得た。

②は、個人データを適法に取り扱うための要件を定めた規定(1995年データ保護指令第7条、GDPR第6条）に関するものであり、その要件には、（ア）データ主体が個人データの取扱いに明確な同意を与えた場合、（イ）データ主体が当事者である契約を履行するため、（ウ）管理者又は第三者が追求する適法な利益のため、などが列挙されている。「取扱い」は域内外であるか否かを問わない。EUでは「同意」は非常に厳格に解釈されており、データ保護指令においても「特定の」、「情報を与えられた」、「自由な」という要件を満たすことが求められてきた。そのため、標準的な契約を事業者ないしは雇用者等があらかじめ用意しており、消費者ないしは従業員側に選択の余地がない場合や、約款の中に同意条項が含まれるような場合には、同意の要件を満たすことは困難と解釈される。また、同意は項目を列挙する形で個別に付与することが必要であり、包括的な同意は認められない。ただし、同意を得ることで国内での取扱いを行っているとの回答もあった。

契約については、「取扱い」が、「契約を履行する」ために「必要」であることが求められるのであって、契約があれば良いというものではなく、これも非常に限定的に解釈されているとのことであった。ただし、データ主体が当事者となっているクレジットカード等の契約を結んでいれば、適法な取扱いの条件を満たすことは可能という意見や、契約の形態によって同意を取得することもあり得るとの説明もあった。

③は、EU域内から第三国等へ個人データを国際移転するためのソリューションに関するものであり、GDPRでは、データ保護指令をより明確化する形で、3段階の規律が設けられた。第1は、第三国等が欧州委員会から「十分な保護レベル」の決定を受けた場合、第2は、第三国等が、BCRやSCCなどの安全保護措置を講じた場合、第3は、特定の状況による例外に該当する場合である。

第3の「特定の状況による例外」を定める条項の中には、（ア）データ主体が移転に明示的な同意を与えた場合、（イ）データ主体と管理者間における契約履行のために移転が必要な場合、（ウ）データ主体の利益のために管理者と第三者間で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、などが列挙されている。これらの条項は、適法な取扱いのための要件を定めた②と共通的であることから、解釈も共通するものとの前提で質問に臨んだところ、異なる回答を得ることとなった。すなわち、各訪問先からは、第3が適用される場合は非常に限定されており、大量・構造的・反復取引には適用できないとの解釈が示された。GDPR

の規定にも「のみ」という限定的な文言が付されている。

ところで、③は、EU域内と第三国との間でカードの決済処理が行われる場合に、個人データの国際「移転」に該当することを前提とするものであるが、そもそも決済処理がデータ「移転」に該当するか否かが明確に認識されてこなかった、という回答もあった。

以上をまとめると、①EUの関係者はクレジットカード番号を含む情報を「個人データ」とみなしている、②適法な取扱いのための要件と第三国移転制限は全く異なる仕組みであるため、文言が類似していても法的効果は異なる、③「同意」は限定的に解釈され、日々データが移転するクレジットカード取引において、包括的な同意を取ったとしても有効ではない、④第三国移転のための例外規定は、大量・構造的・反復取引には適用できない、⑤十分性を取得していないのであれば、EUから個人データを受けるためにはSCCかBCRを用いる必要がある、という点で一致していた。ただし、そもそも決済行為が個人データの移転に該当するか否かという点は、関係者間で明確なコンセンサスを確立する必要があるようである。

今回の調査では具体的な意見を聞くことはできなかったが、適法な取扱いは、「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」該当する可能性があるように思われる。この規定の解釈はGDPRの前文で示された通り、マーケティングを含む営利目的でも認められている。

日本の個人情報保護法では、「適法な取扱い」に直接に相当する規定はないが、国外移転については第24条及び移転に伴い記録の作成を義務づける第25条及び第26条が新設された。前述の通り、クレジットカード会社にとっては遵守に困難を伴う規定と考えられる。

第三国移転について、EUのデータ保護指令やGDPRに倣って考えるのであれば、クレジットカードのような大量・構造的・反復的取引には同意や個別契約に基づく例外を用いることはできず、現状ではSCCかBCRが必要となる。日本の個人情報保護法にBCRに類する規定を導入すべきとは考えないが、同法の今後の改正時に、標準的な契約条項を用いることによる移転を取り入れる余地はあり得る。

ところで、データの越越移転についてはEUのBCRとAPECのCBPRには相互運用の議論があり[54]、APECのデータプライバシー・サブグループは、2015年より、民間部門を交える形でBCR制度とCBPR制度に関する共同作業チームを設置し、検討を進めている[55]。短期及び中期的には、BCRとCBPRの共同申請フォームの作成、両制度の遵守を証明するための、企業の方針、関連する個人データ及びプライバシー計画の実務、効果的な手段のマッピングを行うこと等を目指している。この議論は先行き不透明であるが、仮に両者の相互運用が進み、CBPRの参加エコノミーが拡大すれば、CBPR認証を受けることが情報の流通に役立つ可能性はある。

第25条及び第26条については、GDPRにも文書化の義務はあるが、原則として個別移転を義務づける日本の規定とは異なっている。大量・構造的・反復的に個人情報を移転し、データの移転先が随時変動するクレジットカード会社に適した規定及び解釈が求められる。

［注］

[1] 1995 O.J.（L 281）31-50. 1995年データ保護指令の邦訳は、堀部政男研究室「欧州連合（EU）個人情報保護指令の経緯とその仮訳」新聞研究1999年9月号17頁以下参照。

[2] 2016 O.J.（L 119）1-88.

[3] 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、最終改正平成28年5月27日法律第51号）。

[4] 1995年EUデータ保護指令及び一般データ保護規則提案の段階における個人データ概念及び匿名化については、拙稿「EUの個人データ概念と匿名化―最新の調査結果を踏まえて」堀部政男編『情報通信法制の論点分析』別冊NBL第153号119頁～150頁（2015年）。なお、Ⅱ章の条文番号は、特段の断りがない限り、データ保護指令の条文番号を指す。

[5] 邦訳は、藤原静雄「EU個人情報保護指令前文」自治研究第76巻第11号（2000年）138頁以下、141～142頁を参考に、一部改訳した。

[6] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, adopted on Jun. 20, 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[7] 藤原・前掲「EU個人情報保護指令前文」141頁を参考に、一部改訳した。

[8] ノルウェー、リヒテンシュタイン、アイスランド。

[9] 詳細は、消費者庁「国際移転における企業の個人データ保護措置調査報告書（2010年3月）」（http://www.caa.go.jp/seikatsu/kojin/H21report1a.pdf）参照。

[10] 標準契約条項の詳細は、武井一浩ほか「モデル契約の概要」消費者庁「国際移転における企業の個人データ保護措置調査報告書」（2010年3月）58-91頁。

[11] Commission Decision 2001/497/EC, 2001 O.J.（L 181）19-31（EC）.

[12] Commission Decision amending Decision 2001/497/EC, 2004 O.J.（L 385）74-84（EC）.

[13] Commission Decision 2010/87/EU, 2010 O.J.（L 39）5-18（EU）.

[14] European Commission, Overview on Binding Corporate Rules, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm（last visited Feb. 3, 2017）.

[15] 楽天株式会社「楽天、EUデータ保護機関より拘束的企業準則（Binding Corporate Rules）の承認を取得―日本企業では初の取得―」（2016年12月26日）（https://corp.rakuten.co.jp/news/update/2016/1226_02.html）。

[16] Article 29 Data Protection Working Party, *Working Document, Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*, WP12, adopted on Jul. 24, 1998, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf.

[17] Article 29 Data Protection Working Party, *Working document on a common interpretation of Article 26(1) of Directive*, WP114, adopted on Nov. 25, 2005, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf.

[18] *Supra* note 16, at 24.

[19] *Supra* note 17, at 9.

[20] EUGDPR.org, www.eugdpr.org.GDPRの邦訳は、一般財団法人日本情報経済社会推進協会が本文の訳を公開している（https://www.jipdec.or.jp/library/archives/gdpr.html）ほか、明治大学法学部の夏井高人教授による私訳がある。夏井教授の私訳のうち、前文はKDDI総合研究所の調査レポートR&A（https://rp.kddi-research.jp/article/GN2016001）、本文は法と情報雑誌第1巻第3号1～186頁（2016年9月25日発行）

において公開されている。なお、Ⅲ章の条文番号は、特段の断りがない限り、データ保護指令の条文番号を指す。

[21] 本調査によるEU関係者へのヒアリング結果による。

[22] Council Directive 93/13, O.J. (L 95) 29-34 (EEC).

[23]「処理者」と訳されることもある。

[24] European Commission Directorate-General for Justice and Consumers, http://ec.europa.eu/justice/mission/index_en.htm. 欧州連合代表部EU MAG「欧州委員会について教えて下さい」(http://eumag.jp/question/f0516/)。

[25] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, Digital Rights Ireland Ltd, [2015] ECLI：EU：C：2015：650. 岩村浩幸「欧州司法裁判所によるセーフ・ハーバー・ルール無効の判決とその日系企業に対する影響」NBL第1061号4-7頁（2015年）参照。

[26] シュレムス判決とは、欧州司法裁判所大法廷において、2015年10月6日、セーフ・ハーバーを無効と判断した判決のことである。この事件では、Facebook利用者であり、オーストリア人であるマキシミリアン・シュレムス氏が、NSA（National Security Agency）の監視活動を理由に、Facebookから米国へのデータ移転の禁止を求めた。同裁判所は、「十分な保護レベル」の解釈について、第三国に対して、EU内で保障されるものと本質的に同等な基本的権利及び自由の保護レベルを実際に保障するよう求めるものとして理解しなければならないとし、2000年7月26日付セーフ・ハーバーに関する欧州委員会決定を無効と判断した。その後、EUと米国の間で交渉が進められ、欧州委員会は、2016年7月12日、新たな仕組みとして、EU-U.S.プライバシー・シールドを決定した。この仕組みは、同年8月1日に開始した。

[27] European Commission, *Communication from the Commission to the European Parliament and the Council, Rebuilding Trust in EU-US Data Flows* (COM (2013) 846 final), Nov. 27, 2013, http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

[28] Commission Nationale de l'Informatique et des Libertés, https://www.cnil.fr/.

[29] Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf.

[30] 個人データの自動処理にかかる個人の保護のための条約。

[31] Commission for the Protection of Privacy, https://www.privacycommission.be/en.

[32] Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, https://www.privacycommission.be/sites/privacycommission/files/documents/Privacy_Act_1992.pdf.

[33] WP136の12頁参照。

[34] ベルギーのeIDカード制度（http://eid.belgium.be/en）参照。

[35] クレジットカード番号はこれに該当する。

[36] 動的IPアドレスが個人データに当たり得るとした法務官意見（Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland）参照。

[37]「直接的」又は「間接的」な識別可能性は、特定の状況に依拠する。非常に一般的な名字は、教室内の生徒を識別するには十分となりうるが、誰かを識別する―国の人口全体から誰かを選び出すには十分ではない。「黒いスーツを着た男性」のような付属的情報ですら、信号で立っている通行人から誰かを識別できるかもしれない（WP136の13頁参照）。

[38] The UK Cards Association, http://www.theukcardsassociation.org.uk/welcome/.

[39] ICOは、1998年データ保護法や2000年情報自由法等の執行を担う独立監督機関である（https://ico.org.uk/）。

[40] ICO, *Determining what is personal data –Quick reference guide* (Dec. 12, 2012), https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf.

[41] 改正法の概要は、主に、個人情報保護委員会「個人情報保護法について」(http://www.ppc.go.jp/personalinfo/)、瓜生和久編著『一問一答　平成27年改正個人情報保護法』(商事法務、2015年)、宇賀克也『個人情報保護法の逐条解説』(有斐閣、第5版、2016年)、岡村久道『個人情報保護法の知識』(日本経

済新聞出版社、第3版、2016年)、関啓一郎『ポイント解説 平成27年改正個人情報保護法』(ぎょうせい、2015年)、辻畑泰喬『Q&Aでわかりやすく学ぶ 平成27年改正 個人情報保護法』(第一法規、2016年)、日置巴美・板倉陽一郎『平成27年改正個人情報保護法のしくみ』(商事法務、2015年)を参照した。

[42] 個人情報の保護に関する法律施行令(平成15年12月10日政令第507号、最終改正平成28年10月5日政令第324号)。

[43] 域外適用及び外国執行当局への情報提供以外に、国外犯処罰の範囲が拡大されている(個人情報保護法改正法第86条)。

[44] 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)」(2016年11月)(http://www.ppc.go.jp/files/pdf/guidelines01.pdf)。

[45] 同ガイドライン1頁。

[46] 同ガイドライン9頁。

[47] 個人情報の保護に関する法律施行規則(平成28年10月5日個人情報保護委員会規則第3号)。

[48] 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(2017年2月16日)(http://www.ppc.go.jp/files/pdf/kojouhouQA.pdf)。

[49] 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(外国にある第三者への提供編)」(2016年11月)(http://www.ppc.go.jp/files/pdf/guidelines02.pdf)2頁。

[50] 同上6-7頁。

[51] 事業者のAPECプライバシー・フレームワークへの適合性を国際的に認証する制度。APECの参加国・地域が本制度への参加を希望し、参加を認められた国がアカウンタビリティエージェントを登録する。このエージェントが自国内の事業者について、その申請に基づきAPECプライバシー・フレームワークへの適合性を認証する。個人情報保護委員会「国際会議」(http://www.ppc.go.jp/enforcement/cooperation/international_conference/#apec)より。

[52] 保存期間は、規則第14条に基づき1年ないしは3年と定められている。

[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(第三者提供時の確認・記録義務編)」(http://www.ppc.go.jp/files/pdf/guidelines03.pdf)5頁。

[54] 拙著『個人情報保護法の現在と未来:世界的潮流と日本の将来像』(勁草書房、2014年)233頁。

[55] APEC, Electronic Commerce Steering Group, http://www.apec.org/groups/committee-on-trade-and-investment/electronic-commerce-steering-group.aspx.