基般

個人情報保護にかかわる法制度をめぐるEUの状況

高崎 晴夫　（株）KDDI 総研

EUにおけるプライバシー保護および個人情報保護法制の沿革

■欧州司法裁判所による「忘れられる権利」の認定

2014年5月，欧州連合の最高裁判所にあたる欧州司法裁判所が，インターネットで自分の名前を検索すると結果に過去に報道された記事が表示されるのは不当だとするスペイン人男性の訴えを認め，米インターネット検索大手Googleに対して，不適切あるいは過度の個人情報を削除するよう命じた．これは，現在，EUにおいて検討が進められている，新たなデータ保護の改革案に盛り込まれた「忘れられる権利」の妥当性を裁判所が先取りし認定したものだとして，大きな反響を呼んだ（忘れられる権利については規則案概要の「データ主体の権利の強化」の項で後述する）．

本稿は，EUにおける現行のプライバシー保護およびデータ保護に関する法的な枠組みがどのような経緯で作られてきたのかを振り返りながら，EUにおいて現在検討されているデータ保護の改革案のポイントや課題について簡潔に解説を行うものである．本稿は法律を専門とされていない方にとってできるだけ分かりやすくすることを目指している．より専門的な視点からの解説を望まれる方は，ぜひ，参考資料として挙げた文献をご参照いただきたい．

■EUにおける沿革

第二次世界大戦前後の状況

個人情報の保護の基礎をなすプライバシー保護の法理が発展したのは，主に米国においてであった．1890年にSamuel D. WarrenとLouis D. Brandeisがハーバードローレビューに発表した「プライバシーの権利（The Right to Privacy）」がその後のプライバシー権に関する議論の発展の基礎を築いたとされる．その後，1900年代に入り，プライバシー権をめぐる多くの裁判例の蓄積を経て，プライバシー権の骨格が徐々に形成されていった．

これに対し，欧州において，プライバシー権とそれを基礎とする個人情報の保護が法制化されるのは，第二次世界大戦以降のことである．ドイツ・ナチスによるユダヤ人など「ナチス国家の敵」に対し，カード・カタログにより個人データをパンチカードに記録し，管理を行ったという悲劇的な教訓が背景にあった．

1950年欧州人権条約から1970年代の各国でのデータ保護法制定の時代

第二次大戦後，欧州では，このような犯罪を防止するため，欧州統合に向けて設立された欧州議会が，1950年に「人権と基本的自由の保護のための条約（「欧州人権条約」）を公布した（1953年に発効）．その第8条で「すべての者は，その私生活及び家族生活，住居並びに通信の尊重を受ける権利を有する」と定め，ここに初めて欧州においてプライバシー権が法定されたのである．

その後，60年代，70年代に入り，コンピュータ

や情報通信技術の飛躍的発達により，欧州諸国の企業と政府との間でさまざまなデータ共有が可能となった．一方で，それは，欧州においてデータ流通とプライバシー保護やデータ保護についての議論を引き起こすこととなった．欧州人権条約は，個人データの処理を適切に扱うための規定を設けておらず，コンピュータによる個人データの処理を適切に規制することができないと考えられた．そこで，プライバシー保護とデータ保護の必要性に迫られた欧州各国は，国民の権利を確保するために，独自の個人データ保護法を制定し始めたのである．しかし，各国の保護法は，個人データの国外処理を制限する条項を定めており，それは，自国民のプライバシー保護には役立つものの，諸国間の情報の自由な流れを妨げるという弊害をもたらした．このような個人データ保護法は，全地球規模の通信ネットワークを保持し，欧州の市場を席巻してきた米国にとって，経済的にも大きな脅威となった．

	OECD プライバシーガイドライン（1980）	EU データ保護指令（1995）	我が国個人情報保護法（2003）
目的	プライバシーと個人の自由を保護し，かつプライバシーと情報の自由な流通という基本的ではあるが競合する価値を調査させること	**個人の権利と基本的な自由，**特に個人データの自動処理に関するプライバシーの権利の尊重の保証（データ保護）	**プライバシー保護とは別に，特定の個人を識別できる「データ」の保護を定める．**
原則等	1. 収集制限の原則 2. データ内容の原則 3. 目的明確化の原則 4. 利用制限の原則 5. 安全保護の原則 6. 公開の原則 7. 個人参加の原則 8. 責任の原則 （OECD ガイドラインの 8 原則）	1. 独立した監督機関 2. 司法による救済 3. データ越境制限 4. 最少データ取得原則 5. 公正で合法的な手続き 6. 監督機関への報告 7. 使用後のデータ廃棄 8. センシティブデータの保護 9. 意思決定の自動化の制限 10. ダイレクトマーケティング利用におけるオプトアウト	1. **主務主管庁制度（独立した第三者機関は存在しない）** 2. 法律の名宛人は事業者（主務大臣による事業者への行政命令が基本，利用者の直接的な救済は民法をベースに裁判所で判断） 3. 利用目的による制限 4. 適正な取得 5. 正確性の確保 6. 安全性の確保 7. 透明性の確保

出典）総務省 「パーソナルデータの利用・流通に関する研究会報告書」（案：2013 年 6 月）を基に編集

表 -1　OECD ガイドライン，EU データ保護指令と我が国個人情報保護法の比較

1980 年 OECD プライバシーガイドラインと欧州議会の条約第 108 号制定の流れ

そこで，個人情報の適正な取り扱いに関するルールを定め，情報の自由な流れと個人のプライバシー保護を調和させることを委ねられたのが，経済協力開発機構（OECD）である．OECD は，1980 年に「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告（「OECD ガイドライン」）を採択した．同ガイドラインは，その基本原則として，「収集制限の原則」，「データ内容の原則」，「目的明確化の原則」，「利用制限の原則」，「安全保護の原則」，「公開の原則」，「個人参加の原則」，「責任の原則」の 8 原則を定めた（一般に「OECD 8 原則」と呼ばれる）．OECD ガイドラインは，経済的に欧州と米国の利害調整をしつつ，各国のプライバシー保護の理念的な対立を乗り越え，強制力を持たない「勧告」ながら，データ保護について国際的な水準を示すことで，各国の法制度の指導的な役割を担うこととなった．これは現行の我が国の個人情報保護法制定にも大きな影響を与えている．OECD ガイドライン，後に説明する EU データ保護指令と日本の個人情報保護法のおおまかな比較を**表 -1** に示しておく．

このように，OECD プライバシーガイドラインは，1980 年の制定以降，データ保護の国際的水準を示すものとして各国のデータ保護法制の指標となってきたが，情報通信技術の急速な進展等個人情報をめぐる環境が大きく変化したことにより，改正の検討が求められることとなった．ガイドラインの 30 周年記念を契機に 2010 年から検討が開始され，改正案は 2013 年 7 月に合意され，同年 9 月に公表されるに至っている．

それとほぼ同時期（OECD ガイドライン制定の 1 週間前）に，欧州評議会の閣僚委員会においても，個人データのプライバシー保護とデータ流通の調整を図るため，「個人データの自動処理に係る個人の保護に関する条約」（「条約第 108 号」）が採択され

た（1985年に発効）．同条約は締約国を拘束する「条約」である点や自動処理されたデータに対象範囲を限定している点で，OECDガイドラインと異なる点があるものの，同ガイドラインと同様に，各国が制定すべき個人データ保護に関する一連の基本原則を定めるものであった．その後，同条約は，ディジタル分野におけるプライバシー保護の強化とフォローアップの仕組みを強力なものとすることを目的として，2011年以降改正作業が進められている．

1995年EUデータ保護指令の制定

個人データ保護に関しては，前述のOECDガイドラインや条約第108号が存在していたものの，欧州委員会は，これらが個人データ保護をめぐるその後の状況に十分に対応していないことや，EUの加盟国の制定した個人データ保護に関する法律の保護水準や内容の違いが，情報の自由な移動に関する障害となり，企業や個人の活動に余分な負担をかけていることを認識した．そこで，プライバシー保護と情報の自由な流通を調整し，EU加盟国の個人情報に関する国内立法の調和，統一を図ることを目的として1995年10月，「個人データの取扱に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（「保護指令」）が採択され，加盟国は当該指令を遵守するために必要な国内法の整備を義務づけられた．

保護指令第1条では，基本的人権の1つとしてプライバシー権が保護される旨が明記されており，第6条以下でOECDプライバシーガイドラインの諸原則（8原則）に対応した一般原則が規定されている．さらにEU保護指令第28条は，各加盟国にパーソナルデータ保護のための独立した監督機関の設置を義務づけている．これに基づき各国で設置されたデータ保護機関（Data Protection Authority：DPA）が，各国内でパーソナルデータ保護の監督等の活動を行っている．また，保護指令第25条は，EU域内から第三国への個人データの移転は，原則として第三国が十分なレベルの保護措置を確保していることを条件としているが，その「十分なレベルの保護措置」の要素の1つとして，「独立した機関の形態をなす外部監督の制度」が挙げられている．これに対し，我が国では，民間部門を対象とした個人情報保護法は当時制定されていなかったため，EU加盟諸国からのデータ移転が禁じられることが危惧された．「十分なレベルの保護」に適合するような対策を講じるため，民間部門を対象にして個人情報保護を目的とした法律の整備を行う検討が開始され，2003年に「個人情報保護法」が制定されたものの，独立した第三者機関は設置されず，執行力の面で課題を残したままとなっていた．2014年6月に出された政府大綱では，現行の個人情報保護法を改正し第三者機関を設置する方針が明記され，また，第三国へのデータ移転についても合わせて制限規定を盛り込むことが基本合意されている．

その後，この分野横断的な保護指令に加え，電子通信部門におけるパーソナルデータ保護に関する特則を規定するものとして，2002年に「電子通信部門における個人データの処理とプライバシーの保護に関する指令」（「eプライバシー指令」）が採択され，加盟国は当該指令を遵守するために必要な国内法の整備を義務づけられた．

EUにおけるデータ保護改革に関する新たな動き

■一般データ保護規則案の提案

保護指令が制定された1995年当時はインターネットの黎明期であった．その後のインターネットを含めたネットワーク技術の急速な進展と経済のグローバル化を受けて，既存の制度枠組みでは，個人情報保護の問題に対処しきれない状況になった．そこで，インターネットユーザの個人情報を効果的にコントロールし，同時にEU域内のディジタル単一市場（digital single market）とデータ保護の一貫性ある体制を実現する目的で，保護指令が全面的に見直されることとなったのである．

まず2009年5月に開催された欧州委員会のブリュッセル会議に端を発し，2010年11月には欧州委員会から保護指令の見直しにあたっての主要課題と

数々の施策方針が示された．その後，同報告書へのパブリックコメント手続きや欧州議会における議論を経た上で，2012 年 1 月に欧州委員会は，現行の保護指令に代わるデータ保護に関する新たな規則提案（「個人データの取扱いに関する個人の保護と当該データの自由な移動に関する欧州議会及び理事会の規則」（「規則案」）を発表した．

2013 年 10 月には，欧州議会における専門委員会（「LIBE 委員会」）は，EU 委員会が提出した原案を修正の上，可決した．膨大な数の修正案が提示されたが，この背景には米国の IT 企業を中心とするロビー活動が活発にあったことが指摘されている．さらに，欧州議会は，2014 年 3 月に LIBE 委員会の修正案を可決している．しかし，規則案が法律として有効に成立するためには，欧州議会の承認のみならず，加盟国の閣僚で構成される閣僚理事会の承認も必要となるが，必ずしも加盟国のコンセンサスは得られていない状況である．イギリス，デンマーク，ハンガリー，オーストリア，ドイツの各政府は，「指令」から「規則」という法的拘束力をまったく異にする構造（規則案概要の「法的拘束力の強化」の項で後述する）に転換することへの憂慮が示されている．また不一致の最大の原因には，複数の加盟国に拠点を持つ管理者や処理者の行為について，主要な拠点のある国の監督機関が一括して管轄する One-stop-shop の構造にあるともいわれている（規則案概要の「監督機関の権限強化」の項で後述する）．

その後，2014 年 5 月には欧州議会の選挙が行われ，議会の構成も変更された．EU 支持派である主要 3 会派（欧州人民党，社会民主進歩同盟，欧州自由民主連盟）が大幅に議席を減らし，反 EU 勢力が議席を伸ばした．新議会ならびに欧州委員会の主要ポストを占める新たなプレーヤたちが，規則案の審議を今後どのように進めていくかはきわめて不透明な状況にあるといえよう．

1995 年制定の保護指令が採択されるまでに 5 年の歳月を要した．現行指令に比べ，各国の立法裁量を抑え，利用者の権利と事業者側の義務を大幅に拡大・強化しようとする野心的な規則案が可決されるまでには，なお紆余曲折が予想される．さらに，規則案の行方は，当然に，我が国の個人情報保護法制のあり方にも大きなインパクトを及ぼしてくると予想されることから，その動向には注視をしていく必要がある．

■ 一般データ保護規則案の概要

規則案をめぐり加盟各国間で政治論争が激しく行われているところであるが，それを記述することは本稿の目的とすることではない．本稿では，全体像を理解していただくため，できるだけ 2014 年 3 月に欧州議会において承認を受けた規則案の修正案をベースに現行の保護指令と比較しつつ（概要比較を**表 -2** に示す），規則案の主要改正点について簡潔に解説を行っていきたい．

法的拘束力の強化

保護指令（Directive）は，その法的な効果が及ぶためには，加盟国内においてそれぞれ国内法として法制化することが求められる．そのため，加盟各国に独自の個人情報保護に関する法律が制定され，それぞれの加盟国がある程度の裁量をもってその法律の運用を行ってきた．規則案では，その規制の位置づけが，これまでの「指令（Directive）」から「規則（Regulation）」に格上げされている．「規則」は，EU の加盟国の法令を統一するために制定され，加盟国に直接の効力を持ち，個々の国に効力をもたらすための国内法を必要としない．また，すべての国内法に優先するものである．このように各国の法令適用の裁量権を抑制する規則化への格上げに対し加盟国のコンセンサスは必ずしも得られているわけではない．この法構造のあり方そのものが，加盟国間の最大の争点の 1 つとなっている．今後の閣僚理事会における議論も含めて改めてその動向を注視していく必要がある．

保護されるべき個人情報の範囲の拡大

保護指令では，「個人データ」を「識別された，または，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」と広範な規定になっていた．規則案では，これをベースにしつつ，さらに，位置

	EUデータ保護指令	一般データ保護規則案
個人情報の範囲	・識別されたまたは識別することのできる自然人に関するすべての情報 ・センシティブデータの処理の禁止	・識別されたまたは識別することのできる自然人に関するすべての情報 ・仮名化データの追加 ・プロファイリングデータの追加 ・センシティブデータに遺伝データと前科または関連する安全措置が追加
適用範囲（および域外適用）	・自動処理される個人データおよびファイリングシステムを構成する個人データ ・処理が加盟国の域内に設置された管理者の活動に関連して行われる場合や域内に設置された設備で利用してデータ処理されている場合の域外適用	・同左 ・域外適用を指令以上に拡大（域内に設置がなくとも，域内データ主体へのサービス等の提供や行動監視を行っている場合に適用）
データ主体の権利	・データ主体の同意（自由かつ十分に情報を提供された上での意思表示） ・データ主体の修正，消去・ブロック権	・データ主体の同意（自由かつ特定的情報を受けた上での明確な意思表示）と管理者の同意取得の立証責任，データ主体の同意撤回の権利 ・データ主体への個人データの削除および拡散を停止させる権利（削除権） ・プロファイリングへの異議申立て権
事業者の義務	・「管理者」および「取扱者」の一般的義務 ・行動規範の策定促進	・同左 ・行動規範の策定促進（考慮規範に消費者の権利尊重を追加） ・データ保護担当者（data protection officer）の指名（中小企業の免除要件） ・データ侵害の通知義務 ・認証制度の奨励（「欧州データ保護シール」） ・データ保護・バイ・デザインとデータ保護影響評価の導入
データ移転	・十分性を満たしていない第三国への個人データ移転を原則禁止	・欧州委員会が十分な保護レベルの決定を下した場合に第三国等へのデータ移転が認められる ・十分性の決定を下していない場合は適切な安全装置を講じることでデータ移転が認められる ・その他例外的取り扱い（データ主体の同意他）
監督機関	・1つまたは複数の機関による監督責任とその独立性の担保 ・監督機関の権限（アクセス・調査権限，仲裁権限，訴訟手続開始権限等） ・罰則と救済（司法的救済と罰則を国内法で規定する）	・監督機関の完全独立性と公平性維持の要件 ・監督機関の執行権限を強化し強制力ある制裁権限を付与 ・データ主体の監督機関への苦情申し立ておよび司法救済を求める権利の明記 ・100M€または全世界年間売上高2%を上限とする制裁金

表-2　保護指令と規則案の概要比較

情報，特有の識別子，生体的データ，遺伝的データ，健康に関するデータ等が追加されている．さらに，議会修正案において「仮名化データ（pseudonymised data）」と「プロファイリング」が追加された点が注視されるべきであろう．仮名化とは，氏名等本人を特定する識別子を他の識別子に置き換えることにより，本人の特定をさせずに同一人物に関する追加データの取得を可能とする方法である．遡って追跡可能な仮名化されたデータは間接的に識別することができる個人に関する情報とみなされるのである．これに対し，匿名化データ（anonymous data）は，技術的にデータ主体が識別できない形にまで加工されたデータであり，仮名化データとは区別されている．匿名化データにはデータ保護の原則が適用されないこととなっている（保護指令前文26項）．ただし，どのような匿名化を行えばデータ保護法の適用をされずに活用されるのかについては，欧州委員会における専門部会において，匿名化技術に関する意見書が2014年6月に示されている．それによれば，匿名化に単一の基準はなく，ケース・バイ・ケースによる判断が必要であり，また完全な匿名化というものは存在しない，とされている．匿名化の要件については引き続き議論されていくことであろう．

また，「プロファイリング」とは，一定の個人の特性や職務能力，経済状況，位置，健康等さまざまな観点から自動的に評価分析することで，これによりさまざまな差別に至るおそれがあることから，個人データの一形態として定義に追加された．また，

データ主体に対するプロファイリングに対する異議申立ての権利（「プロファイリングされない権利」）が追加されることとなった（同権利については規則案概要の「データ主体の権利の強化」の項で後述する）．

域外適用の明記

保護指令は，第4条でデータ保護に関して各国が定める国内法を適用するには，データ処理を行う管理者が加盟国内に事業所を設置しているか，事業所が設置されていない場合には，そのデータ処理の設備を加盟国領域内に置いて活動していることを要件としていた．ところが，規則案では，必ずしも管理者の事業所がEU域内に設置されていなくとも，域内の利用者（データ主体）への商品やサービスを提供し，その利用者の行動監視を行っている場合には，規則案が適用されるとする「域外適用」が新たに規定された．後述する制裁規定とともに，Google等を念頭に置いた規制強化とみられているが，その実効性についてはなお慎重な議論が必要であると思われる．

データ主体の権利の強化

保護指令におけるデータ主体の権利規定をベースにしつつ，規則案は，データ主体の権利のさらなる強化を目指している．

①同意原則の強化

利用者による「明確な同意」の定義をより詳細に規定するとともに，利用者の同意の撤回権と，データ管理者による同意の立証責任などの新たな要件が加えられている．

②忘れられる権利および削除権

保護指令は，利用者に不完全，不正確なデータを修正，消去またはブロックする権利を認めていた．規則案は，さらに利用者のデータに対するコントロールの権利を強化するため，収集された目的にとってもはや必要ではなくなった際にはデータを完全に消してもらう権利として「忘れられる権利」が設けられることとなった．その名称から世界的に注目を浴びたが，この権利は規則案において新たに創設されたものではなく，保護指令の削除権を精緻化し具体化したものであると説明されている．それゆえ，冒頭で紹介した欧州裁判所によりGoogleに対するデータ削除命令の判決が可能であったことが理解できる．なお，2014年3月の議会修正案で「忘れられる権利」の文言は削除され，「削除権」と修正されている．

③プロファイリングされない権利

「忘れられる権利」に比べてあまりマスコミで注目されてこなかったが，規則案では「プロファイリングされない権利」が盛り込まれている．行動ターゲティングなどビッグデータ解析をベースに新たな事業を展開しようとする事業者にとっては非常にインパクトのある規定であろう．

前述のとおり保護されるべき個人データの1つにプロファイリングデータが規定され，すべての人が，「一定の特性を評価し，個人の職務能力，経済状況，位置，健康，個人的嗜好，信頼性や行動を分析，予測することを目的とした自動処理のみに基づく措置（プロファイリング）に対する異議申し立てを行う権利（「プロファイリングされない権利」）が認められた．

プロファイリングに関しては，2010年11月に欧州評議会がその規制化に向けた勧告を採択しており，また，世界のプライバシー法制について議論を行っているデータ保護プライバシー・コミッショナー国際会議の2013年9月会合でもプロファイリング禁止に関する決議が採択されるなど，ビッグデータ・ビジネスを背景としたプロファイリングに対する規制化が国際的な潮流となりつつある．この点を考慮し，我が国の政府大綱でも，プロファイリング問題は，現状では民間の自主規制に委ねるとしつつも，継続して検討すべき課題とされた．なお，米国では，一般的にWebサイトやオンラインサービスにおいて個人識別可能な情報を収集することに対しDo Not Trackを選択し得ることをプライバシーポリシー上で明記すべきという形（追跡拒否権）で議論されている．連邦法においては未成立であるが，カリフォルニア州では2013年9月に法制化されている．

事業者の義務の強化

規則案では，事業者（個人データ処理の決定等を行う「管理者」と「管理者」のために処理を行う「処理者」がいるが，本稿では，表記を簡単にするため両者を合わせて「事業者」としている）に対する「文書化の義務（自らの責任に基づくすべての取扱業務に関する文書の保持義務）」や「安全保護義務」等の義務規定に加えて，以下に述べるようなさまざまな義務規定を設け，データ保護の実効性を高めるため，事業者の義務の強化を図っている．

①データ保護・バイ・デザイン

事業者の一般的義務規定に加えて，「データ保護・バイ・デザイン及びデータ保護・バイ・デフォルト」が設けられた．これはカナダで提唱された「プライバシー・バイ・デザイン（PbD）」を取り入れた規定である．PbDは，前カナダ・オンタリオ州の情報・プライバシー・コミッショナーである，Ann Cavoukian博士が1990年代から提唱してきた考え方で，さまざまな技術に関する設計仕様にプライバシーを組み込むという考え方である．PbDはプライバシー促進技術（PETs）をもとに発展してきた概念とされる．規則案は，PbDの考え方を取り入れ，事業者に対し，最新技術や実施費用を考慮しつつ，適切な技術的・組織的対応を行うことを義務づけている．

②データ侵害の通知義務

利用者のデータ侵害が生じた場合には，事業者は，遅滞なく，監督機関に通知すべき義務が追加されている．委員会原案では，「可能であれば24時間以内に」通知すべきとされていたが，その実効性に問題があるとされ，議会修正案で，その文言は削除された．ただし，規則案前文で72時間以内の通知が要求されている．

③データ保護評価

規則案では，事業者は，リスクのある取扱業務に先立ち，データ保護影響評価を実施するよう義務づけられることとなった．この制度は，米国，カナダ，オーストラリア等で行われてきたPIA（Privacy Impact Assessment）に相当するものである．我が国の共通番号法にも一部導入されている．PIAとは，情報システム等におけるプライバシー保護策についての評価手法であり，この評価を通じて改善点を見出し，プライバシー保護の最適化を目指す仕組みである．PIAの具体的な評価手法等については，今後，EU委員会における専門部会で検討されていくものと思われる．

④データ保護担当者の指名

事業者におけるプライバシー保護を実効あらしめるため，規則案は，事業者に対し，「データ保護管理者（data protection officer）」を指名すべきことを命じている．ただし，中小企業等への一定の配慮が行われ，免除要件が検討されている．委員会原案では，従業員250名以上の企業を対象としていたが，議会修正案で，「過去12カ月間5,000件以上」のデータ処理を行っている企業を対象とする旨修正が行われている．

データ保護管理者には，一定の任期を保証する（従業員4年，外部契約者2年）とともに，事業者に対し新規則案の義務遵守に関して「通知」「助言」を行わせるべきことを定めている．

⑤認証制度の奨励

規則案では，事業者によるデータ保護レベルを迅速に評価できるよう，データ保護認証の仕組みや標準的なデータ保護マークの確立を奨励しなければならないと定められた．我が国では，すでにプライバシーマーク付与適格性審査制度が導入され，普及している．EUにおいても同種の制度が導入されたことは，我が国の取り組みに対する一定の評価が下されたものとして注目に値するであろう．

第三国へのデータ移転制限規定の詳細化

保護指令においても第三国への個人データの移転が一定の要件のもとで制限されていたが，規則案は，さらに詳細に条件を規定している．独立監督機関（プライバシーコミッショナー）の必要性や十分性認定に代わり，欧州委員会が承認した，個人データの取扱い等を定める標準契約を第三国の当事者間で締結する場合に，当該事業者間のデータ転送が認められる「標準契約条項」の取扱いや，主に多国籍企業を

対象とし，監督機関による法執行可能性や法令遵守の実践性に留意した準則（ルール）を策定し，EU内の監督機関がそのルールを承認した場合にデータ流通が認められる「拘束的企業準則（BCR）」の明文化等が行われている．

ところで，2013年6月に発覚したPRISM問題を契機に，欧米間では「セーフハーバー協定」の存続について激しく議論が戦わされている．統一的なプライバシー保護に関する法律を規定しているEU（オムニバス方式と呼ばれる）と異なり，米国では，事業分野別にプライバシー保護の規定が定められ（セクトラル方式と呼ばれる），統一法が存在しない．この法体系の違いからEUからの十分性の認定を受けられないことを危惧した米国が，EUと足かけ5年にわたる交渉を行い，合意に至ったのが上記協定である．米国務省が，申請した企業のセーフハーバー・プライバシー原則に適合しているか審査の上，認証を行い，その一覧を公表している．セーフハーバーのプライバシー原則に違反した場合，米国連邦取引委員会が法執行の権限を有している．

現在，日欧間におけるデータ流通問題は表立って議論されることはなさそうだが，政治・経済関係の動向如何で日欧間で政治問題化する可能性もある．我が国の個人情報保護法の改正を契機に，EUに対する十分性認定の申請の可否を含め，早急かつ慎重な検討が必要である．

監督機関の権限強化

規則案は，保護指令をベースにしながらも，プライバシー保護の執行力を高めるため，監督機関（プライバシーコミッショナー）の独立性や権限を強化するとともに違反行為に対する行政的制裁を課す権限を付与する規定を盛り込んでいる．

①監督機関の完全独立性の明記

保護指令において，監督機関の独立性は規定されていたが，欧州裁判所において，ドイツの監督機関の独立性が否定された判決が2010年3月に出されてしまい，現行指令は，監督機関の完全独立性を必ずしも保証していない点が問題とされていた．規則案は監督機関の完全独立性を明記するとともに，詳細にその義務および権限について規定している．

②執行権限の明記

保護指令のもとでは，EU加盟国間において執行のばらつきがあることが指摘されていた．規則案は，監督機関の執行権限を詳細に規定することでそのばらつきを解消している．

③相互支援体制の強化

保護指令においては，各監督機関は相互に協力しなければならない，という単純な条文のみが置かれていた．しかし，規則案では，委員会原案に，One-stop-shopの概念が導入された．One-stop-shopは，加盟国間の監督機関の権限と運用にバラつきがあり，加盟国によって対応が割れてしまうというデメリットを克服する目的で提案されたものである．委員会は，複数の加盟国に拠点を持つ事業者の行為について，主要な拠点のある国の監督機関が全加盟国における処理活動を管轄することでOne-stop-shopの構造を示した．そして，いかなる国の監督機関でも苦情申立てを受理することで加盟国間の利用者の権利を統一的に保証することを狙いとしている．議会は委員会提案を承認し，さらにOne-stop-shopの考え方を「一貫性ある対応（consistency mechanism）」として強固なものとしている．これに対し，冒頭に述べたとおり，One-stop-shopに対する理事会における加盟国間の対立は強く，新規則案をめぐる最大の争点となっており，理事会における今後の審議動向が注視されるところである．

④制裁規定の具体化

保護指令では，加盟国に違反に対する制裁の規定を設けるべきことを定めるにとどまっていたが，規則案では具体的な制裁について条文が置かれた．委員会原案では，違反の種類を列挙し，それによる段階的制裁金が設けられていた（最も高額な場合で，100万ユーロ，または，全世界の総売上の2%まで）．それに対し，議会修正案は，3種類の制裁（文書警告，定期的保護観察，制裁金）から1つを監督機関に選択させる方式を採用している．制裁金についても，「1億ユーロ，または全世界の総売上5%まで」と定め，大幅に増額した．域外適用の問題に加え，高額

な制裁金賦課に対し，米系企業を中心に海外事業者の反発は強い，引き続き強力なロビー活動が展開されるものと思われる．今後の理事会の審議において，ある程度の揺り戻しがあるかもしれない．

今後の展望

駆け足でEUにおける個人情報保護制度をめぐる動向を，保護指令が出されるまでの経緯を振り返りながら，現在，審議が進められている規則案の概要とその要点についてまとめてみた．プライバシー保護のあり方は，その文化的背景の違いを反映してさまざまに異なり得る．我が国におけるプライバシー保護のあり方が今後どうあるべきなのかを考える上で，欧州における議論は野心的でチャレンジングではあるものの，大いなる示唆を我々にもたらす．ビジネスに携わる者の1人として，規則案の行方は非常に気にかかり，絶えず，その動向を注視してきた．しかしながら，規則案は前文139項，全11章，91条で構成される膨大な法文である．また，委員会が提出した原案も大幅に修正され，議会で可決される際にも数々の修正を経ている．その複雑多岐にわたる条文を網羅的に解説することは困難であるが，幸いにも，参考文献として挙げさせていただいた優れた文献，資料が存在している．本稿もそれらを頼りとして，その一部を紹介した．ただ，現在，我が国でも検討が進められている個人情報保護法の改正のあり方を考える上で，最低限押さえておくべき項目は押さえたつもりである．本稿において狙いどおりの効果が得られたかどうかは，ぜひ，読者の方々のご判断にお任せしたい．

参考文献

1) 石井夏生利：個人情報保護法の理念と現代的課題―プライバシー権の歴史と国際的視点，勁草書房 (2008).
2) 石井夏生利：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).
3) 小林新太郎：パーソナルデータの教科書，日経BPマーケティング (2014).
4) 消費者庁：個人情報保護における国際的枠組みの改正動向調査報告書（2014年3月28日）.
5) 宮下　紘：プライバシー・イヤー2012―ビッグデータ時代におけるプライバシー・個人情報保護の国際動向と日本の課題，Nextcom, Vol.12 (2012).

(2014年9月4日受付)

■**高崎 晴夫**　ha-takasaki@kddi.com
（株）KDDI総研　取締役主席研究員．1980東北大学法学部卒，1980年国際電信電話（株）（現KDDI（株））入社．2005年より現在に至る．プライバシー保護政策等の研究に従事，ISO/SC 27/WG 5委員，カナダ・オンタリオ州よりプライバシーバイ・デザイン・アンバサダーの認定を受ける．