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

平成 22 年 3 月

目　次

Ⅰ　調査研究の概要

Ⅰ　調査研究の概要

１．調査研究の目的

個人情報保護の取組を推進するに当たっては、OECD を始めとして、APEC、EU など様々な場で進められている取組を踏まえ国際的な協調を図っていくとともに、我が国の法制度についても国際的な理解を深めていくことが重要であるとされている（「個人情報の保護に関する基本方針（平成 16 年 4 月閣議決定）」）。

現在、OECD では、プライバシー法執行の越境的な課題が検討されており、APEC では、越境的なプライバシー規則の構築、情報共有及び調査・執行の越境協力の課題などが検討され、国際的な取組が進められている。また、EU 諸国においては、EU データ保護指令（EU Data Protection Directive）に基づき、個人情報保護に係る第三者機関が存在しており、この機関を中心として、国内及び国際的な個人情報保護に関する問題を処理している。

今後の我が国における個人情報保護制度を考えるに当たっては、我が国の制度や実態に加え、これらの OECD、APEC、EU などの国際機関における国際的動向を十分に踏まえる必要がある。

とりわけ、EU データ保護指令では、EU と同等のレベルにない個人情報保護法制を有する第三国へのデータ移転を原則禁止するという厳格な規定を有している。他方で、同条項の特例制度として拘束的企業準則（BCR）やモデル契約（なお、本報告書では、「モデル契約」のほか、「SCC」、「標準契約」という単語が使われているが、いずれも同じ意味で使用している。）が設けられており、日本企業の同制度の利用可能性について、企業の見解を聞きつつ、調査・分析することが重要である。

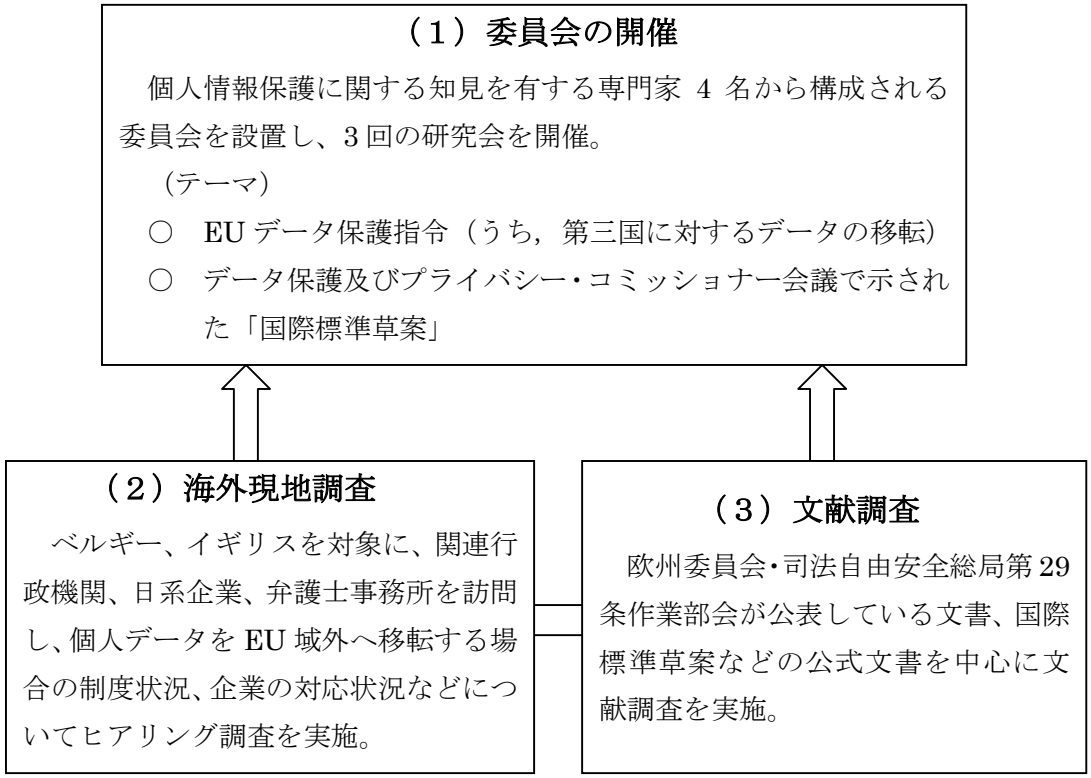
また、EU は、アメリカ合衆国やオーストラリアとの交渉経験から、EU データ保護指令を EU 域外の諸外国へ押しつけるのではなく、諸外国との調和・妥協点を探る動きも見せている。その具体的な案が、2009 年にスペインで開催されたデータ保護及びプライバシー・コミッショナー会議で示された国際標準草案である。この国際標準草案は、EU 基準そのものを反映したものではなく、世界の最大公約数的な要素を抽出したものであり、世界共通の個人情報保護ルールの形成を図ろうとしている。

この国際標準草案が、日本の国際取引を行う企業にどのような影響があるのか、その内容を調査することは重要である。

そこで、本調査では、EU 域外へのデータ移転の方法（拘束的企業準則、モデル契約）、国際標準草案の内容及びそれらに対する日本企業の対応状況について、研究会を設け、調査・分析を行った。

２．調査研究の内容

【調査研究の全体像】



（１）委員会の開催

【委員会の設置】　　＊敬称略

座長	堀部　政男	一橋大学名誉教授
	石井　夏生利	情報セキュリティ大学院大学准教授
	武井　一浩	西村あさひ法律事務所パートナー弁護士
	藤原　靜雄	筑波大学法科大学院教授

【オブザーバー】

濃川　耕平	西村あさひ法律事務所 弁護士
松本　絢子	西村あさひ法律事務所 弁護士
迎　奈央子	西村あさひ法律事務所 弁護士

【委員会の開催】

	議事内容
第 1 回研究会	1. 調査の趣旨説明 2. 拘束的企業準則の制度的概要について 3. 海外現地調査の概要説明
第 2 回研究会	1. 第三国ルールと企業の対応状況について 2. 国際標準草案について 3. 海外現地調査の質問項目について
第 3 回研究会	1. 海外現地調査報告－ベルギー・イギリス－ 2. 報告書のとりまとめについて

（2）海外現地調査

①訪問先

【ベルギー】

- ○ 欧州委員会・司法自由安全総局（European Commission Directorate-General-Justice, Freedom and Security）
- ○ リンクレーターズ法律事務所（Linklaters LLP）
- ○ 在欧日系ビジネス協議会（Japan Business Council in Europe, JBCE）
- ○ 日系企業（3 社）

【イギリス】

- ○ ICO（Information Commissioner's Office）
- ○ 日系企業（3 社）

②主な質問項目

- ○ EU 域外への個人データ移転の現状（移転するデータの内容、方法など）
- ○ 第三国に対するデータの移転を禁止する EU データ保護指令及びその特例（Derogations）に対する認識
- ○ 特例（Derogations）制度としての BCR（Binding Corporate Rules）とモデル契約への認識と利用状況
- ○ BCR やモデル契約を利用する際の弁護士等の専門家の利用状況
- ○ BCR やモデル契約を利用する際の課題や障壁　　など

３．報告書の構成と執筆担当

本報告書の構成と執筆担当者は以下のとおりである。

Ⅰ　調査研究の概要	－
Ⅱ　EU データ保護指令と個人データの国際移転	1．EU における個人データの国際移転に関する実態 堀部　政男　　一橋大学名誉教授
	2．BCR の制度的概要 石井　夏生利　　情報セキュリティ大学院大学准教授
	3．モデル契約の概要 武井　一浩　　西村あさひ法律事務所　弁護士 濃川　耕平　　西村あさひ法律事務所　弁護士 松本　絢子　　西村あさひ法律事務所　弁護士 迎　奈央子　　西村あさひ法律事務所　弁護士
Ⅲ　「個人データの処理に係るプライバシー保護の国際標準のための共同提案」について	藤原　靜雄　　筑波大学法科大学院教授
Ⅳ　まとめ	藤原　靜雄　　筑波大学法科大学院教授

＊本調査研究の事務局作業は、社団法人日本リサーチ総合研究所が担当

Ⅱ　EU データ保護指令と個人データの国際移転

Ⅱ　EU データ保護指令と個人データの国際移転

１．EU における個人データの国際移転に関する実態

一橋大学名誉教授　　堀部　政男

（１）EU データ保護指令提案の背景

1）OECD プライバシー・ガイドラインの採択

ア　プライバシー保護と情報の自由な流れ

EU データ保護指令（EU Data Protection Directive）として知られている EU（European Union, 欧州連合）の指令は、個人情報保護法の早期制定国、特に欧州におけるデータ保護法の考え方を反映したものであるといえる。

欧州では、1970 年代に個人情報保護法制定国が現れた。それらの国の中には、個人データの海外移転・国際移転についてデータ保護機関（Data Protection Authority, DPA）と総称されることのある独立性の強い機関の承認を要するものもあった。

一方、データ処理に長けている国は、そのようなプライバシー保護（protection of privacy）傾向に対抗するために情報の自由な流れ（free flow of information）を主張するようになった。

この利害対立の調整をゆだねられたのが、OECD である。OECD は、1978 年初めに、「国際データ障害とプライバシー保護専門家グループ」（Expert Group on Transborder Data Barriers and Privacy Protection）という新しいアド・ホックのグループを設置し、個人データの国際流通と個人データおよびプライバシーの保護についての基本的ルールに関するガイドラインを作成するように指示した。

イ　OECD 理事会勧告（1980 年）

OECD は、この専門家グループの作業を基に、1980 年 9 月 23 日に「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」（Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）を採択した。この理事会勧告は、プライバシー保護の国際水準を示したものとして注目に値するとともに、日本においては、プライバシーをどのようにして保護するかを国レベルで検討する契機の一つになった。これは、最近では、OECD プライバシー・ガイドライン（OECD Privacy Guidelines）と呼ばれている[1]。

[1] OECD プライバシー・ガイドラインなどについては、とりあえず、堀部政男『現代のプライバシー』（岩波書店、1980 年）、同『プライバシーと高度情報化社会』（岩波書店、1988 年）、石井夏生利『個人情報保

ウ　勧告の内容

OECD 理事会は、次のような認識を明らかにしている（邦訳は総務庁行政管理局（当時）の仮訳によるが、一部改訳したところもある）。

「1960 年 12 月 14 日の OECD 条約第一（c）、3（a）及び 5（b）の各項に留意し、加盟国は、国内法及び国内政策の相違にもかかわらず、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、競合する価値を調和させることに共通の利害を有すること、個人データの自動処理及び国際流通は、国家間の関係に新しい形態を作り上げるとともに、相互に矛盾しない規則と運用の開発を要請すること、個人データの国際流通は経済及び社会の発展に貢献すること、プライバシー保護と個人データの国際流通に係る国内法は、そのような国際流通を妨げるおそれがあること。」

理事会は、このような認識に基づき「加盟国間の情報の自由な流通を促進すること及び加盟国間の経済的社会的関係の発展に対する不当な障害の創設を回避することを決意し」、次のように勧告した。

1　加盟国は、本勧告の主要部分である勧告付属文書のガイドラインに掲げているプライバシーと個人の自由の保護に係る原則を、その国内法の中で考慮すること。

2　加盟国は、プライバシー保護の名目で個人データの国際流通に対する不当な障害を創設することを除去し又は回避することに努めること。

3　加盟国は、勧告付属文書に掲げられているガイドラインの履行について協力すること。

4　加盟国は、このガイドラインを適用するために、特別の協議・協力の手続についてできるだけ速やかに同意すること。

エ　勧告付属文書の構成

ここに出てくる勧告付属文書「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」は、第 1 部・総則、第 2 部・国内適用における基本原則、第 3 部・国際適用における基本原則―自由な流通と合法的制限、第 4 部・国内実施、及び第 5 部・国際協力からなっている。それらのうち、第 2 部の「国内適用における基本原則」が、日本におけるプライバシー保護を考える上でとりわけ重要な役割を果たしてきている。

オ　8 原則

上掲の第 2 部「国内適用における基本原則」に示されている 8 原則は、日本でもあまりにも有名であるので、説明は省略し、原則のみを掲げることにする。それらは、次のようになっている。

①収集制限の原則(Collection Limitation Principle)

②データ内容の原則(Data Quality Principle)

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 年）等参照。

③目的明確化の原則(Purpose Specification Principle)
④利用制限の原則(Use Limitation Principle)
⑤安全保護の原則(Security Safeguards Principle)
⑥公開の原則(Openness Principle)
⑦個人参加の原則(Individual Participation Principle)
⑧責任の原則(Accountability Principle)

2）CoE 個人情報保護条約の締結

ア　CoE と個人情報保護条約

日本が OECD 加盟国であるためか、OECD プライバシー・ガイドラインについてはかなりよく知られているが、ほぼ同じ時期に採択された、欧州評議会(Council of Europe, 以下「CoE」という。）の個人情報保護条約はほとんど知られていない。ちなみに、この CoE は、欧州統合の推進を目的として第二次大戦後の 1949 年に設立された国際機関で、日本の外務省の資料によると、現在の加盟国は 47 か国（EU 全加盟国、南東欧諸国、ロシア、トルコ、NIS 諸国の一部）である。その CoE の閣僚委員会は、1980 年 9 月 17 日、「個人データの自動処理に係る個人の保護に関する条約」（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data）（条約第 108 号（Convention 108)）を採択した（当時の加盟国は 21 か国であった)。そして、この条約は、翌 1981 年 1 月 28 日、各国の署名に付され、1985 年に、5 か国目の西ドイツ（当時）が批准をしたので、同年 10 月 1 日に、発効した。この条約に具体化されている個人データ保護の原則は、内容的には OECD 理事会勧告のそれとほぼ同じであるが、形式的には異なった方法で定められている。それらは、ヨーロッパ諸国を基準とした、個人情報の国際水準を示しているので、中身を見ておくことにする[2]。

イ　CoE 個人情報保護条約の概要

7 章 27 か条からなる条約のうち、第 2 章がデータ保護に関する基本原則と題されていて、第 4 条から第 11 条に及んでいる。それらのうち、主要なものと考えられる第 5 条（データ内容)、第 6 条（特別の種類のデータ)、第 7 条（データの安全保護）及び第 8 条（データ主体のための追加的保護措置）を紹介するにとどめることにする（邦訳は総務庁行政管理局（当時）の仮訳によるが、一部改訳したところがある)。

[2] CoE についても、堀部政男『現代のプライバシー』（岩波書店、1980 年)、同『プライバシーと高度情報化社会』（岩波書店、1988 年)、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 年）等参照。

・データ内容等

まず、データ内容(Quality of data) に関する第 5 条は、次のようになっている。

「自動処理を受ける個人データは、

a　公正かつ適法に収集され、処理される。

b　明確化されたかつ正当な目的のため蓄積され、かつこれらの目的に合致しない形で利用されない。

c　蓄積する目的に照らして十分であり、適切であり、かつ、過剰にわたるものでない。

d　正確であり、必要な場合には最新なものに保たれる。

e　当該データが蓄積された目的のために必要とされる期間より長くデータ主体を特定できる形で保持されない。」

これは、OECD ガイドラインの収集制限の原則、データ内容の原則、目的明確化の原則および利用制限の原則に対応している。

次に、特別の種類のデータ(Special categories of data)に関する第 6 条は、「人種、政治的意見又は宗教、その他の信条を明らかにする個人データ及び健康又は性生活に関する個人データは、国内法により適当な保護措置が採られていない限り、自動処理することはできない。罪科に関する個人データについても同様とする」と定めている。

ヨーロッパ諸国のデータ保護法には、センシティブなデータについて特別の保護措置が採られている場合があるので、このような条項が設けられたと見てよいであろう。

・データの安全保護等

また、データの安全保護(Data security) についての第 7 条は、「偶発的若しくは権限のない破壊又は偶発的紛失並びに権限のないアクセス、改変又は伝幡から、自動処理データファイルに蓄積されている個人データを保護するため適当な安全保護措置を採る」としている。

これは、OECD ガイドラインの安全保護の原則に相当する。

さらに、データ主体のための追加的保護措置(Additional safeguards for the data subject)にかかわる第 8 条は、次のように規定している。

「何人も、

a　自動処理個人データファイルの存在、その主たる目的、及びファイル管理者の身元、現住所、又は主たる事務所を確認することができる。

b　合理的な期間でかつ過度な遅滞又は支出を伴うことなく、自己に関する個人データが自動処理データファイルに蓄積されているか否かを確認し、又、わかり易い形で当該データについて通知を受けることができる。

c　この条約の第五条及び第六条に定める基本原則を実施する国内法の規定に違反してデータ処理が行われる場合には、それぞれの場合に応じて当該データを修正、又は消去することができる。

d　この条の（b）及び（c）にいう確認請求、又はそれぞれの場合における通知、訂正若しくは消去の要求が遵守されないときは救済を受けることができる。」

このデータ主体のための追加的保護措置は、OECD ガイドラインの公開の原則及び個人参加の原則に対応する。

ウ　非加盟国の加入

日本は、CoE の加盟国ではないが（1996 年以降、日本はオブザーバー）、この CoE 条約は、非加盟国の加入(Accession by non-member States)についても条項を設けている。これに関する第 23 条は、次のように定めている。

「1　この条約の発効後、欧州評議会閣僚委員会は、欧州評議会憲章第 20 条(d)に規定された過半数による決定及び同委員会に出席する資格のある加盟国代表者の満場一致の議決により、欧州評議会非加盟国に対し、この条約への加入を招請することができる。

2　加入する国に対しては、この条約は、欧州評議会事務総長へ加入書が寄託された日の後の 3 か月の期間を満了した日の属する月の翌月の第一日に効力を発生する。」

前述のように、この CoE 条約は、1985 年 10 月 1 日に発効したので、条約上は、欧州評議会閣僚委員会が、日本に対して、CoE 条約への加入を招請することができる。1980 年代後半にこのような議論もあった。

エ　追加議定書

2001 年 11 月 8 日に、「個人データの自動処理に係る個人の保護に関する条約への監督機関及び越境データ流通についての追加議定書」（Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows）が各国の署名に付された。

これは、3 か条からなるもので、各条の条文見出しは、次のようになっている。

第 1 条　監督機関（Supervisory authorities）

第 2 条　本条約の締約国の管轄に服さない受領者への個人データの越境流通（Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention）

第 3 条　最終条項（Final provisions）

（２）EU データ保護指令提案

1）モデルとなった CoE 条約

日本では、上掲の OECD プライバシー・ガイドラインは有名であるのに対して、CoE 条約についてはこれまでにも紹介してきているけれども、意外に知られていない。

ところが、欧州においては、CoE 条約が大きな役割を担ってきている。CoE 条約は、欧州では、データ保護基本権（fundamental right to protection of personal data）に関する最初の法的枠組みであると考えられているものであって、後述する EU データ保護指令のモデルであるということができる[3]。

2）データ保護指令提案の採択

ア　最初のデータ保護指令提案

当時の欧州共同体（European Communities, EC）理事会（Council）は、1990 年 7 月に、①「個人データ取扱いに係る個人の保護に関する理事会指令提案」（Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data）及び②「公衆デジタル通信網特に ISDN 及び公衆デジタル移動体通信網における個人データ及びプライバシー保護に関する理事会指令提案」（Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital networks (ISDN) and public digital mobile networks）を採択した。

この段階で、①のデータ保護指令提案は、日本のように EC 構成国（当時）でない第三国への個人データの移転についても規定していた（第 24 条）。その第 1 項は、次のようになっていた。

「構成国は、取扱い過程にある個人データ又は取扱いを目的として収集された個人データの第三国への移転は一時的又は恒久的であるかを問わずその国が十分なレベルの保護（adequate level of protection）を確保している場合に限って行うことができるということをその法に規定しなければならない。」

また、その第 3 項は「委員会は、構成国によって提供された情報に基づき又はその他の情報に基づき第三国が十分なレベルの保護をしていないと認定し、また、その結果として生ずる状況が委員会又は構成国の利益を害するおそれがあると認定する場合には、その状況を矯正する目的で交渉に入ることができる」と日本を含む第三国と交渉することがあり得ることを明らかにしていた。

ここに出てくる指令（Directive） というのは、EEC 条約において、「達成すべき結果について、これを受領するすべての構成国を拘束するが、方式及び手段については構成国の

[3] EU データ保護指令などについては、堀部政男「プライバシー・個人情報保護の国際的整合性」、堀部政男編著『プライバシー・個人情報保護の新課題』（商事法務、2010 年）所収などを参照。

機関の権限に任せる」（同条約第 189 条）ものである（これに対し、最も拘束力の強い規則（Regulation）は、「一般的な効力を有し、そのすべての要素について義務的であり、すべての構成国において直接適用することができる」というものである）。換言すれば、指令は、規則のように直接適用するものではないが、構成国を拘束することに注意する必要がある。こうすることによって、構成国間において個人データ保護法の調和・統一を図ろうとする方向が出てきている。

イ　改正提案と採択

この最初のデータ保護指令提案をめぐって各方面で多彩な議論が展開された。それらの議論を踏まえて、EC 委員会は、1992 年 10 月 15 日、「個人データ取扱い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理事会指令の改正提案」（Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data）を明らかにした。

最初の提案の第 24 条は、改正提案では第 26 条となり、ただし書が追加された。それは、次に掲げる場合には、十分な保護を講じていない第三国に対しても移転を行うことができるとするものである。

―……データ主体が契約締結に先立って手段を講じるために提案された移転に同意した場合

―データ主体が十分な保護を講じていない第三国にデータを移転することが提案され又は提案されることがあり得るという事実について情報を与えられていることを条件として、その移転がデータ主体と管理者との間の契約の履行のために必要である場合

―移転が重要な公益上の理由で必要な場合

―移転がデータ主体のきわめて重大な利益を保護するために必要である場合

ちなみに、1991 年 12 月にオランダのマーストリヒトで開催された理事会で「欧州連合条約」（Treaty on European Union）（一般に「マーストリヒト条約」と呼ばれている。）の締結について合意され、1992 年 2 月にこの条約が調印された。マーストリヒト条約は、1993 年 11 月 1 日に発効し、欧州連合（European Union, EU）が発足した。

その後、欧州議会及び理事会は、1995 年 2 月 20 日に「個人データ取扱い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・・・指令を採択するために 1995 年 2 月 20 日に理事会によって採択された・・・共通の立場」（Common Position...adopted by the Council on 20 February 1995 with a view to adopting Directive...of the European Parliament and of the Council of...on the protection of individuals with regard to the processing of personal data and on the free movement of such data）を明らかにした。

これは、「個人データ取扱い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 1995 年 10 月 24 日の欧州議会及び理事会の 95／46／EC 指令」（Directive 95/46/EC of the

European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)として採択された。これが EU データ保護指令(EU Data Protection Directive)、指令 95/46/EC（Directive 95/46/EC）などと略称されているものである。

この EU データ保護指令は、3 年後の 1998 年 10 月 24 日に発効した。

また、前掲の②の「公衆デジタル通信網特に ISDN 及び公衆デジタル移動体通信網における個人データ及びプライバシー保護に関する理事会指令提案」は、これまでに見てきたデータ保護指令よりもかなり遅れて、1997 年 12 月 15 日に「電気通信分野における個人情報取扱い及びプライバシー保護に関する 1997 年 12 月 15 日の欧州議会及び理事会の指令 97/66/EC」（Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector）として採択された。この 1997 年の電気通信分野の指令は、2002 年 7 月 12 日に「電子通信分野における個人情報取扱い及びプライバシー保護に関する 2002 年 7 月 12 日の欧州議会及び理事会の指令 2002/58/EC(プライバシー及び電気通信に関する指令)」（Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications）によって全面的に修正された。

ウ　第三国への個人データの移転―第 25 条

第三国へのデータの移転については、「諸原則」（Principles）に関する第 25 条で最初のデータ保護指令提案の第 24 条の「諸原則」とは少し異なる規定が設けられている（「共通の立場」の段階で修正)。その第 1 項は、次のようになった。

「構成国は、取扱い過程にある個人データ又は移転後取り扱うことを目的とする個人データの第三国への移転は、この指令の他の規定に従って採択されたその国の規定の遵守を損なうことなく、当該第三国が十分なレベルの保護（adequate level of protection）を確保している場合に限って行うことができるということを規定しなければならない。」

この十分性の評価がどのようになされるかについては、第 25 条第 2 項に規定されている。その第 25 条第 2 項は、次のようになっている。

「第三国によって保障される保護レベルの十分性は、一つのデータ移転の運用又は一連のデータ移転の運用に関するあらゆる状況にかんがみ評価されなければならない。特に、データの性格、予定されている取扱いの運用の目的及び期間、発出国及び最終目的国、当該第三国において有効である一般的及び分野別の法規範（the rules of law, both general and sectoral, in force in the third country in question)、並びに当該国において遵守されている専門的規範（professional rules）及び安全保護対策措置（security measures）が考慮されなければならない。」

第 25 条の第 3 項以下の規定は、次のようになっている。

3. 構成国及び委員会は、第三国が第 2 項の規定の意味における十分なレベルの保護を保障していないと考えられる事例について、相互に情報提供しなければならない。

4. 構成国は、第 31 条第 2 項に規定する手続に基づいて委員会が、第三国が本条第 2 項の規定の意味における十分なレベルの保護を保障していないと認定した場合には、当該第三国への同一タイプのデータの移転を阻止するために必要な措置を講じなければならない。

5. 委員会は、適切な時期に、第 4 項に基づく認定によってもたらされる状況を改善することを目的とする交渉を開始しなければならない。

6. 委員会は、第 31 条第 2 項に規定する手続に基づいて、第三国が私生活、個人の基本的な自由及び権利を保護するための当該第三国の国内法、又は特に本条第 5 項に規定された交渉の結果に基づいて締結した国際公約を理由として、第 2 項の規定の意味における十分なレベルの保護を保障していると認定することができる。

構成国は、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。

エ　第 26 条　例外

第 25 条に続く「第 26 条　例外」は、次のように規定している。

1. 構成国は、第 25 条の適用を制約するものとして、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いて、第 25 条第 2 項の規定の意味における十分なレベルの保護を保障しない第三国に対する個人データの移転又は一連の移転は、次の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、データ主体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) 移転が、重要な公共の利益を根拠として、又は法的請求の確定、行使若しくは防御のために必要である場合、又は法的に要求される場合。又は、

(e) 移転が、データ主体の重大な利益を保護するために必要である場合。又は、

(f) 法律又は規則に基づいて情報を一般に提供し、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録から、閲覧に関する法律に規定された条件が特定の事例において満たされる範囲内で、移転が行われる場合。

2. 構成国は、第 1 項の規定に実体的な効果を持つことなく、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、並びにこれらに相当する権利の行使に関して、十分な保護措置を提示する場合には、第 25 条第 2 項の規定の意味における十分なレベルの保護を保障しない第三国への個人データの移転又は一連の移転を認めることがで

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. 構成国は、第 2 項によって付与された許可を、委員会及び他の構成国に通知しなければならない。

一つの構成国又は委員会が、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を含む正当な理由に基づいて異議申立てを行った場合には、委員会は、第 31 条第 2 項に規定された手続に基づいて適切な措置を講じなければならない。

構成国は、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。

4. 構成国は、第 31 条第 2 項に規定された手続に従って、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保護措置を提供していると決定する場合には、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。

3）十分性認定基準

ア　第 29 条作業部会の「作業文書」

日本にとって特に重要であるのは、「十分性」の認定基準である。

EU データ保護指令に定められている第 29 条作業部会（Article 29 Working Party）は、EU データ保護指令の「十分性」基準（データ保護指令第 25 条及び第 26 条）に基づいて評価を行うが、具体的には、「個人データの第三国移転 : EU データ保護指令第 25 条及び第 26 条の適用 (WP 12 5025/98)」*Transfers of personal data to third countries: Applying Articles 25 and* 26 *of the EU data protection directive* (WP 12 5025/98)(adopted by the Working Party on 24 July 1998)（以下「WP 12」という。）という文書によっている。

WP 12 は、次のような章などからなっている。

これらのうち、第 1 章（Chapter 1）の「何が『十分な保護』を構成するか」には、具体

的な基準が示されている。その一部を紹介すると、次のようになる。

（ｉ）実体原則（*Content Principles* ）

基本原則は、次のとおりである。

1）目的限定原則（purpose limitation principle）
2）データ内容・比例原則（data quality and proportionality principle）
3）透明性原則（transparency principle）
4）セキュリティ原則（security principle）
5）アクセス、訂正及び異議申立ての権利（rights of access, rectification and opposition）
6）再移転制限（restrictions on onward transfers）

追加的原則の例

1）センシティブ・データ（sensitive data）
2）ダイレクト・マーケティング（direct marketing）
3）自動処理による個人に関する決定（automated individual decision）

（ⅱ）手続／執行メカニズム（*Procedural/ Enforcement Mechanisms*）

データ保護システムの目的は、基本的には次の 3 要素を満たすことである。

1）ルールの善良なレベルのコンプライアンス（a good level of compliance）を果たすこと。
2）データ主体がその権利を行使するに当たって個々のデータ主体に支援と援助（support and help to individual data subjects）を提供すること。
3）ルールが遵守されなかった場合に被害者に適切な救済策（appropriate redress）を提供すること。

ここで紹介したのは、WP 12 のほんの一部である。

イ　第 29 条作業部会の「十分性」評価と欧州委員会による認定国等

欧州委員会は、第 29 条作業部会が第一段階として WP 12 により評価したところに基づいて最終的に判断してきているが、これまでに、スイス（Switzerland）、カナダ（Canada）、アルゼンチン（Argentina）、アメリカ合衆国セーフハーバー・スキーム（the United States “safe harbor” scheme）、ガーンジー（Guernsey）、マン島（Isle of Man）、ジャージー（Jersey）、フェロー諸島（Faeroe Islands）について「十分性」の認定を行った。また、第 29 条作業部会は、2009 年 12 月 1 日に、イスラエル（Israel）及びアンドラ（Andorra）について十分性を認める意見を採択した。

ウ　オーストラリアに関する評価

これらに対し、オーストラリアの 2000 年プライバシー修正（民間部門）法（Privacy Amendment (Private Sector) Act 2000）について、第 29 条作業部会は、「オーストラリアへのデータ移転は、上述の懸念に見合う適切な保護措置が導入された場合にのみ十分であると見ることができると考える」という結論を出した。（Article 29 Data Protection Working Party Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000 Adopted on 26th January 2001）

その意見（OPINION）として掲げられている項目の概要は、次のようになっている（ここでは、要約している場合があり、また、番号も適宜付した)。

（1）適用除外されるセクター及び活動（*Sectors and activities excluded* ）

作業部会は、いくつかのセクター及び活動が法の保護から除外されることを懸念する。特に、

・小規模ビジネス（small business）（法第 6D 条は、年間の総売上高が 300 万オーストラリアドル（1 ドル 75 円として、2 億 2,500 万円）以下のビジネスと規定している）が適用除外であること。

・被用者データ（employee data）が適用除外であること。

（2）除外（*Exceptions*)

全国プライバシー原則 2.1(g)（National Privacy Principle NPP 2.1(g)）が、情報の利用又は開示が法により要求され又は授権される場合には、二次的目的のために利用され又は開示されることを認めていること。

（3）一般に利用可能なデータ（*Publicly available data*)

一般に利用可能な公刊物に掲載することを目的とするデータの収集は、NPPs 1 （収集）の範囲内に入るが、一たび、情報が一般に利用可能な公刊物の定義に該当するようなフォーマットで編集されるならば、他のプライバシー原則が適用されなくなること（これは、アクセス及び訂正のような個人の権利を排除することになる)。

（4）データ主体への透明性（*Transparency to data subjects* ）

NPP 1.3（収集）は、組織が収集前又は収集時の個人に通知することを認めているが、しかし、これが現実的でないならば、その後において可及的速やかに通知してもよいと付け加えている。収集が行われた後に組織が個人に通知することを認めることは、OECD ガイドラインの目的明確化の原則（個人データの収集は、収集時より遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないで、かつ、目的の変更ごとに明確化された他の目的の達成に限定されるべきである）に反する。

（5）特にダイレクト・マーケティングに関するデータの収集及び利用（*Collection and use of data in particular with regard to direct marketing*)

NPP 1（収集）及び 2（利用及び開示）は、個人情報の収集はその必要性、公正かつ適法

な手段によることを要求することにより、また、利用及び開示に限定及び条件を課すことにより、目的明確化の原則をカバーしている。しかし、ダイレクト・マーケティング用に個人データを利用するためには、個人の同意を得ることを必ずしも必要としていない。

（6）センシティブ・データ（*Sensitive data*）

NPP10（センシティブ・データ）は、センシティブ・データの収集のみに制限を課しているにすぎない。NPP2 にいくつかの規定がある健康データ以外のセンシティブ・データの利用又は開示に対して特別な制限又は条件はない。

（7）EU 市民の訂正権の欠如（*Lack of correction rights for EU citizens*）

第 41 条第（4）項は、NPP6 又は 7 に基づき、オーストラリア市民又は永住者のプライバシーに対する干渉がある場合にのみその行為又は実態をプライバシー・コミッショナーが調査することを認めている。その結果、永住権を持たない EU 市民は、アクセス権及び訂正権を行使できない。

（8）オーストラリアから第三国への再移転（*Onward transfers from Australia to other third countries*）

オーストラリアから第三国への再移転を禁止していない。

4）日本に関する評価

ア　ブリュッセルのデータ保護会議の開催（2009 年 4 月 23 日）とアジェンダ

ベルギーの首都ブリュッセルにおいて、2009 年 4 月 23 日、日白協会（Belgium-Japan Association）主催のデータ保護会議（BJA-Conference on Data Protection）が開催された。この会議は、BJA 副理事長であるタンギー・バン・オーバーストラテン（Tanguy Van Overstraeten）弁護士（リンクレーターズ法律事務所（Linklaters LLP）のパートナー）が中心になって企画された。

2009 年 4 月 23 日の「EU と日本におけるプライバシー・個人情報保護」（Privacy and Personal Data Protection between EU and Japan）会議と称することができるデータ保護会議のアジェンダは、次のようになった。

○序論（Introduction）　リンクレーターズ法律事務所　タンギー・バン・オーバーストラテン

○日本におけるプライバシー・個人情報保護（Privacy and personal information protection in Japan ）　一橋大学名誉教授　堀部政男

○欧州連合におけるデータ保護―EUから第三国への個人データ移転（Data Protection in the European Union – Personal Data Transfers from the EU to third countries）　タンギー・バン・オーバーストラテン

○十分性認定手続（Adequacy finding procedure）　欧州委員会・司法自由安全総局（European Commission Directorate-General-Justice, Freedom and Security）法務政策部（Legal Affairs and Policy）ユニットD5・データ保護（Unit D5 –Data Protection）事

務官（Desk Officer）　ハナ・ペチャコバ（Hana Pechackova）
○日本におけるデータ保護―2006年第一段階のCRIDによる調査結果（Data Protection in Japan: Findings by CRID in FIRST STEP report of 2006）［CRIDは Centre de recherche informatique et droit（情報法研究センター）の略］　ナミュール大学教授（Prof. At the University of Namur）　イブ・プレ（Yves Poullet）→当日、プレ教授が病気のため出席できなかったので、フランク・デュモルチィエ（Franck Dumortier）氏が出席して講演
○ケース・スタディ：EUにおけるAGCのデータ保護ルールの取扱い（Case study: AGC dealing with data protection rules in the EU）　AGC Europe［AGCは、Asahi Glass Corporation］ 租税・監査・リスク・マネージメント・デレクター（Tax, Audit & Risk Management Director） エマニュエル・ハザール（Emmanuel Hazard）
○閉会の辞（Closing remarks）タンギー・バン・オーバーストラテン

イ　ブリュッセルのデータ保護会議の意義

データ保護会議におけるスピーカーのプレゼンテーションは、それぞれ極めて重要であった。

しかし、そのすべてを紹介することは不可能であるので、ここでは、会議開催の趣旨、欧州委員会による日本個人情報保護法の評価手法、また、日本個人情報保護法に関する分析について少し述べるにとどめることにする。

ウ　欧州委員会の「十分性認定手続」―ペチャコバ女史のプレゼンテーション

このデータ保護会議では、前述のように、欧州委員会・司法内務総局のハナ・ペチャコバ女史が、「十分性認定手続」というプレゼンテーションを行った。

女史のプレゼンテーションは、次のような構成になっていた（番号は、本稿で説明する便宜上ふった）。

(1)プレゼンテーションの目的（Goal of the presentation）
(2)ECの法的枠組み（EC legal framework）
(3)指令95/46/ECの適用範囲（Scope of Directive 95/46/EC）
(4)諸原則（Principles）
(5)データ取扱いは合法でなければならない（Data processing must be legitimate）
(6)データ保護機関（Data Protection Authorities）
(7)第29条作業部会（Article 29 Working Party）
(8)十分性：一般的論点（Adequacy–general issues）
(9)十分性：法的手順（Adequacy–legal steps）
(10)十分性（Adequacy）
(11)「十分な保護」の第三国（“Adequate” 3rd countries）
(12)十分性：結論（Adequacy–conclusions）

これらのうちには、既に別稿で検討しているものも多いので、ここでは日本との関係で注目すべきいくつかの点について見ることにする。

ペチャコバ女史は、プレゼンテーションの目的の中でデータ保護・プライバシーの分野における欧州委員会の作業についてばかりでなく、十分性認定手続とは何か、欧州委員会は日本との関係でどのようなところにあるかについても説明するとした。

また、十分性の法的手順について述べたところをEUデータ保護指令との関係で、簡単にコメントを加えて見ることにする。

欧州委員会が、第三国が十分なレベルの保護を確保しているかどうかを決定する権限を与えられていることを述べた。

これは、EUデータ保護指令第25条第（6）項を指している。繰り返しになるが、第25条第（6）項は、次のように規定している。

「委員会は、第 31 条第 2 項に規定する手続に基づいて、第三国が個人の私生活並びに基本的自由及び権利を保護するための当該第三国の国内法、又は特に本条第 5 項に規定された交渉の結果に基づいて締結した国際公約を理由として、第 2 項の規定の意味における十分なレベルの保護を保障していると認定することができる。」

これは、欧州委員会の認定権限に関する規定である。第（6）項の前の同条第（4）項は、「構成国は、第 31 条第 2 項に規定する手続に基づいて委員会が、第三国が本条第 2 項の規定の意味における十分なレベルの保護を保障していないと認定した場合には、当該第三国への同一タイプのデータの移転を阻止するために必要な措置を講じなければならない」とし、同条第（5）項は、「委員会は、適切な時期に、第 4 項に基づく認定によってもたらされる状況を改善することを目的とする交渉を開始しなければならない」と規定している。

欧州委員会関係者によると、これらの規定に基づき委員会が「十分性」評価を行い、その評価が得られない場合には、交渉に入るということであった。しかし、必ずしもそうではないという話も聞いていた。

このようなことを認識している私にとって、ペチャコバ女史が、公の会議で「十分性認定手続を開始するためには、第三国の代表による公式な要請が欧州委員会に提出されなければならない」と述べたことは、EU データ保護指令の解釈の変更であるようにも受け取れる。というのは、欧州委員会は、EU データ保護指令に基づき、当初、自ら十分性認定手続を開始するとしていたからである。

ペチャコバ女史は、前掲の「(10)十分性」において、特に日本について、次のようなことを述べた。

・委員会は、第三国が十分なレベルの保護を確保していると認定することができる。

・このような決定の効果は、個人データが 27 の EU 構成国及び 3 つの欧州経済領域（European Economic Area, EEA）（ノルウェイ、リヒテンシュタイン及びアイスランド）からその第三国へ、追加的な安全保護措置を必要としないで、流通することができることである。

・日本は、個人の私生活にかかわる個人データ及び基本権に関して十分なレベルの保護を提供している国であるとは、EU によってまだ考えられていない。
・したがって、EU 構成国から日本へのデータの移転は、EU 構成国各国のデータ保護機関による事前の情報／権限付与（prior information/authorization）を意味する指令 95/46/EC 第 26 条に従って行われなければならない。

（EU データ保護指令第 26 条は、前掲のとおりであるので、ここでは繰り返さないことにする。）

・移転がデータ主体の保護を確実なものとする適切な保障を提供することを証明するためには、特に特別の契約上の取決めによって、例えば、委員会によって承認された標準契約条項モデルの一つを使用することによって、行うことができる。

また、前述の「(12)十分性：結論」として、女史は、次のようなことを明らかにした。

・委員会は、日本のやり方の評価を開始する予備的段階に入った。
・日本におけるデータ保護・プライバシー立法に関する分析を準備している。
・EU-日本ビジネス・ダイアログ・ラウンドテーブルは、2008 年 7 月 3 日・4 日、東京で「データ保護レジーム」について議論した。
・ビジネス・ダイアログ・ラウンドテーブルは、EU と日本の機関が両者の間で、国際的な平等、透明及びセキュアなデータ保護レジームを確保するために協働すべきであると勧告した。
・委員会は、ビジネス・ダイアログ・ラウンドテーブルのために経過報告を準備している。
・委員会は、個人データの保護とデータ移転の領域における協力関係を改善し、最高度の国際的基準に従い EU と日本間における個人データの自由な移転に向けて作業を進めるつもりである。
・委員会は、日本のデータ保護法の全体像を把握し、十分性認定手続をおそらく開始するために、詳細な分析を行うことを考えている。
・とはいえ、この構想も日本側によって支持されなければならない。
・十分性認定手続を開始するためには、日本の代表部によってなされる公式の要請が欧州委員会に提出されなければならない。

以上が「(12)十分性：結論」部分である。

（３）日系企業の対応状況

1）個人データ移転法的不可能国

日本は十分性未認定国であるため、次に掲げる EU 構成国及び欧州経済領域（European Economic Area, EEA）からは、日本に個人データを自由に移転することは、法的には不可能である。

・EU 構成国（27 か国）

オーストリア、ベルギー、キプロス、チェコ、デンマーク、エストニア、ドイツ（加盟時西ドイツ)、ギリシャ、フィンランド、フランス、ブルガリア、ハンガリー、アイルランド、イタリア、ラトビア、リトアニア、ルーマニア、ルクセンブルク、マルタ、ポーランド、ポルトガル、スロバキア、スロベニア、スペイン、スウェーデン、オランダ及びイギリス

・欧州経済領域（3 か国）

ノルウェイ、リヒテンシュタイン及びアイスランド

2）日系企業の対応調査の質問事項

このことは、上記の各国に所在する日本企業が、例えば、従業員や顧客の個人データを日本に移転することも法的には不可能であることを意味している。これについては、以前から日本企業の関係者から問い合せを受けてきたが、今回、ブリュッセル及びロンドンにおいてヒアリングを実施した。ここでは個別の企業名を掲げないが、それぞれどのように認識しているかが分かるであろう。

主な質問事項は、次のようになっている。

① 国際取引において EU 構成国所在の企業か日本を含む第三国にどのような種類の個人データを移転するか。
② 1995 年 EU データ保護指令 及びこれに基づく各国のデータ保護法で、日本を含む第三国が十分なレベルの保護を講じていない場合には、個人データを移転してはならないという規定をどのように認識しているか。
③ 日本を含む第三国が十分なレベルの保護を講じていない場合にも、Binding Corporate Rules（BCR）や Standard Contractual Clauses（SCC）に依拠すれば、個人データを移転できることをどのように認識しているか。
④ BCR に依拠したことがあるか。
⑤ BCR について専門家に相談したことがあるか。
⑥ BCR のメリットやデメリットは何か。
⑦ SCC　に依拠したことがあるか。
⑧ SCC について専門家に相談したことがあるか。

⑨ SCC のメリットやデメリットは何か。
⑩ 国際取引における個人データ移転について意見があるか。

これらの質問事項は、今回の調査において明らかにすることができることを期待して作成した。しかし、実際の回答は、これらの質問事項のそれぞれに対応するという形でまとめることが困難であるので、回答の趣旨を概要としてまとめることにする。この場を借りて、ミーティングの設定をはじめ調査にご協力いただいた、ブリュッセルにある在欧日系ビジネス協議会（Japan Business Council in Europe, JBCE）、ミーティングに参加された日系企業の関係者、また、ロンドンで調査に応じていただいた関係者にお礼を申し上げたい。

3）日系企業からのヒアリングの概要

① A 社（コンサルティング）

Q 日系企業が日本に送るデータとはどのようなものか。

○ 現時点での個人データ移転のニーズはそれほど大きくない。日本企業の海外展開の形として、日本にある親会社と欧州にある子会社とのコミュニケーションは、日本の本社に籍のある日本人従業員を通じて行われている。このような日本人の人事評価は日本で行われており、ローカルの人事はローカルで完結しているため、個人データ移転の必要性は、従来あまりなかった。しかしながら、徐々に、子会社の幹部レベルの人事を日本の本社で管理又は把握しておきたいというニーズは増えている。もっとも対象となる幹部の人数が比較的限られているうちは、個々人の承認（同意）を取って送ることも可能だと言える。

Q 日系企業の対応はどのような状況か。

○ 日系企業の法規制への対応状況を見ると、以下の 3 つくらいではないか。

・ 意識の高い企業→①全く送らない
・ 意識の高い企業→②本人の同意
・ ③知らないで送る

Q 日系企業は BCR 又は標準契約をあまり利用していないのはどうしてか。

○ 日系企業が BCR 又は標準契約をあまり利用していない理由は、これらの制度自体が障害になっているわけではなく、その裏付けとなるべき内部統制システムが十分整備されていないためで、標準契約を結んでも実際には遵守できないおそれがあるという点にある。それは BCR についても同じである。

Q 日系企業の内部統制システムはどうなっているか。

○ 日系企業の内部統制システムは主として日本国内を対象にしており、全世界に共通の制

度を入れるという発想は少ない。他方米系企業の場合は、本社で創ったシステムを国外にそのまま持って行こうとすることが多い。英語と日本語という言語の違いが、この発想の違いを生む重要な要因の一つであると思う。

Q　人事情報以外のデータ移転の要請はあるのか。
○　業種によって異なる。小売の場合は、消費者等のデータ処理をどうするのかという問題はあると思う。通信系企業ではそうしたデータをやり取りする可能性が高いのではないか。
○　日系企業が大きな欧州企業を買収した案件でも、個人データの移転は行っていないようである。

Q　御社の場合、欧州からその他の国に個人データを移転することはないのか。
○　トレーニング、品質管理は全世界で統一されている。例えば、オンライン・トレーニングでは個人情報を登録するが、そのサーバーの場所やシステムの開発は米国と欧州が中心で、そこで完結しているのではないか。

Q　BCR についてどのように考えるか。
○　BCR は使っていない。日本との間でのデータの交換はほとんどないので、社としてのニーズはないが、顧客からのニーズに対応するために、この問題を考えておかなければならないと思っている。

Q　日系企業関係者との話の中で、個人データ移転のニーズはあるのか。
○　話を聞きたいという程度で、具体的な話までたどりつかないことも多い。日本企業（本社）の場合、現在、主として財務面にかかわる内部統制システムの整備を進めている最中であるが、一部の企業には内部統制疲れの様相も見受けられる。内部統制システムがしっかりできていれば、個人データ保護をそのシステムに乗せることはそれほど難しいことではない。その観点からは、BCR か SCC のどちらにするかは、テクニカルな問題にすぎないと言える。問題は日本の本社で国際的に通用する内部統制システムがしっかりできているかどうかであるが、まだそこまで至っていない企業がほとんどであろう。

Q　BCR の承認を取るのは大変であると聞いているが、どうか。
○　承認を取る手続自体にもお金は掛かるが、BCR の担当者を各国に配置しなければならないので、その人件費もかなりの負担であると聞いている。

Q　一般論として、このような申請をする場合に、弁護士などの専門家に依頼するか。
○　書類の申請関係は弁護士に依頼することが多いと思う。費用が高いので、ドラフトの作

成まで依頼するかは別にして、少なくともアドバイスは受けるのではないか。弁護士費用が高いのはイギリスで、ベルギーは 1 時間 200 ユーロ程度である。

Q　BCR と SCC のどちらがよく使われるか。
○ データ保護機関（Data Protection Authority, DPA）側の意向としては、BCR と SCC のいずれを利用してほしいというようなものは見られない。その一方で、EU データ保護指令第 26 条の例外（Derogations）に含まれている、個人の同意に基づく方法については、例外中の例外であるとされているようだ。
○ 個人的な印象だが、BCR に関しては、全世界で内部統制システムが標準化されており、かつ、インドにデータセンターを持つ企業（特に米系企業）への対応だったのかと思う。インドにデータセンターを置く場合には、SCC では対応が難しかったからであろう。

Q　EU におけるデータ保護についてはどのように見ているか。
○ 病院、自治体、保険会社などを除いて、EU 域内での個人データ保護の体制が一般の企業で整ってきたのは最近のことである。過去数年の内部統制強化の流れの中で整備が進んだ点は、日系企業と同様であるが、個人データ保護意識の点では、日本国内の方が、むしろ進んでいるかもしれない。

② B 社（メーカー）
Q　御社では、BCR とモデル契約のいずれを利用しているか。
○ モデル契約を利用している。他の企業が何を利用しているかについては知らない。

Q　今後 BCR を利用する予定はあるか.
○ モデル契約の利用で問題がない上に、これから BCR に変更することは、膨大な労力を要することになるため、現段階では考えていない。
○ もっとも、モデル契約を一切利用しておらず、これからこの問題に対処するのであれば BCR を利用するだろう。
○ 弊社は、いわゆる一般の顧客というものを有していない。そのため、顧客や DPA へプライバシーへの対応状況を説明・証明する必要性はない。それほど BCR という煩瑣な手続を採る必要性はないのではないか。

Q　これまで個人情報に関する越境的な紛争はあるか。
○ ない。おそらく、越境的な個人情報の移転は、そのデータ管理者によって行われていることがほとんどであるため、事故や紛争が起こりにくいのではないか。

Q　これまでモデル契約の利用に際して不便を感じることはあったか。

○ ない。十分機能していると考えている。

Q モデル契約の利用に際しては、DPA の承認を要するか。そうであれば、その審査手続は。

○ 必要である。弊社では、オランダで承認を取った。ベルギーであってもおそらく必要であろう。

○ モデル契約をそのまま利用するのであれば、5 ページ程度の書類作成の作業のみで足りる。

○ その審査期間は大体 1 ヶ月程度である。モデル契約を修正すればもっと掛かるであろうし、移転したい項目が基礎的なものでなく、センシティブ情報などを含むとすれば、より時間が掛かるだろう。BCR についてはよくわからないが、1 年程度ではないか。

Q どのような種類のデータ移転を必要としているか。

○ 従業員のデータを東京本社が一元化して持つ必要がある。人事関係の情報を一元化しなければ、統一した給与体系などができないからである。また、人事管理を一元化することによって、その人物の適性に応じた異動を越境的に行うことができる。センシティブ情報が含まれていることもあるので、入社時に越境的データ移転に対して同意を得ている。

Q 従業員の個人データ以外にどのような個人データを移転するか。

○ 顧客の個人データもあり得るが、弊社では必要性がないので、前述のように、モデル契約の対象とはしていない。

Q 弁護士など専門家に相談しているか。

○ 社内に専門家がいる。

③ C 社（メーカー）

Q EU 構成国所在の企業か日本を含む第三国にどのような種類の個人データを移転するか。

○ 主としては従業員の個人データである。

Q 1995 年 EU データ保護指令 及びこれに基づく各国のデータ保護法で、日本を含む第三国が十分なレベルの保護を講じていない場合には、個人データを移転してはならないという規定をどのように認識しているか。

○ 個人のプライバシー権は、個人の重要な財産である。テクノロジーの進展によって今日では世界中のどこへでも個人データを送ることができるようになった。何らかの保護措

置がないならば、個人データは簡単に悪用される。そのため、EU データ保護指令に定められている諸原則は個人の利益を保護する上で大変有益であると考える。他方、EU データ保護指令に基づく各国の立法は厳格過ぎるととらえられ得る。そして企業がそれを遵守するのに多大な時間と努力を必要とする。

Q　日本を含む第三国が十分なレベルの保護を講じていない場合にも、BCR や標準契約条項に依拠すれば、個人データを移転できることができるが、BCR を利用しているか。
○　弊社では、現在のところ、BCR は利用していない。

Q　BCR について専門家に相談したことがあるか。
○　BCR の申請について弁護士のアドバイスを受けたことはある。

Q　BCR のメリットやデメリットについてどのように考えているか。
○　BCR は、一たび DPA から承認を得るならば、運用は容易である。しかし、欧州のすべての DPA から承認を得るのにかなり時間が掛かる。また、承認されないならば、別の方法を採らなければならない。

Q　それでは、標準契約を使うということか。
○　そのとおりである。弊社は、現在、標準契約を使っている。

Q　その場合に、弁護士に相談したか。
○　弁護士に相談して、標準契約を作成した。

④　D 社（メーカー）
Q　日本にどのような個人データを移転するか。
○　海外事業比率が高まってきている。今後はもっと増やす方向にある。海外事業で利益をあげようとしている。そのため、海外の人材の活用が重要になってきている。

Q　人事情報を日本で一元的に管理する企業もあるが、そのように考えてよいか。
○　幹部候補については、一元的に管理してグローバルに活躍してほしいとの方向性が打ち出されている。その場合に、従業員の個人情報を東京に集める場合の問題点を検討し、どのような問題があり、どのような方法で可能なのかを調査した。

Q　EU データ保護指令及び EU 各国のデータ保護法にはどのように対応しているか。
○　EU のデータ保護指令等の制度的な状況がわかったので、実際にどのように進めるのかを検討している段階である。

Q　弁護士などに相談しているか。

○　フランスの弁護士に相談し、アドバイスを受けて次のような方向で検討している。

①　法の検討

BCR：幹部候補の限られた人事データなので量は少ない。手続が複雑すぎて利用は難しい。

個別同意：個別同意だけでは国際的なデータ移転が認められない場合がある。紛争があった場合には個別同意だけでは不安が残る。

SCC：現在のところ、これを採用することになるであろう。

②　実施ステップ

ステップ 1：欧州の各会社の人事マネージャーに個人情報の移転（幹部候補の一元管理の実現）の実施に当たって各国の法制度に基づいた対応が必要である旨を日本の本社から通知する。

ステップ 2：EU 指令、各国の法制度に基づいて従業員への通知を作成する。

ステップ 3：SCC を作成する。

ステップ 4：各国の所轄官庁に届ける（各国法に基づいた対応）。

ステップ 5：従業員に通知する。

○　他の企業の事例も参考にしているが、従業員に対する通知のフォーマットや個別同意が不要かどうかなど疑問点も残っており、今後問い合わせる予定である。

○　実際に文書の作成を外部の弁護士に依頼するとコストが高くなるので、それを回避できる方法はないか社内弁護士と相談している。

○　社員教育も e ラーニングになってきている。その際の入力データ（個人データ）をどう管理するかが問題になった。例えば、どこでデータを管理するかである。まずは EU 域内でとどまる形で始めようということになったが、実際には EU 域内にとどまらなかった。委託先業者のサーバーがアメリカにあったが、セーフハーバーで移転が可能な企業であったため、この点は問題にならなかった。

Q　社内的にかなり検討していることがよく分かったが、具体的にはどのように進める予定か。

○　それぞれの日系企業によって事情は異なるが、他の企業の例を見ながら、どれが最善の方法かを検討している。

⑤　E 社（メーカー）

Q　EU において個人データの国際移転がどのように行われているのか日本で議論している。欧州委員会は、日本について「十分レベルの保護」を講じている国という評価をしていない。このような状況でどのようにすれば個人データの国際移転が可能か。

○　十分性の評価は限られた国についてなされているにすぎない。例えば、マン島は十分性の評価を受けた。マン島は大規模な商業センターになっている。

○　十分性の認定を受けていない国の場合には、グループ企業で BCR を利用することが考えられる。しかし、DPA から BCR の承認を得るのは容易ではない。短期間では無理である。また、費用も掛かる。外部の専門の弁護士に依頼するのが通常である。

○　まず、それぞれの国の DPA に問い合わせ、申請書を提出する。承認が得られるまでに数か月は掛かる。

○　BCR についてローファームに相談した。弊社の主要な一つの事業として、データ取扱者として個人データを処理することがあるが、これには、第三国で個人データを処理することも含まれる。

○　現在のところ、それに適している方法として、契約によっている。

○　BCR は、グループ企業について有効である。これについても検討してきている。

○　弊社の企業グループでは、人事情報を共有している。多数の国に所在するグループ企業で相互に人事情報を利用する。これについても契約で対応している。

Q　第三国において個人データの処理を行う場合にはどのように対応しているか。

○　弊社では、例えば、インドで個人データの処理を行う場合がある。これについては契約で対応している。

Q　データセンターが EU 構成国以外に存在することが多いと思うが、データ保護についてどのように対応すべきであると考えるか。

○　クラウドコンピューティングが一般化してくると、個人データ保護はますます重要になってくる。日本はデータ処理の面でも優れているが、現状では EU 構成国から日本に個人データを法的に自由に送ることができない。日本としてこの問題にどのように対処するか検討すべきである。データセンターは、中国、アフリカも含め多数の国で機能している。BCR は、グループ企業間では有効ではあるが、クラウドコンピューティングではそうではない。自由に個人データを国際移転することができる方法を考え出す必要があると思う。

⑥　F 社（情報サービス）

Q　御社ではどのような個人データを日本に送っているか。

○　日本に送っている個人情報は、現在、社員情報と顧客情報（法人の担当者の個人情報）の 2 種類である。

Q　その場合に、EU データ保護指令や国内のデータ保護法にどのように対応しているか。

○　社員情報については、雇用契約を交わすときに、個人情報を日本と共有することについての同意を交わしており、顧客情報についても契約の中に日本と情報を共有する旨を入れている。

Q　同意書を作成するのに弁護士などの専門家に相談しているか。

○　労働契約の個人の同意書を作成する際には弁護士に相談したが、現在は特に相談していない。簡単で費用も掛からない手法だと思う。

Q　日本以外の第三者に個人データを移転することはあるか。

○　コールセンターをインドに設けるなどの依頼があれば、個人情報の第三国移転の問題が出てくる可能性はあるが、現在のところ需要がない。

○　フィンランドが北において情報のハブになってきている。

4）第 29 条作業部会への在欧日系ビジネス協議会の BCR に関する回答

①　在欧日系ビジネス協議会の紹介

欧州には、在欧日系ビジネス協議会（Japan Business Council in Europe, JBCE）という団体がある。JBCE が 2003 年 9 月に、前述の第 29 条作業部会に対して、BCR について回答した英文の文書がある。これは、公開されているものであるので、その概要を見ることにする[4]。

その文書の冒頭に JBCE に関する記述がある。それによると、JBCE は、欧州連合で事業を行っている日本企業を代表する組織の一つとして 1998 年に設立された。JBCE の会員企業は、広範な製品やサービスを提供し、また、欧州連合に多額の投資をしてきている。現在（2003 年 9 月現在）、JBCE は 49 社で構成されている【2010 年 3 月現在、59 社】。

②　序説

まず第 1 に、「Ⅰ．序説」（I. Introduction）において、「JBCE は、第 29 条作業部会が EU の域外に個人データを移転する法的基盤として拘束的企業準則（BCRs）の利用に関する 2003 年 6 月 3 日の文書 WP74 について意見照会したことを評価する。データ主体の権利を保護し、データ保護の実行可能な枠組みを確保するためにビジネスとデータ保護機関

[4] http://web.archive.org/web/20031205180009/http://www.jbce.org/files/codes_of_conduct_FINAL.pdf

とが協力することは非常に重要であり、このような意見照会はこの目的を促進する優れた方法である。JBCE は、本件及び他の重要なデータ保護問題について第 29 条作業部会と引き続き意見交換することに多大の関心を寄せている」と述べている。

③　全般的なコメント

第 2 に、JBCE は、「Ⅱ．　全般的コメント」（Ⅱ. General Comments）において、「データ保護指令 95/46/EC（Data Protection Directive 95/46/EC）の実施の検討に関して JBCE が委員会に提出した文書の中で明らかにしたように、JBCE の会員は、データ保護指令の第 2 条第（2）項の意味内でデータ管理者によって提示される十分な保護措置として BCRs を発展させることに明確に賛意を表する。現行の法的根拠に基づく EU から第三国（例えば、日本）への個人データの移転は、現在、多くの困難、特に次のような困難を伴っている」として、次のように記している。

・未だに（日本を含む）ほとんどの国をカバーする十分性の決定がなされていない（第 25 条)。

・同意の利用（第 26 条第（1）項（a））が第 29 条作業部会（1998 年 7 月 24 日の作業文書 WP12「第三国への個人データの移転：EU データ保護指令の第 25 条及び第 26 条の適用」参照)、及び、国内法（例えば、2002 年 3 月 7 日-8 日のドイツデータ保護機関の決議）によって厳格に制限されており、その者のデータが移転されることとなるすべてのデータ主体の同意を得ることは実際には不可能となるであろう。

・多くのケースにおいて、第 26.1 条（移転がデータ主体との契約履行のために必要であるというようなもの）に基づいて規定されている例外が適用になるかどうか国内法では不明確である。

・各構成国による別々の承認は、時間が掛かり過ぎることもあり得る（第 25 条)。並びに

・委員会の標準契約を用いると、個別の企業の間で何百又は何千もの契約を必要とする可能性がある（第 26 条第（4）項)。

JBCE は、以上のような問題点を指摘している。

そこで、JBCE は、BCRs のメリットに次のように着目している。

「JBCE は、多くのケースにおいて、BCRs は世界規模の企業グループ間における個人データ移転の重要な解決策になり得ると考える。しかしながら、拘束的企業準則の法的枠組みは、次の点を考慮する場合に限って、有用となるであろう」として、その考慮すべき点を具体的に挙げている。

・受領国、データのセンシティブ性その他の関連要因のような諸要因次第であるが、BCRs の基礎として様々な実体的データ取扱ルールを利用することができるようにすべきである。

・標準契約条項と BCRs の相互関係が明確にされなければならない。

・EU 域内に本社がある企業と EU 域外に本社がある企業の間で法的枠組みで差別すべきではない。

・執行メカニズムは柔軟であるべきであり、受領国の法的伝統及びシステムを尊重すべきである。
・移転が開始する前に企業が構成国又はデータ保護機関（DPA）の単一の承認を得さえすればよいように、BCRs は、共同体レベルで承認されることができるようにすべきであり、そうでなければ、少なくとも構成国の DPAs 間で調和のとれた、透明な承認手続がとれるようにすべきである。

④　個別的コメント

JBCE は、以上のような全般的コメントに続いて、「Ⅲ.　個別的コメント」（III. Specific Comments）を明らかにしている。それらは、JBCE 自身が述べているように、仮説の形式を採っている。論点として次のような 4 つのものを挙げている。

論点 1：「企業グループ」の定義
論点 2：標準契約条項と BCRs の相互関係
論点 3：調和の欠如
論点 4：DPAs との協力及び監査

今回の日系企業からのヒアリングでは、BCRs を利用しているところがないので、ここでは、割愛することにする。

（４）欧州委員会からのヒアリングの概要

欧州委員会・司法自由安全総局（European Commission Directorate-General-Justice, Freedom and Security）データ保護主任行政官に BCRs についてヒアリングを行った。ヒアリングの結果を要約すると、次のようになる。関係者にお礼を申し上げたい。

Q　BCRs について第 29 条作業部会が多くの文書を作成してきているが、それらは、次のようなものであると理解してよいか。

○そのとおりである。

○第 29 条作業部会作成の文書

・WP74　「第三国への個人データ移転：国際データ移転のための拘束的企業準則への EU データ保護指令第 26 条第(2)項の適用」（Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers）　2003 年 6 月 3 日採択

・WP107　「『拘束的企業準則』から結果する十分な安全措置に関する共通の意見を発するための協力手続を定める作業文書」（Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From “Binding Corporate Rules”）　2005年4月14日採択

・WP108　「拘束的企業準則の承認申請のモデルチェックリストを定める作業文書」（Working Document Establishing a Model Checklist Application for Approval of Binding　Corporate Rules）　2005年4月14日採択

・WP133　「個人データの移転のための拘束的企業準則に係る標準申請書に関する 2007 年 1 月の勧告」（Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data）2007 年 1 月 10 日採択

・WP153　「拘束的企業準則で設けられるべき要件及び諸原則の表を定めた作業文書」（Working Document setting up a table with the elements and principles to be found in　Binding Corporate Rules）　2008 年 6 月 24 日採択

・WP154　「拘束的企業準則の構成の枠組みを定めた作業文書」（Working Document Setting up a framework for the structure of Binding Corporate Rules）　2008 年 6 月 24 日採択

・WP155　「拘束的企業準則に関連するよくある質問に関する作業文書」（Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules）　2008 年 6 月 24 日採択

近く BCR に関する法令、各国のデータ保護機関の状況、十分性等を説明する、新たな文書を公表する予定であり、現在、作成中である。各国のデータ保護機関からのインプットも反映する。

Q　EU 全体の BCR の承認申請したリストはあるか。

○　BCR 承認申請件数

欧州委員会には各国のデータ保護機関が承認した BCR のリストはないが、ここ 6 か月の間に 15 件の申請があり、さらに多くの申請がなされている。どの企業であるかは、企業秘密にかかわることであるので、知らない。詳しくは各データ保護機関に聞いてほしい。

Q　EU 全体の BCR の承認したリストはあるか。

○　BCR 承認件数

EU 全体でこれまでに約 20 の企業が BCR の承認を受けている。それらは、すべて多国籍企業である。BCR が始まったときからそれほど年数が経過していないことを考えると、決して悪い結果ではない。イギリスでも増えていると聞いている。

Q　BCR のサンプルはあるか。

○　BCR のサンプル

BCR は、企業秘密にかかわる部分があるので、企業は、ミーティングなどで説明資料を出しても、回収していく。サンプルはない。

Q　BCR はグループ企業が所在している国のすべてのデータ保護機関から承認を受けなければならないのか。

○　BCR の承認データ保護機関

BCR は、関係する企業がそれぞれ所在する国のデータ保護機関から承認されなければならないと考えられているようであるが、本社の所在国のデータ保護機関から承認されることで足りる。そのようなデータ保護機関は、主管データ保護機関（lead Data Protection Authority）と呼ばれている。主管データ保護機関は、例えば、WP153 を使って、第三国への個人データの移転が要件を満たしているかどうかをチェックする。時としてデータ保護指令を逸脱することがあるからである。それは、データ保護機関と企業とのピンポン・ゲームのようなものである。承認されるまでに 6 か月は掛かる。

また、相互承認手続（Mutual Recognition Process）が有用であると考えている。これは、ヨーロッパの指導的なデータ保護機関に申請し、例えば、ドイツのデータ保護機関が承認すれば、他のデータ保護機関も承認するという方式である。これを用いるならば、全体の手続は、簡素化される。

Q　BCR を実際に取り扱っているデータ保護機関はどこか。

○　BCR の主要なデータ保護機関

BCR の主要なデータ保護機関は、現在、フランスの CNIL（Commission nationale de

l'informatique et des libertés）とイギリスの情報コミッショナーである。ドイツも入れることができる。

Q　BCR にはメリットがある一方で、デメリットもあるようだが、どのように考えているか。

○　BCR のメリットとデメリット

BCR を作成し、承認を得るには時間も費用も掛かることは確かである。さらに、BCR は、関係企業の内部のポリシーにかかわることであるので、情報の開示をちゅうちょする傾向がある。

法律専門家に依頼することも必要な場合もあり、その費用も掛かる。

一方、BCR の承認を受ければ、個人データをそのグループ企業の間では自由に移転することができる。

Q　BCR は、今後、どのようになっていくと考えるか。

○　BCR の今後

BCR は、大規模な多国籍企業向けのものであって、中小企業向けではない。今後、モデル契約条項（model contract clause）と同様に、モデル BCR を作成することを考えている。現在は、BCR については単にコピー・アンド・ペイストすべきでないとしているが、将来的には、モデル BCR をコピー・アンド・ペイストすることも考えられる。しかし、これは、すぐに実現するわけではない。このようなことを実現するためには、EU データ保護指令の改正も必要になるかもしれないし、3、4 年は要するであろう。

（５）弁護士からのヒアリングの概要

1）弁護士からのヒアリングの概要（1）

ブリュッセルにあるリンクレーターズ法律事務所（Linklaters LLP）において、BCR を多数取り扱っているリチャード・カンブリー（Richard Cumbley）弁護士から話を聞くことができた。同弁護士は、ロンドンにあるリンクレーターズ法律事務所に属しており、同氏の日程との関係で、当初、ブリュッセル・ロンドン間のテレビ会議で話を聞く予定であったが、都合をつけてブリュッセルまで足を運んでいただいた。これは、ブリュッセルのリンクレーターズ法律事務所のパートナーである後掲のタンギー・バン・オーバーストラテン（Tanguy Van Overstraeten）弁護士の御厚意により実現した。この場を借りて、両弁護士に謝意を表する。カンブリー弁護士とのやり取りの内容をまとめると、次のようになる。

① BCR の取扱い

Q BCR を多数取り扱ってきているか。

○ 私たちは、BCR を多数扱ってきている。法律事務所としては、2004 年から BCR について相談を受けている。国際商業会議所（International Chamber of Commerce）とも議論してきた。

② BCR の承認状況

Q BCR の承認状況はどうなっているか。

○ 私が知る限りでは、これまでに EU 全域で 12 件の BCR が承認されている。

③ 日系企業の関心

Q 日系企業で BCR に関心を示しているところがあるか。

○ ある。

④ 個人データの種類

Q 先に挙げた企業はどのような個人データのために BCR の承認を受けたか、また、申請しているか。

○ 主としては従業員の個人データである。欧州では、従業員の同意を取るのは容易ではない。最近では、顧客やゲストの個人データも増えている。

○ 日系企業には、従業員の個人データも集中管理する傾向がある。しかし、社会保障や税金などの個人データはローカルなものである。個人データを分散管理するよりも集中管理する方が経費が安いので、集中管理する傾向があると思う。

Q　センシティブな個人データの国際移転も行われているか。
○　イギリスでは国内法でセンシティブな個人データを国際移転することは困難である。製薬会社では、BCR のもとで、治験データを移転しているところもある。個人データは、新たな資産であり、その利活用にも関心が高まっている。行動ターゲティング広告などのその一例である。

⑤　BCR 以外の国際移転方法
Q　個人データの国際移転をするには、BCR の他にどのような手法を用いているか。
○　セーフハーバーも使っている。しかし、これはアメリカ合衆国への移転の場合である。また、標準契約条項も使っている。
　さらに、多数間当事者契約（Multiparty Agreement）を用いることもしばしばある。一つの契約に 20 社とか 40 社が署名する。多数間当事者契約を用いる者の場合、世界中の多くの国に受領者がいる。

Q　多数間当事者契約と標準契約条項はどのように異なるか。
○　拘束力の面では、非常に類似している。多くのクライアントは、安価で効率的な方法を求めているため、多数間当事者契約が好まれている。しかし、それぞれにメリットとデメリットがある。

⑥　BCR の利用状況
Q　BCR についてどうか。
○　BCR は初期段階では費用が掛かる。文書の作成、研修計画、新たな文化を浸透させるなど時間も経費も必要である。しかし、長い目で見れば、有効である。また、データ保護機関も好意的である。

Q　しかし、全般的にはまだそれほど使われているとは言えないと思うが。
○　そのとおりである。

Q　どのような理由からか。
○　費用が掛かるからである。そのため、モデル契約を好む企業もあるが、データ保護機関は、モデル契約ではコンプライアンスが確保できないので、好まない。

Q　BCR の利用は増加すると考えてよいか。
○　BCR は、多国籍企業などの企業グループで用いられる。BCR を使う企業は、他の企業と差別化を図ることができる。
○　BCR に要する経費は、その約 25%が文書の作成、研修、監査などに掛かり、約 75%が

データ保護機関から承認を受けるのに必要である。

○　大きな企業は、BCR をセールスポイントにしている。

○　一つの国の主管データ保護機関が承認すると、他の国のデータ保護機関も、相互承認する。EU には相互承認をする国の非公式なクラブがある。このクラブには現在 19 か国が入っている。また、2 つのスカンジナビア諸国も同様な方針を採っている。欧州連合の 27 か国のうち 21 か国になっている。もちろんそれぞれのデータ保護機関によって方針は異なっている。

○　イギリスの情報コミッショナーのウェブサイトに出ているハイアットは、イギリスの情報コミッショナーによって承認されると、その 1 か月以内に、フランスとドイツによって承認され、また、欧州連合の構成国でないスイスによっても承認された、と聞いている。

⑦　弁護士費用

Q　先ほどの経費の中で弁護士の費用はどのくらいの割合か。

○　社内弁護士を使うこともできる。

○　10%から 25%である。研修に最も多くの費用が掛かる。新しい義務について世界中のスタッフを研修しなければならない。これには時間も要する。E ラーニングの開発、翻訳、モニターも必要であり、その結果のチェックもしなければならない。これには人事やマーケティングの分野で専門家を育てる必要がある。

⑧　BCR の申請手数料

Q　BCR の申請手数料は必要か。

○　イギリスでは申請手数料は必要ない。イタリアでは 1000 ユーロだが、わずかな額である。ドイツのような連邦国家では、州によって異なる。申請手数料のない州もあるが、タイム・チャージの州もある。フランスでは小額で、100～200 ユーロである。

○　しかし、費用が高額化する傾向がある。

○　EU 全体で指令は一つであるが、27 か国はそれぞれ独自の法制度を持っている。それぞれの国内法との関係も重要である。国内法が障壁になっているところもある。

⑨　ポピュラーなデータ保護機関

Q　データ保護機関の中でどこがポピュラーか。

○　イギリスの情報コミッショナーである。約 50%の申請がイギリスで行われていると言われている。

2）弁護士からのヒアリングの概要（2）

ブリュッセルにあるリンクレーターズ法律事務所（Linklaters LLP）のパートナーであ

るタンギー・バン・オーバーストラテン（Tanguy Van Overstraeten）弁護士からのヒアリングの概要は、次のようになる。同弁護士は、データ保護に詳しく、また、日本のデータ保護システムについても精通している。

① 国際データ移転

Q 国際データ移転の必要性はどの程度あるのか。

○ 国際データ移転の必要性は極めて高いと考えている。例えば、雇用関係の情報は、本社が一元化して収集する必要のあることが多い。なぜなら、統一性のあるボーナス制度などを構築するに当たり、情報を 1 か所に集積させておくことが必要だからである。

○ その他にも、情報をいくつかのサーバーに保存しておき、そのうちの一つのサーバーのみ 24 時間利用可能にしているが、他のサーバーは通常の就業時間のみ利用可能にしており、それぞれのサーバーが異なる国々に設置されている場合、日常的に国際的データ移転が必要となる。

○ また、旅行代理店やホテルなどの顧客情報は、より良いサービスを提供するため、客の嗜好などを共有する必要性が高い。例えば、A 国のホテルに滞在した客の情報について、同じチェーン店の B 国にあるホテルが、その客のニーズに応えるため、A 国のホテルから情報を移転してもらうという場合がある。

Q 匿名化して業務を行うことはできないのか。

○ 例えば、雇用関係について、誰をどこに配置するかといった問題を処理する際に、匿名化していては業務が遂行できない場合が多い。

○ 仮に、匿名化できる場合であったとしても、匿名化の作業及びその解除作業には膨大なコストがかかる。

Q 同意を取って業務を遂行することはできないのか。

○ 雇用関係において、従業員の同意を取ることも一つの方法である。

Q 国際データ移転には、センシティブ情報なども含まれているのか。

○ センシティブ情報というものをどう理解すべきか難しい問題がある。例えば、飛行機に乗る際に、食事で豚肉を除いて欲しいという個人情報は、イスラム教であることを伝えるに等しくなるため、センシティブ情報となる。同様に、長期休暇の理由に出産休暇と記載すれば、センシティブ情報となるだろう。しかし、これらについても特別な扱いをするとすれば、膨大な作業を要求することになる。

Q 国際データ移転の方法のうち、最も利用されているのはどれか。

○ 5,6 年前であれば、モデル契約が一番利用されていたと思う。ただ、モデル契約は、様式が決まっているため柔軟性がない。そのため、企業のニーズに応える形で、それを修

正した契約が利用されることもあった。しかし、現在では、BCR の利用が可能であれば、それを利用すると思う。

○ モデル契約はあくまでも 2 当事者間の契約である。それによって、データ主体の権利も発生するが、認められるべきすべての権利が網羅されているわけではない。他方、BCR は、顧客との関係などについても適切に規定されることになるためこちらの方がより良いといえる。

② 弁護士関連

Q 国際データ移転に際して、弁護士の助力は必要か。

○ モデル契約を一切修正せず、そのまま利用するのであれば、必要な事項を記載すればいいので弁護士の助言は不要だろう。

○ しかし、そのモデル契約を修正する場合や、とりわけ、BCR では専門家の助力なしに行うことは困難であるし、実際に雇っているか、社内に専門家が存在すると思う。

○ ちなみに、私が所属するリンクレーターズには、BCR を専門的に扱っている弁護士もいる。

Q 弁護士費用はどの程度掛かるか。

○ 個人情報保護の分野において、私たちが多額の投資をしていること、プライバシーの分野は専門的な分野であることを理解して欲しい。よって、ある程度高額な費用とならざるを得ない。

○ もっとも、どの程度その企業において個人情報保護に関する対応が進んでいるかによって、掛かる費用は当然異なってくる。

Q 個人データ保護分野の弁護士業務はどのようなものか。

○ 個人としては、ある企業の BCR 申請を担当しており、イギリス、フランス、ドイツからの承認も得ているが、その他の国からの承認は待っている状態である。

○ 小さな法律事務所では、プライバシーに関する日常的な苦情処理に関する相談などの業務もあるだろう。

○ いずれにせよ、一般市民の関心は高くなってきており、データ保護機関も、その執行を強化している。個人データ保護違反行為に対し、100 万ユーロの罰金や 1 年間の執行猶予付判決が出たケースも出てきている。それゆえ、危機管理という観点からも、弁護士の助力を必要とするようになっているだろう。

○ これまでのところ、総じて日系企業のプライバシー保護の問題に対する意識は低いため、弁護士に依頼していないのではないか。

③ BCR の承認手続

Q データ保護機関の承認手続の厳格性や期間はどうか。

○ 最初に BCR の承認を受けたのは、GE で、イギリスの情報コミッショナーによるものであったと記憶しているが、何年も掛かっていると聞いている。データ保護機関の審査手続が確立されていなかったからである。しかし、このケースから多くのことを学んだようであり、現在では、1 年以内に承認されるのではないだろうか。

○ 実際には、データ保護機関との文書のやり取りにおいて修正を求められることがあるので、企業がそれまでどの程度この問題に対応してきたかにより、その審査期間は異なってくるだろう。

○ 1 回承認を受ければ、その後のデータ移転は楽になるため、長い目で見ると BCR の方がモデル契約よりプラスとなる可能性がある。

○ 承認を主管するデータ保護機関は、他国のデータ保護機関に対しても承認するか否か照会がなされるのが通常である。自動的に相互承認という制度が採用されているわけではない。

④ BCR の相互承認手続

Q BCR の相互承認手続はどうなっているか。

○ BCR の相互承認手続は欧州連合構成国のデータ保護機関のうち少なくとも 18 の機関で行われている。イギリス、フランス、ドイツ以外の国も積極的になってきている。

⑤ 審査に必要な文書量

Q 審査のために要求される文書量はどのくらいか。

○ BCR で要求されている項目は、第 29 条作業部会で 20 頁程度にまとめられているが、具体的に証明する資料を作成すると 200 ページは超えるだろう。この作業は大変であるが、企業が顧客に対して、企業が個人データ保護についてなすべき対応措置を採っているということを証明することにもなるため、結局、企業にとってプラスである。

⑥ 標準契約条項について

Q 標準契約条項の場合、データ保護機関の承認は必要か。

○ ベルギーでは必要である。ほとんどの国では必要と理解している。

Q 再委託に関する 2010 年 2 月 5 日の欧州委員会の変更点のポイントは何か。

○ 個人データの処理の再委託は、受託業者に対する標準契約条項の内容への拘束力の確保が問題となるため従来認められていなかった。しかし、これでは、実際に再委託が頻繁に行われている現実のビジネスモデルに合致しないことから、受託業者が委託する業者との間において、同一の契約を締結することにより、再委託できることとした。

⑦　その他

○　OECD で行動広告（behavioral advertising）に関するガイドラインを作成中だが、現行案はビジネス界から評判が悪い。その理由は、公的団体についてはガイドラインの規制対象から外していること、また、柔軟性がなく厳格に過ぎることが挙げられている。

（６）イギリス情報コミッショナーの BCR 関係文書・事務局からのヒアリングの概要

1）情報コミッショナーと副情報コミッショナー

イギリスの情報コミッショナーは、最初は 1984 年データ保護法（Data Protection Act 1984）でデータ保護登録官（Data Protection Registrar）であったが、現行の 1998 年データ保護法（Data Protection Act 1998）でデータ保護コミッショナー（Data Protection Commissioner）となり、2000 年情報自由法（Freedom of Information Act 2000）により現在の「情報コミッショナー」（Information Commissioner）と呼ばれるようになった。この経緯からも明らかなように、情報コミッショナーは、データ保護ばかりでなく、情報公開も所掌している。

情報コミッショナーのもとに 2 人の副情報コミッショナー（Deputy Information Commissioner）が置かれている。それぞれデータ保護と情報公開を扱っている。そのデータ保護の副情報コミッショナーが今回のインタビューに応じてくれた、後述のデイビッド・スミス（David Smith）であり、 ここで紹介する「拘束的企業準則承認書」（Binding Corporate Rules Authorisation）にはスミス氏が署名している。

2）情報コミッショナー事務局からのヒアリングの概要

EU 各国にはデータ保護機関があるが、イギリスのデータ保護機関は、現在、情報コミッショナー（Information Commissioner）であり、本調査では BCR の担当者にヒアリングを行った。関係者に謝意を表したい。

その概要は、次のようにまとめることができる。

① BCR の申請件数と処理期間

Q 先週、ブリュッセルで欧州委員会の担当者、専門の弁護士などから話を聞いたが、イギリスの情報コミッショナーが最も多くの BCR 申請を取り扱っているということがわかった。これまでにどのくらいの BCR 申請を扱っているか。

○ ICO は、これまでに 11 件の申請を受け付けた。さらに 4 ないし 5 のビジネスがまだ正式の申請書を提出していないが、照会してきている。欧州の他のデータ保護機関は、現在、5 ないし 6 件の申請を取り扱っている。

Q BCR 申請を承認するのにどのくらいの日数が掛かるか。

○ それぞれの申請ごとに異なるので、一般的にどのくらいの日数が掛かるか答えるのは困難であるが、相互承認の手続によって以前にくらべると、かなり速くなってきている。

○ この相互承認手続では、主管データ保護機関及び 2～3 のデータ保護機関が申請を認めるならば、他のデータ保護機関もそれに従うようになる。そのため、期間はかなり短縮され、通常は数か月である。他のデータ保護機関は、その後、遅滞なく承認する。4 年も掛かった事例もあるが、それは、グループ企業の中で手続を進めるのに多くの時間が

掛かっているからである。グループ企業内で個人データ保護についてシステムが確立していても、BCR の要件に適合するために修正を必要とするならば、その場合もかなり時間を要することになる。

○ また、承認までの期間は、データ保護機関の事務量にも左右される。ICO が、多数の申請を処理しなければならない場合には、時間がかからざるを得ない。

○ 申請書類が整っていれば、それほど時間は必要なくなる。そのため、事前に BCR について説明するミーティングなども開催してきている。

○ 最近もマンチェスターで個人データ保護について関係者に説明するミーティングを開催し、その中でも BCR についてプレゼンテーションした。

② ポピュラーなデータ保護機関

Q 最もポピュラーなデータ保護機関はイギリスの ICO であるといえるか。

○ そのとおりである。アメリカ合衆国の企業が英語が通じるデータ保護機関を好む傾向があることにもよる。それは件数に表れている。EU の他のデータ保護機関が 5～6 の申請を取り扱っているのに対して、ICO だけで 11 件の申請を扱っている。

③ BCR 承認状況

Q BCR が承認された企業がどこであるか EU 全体の状況はわかるか。

○ 全体をまとめたデータはない。それらを明らかにするウェブサイトもない。しかしながら、そのようなものを立ち上げる計画があり、すでに作業グループが設置された。問題は、各データ保護機関がそれぞれ異なる手続を採っており、手続も標準化されていないところにある。

④ BCR のメリットとデメリット

Q BCR について検討してみると、そのメリットが大きいことが明らかになる反面、デメリットも見えてくる。これについてどのようにとらえているか。

○ メリットとしては、次のようなことを挙げることができる。

・コーポレート・ガバナンスのために役立つこと。
・テンプレートを提供すること。
・優れたビジネス・ソルーションとなること。
・優れた枠組みができていること（その中で柔軟性があること）。
・契約よりも優れていること。

○ デメリットとしては、次のようなことを挙げることができる。

・限界があること。
・手続が煩雑であること。
・費用が掛かること。

・何人にも適しているとはいえないこと。

○　その他の特徴としては次のようなことを挙げることができる。

・主として大規模な企業向けであること。

・広範囲な分野に適していること。

・主として従業員及び顧客の個人データ保護用であること。

⑤　弁護士の関与

Q　BCR 申請にかなり弁護士がかかわっているといえるが、弁護士がどのように関与していると見ているか。

○　大部分のビジネスは、申請に当たって弁護士に依頼している。しかし、申請手続の全プロセスにかかわってもらう必要はなく、ビジネス内でかなりのことはできる。かなり専門性の高い分野であることは確かであるが、どのような文書が必要かなど欧州委員会の第 29 条作業部会がまとめた文書に出ているし、それらは、法律文書ではない。

Q　BCR 分野の専門弁護士はどのくらいいるか。

○　BCR 分野を専門にしている弁護士は、4～5 人である。必要なときに専門の弁護士に相談することを勧めている。すべての手続を依頼すると、相当な費用が掛かる。社内弁護士や社内の者が手続を進めることは可能である。

⑥　テンプレート申請書式

Q　テンプレート申請書式はどのようなものか。

○　欧州委員会第 29 条作業部会が作成した WP133 の書式を使うことになる。これは、2 部に分かれている。第Ⅰ部は、企業グループの詳細な情報、個人データ取扱い・データの流れ、主管データ保護機関の決定など申請者に関する情報を記入することになる。第Ⅱ部は、BCRs の拘束性、内部の対応体制、データ保護措置など、一定の要件を満たすことができる情報を記述することになる。また、実際の BCRs も添付する必要がある。

⑦　申請書類の分量

Q　申請書類はどのくらいの分量になるか。

○　かなり多くの分量になる。必要な説明資料なども含めると、通常、2～3 インチ（5 センチ～7.5 センチ）くらいの厚さにはなる。

⑧　申請書の審査

Q　ICO では、何人くらいで申請書の審査をしているか。

○　申請件数にもよるが、今は、12 人が当たっている。審査手順を作り、チェックしてい

る。

Q　欧州委員会の BCR 担当者によると、データ保護機関と申請した企業との間でのやり取りはピンポン・ゲームのようにかなり頻繁になされているということだが、ICO ではどうか。

○　まさにそのとおりである。

○　以前は、関係するデータ保護機関がそれぞれチェックしたので、かなりの時間が掛かったが、主管データ保護機関が審査し、相互承認手続で、他のデータ保護機関が承認するようになってからは、期間もかなり短縮された。提出された書類をチェックするだけでは確認できないこともあるが、それらの書類で必要要件の 90%は確認できるようにして欲しいと望んでいる。

⑨　承認企業名等

Q　ICO のウェブサイトに、その承認年月日、企業名、個人データの種類が、2009 年 3 月現在で次のように出ている。

15 December 2005 - The General Electric Company for employee data.

2 April 2007 – Koninklijke Philips Electronics NV for employee data.

22 April 2009 - The Atmel Corporation for employee data.

30 April 2009 - Accenture Limited

15 September 2009 – The Hyatt Hotel Corporation for employee and guest data

26 February 2009 - JPMorgan Chase & Co.

これらのうち、個人データの種類が出ていないのは、どうしてか。

○　従業員の個人データが多いが、明記していない場合には、すべての個人データということになる。

⑩　標準契約条項の承認不要

Q　個人データ国際移転を行うことができる他の方法として標準契約条項がある。ヨーロッパの国によってはこれについてもデータ保護機関の承認を要するところがあるということであるが、イギリスではどうか。

○　他の国ではデータ保護機関の承認を必要としているところもあるが、イギリスでは不要である。

3）BCR 承認に関する副情報コミッショナー文書の概要

(1)　文書の冒頭と前文部分

前述の「拘束的企業準則承認書」（Binding Corporate Rules Authorisation）という文書は、冒頭で「情報コミッショナーは、1998 年データ保護法（以下「法」という。）附則第 4 第 9 項に従いこの承認書を付与する」と記して、各項目を導く接続詞（WHEREAS）を使って、次のようにその根拠を挙げている。

「A.　法附則第 1 第 1 部第 8 項（第 8 原則）は、当該国又は地域が個人データの取扱いについてデータ主体の権利及び自由のために十分なレベルの保護を確保していなければ、個人データは欧州経済領域の外の国又は地域に移転されてはならない、と規定しているので、

B.　法附則第 4 第 9 項は、第 8 原則は移転がデータ主体の権利及び自由のために十分なレベルの保護を確保するような態様でなされているとしてコミッショナーによって承認されている場合には適用されないと規定しているので、

C.　WP12 は、企業グループが拘束的企業準則（BCR）を実施することによりグループ全体で十分な保護措置を確保することができることを描き、また、申請者が承認を得るためにデータ保護機関に対して示さなければならないことを明らかにしているので、

D.　各事案において情報コミッショナーは、BCR が WP74、WP108 及び WP153 の要件に適合することを示すすべての必要な情報を受け取っているので、」

このように法律文書に特有な表現を用いて、次のように承認する旨のことを記述している。

「1.　ここに、情報コミッショナーは、付属文書 1 に掲げるグループ内の企業が連合王国（UK）情報コミッショナーの管轄する領域から欧州経済領域の外に位置する団体グループ内の企業に個人データを移転することを承認する。それは、各申請について次のことを条件としてデータ主体の権利及び自由のために十分な保護措置を確保するような態様でなされる BCR に基づき、また、BCR に従い、行われるものである。

1.1.　この承認は、付属文書 1 に掲げる BCR 文書で確認されているカテゴリの個人データの移転に限って適用されること。

1.2.　BCR は、WP133 の申請書又は同等の背景文書で行われた表現及びその他の表現に従い、解釈され、適用され、また、執行されなければならないこと。

1.3.　付属文書 1 に掲げる企業は WP74 の 4.2 項で示されている BCR の重要な変更について情報コミッショナーに通知すること。

2.　情報コミッショナーが企業がその BCR の規定に違反したか又は違反していると認める場合には、この承認を撤回する通知をグループ内の連合王国企業に送達することができる。当該通知は、通知で特定された日に効力を生じ、そのグループは付属文書から削除されるものとする。

3.　この承認書の条件に企業が従わないことについて情報コミッショナーが寛大であっても、後の機会に執行する権限を行使することを妨げるものではない。」

この後に前述のデイビッド・スミス氏（副情報コミッショナー）が署名している。

これまでにも出てきている付属文書 1 には、前掲の 6 つのグループ名等が掲載されている。しかし、この付属文書では、それぞれについて登記地、グループの状況、BCR の構成等も掲げられているので、より詳しく知ることができる。

4）個人データの国際移転に関する ICO の説明文書の概要

(1)　ICO の「国際移転」に関する説明

ICO は、個人データ保護について説明している多くの文書を発行している。そのうちの一つに「国際移転」（International Transfers）という文書がある。その概要を見るならば、イギリスという国から第三国への個人データの移転がどのようにすれば可能であるかを知ることができるので、この文書を部分的に紹介することにする。

(2)　国際移転の要件

この文書は、まず、次のように国際移転の要件（Requirements）について説明している。

「1998 年データ保護法（Data Protection Act 1998）の第 8 原則は、欧州経済領域（27 の EU 構成国並びにアイスランド、リヒテンシュタイン及びノルウェイからなる）外の国又は領域に個人情報を移転することを禁止している。

この移転は、個人に関する情報の取扱いについて個人の権利及び自由に対して十分な保護がなされている場合に限って行うことができる。これは、個人情報が法的保護を享受できず、また、個人がそれに関して何らの権利も持っていないところに個人情報を移転することによって、データ保護のルールの抜け道ができないように確保することを目的としている。移転の特定の状況の中で他の手段によって十分性が確保される場合には、同等のデータ保護立法を有しない国に対して移転を行うことは可能である。」

(3)　ICO ガイダンス

この文書は、ICO ガイダンス（ICO guidance）について次のように述べている。

「情報コミッショナーは､第 8 原則を遵守できるように次のようなアドバイスをしている。

第 8 原則の詳細と欧州経済領域外に個人データを移転する前に十分性を評価するグッドプラクティスアプローチについては、International transfers detailed guidance

海外に個人データを移転する企業のための一般的コンプライアンスのアドバイスは、私たちの guide to data protection の第 8 原則の箇所で見ることができる。

私たちはまた、中小企業のためのアウトソーシングに関する good practice note を有している。」

(4) BCR に関する説明

これら以外にも「十分性の決定」（Adequacy decisions）、「セーフハーバー：合衆国への移転」（Safe Harbor-transfers to the USA）、「契約」（Contracts）について概要を明らかにした後に「拘束的企業準則」（Binding corporate rules）について説明している。ここでは、前掲の第 29 条作業部会の文書（WP）を簡潔にまとめている部分のみを掲げることにする。それは、「多国籍企業は欧州経済領域外であるが、十分性を確保している態様でその企業グループ内において個人データを移転することが可能である。この十分性は、拘束的企業準則（BCR）として知られている、組織による企業行動の拘束的コード採用によって達成することができる。十分性を確保する BCR を利用するためには、そのグループが個人データを取り扱う諸国のデータ保護機関から承認を受けることが要求される。第 29 条作業部会は、この手続を進めるのを手助けするためにいくつかの文書を採択した。最近の文書は、次のようなものである」としている。

・BCR の要件のテーブル（WP153）—これは、BCR のセットで必要とされる要素を明らかにしている。この文書は、新たな要件を作り出したものではなく、WP74 及び WP108 の要約である。

・BCR の枠組み（WP154）—これは、BCR が何をもって WP74 及び WP108 のすべての必要要件を包含しているといえるかを示している。

・第 29 条作業部会の BCR に関するよくある質問（WP155）—これは、BCR 申請を取り扱っている最新の経験に基づいている。

また、「その他の第 29 条作業部会文書は、次のとおりである」として、次のように簡潔にまとめている。

・国際移転のための BCR の利用（WP74）—BCR が個人データの十分なレベルの保護のために利用できる方法を説明している。

・協力手続（WP107）—これは、データ保護機関による承認を受けるためのコードの提出の方法及びデータ保護機関がそのコードについて共通の意見に達する方法を説明している。

・モデルチェックリスト（WP108）—これは、一連の拘束的企業準則の承認のためにデータ保護機関への申請書の要求される内容を明らかにしている。

・標準申請書式（WP133）—私たちは、これを使うことを強く勧めたい。これは、WP108 のチェックリストに基づいている。

これらを見るならば、前掲の各文書（WP）がそれぞれどのようなものであるかを理解できるであろう。

5）BCR に関する「よくある質問」の概要

ICO は、「拘束的企業準則　よくある質問」（Binding Corporate Rules Frequently Asked Questions）を出しているので、その概要を紹介することにする。上述の「情報コミッショ

ナー事務局からのヒアリングの概要」と併せてみるならば、ICO が BCR についてどのように考えているかがよりよく理解できるであろう。

この「よくある質問」は、9 つの質問と回答からなっている。ここでは「です」調で表記することにする。

「1　拘束的企業準則（BCRs）は何を成し遂げることを目的としていますか。」

BCRs は、多国籍企業が、［データ保護法］の第 8 原則及び 95/46/EC 指令（以下「指令」という。）第 25 条に従って、欧州経済領域から欧州経済領域の外に所在するその系列企業に個人データを移転することを認めることを目的としています。

Applicants must demonstrate that their BCRs put in place adequate safeguards for the protection of personal data throughout the organisation in line with the requirements of the Working Party paper on Binding Corporate Rules, known as WP 74

申請者は、自らの BCRs が WP74 として知られている、拘束的企業準則に関する作業部会文書の要件に沿ってその組織を通じて個人データの保護が十分なレベル保護措置を講じていることを証明しなければなりません。【WP74 の URL を次のように示している。】
(www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm).

「2　 BCRs を承認する手続はどのようなものですか。」

その手続は、申請する会社が各個別のデータ保護機関に別々にアプローチしなければならないのを省くことを目的としています。

申請する組織は、主管データ保護機関となるデータ保護機関（DPA）を選択します。主管機関の選択は、申請会社の EU 内の本部の所在地又はグローバルなデータ保護遵守の責任を負うのに最適な会社の部署のヨーロッパ内の所在地によって決まります。主管機関の選択に関する詳細な基準は、作業部会の 107 文書及び 108 文書で明らかにされています。
【WP107 及び WP108 の URL を次のように示している。】
(www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm).

主管データ保護機関が BCRs の中に定められた保護措置の十分性について確信するならば、そのデータ保護機関は、申請者が承認を得ようとする欧州の他のデータ保護機関に BCRs の案を回付します。主管データ保護機関は、コメントを受けると、それらを申請者に伝達します。主管データ保護機関の役割は、承認手続を容易にすることです。

申請書を提出するときに、会社は、WP108 に基づく申請書式である、作業部会文書 133 を使わなければなりません。会社は、自らの申請書を作成して申請することもできます。私たちや他のデータ保護機関は、申請者が WP133 を使うことを強く勧めます。
【WP133 の URL を次のように示している。】
(www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm).

BCRs は、そのグループ外になされる移転の根拠となるものでないことを認識することが重要です。

「3　第 8 データ保護原則の要件を満たす十分な保護措置を講じる他の方法と比較して、BCRs の利点は何でしょうか。」

十分な保護措置を講じる他の方法よりも BCRs が優れている主な点は、一たび開発され機能するようになると、BCRs は、その組織の要件に適合する様々なグループ内の移転のために枠組みを定めることができるということです。その BCRs で承認を受けた会社の継続的な義務は、当該承認の範囲内でそれが機能していることを確認する遵守義務をモニターすることです。これには、定期的な監査及び個人データを取り扱うスタッフの研修プログラムのメンテナンスを要求されることを含まれます。

BCRs はまた会社がプライバシーの関心を呼び起こし、その組織内のデータ保護の意識を高めなければなりません。これは、組織が、申請書をまとめるプロセスにおいて、欧州経済領域から同じグループの他のメンバーに移転する個人データを考慮し、また、スタッフがどのようにして指令の要件を認識しまた尊重するかを考慮しなければならないからです。承認手続の必須の部分は、第三国の系列会社のスタッフが、例えば、欧州経済領域から移転される個人データを取り扱うことを意味するところについて、スタッフ研修プログラムを通してどのように認識させるかを申請者が証明することを要件としています。

BCRs が柔軟に起草されるならば、BCRs は、会社の構造の変更やデータ流通のタイプの若干の変化に適応させることができなければなりません。承認に影響を与えない会社内の変更は、承認を付与したデータ保護機関に通知する必要はありません。したがって、BCRs は、かなりの柔軟性が認められるものです。

承認の範囲を超える組織のより実質的な変更がある場合には、会社は、その手続の全部又は一部に関する承認の改定を得る必要があります。

十分な保護措置を講じる手段として多国籍企業が利用することができるもう一つの解決策は、欧州委員会によって承認されたモデル契約を用いることです。しかしながら、特に複雑な構造の多国籍企業にあっては、契約の利用について障害がある。というのは、すべての系列企業の間における移転をカバーするのにときには数百の契約が必要とされるからです。契約が企業の構造変化と歩調を合わせるために最新のものにすることを確保する作業もまた、困難を伴いまた時間がかかり得ます。

個々のデータ保護機関がモデル契約の脚色について双務契約とは異なる多数間当事者契約を認める程度はまた、データ保護機関ごとに異なり、会社が必要とされる契約の数を減らす範囲を制限します。また、例えば、その組織が一法人である場合のように、モデル契約が利用できない状況もあります。

モデル契約が欧州委員会によって利用が認められてきたという事実にもかかわらず、いくつかの国においては、輸出するデータ管理者が時間の掛かることになり得る承認手続の方式を採ることを依然として義務づけています。

データ管理者に開かれているもう一つの選択肢は、セーフハーバーのスキームですが、

しかし、これは、アメリカ合衆国への移転に制限されていますし、金融サービスのような一定のセクターは含まれません。

イギリスでは、第 8 データ保護原則は、データ管理者が十分性について自ら評価することを認めていますが、しかし、これは、もちろんのこと、欧州経済領域の他の地域からも個人データを移転する多国籍企業にとって限定的に役立つものです。ICO は、データ管理者が評価をするのを手助けするためにガイダンスを作成しています。

【ガイダンスの URL を次のように示している。】

(www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers).

「4　他のデータ保護機関は BCRs の概念を支持しますか。」

多くのデータ保護機関は、BCRs の促進に積極的に取り組んでいますし、次第に私たちはこの数は増え続けるであろうと予測しています。

WP74 は、データ保護機関はそれぞれの国内法に最も適合的な態様で承認申請を取り扱うことが自由であることを明らかにしていますし、また、いくつかの国ではデータ保護機関がそのような申請を取り扱う十分なリソースを欠いているかもしれないことを認識しています。データ保護機関内でリソースが欠けていることが承認提唱を遅延させている一つの理由です。

WP74 で言及されまた実際にも難問であることが証明された問題は、いくつかの構成国においては国内法が一方的な宣言という概念を認めていないということです。このことは、BCRs がグループ全体で拘束力を持つような方法を扱うようにいくつかの申請を構成する根拠となります。これらの事例においては申請者は、その要件に対応するために問題提起となる構成国の法に基づいて執行できるようなその他の解決策を見いださなければならないかもしれません。このことは、申請書を協力手続に基づいて回付される前に主管データ保護機関と協議されるような類の問題です。

やがて私たちは、より多くのデータ保護機関がこの手続を積極的に取り組むようになるであろうと予測していますが、その国内法の困難性から、そうすることができない国が少しあり得るでしょう。したがって、現時点においては、BCRs は、欧州全体の解決策となるであろうと期待されたようなものではありません。

「5　情報コミッショナーはどのくらいの承認申請を受け付けていますか。」

私たちは、BCRs の利用に関心を持っている会社から定期的に問い合わせを受けています。申請数は承認手続がより効率的になり、申請がうまくいくであろうという現実的な見通しがあるという確信が得られるならば会社の数は増える見込みがあります。

「6　　申請手続にはどのくらいの期間が掛かりますか。」

会社が申請を開始するのをちゅうちょさせている一つの問題は、承認手続に掛かる見込

みの期間の長さです。

私たちはICO内では比較的迅速に申請を取り扱うことができますが、協力手続で申請が始められると、他のデータ保護機関での承認手続で遅延が生じないようにすることを保証することはできません。現在のところ、私たちは、現実的には、協力手続の開始から、明快な申請でも結論が出るまでに12カ月掛かるといっています。

協力手続（WP107）は、申請が取り扱われなければならない期間を示していますが、多少の遅れが生じることがしばしばあります。データ保護機関からのコメントに対応し、文書を修正する会社の力も一つの要因となるでしょう。

第29条作業部会（WP133）によって承認されたモデル申請書式を用い、WP153に明記されている要件のすべてを満たしていることを確実にするならば、手続の迅速化にも役立つはずです。私たちは、モデル申請書式を用いることを強くお勧めします。

WP107に基づいて申請書を回付するのに必要とする時間は、各国のデータ保護機関に個別にアプローチし、その移転について承認を得なければならない会社が要する時間（及びコスト）と比較考量されなければなりません。

いくつかのデータ保護機関が歓迎しICOが支持する一つの実際的なやり方は相互認証です。相互認証においては、BCRsが十分な保護措置を講じていると主管データ保護機関が確信するならば、他の参加データ保護機関は、その決定を信頼し更なる精査又はコメントをしないでその認定を受け入れるべきであるというものです。この相互認証は現在開発中です。

「7　申請書はどのように構成されるべきですか。」

モデル・チェック・リスト（WP108）がBCRs一式を提出する要件を明らかにしています。これらの要件は、現在では、WP133に統合されています。

WP133は、承認手続について申請者及びデータ保護機関の双方に役立つはずです。申請書の標準化は、申請者が提供している情報がWP74の要件に合致しているというある種の安心感を申請者に与え、次にはデータ保護機関の承認手続を容易にするはずです。

テンプレート申請書式を申請者が使うことは義務ではありませんが、申請者がいかにWP74及びWP108の要件に適合しているかについてデータ保護機関に証明するのに役立つことを意図していますので、私たちは、ほとんどの申請者がそれを使うことを望むであろうという考えです。

第29条作業部会は、BCRの枠組みを作成しました（WP154）。これは、WP74及びWP108のすべての要件がどのようなものであるかについて一つの文書で説明しています。申請者は、この枠組みに依拠するのも自由で、義務ではありません。

【関連するWP 153, WP 154 and WP155のURLを次のように示している。】

（www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm).

「8　構成国の多くにおける行政上の要件はどのようになっていますか。」

イギリスにおいては、BCRs が EU データ保護指令の第 26 条第（2）項の意味での十分な保護措置を講じているという点で WP74 の要件を満たしていることに基づいて承認しています。これは、1998 年データ保護法第 4 附則第 9 項に基づく承認の根拠を提供しています。個人データの移転を含む、取扱いが情報コミッショナーに通知されるならば、申請会社が承認に基づいてグループ内で個人データを移転する前に必要とされる段階はありません。

しかしながら、多くの構成国においては、データ保護機関は BCRs の承認に加えてその構成国から一つ又は複数の第三国に移転する許可を与えなければなりません。

このことは、協力手続及び WP74 の基本的な原則の目的を無にするように見えるかもしれませんが、国内法がそのような許可が必要であると定めている場合にはなすすべがありません。

「9　情報コミッショナーは、情報自由法に基づく BCRs に関する情報の公開請求をどのように扱いますか。」

BCR の概念は比較的新しいものですので、私たちがすでに取り扱った申請について、申請書を作成することに関心を持っている他の会社及びそのアドバイザーから、大いなる関心が示されています。その結果、私たちは、文書の写しに対して多くの情報公開請求を受けています。

BCRs の承認を求めている組織は、ICO から遵守のアドバイスを求めている他のデータ管理者と同様な方法で扱われます。このことは、申請書を私たちに提出したという事実について、その同意がなければ又はその情報がパブリック・ドメインになっていなければ、公開することができないことを意味します。しかしながら、ひとたび承認がなされれば、これは、公的記録となります。申請者には通知されますし、承認は ICO のウェブサイトに掲載されます。

組織によってはその BCRs の内容のいくつかをウェブサイトでパブリック・ドメインとするところがあります（例えば、プライバシーポリシーやデータ保護コード）ので、このことは明らかに私たちが情報公開請求を取り扱うのに役立ちます。しかしながら、申請書にはパブリック・ドメインとはなりにくい営業秘密情報が多数含まれている可能性があります。そのような情報は、情報コミッショナーがその制定法上の職務として受け取るその他の秘密情報と同様に取り扱われます。

【問い合せ先は、次のようになっている。】
Head Office
Phone: 01625 545 745 or 08456 306 060
Notification helpline: 01625 545 740
E-mail: please use the online enquiry form on our website
Website: www.ico.gov.uk

２．BCR の制度的概要

情報セキュリティ大学院大学准教授　　石井　夏生利

（１）拘束的企業準則(Binding Corporate Rule, BCR)とは

BCR とは、主に多国籍企業を対象として、1995 年 EU 個人データ保護指令[1]第 26 条第 2 項に基づくデータの国際移転を効果的に行うためのルールをいう。

同指令の第 4 章は、「第三国に対する個人データの移転」(Transfer of personal data to third countries)の定めを置き、第 25 条「原則」(Principles)の中で、次のように定めている。

「1　加盟国は、取り扱われている又は移転後の取扱いが予定されている個人データ[2]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損なうことなく、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。」

このように、指令第 25 条は、個人データの保護について「十分なレベルの保護」を講じていない第三国に対しては、データの移転を禁じることを可能とする規定を設けた関係で、国際的に注目されることとなった。

他方、指令第 26 条は、第三国への個人データ移転を認めるためのいくつかの「特例」(Derogations)を設けている。そのうち、BCR の根拠となるのは第 2 項である。

「2　加盟国は、第 1 項の規定を損なうことなく、管理者[3]が個人のプライバシー並びに基本的な権利並びに自由の保護、及びこれらに相当する権利の行使に関して、十分な保護措置を示す場合、第 25 条第 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連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。」

BCR は、主に多国籍企業に用いられる。具体的には、十分な保護レベルを確保するために、データ保護機関(Data Protection Authority, DPA)等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、などに留意した「国際データ流通に対する拘束的企業準則」又は「国際データ移転に対する法的に執行可能な企業準則」を策定し、欧

---

1 「個人データの取扱い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 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC 指令」。Council Directive 95/46, 1995 O.J. (L 281) 0031-0050 (EC). 以下、「95/46/EC 指令」と称することがある。

2 「個人データ」(personal data)とは、「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、その人の肉体的、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 条第(a)項。

3 「管理者」(controller)とは、「単独で又は他と共同して、個人データ取扱いの目的及び手段を決定する自然人、法人、公的機関、当局又はその他の団体をいう。第 2 条第(d)項。

州域内のデータ保護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[4]。BCR は、EU 個人データ保護指令が明文上定めた制度ではないが、セーフハーバー、国際標準契約条項と並ぶ、個人データを流通させるための手段である。多国籍企業にとって、画一的かつシンプルなルールを策定することができれば、低コストで強制しやすいというメリットがある。

[4] 内閣府「諸外国等の個人情報保護制度の実態調査検討委員会報告書」(2009 年 4 月)265 頁。

（２）BCR に関する文書

BCR については、次のように、第 29 条に基づくデータ保護作業部会[5]が一連の文書を公表している[6]。

・WP74

「第三国への個人データ移転：国際データ移転のための拘束的企業準則への EU データ保護指令第 26 条第(2)項の適用」(Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers)　2003 年 6 月 3 日採択

・WP107

「『拘束的企業準則』から結果する十分な安全措置に関する共通の意見を発するための協力手続を定める作業文書」(Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules")　2005年4月14日採択

・WP108

「拘束的企業準則の承認申請のモデルチェックリストを定める作業文書」(Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules)　2005 年 4 月 14 日採択

・WP133

「個人データ移転のための拘束的企業準則に係る標準申請書に関する 2007 年 1 月の勧告」(Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data)　2007 年 1 月 10 日採択

・WP153

「拘束的企業準則の中で設けられるべき要件及び諸原則の表を定めた作業文書」(Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules)　2008 年 6 月 24 日採択

・WP154

「拘束的企業準則の構成の枠組みを定めた作業文書」(Working Document Setting up a framework for the structure of Binding Corporate Rules)　2008 年 6 月 24 日採択

・WP155

「拘束的企業準則に関連するよくある質問に関する作業文書」(Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules)　2008 年 6 月

---

[5] データ保護作業部会は、第 29 条により設置された独立の助言組織であって、EU 域内及び第三国における保護レベルに関する意見を欧州委員会に提出する等の職務を担っている。

[6] 各文書の原文は、下記ウェブサイトから入手することができる。
(http://ec.europa.eu/justice_home/news/information_dossiers/personal_data_workshop/documents_en.htm)

24 日採択、2009 年 4 月 8 日改正及び採択

上記各文書のうち、BCR の解釈適用に当たって基本となる考え方を示しているものは、WP74 及び WP108 である。これらに基づいて、WP133 が BCR を申請するに当たっての標準申請書を、WP153 が BCR に含めるべき事項と申請に当たってデータ保護機関に示すべき事項を区別して一覧表化したものを、WP154 が BCR の枠組みを、それぞれ明らかにしている。そこで、以下、主にこれらの 5 つの文書を参照しつつ、BCR の制度的概要を述べることとする。

（３）BCR の概要

1）BCR の性格[7]

WP74 によると、BCR は、「国際データ流通に対する拘束力的企業準則」又は「国際データ移転に対する法的に執行可能な企業準則」であると説明されているが、それは、次のような意味を有している。

・「拘束力ある、又は、法的に執行可能な」　かかる性質を持ってはじめて、第 26 条第(2)項の「十分な安全保護措置」としてみなされる。

・「企業の」　多国籍企業で導入され、通常は本社が責任を持って制定するルールで構成される。企業グループは、実質的に拘束される企業グループをいう。

・「国際データ流通」　準則を存在させる主な理由である。

2）BCR の適用範囲[8]

BCR は、主に多国籍企業に適用される。その理由は、多国籍企業では、BCR を用いて、企業グループ内における世界規模の情報移転を統括することが可能となる点にある。

多国籍企業には、緊密に結合し、階層的な支配構造を持ったものから、緩やかな連携を取っている複合企業群まで様々であるが、後者には統一ルールを適用することが困難であるため、BCR の利用は適さない。また、BCR は、企業グループ内の情報移転のみを対象に置いており、企業グループ外への移転は、他の法的根拠が適用される(標準契約条項、モデル契約、情報受領者と締結した特定の契約等)。

3）BCR の拘束力[9]

BCR は、Binding という言葉のとおり、法的な拘束力及び実際の拘束的性質を持たせることが重要視されている。多国籍企業は、それぞれの国において、異なる法的及び文化的背景を持ち、異なる経営哲学や商慣習に基づいて活動している。そして、ほとんどの多国籍企業は、BCR に関する経験も浅いため、ばらばらのやり方でこの問題にアプローチすることが予測される。しかし、第三国へのデータ移転を目的とした安全保護措置を示すためには、いかなるシステムにおいても、企業内部と外部の両方の場面で、企業ルールに拘束的性質を持たせること(ルールの法的執行可能性)が必須である。「企業内」には、グループの構成員、従業員、下請業者に対する拘束力を含み、「企業外」は、個人がルールの遵守を強制できる手段を有することを意味する。

---

[7] WP74 のパラグラフ 3.1(8 頁)参照。
[8] WP74 のパラグラフ 3.1(9 頁)参照。
[9] WP74 のパラグラフ 3.3.1-3.3.2(10～13 頁)、WP108 のパラグラフ 5(4～7 頁)参照。

(a)　企業ルールの「拘束的性質」

前述のとおり、企業ルールの「拘束的性質」は、法的な拘束力(法的執行可能性)と実際の拘束力(コンプライアンス)を意味する。

実際の拘束力とは、企業グループの構成員及びその中で働く従業員が、内部ルールに従うのを強制されていると感じることである。申請者は、BCR の申請に当たって、グループの構成員に対してルールの拘束力を持たせるための方法、組織内で従業員に対してルールの拘束力を持たせる方法及びルールに従わない場合の制裁、下請業者に対し、ルールに拘束力を持たせる方法及びそれに従わない場合の制裁を具体的に説明しなければならない。

(ア)　グループの構成員の間で、ルールに拘束力を持たせる方法

申請者は、グループ内の他の構成員による BCR の遵守を確実にしなければならない。とりわけ、本社が存在しない場合や本社が欧州経済領域(European Economic Area, EEA)の外にある場合は重要である。これを達成する方法は、申請組織の構造によるが、組織が位置する加盟国の国内法にも服する。

また、次に掲げる事項は、WP108 が提案した、一連の企業ルールに拘束力を持たせる方法である。ただし、申請組織が提案した取決めにとって、より適した手段が存在することもある。

－グループ内の他企業に対して執行可能な BCR 又は契約によるルール

－グループ内の他の構成員を拘束する親会社の片務的宣言又は約束

－他の規制措置の導入　例えば、明確な法的枠組みの中での制定法に含まれる義務

－適切なポリシー、監査及び制裁による裏付けを得て、組織の一般事業原則内でのルールの導入

また、以上の提案は、加盟国が変われば効果も変わるかもしれない。例えば、加盟国の中には、単純な片務的宣言では拘束力を持たないとみなすものがある。したがって、かかる宣言に頼ることを予定している場合は、地域の助言を得る必要がある。

(イ)　従業員に対する拘束力

従業員に対する拘束力は、雇用契約に特別な義務を定めることや、ルールの遵守と懲戒手続を結びつけることで実現できる可能性がある。加えて、十分な研修プログラム及び上級職の約束、並びに、組織内において遵守の最終責任を負う人物の肩書も、申請の際に加えておくべきである。

(ウ)　下請業者に対する拘束力

BCR が下請業者に拘束力を持たせる方法を説明する必要がある。それを裏付ける契約条項として、違反の結果が生じたときに、契約がどう対処するかも説明しなければならない。

(b)　データ主体による法的執行可能性

外部的拘束力である。

データ主体は、企業グループの構成員間が締結する契約等の法的効果によって利益を得る第三者となる。データ主体は、第三受益者として、管轄のデータ保護機関又は EU 域内の管轄裁判所に苦情を申し立てることによって、遵守を強制する権利を与えられるべきである。

この 2 つの苦情申立手段については、データ保護機関に対するものを用いる方が簡便にも見えるが、裁判手続を必要とするには理由があり、データ保護作業部会は、両者の存在を重要と考えている。

・協力義務は 100 パーセントの遵守を保障するものではない。データ主体は、必ずしもデータ保護機関の見解に同意するとは限らない。

・データ保護機関の法的権限に、国によって若干の違いがある(一部の保護機関は、制裁を課したり、移転を直接阻止することができない)。いずれも損害賠償命令は下せない。それを行えるのは裁判所だけである。

また、裁判手続との関連では、個人は次に掲げる管轄権を持つ裁判所に請求を申し立てることができなければならない。

－情報発信地であるグループの構成員、又は、

－EU 本部又はデータ保護責任をゆだねられた欧州のグループの構成員

以上を踏まえ、申請者は、BCR の申請に当たって、次の各事項を示す必要がある。

－苦情処理手続を含め、データ主体が申請組織から救済を得るための実際の手段

例えば、本社及び経営首脳がベルギーにあり、イタリアにあるグループ企業の 1 つが企業ルールに違反した場合、データ主体がイタリア内の違反企業に苦情を述べることも、ベルギーの本社に苦情を述べることもできる点を明確にすべきである。

－組織の欧州本社、又は、EU 内のデータ保護責任をゆだねられた組織の当該部門が、組織のいずれかの部門の BCR 違反によって生じた損害を賠償するに十分な資産を有する、又は適切な取決めを行ったことの確認。

－苦情処理の担当部門を明記し、かつ、個人が苦情処理手続を利用できる方法の特定

－ルール違反の疑いに関する証明責任が、発信国のグループ構成員、欧州本社、又は、データ保護責任者をゆだねられた組織の当該部門に属すること。

－データ主体が 95/46/EC 指令で付与された権利を有すること。

－監督機関の下す決定に関してデータ保護機関と協力し、WP74 の解釈についてデータ

保護機関から受けた助言に従う旨の確認。

(c) 管轄のデータ保護機関による法的執行可能性

国際データ移転のための許可申請を行うことによって、企業グループは、自ら挙げた安全保護措置を尊重することに拘束される。

（４）BCR を利用するにあたっての留意事項[10]

データ保護作業部会は、BCR に関する一連の文書を公表する一方で、次のとおり、いくつかの留意事項を述べている。

・BCR は、国際移転のための唯一又は最善のツールと考えるべきでなく、標準契約条項に関する委員会の決定やセーフハーバーなどに問題がある場合に、追加的手段を提供するものと見るべきである。

・WP74 は、強制的なものではなく、国内の監督機関は、完全に自由な分析に基づき、申請に対する決定を下すことができる。

・第 26 条第(2)項の定める安全保護措置は、BCR のみならず、契約その他の手段を含む広い概念である。WP74 は、BCR を個別に取り上げて、同条項を適用させるための条件を述べたものである。

・WP154 の述べた BCR の枠組みは、BCR のひな型ではなく、内容とルールを 1 つの文書に盛り込むための案であり、申請者である企業グループの構成、当該企業グループが個人情報保護のために講じる政策や手続を考慮してカスタマイズされるべきである。監督機関は、この枠組みの単なるコピー&ペーストでは受け入れない。

・BCR における諸原則は、第三国の組織による取扱いに現実的に適合し、当該組織内で、データ保護責任者が理解して効果的に運用できるように、展開し、詳細化すべきである。

・企業グループの内規は、企業グループの構成員が義務づけられる法律上のデータ保護義務に取って代わることはできない。国内法の遵守は、当然のことながら、許可を受けるための必須条件である。

・BCR は世界的なルールであり、適用に当たって区別をつけるべきでない。しかし、その執行可能性との関連では、EU 域内で生じたデータ(いったん EU 法に服した個人データであって、その後外国へ移転したデータ)とそれ以外のデータとは異なる。後者について、企業グループは、EU 域内でデータ主体に認められるべき権利を付与する義務はなく、それが許可を付与する必要条件でもない。しかし、企業グループがその義務を取り入れれば、データ保護の必要性に真剣に取り組んでいるとして、大いに歓迎される。

[10] WP74 のパラグラフ 1(1～2 頁)、3.1(7～8 頁)、WP108 の冒頭部分(2 頁)、WP154 の留意事項(3 頁)参照。

（５）誓約・説明事項

WP154 は、WP74 を具体化して枠組みを作った文書である。その中に、BCR を申請しようとする企業グループが誓約ないしは説明を行わなければならない事項が掲げられている。また、WP108 は、BCR を申請する際に求められる要件を示している。そこで、以下、WP154 を基に、適宜 WP74 及び WP108 による補足説明を追加しつつ、誓約・説明事項をまとめることとする。

まず、BCR を申請しようとするグループ企業は、グループの全企業及びその従業員が、BCR を尊重するという明確な義務を持つこと、記載したルールの遵守を確実にする旨を企業の取締役会が誓約すること、企業グループが、個人データの移転及び取扱いに関して十分な保護を提供すること、データ保護に関して準拠すべき文書を参照すること(95/46/EC 指令及び 2002/58/EC 指令[11])を確実にしなければならない。

1）適用範囲

BCR の適用範囲に関する説明を行うこと。とりわけ、

－BCR は、グループ内の移転及び取扱いに適用されること

－地理的範囲(EU 域内で取り扱われ、EU 域外に移転されるデータのみ、又は、すべてのデータ)

－内容面の範囲(取扱いの類型、自動又は手作業、データの性質、顧客/人的資源/仕入先の性質)

次に掲げる事項を含む、データ流通及び取扱目的に関する一般的説明を行うこと。

－移転するデータの性質

－移転/取扱の目的

－EU 域内及び EU 域外のデータの受領者／提供者

データの流通及び取扱いに関する説明事項は、具体的には以下のとおりである。

・データの性質。すなわち、BCR が 1 つの類型のデータ（例えば、人事データ）のみに関連するかどうか。又は、ルールが 2 つ以上のデータに関係する場合に、これが BCR の中でどのように扱われるか。いずれにせよ、講じられた安全保護措置が、行われた取扱いの性質に適切に対応するか否かについて、監督機関が評価できるための十分な詳細情報を申請に加えるべきである。

[11] 2002 年プライバシー及び電子通信に関する指令。Council Directive 2002/58, 2002 O.J. (L 201) 0037-0047 (EC).

・データが取り扱われる目的
・ルールが対象にするグループ内の移転範囲であって、次の詳細が必要である。
－個人データを移転(発信)できる EU 域内のグループ構成員
－個人データを移転(受領)できる EEA 外のグループ構成員
・BCR が EU 域内からの移転のみに適用されるか否か、又は、グループ内の構成員間のすべての移転を対象とするか否かを示す必要がある。データ保護機関は、転送(すなわち、EEA 外のグループ構成員から第三者へのデータ移転)を行う根拠を理解する必要がある[12]。

2）定義

主な用語及びその定義を説明すること。

－主な定義(個人データ、センシティブな個人データ、データ主体、管理者、取扱者、取扱い、第三者、データ保護機関)
－他の関連定義を用語集に盛り込むこともあり得よう。例えば、データ提供者、データ受領者、EU 本部又は代理で責任を負う EU 加盟国、グループの構成員[13]、プライバシーオフィサー/プライバシー保護の職責を担う者(officer function)
－BCR 上の用語を 95/46/EC 指令及び 2002/58/EC 指令に沿って解釈する旨の誓約

3）目的の制限

データの取扱目的及び移転目的の説明、並びに、次に掲げる事項の確認を行うこと。

－個人データを特定かつ適法な目的のために移転し、取り扱う。
－個人データが、それらの目的に適合しない態様でさらに取り扱われないようにする。
－センシティブ・データには、95/46/EC 指令で定めたものなどの追加的な安全保護措置を講じる。

4）データの質及び均衡性

誓約には次に掲げる事項を含むこと。

－個人データは、正確であり、かつ、適宜更新しなければならない。
－個人データは、移転し、さらに取り扱う目的に関して、適切であり、関連性を有し、過剰でないようにすべきである。
－個人データは、収集し、さらに取り扱う目的のために必要な期間を超えて、取り扱うべきではない。

[12] WP108 のパラグラフ 7(7～8 頁)参照。
[13] 構成員は、管理者又は取扱者、データ提供者又はデータ受領者の場合がある。

5）個人データの取扱いの法的根拠

個人データは、次に掲げる根拠に基づき取り扱われるべきである。

－データ主体が明確な同意を与えた。

－取扱いが、データ主体を当事者とする契約の履行において必要である。又は、データ主体の要請に応じて、契約締結前の措置を講じるために必要である。

－取扱いが、管理者の服する法的義務を履行するために必要である。

－取扱いが、データ主体の重要な利益を保護するために必要である。

－取扱いが、公益のため、又は、管理者若しくはデータの開示を受ける第三者に与えられた公的権限が存在する中で、実施される任務の履行に必要である。

－取扱いが、管理者又はデータの開示を受ける第三者もしくは当事者による適法な利益を追求するために必要である。ただし、かかる利益に対し、データ主体の基本的権利及び自由を求める利益が優先される場合はこの限りではない。

6）センシティブ・データを取り扱うための法的根拠

センシティブ・データを取り扱うことは禁止される。ただし、次に掲げる場合はこの限りではない。

－データ主体が、それらのセンシティブ・データを取り扱うことに明示的な同意を与えた場合。ただし、準拠法令がそれを禁じた場合を除く。

－雇用法の分野で、十分な安全保護措置を定める国内法で許可される限りにおいて、データ管理者が義務の遂行及び個別の権利の行使のため必要とする場合

－データ主体が、身体的又は法的に同意を与えることができないとき、データ主体又は他の者の重大な利益を保護するため、取扱いが必要な場合

－基金、協会、又は、政治・哲学・宗教若しくは労働組合の目的を持つ他の非営利団体が、適切な保障を伴った適法な活動の一環として実施し、かつ、組織の構成員又は組織と日常的に接触する者が、かかる目的との関連で取り扱い、データ主体の同意なくして第三者にデータが提供されない場合

－取扱いが、データ主体が明白に公開したセンシティブ・データに関わる場合

－センシティブ・データの取扱いが、法的請求を立て、行使し、又は防御するために必要である場合

－センシティブ・データの取扱いが、予防医学、医学的診断、介護や治療の提供、保健サービスの運営のため必要で、かかるセンシティブ・データが、国内法もしくは国内の所管組織の設定した規則のもとで専門家の守秘義務を負う保健専門職によって取り扱われる場合、又は、同等の守秘義務を負う他の者にとって取り扱われる場合

7）透明性及び情報に関する権利

すべてのデータ主体が容易に BCR を入手できる旨を誓約すること。

さらに、BCR では、データ主体が自らの個人データの移転及び取扱いに関する情報を得る方法を説明しなければならない。

データが取り扱われる前に、データ主体が次に掲げる情報を与えられる旨を誓約すること。

－管理者の身元、及び、その代理人がいれば、その身元、

－意図されたデータ取扱いの目的

－例えば次のような追加情報

ⅰ） データの受領者又は受領者の種別

ⅱ） 自らに関するデータのアクセス権及び訂正権の存在

追加情報が必要な限りにおいて、データが取得される個別状況を考慮し、データ主体に関する公正な取扱いを保障すること。

データがデータ主体から収集されていないとき、データ主体に通知を行う義務は、かかる情報の提供が不可能と判明する若しくは過大な努力を伴うであろう場合、又は、記録もしくは開示が法により明確に規定されている場合には、適用されない。

十分な安全保護措置を掲げた企業グループは、法的に執行可能な企業ルールに基づくデータ保護機関の許可に則して、個人データが EU 域外の企業グループの構成員に送られていることをデータ主体に認識させた旨を証明できる立場でなければならない。また、法的に執行可能な企業ルールの存在と範囲は、個人が容易に入手できなければならない。

個別の情報提供義務とは、企業ルール全体へのアクセスを妨げられることなく、グループが負った主なデータ保護義務、ルールに拘束される構成員に関する最新情報、データ主体がルール遵守の確認に利用できる手段について、各個人が容易に情報を入手できることを企業グループが証明する立場になければならないことを意味する[14]。

8）データのアクセス、訂正、消去及び利用停止の権利

データ主体が自らの個人データにアクセスできる方法を説明すること。誓約は次に掲げる事項を含む。

－すべてのデータ主体は、制約なく、適度な間隔をもって、過度な遅れや費用を伴うことなく、自らに関して取り扱われるすべてのデータの写しを入手する権利がある。

－すべてのデータ主体は、とりわけデータが不完全又は不正確であることを理由に、デ

[14] WP74 のパラグラフ 5.7(19 頁)参照。

ータの訂正、消去又は利用停止を得る権利を有する。
－すべてのデータ主体は、いつの時点においても、自らの特定の状況に関する非常に強力な正当事由に基づき、自らの個人データの取扱いに異議を申し立てる権利を有する。ただし、取扱いが法によって義務づけられる場合はこの限りではない。異議が正当化された場合、取扱いは停止しなければならない。
－すべてのデータ主体は、申請に基づき、無料で、自らに関するダイレクト・マーケティング目的の個人データの取扱いに異議を申し立てる権利を有する。

データ主体が自らの個人データにアクセスできる方法を説明すること。

9）自動化された個人に関する決定

データ主体に関して重大な影響を与える評価又は決定が、自動化したデータの取扱いのみによらない旨を誓約すること。ただし、次に掲げる場合はこの限りではない。

－決定が契約の締結又は履行の過程で行われた場合で、データ主体が出した契約締結若しくは履行の要請が満たされる、又は、自らの見解を述べることを認める取決め等、当人の正当な利益を保護する適切な手段が存在するとき。
－決定が、データ主体の正当な利益を保護するための措置を設けた法によって認められた場合

10）安全保護及び機密性

偶発的若しくは違法な破壊、又は、偶発的な損失、改変、無権限の開示若しくはアクセスで、特に取扱いがネットワークを通じたデータ送信を伴うとき、及び、他のあらゆる違法な形の取扱いに対し、個人データを保護するための適切な技術的及び組織的手段が講じられた旨を誓約すること。

実施の最新状況及び費用を考慮した上で、かかる措置は、保護されるべきデータの取扱い及び性質が示すリスクに適した安全保護レベルを確保しなければならない。

この点で、センシティブ・データは、より強化された安全保護措置を伴って取り扱われるべきである。

BCR には、指令 95/46/EC に準拠したデータの安全保護措置基準に関する明確な説明を含まなければならない。これらの要求事項を組織内で充足させる方法も説明しなければならない。

また、とりわけ、BCR は次に掲げる事項に対処しなければならない。

・データ主体に対する透明性及び公平性
・目的の制限
　－データの質の確保
　－安全保護措置
　－個人のアクセス権、訂正権、及び、取扱いへの異議を申し立てる権利
・ルールの対象となる多国籍企業の外への転送の制限(移転を促進する他の取り決めの下で可能になるかもしれない)

これらの説明を行う際には、関連するポリシーなどの裏付け文書も添付することが求められる[15]。

11）グループを構成する取扱者との関係

グループの構成員である取扱者を用いるときに、個人データをどのように保護するかを説明すること。とりわけ、次に掲げる事項が求められる。

－管理者は、実施される取扱いを統括する技術的安全保護措置及び組織的措置に関して、十分な保証を提供する取扱者を選択しなければならない。また、それらの措置を確実に施行しなければならない。

－管理者は、取扱者に対し、準拠法に基づく文書契約によって指示を行うものとする。また、本契約はとりわけ、次に掲げる事項を明記する。

ⅰ） 取扱者は、管理者からの指示のみに基づいて行動すること。

ⅱ） 取扱者が義務を負う、安全保護及び機密性に関するルール。

12）外部の取扱者及び管理者(グループの構成員ではない)に対する移転及び転送の制限

グループ外への移転及び転送を制限するため導入する手段を説明し、並びに、次に掲げる事項を誓約すること。

－EU 域内又は欧州委員会が十分な保護レベルを確保していると認めた国に位置する外部の取扱者は、管理者の指示のみに従って行動すること、及び、十分な安全保護及び守秘の手段を講じる責任を負うことを明記した文書合意に拘束される。

－EU 域外に位置する外部管理者へのデータ移転はすべて、国際データ流通に関する欧州ルール(95/46/EC 指令第 25 条及び第 26 条：例えば、欧州委員会が 2001/497/EC 又は 2004/915/EC で承認した EU 標準契約条項の利用、又は、指令第 25 条及び第 26 条に基づく他の適切な契約的手段)を尊重しなければならない。

－EU 域外に位置する外部取扱者へのデータ移転はすべて、国際データ流通に関するルール(95/46/EC 指令第 25 条及び第 26 条)に加えて、取扱者に関するルール(95/46/EC 指令第 16 条及び第 17 条)を尊重しなければならない。

[15] WP108 のパラグラフ 8(8 頁)参照。

13）訓練プログラム

個人データに永続的若しくは日常的にアクセスし、個人データの収集又は個人データの取扱いに用いられるツールの開発に携わる職員に対し、BCR に関する適切な訓練プログラムを実施する誓約を行うこと。

14）監査プログラム

グループによる BCR の遵守を監査する旨を誓約すること。とりわけ次に掲げる事項を誓約すること。

－監査プログラムは、是正措置を確実に行わせる方法を含め、BCR のすべての側面を対象とする。

－かかる監査は、内部又は外部の認可された監査チームによって定期的に(時期を明記)、又は、プライバシーオフィサー/機関(もしくは、組織内の他の権限ある機関)から個別の要請を受けて、実施しなければならない。

－監査結果は、プライバシーオフィサー/機関(又は、組織内の他の権限ある機関)及び取締役会に報告しなければならない。

－データ保護機関は、請求により、監査結果の写しを得ることができる。

－監査計画は、データ保護機関が必要に応じて、データ保護監査を実施する権限を持つことを認めるべきである。

－グループの各構成員は、データ保護機関による監査を受ける可能性があること、及び、これらのルールに関するあらゆる問題で、データ保護機関の助言に従うことを受け入れることとする。

申請組織は、データ保護監査プログラム及び監査計画の詳細を示さなければならない。

データ保護監査プログラム及び監査計画は、データ保護基準を含む文書又は他の内部手続文書のいずれかで明確に述べ、監査結果は請求に応じてデータ保護機関に提供する必要がある。データ保護機関は、是正措置の実行を確保する手段を含め、BCR のすべての側面が監査プログラムに十分含まれることで納得する必要がある。監査計画は、監督機関が必要に応じてデータ保護監査を実施する権限を持つことを考慮すべきである。

コーポレート・ガバナンス(データ保護の遵守に影響しない限り)や商業的に機微性の高い情報など、監査結果の中でデータ保護に関連しないものは必要ではないが、データ保護とそれに関連しない情報を切り分けられない場合もある。

また、申請組織は、データ保護事項に対する監査計画、及び、組織内で監査報告書を取り扱う方法を要約しなければならない[16]。

[16] WP108 のパラグラフ 6(7 頁)参照。

データ保護機関による監査が必要とされる理由は、企業グループにおける監査が何らかの理由で行われず、通常の許可を継続させるために必要な情報が得られない場合や、緊急事態に基づき、管轄のデータ保護機関又は代理の独立監査人による直接参加が求められることにある。かかる監査は、データ保護機関の調査権限を定めた関連法及び規則に従って行われる。監査にあたっては、機密保持及び営業秘密を十分に尊重し、BCR の遵守を確保することに厳しく制限して行われる。その他、データ保護機関は、ルールの更新が届け出られた場合や、データ保護機関との相互協力の枠組みの中で必要とされる場合に、請求に基づき監査結果の写しを得ることができる[17]。

15）遵守及び遵守の監督

ルールの遵守を監督し、確保するため、経営首脳陣の支援を受ける適切な職員(プライバシーオフィサーのネットワークなど)を指名する旨を誓約すること。

ルールの遵守を確保するため創設された、ネットワーク若しくはプライバシーオフィサー又は類似の機関の内部構造、役割及び責任を簡潔に説明すること。例えば、チーフプライバシーオフィサーは、取締役会に進言するとともに、データ保護機関の調査に対応し、遵守に関して毎年報告し、グローバルレベルで遵守を確実にする。プライバシーオフィサーは、地元のデータ主体からの苦情を処理し、大きなプライバシー問題をチーフプライバシーオフィサーに報告し、地方レベルの遵守を確実にすることに責任を負うだろう。

16）国内法が BCR の尊重を妨げる場合の措置

次に掲げる事項を明示的に誓約すること。グループの構成員が、自らに適用される法のため、企業が BCR に基づく義務を果たせず、ルールの定める保証に重大な影響があると信じる理由がある場合、その者は速やかに、EU 本部又はデータ保護責任を委任された EU 加盟国又は他の関連するプライバシー機関に対し、通知する(ただし、法執行機関により禁止される場合、例えば、刑事法に基づき法執行捜査上の秘密を保持しなければならない場合はこの限りでない)。

加えて、国内法と BCR 上の誓約に矛盾がある場合、EU 本部又はデータ保護責任を委任された EU 加盟国又は他の関連するプライバシー機関が、取るべき行動について責任ある決定を下し、疑義があれば権限あるデータ保護機関に諮る旨を誓約すること。

17）内部の苦情処理体制

次に掲げる苦情処理手順を置く旨を誓約すること。

－データ主体は、グループの構成員が BCR を遵守していない旨の苦情を述べることがで

[17] WP74 のパラグラフ 5.2(16 頁)参照。

きる。
－苦情を取り扱うのは、明確に識別される部門/人であって、自らの権限の行使に当たって、適切なレベルの独立性を与えられなければならない。

BCR は、明確に指定された苦情処理部門が個人の苦情を処理する体制を定めなければならない。データ保護担当者又はこれらの苦情の担当者は、職務遂行に当たり、適切な水準で独立性を得なければならない。代替的紛争解決制度は、データ保護機関が適宜関与できるため、準拠する国内法及び規則に則して、活用を促進すべきである[18]。

18）第三者の受益権

BCR はデータ主体に対し、受益者である第三者としてルールを強制する権利が与えられるとの明確な声明を出すこと。この権利は、保障された権利の侵害に対する司法的救済や、損害賠償を受ける権利を含むべきである(EU 指令第 22 条、第 23 条参照)。

データ主体は、次の各機関に申立てをすることを選択できる旨の声明を出すこと。
－EU 域内に位置するデータ提供者の裁判所
－EU 本部/責任を委任された EU 加盟国の裁判所
又は、
－権限あるデータ保護機関

第三者の受益権の利益を受けるあらゆるデータ主体が、本条項に容易にアクセスできるようにすべきとの誓約を行うこと。

19）責任

次に掲げる事項を誓約すること。
－EU 本部又は責任を委任された EU 加盟国は、EU 域外の企業グループの他の構成員の行為に対する救済や、グループ構成員の BCR 違反から生じた損害への賠償金支払いに、必要な措置を講じる責任を負い、講じることに同意する。
－EU 本部又は責任を委任された EU 加盟国は、EU 域外の構成員が、データ主体の主張した損害賠償額のもととなる違反行為に責任を負わない旨を立証する責任を負う。

EU 本部又は責任を委任された EU 加盟国は、EU 域外の構成員が違反の責任を負わない旨を証明できる場合、一切の責任を免れることができる。

[18] WP74 のパラグラフ 5.3(17 頁)参照。

救済及び補償を受ける一般的権利について、ルールは、データ主体が EU 個人データ保護指令第 22 条及び第 23 条[19]に基づき、救済を受けられることを示すべきである。その方法と範囲は、企業グループの行う取扱業務がデータ保護指令及びそれを導入した国内法の対象となる場合に得られる便宜と同じものとする。この一般的権利を補完すべく、ルールは、責任及び裁判権に関する規定を含むべきである。

責任に関するルールについて、本社(所在地は EU 域内)又はデータ保護責任をゆだねられた欧州の構成員は、企業グループの EU 域外の他の構成員の行動に責任を負うのを受け入れ、その行動に対する救済を与えるため必要な措置を講じることに同意すべきである。また、適宜、BCR 違反のため生じた損害を賠償することも同意すべきである。

企業グループは、本社又はデータ保護責任をゆだねられた欧州の構成員が、通常の状況下で発生した BCR 違反を補償するための十分な資産を有する証拠を許可申請に添付することが必要である。

また、本社又はデータ保護責任者をゆだねられた欧州の構成員は、EU 内で訴訟を起こされ、損害賠償を適宜支払うことも受け入れなければならない。

・BCR 違反の結果として損害賠償が請求された場合

・損害賠償は求められていないが、データ主体が内部の苦情処理手続又は管轄のデータ保護機関への苦情申し立てで付与された救済に納得していない場合

立証責任について、ルールは、第三国の企業で行われた取扱いが企業ルールに反する旨をデータ主体が立証するのではなく、本社又はデータ保護責任をゆだねられた欧州の構成員が、企業グループの EU 域外の構成員がデータ主体の主張する損害をもたらした違反に責任を負わない旨を常に立証する旨を述べるべきである[20]。

20）データ保護機関との相互援助及び協力

次に掲げる事項を誓約すること。

－グループの構成員は、個人からの要請若しくは苦情、又は、データ保護機関による調査又は質問に対処するために、互いに協力援助し合うものとする。

－各主体は、BCR の解釈に関するいかなる問題についても、データ保護機関の助言に従う。

WP12(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 条の適用に関する作業文書[21](第三国への個人データ移転に関する作業文書)で述べられているように、自主規制制度の適切性を評価する最も重要な要素の一つは、データ主体が個人データに関す

---

19 第 22 条は司法的救済、第 23 条はデータ管理者の責任を定める。

20 WP74 のパラグラフ 5.5(18～19 頁)参照。

21 Data Protection Working Party, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (1998), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf.

る問題に直面したときに、一人で放置されることなく、自分の困難に対処できるような制度的支援が受けられることにある。

これは、BCR の最も重要な要素の 1 つである。ルールは、個人が WP12 で述べた制度的支援の恩恵を得られるようにするため、データ保護機関との明確な協力義務を含まなければならない。

また、企業グループ全体ないしは個々の構成員は、監査義務を受け入れる旨を明確に約束し、BCR の解釈適用に関するあらゆる問題で、管轄のデータ保護機関の助言に従う旨を明確に約束しなければならない。管轄のデータ保護機関の助言は、質問への回答、データ主体が申し立てた苦情の結果、又は、データ保護機関が自ら発する行動による、企業グループ宛の勧告で構成される。

なお、助言を発する前に、管轄のデータ保護機関は、企業グループ、当該データ主体、相互協力の結果関連する可能性のあるデータ保護機関の意見を求めることができる。助言は公開してもよい。

国内レベルの関連規定のほかに、企業グループが、管轄のデータ保護機関への協力やその助言の遵守を強硬かつ/又は継続的に拒んだ場合、許可の停止や取消しを伴う可能性がある。この決定は行政処分の形態を採り、対象者は国内法の定める管轄裁判所に提訴することができる。決定は、欧州委員会及び他の関連するデータ保護機関に通知され、公開される可能性もある[22]。

21）ルールの更新

BCR 又は構成員一覧に関する重大な変更があれば、全構成員及びデータ保護機関に報告する旨を誓約すること。その際、規制環境及び企業構造の変更、より正確には、次の事項を考慮に入れる。

－一部の修正は、データ保護機関からの新たな許可が必要とする可能性がある。

－BCR の更新又は BCR に拘束されるグループ構成員の一覧の更新は、次に掲げる要件を満たす場合、許可を再申請することなく行うことができる。

ⅰ） 特定個人又は企業グループ内の特定部門が、構成員に関する完全な更新リストを保持しており、ルールのあらゆる更新の経過を把握して記録をつけ、かつ、請求があれば、必要な情報をデータ主体又はデータ保護機関に提供する。

ⅱ） 新構成員が BCR に実質的に拘束され、かつ、遵守を提供できるようになるまでは、その新構成員にデータを移転しない。

ⅲ） BCR 又は構成員一覧のいかなる変更も、更新を正当化する理由を簡潔に説明した上で、許可を与えるデータ保護機関に年 1 回は報告すべきである。

ルールの重要な修正は、データ主体にも通知する旨を誓約すること。

[22] WP74 のパラグラフ 5.4(17 頁)参照。

ただし、管理上の変更は、BCR の運用に影響が出ない限り、報告する必要はない[23]。

22）国内法と BCR の関係

次に掲げる事項を説明すること。

－地域の法、例えば EU 法が、より高いレベルの個人データ保護を求める場合、BCR に優先する。

－いかなる場合も、データは、95/46/EC 指令第 4 条の定める準拠法及び関連する地域の法に則して取り扱われる。

また、国際的に承認された制裁、税務申告義務又は反資金洗浄報告義務のような、民主社会に必要な範疇の強制義務は、BCR に違反しない。疑義がある場合には、データ保護機関に相談することが必要である[24]。

23）最終条項

－発効日

－経過規定

BCR は、指定書式に基づいて、データ保護機関等に提出する。その際、BCR で述べた誓約を裏付ける文書を添付することが推奨されている。具体的には、取扱いごとのプライバシーポリシー、個人データにアクセスする従業員向けのガイドライン、データ保護監査計画及びプログラム、訓練プログラムの例及び/又は説明、EU 域外でデータ移転の源となる構成員及び EU 本部又は責任を委任された EU 加盟国が、BCR 違反による損害賠償を支払う十分な資産を有していることの証明文書、内部の苦情処理制度の説明、BCR に拘束される主体の一覧、EU の個人データを取り扱う IT システムのためのセキュリティポリシー、EU のデータを取り扱う新たな IT アプリケーションがすべて、BCR に適合していることを確認する認証手順、EU のデータを取り扱うデータ取扱者に対して用いられる標準契約書、データ保護責任者又は企業内でデータ保護に責任を負う他の者の職務に関する説明がこれに該当する。

[23] WP108 のパラグラフ 9(8～9 頁)参照。

[24] WP74 のパラグラフ 3.3.3(13～14 頁)参照。

（６）BCR の承認を得るための申請手続

申請手続については、WP133 が標準申請書類のひな形を公表しているほか、WP108 の中にも、申請手続を行う際の必要事項がまとめられている。

1）申請先のデータ保護機関[25]

グループの最上位の親会社又は営業上の本部が EU の加盟国内に置かれている場合は、当該加盟国のデータ保護機関に申請すべきである。

最上位の親会社若しくは営業上の本部の所在地が明確でない場合、又は、親会社若しくは本部が EU 域外にある場合は、以下の基準に従って、最も適切なデータ保護機関に申請すべきである。

また、申請組織は、申請したデータ保護機関が最も適切であることを詳しく説明する必要がある。その際には、次の各事項が考慮される。

・グループの欧州本社の所在地
・グループ内でデータ保護責任をゆだねられた企業の所在地
・グループ内で申請を処理し、BCR を執行するのに最も適した体制(経営能力、管理負担などの観点から)にある企業の所在地
・取扱いの目的及び手段の点で、大半の決定が下される場所
・EEA 外への移転の大半が実行される EU 加盟国

以上の中で最も優先されるのは、グループの欧州本社の所在地である。ただし、かかる基準は正式なものではない。申請を送った先のデータ保護機関の裁量により、他のデータ保護機関に割り振られることもある。

2）申請の際に提出する文書[26]

申請組織は、以下の情報を個々の文書で提出しなければならない。

・問い合わせ対応責任者の連絡先
・データ保護機関の選択を正当化するためのすべての関連情報で、以下を含むもの。
  グループの基本的構成
  EU 及び EEA における取扱活動の性質及び構造であって、とりわけ、決定が下される場所
  EU 内の関連会社の所在地
  取扱いの手段及び目的
  第三国への移転が行われる発信地の場所及び受領国

[25] WP108 のパラグラフ 3(3 頁)参照。
[26] WP108 のパラグラフ 4(4 頁)参照。

・WP74 の要求事項がどのように満たされたかを要約した説明文書(データ保護機関が、提出した文書の関連条項を特定するのに役立つ)

・申請者が採用する BCR を構成するすべての関連文書(例えば、申請に関連するかもしれないあらゆるポリシー、規範、通知、手続及び契約)。データ保護機関は、個人データがグループ内で実際にどう取り扱われるかを把握する必要がある。

注意すべき点は、データ保護機関は許可手続の一環としてデータ管理者から受け取った情報につき、国内法に基づく守秘義務を負うが、一部のデータ保護機関は情報公開法にも従わなければならないことである。したがって、BCR の許可申請の裏付けとして提出した書類が商業的に機微な場合には、適切な書類に適切な形で印をつけることが必要である。ただし、情報開示の可否は、データ保護機関が自国の情報公開法に基づいて判断する。他のデータ保護機関が BCR の評価を行うために必要な場合、情報は回覧される。

3) 申請書類のひな型

WP133 は、総則的説明とともに、申請書類のひな型を明らかにしている。

導入部分では、EEA からの国際データ移転に法的根拠を与えるために BCR を活用するには、データ発信国にある EEA のデータ保護機関のそれぞれから承認を受ける必要がある旨が明らかにされている。

また、総則的説明の中では、おおむね、次のような事項が述べられている。

・書式を一部のみ用意し、WP108 の 3.3 及び 3.4[27]に基づいて主管機関になると考えられるデータ保護機関あてに提出する。この書式は全 EEA 加盟国で用いることができる。
・すべての記入項目を埋めること。
・スペースが不足して回答をすべて記入できない場合は、追加のページや別冊を添付することができる。
・申請者において、商業的に機微で秘密にしておくべきと考える回答や資料を指定することができる。ただし、第三者がかかる情報の開示を請求した場合、関係する各データ保護機関が国内法に則して処理する。
・書式提出先のデータ保護機関は、どこが主管となるべきかを判断するため、申請者が承認を求めるあらゆるデータ保護機関あてに、書式の第 1 部を回覧させる。
・最終的にどこが主管データ保護機関に選ばれたかについては、提出先のデータ保護機関から連絡を受ける。
・主管データ保護機関は、協力手続の各段階に対処するため、申請者が承認を求めるすべてのデータ保護機関にあてて、申請者の BCR を含む残りの書類を回覧する。

[27] 本報告書　2. BCR の制度的概要　(6) BCR の承認を得るための申請手続　1) 申請先のデータ保護機関参照。

申請書類のひな型は、第 1 部(申請者の情報)及び第 2 部(状況説明書)に分かれており、第 1 部は、「1. グループの構成及び連絡先」、「2. 取扱い及びデータ流通に関する概要」、「3. 主管データ保護機関（DPA）の決定」、第 2 部は、「4. 拘束力ある企業ルール(BCRs)の拘束的性質」、「5. 実効性」、「6. データ保護機関との協力」、「7. 取扱い及びデータ流通の説明」、「8. 変更の報告と記録の仕組み」、「9. データ保護措置」にて構成されている。

これとは別に、BCR のひな型を添付することとなっているが、必ずしも 1 つの文書にまとめられている必要はなく、文書間の法的関係を明らかにした上で、複数の文書で提出することもできる。また、添付書類は、主管データ保護機関との協議の後、別途提出することもできる。以下、WP133 に掲載された標準申請書を邦訳する。

第 1 部　申請者の情報

1. グループの構成及び連絡先

グループ名、（最上位の親会社の）本社所在地
グループの本社は EEA 内にありますか？ ☐ はい ☐ いいえ

申請者の名称及び所在地
識別番号(もしあれば)
申請者の法的性格(法人、パートナーシップ等)
グループ内の申請者の地位に関する説明(例えば、EEA 内のグループの本社、又は、グループが EEA 内に本社を置いていない場合は、EEA 内でデータ保護責任をゆだねられたグループ構成員)
連絡担当者の氏名及び/又は部署(注：連絡担当者は変更できる。特定個人の氏名ではなく部署を指定することができる。)
住　所
国
電話番号：　　FAX：　　電子メール：

BCR の承認を求める EEA 加盟国

2. 取扱い及びデータ流通に関する概要
次の事項を述べてください。 －BCR が対象とするデータの性質、及び、とりわけ、BCR が 1 つのカテゴリのデータに適用されるのか、2 つ以上のカテゴリに適用されるのか(例えば、人事情報、顧客情報等) －BCR が EEA からの移転のみに適用されるのか、グループ構成員間のすべての移転に適用されるのか。 －EEA 域外で最も多くのデータが発信される国を明記してください。 －BCR が対象とするグループ内での移転の範囲。それには、個人データが移転されるであろう EEA 内又は EEA 外のグループ構成員の説明が含まれる。

3. 主管データ保護機関（DPA）の決定
以下の基準に基づき、どこが主管データ保護機関となるべきかを説明してください。 －グループが EEA 内に本社を置いていない場合、データ保護責任をゆだねられたグループ事業体の EEA 内の所在地 －申請を扱い、グループ内で BCR を執行するに最も適した企業(管理機能、事務的負担等の面で) の所在地 －データの取扱いの目的及び手段について大部分の決定を下す国 －EEA 域外への移転で、最も多くの発信国となる EEA 加盟国

4.　拘束力ある企業ルール(BCRs)の拘束的性質

内部の拘束的性質

グループ事業体内の拘束

BCRs は、どのようにしてグループの構成員に対して拘束力を持たせますか？

☐　グループの全構成員を法的に拘束する方策又はルール
☐　グループ構成員間の契約
☐　親会社が下し、グループの他の構成員を拘束する一方的宣言又は約束
☐　他の規制的手段の組み入れ(例：定められた法的枠組みの中で、成文化した規則に含まれる義務)
☐　適切な政策、監査及び認可によって裏付けられたグループの一般的な経営理念への BCRs の組み入れ
☐　その他(具体的に述べて下さい)

上記の仕組みが、グループの他の構成員（特に本社）によって執行可能であるという意味で、グループの構成員にどのように法的拘束力を持つのかを説明してください。

BCR の内部の拘束力は、グループ全体に及びますか？(一部のグループ構成員を対象外とすべき場合は、方法と理由を明確に述べてください)

従業員に対する拘束性

御社グループは、BCRs が従業員に対して確実に拘束力を持つように、以下の措置の一部又は全部を講じるかもしれませんし、他にも措置があるかもしれません。詳細を以下に記してください。

－雇用契約書

－団体契約(労働者委員会/その他の組織が承認したもの)

－従業員は、BCR 又は BCR が組み入れられた関連倫理ポリシーを通読したことを、署名又は証言しなければならない。

－BCRs を関連する企業ポリシーに組み入れる。

－関連する企業ポリシーを遵守しないことに対する規律上の制裁(違反を理由とする解雇を含む)。

BCR が従業員に対してどのように拘束力を持つのかを説明するため、必要に応じて、ポリシー及び手順又は秘密保持契約書の抜粋によって裏付けられた要旨を提出してください。

データを取り扱う下請業者に対する拘束

個人データの取扱いに対する保護措置の適用を下請業者に義務づけるため、どのような措置を講じましたか(例えば、下請業者との契約の中の義務を用いる)。具体的に述べてください。

かかる契約は、違反の影響にどう対応していますか。

下請業者が遵守しないときに下される罰則を具体的に述べてください。

外部への拘束的性質

個人のため(第三者の受益権)、対外的に拘束力を持つルールはどのようなものですか。あるいは、どのようにして、かかる権利を創出するつもりですか。例えば、契約や一方的宣言の中で、何らかの第三者の受益権を創出したかもしれません。(筆者注：脚注 11 では、「一部の法域（例えばイタリアやスペイン）の民法では、一方的宣言や一方的約束が拘束力を持たないことを十分認識してください。かかる宣言の拘束性に関して、明確な法律上の規定がないため、第三者の受益権の規定を伴う契約をグループ構成員間で交わさなければ、拘束力を証明できないでしょう。」と付記されている)

法的請求又は訴訟
WP108 のパラグラフ 5.14(筆者注：裁判所への訴訟提起)の要求に従い、どのように義務を履行するのかを説明してください。

グループの欧州本社、又は、欧州経済領域内でデータ保護責任をゆだねられたグループ内の組織は、自ら又は発信地のグループ構成員が、グループのいずれかの部門による BCR 違反からの損害に対する賠償金を支払えるように、適切に手配されていることを確認してください。さらに、それがどのように確保されるのかを説明してください。
訴えがどこから起こされたかに関係なく、ルール違反の疑いに関する挙証責任が、移転の発信地のグループ構成員又は欧州本社又はデータ保護責任をゆだねられた組織部門にあることを確認してください。

5. 実効性

御社の内部で施行されている BCR が、どのように実際にいかされているのか(特に、BCR に基づきデータが移転される EEA 域外諸国で)を示すのが大切です。安全保護措置が十分かどうかを評価する際に重要だからです。

訓練及び認識の向上(従業員)

－特別訓練プログラム －従業員が BCR とデータ保護について試験を受けること －BCR が書面又はオンラインで全従業員に通知されていること －会社幹部による点検と承認 －従業員が自己の業務におけるデータ保護の意味合いを認識する、すなわち、関連するプライ

バシーポリシーが自身の行動に適用されるのを認識し、それに則して対応するように、どのような訓練を受けているか(この点は、従業員が EEA を拠点にしているかどうかに関係なく適用される)。

下請業者に対し、個人データの取扱いに安全保護措置を取り入れるように義務づけるため、いかなる手段を講じましたか（例えば、御社と下請業者の契約上の義務を用いて)。具体的に説明してください。

内部の苦情処理

BCR には、遵守を強制するような内部の苦情処理制度が含まれていますか。

その苦情処理制度を説明してください。

遵守の検証

御社グループは、各構成員の BCR 遵守を監査するため、どのような検証の仕組みを導入していますか(例えば、監査プログラム、遵守プログラム等)。具体的に説明してください。

検証や遵守プログラムがグループ内でどう機能するのかを説明してください(例えば、監査報告書の受領者や、グループ組織内での受領者の地位に関する情報)。

BCR は以下の活用を定めていますか。

－データ保護責任者(Data Protection Officer)
－内部監査人
－外部監査人
－内部監査人と外部監査人の組合せ
－内部遵守部門による検証

BCR は、検証の仕組みが下記に明記されたかどうかを述べていますか。

－御社のデータ保護基準を含む文書
－他の内部手続文書及び監査報告書

6. データ保護機関との協力

御社の BCR がデータ保護機関との協力の問題をどう扱っているのか、具体的に述べてください。

御社の承認を与えたデータ保護機関に対し、御社の遵守状況の監査を許可すると認めますか。

グループ全体及びグループ内の各企業が、BCR の解釈及び適用に関して、権限ある機関の助言に従うことを認めますか。

7. 取扱い及びデータ流通の説明

次に掲げる事項を示してください。
－BCR の対象となるデータの性質(例えば、人事データ)、及び、特に、BCR が 1 つのカテゴリのデータに適用されるのか、複数のカテゴリに適用されるのか。
－移転される個人データはどのような性質か。
－広い意味で、データはどこからどこに流れるのか。
－広い意味で、データ流通の範囲はどのようになっているか。
－移転及び移転後に行われる取扱いの目的は何か。
－BCR 対象データが第三国に移転される目的。
－BCR の対象となるグループ内の移転の範囲(個人データが移転され得る EEA 域内又は域外のグループ構成員の説明を含む)。

BCR は、EEA からの移転だけに適用されますか。あるいは、グループ構成員間のあらゆる移転に適用されますか。具体的に述べてください。

8. 変更の報告と記録の仕組み

御社の BCR は、承認に対して原則的に影響を与えるような BCR の重要な変更について、グループの他部門及び関連するデータ保護機関への通知をどのように考慮しているのか、説明してください(要旨)。

御社の BCR の変更を記録する制度が導入されていることを確認してください。

9. データ保護措置

下記の問題をどこでどう対処するのか、御社の BCR を参照しながら、具体的に述べてください。裏付けとなる文書は適宜添付してください。

－データ主体に対する透明性及び公平性
－目的の制限
－データの質の確保
－安全保護措置
－個人のアクセス権、訂正権、及び、取扱いへの異議を申し立てる権利
－転送の制限
－その他(例えば、児童の保護等)

付属文書 1： 正規の拘束力ある企業ルールの写し

御社の BCR の写しを 1 部添付してください。提出を希望する補助的文書(例えば、個別のプライバシーポリシーや規則)が含まれないようにご注意ください。

（７）BCR に記載すべき事項と申請書類に記載すべき事項

以上、BCR の内容及び申請手続の概要を述べた。BCR に記載すべき事項と申請書類に記載すべき事項には重複するものが多いが、異なる項目も存在する。WP153 は、以下のように、その関係を一覧表の形で整理している。

BCR 承認の基準	BCR	申請書類
1－拘束的性質		
内部		
BCR の遵守義務	○	○
グループの構成員と従業員に対する拘束力をルールに持たせる方法の説明	×	○
外部		
管轄のデータ保護機関や裁判所への苦情申立てなど、第三者の受益権の設定	○	○
企業が、BCR 違反に対する損害賠償及び救済責任を認める旨	○	○
企業が十分な資産を有すること	×	○
証明責任は個人ではなく企業に課せられること	○	○
データ主体が、BCR、とりわけ、自らに有利に働く第三者の受益権に関する情報に、容易にアクセスできること	○	×
2－実効性		
適切な訓練プログラムの存在	○	○
BCR に関する苦情処理手順の存在	○	○
BCR を対象とした監査プログラムの存在	○	○
苦情を取り扱い、ルールの遵守を監督及び保証するプライバシーオフィサー又は適切な係員のネットワークの設置	○	×
3－協力義務		
データ保護機関と協力する義務	○	○
4－取扱い及びデータ流通に関する説明		
BCR が対象とするデータ移転に関する説明	○	○
BCR の地理的及び内容的範囲の説明(データの内容、データ主体の種類、国)	○	○

BCR 承認の基準	BCR	申請書類
5－変更の報告及び記録に関する仕組み		
BCR の更新手順	○	○
6－データの安全保護措置		
EU 域外への移転又は転送に関するルールを含むプライバシー諸原則に関する説明	○	○
BCR に拘束される事業者のリスト	×	○
国内法のためグループが BCR を遵守できない場合に、透明性を維持する必要性	○	×
国内法と BCR の関係に関する声明	×(ただし推奨される)	×(ただし推奨される)

３．モデル契約の概要

弁護士　武井　一浩
弁護士　濃川　耕平
弁護士　松本　絢子
弁護士　迎　奈央子

（１）概要

1）個人データの EU 域内から EU 域外の第三国への移転

EU において 1995 年 10 月 24 日に採択され、1998 年 10 月 24 日に発効した「個人データの取扱い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」(DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)(EU データ保護指令)は、個人データ[1]の国際移転についての規制を設けている。

具体的には、EU データ保護指令 25 条 1 項は、EU 加盟国(EU 加盟国 27 か国並びに EEA(欧州経済領域)構成国であるノルウェイ、リヒテンシュタイン及びアイスランドを含む。以下同じ。)[2]は、EU データ保護指令の他の規定に従って採択された国内規定の遵守を損なうことなく、EU 加盟国以外の第三国については、「十分なレベルの保護」(adequate level of protection)を確保している第三国に限って個人データを移転できることを定めなければ

---

[1] 個人データとは、特定の又は特定可能な自然人(データ主体 data subject)に関するすべての情報(any information relating to an identified or identifiable natural person)をいい、ここにいう特定可能な人とは、具体的には、識別番号又は当該人の身体的、生理的、精神的、経済的、文化的又は社会的アイデンティティに特有の 1 つ以上の要素を参照することにより、直接又は間接に特定することができる人(one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity)をいう(EU データ保護指令 2 条(a))。

[2] EU データ保護指令に基づく個人データ移転に関する規制は、スイスを除く EFTA(欧州自由貿易連合)加盟国であるノルウェイ、リヒテンシュタイン及びアイスランドにも適用されている。EEA には上記 3 国も加盟しているが、"DECISION OF THE EEA JOINT COMMITTEE No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement"(以下「EEA 合同委員会決定」という。) Whereas 条項(4)項によると、EU データ保護指令は EEA 協定に組み込まれ、EU データ保護指令第 4 章は EEA 協定の目的に適合させるものとされており、EEA 加盟国にも EU データ保護指令 4 章の規定が適用される。なお、EEA 合同委員会決定 2 条により、欧州委員会が EU データ保護指令 25 条 4 項、25 条 6 項、26 条 3 項 2 文又は 26 条 4 項に従って同 31 条に基づき十分なレベルの保護を確保している第三国の認定や十分な保護措置の決定等の措置をとる場合において、EEA 合同委員会が EEA 協定への当該措置の組み込みを留保したときは、EFTA 加盟国が当該措置を適用しない旨の決定及び欧州委員会に対する通知をしない限り、EFTA 加盟国に当該措置が適用されるものとされている(ただし、EEA 合同委員会が当該措置を EEA 協定に組み込むことについて当該措置の効力発生日後 12 か月以内に合意に至らなかった場合には、EFTA 加盟国は当該措置の適用を止めることができる。)。また、当該措置を適用しない EFTA 加盟国に対しては個人データを移転してはならないものとされている。

ならない旨規定しており[3]、同 2 項は、第三国が提供する保護の十分性について、データ移転に関するあらゆる状況、特に、データの性質、取扱いの目的及び期間、データの発信国及び最終目的国、当該第三国の一般的及び分野別の法規範並びに専門的規範及び安全保護対策措置等に鑑みて、評価されなければならない旨を規定している[4]。

[3] EU データ保護指令 25 条 1 項の原文は以下のとおりである。
The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

[4] EU データ保護指令 25 条 2 項の原文は以下のとおりである。
The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

この点、日本には個人情報保護法が存在するものの、EU(欧州委員会)により十分なレベルの保護を確保しているとは正式に認められていないため[5]、EU 加盟国から日本への個人データの移転は行うことができないのが原則である。

もっとも、上記 25 条の例外として、EU データ保護指令 26 条は、十分なレベルの保護を確保していない第三国に対して個人データを移転できる場合を定めており、EU データ保護指令 26 条 1 項において、EU 加盟国は、データ主体が個人データの移転に対して明確な同意を与えている場合等の条件を満たす場合[6]には、十分なレベルの保護を確保していない第三国に対して個人データを移転できる旨定めなければならないとされるほか、EU データ保護指令 26 条 2 項では、個人データの管理者[7]が、個人のプライバシー、基本権及び自由の保護並びに対応する権利の行使に関する「十分な保護措置(adequate safeguards)」(特に適切な契約条項によって生じ得る。) を提示する場合にも、十分なレベルの保護を確保していない第三国に対する個人データの移転を認めることができるとしている[8], [9]。

---

[5] EU(欧州委員会)において十分な保護を提供していると認められている国・地域としては、本報告執筆時点において、スイス、カナダ、アルゼンチン、ガーンジー、マン島、ジャージー、フェロー諸島がある。

[6] (a)データ主体が移転に対して明確な同意を与えている場合(the data subject has given his consent unambiguously to the proposed transfer)に加え、
(b)移転が、データ主体と管理者との間の契約の履行のために、又はデータ主体の請求に応じて契約締結前の措置の実施のために必要である場合(the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request)、
(c)移転が、データ主体の利益のために管理者と第三者との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(the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party)、
(d)移転が、重要な公共の利益を根拠として、又は法的請求の確定、行使若しくは防御のために必要である場合、又は法的に要求される場合(the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims)、
(e)移転が、データ主体の重大な利益を保護するために必要である場合(the transfer is necessary in order to protect the vital interests of the data subject)、
(f)移転が、法令に従って公衆に情報を提供することを目的とし、公衆一般又は正当な利益を証明する者による閲覧のために公開されている記録から、具体的な事例において閲覧に関する法律に規定された条件が満たされる範囲内で行われる場合(the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case)
が条件として列挙されている。

[7] 管理者とは、個人データの取扱いの目的や手段を決定する主体(the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data)をいう(EU データ保護指令 2 条(d))。

[8] EU データ保護指令 26 条 2 項の原文は以下のとおりである。
… a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

[9] EU データ保護指令 24 条は、EU 加盟国に対し、EU データ保護指令に従って採択された国内規定の違反に対して課される制裁に関して規定しなければならないものとしている。

「十分な保護措置」を提示する場合とは、個人データの管理者である企業、組織等が、①EU(欧州委員会)により承認されたモデル契約(Model Contract Terms)を利用する場合、②国際移転に係る拘束力のある企業ルール(binding corporate rules for international transfers)を定め、データ保護機関に申請して承認を得た場合、③セーフハーバーに参加し、セーフハーバー原則による場合[10]等が挙げられており、これらの場合には、第三国への個人データの移転が可能となる。

日本は EU との間でセーフハーバー協定を締結していないため、③の方法によることはできない。よって、日本企業の場合、EU 域内(EU 加盟国内をいう。以下同じ。)の企業から日本に所在する企業その他の EU 域外（EU 加盟国以外の第三国をいう。以下同じ。）の企業への個人データの国際移転（グループ会社間の個人データ移転を含む。）を行う際には、①又は②の方法をとることが考えられる。

①の方法は、個人データ移転の取引を行う EU 域外の企業と個別に契約を締結することで、契約当事者間において個人データの国際移転を可能にするものであり、②の方法が承認される以前から欧州委員会の承認に基づき利用されていた方法である。これに対し、②の方法は、企業グループ内における個人データ移転に関するルールにつき EU 域内のデータ保護機関によって拘束力のある企業ルールとして承認されることで、当該ルールの適用される企業グループ内での個人データの国際移転を可能にするものであり、2003 年に欧州委員会によって承認された方法である。

以下、企業における上記①のモデル契約の利用について、②の拘束力ある企業ルールの利用とも比較の上、検討を行う。

2）モデル契約の概要

上記モデル契約について、欧州委員会は、EU データ保護指令 26 条 4 項に従って、3 種類のモデル契約を採択している。

まず、欧州委員会は、EU 域内のデータ管理者から十分なレベルの保護を確保していない第三国のデータ管理者への個人データ移転の取引を行うためのモデル契約として、”COMMISSION DECISION of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries”(以下「2004 年決定」という。）において、2 種類のモデル契約を採択した（以下併せて「管理者移転型モデル契約」という。)。具体的には、”COMMISSION DECISION of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC”(以下「2001 年決定」という。）において既に採択されていたモデル契約を SET Ⅰ、2004 年決定において新たに採択したモデル契約を SET Ⅱとし、当事者は両モデル契約のいずれかを選択して使用

[10] 米国は、EU データ保護指令への対応として、2000 年 5 月、EU との間でセーフハーバー協定(Safe Harbor Agreement)を締結し、米国商務省が作成するセーフハーバー原則(2000 年 7 月公表)を産業界が遵守していれば EU データ保護指令 25 条違反にならないというセーフハーバーを設定している。

することができることとされた。

また、欧州委員会は、上記第三国において設立されたデータ処理者[11]に対する個人データ移転の取引を行うためのモデル契約として、上記のモデル契約とは別に、”COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council”(以下「2010 年決定」という。）[12]において、1種類のモデル契約を採択している（以下「処理者移転型モデル契約」という。)。

上記モデル契約は、以下の EU データ保護指令の定めを反映しているものである[13]。

① 個人データは、特定の、明確な、及び合法的な目的のためにのみ収集されなければならない。

② 関係する個人は、当該目的及びデータ管理者の属性について知らされなければならない。

③ 関係するいかなる個人も、自己のデータにアクセスする権利と、不正確な情報につき変更又は削除をする機会を与えられなければならない。

④ 何か不正なことが起きた場合、管轄裁判所を通じた損害賠償を含む適切な救済により当該不正が是正可能でなければならない。

以下、各モデル契約の規定内容について説明する。

---

[11] 処理者とは、管理者に代わって個人データの処理を行う主体(the natural or legal person, public authority, agency or any other body which processes personal data on be half of the controller)をいう(EU データ保護指令 2 条(e)項)。

[12] 上記 2010 年決定により、同決定において採択されたモデル契約が、2010 年 5 月 15 日をもって、”Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC of the European Parliament and of the Council”(以下「2002 年決定」という。）において採択されたモデル契約に代えられるものとされている。よって、2010 年 5 月 15 日より前においては、引き続き従前のモデル契約が用いられることとなる。

[13] 2005年1月7日付け”Standard contractual clauses for the transfer of personal data to third countries - Frequently asked questions”(以下「2005 年 FAQ」という。）参照。

（２）管理者移転型モデル契約の内容

1）概要

上記のとおり、管理者移転型モデル契約は、EU 域内のデータ管理者から EU 域外のデータ管理者に対して個人データを移転する場合に適用されるモデル契約である。

管理者移転型モデル契約には、SET Ⅰ及び SET Ⅱの二種類があり、2004 年決定がなされる以前においては、2001 年決定に基づくモデル契約(SET I)のみが利用されていたものである。

しかし、この SET Ⅰを用いた実務に対しては、経営者において幅広い選択を可能にしてほしいというビジネス上の要請があり[14]、これを踏まえて国際商業会議所(International Chamber of Commerce)を筆頭とするビジネス団体の連合[15]が新しいモデル契約の提案を行った結果、欧州委員会の協議を経て、新たに SET Ⅱが決定された。当該ビジネス団体連合によると、SET Ⅱは、訴訟、責任の分配又は監査要求等に関連する規定について企業に優しいものとなっており、ビジネス上の要請に合致するものであるとしている。ただし、SET Ⅱにおいても、データやデータ主体の保護という観点から、SET Ⅰと同程度のデータ保護を施しているものである[16]。

以下、SET Ⅰ及び SET Ⅱの規定内容の要旨を記載する。

2）SET Ⅰの主な規定内容

SET Ⅰの各条文の規定内容の要旨は以下のとおりである。

①　定義条項(1 条)

(a)「個人データ」、「特殊な分類のデータ」、「処理」、「管理者」、「処理者」、「データ主

---

[14] 具体的には、アメリカの企業は以下の点等において従来のモデル契約(従来の処理者移転型モデル契約も含む。）を批判していた(David Bender & Larry Ponemon, *Binding Corporate Rules for Cross-Border Data Transfer*, Rutgers Journal of Law & Urban Policy Vol.3:2 154, 160 (2006))。

① 執行可能な第三受益者の権利をデータ主体に対して付与していること

② 準拠法がデータ発信者が設立された EU 加盟国の法とされており、当該加盟国における紛争解決にデータ受信者が従わなければならないこと

③ データ発信者の国のデータ保護機関の要求により契約書のコピーを納めなければならず、また当該データ保護機関は当該契約につき監査する権利を有するものとされていること

④ データ発信者及びデータ受信者の連帯責任が規定されていること

[15] 具体的には、International Chamber of Commerce のほか、Japan Business Council in Europe(在欧日系ビジネス協議会)、European Information and Communications Technology Industry Association(現 DIGITALEUROPE)、EU Committee of the American Chamber of Commerce in Belgium、Confederation of British Industry、International Communication Round Table 及び Federation of European Direct and Interactive Marketing の 7 団体である。

[16] EU データ保護指令 29 条に基づき設置された ARTICLE 29 Data Protection Working Party(以下「29 条ワーキンググループ」という。）が 2003 年 12 月 17 日付けで採択した”Opinion 8/2003 on the draft standard contractual clauses submitted by a group of business associations (“the alternative model contract”)”によると、既に存在するモデル契約に加えてさらに採択することとなる新しいモデル契約は、2001 年決定におけるモデル契約と同レベルの保護を与えるものであり、かつ企業及び市民にとってより優しいという付加価値を有するものであること、という条件を満たすものでなければならないとされている。

体」及び「監督当局」とは、EU データ保護指令におけるそれと同じ意味を有する。

(b)「データ発信者」とは、個人データを移転する管理者をいう。

(c)「データ受信者」とは、十分な保護が確保された第三国のシステムに従うのではなく、本契約の条項に従って更なるデータ処理を行うため、データ発信者から個人データを受領することにつき合意したデータ管理者をいう。

② データ移転に係る詳細(2 条)

データ移転の詳細、特に個人データの分類及びデータ移転の目的について、添付書類 1[17]において特定する。

③ 第三受益者条項(3 条)

データ主体は、本条、4 条(b)項、(c)項及び(d)項、5 条(a)項、(b)項、(c)項及び(e)項、6 条(a)項及び(b)項、7 条、9 条並びに 11 条について第三受益者の権利として執行できる[18]。

④ データ発信者の義務(4 条)

(a) 個人データの移転を含む処理は、その移転のときまでデータ発信者が設立された EU 加盟国の関連法令に従って行う。

(b) 特殊な分類のデータに関わる移転を行う場合には、十分な保護が提供されない第三国へのデータ移転につき事前にデータ主体に対して通知する。

(c) データ主体に対し、その要請に応じ、本契約のコピーを認める。

(d) 監督機関及びデータ主体からの、データ受信者による関連個人データの処理についての質問に対し、合理的期間内に、合理的に可能な範囲で回答する。

⑤ データ受信者の義務(5 条)

(a) 適用法令により契約に基づく義務の履行が妨げられると信じる理由はないことを保証し、また、本契約に基づく保証に実質的に反する可能性のある法令の変更がある場合には、データ発信者及びデータ発信者が設立された場所における監督機関に対して当該変更を通知する。このとき、データ発信者はデータ移転を延期し、及び/又は契約を解除することができる。

---

17 添付書類 1 には、データ発信者、データ受信者、データ主体、データ移転の目的、データの分類、センシティブ・データ、データ開示が許容されるデータ受領者及び保管期間を特定して記載しなければならない。

18 第三者たるデータ主体は、モデル契約の契約当事者ではないが、モデル契約に規定された内容に従って直接自己の権利として執行できるものとされている。

(b) 添付書類 2[19]に定めるデータ保護方針に従って個人データの処理を行う。又は、添付書類 3[20]に定めるデータ保護方針に従う旨明示的に合意された場合には、自然人の基本的権利及び自由(特に、データ発信者の設立国においてデータ管理者に適用される個人データの処理に対するプライバシー権)を保護する国の関連法令又は EU データ保護指令 25 条 6 項に基づく欧州委員会の決定に従ってデータ処理を行う。

(c) データ発信者又はデータ主体からの個人データの処理に関する合理的質問に対し、速やかにかつ適切に対応し、また、質問の過程で管轄の監督機関と協力し、移転データの処理に関して監督機関の助言に従う。

(d) データ発信者の要請に基づき、データ発信者による、又は監督機関との合意に基づきデータ発信者により選出された、独立性を有し、専門資格を有するメンバーで構成された監査機関による監査に付するため、データ処理設備を提供する。

(e) データ主体に対し、その要請に応じ、本契約のコピーを認め、苦情処理を担当するオフィスを知らせる。

⑥ 責任(6 条)

1. データ主体は、3 条に定める条項の違反により損害が発生した場合には、当該損害につき契約当事者から補償を受ける権利を有する。契約当事者は、当該違反につきいずれの当事者にも責任がないことを立証しない限り、責任を免れることはできない。

2. データ発信者及びデータ受信者は、データ主体に対し、3 条に定める条項の違反により生じた損害について連帯責任を負う。

---

19 データ保護方針として、以下の旨が規定されている。

1. 添付書類 1 に記載された目的に従って、データの処理及び使用又は交換をしなければならず、目的に必要な範囲でデータを保持すること

2. データは、正確かつ必要に応じて最新のものでなければならず、目的との関係で十分であり、関連性を有し、及び過度でないものであること

3. データ主体に対し、処理の目的及び第三国におけるデータ管理者の身元その他公正な処理のために必要な情報を提供すること

4. データ管理者により機密保持のための措置がとられること

5. データ主体は、処理されるすべての関連データにアクセスすることができ、本方針に反する処理に対してデータの訂正、削除及び阻止をすることができ、並びに正当な理由がある場合にはデータ処理に異議を述べることができること

6. データ受信者から第三国の別の管理者への個人データの転送は、一定の場合に限られること

7. 人種、政治的見解、宗教等の特殊な分類の情報については、追加的な保護措置を施さなければならないこと

8. 直接販売の目的で処理される情報については、データ主体による当該使用からのオプト・アウトを可能にするための有効な手段を設けること

9. データ主体は、個人の正当な利益を保護する他の措置が講じられていない限り、データの自動処理のみに基づく決定を受けない権利を有すること

20 データ保護方針として、上記のうち 1、5 及び 6 が規定されている。

3. 一方当事者が他方当事者による 3 条に定める条項の違反に関して責任を負わされた場合には、他方当事者は、自己の責任の範囲で一方当事者が負担した費用、損害等を補償する[21]。

⑦ 調停又は裁判管轄(7 条)

1. データ主体と契約当事者の間における紛争が友好的に解決されず、データ主体が 3 条に定める第三受益者条項を発動する場合には、データ主体の選択により、独立者又は監督機関による調停又はデータ発信者が設立された EU 加盟国における裁判に付される。

2. 当該当事者が仲裁裁定の執行に関する New York Convention を批准している国で設立されている場合には、データ主体及び関係当事者の合意により、仲裁に付することができる。

3. 前 2 項は、データ主体が国の又は国際的な法令に従って救済を求めることを妨げるものではない。

⑧ 監督機関との協力(8 条)

監督機関又は国の法令の要請がある場合、契約当事者は監督機関に対して本契約のコピーを提出する。

⑨ 契約終了(9 条)

いついかなる状況及び理由により本契約が終了した場合においても、移転データの処理に関する本契約に基づく義務及び/又は条件が免除されるものではない。

⑩ 準拠法(10 条)

データ発信者が設立された EU 加盟国の法に準拠する。

⑪ 契約の修正(11 条)

本契約の条項を修正変更してはならない。

3) SET Ⅱの規定内容

SET Ⅱの各条文の規定内容の要旨は以下のとおりである。

① 定義条項

(a)「個人データ」、「特殊な分類のデータ/センシティブ・データ」、「処理」、「処理者」、

[21] 2001 年決定の Whereas 条項(20)項によると、本条項は、データ主体の保護のため必要な事項ではなく、当事者間の交渉の便宜のために入れているものであるから、3 項は削除することができるものとされている。

「データ主体」及び「監督当局/当局」は、EU データ保護指令におけるそれと同じ意味を有する(ただし、「当局」とは、データ発信者の設立国における管轄データ保護機関を意味する。)。

(b)「データ発信者」とは、個人データを移転する管理者をいう。

(c)「データ受信者」とは、十分な保護が確保された第三国のシステムに従うのではなく、本契約の条項に従って更なるデータ処理を行うため、データ発信者から個人データを受領することにつき合意したデータ管理者をいう。

(d)「本契約」とは、当事者間の個別の商業上の契約に定められた営利事業上の条件を包含しない独立の文書としての当該契約をいう。

② データ発信者の義務(1 条)

(a) 個人データの収集、処理及び移転は、データ発信者に適用される法令に従って行う。

(b) データ受信者が本契約に基づく法的義務を履行する能力を有することについて合理的努力[22]をもって判断する。

(c) データ受信者の要請に基づき、データ発信者の設立国の、関連するデータ保護法令又は参考資料(法的助言を含まない。) のコピーを提供する。

(d) データ主体及び当局からの、データ受信者による個人データの処理についての質問に対し、契約当事者間においてデータ受信者が回答する旨の合意[23]がある場合を除き、回答する。上記合意がある場合においても、データ受信者が回答しない又は回答できないときは、データ発信者が、合理的期間内に、合理的に可能な範囲で、合理的に取得可能な情報に基づき回答する。

(e) 本契約に機密情報が含まれる場合(この場合、当該情報を削除することができる。)を除き、第三受益者たるデータ主体に対し、その要請に応じ、本契約のコピーを認める。当該情報を削除したときは、データ主体に対して文書にて削除の理由及びデータ主体において当該削除について当局宛に通知する権利を有する旨を通知する。ただし、データ主体が削除された機密情報の機密保持に合意する限り、データ主体に本契約の全文を開示するとの当局の決定に従わなければならない[24]。当局にもその要請に基づき

---

[22] ビジネス団体側は、「商取引上の合理的な努力」とすることを求めていたが、欧州委員会は、データ発信者の義務は経済的要因に条件付けられるものであってはならないことを根拠にこれを拒否した(Christopher Kuner, *The E.U. Alternative Standard Contractual Clauses for International Data Transfers*,BNA International World Data Protection Report (2005)(以下「Kuner Report」という。) p.2)。

[23] データ発信者においてすべての質問に対応することはデータ発信者に負担を課すものであり(SET Ⅰの 4 条(d)項参照。)、データ移転後は、データ受信者の方がデータ処理に関する報告に適していることが考えられることから、データ受信者において質問に対応することを可能にすべく規定されたものである(Kuner Report p.2)。

[24] ビジネス団体側が本契約には機密情報も含まれることを懸念していたのに対し、欧州委員会は、データ主体は本契約のコピーを取得しない限り第三受益者としての権利を行使することが不可能であるとして、上記規定にて合意されたものである(Kuner Report p.2)。

本契約のコピーを提供する。

③ データ受信者の義務(2 条)

(a) 不測の又は違法な破壊、不測の滅失、変更、無断の開示又はアクセス等から個人データを保護すべく、データ処理及びデータの性質に基づくリスクに対して適切なレベルの、技術的及び組織的な保護対策を採る。

(b) データ処理者を含む個人データにアクセスする権限を有するすべての第三者が、個人データの機密保持及び保護につき遵守及び維持するための手続を置く。データ処理者を含むデータ受信者の権限に基づき行動するすべての者は、データ受信者の指示のみによって個人データを処理する義務を負う。ただし、法令又は規則により個人データへのアクセス権限を認められた個人については本条項は適用されない。

(c) 本契約を締結する時点で、本契約に基づく保証に実質的に反する可能性のある地域の法令があると信じる理由はないことを保証し、また、そのような法令が発覚した場合には、データ発信者に対して通知する[25]。

(d) 添付書類 B[26]に定める目的に従って処理し[27]、本契約に定める事項を保証し、及び履行する法的権限を有することを保証する。

(e) データ発信者に対し、個人データの処理に関する質問の対応権限を有する組織内の窓口を明らかにし、当該質問に関し合理的間内に対応すべく、データ発信者、データ主体及び当局と誠実に協力する。データ発信者が解散した場合、又は当事者がそう合意した場合には、データ受信者は上記 1 条(e)項を遵守する責任を負うものとみなされる。

(f) データ発信者の要請に基づき、データ発信者に対して下記 3 条に係る責任を履行するために十分な財源の証明を提供する。

(g) データ発信者の合理的要請に基づき、データ発信者(又は、データ受信者による合理的な異議がある場合を除き、データ発信者が選任した独立の若しくは公平な検査機関若しくは監査役)による、本契約の遵守についての、合理的な通知をもって及び通常の営業時間内において行う検討、監査及び/又は証明に必要なデータ処理設備、データファイル及び書類を提供する[28]。上記要請は、データ受信者の国における規制機関又は

[25] SET Ⅰの 5 条(a)項の規定につき、すべての法令が契約に基づく履行を妨げるものではないことを確認することは不可能に近く、データ受信者にとっての負担が大きいとの企業側の要請を受け、柔軟かつ合理性を有する規定とされた(Kuner Report p.3)。

[26] SET Ⅰの添付書類 1(脚注 17 参照。) の内容とほぼ同様である。

[27] 当初ビジネス団体側は、データ受信者のデータ処理の目的についてデータ収集目的に矛盾しない範囲で広く認めることを要請していたが、欧州委員会及び 29 条ワーキンググループは、データ主体はデータ収集目的を知ることができないこと及び EU 加盟国間において目的に矛盾しないとされる範囲につき解釈の違いがあることから、添付書類 B に記載した目的に限るものとされた。ただし、欧州委員会は、非公式にデータ処理の目的は広く記載することができることを認めたとのことである(Kuner Report p.3)。

[28] ビジネス団体側が、データ受信者が、データ発信者の要請に基づきいつでも上記書類等を提出しなければならないとすることは合理的ではなく、また実務に合わない旨の主張をしたことから、当該主張が取り入れられて規定されたものである(Kuner Report p.3)。

監督機関の同意又は承認に付され、データ受信者は、当該同意又は承認につき適時に取得するよう努力する。

(h) データ発信者の設立国のデータ保護法令、EU データ保護指令 25 条 6 項に基づく欧州委員会の決定の関連規定又は添付書類 A[29]記載のデータ処理方針のいずれかを選択して、これに従ってデータ処理を行う。

(i) EEA 以外に存する第三データ管理者に対して、データ発信者に対して移転に関して通知し、かつ、(ⅰ)第三データ管理者が、第三国において十分な保護を有するものとする欧州委員会の決定に従って個人データを処理する場合、(ⅱ)第三データ管理者が、本契約若しくは他の EU の管轄当局により承認されたデータ移転の契約に署名した場合、(iii)データ主体が、データ移転の目的、受領者の分類及びデータ発信先の国において異なるデータ保護基準を有する可能性があるとの事実につき通知を受けた後において異議を述べる機会が与えられた場合、又は(iv)センシティブ・データの転送について、データ主体がこれに明確に同意を与えた場合を除いて、個人データを開示又は移転してはならない。

④ 責任及び第三者の権利(3 条)

(a) 各当事者は、本契約の違反について生じたいかなる損害についても、他方当事者に対して責任を負う。当事者間の責任は、実際に生じた損害に限られ、懲罰的賠償は除外される。各当事者は、本契約に基づく第三受益者の権利に係る違反によってデータ主体に生じた損害につき責任を負う[30]。

(b) データ主体は、データ受信者又はデータ発信者に対し、関連する契約上の義務の違反について、第三受益者の権利(本条項、1 条(b)項、(d)項及び(e)項、2 条(a)項、(c)項、(d)項、(e)項、(h)項及び(i)項、3 条(a)項、5 条、6 条(d)並びに 7 条)を執行する権利を有し、このとき、管轄はデータ発信者の設立国とする。データ受信者の違反についての主張を含む場合には、データ主体は、まず最初にデータ発信者に対してデータ受信者に対する権利を適切に行使するよう要求し、データ発信者が合理的期間内(通常 1 ヶ月内)に当該行動を採らなかった場合、データ受信者に対して直接権利行使できるものとする。データ主体は、データ受信者が本契約に基づく法的義務を履行する能力を有することについて合理的努力をもって判断することを怠ったデータ発信者に対しては、直接手続を採る権限を有する(データ発信者は、合理的努力をしたことを証明する責任を負う。)。

---

[29] SET Ⅰの添付書類 2 (脚注 19 参照。) とほぼ同様である。ただし、脚注 19 の 5 項の内容について、ビジネス団体側が、データ主体がアクセスの要請をすることにつき悪用し、又は反復的に行う可能性を懸念していたことを受け、データ主体によるアクセスにつき一定の制限がされている(Kuner Report p.6)。

[30] ビジネス団体側は、SET Ⅰの 6 条に規定するデータ発信者及びデータ受信者の連帯責任につき、商取引上の契約において非常に稀な規定であるとして異議を述べた。本契約においては、データ発信者につき 1 条(b)項及びデータ受信者につき 2 条(f)項に基づくデューデリジェンスに係る義務を課し、両当事者間の連帯責任は規定していない(Kuner Report p.4)。

⑤　準拠法(4 条)

本契約は、2 条(h)項に基づくデータ受信者による個人データ処理に適用される法令を除き、データ発信者の設立国の法に準拠する。

⑥　データ主体又は当局との紛争解決(5 条)

(a) データ主体又は当局により紛争又は苦情が主張された場合には、契約当事者は互いに当該紛争又は苦情について通知し、友好的に解決すべく協力する[31]。

(b) 契約当事者は、データ主体又は当局により開始された非拘束的な調停に応じ、他の仲裁、調停又はその他のデータ保護紛争に係る紛争解決方法への参加も検討する。

(c) 各当事者は、最終的かつ上訴不可能な、データ発信者の設立国の管轄裁判所又は当局の決定に従う[32]。

⑦　終了(6 条)

(a) データ受信者が本契約に基づく義務に違反した場合には、データ発信者は、違反の治癒又は契約終了までの間、個人データのデータ受信者に対する移転を一時的に停止することができる。

(b) (ⅰ)上記(a)項に基づきデータ移転が 1 ヶ月を超えて停止されている場合、(ⅱ)データ受信者による本契約の遵守が受信国の法令又は規則に違反する場合、(ⅲ)データ受信者が実質的又は継続的に本契約に基づく保証事項等に違反している場合、(ⅳ)データ受信者又はデータ発信者によって本契約の違反があった旨の、最終的かつ上訴不可能な、データ発信者の設立国の管轄裁判所又は当局の決定がある場合、(ⅴ)管理又は解散に係る申立てがされ、適用法令に基づき当該申立てが有効期間中に棄却されなかった場合、解散命令がなされた場合、ある資産について管財人が指名された場合、データ受信者が個人である場合において破産管財人が指名された場合、会社更生が開始された場合又はいかなる同様の法的事由が生じた場合には、データ発信者は、その他のデータ受信者に対して有する権利に影響することなく、本契約を解除することができる。当局の要請がある場合にはこれを通知する。(ⅰ)、(ⅱ)又は(ⅳ)の場合には、データ受信者も本契約を解除することができる。

(c) いずれの当事者も、(ⅰ)データ受信者にデータが移転され処理される国(又は領域)について、欧州委員会により EU データ保護指令 25 条 6 項に基づく十分性を認める決定がされた場合、又は(ⅱ)当該国において EU データ保護指令が直接適用されるに至った場合には、本契約を解除することができる。

---

[31] 紛争は、事実解明及び当事者間における情報取得に基づき解決され得ることから、協力関係に関する定めは極めて重要な規定であると考えられている(Kuner Report p.4)。

[32] ビジネス団体側が、SET Ⅰの 5 条(c)項において監督機関の「助言」に従うものと規定されていることにつき、「助言」は口語であり法的概念でないため、データ保護機関の非公式な発言も含めて遵守しなければならないものと解され得るものとして、これに対して異議を述べた経緯があり、本契約では、最終的な「決定」に従うものと規定されている(Kuner Report p.4)。

(d) いついかなる状況及び理由により本契約が終了した場合においても(上記(c)項の場合を除く。)、移転データの処理に関する本契約に基づく義務及び/又は条件が免除されるものではない。

⑧ 契約の修正(7 条)

契約当事者は、添付書類 B の更新を除いて、本契約の条項を修正することはできない。商取引上の条項を追加することは妨げられない[33]。

⑨ 移転の説明(8 条)

移転及び個人データの詳細については、添付書類 B において特定する。添付書類 B は、法令の要請がある場合、規制若しくは政府に応える場合又は 1 条(e)項による場合を除き、第三者に開示してはならない企業機密情報を含む場合がある。契約当事者は、追加移転について追加の添付書類を締結することができ、必要に応じて当局にこれを提出する。そのほか、添付書類 B を複数の移転に適用されるよう作成する方法によることもできる。

4) SET Ⅰ及び SET Ⅱの相違点

SET Ⅰ及び SET Ⅱの規定内容は上記のとおりであり、両規定内容の主な相違点は、以下のとおりと考えられる。

① データ発信者及びデータ受信者の責任について

SET Ⅰにおいては、6 条 1 項及び 2 項により、データ主体は、データ発信者及びデータ受信者の一方又は双方から補償を受けることができ、データ発信者及びデータ受信者は、データ主体に対し連帯責任を負うものとされている。そして、データ発信者及びデータ受信者においては、双方ともに責任がないことを立証しない限り、データ主体に対する責任を免れることはできないものとされている。

これに対し、SET Ⅱにおいては、1 条(b)項により、データ発信者には、データ受信者が本契約に基づく義務の履行をする能力を有することにつき合理的努力をもって判断する義務(デューデリジェンス義務)があるものとされており、また、2 条(f)項により、データ受信者においても、データ発信者の要請に基づき、本契約に基づく責任を履行するために十分な財源の証明を提供する義務があるものとされている。そして、3 条により、データ発信者は、データ受信者の行為に係る責任について、連帯責任を負うものではなく、上記デューデリジェンス義務を怠った場合にのみ責任を負うものとされており、デューデリジェンス義務を尽くしている限りはデータ主体に対して責任を負

[33] ビジネス団体側は、いかなる修正も認められないとすることは柔軟性に欠け、現実的ではないものと考えており、本規定では、データ処理に係る状況の変化に応じて添付書類 B を更新することが許容された(Kuner Report p.5)。

わないこととなる。

したがって、データ発信者の観点から考えると、個人データ移転の取引を行う企業にとっては、デューデリジェンス義務を果たしている限りでデータ受信者の行為に係る責任を免れることができるSET Ⅱを利用する方が有利であると考えられる。これは、データ受信者に責任がある限り、データ発信者において責任を免れることができないものとされているSET Ⅰを利用した場合と比して、大きな違いが生じる点であると考えられる。

また、データ受信者の観点から考えても、SET Ⅱにおいては、データ受信者の行為に係る責任につき、第一次的にはデータ受信者がデータ主体から直接請求を受けるのではなく、データ主体がデータ発信者に対してデータ受信者に対する権利を適切に行使するよう要求することとされていることから、データ受信者においてデータ主体から直接責任を追及される前に一定期間違反を是正する機会が与えられているものと考えることもできる。

さらに、データ主体の観点からも、データ発信者及びデータ受信者に対して上記のようなデューデリジェンスに係る義務が課されていることにより、データ受信者に対する補償請求権の実効性の確保が一定程度担保されており、SET Ⅰと比してデータ主体の保護が劣るものではないと評価することが可能である。

② データ主体のアクセス権について

SET Ⅰにおいては、添付書類2の5項により、データ主体による関連データへのアクセス権は何ら制限されていない。

これに対し、SET Ⅱにおいては、添付書類Aの5項により、不合理な間隔や数により明らかに悪用して、反復して若しくは計画的にアクセスに係る要求がされた場合、又はデータ発信者の国の法令によりアクセスを与える必要がないものとされている場合には、データ受信者は、データ主体によるデータのアクセスを拒絶できるものとされている。また、1 条(e)項により、本契約に機密情報が含まれる場合には、データ発信者のデータ主体に対するコピー提供に係る義務が制限され、機密情報を削除する措置を採ることが許容されている。

したがって、SET Ⅱは、データ主体の正当な権利を害することなく、データ主体にアクセス権を認める必要がない又は認めることにより他の不利益が生じるような一定の場合には、データ主体のアクセス権を制限し、データ発信者及びデータ受信者の義務に係る負担を軽減する内容となっていると考えることができる。

③ 質問に対する対応について

SET Ⅰにおいては、4条(d)項により、データ発信者には、データ主体又はデータ保護機関からのデータ処理に関する質問につき回答する義務があるものとされている。

これに対し、SET Ⅱにおいては、1条(d)項及び2条(e)項により、データ発信者及びデータ受信者の合意により、上記質問に対する回答義務につき、一定の場合を除いてデータ受信者のみに負わせることを認めている。この点、データ保護機関からの質問につきデータ受信者においても対応できるようにされていることで、データ発信者及びデータ受信者においてデータ処理の実態に応じて柔軟に対応できるようになっているものと考えられる。

④　地域法令の遵守に関する保証について

SET Ⅰにおいては、5条(a)項により、データ受信者において、適用法令により契約に基づく履行が妨げられると信じる理由はないことを保証しなければならないものとされている。

これに対し、SET Ⅱにおいては、2条(c)項により、上記の義務につき、当該データ受信者が本契約を締結する時点において知る限りにおいて保証することで足り、また、保証の対象が、本契約の遵守につき実質的に反する効果を有することとなる法令がないと信じる理由はないことに制限されている。

これは、SET Ⅰを利用した場合には、データ受信者においてすべての適用法令につき契約に基づく履行を妨げるものではないことを確認する必要があり負担が大きいのに対し、SET Ⅱでは、上記保証の対象が合理的に制限されたものと考えることができる。

⑤　データ受信者に対する監査について

SET Ⅰにおいては、5条(d)項により、データ受信者は、データ発信者の要請に基づき、データ発信者又は監査機関による監査に付するため、データ処理設備を提供しなければならないが、この監査機関は、データ発信者とデータ保護機関の合意により選出される必要があるとされている。

これに対し、SET Ⅱにおいては、2条(g)項により、監査機関の選出に限らず、監査に関するデータ発信者の要請についてデータ保護機関の同意又は承認に付されることとされる一方、データ発信者の要請は合理的なものでなければならないこと、監査機関による監査につきデータ受信者は合理的な異議を述べる権利を有すること、監査手続や監査対象の範囲等につき一定の条件等が付されていること等が規定されており、データ受信者が監査に付される場合につき合理的な範囲に制限がされたものといえる。

⑥　データ保護機関との協力について

SET Ⅰにおいては、5条(c)項により、データ受信者は、移転データの処理に関してデータ保護機関の「助言」に従わなければならないものと規定されているが、ここにいう「助言」の範囲が不明確であるとの批判がされていたところである。

これに対し、SET Ⅱにおいては、5 条(c)項により、各当事者は、管轄裁判所又はデータ保護機関の最終かつ上訴不可能な「決定」に従わなければならないものとされており、契約当事者として従うべき内容が明確になったものと考えることができる。

⑦ 契約の終了について

SET Ⅰにおいては、契約終了について、9 条より、契約終了後の契約当事者の義務等の残存について規定しているのみである。

これに対し、SET Ⅱにおいては、6 条により、データ移転の一時停止及び契約の解除事由について詳細に規定しており、契約違反が生じ契約が終了するか否か不安定な状態でのデータ移転の継続による不都合を回避し、契約が終了する場面を明確化している。

⑧ 契約の修正について

SET Ⅰにおいては、11 条により、本契約の条項の修正変更を禁じるものと規定されている。

これに対し、SET Ⅱにおいては、7 条により、本契約の条項の修正は原則として禁じられているものの、添付書類 B の内容の更新をすること、及び商取引上の規定を追加できることが明文にて規定されており、個別の事情に応じた柔軟な対応を許容している。

（３）処理者移転型モデル契約の内容

1）概要

上記のとおり、処理者移転型モデル契約は、EU 域内のデータ管理者から EU 域外のデータ処理者に対して個人データを移転する場合に適用されるモデル契約であり、管理者移転型モデル契約と異なり、個人データの委託処理の場合にも適用されるものである。

この点、個人データの移転先がデータ処理者であるかデータ管理者であるかの区別については、実務上必ずしも明確に区別できない実態もあるようであるが、基本的に、EU データ保護指令に定める定義に従い、データ管理者は、データの取扱いの目的や手段について決定を行うものであり、データ処理者は、データ管理者の指示に従い、単にデータ管理者に代わってデータ処理を行うものにすぎないものと考えられている[34]。

2010 年決定により採択された処理者移転型モデル契約は、データ処理に係る外部委託がグローバルに行われている現状に対応するため、具体的に下請処理に係る条項を規定し、下請処理を行う場合の一定の手続等について規定しており(下記 11 条参照。)、この点が従来の処理者移転型モデル契約との比較で最も大きな変更点である[35]。

2）モデル契約の規定内容

① 定義条項(1 条)

(a)「個人データ」、「特殊な分類のデータ」、「処理」、「管理者」、「処理者」、「データ主体」及び「監督当局」とは、EU データ保護指令におけるそれと同じ意味を有する。

(b)「データ発信者」とは、個人データを移転する管理者をいう。

(c)「データ受信者」とは、データ発信者の指示及び本契約に従ってデータ発信者に代わってデータ処理を行うことを意図して、データ発信者(データ管理者)からデータを受領するデータ処理者をいう。

(d)「下請処理者」とは、データ受信者又は他の下請処理者に従事し、データ発信者の指示、本契約及び下請契約に従ってデータ発信者に代わってデータ処理を行うことを意図して、これらの者から個人データを受領することにつき合意したデータ処理者をいう。

(e)「適用保護法令」とは、データ発信者が設立された EU 加盟国においてデータ管理者に適用される、個人の基本的な権利及び自由を保護する法律をいう。

---

[34] 29 条ワーキンググループが 2010 年 2 月 16 日付けで採択した"Opinion 1/2010 on the concepts of "controller" and "processor""(以下「Opinion」という。)においては、データ管理者及びデータ処理者の区別について一定の考察がされている。具体的に、データ管理者については、データ処理の「目的」を決定する者こそがデータ管理者に該当するものであり、データ処理の「手段」については、データ処理の適法性の本質部分に係る内容の決定がデータ管理者に留保されていればよいものであり(Opinion p.15)、また、データ処理者については、データ管理者と別法人であること及びデータ管理者に代わって個人データの処理を行うことが基本的な条件である(Opinion p.25)等が記載されている。

[35] Wim Nauwelaerts, *European Commission Updates Model Clauses for International Data Transfers*, Hogan & Hartson(2010)参照。

(f) 「技術的及び組織的な保護対策」とは、不測の又は違法な破壊、不測の滅失、変更、無断の開示又はアクセス等から個人データを保護することを目的とした対策をいう。

② データ移転に係る説明(2 条)

データ移転の詳細、特に個人データの特殊な分類について、添付書類 1[36]において特定する。

③ 第三受益者条項(3 条)

1. データ主体は、データ発信者に対して、本条、4 条(b)項ないし(i)項、5 条(a)項ないし(e)項及び(g)項ないし(j)項、6 条 1 項及び 2 項、7 条、8 条 2 項並びに 9 条ないし 12 条について第三受益者の権利として執行できる。

2. データ主体は、データ発信者が事実上又は法律上消滅した場合(承継者がデータ発信者の義務を負うこととなり、データ主体が当該承継者に対して執行できる場合を除く。)には、データ受信者に対して、本条、5 条(a)項ないし(e)項及び(g)項、6 条、7 条、8 条 2 項並びに 9 条ないし 12 条について第三受益者の権利として執行できる。

3. データ主体は、データ発信者及びデータ受信者が事実上又は法律上消滅した場合(承継者がデータ発信者又はデータ受信者の義務を負うこととなり、データ主体が当該承継者に対して執行できる場合を除く。)には、下請処理者に対して、本条、5 条(a)項ないし(e)項及び(g)項、6 条、7 条、8 条 2 項並びに 9 条ないし 12 条について第三受益者の権利として執行できる。当該下請処理者の責任は、本契約に基づく自己の処理手続の範囲に制限される。

4. 契約当事者は、データ主体が他の者により代理されることにつき異議を述べない。

④ データ発信者の義務(4 条)

(a) 個人データの移転を含む処理は、データ発信者の設立国の適用データ保護法令に従って行う。

(b) 個人データの処理業務を行う期間において、データ受信者に対し、移転された個人データにつき、データ発信者のみのために、適用データ保護法令及び本契約に従って処理を行うよう指示を行う。

(c) データ受信者が、添付書類 2 において特定される技術上及び組織上の保護対策に関して十分な保証を与えることを保証する。

(d) 適用データ保護法令の要求の評価の後において、不測の又は違法な破壊、不測の滅失、変更、無断の開示又はアクセス等から個人データを保護すべく、データ処理及びデータの性質に基づくリスクに対して適切なレベルの、技術的及び組織的な保護対

[36] 添付書類 1 には、データ発信者、データ受信者、データ主体、データの分類、特殊な分類のデータ及び処理手続を特定して記載しなければならない。

策を採る。
(e) 保護対策の遵守を確保することを保証する。
(f) 特殊な分類のデータに関わる移転を行う場合には、十分な保護が提供されない第三国へのデータ移転につき事前にデータ主体に対して通知する。
(g) データ発信者が移転を継続し又は移転中止を止める場合、5 条(b)項及び 8 条 3 項に従ってデータ受信者又は下請処理者から受領した通知をデータ保護機関に転送する。
(h) データ主体に対し、その要請に応じ、添付書類 2 を除く本契約及び保護対策の概要のコピー並びに下請処理業務に係る契約のコピーを認める。ただし、当該契約に商業情報が含まれる場合には、当該情報を削除することができる。
(i) 下請処理について、下請処理者により、本契約におけるデータ受信者と同じレベルにおける個人データの保護及びデータ主体の権利を確保した上、11 条に従って処理が行われることを保証する。

⑤ データ受信者の義務(5 条)
(a) データ発信者に代わってのみ、データ発信者の指示及び本契約に従って、個人データの処理を行う。これらに従うことができない場合には、直ちにデータ発信者に対して通知するものとし、このとき、データ発信者はデータ移転を延期し、及び/又は契約を解除することができる。
(b) データ発信者の指示及び本契約に基づく履行が妨げられると信じる理由はないことを保証し、また、本契約に基づく保証及び義務に実質的に反する可能性のある法令の変更がある場合には、データ発信者に対して当該変更を直ちに通知する。このとき、データ発信者はデータ移転を延期し、及び/又は契約を解除することができる。
(c) 個人データの処理を行う前に、添付書類 2 において特定される技術上及び組織上の保護対策を講じたことを保証する。
(d) (ⅰ)法執行機関により個人データの開示につき法的拘束力のある要求をされた場合(通知が禁じられる場合は除く。)、(ⅱ)不測の又は無断のアクセスがあった場合、及び(ⅲ)データ主体から直接要請を受け、これに応答していない場合(権限を有する場合は除く。)には、データ発信者にその旨直ちに通知する。
(e) データ発信者からの個人データの処理に関するすべての質問について、速やかにかつ適切に対応し、また、移転データの処理に関する監督機関の助言に従う。
(f) データ発信者の要請に基づき、データ発信者による、又は監督機関との合意に基づきデータ発信者により選出された、独立性を有し、専門資格を有するメンバーで構成された監査機関による監査に付するため、データ処理設備を提供する。
(g) データ主体に対し、データ主体がデータ発信者からコピーを取得することができなかった場合には、保護対策の概要をもって代えられることとなる添付書類2を除き、本契約又は下請処理業務に係る契約のコピーを認める。ただし、当該契約に商業情報

が含まれる場合には、当該情報を削除することができる。

(h) 下請処理について、データ発信者に事前に通知し、書面による同意を得たことを保証する。

(i) 下請処理者による処理業務が 11 条に従って行われることを保証する。

(j) データ発信者に対し、本契約に基づき締結された下請処理に係る契約のコピーを直ちに送付する。

⑥ 責任(6 条)

1. データ主体は、契約当事者又は下請処理者の 3 条又は 11 条に定める条項の違反により損害が発生した場合には、当該損害につきデータ発信者から補償を受ける権利を有する。

2. データ主体が、データ発信者が事実上若しくは法律上消滅した場合又は倒産したことにより、データ発信者に対してデータ受信者又は下請処理者の 3 条又は 11 条に定める条項の違反につき第 1 項に基づく補償の請求ができない場合には、データ受信者は、承継者がデータ発信者の義務を負うこととなりデータ主体が当該承継者に対して執行できる場合を除き、データ主体がデータ受信者に対して請求を行うことができることにつき合意する。

データ受信者は、下請処理者の違反であることにより自己の責任を免れることはできない。

3. データ主体が、データ発信者及びデータ受信者が事実上若しくは法律上消滅した場合又は倒産したことにより、データ発信者及びデータ受信者に対して下請処理者の 3 条又は 11 条に定める条項の違反につき補償の請求ができない場合には、下請処理者は、承継者がデータ発信者又はデータ受信者の義務を負うこととなりデータ主体が当該承継者に対して執行できる場合を除き、データ主体が下請処理者に対して本契約に基づく下請処理者の処理の範囲において請求を行うことができることにつき合意する。当該下請処理者の責任は、本契約に基づく自己の処理手続の範囲に制限される。

⑦ 調停又は裁判管轄(7 条)

1. データ受信者は、データ主体が本契約に基づく損害につき第三受益者の権利を主張及び/又は補償請求を行った場合には、データ主体の選択により、調停又はデータ発信者が設立された EU 加盟国における裁判に付されることに合意する。

2. 上記選択は、データ主体が国の又は国際的な法令に従って救済を求めることを妨げるものではない。

⑧　監督機関との協力(8 条)

1.　監督機関又は国の法令の要請がある場合、データ発信者は監督機関に対して本契約のコピーを提出する。

2.　監督機関は、適用保護法令に基づきデータ発信者に対して行われる監査と同じ範囲及び条件において、データ受信者及び下請処理者に対して監査を行う権利を有する。

3.　データ受信者は、データ発信者に適用される法律の存在、データ受信者の監査を妨げる下請処理者の存在、及び 2 項の下請処理者につき、直ちにデータ発信者に対して通知する。このとき、データ発信者は、5 条(b)項における対策を採る権利を有する。

⑨　準拠法(9 条)

データ発信者が設立された EU 加盟国の法に準拠する。

⑩　契約の修正(10 条)

契約当事者は、本契約の条項を修正することはできない。本契約に反しない限り、商取引上の条項を追加することは妨げられない。

⑪　委託(11 条)

1.　データ受信者は、データ発信者の書面による同意がない限り、本契約に基づきデータ発信者に代わって行う処理につき、下請に出してはならない。本契約に基づく義務につき、データ発信者の同意に基づきデータ受信者が下請に出す場合には、データ受信者が本契約に基づき負っている義務と同じ義務を下請処理者に対して課すものとし、下請処理者との書面による契約によらなければならない。データ受信者は、下請処理者の当該契約に係る違反につき、データ発信者に対して責任を負う。

2.　データ主体が、データ発信者及びデータ受信者が事実上若しくは法律上消滅した場合又は倒産し、データ発信者又はデータ受信者の義務を負う承継者がいないことにより、データ発信者及びデータ受信者に対して 6 条 1 項に基づく補償の請求ができない場合のために、データ受信者と下請処理者との間の書面による契約には、3 条と同様に第三受益者の権利について規定する。

3.　1 項に基づく契約における下請処理に係るデータ保護の側面に関する規定は、データ発信者が設立された EU 加盟国の法に準拠する。

4.　データ発信者は、本契約に基づき締結され、データ受信者より 5 条(j)項に基づく通知を受けた下請処理契約のリストを保管し、少なくとも年1回更新するものとする。当該リストは、データ発信者の国のデータ保護機関が入手できるものとしなければならない。

⑫　個人データ処理業務の終了後の義務(12 条)

1.　データ処理義務の規定につき終了した場合、データ受信者及び下請処理者は、データ発信者の選択により、すべての個人データ及びそのコピーをデータ発信者に返還し、又は個人データを破棄の上当該破棄を証明する。ただし、データ受信者に適用される法律により当該返還又は破棄が妨げられる場合は除くものとし、このとき、データ受信者は、個人データの機密保持及び処理を行わないことを保証しなければならない。

2.　データ受信者及び下請処理者は、データ発信者及び/又は監督機関の要請により、1 項に基づく方法の監査のため、データ処理設備を提供する。

（４）モデル契約の運用について

1）管轄当局によるモデル契約の承認

契約当事者において、モデル契約及びデータ主体の基本的な権利及び自由と直接又は間接に矛盾しない範囲において、他の条項を加えて、契約を締結することは自由である。ただし、モデル契約における条項自体を修正することは認められておらず、また、追加条項については第三受益者の権利に含まれないため、データ主体はこれを執行できないこととなる[37]。

上記モデル契約は、モデル条項ではあるが、データ発信者が属する国のデータ保護法令の規制内容によっては、個人データ移転の取引を行う企業間でモデル契約を用いて契約を締結する場合及びこれに基づき個人データ移転の取引を行う場合において、管轄当局の承認が必要な場合もある。管轄当局の承認が必要かどうかは、データ発信者を管轄する国の法律の規定内容に従うこととなる[38]。

2）モデル契約に係る管轄当局の監督

モデル契約の運用に当たっては、管轄当局において、個人データ保護のため、データ移転を禁止又は停止する権限が与えられている。

具体的に、管理者移転型モデル契約の SET Ⅰ又は処理者移転型モデル契約が利用された場合には、以下の場合に、上記権限を行使できるものとされている。

① モデル契約に基づく保証に実質的に反する可能性があり、EU データ保護指令 13 条に定める民主社会に必要な規制を超える関連データ保護規制における権利を損なうこととなる、データ受信者に適用される法令が定められた場合
② 管轄当局が、データ受信者につき契約条項を遵守していないとの確証を得た場合
③ モデル契約が遵守されておらず、あるいはされる見込みがなく、継続的なデータ移転がデータ主体に対して切迫した重大な損害を与える実質的可能性がある場合

また、管理者移転型モデル契約の SET Ⅱが利用された場合には、当該規定内容に柔軟性が付与されたことによる悪用を禁止するため、データ保護機関によるデータ移転の禁止又は停止の権限をより容易に行使できるようにすることが適切であるとされており、上記の場合に加え、以下の場合にも、上記権限を行使できるものとされている[39]。

④ データ受信者が、管轄データ保護機関に誠実に協力すること(例えば、監査についての協力。）又は契約上の義務の遵守をすることにつき拒絶した場合
⑤ データ発信者が、管轄データ保護機関によりデータ受信者の契約履行が必要であることにつき通知を受けたにもかかわらず、1 か月のうちにデータ受信者に対して当該契約

[37] 2005 年 FAQ 参照。
[38] 例えば、オランダにおいては、管轄当局による承認が必要であるが、イギリスにおいては、管轄当局による承認は不要とされているようである。
[39] 2004 年決定の Whereas 条項(7)参照。

履行を強制させるよう適切な措置を講じることにつき拒絶した場合

（５）日本企業にとってのモデル契約と Binding Corporate Rules との比較

1）(管理者移転型)モデル契約の比較優位

現状、EU 全体において、日本企業に限らず BCR(以下に定義する。）を利用している企業は、限られているのが実態のようであり[40]、個人データ移転の取引を行うほとんどの企業においては、モデル契約が利用されているようである。なお、管理者移転型モデル契約を利用する場合には、上記（２）の 4)記載のとおり、SET Ⅱを利用することが企業にとって有利であり利用しやすいものと考えられ、実際に、SET Ⅱが導入された 2004 年以降は、SET Ⅱが利用されるケースが多いのではないかと推測される。

本報告は、BCR がグローバルに展開する日本企業にとっていかなる利用価値があるのかについて検討することが目的である。そこで、いかなる理由でモデル契約の方が BCR よりも優れている面があるのかについて、検討結果を以下に述べる。

2）前提としての Binding Corporate Rules の概要

①　BCR の概要

2003 年、第 29 条ワーキンググループは、原則として「国際的なデータ移転に係る拘束力のある企業ルール」(binding corporate rules for international transfers)[41](以下「BCR」という。）の使用を承認する旨の文書を公表した。

BCR によることが実務上最も想定されるのは、企業グループ内で個人データの国際的移転を行う多国籍企業であり、このような統一ルールを定めることで従業員等が容易にこれを実施し、データ対象者にとっても理解しやすい、シンプルかつ実効的なシステムとすることができるとされている[42]。

BCR の詳細な概要については本報告の他の章に譲る。

②　BCR を利用する場合における長所及び短所

(a)　長所について

BCR を利用する場合には、企業グループ内の個人データの移転につき、新しいデータ移転の度に契約を締結(及び状況把握)等して対応する必要がなく、一つのルールにて全グループ企業を拘束することができることから、EU 域外に存する多数の企業に対して個人データ

---

[40] 例えば、2010 年 2 月 26 日時点で、イギリスのデータ保護機関(Information Commissioner's Office)により BCR の承認を受けた企業は、General Electric Company、Koninklijke Phillips Electronics NV、Atmel Corporation、Accenture Limited、Hyatt Hotels Corporation、JPMorgan Chase & Co 及び British Petroleum p.l.c の 7 企業に限られる(ICO"Biniding Corporate Rules Authorisation"(Mar. 31, 2010))。

[41] 「国際的なデータ移転に係る法的執行力のある企業ルール(legally enforceable corporate rules for international transfers)」ともいう("Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers"(2003 年 6 月 3 日採択、WP74)p.8 参照)。

[42] "Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules"(2008 年 6 月 24 日採択、2009 年 4 月 8 日改訂)1 参照。

の移転を行う企業においては、時間の消費及び費用の支出を減少させることができる。また、法的拘束性を持たせるルールの規定方法は多様にあると考えられるところ、企業グループの事業活動の特性等に応じた柔軟なルールの策定が可能となる。

また、BCR においては、ルールの遵守の確保につき、データ保護機関による監査やデータ主体による苦情といった制裁措置に対する脅威を通じてではなく、企業自身が負担することとされているため、例えばデータ保護機関による厳しい監査が行われているような国においては利用しやすい手段といえる。

また、BCR の利用は、企業文化として、データ主体のプライバシーを保護し、及びデータ保護規制を遵守することにつながる[43]。

(b) 短所について

まず、BCR を利用する場合には、原則としてデータ移転を想定している各国のデータ保護機関による承認が必要となるところ、当該承認に時間が掛かるだけでなく、25 のデータ保護機関それぞれの修正要求を受ける可能性もあり、そもそも BCR の利用に慎重なデータ保護機関もあることから、全データ保護機関の承認を得ることは困難であるという点が挙げられる[44]。

また、BCR は最低限のレベルにおける保護標準を定めるものにすぎないため、特定の地域の法令が BCR より規制的である場合には、データ主体は当該地域の法令に基づき請求を行うことができる。他方、BCR の方が特定の地域の法令より厚い保護を与えている場合には、データ主体は BCR に基づき請求を行うことができる。よって、BCR は、企業の潜在的責任を重くする方向に働く可能性があるといえる[45]。

さらに、BCR の規定方法についてはモデル条項が存在しないため[46]、上記のとおり柔軟

---

[43] ICC Task Force on Privacy and Protection of Personal Data, ICC report on binding corporate rules for international transfers of personal data (2004)(以下「ICC レポート」という。) p.11 参照。

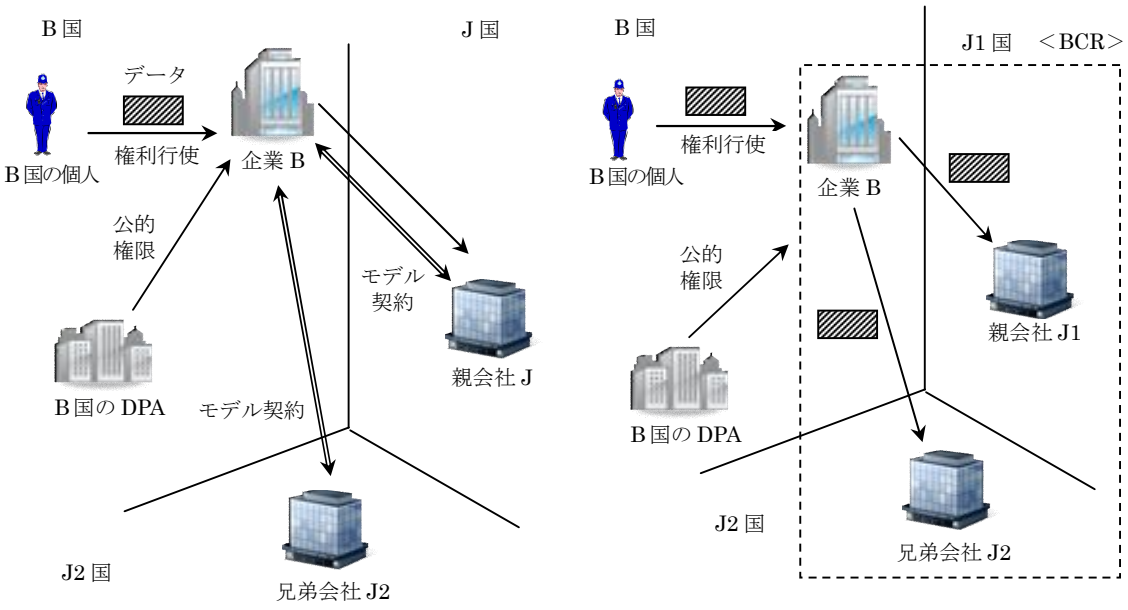
[44] なお、データ保護機関による承認手続につき、これを簡略化した手続として、相互承認(mutual recognition)による手続も用いられており、この手続によれば、主要機関により承認がなされた場合には、他のデータ保護機関も承認したものとみなされることとなる。
2009 年 2 月 25 日時点では、13 のデータ保護機関(フランス、ドイツ、アイルランド、イタリア、イギリス、オランダ、スペイン、ラトビア及びルクセンブルグは既に合意しており、EU 加盟国以外に、ノルウェイ、アイスランド、リヒテンシュタイン及びキプロスも参加している。) がこの手続によることに同意している(Heidi C. Salow & Micah R. Thorner, *Binding corporate rules now a more attractive option for Europe-to-US data transfe*r, DLA PIPER E-COMMERCE AND PRIVACY ALERT, (Feb. 25, 2009), http://www.dlapiper.com/binding_corporate_rules_now_a_more_attractive_option_for_europe-to-us_data_transfer/)。また、2009 年 9 月 25 日時点では、17 のデータ保護機関がこの手続によることに同意しているとされ、イギリスのデータ保護機関(Information Commissioner's Office)は、同年 9 月 15 日付け Hyatt Hotels Corporation の BCR 承認について、初めて相互承認の方法により承認を行った(HUNTON & WILLIAMS LLP, *UK Regulator Approves Hyatt Hotel BCR -First Approval under Mutual Recognition Procedure*, Privacy and Information Security Law Blog,(Sep. 25, 2009), http://www.huntonprivacyblog.com/2009/09/articles/european-union-1/uk-regulator-approves-hyatt-hotels-bcr-first-approval-under-the-mutual-recognition-procedure/)。

[45] ICC レポート p.12 参照。

[46] "Working Document setting up a framework for the structure of Binding Corporate Rules"(2008 年 6

なルール策定が可能となる反面、どのような内容にて規定した場合にデータ保護機関の承認が得られるのかが不確実であるという問題がある[47]。

モデル契約条項型　　BCR 型



3）モデル契約の現実的利便性

データ保護機関による承認を得た BCR は、当該 BCR に係る企業グループ内のいずれの会社に対しても一括して個人データを移転することができることとなり、当該企業グループ内の個人データの移転については当該 BCR のみで対応できることとなる。

これに対し、モデル契約を利用して個人データを移転する場合には、当該個人データ移転の取引の相手方たるデータ受信者一社ずつと個別に契約を締結しなければならないこととなることから、当該契約締結手続が煩雑になることも考えられる。

この点、モデル契約は、そのまま締結することが可能な形となっているため、当該モデル契約のとおりに規定をすれば問題が生じない建て付けとなっている。そのため、モデル契約自体の作成は難しくないといえ、モデル契約の条項に対して追加修正を行うことなくモデル契約のままで締結する限りは、データ保護機関による承認が必要な場合には、これ

月 24 日採択)においては、BCR の枠組みが示されているものの、企業の構造に応じて作成されなければならず、当該枠組みどおり作成したとしてもデータ保護機関による承認が得られるものではない旨記載されている。

[47] ICC レポートにおいては、EU 加盟国各国の企業及び法律事務所を対象に、法的拘束性が認められるための様々な方法及び各国において当該方法が法的拘束性を有すると認められるか否かについて調査しており、その結果、企業グループにおける拘束力、従業員に対する拘束力及び請負人に対する拘束力それぞれにつき、国によって法的拘束性が認められるか否かの結論が異なることを示している。

が得られるものとして予測可能性を確保することができるものと考えられる。そして、データ移転を行う企業において、モデル契約に基づいた運用で何らの不便も生じないといえる。

これに対して、BCR を利用する場合には、企業グループ及び構造の複雑性及び多様性並びに処理の目的にかんがみて、モデル条項はなく、企業の特性に応じた内容として独自に作成する必要がある。このことから、当該企業グループにおいて柔軟なルール設計ができる一方で、当該ルール設計に一定の労力及び費用を要することとなる。また、BCR の場合には、企業グループにおいて一つのルールで対応することから、申請時の一回のリーガルチェックで足りるようにも思われるが、BCR を変更する場合にはデータ保護機関に対する報告義務を負うことから、結局変更の際には改めてリーガルチェックが必要ということになり、リーガルコストの面で負担を軽減できるとは限らないこととなる。さらに、データ保護機関による承認を得ることができるのか不確実であるという問題も残る。

なお、そもそも、EU 域内に拠点を有する日本企業において、国境を越えて移転する必要がある個人データがどの程度あるのかという点についても考える必要がある。現実論としては、ある程度限られた業種においてのみ、BCR が念頭に置いている枠組みでのデータ移転が必要となるにすぎないのではないかと推察される。

4）責任構造の観点からのモデル契約の優位性

データ受信者の行為による BCR 又はモデル契約の違反に基づきデータ主体に損害が生じた場合における責任構造につき、以下の重要な相違点が認められる。

BCR においては、企業グループ内において、EU 域内の本社又はデータ保護責任を委譲された EU 域内のメンバーは EU 域外のメンバーの行為に係る責任を負うものとされており、データ発信者及びデータ受信者ともに責任がないことを立証しない限り、データ主体に対して責任を負うものとされている。なお、理論的には、データ受信者も、データ受信者に帰責性のある損害についてはデータ主体に対して責任を負うこととなるが、BCR は、データ主体が EU 域内の一定の企業に対して責任追及することを可能にしたものであり、また、上記の EU 域内において責任を負う企業は一定の資産を有するものと考えられること[48]、及び地理的な問題等も考慮すると、データ主体が EU 域外のデータ受信者に対して責任追及をすることは、現実的には余りないものと考えられる。

管理者移転型モデル契約においては、上記（２）の 4)①記載のとおり、SET Ⅰを利用した場合は、データ発信者及びデータ受信者は、データ主体に対して連帯責任を負うものとされており、データ受信者の行為に係る責任について、データ発信者において、データ発信者及びデータ受信者ともに責任がないことを立証しない限り、データ主体に対して責任

[48] BCR の申請時に、EU 域内において責任を負うものとされるメンバーについては、BCR 違反に基づく損害を賠償するに足りる十分な資産を有することを裏付ける資料を提出しなければならないものとされている("Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules"(2008 年 6 月 24 日採択、WP153)(以下「WP153」という。）§1.5 参照。

を負うこととなる点においては、BCR と同様であると考えられるのに対し、SET Ⅱを利用した場合には、データ発信者は、データ受信者の行為に係る責任について、デューデリジェンス義務を怠った場合にのみ責任を負うものとされている。

以上より、データ発信者及びデータ受信者のいずれの観点からも、個人データ移転の取引を行う企業にとって最もメリットがある方法は、デューデリジェンス義務を果たしている限りでデータ受信者の行為に係る責任を免れることができる、管理者移転型モデル契約の SETⅡではないかと考えられる。データ受信者に責任がある限り、BCR を利用した場合は EU 域内において責任を負う企業において、また SET Ⅰを利用した場合はデータ発信者において、責任を免れることができないものとされていることと比して、大きな違いが生じる点であると考えられる。

5）データ受信者の存する国の法制度の調査

BCR では、申請書類において、法的拘束力の根拠としての他の regulatory measures についての記載をすること[49]が必要とされたり、BCR において、データ受信者の国のデータ保護法制が BCR と矛盾する等 BCR 遵守が妨げられるような法令がある場合の対応に関する規定を入れること[50]等が必要となることがあり得る。その結果、事実上、データ受信者の国のデータ保護法制を一定程度調査する必要があることになる。

これに対し、モデル契約を利用する場合には、当事者間の権利義務等は、当事者間の合意内容に律せられることとなるから、データ受信者の国の法律を調べずにこれを締結することも可能である。なお、データ発信者において、モデル契約の締結時に、準拠法をデータ発信者の国の法律とすることがデータ受信者の国において認められるか及びモデル契約に基づく執行が可能かどうか等につき調査を行うことは考えられる。

よって、法制度の調査が一定程度必要とされる BCR の場合には、調査に係る負担が大きくなることが考えられる。ただし、いずれの場合であっても、各国のデータ保護法制のレベルが十分といえるかによって、BCR 及びモデル契約の有効性等につき結論が変わるものではないと考えられる。

6）統一ルールの作成の必要性

BCR については、企業グループ内の統一ルールの作成により、個人データ移転につき一括して対応できる点に、最も大きな意義があると考えられている。

しかし、BCR を利用した場合には、データ発信者は、データ受信者に係る違反行為について、データ発信者の国の規範に従ってサンクションを受けることとなることから、データ発信者としては、データ受信者が相当程度信頼の置ける企業でない限り、BCR における企業グループの一員とはしないのではないかと考えられる。そうであれば、そのような信

[49] “Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data”(2007 年 1 月 10 日採択、WP133）§4.参照。
[50] WP153 §6.3 参照。

頼を置ける企業との間では、個別にモデル契約を締結することも可能であるように考えられ、個人データの移転先の企業が多数存在する場合におけるモデル契約の締結の煩雑さを避けることを除いて、あえて統一ルールを作成するメリットがどの程度あるのかは明確ではないと考えられる。

7）まとめ

以上のとおり、管理者移転型モデル契約の SET Ⅱを利用することで特段の不便は認められず、BCR の導入に向けた制度対応を、日本が国として検討する必要がある状況にあるとは認められないと思料する。

Ⅲ　「個人データの処理に係るプライバシー保護の国際標準草案のための共同提案」について

Ⅲ　「個人データの処理に係るプライバシー保護の国際標準草案のための共同提案」について

筑波大学法科大学院教授　　藤原　靜雄

１．第三国への個人データの移転の問題の概要

（１）出発点としての EU 指令

①　1995 年の EU のデータ保護指令（以下、「EU 指令」と略す）の目的は、できる限り高いレベルの統一的な個人情報保護の制度の構築を通じて、EU 域内及びヨーロッパ経済圏（すなわち、構成国にアイスランド、リヒテンシュタイン、ノルウェイが加わる）における自由なデータ流通を一層促進しようというものであった。と同時に、EU 指令は、対外的な側面も併せ持つ。それを規定しているのが、第三国への個人データの移転に係る 25 条及び 26 条である[1]。

---

[1] 25 条及び 26 条の重要な部分のみ、抜き出しておけば、
25 条 1 項　加盟国は、処理の対象となる、又は後に処理される予定の個人データの第三国への提供は、この指令に基づき制定された各国の国内規定を守られるという条件の下、当該第三国が十分なレベルの保護を保証している場合には許されることを、定める。
　2 項：第三国によって提供される保護レベルの十分性は、データ移転あるいはデータの類型的移転におけるすべての事情を考慮して判定される。特にデータの性質、計画された処理作業の目的及び期間、データの移転元の国及び最終目的国、当該第三国で効力を有する一般的な又は分野別の法律、並びに当該第三国で適用されている職業上の準則、及び安全管理措置が考慮に入れられる。
26 条 1 項　第 25 条の規定にかかわらず、一定の事案について国内法にこれに反対する趣旨の規定がない限り、加盟国は、第 25 条 2 項の意味における適切な保護レベルを確保していない第三国に対する個人データの移転及び類型的移転を、以下の場合には行なうことができる旨を定める。
（ａ）データの当事者が明確な同意を与える
（ｂ）移転がデータの当事者と管理者との間の契約の履行、又はデータの対象者の要請よる契約前の措置の実施のために必要である
（ｃ）移転がデータの対象者のために管理者と第三国との間で締結された又は締結される契約の締結又は履行のために必要である
（ｄ）移転が重要な公共の利益を守るため、又は法廷での法的請求の主張、行使若しくは防御のために必要であるか法律上規定されている
（ｅ）移転がデータの当事者の極めて重要な利益を保護するために必要である
（ｆ）移転が、法規定又は行政規則に従って国民への情報提供のために整えられておりかつ、国民又は正当な利益を証することができるすべての者が、個別の場合に閲覧のための法律上の要件を充たせば閲覧できる登録簿から移転が行われること。
2 項　管理者が、個人のプライバシー、基本権及び自由権の保護に関する保証、及びこれらと結びついた権利の行使に関する十分な保証を提供
する場合には、加盟国は、第 1 項の規定にかかわらず、第 25 条 2 の意味における十分な保護レベルを確保していない第三国に対する個人データの又は個人データの類型的移転を許可することができる。このような保証は、特に、適切な契約の条文によって設定することができる。

②第三国移転に関する EU 指令については以下の点が重要である。

第 1 に、第三国への移転の基本原則は、当該国に「十分なレベルのデータ保護のレベル」が存在することである。ここで注意すべきは、EU 指令は、意識的に、一致したレベルのとか同等のレベルのとは言っていないということである[2]。

第 2 に、個人情報保護のレベルの十分性の判断は、EU 委員会が定めた手続に則って行われるが、これまで、セーフハーバー協定によるアメリカ以外に適切とされた国は少ない。わずかに、スイス、カナダ、アルゼンチン、ガーンジー（Guernsey）[3]、マン島（Isle of Man）[4]、ジャージー（Jersey）、フェロー諸島（Faeroe Islands）のみである。オーストラリア[5]については審査が終了していないという形での不適となっている。

第 3 に、十分性の問題については、例外扱いがあり、ア）セーフハーバーという協定を採用する仕組み、イ）26 条を利用した標準契約を利用する仕組み、ウ）拘束的な企業準則という仕組みを事業者（あるいは事業者団体）が採用するという仕組みがある。

---

[2] Alexander Dix, Anja-Maria Gardain, Datenexport in Drittstaaten, DuD 2006, S.343.

[3] イギリス海峡チャネル諸島に位置するイギリス王室属領。

[4] アイリッシュ海の中央に位置するイギリス王室属領。

[5] 1988 年施行の「プライバシー法」の適用範囲を民間事業者にまで広げた「プライバシー修正法」を 2000 年に施行している。これにより、法形式はセクトラル方式からオムニバス方式へと改変されたが、（ⅰ）年商 300 万豪ドル未満の小規模事業者及び被雇用者のデータが規制対象外とされたこと、（ⅱ）一般に利用可能な個人データが規制対象外とされたこと、（ⅲ）データ取得時の本人への通知が困難な場合には、事後の通知でもよいとされたこと、（ⅳ）ダイレクト・マーケティングが主目的のデータ利用について、オプトアウトが認められていないこと、（ⅴ）センシティブ・データの規制が収集のみで、利用や開示については規制がないこと、（ⅵ）EU 市民の個人データについて、本人の訂正請求権が認められていないこと、（ⅶ）EU から取得した個人データをオーストラリアから第三国へ移転することが規制されていないこと等を理由に、保護水準の十分性を欠くとされた。なお、その後、オーストラリアでは、2004 年 4 月にプライバシー法の改正が（PrivacyAmendmentAct2004(Cth).）行われている。そこでは、（ⅰ）個人情報の訂正請求に関する苦情の申立てについて、プライバシー・コミッショナーの関与の範囲を拡大、（ⅱ）法の適用を受けない事業者についてもプライバシー・コードの策定を柔軟に行うことができる等の改正がなされている。さらに、2008 年 8 月には、オーストラリア法改革委員会（AustralIianLawReformCommission：ALRC）が、現行法によるプライバシー保護の有効性について調査を行い、報告書を公表している。

（２）例外的枠組みの概要

① EU はアメリカ合衆国（以下「アメリカ」という）との間で、長年にわたり「セーフハーバー」と呼ばれる交渉を重ねてきている[6]。しかし、この方式については、少なくともヨーロッパのデータ保護当局は、個人情報保護の観点からは、積極的に評価していない。

② 契約による例外

第三国移転に係る EU 指令の条文には、一連の例外条項が存在する。当初、この例外規定の存在が、我が国等、域外の第三国に、EU のデータ移転に関する態度は厳しいものではないのではないかという印象を与えたのも事実である。この点については、以下の点をコメントしておくこととしたい。

第 1 に、例外規定は、1990 年の最初の EU 指令提案にはなかったものであるが、関係当事者の働きかけがあり、議会の修正として 1992 年の修正案[7]で挿入されたものである。

第 2 に、この例外の解釈として、いわゆる 29 条グループ[8]が 2005 年に具体的な解釈ガイドラインを示している[9]。

第 3 に、契約による例外[10]は、ほぼ以下のような形で展開している。

まず、指令発行後間もなくの間は、法 26 条 1 項による例外が、実務に耐えうる唯一の手法と受け止められた[11]。この間、この契約方式による例外は、第三国所在の人事担当者への被用者データの提供[12]、関係国の通関当局への航空機関係データの提供、サーベンス・オッ

---

6 アメリカは、セクトラル方式で法整備を進めてきており、また、民間部門の自律（自主規制）を重んじるため、民間部門を規律する一般法は存在しない。したがって、法制による EU データ保護指令への準拠は難しい。そこで、特定の認証基準を設け、その認証を受けた企業ごとに適切性を付与する「セーフハーバー原則」のための交渉が 1998 年から始まり、2000 年に協定が締結されている。アメリカ企業がセーフハーバーに参加することは任意であるが、参加可能な企業は連邦取引委員会（FTC：Federal Trade Commission）及びアメリカ運輸省の管轄にある企業に限られており、連邦準備理事会（FRB）管轄の金融機関や、コモンキャリア、航空会社等は含まれていない。これまでの（例えば 2004 年）EU 委員会の監査においては問題点が多く指摘され、①原則遵守の意思表明の必要性、②連邦政府（商務省）の強力な指導とモニタリングの必要性、③違反者に対する強力な影響力の行使の必要性などが連邦政府に要請されており、EU の専門家の中には「十分性」に疑問を抱く者もいる。

7 Amended proposal for a COUNCIL DIRECTIVE,p4,34

8 EU 指令 29 条に基づき設置されるワーキンググループである。各国のデータ保護当局（監視機関）の代表等からなり、その権限は、（ａ）統一的な適用に資するように、この指令の国内法化に伴い発せられた各国の規定に関連するすべての問題を審査すること、（ｂ）共同体及び第三国の保護レベルに関して、委員会に意見を述べること、（ｃ）本指令修正のための提案、個人データの処理に係る自然人の権利及び自由を保護するための追加的又は個別の案、及びその他の共同体のすべての措置に関して、委員会に助言を与えること、（ｄ）共同体レベルで作成された行動規約に関して意見を述べること、である（第 30 条）。

9 「Standard contractual clauses for the transfer of personal data to third countries - Frequently asked questions」（「2005 年 FAQ」）, 2005 年 1 月 7 日がそれである。

10 契約による例外、とくにモデル契約による例外については、本報告書「3. モデル契約の概要」参照。

11 ドイツでは、アメリカにおける鉄道カード発行に関して、連邦鉄道とシティバンクの間で契約が交わされたのが著名である。

12 ただし、この点については、グローバル展開をしている企業の人事政策を調査する必要があろう。現在でも、大多数の事業者において、本社が第三国からの個人データを求めているかどうかは定かではない。

クスリー法（Sarbanes - Oxley act）[13]の枠内での通報のための提供を正当化するために利用されてきた。しかしながら、これらのすべての場合について、29 条グループは、契約の実現のための必要性という点に関し疑問を抱いているとされている。

次に、26 条 4 項に基づくモデル契約ないし標準契約と呼ばれる方式が重要な位置を占めるようになった。モデル契約として 2001 年様式[14]、2004 年様式[15]、2010 年様式[16]の 3 つがある。このうち、前 2 者は、EU 域内のデータ管理者から EU 域外のデータ管理者に対して個人データを移転する場合に適用されるモデル契約であり、最後のものは、EU 域内のデータ管理者から EU 域外のデータ処理者に対して個人データを移転する場合に適用されるモデル契約である（個人データの委託[外部委託]処理の場合にも適用される点が前 2 者とは異なる）。

2001 年様式が、当初 EU 委員会が「十分性」を有すると考えたものであるが、国際的な経済団体[17]から柔軟性を欠くとの批判を受けて、経済団体側の提案の条項を EU 委員会が受け入れたのが 2004 年モデルである。この点について、各国のデータ保護当局は、2004 年様式によって実務に大幅に歩みよったことは、EU 市民にとっては個人情報保護の水準の低下であると評している[18]。

③　拘束的企業準則

標準契約より遅く、EU 指令 26 条 2 項に基づく例外的措置として登場したのが、拘束的企業準則(Binding Corporate Rule, BCR)である。これは主に国際的に活動する企業集団[19]（多国籍企業）内部の個人データ移転を対象とするルールである。具体的には十分な保護レベルを確保するために、データ保護当局(Data Protection Authority, DPA)等により法的

---

[13]「Public Company Accounting Reform and Investor Protection Act of 2002：上場企業会計改革及び投資家保護法」が正式名称。周知のように、2006 年に J-SOX と呼ばれる我が国の金融証券取引法が制定される 1 つのきっかけになった。

[14]「COMMISSION DECISION of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC」（WP47）により定められている。

[15]「COMMISSION DECISION of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries」による。

[16]「COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council」による。

[17]　国際商業会議所(International Chamber of Commerce)の他、European Information and Communications Technology Industry Association(現在の DIGITALEUROPE)、Federation of European Direct and Interactive Marketing のような情報通信、ダイレクト・マーケティングの業界団体等である。なお、Japan Business Council in Europe(在欧日系ビジネス協議会)も入っている。

[18] 例えば、不適切なあるいは過剰な回数の開示請求を拒否できるという条項、データの被移転国は、契約締結時において、契約条項から生じる保障を「著しく」損なう法規定が自国に存在しないことのみを保証することのみ義務付けられるが、「著しい」か否かの実質的判断権は移転国にはない。これらは、2001 年モデルとの変更点である。

[19] 初期の個人情報保護法制はコンツェルンのことを考えていなかったというのが、ヨーロッパのデータ保護当局の関係者の一致した見解である（ドイツ連邦保護観察官事務所の担当者の発言）。

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、などに留意した「拘束的企業準則」を事業者が策定し、欧州域内のデータ保護当局が当該準則を承認した場合には、当該企業集団は、EU 域外の当該集団に属する企業に個人情報を提供できる、というものである。

ドイツの場合を見てみると、これまでに次のような例が紹介されている[20]。ア）ダイムラー・クライスラーによる 2 本の企業準則（2002 年 7 月、1 つは被用者データ、他の 1 本は顧客データ）、イ）ドイツ保険連合会によるモデル規約（加盟企業が自社で準則にする、2002 年 11 月）、ウ）GE(General Electric)の企業準則（2003 年 7 月、ドイツの 100 余の支社の被用者データを国大に移転する目的）、エ）ドイツテレコム（被用者データ及び顧客データ、2003 年 11 月）、オ）シェーリング（Schering）株式会社（被用者データ、顧客データ及び製薬研究から生じた個人データ、2005 年秋）等である。

イ）EU 指令 25 条に関するこの例外的措置において重要なのは、EU レベルの担当部局と各国のデータ保護当局相互間の協議である。そのために、29 条グループは、オーストリアとオランダの支援の下なされた提案（ベルリン提言）の下、2003 年 6 月に最初の事前協議手続のための解釈を（WP74）[21]、そして、2005 年 4 月には作業のための文書（WP107）[22]とチェックリスト（WP108）[23]を示している[24]。これらの監督機関同士の合意は、事業者にワンストップの手続を可能にすること、他方で、いわゆる forum shopping（法廷地あさり）を防ぐ意味合いもある。

ウ）BCR の申請

BCR の手続では申請の管轄が重要となるが、これは以下のような客観的な要素を考慮して決定される[25]。

a.グループの欧州本社の所在地

b.グループ内でデータ保護の責任をゆだねられた企業の所在地

c.グループ内で申請を処理し、BCR を執行するのに最も適した体制にある企業の所在地

d.処理の目的及び手段について、決定が下される場所

---

[20] Alexander Dix, Anja-Maria Gardain(Fn.2), S.344.

[21] 「第三国への個人データ移転：国際データ移転のための拘束的企業準則への EU データ保護指令第 26 条第(2)項の適用」(Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers、2003 年 6 月 3 日)

[22] 「『拘束的企業準則』から結果する十分な安全措置に関する共通意見提出のための協力手続を定める作業文書」(Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From “Binding Corporate Rules”、2005年4月14日)

[23] 「拘束的企業準則の承認申請のモデルチェックリストを定める作業文書」(Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules、2005 年 4 月 14 日)

[24] この他の WP については、12. Jahresbericht der Artikel 29 Datenschutzgruppe、2009 年 6 月 16 日）に説明がある。概要及び内容に関しては、WP74 及び WP108 が重要である。

[25] WP108, p3(Which data protection authority should you apply to?)

e.第三国への移転がもっとも多く実行される加盟国

以上のうち最も優先されるのは、グループの欧州本社の所在地である。しかし、管轄の決定権は EU の監督機関にあり、申請事業者の申請とは異なった決定となることもある。

また、個人データを移転する形となる国の監督機関は、EU 指令自体に基づいてデータ移転の許可の権限を有しているので、上記の協議手続に参加する義務はない。しかし、移転国も 5 つの企業集団（ダイムラー・クライスラー、KPMG,BP,GE,フィリップス）[26]については、試行的に任意に手続に参加している。

エ）BCR の手続

所管のデータ保護機関は、まず、当該事業者について、整理された文書を見る。これが終了し次第、データの移転が予定されているすべての参加国が意見を表明する。意見表明は 1 ヶ月以内に行われる。事業者がこの意見に応じることができれば、最終的な案を提出し、これが十分性を認証するものとなる。この手続は各国の合意の下に行われるので、1 つの国がデータ移転をデータ保護措置が十分でないという理由で拒否することはできない。

また、関係データ保護機関は、許可を国内法に基づく要請と結びつけることを留保しうる点も重要である。例えば、ドイツでは、データ移転の問題は 2 段階の審査に服することになる[27]。第 1 段階の審査として、連邦データ保護法 28 条[28]の枠内で処理の許容性が審査

---

[26] ちなみに、EU レベルでの申請を管轄するデータ保護当局は、ダイムラー・クライスラーがフランス（CNIL）、フィリップスと LPMG はオランダ、BP と GE はイギリスである。

[27] Tinnefeld/Ehmann/Gerrling, Einfuehrung in das Datenschutzrecht 4Aufl. S346ff.

[28] 第 28 条　自己の目的のためのデータ収集､処理及び利用

（1）自己の業務目的の遂行のための手段として、個人データを収集、蓄積、変更若しくは提供し、又はそれを利用することは、以下の各号に掲げる場合に許される。

1　それが本人との契約関係若しくは契約類似の信頼関係の目的に資する場合

2　責任機関の正当な利益を守るために必要で､かつ処理若しくは利用させないことについての本人の保護に値する利益が優越すると推定させる理由が存在しない場合

3　データが一般にアクセス可能であるか、又は責任機関がそれを公表することが許されている場合、ただし、責任機関の正当な利益と比較して、処理若しくは利用させないことについての本人の保護に値する利益が明らかに優越する場合はこの限りでない。

個人データの収集の際データが処理され､利用される目的が具体的に確定されなければならない。

（2）他の目的のためには、個人データは第 1 項第 1 文第 2 号及び第 3 号の要件のもとでのみ提供され､又は利用することが許される。

（3）他の目的のための提供又は利用は､以下の各号に定める場合にも許される。

1　第三者の正当な利益を守るために必要な場合、又は、

2　国家の､及び公共の安全にとっての危険の防止ならびに犯罪行為の追及のために必要な場合、又は、

3　宣伝又は市場若しくは世論調査の目的のため、人的集団の構成員に関して、以下に限定された項目につき名簿の形で又はその他の方法でまとめられたデータが取り扱われる場合で、かつ本人が提供又は利用させないことについての保護に値する利益を有すると推定する理由が存在しない場合

a)当該人的集団への本人の所属に関する記載
b)職業､部署又は業務の名称
c)氏名
d)称号
e)学位
f)住所　及び
g)生年

され、続いて、同法 4b 条及び 4c 条（データ保護レベルの十分性）[29]に基づく移転の許容性

4　研究施設の利益のために、学術研究の実施のために必要な場合、研究計画の実施についての学術上の利益が、目的変更の排除に対する本人の利益に著しく優越し、かつ研究目的が他の方法で達成できないか又はその達成に均衡を欠く過度の出費を要するとき

　第 1 文第 3 号の場合、契約関係又は契約類似の信頼関係の目的の範囲内で蓄積された以下の項目に関連したデータが提供されることとなる場合には、提供をさせないことについての保護に値する利益が存在すると推定される。

1　犯罪行為

2　秩序違反ならびに

3　使用者によって提供がなされる場合に労働法上の法律関係

（4）本人が、責任機関に、宣伝又は市場若しくは世論調査の目的のための当該本人の情報の利用又は提供について異議を申し立てる場合、この目的のための利用又は提供は許されない。本人は、宣伝又は市場若しくは世論調査の目的のための請求については、責任機関、データの出所､及び第 1 文に基づく反論権について知らされるものとする。請求者が、本人の知らない機関に蓄積されている本人の個人データを利用するときは、請求者は、本人が当該データの出所について知ることができるようしなければならない。本人が、第三項に従ってデータが提供された第三者に、宣伝又は市場若しくは世論調査の目的のための利用又は提供について異議を申し立てる場合、第三者はこの目的のためのデータを封鎖しなければならない。

（5）データが提供された第三者は、これを、それが提供された目的を遂行するために処理し又は利用することが許される。他の目的のための処理又は利用は､非公的機関は第 2 項及び第 3 項の要件のもとでのみ、ならびに公的機関は、第 14 条第 2 項の要件のもとでのみ許される。提供機関は、第三者にそのことを告知しなければならない。

（6）自己の業務目的のための、特別な種類の個人データ（第 3 条 9 項）の収集､処理及び利用は、本人が第 4 a 条第 3 項により同意しないときは、以下の各号の場合に許される

1　本人又は第三者の死活的な利益の擁護のために必要であり、そして当事者が、肉体的又は法的な理由から、同意を与えることができる状態にない場合

2　本人が公にしたことが明白であるデータが問題になっている場合、

3　法律的な請求権の主張､行使又は防御のために必要であり、収集､処理又は利用を排除することにおる本人の保護に値する利益が優越するということを推定させる根拠が存しない場合、又は

4　学術研究の遂行のために必要であり、研究計画の遂行における学術的な利益が、収集､処理又は利用を排除することによる本人の利益より著しく優越し、かつ研究目的が他の方法で達成できないか又はその達成に均衡を欠く過度の出費を要する場合

（7）特別な種類の個人データ（第 3 条 9 項）の収集は、さらに、これが、健康への配慮、医学上の診断、健康管理、又は公衆衛生業務上の取扱い若しくは公衆衛生行政のために必要であり、かつ、これらのデータの処理が、医師又はその他これと同様の守秘義務に服する者によって行われる場合に許される。第 1 文に挙げられた目的のためのデータの処理及び利用は、第 1 文に挙げられた者に適用される守秘義務規定に従う。

第一文に挙げられた目的のために、健康に関するデータが、その職務の遂行が病気の確認、治癒若しくは鎮静、又は薬の製造若しくは販売をもたらすが、刑法 203 条 1 項及び 3 項に挙げられている職業ではない職業の関係者によって収集、処理又は利用される場合には、これらは、医師自らがこれについて権限を有するであろう場合と同一の条件の下でのみ許される。

（8）特別な種類の個人データ（第 3 条 9 項）は、他の目的のためには、第 6 項第 1 号から第 4 号までの要件の下でのみ提供、利用することが許される。提供又は利用は､これが、国家及び公共の安全にとっての危険の防止並びに犯罪行為の追及のために著しい重要性を有する場合のために必要な場合にも許される。

（9）政治的､哲学的､宗教的又は労働組合的な傾向を有し､収益目的を追求しない組織は、それが組織活動にとって必要である限り、特別な種類の個人データ（第 3 条 9 項）の収集､処理又は利用を許される。このことは、その構成員､又はその組織の活動目的との関連で、その組織と定期的に接触する者の個人データにのみ適用される。この個人データの組織外の者又は機関への提供は、第 4 a 条第 3 項の要件のもとでのみ許される。第 3 項第 2 号が準用される。

[29]　第 4 b 条　個人データの外国ならびに超国家的又は国家間的機関への提供

（1）次の各号に掲げる機関、すなわち

1．他の EU 構成国内にある機関

2．他のヨーロッパ経済圏に関する条約締結国内にある機関、又は、

3．ヨーロッパ共同体の組織及び施設

への個人データへの提供については、その全部又は一部がヨーロッパ共同体法の適用を受ける活動の枠内

が判断される。関係者によれば、この審査の仕組みの中で、拘束的企業準則は、法 28 条に基づく第一段階の許容性審査の中で参照され得るが、準則が不法な処理を合法にできるわけではない、という点が強調されている[30]。

オ）BCR の内容

BCR は、その名のとおり、「拘束力」ある企業準則である。この企業集団内部のルールが

で提供が行われる限り、ここでの提供に適用される法律及び合意に応じて第 15 条第 1 項、第 16 条第 1 項、及び第 28 条から 30 条までが適用される。
（2）第 1 項に掲げる機関に対する個人データの提供について、当該提供が、その全部又は一部がヨーロッパ共同体法の適用を受ける活動の枠内で行われるものではないとき、及び、その他の外国の機関、若しくは、超国家的又は国家間的機関への提供であるときには、
第 1 項が準用される。本人が、提供の排除について保護に値する利益を有している場合には、とりわけ第一文に掲げられた機関において適正なデータ水準保護が保障されていない場合は、提供は行われない。第 2 文は、提供が、連邦の公的機関の固有の事務の遂行のために、防衛、又は危機の克服若しくは紛争の阻止若しくは人道的措置の分野において国家を超えた若しくは国家間の義務を果たすために不可欠であるという理由で必要な場合には、適用されない。
（3）保護水準の適正性は、一のデータ提供、又はデータ提供の一つの範疇において重要なすべての事情を考慮して判断される。とりわけデータの種類、提供の目的、予定された処理の期間、発信国及び最終の目的国、当該受領者に適用される法規範、ならびに適用される身分上の規律及び安全措置が考慮され得る。
（4）第 16 条第 1 項第 2 号の場合に、提供機関は、本人に、データの提供について知らせる。これは、本人が他の方法でそれを知ることが予想される場合、又は知らせることが公共の安全に危険を及ぼし、あるいは連邦若しくは州の福祉に不利益をもたらすおそれがある場合には適用されない。
（5）提供の許容の責任は、提供機関が負う。
（6）データが提供される機関に、提供されたデータを、それが提供された目的を遂行するためにのみ処理し又は利用することが許されることを、指示しなければならない。

第 4 c 条　例外
（1）その全部又は一部がヨーロッパ共同体法の適用を受ける活動の枠内において、第 4 b 条 1 項に挙げられている以外の機関に個人情報を提供することは、当該機関に適切なデータ保護水準が存在しないとしても、以下の場合に限り許される。
1　本人が同意した場合、
2　提供が、本人と責任機関との間の契約の履行のために必要であるか、又は本人の指示に合致した、契約の予備的な措置の遂行に必要である場合、
3　本人のために責任機関によって第三者と結ばれたか、結ばれるような契約の締結又は履行のために提供が必要な場合、
4　重要な公益の確保のため、又は、法廷における法的請求権の主張、行使、又は擁護のために提供が必要な場合、
5　提供が、本人の生命にとって重要な利益の確保にとって必要である場合、又は
6　一般に対する情報であり、かつ、個別事例において法律上の条件が満たされている場合に、何人でもあるいは正当な利益を証明できるすべての者が閲覧可能な登録簿から提供が行われる場合
データが提供される機関に、提供されたデータを、それが提供された目的を遂行するためにのみ処理し又は利用することが許されることを、指示しなければならない。
（2）第 1 項第 1 文にかかわらず、責任機関が人格権及びそれと結びついた諸権利の行使の保護に関して、十分な保障を示すならば、所管の監督官庁は、第 4 b 条第 1 項に挙げられた機関以外に個別の個人データの提供又は個人データの特定の態様の提供を許可することができる。この保証は、とりわけ契約条項又は拘束力ある企業の定めからあきらかになる。郵便及びテレコミュニケーションの企業については、連邦データ保護監察官が所管する。提供が、公的機関を通じてなされる限り、公的機関が第一文に従い審査を行う。
（3）州は、連邦に、第 2 項第 1 文に従ってなされた決定を報告するものとする。
[30] その意味では、完全なワンストップサービスはまだ実現されていないということになる（ただし、2008 年の段階であることをお断りしておく）。

内容的に承認されるか否かは、指令との一致及び当事者に対する法的拘束力に係っている。

指令との一致について言えば、EU 指令は、第三国における十分な個人情報保護の保証の確立のために、企業内部の規律を明示的に規定しているわけではないが、他方、企業準則という手法についての最終的な規準も含んでいない。規定されているのは「特別な契約条項」のみである。したがって、指令との一致は削除され得ない要請ということになる。

また、法的拘束力がある[31]というためには、法的に執行可能であること、実際に当該企業集団内部で拘束的に機能していること、強制されていること、を意味する。これについて、チェックリストでは、事業者は、準則がすべての企業グループの構成企業（まさしく第三国においても）、従業員、下請企業、顧客についても拘束的であることを、詳細に説明しなければならないと述べている[32]。また、拘束力の有無については、司法や苦情処理のレベルも一定の役割を果たすとされている。

[31] EU 指令 25 条・26 条と個人データの第三国への移転のルールを考える上で、日本の行政指導（あるいは○○省の○○に関する指針）との関係がよく問題とされる。
[32] WP108、pp.4-7.

２．個人情報の処理に係るプライバシー保護の国際標準草案のための共同提案

「個人情報の処理に係るプライバシー保護の国際標準草案のための共同提案」（以下「国際標準草案」と略す）とは、個人情報及びプライバシー保護のための国際標準を策定するとの目的で、2009 年 11 月 5 日にスペインのマドリッドで開催されたデータ保護及びプライバシー・コミッショナー会議（以下、「コミッショナー会議」と略す）で提案されたものである。

「１.」で見た EU 指令を中心とした枠組みが EU 以外の諸国との間では依然として、進展せず、その一方で、個人情報の国際的移転の問題はますます重要な課題となっていることに対するコミッショナー会議からの 1 つの方向性の発信である。この国際標準草案は、各国の政府機関によってオーソライズされたものではないが、今後の展開次第では、我が国にも大きな影響を及ぼすものである。そこで、以下では、前提問題として、コミッショナー会議とはどういうものかについて紹介し、その後、国際標準草案の概要と内容、従来の国際文書との違い、各国のデータ保護機関の反応、我が国の法制を前提とした分析の順で、検討を加えることとする。

（１）コミッショナー会議[33]

① まず議論の前提として、コミッショナー会議とは何かということと、我が国の立ち位置について簡単に触れておく。

コミッショナー会議は、1979年に初回が開催され、2010年で32回を数えるものであるが、当初はヨーロッパの個人情報保護先進国間の経験の交換の場であったようである。その後、回を重ね、今日では、独立した第三者機関である個人情報保護機関以外にも、独立した第三者機関を持たない国家の代表（日本はここに分類される）、NGO,経済団体、学術団体等も参加している。コミッショナー会議では、正規メンバーとして認められた個人情報保護機関による決議がなされるのが通例である。この決議に拘束力があるわけではないが、一定の影響力を持つ場合もある。本稿で紹介する、マドリッドでの決議（国際標準草案の提言）は、そのような影響力あるものとなり得る決議であると言われている[34]。

② データ保護当局のこの国際会議への参加資格を認証するための手続と基準は、2001 年のパリ会議で定められており、それが、翌 2002 年カーディフの会議で修正されている[35]。

---

[33] CRITERIA AND RULES FOR CREDENTIALS COMMITTEE AND THE ACCREDITATION PRINCIPLES

[34] 以上は、BFDI（Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ）、http://www.bfdi.de/による。

[35] CRITERIA AND RULES FOR CREDENTIALS COMMITTEE AND THE ACCREDITATION PRINCIPLES
Adopted on 25 September 2001 during the 23rd International Conference of Data Protection Commissioners held in Paris, 24-26 September 2001 and as amended on 9 September 2002 during the

コミッショナー会議は、委員会（正規メンバーのみの閉じられた合議体）と会議（正規メンバ以外も参加可能）とから成るが、正規メンバーになるための資格とその理由を示しておくと、

a)データ保護機関が、法的基盤に基づいて設置された公的な機関であること。権威ある判断・関与をする必要があるからというのが理由である。

b)データ保護機関が、その機能を果たすために一定の自律性と独立性を有していること。自律というのは、法的にも実際にも、他者の許可を求めることなく一定の行為をなす権限が付与されていることであり、独立とは、政治あるいは政府の干渉から自由に行為でき、既得権に抵抗できる機関であることである、とされている。典型的には、一定期間の任期、身分保障、政府あるいは立法のトップに直接に報告でき、国民に関心事について語ることができること、義務としてなした行為に対する法的免責、調査権等の付与が要件となる。

c)国際的な法的整合性

データ保護機関が扱う法的文書が、個人データ及びプライバシーを扱う国際的な法的文書に対応するものであること。国際的な法的文書とは、OECD ガイドライン（1980）、CE 条約（1981）、国連ガイドライン（1990）、EU 指令（1995）、関連する限りで、国内機構の地位に関する原則（パリ原則；1991）[36]である。

d)データ保護機関が適切な範囲で機能及び当該機能を実行するための法的な権限を有していること。適切な範囲とは、コンプライアンス、監督、是正、指導、公教育などの分野のことである。当該機関は、単に助言的（advisory）な権限を有しているだけではだめで、法的あるいは行政的な結果を伴う監督的（supervisory）な権限を有していなければならない。

③　わが国は、委員会にはオブザーバーとしての参加しか認められていないが、b)、d)の要件が問題となっているものと考えられる。

24th International Conference of Data Protection and Privacy Commissioners held in Cardiff 9-11 September 2002、文書は A と B に分かれていて、A が正式メンバーとなるための基準と規則、B が認証の原則である。メンバーになるための資格は B に定められている。

[36] 1991 年、国連人権委員会の決議に基づいてパリで開かれた第 1 回国内機構ワークショップおいて採択、1993 年、国連総会でも附属文書として採択された原則。国内人権機構の権限・責務、構成等についての指針を提供するもの。

（２）内容的特色[37]

① 提案の経緯

プライバシー及び個人データ保護について、地域によって異なるアプローチが存在するのが現状である。EU には 1995 年の EU 指令が存在し、それ以外の地域では、今も、1980 年の OECD ガイドラインが基準となっている。また、近時では、APEC において、プライバシー・フレイムワーク[38]が議論されている。さらに、ヨーロッパでは OECD ガイドラインより拘束力あるものとして、1981 年の CE 条約が存在する[39]。

しかし、これらの文書のいずれについても言えることは、一方で個人の保護に薄く、他方でビジネスには複雑に過ぎるということである。そこで、第 30 回コミッショナー会議では、スイスとスペインの提案により、国際標準の作成のための作業部会が設置された。

② 提案の指標

提案の主な指標は、第 1 に国際的に受容されうる最高のレベルのものを達成するための諸原則及び権利を詳細に述べる、第 2 に国際的なデータ移転の改善を保証する、第 3 に自主規制の役割を検討する、第 4 にできるだけ広範な組織的、社会的コンセンサスを獲得することであった。

③ 国際標準草案の概要（条文見出し）

国際標準草案の概要を、条文見出しを抽出することで示しておくと、以下のような構成になっている。

第Ⅰ部：総則（Part I: General Provisions）
- 1 目的（Purpose）
- 2 定義（Definitions）
- 3 適用範囲（Scope of application）
- 4 追加的措置（Additional measures）
- 5 制限（Restrictions）

第Ⅱ部 基本原則（Part II: Basic Principles）
- 6 適法性及び公平性（Principle of lawfulness and fairness）
- 7 目的明確化の原則（Purpose specification principle）
- 8 比例原則（Proportionality principle）

---

[37] 以下の検討は、開催国であるスペインのコミッショナーの HP に掲載されている、草案及び会議のレジュメ等に基づいて、執筆者が整理・要約したものである。

[38] APEC 及び EU の動きについて、藤原靜雄「ドイツ・シュレスヴィッヒ・ホルシュタイン州のマーク制度」季報情報公開・個人情報保護 25 号(2007 年)11 頁以下。

[39] これらの関係については、藤原靜雄「個人データの保護」岩村正彦他編『岩波講座 現代の法 10 情報と法』（岩波書店、1997 年）193 頁以下。

9　データの質に関する原則（Data quality principle）
10　公開原則（Openness principle）
11　責任原則（Accountability principle）
第Ⅲ部　処理の適法性（Part III: Legitimacy of processing）
12　適法性の一般原則（General principle of legitimacy）
13　センシティブ・データ（機微にわたる事項に属する個人情報）（Sensitive data）
14　処理役務の提供（Provision of processing services）
15　国際移転（International transfers）
第Ⅳ部　データ主体の権利（Part IV: Rights of the Data Subject）
16　アクセス権（Right of access）
17　訂正及び削除権（Rights to rectify and to delete）
18　異議申立権（Right to object）
19　権利の行使（Exercise of these rights）
第Ⅴ部　セキュリティ（Part V: Security）
20　安全管理措置（Security measures）
21　守秘義務（Duty of confidentiality）
第Ⅵ部　コンプライアンス及び監督（Part VI: Compliance and Monitoring）
22　予防的な措置（Proactive measures）
23　監督（Monitoring）
24　協力及び協調（Cooperation and coordination）
25　責任（Liability）

④　従来の文書との異同

この草案の従来の文書（OECD ガイドライン以来の国際文書）との違いは以下の点にあるとされる。ポイントのみ示しておく。

ⅰ）国際的なデータ移転の促進（草案 15 条）
EU 指令が「十分な」（adequate[ad＋equal]：等しくするという語感からは逃れることはできないであろう）レベルであるのに対して、「国際標準により提供されるのと同様の（similar）レベルの保護」と解説されている[40]点は注目に値する。

ⅱ）ファイリングシステムの定義の見直し（草案 3 条 1 項）
EU 指令の定義[41]における「個人データの処理」と「ファイリングシステム」

[40] http://www.privacyconference2009.org., p7
[41]EU 指令第 2 条　（ｂ）「個人データの処理」（処理）とは、自動的な手段であるかどうかに関わらず、個人データに対して行われる作業又は一連の作業を意味するものとする。これには、収集、蓄積、編成、保

の整理、見直しがなされ、マニュアル処理は主たる対象でないことが明確にされている。

iii）事前の措置による責任の軽減（リスク回避の予防的措置）（草案 22 条）

違反の場合の法的責任を軽減する手法として事前に予防的措置の導入を提唱している。

iv）官僚的な要請の縮減（草案 24 条 2 項）

データ保護を改善するわけではない些末な手続きを減量すべきことが、協力関係の項で述べられている。

v）責任主体概念の見直し（草案 2 条 d,e）

EU 指令における責任主体、処理者という概念[42]を見直し、簡潔にしている。

vi）第三者機関概念の拡大（草案 23 条）

監督機関は草案 15 条 3 項で個人データの国際移転に関与するが、これが拡大されている。ちなみに、データ保護コミッショナー会議の正規メンバーになるための基準よりも広い。解説によれば、仲裁機関や消費者保護機関でもよいとされている。

vii）セキュリティ違反の行為の個人への情報提供（草案 20 条 2 項）

深刻な被害が生じうる場合には、データ主体に漏洩等の安全管理措置違反の事実について情報を提供することが定められている。これは、カリフォルニア州のシステムから示唆を受けたものと推測される。

存、編集若しくは変更、検索、参照、利用、又は移転、公開、その他の方法による提供、若しくは連結、封鎖、消去又は破壊が含まれる。

（c）「個人データのファイリングシステム」（ファイリングシステム）とは集約型であるか分散型であるか、それとも機能又は地理的条件に基づいて分散されているかどうかに関わらず、一定の基準に基づいてアクセスすることのできるように構成されている個人データの集合を意味する。

[42] （d）「管理者」とは、個人データの処理の目的及び手段を決定する自然人、法人、行政機関、施設、又はその他のすべての団体を意味するものとする。処理の目的及び手段が国家の又は共同体の法規定や行政規則によって決定される場合には、各構成国又は共同体の法規定により、管理者又はその指名に対する個別の基準を規定することができる。

（e）「処理者」とは、管理者のために個人データの処理を行う自然人、法人、行政機関、施設、又はその他のすべての団体を意味するものとする。

（３）我が国としての分析と検討

① 上述のような内容を持つ国際標準草案について、ドイツの連邦データ保護・情報自由監察官は、NGO 等をも巻き込んだ形[43]での世界ではじめての試みであると好意的な評価をしている。また、アメリカ等の専門家も、この国際標準草案が、EU 指令に従属するものではないことから世界の個人情報保護のベンチマークになりうるのではないかと述べる[44]。

他方、本件文書は国際的文書となる可能性のあるものであるが、拘束力があるわけではない。また、コミッショナー会議の性格については、既に触れたとおりである。また、我が国は正規のメンバーには入っていない。そこで、以下では、我が国の現状を前提として、この文書について簡単な分析を加えておくこととする。

② 国際標準草案と我が国の現行法制

我が国の現行法制から見た今後検討すべき点として、以下のような点が指摘できる[45]。

ｉ）我が国の法制では採用しなかったセンシティブ・データの考え方[46]が採用されている。

ii）3 条の適用範囲は、我が国の個人情報保護法とほぼ同じといってよい。ただし、マニュアル処理が対象ではない（我が国では法 15 条から 18 条がマニュアル処理でも対象となっている）点は異なる。もっとも、完全に対象外か否かはなお確認の必要があろう。

iii）6 条から 11 条の各原則は、OECD　8 原則を現代的に組み替えた感があるが、比例原則、データの質に関する原則は EU 法的な考え方であり、透明性の原則の中に、未成年者であるとか、オンライン収集についての定めがあるのは現代的である。

iv）データ主体の権利に関し、既に述べたように、漏洩等に際して情報提供を受けることができることとされた点は、重要である。

v）独立した第三者機関の要件が、従来の EU 基準より緩やかなものになったことは特記すべき点であろう。国際的データ移転がこのような第三者機関の事前承認により可能となるという点に、この国際標準が世界基準になり得る可能性を秘めていると言えるであろう。

vi）予防的措置として、個人情報保護法制の新たな道具が挙げられている。例えば、個人情報保護監査[47]、プライバシー影響評価（PIA:Privacy Impact Assessment）[48]という

---

[43] ただし、草案そのものはクローズセッション（正規メンバーのみ）で検討されている。

[44] Lexolgy, Observations on standards document adopted by 31st International Conference of DataProtection and Privacy Commissioners, Hunton & Williams LLP（2009.11.13）

[45] 国際標準草案は提案されたばかりで、執筆時点では、詳細に論じる外国文献も存在しないようであるので、個別の問題点に対する解は別稿で論じることとしたい。本文で触れた条項についてもコメントは省いている。本稿では、論点と簡単なコメントを付しておく。

[46]第 8 条　特別カテゴリのデータの処理
1. 加盟国は、人種、民族、政治的見解、宗教、思想、信条、労働組合への加盟に関する情報を漏洩する個人データの処理、若しくは健康又は性生活に関するデータの処理を禁止するものとする。

[47] 例えば、2001 年のドイツ連邦データ保護法で考え方が示されている。第 9 a 条　データ保護監査　デー

考え方である。

vii）国際的な職務共助の定めがあり、国際標準が現実のものになれば、我が国としても対応を迫られることになる。

③　国際標準草案の今後

最後に、国際標準草案をめぐる政治状況について一言しておけば、EU 諸国を始めコミッショナー会議の正規メンバーとなっている国々では、次の課題は、いかにして国際標準草案に法的拘束力を持たせるか、条約的なものにするかということで一致している[49]。

しかしながら、この標準草案作成に際してはアメリカがオブザーバー参加していたという事実があること、また、個人データの移転に関する EU 指令の例外条項には限界があることが、EU 関係者にも認識されていること（データ保護機関と実務界との対立)、データの国際移転については、APEC でも重要な課題となっていること、等を踏まえれば、国際標準草案をめぐる議論の動向を我が国としても注視していく必要があろう。

タ保護及びデータセキュリティの改善のために、データ処理システム及びデータ処理プログラムの提供者とデータ処理機関は、そのデータ保護コンセプト及びその技術設備を、独立のかつ資格を与えられた鑑定人に審査、及び評価をさせ、ならびに審査の結果を公表することができる。審査及び評価へのより詳細な要求、方法ならびに鑑定人の選抜及び資格の付与は、特別法で定められる。

[48] これも、既に 1990 年のカナダ法で示されている考え方である。環境アセスメント的な発想であり、個人情報の収集を伴う情報システムの導入等に際しては、プライバシーへの影響を事前評価し、問題を回避・緩和するためのシステム変更等をするという考え方である。英米系の国（カナダ、オーストラリア等）で導入されているが、発想としては、ドイツ連邦データ保護法にも類似の考え方がある。同法第 3a 条　データ回避及びデータ倹約　データ処理システムの構築及び選択は、個人データの収集処理又は利用を行わないか、できる限り少なくするという考えに準拠しなければならない。とくに、それが可能であり出費が保護目的と適切な関係にある限り、匿名化と仮名化の可能性が利用されなければならない。

[49] もっとも各国がどのような立場であるかについては、現地での調査の必要があると思われる。

資料

個人データの処理に関するプライバシー保護の国際標準草案のための共同提案（仮訳）

第 1 章　一般規定

1 条　目的

本文書の目的は次のとおりである。

a. 個人データの処理に関する効果的で国際的に統一化されたプライバシーの保護を保証する一連の原理や権利を明確にすること。
b. グローバル化する世界において必要とされる個人データの国際的な流通を促進すること。

2 条　定義

本文書の文脈における文言を以下の定義のとおりである。

a. 「個人データ」とは、特定の自然人又は通常利用される可能性がある手段によって特定されうる自然人に関する情報を意味する。
b. 「処理」とは、その措置が自動でなされたか否かにかかわらず、収集、蓄積、利用、開示、削除等個人データになされる措置又は一連の措置を意味する。
c. 「データ主体」とは、当該個人のデータが処理される自然人を意味する。
d. 「責任主体」とは、単独又は共同でデータ処理を決定する公的又は私的な自然人又は組織を意味する。
e. 「処理サービス提供者」とは、責任主体のために個人データの処理を遂行する当該責任主体を除く自然人や組織を意味する。

3 条　適用範囲

1. 本文書は、その適用において、全部又は一部の個人データを自動、さもなければ体系的に構成することによって、公的又は私的部門がなした個人データの処理に照準を定めている。
2. 本文書の規定は、もっぱら私生活又は家庭生活のみに関係する活動における自然人による個人データ処理に対して適用されない旨を国内法で定めることができる。

4 条　付加的措置

1. 各国は、個人データの処理に関するプライバシーの更なる保護を保証する付加的措置によって、本文書で定められている保護の水準を補強することができる。

2. いかなる場合でも、本文書は、国際的な個人データの移転が本文書の 15 条に従ってなされている限り、これを許容する適切な根拠となる。

5 条　制限

各国は、民主的な社会における国家安全の利益や公共の安全、公衆衛生の保護又は他者の権利や自由の保護のため必要な場合、本文書の 7 条ないし 10 条及び 16 条ないし 18 条に定められている規定の適用範囲を制限することができる。このような制限は、データ主体の権利を保持するために適切な保証や制約を確定する国内法によって、明示的に定められるべきである。

第 2 章　基本原則

6 条　遵法性及び公正の原則

1. 個人データは、本文書に定められている個人の権利や自由及び適用を受ける国内法を尊重し、また、世界人権宣言や市民的及び政治的権利に関する国際規約の目的及び原則に合致するよう公正に処理されなければならない。
2. とりわけ、違法又はデータ主体に対する恣意的な差別を生じさせる個人データのいかなる処理も不公正なものとみなされる。

7 条　目的特定の原則

1. 個人データの処理は、責任主体の個別的、明示的かつ正当な目的の遂行の範囲に制限されなければならない。
2. 責任主体は、データ主体の明確な同意なき限り、個人データが収集された目的と合致しないいかなる処理もしてはならない。

8 条　比例原則

1. 個人データの処理は、適切かつ関連性あるもので、かつ、前条で定められた目的のとの関係で過度なものであってはならない。
2. とりわけ、責任主体は、処理される個人データが最小限度の必要な範囲にとどめられるよう合理的な努力をしなければならない。

9 条　データの質に関する原則

1. 責任主体は、個人データが正確であるのみならず、それらが処理される目的の遂行のために必要にして十分かつ最新のものであることを常に確保するものとする。
2. 責任主体は、処理された個人データの保有期間を必要最小限度の範囲にとどめるものとする。個人データの処理が適法とされた目的の遂行のため、もはやそのデータが必

要でない場合には、それらは削除又は匿名化されなければならない。

10 条　透明性の原則

1. すべての責任主体は、個人データの処理に関する公開された方針を有するものとする。
2. 責任主体は、データ主体に対して、少なくとも、責任主体の個人属性（アイデンティティ）、予定されている処理の目的、個人データの開示される相手方、本文書で定められた権利行使の方法に関する情報、及び、個人データの公正な処理を保証するために必要なその他の情報を提供するものとする。
3. 個人データがデータ主体から直接収集された場合、その情報は、既に提供されている場合を除いて、その収集時に提供されなければならない。
4. 個人データがデータ主体から直接収集されていない場合、責任主体は、当該主体に個人データの情報源についても知らせなければならない。この情報は合理的期間内に与えられるべきであるが、責任主体による遵守が不可能又は均衡の取れない努力を伴う場合には他の手段に代えることができる。
5. データ主体に与えられるいかなる情報も、とりわけ、未成年者に個別的に向けられたデータ処理については、明確かつ明瞭な表現を用い、わかりやすい形で提供されなければならない。
6. 個人データが電子交流ネットワークを通じて、オンライン上で収集された場合には、本条の 1. 及び 2. で示された義務が、容易にアクセスできかつ上記の情報のすべてを確認し、かつ含むプライバシーポリシーによって果たされなければならない。

11 条　アカウンタビリティの原則

責任主体は以下の義務を果たすものとする。

a.本文書及び適用を受ける国内法で示された諸原則及び義務を遵守するために必要なあらゆる措置を採ること。

b.23 条に定められているように、その権限行使に際して、データ主体及び監督機関に対し、その遵守を証明するために必要な内部的仕組みを有すること。

第 3 章　処理の適法性

12 条　適法性の一般原則

1. 原則として、個人データは、以下のいずれかに該当する場合に限り処理できるものとする。

a.データ主体から自由で明確なインフォームドコンセントに基づいた同意を得ている場合。

b.責任主体の正当な利益が当該処理を正当化し、かつ、データ主体の正当な利益 、権利、

自由が優越しない場合。

c.当該処理が、責任主体とデータ主体との法的関係の維持や遂行のため必要である場合。

d.当該処理が、適用を受ける国内法によって責任主体に課される法的義務を遵守するために必要な場合又は公的機関の正当な権限行使のため必要であるときに当該機関によってなされる場合。

e.データ主体やそれ以外の者の生命、健康又は安全が脅かされる例外的状況のある場合。

2. 責任主体は、データ主体がいつでもその同意を撤回でき、不当な遅延や費用を伴わず、かつ、責任主体がいかなる利益も得ないような、簡易迅速で効果的な手続を提供するものとする。

13 条　センシティブ・データ

1. 以下の個人データは、センシティブなものとみなされる。

a.データ主体の最も個人的な領域に影響するデータ

b.濫用された場合に、以下の虞があるデータ

i　違法な又は恣意的な差別

ii　データ主体に対する深刻な危険（リスク）

2. とりわけ、人種的若しくは民族的出生、政治的意見、宗教的若しくは哲学的信念又は健康若しくは性生活に関係するデータは、センシティブ・データと考えられる。前項で定める要件を充足する場合、国内法で、その他センシティブ・データの類型を定めることができる。

3. 国内法によるデータ主体の権利保護のため、正当な保証が定められるべきであり、そこでは、センシティブ個人データを処理する際の追加的条件を定めるものとする。

14 条　処理サービスに関する規定

責任主体は、以下の場合、データの第三者提供と解することなく、一のあるいは複数の処理サービス提供者を通じて個人データの処理をなすことができる。

a.処理サービス提供者が少なくとも本文書及び適用を受ける国内法に定められた保護のレベルを有していることを責任主体が保証している場合。

b.契約又は法的手段によって法的な関係が確立されており、それによって、提供の存在、範囲及び内容を定められ、かつ、前号の保証の遵守及び当該個人データが責任主体の指示に従い処理されることを確保するための処理サービス提供者の義務が定められている場合。

15 条　国際的移転

1. 原則として、個人データの国際的移転は、そのようなデータを移転される国家が、少なくとも本文書に定められた保護のレベルを有している場合になすことができる。

2. 個人データを移転しようとする者は、その受領者が本文書で定められた保護のレベルを有することを保証する場合には、当該データをその保護レベルを有しない国家へ国際的に移転することが可能である。このような保証は、例えば、適切な契約条項によってなし得る。とりわけ、その移転が企業内又は国際的なグループ内においてなされる場合、このような保証は、その遵守が義務的である内部的なプライバシー・ルールに含まれ得る。
3. さらに、データ移転をする予定の者に適用される国内法では、契約関係の枠組みにおいて必要かつデータ主体の利益である場合、データ主体若しくは他人の極めて重要な利益を保護するために必要である場合、又は、重要な公共の利益のため法的に要求されている場合、本文書で定められている保護のレベルを有しない国家への個人データの国際的移転を許容することができる。

   国内法では、23 条で定められた監督機関に対し、その所管区域内で行われる国際的移転の一部又はすべてを事前に認可する権限を付与することができる。いかなる場合も、個人データの国際的移転をなす予定の者は、その移転が、本文書で定められた保証、とりわけ 23 条 2. で定められた権限に従い監督機関によって要求されている場合にはそれに定められた保証を遵守していることを証明できなければならない。

第 4 章　データ主体の権利

16 条　アクセス権

1. データ主体は、処理される個別の個人データ、そのデータの情報源、処理目的及びそのデータが開示される又は開示される予定の相手方又は相手方の範囲に関する情報を、申請に基づき、責任主体から得る権利を有する。
2. データ主体に与えられるいかなる情報も、明確かつ平易な表現を使い、分かりやすい形で提供されなければならない。
3. 国内法では、データ主体がその権利行使に際して正当な理由を述べない限り、多数の申請に短期間で対応することを責任主体に対し要求する反復的な権利行使を制限することができる。

17 条　訂正及び削除の権利

1. データ主体は、不完全、不正確、不必要又は過剰な個人データの削除又は訂正を責任主体に求める権利を有する。
2. 正当化される場合、責任主体は、求められた訂正や削除を行わなければならない。また、責任主体は、個人データが開示された第三者を知っている場合、彼らにその事実を知らせなければならない。
3. 個人データの削除は、適用を受ける国内法又は場合によって責任主体とデータ主体と

の契約関係によって責任主体に課されている義務の履行のため保持しなければならない場合には正当化されない。

18 条　異議申立ての権利

1. データ主体は、自己の特定の個人的状況に関係する正当な理由がある場合には、個人データの処理に異議を申し立てることができる。
2. この異議申立ての権利は、当該処理が適用を受ける国内法によって責任主体に課される義務の履行に必要な場合には正当化されない。
3. いかなるデータ主体も、個人データの自動処理のみを根拠として法的効果を生み出す決定に対して異議を申し立てることができる。ただし、その決定が、データ主体によって特に求められた場合、又は、責任主体とデータ主体との法的関係の設定、維持若しくは履行に必要は場合を除く。後者の場合、データ主体は、自己の権利や利益を保護するため、自己の見解を主張することができなければならない。

19 条　同章の権利行使

1. 本文書の 16 条ないし 18 条に定められている権利は、以下の者によって行使することができる。

a.責任主体に対して自己のアイデンティティを十分立証しなければならないデータ主体本人

b.責任主体に対して自らの地位を十分証明しなければならない代理人

2. 責任主体は、データ主体が、不当な遅延、費用及び責任主体のいかなる利益も伴わない、簡便、迅速かつ効果的な方法で、本文書の 16 条ないし 18 条に定められた権利行使が可能となるよう措置を採らなければならない。
3. 責任主体が、適用を受ける国内法に従い、この章に定める権利行使が正当化されないと結論付けた場合、データ主体はその結論に至る理由を告知されなければならない。

第 5 章　安全

第 20 条　安全管理措置

1. 責任主体及び処理サービス提供者は、完全性、秘密性、利用可能性を確保する適切な技術的かつ組織的措置によって、処理にさらされる個人データを保護しなければならない。これらの措置は、現存する危険、データ主体に対する起こりうる結果、個人データのセンシティブな性質、最新技術、当該処理がなされた脈絡及び適用を受ける国内法に含まれる義務が存在する場合、それを含めた事項によって決まる。
2. データ主体は、金銭又は非金銭的権利に重大な侵害をもたらす可能性がある安全保護違反行為及びその解決のために採られた措置について、当該処理のいかなる段階であ

ってもそれに関与した者によって報告を受けるべきである。この情報は、データ主体が自己の権利保護を図れるようにするため、合理的期間内に提供されなければならない。

第 21 条　秘密保持義務

責任主体及び処理のいかなる段階でも関与する者は、個人データの秘密を保持するものとする。この義務は、データ主体との関係が終了後であっても、また、必要な場合には、責任主体との関係終了後であっても、継続するものとする。

第 6 章　法令遵守と監督

第 22 条　予防的措置

各国は、国内法を通じて、個人データの処理に関するプライバシー保護について適用する法のより良い遵守を促進するための措置が、いかなる段階であってもその処理にかかわる者によって実施されることを奨励すべきである。このような措置には、とりわけ以下のことを含む。

a.情報安全統制と管理の両者又はその一方の基本モデルに基づく、違反行為を防止及び発見するための手続を実施すること。

b.適切な職務遂行のための適切な資格、資質及び権限を有する 1 名以上のデータ保護担当者又はプライバシー担当者を指名すること。

c.個人データの処理に関するプライバシーの保護について適用を受ける法及びその目的のために組織によって定められた手続のより良い理解に向けた組織の構成員に対する、訓練、教育及び啓発プログラムを定期的に実施すること。

d.個人データの処理に関するプライバシーの保護について適用を受ける法及びその目的のために組織によって定められた手続の遵守を証明するため、資格のある、可能であれば独立した機関による透明性の高い監査を定期的に実施すること。

e.とりわけ、技術的仕様、発展及び装置に関する決定の際、個人データの処理に関するプライバシーの保護について適用を受ける法に従い、個人データを処理する情報のシステムとその技術の両者又はその一方を改良すること。

f.個人データ処理のための新しい情報のシステムと技術の両者又はその一方を実施する前、又は、個人データの処理方法の新しい方法若しくは既存の処理の実質的な変更を実施する前に、プライバシー影響評価を実施すること。

g.法令遵守及び個人データの保護水準に関連する効率の測定を可能とする要素を含む、非遵守の場合の効果的措置を定める拘束的な遵守すべき行為規範を制定すること。

h.個人データの処理に関するプライバシーの保護について適用を受ける法の違反を立証する場合における行動のためのガイドラインを定める応答計画を実施すること。それ

には、少なくとも、違反行為の原因と範囲を確定すること、その悪影響を説明すること及び将来の違反行為を防止するための適切な措置をとることという義務を含むこと。

第 23 条　監督

1. すべての国家は、本文書で定められた原則の遵守を監督する責任を負う一つ以上の監督機関を国内法に従い有するものとする。
2. これらの監督機関は、公平なものでありかつ独立しているものとし、データ主体によって申し立てられた苦情の処理及び個人データの処理に関するプライバシー保護の国内法遵守を確保する必要がある場合の調査や介入実施のための技術的能力、十分な権限及び適切な資質を有しているものとする。
3. いかなる場合も、前項で定めた監督機関の行政措置又は司法的判断の司法上の監督を妨げない限り、データ主体は、適用を受ける国内法に定められた規定のもと、自らの権利を行使するため、裁判所に直接訴えることができる。

第 24 条　協力と協同

1. 前条で定めた機関は、個人データの処理に関して、国内及び国際的なレベルで協力するよう努めるものとする。この協力を促進する目的のため、各国がこの領域で権限ある監督機関を必要に応じて特定できなければならない。
2. これらの機関は、とりわけ以下の事項のため、あらゆる努力をするものとする。

a.職務を効率的に行使するため、とりわけ、調査又は介入実施に際して他の監督機関による協力要請のあった場合、報告書、調査、技能、コミュニケーション及び規制戦略その他の有益な情報を共有すること。

b.国内及び国際的なレベルにおいて、2 つ以上の機関が利害関係を有する事柄に、連携して調査や介入を実施すること。

c.共同歩調の採用及び監督機関のようなスタッフの職務行使の技術能力の向上の推進に資する団体、作業グループ、共同フォーラム、セミナー、ワークショップ、コースへ参加すること。

d.協力過程で交換した情報の秘密に関して適切な水準を維持すること。

3. 各国は、監督機関間における、本条のより効果的な遵守に資する地域的、国内的、国際的協力合意の交渉を促進すべきである。

第 25 条　責任

1. 責任主体は、個人データの処理に関するプライバシーの保護について適用される法に違反した個人データ処理の結果生じたデータ主体への金銭的損害と非金銭的損害の両者又はその一方に対する責を負う。ただし、責任主体が、その損害に対して責を負

わないことを証明した場合を除く。この責任は、その処理段階で関与した処理サービス提供者に対する責任主体によるいかなる行為も妨げないものとする。

2. 各国は、前項で定められた損害賠償請求を認める司法上及び行政上の関連手続に対するデータ主体のアクセスを容易にする適切な措置を促進するものとする。
3. 前述の責任は、個人データの処理に関するプライバシー保護についての国内法の規定に違反する場合に必要に応じて定められている刑事罰、民事罰、行政罰を妨げずに存在すべきである。
4. 本文書の 22 条で定められているような積極的な措置の実施は、本条で定められた責任及び罰を決する際に考慮されるべきである。

提案者

・スペイン、スイス、フランス、アイルランド、カナダ、チェコ、ドイツ、イタリア、オランダ、ニュージーランド、イギリスのデータ保護執行機関
・ヨーロッパデータ保護監督官

Ⅳ　まとめ

Ⅳ　まとめ

筑波大学法科大学院教授　　藤原　靜雄

１．個人データの国際移転の問題と EU 指令

(1) 我が国はじめ世界の国々の個人情報保護法制に大きな影響を与えてきた 1980 年の OECD 理事会ガイドラインの正式名称が、「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」であることからうかがわれるように、個人データの国際流通の問題は、個人情報保護法制の黎明期からの課題である。そして、この課題は、企業のグローバルな事業展開が進むにつれて―潜在的なリスクに止まっている場合も含め―事業者にとっても、消費者等の情報主体にとっても、また各国の規制当局にとってもより深刻な問題となってきたと言える。

(2) このような中で、1995 年の EU 指令は、その 25 条において、個人データの保護措置が「十分」でない国に対する EU 市民の個人データの移転の拒否があり得ることを宣言し、日米はじめ多くの国々に個人データの国外移転の問題に対する対応を迫った。「十分性」の判断は、移転を受ける主体のあらゆる事情の評価（移転国側が自己の責任で行う）と EU 委員会による同様の確認手続の下でなされる（指令 25 条 4 項、6 項)。仮に、「十分な」保護レベルにあると認定されれば、個人データの移転にそれ以上の手続は必要としない。

(3)　もっとも、この EU 指令の要請については、26 条で例外が定められており、「十分性」が欠けている第三国にも、次のような例外的措置による移転可能性が認められている。

① 指令 26 条 1 項に列挙されている事由が存在する場合（例：当事者の同意）
② 指令 26 条 2 項により、移転国のデータ保護機関が例外的に認める場合（「十分な保護措置［特に適切な契約条項によって生じ得る]を提示する場合」)。 この例外は、個別許可である。
③ EU 委員会の承認による標準契約条項による場合（指令 26 条 4 項)。同一の様式により、各国のデータ保護機関の審査の負担を軽減することが狙いである。指令 31 条 2 項の手続により行われる。

標準契約の主たるものは、2001 年モデルと 2004 年モデルである。2001 年モデルが、当初 EU 委員会が「十分性」を有すると考えたものであるが、国際的な経済団体から柔軟性を欠くとの批判を受けて、経済団体側の提案の条項を EU 委員会が受け入れたのが 2004 年モデルである。この点について、各国のデータ保護当局は、2004 年様式によって実務に大幅に歩み寄ったことは、EU 市民にとっては個人情報保護の水準の低下であると評している。

(4) 多国籍企業（コンツェルン）が展開する現代社会において、EU 指令はこれを前提とした定めを置いていない。例外としてあり得るのは個別の契約（標準契約は裁量による変更が許されないので多国籍企業が使うことは不可能）と拘束的企業準則（BCR）である。実際には、BCR のみが実務で議論されている。しかしながら、この BCR も企業準則自体いいかえればルールの全体がデータ保護機関によって認められるのではなく、個人データの類型等に区別して行われるという限界がある。したがって、BCR を国際移転のための唯一又は最善のツールと考えるべきでなく、標準契約条項に関する委員会の決定やセーフハーバー（アメリカ[セクトラルな規制であり、適時な規制もなされない場合がある]との間で EU が認めた「経済界の自主規制」を「十分」と認定するシステムであり、我が国には妥当しない）などに問題がある場合に、追加的手段を提供するものと見るべきである、というのが EU データ保護関係者の見方である。

(5) このように、現在、個人データの国際移転をめぐっては決め手がなく、ある意味で法的議論と柔軟な移転を望む実務との乖離が語られている状況である。このような問題意識があってかどうかは定かではないが、個人データ・プライバシー・コミッショナー会議で国際標準契約という試みが提案され（第 30 回）、その草案が明らかにされている（第 31 回）。

従来の国際的文書が、一方で個人の保護に薄く、他方でビジネスには複雑に過ぎるという問題意識の下、「第 1 に国際的に受容されうる最高のレベルのもの」という目標を掲げ、国際的なデータ移転の促進（「国際標準により提供されるのと同様の（similar）レベルの保護」と解説されている）、監督機関（個人データの国際移転に関与する）概念などを提言している（解説によれば、仲裁機関や消費者保護機関でもよいとされる）。

この草案は、EU 指令のくびきを免れているという点で EU 域外の国からも評価されているものであるが、今後はこの文書にいかに法的拘束力を持たせるかのステージに入ったとされている。

２．近時の動向の我が国から見た分析

(1) まず第１に、EU 指令との関係であるが、EU 関係者によれば、日本は、個人の私生活にかかわる個人データ及び基本権に関して十分なレベルの保護を提供している国であるとは、EU によっていまだ考えられていない、とのことである（もっとも、十分性認定手続の開始は、日本の代表部によってなされる公式の要請の欧州委員会への提出を条件とする）。

となると、EU 構成国から日本へのデータの移転は、EU 構成国各国のデータ保護機関による事前の情報／権限付与（prior information/authorization）を意味する指令 95/46/EC 第 26 条に従って行われなければならないことになる。この例外事由については、上記１．で述べたとおりである。

(2) 国際的データの移転といった場合に、主に問題となっているのは、被用者データ（人事関係情報）であるようであるが、これが我が国でどの程度の現実性を有する問題なのかの調査等も必要となろう。また、顧客データも問題となりうるが、この場合には、実は犯罪対策等の問題と密接な関係があることにも留意すべきであろう。

なお、まだ、議論が動き出したばかりで、拘束力を持つ文書となるかどうかの判断は難しいが、国際標準草案の場合には、かなり柔軟な仕組みとなる可能性があるので、我が国の監督機関の設計次第によっては対応が可能であろうと思われる。その意味で、国際標準草案の行方を注視する必要があろう。また、現在進行中の、APEC での個人情報保護プロジェクト（APEC パスファインダー・プロジェクト）との関係についても整理しておくことが望ましいと思われる。

また、BCR については、我が国でこれを必要とする多国籍企業がどの程度存在するかという問題の他、標準契約との使い勝手の比較検討も必要となろう。