

商事仲裁・商事調停と商取引の実務・法務

2016

# JCAジャーナル

## CONTENTS

7  
JULY

- ◆ 第18回 国際民事執行・保全法裁判例研究  
「相互の保証」を欠くとして中国判決の執行判決を求める訴えを棄却した事例／高杉 直
- ◆ TPP研究フォーラム（6）第6回  
越境サービス貿易・電気通信・留保表／ト部 晃史
- ◆ 最新クロスボーダー紛争実務戦略シリーズ 第27回  
EUの一般データ保護規則：日本企業への影響と具体的対応策／クリスチャン・シュローダー、高取 芳宏、矢倉 信介



# JCAジャーナル

目次

Contents

2016年 7月号 No.709

- 1 ● 目次
- 2 ● 英文目次

---

## 仲裁とADR

- 3 ● 國際民事執行・保全法裁判例研究(18)  
「相互の保証」を欠くとして中国判決の執行判決を求める訴えを棄却した事例  
東京高判平成27年11月25日(判例集未登載、LEX/DB:25541803)及び東京地判  
平成27年3月20日(判タ1422号348頁)／高杉 直
- 10 ● 投資協定仲裁判断例研究(80)  
BIT上の投資家の定義において「設立準拠法」に加えて規定される場合の「本拠地」の  
解釈／猪瀬 貴道
- 56 ● 新・國際商事仲裁関係判例紹介(109)／吉田 一康
- 58 ● 仲裁文献紹介(272)／秦 公正

---

## 商取引

- 17 ● TPP研究フォーラム(6) 第6回 越境サービス貿易・電気通信・留保表／卜部 晃史
- 20 ● アジア諸国を中心とした各国のビジネス法制度について 第22回  
マレーシアの外国投資関連法(1)／阿部 道明
- 30 ● アジア新興国における知的財産ビジネス実務対策  
第4回 インドの知財概要／岩井 久美子
- 36 ● ベトナム「判例」制度—ベトナム法務の新機軸— 第5回  
／伏原 宏太、ブイ・ティ・ホン・ズオン
- 39 ● 中国ビジネス法務の最新事情 第46回  
中国独禁法 合弁会社の設立と企業結合規制～商法函【2016】175号の衝撃～  
／藤本 一郎
- 42 ● 最新クロスボーダー紛争実務戦略シリーズ 第27回  
EU一般データ保護規則：日本企業への影響と具体的対応策  
／クリスチャン・シュローダー、高取 芳宏、矢倉 信介
- 53 ● 貿易実務Q&A【33】／有本 泰夫

- 
- 60 ● 会員通信
  - 67 ● バックナンバー紹介
  - 表3 ● 英文および中文契約書ひな型のご案内

# Contents of July, 2016

- 1 ● Contents

---

## Arbitration and ADR

- 3 ● Case Studies of International Civil Execution and Provisional Remedies, No.18  
Refusal to Enforce the Chinese Money Judgment due to Lack of Reciprocity / Naoshi Takasugi
- 10 ● Case Notes on Investment Treaty Arbitration Awards and Decisions (80)  
The interpretation of the "Seat" as an additional requirement in the definition of investor in BIT/ Takamichi Inose
- 56 ● New Introduction of the Court Precedents Relating to International Commercial Arbitration (109)/ Ikko Yoshida
- 58 ● Introduction of the Arbitration Literature (272)/ Kimimasa Hata

---

## Business Transactions

- 17 ● TPP Study Forum (6) ~6th forum ~ Cross Border Trade in Services, Telecommunication and Reservation List/ Akifumi Urabe
  - 20 ● Business Law Systems in Asian Countries (22)  
Foreign Investment Related Laws in Malaysia (1)/ Michiaki Abe
  - 30 ● Points of Business Practice concerning Intellectual Property in Developing Countries of Asia (4)  
Outline of Intellectual Property in India / Kumiko Iwai
  - 36 ● Commencement of "Case Law" system in Vietnam (5)  
A New Line for Legal Service of Vietnam law/Hirota Fushihara, Bui Thi Hong Duong
  - 39 ● Updates on Commercial Legal Practice in China (46)  
Incorporation of Joint Venture Company and Regulations for Business Combination concerning Chinese Anti-Monopoly Act -Impact of Announcement No.175 (2016) of Ministry of Commerce -/ Ichiro Fujimoto
  - 42 ● Current Practical Strategy for Cross-Border Disputes (27)  
EU General Data Protection Regulation: Potential Impact on Japanese Business and Strategic Measures/ Christian Schröder, Yoshihiro Takatori, Shinsuke Yakura
  - 54 ● International Trade Business Q & A 【33】 / Yasuo Arimoto
- 
- 60 ● Information for JCAA Members
  - 67 ● Table of Contents of Back-Numbers

オリック東京法律事務所・外国法共同事業の訴訟チームにより、国境を超えるプロジェクトにおける紛争解決戦略について毎月開催されているオリックライブラリーセミナーの内容に基づき、実務的な観点から紹介して頂く論稿シリーズで、JCAジャーナル2011年11月号から連載頂いております。

## EU一般データ保護規則 日本企業への影響と具体的対応策

### I. 序文

長年の集中協議を経て、EU一般データ保護規則 (General Protection Regulation、以下「規則」) が、2016年4月に可決された。規則は不統一であったEUデータ・プライバシー法を調和させ近代化するものである。この新しいデータ・プライバシー制度は、欧州企業や欧州に子会社を持つ企業に影響を与えるだけではない。規則はまた、EU内における居住者の個人データ（例えばインターネット上の）を処理しているEU外の企業にも大きな影響を与える。規則は、新しいデータ保護とプライバシー規制を無視している企業に対して、厳しい制裁（全世界年間売上高の4%まで）を執行する可能性がある点にも留意が必要である。

以下では、規則がもたらすこれまでの制度から主な変更点の概要を説明し、EUに子会社を有しているかEUの居住者の個人データを処理しているために、規則の適用範囲に含まれうる日本企業への影響について説明する。

### II. 概要

規則は、EUのデータ保護の状況に大幅な変更をもたらす。変更の一部は、国際的にビジネスを行う企業にとって特に重要である。

日本の企業に直接的な影響を与える可能性のある規則の要点は次の通りである。

・**重い制裁** 規則に違反する場合には、企業は、全世界の年間売上高の4%までの制裁金という制裁リスクに直面する。また、被害者には、非金銭的損害を請求する権利が付与され、例えば、消費者団体は、データ保護の侵害に基づく損害

クリスチャン・シュローダー (Christian Schröder)

オリック・ヘリントン&サトクリフ LLP デュッセルドルフ・オフィス  
ドイツ弁護士

たかとり よしひろ  
高取 芳宏

オリック東京法律事務所・外国法共同事業  
弁護士(日本及び米国ニューヨーク州登録)、英国仲裁人協会上級仲裁人(FCIARb)

やくら しんすけ  
矢倉 信介

オリック東京法律事務所・外国法共同事業  
弁護士(日本及び米国ニューヨーク州登録)、弁理士

賠償の集団的請求のための訴訟が可能になる。

・**より広い適用範囲** 規則は、EU外に確立されたデータ・コントローラ（自らの目的のため個人データを収集する主体）およびデータ・プロセッサ（データ・コントローラからの指示により個人データの処理を実施する主体）に適用される。これは、ビジネスの処理活動が、EUに所在する個人への商品やサービスの提供、またはEUに所在する個人の行動の監視に関連する場合である。

・**コンプライアンス組織のためのより強いインセンティブ** 一部の企業は、これまで以上に広汎なデータ保護のためのコンプライアンスシステムの構築に向けて投資し、リスク評価とコンプライアンス・チェックを定期的に実施し、監督調査が実施された場合のリスクを軽減するために、それら対応策の具体的な実施内容を文書化する必要がある。データ保護に向けたコンプライアン

スの遵守は、おそらく日々の意思決定に対しさらに強い重みを持つことになり、データ処理そのものがビジネスに与える影響は大きくなる。

・データ・セキュリティ侵害の通知 規則は、一般的なデータ侵害通知要件を規定している。対象は、すべての個人データに拡張され、更新された有効な社内方針の実施が必要な場合がある。

・データ転送 規則の下では、適切なデータ保護水準を提供していないEU以外の国々への個人データの転送は、一般的に禁止されている。EUモデル契約条項は、従前どおり、このようなデータをEU外に転送するための有効な仕組みとなる。規則は、有効なデータ転送メカニズムとしての拘束的企業準則の使用を明示的に言及している。そのため、国際的なデータ転送に関するEUのデータ保護法の遵守は、拘束的企業準則を採用することにより実現されるうる。

## III. 規則の重要な側面

### 1. 経緯

規則は2016年4月14日、4年間の起草と交渉を経て、EUレベルで採択された。<sup>(1)</sup> 規則の最初の草案が、欧州委員会（「委員会」）により2012年1月に発行され、統合された規則の本文は2015年12月15日に発表された。<sup>(2)</sup>

規則はEU官報での公表後20日に発効する。その規定は、この日付の2年後、2018年春に、EUの全加盟国において直接適用される。

### 2. EUデータ保護指令と新しいデータ保護体制を確立するための理由

規則は、今から20年以上前にさかのぼる1995年に制定されたEUデータ保護指令95/46 / EC（「指令」）にとって替わるものである。今まででは、EUのデータ保護制度には調和のとれたものがなかった。国内法とEUの加盟国（「加盟国」）に実施される必要のあった指令は、実施に当たり異なるアプローチを取っている。加盟国の制度上の違いは、毎年約23億米ドルの巨額な不一致コストにつな

がっている。<sup>(3)</sup> 欧州の複数国で事業を行う企業は、多くの場合、不必要的コストに直面する（立法の調和、III. 5も参照のこと）。これに対し、規則は、すべての加盟国で直接適用可能であるため、国内実施の必要性がなくなった。規則の制定によりEUのデータ保護体制は大幅に調和され、したがって不一致コストが大幅に削減される。

### 3. 国際間での個人データの転送

#### （1）日本企業への影響

指令および規則の双方は、欧州経済領域（「EEA」）外の事業体への個人データの転送を制限する。個人データの定義は、特定されるまたは特定可能な自然人に関するあらゆる情報、という広い範囲のデータを対象とする。これには、オンライン識別子または個人の物理的、生理的、遺伝的、精神的、経済的、文化や社会的アイデンティティに固有の要因が含まれている。この制限は、欧州で事業所を有するすべての日本企業、および自社のグループ内、例えば日本の親会社とデータを共有したいすべての日本企業に適用される。

#### （2）ヨーロッパと米国間での個人データの転送

日本企業が米国に子会社を有し、欧州市場でビジネスを行っている場合、それらの間でのデータの転送は、2015年10月に下された裁判所の判決によって深刻な影響を受けているため、欧州と米国間での個人データ転送について検討する価値がある。

2015年10月、欧州司法裁判所は「米国-EU間セーフハーバーの枠組み」は無効であるとの判決を下した。<sup>(4)</sup> その結果、この枠組みに基づくすべての個人データの転送は、明確な法的安全性の裏付けなしに行われていることになる。<sup>(5)</sup>

この判決以降、企業は合法的に個人データを転送するための代替的手段を見つけなければならなかつた。<sup>(6)</sup>

2016年2月29日に、欧州委員会は、セーフハーバーに関する代替的な枠組みおよび解決策として、「EU-米国プライバシー・シールド」を提案した。<sup>(7)</sup> 第29条作業部会の最新の見解によると、EU-米国プライバシー・シールドの現行版は、米

国に転送される個人データのための適切な保護を提供していない。<sup>(8)</sup> 第29条作業部会は、各加盟国、EUデータ・プロテクション・オフィサー、および委員会のデータ保護当局からの代表からなるデータ保護の専門家のグループから構成される。

EU-米国プライバシー・シールドは未だ構築途中だが、企業はEUモデル契約条項の導入を検討すべきである（データ転送のためのEU承認条項）。その他の方法として、グループ内の合意または拘束的企業準則の実施がある。拘束的企業準則は、EUのデータ保護監督当局によって承認され、それぞれのデータ転送ごとに新たな契約の締結を必要としない、より使い勝手のよい枠組みを提供できる企業準則である。<sup>(9)</sup>

### （3）第三国への個人データの転送

加盟国以外の国々およびEEAの加盟国は第三国として分類されているため、グループ内でのデータの共有、さらに「第三国」へのデータの転送には、多くの問題がある。

データ転送に関しては、データ・コントローラとデータ・プロセッサとを区別する必要がある。前述のとおり、データ・コントローラは、例えば、個人データの処理の目的と手段を決定する主体を意味し、データ・プロセッサは、データ・コントローラに代わって個人データを処理する主体を意味する。

企業が第三国へ個人データを転送することができるいくつかの方法がある

- **委員会の妥当性テスト** 委員会は、第三国としての個々の国、地域、または処理部門での妥当性の判断を下す権限を有している。妥当性テストのために、委員会は、特定の地域、国などにおけるデータ保護法を確認し、それぞれデータ保護法は、EUデータ保護法と比較して個人データへの同等の保護を提供するかどうかを決定する。なお、このような保護は、米国や日本についても確認されていない。

- **EUモデル契約条項** 妥当性テストとは別に、個人データを転送するための他の可能性があ

る。最も一般的なものは、EUモデル契約条項の適用である。これまでのところ、欧州委員会は、EU/EEA外で設立されたデータ・コントローラからデータ・コントローラへ個人データを転送するための標準的な契約条項二組と、EUおよびEEA外で設立されたデータ・プロセッサへ転送するための同契約一組を発行した。<sup>(10)</sup>

- **拘束的企業準則** 企業はまた、個人データ転送の基礎として、拘束的企業準則の確立を検討することができる<sup>(11)</sup>。過去には、拘束的企業準則は、データ・コントローラが居住地を有する様々な加盟国にあるすべてのEUデータ保護監督当局による承認を必要としたため、過剰な負担がかかることが判明した。

規則のもとでは、必要な承認について、データ・コントローラまたはデータ・プロセッサが、その主な事業所または代表者を有する加盟国のデータ保護監督官庁である、いわゆる「主導監督当局」によって承認が付与されれば足りる（立法の調和Ⅲ.5も参照のこと）。

もう一つの问题是、公的当局に個人情報を開示する義務である。例えばEU外に所在するデータ・コントローラは、EUデータ保護法の対象となる個人データについて、EU外管轄当局により開示を強制される場合がある（例えば、金融当局や裁判所）。しかしながら、多くの場合、両方の管轄下における要求事項を遵守する方法に関する重大な問題が生ずる。

規則の下では、対象としたデータ・コントローラまたはデータ・プロセッサを必要とする第三国の行政当局による個人情報の開示を命じる決定は、以下の場合にのみ、承認または、執行可能である。

- 刑事共助条約に基づく場合、または
- 要求第三国とEUや加盟国間で有効な国際的合意に基づく場合

## 4. 制裁の厳格化と増加する執行力

### （1）日本企業への影響

規則の下で、可能な制裁の内容は飛躍的に重大

化している。同時に、執行可能性は、指令の下にあった時より規則の下でははるかに高くなる。

## (2) 指令の下での執行

従前のEUデータ保護法は、効果的な執行の欠如を批判してきた。個人による民事上の請求は、多くの場合、現実の金銭的損害賠償に限定され、非金銭的損害（例えば、精神的苦痛に対する）は特別な場合に限定され、その後もごく低い損害賠償しか認められない。データ保護監督当局により命ずることができる制裁（過料）は、脅威として機能するにはあまりにも低いと考えられている。さらに、人員不足のため、データ保護監督当局はほとんど積極的な調査を行うことはなかった。

## (3) 新しい制裁と増加する執行力の導入

規則は、その執行を強化するため、以下の制裁や仕組みを導入することにより、執行上の問題点に対処することを目指している。

- ・制裁の範囲は、最大2,000万ユーロまたは企業グループの世界的な年間売上高の4%に相当する額まで制裁金の額が増加された。これは、例えば、そのような同意のための条件として、国際的な転送や処理のための基本原則に関する要件の違反に適用される。その他特定の違反に対する制裁は、世界的な年間売上高の2%までの制裁金となる。<sup>(12)</sup>
  - ・個人は、非金銭的損害賠償を含む司法上の救済を受ける権利を付与される。
  - ・公益団体、組織、または団体に付与される訴訟を提起する集団的権利。
  - ・個人に対するデータ・コントローラおよびプロセッサの直接の義務が導入される。
  - ・国家レベルでのデータ保護監督当局が強化されようとしている。
- 規則の違反に対する制裁金の算定には、違反発覚後における違反者の協力だけでなく、とりわけ以下が考慮に入れられる。
- ・違反の本質、重大性、および期間、並びに影響を受けた個人の数と被害の程度
  - ・実施された技術的および組織的手段や手続きに

関する、データ・コントローラまたはデータ・プロセッサの責任の度合い。これには意図的およびデフォルトのプライバシー、およびデータ保護行為の影響評価が含まれる（意図的およびデフォルトのプライバシー、III. 9 を参照のこと）。規則によって導入された前述の請求プロセスにより、規則に違反した場合の損害賠償および請求を受けるリスクが大幅に高まる。加盟国におけるデータ保護監督当局は、人員不足のため即座に調査に積極的になる可能性は必ずしも高くないが、個人および特に消費者保護団体は、以下に述べる二つの理由から、データ保護監督当局に苦情を提出するか民事訴訟を開始するより強いインセンティブを有する可能性がある。

まず、救済は彼らにとってより興味深いものになり（非金銭的損害に対する損害も）、損害への集団請求が訴訟を開始するための費用とリスクを削減し、またコンプライアンス違反を立証するために必要な証拠へのアクセスを得ることが容易になる。例えば、個人または消費者保護団体は、データ保護監督当局に苦情を申し立てることで、当局が内部コンプライアンス条項に関する情報をデータ・コントローラに要求できる。その結果についてデータ保護監督当局は申立人に報告しなければならないため、申立人は、おそらくそのような情報へのアクセスを得ることになる。

次に、規則の下で、訴訟は事業所の場所、または個人の居住地の場所で提起することができる。

## 5. 立法の調和

前述したように、指令の下では、EUのデータ保護法の不調和により、毎年約23億米ドルの巨額な不一致コストをもたらし、様々な事業に影響を与えている。規則の下で調和が図られることにより、規則はすべての加盟国において直接適用可能となり、それぞれの国において改めて施行に伴う措置を行う必要がなくなる。ただし、政治的プロセスやその他の要因により、すべての領域が調和されるわけではなく、各国法により個別に規制される部分も存在する（例えば、国家安全保障、加盟国は、独自の従業員データのプライバシー法を

自由に導入できる)。

#### (1) 日本企業への影響

前述したように、多くの分野において調和されることになるが、依然としていくつかの分野では非調和のままとなる。この非調和の分野に関し影響を受ける製品やサービスを提供する企業は、とりわけ注意が必要である。

#### (2) 管理負担の軽減

前述の調和は管理負担の軽減につながる。規則の下では、国ごとの登録手続や事前承認登録の必要性が削減される。基本的に、データ・コントローラは、データ処理活動の記録管理をすれば足りる。

#### (3) ワンストップショップ

調和の取れたデータ保護体制のもう一つの利点は、「ワンストップショップ」制度の導入である。事業が複数の加盟国で実施される場合に備えて、事業の主要事業所の所在地を管轄するデータ保護当局は、国境を越えた処理のための主導当局として機能する。このデータ保護監督当局はまた、規則に対する違反および規則に関する事業に対する他の苦情処理を管轄する。<sup>(13)</sup>

#### (4) 非調和分野

多くの分野が調和されることになるが、規則の下で調和されていないいくつかの分野が残っている：

- 国家安全保障
- ジャーナリズムと表現の自由
- (加盟国が選択する場合) 雇用法
- 職業的機密に関する法
- 通信の傍受に関する法

なお、加盟国は、電子プライバシー指令(2002/58/EC)の下に傍受法を有している。

### 6. データ・プロセッサの義務

指令とは異なり、規則はデータ・プロセッサに対しても直接的にコンプライアンス義務を課している。

#### 【日本企業への影響】

データ・コントローラとしては機能しないが、

データ・プロセッサとして機能する企業は、規則の下における新たな義務を認識する必要がある。

規則の下でのデータ・プロセッサにとって最も重要な義務は以下の通りである。

- 適切なデータ処理契約の締結
- 監督当局への協力
- 適切なセキュリティ対策の実施
- データ処理記録の維持
- データ・セキュリティ違反に備えた、データコントローラに対する情報開示要件
- 規則の国境を越えたデータ転送要件の遵守  
データ処理活動をアウトソーシングする場合、データ・プロセッサに直接向けられた新たな義務について、データ・コントローラとデータ・プロセッサとの間で交わされたデータ処理契約によって規律する必要がある。規則は、契約において対処する必要がある具体的な点に言及している。データ・プロセッサは、例えば、

- データ・コントローラからの文書化された指令の個人データのみを処理すること
- 個人データを処理することを許可される人物は、機密性の遵守を確約すること
- あらゆる必要なセキュリティ対策を実施すること
- データセキュリティおよび監督当局との協議に関する義務の遵守において、データ・コントローラを支援すること
- 可能な場合、データ・コントローラが個人の権利を尊重するための手配をすること
- 処理の終了後、データ・コントローラにすべての関連する個人データを返却すること
- データ・コントローラや監督当局に対して、処理活動に関するすべての必要な情報の利用を可能にすること

規則は、監督当局によって、直接データ・プロセッサに対して執行される。

### 7. データ主体の権利

規則は、個人についていくつかの既存の権限を強化し(例えば、削除権)、新たな権利を導入する(例えば、データポータビリティ)。全体的に、規則は個人の個人データに対する支配を回復する

ための権利を与えていた。(14)

#### (1) 削除権/忘れられる権利 (Right to be forgotten)

規則によれば、個人は、自身に関する個人データを是正する権利を有する。それに加えて、個人は、係るデータの保持が、データ・コントローラを対象とする規則、連合法、または加盟国の法律を侵害する場合には忘れられる権利 (Right to be forgotten) を有する。忘れられる権利は、欧州司法裁判所のCosteja対Google<sup>(15)</sup>の判決で支持されたように、削除権の一部である。個人は、データ・コントローラに、自身の個人データ、そのコピーまたはデータへのリンクを削除するよう要求することができる。また削除権に基づき、データ・コントローラが第三者に働きかける義務を求めることが可能である。<sup>(16)</sup>

#### (2) データポータビリティの権利

忘れられる権利の次に、データポータビリティの権利という、おそらくより頻繁に使用されるであろう個人が有する権利がある。この権利は、規則によって新たに創出された。個人は、他のデータ・コントローラにデータを転送する権利を有する。データポータビリティの権利は、データ処理が同意に基づくものである、または個人との契約履行において必要であり、処理が自動化された手段により実施される場合において適用される。データ・コントローラは、個人が別のデータ・コントローラにデータを転送できるように、構造化され、一般的に使用され、機械による読み取りが可能で相互運用可能な形式のデータを利用できるようにする必要がある。さらに技術的に可能な場合、個人は、新しいコントローラ宛てに個人データを送信するようデータ・コントローラに要求することができる。なお現時点では、特にインターネットのソーシャルメディア・ネットワーク間では、データの相互運用性はほとんどない。<sup>(17)</sup>

#### (3) 異議を述べる権利

また、事業に多大な影響を与える一つの権利は、異議を述べる権利である。個人は、データ・コントローラの正当な利益に基づいて、またはダイレ

クト・マーケティングの目的のために、公共の利益のために実施されている個人データの処理に異議を述べる権利を有する。企業は、この権利をデータ主体に明示的に知らせる必要があり、個人がこれらの権利行使した場合、企業はその意図されるデータ処理が正当化できるものであるかどうかを再評価する必要がある。

#### (4) プロファイリング

企業に対するもう一つの情報管理上の義務は、プロファイリングに関連するものである。規則は、特に個人データに関して行われる、あらゆるプロファイリング活動について、個人に通知し、係るプロファイリングについて異議を述べる権利を付与する義務が含まれる。<sup>(18)</sup> この義務の範囲を理解するには、プロファイリングに関する規則上の定義に目を向けることが重要である。すなわち、プロファイリング活動とは、自然人に関連する特定の個人的側面を評価するための、個人データの利用からなる個人データの自動処理のいずれかの形式で、特に自然人の職場でのパフォーマンス、経済状況、健康状態、関心、所在地などに関する側面を分析し、また予測することをいう。<sup>(19)</sup>

プロファイリング活動について、個人への通知という新たな義務の背後にある理由は、多くの場合、企業がデータ主体が気づかないうちに、個人の行動を分析することができ、さらに彼らの将来の行動や関心を予測することができるからである。

企業は、現在のすべてのプロファイリング活動について分析し、どの具体的な活動について明示的な同意を必要とするかを判断する必要がある(例えば機密性の高い個人データを使用するプロファイリング活動、および法律によって要求されていないプロファイリング活動について分析する必要がある。)。

その後、現在のプロファイリング活動は適法であるかどうかを評価する必要がある。企業はプロファイリング活動が適法であることを評価するとともに、個人が自らの権利行使できることを保証するために適切な措置を実施していることを確認する必要がある(例えばプロファイリング活動

の対象にならざることを要求する権利を付与すること等)。プロファイリング活動に対応するために必要である適切な同意の仕組みの実施は、いくつかの案件においては最適な解決策ではないかも知れない。企業がほとんどプロファイリング活動を行わない場合には、プロファイリング活動を停止するほうが、経済的に望ましい解決策である可能性がある。

#### (5) 情報に関する通知

規則の下での個人の権利に関して、情報に関する通知は別途重要な項目であり、事業に重大な影響を有する可能性が高い。企業は、個人データの処理に関する情報を、簡潔、透明、明瞭、および容易にアクセスできる形で個人に提供するために、適切な措置を講じなければならない。データが個人から収集される場合、情報に関する通知は、データの収集と同時に提供されるべきである。データが直接個人から収集されていない場合、情報に関する通知は、次のいずれかの方法で提供されるべきである。

- ・収集の前
- ・データの収集後の妥当な期間内（最長1ヶ月）
- ・第三者へ開示する場合
- ・個人との最初のコミュニケーションの場面

規則は、情報に関する通知で提供されなければならない項目を増やすだけでなく、通知に関する要件に従わない場合の制裁についても重いものを課している。すなわち、違反に対しては最大2,000万ユーロまたは世界的年間売上高の4%のいずれか高い方の制裁につながる可能性がある。

企業は、このように自らについて必要となる通知についてよく検討し、必要に応じて通知の内容を更新する必要がある。

### 8. より広い範囲 - 域外適用

従来の制度では、EUデータ保護法の適用は、主に処理活動の場所に依存してきた。これは規則の下では変更される。

#### 【日本企業への影響】

従来、個人データをEUでは処理せず、日本ま

たはその他の国でのみ行った日本企業は、一般的には、EUのデータ保護法の適用はなかった。かかる取り扱いは、規則のもとでは異なる。対象企業がEUに事業所を有するかどうかは、規則の適用関係を決める決定的な要素ではない。

規則は、EUデータ保護法をさらに拡張する、いわば域外適用につながる。データ処理活動が、EUでの事業所の活動に関連して行われる場合、あるいはそのような処理活動がEUでの商品やサービスの提供、またはEUに居住する消費者の行動のモニタリングに関連している場合のいずれかに該当するすべての企業は、規則の対象となる。

ここで「商品やサービスを提供する」とは、例えば、EUにおいてデータ・コントローラまたはデータ・プロセッサのウェブサイトへのアクセス可能性または電子メールの利用可能性以上のものを言うと理解される。一以上の加盟国で一般的に使われる言語または通貨での商品やサービスの注文、さらにはEU内に存在する顧客やユーザーの行動のモニタリングの可能性などの諸要因によって判断されることがある。

「行動のモニタリング」とは、例えば、意思決定を可能にする、または個人的な嗜好を予測するためにプロファイルを適用する技法によって、インターネット上でデータ主体の行動が追跡される場合を言う。

したがって、多くの企業は、規則の適用を視野に入れ、EUに、企業と監督当局間の接点になる担当者を置くことになる。しかし、監督当局は、自由にそれぞれのデータ・コントローラまたはデータ・プロセッサに直接連絡することができることに留意が必要である。

### 9. 意図的またはデフォルトのプライバシー (Privacy by design and default)

規則の下で増加した義務は、いわゆる意図的なプライバシー (Privacy by design) およびデフォルトのプライバシー (Privacy by default) の原則の下でも明らかにされている。企業は、新製品ないしサービスを設計および導入する際には、プライバシーの問題を考慮に入れる必要がある。例え

ば、個人データは意図された目的のために必要な場合にのみ処理されることを保証する必要がある、技術的および組織的措置を設定ないし維持する必要がある。さらに、製品は、当初からプライバシーを考慮した設定を有する必要がある。それに加えて、企業はデータの匿名化と偽名化について検討する必要がある。場合によっては、企業はデータの背後にある個人を特定することなく、個人に関するデータを使用することができる。データの匿名化及び偽名化により、対象データを規則の範囲から除外できる可能性がある。

## 10. データ侵害通知

規則の下で、データ・コントローラは、データ保護監督当局にほとんどのデータ侵害を通知する必要がある。個人的なデータ侵害は、送信、保存、または処理された個人データの偶発的または違法な破壊、紛失、改ざん、不正開示、またはアクセスにつながるセキュリティ違反である。

### 【日本企業への影響】

データ・セキュリティ侵害を受け、当該侵害事実が規則上の制限に該当するあらゆる企業には、規則上の新たな通知義務が課される。

データ保護監督当局への通知は、不合理な遅延なしに行い、可能な場合は、データ侵害の認知から72時間以内に行われなければならない。場合によっては、データ・コントローラは、不合理な遅延なく影響を受けた個人にも通知しなければならない。違反が個人の権利と自由にリスクをもたらす可能性がほとんどない場合、データ保護監督当局に通知する必要はない。<sup>(20)</sup>

この義務の不遵守は、最大1,000万ユーロまたは会社の全世界年間売上高の2%のいずれか高い方の制裁に関する措置を監督当局が執行する場合があるため、すべての企業は、データ侵害を扱うための内部手続を完備すべきである。

データ侵害を扱うためのこれらの内部手続には、本件に関して、社内の人々の具体的な役割や責任の策定、および関係従業員の訓練を含むべきである。さらに、事前に通知の雛形を準備する必要もある。

データ侵害通知義務の遵守が企業に追加の管理上、財政上の負担を強いるとしても、加盟国全体での通知義務の調和により、EUにおける複数の事業体を持つ企業は、データ侵害通知については1件のみ行えば足りることになる。

## 11. コンプライアンス組織/説明責任のためのより強いインセンティブ

### (1) 日本企業への影響

規則は、企業のデータ処理活動が規則に準拠していることを確保するための措置の実施を要求する。規則の遵守は、監督当局および個人ないし顧客に対して実証できる、および時には実証する必要がある。この要件は、多くの日本企業に影響を与えることになる。

規則は、企業における上記の措置を確立するために、データ保護ガバナンスの仕組み、記録、および制御を実施するための様々な義務を課している。これには、会社とデータ処理案に応じて、データ・プロテクション・オフィサー（「DPO」）を任命する、処理活動の記録を維持する、データ保護ポリシーを導入する、行動規範を確立する、およびデータプライバシー影響評価に着手するための各義務が含まれる（「DPIA」）。

現在、データ・コントローラは、データを安全に維持し、データ保護の遵守を保証する組織を有することのみが義務付けられている。このようなコンプライアンス組織をどのように設置、運営しなければならないかについての明示的な規定はない。特に機密性の高いデータ処理操作は、社内のDPOによる内部監視を必要とする。

適切な技術的および組織的対策を実施することにより、データ・コントローラは、当初段階においては、データ量、処理の程度、保管の期間、およびそれらのアクセシビリティの観点から、それぞれの処理の特定の目的のために必要な個人データのみを処理することを保証すべきである。

それぞれの処理作業に応じて、データ・コントローラは、規則に準拠してデータの処理が行われることを保証し、実証することができるように、適切なデータ保護ポリシーを採用する必要がある。

また、個人データの処理が規則に準拠して行われることを確保するために、現実に当該企業において実施可能な技術的および組織的対策が実施される必要がある。

完全で良好なコンプライアンス組織の構築及び運用は、制裁リスクを低減するための大きな要因となるため、企業はコンプライアンス組織の構築およびその運用に十分な投資をする必要がある。

以下では、データ保護ガバナンスの仕組みの実施に関する重要な点のいくつかを検証する。

## (2) データ・プロテクション・オフィサー (DPO)

指令の下では、該当する加盟国の法律で定めない限り、DPOを任命する義務はなかった。規則の下では、DPOは、以下の場合に任命されなければならない。

- ・データ・コントローラの主要活動が機密データの大規模な処理を必要とする場合
- ・データ・コントローラが公共部門である場合、または
- ・データ・コントローラの主要活動が、大規模な体系的監視を伴う場合

DPOに関し、加盟国の法律で追加的要件が規定される可能性がある。

## (3) 行動規範

DPOを任命する必要があるかどうかの確認とは別に、企業は行動規範の確立を検討すべきである。行動規範は、企業がその顧客に対して、当該企業がデータ保護のコンプライアンスを考慮しており、それに関連する責任を真に果たそうとしていることを示すための有効的な方法である。行動規範は、通常、特定の業界やデータ処理カテゴリに固有のものであり、業界におけるベスト・プラクティスの遵守を実証するために使用されている。規則は、例えば、EUデータ保護法の遵守を確保することを目的とした、行動規範の策定を奨励するよう、加盟国に要求している。承認された行動規範に基づくデータ転送が可能であることについて、規則に規定されている。

## (4) データプライバシー保護影響評価 (DPIA)

企業は、場合により、データに関する処理を実施する前に、DPIAを実施する必要があり、特に新たなデータ処理がデータ主体の権利と自由にとって高いリスクにつながる可能性がある場合にはかかる評価が必要とされている。DPIAでは、データ処理に関する活動に関する活動に連携してデータ主体へどのようなリスクがあるかという点が評価され、これらのリスクに対処するための措置が特定されなければならない。特に以下の場合に、DPIAそのものがデータ・コントローラによって行われなければならない。

- ・対象となるデータ処理が新しい技術を用いて導入される場合
- ・対象となるデータ処理が個人の権利に高いリスクをもたらす可能性がある場合
- ・特に以下の場合に必要とされている。
  - ・データに関する個人的側面の体系的かつ広範な評価で、プロファイリングを含む自動処理に基づき、それにより意思決定がされるため、個人に関して法的影響をもたらす、または同様に大幅に個人に影響を与える場合
  - ・特定のデータ・カテゴリの大規模な処理を行う場合（例えば、人種や民族、宗教や哲学的信念に関する処理を行う場合）、または
  - ・公的にアクセス可能な大規模な領域について体系的なモニタリングを実施する場合

企業は、DPIAを行う場合の雛形を準備し、DPIAに従事する従業員に対するトレーニングを実施する必要がある。

## IV. 日本における近時の動き

日本でも、2014年11月にサイバーセキュリティ基本法が成立して以降、関連法制が徐々に整備され、2015年12月には、サイバーセキュリティ経営ガイドラインが制定された。これは、経済産業省及び情報処理推進機構(IPA)が開催した「サイバーセキュリティリスクと企業経営に関する研究会」における検討に基づき、経済産業省・IPA共同で、パブリックコメントを経た上でガイドラインを策定したものである。大企業及び中小企業のうち、ITに関するシステムやサービス等を供給する企業

及び経営戦略上ITの利活用が不可欠である企業の経営者を直接の名宛人とし、経営者が認識する必要がある「3原則」、及び、情報セキュリティ対策を実施するまでの「重要10項目」を提示している。

3原則の中で、経営者はIT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めが必要等と明記し、経営者自身を名宛人としてサイバーセキュリティの責任者であることを唱っている。そして、重要10項目の一つとして、経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取り、サイバーセキュリティリスクマネジメントの方針(セキュリティポリシー)を策定するよう要求している。但し、具体的にどのようなポリシーを策定すべきかの具体的な基準や指針は示されておらず、具体的な内容の策定は、各企業の責任において、その業務内容や扱う情報の種類、性質等により検討する必要がある。また、ポリシーを策定さえすれば足りるものではなく、その運用を適正に行うことこそが肝要である。

これらガイドラインに要求されている事項の遵守は、仮に情報漏洩等により損害が生じて、訴訟・仲裁等が提起された場合に、取締役の情報セキュリティにかかる善管注意義務違反があったか否かの重要なポイントになる可能性がある。もっともこのガイドラインは、あくまで日本政府ないしはその関連機関が策定したものであり、これを遵守さえしていれば、グローバルな意味でのセキュリティスタンダードを満たしたことになるという保障はない。国境を超えたビジネスを行う日本企業としては、技術的にも、法的な意味でも（どのように証拠を残しておくべきかという意味でも）、米欧の法規制を含めてキャッチアップし、対応を取る、ないしは対応を取っているという証拠を残していくことを心掛けなければならない。

## V. まとめと提言

日本の企業が規則の適用に関して準備するための5つの重要事項は次の通りである。

### 1. データ処理機構とマップデータ・フローの分析

- 個人データを処理する法的根拠を分析する。個人の同意が必要か、個人データを処理する上で正当な利益を示すことはできるかについて検討する。

- どの処理/操作が規則によって影響を受けるかを理解する。
- どのシステムが影響を受け、どのような変更が必要とされるかを理解する。

### 2. グループ内のデータ転送および国境を越えたデータ転送

- 規則の影響を受けるグループ内および国境を越えたデータ転送のための現在の法的根拠を調査する。
- 拘束的企業準則の実施を検討する。

### 3. コンプライアンス体制の見直しおよび強化

- データ・プライバシー・ガバナンス構造を導入/データ侵害に対する管理を確立する。ホワイトペーパーを準備する。
- すべての既存のポリシーと手順を確認する。契約書の標準テンプレートを準備する。
- データ侵害の可能性が生じた後で、迅速な反応を保証するために、明確な方針を設定する。
- 従業員の審査（データ保護責任者の候補の検討）・トレーニング。

### 4. 意図的またはデフォルトのプライバシーの採用

- あらゆる製品の設計と開発プロセスの開始段階から、データ保護の問題を考慮に入れるようにする。また、新製品においてプライバシーに考慮したデフォルト設定を検討する。

### 5. 個人の新しい権利を詳しく調べる。

- 規則の下で個人の権利行使のための枠組み作り（例えば、データ・ポータビリティに関する枠組み）。

[注] \_\_\_\_\_

(1) [http://europa.eu/rapid/press-release\\_STATEMENT-16-1403\\_en.htm](http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm).

- (2) [http://europa.eu/rapid/press-release\\_IP-15-6321\\_en.htm](http://europa.eu/rapid/press-release_IP-15-6321_en.htm).
- (3) [http://europa.eu/rapid/press-release\\_IP-15-6321\\_en.htm](http://europa.eu/rapid/press-release_IP-15-6321_en.htm).
- (4) <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>.
- (5) [http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?\\_r=0](http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0).
- (6) <http://blogs.orrick.com/trustanchor/2016/03/02/eu-u-s-privacy-shield-is-gonearly/>.
- (7) [http://europa.eu/rapid/press-release\\_IP-16-433\\_en.htm](http://europa.eu/rapid/press-release_IP-16-433_en.htm).
- (8) [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/2016/press\\_release\\_shield\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf).
- (9) Loidean、Nora Ni、安全港の終了：EUのデジタル・プライバシーおよびデータ保護法への影響、インターネット法律のジャーナル、19第8号 J L. 2016年2月1日。
- (10) [http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).
- (11) [http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm).
- (12) ルース・ボードマン、アリアン・モール、ジェームズ・ミロック、アレクサンダー・デュイスバーグ、ファビアン・ニーマン、ベノイト・ヴァン・アスプロック、一般データ保護規則に関する合意、サイバースペース弁護士NL 4、21 No. 2。
- (13) ルース・ボードマン、アリアン・モール、ジェームズ・ミロック、アレクサンダー・デュイスバーグ、ファビアン・ニーマン、ベノイト・ヴァン・アスプロック、サイバースペース弁護士 NL 4、21 No. 2.
- (14) [http://europa.eu/rapid/press-release\\_IP-15-6321\\_en.htm](http://europa.eu/rapid/press-release_IP-15-6321_en.htm).
- (15) <http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre=>.
- (16) セデリック・バートン、ローラ・デ・ボエル、クリストファー・クナー、アナ・パテラクト、サラ・キャディオット、サラ・G・ホフマン、ブルムバーグ国政局、プライバシーとセキュリティ法律レポート、15 PVLR 153、1/25/16。
- (17) ポール・デ・ハート、バゲリス・パパコンスタンティノウ、新たな一般データ保護規則：それでも個人保護のために健全なシステム？、コンピュータ法&セキュリティ・レビュー32（2016）、189頁、189。
- (18) セデリック・バートン、ローラ・デ・ボエル、クリストファー・クナー、アナ・パテラクト、サラ・キャディオット、サラ・G・ホフマン、ブルムバーグ国政局、

