EUはじめ世界に広がる越境移転規制・域外適用と日本企業の対策

渡辺翔太

CONTENTS

要 約

1 近年、EU（欧州連合）や中国、ASEANなど、日本企業にとって重要な地域で個人情報の越境移転を禁じる法令や域外適用を認める法令・運用が導入されつつあり、マーケティングでの活用や人事データの集約が困難になるなど、日本企業の事業上のリスクとなっている。

2 EUでは「GDPR（EU一般データ保護規則）」が制定され、従来の「データ保護指令」と同様に同意や契約の締結による体制整備などを通じて、移転先がEUと個人情報の保護において同等以上の水準でない限り、EU域外への移転が禁止されている。また、GDPRは域外適用も規定しており、日本に所在する日本企業であっても、越境的なサービスをEUに提供する場合にはGDPRの遵守が求められることとなった。

3 中国やベトナム、インドネシアなどは、個人情報保護をうたいつつ、実質的には必要以上に越境移転を制限する規制を導入することで、インターネット上の情報統制、国内産業の保護や国内のデータセンターへの投資を誘導している。

4 日本企業は以上の傾向を踏まえ、個人情報保護に関する法令上の義務の全体像、および自社の越境移転や社内ルールなどの整備に関する現状を把握し、適切な対処方針を策定すべきである。また、対処方針を実行に移すとともに、継続的にモニタリングしていく必要がある。

Ⅰ「越境移転規制」「域外適用」とは

本稿では､EU（欧州連合）における「GDPR（EU一般データ保護規則）」、およびEU以外の国における個人情報保護に関する法令に関して、特に国際的な側面について企業担当者が押さえておくべきポイントを解説する。法令の国際的側面を押さえる上では、大きく「越境移転規制」および「域外適用」の２つが重要となる。

越境移転規制とは、個人情報保護の制度が十分整っていない国へ情報が移転されることで個人情報の侵害が起きる事態を防ぐため、個人情報の国外移転を規制するものであり、これによって企業は本社への個人データの集約が制限され、グローバルな人事データベースの構築や、データの集約に基づく高度な解析（たとえばWebの閲覧履歴、属性情報を組み合わせた大規模なマーケティング分析など）などができなくなる可能性がある。越境移転規制はEUでは既に1995年の「データ保護指令[注1]」に見られたが、その後、2000年代に入ってシンガポールやマレーシア、ベトナム、インドネシアなどのASEAN諸国や中国、ロシア、トルコなどの新興国に広がりを見せている。

次に域外適用とは、企業が当該国に拠点を持たない場合であっても、当該国・地域の法令を適用することを指す。たとえば日本にのみ活動拠点のある企業が、日本からEU域内に所在するEU市民に対してインターネットを通じてサービスを提供する場合、EUの個人データを取り扱うことに違いはなく、このような越境的活動によって生じるEU市民に対するデータ保護を保つ趣旨である。また、一般に厳しい規制を課される域内企業と、域外適用がない場合には規律を受けない越境的なサービス供給を行う域外企業との競争上の公平（いわゆるレベル・プレイング・フィールド）を保つ趣旨もある。

Ⅱ GDPRにおける越境移転規制と域外適用

2018年５月25日に施行されたGDPRの日本企業に与える影響について、第Ⅰ章で述べた域外適用と越境移転規制という観点から、GDPRの規定内容とその企業活動への影響について論じたい。

1 GDPRの適用範囲

GDPRの適用対象となるのは、原則としてEU域内に管理者（単独または共同してデータ処理の目的及び手段を決定する者）または処理者（委託などに基づき管理者に代わってデータの処理を行う者）が設置されている場合である。この場合、GDPRの前文22項によれば、EU域内にある管理者または処理者の事業所の活動に関連する個人データの処理について、その処理がEU域内で行われたか否かにかかわらずGDPRが適用される。事業所とは法人格の有無を問わないため支店や営業所も含まれ、たとえば本社が日本にある企業のEU域内の出張所職員（EU市民）に関する本社でのデータ処理（たとえば社会保険や健康管理、給与計算など）や、アフターサービスなどを目的とした当該出張所の顧客リストの本社での管理も、GDPRの適用対象となる。

次に、例外的に管理者または処理者の設置にはあたらないがGDPRが域外適用される場

合がある（GDPR第３条第２項）。すなわち、GDPRは①EU域内の個人に対する物品又はサービスの提供、②EU域内の個人に関する行動の監視、に関するデータの処理にも適用を認めている。

ここで、①の物品又はサービスの提供とは、たとえばEC（電子商取引）サイトを通じてEUに対して商品を販売している場合を指すが、GDPRの前文23項によれば、単にEU域内から当該ECサイトにアクセスができるというだけでは認められず、EUをサービスの対象としている意図、たとえばEU域内で流通する貨幣（ユーロなど）での決済、Webサイトの言語がEU域内の公用語（たとえばドイツ語やフランス語など）であること、EUへの発送が可能であることをうたっている、といった要素が必要とされる。従って、日本のEC事業者が英語のWebサイトを構築しており、そこに偶然EU市民がアクセスしただけでは適用はないと思われるが、EU市民への商品発送を明示的に行っているような場合には、事業者がEUへの物品・サービスの提供を行う意図を確認できるので、GDPRが適用され得る。

また、②は前文24項によれば、監視とは個人の嗜好、行動および態度を分析したり予測したりするためのプロファイリングを指し、クッキーなどを含めたWebの追跡なども含まれる。先の例でいえば、適切な商品の推奨を行うため、EC事業者が自社のWebサイトを来訪したEU市民に対してクッキーなどの追跡を行って行動履歴を蓄積しているような場合には、GDPRが適用され得る。ここでは、EU市民をターゲットとする意図がなくとも、GDPRが適用される点に注意が必要である。

そして、GDPRが適用されない場合についても述べておきたい。ここでは特に疑問が寄せられることの多い、インバウンド対応を例として取り上げる。たとえば日本にEUから取引先が来訪し、対面で入手した取引先の名刺などの個人データについては、GDPRの適用を受けない。また、EUからの宿泊客について日本に所在する宿泊施設が対面で受領した場合も同様である。日本国内で完結するやりとりについては、相手がEU市民であるというだけでは、GDPRの適用を受けないという点に留意する必要がある[注2]。また、いうまでもないことではあるが、これらの場合、日本の個人情報保護法の適用は受けるため、同法に則っていることは必要となる。

他方、インバウンドでもGDPRの適用を受ける場合はある。たとえば、アプリを通じたECサイトの利用について、インバウンドで来訪したEU市民に対して、日本でアプリをインストールするとともに個人情報を登録させるが、日本だけではなくEUでも明示的に当該サービスを利用させ、ユーロの利用やアプリのEU各国語版が提供されている場合には、GDPRの適用があり得るというべきである。

2　GDPRにおける越境移転規制

データ保護指令においても、十分性認定、標準契約条項（SCC：Standard Contractual Clauses）や拘束的企業準則（BCR：Binding Corporate Rules）を通じた企業単位の体制整備、同意という３つの例外を除いては越境移転が禁じられていたが、今回GDPRで新たに認証と行動規範が追加された。認証と行動

規範がもたらす企業の越境移転実務への影響については、実際のEU当局の運用を待たなければ評価は難しいが、企業にとっては越境移転規制が緩和される可能性がある。企業担当者は、この５つの例外のいずれかに該当しない限り、EUから日本を含めた域外への個人データ移転を行うことができない点に留意する必要がある。

次に、企業は５つの例外のどれに依拠すべきであろうか。最も簡易なものは自国の取得する十分性認定であり、これはGDPR第45条に基づいて、EUが外国の法制度を調査・分析し、当該国がEUと同程度の個人情報の保護水準にあると認めるものである。日本はEUからの十分性認定取得に向けて個人情報保護法の改正を2015年に行い、現在その最終段階にある。18年７月17日の個人情報保護委員会のステートメントによれば、18年秋頃に十分性認定に必要となる手続きが完了される見込みである[注3]。十分性認定を得た後は、EUからの移転データに対して、個人情報保護委員会の策定するガイドライン上の義務を追加で遵守することで、企業による個人データのEUからの越境移転が可能になる見込みである[注4]。従って、日本がEUから十分性を認定された場合には、越境移転に関する企業の対応は、個人情報保護委員会によるガイドラインの遵守以外は不要となる。もちろん十分性認定のない現在、既に企業がEUからの個人データの越境移転を行っているのであれば、それ以外の例外に依拠する必要がある。

では、十分性認定を控えているため、日本企業にとってそれ以外の４つの例外がまったく不要かというとそうではない。たとえば、グローバルな人事データベースを構築した場合、日本本社のサーバを経由して米国やASEANなどの拠点でもEU個人データが閲覧可能となる場合もある。この場合、日本のほか、閲覧可能なすべての拠点に対して越境移転がなされることとなるため、BCRまたはSCCの締結が第一の選択肢となる。特にSCCは既に定型的な雛形が示されているため、これを締結するだけで（もちろん締結した内容を社内規定や現場の運用に反映させる必要があるが）移転が実施できることとなる。

GDPRで導入された認証や行動規範については、いまだガイドラインなどが示されていないため、ここでは詳細に触れることを控えたい。

また、企業実務にとって重要な点として、越境移転規制の対応のみを行えば足りるものではない点に留意が必要である。前節の適用範囲で述べた通り、EU子会社の収集した個人情報を、本社もGDPRの義務に準拠して取り扱う必要があり、たとえば漏洩時報告やプロセッサの監督などの実体義務については、本社も遵守する必要がある。実体義務の遵守については、本特集の他論考を参照いただきたい。

Ⅲ EU以外の諸外国における越境移転規制と域外適用

第Ⅱ章ではEUでの越境移転規制を見たが、EU以外の諸国においても越境移転規制や域外適用が広がっている。特に日本企業に影響が大きいと目されるのが越境移転規制であり、これは中国やASEAN諸国などの新興国でも導入されつつある。また、特に米国な

表1　代表的な新興国の越境移転規制の導入状況

国名	法令などの名称（通称）	越境移転規制の概要
中国	サイバーセキュリティ法	個人データの国内保管を原則とする。移転が必要な場合には、安全性評価を行う
ベトナム	サイバーセキュリティ法	個人データの国内保管を原則とする。移転が必要な場合には、公安省の定めるルールに従って安全性評価を行う
マレーシア	個人情報保護法	原則として越境移転を禁止するが、マレーシアと同等の水準を有すると当局から認められた国、同意、契約の履行などをその例外とする
シンガポール	個人情報保護法	原則として越境移転を禁止するが、法令や契約などで受領者がシンガポール法と同等以上の義務を負う場合を例外とする
インドネシア	情報通信省規則第20号	越境移転については、情報通信省と移転について協力をする必要がある（本文参照）
ロシア	連邦法No.242-FZ「情報通信網における個人データ処理手順精査においての個々のロシア連邦法令への修正に関する連邦法」	ロシア国内のサーバに個人情報を保管する義務を規定。ただし、国外にミラーサーバを置くなどを妨げるものではない

出所）野村総合研究所「平成29年度EUとの規制協力を推進するための調査（情報の自由な流通及びサイバー空間の公平と平等の確保に向けた調査）報告書[注5]」（経済産業省委託調査）などから作成

どの個人情報保護に関する法令では積極的に域外適用がなされており、この点にも注意が必要である。

1　越境移転規制

日本企業が事業上大きな影響を受け得る、中国、ASEANなどの代表的な新興国で、越境移転規制を導入している主な国は表1の通りである。後に述べる通り、新興国では包括的な個人情報保護法がなく、パッチワーク的にほかの法令の中で個人情報保護についても規定される場合（中国、ベトナムなど）、またはインドネシアのように行政機関が策定する施行令の中で包括的な個人情報保護制度が規定されるといった場合もある点に留意が必要である。

マレーシアとシンガポールについては、日本と同様、包括的な内容を持った個人情報保護法が制定されている。いずれも越境移転規制を含むものであるが、マレーシアについては同等性を認める国として日本を挙げており、日本への移転については問題がない見込みであるが、GDPRで述べたようにASEAN拠点間の共有などでは問題となり得るであろう。また、シンガポールについては同等性を認め得る根拠として法令や契約などを多様に挙げており、ビジネスへの影響に配慮したとみられる規定ぶりとなっている。

他方、ロシア、中国、ベトナム、インドネシアおよびベトナムについては、個人情報保護を目的として掲げるものの、そのデータ移転に対する制限は目的に照らして過剰であり、国内産業の保護や、自国データセンターへの投資など、保護主義的な背景を持つもの

と推測される。

以下、代表的な新興国の越境移転規制の状況について、国別に詳細を見ていくことにする。

(1) 中国

中国で2017年6月に施行された「サイバーセキュリティ法」は、その名前にもかかわらず個人情報保護に関する規定も有している。越境移転との関係では、重要インフラ運営者（後述）に対して、原則個人データを中国国内に保管することを求めており、例外は企業自身の安全性評価に基づく移転である。この安全性評価の具体的な基準は示されていないが、17年4月にパブリックコメントにかけられた、同法の施行令の一つである「個人情報及び重要データ国外持出安全評価弁法（案）」では、規制の対象がネットワーク運営者に拡大されている。

ここで、重要インフラ運営者とは、機能の破壊、喪失またはデータの漏洩に遭遇した場合、国の安全、国民経済と民生、公共の利益に重大な危害を与え得る情報システムの運営者を指し、その解釈は運用を待たなければならないが、文面上は日本企業で該当する企業は少数に限られると思われる。他方、ネットワーク運営者とは社内LANやインターネット上に自社のWebサイトを運営しているなど、およそネットワークを利用している事業者が当てはまり、日本企業のほとんどが該当するものと解される。「個人情報及び重要データ国外持出安全評価弁法（案）」はいまだ確定版の策定に至っていないが、このように施行令によって大幅に義務のかかる範囲が変化し得る点、そしてこのままの流れでは日本企業にも個人データの国内保管義務が課される可能性が高い点に留意する必要がある。

(2) ベトナム

ベトナムについても、以前から中国サイバーセキュリティ法と類似する内容の法令を定めることが報道されてきており、2017年には草案も公表されていたが、18年6月にベトナムのサイバーセキュリティ法案が国会にて可決された。同法は19年1月1日に施行されることとなるが、この中でも個人データの国内保管を原則とし、公安省の評価を経た場合のみ海外に移転できるという、中国に類似する越境移転制限が盛り込まれている。また、ベトナムについては、SNSサイトなどを規制するDecree 72（13年施行）においてサーバの国内設置義務が課されるなど、行政機関が単独で策定・改変できるため融通の利くDecree、Orderなどの施行令によって義務が課されることが多い点に留意が必要である[注6]。

(3) インドネシア

インドネシアもベトナムと同様、施行令において個人情報保護が規定されており、特に表1に記載した2016年の情報通信省規則第20号は、他国の個人情報保護法に相当するような、個人データの取り扱いに関する包括的な一連の義務を定めている。この中では越境移転規制についても定めがあり、事業者は情報通信省と越境移転について協力をする必要があり、具体的には次の行為が必要となる。

①情報通信省に、最低限下記の情報を盛り込んで報告をする

- 移転先の国
- 移転先の名称
- 移転する日

● 移転の理由/目的

②必要な場合、情報通信省の援助を求める

③移転行為の結果を通知する

また、同規則は2018年12月１日から施行されるが、現在は同規則の施行前であるため、この報告義務の詳細な運用は不明である。

(4) ロシア

最後に、ロシアは連邦法No.242-FZ「情報通信網における個人データ処理手順精査においての個々のロシア連邦法令への修正に関する連邦法」において、ロシア国民の個人データは、ロシア国内に設置されたデータベースで管理されることが要求されている。より具体的には、初期データ収集、記録、システム化、集約、集積、アップデート、復旧などの作業は、ロシア国内に設置されたデータベースを利用してなされる必要がある。しかしながら、これらの個人データを同時にロシア国外でも保持することを妨げるものではないとされている。

以上の主要国のほかにも、台湾では2010年、韓国も11年に個人情報保護法を制定し、タイについても個人情報保護法の起草作業が進みつつあり、18年５月には法案が閣議決定されている。閣議決定された法案では、越境移転規制が導入され、移転先が十分な保護水準を有する国であり、後に公表されるガイドラインに沿ったものである場合にのみ移転が認められると規定する。また、法案は域外適用についても規定し、実行行為の一部がタイ域内で行われる、またはタイ域内で効果が発生する、またはし得る場合に域外適用があると定められている。ここでは東アジア、ASEANなどの日本企業の事業展開上重要な新興国において近年越境移転規制が進みつつあること、それらの中には（実際の運用を待たなければならないが）不当に越境移転を規制すると思しきものもあること、特に18～19年にかけて多くの規制が施行される点に注意していただきたい。

また、このような個人情報保護は顧客のみならず従業員情報も含むため、影響の軽重はあるにせよ、実質的にはあらゆる業種に対して影響を持つ点にも注意していただきたい。

2 域外適用

域外適用について明示的に認めた個人情報保護関連の法令は、GDPRを除くと日本の個人情報保護法（75条）などに限られる。しかし、法令が域外適用を明示しないことは、法令が域外適用されないことを必ずしも示すものではない点に注意する必要がある。たとえば、米国には13歳未満の児童のオンライン上の個人情報保護を規定した法令（COPPA：Children's Online Privacy Protection Act）が存在するが、同法を管轄する米国の連邦取引委員会（FTC）は、同法には明示的な域外適用の規定がないにもかかわらず[注7]、海外の事業者でも米国の児童をターゲットとする場合には域外適用があり得るとし[注8]、警告書の送付など海外の事業者への執行事例もある[注9]。

従って、外国をターゲットとして越境的にサービスを提供する場合には、域外適用もあり得る前提で当該国の法令を調査し、対策を進めていく必要がある。

3　過度な越境移転制限への規律

一部の国に見られる過度な越境移転規制は、事業者の活動を阻害するため、業界団体や政府などから大きな批判が寄せられている[注10]。この点について、当面は第Ⅳ章で述べる対策を実施することが必要となるが、他方で、不当なルールそのものを変更させる働きかけを、政府と一体となって進めることも重要である。

このような規制についてはかねてより、国際的な経済関係のルールとの整合が問題となってきた。国際ルールとは、たとえば世界貿易機関（WTO）のサービスの貿易に関する一般協定（GATS）であるが、特に2018年に合意されたTPP11[注11]では、電子商取引において個人情報を含めたデータの過度な越境移転規制が規律されることとなっており、第14.11条において、「事業の実施のために行われる場合には、情報（個人情報を含む）の電子的手段による国境を越える移転を許可する」が、これは「公共政策の正当な目的を達成するため」であって、「恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと」および「目的の達成のために必要である以上に情報の移転に制限を課するものではないこと」を条件として例外が認められているとしており[注12]、許容される越境移転制限の範囲を画定している。

上記のロシアやベトナム、インドネシアの法令は、マレーシアやシンガポールに比べて認められる例外が少ない。また、移転の報告などは個人情報の保護にとって不要な手続きであり、過度な移転制限となる可能性が高く、これら諸国が加盟国であった場合、TPP11協定に反する可能性が高い[注13]。TPP11はベトナム、マレーシアを含むほか、インドネシアも関心を示しており[注14]、1節で挙げた諸国に対して規律を及ぼし得るといえよう。

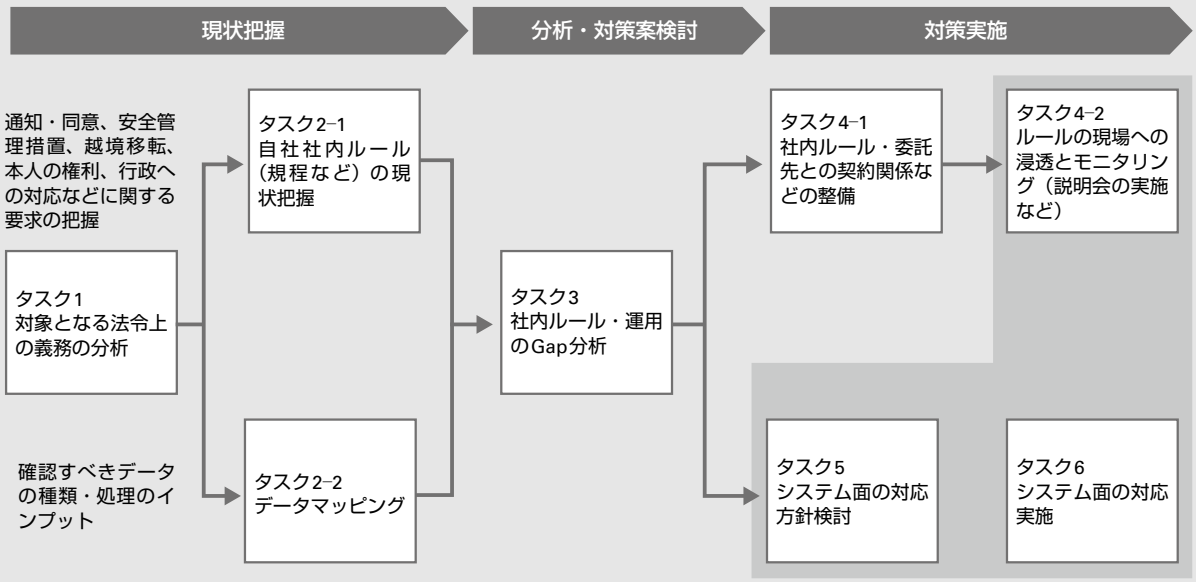
特に日本政府は、国際ルールに基づいて各国に対して措置の是正を働きかけていくことに注力しており[注15]、企業としても日本政府と連携しつつ、各国にルールに基づく是正を促していくことが重要である。このような場としては、個別企業が政府に対して申し入れを行うほか、日本大使館を経由した協議、日系の商工会や地場のものを含めた各種業界団体を通じた現地政府との対話などが考えられる。また、特にマレーシア、インドネシア、ベトナム、タイなどのASEAN諸国については、日本との経済連携協定（EPA）に基づいてビジネス環境上の障壁を幅広く扱う、「ビジネス環境の整備に関する委員会」が設置されており、このような場で取り上げてもらうことも検討に値するだろう。

Ⅳ　越境移転規制に対する日本企業の対応

さて、それでは第Ⅱ、Ⅲ章で見たEUをはじめとする世界各国の越境移転規制に対して、企業はどのように対応すればよいのであろうか。第Ⅲ章3節で述べた通り、国際ルールに反するような不当な法令については、中長期的には日本政府とも連携して是正を求めることが肝要であるが、短期的にはいずれにせよ企業側での対応が必要になる。

野村総合研究所（NRI）では、過去の多数のデータ越境移転に関する調査や民間企業への支援経験から、図1のような流れでデータ

図1　データ関連規制へのコンプライアンス体制整備の進め方



の越境移転規制対応を進めることを提案している。これはGDPRのほか、シンガポールやマレーシアの個人情報保護法、中国サイバーセキュリティ法などの越境移転規制に汎用的に適用できる手法である。

出発点となるのは、法令上の義務の分析（タスク１）である。ここでは、法令そのものに加えて、GDPRであればガイドラインや執行例の分析、新興国の法令であれば頻繁に追加・更新される施行令を踏まえた法令の全体像の理解に基づくものでなくてはならない。自社の法務部のほか、必要に応じて外部の弁護士事務所などを利用して、正確な理解に努めるべきであろう。法令の全体像を把握することで、あるべき姿を描けるようになるからである。

次に実施するのが自社の現状分析であり、具体的にはルール面と運用面の２つから現状を分析する必要があると考えられる（タスク２）。ルール面については、たとえば個人情報保護規程などの社内規程やプライバシーポリシーが挙げられる。また、個人情報保護の関連法令では漏洩時対応や安全管理措置などに関する義務も多いため、たとえば情報セキュリティ規程やインシデント報告などの社内の規程類を確認することも必要になる。

他方、特に重要となるのが運用面の把握であり、具体的には海外の法令で規律されるような海外から日本へ、または海外拠点間の個人データの移転があるか否か、またある場合は、どのような目的のため、どの程度の規模で、どのようなITシステムに、どのような形態で個人データが保管されているかを調査する（データマッピング）。詳細な調査を実施するのは、特にGDPRなどではリスクベースのアプローチが採用されており、リスクに応じた対応が必要となるためである。運用面の現状分析は、法令とITシステムに精通し

た専門家の助言を得ておくことを推奨したい。

現状把握の次は、ルール並びに運用のGap分析（タスク３）である。ここでGapの正確な分析を行うことで、対策を考える際の出発点を構築する。そのため、法令と社内の現状の双方に精通しているチームがこれを実施すべきである。

Gap分析の結果、ルールおよび運用上の問題点（Gapのある部分）が明らかになる。早急に整備しなくてはならないのは、ルール面での整備である。これは各種規定やマニュアルの改定などであり、システムの改修などに比べれば比較的手がつけやすい。不備を指摘する当局側にとっても容易にGapを判断できる部分であるため、真っ先に手をつけておく必要がある（タスク４−１）。しかし、ここで難しいのは、整備したルールを現場に落とし込むことである。えてして社内規程は、法令の内容を正しく反映するために難解な言葉遣いになりがちであり、結果として現場の社員にとって分かりやすいとは言いがたいものとなる。しかし、重要なのは法令を適切に反映した社内規程を一人一人の社員が遵守することであり、現場への浸透に相応の時間とコストをかけるべきである。また、規程類の浸透と並行して、どのように現場への浸透をモニタリングするかについても検討する必要がある（タスク４−２）。適切なGap分析がなされていれば、そこからGapを埋めるToDoを導くことができ、当該ToDoの実施状況を、定期的に各部署について質問表などを送付してモニタリングするなどの手段が考えられる。現場への浸透には時間を要し、また、継続的に取り組まなければ組織に定着しないため、このようなモニタリングは中長期的な視点から継続的に実施することが必要となる。

最後に、システム面の改修も中長期では重要な課題である。まずは、法令に対応するためのシステム改修項目について、Gap分析を基に改修計画を策定する（タスク５）。ここでは特にリスクの高いシステムを優先的に改修するといったことが考えられる。その後、策定したシステムの改修計画を実行に移していく（タスク６）。システム対応のポイントは、法令上の要件をGap分析の結果を踏まえつつ、いかに適切にシステム要件に落とし込むかであり、これは既存のシステム構成や運用実態を踏まえた設計が必要となるため、法令・システム双方に精通した者が行う必要がある。自社内にそのような人材が不足している場合には、適宜外部の人材を用いることを検討すべきである。

また、第Ⅱ章や第Ⅲ章で述べた通り、特に新興国の法令は施行令などの法令の下位規則の形で頻繁に追加・改正され、かつその影響が大きいため、法令の分析とそれを基にした体制整備についても継続して行う必要がある点には注意が必要である。

Ⅴ 世界の動向を踏まえて日本企業に求められること

ここまで述べてきた通り、近年ではEUやASEAN、中国などの日本企業に事業上重要な影響を与える地域において、個人情報保護に関する取り組みが進んでいる。このような取り組みの一環として個人情報の国際的な流通を規制し、特に自国よりも保護水準の劣る国への移転に対して厳しい規制が導入されつ

つある。他方、一部の国はこのような個人情報保護を隠れ蓑として、実質的には自国の国内産業を保護したり、あるいはデータセンターなどへの投資を求めるような規制を導入したりしつつある。後者の保護主義的な規制については、TPP11などのFTA/EPAにおいても一定の規律が及びつつあり、特にTPP11は過度な保護主義を規律する重要な国際協定である。日本企業は、日本政府とも適切に連携しつつ国際ルールに則った制度整備を相手国政府に対して働きかけていくべきである。

他方、企業はいずれにせよ越境移転規制などへの対応が求められる。このような対応措置は法令並びにシステム面、そして現場の運用に関する高度な知見が必要とされるため、NRIの提示するフレームワークなどに従って適宜外部の知見も活用しつつ、対応を進めていくことが重要である。

以上、本稿が日本企業の個人情報保護に関する国際的な側面への対応の一助となれば幸いである。

注

1 正式名称は「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」

2 2018年５月31日に駐日欧州連合代表部で開催されたGDPRセミナーにおける、欧州委員会担当者の発言

3 個人情報保護委員会「熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメント」（https://www.ppc.go.jp/files/pdf/300717_pressstatement2.pdf）

4 いまだガイドラインの最終版は公表されていないが、パブリックコメントにかけられたものとして、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（EU域内から十分性認定により移転を受けた個人データの取扱い編）（案）」を参照

5 http://www.meti.go.jp/policy/mono_info_service/connected_industries/pdf/gdpr02.pdf

6 詳細については、たとえば野村総合研究所「EUとの規制協力：サイバー空間及びIoTに係る規制等に関する調査報告書」（経済産業省委託調査）を参照（http://www.meti.go.jp/meti_lib/report/H28FY/000157.pdf）

7 ただし、同法は事業者（Operator）の定義において海外事業者を含んでいるため、厳密には全く域外適用を想定していないわけではない

8 https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

9 https://www.ftc.gov/news-events/press-releases/2018/04/ftc-warns-gator-group-tinitell-online-services-might-violate

10 たとえば「世界ICT業界12団体によるG20に向けたデジタル経済の発展のための共同提言」（https://www.jeita.or.jp/japanese/public/pdf/20170221_en.pdf）

11 正確には「環太平洋パートナーシップに関する包括的及び先進的な協定」であるが、政府の用語に従い本稿ではTPP11としている（参考：内閣官房「TPP11について」http://www.cas.go.jp/jp/tpp/tpp11/index.html#about）

12 念のため付言すれば、日本とベトナムはTPP11における交換公文において、ベトナムとは第14.11条を協定発効後5年間は紛争解決手続の対象としないことで合意している。しかし、これは紛争解決について規定したものであって、ベトナムがTPP11によって負う国際法上の義務自体には変化がなく、日本としてその他の手段での義務違反の追及を妨げられるものではないと解される。交換公文については、たとえば、川瀬剛志「TPP11（CPTPP）協定の法構造」『JCAジャーナル』（2018年６月号）P.５～６を参照

13 この議論については紙幅の関係上詳細に取り上げないが、日本語ではたとえば次の文献を参照されたい。渡辺翔太「個人情報の越境移転制限に対する規律―国際経済法の果たす役割の模索―」『日本国際経済法学会年報』26号（2017年）

14 インドネシア副大統領「TPP11に参加の意思」（日本経済新聞電子版　https://www.nikkei.com/article/DGXMZO31652000S8A610C100000/）

15 経済産業省『不公正貿易報告書』（2018年版）の序論を参照

著者

渡辺翔太（わたなべしょうた）
ICTメディア・サービス産業コンサルティング部副主任コンサルタント
専門は国際通商および個人情報保護を含む情報通信に関する制度・政策の調査研究、および情報通信産業の海外進出支援（市場調査、事業提携、企業買収など）