



データ越境コンプライアンス実務

Q&A 50 (2025)

環球法律事務所 日本業務チーム 翻訳

2025年5月発行

GLO-JP-Newsletter@glo.com.cn

前書き

デジタル経済の急発展に伴い、重要な生産要素として、また経済成長を牽引する因子として、データは中核的な作用を担っている。データがもたらす経済効果波及を大きく押し上げ、新たな成長戦略を支える基盤として、データ越境流通は、目下、世界経済の成長、テクノロジーイノベーション、貿易取引等の面において、計り知れない商機をもたらしている。一方で、データ越境流通は、データセキュリティ、プライバシー保護といった面での問題も多く抱えており、その規制のための法整備が各国で押し進められている。

中国では、「データ越境安全評価弁法」等の法令等が施行され、データ越境を規制するための骨組みはできたといえるが、まだまだ不明瞭な部分も多い。そのため、データ越境にあたっては、様々な要素(越境元の性質、越境データの類型、累計越境数量等)を考慮して、「データ越境安全評価の申告・合格」、「個人情報越境標準契約の締結・届出」、「個人情報保護認証の取得」のうち、どの適法化手続を選択すべきかを判断する必要がある。2023年9月28日、国家インターネット情報弁公室より「データ越境流通の規範化及び促進に関する規定(意見募集稿)」が公表されると、各界ではデータ越境コンプライアンス措置の選択について様々な議論が行われた。

提出意見をもとに検討が重ねられ、半年後の2024年3月22日、「促進」と「規範化」の順序を逆にした「データ越境流通の促進及び規範化に関する規定」が国家インターネット情報弁公室より公布され、即日施行された。同規定では、データ越境流通の要件が緩和され、それに伴い、データ越境安全評価の適用範囲が狭められている。また、「促進」を前に置くことで、データ越境流通の利便性や企業のコンプライアンスコストの低減への重視を示し、サービス貿易やデジタル経済の成長を加速化させる狙いがあるとみられる。

企業が抱えるデータ越境における主な疑問に回答するために、環球法律事務所データチームは、対外経済貿易大学デジタル経済・法律イノベーション研究センター、蔚来控股有限公司、奇安信科技集团有限公司、北京奥美互動諮詢有限公司、

杭州有贊科技有限公司とともに、「データ越境コンプライアンス実務 Q&A50(2025)」(以下、「本実務 Q&A」という)を作成した。本実務 Q&A は上篇と下篇からなり、上篇(基礎篇)では、主にデータ越境に関連する法体系、用語の定義、注意事項等について解説し、下篇(実践篇)では、データ越境の状況・シチュエーションやデータ類型に関する確認・判断、データ越境安全評価の申告の流れ、リスク評価、リスク対策等について説明を行っている。

なお、本実務 Q&A は当初、中国語版と英語版のみであったが、複数の日本企業・日系企業からの要望を受け、このたび、環球法律事務所日本業務チームが、これまでの日本企業・日系企業へのデータ関連リーガルサービス提供経験を踏まえて、本実務 Q&A の日本語版を作成する運びとなった。

デジタル経済が急成長する中、データ越境に関わるコンプライアンス管理は、事業運営において不可欠な事項となっている。本実務 Q&A が、企業にとって有益な情報として、規範的なデータ越境の発展を推進し、安全、効率的かつ秩序あるデジタル経済の成長に貢献できることを願ってやまない。

最後に、本実務 Q&A の編纂にご協力いただいた皆様に感謝を表す。特に、威科先行の多大なる支援、各専門家からの貴重な意見・提言について、ここに感謝申し上げます。

本実務 Q&A についてご質問等がございましたら、当事務所の下記対応窓口(日本語対応可能)までお問い合わせいただければ幸いです。

日本業務チーム責任パートナー・劉淑珺:liushujun@glo.com.cn

日本業務チーム:GLO-JP-Newsletter@glo.com.cn

目次

上篇:基礎篇

一、	中国のデータ越境に関する法令にはどのようなものがあるか？	1
二、	どのような行為がデータ越境伝送に該当するのか？	8
三、	越境するデータの「国外移転先」はどのように定義するのか？	8
四、	現行のデータ越境制度における3種類のデータ越境適法化手続とは何か？ どの手続を選択するかをどのように判断すべきか？	9
五、	どのような場合に、3種類のデータ越境適法化手続をとることなく、データを 越境することが可能か？	13
六、	「法律、行政法規において別段の定めがある場合、その規定に従い評価/認 可する」とあるが、それは、どのようなデータ越境の状況が想定された規定な のか？	18
七、	どのような場合にデータ越境安全評価の申告が必要となるのか？	19
八、	データ越境安全評価はどのような手順で行うのか？	20
九、	データ越境安全評価の申告にはどの程度の期間を要するか？	23
十、	どのような場合に、個人情報越境標準契約の締結・届出という方法を選択可 能か？	24
十一、	個人情報越境標準契約の締結及び届出はどのような手順で行うのか？	25
十二、	どのような場合に、個人情報保護認証の取得という方法を選択可能か？	27
十三、	個人情報保護認証の取得はどのような手順で行うのか？	29
十四、	CHOによるデータ越境の要件は何か	34
十五、	重要データの識別に関する法令上の根拠はどのようなものがあるか？	36
十六、	重要データ越境の要件には何があるか？	37
十七、	個人情報越境標準契約の具体的な内容はどのようなものか？	38
十八、	個人情報保護認証の具体的な要件は何か？	39
十九、	データ越境制度違反に対する罰則はどのようなものか？	43
二十、	その他、留意すべき事項は？	44
二十一、	個人情報越境に関し、中国の粵港澳大湾区を対象とした特別な便宜的措	

置はあるか？ 45

下篇:実践篇

二十二、データ越境シチュエーションの正確な識別方法は？ 48

二十三、企業が関与する可能性のあるデータ越境伝送のシチュエーションにはどのようなものがあるか？ 54

二十四、越境伝送するデータの種類の正確な識別方法は？ 58

二十五、越境伝送するデータの数量を正確に算定する方法は？ 59

二十六、データ越境伝送に関するコンプライアンス対策の牽引部署はどのように決定すればよいか？ 62

二十七、データ越境安全評価の申告主体はどのように確定すればよいか？ 63

二十八、データ越境安全評価の申告スケジュールはどのように把握すればよいか？ 64

二十九、要件を満たす企業は、どの機関に対してデータ越境安全評価を申告すべきか？ 65

三十、PIA はどのように実施すべきか？ 66

三十一、データ越境リスク自己評価はどのように実施すべきか？ 67

三十二、データ越境伝送におけるPIAとデータ越境リスク自己評価は同一のものか？ 70

三十三、データ取扱者と国外移転先の技術及び制度措置が十分であるか否かは、どのように評価すべきか？ 72

三十四、国外移転先の所在国・地域における法制度及び政策環境の整備状況はどのように評価すればよいか？ 75

三十五、EU はどのように法制度・政策環境を評価しているか？ 79

三十六、データ越境安全評価の有効期間はどれぐらいか？どのような場合に、データ越境安全評価の再申告が必要となるのか？ 81

三十七、どのような場合に、個人情報越境標準契約の再締結及び再届出が必要となるのか？ 82

三十八、監督管理機関が公表している標準契約を締結する際に、その内容を修正することは可能か？ 83

三十九、すでに国外外移転先と「データ取扱契約」を締結している場合、標準契約を

その別紙と位置付けることは可能か？	83
四十、 どの機関に対して個人情報保護認証を申請すべきか？	84
四十一、国際的な紛争解決のためにデータの越境伝送を求められた場合、どのよう に対応すべきか？	86
四十二、中国粵港澳大湾区の個人情報越境標準契約はどのように締結及び届出を 行うのか？	88
四十三、上海自由貿易試験区に、データ及び個人情報の越境に関する優遇措置は あるか？	91
四十四、銀行・金融業のデータ越境に関して注意を要する特別な規定はあるか？ .	93
四十五、証券ファンド業界のデータ越境に関して注意を要する特別な規定はある か？	95
四十六、医薬業界における越境伝送の一般的なシチュエーションにはどのようなも のがあるか？	98
四十七、医薬業界における越境伝送ではどのような種類のデータが伝送されるか？	99
四十八、医薬業界におけるデータ越境伝送に関する義務にはどのようなものがある か？	101
四十九、中国国内のデータ取引所を通じてクロスボーダーデータ取引を行う場合に 考慮すべきデータコンプライアンス上の事項は？	104
五十、 公共データ運営主体が、公共データを国外主体に対して使用許諾又は開 放・共有することはできるか？	106
別紙 1 国家・各地方省レベルインターネット情報機関の連絡先	109



上篇：基礎篇

一、 中国のデータ越境に関する法令にはどのようなものがあるか？

経済のグローバル化及びデジタル化が進むに伴い、データ越境は世界経済の成長を推進する重要な要素となっている。貿易取引、二国間・多国間の技術協力、データ資源の共有といった面で越境データが担う役割はますます大きくなっており、データ越境流通はデジタル経済の発展を推進し、世界を繋ぐ重要な手段となっている。

中国のデータ越境流通の規制は、先進国と比べていささか出遅れた感があるが、目下、法令、機関規則、規範性文書に分散していた統一性に欠ける法規範を整理し、規制体系の整備に向けて急ピッチで取組みが進んでいる段階にあるといえる。

データ越境に関する中国の法律は、2017年6月1日施行の「中華人民共和国サイバーセキュリティ法」(以下、「サイバーセキュリティ法」という)にまで遡る。「サイバーセキュリティ法」は、データ越境安全評価制度を初めて打ち出した法律であり、重要情報インフラ運営者(以下、「CIIO」という)が業務上、確かに個人情報及び重要データを国外提供する必要がある場合は、国家インターネット情報機関と國務院関係機関が共同で制定する規則に従い安全評価を行わなければならない¹と定めている。その後、全国サイバーセキュリティ標準化技術委員会(TC260)(以下、「サイバーセキュリティ標準化委員会」という)が2017年8月30日、「情報安全技術 データ越境安全評価ガイドライン(意見募集稿)」(以下、「安全評価ガイドライン(案)」という)を公表している。これは、後述する「データ越境安全評価弁法」(2022年施行)が公布されるまで、データ越境安全評価の流れ、評価の要点、評価方法等の内容の指針を示すものとして、大いに参考とされた。

2021年9月1日施行の「中華人民共和国データセキュリティ法」(以下、「データセキュリティ法」という)では、CIIOによるデータ越境に関し、「国内の運営中に収集及び生成した重要データ」について安全評価を受ける必要があることをあらためて強調しており、また、その他のデータ取扱者による重要データ越境に対する原則的な規制を設けている²。このほか、「データセキュリティ法」では、国外の司法及び法執行機関に対するデータ提供を規制しており、国内の組織、個人が国外の司法又

¹「サイバーセキュリティ法」第37条。

²「データセキュリティ法」第31条。

は法執行機関に対して中華人民共和国国内に保管するデータを提供する場合には、主管機関の認可を取得することを義務付けている³。後日公布された「中華人民共和国個人情報保護法」(以下、「個人情報保護法」という)でもこの点を受け継ぎ、「個人情報取扱者は、中華人民共和国の主管機関の認可を経ずに、外国の司法又は法執行機関に中華人民共和国国内に保管する個人情報を提供してはならない」と定めている。

2021年11月1日、「個人情報保護法」が施行され、同月、国家インターネット情報弁公室より、「ネットワークデータセキュリティ管理条例(意見募集稿)」(以下、「ネットワークセキュリティ条例(案)」という)が公表された。その第五章では、データ越境に関するセキュリティ管理について、詳細な規定を設けている⁴。「個人情報保護法」第38条及び「ネットワークセキュリティ条例(案)」第35条では、データ越境を適法に行うための3種類の手続、即ち、「国家インターネット情報機関による安全評価の合格」、「国家インターネット情報機関の規定に従って、専門の機構による個人情報保護認証を取得すること」、「国家インターネット情報機関が制定する標準契約に従い、国外の移転先と、両当事者の権利及び義務を定めた契約を締結すること」(以下、3種類の手続を総称して「データ越境制度」という)⁵について定めている。

上述のデータ越境制度の運用を推進するために、その後、国家インターネット情報弁公室及び関連業界の主管監督管理機関より、一連の政策文書が次々と公表されている。

個人情報保護認証については、2022年11月4日、国家市場監督管理総局と国家インターネット情報弁公室が共同で「個人情報保護認証の実施に関する公告」(以下、「認証公告」という)を出している。その別紙「個人情報保護認証実施規則」(以下、「認証規則」という)では、個人情報保護認証を実施するうえでの基本規則が定められ、中国の個人情報保護認証制度が確立されたことを示している。サイバーセキュリティ標準化委員会より2022年6月に公表された「サイバーセキュリティ標準実践ガイドライン-個人情報越境取扱活動安全認証規範」(以下、「認証規範 V1.0」

³「データセキュリティ法」第36条。

⁴「ネットワークセキュリティ条例(案)」第五章。

⁵「個人情報保護法」第38条。

という)では、個人情報保護認証制度の運用を推し進めるための詳細な規定が設けられており、その後、2022年12月、再度、サイバーセキュリティ標準化委員会より公表された「サイバーセキュリティ標準実践ガイドライン-個人情報越境取扱活動安全認証規範 V2.0」(以下、「**認証規範 V2.0**」という)では、法律文書(契約書等)に記載すべき内容、個人情報保護機構(部門・委員会等)の職責、個人情報保護影響評価(以下、「PIA」という)において評価すべき事項、個人情報主体の権利、個人情報取扱者・国外移転先の責任・義務等について、「認証規範 V1.0」よりも更に詳細な要求を定めている。2023年3月16日、サイバーセキュリティ標準化委員会より公表された推奨性国家標準(GB/T)「情報安全技術 個人情報越境伝送認証要求(意見募集稿)」(以下、「**越境認証要求(案)**」という)は、(制定されれば)その規制の効力としては、「認証規範 V2.0」を上回る。「越境認証要求(案)」は、「認証規範 V2.0」の内容を踏襲したものであり、「機微な個人情報」及び「個別の同意」の定義が加えられ、「認証主体」に関連する要件が削除されたほかは、基本的には同じである。「粵港澳大湾区におけるデータ越境流通の促進に関する提携備忘録」及び該当地域の関連法令に基づき、サイバーセキュリティ標準化委員会により2023年11月1日に作成された「サイバーセキュリティ標準実践ガイドライン-粵港澳大湾区個人情報越境保護要求(意見募集稿)」では、粵港澳大湾区(グレーターベイエリア)における個人情報の越境取扱において遵守すべき基本原則及び保護上の要件が定められ、粵港澳大湾区における個人情報保護認証制度の運用における根拠が示されている。2025年1月3日、国家インターネット情報弁公室より公表された「個人情報越境個人情報保護認証弁法(意見募集稿)」(以下、「**認証弁法(案)**」という)では、データ越境適法化手続の一つである個人情報保護認証について、具体的な手続の流れや法的根拠を示している。

データ越境安全評価については、国家インターネット情報弁公室より2022年7月7日に公布され、2022年9月1日から施行されている「データ越境安全評価弁法」(以下、「**評価弁法**」という)において、申告事由、要件等を定めている。個人情報越境標準契約の契約・届出については、国家インターネット情報弁公室より2023年2月22日に公布され、2023年6月1日から施行されている「個人情報越境標準契約弁法」(以下、「**標準契約弁法**」という。)において、当該方法を選択することができる

事由を定めており、また別紙として標準契約の雛形を提供している。

既に土台が完成しているデータ越境制度(即ち、データ越境を適法化する3種類の手続)の最適化・整備を推し進めるため、2024年3月22日、国家インターネット情報弁公室より、これまでのデータ越境規制業務の経験を踏まえた「データ越境流通の促進及び規範化に関する規定」(以下、「越境流通規定」という)が公布された。

「越境流通規定」では、主に次の5つの方面からデータ越境制度について最適化を行っている。1つ目が、重要データの認定基準の明確化、2つ目がデータ越境制度の適用外となるデータ越境の明文化、3つ目が自由貿易試験区ネガティブリスト制度の設置、4つ目がデータ越境制度の適用を受けるデータ越境活動の基準の調整(データ越境流通の規制緩和、データ越境安全評価の適用範囲の縮小)、5つ目がデータ越境安全評価の結果の有効期間の延長である。

また、「越境流通規定」の運用を推し進めるために、国家インターネット情報弁公室より、同日に公表された「データ越境安全評価申告ガイドライン(第二版)」(以下、「評価申告ガイドライン(第二版)」という)及び「個人情報越境標準契約届出ガイドライン(第二版)」(以下、「標準契約届出ガイドライン(第二版)」という)では、データ越境安全評価の申告、個人情報越境標準契約の届出に関する方法、手続の流れ、提出資料等に関する具体的な要求が定められ、データ取扱者が提出すべき関連資料について簡素化が行われている。

「越境流通規定」、「評価申告ガイドライン(第二版)」、「標準契約届出ガイドライン(第二版)」では、主管機関のデータ越境ガバナンスに関する考え方の変化が示されている。即ち、データ流通を法に則った、秩序ある活動にすることで、組織又は個人によるデータの越境に法的な保証を与えるとともに、データの自由な流通を促進することによって、デジタル経済の成長を推し進めるといった目論見がみられる。具体的には、監督管理機関による事前・事中・事後にわたる全プロセスの規制、データ取扱者によるデータ越境時の義務履行の監督・指導(例えば、告知、個別の同意の取得、PIAの実施、技術的措置によるデータセキュリティ保障、省レベル以上のインターネット情報機関その他関係主管機関へのデータ越境セキュリティインシデントの報告等)の強化を明確化する一方、データ越境制度によるデータ貿易の円

滑化を図り、データ越境流通の展開による貿易取引の発展を奨励しており、個人情報又は重要データが含まれないことを前提として、貿易取引、越境輸送、学術協力、国を跨ぐ生産・製造、マーケティング等の活動において発生するデータ越境についてはデータ越境制度の適用外とする等、企業におけるコンプライアンスコストを大幅に軽減している。

国家インターネット情報弁公室より「ネットワークセキュリティ条例(案)」が公表されてから3年近くが経過した2024年8月30日、国務院第40回常務会議において、「ネットワークデータセキュリティ管理条例」(以下、「ネットワークデータ条例」という)が可決し、2024年9月24日に公布、2025年1月1日より施行された。「ネットワークデータ条例」第五章(ネットワークデータの越境伝送に関するセキュリティ管理)に定める主な内容を以下に示す。

1. 国外への個人情報提供に関するコンプライアンスメカニズム

「ネットワークデータ条例」では、「評価弁法」、「標準契約弁法」、「越境流通規定」等の機関規則の制定・運用の成果を踏まえ、ネットワークデータ越境活動における国家インターネット情報機関の機能及び役割が更に明確に示され、データ越境制度の最適化が行われている。「ネットワークデータ条例」第35条では、国外へ個人情報を提供することができる条件として8項目(うち1つは包括条項)を掲げており、そのうちにはデータ越境制度(3種類の適法化手続)だけでなく、「越境流通規定」に定めるデータ越境制度の適用除外事由も盛り込まれている。「ネットワークデータ条例」第36条に定める「中国が参加する国際条約、協定に定める国外への個人情報提供の特段の事由がある場合」も含めると、目下、中国から適法に国外に個人情報を伝送するには、次の9種類の事由のいずれかを満たす必要がある。

(1) データ越境安全評価の合格: 国家インターネット情報機関によるデータ越境安全評価に合格しているとき

(2) 個人情報保護認証の取得: 国家インターネット情報機関の規定に従い、専門機構による個人情報保護認証を取得しているとき

(3) 個人情報越境標準契約の契約: 国家インターネット情報機関が制定した標準契約に従い、国外移転先と契約を締結し、双方の権利及び義務を取決めている

とき

(4) 契約の履行に必要:個人が一方当事者となる契約を締結し、履行するために、確かに国外への個人情報提供が必要なとき

(5) 人的資源管理に必要:法により制定した労働規則・制度及び法により締結した労働協約に従い越境人的資源管理を実施するために、確かに国外に従業員の個人情報を提供する必要があるとき

(6) 法定義務の履行に必要:法定職責又は法定義務を履行するために、確かに国外に個人情報を提供する必要があるとき

(7) 緊急の状況:緊急の状況下において、自然人の生命・健康及び財産の安全を保護するために、確かに国外に個人情報を提供する必要があるとき

(8) 法律、行政法規又は国家インターネット情報機関の定めるその他の条件

(9) 国際条約の規定:中華人民共和国が締結し、又は参加する国際条約、協定に、中華人民共和国国外に個人情報を提供する条件等について規定があるとき

2. 国外への重要データ提供に関するコンプライアンスメカニズム

「ネットワークデータ条例」第 37 条では、「評価弁法」の規定を踏まえ、ネットワークデータ取扱者が中華人民共和国国内での運営中に収集及び生成した重要データを確かに国外に提供する場合、国家インターネット情報機関が手配するデータ越境安全評価に合格しなければならないと定めている。

重要データの認定基準について、「ネットワークデータ条例」では、次の 2 点をあらためて強調している。1 つ目は、中華人民共和国国内での運営中に収集及び生成した重要データを国外に提供するにあたっては、十分な必要性が求められること。そのため、重要データを越境する企業は、自ら評価・論証を行い、「確かに」提供が必要であることの根拠を示す証明性資料を提出する必要がある。2 つ目は、「越境流通規定」の要求に基づき、重要データの認定基準は、地方政府及び業界主管機関の通知又は公告によること。仮にそれらの通知を受けたことがなく、又は公開されている重要データ目録にも自社が取扱うデータが含まれていないのであれば、そのデータを重要データとして扱う(つまり、越境にあたりデータ越境安全評価を申告

する)必要はない⁶。

3. 国外へのデータ提供に係るその他のコンプライアンス義務

「ネットワークデータ条例」第 38 条では、「評価弁法」に定めるデータ越境安全評価の内容に関する要求を踏まえ、ネットワークデータ取扱者はデータ越境安全評価に合格した後、国外に個人情報及び重要データを提供するにあたり、評価時に明確化したデータ越境の目的、方法、範囲及び種類、規模等を逸脱してはならないと定めている。したがって、企業はデータ越境安全評価を受ける際に提出した資料及び国外移転先との契約で取決めた内容に厳格に従い、データ越境活動を展開しなければならない。仮に、安全評価を受ける際に申告した内容を逸脱してデータ越境を行った場合には、国家インターネット情報機関より、「データ越境活動が実際の取扱過程においてデータ越境セキュリティ管理要求に合致しなくなった」とみなされ、「評価弁法」に基づき、データ越境活動の中止を命じられる可能性がある。この場合、データ取扱者がデータ越境活動を引続き展開する必要があるときは、要求に従い改善を行ったうえで、再度評価を申告しなければならない。

このほか、「ネットワークデータ条例」第 39 条では、データ越境におけるセキュリティリスク防止に係るネットワークデータ取扱者の責任があらためて強調されている。具体的には、国がネットワークデータ越境に関するセキュリティリスク及び脅威を防止、対処するための措置を講じるとするだけでなく、ハッカー等による犯罪ツールの拡散を抑制するため、いかなる個人、組織も、技術的措置の破壊、回避に使用する専門のプログラム、ツール等を提供してはならないとしている。また、他人が技術的措置の破壊、回避等の活動に従事していることを知りながら、それに技術的支援又は援助を提供してはならないとしている。同条では、個人又は組織が直接、技術的

⁶ 中国では現在、地方レベルのデータ分類・等級付け保護制度の確立を積極的に推し進めており、データ越境流通のポジティブ/ネガティブリストを制定し、「重要データ」の類型を明確化している。例えば、天津自由貿易試験区より 2024 年 2 月 5 日に公布された「中国(天津)自由貿易試験区企業データ分類・等級付け基準規範」では、データを 13 の大分類、40 の小分類に分け、また等級としては中核、重要、一般の 3 つの等級に分けている。上海臨港新片区より 2024 年 2 月 8 日に公布された「中国(上海)自由貿易試験区臨港新片区データ越境流通分類・等級付け管理弁法(試行)」では、越境データに対し分類・等級付け管理を行うとしたうえで、重要データ目録を制定し、応用・更新メカニズムの管理に関する要件を掲げている。北京市インターネット情報弁公室等 3 機関が 8 月 26 日に公布した「中国(北京)自由貿易試験区データ越境ネガティブリスト管理弁法(試行)」、「中国(北京)自由貿易試験区データ越境管理リスト(ネガティブリスト)(2024 版)」では、自動車、医薬品、小売、民間航空、人工知能の 5 分野が第一群としてリスト入りし、また、各分野においてデータ越境安全評価の合格を要する重要データをリスト化し、18 の子分類及びその基本的な特徴の説明を行っている。

措置を破壊し、回避したわけでもなく、上述の行為があるだけで、「共犯者」として同様に法的責任を負う必要があることを明確にしている。

二、 どのような行為がデータ越境伝送に該当するのか？

「評価申告ガイドライン(第二版)」及び「標準契約届出ガイドライン(第二版)」の「一、適用範囲」では、「データ越境」に該当する 3 つの行為について明確に定めている。

1. データ取扱者が中国国内での運営において収集及び生成したデータを国外に伝送すること
2. データ取扱者が収集及び生成した個人情報を中国国内に保管し、中国国外の機構、組織又は個人が照会、取得、ダウンロード、エクスポートできること
3. 「個人情報保護法」第 3 条第 2 項⁷に定める事由に合致するもの、及び中国国外における中国国内の自然人の個人情報取扱等のその他の個人情報取扱活動

(詳細は「下篇:実践篇 二十二、データ越境シチュエーションの正確な識別方法は？」を参照)

三、 越境するデータの「国外移転先」はどのように定義するのか？

「評価申告ガイドライン(第二版)」では、データが中国国外に移転・保管されていなくとも、国外の機構、組織、個人によりアクセス、閲覧、使用される場合(公開情報、ウェブサイト訪問を除く)は、データ越境に該当する、と定めている。同様に、中国国内の企業が、海外のサービスプロバイダを起用して、中国国外のサーバーを通じて

⁷ 中華人民共和国国外において、中華人民共和国国内の自然人の個人情報を取扱う活動であって、次の各号に掲げる事由のいずれかに該当するものについても、本法を適用する。

(一) 国内の自然人に製品又はサービスを提供することを目的とするもの
(二) 国内の自然人の行為を分析し、評価するもの
(三) 法律、行政法規の定めるその他の事由

中国国内において生成された個人情報¹を直接収集する場合も、データ越境に該当する。

「国外移転先」は、一般的には直接的にデータを受け取る国外の移転先を指す。直接的にデータを受け取る国外の移転先が複数存在する場合、移転元はデータ越境自己評価報告書において、データ越境を要する業務のシチュエーション、越境データの規模、データ取扱の用途、方法、及びデータ移転先の責任・義務を履行するために講じる管理及び技術措置等の要素を考慮して、各移転先における越境データのセキュリティ保障能力をそれぞれ評価する必要がある。また、データが越境された後、さらに他の国外移転先に再移転される場合は、当該再移転行為についても評価する必要がある。

多国籍企業とそのプロバイダの関係は委託・受託の関係である場合が多く、また、ほとんどの場合においては、多国籍企業の本部が直接中国国外のプロバイダに委託し、プロバイダとの間でデータ取扱に関する契約(多国籍企業及びその支店等がデータ取扱者となり、プロバイダがデータ取扱の受託者となる旨定めるもの)を締結する。このような場合において、もし中国国外の親会社が中国国外のサーバーに保管されている中国子会社のデータに自由にアクセス、閲覧することができ、かつ、データ取扱に関する契約においても、中国国外の親会社が国外のプロバイダにより収集されたデータを取扱うことができると定めているときは、当該データ越境においては中国国外の親会社が国外移転先となり、中国の子会社が個人情報を中国国外の親会社に越境したものと解される。

四、 現行のデータ越境制度における 3 種類のデータ越境適法化手続とは何か？どの手続を選択するかをどのように判断すべきか？

「サイバーセキュリティ法」、「データセキュリティ法」及び「個人情報保護法」のデータ三法に基づけば、企業がデータ越境活動を展開する場合、自身が CIO であるか否か、越境データの類型及び数量に応じて、(1)「データ越境安全評価の申告・合格」、(2)「個人情報越境標準契約の締結・届出」、(3)「個人情報保護認証の合

格(取得)」の 3 手続をとる必要があるか否か、とる必要がある場合はいずれをとるべきかを判断しなければならない。詳細については下表を参照されたい。

法律名称	発効日	規制対象	適法化手続	
「サイバーセキュリティ法」	2017年 6月1日	CIO	国外に 個人情報 及び 重要データ を提供する場合、国家インターネット情報機関が国务院関係機関と共同で制定する規則に従い 安全評価 を行わなければならない	
「データセキュリティ法」	2021年 9月1日	CIO	国外に 重要データ を提供する場合、 安全評価 を行わなければならない	
		CIO 以外のデータ取扱者	国外に 重要データ を提供する場合、国家インターネット情報機関が国务院関係機関と共同で制定する弁法に従う	
「個人情報保護法」	2021年 11月1日	CIO	国外に 個人情報 を提供する場合、 安全評価 を行わなければならない	
		CIO 以外のデータ取扱者	取扱う 個人情報 が国家インターネット情報機関の定める数量に達した 個人情報 取扱者	国外に 個人情報 を提供する場合、 安全評価 を行わなければならない
			取扱う 個人情報 が国家インターネット情報機関の定める数量に達しない 個人情報 取扱者	国外に 個人情報 を提供する場合、次のいずれかを選択する (1) 個人情報越境標準契約 を締結し、届出を行う (2) 個人情報安全保護認証 に合格する

表 1 中国データ三法に定めるデータ越境制度

2024年3月22日施行の「越境流通規定」では、上記適法化手続の適用範囲について詳細に定めている。

1. 越境予定のデータが「越境流通規定」第3条から第6条に定める事由(以下、併せて「適用除外事由」という)に該当する場合、企業は、法令に従い、自由にデー

タ越境活動を展開することができる。(詳細は「上篇:基礎篇 五、どのような場合に、3 種類のデータ越境適法化手続をとることなく、データを越境することが可能か？」を参照)適用除外事由に該当しない場合は、以下の 2~4 に従い、判断することができる。

2. CHIO の場合、中国国外に個人情報又は重要データを提供するにあたっては、所在地の省レベルのインターネット情報機関を通じて、国家インターネット情報機関にデータ越境安全評価の申告を行わなければならない。

3. CHIO 以外のデータ取扱者の場合、まず関係機関、地方政府により告知又は公表された情報に基づき、越境予定のデータが重要データに該当するか否かを判断し、越境データが重要データに該当する場合には、データ越境安全評価を申告しなければならない。

4. CHIO 以外のデータ取扱者であり、越境するデータが個人情報である場合、

(1) 当年 1 月 1 日から中国国外に提供した個人情報(機微な個人情報を含まない)が累計で 100 万人分以上、又は機微な個人情報が累計で 1 万人分以上であるときは、データ越境安全評価を申告しなければならない。

(2) 当年 1 月 1 日から中国国外に提供した個人情報(機微な個人情報を含まない)が累計で 10 万人分以上 100 万人分未満、又は機微な個人情報が累計で 1 万人分未満であるときは、法により国外移転先と個人情報越境標準契約を締結し、又は個人情報保護認証に合格しなければならない。

以下、企業における判断の便宜のために、図 1 にてデータ越境適法化手続の判断フローチャートを示し、表 2 にて各データ越境適法化手続の適用事由について整理する。

データ越境コンプライアンス実務 Q&A50(2025)

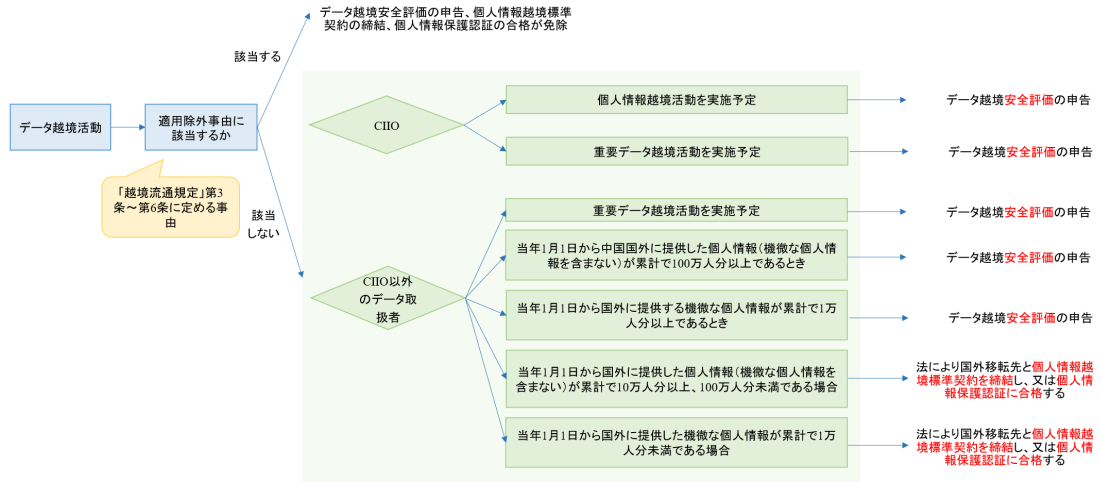


図1 「越境流通規定」に基づくデータ越境適法化手続判断フローチャート

		関係する個人の数量			
越境主体	データの類型	<10,000	≥10,000, <100,000	≥100,000, <1,000,000	≥1,000,000
C/O	重要データ	データ越境安全評価の申告			
	個人情報	データ越境安全評価の申告			
C/O 以外のデータ取扱者	重要データ	データ越境安全評価の申告			
	機微な個人情報	個人情報越境標準契約の届出、又は個人情報保護認証の合格	データ越境安全評価の申告		
	機微な個人情報を含まない一般個人情報	データ越境安全評価の申告、個人情報越境標準契約の締結、個人情報保護認証の合格が免除される	個人情報越境標準契約の届出、又は個人情報保護認証の合格	データ越境安全評価の申告	

表2 各データ越境適法化手続の適用事由

五、 どのような場合に、3 種類のデータ越境適法化手続きをとることなく、データを越境することが可能か？

「越境流通規定」第 3、4、5、6 条では、中国国外において収集及び生成した個人情報在中国国内に伝送し、処理後に中国国外に提供する場合において、処理過程において、中国国内の個人情報又は重要データを導入しないときは、データ越境適法化手続きをとる必要はないとしている。

1. 個人情報の一時的越境(中国語: 过境)

「越境流通規定」第 4 条では、中国国外において収集及び生成した個人情報を中国国内に伝送し、処理後に中国国外に提供する場合において、処理過程において、中国国内の個人情報又は重要データを導入しないときは、データ越境適法化手続きをとる必要はないとしている。例えば、中国国内のある電子商取引プラットフォームが、中国国外に物流拠点を有しているとする。中国国外の消費者が当該プラットフォームから商品を購入した後、プラットフォーム内事業者は商品の郵送を中国国外の物流会社や航空会社に依頼し、これら物流会社や航空会社が商品を輸送し、消費者に引き渡す。このような過程においては、中国国内の電子商取引プラットフォーム、プラットフォーム内事業者、物流会社、航空会社等がいずれも消費者個人情報の取扱いに関与する。中国国外の消費者の注文情報は電子商取引プラットフォームの中国国外拠点によって収集され、中国国内に移転されたものであり、ユーザーアカウントも当該国外拠点によって運営・管理されているため、中国国外の消費者個人情報の収集は中国国内で行われたものではなく、処理過程において、中国国内消費者の個人情報が導入されることはない。したがって、「越境流通規定」第 4 条に基づけば、上記のようなケースでは、電子商取引プラットフォームがデータ越境適法化手続きをとる必要はない。

2. 人的資源管理のために、従業員の個人情報を越境することが必須である場合

「越境流通規定」第 5 条第 1 項第 2 号では、法により制定した労働規則・制度及び法により締結した労働協約に従い越境人的資源管理を実施するために、確かに

中国国外に従業員の個人情報を提供する必要がある場合には、データ越境適法化手続きをとる必要はないとしている。ただし、この事由に基づいてデータ越境適法化手続きの免除を得ようとする場合は、自社におけるデータ越境の状況を精査し、従業員個人情報の越境が人的資源管理のために「確かに必要」であることを確保する必要がある。

3. 個人が一方当事者となる契約の締結・履行に必須である場合

「越境流通規定」第5条第1項第1号では、「個人が一方当事者となる契約を締結し、履行するために確かに必要である」ことを前提として、確かに中国国外に個人情報を提供する必要があるときは、データ越境適法化手続きをとる必要はないとしている。同号では、「契約を履行するために確かに必要である」ケースの例として、越境ショッピング、越境郵送、越境送金、越境支払、越境口座開設、航空券・ホテルの予約、査証手続、検定試験サービス等を挙げている。例えば、消費者が国際金融商品に投資する場合、契約上の要件や法律又は業界の規制要件を満たすために、投資家の氏名、身分証明書情報、連絡先情報、財務状況等の個人情報を外国に提供することが必要となるが、これは「契約を履行するために確かに必要である」ケースに該当しうると考えられる。

4. 緊急な状況において、自然人の生命・健康及び財産の安全を保護するために、確かに必要である場合

「越境流通規定」第5条第1項第3号では、緊急の状況において、自然人の生命・健康及び財産の安全を保護するために、確かに中国国外に個人情報を提供する必要があるときは、データ越境適法化手続きをとる必要はないとしている。例えば、ある国で突発的な感染症の流行が発生した場合、人々の安全を確保するために、特定の組織が患者の個人情報を国際救援機関に送信し、当該感染症の発生原因、他の国・地域で同様又は類似の感染症が発生しているか否か、流行地域における医薬品の供給状況、必要な救援措置等についてやり取りすることが本適用除外事由に該当しうると考えられる。

5. 国際貿易

「越境流通規定」第 3 条では、国際貿易において収集及び生成したデータを国外に提供する場合において、個人情報又は重要データを含まないときは、データ越境適法化手続をとる必要はないとしている。例えば、中国国内の対外貿易企業が他国に対し商品を輸出する場合、税関対応や物流会社による輸送、取引先への引き渡し等を円滑に行うために、輸出商品の数量、仕様、重量、金額、輸送方法等の情報を輸出先に提供することが必要となるが、これは本適用除外事由に該当しうると考えられる。ただし、「国際貿易」の概念は非常に幅広いため、どのような種類の商業活動が「国際貿易」に該当するのか、一連のプロセスの中のどのステップが「国際貿易」に該当するのか、国外移転先は輸出先に限られるのかといった問題については現時点必ずしも明確ではなく、より詳細な説明が待たれる。

6. 越境輸送

「越境流通規定」第 3 条では、越境輸送において収集及び生成したデータを国外に提供する場合において、個人情報又は重要データを含まないときは、データ越境適法化手続をとる必要はないとしている。よくある例としては、中国国内の消費者が電子商取引プラットフォームで中国国外の店舗から商品を購入する場合がある。発送元は中国国外であり、商品は中国国外から中国国内へ国境を越えて輸送されるが、この過程においては、輸送上の必要から、電子商取引プラットフォームが中国国内の消費者の住所や連絡先等の個人情報を中国国外の輸送業者に提供することがあり、そのようなケースは本適用除外事由に該当しうると考えられる。しかし、「越境輸送」の概念は非常に幅広く、日常的な電子商取引プラットフォームでの取引に伴う物品の輸送だけでなく、鉱石資源や農産物、原油等の非小売商品の国際長距離輸送等、より複雑な輸送シチュエーションも「越境輸送」に含まれる可能性がある。これらのシチュエーションがすべて適用除外の範囲に含まれるか否かは、更なる検討が必要となる。

7. 学術協力

「越境流通規定」第 3 条では、学術協力において収集及び生成したデータを国外に提供する場合において、個人情報又は重要データを含まないときは、データ越境適法化手続をとる必要はないとしている。例えば、中国国内のある大学が、中国

国外の研究者と協力して学術研究を行っており、実験結果、調査結論、統計データ等の、個人情報や重要データを含まないデータを共有する場合はこれに該当しうると考えられる。ただし、「学術協力」は幅広い概念であり、一部の産業分野のデータは、個人情報や重要データに該当しなくとも、それが大規模な統計データや機密データであれば「情報」(中国語: 情報)、「国家機密」等に該当する可能性がある。また、学術協力のシチュエーションで越境される学術データが重要データや国家機密に該当しないことをどのように識別するかも、難しい課題となる。したがって、本適用除外事由に該当することを根拠として、データ越境適法化手続をとることなく越境を行うとする場合は、国家安全や社会の利益に危害を及ぼさないよう、慎重な対応が必要となる。

8. 国を跨ぐ生産・製造

「越境流通規定」第 3 条では、国を跨ぐ生産・製造において収集及び生成したデータを国外に提供する場合において、個人情報又は重要データを含まないときは、データ越境適法化手続をとる必要はないとしている。例えば、製造業を営む中国国有企業が世界各国に生産拠点を設置し、製品の製造・組立を行っている場合、海外拠点に対して効果的なサプライチェーンマネジメント・速やかな資材供給を行うためには、資材在庫管理情報、部品生産計画、物流・輸送情報等のデータを海外拠点に提供する必要があるが、これは本適用除外事由に該当しうると考えられる。ただし、「国を跨ぐ生産・製造」は幅広い概念であり、複数のプロセス・様々な関与者からなるものであるため、その中でやり取りされるデータの流れも複雑なものとなる可能性がある。したがって、本適用除外事由に該当することを根拠として、データ越境適法化手続をとることなく越境を行うとする企業は、コンプライアンス基準をさらに検討する必要があり、また、疑問がある場合は速やかに規制当局に相談することが望ましい。

9. 国を跨ぐマーケティング

「越境流通規定」第 3 条では、国を跨ぐマーケティングにおいて収集及び生成したデータを中国国外に提供する場合において、個人情報又は重要データを含まないときは、データ越境適法化手続をとる必要はないとしている。例えば、製造業を営む

多国籍企業が、中国市場への参入や中国市場での事業拡大を予定する場合、中国国内市場の調査を実施するのが一般的である。この場合、企業は消費者ニーズや市場競争の状況、市場動向等を十分に理解するために、市場調査報告書や同業他社の市場シェアデータ、消費者行動データ等、数多くの市場データを中国国内で収集し、国外に越境伝送することになるが、これは本適用除外事由に該当しうると考えられる。

10. その他の一般データ

「越境流通規定」第3条では、先述の5から9以外のシチュエーションにおいても、データ越境適法化手続が不要となりうる余地を残している。具体的には、同条では「国際貿易、越境輸送、学術協力、国を跨ぐ生産・製造及びマーケティング等の活動において収集及び生成したデータを国外に提供する場合において、個人情報又は重要データを含まないときは、データ越境安全評価の申告、個人情報越境標準契約の締結、個人情報保護認証の合格を免ずる」と定めており、この中の「等の活動」という文言によって、データ越境適法化手続が不要となるのが先述の5から9のシチュエーションに限られないことを示している。ただし、先述の5から9に類似するシチュエーションにおける一般データの越境伝送であればデータ越境適法化手続が不要となるのか、「等の活動」には具体的にどのようなものが含まれるのか、先述の5から9以外のシチュエーションに対し実務上どのように同条の類推適用がなされるのかについては現時点必ずしも明確でなく、今後の事例公表等による明確化が待たれる。

11. 「自由貿易試験区ネガティブリスト」に掲載されるデータ

「越境流通規定」では、先述の1から10のほか、「自由貿易試験区ネガティブリスト」に掲載されるデータに関する特別規制を設けている。具体的には、自由貿易試験区は、国のデータ分類・等級付け保護制度の枠組みのもとで、自区内においてデータ越境安全評価、個人情報越境標準契約、個人情報保護認証の管理範囲に組入れる必要があるデータのリストを自ら制定し、省レベルのサイバーセキュリティ情報化委員会の認可を経た後で、国家インターネット情報機関、国家データ管理機関に届け出ることができる、としたうえで、自由貿易試験区内のデータ取扱者が

国外にネガティブリストに含まれていないデータを提供する場合、データ越境安全評価の申告、個人情報越境標準契約の締結、個人情報保護認証の合格を免ずることができる」と定めている。

六、 「法律、行政法規において別段の定めがある場合、その規定に従い評価/認可する」とあるが、それは、どのようなデータ越境の状況が想定された規定なのか？

企業は、データ・サイバーセキュリティ体系を構築するうえで、「サイバーセキュリティ法」、「データセキュリティ法」、「個人情報保護法」だけでなく、他の関連法令に定める内容についても注意を払う必要がある。例えば、次の法令等が挙げられる。

「国家秘密保持法」第37条の規定に基づけば、国家機関や国家秘密に関わる単位(以下、「**機関・単位**」という)が、国外又は中国国内に設立された国外の組織・機構に国家秘密を提供する場合や、任用・起用する国外の人員が、業務の必要により国家秘密を知ることになる場合には、国の関連規定に従い手続をとらなければならない。また、同法第42条の規定に基づけば、国家秘密にかかわる貨物、サービスを購入する機関・単位、直接国家秘密にかかわる工事建設、設計、施工、監理等の単位は、国家秘密保持に関する規定を遵守しなければならない。機関・単位が、企業・事業単位に委託し、国家秘密に関わる業務に従事させる場合、秘密保持契約を締結し、秘密保持を要求し、秘密保持に係る措置を講じなければならない。

ヘルスケア分野のビッグデータについては、「国家健康医療ビッグデータ基準、安全及びサービス管理弁法(試行)」第30条の規定に基づき、中国国内の安全かつ信頼できるサーバーに保管しなければならないが、業務の必要により確かに国外に提供する必要がある場合には、関連法令及び関連要求に従い、安全評価の審査を受けなければならない。

測量・製図の成果に関わる場合、「測繪法」第34条の規定に基づき、国家秘密に該当するものについて、秘密保持に係る法律、行政法規の規定が適用される。対

外的に提供する必要がある場合には、国務院及び中央軍事委員会が定める審査・認可手続を踏まなければならない。

ヒト遺伝資源情報に関わる場合には、「生物安全法」第 57 条の規定に基づき、国外の組織・個人及びそれらが設立又は実質的に支配する機構に提供し、又は自由に使用させるときは、事前に国務院科学技術主管機関に報告し、情報のバックアップを提出しなければならない。

七、 どのような場合にデータ越境安全評価の申告が必要となるのか？

「越境流通規定」及び「評価申告ガイドライン(第二版)」に基づけば、データ取扱者が中国国外に提供するデータが、「越境流通規定」に定めるデータ越境安全評価の適用除外事由に該当しない場合において(詳細は「[上篇:基礎篇 五、どのような場合に、3 種類のデータ越境適法化手続をとることなく、データを越境することが可能か?](#)」を参照)、以下のいずれかの事由に該当するときには、データ越境安全評価を申告しなければならない。

1. CIO が中国国外に個人情報又は重要データを提供するとき
2. CIO 以外のデータ取扱者が、中国国外に重要データを提供するとき
3. CIO 以外のデータ取扱者が当年 1 月 1 日から中国国外に提供した個人情報(機微な個人情報を含まない)が累計で 100 万人分以上であるとき
4. CIO 以外のデータ取扱者が当年 1 月 1 日から中国国外に提供した機微な個人情報が累計で 1 万人分以上であるとき

また、「越境流通規定」では、「自由貿易試験区は、国のデータ分類・等級付け保護制度の枠組みのもとで、区内においてデータ越境安全評価、個人情報越境標準契約、個人情報保護認証の管理範囲に組入れる必要があるデータのリスト(以下、「ネガティブリスト」という)を自ら制定し、省レベルのサイバーセキュリティ情報化委員会の認可を経た後で、国家インターネット情報機関、国家データ管理機関に届け

出ることができる。自由貿易試験区内のデータ取扱者が国外にネガティブリストに含まれていないデータを提供する場合、データ越境安全評価の申告、個人情報越境標準契約の締結、個人情報保護認証の合格を免ずることができる」と定めている。

八、 データ越境安全評価はどのような手順で行うのか？

データ取扱者がデータ越境安全評価の申告を円滑に行えるよう、国家インターネット情報弁公室はこれまでの申告業務経験を踏まえた「評価申告ガイドライン(第二版)」を発表し、データ取扱者の要提出資料を最適化・簡素化するとともに、「データ越境申告システム」を開設した。

「評価申告ガイドライン(第二版)」によれば、データ越境安全評価の申告は、オンライン申告及びオフライン申告の2種類に分けられる。

オンライン申告は、一般的に、CIO以外のデータ取扱者によるデータ越境安全評価の申告に適用される。例えば、当年1月1日から国外に提供した個人情報(機微な個人情報を含まない)が累計で100万人分以上である場合、申告はオンラインで行うことになる。

一方、CIOによるデータ越境安全評価、又はその他のオンライン申告に適しないデータ越境安全評価については、オフライン申告で行われる。ただし、「その他のオンライン申告に適しないデータ越境安全評価」が具体的に何を指すかは現時点必ずしも明確でなく、関係当局による更なる説明が待たれる。

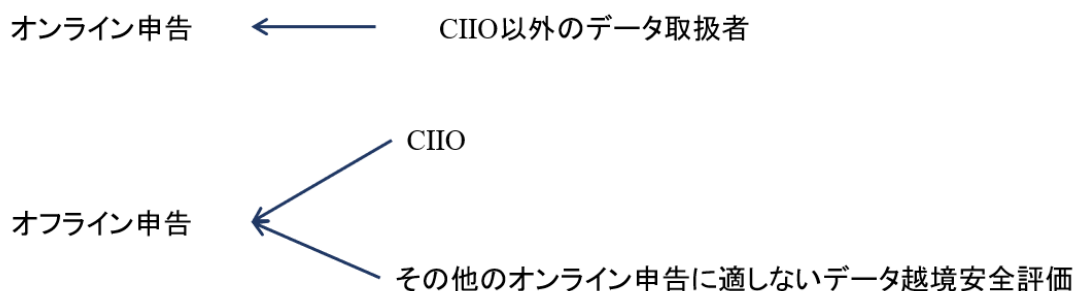


図2 データ越境安全評価の申告方法の適用範囲

1. オンライン申告の流れ

オンライン申告の場合、データ取扱者はデータ越境申告システムを通じて申告資料を提出しなければならない。システムの URL は <https://sjcj.cac.gov.cn> である。システムに掲載されている「データ越境申告システムの使用説明(第一版)」によると、データ越境安全評価の申告と個人情報越境標準契約の届出はいずれも同システムを通じて行う。個人情報保護認証の申請については、現時点では同システムを通じて行うことはできないが、今後対応される可能性がある。現時点、個人情報保護認証を申請する場合は、個人情報保護認証システム <https://data.isccc.gov.cn>⁸を通じて行う必要がある。

データ取扱者は正式に評価の申告を行う前に、「評価申告ガイドライン(第二版)」第3条、及び「データ越境申告システムの使用説明(第一版)」に従い、以下の書類を準備しなければならない。

- 統一社会信用コード証明書の写し(社印押印済みのもの)
- 法定代表者の身分証明書の写し(社印押印済みのもの)
- 手続者の身分証明書の写し(社印押印済みのもの)
- 手続者の授権委託書、誓約書
- データ越境安全評価申告表
- データ越境に関する契約又はその他の法的効力を有する文書の写し(社印押印済みのもの)
- データ越境リスク自己評価報告書の写し

上記書類の準備完了後、データ取扱者はデータ越境評価システムにアクセスし、「ユーザーアカウント登録→システム使用環境設定→新規評価記入ページを選択」という流れでデータ越境評価申告を行う。

(1) ユーザーアカウントの登録にあたっては、データ取扱者は統一社会信用コード証明書、法定代表人身分証明書、システム登録者の身分証明書、登録に係る授権委託書等の書類の電子版又は写真を準備しておかなければならない。申告を行う主体が個人である場合、「法定代表者の情報なし」を選択し、システムの案内

⁸「データ越境流通の促進及び規範化に関する規定」に関する記者質問への回答. 網信中国.https://mp.weixin.qq.com/s/-Y-dY_HL21jHTFQsMbeiVQ

に従って必要な情報を記入する。

(2) システム使用環境の設定においては、データ取扱者は自身の実情に基づき、三種類のユーザー認証方法(ショートメッセージによる認証、プロフェッショナルブラウザとソフト証明書による認証、Ukeyによる認証)のいずれかを選択することができる。

(3) 「データ越境評価管理」-「新規評価」をクリックして新規評価の申告画面に入り、安全評価申告資料をアップロードしたうえで、システムの案内に従い、申告情報を記入する。より具体的には以下のステップがある。

- データ越境安全評価申告の適用事由に該当するか否かの確認
- データ取扱者の状況の記入
- 法定代表者情報の記入
- データセキュリティ責任者及び管理機構情報の記入
- 手続者情報の記入
- データ取扱者における中国の法律、行政法規、機関規則の遵守状況の記入
- データ越境シチュエーションの記入
- その他のデータ越境安全評価申告資料のアップロード

2. オフライン申告の流れ

CHIO がデータ越境安全評価の申告を行う場合、又はその他のオンライン申告に適しないデータ越境安全評価については、オフラインで申告を行う。申告先は所在地のインターネット情報弁公室であり、「評価申告ガイドライン(第二版)」に従い以下の資料を製本のうえ、電子版資料を付して提出しなければならない。

- 統一社会信用コード証明書
- 法定代表者の身分証明書の写し
- 手続者の身分証明書の写し
- 手続者の授権委託書
- データ越境安全評価申告書
- 国外移転策と締結予定のデータ越境に関する契約又はその他の法的効力を有する文書

- データ越境リスク自己評価報告書
- その他の関連する証明資料

九、 データ越境安全評価の申告にはどの程度の期間を要するか？

「評価申告ガイドライン(第二版)」では、データ取扱者によるデータ越境安全評価の申告について、オンライン申告とオフライン申告で異なる所要期間を設定していない。データ越境安全評価の申告に要する期間は、一般的には図 3 のとおりである。



図 3 データ越境安全評価の申告に要する期間

「評価申告ガイドライン(第二版)」第 2 条によると、省レベルのインターネット情報弁公室は、申告資料の受領日から 5 営業日以内に完全性検査を完了し、データ取扱者に検査結果を告知する。完全性検査に合格した場合、省レベルのインターネット情報弁公室は申告資料を国家インターネット情報弁公室に提出する。完全性検査に不合格となった場合、省レベルのインターネット情報弁公室は不合格理由をデータ取扱者に告知する。

国家インターネット情報機関は、省レベルのインターネット情報弁公室から提出された申告資料の受領日から 7 営業日以内に、受理するか否かを決定のうえ、書面によりデータ取扱者に通知する。「評価弁法」第 12 条によると、国家インターネット情報機関は、データ取扱者に書面による受理通知書を発送した日から 45 営業日以内に、データ越境安全評価を終了しなければならない。

評価において、状況が複雑なとき、又は資料の補充、訂正の必要があるときは、国家インターネット情報弁公室は評価期間を適切に延長し、データ取扱者に予測される延長期間を告知することができる。データ取扱者が正当な理由なく、資料を補

充、訂正しない場合、国家インターネット情報弁公室は安全評価を終了することができる。評価完了後、国家インターネット情報弁公室はデータ取扱者に評価結果通知書を交付する。データ取扱者はデータ越境セキュリティ管理に関する法令及び評価結果通知書の関連要求に従い、データ越境安活動を規範化しなければならない。データ取扱者は、評価結果について異議がある場合、評価結果通知書受領日から15営業日以内に、国家インターネット情報弁公室に再評価を申立てることができる。再評価の結果は最終結論となる。

十、 どのような場合に、個人情報越境標準契約の締結・届出という方法を選択可能か？

「越境流通規定」により、データの越境流通の条件が適度に緩和され、従来では個人情報越境標準契約の締結が必要とされていた要件が調整された。具体的には、「越境流通規定」及び「標準契約届出ガイドライン(第二版)」に基づけば、以下の事由に同時に該当する場合であって、「越境流通規定」の定める適用除外事由(詳細は「上篇:基礎篇 五、どのような場合に、3種類のデータ越境適法化手続きをとることなく、データを越境することが可能か?」を参照)に該当しないときは、個人情報越境標準契約を締結し、届け出ることにより、中国国外へ個人情報を提供することができる。

1. CHIO 以外のデータ取扱者であること
2. 当年 1 月 1 日から国外に提供した個人情報(機微な個人情報を含まない)が累計で 10 万人分以上、100 万人分未満であること
3. 当年 1 月 1 日から国外に提供した機微な個人情報が累計で 1 万人分未満であること

なお、重要データであることが関係機関又は地方政府により告知又は公表されている個人情報を国外提供する場合は、データ越境安全評価の申告を行わなければならない。個人情報越境標準契約の締結・届出又は個人情報保護認証の取得という方法を通じて国外提供をすることはできないため、注意が必要である。

十一、個人情報越境標準契約の締結及び届出はどのような手順で行うのか？

個人情報取扱者が個人情報越境標準契約の届出をルール通りに行えるように、国家インターネット情報弁公室により従前の届出実務を踏まえて作成・公表された「標準契約届出ガイドライン(第二版)」では、個人情報越境標準契約の届出の適用範囲、届出方法、届出手順及び資料、問い合わせ先・通報先等の具体的な事項について改めて説明されている。

標準契約の届出手順は、以下のように整理できる。

「PIA の実施及び契約の締結 → 資料の提出 → インターネット情報弁公室による資料確認及び届出結果のフィードバック → 補充又は再届出 → 届出完了 → 個人情報越境活動の開始」

各段階の時間的制約及び詳細なフローは図 4 に示すとおり。

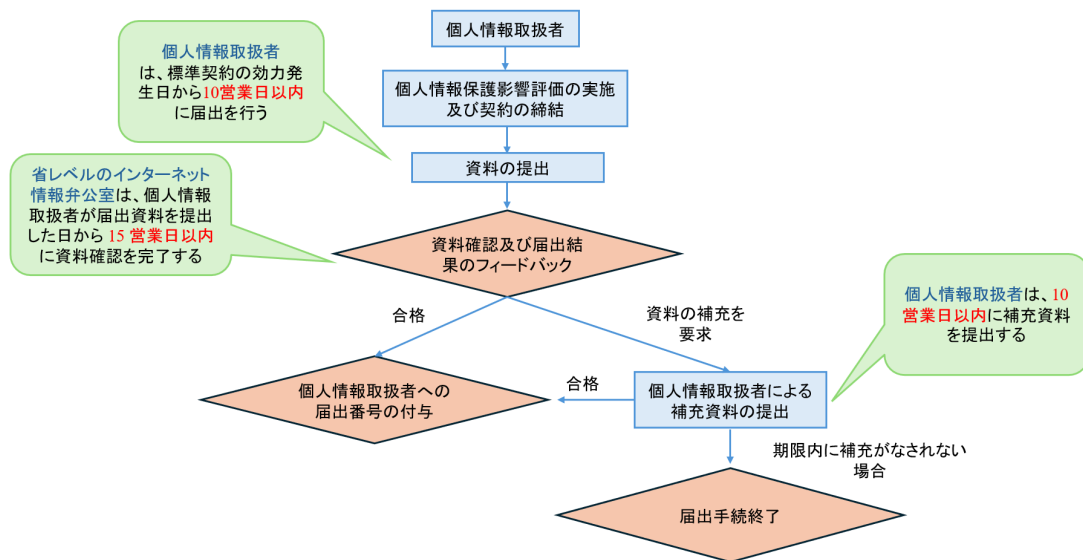


図 4 個人情報越境標準契約届出フロー図

個人情報越境標準契約の締結及び届出の主要プロセスは以下のとおりである。

1. PIA の実施及び契約の締結

まず、個人情報取扱者は、個人情報越境標準契約の届出を実施する前に、PIAを実施する必要がある。具体的には、「個人情報保護法」第55条及び「標準契約弁法」第5条に基づき、国外へ個人情報を提供する際に、事前にPIAを実施し、取扱状況を記録しなければならない(詳細は「[下篇:実践篇 三十、PIAはどのように実施すべきか?](#)」を参照)。また、個人情報取扱者は国家インターネット情報弁公室が公表している標準契約の雛形をベースとして、自身の個人情報の越境状況を踏まえた附録二を作成したうえで、国外移転先と標準契約を締結しなければならない。

2. 届出の実施(資料の提出)

届出方式は一律、従来のオフライン方式からオンライン方式に変更となったため、個人情報取扱者は、「標準契約弁法」第7条及び「標準契約届出ガイドライン(第二版)」に基づき、標準契約の効力発生日から10営業日以内に、データ越境申告システム(<https://sjcj.cac.gov.cn>)を通じて届出を行わなければならない。「データ越境申告システム使用説明(第一版)」によれば、個人情報取扱者は、データ越境申告システムを使用する際、「ユーザーアカウントの登録→システム使用環境の設定→新規届出申請入口の選択」という手順で、個人情報越境標準契約の届出を行う必要がある。

このうち、ユーザーアカウントの登録及びシステム使用環境の設定に関する具体的な操作手順と要件は、データ越境安全評価の申告と同一である(詳細は「[上篇:基礎篇 八、データ越境安全評価はどのような手順で行うのか?](#)」を参照)。

個人情報取扱者はシステムにログインした後、「新規届出」を選択して個人情報越境標準契約の届出を行う必要があり、「標準契約届出ガイドライン(第二版)」及び「データ越境申告システム使用説明(第一版)」によれば、その際には以下の書類を提出しなければならない。

- 統一社会信用コード証明書の写し
- 法定代表者の身分証明書の写し
- 手続者の身分証明書の写し
- 手続者の授權委託書
- 署名捺印済み誓約書の写し

- 個人情報越境標準契約の写し(社印押印済みのもの)
- PIA 報告書の写し(社印押印済みのもの)

実際にデータ越境申告システム上で届出を行う際には、個人情報取扱者はシステム上のガイドに従って、以下の情報又は書類を段階的に確認・提出していくことになる。

- 個人情報越境標準契約の適用状況の確認
- 個人情報取扱者の基本状況の記入
- 法定代表者情報の記入
- 手続者情報の記入
- 署名捺印済み誓約書の写しのアップロード
- 個人情報取扱者における中国の法律、行政法規、機関規則の遵守状況の記入
- 個人情報越境シチュエーションの記入
- 社印押印済みの個人情報越境標準契約の写しのアップロード、関連情報の記入
- 社印押印済みの PIA 報告書の写しのアップロード
- その他の関連証明資料のアップロード

3. インターネット情報弁公室による資料確認及び届出結果のフィードバック

個人情報取扱者による資料提出の完了後は、資料確認及び届出結果のフィードバックの段階に入る。「標準契約届出ガイドライン(第二版)」第 3 条によれば、省レベルのインターネット情報弁公室は、個人情報取扱者が届出資料を提出した日から 15 営業日以内に資料確認を完了し、かつ、届出要求に合致する個人情報取扱者に届出番号を付与しなければならない。資料の補充が必要な場合、個人情報取扱者は、10 営業日以内に補充資料を提出しなければならない。期限を徒過しても資料の補充がなされない場合、省レベルのインターネット情報弁公室は当該届出手続を終了することができる(届出が完了しないまま、手続が中途終了する)。

十二、どのような場合に、個人情報保護認証の取得という方法を選択

可能か？

個人情報取扱者は、以下の3つの観点から、個人情報保護認証の取得という方法の選択可否を判断することができる。

1. 適用除外事由の該当有無:「越境流通規定」の定める、3種類のデータ越境適法化手続が免除される6つの事由のいずれかに該当するか？

2. 越境主体の CIO 該当有無:越境主体が CIO に該当するか？

3. 越境データの類型及び数量:越境するデータが重要データに該当するか？越境する個人情報に係る自然人の数が100万人を超えるか？越境する機微な個人情報に係る自然人の数が1万人を超えるか？

上記の問いに対する回答がすべて「No」であり、かつ「当年1月1日から国外に提供する個人情報(機微な個人情報を含まない)が累計で10万人分以上100万人分未満、かつ機微な個人情報が累計で1万人分未満である場合」、個人情報取扱者は、個人情報保護認証の取得又は標準契約の届出のいずれかの手続を実施することで、合法的な個人情報の越境伝送が可能となる。

この場合、標準契約の届出と個人情報保護認証の取得のうちどちらを選択するかは、個人情報取扱者が自身の意思で決定することができる。このため、どちらを選ぶか、どちらがより適切かをどう判断するかが、個人情報取扱者の関心の的となっている。両手続は申請主体、有効期間、審査メカニズム及び国家による監督等の面で顕著な相違があることから、企業は自社の個人情報越境の具体的状況に応じて、以下に示す両手続の特性を踏まえて総合的な評価を行い、最も実情に合った方法を選択することが望ましい。

	個人情報保護認証の取得	標準契約の届出
申請又は届出主体	中国国内に所在する個人情報取扱者と中国国外に所在する個人情報取扱者のいずれも、個人情報保護認証の申請を行うことができる。	標準契約の届出主体は、標準契約の中国国内の署名主体と同一である必要がある。
有効期間	3年	契約当事者が自由に定めることができる

審査主体	専門認証機関	省レベルのインターネット情報弁公室
申請のプロセス	認証の申請、技術的検証、現地審査、認証の決定、継続的監督	届出申請、資料の確認、結果のフィードバック、補充又は再届出
国家による監督	<p>1. 認証機関が個人情報に係る権益に重大な影響を及ぼす問題を発見した場合、国家インターネット情報機関及び関係機関に速やかに報告される。</p> <p>2. 市場監督機関及びインターネット情報機関が、認証プロセス及び認証結果に対して抜き取り検査を実施する。</p>	<p>当事者双方が標準契約の条項に基づき、個人情報保護に関する義務を履行する。また、署名済み契約書及びPIA報告書をインターネット情報機関へ提出し、届出を行う必要がある。</p>

なお、重要データであることが関係機関又は地方政府により告知又は公表されている個人情報を国外提供する場合は、データ越境安全評価の申告を行わなければならない。個人情報越境標準契約の締結・届出又は個人情報保護認証の取得という方法を通じて国外提供をすることはできないため、注意が必要である。

十三、個人情報保護認証の取得はどのような手順で行うのか？

2022年11月18日、国家市場監督管理総局及び国家インターネット情報弁公室により、「認証公告」及びその別紙である「認証規則」が発表された。これらの文書では、認証の申請、技術的検証、現地審査、認証結果の評価及び認可等の段階を含む個人情報保護認証の実施手順について、詳細な説明がなされている。

「認証公告」では、「個人情報保護認証業務を行う認証機関は、認可を受けた後で関連する認証活動を実施しなければならない」としている。関連法令では、法律に基づいて認証機関の資格を取得した企業のリストは明確に示されていないが、中国サイバーセキュリティ審査認証及び市場監督管理ビッグデータセンター（以下、「サイバーセキュリティ審査認証及び市場監督管理ビッグデータセンター」という）への照会結果、及び国家インターネット情報弁公室が2024年3月22日に発表した「『データ越境流通の促進及び規範化に関する規定』に関する記者質問への回答」に基づけば、企業は個人情報保護認証管理システム(<https://data.isccc.gov.cn>)を通

じて、サイバーセキュリティ審査認証及び市場監督管理ビッグデータセンターに個人情報保護認証の申請を行うことができる(詳細は「下篇:実践篇 四十、どの機関に対して個人情報保護認証を申請すべきか?」を参照)。

また、「越境認証要求(案)」では、個人情報の越境伝送に際する個人情報保護認証の適用事由、基本原則及び基本要件について具体的に規定している。同文書は、認証機関が個人情報の越境取扱活動について個人情報保護認証を行うための根拠を提供するものであると同時に、企業が個人情報取扱者として個人情報の越境取扱活動を合法的に実施するにあたっての参考資料ともなっている。

個人情報保護認証の取得には、「認証の申請、技術的検証、現地審査、認証結果の評価及び認可、認証取得後の監督」の5つの段階がある。詳細なフローは図5に示すとおり。

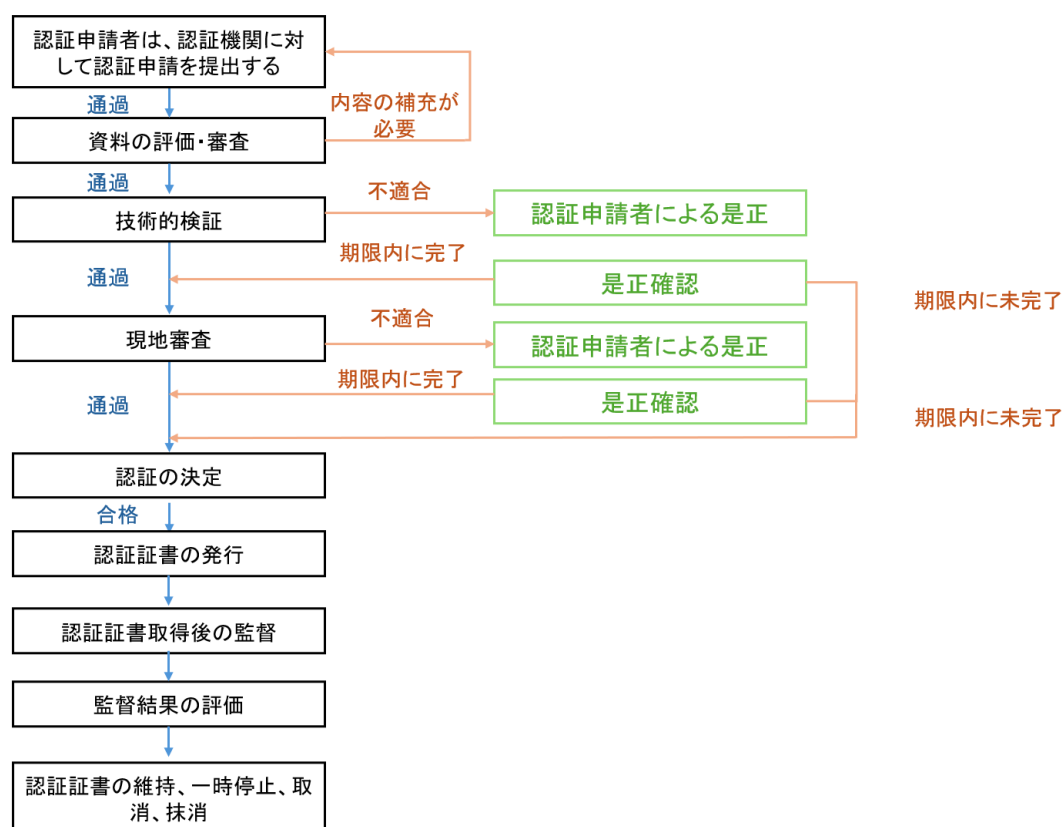


図5 個人情報保護認証フロー図

「認証弁法(案)」の関連内容を踏まえれば、認証申請者と認証機関は以下の手順を踏んで認証手続を行うことになる。

段階	認証申請者 To do	認証機関 To do
1. 認証の申請	<p>(1) 申請前の是正: 個人情報保護認証を申請する前に、要件に基づき自己評価及び是正を行い、要件に適合させる。</p> <p>(2) 認証申請資料の提出: 個人情報取扱者(すなわち認証申請者)が、認証申請資料(認証申請者の基本情報、認証申請書、関連証明資料等を含むがこれらに限らない)を提出する。</p>	<p>(1) 受理通知: 認証機関は、認証申請資料を審査後、受理したか否かを遅滞なくフィードバックする。</p> <p>(2) 認証案の確認と通知: 認証機関は、認証申請資料に基づき認証案(個人情報の類型・数量、関係する個人情報取扱活動の範囲、技術検証機関の情報等を含む)を確定し、認証申請者に通知する⁹。</p>
2. 技術的検証	<p>技術検証機関が認証案に基づいて行う技術検証に積極的に協力し、技術検証報告書を受け取る。</p>	<p>技術検証報告書を発行する¹⁰。</p>
3. 現地審査	<p>認証機関による現地審査に積極的に協力し、現地審査報告書を受け取る。</p>	<p>現地審査を実施し、認証申請者に対して現地審査報告書を発行する¹¹。</p>
4. 認証結果の評価及び	/	<p>(1) 認証の決定: 認証申請資料、技術検証報告書、現地審査報告書及びその他の関連</p>

⁹ 「認証規則」第 4.1 条。

¹⁰ 「認証規則」第 4.2 条。

¹¹ 「認証規則」第 4.3 条。

段階	認証申請者 To do	認証機関 To do
認可		資料・情報に基づき総合評価を行い、認証の決定を行う。
	認証証書を受領する。	a. 認証要件に適合する場合、認証証書を発行する。
	認証機関の要求に応じて是正を行い、再度認証資料を提出する。	b. 認証要件に適合しない場合、認証申請者に対して期限付きで是正を求める。是正後も依然として要件に適合しない場合、書面形式にて認証申請者に対して認証終了(認証を取得できないまま、手続が中途終了する)を通知する。
	欺瞞、情報の隠蔽、故意に認証要件に違反する行為を行ってはならない。	c. 認証申請者、個人情報取扱者による欺瞞、情報の隠蔽、故意に認証要件に違反する行為等、認証の実施に重大な影響を与える行為があることが判明した場合、認証を与えない。
	/	(2) 認証結果の報告: 認証証書発行から 5 営業日以内に、全国認証認可公共情報プラットフォームに認証証書の関連情報(認証証書番号、認証証書を取得する個人情報取扱

段階	認証申請者 To do	認証機関 To do
		<p>者の名称、認証範囲、証書ステータス変更情報等)を報告する。</p>
<p>5. 認証証書取得後の監督</p>	<p>個人情報の越境取扱活動が認証要件に継続して適合することを確保できる場合、引き続き認証証書が維持される。そうでない場合は、認証証書の効力が一時停止され、後日、認証証書が取り消される可能性がある。</p>	<p>(1)継続的監督: 認証の有効期間(3年)において、認証を取得した個人情報取扱者に対して合理的な頻度で継続的に監督を行う。</p> <p>(2)評価結論の作成: 認証証書取得後の監督に関する結論とその他の関連資料に基づき総合的な評価を行う。評価結果が合格の場合は、引き続き認証証書が維持される。不合格の場合は、状況に応じて、認証証書が取り消されるまで、その効力を一時停止する。</p>
<p>6. 認証証書の有効期間延長</p>	<p>証書の有効期間延長が必要な場合、証書の有効期間満了前の6か月以内に、認証申請を行う。</p>	<p>認証証書取得後の監督の方式により、認証要件に適合する申請に対して新たな証書を交付する。</p>
<p>7. 認証証書の変更</p>	<p>(1)変更申請: 認証証書の有効期間内に、認証を取得した個人情報</p>	<p>(1)変更内容の確認: 変更内容に基づき関連資料を評価</p>

段階	認証申請者 To do	認証機関 To do
	<p>取扱者の名称・登録住所・認証要件・認証範囲等に変更が生じた場合、認証機関に対して認証証書の変更を申請しなければならない。</p> <p>(2) 技術的検証及び/又は現地審査(必要な場合)に協力する。</p>	<p>し、承認可否を判断する。</p> <p>(2) 技術的検証及び/又は現地審査: 技術的検証及び/又は現地審査が必要な場合、変更承認前に技術的検証及び/又は現地審査を実施する。</p> <p>(3) 認証結果の報告: 認証証書のステータス変更後 5 営業日以内に、全国認証認可公共情報プラットフォームへ個人情報保護認証証書の関連情報を報告する。</p>
<p>8. 認証証書の抹消、一時停止、取消</p>	<p>認証証書の有効期間内においては、認証証書の一時停止、抹消を申請することができる。</p>	<p>認証証書を取得した個人情報取扱者による個人情報越境の状況が認証範囲と一致しない等、認証要件に適合しないことが判明した場合、認証証書の取消がなされるまでその効力を一時停止したうえで、それを公表する。</p>

十四、C/Oによるデータ越境の要件は何か

C/Oには、通信事業者、金融機関、エネルギー供給業者等が含まれる。C/Oは大量の個人情報及び重要データを保有しており、これらのデータの安全性は国及び個人にとって極めて重要である。例えば、金融機関は顧客の財務情報を、通信

事業者はユーザーの通信データを取扱っており、エネルギー供給業者はエネルギー供給及び配分に関する重要なデータを保有している。CIIO による個人情報及び重要データ越境提供に対して監督を行うことで、これらのデータの濫用・漏洩や不法な目的に使用されることを防止することができる。

現時点で有効な中国の法律では、CIIO によるデータ越境活動について明確な規制を設けている。具体的には、「サイバーセキュリティ法」第 37 条で、CIIO が国外にデータを提供する際の安全評価義務を定めている。「個人情報保護法」第 40 条ではさらに踏み込んで、CIIO は「中華人民共和国国内で収集及び生成した個人情報を国内において保管しなければならない。確かに国外に提供する必要がある場合には、国家インターネット情報機関による安全評価に合格しなければならない」と規定している。CIIO のデータが漏洩、破壊、喪失した場合、国家の安全、社会公共の利益及び個人のプライバシーに重大な影響を及ぼす可能性があることから、中国では CIIO のデータ越境活動に対して厳格な管理態度が取られているのである。

ただし、注意すべきは、「越境流通規定」第 7 条では CIIO がデータ越境安全評価を申告すべき条件を明確に定めると同時に、「第 3 条、第 4 条、第 5 条、第 6 条に定める事由に該当する場合は、その規定による」としている点である。「越境流通規定」第 5 条第 1 項第 1 号から第 3 号では、データ取扱者が個人情報を国外に提供する際にデータ越境適法化手続が免除される 3 つの事由として、(i) 個人が一方当事者となる契約を締結し、履行するために、国外に個人情報を提供するとき、(ii) 法により制定した労働規則・制度及び法により締結した労働協約に従い越境人的資源管理を実施するために、国外に従業員の個人情報を提供するとき、(iii) 緊急の状況において、自然人の生命・健康及び財産の安全を保護するために、国外に個人情報を提供するとき、が列挙されている。したがって、CIIO が国外に個人情報を提供する場合に、上記 3 つの事由のいずれかに該当するのであれば、「越境流通規定」のこれらの規定に基づき、データ越境安全評価の申告が免除される。

現在のところ、大多数の企業は CIIO に認定されていないため、上記規定がそれらに与える直接的な影響は相対的に小さいが、CIIO に認定されていない企業であ

っても、自社の顧客又は提携先が CHIO に該当する可能性に注意を払う必要があり、仮に顧客又は提携先が CHIO に該当するようであれば、移転先として、CHIO による越境データ連携に関連する義務を遵守する必要がある。

十五、重要データの識別に関する法令上の根拠はどのようなものがあるか？

データセキュリティ確保や国益擁護の観点から、各国各地域において、重要データの越境伝送が規制上の焦点となっている。中国の規制当局もデータ越境伝送に対する管理監督を強化し、データの安全を確保するために、「重要データ」の越境伝送にあたってはリスク自己評価を行うだけでなく、インターネット情報機関にデータ越境安全評価の申告を行うよう企業に求めている。

「データセキュリティ法」第21条では、国家データセキュリティ業務協調メカニズムが関係機関を統括・調整して重要データ目録を制定し、重要データに対する保護を強化することを定めており、2024年3月15日には、当該規定に基づくGB/T 43697-2024「データ安全技术 データ分類等級付け規則」が公表された。同規則の第6.5b)条及び附録G「重要データ識別ガイドライン」では、国家全体というマクロ的な視点から重要データ識別に関する明確な判断基準を示し、以下のいずれかに該当するものは重要データであるとしている。

(i) 漏洩、改竄、破壊又は不法取得、不法使用、不法共有された場合、国家安全に直接的に一般的な危害を及ぼすもの

(ii) 漏洩、改竄、破壊又は不法取得、不法使用、不法共有された場合、経済運営に直接的に重大な危害を及ぼすもの

(iii) 漏洩、改竄、破壊又は不法取得、不法使用、不法共有された場合に、社会秩序に直接的に重大な危害を及ぼすもの(社会の安定に悪影響を与える等)

(iv) 漏洩、改竄、破壊又は不法取得、不法使用、不法共有された場合に、公共利益に直接的に重大な危害を及ぼすもの(公衆衛生及び安全に危害を及ぼす等)

(v) 国家安全、経済運営、社会の安定、公衆衛生及び安全における特定分野、特定集団又は特定区域に直接かかわるもの

(vi) 一定の精度、規模、深度又は重要性に達し、国家安全、経済運営、社会の安定、公衆衛生及び安全に直接影響を与えるもの

(vii) 業界・分野の主管(監督管理)機関が評価のうえ重要データと確定したもの。

また、中国の各地方政府、各関係当局も、諸企業に運用性の高い重要データ識別の指針を提供すべく、主管業界・分野又は関連業界・分野に関する当該地域の重要データ目録の制定を急ピッチで推進している。

したがって、法令上で重要データについて明確な定義がなされ、またマクロ的視点から重要データ識別に関する判断基準が示されているとはいえ、各地域・各業界の重要データ目録が公表されていない以上、企業における重要データの識別には一定の不確実性が伴うことは避けられないのが現状である。そこで、「越境流通規定」第2条では、この点に関し、重要データであるか否かは、CICの該当性判断と同じように、関係機関、地方政府の告知に基づくとしている。当該規定は、「重要データの識別が難しい」という諸企業におけるコンプライアンス確保上の問題を一定程度軽減するものであり、企業は自社の取扱うデータの中に関係機関、地方政府によって重要データとされているものがないかという点にのみ注意すればよい。したがって、企業においては、今後関係当局により続々と公表されるであろう重要データの目録・リストを順次チェックして、予定するデータ越境の適法性について段階的に確認するとともに、関係当局との円滑な意思疎通を保ちながら、データ越境計画を適時調整することで、潜在的なコンプライアンスリスクを回避することが望ましい。

十六、重要データ越境の要件には何があるか？

データ取扱者が重要データを国外に提供する場合、データ越境安全評価を申告する必要がある¹²(詳細は「上篇:基礎篇 八、データ越境安全評価はどのような手

¹²「評価弁法」第4条。

順で行うのか？」を参照)。

また、データ取扱者は、データ越境安全評価を申告する前に、データ越境リスク自己評価を実施しなければならない。データ越境リスク自己評価においては、越境データの種類や機微度、データ越境が中国の国家安全、公共利益、個人又は組織の合法的権益にもたらしうるリスク等を重点的に評価する必要がある¹³(詳細は「下篇:実践篇 三十一、データ越境リスク自己評価はどのように実施すべきか？」を参照)。

十七、個人情報越境標準契約の具体的な内容はどのようなものか？

「標準契約弁法」第 6 条では、標準契約はインターネット情報弁公室が定めたバージョンに厳密に従って締結されなければならないこと、個人情報取扱者は国外移転先とその他の条項を取決めることができるが、標準契約と抵触する条項は取決めてはならないことが定められている。

「標準契約弁法」に別紙として付されている現行の標準契約の主な内容は以下のとおりである。

1. 個人情報取扱者及び国外移転先の基本情報:名称、住所、連絡人の氏名/職位、連絡先を含むが、これらに限らない。
2. 個人情報越境の目的、方法、規模、種類、伝送方法、保存期間及び場所等
3. 個人情報取扱者及び国外移転先における個人情報保護義務、並びに個人情報越境によりもたらされうる安全リスクを防止するための技術的措置及び管理措置
4. 国外移転先の所在国又は地域の個人情報保護に関する政策及び法規が標準契約の履行に与える影響
5. 個人情報主体の権利、並びに個人情報主体の権利を保障するための方法及びルート

¹³「評価弁法」第 5 条。

6. 救済措置、契約解除、違約責任、紛争解決等。

個人情報の越境は個人情報取扱の一形態であるため、越境にあたっては「個人情報保護法」に定められた基本要件を遵守しなければならない。実際に、現行の標準契約の一部条項も、同法の一般原則が反映されたものとなっている。

このほか、標準契約では、個人情報取扱者及び国外移転先が個人情報越境伝送時に履行すべき義務が定められているが、個人情報取扱活動において両者間で権利義務をどのように配分すべきかについては具体的な要求が示されていない。このため、両者間での権利義務の配分に関しては、標準契約の別紙で、又は別途契約を締結することにより、独自に取決めることが可能である。ただし、先述のとおり、「標準契約弁法」第6条により、標準契約と抵触する条項は取決めてはならないとされているので、注意が必要である。なお、同条の内容からすれば、仮に個人情報取扱者と国外移転先間で標準契約の締結前に個人情報越境伝送に関する別の契約が締結されており、当該契約の条項が標準契約に抵触するものである場合には、標準契約の条項が優先して適用されることになると考えられる。

十八、個人情報保護認証の具体的な要件は何か？

個人情報保護認証は中国が推奨する自発的認証として位置付けられており、条件を満たす個人情報取扱者は、個人情報の収集、保管、使用、加工、伝送、提供、公開、削除、越境等の取扱活動に関して、自発的に認証を申請することが奨励されている。

「個人情報保護認証実施規則」によれば、個人情報保護認証の根拠となるのは「情報安全技術 個人情報セキュリティ規範」(GB/T 35273-2020)であるので、認証を申請する場合は、同文書の要件を満たす必要がある。そして、個人情報の越境取扱活動に関する認証を申請する個人情報取扱者は、さらに「個人情報越境個人情報保護認証弁法(意見募集稿)」の重点評価内容を参照し、「認証規範 V2.0」の要件を満たす必要がある。

1. 「情報安全技術 個人情報安全規範」(GB/T 35273-2020)

「情報安全技術 個人情報セキュリティ規範」(GB/T 35273-2020)は、個人情報の収集、保管、使用、個人情報主体の権利、取扱委託、共有、譲渡、公開・開示、セキュリティインシデント対応、組織の管理要求等の側面から、個人情報取扱活動に関して遵守すべき原則とセキュリティ要件を規定している。

2. 「個人情報越境個人情報保護認証弁法(意見募集稿)」

個人情報の越境取扱活動に関して、「越境認証要求(案)」では、法的拘束力のある文書、組織管理、個人情報の越境取扱規則、PIA、個人情報主体の権利、個人情報取扱者及び国外移転先の責任義務等の側面から、個人情報取扱者に対する基本的な要求事項を定めている。詳細は以下のとおりである。

(1) 個人情報取扱者は、国外移転先と法的拘束力及び執行力のある文書を締結し、個人情報主体の権益が十分に保障されることを確保する必要がある。

(2) 個人情報の越境取扱活動を実施する個人情報取扱者及び国外移転先は、いずれも個人情報保護責任者を指定し、個人情報保護機関を設置する必要がある。

(3) 個人情報の越境取扱活動を実施する個人情報取扱者及び国外移転先は、同一の個人情報越境取扱規則を定め、これを共同で遵守する必要がある。

(4) 個人情報取扱者は、予定する国外移転先への個人情報提供活動についてPIAを実施し、PIA報告書を作成する必要がある。

(5) 個人情報取扱者及び国外移転先は、個人情報主体からの適切な請求に応える必要がある。

(6) 個人情報取扱者及び国外移転先は、対応する責任義務を履行する必要がある。

「認証弁法(案)」に規定される個人情報越境に関する認証の重点評価内容は、以下のとおりである。

(一)個人情報越境の目的、範囲、方法等の合法性、正当性、必要性。個人情報

取扱者は、越境の合法性、正当性、必要性について論証・説明を行う必要がある。合法性とは、個人情報の越境に法的根拠があり、個人情報主体が越境について個別に同意しており、法令の定める越境禁止事由に該当しないどうかをいう。正当性には、個人情報越境の目的が明確かつ合理的であるかどうかが含まれる。必要性には、主に目的の必要性と越境される個人情報の範囲の必要性(即ち、越境される個人情報は越境目的と直接関連があるものでなければならず、また、その数量は最小限でなければならない)が含まれる。

(二) 国外の個人情報取扱者及び国外移転先の所在国・地域における個人情報保護に関する政策・法令及びサイバーセキュリティ・データセキュリティ環境が、越境される個人情報の安全に及ぼす影響: 個人情報取扱者は、国外の個人情報取扱者及び国外移転先の所在国・地域における個人情報保護に関する法令、現地の法執行・司法機関の対応状況等を整理し、当該国・地域の個人情報保護に関する政策・法令及びサイバーセキュリティ・データセキュリティ環境が、越境される個人情報の安全に悪影響を及ぼさないことを証明する必要がある。

(三) 国外の個人情報取扱者及び国外移転先における個人情報保護水準が中華人民共和国の法律・行政法規の規定及び強制性国家標準の要求を満たしているか: 当該国・地域がデータ保護関連の国際機関に加盟しているか、データ保護分野で拘束力のある国際的コミットメントを行っているか又は中国との間でデータ流通・共有等に関する二国間若しくは多国間協定を締結しているかを説明する必要がある。

(四) 個人情報取扱者と国外移転先との間で締結された法的拘束力のある契約に個人情報保護義務が定められているか: 個人情報取扱者が国外移転先とデータ取扱契約(DPA)を締結している場合、DPA においては個人情報保護に関する双方の責任義務を明記した特別条項を設け、越境データの安全を確保する必要がある。

(五) 個人情報取扱者及び国外移転先の組織構造、管理システム、技術的措置がデータセキュリティ及び個人情報の権益を十分かつ効果的に保障し得るかについて: 個人情報取扱者は、個人情報保護部門又は管理機関を設置しているか、PIPO(個人情報保護責任者)ポジションを設置しているか、並びに個人情報の越境

活動に対してどのような技術的保護措置を実施しているか等について具体的に説明する必要がある。

「認証弁法(案)」では、個人情報取扱者が認証を申請する際の具体的な提出書類リストを明示していないが、2022年に公布された「認証規則」では、認証委託資料には認証委託者の基本資料、認証委託書、関連証明書類等が含まれることが規定されている。また、サイバーセキュリティ審査認証及び市場監督管理ビッグデータセンターへの照会結果及び国家インターネット情報弁公室が2024年3月22日に公表した「『データ越境流通の促進及び規範化に関する規定』に関する記者質問への回答」によれば、企業は個人情報保護認証管理システム(<https://data.isccc.gov.cn>)を通じて同センターに申請を行うことが可能である。個人情報取扱者は、「認証規則」及び同センターの公式サイトで公表されている「個人情報保護認証申請書」を参照し、認証に必要な書類の内容を確認することができる。

個人情報保護認証と標準契約の締結・届出は適用要件が同一であること、また、評価が必要となる項目も「PIA 報告書」の評価項目と重なる部分が多いことから、企業は認証機関に個人情報保護認証の申請書類を提出する際、既に個人情報越境取扱活動についてPIAを実施し、報告書を作成済みであるのならば、当該「PIA 報告書」を、コンプライアンス義務を果たしていることを示す重要参考資料として提出することが考えられる。

なお、粵港澳大湾区内、即ち広東省広州市、深セン市、珠海市、仏山市、惠州市、東莞市、中山市、江門市、肇慶市及び香港特別行政区で登録された(組織の場合)/所在する(個人の場合)個人情報取扱者が個人情報の越境取扱を行う場合、「サイバーセキュリティ標準実践ガイドライン-粵港澳大湾区個人情報越境保護要求(意見募集稿)」の関連要求に適合する必要がある。同意見募集稿は、範囲、用語定義、個人情報取扱に関する要求、基本原則、個人情報に係る権益の保障に関する要求、及び個人情報の安全に関する要求の6部分から構成され、「個人情報保護法」に定める要求事項を改めて示すとともに、香港の「個人データ(プライバシー)条例」(中国語:《个人资料(私隱)条例》)の規定(例:個人情報を商業マーケティングに利用する場合は個人情報主体の同意を得る必要がある等)も盛り込んでいる。

十九、データ越境制度違反に対する罰則はどのようなものか？

「評価弁法」では独自の違反責任及び罰則を規定しておらず、「サイバーセキュリティ法」、「データセキュリティ法」、「個人情報保護法」の関連罰則を援用している。また、データ取扱者の行為が犯罪を構成する場合は、法により刑事責任を追及するとしている。具体的には以下のとおりである。

1. 「サイバーセキュリティ法」第 66 条

「重要情報インフラの運営者が本法第三十七条の規定に違反し、国外でネットワークデータを保管し、又は国外にネットワークデータを提供した場合、関係主管機関は、是正を命じ、警告を与え、違法所得を没収し、5 万人民元以上 50 万人民元以下の過料を科するものとし、かつ、関連業務の一時停止、営業停止、ウェブサイト閉鎖を命じ、関連事業許可を取消し、又は営業許可証を取消することができる。直接責任を負う主管人員及びその他直接責任者に対しては、1 万人民元以上 10 万人民元以下の過料を科する。」

2. 「データセキュリティ法」第 46 条

「本法第 31 条の規定に違反し、国外に重要データを提供した場合、関係主管機関は、是正を命じ、警告を与えるものとし、10 万人民元以上 100 万人民元以下の過料を併科することができ、直接責任を負う主管人員及びその他直接責任者に対し、1 万人民元以上 10 万人民元以下の過料を科することができる。情状が重大な場合には、100 万人民元以上 1,000 万人民元以下の過料を科するものとし、かつ、関連業務の一時停止、営業停止を命じ、関連事業許可証を取消し、又は営業許可証を取消することができ、直接責任を負う主管人員及びその他直接責任者に対し、10 万人民元以上 100 万人民元以下の過料を科する。」

3. 「個人情報保護法」第 66 条

「本法の規定に違反して個人情報を取扱い、又は個人情報取扱において本法に定める個人情報保護義務を履行しない場合、個人情報保護職責履行機関は、是正を命じ、警告を与え、違法所得を没収し、違法な個人情報取扱を行ったアプリケーションプログラムについて、サービス提供の一時停止又は終了を命じる。是正が

なされない場合、100 万人民元以下の過料を併科する。直接責任を負う主管人員及びその他直接責任者に対しては、1 万人民元以上 10 万人民元以下の過料を科する。

前項に定める違法行為があり、情状が重大な場合には、省レベル以上の個人情報保護職責履行機関は、是正を命じ、違法所得を没収し、5,000 万人民元以下又は前年度の売上高の 5%以下の過料を併科し、かつ、関連業務の一時停止又は営業停止を命じ、関係主管機関に関連事業許可を取消し、又は営業許可証を取消すよう通告することができる。直接責任を負う主管人員及びその他直接責任者に対しては、10 万人民元以上 100 万人民元以下の過料を科し、かつ、一定の期間内において関連企業の董事、監事、高級管理職及び個人情報保護責任者に就任することを禁止する決定を行うことができる。」

4. 「中華人民共和国刑法」(以下、「刑法」という)第 253 条の一

国の関連規定に違反して公民個人情報を他人に販売又は提供し、情状が重大な場合、3 年以下の有期懲役又は拘役に処し、罰金を併科又は単科する。情状が特に重大な場合、3 年以上 7 年以下の有期懲役に処し、罰金を併科する。国の関連規定に違反して職責の履行又はサービスの提供中に取得した公民個人情報を他人に販売又は提供した場合、前項の規定に基づき、重きに従い処罰する。公民個人情報を窃取し、又はその他の方法により不法に取得した場合、第一項の規定に基づき処罰する。単位が前三項の罪を犯した場合、単に対しては罰金を科し、その直接責任を負う主管人員及びその他直接責任者に対しては、当該各項の規定に基づき処罰する。

二十、その他、留意すべき事項は？

企業は以下の点に特段の注意を払わなければならない。

「中華人民共和国国家秘密保持法」に基づけば、法令に違反して国家秘密を越境伝送した場合、犯罪を構成し、刑事責任を問われる可能性がある。

また、「刑法」の規定にも留意する必要がある。例えば、「刑法」第 111 条では、外国の機関・組織・個人のために、国家秘密又は情報を窃取・探知・買収し、又は不法に提供した場合、5 年以上 10 年以下の有期懲役を科し、情状が特に重大な場合には 10 年以上の有期懲役又は無期懲役を、情状が軽微な場合には 5 年以下の懲役・拘役・保護観察又は政治的権利の剥奪を科するとしている。

加えて、特定の業種又は分野に関与する企業は、当該業界の関連法令や機関規則、規範性文書を詳細に確認し、特別規制の有無を確認する必要がある。

二十一、 個人情報越境に関し、中国の粵港澳大湾区を対象とした特別な便宜的措施はあるか？

香港創新科技及び工業局と国家インターネット情報弁公室が締結した「粵港澳大湾区におけるデータ越境流通の促進に関する協力覚書」及び両機関が共同で公表した「粵港澳大湾区(中国本土、香港)個人情報越境流通標準契約実施ガイドライン」に基づけば、粵港澳大湾区内の中国本土 9 都市(広州市、深セン市、珠海市、仏山市、惠州市、東莞市、中山市、江門市、肇慶市)と香港間での個人情報の越境流通については、個人情報取扱者と移転先間で「粵港澳大湾区(中国本土、香港)個人情報越境流通標準契約」(以下、「大湾区標準契約」という)を締結することにより行うことができる(ただし、関係機関、地方政府から告知又は公表された重要データに該当する個人情報はこの限りでない)。「大湾区標準契約」の取決めに従い越境流通される個人情報を、粵港澳大湾区外の組織又は個人に提供することはできない。

「大湾区標準契約」を締結した個人情報取扱者及び移転先は、「大湾区標準契約」が発効した日から 10 営業日以内に、所轄に応じて広東省インターネット情報弁公室又は香港特区政府資訊科技總監弁公室に標準契約の届出を行わなければならない。

中国本土の標準契約届出手続と比較すると、「大湾区標準契約」の届出手続では PIA 報告書の提出義務が免除されているものの、企業においてはなおも自主的

にPIAを実施し、その評価結果に基づいてコンプライアンス誓約を行うことが求められている。



下篇：实践篇

二十二、 データ越境シチュエーションの正確な識別方法は？

「評価申告ガイドライン(第二版)」及び「標準契約届出ガイドライン(第二版)」では、どのような行為が「データ越境」に該当するのかを明確に示している。具体的には次のとおりである。

- データ取扱者が国内での運営において収集及び生成したデータを国外に伝送すること
- データ取扱者が収集及び生成した個人情報を中国国内に保管し、中国国外の機構、組織又は個人が照会、取得、ダウンロード、エクスポートできること
- 中華人民共和国国外における国内の自然人の個人情報取扱等のその他のデータ取扱活動

(詳細は「[上篇:基礎篇 二、どのような行為がデータ越境伝送に該当するのか?](#)」を参照)

したがって、「データ越境」に該当するか否かを判断するにあたっては、次の点に注意する必要がある。

- そのデータが「国内での運営中に」収集及び生成されたものか否か
- その行為が「国外への提供」に該当するか否か、又は国外から「照会、取得、ダウンロード、エクスポート」されうるか否か
- 国外において国内の自然人の個人情報を取扱う等のその他のデータ取扱活動については、「個人情報保護法」第3条第2項に定める事由に合致するか否か。即ち、中華人民共和国国外において中華人民共和国国内の自然人の個人情報を取扱う活動(①国内の自然人に製品又はサービスを提供することを目的とするもの、②国内の自然人の行為を分析し、評価するもの、③法律、行政法規の定めるその他の事由)に合致するか否か。

1. 「国内での運営中に」収集及び生成されたものか否か

まず、「国内」とはどの範囲を指すのか、また「国内での運営」とは何を指すのかについて明確にしておく必要がある。

「国内」(中国語:「境内」)の定義について、目下、中国では「国境内」と「関境内」の 2 つの概念が存在している。「国境内」とは、中国の主権が及ぶ領土、領海、領空の範囲を指し、中国本土(大陸部)だけでなく、香港特別行政区、マカオ特別行政区、台湾地区(以下、「香港・マカオ・台湾地区」と総称する)が含まれる。「関境内」とは、同一の税関法が適用される、又は同一の関税制度が運用されるエリアを指す¹⁴。「中華人民共和国出入境管理法」の附則に定める定義によると、「越境」(中国語:「出境」)とは、中国本土から他の国・地域に移転することを指し、中国本土から香港特別行政区やマカオ特別行政区、台湾地区に移転することが含まれる。このような定義においては、香港・マカオ・台湾地区は「国外」(中国語:「境外」)に該当する。「ネットワークセキュリティ条例(案)」第 13 条では、「データ取扱者が香港で上場し、国家安全に影響を与え、又はその可能性がある場合」には、関連規定に従いサイバーセキュリティ審査を申告する必要があると定めている。同規定から推測するに、データ越境に関連する法令において、「国内」は「関境内」と解釈されているものと考えられる。即ち、中国大陸部から香港・マカオ・台湾地区に向けてデータを伝送する行為は、「越境」行為に該当すると解される。

「国内での運営」に関しては、目下、ネットワーク運営者が中国国内において業務を展開し、製品又はサービスを提供することである、と業界内では一般的にみなされている。実務上、扱う製品又はサービスが国外向けであり、かつ国内のデータは収集しないのであれば、「国内での運営」には該当しない。また、国内のネットワーク運営者が国外の機構、組織又は個人向けに業務を展開するだけで、国内の個人情報及び重要データを取扱わないのであれば、この場合も「国内での運営」には該当しない。

2. 3 種類の典型的なデータ越境行為に該当するか否か

実務においてみられる一般的なデータ越境行為は、次の 3 種類に分けることが

14 中国社会科学院法学研究所教授・周漢華ら、『“個人情報保護法”条文解説・適用の手引き』北京:法律出版社, 2022, P244

できる。

(1) データ取扱者が国内での運営中に収集及び生成したデータを国外に伝送し、国外で保管するケース

このケースにおいては、次のようなシチュエーションが「データ越境」とみなされる可能性がある。

a) データ転送機能を持つ媒体によりデータを国外に提供する(図 6)

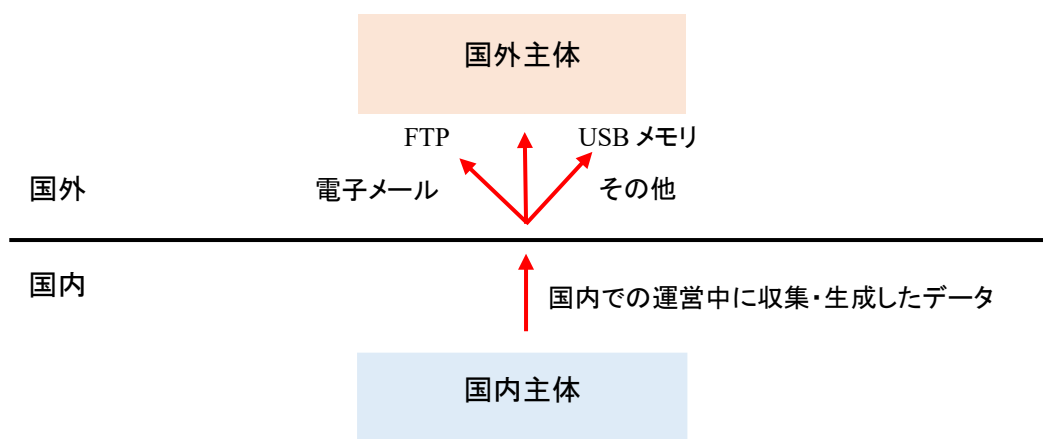


図 6

データ転送機能を持つソフトウェア又はハードウェア等の物理的な記憶媒体には、電子メール、FTP(ファイル転送プロトコル)、国外のサーバーに繋ぐための VPN、API、USB メモリ、ポータブル HDD、モバイルパソコン等が含まれる。このシチュエーションは、データ越境に該当するとみなされやすい。

b) データを国外サーバー又はクラウドにアップロード又は保管する(図 7)

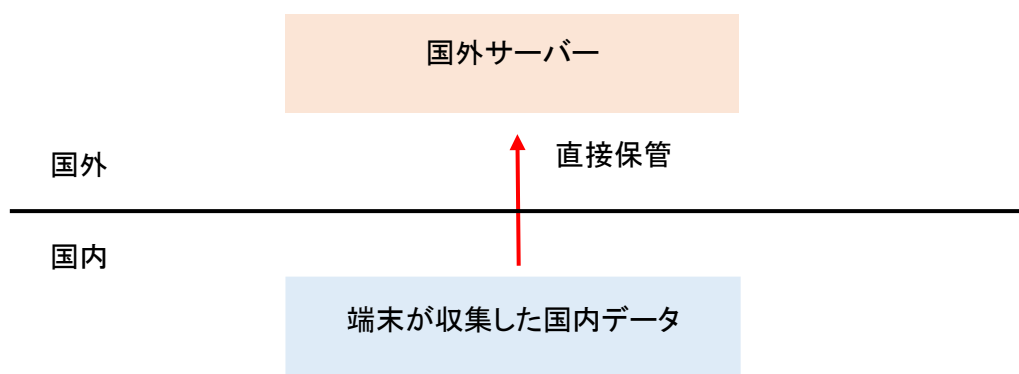


図 7

情報システム、ソフトウェアプラットフォーム、データベースのサーバー、クラウドシステムが国外にある(例えば、多国籍企業が国外プロバイダーの運営及び/又は構築する情報システムを使用している)場合であっても、国内主体による自発的な国外へのデータ伝送に該当する。

c) 第三者を経由した国外へのデータ伝送(図 8)

このほか、国内主体と国外主体との間におけるデータ伝送活動では、第三者(ベンダー)が絡むことが多い。例えば、国外主体の委託を受け、国内又は国外のベンダーが、国内での運営において生成されたデータを代わりに収集するといったやり方である。このような状況において、国外主体は、データを直接収集しているわけではないが、ベンダーが国外主体からの委託を受けてデータを取扱っているのであれば、国外主体がデータ取扱者となり、データの国外移転先とみなされる可能性がある。

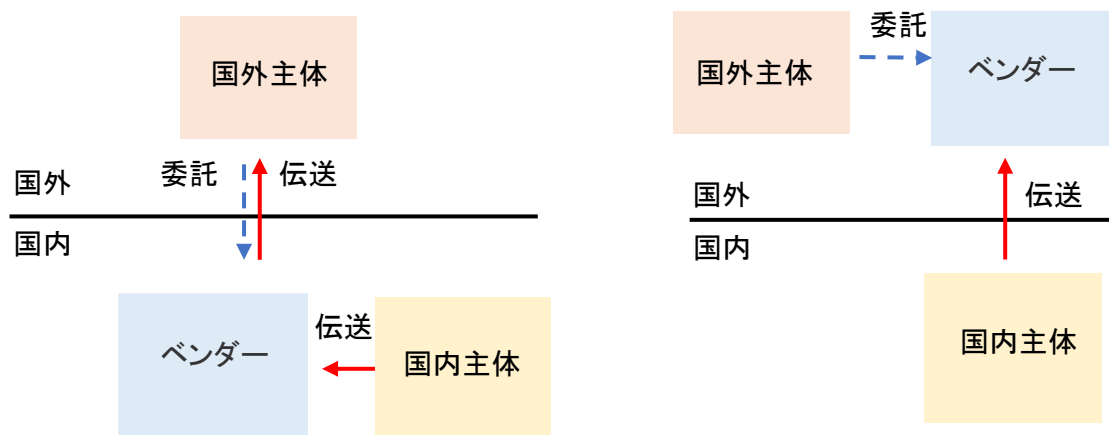


図 8

(2) 収集及び生成したデータを国内に保管し、国外の機構、組織又は個人が照会、取得、ダウンロード、エクスポートすることができるようになっているケース(公開情報、ウェブサイト訪問を除く)

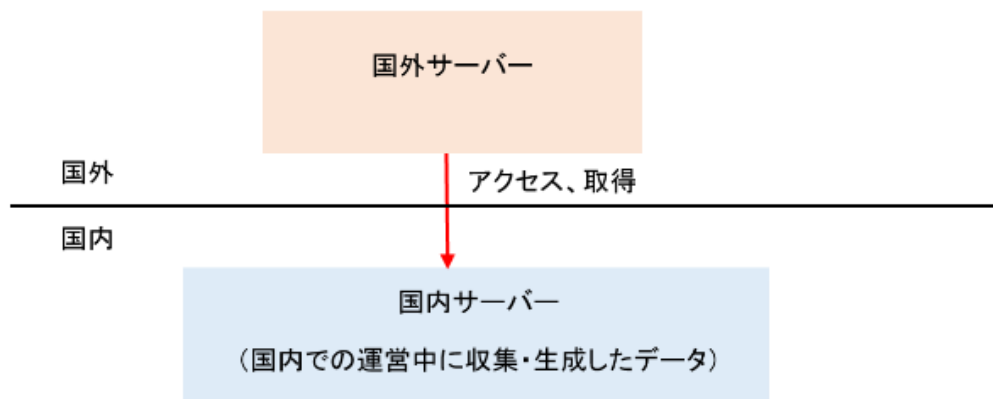


図 9

このケースにおいて「データ越境」に該当するか否かを判断するにあたっては、「国外主体が国内データを取得する/国内データにアクセスする」か否かについても注意しなければならない。即ち、国内主体と国外主体がどのようなデータ伝送を行うにしろ、国内での運営中に生成したデータを国外データ取扱者が照会、取得、ダウンロード、エクスポートするのであれば、それはデータ越境に該当する(図9参照)。

したがって、多国籍企業や同一の経済/事業主体の子会社又は関連会社が、国内に保管されたデータを訪問、取得、ダウンロード、エクスポートする行為についても「データ越境」に該当することが分かる。例えば、外国の会社により中国で設立された企業(外商投資企業)が中国サーバーに保管しているデータに国外の親会社がアクセスする行為についても、データ越境とみなされる。

(3) 国外で国内の自然人の個人情報を取扱う等のその他のデータ取扱活動

「評価申告ガイドライン(第二版)」及び「標準契約届出ガイドライン(第二版)」では、上記 1 及び 2 のケース以外に、3 つ目の越境行為として、「『個人情報保護法』第 3 条第 2 項の事由に該当する、国外で国内の自然人の個人情報を取扱う等のその他の個人情報取扱活動」が挙げられている。

「個人情報保護法」第 3 条第 2 項の規定は以下のとおりである。

「中華人民共和国国外において、中華人民共和国国内の自然人の個人情報を取扱う活動であって、次の各号に掲げる事由のいずれかに該当するものについても、本法を適用する。

- (一)国内の自然人に製品又はサービスを提供することを目的とするもの
- (二)国内の自然人の行為を分析し、評価するもの
- (三)法律、行政法規の定めるその他の事由

上記のうち、「国内の自然人に製品又はサービスを提供することを目的とするもの」については、中国をターゲット市場とし、かつ個人を対象とした越境取引を指すものと理解することができる。国外の個人情報取扱者が中国をターゲット市場としているか否かについては、各種要素を総合的に考慮のうえ、その商業上の目的に基づき判断される。例えば、国外の個人情報取扱者のウェブサイト、アプリケーションプログラムにおいて、製品及びサービスについて中国語を用いて表示している場合や、人民元を支払通貨としている、又は中国国内の決済システムに接続される等の場合には、国外の個人情報取扱者が中国をターゲット市場としていると解することができる¹⁵。

また、「国内の自然人の行為を分析し、評価するもの」は、「一般データ保護規則」(EU 第 2016/679 号規則)(以下、「GDPR」という)における「監視」(Monitoring of EU Customers' Behaviour)の概念に類似するものである¹⁶。GDPR 前文(24)では、「取扱行為がデータ主体の行動の監視と考えられうるか否かを判断するためには、自然人のプロファイリングを構成する個人データの取扱技術が後に使用される可能性を含め、自然人がインターネット上で追跡されているかどうか、特に、データ主体に関連する判断をするため、又は、データ主体の個人的な嗜好、行動及び傾向を分析又は予測するために追跡されているかを確認しなければならない。」¹⁷と定めている。上記を踏まえると、「分析、評価」とは、個人の関連データを持続的に記録・追跡し、事後的に処理を行うことによって、その個人の習慣、興味・趣味、資産状況、健康、信用状況等を分析・予測することであると解される¹⁸。例えば、中国のユーザーが求人情報プラットフォームの国際版サイトに掲載される人材募集情報を

¹⁵ 全国人民代表大会常務委員会法工委経済法室 立法専門家・楊合慶ら『個人情報保護法釈義』北京：法律出版社，2022

¹⁶ 程嘯ら『個人情報保護法理解と適用』北京：中国法制出版社，2021

¹⁷ 個人情報保護委員会。“EU(外国制度)GDPR(General Data Protection Regulation: 一般データ保護規則)”。個人情報保護委員会。<https://www.ppc.go.jp/enforcement/infoprovision/EU/>。(2025-5-22)

¹⁸ 法律出版社法規センター『中華人民共和國個人情報保護法注釈本』北京：法律出版社，2022

閲覧するためにアカウント登録した場合、国外のプラットフォーム運営会社が当該ユーザーの個人情報を分析・評価し、志望している職に関連するパーソナライズされた通知を行う。このような行為は、「国外での国内の自然人の行為を分析、評価するもの」であるため、データの「越境」に該当する。

また、「法律、行政法規の定めるその他の事由」は包括条項である。新たな技術や応用方法の発展に伴い、将来的に、現行の法規定では個人情報取扱活動について十分かつ網羅的な規制ができなくなることが予想されることから、出現しうる新たな問題に対応するために、包括条項を設けて適用の余地及び柔軟性を持たせているのである。

二十三、 企業が関与する可能性のあるデータ越境伝送のシチュエーションにはどのようなものがあるか？

1. 人的資源データの越境

(1) 企業の採用活動(求人応募者の個人情報の越境)

外資系企業を例にとると、従業員の採用活動においてデータ越境と認定される可能性のある典型的なシチュエーションは以下のとおり。

a) 外資系企業の海外本社のウェブサイトで一元的に従業員募集が行われており、応募者は直接、当該ウェブサイトアクセスして個人情報を提供しなければならない(図 10)

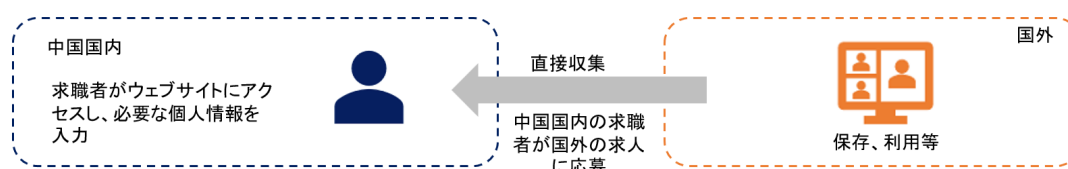


図 10

b) 中国国内の企業が中国国内で収集し、中国国内のサーバーにアップロードした採用活動に関連する個人情報に、中国国外の親会社が直接アクセス、取得する

(図 11)

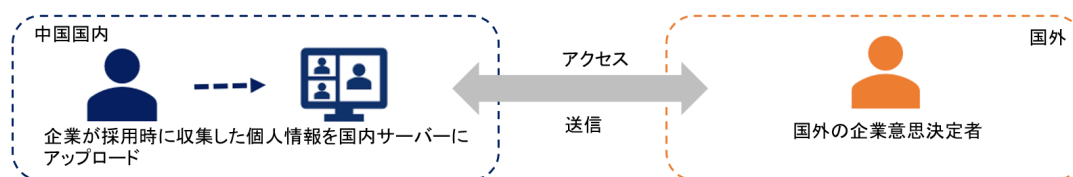


図 11

c) 中国国内の企業が第三者を起用して応募者の情報を収集する場合において、当該第三者により収集されたデータが中国国内の企業に送信されると同時に中国国外(海外本社等)にも送信される(図 12)



図 12

また、企業は採用活動において応募者の氏名、性別、連絡先、学歴、職歴等の個人情報を収集することになるが、この時点では応募者との間で雇用契約を締結していないことから、「個人情報保護法」第 13 条第 1 項第 2 号の「法により制定した労働規則及び法により締結した労働協約に従い人的資源管理を行うために必要な場合」を個人情報収集の根拠とすることはできず、同条第 1 項第 1 号の「個人の同意を取得している場合」を根拠とする必要がある。そのため、企業は個人情報の収集や国外への提供等一連の取扱活動に先立って、求人応募者に個人情報の取扱目的を告知し、法律に基づいてその個別の同意を取得しなければならない。

(2) 従業員データの越境

会社の人事管理においてデータ越境と認定される可能性のある典型的なシチュエーションは以下のとおり。

a) 人事担当者等がメール又は特定の方法により中国国外の主体に従業員データを定期的に送信する(図 13)

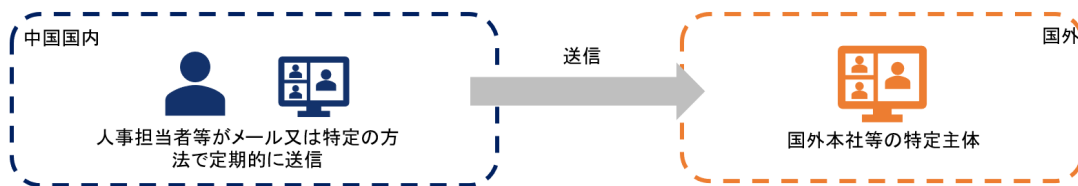


図 13

b) 人事担当者等が中国国内のシステムにアップロードした従業員データに、中国国外の主体が国外からリモートアクセスする、又は中国国外の主体に所属する従業員が中国への出張時に中国国内からアクセスする(図 14)

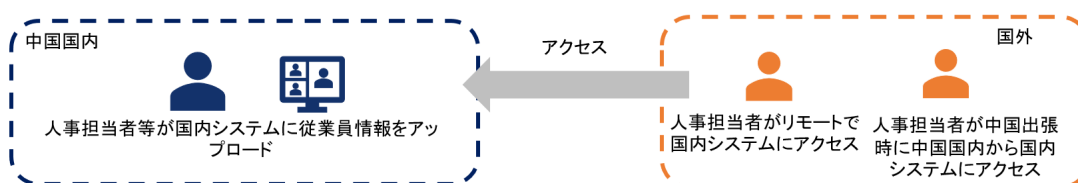


図 14

c) 中国国外の主体がグローバル人事管理システムを通じて中国国内の従業員データを直接収集する(図 15)

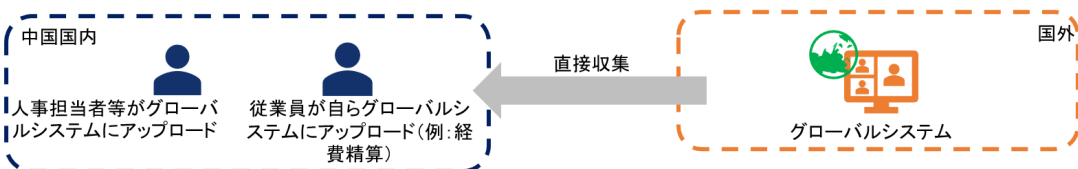


図 15

(3) 事業データの越境

事業活動の展開において生じるデータ越境シチュエーションとしては、主に以下の3つがある。a) 中国国内の企業が、BtoB 及び BtoC 事業を通じて収集したユーザーの個人情報を中国国外に移転する、又は中国国外の主体が中国国内に保管されている当該個人情報にアクセスすることを許可する。b) 海外本社の指示に基づいて、企業が自らの事業運営において生成されたデータ(生産、技術、事業運営データ、重要/中核データ等)を直接国外に所在するサーバーに保管する、又は中国国内のサーバーに保管するが、中国国外の主体が当該中国国内サーバーに保管される当該データを照会、取得、ダウンロード、エクスポートすることを許可する。c) 中国国外に設立された企業が中国国内のユーザーの個人情報を直接収集する(図 16)。

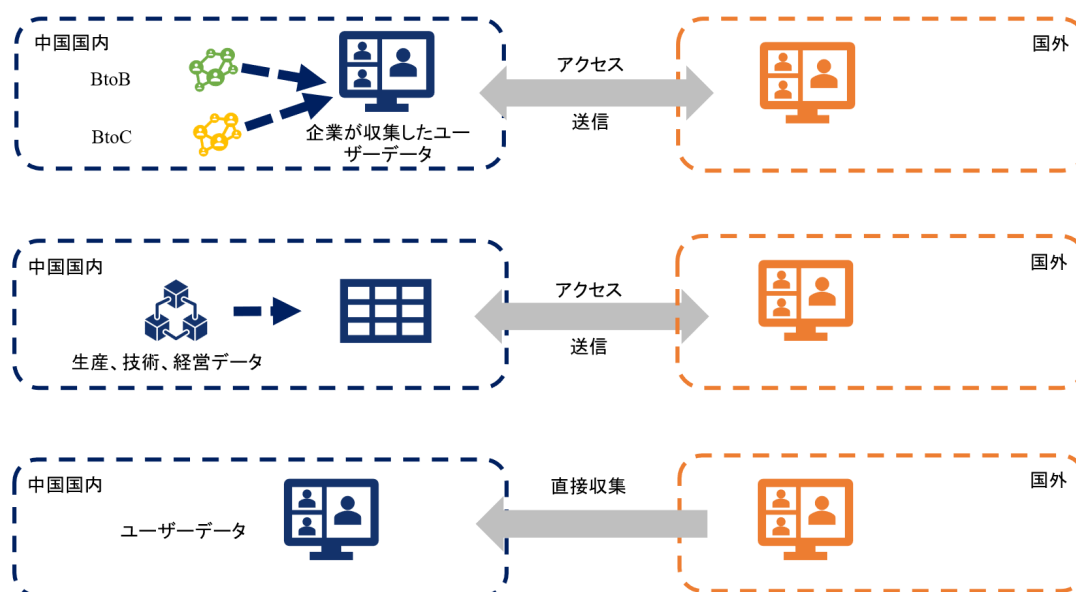


図 16

なお、企業においては、これらのシチュエーション中の各行為を第三者に委託し、その過程で当該第三者にデータを取扱わせる(例えば、第三者に従業員の給与管理業務を委託し、その過程で当該第三者に従業員の個人情報を取扱わせる等)こともあると思われるが、そのような場合においても、当該越境伝送シチュエーションにおいてデータ取扱者/データ提供元となるのは依然として企業であり、委託先の第

三者は受託者又は技術提供者に留まるので、注意が必要である。

二十四、越境伝送するデータの種類の正確な識別方法は？

実務上、企業における個人情報、機微な個人情報、重要データの識別には困難を伴うことが多い。

1. 個人情報の識別

「個人情報保護法」及び「サイバーセキュリティ法」では、個人情報の明確な定義が示されており、自然人の身分が「識別済み」又は「識別可能」であるか否かがその判断基準とされている。ただし、匿名化処理が施された情報は個人情報に該当しない¹⁹。

企業は通常、個人情報について非識別化又は匿名化処理を行うが、これに関しては注意が必要な点がある。即ち、匿名化処理後の個人情報は個人を再識別できないため、個人情報には該当しない一方、非識別化処理後の個人情報は、追加情報と組み合わせることで再識別が可能な場合、依然として個人情報として扱われることである。例えば、企業が過去に国外移転先にユーザーの電話番号、住所、氏名等の完全なデータを伝送し、国外移転先がデータベースにこれらの情報を保持している場合、移転元がデータ伝送において非識別化処理を施していても、国外移転先はアカウントハックやユーザーID マッピングを通じて、これらの情報から個人を再識別できる可能性がある。この場合、越境後のデータは依然として個人情報に該当するため、当該伝送行為は個人情報の越境と見なされる。

2. 機微な個人情報の識別

「個人情報保護法」では、機微な個人情報を以下のように定義している。「機微な個人情報は、漏洩し、又は不法使用されると、自然人の人格・尊厳が侵害され、又は人身、財産の安全が脅かされることを容易に招く個人情報であり、生体認証、宗教・信仰、特定身分、医療・健康、金融口座、移動履歴等の情報、及び14歳未満の

¹⁹「個人情報保護法」第4条、「サイバーセキュリティ法」第76条。

未成年者の個人情報を含む」²⁰。機微な個人情報は個人情報と比べて、漏洩時の影響がより深刻である。「GB/T 35273-2020 情報安全技術 個人情報セキュリティ規範」の附録 B には、具体的な機微な個人情報の類型が記載されており、企業にとっては大いに参考となる。

しかし、実務上、多くの企業が、非識別化処理後の機微な個人情報が依然として機微な個人情報に該当する否かについて疑問を抱えている。これについて、省レベルのインターネット情報弁公室等の監督管理機関に確認したところ、非識別化処理により「機微」という性質を変えることができるのであれば、かかる処理を施された後の個人情報は機微な個人情報に該当しない、との回答が得られた。換言すれば、仮に非識別化処理後の機微な個人情報が漏洩又は不法使用された場合でも、その漏洩又は不法使用が自然人の人格尊厳の侵害や身体・財産の安全を脅かすことに繋がらないのであれば、非識別化処理後の個人情報は、機微な個人情報に該当しないのである。

3. 重要データの識別

(詳細は「[上篇:基礎篇 十五、重要データの識別に関する法令上の根拠はどのようなものがあるか?](#)」を参照)

二十五、越境伝送するデータの量を正確に算定する方法は？

越境伝送するデータの量を算定する際には、以下の点に留意する必要がある。

1. 空間的な視点

「越境流通規定」の公布・施行前においては、越境伝送するデータの量を算定する際には、データ取扱プロセスに関与する全ての関係者を包括的に考慮する必要がある。例えば、企業が収集したユーザーの個人情報だけでなく、社内の従業員情報や顧客、サプライヤー等の商務連絡担当者の情報も個人情報に該当し、データ越境の一般ルールが適用された。したがって、個人情報の量を算定する際、

²⁰「個人情報保護法」第 28 条。

特にデータ越境安全評価の申告基準に達しているか否かを判断する際には、BtoCにおけるユーザー数のみならず、内部の従業員や顧客、サプライヤー等の BtoB における連絡担当者の数も計上する必要があった。

しかし、「越境流通規定」第 7 条第 2 項及び第 8 条第 2 項、並びに「『データ越境流通の促進及び規範化に関する規定』に関する記者質問への回答」では、越境伝送するデータの数量がデータ越境制度の適用要件を満たしているか否かの判断に先立って、「越境流通規定」の定める以下の適用除外事由に該当するか否かを評価する必要があるとされた。

(1) 国際貿易、越境輸送、学術協力、国を跨ぐ生産・製造及びマーケティング等の活動において収集及び生成された、個人情報又は重要データを含まないデータを国外に提供する場合

(2) 国外で収集された個人情報が国内で取扱われた後、国内の個人情報又は重要データを含まずに国外へ提供される場合

(3) 個人が一方当事者となる契約を締結、履行するために、確かに国外に個人情報を提供する必要がある場合

(4) 法により制定した労働規則・制度及び法により締結した労働協約に従い越境人的資源管理を実施するために、確かに国外に従業員の個人情報を提供する必要がある場合

(5) 緊急の状況において、自然人の生命・健康及び財産の安全を保護するために、確かに国外に個人情報を提供する必要がある場合

(6) CIO 以外のデータ取扱者が当年 1 月 1 日から国外に提供した個人情報が累計で 10 万人分未満であり、かつ機微な個人情報を含まない場合

(7) 自由貿易試験区内のデータ取扱者が国外にネガティブリストに含まれていないデータを提供する場合

上記のうち(6)以外の適用除外事由に該当するデータについては、その数量を累計数に計上する必要はない。

また、「『データ越境流通の促進及び規範化に関する規定』に関する記者質問への回答」や「データ越境安全評価申告書(様式)」等により、さらに以下の点が明確化された。(i)越境伝送される個人情報の数量を把握する際は、自然人単位で重複を除いた統計結果を基準とすること。(ii) 国外移転先が多数かつ範囲が不確定で、逐一系列することが困難な場合には、申告時に統計データを提供することが可能であること(ただし、この要件の実際の運用方法については、監督管理機関のより詳細な説明が待たれる)。

このほか、越境伝送するデータの数量を算定する際には、国内から国外へのデータ伝送シチュエーションだけでなく、国内の運営中に収集されたデータに国外からアクセスするシチュエーションも越境伝送に該当する(詳細は「下篇:実践篇 二十二、データ越境シチュエーションの正確な識別方法は?」を参照)ことから、当該シチュエーションに関係するデータの数量も、越境伝送するデータの総量に含めなければならない。例えば、国外の従業員が国内のデータベースにアクセスする場合や、外国籍の従業員が出張で訪中し、中国国内でデータベースにアクセスする場合等においては、アクセスされるデータの数量を越境伝送されるデータの総量に計上する必要がある。このようなシチュエーションに関しては、データ越境申告者は、ネットワークトラフィック監視の手法を活用してデータ越境行為を検知することが考えられる。具体的には、データ越境伝送の方式、データ越境伝送先の IP アドレス、IP アドレスデータベースを用いて特定した国内から国外へ伝送されたデータ又は国外からアクセスされた国内データの数量を検知・記録することが考えられる。なお、監督管理機関への照会結果によれば、国外のデータ取扱者が国内データにアクセスする場合のデータ数量は、国外の取扱者がアクセス可能なデータの数量を基に算出すべきとのことである。

2. 時間的な視点

「評価弁法」及び「標準契約弁法」では、越境データの数量の算定において、計算起点を「前年 1 月 1 日」とし、前年 1 月 1 日以降に国外へ提供した個人情報/機微な個人情報の累計数量を算定対象としていた。しかし、「越境流通規定」の公布・施行後は、「当年 1 月 1 日」からデータ越境安全評価の申告日までに越境された個人

情報/機微な個人情報の累計数量が算定対象とされた。両者はいずれも企業の過去の国外へのデータ伝送量を判断基準としているが、後者では計算期間が短縮され、データ越境制度の適用要件がある程度引き上げられている。

また、注意すべき点として、「データ越境リスク自己評価報告書(様式)」では、個人情報越境に関与するデータ取扱者に対し、自己評価報告書において自然人単位(重複除外)で当年の越境数量について統計を取るだけでなく、今後3年間の越境数量の予測も求めている。

二十六、 データ越境伝送に関するコンプライアンス対策の牽引部署はどのように決定すればよいか？

企業においてデータ越境伝送に関するコンプライアンス対策を実施するにあたっては、法務部、情報セキュリティ・セキュリティ運用部門、内部監査部門、人事部等、複数の部署の連携・協力が必要となる。

データ越境伝送に関するコンプライアンス対策の実施においては、法務部は通常、関係部署に協力しながら、事業活動において関与する各種データの類型の特定、各類型のデータの国内外の伝送ルートの整理、企業と提携先、サプライヤー等の異なる役割間におけるデータ取扱関係(取扱委託又は共有等)の確定等を行う。情報セキュリティ及びセキュリティ運用部門は通常、データ越境における安全な操作プロセスの整理やデータセキュリティ管理制度の構築、データ越境に関するセキュリティインシデント緊急対応策の策定、緊急対応演習の実施等を担当する。内部監査部門は通常、上記各部門が策定するデータ越境に関するセキュリティ戦略、管理制度、越境操作プロセス及びセキュリティ対策等の充足性と有効性について監査を行う役割を担う。さらに、データ越境シチュエーションによっては、人事部やその他の事業部門の参加・協力が求められる場合もある。

以上のことから、データ越境伝送に関するコンプライアンス対策を実施するにあたっては、特定の部署/チームを牽引部署として定めることが考えられる。牽引部署は、効果的なデータコンプライアンス対策を策定・実施し、各部署を統括・調整する

役割を担うため、法律や技術、リスク管理等の専門知識・経験を含む十分な専門能力とリソースを有していなければならない。実務においては、法務部が牽引部署となり、第三者コンサルティング機関(弁護士事務所等)の協力と助言を受けながら、データ越境の各段階における法令遵守を確保することが一般的である。

二十七、 データ越境安全評価の申告主体はどのように確定すればよいか？

「評価弁法」第 2 条によれば、データ越境安全評価の申告主体となるのは、中華人民共和国国内において収集及び生成した重要データ及び個人情報を国外に提供するデータ取扱者である。

なお、「評価申告ガイドライン(第二版)」及び「標準契約届出ガイドライン(第二版)」に基づけば、中国国内に事務所や支店等を設置していない国外主体であっても、国内の自然人に対して製品又はサービスを提供するために、国内の自然人の個人情報を国外で取扱う場合、データ越境安全評価の申告を要する法定事由に該当するときは、「評価弁法」の規定を遵守することが必要となるので、注意が必要である。「個人情報保護法」第 53 条において「国内の自然人に製品若しくはサービスを提供することを目的とする、又は国内の自然人の行為を分析、評価する国外の個人情報取扱者は、中華人民共和国国内において専門の機構を設立し、又は代表者を指定して、個人情報保護関連事務処理の責任を負わせなければならない、かつ、関連機構の名称又は代表者の氏名、連絡先等を個人情報保護職責履行機関に提出しなければならない」と定められていることからすると、データ取扱者が国外から直接的に国内の重要データ及び個人情報を取得する場合、申告基準に達するときは、当該データ取扱者は国内の指定機構を通じて申告を行う必要がある。

また、実務においては、企業は第三者サプライヤーにデータ取扱業務を委託することが通常である。このため、それらのサプライヤーにデータ越境安全評価の申告も代行させればよいと考える向きがあるが、これについては一概に認められるものではない。仮に第三者サプライヤーが、企業から委託されたデータの取扱目的

及び範囲に従ってデータを取扱うのみであるのならば、当該サプライヤーは「代理人」としての役割を担うにすぎず、データ取扱者には該当しないため、データ越境安全評価の申告主体となることはできない。

二十八、 データ越境安全評価の申告スケジュールはどのように把握すればよいか？

企業においてデータ越境安全評価申告のタイムテーブルを策定する際には、申告時の提出資料が多様であることや申告手続が複雑であることを踏まえて、資料の「準備」と「審査」の2つの段階のために十分な時間を確保する必要がある。

まず、企業は自己評価及びコンプライアンス是正措置の実施に十分な時間を割り当てる必要がある。データ越境安全評価の申告過程において、企業はデータ越境リスク自己評価報告書、データ越境安全評価申告書、国外移転先と締結する予定のデータ越境に関連する契約又はその他の法的効力のある文書等、一連の資料を提出する必要がある²¹。データ越境リスク自己評価作業には複数部署間の調整及び連携が必要となり、また一定のコンプライアンス是正措置(例えば、社内規程の整備や既存のデータ取扱契約の修正等)の実施が必要となるケースが多いことを踏まえれば、自社で実施するか第三者機関に委託するかにかかわらず、自己評価作業には相当な時間が必要となるため、企業は自社のデータコンプライアンス状況に応じて、当該準備作業のための時間を事前に十分に確保しておく必要がある。ただし、データ越境リスク自己評価は、データ越境安全評価の申告日前の3か月以内に完了しなければならないとされている²²ことから、企業は申告を行う前に自己評価の完了日を確認する必要があり、もし自己評価の完了日が申告日から見て3か月超前である場合は、再度自己評価を実施し、報告書の内容を更新する必要がある。

次に、企業は資料提出後の審査段階のためにも十分な時間を確保すべきである。

²¹「評価弁法」第6条、「評価申告ガイドライン(第二版)」第3条。

²²「評価申告ガイドライン(第二版)」別紙4「データ越境リスク自己評価報告書(様式)」。

先述の通り、データ越境安全評価申告の全体所要期間は 57+N 日(N は補足資料の審査期間)であり、再評価が行われる場合には 72+N 日となる(詳細は「[上篇:基礎篇 八、データ越境安全評価はどのような手順で行うのか?](#)」参照)。実際の申告において、企業はインターネット情報機関の要求に応じて申告資料を複数回にわたり修正・補足することが必要となる可能性がある。法令では補足資料の審査期間(すなわち上記の N 日の部分)に対して制限が設けられていないため、実際に必要となる期間は 57 日又は 72 日を大きく超える可能性がある。

以上の理由から、企業においては、自社における自己評価及びコンプライアンス是正措置に要する期間とインターネット情報機関の審査に必要な期間を総合的に考慮したうえでデータ越境安全評価の申告スケジュールを事前に策定し、もってデータ越境安全評価申告が原因でデータ越境関連業務の合法的な実施が遅延することを防止することが重要となる。

二十九、要件を満たす企業は、どの機関に対してデータ越境安全評価を申告すべきか？

「評価申告ガイドライン(第二版)」の規定によれば、オンラインでデータ越境安全評価の申告を行う場合、データ取扱者はデータ越境申告システムを通じて資料を提出しなければならない。また、オフラインで申告を行う場合、データ取扱者は所在地の省レベルのインターネット情報機関を通じて、国家インターネット情報機関に申告を行わなければならない。(詳細は「[上篇:基礎篇 八、データ越境安全評価はどのような手順で行うのか?](#)」を参照)

データ越境安全評価の申告先に関しては、本実務 Q&A の別紙において、国家・各地方省レベルインターネット情報機関の連絡先をリストアップしているのので、適宜そちらを参照されたい。(詳細は「[別紙 1:国家・各地方省レベルインターネット情報機関の連絡先](#)」を参照)

三十、PIA はどのように実施すべきか？

企業は、データの越境伝送に先立ち、自社の業務状況に応じて、法律に基づいてデータ越境に伴う安全リスクを評価したうえで、適切なセキュリティ保障措置を講じる必要がある。これは、データ越境の適法性を確保する上で極めて重要である。

越境の適法性を確保するための第一歩は、PIA を実施し、自主的に個人情報の越境に伴う安全リスクを評価することである。「個人情報保護法」第 55 条の規定に基づき、個人情報取扱者である企業は、個人情報を国外に提供する場合、事前に PIA を実施しなければならない。また、「標準契約弁法」第 5 条でもこの要件を改めて示している。さらに、「標準契約弁法」第 7 条では、企業が個人情報越境の適法化手続として標準契約の締結及び届出を選択する場合、PIA 報告書も提出する必要があると定めている。「標準契約届出ガイドライン(第二版)」の別紙 3 によれば、提出される PIA 報告書は標準契約の届出日前の 3 か月以内に作成されたものでなければならず、また、届出日までに重大な変更が生じていないことが求められる。

以上を踏まえれば、企業は「個人情報保護法」第 56 条、GB/T 39335-2020「情報安全技術 個人情報セキュリティ影響評価ガイドライン」、「標準契約弁法」及び「標準契約届出ガイドライン(第二版)」の関連規定を参照して、PIA 報告書を作成しなければならないということになる。特に、「標準契約届出ガイドライン(第二版)」の別紙 5「個人情報保護影響評価報告書(様式)」(PIA 報告書の様式)では、標準契約の届出に用いる PIA 報告書は厳格に当該様式に従って作成することを求めている。当該様式には以下の内容が含まれている。

1. 越境活動の全体的な状況

- 個人情報取扱者の基本状況：個人情報取扱者の基本状況の概要、事業全体と個人情報取扱の状況、越境しようとする個人情報の状況及び個人情報保護に関連する法令の遵守状況
- 国外移転先の状況：国外移転先の基本状況、国外移転先による個人情報取扱の用途及び方法、国外移転先における責任・義務の履行に関する管理及び技術措置、能力等

- 個人情報取扱者が説明する必要があると認めるその他の事項

2. 予定する越境活動についての影響評価の状況及び結論

「標準契約弁法」第5条に定める以下の評価事項に基づき、PIA の状況を説明し、評価で発見された問題点及びその是正状況について重点的に説明したうえで、個人情報越境活動について客観的な影響評価の結論を示すとともに、当該結論に至った理由及び根拠について十分に説明する。

- 個人情報取扱者及び国外移転先における個人情報取扱の目的、範囲、方法等の合法性、正当性、必要性
- 越境する個人情報の規模、範囲、種類、機微の度合い、個人情報の越境が個人情報に係る権益にもたらしうるリスク
- 国外移転先が負担を誓約する義務、並びに義務履行に関する管理及び技術措置、能力等が個人情報越境の安全を保障できるか否か
- 個人情報越境後に改竄、破壊、漏洩、紛失、不法利用等に遭うリスク、個人情報に係る権益を保護するための手段に障害がないか等
- 国外移転先の所在国又は地域の個人情報保護に関する政策及び法規が標準契約の履行に与える影響
- 個人情報越境の安全に影響を与えうるその他事項

三十一、 データ越境リスク自己評価はどのように実施すべきか？

インターネット情報機関に対するデータ越境安全評価の申告が必要となる事由に該当する場合、企業は PIA のほかに、申告の前提手続として、データ越境リスクの自己評価を実施しなければならない。

「評価申告ガイドライン(第二版)」の別紙 4「データ越境リスク自己評価報告書(様式)」では、自己評価報告書は厳格に様式に従って作成しなければならないと定めている。当該様式には、以下の内容が含まれている。

1. 自己評価の実施状況

2. 越境活動の全体的な状況

- データ取扱者の基本状況：概要、組織構成及びデータセキュリティ管理機構に関する情報、事業全体及びデータ資産の状況
- 越境予定データに関する情報：①データ越境に関連する業務、データ資産等の状況、②データ越境及び国外移転先によるデータ取扱の目的、範囲、方法、並びにその適法性、正当性、必要性、③申告する業務のシチュエーションに応じて整理された越境データの状況、④越境予定データが保管されている国内のシステム、データセンター（クラウドサービスを含む）等の情報、データ越境チャネルの関連状況、越境後に保管予定のシステム、データセンター等の情報等、⑤データ越境後における他の国外移転先への提供状況、⑥個人情報に関わる場合、自然人ベース（重複除外）での当年における越境数量及び今後3年間の越境数量の見込み
- データ取扱者におけるデータセキュリティ保障能力の状況：データセキュリティ管理能力、データセキュリティ技術能力、データセキュリティ保障措置の有効性に関する証明、データセキュリティ及びサイバーセキュリティ関連法令の遵守状況
- 国外移転先の状況：国外移転先の基本情報、国外移転先によるデータ取扱の用途、方法等、国外移転先における責任・義務の履行に関する管理及び技術的措置、能力等。
- 法的文書において定められたデータセキュリティ保護に関する責任・義務の状況：①データ越境の目的、方法及び対象データの範囲、並びに国外移転先によるデータ取扱の用途、方法等、②データの国外保存先、保存期間、及び保存期間の満了後、合意された目的の達成後又は法的文書の終了後における越境データの処理措置、③国外移転先が越境データを他の組織又は個人に再移転する場合の制約的要件、④国外移転先の実質的支配権若しくは経営範囲に実質的な変化が発生したこと、所在国・地

域のデータセキュリティ保護に関する政策・法令及びサイバーセキュリティ環境に変化が発生したこと、又はその他不可抗力により、データセキュリティの確保が困難となった場合に講ずべき安全措置、⑤法的文書に基づくデータセキュリティ保護義務に違反した場合の救済措置、違約責任及び紛争解決方法、⑥越境データが改竄、破壊、漏洩、紛失、移転された場合又は不法取得、不法利用された場合における、適切な緊急対応措置の要件及び個人が自己の個人情報に係る権益を保護するための手段及び方法。

- データ取扱者が説明する必要があると認めるその他の事項

3. 越境活動に係るリスク自己評価の状況及び結論

「評価弁法」第 5 条に定める以下の評価事項に基づき、データ越境リスクに関する自己評価の実施状況を説明する。特に、自己評価で発見された問題点及びその是正状況について重点的に説明したうえで、申告予定のデータ越境活動について客観的なリスク自己評価の結論を示すとともに、当該結論に至った理由について十分に説明する。

- データ越境及び国外移転先におけるデータ取扱の目的、範囲、方法等の合法性、正当性、必要性
- 越境データの規模、範囲、種類、機微の度合い、データ越境が国家安全、公共利益、個人又は組織の合法的権益にもたらしうるリスク
- 国外移転先が負担を誓約する責任・義務、並びに責任・義務履行に関する管理及び技術措置、能力等が越境データの安全を保障できるか否か
- データ越境中及び越境後に改竄、破壊、漏洩、紛失、移転、又は不法取得、不法利用等に遭うリスク、個人情報に係る権益を保護するための手段に障害がないか等
- 国外移転先と締結する予定のデータ越境に関連する契約又はその他の法的効力のある文書等において、データセキュリティ保護に関する責任・義務が十分に取決められているか否か

- データ越境の安全に影響を与えるその他の事項

三十二、 データ越境伝送における PIA とデータ越境リスク自己評価は同一のものか？

PIA とデータ越境リスク自己評価は同一のものではない。PIA は「個人情報保護法」第 55 条に基づくもので、企業が個人情報を国外に提供する前に実施すべき自己評価作業である。他方、データ越境リスク自己評価は「評価弁法」第 5 条に基づくもので、データ越境安全評価の申告が必要となる事由に該当する企業が申告前に実施すべき自己評価作業である。

換言すれば、国外に提供しようとする個人情報が「評価弁法」及び「越境流動規定」に定める申告基準に達していない場合、企業は PIA を実施すれば、適切なデータ越境制度（標準契約の締結及び届出又は個人情報保護認証の取得）を活用することで、個人情報を国外に移転することができる。他方、データ越境安全評価の申告が必要となる事由に該当する場合（詳細は「[上篇：基礎篇 七、どのような場合にデータ越境安全評価の申告が必要となるのか？](#)」を参照）、企業は PIA のほか、データ越境リスク自己評価も実施しなければならない。

PIA の評価項目及びデータ越境リスク自己評価の項目を比較すると、両者には一定の共通点及び相違点が存在することが分かる。

PIA	データ越境リスク自己評価
<p>「個人情報保護法」第五十六条</p> <p>個人情報保護影響評価の内容は、次の各号に掲げる内容を含まなければならない。</p> <p>(一) 個人情報の取扱目的、取扱方法等が合法、正当、必要であるか否か</p>	<p>「評価弁法」第五条</p> <p>データ取扱者は、データ越境安全評価を申告する前に、データ越境リスク自己評価を展開し、以下の事項について重点的に評価しなければならない。</p> <p>(一) データ越境及び国外移転先におけ</p>

<p>(二)個人の権益への影響及び安全リスク</p>	<p>るデータ取扱の目的、範囲、方法等の合法性、正当性、必要性</p>
<p>(三)講じる保護措置が合法、有効で、かつ、リスクの程度に相応しいものであるか否か</p>	<p>(二)越境データの規模、範囲、種類、機微の度合い、データ越境が国家安全、公共利益、個人又は組織の合法的権益にもたらしうるリスク</p>
<p>個人情報保護影響評価報告書及び取扱状況記録は、少なくとも3年間保存しなければならない。</p>	<p>(三)国外移転先が負担を誓約する責任・義務、並びに責任・義務履行に関する管理及び技術措置、能力等が越境データの安全を保障できるか否か</p>
	<p>(四)データ越境中及び越境後に改竄、破壊、漏洩、紛失、移転、又は不法取得、不法利用等に遭うリスク、個人情報に係る権益を保護するための手段に障害がないか等</p>
	<p>(五)国外移転先と締結する予定のデータ越境に関連する契約又はその他の法的効力のある文書等において、データセキュリティ保護に関する責任・義務が十分に取決められているか否か</p>
	<p>(六)データ越境の安全に影響を与えうるその他の事項</p>

PIAは個人情報主体の権益保護に重きを置いており、個人情報取扱活動が正当、合法、必要であるか、及びセキュリティ保護措置が講じられているか否か等に焦点を当てている。他方、データ越境リスク自己評価は、データ越境活動が国家の安全、公共の利益、個人又は組織の合法的権益に及ぼすリスクに重きを置いている。

内容面では、データ越境リスク自己評価の評価範囲はPIAより広い。データ越境リスク自己評価にはPIAの評価項目がすべて含まれているうえ、「データ越境に関する契約又はその他の法的効力を有する文書等においてデータセキュリティ保護に関する責任及び義務が十分に定められているか否か」等、PIAには無い項目も存在する。

総じて言えば、個人情報の越境というシチュエーションにおいて、データ越境リスク自己評価とPIAは注目される点こそ異なるものの、両者の目的及び基本的な評価内容は類似しており、いずれも個人情報の越境活動について分析及び評価を行って潜在的な脆弱性及びリスクを特定し、講じる保護措置が個人情報の安全を確保するに足るか否かを判断することを趣旨としている。

実務においては、PIAを行う場合、データ越境リスク自己評価と同時に実施することが多い。両者には重なる内容が多いことから、PIAの内容を基礎として追加的な評価を行うことで、データ越境リスク自己評価の要件を満たすことが可能であり、2度に分けて評価を行うことを避けられるためである。ただし、先述のとおり、「評価申告ガイドライン(第二版)」ではデータ越境リスク自己評価報告書を厳格に様式に則って作成することを求めているため、PIAをベースに追加評価を行う場合でも、当該様式をしっかりと参照して自己評価報告書を作成する必要がある。

三十三、 データ取扱者と国外移転先の技術及び制度措置が十分であるか否かは、どのように評価すべきか？

「評価弁法」第5条及び「評価申告ガイドライン(第二版)」別紙4「データ越境リスク自己評価報告書(様式)」によれば、データ取扱者は、データ越境安全評価の申告に先立ち、データ越境リスク自己評価を実施しなければならない。当該評価においては、データ取扱者自身のデータセキュリティ保障能力だけでなく、国外移転先が「責任・義務履行に関する管理及び技術措置、能力等が越境データの安全を保障できるか否か」についても、重点的な評価項目とする必要がある。このことから、データセキュリティ保障能力を正確に評価することが、企業がデータ越境を行う上

で極めて重要であることが分かる。他方で、この評価を適切かつ十分に行うことは、多くの企業にとってデータ越境リスク自己評価を行う際の課題となっている。以下では、データ取扱者のデータセキュリティ保障能力の評価を例に取り、その具体的な進め方について詳しく説明する。

「評価申告ガイドライン(第2版)」の別紙4「データ越境リスク自己評価報告書(様式)」では、データ取扱者のデータセキュリティ保障能力を評価するにあたり、以下の内容を含めるべきとしている。

1. データセキュリティ管理能力

管理組織体制及び制度構築の状況、データライフサイクル全体にわたる管理、分類・等級付け、緊急対応措置、リスク評価、個人情報に係る権益保護等の制度及びその実施状況(個人情報の越境を行う場合には、告知義務の履行及び個人からの個別の同意取得等の「個人情報保護法」第39条に定める事項の履行状況についての説明及び証拠資料をインターネット情報弁公室に追加提出する必要がある。ただし、企業が同法中の同意取得が不要となる事由に該当する場合は、個人の同意を取得する必要はない)。

2. データセキュリティ技術能力

データの収集、保管、利用、加工、伝送、提供、公開、削除等の全プロセスにおいて講じられているセキュリティ技術措置。

3. データセキュリティ保障措置の有効性を示す証拠

実施されたデータセキュリティリスク評価、データセキュリティ認証、セキュリティチェック・テスト、データセキュリティコンプライアンス監査、サイバーセキュリティ等級保護評価等の状況。

4. データセキュリティ及びサイバーセキュリティ関連法令の遵守状況(行政処罰や是正命令を受けた場合には、是正完了を証明する資料を追加でインターネット情報弁公室に提出することができる)

上記の評価項目に関し、監督管理機関への照会結果に基づけば、監督管理機

関は企業が提出した資料を審査する際、社内制度及びデータ伝送プロセスにおけるセキュリティ技術を総合的に審査する方針である。理論上は、上記すべての内容を企業が提出する「データ越境リスク自己評価報告書」に明記することが求められる。監督管理機関は、企業が提出する総合評価の内容が詳細であればあるほど、企業のデータセキュリティ保障能力を正確に評価する助けとなるとの見解を示している。

実務においては、一般的に「管理制度による保障能力」と「技術的手段による保障能力」の2つの側面から企業の「データセキュリティ保護能力」を評価する。

1. 管理制度による保障能力

企業は、関連法令に基づき、データセキュリティに関する管理体制や制度の整備状況を詳しく説明する必要がある。例えば、社内のセキュリティ管理、従業員管理、契約上の制約、監査メカニズム、緊急対応、個人情報に係る権益保護等の制度とその実施状況が含まれる。一般に、この部分の評価は、法務、セキュリティ、技術、監査等の部門が連携して行う必要がある。

2. 技術的手段による保障能力

企業は、送信されるデータの機密性、完全性、可用性を保障するための総合的なセキュリティ技術及びデータセキュリティ保護体系を備えていなければならない。

評価事項には、企業が講じているセキュリティ対策、データセキュリティインシデントの予防、検知及び対応能力、データ転送中の身分識別及びアクセス制御の実施能力、データ送信ログの保持能力、及びデータの送信・転送・消去等各段階に対する監査能力等²³の詳細な説明が必要である。これらの技術的手段は書面審査だけでは十分に評価できないため、企業は自己評価を行う際、関連分野の技術専門家に意見を求め、技術的手段による保障能力を十分に評価し、専門的見解を得ることが望ましい。

これら2つの側面に加え、企業は自身の全体的なデータセキュリティ保障能力をより確実に証明するために、データセキュリティ保障措置の有効性を証明する資料、

²³ 詳細は「評価弁法」、「評価申告ガイドライン(第二版)」を参照。

例えば、実施したデータセキュリティリスク評価、データセキュリティ認証、データセキュリティチェック・テスト、データセキュリティコンプライアンス監査、サイバーセキュリティ等級保護評価、ISO 認証等に関する資料の提出も必要となる²⁴。

監督管理機関への照会結果によると、企業が国外移転先のデータセキュリティ保障能力を評価する際には、データ取扱者の評価と同様の観点から評価を行うべきであり、移転先が国外の主体であることを理由に評価基準を変更してはならないとのことである。監督管理機関はデータ越境のリスクを判断するにあたり、国外移転先のデータ管理体制及びデータ取扱に関するセキュリティ技術措置も根拠とするとしている。

三十四、 国外移転先の所在国・地域における法制度及び政策環境の整備状況はどのように評価すればよいか？

国家インターネット情報弁公室が発表した「越境データリスク自己評価報告書(様式)」及び「個人情報保護影響評価報告書(様式)」では、企業が越境データリスク自己評価又はPIAを行う際、国外移転先が所在する国又は地域の個人情報保護に関する政策・法制度の状況の評価する必要はないとしており、企業の負担を軽減している。ただし、データ越境リスク自己評価報告書やPIA報告書に当該事項を記載することこそ必要なくなったものの、国家インターネット情報弁公室が制定した「個人情報越境標準契約」第4条の規定に基づけば、企業はなおも、国外移転先の所在国又は地域の個人情報保護に関する政策及び法制度が、契約上の義務履行に影響を及ぼすか否かを評価し、その評価過程及び結果を記録する義務があるので、注意が必要である。また、「評価弁法」第8条では、データ越境安全評価を行う際に、「国外移転先が所在する国又は地域のデータセキュリティ保護に関する政策・法令及びサイバーセキュリティ環境が越境データの安全に与える影響」を考慮しなければならないとしている。以上のことから、国外移転先の所在国又は地域の法制度及び政策環境の整備状況は、依然として企業が注視すべきリスク評価項目

²⁴「評価申告ガイドライン(第二版)」別紙4「データ越境リスク自己評価報告書(様式)」。

であるといえる。したがって、企業はデータの国外提供に先立って、国外移転先の所在国又は地域の法制度及び政策環境を評価し、越境データ活動に存在しうる安全リスクを判断することが必要となる。

「評価弁法」、「認証規範 V2.0」、「安全評価ガイドライン(案)」、「越境認証要求(案)」等の規定によれば、国外移転先の所在国又は地域の法制度・政策環境の整備状況を評価する際には、以下の内容を含める必要がある。

1. 国外移転先が所在する国又は地域のデータセキュリティ保護に関する政策・法令及びサイバーセキュリティ環境が越境データの安全に与える影響。
2. 国外移転先のデータ保護水準が、中国の法律、行政法規の規定及び強制性国家標準の要求に達しているか否か
3. 国外移転先が所在する国又は地域のデータセキュリティ保護に関する政策・法令が、個人情報保護義務の履行及び個人情報に係る権益の保障に与える影響。具体的には以下を含む。
 - 国外移転先の過去における類似の個人情報の越境伝送及び取扱の経験、国外移転先におけるデータセキュリティインシデントの発生有無及びその際に迅速かつ有効な対応が行われたか否か、国外移転先が所在する国又は地域の公的機関から個人情報の提供を求められたことの有無及びその対応状況
 - 当該国又は地域における現行の個人情報保護に関する法令及び一般的に適用されている標準の状況、並びに中国の個人情報保護関連の法令、標準との相違点
 - 当該国又は地域が加盟している地域的又は国際的な個人情報保護に関する組織、及び当該国又は地域が行った法的拘束力のある国際的なコミットメント
 - 当該国又は地域における個人情報保護の実行体制。個人情報保護を担当する監督・法執行機関や関連の司法機関の有無等

4. 重要データの国外移転先の所在国又は地域の法制度及び政策環境。具体的には以下のとおり。

- 当該国又は地域におけるデータセキュリティに関する現行の法令及び一般的に適用されている標準の状況
- データセキュリティを所管する法執行機関、関連する司法機関等
- 当該国又は地域の法執行機関、司法機関等のデータ取得に関する権限及び法律上の手続
- 当該国又は地域が他の国や地域と締結しているデータの流通・共有等に関する二国間又は多国間の協定（法執行、監督等の面のデータの流通・共有に関する協定を含む）

国外移転先が所在する国又は地域の法律・政策環境の保障能力については、以下の標準²⁵を参照して、「高・中・低」の三段階で評価する。

高レベル	中レベル	低レベル
<p>個人情報保護に関する法令が比較的成熟しており、体系的に整備されている。標準が法令の補完として広く用いられ、個人情報の主体のあらゆる権利が保障されている。個人情報保護の専門機関が存在し、有効で行き届いた多層的な救済手段が整っている。</p>	<p>個人情報保護に関する法令・標準は概ね整っており、個人情報主体の一部の権利が保障されている。個人情報保護を担う機関が設置されており、行政的及び司法的な救済手段が存在する。</p>	<p>個人情報保護に関する法令・標準が不十分又は未整備であり、個人は司法的な救済手段によってのみ権利を守ることができる。</p>

²⁵ 「安全評価ガイドライン(案)」附録 B.3.3.1。

重要データの移転先が所在する国・地域の法制度及び政策環境における保障能力については、以下の標準²⁶を参照して、「高・中・低」の三段階で評価する。

高レベル	中レベル	低レベル
<p>サイバーセキュリティやデータセキュリティに関する法令が整備されており、主管機関や監督機関は比較的強い監督及び法執行能力を有している。データセキュリティインシデントについて、効果的な事後の責任追及及び監督の仕組みが存在する。法執行機関及び司法機関によるデータの取得は法律によって制約されており、その手続は公開かつ透明であり、近年において否定的な事案は存在しない。</p>	<p>サイバーセキュリティやデータセキュリティに関する法令・標準は基本的に整っており、主管機関や監督の枠組みも初期的に形成されている。データセキュリティインシデントに対しては、主に行政的な監督によって対応している。法執行機関及び司法機関がデータを取得する際には、一定の手続を遵守する必要がある。</p>	<p>サイバーセキュリティやデータセキュリティに関する法令・標準が不十分又は未整備であり、主管機関や監督機関が不明確であるか、又は必要な能力を欠いている。データセキュリティインシデントについて、効果的な事後の責任追及の仕組みが存在しない。法執行機関及び司法機関によるデータ取得の権限はほとんど制約されておらず、又は近年において否定的な事案が存在している。</p>

なお、国外移転先が所在する国又は地域の法制度・政策環境を評価するには、評価者が現地の関連政策、法律、文化、社会等あらゆる側面について十分な理解を持っていることが必要である。このため、企業において実際に評価を行う際には、国外移転先と緊密に連携するとともに、弁護士やその他の国際的なサービス機関の支援を受けることが望ましい。

²⁶ 「安全評価ガイドライン(案)」附録 B.3.3.2。

三十五、 EU はどのように法制度・政策環境を評価しているか？

中国では、データ移転先が所在する国又は地域の法制度や政策環境をどのように評価すべきかについて、明確かつ詳細な指針がまだ存在していない。このため、実務においては、データプライバシー保護において先進的な EU の基準を参考にすることが考えられる。

2020年7月に欧州司法裁判所が Schrems II 事件に関する判決を下したことを受けて²⁷、欧州データ保護委員会(EDPB)は同年11月、国外移転先が EU と同等の個人データ保護レベルを確保できるようにするため、「Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data」及び「Recommendations 02/2020 on the European Essential Guarantees for surveillance measures」²⁸を公表し、データ移転影響評価(DTIA)を実施するための指針を提供した。両文書では、第三国におけるデータ保護の法律や実務について評価することを強調している。

欧州データ保護委員会は、国外移転先(第三国)への個人データ越境にあたっては、移転先所在国のデータ保護水準が、欧州司法裁判所及び欧州人権裁判所の判例で求められる基準に合致しているかを評価するよう求めている。当該評価においては、政府にデータへのアクセス等の権限を付与している当該国の法制度が、以下に示す EU の要件に合致しているかを重点的に評価しなければならない。

1. 明確で正確かつ公開された規則に基づいてデータを処理しなければならない。この点においては、国外移転先が所在する国において、データ取扱に関する法的根拠があるかどうかの評価に加え、データ保護に関する法律規定が整備されており明確であるか、安定性及び予見可能性があるか否かを評価する必要がある。

2. 講じられる措置は合理的な目的を達成するために必要かつ適切なものでなければならない。当該措置の必要性及び適切性を説明する必要がある。特に、第三国

²⁷ 同事件において、欧州司法裁判所は EU-米国プライバシーシールドフレームワークの有効性を否定した。これは、当該フレームワークの下では、受領者(米国)が EU と実質的に同等のデータ保護水準を提供していないと判断されたためである。

²⁸ 2021年6月、欧州委員会が「Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0」を更新、発表した。

の立法機関又は法執行機関が国家安全や公共の安全を理由に個人の権利や自由を制限する場合、それが本当に必要かつ適切であるかどうか重視される。

3. 独立した監督メカニズムを備えていなければならない。

4. データ主体は有効な救済手段を得られなければならない(データ主体の権利の行使、及びその権利が侵害された場合における司法やその他の機関による救済を含む)。

2023年7月10日、欧州委員会は「EU-U.S. Data Privacy Framework」に基づく十分性認定を採択した。この認定により、同フレームワークに参加している米国企業は、EUと同等のデータ保護水準を提供していると認められた。新たな十分性認定に基づき、EUから当該フレームワークの認証を受けた米国企業への個人データの移転は、追加のデータ保護措置やさらなる許可を要することなく、安全に実施できるようになった。

上記の中国及びEUにおける関連法令を総合的に考慮した場合、企業が国外移転先の所在する国又は地域の法制度・政策環境を評価する際には、以下の点を重点的に検討することが望ましい。

1. 法制度。国外移転先の所在地における個人情報保護、サイバーセキュリティ、データセキュリティに関する法令や標準の整備状況、及び中国の法制度との違い。

2. 国際的なコミットメント。国外移転先の所在地が地域的又は国際的なデータ保護団体に加盟しているか、又は拘束力のある国際的コミットメントを行っているかどうか。

3. 実施メカニズム。国外移転先の所在地の個人情報、サイバーセキュリティ又はデータセキュリティ保護に関する監督・法執行機関や司法機関の有無、独立性、監督・法執行能力、データセキュリティインシデント発生後の責任追及及び監督メカニズムの有効性等の実施状況。

4. 機関の権限。国外移転先の所在地の法執行機関や司法機関等のデータ取得の権限及び法的手続、これらの権限が適切に制約されているか否か、透明性が確保されているか否か、近年における関連する否定的事案の有無。また、国外移転

先が現地の公共機関から個人情報提供を求められた経験及びその対応状況²⁹。

5. 個人情報主体の救済手段。国外移転先の所在地において個人情報主体の各種権利が保障されているか、個人情報保護の専門機関が存在するか、有効で行き届いた多層的な救済手段が用意されているかどうか。

6. 国際協定。国外移転先の所在地と他国・他地域との間における、データの流通や共有に関する二国間・多国間協定(法執行・監督等の面のデータ流通・共有に関する協定を含む)の有無。

7. 差別的措置。国外移転先の所在地がデータに関して、中国に対する差別的な禁止・制限又はその他これらに類する措置³⁰を講じているかどうか。

三十六、 データ越境安全評価の有効期間はどれぐらいか？どのような場合に、データ越境安全評価の再申告が必要となるのか？

「越境流通規定」第 9 条では、データ越境安全評価合格の結果の有効期間が、「評価弁法」に規定される 2 年から 3 年に延長されるとともに、有効期間の起算点を評価結果の発行日とすることが定められた。また、「越境流通規定」には、データ取扱者による評価結果の有効期間の延長申請に関する内容も追加された。具体的には、有効期間満了後も引き続きデータ越境活動を展開する必要があり、かつデータ越境安全評価の再申告を必要とする事由が発生していない場合、データ取扱者は、有効期間満了の 60 営業日前から、所在地の省レベルのインターネット情報機関を通じて、国家インターネット情報機関に評価結果の有効期間延長を申請することができる。国家インターネット情報機関の認可を得れば、評価結果の有効期間は 3 年間延長される。

さらに、「評価弁法」第 14 条では、データ越境安全評価結果の有効期間内に、次のいずれかの事由が発生した場合、データ取扱者は再度、データ越境安全評価を

²⁹ 「認証規範 V2.0」第 5.4 条 e) 1)号。

³⁰ 蔡開明及び阮東輝『「データ越境安全評価申告ガイドライン(第一版)」についての簡単な分析』,2022-9

申告しなければならないと定めている。

1. 国外へのデータ提供の目的、方法、範囲、種類及び国外移転先のデータ取扱の用途、方法に変化が発生したことにより、越境データの安全に影響が及ぶとき、又は個人情報及び重要情報の国外での保存期限を延長するとき
2. 国外移転先が所在する国又は地域のデータセキュリティ保護に関する政策及びサイバーセキュリティ環境に変化が発生したこと並びにその他の不可抗力事由が発生したこと、データ取扱者又は国外移転先の実質的支配権に変化が生じたこと、データ取扱者と国外移転先の法律文書の変更等により、データ越境の安全に影響が及ぶとき
3. データ越境の安全に影響を与えるその他の事由が発生したとき

三十七、 どのような場合に、個人情報越境標準契約の再締結及び再届出が必要となるのか？

「標準契約弁法」第 8 条及び「標準契約届出ガイドライン(第二版)」では、標準契約を補充締結又は再締結し、届出手続を再履行することが必要となる事由について、以下のとおり定めている。

1. 国外への個人情報提供の目的、範囲、種類、機微の度合い、方法、保存場所若しくは国外移転先による個人情報取扱の用途、方法に変化が発生し、又は個人情報の国外保存期間を延長するとき
2. 国外移転先の所在国又は地域の個人情報保護に関する政策及び法規に変化等が発生し、個人情報に係る権益に影響を与えうるとき
3. 個人情報に係る権益に影響を与えうるその他の事由

なお、上記の事由が発生した場合、個人情報取扱者は、標準契約を補充締結又は再締結したうえで届出手続を再履行するだけでなく、PIA を再実施し、適切な報告書を作成することも必要となるので、注意が必要である。

三十八、 監督管理機関が公表している標準契約を締結する際に、その内容を修正することは可能か？

「標準契約弁法」第 6 条では、「標準契約は、厳格に本弁法の別紙に従ってこれを締結しなければならない。国家インターネット情報機関は、実情に基づき別紙の調整を行うことができる。個人情報取扱者は、国外移転先とその他の条項を約定することができるが、標準契約と抵触してはならない。」と明確に定めている。

したがって、標準契約の締結に際しては、インターネット情報機関が提供する様式をそのまま使用しなければならず、内容を修正することはできない。ただし、標準契約の別紙において、個人情報の越境に関する具体的な情報を補足することは認められている。国家インターネット情報弁公室が公表している「個人情報越境標準契約」には、「附録二 双方が合意するその他の条項」という項目が設けられており、標準契約に抵触しないことを前提として、当該別紙において追加条項を定めることが可能である。

ただし、これらの追加条項はあくまで「補足」の役割を果たすものであり(例えば、国外移転先が講じる管理・技術措置の詳細等を具体的に定める等)、標準契約の条項を実質的に変更する(例えば、個人情報主体の権利を制限したり、個人情報取扱者や国外移転先の責任・義務を軽減したりする等)ことはできないため、この点に注意する必要がある。

本実務 Q&A の末尾に、国家レベル及び省レベルのインターネット情報機関の連絡先をリスト形式で掲載しているので、個人情報越境標準契約を締結し、届出を行う際は、当該リストを参照して該当するインターネット情報機関に問い合わせを行い、最新の要求事項を把握することが望ましい(詳細は「[別紙 1: 国家レベル及び各省レベルのインターネット情報機関の連絡先](#)」を参照)。

三十九、 すでに国外外移転先と「データ取扱契約」を締結している場合、標準契約をその別紙と位置付けることは可能か？

「個人情報越境標準契約」の締結・届出を個人情報越境の適法化手続として選択する場合、たとえその時点ですでに国外移転先と「データ取扱契約」を締結していたとしても、「個人情報越境標準契約」に関する諸義務は免除されないため、国家インターネット情報弁公室が公表している「個人情報越境標準契約」のひな形を使用して、国外移転先と標準契約を締結し、署名・発効後にデータ越境届出システムを通じて届出を行う必要がある。ただし、その場合、新たに締結する標準契約を、過去に締結した「データ取扱契約」の別紙と位置付け、インターネット情報機関の審査における補助資料として活用することが可能である。

なお、手続の形式に関して不明点がある場合は、「別紙 1: 国家レベル及び各省レベルのインターネット情報機関の連絡先」を参照して、該当するインターネット情報機関に連絡を取り、具体的な要求事項を確認することが望ましい。

四十、どの機関に対して個人情報保護認証を申請すべきか？

「認証公告」では、「個人情報保護認証業務を行う認証機関は、認可を受けたうえで関連する認証活動を実施しなければならない」としている。ただし、関連法令において、法律に基づいて認証機関の資格を取得した企業の名簿は公表されていない。

サイバーセキュリティ審査認証及び市場監督管理ビッグデータセンターは、公式ウェブサイト上で「当センターが個人情報保護認証の具体的な実施業務を担当する」との公告³¹を公表している。また、同センターは、ウェブサイト上で個人情報保護認証申請書の様式を公開し、個人情報保護認証業務を受け付ける「データセキュリティ認証業務管理システム」(<https://data.isccc.gov.cn>)を運用している。同センターへの照会結果、及び国家インターネット情報弁公室が2024年3月22日に発表した「『データ越境流通の促進及び規範化に関する規定』に関する記者質問への回答」によると、企業は個人情報の越境伝送に際し、「データセキュリティ認証業務管理システム」内の「個人情報保護認証管理システム」を通じて、同センターに対し個人情

³¹ <https://www.isccc.gov.cn/zxyw/sjaq/grxxbhrz/index.shtml> (2024-3-23)

報保護認証の申請を行うことが可能である。

「中華人民共和国認証認可条例」及び「認証弁法(案)」の関連規定によれば、データセキュリティ及び個人情報保護分野で業務を行う専門機関は、以下の要件を満たす必要がある。

1. 合法的設立:法律に基づいて設立され、独立した法人格を有する機関である必要がある。また、国家市場監督管理機関の認可を受け、個人情報保護認証の資格を取得し、法律に基づき国家インターネット情報機関に対し認証機関として届け出なければならない(さらに、「認証弁法(案)」第 8 条では、認証機関は、届出資料として「過去 3 年間のデータセキュリティ及び個人情報保護分野での専門的業務実績」を提出することが求められている。これは、認証機関が設立後 3 年以上経過している組織であることを要件とする、いわば暗黙のハードルが設けられていると考えられる)。

2. 専門能力:認証分野に関連する専門技術能力を有し、データセキュリティ及び個人情報保護について正確な評価と認証ができること、現行の法令及び標準に基づいて、越境に係る個人情報保護認証に関する基準や手続を策定する能力を有すること、技術検証を行う能力を有し、個人情報取扱者のセキュリティ技術及び措置を有効に評価できることが必要となる。技術検証には、技術構造の確認、データ暗号化、アクセス制御等の検証が含まれ、これらの検証により個人情報の越境時の安全性を確保する。

3. 人員:相応の専門知識と実務経験を備え、組織の個人情報取扱活動の適法性及びリスクコントロール措置の有効性を適切に評価できる一定数の専門技術者及び管理者を擁することが必要となる。

4. 管理体制:詳細な認証プロセス、認証実施細則、作業計画、審査基準及び品質管理措置の策定を含む内部管理体制及び品質保証体制を構築・整備し、認証業務の専門性と適正性を確保していることが必要となる。また、紛争受理及び苦情対応のメカニズムを備えていることも求められる。

5. データセキュリティリスクの防止:データセキュリティリスク防止体制を構築しており、認証プロセス中のデータが改竄、破壊、漏洩、紛失、転送、又は不法取得・

不法利用されないことを確保できることが求められる。

6. 継続的な監督: 認証を受けた個人情報取扱者が行う個人情報の越境活動が認証基準を満たしているかを継続的に監視するための、認証取得後の監督制度を確立していることが求められる。

7. 公正性: 認証活動を実施する際には、独立性と客観性を保持し、利益相反を回避したうえで、外部の影響を受けることなく、客観・公正の原則に則って認証を行い、認証結果の真実性と有効性を確保しなければならない。

8. 情報公開: 認証の根拠、手続、料金基準等の情報を一般に公開し、社会からの監督を受け入れなければならない。

四十一、 国際的な紛争解決のためにデータの越境伝送を求められた場合、どのように対応すべきか？

国際的な紛争が発生した場合、外国の司法機関が中国国内の企業に対し、中国国内に保管されているデータや個人情報を証拠として提供するよう求める可能性がある。その場合、データの越境伝送の問題に関わってくる。

「データセキュリティ法」第 36 条及び「個人情報保護法」第 41 条では、企業が国外の司法機関や法執行機関に対して国内に保管されているデータや個人情報を提供するにあたっては、中国の主管機関の認可が必要であるとしている。また、中国司法部は 2022 年 6 月 24 日に発表した「国際民商事司法共助に関する FAQ」において、国際司法共助に関係する場合、中国の主管機関の許可なしに、国内の組織や個人が外国の司法機関や法執行機関に対し中国国内に保管されているデータや個人情報を提供してはならないと強調している。

したがって、かかる状況においては、主管機関が関連する法律、中国が締結又は参加する国際条約・協定、又は平等互惠の原則に基づき、外国の司法機関又は法執行機関からの国内に保管されているデータ又は個人情報の提出要請を処理することになる。国際刑事分野では、国家監察委員会、最高人民法院、最高人民

検察院、公安部、国家安全部等が刑事司法共助の主管機関となるため、国際刑事に関わる司法共助は、これらの機関が「中華人民共和国国際刑事共助法」等の法律及び関連する国際条約・協定に基づき処理することになる。国際民商事分野では、司法部が主管機関となるため、民商事分野に関わる司法共助は、司法部が「ハーグ送達条約」、「ハーグ証拠収集条約」及び現在中国が締結している 86 件の二国間司法共助条約の規定に基づき実施することになる。或いは、司法手続が適用されない場合には、外交部が外交ルートを通じて実施することになる。

しかし、近年の実務では、国外の民事訴訟において、外国の裁判所やその他の司法機関が司法ルート又は外交ルートを通さずに、企業に対して直接、中国国内のデータを証拠として提出するよう求めるケースがよく見られる。この点に関し、司法部司法共助センターによる同様の質問に対する回答によると、企業が国外の司法機関の要請に基づいて証拠を提出する場合であっても、企業が自主的に証拠を提供する場合であっても、いずれにせよ司法部司法共助センターの認可を得る必要があり、具体的な手続は以下のとおりとのことである。

1. 申請書: 外国の裁判所での訴訟に関する基本情報、証拠提出に関する外国の裁判所の要請等の情報が記載されているもの。

2. 証拠リスト: 提出予定の証拠資料の詳細(証拠の名称、証明する事項、事案との関連性、国家安全・国家機密・政府関連文書・営業秘密・個人情報に該当するかどうか等を含む)。

3. 自己評価報告書: 企業が提出予定の証拠資料について初期的に評価した結果をまとめたもの。

4. 法律評価報告書: 企業の法務部門又は法律事務所が発行した提出予定の証拠資料についての法的意見をまとめたもの。

(注: 自己評価報告書と法律評価報告書には、提出する証拠が国家機密を含まないこと、営業秘密が含まれる場合はその部分が適切に塗りつぶされていること、個人情報が含まれる場合は個人による個別の同意を得たことを明記する必要がある。)

司法部司法共助センターは、上記の資料を受け取った後、最高人民法院、インターネット情報弁公室、申請企業の業界主管機関(工業情報化部等)とともに、越境される予定の証拠について審査を行う。審査には通常 1~2 か月を要し、重大で複雑な事案の場合は 2~4 か月を要する。審査を通過した後、司法部は申請企業に対して承認文書を発行し、企業はその文書を基に証拠の越境を行うことができる。したがって、企業はこのような状況に直面した場合、司法部と積極的に連絡を取り、関連する手続や必要な資料を早期に確認し、その要求に従い資料を準備して申請を行うことで、司法部等の関係機関の審査に要する時間を正しく予測できない、又は審査プロセス中に発生するその他の問題により期限内に証拠を提出できないといった事態を防ぐことが重要となる。「個人情報保護法」及び「データセキュリティ法」が施行されてから現在まで、多くの企業が上記のプロセスに従って司法部に審査を申請し、認可を受けてきた。

中国では、データセキュリティに対する保護強化が進んでおり、各主管機関は当事者の申請手続の利便化、関連機関の審査効率の向上を絶えず図っている。例えば、司法訴訟に関するデータ越境においては、司法部の意見を基に、司法部と他の関係機関により共同で企業の提出した資料が検討されるため、企業がインターネット情報機関に別途申告を行うことは不要となる可能性がある。企業が自らインターネット情報機関、業界主管機関等と個別に連絡して評価を申請するのと比べると、このようなやり方は、企業のコスト削減及び証拠としてのデータ越境流通の効率化に資するものであると言える。実務においては当事務所も、企業が個別の事情に基づいて早期に主管機関を確定して連絡を取り、必要な資料、手続、期限等について確認し、最新の規制要求に基づいて計画的に対応することを推奨している。

四十二、 中国粵港澳大湾区の個人情報越境標準契約はどのように締結及び届出を行うのか？

「大湾区標準契約」は、粵港澳大湾区の中国本土又は香港特別行政区で登録され(組織の場合)、又は所在する(個人の場合)個人情報取扱者(大陸部では、個人

情報取扱活動において、取扱目的、取扱方法について自ら決定を行う組織・個人を指す。香港特別行政区では、「資料使用者」、すなわち、個人資料について、単独又は他の者と連携若しくは共同して、そのデータの収集、保有、処理又は使用を管理する者も含まれる)と移転先(個人情報取扱者から個人情報を越境受領する組織・個人)が、個人情報の越境伝送を行う際に締結する契約である。「大湾区標準契約」の主な内容には、双方の契約上の義務と責任、個人情報主体の権利と救済方法、契約解除、違約責任、紛争解決等が含まれる。

個人情報取扱者は、「大湾区標準契約」を締結して個人情報を越境提供する前に、PIAを実施し、以下の内容を重点的に評価しなければならない。

1. 個人情報取扱者と移転先における個人情報の取扱目的、方法等の合法性、正当性及び必要性。
2. 個人情報主体の権益に対する影響及び安全リスク。
3. 移転先が誓約する義務、並びにその義務を履行するための管理及び技術措置・能力等が、越境提供される個人情報の安全を保障できるか。

個人情報取扱者は、移転先との間で追加の条項を取決めることができるが、当該追加条項は「大湾区標準契約」に抵触するものであってはならない。個人情報の越境提供の目的、範囲、種類、方法や、移転先の個人情報取扱の用途、方法に変更が生じた場合、保存期間を延長する場合、又はその他の個人情報に係る権益に影響を及ぼす事態若しくは及ぼす可能性のある事態が発生した場合、個人情報取扱者は、再度PIAを実施し、標準契約を補充締結又は再締結したうえで、必要な届出手続を履行しなければならない。

「大湾区標準契約」が締結され発効した後、個人情報取扱者と移転先は個人情報の越境を実施することができる。個人情報取扱者と移転先は契約発効日から10営業日以内に、それぞれの管轄区域に応じて、広東省インターネット情報弁公室及び政府資訊科技總監弁公室に届出を行い、必要な書類を提出しなければならない。実務上は、広東省インターネット情報弁公室が届出資料を直接受理することはないため、個人情報取扱者と移転先は、まず所在地の地級市以上のインターネット情報

弁公室に、電子版の届出資料(正式なスキャン PDF 版と WORD 版、光ディスク)を提出する必要がある。その後、資料の完全性が確認された後、所在地の地級市以上のインターネット情報弁公室により広東省インターネット情報弁公室に電子版届出資料が送付され、予備審査が行われる。そして、予備審査を通過した後、個人情報取扱者と移転先は、製本した紙媒体資料と電子版資料(光ディスク)を広東省インターネット情報弁公室に提出する。この電子版資料は、紙媒体資料と同一内容の PDF スキャン版及び WORD 版でなければならない。広東省インターネット情報弁公室は上記資料を受領後、届出手続を進める。

「大湾区標準契約」の届出手続には、書類の提出、書類の審査及び届出結果の通知、補充又は再届出等が含まれる。届出書類には、法定代表者の身分証明書の写し、誓約書、締結済みの「大湾区標準契約」が含まれる。PIA は、「大湾区標準契約」届出日前の 3 か月以内に完了しなければならない、また届出日までに重大な変更が生じていないことが求められる。中国本土の標準契約の届出要件とは異なり、PIA 報告書の提出は不要である。

広東省インターネット情報弁公室は、紙媒体資料を受領後 10 営業日以内に審査を完了し、個人情報取扱者に届出結果を通知する。結果は「通過」(合格)と「不通過」(不合格)があり、通過の場合、広東省インターネット情報弁公室は個人情報取扱者に対し届出番号を発行する。不通過の場合、個人情報取扱者は不通過の通知と理由を受領することになる。この場合、資料の補足を求められたときは、個人情報取扱者は、補足した資料を 10 営業日以内に再提出しなければならない。

個人情報の越境提供の目的、範囲、種類、方法や、移転先の個人情報取扱の用途、方法に変更が生じた場合、保存期間を延長する場合、又はその他の個人情報に係る権益に影響を及ぼす事態若しくは及ぼす可能性のある事態が発生した場合、個人情報取扱者は、再度 PIA を実施し、「大湾区標準契約」を補充締結又は再締結したうえで、必要な届出手続を履行しなければならない。

標準契約の有効期間内に「大湾区標準契約」を補充締結する場合、個人情報取扱者は補充資料を提出しなければならない、再締結する場合は再度届出を行わなければならない。補充資料又は再届出資料の審査期間は 10 営業日である。

四十三、 上海自由貿易試験区に、データ及び個人情報の越境に関する優遇措置はあるか？

「越境流通規定」第 6 条では、自由貿易試験区はデータ越境手続の管理範囲に組入れる必要があるネガティブリストを自ら制定することができること、ネガティブリスト未掲載のデータを越境伝送する場合、データ越境手続が免除されることを定めている。

上海自由貿易試験区(以下、「**上海自貿区**」という)には、上記規定に基づくデータ越境の優遇措置が存在する。その主な根拠となるのは、「上海市における『高水準の国際経済貿易ルールへの全面的な対応による中国(上海)自由貿易試験区における高水準制度型開放の推進に係る全体計画』の実行に関する実施計画」(滬府発[2024]1号、2024年2月3日発効。以下、「**実施計画**」という)、「中国(上海)自由貿易試験区及び臨港新片区データ越境ネガティブリスト管理弁法(試行)」(2025年2月8日施行。以下、「**上海自貿区ネガティブリスト管理弁法**」という)及び「中国(上海)自由貿易試験区及び臨港新片区データ越境管理リスト(ネガティブリスト)(2024版)」(2025年2月8日発効。以下、「**上海自貿区ネガティブリスト**」という)である。

「実施計画」には、上海自貿区管理委員会及び臨港新片区管理委員会が、データ分類・等級付け保護制度に基づき、区内の実情に応じて率先して重要データ目録を作成するとともに、臨港新片区でのデータ越境サービスセンター設立等を通じて、データ取扱者におけるデータ越境に係る自己評価等のデータ越境に関するセキュリティ・コンプライアンス業務の利便化を図ることが盛り込まれている。

前述のとおり、「越境流通規定」では、自由貿易試験区におけるネガティブリスト制度について規定している。具体的には、「自由貿易試験区は、国のデータ分類・等級付け保護制度の枠組みのもとで、区内においてデータ越境安全評価、個人情報越境標準契約、個人情報保護認証の管理範囲に組入れる必要があるデータのリスト(以下、「**ネガティブリスト**」という)を自ら制定し、省レベルのサイバーセキュリティ情報化委員会の認可を経た後で、国家インターネット情報機関、国家データ管

理機関に届け出ることができる。自由貿易試験区内のデータ取扱者が国外にネガティブリストに含まれていないデータを提供する場合、データ越境安全評価の申告、個人情報越境標準契約の締結、個人情報保護認証の合格を免ずることができる。」としている。

「上海自貿区ネガティブリスト管理弁法」は、上海自貿区及び臨港新片区で登録され、かつ同区域内でデータ越境活動を行うデータ取扱者に適用される。同弁法第8条は、上海自貿区及び臨港新片区で登録されたデータ取扱者であって、既にネガティブリストが公開されている業種・分野に属するものは、ネガティブリスト未掲載のデータを国外に提供する場合、データ越境安全評価の申告、個人情報越境標準契約の締結、個人情報保護認証の取得が免除されることを明確に規定している。

「上海自貿区ネガティブリスト」は、再保険、国際航運、商業・貿易（小売・飲食業、宿泊業）の3つの重要分野をカバーしたもので、重要データと個人情報という2種類のデータに関し、6つの具体的なシチュエーション、84のデータ項目を対象としている。同リストは、重要データ及び個人情報についてその影響度や数量等に基づきサブカテゴリーに分類したうえで、サブカテゴリー毎に、「データ越境安全評価への合格を要するデータのリスト」と「個人情報越境標準契約の届出、個人情報保護認証により越境する必要があるデータのリスト」を示している。なお、「上海自貿区ネガティブリスト」では、説明及び注釈において、その適用範囲を明確にしている（例えば、説明第2条では、CIIOは同リストの適用対象外であることを明記している）ほか、対象となるデータ取扱者及びデータの類型を定義したうえで、同リストに掲載されるデータ越境シチュエーションについて説明を行っている。したがって、データ取扱者は同リストを利用してデータを越境するにあたり、自身が適用範囲に該当するか、対象データやシチュエーションが同リストの定義に適合するかを逐一確認する必要がある。

また、データ取扱者が上海自貿区及び臨港新片区内でネガティブリストを利用してデータ越境活動を実施することの指導及び支援を目的として、上海市より「中国（上海）自由貿易試験区及び臨港新片区データ越境ネガティブリスト実施ガイドライン（試行）」が公表されている。同ガイドラインでは、申告手続及び方法、注意事項

が詳細に規定されているほか、別紙として、具体的なデータ越境ネガティブリストの利用に関する提出資料についての要求事項、データ越境ネガティブリストの利用状況説明書等の様式、及び上海自貿区内の各データ越境サービスセンターの連絡先が示されている。

四十四、 銀行・金融業のデータ越境に関して注意を要する特別な規定はあるか？

銀行・金融業のデータ規制に関しては、本実務 Q&A で先述している一般規定だけでなく、中国人民銀行等他の機関が発表した関連規範にも注意を払う必要がある。それらのうち、データの越境に関連する主なものとしては、「個人金融情報保護技術規範」(JR/T 0171—2020、2020 年 2 月 13 日施行)、「金融データセキュリティデータセキュリティ等級付けガイドライン」(JR/T 0197—2020、2020 年 9 月 23 日施行)、「金融データセキュリティ データライフサイクルセキュリティ規範」(JR/T 0223—2021、2021 年 4 月 8 日施行)等がある。

銀行・金融業の CIO の認定や遵守すべき事項については、「下篇:実践篇 四十五 証券ファンド業界のデータ越境に関して注意を要する特別な規定はあるか？」を参照されたい。

銀行・金融業の重要データに関し、「金融データセキュリティデータセキュリティ等級付けガイドライン」では、金融データセキュリティ等級付けの目的、原則、範囲、及びデータセキュリティ等級付けの要素、ルール、プロセスを規定している。同ガイドラインでは、金融機関のデータセキュリティが侵害された場合の影響対象とその程度に基づき、データセキュリティ等級を高いものから順に 5 級、4 級、3 級、2 級、1 級に分類している。そのうち、5 級データの特徴には以下の 2 点が含まれる。(1)重要データであること。すなわち、通常、金融業の大型又は特大型機関、金融取引プロセスにおいて中核的役割を果たす機関の重要業務に使用されるものであって、一般に特定の人員にのみ公開され、必要な対象のみがアクセス又は使用可能なものであること。(2)データセキュリティが侵害された場合、国家安全に影響を与える、又

は公衆の権益に重大な影響を与えるもの。

同ガイドラインの附録 C では、銀行・金融業の重要データの認定について詳細に説明しており、具体的には以下が含まれる。(1)マクロ特性:変更不可能又は長期的に安定した経済特性、社会特性を反映できるデータ。(2)大量の情報集約から得られる派生的特性データ:集約後に複数の省をカバーする金融消費者の実際の取引情報。(3)業界監督管理機関の意思決定と法執行プロセスにおけるデータ:行政機関、法執行機関が職務遂行又は法執行過程で収集・生成した、国家機密に関わらない未公開の管理データ。(4)重要情報インフラのネットワークセキュリティホール情報:ネットワーク設備、サーバー、情報システム等の脆弱性情報。

なお、一般的に、上記の重要データには企業の事業運営や内部管理情報、個人情報等は含まれないので、注意が必要である。「金融データセキュリティ データライフサイクルセキュリティ規範」では、銀行・金融業機関の国外の支店、子会社、支店等が国外で業務を展開する過程で収集・生成したデータのセキュリティ等級付けとデータ保護は、データ越境に関する要件に従って実施しなければならないとしている。また、国及び業界主管機関が別途規定する場合を除き、中国国内で生成された金融データは原則として中国国内に保管すべきであることが強調されている。特に、中国国内で生成された 5 級データ(銀行・金融業の重要データを含む)は中国国内でのみ保管しなければならない。

「越境流通規定」によれば、現在、主管機関や地方政府から重要データとして告知又は公表されていないものについては、データ取扱者は重要データとしてデータ越境安全評価を申告する必要はないが、銀行・金融業機構は依然として、上記の規定に基づいてデータの分類・等級付け管理を適切に行い、重要データ等級に関わる可能性のあるデータの越境伝送時には、より慎重な態度を取る必要がある。

個人情報とは、銀行・金融業では一般的に個人金融情報として現れる。「個人金融情報保護技術規範」では、個人金融情報には口座情報、認証情報、金融取引情報、個人身分情報、財産情報、借入情報、及びその他特定の個人金融情報主体の特定の状況を反映する情報が含まれると定義したうえで、個人情報を 3 つの等級に分類している。個人金融情報の越境に関しては、中華人民共和国国内で金融商品又

はサービスを提供する過程で収集・生成された個人金融情報は、国内で保管、処理、分析されなければならない。業務上の必要性により、確かに国外機関(本社、親会社又は支社、子会社及びその他の業務完了に必要な関連機構を含む)に個人金融情報を提供する必要がある場合は、以下の要件を満たす必要がある。(1)国の法令及び業界主管機関の関連規定に適合すること。(2)個人金融情報主体の明示的な同意を得ること。(3)国、業界関係機関が制定した弁法と標準に基づいて個人金融情報の越境安全評価を実施し、国外機関のデータセキュリティ保護能力が国、業界関係機関及び金融機関のセキュリティ要件を満たすことを確保すること。(4)国外機関との契約の締結、現地調査等の方法を通じて、国外機関が個人金融情報の秘密保持、データ削除、事件調査協力等の責任と義務を効果的に履行することを明確化し、またこれを監督すること。銀行・金融業の機微な個人情報については、現在、GB/T 35273-2020「情報安全技術 個人情報セキュリティ規範」附録 B を参照することができる。同附録では、銀行口座、認証情報(パスワード)、預金情報(資金額、支払い・入金記録等を含む)、不動産情報、信用記録、与信情報、取引・消費記録、キャッシュフロー履歴等、及び仮想通貨、仮想取引、ゲーム類の交換コード等の仮想財産情報等の個人財産情報が機微な個人情報に該当するとしている。

銀行・金融業機関が国外に個人信用情報を提供する際には、「与信管理弁法」の関連規定にも注意を払う必要がある。関連する適用条件に合致し、「与信機構による国外への個人信用情報の提供」に該当する場合には、国外の情報使用者の身元、情報の用途について必要な審査を行い、越境提供後の情報が越境貿易や投融资等の合理的な目的に使用され、国家安全を脅かさないことを確保しなければならない。

中国人民銀行が発表した「中国人民銀行業務分野データセキュリティ管理弁法(意見募集稿)」にもデータ越境の制限・管理に関する規定があるため、同弁法が正式に発効した後は、銀行・金融機関はこれについても遵守する必要がある。

四十五、証券ファンド業界のデータ越境に関して注意を要する特別な規定はあるか？

証券ファンド業界のデータコンプライアンスについては、本実務 Q&A で解説している一般的な規定に加えて、中国証券監督管理委員会等の関係機関が発表した規范文書にも注意が必要である。

データ越境に関連する主な規范文書には以下のものがある。

- 「証券先物業界データ分類・等級付け指針」(JR/T 0158—2018。2018年9月27日施行)
- 「証券先物業界データセキュリティ管理及び保護指針」(JR/T 0250—2022。2022年11月14日施行)
- 「証券先物業界データセキュリティリスク防止 データ分類・等級付け指針」(GB/T 42775-2023。2023年8月6日施行)

また、証券ファンド業界の企業は、国家の経済や金融の安全に関わることから、CHIO(CHIO)に該当する可能性が高いと考えられる。ただし、現時点では、証券ファンド業界の主管機関により CHIO のリストが公表されたり、明確に指定されたりといった事実は確認されていない。

証券ファンド業界における重要データに関しては、「証券先物業界データ分類・等級付け指針」が比較的早い時期に発表されているが、同指針は重要データについて明確に定義しておらず、現行の重要データやデータ越境に関する規定との整合性には一定の不確実性がある。同指針では、データの影響対象(業界、機関、顧客)、影響範囲(複数業界、業界内の複数機関、自機関)、データセキュリティ特性(完全性、機密性、可用性)が損なわれた際の影響度(重大、中程度、軽微、無し)に基づいて、証券ファンド業界のデータを四等級に分類し、それぞれの取扱に関する要求を定めている。

- 4 級(極高)は、業界内の大規模又は特大規模の機関における重要業務で使用されるもので、一般に特定の関係者にのみ公開され、必要不可欠な対象者のみがアクセス・利用できる。
- 3 級(高)は、重要業務で使用されるもので、一般に特定の関係者にのみ公開され、必要不可欠な対象者のみがアクセス・利用できる。

- 2級(中)は、一般業務で使用されるもので、一般に制限された範囲内で公開される。一般に内部管理目的のものであり、広範な公開には適さない。
- 1級(低)は、一般に公開可能又は広く公衆が知り、利用することができるものである。

証券ファンド業界のデータ越境活動においては、同指針で言及されているデータの集約やデータの適時性による等級の変更にも注意が必要である。具体的には、データの流通・伝送・使用の過程で、各種業務ニーズに応じて、同じ等級や異なる等級のデータを集約して分析・処理するケースがある。このようなデータの集約に関しては、いくつかの点に注意が必要である。

1. 業務上の必要性から異なる経路やシステムから取得したデータを集約し、データの元の用途や所在システムに変更が生じた場合、データの分類や等級を再評価する必要がある。

2. 集約後のデータから元のデータよりも多くの情報が得られる可能性があるかを分析したうえで、集約後のデータセキュリティ特性(完全性、機密性、可用性)が損なわれた場合に生じる影響を考慮し、適切な等級付けを行う必要がある。

3. 一般に、集約後のデータの等級は、集約前の元データの最高等級を下回らないようにする必要がある。同様に、データの適時性がデータの分類・等級付けに与える影響にも留意すべきである。これらの原則は、証券ファンド業界における重要データの認定やデータ越境コンプライアンスにも適用可能であると考えられる。

「証券先物業界データセキュリティリスク防止 データ分類・等級付け指針」は、「証券先物業界データ分類・等級付け指針」の等級付け基準を基本的に踏襲している。また、「証券先物業界データセキュリティ管理及び保護指針」では、主に引用の形で、国外へのデータ・個人情報の提供について「サイバーセキュリティ法」等の関連法規に基づくべきであるとしている。

加えて、証券ファンド業界の機関がデータ越境を行う際には、「証券法」や「先物及びデリバティブ法」等の規定にも注意を払う必要がある。証券、先物等のクロスボーダー取引に対する監督管理は、国务院の証券監督管理機関が関与する形で行

われるべきとされており、海外の証券監督機関が中華人民共和国国内で直接的な調査や証拠収集等の活動を行うことは認められていない。また、国務院の証券監督管理機関及び国務院の関係主管機関の同意なくしては、いかなる組織や個人も、証券・先物等の業務活動に関する文書や資料を無断で国外に提供することはできない。

「越境流通規定」によれば、現在のところ主管機関や地方政府により「重要データ」として告知・公表されていないデータについては、データ取扱者が重要データとして申告し、データ越境安全評価を行う必要はない。しかし、証券ファンド業界の企業は、上述の規定に基づきデータの分類・等級付け管理を適切に実施する必要があり、重要データに該当する可能性のあるデータを越境伝送する場合は、慎重な対応を取るべきである。

四十六、 医薬業界における越境伝送の一般的なシチュエーションにはどのようなものがあるか？

医薬業界では、海外市場への進出を目指す中国企業だけでなく、中国市場に注力する多国籍企業でも、さまざまな場面でデータの越境伝送が発生している。これらのデータ伝送は、研究開発から市場投入、商業化、クロスボーダーライセンス取引まで幅広いシチュエーションにわたる。

医薬品開発の過程では、国際共同治験 (Multi-regional clinical trials、MRCT) が一般的なシチュエーションの一つとなる。MRCT では、異なる国や地域で同一の臨床試験プロトコルに基づき試験が実施され、大量の臨床データが交換・共有され、製薬企業によって統合管理される。このシチュエーションで収集・伝送されるデータには、上述のデータや個人情報に加え、人類遺伝資源情報等のデータも含まれる。また、このシチュエーションでは、製薬企業は電子データ収集 (EDC) 等の第三者サービス事業者にデータ管理等のサービスを依頼する場合があります、それに伴いサーバーが海外に設置されるケースもある。

海外の医薬品規制当局に対して、IND (Investigational New Drug、新薬臨床試験

申請)や NDA(New Drug Application、新薬承認申請)等の申請を行う際にも、関連データの越境伝送が必要となる。例えば、IND 申請では、中国国内から海外に対して研究計画や試験プロトコル等の資料が提出されることがある。NDA 申請では、国内の臨床データ、症例報告、統計データ等が海外に提供される可能性がある。

クロスボーダーライセンス取引(License-in/License-out)においては、海外のライセンサーが、国内のライセンサーとの契約に基づき、関連技術や資料の提供を求めることがあり、その中には国内ライセンサーが保管している臨床試験データや資料、報告書が含まれる可能性がある。

また、クロスボーダー学術交流や、海外機関への臨床データの共有・公表といった場面でも、国内の医薬業界データの越境伝送が行われることがある。

四十七、 医薬業界における越境伝送ではどのような種類のデータが伝送されるか？

前述のとおり、医薬業界においてはさまざまな場面でデータの越境伝送が発生する可能性がある。インターネット情報機関の監督管理の観点から見ると、(現時点で多くの企業が CHIO に認定されていないことを考慮すれば、)製薬企業は越境伝送しようとするデータの属性を判断し、それに基づいてデータの数量等の他の要素も考慮して、とるべきデータ越境適法化手続を判断する必要がある。関係機関による監督管理の観点からも、データの属性に基づいて、満たすべきコンプライアンス要件を確定することが求められる。

データに対する監督管理の観点からは、企業は越境伝送しようとするデータが重要データ又は中核データに該当するか否かを判断する必要がある。先述のとおり、現在では、企業における重要データ識別の負担を軽減するため、「データ越境流通規定」第2条に基づき、重要データに該当するものは地域及び業界主管機関により通知・公表されることとなっており、告知・公表されていないデータについては、重要データとしてデータ越境安全評価を申告する必要はない。また、個人情報に対する監督管理の観点からは、製薬企業は越境伝送しようとするデータに含まれる個人

情報の数量が「越境流通規定」で定められた各基準値に達しているか、又は機微な個人情報に該当するかを判断する必要がある。

先述のとおり、「個人情報保護法」では、機微な個人情報を「漏洩し、又は不法使用されると、自然人の人格・尊厳が侵害され、又は人身、財産の安全が脅かされることを容易に招く個人情報」と定義し、生体認証、宗教・信仰、特定身分、医療・健康、金融口座、移動履歴等の情報、及び 14 歳未満の未成年者の個人情報を含むとしている。

GB/T 35273-2020「情報安全技術 個人情報セキュリティ規範」附録 B では、機微な個人情報の類型が以下のとおり列挙されている。

(i) 個人生体認証情報：個人の遺伝子、指紋、声紋、掌紋、耳介、虹彩、顔認証特性等

(ii) 個人の健康・生理情報：病気の治療に関連する記録（病歴、入院記録、医師指示書、検査報告書、手術・麻酔記録、看護記録、服薬記録、薬物・食品アレルギー情報、生育情報、過去の病歴、診療記録、家族病歴、既往症、感染症歴等）、及び個人の健康状態に関する情報（体重、身長、肺活量等）

無論、これらの判断の前提となるのは、関連データが個人情報に該当することである。「個人情報保護法」では、「個人情報は、電子的又はその他の方式で記録された、既に識別され、又は識別可能な自然人に関する各種情報であり、匿名化処理後の情報を含まない」と規定している。

臨床試験等の場面では、被験者の身元は、被験者識別コード等の方式で非識別化されることが一般的である（対応するアンブラインド措置によって個人の身元を復元することが可能である）。しかし、非識別処理後の情報が依然として機微な個人情報に該当するか否かはどう判断すればよいのだろうか？

この点については、先述したとおり、一部の省レベルインターネット情報弁公室等の監督機関が示した見解によれば、「機微」という性質に変化があったか否かによる。つまり、非識別化処理を施した機微な個人情報が漏洩又は不法使用された場合に、個人の人格・尊厳が侵害されず、身体・財産の安全にも危害を及ぼさないの

であれば、その情報はもはや機微な個人情報には該当しないと解釈される。ただし、現在のところ、医薬業界における非識別化データの取扱いについて公式な解釈は示されていない。したがって、一部の企業では慎重を期し、非識別化後の臨床試験データを引き続き機微な個人情報として扱うケースも見られる。

また、業界特有の個別法規に基づいて、越境伝送しようとするデータの属性を判断する必要もある。その代表的な例としては、「人類遺伝資源管理条例」(以下、「人遺条例」という)等の法規が規定する人類遺伝資源情報がある。「人遺条例」によれば、人類遺伝資源情報とは、人類遺伝資源材料を利用して生成されたデータ等の情報資料を指す。また、人類遺伝資源材料とは、ヒトゲノム、遺伝子等の遺伝物質を含む器官、組織、細胞等の遺伝子材料を指す。「人類遺伝資源管理条例実施細則」(以下、「人遺細則」という)ではさらに踏み込んで、人類遺伝資源情報には、人類遺伝資源材料を利用して生成されたヒト遺伝子やゲノムデータ等が含まれるが、臨床データ、画像データ、タンパク質データ及び代謝データは含まれないとしている。人類遺伝資源情報に該当するデータを越境伝送しようとする場合には、人類遺伝資源情報に対する特別な監督管理が適用されることになる。臨床試験等のシチュエーションでは、このような情報の取扱いが頻繁に求められるため、慎重な対応が必要となる。

四十八、 医薬業界におけるデータ越境伝送に関する義務にはどのようなものがあるか？

先述のとおり、インターネット情報管理機関による監督管理の観点からは、製薬企業は自社が CHIO に該当するか否かを判断したうえで(現時点では、多くの企業は CHIO に認定されていない)、越境伝送しようとするデータの属性に基づき、データ数量等の他の要素も考慮して、とるべきデータ越境適法化手続を判断する必要がある(詳細は「[上篇:基礎篇 四、現行のデータ越境制度における3種類のデータ越境適法化手続とは何か?どの手続を選択するかをどのように判断すべきか?](#)」を参照)。

「データ越境流通規定」第 2 条により、製薬企業は「重要データ」に関しては一定の緩和措置を受けているものの、個人情報の取扱いに関しては、「越境流通規定」を参照して、個人情報の数量や「機微な個人情報」に該当するか否かに基づき、適切な適法化手続を選択する必要がある。研究開発能力の高い企業では、臨床試験等の場面でのデータの取扱い状況を総合的に考慮し、データ越境安全評価の申告が必要となる基準に達しているかを慎重に判断することが求められる。一方で、規模が小さい製薬企業の場合は、個人情報越境標準契約の締結・届出を選択することとなる可能性が高い。

このほか、国内の製薬企業は「個人情報保護法」等の法令に基づき、以下の措置を講じる必要がある。

(i)「個人情報保護法」に従い、被験者等の関係者に対して、データ越境伝送に関する事項を通知し、個別の同意を取得する(このために説明同意書等の文書を更新する)。

(ii)データ流通・取扱いに関する分類・等級付け管理を強化する。具体的には、社内データと外部サプライヤーのデータを分けて管理する、一般データと機微な個人情報を適切に分類して管理する等。

(iii)国外移転先のデータコンプライアンスに対する監督を強化する。具体的には、グローバル企業内で統一的な個人情報及びデータ管理制度を構築する、非識別化や暗号化等の技術措置を広範に採用する、国外移転先がデータを第三者に再伝送する場合、適切な契約を締結させ、個人情報の取扱いが中国法の求める水準で行われるよう確保する等。

人類遺伝資源の監督管理の観点からは、製薬企業は国外に人類遺伝資源情報を越境伝送するにあたり、法定の義務を履行する必要がある。

「人遺条例」等の法令により、外国組織及び外国組織、個人が設立又は実際に支配する機関、すなわち「人遺条例」のいうところの「外国側機関」(外方単位)が、中国の人類遺伝資源を利用して科学研究活動(臨床試験を含む)を実施する場合、中国側の機関と協力する形で実施することが義務付けられている。また、この

協力については、中国人類遺伝資源管理弁公室(以下、「人遺弁」という。2024年5月1日より、人遺弁の管轄は科学技術部から国家衛生健康委員会へ移管された)に事前の承認申請又は届出を行う必要がある。外国組織が直接関与する場合だけでなく、外国組織が中国国内で設立した機関又は外国組織が支配する中国国内の機関を通じて関与する場合でも、人類遺伝資源を海外主体と直接又は間接的に共有することになる可能性があることから、上記の義務の履行が必要となる。

国際協力臨床試験を実施する場合、国際協力科学研究の承認を取得して実施する方法と、国際協力臨床試験の届出を行って実施する方法の2つがある。

届出を行って国際協力臨床試験を実施する場合は、一般に以下の要件を満たす必要がある。

1. 試験の目的が、中国国内での医薬品・医療機器の上市許可取得である(主に第 I、II、III 相臨床試験及び生物学的同等性試験(BE 試験)を含む)。
2. 人類遺伝資源材料を国外に持ち出さない。
3. 臨床機関内で人類遺伝資源を利用する。具体的には、
 - a) 人類遺伝資源の採取・検査・分析、人類遺伝資源材料の残余処理等が臨床医療機関内で行われる。
 - b) 人類遺伝資源の採取が臨床医療機関内で行われ、検査・分析・残余サンプルの処理が医薬品・医療機器の上市許可申請試験のプロトコルで指定される国内機関により実施される。

上記の3つの要件をすべて満たす場合、国際協力臨床試験は人遺弁への届出のみで実施可能となる。一方、いずれか1つでも満たさない場合は、国際協力科学研究の承認取得が必要となる。また、臨床試験終了後6か月以内に、外国側・中国側が共同で人遺弁へ研究状況報告書を提出する必要がある。

このほか、人類遺伝資源情報を外国側機関に提供又は開放する場合、中国側の情報所有者は事前に科学技術部へ報告し、情報のバックアップを提出しなければならない。ただし、すでに上述の承認取得・届出を実施済みの臨床試験において、

国際協力契約の中で「生成された人類遺伝資源情報は外国側・中国側双方が利用可能」と明記されている場合、別途の事前報告や情報バックアップの提出は不要となる。また、かかる状況において、中国の公衆衛生、国家安全、社会公共利益に影響を及ぼす可能性がある場合、国務院科学技術行政機関の安全審査に合格する必要がある。

このほかにも、健康医療ビッグデータ等に関する個別の法規や規范文書、ルールが存在しており、製薬企業はデータの越境伝送においてこれらにも注意を払う必要がある。

四十九、 中国国内のデータ取引所を通じてクロスボーダーデータ取引を行う場合に考慮すべきデータコンプライアンス上の事項は？

中国信通院のデータによると、2023 年における中国のデジタル経済の規模は 56.1 兆元に達し、デジタル経済が GDP に占める割合は第 2 次産業とほぼ同等となり、国民経済における比率は 40%を超えた。デジタル技術の台頭とデジタル経済関連の政策・法律の整備が進む中、データの越境流通を基盤とするクロスボーダーデジタル取引が急速に発展し、従来の国際貿易の構造を大きく変化させている³²。

クロスボーダーデータ取引のチャネルは、データ取引所を活用した取引所内取引（場内取引）と、取引当事者間において P2P 方式で行われる取引所外（場外）クロスボーダーデータ取引の二つに大別される。現在、中国のデータ取引市場は発展途上にあり、国内のデータ取引の約 95%が取引所外取引であり、取引所内取引の規模はまだ小さい³³。取引所外取引は主に P2P 方式の直接取引が主流であり、取引契約の締結に依存しているため、データの流通回数はまだ多くない。

取引所内取引に関しては、中国の政策及び法令による支援・保障のもと、データ取引所がクロスボーダーデータ取引において重要な役割を果たし始めている。主要なデータ取引所の例としては、北京国際ビッグデータ取引所が開発した「北京デー

³² 中国信息通信研究院「中国デジタル経済発展年度研究報告」.2023

³³ TMPOST「わが国のデジタル経済は新たな段階へと進んでいる」

「データカストディサービスプラットフォーム」が 2022 年に運用を開始している。同プラットフォームは、中国初の企業によるデータの越境流通を支援するデータカストディサービスプラットフォームであり、標準の統一化、効率的な管理、カスタマイズ可能なサービスの特徴とし、データの保管、匿名化出力、フュージョンコンピューティング、アーカイブ登録等のサービスを提供しており、現在、試験運用が進められている。また、上海データ取引所は、国際データ流通市場の拡大に向けた取り組みを積極的に進めており、海外プラットフォームとのデータ双方向流通の協力メカニズムを構築し、「国際ゾーン」セクションを設置し、海外のデータ取引所との協力を強化することで、「データ取引所+グローバルデジタルプラットフォーム」の新たなビジネスモデルを生み出した。深センデータ取引所も、クロスボーダーデータ取引に関する一連の革新的な実証的成果を収め、データ越境の試験運用を積極的に進めており、香港・マカオに隣接する地理的優位性を活かし、中国国内初の取引所内クロスボーダーデータ取引を成功させた。

取引所内取引におけるクロスボーダーデータ取引は、データ越境を伴うことから、データ越境に関する法規制の遵守が不可欠となる。現在、中国国内の法律では、取引所内取引を通じたデータの越境に対する特別な適用除外メカニズムは規定されていないため、データ取引所を通じてクロスボーダーデータ取引を行う場合も、既存のデータ越境に関する法令を遵守する必要がある。また、データ取引所は取引プラットフォームとして、越境されるデータ商品に対して独立したデータコンプライアンス・セキュリティ審査を行っているほか、データ提供者に対して、第三者専門機関（例：法律事務所）によるコンプライアンス審査報告書の提出を求めている。

例えば、公開情報によると、深センデータ取引所が完了させた中国初の取引所内クロスボーダーデータ取引の取引対象は、数庫（上海）科技会社が開発した「数庫 SmarTag ニュース分析データ」であった。この取引では以下の措置が講じられ、最終的に総額 500 万元に上る 5 件の取引が成立した。

1. データ提供者による「自己証明資料」の提出

データ提供者が深センデータ取引所に対し、取引対象、取引当事者、取引シナリオ、データセキュリティ等の基本情報を記載した情報収集フォームを提出。また、国

及び地方の関係機関の要求により申告又は承認申請(データセキュリティ審査や越境評価等)が必要な場合には、該当する申請書類を提出。

2. 法律事務所作成の「第三者証明資料」の提出

データ提供者が法律事務所に依頼して作成した、当該データ取引における法的リスクを開示したコンプライアンス評価報告書を提出。

3. 提出された上記資料をもとに、深センデータ取引所がデータの越境、取扱、流通、管理、技術的措置、合法性、安全性等に関する包括的なコンプライアンス評価を実施。

五十、公共データ運営主体が、公共データを国外主体に対して使用許諾又は開放・共有することはできるか？

「データ基本制度の構築によりデータ要素の作用をよりよく発揮させることに関する意見」(以下、「データ二十条」という)では、データを公共データ、企業データ、個人データに分類している³⁴。「データ二十条」及び各地方政府のデータ条例や公共データ運営に関する行政法規・規則によれば、公共データとは、各級の共産党・政府機関、企業・事業単位が法律に基づき職務を遂行又は公共サービスを提供する過程で生成されるデータを指す。このような公共データ運営の背景において本問題を検討すると、もう一つの論点が浮かび上がる。それは、各地の公共データ運営は「原始データを域外に出さない、データを閲覧せずに処理可能にする」という原則に基づいて行われていることから、公共データ運営主体が言及する公共データとは、一般的に原始データや初期的に処理された公共データ資源ではなく、公共データの使用許諾や条件付き共有・開放の段階における公共データ製品を指すことである³⁵。

³⁴ 「データ基本制度の構築及びデータ要素のより良い活用に関する意見」(三)データ財産権の構造的分置制度の模索。公共データ、企業データ、個人データの分類・階層化による権利確定及び許諾制度を確立する。中国政府網 (www.gov.cn)

³⁵ ここでいうデータ製品は広義のものであり、統計データ、データセット、データサービス、データアプリケーション、狭義のデータ製品等を含むが、これらに限らない。例えば、モデルや検証といったプロダクト・サービスの形で社会に提供されるデータ製品も含まれる。

各地方のデータ条例や公共データ運営に関する行政法規・規則によれば、公共データは適法かつ安全という前提の下で、外部への使用許諾又は開放・共有が可能となっている。特に、多くの省や市の地方政府は、公共データについて、分類・等級付けの結果に応じて、条件付きで使用許諾や開放・共有できるとする制度を設置している。一方で、「データ二十条」では、公共データの運営主体が個人のプライバシー保護、公共安全の確保という前提の下で、「原始データを域外に出さない、データを閲覧せずに処理可能にする」という原則に基づき、モデル・検証等の製品・サービスの形で社会に提供することを奨励している。では、このような基本制度の下で、国外主体(特に、国内の公共データを用いてモデルトレーニングを行う国外企業)は、公共データの使用許諾や開放・共有の対象となり得るのだろうか？

これは比較的複雑な問題であり、許諾元の具体的な運営モデルに基づいて個別に分析する必要がある。現行の法律・規則には、このような使用許諾や開放・共有を明確に禁止する規定は存在しないため、法令遵守と安全性の要件を満たせば、国外主体も技術的に可能な方法を通じて国内の公共データを取得できると解される。法的観点からは、公共データの国外への使用許諾や開放・共有について、国外主体は以下の点に留意する必要がある。

まず、「データ越境流通の促進及び規範化に関する規定」によれば、国外主体が国内の公共データを取得することは、データ越境に該当する。この種の公共データの越境においては、具体的なシチュエーションや製品に応じて、同規定に基づき適切なデータ越境に関する義務を履行する必要がある。

認められないか、又はデータセキュリティ審査及び改善を経た後でなければ越境できない。また、「データセキュリティ法」によれば、国外主体が合法的に公共データを取得できた場合でも、データの現地保管や輸出管理その他の法的要件や制限に直面する可能性がある。これらの問題については、本実務 Q&A の関係箇所を参照されたい。

さらに、公共データに個人情報が含まれる場合、公共データの越境は当初の収集・取得時の目的及び範囲を超えて行われるものであることから、データ提供者は「個人情報保護法」に基づく義務を履行する必要がある。例えば、個人への告知と

越境に関する個別の同意の取得等の手続が必要となる。具体的な要件については、本実務 Q&A の関係箇所を参照されたい。ただし、このような告知や同意の取得には適切なチャンネルが必要であるが、公共データの分野では一般的にそのようなチャンネルの確保が難しいことも予想される。また、公共データ運営企業と国外主体との間で、データ提供者及びデータそのものを十分に保護するデータ許諾又は開放・共有契約を締結することも必要となる（標準契約を締結してデータを越境する場合は、標準契約の要件に従い契約を締結する必要がある）。例えば、契約において、データ提供者の許可なくして、国外主体はデータを第三者に譲渡・共有・許諾してはならないとする条項を明確に定めることで、公共データの安全な使用を確保することが考えられる。

加えて、公共データの使用許諾や開放・共有の分野では、「原始データを域外に出さない、データを閲覧せずに処理可能にする」という原則に厳格に従ってデータを運営する必要があることから、国外主体はプライバシーコンピューティングやサンドボックス技術等を活用し、公共データ運営プラットフォーム上で自らが必要とするデータやデータの結果を取得することが必要となる可能性がある。このため、国外主体は公共データ運営者に対し、自らのデータモデルを提供する必要性が生じる可能性があり、これにより国外主体がその管轄区域内でデータ越境の適法性に関する問題に直面する可能性がある。また、データモデルと「閲覧せずに処理可能」なデータを組み合わせることにより生成されたデータを越境することに関しても、適法性の問題に直面する可能性がある。

以上のとおり、公共データの越境は、公共データ分野における「データの適法性」と「データ越境の適法性」という 2 つの問題に関わるものであるため、公共データ運営主体及び国外主体は、同様の問題に直面した場合、できるだけ早期に法律の専門家に相談を行うことが望ましい。

別紙1 国家・各地方省レベルインターネット情報機関の連絡先

機関名	所在地	連絡先
国家インターネット情報弁公室	北京市西城区車公莊大街11号	データ越境安全評価申告 :010-55627135
		個人情報越境標準契約届出 :010-55627565
		個人情報保護認証申請 :010-82261100
北京市インターネット情報弁公室	北京市朝陽区華威南路弘善家園413号	010-67676912
天津市インターネット情報弁公室	天津市河西区梅江道20号	022-88355322
河北省インターネット情報弁公室	河北省石家莊市橋西区維明南大街79号	0311-87909716
河南省インターネット情報弁公室	河南省鄭州市金水区金水路16号	0371-65901067
浙江省インターネット情報弁公室	浙江省杭州市西湖区省府路29号	0571-81051250
上海市インターネット情報弁公室	上海市徐匯区宛平路315号	021-64743030-2711
江蘇省インターネット情報弁公室	江蘇省南京市建鄴区白竜江東街8号	025-63090194
福建省インターネット情報弁公室	福建省福州市鼓楼区北大路133号	0591-86300613
安徽省インターネット情報弁公室	安徽省合肥市包河区中山路1号	0551-62606014
重慶市インターネット	重慶市渝北区青竹東路6号	023-63151805

機関名	所在地	連絡先
情報弁公室		
貴州省インターネット 情報弁公室	貴州省貴陽市雲岩区宝山北路 39号	0851-82995001/ 82995061
山東省インターネット 情報弁公室	山東省済南市市中区経十路 20637号	0531-51773249/ 51771297
広東省インターネット 情報弁公室	広東省広州市越秀区中山一路 104号	020-87100794/ 87100793
陝西省インターネット 情報弁公室	陝西省西安市雁塔区雁塔路南 段10号	029-63907136
甘肅省インターネット 情報弁公室	甘肅省蘭州市城関区南昌路 1648号	0931-8928721
山西省インターネット 情報弁公室	山西省太原市迎沢区五一路36 号	0351-5236020
江西省インターネット 情報弁公室	江西省南昌市紅谷灘区臥竜路 999号	0791-88912737
雲南省インターネット 情報弁公室	雲南省昆明市西山区日新中路 516号	0871-63902424
湖北省インターネット 情報弁公室	湖北省武漢市武昌区水果湖路 268号	027-87231397
湖南省インターネット 情報弁公室	湖南省長沙市芙蓉区韶山北路 1号	0731-81121089
青海省インターネット 情報弁公室	青海省西寧市海湖新区文景街 32号	0971-8485510
遼寧省インターネット 情報弁公室	遼寧省瀋陽市和平区光荣街26 号甲	024-81680082
吉林省インターネット 情報弁公室	吉林省長春市朝陽区新発路 666号	0431-82761087

機関名	所在地	連絡先
黒竜江省インターネット情報弁公室	黒竜江省哈爾濱市南崗区華山路 12 号	0451-58685723
海南省インターネット情報弁公室	海南省海口市国興大道 69 号	0898-65380723
四川省インターネット情報弁公室	四川省成都市青羊区桂花巷 21 号	028-86601862
広西チワン族自治区インターネット情報弁公室	広西チワン族自治区南寧市青秀区民族大道 112 号	0771-2093017/ 2093049
寧夏回族自治区インターネット情報弁公室	寧夏回族自治区銀川市金鳳区康平路 1 号	0951-6668938
西藏自治区インターネット情報弁公室	西藏自治区拉薩市城関区農科路 7 号	0891-6591509
内蒙古自治区インターネット情報弁公室	内蒙古自治区呼和浩特市賽罕区銀河南街 8 号	0471-4821277
新疆ウイグル自治区インターネット情報弁公室	新疆ウイグル自治区烏魯木斉市新市区西環北路 2221 号	0991-2384855
新疆生産建設兵団インターネット情報弁公室	新疆ウイグル自治区烏魯木斉市天山区中山路 462 号	0991-2899091

「実務 Q&A」発行

威科先行

共同発表機関及び著者

環球法律事務所

孟潔 李玲 劉展 張桐 林奕 田梓儀 王紫璇

對外經濟貿易大学 デジタル経済及び法律イノベーション研究センター
許可

蔚来控股有限公司

高崗 王詩笋

奇安信科技集团有限公司

馬蘭 劉前偉 劉洪亮

北京奧美互動諮詢有限公司

殷振華

杭州有贊科技有限公司

方子雯 陳昕 魏東傑

その他

郭俊彤 田亮 王程 董傑睿 尹童暉

翻訳

環球法律事務所 日本業務チーム

免責事項及び著作権情報

免責事項:

本文書は、共同発表機関による関連問題に関する法的意見を示すものではありません。本文書の全部又は一部の内容に基づく何らかの決定及びそれによって生じた結果については、行為者自身が責任を負うものとします。法的意見又はその他の専門的な助言が必要な場合は、関連資格を有する専門家に相談してください。

著作権:

本文書に関するすべての権利は、共同発表機関が保有します。すべての共同発表機関の書面による許諾を得ない限り、いかなる者も、いかなる形式又は方法によっても、本文書の著作権で保護された内容を複製又は配布してはなりません。

連絡先:

E. liushujun@glo.com.cn

E. GLO-JP-Newsletter@glo.com.cn

