

サイバーセキュリティと データ管理監督法制 の実務上のポイント

～中国の安全保障貿易管理に関する制度情報
専門家による政策解説～

2021年11月

日本貿易振興機構（ジェトロ）

北京事務所

海外調査部

【免責条項】

本レポートは、北京市環球法律事務所に委託し、作成したものです。
本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用下さい。ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益等を被る事態が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承下さい。

1. 企業からの問い合わせが多い点

(1) 「データ三法」の関係とは？

「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」）、「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」）および「中華人民共和国個人情報保護法」（以下、「個人情報保護法」）（以下、これらを総称して「データ三法」）は、それぞれ独自の立法目的や規制内容を有していますが、重複して適用される点が多くあります。

例えば、個人情報の取り扱いについては、「個人情報保護法」だけでなく、「データセキュリティ法」の規定も適用されます。なぜなら、「データセキュリティ法」第 3 条によると、「データ」とは、「電子的またはその他の方式による、情報に対するあらゆる記録」と定義され、「個人情報」は「データ」に含まれるためです。したがって、企業が個人情報を取り扱う際には、「個人情報保護法」だけでなく、「データセキュリティ法」に定められたルールも遵守する必要があります。なお、個人情報は、「データセキュリティ法」に定める「重要データ」に該当する可能性があります。また、「サイバーセキュリティ法」第 37 条において、「個人情報および重要データは国内にて保管しなければならない」と、個人情報と重要データを並列させていることからみると、個人情報だからといって必ずしも重要データに該当するわけではないと解されます。ただし、「自動車データ安全管理規定（試行）」第 3 条によると、自動車分野において「10 万人分を超える個人情報」は重要データに該当する、と定められているため、他の分野においても、一定数量に達した個人情報は重要データと見なされる可能性があります。

また、「サイバーセキュリティ法」に定めるネットワークデータ（ネットワークを通じて収集、保管、伝送、処理および発生する各種電子データ）に該当するデータの取り扱いについては、「データセキュリティ法」だけでなく、「サイバーセキュリティ法」の規定も適用されます。「データセキュリティ法」第 27 条では、「インターネット等の情報ネットワークを利用してデータを取り扱う活動を展開するにあたっては、サイバーセキュリティ等級保護制度に基づき、データセキュリティ保護義務を履行しなければならない」と定めています。

(2) データの域外移転時の注意点は？

データの域外移転については、重要情報インフラ運営者に該当する場合は、中国国内で収集および発生した個人情報および重要データは国内で保管するものとし、業務上の必要性により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が国务院関係機関と共同で制定する規則に基づいて安全評価を行うことが義務付けられています（「サイバーセキュリティ法」第 37 条）。

また、重要情報インフラ運営者に該当しない個人情報取り扱い者は、業務等の必要により、確かに中国国外に個人情報を提供する必要がある場合、次の各号に掲げる要件の 1 つを備えなければならないと定められています（「個人情報保護法」第 38 条）。

(a) 取り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するときは、国家インターネット情報機関による安全評価に合格していること

(b) 国家インターネット情報機関の規定に従い、専門機関による個人情報保護の認証を

受けていること

(c) 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、国外の移転先と契約を締結し、両当事者の権利および義務を取り決めること

(d) 法律、行政法規または国家インターネット情報機関の定めるその他の要件

中国が締結し、または参加する国際条約、協定に中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場合には、その規定に従い執行することができます。

なお、重要情報インフラ運営者に該当しないデータ取り扱い者が中国国内で収集および発生した重要データに関する域外移転セキュリティ管理規則（未公布）は、国家インターネット情報機関が國務院関係機関と共同で制定される予定です（「データセキュリティ法第 31 条」）。

(3) どのようなデータが重要データに該当するか？

「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調整メカニズムは、関係機関を統括・調整し、重要データ目録を制定する」「各地域、各機関は、自地域、自機関および関連業界、分野の重要データの具体的な目録を確定し、目録に掲載されたデータについて、重点的な保護を行わなければならない」と定めていますが、現時点では、どの業界の主管機関からも「重要データ目録」は制定・公表されていません。そのため、国家標準「情報安全技術 データ域外移転安全評価ガイドライン（草案）」の附録 A「重要データ識別ガイドライン」（27 の業界に分けて、重要データの範囲・識別の指針を示しています）や国家標準「情報安全技術 重要データ識別ガイドライン（意見募集稿）」等が、重要データの識別と認定において、参考になると考えられます。

さらに、特定の分野・業界の主管機関により、当該分野・業界における重要データの定義付けが行われています。例えば、前出の「自動車データ安全管理若干規定（試行）」では、自動車業界における重要データについて具体例が挙げられています。

2. 日本企業・日系企業が留意すべき点

前述のとおり、現時点では、「重要データ目録」は公表されていませんが、近い将来、公表される見通しです。企業は、「重要データ目録」が公表されるまで何もせずに待つのではなく、既存の法令・規則・標準（草案段階のものを含む）に基づき、あらかじめデータに関するコンプライアンス対策を講じることが望ましいと思われれます。具体的な対策としては、以下のようなものが挙げられます。

(1) データ取り扱いの現状を把握・整理

事業運営上、現状、どのような種類のデータを、どれくらいの頻度で、数量的にどのくらい取り扱っているか、また将来的に取り扱う可能性があるかについて把握し、種類（個人情報、公共のデータ、経営に関するデータ等）別にデータ分類し、リストを作成しておきます。

(2) セキュリティ上の脅威を整理・評価、対策を講じる

データの用途を確認し、発生しうるセキュリティ上の脅威の要素を整理し、脆弱性を点検します。データが破壊され、または漏洩した場合の国家安全や公共利益に与える潜在的な影響の程度を事前に評価・判断し、緊急対応マニュアルを策定する等の対策を講じます。

(3) 「データ三法」の要求に従い、自発的に重要データ保護措置を講じる

自社で取り扱うデータのうち、重要データに該当しうるものの有無を確認・整理します。自己評価の結果、重要データに該当しうる可能性が高いデータについては、「データ三法」の関連要求に基づき、自発的に重要データ保護措置（データセキュリティの責任者および管理部署の設置、全プロセスデータセキュリティ管理制度の確立、技術的な措置およびその他必要な保護措置等）を講じます。

3. 今後の見通し

現時点では、サイバーセキュリティとデータ規制における原則が既に確定されていますが、具体的に定めた細則は制定されておらず、不明瞭な事項に関する明文化が待たれます。日本企業・日系企業は、今後の法制定の動向や実務に与える影響に注意を払う必要があります。また、「データ三法」の要求を把握したうえで、早い段階から、実情を踏まえ、予防策・対応策を検討・策定し、データに関連する事件が発生したとき、その緊急度や重要度により、優先順位を決めて対応にあたることが重要です。

北京市環球法律事務所

レポートをご覧いただいた後、アンケート（所要時間：約 1 分）にご協力ください。

<https://www.jetro.go.jp/form5/pub/ora2/20210047>



本レポートに関するお問い合わせ先：
日本貿易振興機構（ジェトロ）
海外調査部 中国北アジア課
〒107-6006 東京都港区赤坂 1-12-32
TEL：03-3582-5181
E-mail：ORG@jetro.go.jp