JETRO
日本貿易振興機構（ジェトロ）

「データセキュリティ法」の概要

～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 12 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。

2021 年 6 月 10 日、第 13 期全国人民代表大会常務委員会第 29 回会議にて、「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）が可決・成立し、2021 年 9 月 1 日から施行されました。

「データセキュリティ法」は中国のデータ分野における基本法であり、データの概念を明確に定義するとともに、データ分類・等級付け保護、リスク評価、監視・早期警報、緊急対応等の各基本制度を確立し、データ取り扱い活動を行う際に履行すべき各義務を明確化しています。「データセキュリティ法」の施行は、中国におけるデータセキュリティ管理の規範化、デジタル産業の発展促進にとって重要な意味を持ちます。

1. 総体的国家安全観の堅持、中国共産党中央国家安全委員会の統括・調整下における業界データ規制メカニズムの確立

「データセキュリティ法」は総体的国家安全観[1]の貫徹を出発点としており、その第 1 条では、同法の立法目的として、「データ取り扱い活動を規範化し、データセキュリティを保障し、データの開発利用を促進し、個人、組織の合法的権益を保護し、国家の主権、安全および発展の利益を擁護する」ことを掲げています。

「データセキュリティ法」では、中国共産党中央国家安全委員会（2013 年 11 月 12 日設立、習近平総書記が委員長を務める。以下、「中央国安委員会」という）の統括・調整下における業界規制メカニズムを確立している。即ち、「中央国安委員会」の統括・調整の下で、各地域、各機関が自地域、自機関の業務において収集および生成したデータ並びにデータセキュリティについて責任を負い、工業、電気通信、交通、金融、天然資源、衛生健康、教育、科学技術等の主管機関が自業界、自分野におけるデータセキュリティ監督管理の職責を負うという体制を打ち出しています。また、公安機関、国家安全機関がデータセキュリティ監督管理の職責を負い、国家インターネット情報機関がネットワークデータセキュリティおよび関連監督管理業務の統括・調整の責任を負うとしています。

2.データを中核とするデジタル経済発展を促進

「データセキュリティ法」第 13 条では、「データ開発利用および産業発展によりデータセキュリティを促進すること、データセキュリティによりデータ開発利用および産業発展を保障することを堅持する」ことを掲げており、また、第 16 条では、「国は、データ開発利用およびデータセキュリティ技術に係る研究を支援し、データ開発利用およびデータセキュリティ等の分野における技術プロモーションおよびビジネスイノベーションを奨励し、データ開発利用およびデータセキュリティ製品、産業体系を育成し、発展させる」と定めています。

これらから分かるように、中国は今後、データセキュリティが保障されることを前提として、合法的に行われるデータの革新的な活用を奨励・支援していく構えです。現在の状況からすると、ビッグデータの応用、データセキュリティ技術製品および認証サービス、データ取引市場等においては、今後も大きな発展が期待されます。

---

[1] 総体的国家安全観は、2014 年 4 月に開催された中央国家安全委員会第 1 回会議において提示された国家安全保障についての概念で、政治、国土、軍事、経済、文化、社会、科学技術、情報、生態系、資源、核など幅広い分野を含むとされる。

3.域外適用の明確化

「データセキュリティ法」第 2 条では、「中華人民共和国国外においてデータ取り扱い活動を展開し、中華人民共和国の国家安全、公共利益または公民、組織の合法的権益を害する場合、法により法的責任を追及する」と定め、「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）および「中華人民共和国個人情報保護法」と同様、同法も域外適用されることを明確化しています。

4.データの分類・等級付け保護を義務付け

「データセキュリティ法」第 21 条では、国がデータ分類・等級付け保護制度を確立することを明確に示したうえで、各地域、各機関、各業界に対し、各自の司る範囲内の重要データの具体的な目録を確定し、重要データに対する保護を強化するよう求めています。また、「中核データ」という概念を打ち出し、国家安全、国民経済の命脈、重要な国民生活、重大な公共利益等に関わるデータは国の「中核データ」に属すとし、より厳格な管理制度を実行することを定めています。

現在、各地域、各機関では「データセキュリティ法」に基づく地方または業界のデータ分類等級付け規範の制定が進められています。例えば、工業情報化部弁公庁は工業データの分類・等級付けの基準を明確化した「工業データ分類・等級付けガイドライン（試行）」を公表しており、金融業界でも、業界標準たる「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）が公表されています。

5.データの国外移転に対する厳格な安全審査の実施

「データセキュリティ法」第 31 条では、重要情報インフラの運営者が中国国内における運営において収集および生成した重要データの国外移転に係るセキュリティ管理については、「サイバーセキュリティ法」の規定を適用すること、その他のデータ取り扱い者が中国国内における運営において収集および生成した重要データの国外移転に係るセキュリティ管理については、国家インターネット情報機関が国務院関係機関と共同で制定する管理弁法を適用することを定めています。「サイバーセキュリティ法」と比べると、「データセキュリティ法」の規定は重要データの国外移転により的を絞ったものとなっています。重要データの違法な国外移転に対する罰則は、「サイバーセキュリティ法」では 50 万元以下の過料とされていますが、「データセキュリティ法」では 1,000 万元以下の過料とされ、過料金額が大幅に引き上げられています。

また、「データセキュリティ法」では、国外機関による国内データの取得に対する対抗措置を定めています。具体的には、第 36 条において、「中華人民共和国の主管機関の認可を経ない限り、国内の組織、個人は、外国の司法または法執行機関に中華人民共和国国内に保管されるデータを提供してはならない」と定めています。同対抗措置は、法により域外の「ロングアーム管轄権（非居住者に対する司法管轄権）」に対応するための防御的な措置であると捉えられています。

6.国家データ安全審査制度の確立

「国家安全審査」制度は「中華人民共和国国家安全法」によって確立された制度です。「データセキュリティ法」第 24 条では、「国は、データ安全審査制度を確立し、国家安全に影響を与え、または影響を与えうるデータ取り扱い活動に対し国家安全審査を行う」と定め、データ分野の国家安全審査制度の構築を打ち出しています。データ安全審査の対象には、国家安全に影響を与え、または影響を与えうる全てのデータ取り扱い活動が含まれ、即ち、オンラインでのデータ取り扱い活動のみならず、オフラインでのデータ取り扱い活動も含まれます。

また、「データセキュリティ法」第 24 条第 2 項では、「法により行った安全審査決定は、最終決定とする」と定めているため、審査決定について、行政不服申立ておよび行政訴訟によって異議を申し立てることはできません。

7.違法行為に対する罰則の強化

「データセキュリティ法」では、規定に従いデータセキュリティ保護義務を履行しない、国家安全、公共利益または公民、組織の合法的権益を害する、規定に従って国外に重要なデータを提供しない、公安機関、国家機関のデータ取得に協力しない、審査・認可を経ずに外国の司法または法執行機関にデータを提供する等、さまざまな違法行為を行った個人または組織に対し、最高 1,000 万元の課徴金の賦課、状況に応じた関連業務の一時停止、営業停止命令、関連業務許可証、営業許可証の取り消しといった厳しい処罰を与えるとしています。また、犯罪を構成する場合、法により刑事責任を追及するとしています。

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/ora2/20210056

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