BLJ法律事務所
東京都千代田区永田町2丁目14番3号　東急不動産赤坂ビル307号室 〒100-0014
TEL. 03-3503-8061　FAX. 03-3503-8062　URL. www.bizlawjapan.com　Email. info@bizlawjapan.com

中国の個人情報・データ安全に係る3つの法律の概要と対応策

遠藤　誠[1]

Ⅰ．はじめに

中国では、従来、「ネットワーク安全法」[2]（2017年6月1日施行）[3]が公布・施行されていたが、2021年になって２つの法律、即ち、「データ安全法」[4]（2021年9月1日施行）[5]及び「個人情報保護法」（2021年11月1日施行）[6]が公布・施行されたことにより、中国の個人情報・データの安全[7]に関する法律が出揃った。

中国は、近時、習近平政権が2014年から推進している「総体的国家安全観」の下、「国家の安全」に重きを置いて規制を強化する動きにあり、上記三法もその中に位置付けられる。

既に、さまざまな細則等が施行され、意見募集稿が公表されているが、今後も引き続き、細則等の公布が行われるであろう。最近になって施行された細則等としては、以下のものがある。

・「情報安全技術　個人情報安全規範」（国家標準GB/T　35273－2017／2020）（2020年3月6日公布）[8]

・最高人民法院による「顔認証技術を使用した個人情報処理に関連する民事事件の審理への適用法律についての若干問題に関する規定」（2021年8月1日施行）[9]

・「重要情報インフラ安全保護条例」[10]（2021年9月1日施行）

・「ネットワーク製品セキュリティホール管理規定」（2021年9月1日施行）[11]

---

1 えんどう　まこと、弁護士・博士（法学）、ＢＬＪ法律事務所（ https://www.bizlawjapan.com/ ）代表。

2 「ネットワークセキュリティ法」、「サイバーセキュリティ法」、「インターネットセキュリティ法」等とも訳される。

3 http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm

4 「データセキュリティ法」等とも訳される。

5 http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

6 http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

7 日本語では「セキュリティ」と称されることも多いが、本稿では、原則として、中国語原文に合わせ「安全」という語を用いることとする（例外としては、「セキュリティホール」等）。

8 個人情報保護法が施行されたことから、近い将来、改正される可能性がある。強制標準ではなく、奨励標準であるので、法的強制力は有しないが、事実上、奨励標準を遵守する必要があると一般にいわれている。

9 http://www.court.gov.cn/fabu-xiangqing-315851.html

10 「重要情報インフラセキュリティ保護条例」等とも訳される。

11 http://www.gov.cn/zhengce/zhengceku/2021-07/14/content_5624965.htm

・「ネットワーク安全審査弁法」（2022年2月15日施行）[12]

本稿では、まず、「ネットワーク安全法」、「データ安全法」及び「個人情報保護法」という3つの法律の概要及び三法の関係について解説し、次に、日本企業及び中国現地法人の対応策について検討することとしたい。

Ⅱ.「ネットワーク安全法」の概要

全79条からなるネットワーク安全法の概要は、以下のとおりである。

1. 用語の定義

（1）ネットワーク安全法は、以下のとおり、用語の定義を規定している（76条）。

①「ネットワーク」とは、コンピュータその他の情報端末及び関連設備により構成され、一定の規則及びプログラムに基づき、情報の収集・伝送・交換・処理を行うシステムをいう。これは、企業内のネットワークも含み、「インターネット」よりも広い概念である。

②「ネットワーク安全」とは、必要な措置を講じることにより、ネットワークへの攻撃、侵入、妨害、破壊、不法な使用及び想定外の事故を防止し、ネットワークを安定的に運用し、ネットワークデータの完全性、秘密保持性、利用可能性の各能力を保障することをいう。

③「ネットワーク運営者」とは、ネットワークの所有者、管理者及びネットワークサービス提供者をいう。

④「ネットワークデータ」とは、ネットワークを通じて収集・保存・伝送・処理及び生産される各種の電子データをいう。

⑤「個人情報」とは、電子その他の方式によって記録され、それ単独で又は他の情報と結合して、自然人個人の身分を識別できる各種情報をいう。これには、自然人の氏名、生年月日、身分証明書番号、生物的個人識別情報、住所、電話番号等を含むが、これらに限られない。

（2）また、「重要情報インフラ安全保護条例」2条によると、「重要情報インフラ」とは、「公共通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政府、国防科学技術産業等の重要な産業・分野、並びにその他の破壊、機能喪失又はデータ漏洩があると、国家安全保障や国民生活、公共の利益が著しく損なわれる可能性がある重要なネットワーク設備、情報システム等をいう。

2. ネットワーク安全の監督管理

中国域内（香港、マカオ、台湾を除いた中国本土内。以下同じ）において構築、運営、維

12 「ネットワークセキュリティ審査弁法」等とも訳される。

持及び使用されるネットワーク及びネットワーク安全の監督管理について、ネットワーク安全法が適用される（2条）。前述したとおり、「ネットワーク」の定義に鑑みると、ネットワーク安全法の適用範囲は、インターネットに限定されないと考えられる。

中国政府は、中国内外のネットワーク安全へのリスク及び脅威を監視、防御、処置するために各種の措置を講じ、重要情報インフラが攻撃、侵入、妨害及び破壊されないように保護し、ネットワーク空間の安全及び秩序を維持しなければならない（5条）。国家は、誠実信用を守り、健康的・文明的なネットワーク行為を提唱し、社会主義における基本的価値観を伝授するよう推し進め、全社会のネットワーク安全の意識及び水準を向上させ、全社会がネットワーク安全の良好な環境の促進に共同で参与するよう措置を講じる（6条）。国家ネットワーク情報部門は、ネットワーク安全業務及び関連監督管理業務を統一的に協調させることに責任を負う。国務院電信主管部門、公安部門その他の関連部門は、ネットワーク安全法及び関連法律、行政法規の規定に基づき、それぞれの職責の範囲内においてネットワーク安全保護及び監督管理業務に責任を負う（8条）。いずれの個人及び組織もネットワークを使用するにあたっては、憲法及び法律を遵守し、公共秩序を遵守し、社会マナーを尊重するものとされ、ネットワーク安全に危害を及ぼしてはならず、ネットワークを利用して国家の安全、名誉及び利益に危害を及ぼし、国家政府の転覆を扇動し、社会主義制度を覆し、国家分裂を扇動し、国家統一を破壊し、テロリズム、過激主義を宣揚し、民族蔑視、民族差別を宣揚し、暴力・わいせつ情報を頒布し、虚偽情報を編集・頒布し、経済秩序及び社会秩序を攪乱し、他人の名誉・プライバシー・知的財産権及びその他の合法的権益等を侵害する活動に従事してはならない（12条2項）。このように、ネットワーク安全法は、「ネットワークやユーザーの安全」というよりも、「国家の安全」に重きを置いているということができる。

ネットワーク運営者が経営及びサービス活動を展開するにあたっては、法律・行政法規を遵守し、社会マナーを尊重し、商業道徳、誠実信用を遵守し、ネットワーク安全保護義務を履行し、政府及び社会的監督を受け、社会的責任を負わなければならない（9条）。ネットワークの構築、運営又はネットワークを通じてサービスを提供するにあたっては、法律・行政法規の規定及び国家標準の強制的要求に従い、技術的措置その他の必要な措置を採り、ネットワーク安全及び安定的運営を保障し、ネットワーク安全に係る事件に効果的に対応し、ネットワークの違法犯罪活動を防止し、ネットワークデータの完全性、秘密性及び利用可能性を維持しなければならない（10条）。

３．ネットワーク安全のシステム構築・サービス奨励

中国政府は、ネットワーク安全標準システムを構築、整備しなければならない。国務院標準化行政主管部門及び国務院の他の関連部門は、それぞれの職責、組織に基づき、関連ネットワーク安全管理及びネットワーク製品、サービス及び運営安全の国家標準、業界標準を制定し、かつ適時に改正しなければならない（15条）。

中国政府は、ネットワーク安全社会化サービスの構築を推進し、関連する企業・機構にネ

ットワーク安全認証・検査・リスク評価等の安全サービスを展開するよう奨励しなければならない（17条）。

４．ネットワーク運営の安全

中国政府は、ネットワーク安全等級保護制度を実施する。ネットワーク運営者は、ネットワーク安全等級保護制度の要求に基づき、以下に掲げる安全保護義務を履行し、ネットワークが妨害、破壊又は無権限のアクセスを受けないよう保障し、ネットワークデータが漏洩、盗用又は改竄されることを防止しなければならない（21条）。

①内部の安全管理制度及び操作規程を制定し、ネットワーク安全責任者を確定し、ネットワークの保護責任を徹底すること。

②コンピュータウイルス、サイバー攻撃、ネットワーク侵入等のネットワーク安全に対する危害を与える行為を防止するための技術的措置を講じること。

③ネットワーク運営状態、ネットワーク安全に係る事件を監視・記録する技術的措置を講じ、かつ関連するネットワークログファイルを6か月以上保存すること。

④データの分類、重要なデータのバックアップ及び暗号化等の措置を講じること。

ネットワーク製品・サービスは、関連する国家標準の強制的要求に合致しなければならない。ネットワーク製品・サービスの提供者は、悪意のプログラムを設置してはならない。ネットワーク製品・サービスにセキュリティ上の欠陥、弱点等のリスクを発見したときは、即座に救済措置を採り、遅滞なくユーザーに告知し、かつ関連主管部門に報告しなければならない（22条1項）。ネットワーク運営者は、ユーザーのために、ネットワーク接続加入、ドメイン名登録サービスの手続を行い、固定電話・携帯電話等のネットワーク加入手続を行い、又はユーザーのために情報発信、インスタントメッセージ等のサービスを提供し、ユーザーと契約書を締結し又は提供サービスを確認するとき、ユーザーに「真実の身元情報」を提供するよう求めなければならない。ユーザーが「真実の身元情報」を提供しない場合、ネットワーク運営者は、その者のために関連サービスを提供してはならない（24条1項）。上記のように、ネットワーク安全法は、ネットワーク運営者に対し、ユーザーの実名等の「真実の身元情報」の確認を義務付けているが、「真実の身元情報」の確認義務については、2014年3月15日施行の「ネットワーク取引管理弁法」（中国語では「網絡交易管理弁法」）第7条、第8条に規定がある[13]。この「ネットワーク取引管理弁法」は、2010年7月1日施行の「ネットワーク商品取引及び関連サービス行為に関する管理暫定規則」（中国語では「網絡商品交易及有関服務行為管理暫行弁法」）を改正したものであるが、この2010年の暫定規則の第10条にも、同様の規定が含まれていた[14]。しかし、ネットワーク安全法は、法律レベルで、ネットワーク運営者に対し、ユーザーの実名等の「真実の身元情報」の確認を全面的に義務

13 https://www.jetro.go.jp/ext_images/world/asia/cn/ip/law/pdf/admin/20140315.pdf
14 https://www.jetro.go.jp/ext_images/world/asia/cn/ip/law/pdf/section/20100531.pdf

付けている点で、重要であるといえる。

ネットワーク製品・サービスの提供者は、その製品・サービスのため継続して安全維持を提供し、規定された又は当事者が約定した期限内において、安全維持の提供を停止してはならない（22条2項）。ネットワーク製品・サービスにユーザー情報を収集する機能がある場合、提供者は、ユーザーに明示しかつ同意を得なければならない。ユーザーの個人情報に係る場合、ネットワーク安全法及び関連法律、行政法規の個人情報保護に関する規定を遵守しなければならない(22条3項)。ネットワークの重要設備及びネットワーク安全専用製品は、国家標準に関する強制的要求に基づき、資格を有する機構による安全認証合格、又は安全検査の要求に合致した後にはじめて販売又は提供することができる。国家ネットワーク情報部門は、国務院の関連部門とともに、ネットワーク重要設備及びネットワーク安全専用製品目録を作成し[15]、かつ安全認証及び安全検査の結果の相互認証を推し進め、認証・検査の重複を回避する（23条）。ネットワーク運営者は、公安部門、国家安全部門の国家安全の維持及び犯罪捜査の活動のために、技術的サポート及び協力を提供しなければならない(28条)。

国家は、公共通信及び情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政府等の重要分野、並びにその他の破壊、機能喪失又はデータ漏洩に一度でも遭遇すると国家安全、国家経済、人民生活、公共利益に重大な危害がもたらされるおそれがある情報インフラに対し、ネットワーク安全等級保護制度の基礎の上で、重点的保護を実行する（31条1項）。重要情報インフラの運営者のネットワーク製品及びサービスの購入が、国家安全に影響を及ぼす可能性がある場合は、国家ネットワーク情報部門が国務院の関連部門とともに組織する国家安全審査を受けなければならない（35条）。重要情報インフラの運営者のネットワーク製品及びサービスの購入にあたっては、提供者との間で秘密保持契約を締結し、秘密保持義務を明確にしなければならない（36条）。重要情報インフラの運営者は、域内の運営において収集・発生した個人情報及び重要なデータについて、域内において保存しなければならない[16]。業務上の必要により域外に提供しなければならない場合、国家ネットワーク情報部門と国務院の関連部門がともに制定した弁法[17]に基づき、安全に関する評価を行わなければならない（37条）。以上のように、重要情報インフラの運営者に対しては、重い責任が課されているものの、日本企業又はその中国現地法人が「重要情報インフラの運営者」に該当することは、ほとんど無いものと思われる。

５．ネットワーク情報の安全

ネットワーク運営者は、収集したユーザー情報を厳格に秘密として保持し、かつ健全なユ

15 2017年6月1日に、「ネットワーク重要設備及びネットワークセキュリティ専用製品目録（第一期）」が発布された。
16 2017年7月、アップル社は、ネットワーク安全法に対応するため、中国のインターネット企業と提携し、データセンターを中国域内に設立することを発表した。
17 2021年12月28日に、「ネットワーク安全審査弁法」が公布された。

ーザー情報保護制度を構築しなければならない（40条）。ネットワーク運営者が個人情報を収集・使用するにあたっては、合法・正当・必要の原則を遵守し、収集・使用の規則を公開し、情報の収集・使用の目的、方式及び範囲を明示し、かつ被収集者の同意を得なければならない。ネットワーク運営者は、それが提供するサービスと無関係な個人情報を収集してはならず、法律、行政法規の規定及び双方の約定に違反して、個人情報の収集・使用を行ってはならず、かつ法律、行政法規の規定及びユーザーとの約定に基づき、それが保存する個人情報を処理しなければならない（41条）。

いかなる個人及び組織も、個人情報を盗用その他の不法な方法で取得してはならず、不法に販売し又は不法に他人に個人情報を提供してはならない（44条）。いかなる個人及び組織も、そのネットワーク使用行為に対して責任を負わなければならず、詐欺、犯罪方法の伝授によって、禁制品、規制物品等の製作又は販売等の違法犯罪活動のウェブサイト、ニュースサイトを開設してはならず、ネットワークで公開された詐欺の実施、禁制品、規制物品及びその他の違法犯罪活動に係る情報を利用してはならない（46条）。

６．監視警告及び緊急時の対応処置

国家ネットワーク情報部門は、関連部門が健全なネットワーク安全リスク評価、及び緊急業務メカニズムの構築に協力し、ネットワーク安全事件の緊急対応マニュアルを制定し[18]、かつ定期的に演習を実施する。ネットワーク安全事件緊急対応マニュアルは、事件発生後の危害の程度、影響範囲等の状況に基づき、ネットワーク安全事件をレベル分けし、相応の応急処理措置を定めておくものとされている（53条）。

ネットワーク安全事件によって突発的事件又は安全事故が発生した場合、「突発事件対応法」、「安全生産法」等の関連法律、行政法規の定めに基づき処置される（57条）。国家安全及び社会公共秩序を維持し、重大な突発的社会安全事件を処置する必要のため、国務院の決定又は承認を得た上で、特定区域においてネットワーク通信に対し制限を設ける等の臨時的措置を講じることができる(58条)。

７．法律責任

ネットワーク運営者がネットワーク安全保護義務を履行しなかった場合、関連主管部門は、是正を命じ、警告を与える。ネットワーク運営者が是正を拒否し又はネットワーク安全に危害をもたらす等の結果をもたらした場合、1万元以上10万元以下の過料を課し、直接の責任を負う主管人員に対し5千元以上5万元以下の過料を課すものとされている（59条1項）。

重要情報インフラ運営者がネットワーク安全保護義務を履行しなかった場合、関連主管部門は、是正を命じ、警告を与える。重要情報インフラ運営者が是正を拒否し又はネットワ

[18] 2017年6月27日に、「国家ネットワーク安全事件緊急対応マニュアル」が発布された。

ーク安全等に危害をもたらす等の結果をもたらした場合、10 万元以上 100 万元以下の過料を課し、直接の責任を負う主管人員に対し、1 万元以上 10 万元以下の過料を課すものとされている（59 条 2 項）。

ネットワーク安全に危害をもたらす活動に従事し、ネットワーク安全に危害をもたらす活動に従事する専用プログラム、ツールを提供し、又は他人がネットワーク安全に危害をもたらす活動に従事するために技術的サポートの提供、広告宣伝、支払精算等の協力をしたが、犯罪を構成しない場合、公安部門が違法所得を没収し、5 日以下の拘留に処し、かつ 5 万元以上 50 万元以下の過料を併せて課すことができる。情状が比較的重い場合、5 日以上 15 日以下の拘留に処し、かつ 10 万元以上 100 万元以下の過料を併せて課すこともできる（63 条 1 項）。

治安管理処罰を受けた人員は、5 年間はネットワーク安全管理及びネットワーク運営の重要業務に従事してはならない。刑事処罰を受けた人員は、ネットワーク安全管理及びネットワーク運営の重要業務に終身間、従事してはならない（63 条 3 項）。

ネットワーク運営者がネットワーク安全法の規定に違反し、以下に掲げる行為のいずれかを行った場合、関連主管部門が是正を命じる。是正を拒否し又は状況が重大である場合、5 万元以上 50 万元以下の過料を課し、直接の責任を負う主管人員及びその他の直接の責任人員に対し、1 万元以上 10 万元以下の過料を課すものとされている（69 条）。

①関連部門の要求に基づき、法律、行政法規が発布又は伝送を禁止した情報について、伝送の停止、削除等の処分措置を講じなかった場合。

②関連部門が法により実施する監督検査を拒絶、妨害した場合。

③公安部門、国家安全部門への技術的サポート・協力の提供を拒否した場合。

外国の機構、組織、個人が、中国の重要情報インフラに対する攻撃、侵入、妨害、破壊等の危害を及ぼす活動に従事し、重大な結果をもたらした場合、法により法的責任が追及される。国務院公安部門及び関連部門は、当該機構、組織、個人に対し、財産の凍結又はその他必要な制裁措置を採る決定をすることができる（75 条）。

Ⅲ.「データ安全法」の概要

全 53 条からなるデータ安全法の概要は、以下のとおりである。

１．立法目的、適用範囲及び用語の定義

本法はデータ安全を保護し、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、安全及び発展の利益を擁護するために制定されたものである（1 条）。

本法は、中国域内におけるデータ処理及びデータ安全の管理に適用される。また、中国域外におけるデータ処理により中国の国家の安全、公共の利益又は国民・組織の合法的権益を

損なう場合には、法に基づき法的責任を追及することができるとされている（2条）。

本法3条には、「データ」の関連用語の定義が規定されている。これらの定義によると、本法の適用対象は、電子・紙を問わず全ての情報ということになり、ネットワーク安全法や個人情報保護法の適用対象よりも広いといえる。

①「データ」とは、電子的又はその他の形態の情報の記録をいう。

②「データの処理」には、データの収集、保存、使用、加工、伝送、提供、公開等を含む。

③「データ安全」とは、必要な措置を講じることにより、データが効果的に保護され、合法的に使用可能な状態を保障し、且つ安全な状態を持続させる能力があることをいう。

２．執行機関及び職責

本法には、データ安全の管理及び各級執行機関の職責内容が規定されている。本法5条によると、中央国家安全保障指導機関が、国家のデータ安全の政策決定及び調整等を行い、国家のデータ安全調整機構及び仕組み（以下「国家データ安全業務協調メカニズム」という）を構築するものとされている。

各地域、各部門は、その管轄する業務において収集したデータとその安全に対し責任を負わなければならない。具体的な部門としては、工業、電気通信、交通、金融、天然資源、保健衛生、教育、科学技術等の重点分野が挙げられている。公安機関、国家安全機関及び国家インターネット情報部門も、業務の範囲内のデータ安全の監督管理の責任を負うものとされている。

３．データ安全の基本的制度

（１）データ分類別・等級別保護制度

本法21条によると、国は、①データの経済社会の発展における重要度、及び②改ざん、破壊、漏えい又は不正取得、不正利用に遭った場合の国家の安全、公共の利益又は国民・組織の合法的権益にもたらす危害の程度に応じて、データの分類別・等級別の保護を実施するものとしている。国家データ安全業務協調メカニズムにおいて、「重要データ保護リスト」が策定される。国家の安全、国民経済の発展、重要な国民の生活、主要な公共の利益に関するデータは、国家の核心データであり、より厳格な管理体制が求められる。各地域、各部門は、国の関連規定に基づき、管轄地域、部門、業界の重要データ保護リストを策定する。

（２）データ安全リスクの早期警戒及び緊急対応措置

本法22条によると、国は、集中的・統一的で、効果が高く、権威あるデータ安全のリスク評価、報告、情報共有、監視・早期警戒体制を構築し、国家データ安全業務協調メカニズムにより、データ安全のリスク情報の取得、分析、検討・判断、早期警戒を強化するものとされている。

また、本法23条によると、国は、データ安全緊急対応措置の仕組みを確立するものとさ

れている。データ安全に係るインシデントが発生した場合には、関係主管部門が法に基づき緊急対応策を実行し、相応の緊急対応措置を講じて、安全の危害の拡大を防止し、潜在的な危険を除去し、かつ速やかに社会公衆に向け注意喚起情報を発表しなければならない。

（３）データ安全審査制度

本法24条によると、国は、データ安全審査制度を構築し、国家の安全に影響し又は影響し得るデータ処理に対し、安全審査を行う。法に基づき下した安全審査決定は、最終決定とされる。

本法では、データ安全審査制度の具体的な内容は明確には規定されていない。「外国投資法」における投資安全審査制度や「ネットワーク安全審査弁法」における重要情報インフラ事業者の安全審査制度等にも関係する可能性があるため、今後、データ安全審査制度の具体的な内容に関する細則の公布が待たれる。

（４）データ域外移転の管理制度

本法25条によると、データの域外移転及び輸出規制については、国家の安全と利益の維持、国際義務の履行に関わる規制品目に該当するデータに対しては、法に基づき輸出規制を実施するものとされている。なお、2020年10月17日に公布された「輸出規制法」（「輸出管理法」とも訳される）[19]には、国際義務の履行に関わる貨物、技術、サービス等の品目の輸出管理の要件及び輸出管理の定義が定められている。

（５）差別待遇による外国制裁への対抗措置

本法26条には、他の国・地域がデータ及びデータの開発・利用技術等に関わる投資・貿易等において、中国に対し差別的な禁止、制限又はその他の類似の措置を講じた場合には、当該国・地域に対し、同等の措置を講じることができるとされている。2021年6月10日に公布・施行された「反外国制裁法」と同じ趣旨の規定といえよう。

４．データ安全の保護義務

本法4章では、国のデータ安全保護制度の下で、組織及び個人がデータに関する活動を行う際に遵守すべき義務が定められている。これには、以下のものが含まれる。

①データの処理を行う際には、安全確保のために、安全管理システムの構築・改善又は技術に関する教育研修等の必要な措置を講じること。ネットワークを利用した処理活動については、「ネットワーク安全法」におけるネットワーク安全等級制度に関する規定等の義務を履行すること（27条）。

②リスクモニタリングを強化すること。データ安全に脆弱性、バグ等のリスクが発見され

19 https://www.cistec.or.jp/service/china_law/20201019-kariyaku.pdf

た場合、直ちに対策を講じること。データ安全のインシデントが発生した場合、迅速にユーザーに通知し、且つ関連主管部門に報告すること（29条）。

③適法且つ正当な方式によりデータを収集すること（32条）。

④公安機関又は国家安全保障機関が、国家の安全の維持又は犯罪捜査のためにデータを入手する必要がある場合には、これに協力すること（35条）。

⑤中国の関連主管部門の認可を得ずに、中国域内に保存されているデータを、外国の司法機関又は法執行機関に提供してはならないこと（36条）。

なお、重要データ[20]処理者は、データ安全責任者及び管理機構を設置し、リスク評価を定期的に実施し、且つ主管部門へ報告しなければならない（30条）。重要情報インフラの運営者が、中国域内の業務の過程で収集・生成した重要データの域外移転の安全管理については、ネットワーク安全法の規定が適用される。その他のデータ処理者が、中国域内の業務の過程で収集・生成した重要データの域外移転の安全管理方法については、国家インターネット情報部門が国務院関連部門と制定する（31条）。この点に関し、「ネットワークデータ安全管理条例（意見募集稿）」によると、安全評価に合格していること、専門機関による個人情報保護認証を得ていること、「標準契約」に基づき域外の移転先と契約を締結していることのいずれかが必要である。「重要データ目録」も、近い将来、公布される予定である。データ取引仲介者は、仲介サービス提供に際し、データ提供者に当該データの出所の説明を求め、当該取引の当事者双方の身元を審査・確認し、審査及び取引の記録を作成・維持しなければならない（33条）。

５．法的責任

本法6章は、データ安全に関する各種の義務違反に対する法的責任を定めている。

例えば、①国家の核心データ管理制度に違反し、国家の主権、安全、発展の利益に危害を与えた者（45条2項）や、②重要データを外国に提供した重要情報インフラの運営者（46条）には、最高1,000万元（約1億7,000万円）の過料が課され、状況により、事業の一時停止、事業停止、事業許可の取消し、営業許可の取消しが命じられ、状況が重大な場合には刑事責任が追及されることがある。本法には、「国家の核心データ」や「重要データ」の明確な定義が規定されていない。具体的な規定により別途、補完されることが望ましい。

Ⅳ．「個人情報保護法」の概要

全74条からなる個人情報保護法の概要は、以下のとおりである。

20 「重要データ」の定義は、現時点では不明である。近い将来、「重要データ保護リスト」が公表されるものと思われる（本法21条）。

１．本法の適用範囲

本法は、中国域内の自然人の個人情報を取り扱う活動に適用されるのが原則である。しかし、①中国域内の自然人に製品又はサービスを提供する目的である場合、②中国域内の自然人の行動の分析と評価を行う場合、③その他、法律や行政法規で定められている場合のいずれかに該当するときは、中国域内の自然人の個人情報を取り扱う中国域外の活動にも適用される（3 条）。例えば、日本企業が中国語のウェブサイトにおいて自社商品を中国にいる中国人向けに販売する場合、本法が適用されることになると思われる。

また、上記の中国域外における個人情報取扱者は、中国域内に個人情報保護に関する事項を取り扱う専門機関を設置し又は代表者を指名し、関連機関の名称又は代表者の名称及び連絡先を個人情報保護担当部門に報告しなければならない（53 条）。

２．個人情報、センシティブ個人情報の定義

本法によると、「個人情報」とは、電子的又はその他の方法で記録された、既に識別され又は識別可能な自然人に関するあらゆる種類の情報であり、匿名化された情報を除くものとされている。個人情報の取扱いには、個人情報の収集、保管、使用、処理、送信、提供、開示、削除が含まれる（4 条）。

他方、センシティブ（中国語では「敏感」）個人情報とは、ひとたび漏洩したり不正に利用されたりすると、自然人の人間としての尊厳が侵害されたり、その人や財産の安全が脅かされたりするおそれのある個人情報であり、生体情報、信仰に関する情報、特定の身分情報、医療・健康情報、金融口座情報、軌跡情報等のほか、14 歳未満の未成年者の個人情報も含まれる。個人情報取扱者は、特定の目的と十分な必要性があり、厳格な保護措置が講じられている場合に限り、センシティブ個人情報を取り扱うことができる（28 条）。

３．個人情報の取扱いが許される場合

個人情報取扱者は、以下のいずれかの状況に該当する場合に限り、個人情報を取り扱うことができる（13 条 1 項）。

①本人の同意を得た場合

②本人が当事者となっている契約の締結・履行のため、又は法律で定められた労働規則や法律に基づいて締結された労働協約に従った人事管理の実施のために必要である場合

③法定の義務又は法的義務の履行のために必要である場合

④公衆衛生上の緊急事態に対応するため、又は緊急事態において自然人の生命、健康、財産を保護するために必要である場合

⑤公共の利益のためにジャーナリズム、世論調査等を行うことを目的とした合理的な範囲内で個人情報を取り扱う場合

⑥本人が自己開示した個人情報、又はその他の方法で合法的に開示された個人情報を、合理的な範囲内で、本法の規定に従って取り扱う場合

⑦その他、法律や行政法規で定められている場合

上記のうち、②乃至⑦の場合は、本人の同意が無くても、個人情報を取り扱うことができる（13条2項）。

個人情報取扱者は、個人情報を取り扱う前に、①個人情報取扱者の氏名又は名称及び連絡先、②個人情報の取扱目的、取扱方法、個人情報の種類、及び保管期間、③本法に基づいて個人が権利を行使することができる方法と手続、④その他、法律や行政法規で通知すべき事項を、真実、正確かつ完全な形で、分かりやすい言葉で、目立つように本人に通知しなければならない（17条1項）。

また、個別に本人の同意を得なければならない場合がある。例えば、①個人情報取扱者は、その取り扱う個人情報を、他の個人情報取扱者に提供する場合には、提供先の名称又は氏名、連絡先、取扱目的、取扱方法及び個人情報の種類を本人に通知し、別途同意を得なければならない（23条）。②センシティブ個人情報の取扱いについては、本人の同意を得なければならない（29条）。

４．個人情報の域外移転

個人情報取扱者が、業務上又はその他の理由で中国域外に個人情報を提供する真の必要性がある場合、以下のいずれかの条件を満たさなければならない（38条1項）。

①本法40条の規定に基づき、国家インターネット情報部門による安全評価に合格していること

②国家インターネット情報部門の規定に基づき、専門機関によって個人情報保護認証を得ていること

③国家インターネット情報部門の定めた標準契約[21]に基づき、域外の移転先と契約を締結しており、双方の権利義務を約定していること

④法律、行政法規又は国家インターネット情報部門の定めるその他の条件

個人情報取扱者は、中国域外に個人情報を提供する場合、海外の受取人の氏名又は名称、連絡先、取扱目的、取扱方法、個人情報の種類、海外の受取人との間で本法に基づく権利を

[21] 標準契約はまだ公表されていないが、「個人情報域外移転安全評価規則（意見募集稿）」13条によると、標準契約には、以下のような内容を記載することになると思われる。①個人情報域外移転の目的、類型、保存期限、②個人情報主体の権益が侵害された場合、自ら又は代理人を経由して、ネットワーク運営者若しくは個人情報受領者又はその双方に対して、損害賠償を請求することが可能であり、ネットワーク運営者又は個人情報受領者はそれを賠償しなければならないこと（責任がないことを立証できる場合を除く）、③個人情報受領者が所在国の法律環境の変更により、契約の履行が困難となった場合、契約を終了し、又は新たに安全評価を行うこと、④契約終了は、契約に定めるネットワーク運営者及び個人情報受領者の責任及び義務を免除するものではないこと（個人情報を廃棄し又は匿名化処理した場合を除く）。

行使するための方法及び手続を本人に通知し、本人の個別の同意を得なければならない（39条）。

①重要情報インフラの運営者、及び②個人情報の取扱量が国家インターネット情報部門の規定する数量に達した個人情報取扱者は、中国域内で収集・発生した個人情報を、域内で保存しなければならない。確かに域外に提供する必要がある場合、原則として、国家インターネット情報部門による安全評価に合格しなければならない（40条）。

５．個人情報取扱者による安全保護義務

個人情報取扱者は、以下の安全保護のための措置をとらなければならない（51条）。

①内部管理制度及び作業規程の制定
②個人情報の分類管理
③暗号化、非識別化等の安全技術的措置
④個人情報取扱いの操作権限の確定、社員に対する定期的な安全教育・研修
⑤安全関連事件が発生した場合の緊急対応マニュアルの作成

６．法的責任

本法66条乃至71条には、本法に違反した者の法的責任について規定されている。例えば、本法の規定に違反して個人情報が取り扱われている場合、又は本法に定める個人情報保護の義務を履行しないで個人情報が取り扱われている場合、個人情報保護担当部門は、是正を命じ、警告を発し、違法所得を没収し、法に違反して個人情報を取り扱っているアプリケーションのサービス提供の停止又は中止を命じ、是正を拒否した場合は100万元以下の過料を課し、直接の責任者及びその他の直接の責任者は、1万元以上10万元以下の過料を課される。上述の違法行為があり、状況が深刻な場合、個人情報保護を担当する省レベル以上の部門は、是正を命じ、違法所得を没収し、5,000万元以下又は前年売上高の5%以下の過料を課し、事業の停止又は是正を命じ、主管部門に通知して事業許可の取り消しを行うことができ、直接責任を負う者には、10万元以上100万元以下の過料を課し、一定期間、関連企業の董事、監事、高級管理職、個人情報保護責任者に就くことを禁止することを決定することができる（66条）。

Ⅴ．上記三法の関係

上記三法の適用関係を、どのように整合させればよいのかは、まだ明確にはなっていない。

上記三法の適用範囲には重なる部分もあれば重ならない部分もあり、また、同一又は類似する概念が多数用いられている。上記三法の関係は極めて多面的かつ複雑であり、さまざまな視点からの分類・比較が可能である（ある特定の分類・比較だけが正しい、ということではない）。

「ネットワーク安全法」と「データ安全法」は、適用範囲が極めて広い。これら２つの法律は、重要情報インフラの運営者がネットワーク製品やサービスを調達する際に適用されるネットワーク安全審査と、情報処理活動に適用されるデータ安全審査制度を、それぞれネットワーク安全とデータ安全という 2 つの側面から、それぞれの適用分野で具体化したものである。ネットワーク安全の審査とデータ安全の審査は全く同じではなく、審査の内容や対象においてそれぞれ重点の置き所が異なるが、本質的には、これら２つの法律の最終目標は同じことである。つまり、いずれの法律も国家の安全に影響を与え又は与える可能性のある客観的状況又は要因を予測し審査することにあり、これら２つの法律は合わせて「国家安全審査」を構成する。

他方、「個人情報保護法」の立法趣旨は、個人情報の権益を保護することにあり、上記２つの法律とはやや異なる面があるが、全く関係がないとはいえない。例えば、個人情報の安全については、個人情報保護法だけでなく、ネットワーク安全法やデータ安全法が適用されることがあり得る。

Ⅵ. 日本企業・中国現地法人の対応策

１．考え方の順序

（１）まず、中国及び日本（場合によっては、他の国・地域も関係する場合がある。以下同じ）の個人情報・データ安全関連の法令等の規制内容を把握することが出発点である。とくに中国では、今後も新たな法令の制定・改正や運用状況の変化等の動きがあり得るので、継続的に最新の情報を得るよう努めることが必要である。個人情報・データ安全関連では、「意見募集稿」段階の細則等が多数存在するが、中国では、「意見募集稿」の内容が大幅に変更されることも少なくないし、そもそも正式な制定に至らないこともあるので、「意見募集稿」が出たからといって、その内容どおり制定されるものと考えてはならない。

（２）次に、日本企業・中国現地法人が現に有する又は将来取得する可能性のある個人情報・データにはどのようなものがあるか、どのような取得方法・管理状況であるか（プライバシー・ポリシー、個人情報取扱規則等はどのようなものか、実際の情報管理は誰がどこでどのように行っているか）等を把握することが必要である。その際、日本企業と中国現地法人の間の連携を十分にとり、意思疎通を図ることが肝要である。また、必要に応じて、業務委託先・協力会社等についても、現に有する又は将来取得する可能性のある個人情報・データにはどのようなものがあるか、どのような取得方法・管理状況であるか（プライバシー・ポリシー、個人情報取扱規則等はどのようなものか、実際の情報管理は誰がどこでどのように行っているか）等を把握することが望まれる。

「現に有する又は将来取得する可能性のある個人情報・データ」は、各企業の業務やビジネス活動等の種類・内容によってさまざまであろう。したがって、「現に有する又は将来取

得する可能性のある個人情報・データ」がどのようなものがあるかについては、各日本企業・中国現地法人ごとに個別に検討・判断する必要がある。

（3）上記の個人情報・データには中国又は日本の個人情報・データ安全関連の法令等の規制が適用される可能性があるか、適用される場合、関連法令の規制に適合させるにはどのように改善すればよいか、業務フロー等において規制に違反する可能性のある点はないか等を把握するようにする。その際、優先順位を踏まえた対応を心掛けることが肝要である。

２．対応策

（1）もし中国現地法人の情報管理体制がまだ十分に整備されていない場合は、親会社のものを参考に、企業規模や法規制等の違いを考慮した上で、整備していくことが考えられる（例えば、親会社のプライバシー・ポリシー、個人情報取扱規則等を修正した上で、中国現地法人で制定する等）。

（2）日本企業及び中国現地法人としては、とくに個人情報・データの域外移転に関する規制には、十分に注意しなければならない。例えば、中国現地法人の従業員の人事に関する情報・データ、中国市場における消費者のアンケートへの回答等に関する情報等を日本本社に送る場合には、中国の法規制に違反しないか否かを確認し、合法的な形（例えば、匿名化処理して統計データとする等）で送るという対応策が考えられる。

（3）取得する必要のある個人情報・データは、使用目的を明確にした上で本人の同意を得て取得することが必要である場合がある。個人情報・データを取得する際の告知文の記述や、同意を得る方法が適切であるか否か等について、法規制に適合しているかを慎重に判断する必要がある。また逆に、そもそも取得する必要のない個人情報・データは取得しないようにすべきであるところ、実際に取得してしまっていないか否かを確認すべきである。

（4）中国の個人情報・データ安全関連三法の場合、「国家の安全」を守るという視点が入ってくるため、日本の個人情報保護法等とは異なる判断がなされる可能性があり、注意を要する。近時、中国では、習近平国家主席の推進する「総体国家安全観」の下、個人情報・データ安全関連三法以外にも、国家の安全に関連する法律が次々と制定・改正されている（例えば、国家安全法、反スパイ法、反テロ法、測絵法、国家情報法）。そのような法律は、いずれも、中国の国家安全保障の根幹となる重要な法律であるといえる。これらの法律は、一見、日本企業・中国現地法人のビジネス活動とは無関係の法律であるように思われるかもしれないが、実は、直接的又は間接的にビジネス活動に重要な影響を及ぼす可能性がある（例えば、ネット通信等の内容が当局に見られる可能性がある等）ため、注意が必要である。

（５）中国では、個人情報・データ安全関連三法の公布・施行により、個人情報・データ安全に関する法規制の大枠は一応定まったといえるが、各法律の規定内容は極めて抽象的なものが多い。法規制の内容を具体化するための上記三法の細則等が、今後続々と公布されるはずであることから、「走りながら検討する」という姿勢で、今できることから着手する（最初から完璧を目指さない）という心構えで対処することが肝要である。

（６）個人情報・データ安全に係る法規制は、現在、世界各国・地域（中国やEUだでなく、米国の州や、インド、タイ、インドネシアその他の発展途上国を含む）で法規制が整備され又は整備されつつある。しかも、法規制の内容は、EU 等の法規制を参考にしつつも千差万別であるため、関連する各国・地域の法規制を一つ一つ確認する必要がある。

※　初出：『特許ニュース　No.15616』（経済産業調査会、2022年、原題は「中国知財の最新動向　第30回　中国の個人情報・データ安全に係る３つの法律の概要と対応策」）。
※　免責事項：本稿は、中国の法制度の概要を一般的に紹介することを目的とするものであり、法的アドバイスを提供するものではない。仮に本稿の内容の誤り等に起因して読者又は第三者が損害を被ったとしても、筆者は一切責任を負わない。