NISHIMURA & ASAHI

西村あさひ法律事務所

中国「データ安全法」のポイント

中国ニューズレター　2021 年 8 月 23 日号

執筆者:
E-mail 野村 高志　E-mail 陳 致遠

※本稿は、みずほ銀行発行の Mizuho China Monthly(2021 年 8 月号)掲載原稿をもとに加筆修正したものです。

1. はじめに

中国は近年、個人情報をはじめとするデータの保護やサイバーセキュリティーに関連する一連の立法及び改正を進めてきました。その中で、2021 年 6 月 10 日に全国人民代表大会常務委員会で可決・公布され、2021 年 9 月 1 日から施行予定の「データ安全法」は、重要な動向の一つとして注目を集めています。「ネットワーク安全法」(全国人民代表大会常務委員会、2016 年 11 月 7 日公布、2017 年 6 月 1 日施行)に次いで、データ安全法は情報安全分野において基礎を成す二件目の法律となり、2021 年 8 月 20 日に可決・公布された「個人情報保護法」(全国人民代表大会常務委員会、2021 年 8 月 20 日公布、2021 年 11 月 1 日施行予定)と合わせて、今後の中国における情報安全法体制の三つの柱になると思われます(三つの柱の全体像イメージについては下図を参照)。

データ安全法は、計 7 章 55 条で構成されており、データ安全体制に関連する基本的な指針に加えて、企業のデータ安全保護義務やデータの越境安全管理に関する規則及びこれらの規則に違反した場合の罰則も定められています。

本稿では、データ安全法の概要及び企業として注目すべき内容を整理して紹介します。

2. データ安全体制の構築

中国工業・情報化部によれば、中国の「デジタル経済」の規模は毎年拡大しており、2020 年には既に中国の GDP の 4 割を占めるともいいます。一方、多くの中国企業は未だにデータ安全の体制が十分ではなく、個人情報、商業秘密の漏洩さらにはサイバー攻撃も多発しているのが現状です。そして、膨大なデータを収集・分析し、特定分野や地域における特性や傾向等を見出そうとする「ビッグデータ技術」も日々進化しているため、データの漏洩や無断利用はもはや社会を脅かす恐れすらあると言えるでしょう。このような背景の中、デジタル経済の石油に例えられるデータの安全について、当局は利用の促進と管理の強化を図ってきました。

この点、データ安全法は、データの利用を引き続き推進すると同時に、データの利用や流動の適法性の確保も強調しました(第 7 条)。同時に、データの越境移転にあたっての安全性にも注目しています(第 11 条)。

第 7 条	国は、個人及び組織のデータに関する権益を保護し、データが法により合理的かつ有効に利用されることを奨励し、データが法により秩序をもって自由に流動することを保障し、データを基幹的要素とするデジタル経済の発展を促進する。
第 11 条	国は、データ安全ガバナンス、データ開発・利用等の分野の国際交流及び提携を積極的に展開し、データ安全に関する国際規則及び標準の制定に参与し、データ越境の安全及び自由な流動を促進する。

即ち、データの利用や流動を単に制限する趣旨ではなく、データ安全とのバランスを取るよう促すことを目標とするものと思われます。

この点に関して、データ安全法は、第 9 条で関係部門、業種団体や企業及び個人の安全保護意識を向上させる方針を打ち出すほか、具体的に(1)データの分類・分級保護制度、(2)データ安全審査制度、(3)データ安全保護義務、及び(4)データの越境安全管理に関わる規則なども定めています。

3. データの分類・分級保護制度

データ安全法は、データの分類・分級保護制度を確立しました(第 21 条)。主に「国家核心データ」、「重要データ」が取り上げられています。また、いわゆる「重要データ」について、各地区や各部門に当該地区及び所管業種・分野の具体的なリストの作成も要求しました。

分類	定義	管理要求
国家核心データ (第 21 条 2 項)	国家安全、国民経済ライフライン、重要な国民生活、重大な公共利益等に関係する。	➢ より厳格な管理制度を実行すること。
重要データ (第 21 条 1 項、3 項)	データの経済社会発展における重要度並びに改ざん、破壊、漏洩又は不法取得及び不法利用にひとたび遭遇した場合において国家安全、公共利益又は個人若しくは組織の適法な権益にもたらす危害レベルに基づき、 ・ 国家データ安全業務調整メカニズムは重要データリストを制定し、 ・ 各地区及び各部門は当該地区及び当該部門並びに関連する業種及び分野の具体的な重要データリストを制定する。	➢ 重点的な保護を実行すること。 ➢ データ安全責任者及び管理機構を明確にすること。(後記 5.) ➢ 定期的なリスク評価及び管轄当局への報告義務。(後記 5.) ➢ データの越境安全管理について、特別な安全管理措置を実施すること。(後記 6.)
その他のデータ (法令上、明確な定義なし)	上記 2 種類のいずれかにも該当しないデータもあり得る。	➢ データ安全保護義務が課される。(後記 5.)

重要データについては未だに具体的なリストが公表されておらず、引き続き注視する必要がありますが、2017 年に意見募集が行われた「情報安全技術　データ越境安全評価ガイドライン」(全国情報安全標準化技術委員会、2017 年 8 月 30 日公布)には、「重要データ識別ガイドライン」という別紙が付けられており、各業種及び分野において想定した重要データが列挙されています。また、「自動車データ安全管理についての若干の規定」(国家インターネット情報弁公室等、2021 年 8 月 16 日公布、2021 年 10 月 1 日施行予定)の第 3 条でも、軍事施設及びその他の重要施設周辺の人・車両の流れ、及び車両流量や物流など経済状況を示すデータが重要データとして定義されました。上記「情報安全技術　データ越境安全評価ガイドライン」及び当該別紙、そして「自動車データ安全管理についての若干の規定」は、中国当局の考えを理解する上で参考になると思われます。

企業としては、中国当局の動向に注目すると同時に、まずは自社の業種、事業内容に照らして、重要データに該当し得るデータ

を洗い出すことが望ましいと思われます。

なお、国家核心データ及び重要データのいずれにも該当しないデータについても、法規制が全く存在しないわけではなく、データ安全保護義務(後記 5.)が課されていることには注意が必要です。

4. データ安全審査制度

データ安全法はデータ安全審査制度を設けました(第 24 条)。上記各分野・級(レベル)のデータとの関連性は不明確であるものの「国の安全に影響を及ぼし、又は影響を及ぼすおそれのあるデータ処理活動」が対象となっています。

他方、2016 年に公布された「ネットワーク安全法」ではネットワーク安全審査制度が確立されており、2020 年 4 月に「ネットワーク安全審査弁法」(国家インターネット情報弁公室、2020 年 4 月 13 日公布、2020 年 6 月 1 日実施)という細則も公布されました。同弁法について、国家インターネット情報弁公室は、データ安全法にも紐付けをした改訂草案意見募集稿を 2021 年 7 月 10 日に公布しました。同意見募集稿は従来の「国家安全法」及び「ネットワーク安全法」に加えて、「データ安全法」も上位法として取り上げた上で、「データ取扱者による国の安全に影響を及ぼし、又は影響を及ぼすおそれのあるデータ処理活動」も審査対象として明記しました。以上からすると、データ安全法におけるデータ安全審査制度を従来のネットワーク安全審査制度に一本化したい意図が推測されます。

ネットワーク安全審査弁法の施行以来、現実の運用例が特にありませんでしたが、2021 年 6 月 30 日に米国ナスダック(NASDAQ)で上場したばかりの「滴滴」(中国最大手の配車アプリ業者)に対する立ち入り式のネットワーク安全審査、並びに米国での上場を検討中と言われる「運満満」、「貨車幇」(いずれもトラック配車アプリ業者)、及び「BOSS 直聘」(人材マッチングアプリ業者)に対するネットワーク安全審査が注目を集めています。本稿作成時点では審査の結論がまだ出されていませんが、米中貿易摩擦及びデータ安全の重視という背景の中で、ネットワーク安全審査(及び今後のデータ安全審査)を本格化していこうという中国当局の姿勢が見受けられます [1]。

5. データ安全保護義務

データ安全法は、データ処理活動(同法第 2 条によれば、データの収集、保存、使用、加工、送信、提供、公開等をいう。)に関して、データ処理者にデータ安全保護義務も負わせています。具体的には、①全プロセスのデータ安全管理制度の確立・健全化、②データ安全に関連する研修及び、③必要な技術措置を講じることなどが要求されています。とりわけ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処理活動を展開する場合には、ネットワーク安全等級保護制度を基礎としてデータ安全管理制度を構築しなければならないとされています。

ネットワーク安全等級保護制度は「ネットワーク安全法」第 21 条で確立された制度であり、確立当時から情報安全責任者の明確化、並びにファイアーウォール、バックアップ及び暗号化等の必要な技術措置が要求されてきました。その後、2018 年から 2020 年にかけて、国家標準化管理委員会は以下をはじめとする一連の国家標準を公布してきました。

名称	公布・施行日
「情報安全技術 ネットワーク安全等級保護基本要求」 (GB/T 22239-2019)	2019 年 5 月 10 日公布、2019 年 12 月 1 日施行
「情報安全技術 ネットワーク安全等級保護実施ガイドライン」 (GB/T 25058-2019)	2019 年 8 月 30 日公布、2020 年 3 月 1 日施行
「情報安全技術 ネットワーク安全等級保護レベル判断ガイドライン」 (GB/T 22240-2020)	2020 年 4 月 28 日公布、2020 年 11 月 1 日施行

また、公共安全分野及び航空業や金融業及びマスコミ業界など一部の分野・業界においては、公安部、民用航空局、中国人民銀行、国家ラジオ・テレビ総局がネットワーク安全等級保護に関連する、より具体的なガイドラインを既に公表しています。

[1] 特に、ネットワーク安全審査弁法の改訂草案意見募集稿第 6 条では、100 万人分以上の個人情報を保有する企業が海外上場する際には、ネットワーク安全審査を経なければならないことが明記されており、中国企業の海外上場もネットワーク安全審査の対象にしようとする姿勢が見られます。

データ安全法の施行に伴い、ネットワークを利用してデータ処理活動を行う企業にとっては、ネットワーク安全等級保護制度の不備がデータ安全法及びネットワーク安全法両方への違反行為になりかねません。この点に関して、データ安全法はより厳しい罰則を設けているため、データ安全法の罰則が優先的に適用されると考えられます[2]。データ安全保護義務及びネットワーク安全保護義務に違反した場合の罰則は下表の通りです。

	データ安全保護義務の違反行為	ネットワーク安全保護義務の違反行為
根拠法令	データ安全法第 45 条	ネットワーク安全法第 59 条
一般違反	是正命令、警告。 5～50 万元の過料を併せて課すことが可能。 ※直接の責任者には 1～10 万元の過料を課すことが可能。	是正命令、警告。
是正命令に応じず、又は重大な結果をもたらした場合	50～200 万元の過料を課すことが可能。 ※関連業務の暫定的停止や営業停止・整理、そして業務許可証の取り消しや営業許可証の取り消しを併せて課すことが可能。 ※直接の責任者には 5～20 万元の過料を課すことが可能。	1～10 万元の過料を課す。 ※直接の責任者には 0.5～5 万元の過料を課す。

ネットワーク安全法の施行から時間が経っていること、またデータ安全法も 2021 年 9 月 1 日に施行予定で中国管理当局が取締りを強化する傾向にあることに鑑み、企業側が、ネットワーク安全等級保護制度を踏まえてデータ安全保護制度を構築することが急務と言えます。

他方、前述の通り、重要データの取扱者には、上記に加えて、より厳しい規則が設けられています。データ安全法によれば、重要データの取扱者はデータ安全責任者及びデータ安全の管理機構を明確にし、データ安全保護責任を具体化しなければならないとされています(第 27 条)。また、重要データの処理者にそのデータ処理活動に対する定期的なリスク評価、そしてリスク評価報告の主管当局への提出義務を負わせています(第 30 条)。リスク評価報告の内容について、重要データの種類及び数量、データ処理活動の展開状況、直面するデータ安全リスク及びその対応措置等が取り上げられているものの、実施頻度や提出先などその他の詳細は未だに不明確であり、引き続き注視していく必要があります。

また、重要データの越境安全管理についての明確なルールも設けられていますので、後記 6.もご参照ください。

6. データの越境安全管理

ネットワーク安全法は、重要情報インフラの運営者がその運営において収集、発生させた個人情報及び重要データを中国国内に保存し、海外にデータを越境させる必要がある場合は安全評価を経なければならないと定めています(第 37 条)。その後、適用対象を重要情報インフラの運営者からネットワーク運営者に拡大しようとする「個人情報及び重要データ越境安全評価弁法」(国家インターネット情報弁公室、2017 年 4 月 11 日公布)については、意見募集稿が公布されたまま正式な公布は行われていません。即ち、重要情報インフラの運営者に該当しない場合における重要データの越境移転について、明確な規則がない状況だと言えます。

この点に関して、データ安全法は、重要情報インフラの運営者の場合はネットワーク安全法が適用されると明記する一方、重要情報インフラの運営者に該当しない場合における重要データの越境安全管理については、「国家インターネット情報部門が国務院の関係部門と共に制定する」と定めています(第 31 条)。本稿作成時点では、当該越境安全管理弁法はまだ未公表ですが、重

[2] 行政処罰法第 29 条によれば、同一の違法行為が複数の法令に違反して過料が課される場合、高い方の過料を課すこととなっています。

要情報インフラの運営者に該当しなくても重要データの越境移転にあたって何らかの規則が課される方針であることが明文で示されました。

一方、前記の通り、重要データに該当しないデータもあり得ます。これらのデータの越境安全管理について、データ安全法では明確な規則が定められていません。もっとも、データ安全法は、外国の司法又は法律執行機関のデータ提供要求に関する規則を定めました(第 36 条)。同条では、法律や条約・協定、そして平等互恵原則に従ってかかるデータ提供要求を扱うと表明すると同時に、中国国内の組織又は個人は、主管機関の承認を経ずに外国の司法又は法律執行機関に対し、中国国内に保存されているデータを提供してはならないという禁止規定も設けています。

> 第 36 条　中華人民共和国の主管機関は、関係法律及び中華人民共和国が締結し、若しくは参加した国際条約若しくは協定に基づき、又は平等互恵原則に従い、外国の司法又は法律執行機関のデータ提供に関する請求を取り扱う。中華人民共和国の主管機関の承認を経なければ、中華人民共和国国内の組織又は個人は、外国の司法又は法律執行機関に対し、中華人民共和国国内に保存されているデータを提供してはならない。

ただ、同条文は 2 文に分かれていて、前段の「外国の司法又は法律執行機関のデータ請求」という下線部の要件が後段にもかかるか否かがやや不明確であり、実際の運用動向を注視する必要があります。

仮に上記要件が後段にもかかるとしますと、中国国内組織又は個人による自主的な提供は制限されず、結局当該禁止規定の運用場面がやや限られている様にも理解されます。他方、上記要件が後段にかからないとしますと、中国国内組織又は個人による自主的な提供も制限されてしまい、特に中国国外における訴訟提起又は仲裁申立の際の証拠提出や、その他の各種法手続における資料の提出などの場面を考慮しますと、中国企業等の自主活動への過剰な制限とならないかとの懸念も生じ得ると思われます。

特に多国籍企業の場合、外国の司法又は法律執行機関の要求に応じて、本店が海外各拠点の情報を取り纏めてから提出することもあり得るでしょう。かかる場合に、中国国内にある拠点としては、最終の提出先が外国の司法又は法律執行機関であることを把握していたとしても、直接の提出先は本店であるため、かかる行為が上記禁止規定に抵触するか否かの判断は非常に難しいものになると思われます。

7. 終わりに

データ安全法の施行に伴い、中国がデータ処理活動を一層強化することが見込まれています。また、企業のデータ処理活動にも大きな影響があるでしょう。一方、データ安全法は 2021 年 9 月 1 日に施行するため、企業側に与えられた準備期間は限られています。前記の通り厳格な罰則もあることに鑑み、データ安全法に照らして早急に対策を検討することをお薦めします。

西村あさひ法律事務所　広報室　E-mail