データセキュリティー法対応における企業の留意点

2022年3月

日本貿易振興機構(ジェトロ)

大連事務所

ビジネス展開支援課

報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）大連事務所が現地法律事務所 上海里格（大連）法律事務所に作成委託し、2022 年 2 月に入手した情報に基づくものであり、その後の法律改正などによって変わる場合があります。掲載した情報・コメントは作成委託先の判断によるものですが、一般的な情報・解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求めください。

ジェトロおよび上海里格（大連）法律事務所は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的損害および利益の喪失については、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたか否かにかかわらず、一切の責任を負いません。これは、たとえジェトロおよび上海里格（大連）法律事務所が係る損害の可能性を知らされていても同様とします。

本報告書に係る問い合わせ先：

日本貿易振興機構（ジェトロ）
ビジネス展開・人材支援部　ビジネス展開支援課
E-mail：BDA@jetro.go.jp

ジェトロ・大連事務所
E-mail：PCD@jetro.go.jp

目次

データセキュリティー法対応における企業の留意点

一、中国ネットワークキュリティーに係る立法の全体象

情報グローバル化時代に各国がデータセキュリティーの重要性を重視するなか、中国サイバー空間の法制化過程の加速傾向も鮮明となった。「サイバーセキュリティー法」が 2017 年 1 月より、「データセキュリティー法」が 2021 年 9 月より、また「個人情報保護法」が 2021 年 11 月より施行され、いずれもデータのコンプライアンス領域内に極めて重要な法律で、中国データ保護の“三本の柱”として位置づけられている。この“三本の柱”をもとに、近年各部門は自らの権限により、各種の条例、弁法および標準等を公布し、データの処理、保存、削除および越境移転等データの全サイクルにおいて多様な保護義務を企業に課している。データセキュリティー法制度のフレームワークを構築する主要な法令を以下のとおり総括する。

公布機関	公布時間	発効時間	法令の名称	主要内容
公安部	2018.6.27	未定	サイバーセキュリティー等級保護条例（意見募集稿）	ネットワークの等級付け・登録、セキュリティーの構築・改善、等級評価、自主検査等。
国家インターネット情報弁公室	2019.6.13	未定	個人情報越境セキュリティー評価弁法（意見募集稿）	個人情報越境移転の前に、省級インターネット情報部門へセキュリティー評価を申告しなければならない。移転の記録作成、保管、報告等も義務付けられる。

国家インターネット情報弁公室	2021.10.29	未定	データ越境セキュリティー評価弁法（意見募集稿）	データ越境移転の前に自己セキュリティー評価が不可欠。場合によっては国家インターネット情報部門へのセキュリティー評価申請が必要。
国家インターネット情報弁公室	2021.11.14	未定	ネットワーク・データセキュリティー管理条例（意見募集稿）	ネットワークデータの取扱活動を規制する。
国家インターネット情報弁公室、国家発展改革委員会、工業情報化部等の十三部門	2021.12.28	2022.2.15より発効	ネットワーク・セキュリティー審査弁法	重要情報インフラ事業者およびネットワーク・プラットフォーム事業者を対象に、国家安全保障に影響をもたらす活動（上場等）を規制する。
国家インターネット情報弁公室、国家発展改革委員会、工業情報化部、公安部、交通運輸部	2021.8.16	2021.10.1より発効	自動車データセキュリティー管理若干規定（試行）	自動車の設計、製造、販売、使用、運用、保守における個人情報や重要なデータなどの自動車データの国内保管、車両内処理、デフォルトでの収集なし、リスク評価・報告システムなどの自動車データ取扱者に要求。

工業情報化部	2020.4.10	未定	ネットワーク・データセキュリティー標準体系建設ガイドライン（意見募集稿）	ネットワーク･データセキュリティー標準体系のフレームワークを提出し、重点的な標準化領域および方向を規定する。
工業情報化部	2022.2.10	未定	工業情報化分野データセキュリティー管理弁法（試行・意見募集稿）（第二回）	工業、通信業領域のデータ取扱活動を規制する。

数々の法令がデータの保護義務を規定する中、中国でビジネスを営む日系企業は、日常経営から大量のデータが生じ、関連法令の規制対象となる可能性が大きいと思われる。日本所在の関連会社とデータを提供・共有することが多い上に、日中のデータ関連法制度が異なるため、下記は日系企業実務上のニーズを念頭に、最新条例をふまえてデータセキュリティーに関する法的義務のフレームワーク、特に重要度が高いと思われる留意すべきポイントについて説明を行う。

二、データセキュリティー関連法令の位置づけ

中国におけるサイバースペースに対する関連の法令は現時点で条文が膨大で、内容が複雑であるものの、おおむね「データセキュリティー関連法令」、「サイバーセキュリティー関連法令」と「個人情報関連法令」とに分けられる。本文で重点的に論述する「データセキュリティー関連法令」とは、データ取扱活動を主な規制対象とする法律法規の総称であり、「データセキ

ュリティー法」、「ネットワーク・データセキュリティー管理条例（意見募集稿）」および「工業情報化分野データセキュリティー管理弁法（試行・意見募集稿）」等を含む。データセキュリティー関連法令は、サイバーセキュリティー関連法令と個人情報関連法令と相まってサイバースペースを規制する法律分野の重要な一環であり、深い関係を有する一方、各法令の立法目的、規制側面および公布機関等が異なるため、内容に相違点も多い。上記法令の趣旨および全体的なフレームワークをより良く把握できるよう、各法令の位置づけを以下のとおり簡潔に論述する。

(一) データセキュリティー関連法令とサイバーセキュリティー関連法令

データ取扱者の活動を主な規制対象とするデータセキュリティー関連法令と異なり、サイバーセキュリティー関連法令は、立法目的がネットワークの安全確保であり、ネットワークの建設者、運営者、サービス提供者を主な規制主体とし、ネットワーク製品とサービス、ネットワーク重要設備、ネットワーク安全製品および重要情報インフラ等の関連取り扱いを規制する。上述の「サイバーセキュリティー法」、「サイバーセキュリティー等級保護条例（意見募集稿）」および「ネットワーク・セキュリティー審査弁法」等を含む。

(二) データセキュリティー関連法令と個人情報関連法令

「データセキュリティー法」における「データとは、いずれかの電子的またはその他の方式による情報の記録をいう」の定義から、厳密に分類すれば、個人情報はデータの一種に属するといっても良い。ただし、個人情報は、識別可能な人に関する各種の情報であり、一般のデータより人の人格権、人権および自由等と深くかかわり、極めて特殊である。データセキュリティー関連法令にはデータである個人情報の処理原則が含まれているが、その一般原則の上で、個人情報関連法令は個人情報の取り扱いに特殊な規則を置いている。例えば、個人情報の取扱者は、自らの名称、連絡方法、個人情報の処理規則・範囲等を個人に告知し、ならびに個人の同意撤回権、修

正権、削除権等の権利を確保しなければならない。すなわち、データ取扱者は個人情報を特殊のデータとして、一般のデータより慎重に保護しなければならない。

三、データセキュリティー関連法令の主要内容

(一) 管轄範囲

データセキュリティー関連法令の主な適用対象は「データの取扱活動」であり、データ取扱者の国籍によって適用されるというわけではない。中国国内のデータの取扱活動は、「中国の安全、公共の利益または公民、組織の合法的権益に損害を与えた場合」中国国外のデータ取り扱いも適用されるため、「中国のデータ取り扱いについて、中国の子会社しか義務付けられていないので、日本本社には無関係」のような意識を持ってはならない。企業側から見ると、中国人をデータ取扱対象とする、またはデータ取り扱いが中国の企業や政府に影響をもたらす可能性がある限り、中国の関連法令が適用されることを念頭に置いておかなければならない。

(二) データ分類・分級保護制度

データ分類・分級保護制度は、データセキュリティー関連法令の中で極めて重要な制度であり、企業は国家安全、公共利益または個人、組織の合法的権益にもたらす影響および重要度を基準に、データを分類・分級をし、相応の保護措置を確立しなければならない。

1. データの分類

全国情報セキュリティー標準化技術委員会が 2021 年 12 月 31 日に公布（同日より施行）した「サイバーセキュリティー標準実践ガイドライン・ネットワークデータ分類・分級ガイダンス」においては、ネットワークデータの分類・分級の原則、枠組みおよび方法が提起され、「データ

取扱者がデータを分類する時、優先的に国家、業界のデータ分類要求に従うべきで、所在業界の業界データ分類規則がなければ、組織経営の観点からデータ分類を行うこともできる」と規定している。分類のルートは簡潔に下記のとおり総括できる。

⑴法律法規または主管監督管理部門による特殊な管理要求のある下記データカテゴリの存否を識別・区別する。

① 個人情報：すでに識別され、または識別可能な人に関する各種の情報

② 公共データ：政府機関または公共事業の団体が公共管理・サービスにより収集、処理するデータ

③ 公共伝播情報：不特定多数の人に対して広範囲で伝播する情報、特に政治・社会に係る情報など

今後、関連法令は上記以外のデータカテゴリを規定する可能性があるので、引き続き注目すべきである。

⑵業界分野の観点から、当該業界分野の主管部門により認可されたデータの分類規則、または業界共通の分類規則があれば、その特別な分類規則に従ってデータを分類しなければならない。特別な分類規則のある業界分野は、例として下記のとおりである。

④ 自動車業界：「自動車データセキュリティー管理若干規定（試行）」等法令により、自動車の設計、製造、販売、使用、運用、保守における自動車データに対して特別な保護制度を設けている。

⑤ 金融業界：「重要情報インフラセキュリティー保護条例」により、金融企業は重要情報インフラに認定される可能性が高いため、相応の法定の義務を履行しなければならない。

⑥ 電信ネットワーク業界：重要情報インフラに認定される可能性が高い上に、「工業情報化分野データセキュリティー管理弁法（試行・意見募集稿）」など法令による電信およびネットワークデータ取り扱いを規制する。

⑦ その他：例えば、医療業界、インフラ業界など。

企業は自らの業界に相応のデータ取扱規則の存否・内容を常に確認・確定する必要がある。

(3)上記のような国家と業界のデータ分類要求がない場合、企業は組織・経営の視点から、データをユーザーデータ、業務データ、経営管理データ、システム運営およびセキュリティーデータに分類し、管理・保護することができる。

2. データの分級

データの分級保護制度は、「データセキュリティー法」をはじめ、「ネットワーク・データセキュリティー管理条例（意見募集稿）」、「工業情報化分野データセキュリティー管理弁法（試行・意見募集稿）」等多くの法令に提起されている。一般的に、データは「一般データ」、「重要データ」および「核心データ」という三つの等級に分けられている。

(1)一般データ

簡単に定義すれば、一般データとは、国家の安全、公共の利益、個人・組織の合法的な権益などにもたらす影響が小さい、影響を受けるユーザーと企業が比較的に少ない、影響範囲が小さい、または企業の運営、業界の発展、技術の進歩および業界のエコシステムに対して引き起こす脅威が小さいデータを指す。規制が厳しい重要データ、核心データと比較すると、一般データはデータ取り扱いの原則規定に従えば良い。

(2)重要データ

重要データの定義について、「データセキュリティー法」等の法律に明確に規定されていないが、2022 年 1 月 13 日に国家標準「情報安全技術 重要データ識別ガイドライン（意見募集稿）」

は公布され、重要データとは「電子的に存在し、一度改ざん、破壊、漏洩または違法な取得・利用が行われると、国家の安全、公共の利益を脅かす恐れのあるデータをいう」と定義されている。同ガイドラインの「5 重要データの識別要素」において、詳細な重要データ種類は下記のように列挙されている。

a) 国家戦略備蓄、応急動員能力を反映する。例えば、戦略物資生産能力、備蓄量

b) 重要なインフラの運行、または重点分野の工業生産をサポートする。例えば、重要なインフラが所在する業界・分野の核心業務の運行、または重点分野の工業生産を直接サポートするデータ。

c) 重要な情報インフラのサイバーセキュリティー保護状況を反映し、重要な情報インフラに対するネットワーク攻撃を実施させることができる。例えば、重要な情報インフラのサイバーセキュリティー方案、システム構成情報、核心ソフト・ハードウェアの設計情報、システムトポロジー、緊急対応マニュアルなど。

d) 輸出制限品目。例えば、輸出制限の商品の設計原理、プロセスフロー、製作方法等を記述する情報およびソースコード、集積回路レイアウト、技術方案、重要なパラメータ、実験データ、検査報告。

e) ほかの国や組織より中国に対する軍事攻撃に利用される可能性がある。例えば、一定の精度要求を満たす地理情報。

上記ガイドラインの「編成説明」に、重要データの識別について「国家安全を焦点に、範囲拡大を避ける」との原則が提起され、「主に国家安全、公共利益等の角度から評価され、範囲はできる限り小さくし、企業の生産経営と内部管理情報、個人情報などは含まれないものとする」との緩和的な観点が示された。同時に、上記のような識別要素を一つ満たせば、重要データに該当するので、データ取扱者は主に下記の厳しい法的規制を受けることになる。

a) 重要データの種類、数量、収集、保存、加工、使用状況、データセキュリティーのリスクおよびその対応措置等を対象にリスク評価を毎年実行し、また関連主管部門にそ

のリスク評価の報告書を送付しなければならない[1]。

b) 重要データを処理するシステムは、原則的に 3 級以上のネットワーク・セキュリティーレベル保護、および重要情報インフラセキュリティー保護の要求を満たさなければならない[2]。

c) 重要データであることが判明すれば、15 営業日以内にデータ取扱者の基本情報、データセキュリティー管理部門の情報、データセキュリティー担当者の氏名と連絡方法、データ取り扱いの目的、規模、方式、範囲、類型、保存制限・場所等を市レベルのネットワーク情報部門に届け出なければならない[2]。

d) 企業内部にデータセキュリティー体系を建設し、担当者と管理部門を確定し、従業員に対して教育・トレーニングを実行しなければならない[3]。

e) 重要データの取扱者は合併、再編、分立または海外上場等の変更が発生する際に、関連部門に報告し、場合によって、ネットワーク・セキュリティー審査を受けなければならない[4]。

f) 重要データの収集、保存、使用、加工、提供、移転（特に越境移転）にあたっては、暗号化、アクセスコントロール、協議書締結等の方法により、セキュリティーを確保しなければならない[5]。

---

1 「データセキュリティー法」第 30 条、「ネットワーク・データセキュリティー管理条例（意見募集稿）」第 32 条、「工業情報化分野データセキュリティー管理弁法（試行・意見募集稿）」第 31 条

2 「ネットワーク・データセキュリティー管理条例（意見募集稿）」第 29 条

3 「工業情報化分野データセキュリティー管理弁法（試行・意見募集稿）」第 13 条、「ネットワーク・データセキュリティー管理条例（意見募集稿）」第 30 条

4 「ネットワーク・データセキュリティー管理条例（意見募集稿）」第 13、14 条、「ネットワーク・セキュリティー審査弁法」

5 「工業情報化分野データセキュリティー管理弁法（試行・意見募集稿）」第 14 条~18 条、「データ越境セキュリティー評価弁法（意見募集稿）」

(3)核心データ

核心データとは、国家の安全、国民経済の命脈、重要な民生、重要な公共利益等に係るデータをいう。「サイバーセキュリティー標準実践ガイドライン ネットワークデータ分類・分級ガイダンス」により、データを分級する際に、「国家と業界分野の核心データ目録、重要データ目録に基づき、順次に核心データ、重要データとなるか否かを判断し、『高く、厳しく準用』の原則に基づき核心データレベル、重要データレベルと判明すれば、その他のデータは一般データとする」と核心データからデータ分級の方法を釈明しているが、現時点で有効的な「核心データ目録」は公布されていない。関連法令において、核心データが重要データとならび特別な要求を提起されることがほとんどであるが、「オフサイトバックアップ」や「異主体間のデータ取り扱いに対するリスク評価」など、より厳しい規制も規定している。

(三) データの越境移転

「情報セキュリティー技術 データ越境セキュリティー評価ガイドライン（意見募集稿）」により、「データの越境とは、ネットワーク運営者がオンライン等の方式により、中国国内における運営過程において収集および発生したデータを中国国外に位置する機構、組織・個人に提供する単発の活動または連続的な活動をいう」とされている。「データセキュリティー法」が詳しく提起していないが、国家インターネット情報弁公室が 2021 年 10 月 29 日に発表した「データ越境セキュリティー評価弁法（意見募集稿）」において、下記のとおりデータ越境の条件、セキュリティー評価および評価事項、評価プロセス等を詳細に規定している。

1. データの越境移転のセキュリティー評価

データ取扱者がデータ越境に先立ち、下記の項目を重点とし、越境リスクを評価しなければならない。

① データ越境の目的、範囲、方法等の合法性、正当性、必要性。

② 移転データの数量、範囲、種類、機密程度、ならびに国家安全、公共利益、個人あるいは組織の合法的権益にもたらすリスク。

③ データ取扱者のデータ移転管理および技術措置、能力等がデータ漏洩、毀損等を防げるか否か。

④ 移転先の誓約する責任・義務、および管理および技術措置、能力等によってその責任・義務を全うできるか否か、またはデータの安全を保障できるか否か。

⑤ データ越境移転および再移転後の漏洩・毀損・改ざん・悪用等のリスク、ならびに個人情報権益の行使ルートの確保。

⑥ 移転先と締結したデータ越境移転契約が、データの安全保護の責任・義務を十分に取り決めているか否か。

すべてのデータは越境移転の前に、上記の自己セキュリティー評価が不可欠である。また、下記の状況の一つに該当すれば、国家インターネット情報部門にデータの越境移転セキュリティー評価を申請しなければならない。

① 重要情報インフラ運営者が収集・精製した個人情報および重要データ

② 越境移転のデータに重要データが含まれる。

③ 100 万人の個人情報を取り扱う個人情報取扱者が域外に個人情報を提供する。

④ 累計で 10 万人以上の個人情報或いは 1 万人以上の機微な個人情報を域外に提供する。

⑤ 政府機関により規定するその他の状況

2. データの越境移転と個人情報の越境移転

前述したように、個人情報がデータに属し、上記のデータ越境移転の一般原則が準用される一方、個人情報を取り扱う時に、「個人情報保護法」等の要求に従い、一般のデータより慎重に処理しなければならない。例えば、一般のデータ保存の現地化について強制的な規定はないが、重

要情報インフラの運営者と個人情報の処理数が国家インターネット通信部門の規定数に達した個人情報処理者に対して、データローカライゼーションの要求が提出された。また、個人情報の越境移転に、次のいずれかの条件を満たさなければならない。

① 国家インターネット情報部門によるセキュリティー評価に合格した。

② 国家インターネット情報部門の規定により専門機関から個人情報保護認証を獲得した。

③ 国家インターネット情報部門の標準契約を移転先と締結し、双方の権利義務を約定している。

現在、セキュリティー評価については、「個人情報越境セキュリティー評価弁法（意見募集稿）」が詳細に規定しているが、未発効であり、個人情報保護認証と標準契約と共に、政府部門の関連規定が発表されていない現状であり、今後の法的実行を引き続き注目すべきである。

四、まとめ

基盤たる「サイバーセキュリティー法」、「データセキュリティー法」および「個人情報保護法」の三法によるサイバーセキュリティー法制度が整備されてきたことを受け、データ分類・分級保護制度、データの越境移転制度等に基づき、一層のデータ流通促進およびデータセキュリティー確保に向けた環境整備が進められている。未発効の「意見募集稿」が多く、一定の領域で詳細な実施規定がまだ作成・発効していないが、実務上関連執行活動において公安部門、インターネット情報部門等のサイバーセキュリティー関連部門により、企業にデータセキュリティーを確保するよう強く求めている。現時点で、データセキュリティー法対応における企業の留意点は本文前述したように、主に下記のとおりである。

① 中国人をデータ取扱対象とする、またはデータ取り扱いが中国の企業や政府に影響をもたらす可能性がある限り、中国の関連法令は中国の会社だけではなく、日本本社に

は適用されること。

② 国家、業界のデータ分類要求に従い、または組織経営の観点から、データを分類・保護すること。

③ データは「一般データ」、「重要データ」および「核心データ」という三つの等級に分類し、「重要データ」と「核心データ」があれば、関連法令の発効時間を注目し、できる限り要求された義務を遵守すること。

④ データ越境移転の前に、まず自己セキュリティー評価を行うこと。

⑤ 「個人情報保護法」等に従い、越境移転等の場合に個人情報をデータより厳密に保護すること。

義務違反・不遵守だと判定された場合、1,000 万人民元に達する罰金、業務停止、強制解散等厳しい法律責任が課される恐れもある。中国にビジネスで関連のある日系企業は、規制対象となる可能性が高いため、引き続き細心の注意を払う必要がある。必要であれば外部弁護士など専門家の意見を尋ねること、調査または懲戒を受ける場合に、専門家に援助を求めることをお勧めする。