

ネットワークデータ安全管理条例

～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～

2025 年 5 月

日本貿易振興機構（ジェトロ）

上海事務所

調査部

【免責条項】

本レポートは、森・濱田松本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。

「ネットワークデータ安全管理条例」（以下「本条例」という。）は、「サイバーセキュリティ法」「データセキュリティ法」および「個人情報保護法」（いわゆるデータ三法）に基づく行政法規レベルの規定であり、国務院から 2024 年 9 月 24 日に公布され、2025 年 1 月 1 日から施行されている。

本条例は、個人情報や重要データを含むあらゆるネットワークデータの取り扱いと監督管理に関してサイバーセキュリティ法、データセキュリティ法および個人情報保護法の原則的な規定の詳細化等を図るものとなっている。

本稿では、本条例の概要を解説するとともに、関連する法律規則の制定動向も併せて紹介する。

1. 適用対象と適用範囲

(1) 適用対象

本条例は、「中国国内におけるネットワークデータ取扱行為」を適用対象としている（2 条 1 項）。本条例の適用対象となる、「ネットワークデータ」とは、「ネットワークを介して取り扱われ、および生成される各種電子データ」と定義されている。

また、本条例で規制される主体は、ネットワークデータ取扱活動の主体である「ネットワークデータ取扱者」であり、「ネットワークデータ取扱行為において取扱目的および取扱方式を自ら決定する個人または組織」と定義されている（62 条 1 項 3 号）。

(2) 適用範囲（域外適用）

域外におけるネットワークデータ取扱行為に本条例が域外適用されるかに関して、本条例は、ネットワークデータのうち個人情報に該当するデータの取扱行為については、個人情報保護法に定められている域外適用の規定（同法 3 条 2 項）が適用されると規定し（2 条 2 項）、一定の場合に域外適用されることが改めて確認された¹。

他方、サイバーセキュリティ法とデータセキュリティ法には域外適用に関する明確な規定はなく、（中国国外で行われたデータ取扱行為が）中国の国家安全、公民等の合法的権益に損害を与えた場合、中国の重要情報インフラに脅威を及ぼした場合等に法的責任を

¹ 「個人情報保護法」3 条 2 項で規定されている域外適用の要件（域外における、中国国内の自然人の個人情報の取扱行為であり、①中国国内の自然人に対する製品または役務の提供を目的とするとき、または②中国国内の自然人の行為を分析し、評価するとき、③法律、行政法規に定めるその他の事由のいずれかに該当する場合）に該当する場合、本条例を適用するとされている。

追及する等が抽象的に定められているのみである²。本条例でも、こうしたデータセキュリティ法およびサイバーセキュリティ法の規定が基本的に踏襲され、域外で行うネットワークデータ（個人情報を除く）取扱行為が、中国の国家安全、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は、法に基づき法的責任を追及する旨が規定された（2条3項）。

2. ネットワークデータ取扱者全般に適用されるルール

ネットワークデータ取扱者の一般的な義務について、本条例は、すでに実施している法令上の義務を強調しながら、次の点を新たに規定した。

- ① セキュリティリスク発生時の報告期限について、ネットワークデータ取扱者が提供するネットワーク製品、サービスに安全上の欠陥、脆弱性等のリスクが存在し、かつ国の安全、公共の利益への危害を伴うときは、ネットワークデータ取扱者は、24時間以内に関連主管部門に報告する必要がある（10条）。
- ② セキュリティインシデント発生時の告知方法について、ネットワークデータのセキュリティインシデントが個人、組織の合法的権益に危害をもたらす場合は、ネットワークデータ取扱者は、ただちにセキュリティインシデントおよびリスクの状況、危害の結果、すでに講じた改善措置等を電話、ショートメッセージ、インスタントメッセージングツール、電子メールまたは公告等の方式で利害関係者に通知する必要がある（11条2項）。
- ③ 個人情報および重要データの取り扱いを他のネットワークデータ取扱者に委託する際の取扱状況記録の保存期間について、ネットワークデータ取扱者は、当該記録を最低3年間保存する必要がある（12条）。
- ④ 「個人情報保護法」22条³の規定を踏まえ、ネットワークデータ取扱者が合併、分割、解散、破産等の原因によりデータを移転する必要がある場合、データ受領者がデータ安全保護義務を引き続き履行する必要がある（14条）。
- ⑤ ネットワークデータ取扱者が、国の機関、重要情報インフラ運営者にサービスを提供し、または他の公共インフラ等の建設、運用、維持保護に携わる場合は、法令および契約の約定に従いネットワークデータ安全保護義務を履行し、安全で安定した持続的なサービスを提供する必要がある。また、委託者の同意を得ることなく、ネットワー

² 「データセキュリティ法」においては、「域外で行うデータ取扱行為が、中国の国の安全、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、法に基づき法的責任を追及する」と規定されており（「データセキュリティ法」2条）、また、「サイバーセキュリティ法」においては、「域外の機構、組織、個人が攻撃、侵入、妨害、破壊等の中国の重要情報インフラを脅かす活動に従事し、重大な結果をもたらした場合は、法により法的責任を追及する」と規定されている（「サイバーセキュリティ法」75条）。

³ 「個人情報保護法」22条：個人情報取扱者は、合併、分割、解散、破産宣告等の原因により個人情報を移転させる必要がある場合、個人に対し、受領者の名称または氏名および連絡先を告知しなければならない。受領者は、個人情報取扱者の義務を引き続き履行しなければならない。受領者は、当初の取扱目的、取扱方式を変更するにあたっては、本法の規定に従い、あらためて個人の同意を取得しなければならない。

クデータにアクセスし、これを取得し、保管し、使用し、漏洩し、または他人に提供すること、ネットワークデータについて関係性分析を行うことは禁止される(16条)。

- ⑥ 自動化ツールの使用について、ネットワークデータ取扱者は、自動化ツールを使用してネットワークデータにアクセスし、ネットワークデータを収集するにあたり、ネットワークサービスにもたらす影響を評価する必要がある、他人のネットワークに不法侵入すること、ネットワークサービスの正常な運用を妨げることは禁止される(18条)。
- ⑦ 生成系人工知能(AI)について、サービスを提供するネットワークデータ取扱者は、訓練データ(機械学習やAIのモデル構築のために用いるデータセット)および訓練データ取扱行為に対する安全管理を強化し、有効な措置を講じてデータ安全リスクに対する防備を行い、対処する必要がある(19条)。
- ⑧ 域外のネットワークデータ取扱者が中国国内の自然人の個人情報を取り扱うにあたり、「個人情報保護法」53条⁴の規定に従って中国国内に専門機構を設立するか代表を指定した場合には、関連機構の名称または代表の氏名、連絡先等の情報を所在地の市レベル(区を設置している市)のネットワーク安全情報部門に提出する必要がある(26条)。

3. 個人情報の取り扱いに適用されるルール

本条例は、従来の法規制を踏まえ、個人情報の取り扱いに関して以下のとおり詳細なルールを規定している。

- ① 個人情報保護法 17 条で要求されている個人情報取扱規則の告知について、ネットワークデータ取扱者は、個人情報の収集および他のネットワークデータ取扱者への提供の目的、方式、種類ならびにデータ受領者の情報を、リストの形式で明記する必要がある(21条2項)。
- ② 個人情報保護法 19 条で要求されている個人情報の保存期間について、原則として個人に告知する必要があるが、保存期間を確定することが難しい場合は、その代わりに保存期間の確定方法を明確にする必要がある(21条1項3号)。
- ③ 個人情報保護法 14 条で要求されている個人の同意の取得方法について、詐欺や脅迫等の方式を通じて個人の同意を取得すること、個人が同意しない旨を明確に表明した後に頻繁に同意を求めることは禁止される(22条)。また、本条例は、「個別の同意」⁵の定義について、「個人がその個人情報に対して特定の取り扱いが行われることについて特に行う具体的かつ明確な同意をいう」と初めて定義した(62条1項7号)。

⁴ 「個人情報保護法」53条：個人情報保護法3条2項に定める域外の個人情報取扱者は、中国国内に専門の機構を設置し、または代表を指定して、個人情報保護に関する事務の処理を担当させ、かつ関連機構の名称または代表の氏名、連絡先等を個人情報保護職責履行部門に届け出なければならない。

⁵ 個人情報取扱者は、個人情報の他の個人情報取扱者への提供(「個人情報保護法」23条)、個人情報の公開(「個人情報保護法」25条)、機微な個人情報の取り扱い(「個人情報保護法」29条)、個人情報の越境提供(「個人情報保護法」39条)等を行う際に、個人の個別の同意を取得する必要がある。

- ④ 個人情報の自動収集について、自動収集技術等の使用により不必要な個人情報または個人の同意を取得していない個人情報の収集を回避することができない場合、ネットワークデータ取扱者は、当該個人情報を削除するか、匿名化処理を行う必要がある。(24条)。
- ⑤ 個人のデータポータビリティ権について、「個人情報保護法」45条3項⁶に原則規定が定められており、「国のネットワーク安全情報部門の定める条件を満たしている」という条件が定められていたが、当該条件の内容に関する規定は設けられていない。この点につき、本条例は、個人情報の移転請求の際の条件を明確にした(25条)⁷。ただし、条件の1つである「個人情報の移転に技術的な実行可能性が備わっているとき」(25条1項3号)については、その判断基準等は依然として明確ではない。

4. 重要データの取り扱いに適用されるルール

従来の法規制においては、個人情報がどの程度の規模になった場合に重要データに該当するかについて、明確な規定は存在していなかった。本条例は、ネットワークデータ取扱者が1,000万人以上の個人情報を取り扱う場合に、本条例30条と32条の重要データを取り扱うネットワークデータ取扱者の義務(安全責任者と安全管理機構の義務、合併等に際する安全保障措置の構築および当局への報告義務)を遵守しなければならないと規定した(28条)。

また、本条例は、重要データの取扱者に対し、ネットワークデータ安全責任者およびネットワークデータ安全管理機構を明確にすることを求めており、関連主管部門が定める特定の種類、規模の重要データを掌握しているネットワークデータ取扱者については、ネットワークデータ安全責任者および重要な職掌の人員のバックグラウンドに関するセキュリティ審査を行い、人員に対する研修を強化しなければならないことを規定した(30条)。

さらに、本条例は、重要データの取扱者が、そのネットワークデータ取扱行為について年度ごとにリスク評価を実施し、かつ省レベル以上の関連主管部門にリスク評価報告を提出しなければならないことを規定した(33条)。

⁶ 「個人情報保護法」45条3項：個人がその指定する個人情報取扱者への個人情報の移転を請求し、国のネットワーク安全情報部門の定める条件を満たしているときは、個人情報取扱者は、移転手段を提供しなければならない。

⁷ 「ネットワークデータ安全管理条例」25条(移転請求)

次に掲げる条件に合致する個人情報の移転請求について、ネットワークデータ取扱者は、個人が指定する他のネットワークデータ取扱者による関連個人情報へのアクセス、取得の手段を提供しなければならない。

(1) 請求人の真実の身分を検証することができるとき
(2) 移転請求があったのが、本人が提供に同意した個人情報または契約に基づき収集した個人情報であるとき

(3) 個人情報の移転に技術的な実行可能性が備わっているとき

(4) 個人情報の移転が他人の合法的権益を損なわないとき

個人情報の移転請求の回数が合理的な範囲を明らかに超えている場合は、ネットワークデータ取扱者は、個人情報移転のコストに基づき必要な費用を徴収することができる。

5. データの域外移転

(1) 個人情報の域外提供の要件

個人情報の域外移転について、本条例は、「個人情報保護法」38条および「データ越境流動の促進および規範化に関する規定」5条の規定を踏襲し、ネットワークデータ取扱者が個人情報を域外に提供するための要件を規定した（35条）。そのうち、下記に掲げる①～③は「個人情報保護法」38条の規定そのままであり、④、⑤および⑦は「データ越境流動の促進および規範化に関する規定」5条の規定であり、⑥が本条例において新たに規定されたものである（ただし、⑥のような規定は各法域において比較的良好に認められる内容である。）。その意味では、従来の規制に実質的に重大な変更を加えるものではないといえる。

- ① 国のネットワーク安全情報部門が手配するデータ域外移転安全評価に合格すること
- ② 国のネットワーク安全情報部門の規定に従い、専門機構が行う個人情報保護認証を受けること
- ③ 国のネットワーク安全情報部門が制定する、個人情報域外移転標準契約に関する規定に合致すること
- ④ 個人を当事者の一方とする契約を締結し、履行するために、確かに個人情報を域外に提供する必要があること
- ⑤ 法に基づき定められた労働規則制度および法に基づき締結された集団契約に従い越境人的資源管理を実施するにあたり、確かに従業員の個人情報を域外に提供する必要があること
- ⑥ 法定の職責または法定の義務を履行するために、確かに個人情報を域外に提供する必要があること
- ⑦ 緊急の状況において自然人の生命・健康および財産の安全を保護するために、確かに個人情報を域外に提供する必要があること
- ⑧ 法律、行政法規または国のネットワーク安全情報部門が定めるその他の条件

(2) 重要データの域外移転の際の安全評価

重要データの域外移転について、本条例は、「データ域外移転安全評価規則」4条および「データ越境流動の促進および規範化に関する規定」2条の規定を踏襲し、ネットワークデータ取扱者が中国国内で収集・生成した重要データを域外に提供する場合には、データ域外移転安全評価に合格しなければならないと規定したうえで、関連地区・部門から重要データであると告知・公表されていない場合は、当該データを重要データとしてデータ域外移転安全評価の申告をする必要はないと規定した（37条）。

6. ネットワークプラットフォームサービス提供者の義務

本条例では、ネットワークプラットフォームサービス提供者が、下記の特別な義務を負う

ことが規定された。

- ① ネットワークプラットフォームサービス提供者（アプリケーション・プログラムがプリインストールされているスマート端末等の設備の生産者も含む）は、そのプラットフォームに接続する第三者製品およびサービス提供者のネットワークデータ安全管理義務を明確にし、第三者製品およびサービス提供者がネットワークデータ安全管理を強化するよう促す必要がある（46 条）。
- ② アプリケーション・プログラム配信サービスを提供するネットワークプラットフォームサービス提供者は、アプリケーション・プログラム確認審査規則を確立し、かつネットワークデータ安全関連の確認審査を実施する必要がある（41 条）。
- ③ ネットワークプラットフォームサービス提供者は、自動化された意思決定の方式を通じて、個人に対して情報のプッシュ配信を行う場合は、パーソナライズドレコメンドを無効にする選択肢（理解しやすく、アクセスおよび操作のしやすいもの）を設け、ユーザーに情報プッシュ配信の受信拒否、その個人の特徴に特化したユーザータグ（消費者の閲覧記録や購入記録等に基づき、当該消費者の好みや購入意向等を分析し、興味があると推測される商品を当該消費者に優先的に提示するようにする技術を使用したもの）の削除等の機能を提供する必要がある（42 条）。
- ④ 大規模ネットワークプラットフォームサービス提供者⁸は、個人情報保護に関する社会的責任報告を年度ごとに公表し（44 条）、ネットワークデータを越境提供するにあたり、関連技術および管理措置を整備し、ネットワークデータ越境安全リスクに対する防備をする必要がある（45 条）。大規模ネットワークプラットフォームサービス提供者が、ネットワークデータ、アルゴリズムおよびプラットフォーム規則等を利用して誤導、詐欺、不正な制限、不合理な差別待遇等の行為に従事することは禁止される（46 条）。

次に、近時公表された「個人情報域外移転に係る個人情報保護認証規則（意見募集稿）」と 2024 年 9 月から施行されている「ネットワーク安全標準実践ガイドライン-機微な個人情報識別ガイドライン」について紹介する。

7. 個人情報域外移転に係る個人情報保護認証規則（意見募集稿）について

「個人情報域外移転に係る個人情報保護認証規則（意見募集稿）」（以下「個人情報保護認証規則意見募集稿」という）は、国家インターネット情報弁公室から 2025 年 1 月 3 日に公表され、同年 2 月 3 日までの期間、意見募集手続きに付された。個人情報保護認証規則意

⁸ 大規模ネットワークプラットフォームとは、登録ユーザー5,000 万以上または月間アクティブユーザー1,000 万以上で、業務類型が複雑であり、ネットワークデータ取扱行為が国の安全、経済運営、国の経済および人民の生活等に対して重要な影響を有するネットワークプラットフォームをいうとされている（「ネットワークデータ安全管理条例」62 条 1 項 8 号）。

見募集稿は、個人情報域外移転に係る個人情報保護認証業務を規範化するもので、個人情報保護認証の適用要件、評定事項等について規定している。

まず、個人情報域外移転に係る個人情報保護認証の方式により域外に個人情報を提供する場面については従来の規定⁹を踏襲している一方で（4条）、中国の個人情報保護法が域外適用される場合において、中国の域外において中国の域内の自然人の個人情報を取り扱う個人情報取扱者は、域外移転に係る認証を取得して、個人情報域外移転行為を行うことができる（5条）。

また、この場合、中国の域外の個人情報取扱者が域内に設立した専門機構または指定した代表者が申請に協力し、かつ相応の法的責任を負い、中国の個人情報保護に関する法律法規を遵守しかつ監督管理を受けることを確約し、認証の有効期間において専門認証機構の継続的監督を受けなければならないとされる（9条2項）。なお、個人情報域外移転に係る個人情報保護認証における重点的な評定内容も定められており、主に個人情報域外移転に関する合法性、正当性、必要性、域外個人情報取扱者または域外受領者の取扱方法、法令規制やネットワーク安全環境等が個人情報の安全に与える影響、個人情報保護の義務の約定有無等が規定されている（10条）。

8. ネットワーク安全標準実践ガイドライン-機微な個人情報識別ガイドラインについて

「ネットワーク安全標準実践ガイドライン-機微な個人情報識別ガイドライン」（以下「機微な個人情報識別ガイドライン」という）は、全国ネットワーク安全標準化技術委員会から、2024年9月14日に公布され、同日施行された。

機微な個人情報識別ガイドラインは、機微な個人情報の識別のために制定されたものである。機微な個人情報識別ガイドラインにおいて、機微な個人情報は、「漏洩され、または不法に使用された場合、自然人の人格の尊厳、人身の安全または財産の安全が侵害されやすい個人情報」と定義されているが（2.2条）、この定義自体は個人情報保護法における定義と同じである。また、単独では機微な個人情報に該当しない場合においても、複数の個人情報が集約されまたは融合されることによって、一旦漏洩され、または不法に使用されると、自然人の人格の尊厳、人身の安全または財産の安全が侵害されやすい場合には、集約されまたは融合された後の個人情報の全体について機微な個人情報として取り扱わなければならないとされている（3条c）。

その上で、機微な個人情報識別ガイドラインは、その付属書において機微な個人情報を下表のとおり列挙している。2020年10月1日から施行されている国家標準 GB/T 35273-2020「情報安全技術・個人情報安全規範」においても付属書としてこれまでも機微な個人情報の一覧が提供されていたが、機微な個人情報識別ガイドラインの内容とは若干異なっ

⁹ 重要情報インフラ運営者でないこと、および当年1月1日以降の累計で、域外に提供する個人情報（機微な個人情報を含まない）が10万人分以上100万人分未満であること、または機微な個人情報が1万人分未満であること。これは、「データ越境流動の促進および規範化に関する規定」における認証の取得（または標準契約の締結）が必要な場合の規定と一致している。

ている（例えば、疾病の予防等の医療サービスの過程で収集されおよび発生する個人情報、個人の身体の秘密部分を示す写真または映像情報等の個人情報が追加された）。

類別	典型例示
生体識別情報	個人の遺伝子 ¹⁰ 、顔 ¹¹ 、声紋 ¹² 、歩容 ¹³ 、指紋、掌紋、網膜、耳介、虹彩等の生体識別情報
宗教信仰情報	個人が信仰する宗教、加入する宗教組織、宗教組織における職位、参加する宗教活動、特殊な宗教的習慣等の個人情報
特定の身分情報	身体障害者の身分情報、公開が不適切な職業身分情報等の個人情報
医療健康情報	1.病状、既往歴、家族の病歴、感染症歴、健康診断の結果、出産情報等、個人の身体的もしくは精神的な傷害、疾病、障害、疾病リスクまたはプライバシーに関わる健康状態情報 ¹⁴ 2.医療受診記録（医療意見、入院記録、医師の指示書、手術および麻酔の記録、看護記録、薬剤使用記録等）、検査・診査データ（検査報告、診査報告等）等、疾病の予防、診断、治療、看護、リハビリ等の医療サービスの過程で収集されおよび発生する個人情報
金融口座情報	個人の銀行、証券、基金、保険、積立金等の口座の口座番号および暗証番号、積立金の共同名義口座番号、支払口座番号、キャッシュカードの磁気データ（またはチップ等価情報）並びに口座情報に基づいて生成された決済トークン情報、個人の収入明細等の個人情報
移動の軌跡情報	連続した正確な測位軌跡情報、車両走行軌跡情報、人の活動軌跡情報等の個人情報
14 歳未満の未成年者の個人情報	14 歳未満の未成年者の個人情報

¹⁰ 遺伝子情報とは、遺伝子識別データであり、具体的には国家標準 GB/T 41806-2022「情報安全技術・遺伝子識別データに係る安全要求」を参照。

¹¹ 顔情報とは、顔の識別データであり、具体的には国家標準 GB/T 41819-2022「情報安全技術・顔識別データに係る安全要求」を参照。

¹² 声紋情報とは、声紋識別データであり、具体的には国家標準 GB/T 41807-2022「情報安全技術 声紋識別データに係る安全要求」を参照。

¹³ 歩容情報とは、歩容の識別データであり、具体的には国家標準 GB/T 41773-2022「情報安全技術 歩容識別データに係る安全要求」を参照。

¹⁴ 個人の体重、身長、血液型、血圧、肺活量等の基本的な体質情報については、個人の疾病および医療受診に関係がない場合には、機微な個人情報の範囲には含まれないと判断できるとされている。

その他の機微な個人情報	正確な測位情報 ¹⁵ 、身分証写真、性的指向、性生活、信用情報、犯罪歴情報 ¹⁶ 、個人の身体の秘密部分を示す写真または映像情報等の個人情報
-------------	--

¹⁵ 個人の携帯電話の正確な位置情報の権限を利用することによって収集された位置情報は正確な測位情報であり、IP アドレス等によって推算された大まかな位置情報は正確な測位情報ではなく、連続的に収集された正確な測位情報を移動の軌跡の生成に用いることができるとされている。

¹⁶ 犯罪記録とは、犯罪を犯した者に関するわが国の国家専門機関の客観的な記録（罪名、刑罰等の記録等）をいうとされている

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/ora2/20250007>



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）
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