

論説

中国におけるデータ越境移転規制の 法的枠組みと課題 ーデジタル主権と自由貿易との調和に基づく 比較考察ー

李 程

はじめに

- 一 データ越境移転をめぐる主な国際的規制
- 二 中国におけるデータ越境移転の規制
- 三 日本におけるデータ越境移転規制
- 四 中国と日本におけるデータ越境移転規制に関する
比較考察

おわりに

はじめに

近年、情報技術とデジタル経済の急速な発展に伴い、国際取引（クロスボーダー）におけるデータの国境を越えた移転は大幅に増加する傾向にある。とりわけグローバルプラットフォームビジネスの広がりにより、データは特定の国に限らず、複数の国の間で移転することが常態化している。

中国はこれまで国の安全やデジタル主権、公共利益の考慮から、厳格なデータローカライゼーション（国内保存）政策を推進してきた。2017年のサイバーセキュリティ法、2021年のデータセキュリティ法および個人情報保護法によって、重要データおよび個人情報の越境移転に対して、事前審査やセキュリティ評価などの義務が定められている。国内企業がデータの越境移転を取り扱う場合の法的規制が増えている。それに対して、日本はEUの一般データ保護規則（GDPR）との整合性を求め、2017年および2020年の個人情報保護法改正を通じて、国際的なデータ移転の促進を目指している。国にとって、国家安全保障、公共利益の維持、国民の権利保護、さらに国際取引の促進および国際信頼の確保等の側面から、データの越境移転に適切な制限を行うことは必要不可欠である。中国はデジタル主権を強調しながら、なお国内規制と国際規制のバランスを保つため、法制度の見直しと整備が続けられている。

本稿はデータ越境移転をめぐる、国際的規制を概観した上で中国の現行法制度の枠組みを分析し、日本との比較法的視点から今後の課題ならびに政策的展望について検討する。

一 データ越境移転をめぐる主な国際的規制

データの国境を越えた移転は個人情報プライバシー保護や国の安全、デジタル主権、公共利益などの一連の問題をもたらす¹。そのため、国際社会は合理的な国際的規制の枠組みの構築に努めながら、データ越境移転する際に各国の法制度との調和を求めなければならないことを認識しつつある。以下においてまずデータ越境移転をめぐる主要な国際的規制について概観する。

（一）EU 一般データ保護規則（GDPR）

欧州連合（EU）は2016年に制定されて2018年より適用開始されている一般データ保護規則²（General Data Protection Regulation, 以下「GDPR」という）を通じて、特に個人情報の保護と越境移転に対して厳しい規定を設

けている。GDPR 第 44 条以下に EU 域内の個人情報が域外の第三国に移転されるとき、欧州委員会は当該第三国が「十分なデータ保護レベル (adequate level of protection)」に達していることを認定する必要があると規定されている。

十分なデータ保護水準 (adequate level of protection) に達しているかどうか、いわゆる「十分性認定 (adequacy decision)」は当該第三国の法制度、実施状況、人権保障体制等に関する包括的な評価に基づき、欧州委員会が個別に行われる (GDPR 第 45 条)。なお、十分性がないと認定された場合であっても、標準契約条項 (Standard Contractual Clauses: SCC) や拘束的企业準則 (Binding Corporate Rules: BCR) など GDPR 第 46 条に基づき「適切な保護措置 (appropriate safeguards)」を講じることによって、データ越境移転は可能とされる。

(二) APEC 越境プライバシールール (CBPR)

2011 年にアジア太平洋経済協力 (APEC) の電子商取引運営グループ (Electronic Commerce Steering Group: ECSG) によって越境プライバシールール (Cross Border Privacy Rules: CBPR) という自主認定制度が定められた。この制度は加盟国間における個人情報の自由な移転を求めると同時に、プライバシー保護の実現を目的とする。企業等が各国の認定機関 (Accountability Agent) による審査を受け、APEC 個人情報保護の枠組み (プライバシーフレームワーク) に適合すると認められた場合、データを越境移転することが可能となる。

これまで、米国、日本、シンガポール、韓国、カナダなどの国と地域が CBPR に参加しており、共通のルールの下でデータ移転が行われている。中国と日本はいずれも APEC メンバーであるが、中国は CBPR に参加していない³。一方、日本は早期から参加して、自国内の認定機関である一般財団法人日本情報経済社会推進協会 (JIPDEC) が CBPR 認定を行っている⁴。その認定結果は他の加盟国においても有効とされ、対象企業は CBPR 認定を通じて他国へ個人情報を合法的に移転することが可能となる⁵。CBPR 制度におけるデータ越境移転は基本的に各国間の自己規律に基づくものであり、法的拘束力

のある政府間協定とは異なるが、参加している国のプライバシー保護当局（Privacy Enforcement Authorities）による認定プロセスや苦情対応メカニズムの監督を行うことで、一定の実効性を担保することができるといえよう⁶。

ところが、CBPR 制度に関する問題点も指摘されている。制度への参加は任意であるため、認定を取得されている企業の数に限定的であり、グローバル企業間におけるデータ移転の一般的ルートとなっていないことは否定できず、EU 一般データ保護規則（GDPR）と比べて、拘束力や強制力に乏しいとの批判が見られる⁷。そこで、CBPR 制度はアジア太平洋地域におけるデータ越境移転の促進に資する一方、制度の実効性の実現および普及が今後の課題になるであろう。

（三）国際的な規制との調和の要請

各国におけるデータ保護制度はそれぞれの国家戦略、政治体制、法律文化および技術発展の段階に基づいて独自に発展しており、その制度的多様性が国境を越えたデータ移転の調整において異なる規範意識と制度設計に基づいており、相互の整合性が欠けている状況にあるため、多様で複雑な課題を引き起こす可能性があると思われる。こうした制度的相違は特に多国籍企業が複数の法域間でデータ移転することに伴う国際取引の展開等に深刻な影響を与えるおそれがある。たとえば、中国において、重要情報インフラにかかわるデータや個人情報の国外への移転に関して、事前セキュリティ審査が義務付けられており、一定のデータローカリゼーション要件も定められている。また、EU において一般データ保護規則（GDPR）に基づき、EU 域外へデータを移転する際に「十分性認定」や「標準契約条項（SCC）」等の法的枠組みが要求され、移転先の国の制度との整合性が厳格に審査されなければならない。このため、国や地域の規制枠組みの間に存在する制度的相違はグローバルなデータ移転の円滑化に影響する現実的な課題として認識されている。それはクロスボーダーにおいて法的予見可能性の低下や取引コストの増加といった形で具体的な影響を及ぼしており、協力的および持続可能なデータガバナンスの構築を求める要因の一つともなっている。

上述した制度的差異および国際取引の実務に及ぼす影響を踏まえながら、次に中国におけるデータ越境移転の法的規制を検討し、日本との規制枠組みの特徴および相違点を明らかにした上、今後の制度調整およびデータ越境移転の円滑化に向けた課題について考察を加えていく。

二 中国におけるデータ越境移転の規制

(一) サイバーセキュリティ法における規制枠組み

中国におけるデータ越境移転の制度的基盤は 2017 年に施行された『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）にあるといつてよい。サイバーセキュリティ法は国による「サイバー空間主権」の理念を明文化にした基本法であると考えられ、中国のデータガバナンスが新たな段階に入ったことを示している。同法によって、データローカライゼーションを原則とし、セキュリティ評価を例外とするデータ越境移転規制の枠組みが確立されている。とりわけ、重要情報インフラ⁸運営者（CIIO）が中国国内で収集または生成した個人情報および重要データを中国国外に保存または提供する場合に、国家の安全保障機関が実施するセキュリティ評価を受けなければならないと規定されている（第 37 条）。また、個人情報処理者が情報主体の同意を得ないと個人情報を提供してはならず、提供先のデータ保護レベルが適切であることを確認しなければならないと定められている（第 40 条）。このように、サイバーセキュリティ法は個人の権利利益、国の安全、公共利益を保障するという観点から国外への不適切なデータ移転を防止しており、データ越境移転に全体的な制限を加えている。

(二) データセキュリティ法による重要データの越境移転規制

『中華人民共和国データセキュリティ法』（2021 年に施行、以下「データセキュリティ法」という）はより広範なデータ規制の枠組みを構築し、国家のデジタル主権と安全保障を図るために、重要データの越境移転に対する厳格な規制を設けている。データセキュリティ法において、データの越境に関

する規制は個人の権利利益、国の安全、公共利益を守る措置として重要な位置付けとされている。国はデータ処理活動に対する全面的な監督管理の体制を構築すると明示しており、特に重要データの越境移転に関しては、国の統一的な監督および管理の枠組みにおいて行うべきことを強調している（第 11 条）。それに、同法は安全と発展をともに重視するというデータ規制の原則を明確にし、データのローカル保管、データの等級保護、移転審査などの重要なデータセキュリティ制度を定め、国のデータ規制のためにマクロフレームワークを構築するとともに、「データ」、「データ処理」、「データセキュリティ」などの基礎概念を明確にした。

データセキュリティ法によって、中国国内で収集また生成された重要データを越境移転する場合、関連部門の組織によるセキュリティ評価を受けるべきであると規定されている（第 31 条）。それに加えて、重要データの分類およびカテゴリー化（国家インターネット情報弁公室『ネットワークデータ安全管理条例』第 29 条に定められている）が進められ、実務において業界別に異なる規制の基準が設けられる試み⁹も見られている。

データセキュリティ法の規定に基づき、2022 年に『データ越境セキュリティ評価方法』（後述）が施行され、より具体的な手続きと評価基準が設けられている。その中、累計で 10 万人以上の個人情報を処理する企業や、重要データを扱う企業は、セキュリティ評価を申請する義務があるとされている。評価項目にデータの種類やデータの規模、提供先のデータ保護措置、越境の必要性、リスク対応措置などが含まれており、重要データの越境移転に対して慎重な立場を取っていると考えられる。この立場は国家安全の強化に資する一方、外国企業にとって、企業活動におけるデータガバナンスと国際的なコンプライアンスの課題を生じさせる。多国籍企業の場合、中国国内で収集されたデータを国外にある本社サーバーへ直ちに転送することが難しくなる可能性がある。

（三）個人情報保護法と個人情報の越境移転規制

『中華人民共和国個人情報保護法』（2021 年に施行、以下「個人情報保護法」という）はデータの越境移転に対して多層かつ系統的な法的規制を設け

て、とりわけ個人情報の国境を越えた移転の効率化と安全性とのバランスを求め、デジタル主権リスクと個人権益侵害を防止することを目的としている。具体的に、個人情報を越境移転する条件の明確化、セキュリティ評価メカニズムの強化、同意規則の細分化、特殊な主体義務の規定を通じて、安全かつ監督可能を核心とする個人情報の越境移転規制の枠組みを構築した。

個人情報保護法に個人情報の越境移転の法的根拠を明示しているのは国家インターネット情報部門によるセキュリティ評価の実施、個人情報保護認定の取得、標準契約の締結、その他法令が定める要件のいずれかを満たす必要があるという規定である（第 38 条）。この規定に基づき、技術的基準（セキュリティ評価）、業界による自主的規制（認定制度）、契約による規律という三つのメカニズムを組み合わせることで、実務において多国籍企業に対する明確なコンプライアンスの指針が示されている。たとえば、100 万人以上の個人情報を処理する場合や機密性の高いデータを取り扱う場合に、セキュリティ評価が義務付けられる一方、中小企業に対して、標準契約条項の活用によりコンプライアンスコストの削減が可能となる。それに、この規定は国際条約優先適用という原則を明らかにしており、中国がグローバルなデータガバナンス枠組みに参画するための制度上の配慮であると考えられる。

なお、重要情報インフラの運営者および大量の個人情報を処理する者に対して、データのローカル保存義務を課し、セキュリティ評価をされた場合に限ってデータの国外提供を認める（第 40 条）。評価内容には越境移転の目的の適法性、移転先のデータ保護レベル、データの規模やセンシティビティなどが含まれ、データ越境移転前の国家セキュリティ審査制度を実質的に構成している。

ちなみに、国内からデータを国外に移転する形に限らず、外国の司法機関または法執行機関による中国国内の個人情報への直接的アクセスも制限され、主管機関による事前承認という手続的要件が設けられている（第 41 条）。この規定はいわゆる「ロングアーム管轄」による中国のデジタル主権への侵害を防止することを目的とし、同趣旨をもつデータセキュリティ法の定める対等の原則と呼応している。すなわち、外国機関によるアクセスには国際条約または互恵的な取り決めに基づくことが要求され、それ以外の場合に国内企

業は協力を拒否することができるとされている。

また、国家インターネット情報弁公室および地方のインターネット情報部門¹⁰にネガティブリスト方式の導入を認め、国家の安全や国民の権益を侵害した域外実体に対してデータ移転の制限を課すことができるとされる（第 42 条）。この規定は EU 一般データ保護規則（GDPR）の「十分性認定」に類似するメカニズムを採用しつつも、EU のいわゆるホワイトリスト方式よりも柔軟性が高く、具体的な侵害に対して的確に制限を実施することが可能である。

（四）データ越境セキュリティ評価方法

サイバーセキュリティ法、データセキュリティ法、個人情報保護法は中国のデータ越境移転に関する主な規制枠組みを構成している。このうち、サイバーセキュリティ法は重要情報インフラにおけるデータローカライゼーションに焦点を当て、データセキュリティ法はデータの分類および等級管理制度を確立して、個人情報保護法は個人情報の越境移転に関する詳細な運用規則を規定している。なお、データ越境移転規制に関する主要な現実的課題がセキュリティ評価手続の非効率性と国際取引の迅速化との矛盾、中小企業にとって過度の高いコンプライアンスコストなどに集約されている。こうしたデータ越境移転規制の実務において、上述した法律の関連条項を補完と細分化するために、国家インターネット情報弁公室は 2022 年にデータ越境セキュリティ評価方法（以下「評価方法」という）を制定した。

評価方法はデータ取扱事業者が海外に重要なデータを提供したり、大規模な個人情報に関連するデータを越境移転する場合、セキュリティ評価を前提とする必要があることを明確に規定している。適用主体について、重要情報インフラ運営者、100 万人以上の個人情報を処理するデータ取扱事業者、前年 1 月 1 日から累計 10 万人の個人情報または 1 万人の機微な個人情報を国外に提供する主体が挙げられている（第 4 条）。重要なデータの越境はデータの規模にかかわらずすべてセキュリティ評価を申告する必要がある。評価基準として、データ越境の合法性、必要性、目的の合理性、および越境移転先によるデータ保護レベルが重点的に審査され、データ越境が国の安全およ

び公共利益を損なってはならないことが要求されている（第5条）。評価プロセスは（1）申請資料の提出（2）省レベルのインターネット情報部門による初期審査（3）国家インターネット情報弁公室による実質審査（実質審査の期間は原則として45営業日、複雑な場合は延長可）の三段階に分けられる（第6、7、12条）。審査を経て、有効期間2年の評価結果が発行され、期限満了後は再申請が必要となる（第14条）。

2025年3月まで、国家インターネット情報弁公室はデータ越境移転に関するセキュリティ評価項目298件を完了している。そのうち、44件は重要データに関連する申請項目であり、評価で承認されなかった案件は7件となつて、不承認率は15.9%であった¹¹。

三 日本におけるデータ越境移転規制

日本のデータ越境移転規制の枠組みも個人の権利利益の保護、国の安全保障や先端技術の流出防止などの配慮から多面的に構築されている。個人情報保護法による個人情報の越境規制のほか、不正競争防止法により保護される営業秘密や重要技術に関する情報について、安全保障と公正な経済秩序の維持の観点から、為替法などによって越境移転が制限される¹²。以下は個人情報保護法における越境移転規制を対象に考察を加えていく。

個人情報保護法は日本のデータ越境移転規制枠組みにおいて中核的な立法として位置付けられていると考えられる。個人情報保護法を中心とする国内データ規制の整備を促進すると同時に、日本は国際社会に向けて「信頼性のある自由なデータ流通」（Data Free Flow with Trust: DFFT）¹³という原則の下で、多国間のデータ越境移転に関するガバナンスに積極的に参加している。

（一）個人情報保護法における規制枠組み

2022年改正後の個人情報保護法は域外適用の拡大、データ取扱事業者の責任および義務の強化、データ主体の権利の拡充、違反時の制裁措置の厳格

化に重点を置き、データ越境移転に関する規制を体系的に整備している。データ取扱事業者に対して、個人情報の提供先である移転先の法制度、移転先が講じる保護措置、その他の関連事項についてあらかじめデータ主体に通知して本人の同意を取得する義務が新たに課される（第 28 条）。ただし、次のように一定の条件を満たす場合に同意が不要とされる例外も認められる。第一に、移転先の国または地域が個人情報保護委員会によって「十分な個人情報保護レベルを有する」と認定（いわゆる十分性認定）されている場合に、本人の同意を要しない。第二に、十分性認定を受けていない国に対しても、移転先との間で標準契約条項（SCC）など適切な契約上の措置が講じられている場合に、例外的に同意なしの移転が認められる。これらの規定は越境データ移転の透明性を高めるとともに、個人の権利保護を強化するものであると考えられる。データ越境移転の具体的な条件に関して、個人情報保護委員会が定める関連ガイドラインによって詳しく掲げられている¹⁴。

（二）国際的規制との整合

EU との間において、日本は「十分性認定」（adequacy decision）を受けており、EU から日本への個人情報を移転する場合に、原則として追加的な認定手続を要しない。十分性認定を取得するために、当該国の個人情報保護制度が EU 一般データ保護規則（GDPR）の求める水準と整合していることが条件とされる。認定基準として、個人情報の収集、利用、保存といった取扱の方法、技術的および組織的な保護措置、監督機関の独立性、また救済手段の有無などが含まれる¹⁵。日本は 2015 年の個人情報保護法の改正および 2019 年に導入された EU との合意に基づく追加措置により、GDPR の要件を満たしていると認定されている¹⁶。また、前述したように、日本はアジア太平洋経済協力（APEC）の加盟国として、CBPR 制度を積極的に導入しており、APEC 域内における個人情報の移転を円滑化することを目指している。

日本政府はこれまで自由貿易の拡大や国内企業の国際展開を背景に、データ越境移転の国際規制枠組みへの積極的な関与を示している。たとえば、G7 や G20 といった国際フォーラムにおいても「信頼性のある自由なデータ流通」（Data Free Flow with Trust: DFFT）を提唱する立場をとっており、

その中で GDPR の十分性認定や CBPR への参加は日本の国際的信頼を高める要因となる。

四 中国と日本におけるデータ越境移転規制に関する比較考察

（一）規制の目的と基本理念

中国と日本のデータ越境移転規制は異なる経済社会の実情、国家戦略に基づいて構築されているため、規制の目的と基本理念に明らかな違いがあると思われる。中国のデータ越境移転規制は国の安全とデジタル主権を重視しており、この点について、サイバーセキュリティ法やデータセキュリティ法、個人情報保護法を通じて明らかに示されており、特にデータの越境移転に対して厳格なセキュリティ評価を求めることなどで、重要データを保護しようとする目的が示されている。一方、日本のデータ越境移転規制は個人情報の保護を基軸に置きながら、データの自由な流通を促進することも目的としている。規制の枠組みから見ると、GDPR に近いアプローチが採用されており、また EU との間の十分性認定によって、EU 加盟国からのデータ移転がスムーズに行われるように配慮がされている。データ越境移転において、個人情報保護を重視しつつ、国際的規制枠組みに適合する柔軟性を持たせていることが特徴的であるといえよう。

（二）規制対象と基準

規制対象について、中国ではデータの種類や重要度に基づいて厳格に分類されており、その上で「重要データ」や「個人情報」に対して異なる規制基準が適用される。データの越境移転に際して、特に個人の権利利益、国家安全と公共利益に関連するデータの移転が厳しく制限されており、セキュリティ評価など審査手続きを経なければならない。一方、日本における越境データ移転規制は比較的に緩和される取扱にされており、個人情報の越境移転に

際して、企業の自主的な判断および内部統制に基づく対応が一般的である。たとえば、標準契約条項（SCC）を利用することで移転先国の法制度が十分でない場合においても、一定の契約上の安全措置が講じられていればデータ越境移転が認められる。

（三）国内規制と国際的規制との整合性

現段階において、中国は国家主導によるデータ越境移転規制の枠組みを構築しつつあり、デジタル主権の確保を重要視している。法制度の全体を見ると、データ越境管理に関する規定は国内企業が業務上必要とするデータの安全かつ自由な越境移転を確保すると同時に、個人の権利利益、国家の安全および公共利益の保障に関わる個人情報や重要データに対して、必要な監督および管理を行うことを目的としている。ただし、現時点では国際的なルールとの整合性の確保において一定の課題が存在していることが否定できない。中国はEUの一般データ保護規則（GDPR）やAPECの越境プライバシールール（CBPR）といった国際的な枠組みに参加しておらず、その背景には多様な要因があると考えられる。他方、日本は個人情報保護委員会の制度運用を通じて、EUからGDPRに基づく「十分性認定」を取得しており、EUとの間におけるデータの自由な移転が実現している。この点において、国際的規制と高い整合性を有していると評価される。

（四）小括

以上の比較考察から、今後に向けて整備しつつある中国のデータ越境移転規制枠組みにとって、日本の法制度は若干の示唆が提供できると思われる。まず、日本はEU一般データ保護規則（GDPR）との制度的整合性を確保しており、十分性認定を受けることで国際的な信頼性と円滑なデータ移転が実現でき、国際的規制との調和を示している。次に、標準契約条項（SCC）やガイドラインといった方法を活用することで、企業の自主的なコンプライアンスに配慮した制度運用がなされており、法制度の実効性を高める上で参考となる。また、データ主体の権利保障や説明責任の明確化など、透明性を重視する点も注目に値する。さらに、データ越境移転先の法制度を評価する上

で、自由なデータ移転を認める十分性認定制度のような仕組みは中国においても安全保障と国際協調のバランスを取る手段として導入の可能性を検討する価値がある。

おわりに

中国におけるデータ越境移転に関する規制はサイバーセキュリティ法、データセキュリティ法、個人情報保護法という中核的な枠組みの下で、分類・等級管理、リスク評価などの方法を通じて、国の安全保障とデータの自由な移転とのバランスを図っている。中国はデータの越境移転に対して監督および管理を行うに際して、重要データおよび個人情報に対しては厳しく規制を課す一方、一般データについて自由な移転を認めている。このような規制体系は「データ安全と発展の主権」という原則を強調しており、国家主権と安全の維持を重視すると同時に、データ価値の最大限の実現やデジタル経済の発展促進を目指している。中国は引き続き国の安全保障を重視する規制を強化する一方、国際的な規制との整合性を高める必要があり、デジタル主権と自由貿易とのよりよいバランスを取るために、国内規制のさらなる整備が今後の課題であろう。

¹ 具体例として、2025年5月2日に、アイルランドのデータ保護委員会（DPC）は中国系動画共有アプリ「TikTok」のアイルランド法人に対して、EUの一般データ保護規則（GDPR）違反を理由に5億3千万ユーロの制裁金を科す決定を下した案件が挙げられる。制裁の理由について、TikTokがユーザーの個人情報を中国に移転するにあたり、GDPRに定められた適切な保護措置や法的根拠を欠いていたことが確認されたためということである。また、DPCはTikTokに対して、6カ月以内に是正措置を講じることを命じた。<https://www.sankei.com/article/20250502-QNXV7V7WEVJSPHTRSL3EHK2624/>

² <https://gdpr-info.eu>

³ 中国はAPEC加盟国であるが、CBPRシステムには参加していない。CBPRシステムは最初はAPEC加盟国によって推進されたが、その後、米国の提案の下、2022年にCBPRシステムはAPECの枠組みから独立し、非APEC加盟国を含むより多

くの国が参加できるようにグローバル CBPR フォーラムが設立された。

<https://www.meti.go.jp/press/2022/04/20220421001/20220421001.html>

ただ、こうした調整は中国の CBPR システムへの参加を排除することを目的とする可能性があると考えられる。

⁴ 2025 年 3 月までに、日本における AEPC CBPR 認定取得事業者にはインタセクト・コミュニケーションズ株式会社、株式会社 Paidy、株式会社インターネットイニシアティブ、PayPay 株式会社という 4 社がある。

⁵ APEC. (2015). *APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines*. p.5.

⁶ APEC. (2015). *APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines*. pp.7-8.

⁷ Greenleaf, G. (2018). *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. Privacy Laws & Business International Report*, p.12.

⁸ 国家インターネット情報弁公室が 2021 年に公布された『重要情報インフラ安全保護条例』第 2 条により、重要情報インフラとは国家安全、国民経済および公共利益に対し重大な影響を与える通信、金融、公共サービスなどの分野に関わる情報システムを指している。

⁹ たとえば、上海市『宝山区教育重要データ識別規則と重要データカタログ管理方法（試行）』に教育分野における重要データ記録やデータ識別監督、重要データカタログ管理、重要データカタログの開示などが定められている。

¹⁰ https://www.cac.gov.cn/wxzw/sjzl/sjcjfmqd/A09370806index_1.htm

¹¹ https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm

¹² 大井哲也＝岡辺公志『データ利活用のビジネスと法務』中央経済社 2024 年 203-206 頁。

¹³ <https://www.digital.go.jp/policies/dfft>

¹⁴ https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/#a3

¹⁵ <https://gdpr-info.eu/chapter-5/>

¹⁶ 個人情報保護委員会「個人情報保護法に基づく制度の概要」2020 年 15 頁。