2025.12.19

中国風険消息〈中国関連リスクニュース〉 <2025 No. 3>

中国における「ネットワークデータ安全管理条例」に関する解説

【要旨】
- 「ネットワークデータ安全管理条例」（以下「安全管理条例」）は、中国国務院により 2024 年 9 月に公布され、2025 年 1 月 1 日から施行された。ネットワークデータの安全管理を一層整備する重要な制度改正であり、中国で事業を展開するすべての企業にとって重大な影響を及ぼす内容となっている。
- 特に大量のネットワークデータを保有する日系企業は、安全管理条例の内容を把握し、関連する管理制度、コンプライアンス審査、教育訓練などの分野で対応措置を講じる必要があると考えられる。
- 本稿では、安全管理条例の背景と意義を紹介した上で、関連法との比較、企業への影響、実際の事例および求められる対応策について整理し、説明する。

1. 安全管理条例の背景と意義

（1）国際的な観点

現在、ネットワークセキュリティを取り巻く状況は世界的に一段と厳しさを増しており、米国や欧州では新たなネットワークセキュリティ関連法が相次いで制定され、より厳格なデータ監督体制が構築されつつある。

米国では、近年「サイバーセキュリティ情報共有法」「海外データ合法的使用明確化法（クラウド法）」「データ安全・保護法案」などが相次いで導入された。特にクラウド法は、米国企業および米国で事業を行う外国企業に対し、世界各地に保存されているデータの提供に協力することを求める内容である。また「データ安全・保護法案」は、個人データの収集、利用、保存、伝送に対してより厳格な要件を課し、企業のデータ安全保護責任を強化するものである。

欧州においては、ネットワークセキュリティ関連立法は、より体系的かつ厳格である。「一般データ保護規則（GDPR）」は 2018 年の施行以来、高い規制水準と厳格な罰則で世界的に知られており、違反した場合は全世界の年間売上高の 4%または 2,000 万ユーロのいずれか高い額が適用科せられる。その後も「サイバーセキュリティ法」「デジタルサービス法」「デジタル市場法」などが順次制定され、ネット空間の監督強化、プラットフォーム責任の明確化、データ安全およびユーザーの権益保護が一層推進されている。

このような国際環境の中で、各国はデータ越境移転やデータ安全保護に対する要求を高めており、データ領域における国際ルール競争が激しさを増している。中国はネットワークデータ大国として、国際ルールの変化に対応し、ネットワークデータ安全を維持するための関連法規体系を早急に整備する必要がある。また中国で事業を展開する企業に対し、明確なコンプライアンス指針を提示し、各国の法制度の差異により企業がコンプライアンス上の困難に陥ることを回避する狙いがあると考えられる。

（2）中国内の観点

中国のデジタル経済は急速に発展しており、ネットワークデータの価値は一段と高まっている。他方で、ネットワークデータを悪用した犯罪も増加しており、個人・企業・国家の安全に深刻な脅威をもたらしている。

個人情報の漏えいの観点において、違法手段を通じて大量の個人情報を取得し、詐欺やターゲティング広告などの違法行為に利用するケースが散見される。

企業データ安全の面では、営業情報の漏えいや基幹データの窃取が生じている。あるテクノロジー企業では、内部従業員が外部者と共謀し、基幹データを窃取して競合他社に流出させ、同社に大きな経済的損失と競争力低下をもたらした。また企業を狙ったハッカー攻撃も増加しており、ランサムウェアで企業データを暗号化し、身代金を要求するなど、企業の正常な運営に甚大な影響を与える事例も発生している。

(3)安全管理条例の意義

中国国内で深刻化するネットワークデータ安全の課題に対し、「サイバーセキュリティ法」「データ安全法」「個人情報保護法」(以下「データ三法」という)はデータ安全および個人情報保護に関する基本制度を定めてきた。しかし、実務レベルではなお細則の不足や制度運用面での課題が存在していた。安全管理条例は、ネットワークデータの処理活動をさらに規範化し、法律運用上の空白を補い、ネットワークデータの安全を保障し、データの適法・合理・有効な利用を促進するために制定されたものである。

2. 安全管理条例の適用範囲

安全管理条例は中国国内で実施されるネットワークデータ処理活動およびその安全監督に適用される。ここでいう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・利用される各種電子データを指す。

さらに、国外の機関・組織・個人が中国国外で行う活動であっても、中国国内の個人情報を処理する行為や、関連するネットワークデータ処理活動が中国の国家安全、公共利益、または公民・組織の合法的権益を損なう場合には、法に基づき責任追及の対象となる。これは中国に進出している企業にとって、在中拠点でのデータ処理のみならず、海外本社とのデータ連携も含め、在中ネットワークデータに関わる一切の活動が本条例の適用を受けることを意味する。

3. 安全管理条例の重点事項

安全管理条例は全 9 章 64 条で構成されており、章の構成及び章ごとの位置づけや対象は次のとおりである。

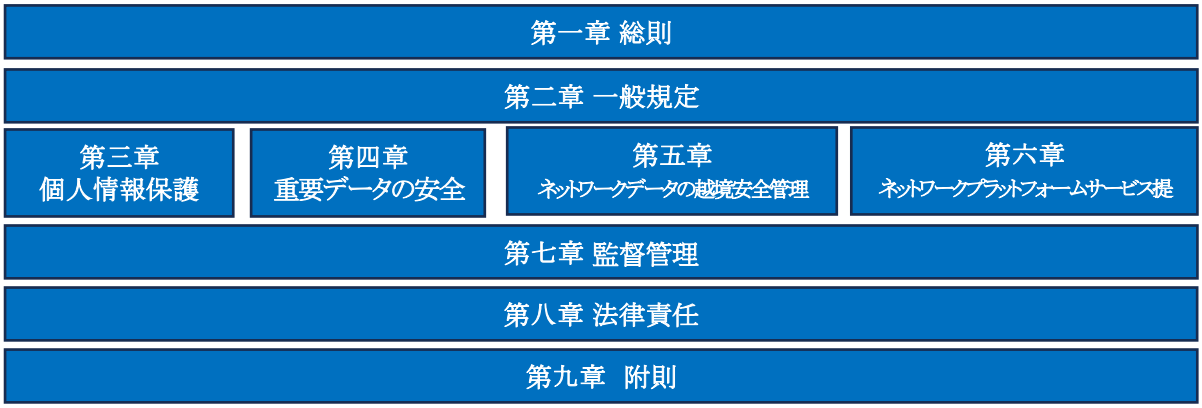

図 1　安全管理条例の章の構成

表 1　安全管理条例の各章の役割・位置づけと対象

章	役割・位置づけ	対象
第1章 第9章	条例の全体的な枠組みを整理し、補足的な規定内容を示す	安全管理条例の適用を受けるすべての事業者
第2章	ネットワークデータ処理活動における一般的な基本要求を定める	中国でネットワークデータを扱うすべての企業
第3章 第6章	個人情報、重要データ、越境データ、ネットワークプラットフォームサービス等に関する制度を体系的に整理する	個人情報・重要データを扱う企業、データを国外に移転する企業、プラットフォーム事業者
第7章 第 8 章	監督管理および法的責任について定め、条例の実効性確保を図る	監督当局およびネットワークデータを扱うすべての企業

(1)一般規定

違法なデータ処理活動の禁止	✓ 違法行為の禁止:いかなる組織または個人も、ネットワークデータを利用して違法な活動を行ってはならない。具体的には、ネットワークデータの窃取、違法な取得、販売、他者への提供などが含まれる。また、これら違法活動に特化したプログラム・ツールを提供したり、インターネット接続、サーバーホスティング等の技術的支援を提供することも禁止される。 ✓ 連帯責任:他人が違法なデータ活動を行っていることを知りながら支援した場合は、法に基づき責任追及の対象となる。
データ処理者の主体責任	✓ 基礎的防御義務:ネットワークデータ処理者は、ネットワークの等級保護制度[1]に基づき、データ安全管理制度を整備しなければならない。暗号化、バックアップ、アクセス制御、安全認証などの技術的措置を講じ、データが改ざん・破壊・漏えい・不正利用されないよう確保する必要がある。 ✓ 製品・サービスの適合性:提供するネットワーク製品・サービスは国家標準に適合していなければならない。安全上の欠陥や脆弱性を発見した場合、速やかに補修措置を講じ、ユーザーおよび主管する当局に通知する義務がある。国家安全または公共の利益に関わる場合は、24 時間以内に報告する必要がある。 ✓ 緊急対応体制:データ安全インシデントに対する緊急対応計画を策定しなければならない。インシデント発生時には直ちに計画を起動し、被害拡大を防止するとともに主管する当局へ報告する。インシデントにより個人または組織の権益が損なわれた場合、電話・SMS 等を通じて利害関係者に迅速に通知する必要がある。
データ協力及び移転の要件	✓ 委託処理とデータ提供:他の処理者に個人情報または重要データを提供し、もしくは処理を委託する場合は、契約により処理目的・範囲・安全義務等を明確に定め、受領側による義務履行状況を監督しなければならない。関連記録は少なくとも 3 年間保存する必要がある。 ✓ 共同処理とデータ移転:複数の処理者が共同でデータ処理の目的を決定する場合は、各者の権利・義務を取り決める必要がある。合併・解散等によりデータを移転する場合、受領側は引き続き安全保護義務を負う。
技術の適用及び自動化ツールの要件	✓ 自動化されたデータ収集:自動化ツールを用いてデータにアクセスし、データ収集する場合、ネットワークサービスに与える影響を評価しなければならず、違法な侵入やネットワークの正常運行への妨害は行ってはならない。 ✓ 生成系 AI サービス:生成系 AI サービスを提供する場合、学習データの安全管理を強化し、データ安全リスクの発生を防止する義務を負う。

[1] 等級保護制度（等保制度）とは、ネットワークや情報システムを重要度に応じて等級分けし、等級ごとに必要な安全対策や評価義務を定める中国の基本的なサイバーセキュリティ管理制度である。在中日系企業においても、中国国内でネットワークや情報システムを運用する場合には原則として適用対象となり、データ安全管理やコンプライアンス対応の前提制度の一つとなっている。

国家安全審査の要求	✓ 審査基準：ネットワークデータ処理活動が国家安全に影響を与え、または与えるおそれがある場合、規定に基づき国家安全審査を受けなければならない。具体的には「サイバーセキュリティ審査弁法」に準拠する（例：100 万人以上の個人情報を処理する企業が国外上場する場合は審査申告が必要となる）。

(2)個人情報保護

安全管理条例では、個人情報保護に関する規定が重点的に細分化されている。

透明性の要求	✓ 告知の形式：個人情報処理ルールを策定し、目立つ場所で一括して公開しなければならない。その内容は明確で理解しやすいものであることが求められる。 ✓ ルールに含むべき内容：処理者の名称・連絡先、処理目的・方法・種類、センシティブ情報を処理する必要性および個人の権益への影響、保存期間と期限到来後の取扱い、個人が権利を行使するための手段等を明示する必要がある。14 歳未満の未成年者の情報を処理する場合は、専用のルールを策定し、保護者の同意を得なければならない。
コンプライアンス義務	✓ 必要性の原則：サービス提供に必要な個人情報のみを収集し、過剰な収集や、誤導・詐欺・威圧等により同意を取得することは禁止される。 ✓ 制限される行為：本人が同意した目的・方法・種類・保存期間を超えて情報を処理してはならない。ユーザーが明確に拒否しているにもかかわらず執拗に同意を求める行為も禁止される。処理目的・方法・種類が変更される場合は、再度同意を取得する必要がある。
本人の権利の保障	✓ 権利行使のチャネル：個人が閲覧・複製・訂正・削除・処理制限・同意撤回・アカウント削除などを求めた場合、処理者は速やかに受理し、合理的で便利な手段を提供しなければならず、不合理な条件を設定してはならない。 ✓ データポータビリティ権：個人情報の転送（ポータビリティ）には、身元が検証できること、転送対象データが同意または契約に基づき収集されたものであること、技術的に実行可能であり他人の権益を害さないこと等の条件を満たす必要がある。
自動収集とデータ処理	✓ 不要情報の処理：自動化技術により、必要でない情報または未承認の情報を避けて収集することができない場合は、当該情報を削除または匿名化して処理する必要がある。技術的に実現が難しい場合は、保存および安全保護を除くすべての処理を停止しなければならないものである。 ✓ アカウント削除後の義務：アカウントの削除に伴い、個人情報を速やかに削除または匿名化しなければならない。
越境・大規模処理に対する義務	✓ 国外の処理者に対する要求：中国国内の個人の個人情報を国外で処理する者は、「個人情報保護法」に基づき、中国国内に専門機構を設立するか代表者を指名しなければならず、その情報を所在地の地級市[2]レベルのサイバー管理当局届け出る必要がある。 ✓ 超大規模処理に対する強化義務：1,000 万人以上の個人情報を処理する者は、データ安全管理機構およびデータ安全責任者を設置しなければならない。合併・解散などでデータ安全に影響が生じる場合は、処置方案を策定し、省レベル以上の主管部門へ報告する必要がある。
コンプライアンス監査と監督体制	✓ 定期監査：個人情報処理活動について、自ら、または専門機関に委託してコンプライアンス監査を定期的に実施しなければならない。

[2] 地級市とは、中国の行政区分において、省の下位に位置する地方行政単位であり、日本の「県庁所在地を中心とする広域市」に近い位置付けである。多くの場合、企業に対する行政手続や監督・届出は地級市レベルの主管部門が所管している。

	✓ プラットフォームの特別責任：大型ネットワークプラットフォーム（ユーザー数が5,000 万超または月間アクティブユーザー数が 1,000 万超）の場合、個人情報保護に関する社会的責任の年度報告を公表する必要がある。

法的責任：個人情報保護関連規定に違反した場合、その程度に応じて警告・罰金等の処分を受ける。例えば、所定の告知義務を履行しなかったり、不適切な方法で同意を取得した場合、5 万元以上 50 万元以下の罰金を科される可能性がある。情状が重い場合は 50 万元以上 200 万元以下の罰金に加え、関連業務の停止、営業停止・整頓等を命じられることがある。

(3) 重要データの安全保障

安全管理条例は重要データを明確に定義している。すなわち、特定の分野・集団・地域に関する、または一定の精度・規模に達するデータであって、改ざん・破壊・漏えい・違法な取得や利用が行われた場合に、国家安全・経済運行・社会安定・公共の健康および安全に直接的な危険をもたらすおそれのあるデータである。例えば、金融業の顧客取引データ、医療業の患者カルテデータ、エネルギー業のパイプライン運転データなどは重要データに該当し得る。

重要データ目録の管理	✓ 国による統括：国家のデータ安全調整メカニズムが重要データ目録の策定を統括し、各地区・各部門がこれに基づき当該地区・当該業界の具体的な目録を定め、動的に更新する。 ✓ 企業の責任：ネットワークデータを扱う事業者は、自らの業務において重要データを識別し、届出を行う責任を負う。所管地区または部門が審査した上で、適宜、その事業者が扱う重要データの目録を通知または公表する。 ✓ 技術支援：データラベルによる識別などの技術を活用し、重要データ管理の効率を高めることを奨励する。
処理者の組織的責任	✓ 機構と人員の設置：重要データ処理者は、安全管理機構と安全責任者を設置しなければならない。安全責任者は専門的知識と管理経験を有し、経営層メンバーが担当することが求められる。金融・エネルギーなどの特定業界では、安全責任者および重要ポストの人員に対してセキュリティ審査を実施し、必要に応じて公安機関または国家安全機関の協力を申請できる。 ✓ 管理機構の責務：安全制度・操作規程・緊急対応計画を策定し、定期的なリスクモニタリング、緊急対応訓練、研修を実施する。また、データ安全に関する苦情や通報を受理し、処理する責任を負う
データ流通リスクの管理	✓ 事前リスク評価：重要データを提供、委託処理、共同処理する前（法定義務を履行する場合を除く）に、リスク評価を実施しなければならない。評価のポイントは、受領側の目的の適法性・信頼性・契約拘束力、データ改ざん・漏えい等のリスクと国家安全への影響、防護措置の有効性などである。 ✓ 特殊事案への対応：合併・解散・破産等により重要データ安全に影響が出るおそれがある場合、処置方案を策定し、省レベル以上の主管部門に対し、受領側情報および防護措置を省級以上の主管部門へ報告する必要がある。
年次リスク評価および報告体制	✓ 報告内容：処理者の基本情報、安全管理機構および安全責任者の連絡先、重要データの処理目的・種類・数量・保存場所および安全措置（暗号化、バックアップ、アクセス制御など）、年間のデータ安全インシデントおよびその処置状況、データの越境状況等が含まれる。 ✓ 強化義務：大型ネットワークプラットフォームは、重点業務およびサプライチェーンに関するデータ安全状況も追加で説明しなければならない。国家安全を害する活

	動が存在する場合、省級以上の主管部門は是正または処理停止を命じることができる。
他分野との連携	✓ 金融業における特例：銀行・保険機関は、重要データをコアデータ階層に組み入れ、最高レベルの保護を実施し、インシデント発生後は 2 時間以内に監督当局へ報告する必要がある。 ✓ 自由貿易区での越境管理：自由貿易区はデータ越境に関するネガティブリストを策定できる。リスト外のデータについては、安全評価の免除が認められ得る一方、リスト内の重要データの越境については通常どおり申告が必要である。

法律責任：重要データの識別・申告を行わなかった場合、またはリスク評価を実施しなかった場合は、10 万元以上 100 万元以下の罰金を科される。情状が重い場合は、100 万元以上 1,000 万元以下の罰金が科され、併せて直接責任を負う主管者およびその他の直接責任者に対して 1 万元以上 10 万元以下の罰金が科される。

(4)ネットワークデータの越境移転に関する安全管理

安全管理条例は、既存の関連部門規章の立案・運営経験を踏まえ、データ越境管理規程のメカニズムをさらに最適化している。

管理の枠組み	✓ 総合調整体制：国家サイバー管理当局が主体となり、データ越境安全管理の専門作業部会を設置し、越境データ管理方針の策定および重大事項の調整を担当する。 ✓ 分類・階層別管理の原則：重要データおよび規定された規模に達する個人情報についてのみ越境移転を管理し、一般データは自由に越境移転できる。 ✓ 自由貿易試験区における新たな制度枠組み：自由貿易試験区は「データ越境ネガティブリスト」を策定することができ、リスト外のデータについては安全評価、標準契約または認証を免除できる。
重要データの越境移転の管理ルール	✓ 重要データの定義：国家安全・経済運行・社会安定等に危害を及ぼすおそれのあるデータである。 ✓ 申告免除：関係部門や地区から重要データとして通知・公表されていないデータについては、越境安全評価を申告する必要はないとされる。 ✓ 越境条件：安全評価の結果として国家安全および社会公共の利益を害さないと認定された場合に限り、越境提供が可能となる。 ✓ リスク評価要件：重要データの越境に際しては、受領側の目的の適法性、契約拘束力、防護措置の有効性等を評価しなければならない。
越境移転メカニズム	✓ 適法な越境移転ルート：国家サイバー管理当局による安全評価、専門機関による個人情報保護認証、個人情報越境標準契約の締結等のルートが定められている。 ✓ 特定状況における免除：個人との契約履行（越境 EC、ビザ申請等）、合法制度に基づく人事管理（従業員情報提供）、法定職務の履行、生命・財産の緊急保護、非重要インフラ運営者による年間 10 万人未満の非センシティブ個人情報[3]の越境など、一定の場面では上記手続の免除が認められる。 ✓ 規模に応じた階層別管理：重要情報インフラの運営者、重要データの越境移転、または年間の越境移転が非センシティブ個人情報 100 万件以上、もしくはセンシティブ個人情報 1 万件以上となる場合は、安全評価を申請しなければならない。

[3] 非センシティブ個人情報とは、中国の「個人情報保護法」に定義されるセンシティブ個人情報（人種、宗教、健康情報、生体識別情報、金融口座情報等）に該当しない個人情報を指す。中国法上、センシティブ個人情報と比べて取扱い要件は相対的に緩やかであるが、個人情報に該当する以上、収集・利用・越境提供等においては合法性、正当性、必要性の原則および安全管理義務が引き続き適用される。

データ処理者のコンプライアンス義務	✓ 契約による監督および記録の保存：国外の受領者に対して、データの使用目的と範囲を契約により拘束し、その義務履行状況を監督する必要がある。データ越境に関する承認記録およびログは、少なくとも 3 年間保存しなければならない。 ✓ 安全保護とインシデント対応：暗号化やアクセス制御などの技術的措置を講じる義務がある。データ安全インシデントが発生した場合、直ちに救済措置を講じ、国家サイバー管理当局に報告しなければならない。個人の権益が害される場合は、利害関係者に速やかに通知する必要がある。 ✓ 禁止行為：安全評価または契約で明示された目的・範囲・データタイプを超えて国外にデータを提供してはならない。

法律責任：ネットワークデータの越境移転に違反した場合、20 万元以上 200 万元以下の罰金が科される。事案の深刻度が高い場合は、200 万元以上 1,000 万元以下の罰金が科され、あわせてデータの越境移転を制限されることがある。さらに、直接責任を負う主管者およびその他の直接責任者には、2 万元以上 20 万元以下の罰金が科される。

(5) ネットワークプラットフォームサービス提供者の義務

ネットワークプラットフォームサービス提供者がデジタル経済および公共サービスにおいて重要な役割を担っていること、ならびに実務上存在する問題を踏まえ、「安全管理条例」はその義務について特別な規定を設けている。ネットワークプラットフォームサービス提供者、第三者の製品およびサービス提供者、プリインストールされたアプリケーションを搭載するスマート端末などの機器製造者に対し、ネットワークデータの安全保護義務を履行することを、安全管理条例では求めている。

第三者に対する管理義務	✓ データ保護：プラットフォーム規則または契約により、第三者のデータ安全保護義務を明確にし、その義務の履行を確保する。第三者の違反行為によってユーザーに損害が生じた場合、プラットフォームは法に基づき相応の責任を負う。
アプリ配信の管理	✓ 審査ルール：アプリケーションの検証ルールを整備し、規定に適合しないアプリについては、警告、配信しない、一時的な配信停止、または配信の終了といった措置を講じる。
自動化決定に関する規定	✓ 情報配信機能：個人に対して情報をプッシュ配信する際には、操作しやすい形でパーソナライズ設定のオフ、配信拒否、およびユーザータグ削除の機能を提供しなければならない。
大型プラットフォームの特別義務	✓ 特別義務：年度個人情報保護に関する社会責任報告の公表、データの越境提供における国家安全要件の遵守、データやアルゴリズム等を利用した誤導、詐欺、威圧、不合理な差別的取扱いなど、ユーザーの権益を損なう行為の禁止が含まれる。

法律責任：ネットワークプラットフォームサービス提供者が関連義務に違反した場合、その処罰は厳しく、違反の程度に応じて 10 万元から 1,000 万元までの罰金が科されるほか、事業の停止や営業停止・是正措置といった処分を受ける可能性がある。

4. 安全管理条例と関連法律の共通点と相違点

「データ三法」は、中国のネットワークデータ安全分野における基本的な法的枠組みを構築しており、安全管理条例はその補完的な行政法規として、これらの法律と密接に関連しつつも、明確な相違点を有している。

（1）共通点

共通点	
立法目的の共通性	これらの法律・法規の根本的な目的はいずれも、国家安全と公共の利益を維持し、個人および組織の合法的権益を保護することにある。 ✓ 「サイバーセキュリティ法」は、ネットワーク安全を保障し、サイバー空間主権を維持し、経済社会の情報化の健全な発展を促進することに重点を置く。 ✓ 「データ安全法」はデータ安全の保障およびデータの開発・利用の促進を目的とする。 ✓ 「個人情報保護法」は個人情報権益の保護、個人情報処理活動の規律に焦点を当てる。 ✓ 安全管理条例も同様に、ネットワークデータ処理活動の規範化とネットワークデータ安全の保障を目標としている。
共通原則の遵守	データ処理活動において、これらはいずれも合法性、正当性、必要性の原則を遵守している。 ✓ 「サイバーセキュリティ法」は、ネットワーク運営者が個人情報を収集・利用する際、収集・利用ルールを公開し、目的・方法・範囲を明示し、本人の同意を得る必要があると規定する。 ✓ 「データ安全法」は、データ処理活動において法令遵守、商業道徳・職業道徳の遵守、誠実信用、データ安全保護義務の履行、社会的責任の負担を求める。 ✓ 「個人情報保護法」は、誤導・詐欺・威圧等の手段による個人情報処理を禁止する。 ✓ 安全管理条例も、個人情報保護や重要データ管理等の面で、これら原則を一貫して踏襲している。
データ安全保護の全過程の重視	これらの法律はいずれも、データの収集、保存、利用、共有から廃棄に至るまでの全過程にわたり、安全保護を求めている。 ✓ 「サイバーセキュリティ法」は、ネットワーク運営者が技術的・その他必要な措置を講じ、ネットワークの安全・安定運行を確保し、インシデントに効果的に対応し、個人情報安全を保護し、情報漏えい・破壊・喪失を防止することを求める。 ✓ 「データ安全法」は、データ処理者に対し、全プロセスのデータ安全管理制度の整備、教育訓練の実施、相応の技術的・その他必要措置の採用を求める。 ✓ 「個人情報保護法」は、個人情報の収集・保存・使用・加工・伝送・提供・公開・削除など各段階における安全保護義務を詳細に規定している。 ✓ 安全管理条例もまた、データの識別、処理、防護、評価、点検、是正、緊急対応といった内容から構成される、体系化された閉ループ型の管理メカニズムを構築している。

（2）相違点

相違点	
法律の階層と効力の違い	「データ三法」はネットワーク安全分野における基本的な法律であり、トップレベルの設計枠組みを構成する。一方で安全管理条例はその下位に位置づけられる実施細則である。 ✓ 「データ三法」は全国人民代表大会常務委員会が制定・採択した法律であり、高い法的効力を有する。 ✓ 安全管理条例は中国国務院が制定・公布する行政法規であり、法律より下位に位置づけられるが、行政法規体系においてネットワークデータ安全管理に重要な規範機能を果たす。条例の内容が法律と一致しない場合は、法律が優先される。法律の枠内で、条例が具体事項を細分・補充する位置づけである。
規律面における重点の相違	「データ三法」はそれぞれの核心分野に重点を置くのに対し、安全管理条例は実務レベルの概念・定義により着目している。 ✓ 「サイバーセキュリティ法」は、ネットワークにおける運用の安全性と情報の安全性という二つの側面に重点を置き、特に重要情報インフラの運行安全、ネットワーク運営者による個人情報収集・利用ルール、インシデント報告等を中心に規定する。 ✓ 「データ安全法」はデータそのものを対象とし、データ処理活動における安全保障措置、データの分類・階層管理、データ安全ガバナンス体制の構築を重視する。 ✓ 「個人情報保護法」は個人情報保護に特化し、処理ルール、越境提供ルール、個人の権利などを全面的かつ詳細に規定する。 ✓ 安全管理条例は、ネットワークデータ処理活動およびその安全監督に焦点を当て、「ネットワークデータ処理者」という統括的概念を打ち出すとともに、行政法規レベルで初めて「重要データ」の定義を明確にしている。
マクロ規定と細則の相違	「データ三法」が国家レベルでの全体要求を定めるマクロ的な枠組みであるのに対し、安全管理条例はこれら要求を実務に落とし込む具体的な細則である。 ✓ 「データ三法」は制度・原則をマクロレベルで確立している。 ✓ 安全管理条例は、法律が定める原則を具体化し、個人情報保護の面では「データポータビリティ権」の行使条件を明示するなど、より詳細な要件を規定している。また、重要データの全ライフサイクル安全管理について、安全責任者は経営層メンバーであるべきこと、さまざまな場面に応じたリスク評価要件などを細かく定めている。

5. 安全管理条例による企業への要求

企業は日常の運営において、従業員の個人情報管理、顧客データの保守、業務データの保存および送信など、大量のネットワークデータ処理活動に関与している。安全管理条例の施行により、企業が自社のデータ安全管理体系を改めて見直し、整備する必要性を意味するものである。

（1）個人情報保護

- プライバシーポリシーの一層の透明化：一元的に公開し、分かりやすく明示することを求めるだけでなく、個人情報の収集および他者への提供に際しては、目的、方式、種類および受領者に関する情報を「一覧」の形式で列記しなければならない。
- 個人情報の移転（ポータビリティ）への対応：個人の「データポータビリティ権」を具体化する 4 つの条件が明示されており、企業は身元確認と技術的実現可能性を前提として、データ移転の手段を、個人情報の移転を請求した個人に提供しなければならない。

- 削除または匿名化が新たに求められる場面：クローラー[4]などの自動化収集技術を使用することにより、必要ではない個人情報や、法に基づき同意を取得していない個人情報を避けて収集することができない場合には、当該情報を削除するか、匿名化処理を行わなければならない。
- 定期的なコンプライアンス監査の重視：企業は、自らまたは専門機関に委託して、個人情報処理活動に関するコンプライアンス監査を定期的に実施する必要がある。
- 国外処理者による情報の報告：国外において中国国内の個人の個人情報を処理する者であり、「個人情報保護法」に基づき中国国内に専任機構を設置するか、代表者を指定している場合には、関連情報を所在地の地級市レベルのサイバー管理部門へ報告する必要がある。

（2）重要データの安全確保

- 重要データの識別：企業は、国家および業界の主管部門が策定する重要データの目録に留意し、それに基づいて自社が重要データを扱っているかどうかを判断する必要がある。
- 管理機関および責任者の設置：重要データを処理する者は、データ安全責任者および管理機関を明確にし、毎年、年度リスク報告を通じて主管部門に報告しなければならない。
- 重要な操作前のリスク評価：重要データを提供する場合、委託処理する場合、または共同処理する場合には、（法定の職責または法的義務の履行に該当する場合を除き）リスク評価を実施しなければならず、さらに毎年、年度リスク報告を通じて主管部門に報告しなければならない。
- 年次リスク評価と報告：重要データ処理者は、毎年自らのネットワークデータ処理活動に対するリスク評価を行い、省級以上の主管部門へリスク評価報告を提出しなければならない。
- 特定状況でのデータ処置：合併・分割・解散・破産等により重要データ安全に影響が生じるおそれがある場合、データ処置方案を作成し、主管部門へ報告しなければならない。

（3）ネットワークデータの越境安全管理

- 個人情報越境の 8 類型：よく知られている安全評価、保護認証、標準契約の三つのルートのほかに、安全管理条例では、契約の履行、越境的人事管理、生命・健康および財産の安全を保護するために必要な場合など、その他のケースも追加している。
- 重要データの国外移転には安全評価が求められる：重要データを国外へ提供する場合には、国家のサイバー管理部門が実施するデータ越境安全評価を受けなければならない。
- 越境提供の範囲制限：データ越境安全評価を経た後に、個人情報や重要データを国外に提供する場合には、評価時に明確にされた目的、方法、範囲、種類および規模を超えてはならない。

（4）ネットワークプラットフォームサービス提供者の義務

- ネットワークプラットフォームサービス提供者、特に大規模プラットフォームは、より厳格な責任を負う必要がある。これには、プラットフォーム上のアプリケーションに対する厳格な検証、ユーザーに対するパーソナライズ設定のオフ機能の提供などが含まれ、また大規模プラットフォームは、年度監査などの強化された義務を履行する必要が生じる場合がある。

（5）中国に進出する日系企業への留意点

- データの国外移転におけるコンプライアンス上の課題：在中の日系企業は、データを日本または地域本部へ送付する必要が生じることが多い。安全管理条例は、データの国外移転に関する多層的な要件を改めて明確にしている。企業は各データルートごとにその適法性を慎重に確認する必要があり、とりわけ重要データが関わる場合には安全評価を必ず受けなければならない。

[4] クローラーとは、プログラムを用いてウェブサイトやネットワーク上の情報を自動的に巡回・収集する仕組み（自動取得ツール）を指す。検索エンジンによる情報収集などの正当な用途がある一方、設定や利用方法によっては、過剰なアクセスや無断取得としてデータ安全・個人情報保護上の問題を生じさせる可能性がある。

- 日中両国の法規制差異への対応：日本にも APPI（個人情報保護法）などのデータ保護規制が存在する。在中の日系企業は、中国と日本の双方のコンプライアンス要件を同時に満たす必要があり、とりわけ中国では重要データ管理、データのローカライゼーション、国外移転に係る評価などの面で、より厳格な規定が設けられている点に注意が必要である。
- サプライチェーンデータの安全管理：在中日系企業の多くはグローバルサプライチェーンに組み込まれている。安全管理条例は、個人情報や重要データを他の処理者へ提供・委託する場合、契約により安全保護義務を明確化し、履行状況を監督することを求めている。したがって、中国国内の協力パートナーに対する契約面・運用面の管理強化が求められる。
- 「重要データ」の識別に関する負荷：在中の日系企業は、中国で長年事業を行う中で膨大なデータを蓄積している可能性がある。特に注意すべき点として、1,000 万人以上の個人情報を処理する場合には、重要データ処理者として一部の義務が適用されることになる。そのため、正確なデータ分類・階層化が極めて重要である。

6. 実際に発生した事例

近年、すでに一部の企業がデータ安全に関する法律・法規に違反したとして処罰を受けている。これらの事例は、在中日系企業に対しデータ安全に関するコンプライアンス業務を極めて重視し、安全管理条例および関連する法律・法規を厳格に遵守し、同様の過ちを繰り返さないよう警鐘を鳴らすものである。

事例 1：

概要	重慶の IT 企業が、自社の自動車レンタルサービス用「OA 情報システム」のデータを計 159 回にわたり窃取された。
原因	当該システムの 3306 番ポートが開放され、MySQL データベースサービスがパスワード未設定の状態で稼働しており、認証情報の脆弱性が存在していた。
違反事項	ネットワーク安全・データ安全保護義務を法に従い履行せず、データ安全を確保するための技術的措置を講じていなかった。
関連法令	「サイバーセキュリティ法」「データ安全法」「ネットワークデータ安全管理条例」

事例 2：

概要	湖南省の IT 企業のイントラネットデータベースがインターネット上に露出し、漏えいリスクが存在していた。
原因	イントラネットデータベースにアクセス認証の脆弱性および弱い認証情報の脆弱性が存在していた。また、エンジニアが大量のユーザーデータをイントラネットデータベースにコピーし、公共インターネットへのアクセスポートを開放していた。
違反事項	ネットワーク安全・データ安全保護義務を履行せず、関連管理制度を構築せず、データ安全を確保する技術的措置を講じていなかった。
関連法令	「サイバーセキュリティ法」「データ安全法」「ネットワークデータ安全管理条例」

事例 3：

概要	上海 IT 企業が運営する自動販売機が、顔情報を違法に収集し、システムに安全脆弱性が存在していた。
原因	決済過程でユーザーの同意を得ずに顔情報を収集していたほか、個人情報保護影響評価制度を構築しておらず、システム上に高リスクの SQL インジェクション脆弱性が存在していた。
違反事項	個人の顔情報の違法収集、個人情報保護影響評価制度の未構築、重大なセキュリティ上の脆弱性の放置。
関連法令	「サイバーセキュリティ法」「個人情報保護法」「ネットワークデータ安全管理条例」

7. 企業に求められる対応策

企業がこのような事例を未然に防止するためには、企業自らが安全管理条例が求める要件に対し、①自社のネットワークデータ処理活動が適合しているか、②要件に対し、有効に機能しているのか、という点を鑑み、

対応を検討し、取組みを進めていく必要がある。取組みを進めていく上で重要な観点として以下が考えられる。

（1）全社を対象とした自己点検と評価

在中企業は、法務・IT・業務などの部門で構成する専門チームを組織し、安全管理条例の要件に照らして、自社の現在のネットワークデータ処理活動について全社を対象とした自己点検を行う必要がある。点検には、データ収集経路が合法であるか、データの保存が安全であるか、利用範囲が付与された権限の範囲内であるか、共有先が適法であるか、データの国外移転プロセスが規定に適合しているかといった全ての段階が含まれる。

また、個人情報保護、重要データ管理、データの国外移転などの側面において、安全管理条例との適合度を評価し、存在するギャップや問題点を詳細に列挙し、書面報告として取りまとめる必要がある。例えば、企業が用いている個人情報収集フォームが必要事項をすべて明確に告知しているか、データ保存システムの安全防護措置が十分であるかなどを確認することが含まれる。

（2）管理制度および業務フローの整備

自己点検の結果に基づき、企業内部のネットワークデータ安全管理制度および操作フローを整備する。各部門や各職務におけるデータ安全管理上の責任を明確化する必要があり、例えば IT 部門はデータ保存の安全性を担保し、業務部門はデータ収集の適法性を確保するなど、役割分担を明確にすることが求められる。

また、データ区分・階層化制度を整備し、安全管理条例が定義する個人情報と重要データの区分に従って、企業が保有するデータを分類・階層管理する。あわせて、リスク評価、安全防護、緊急対応などの制度を策定し、定期的なデータ安全リスク評価の実施や、データ漏えい時の緊急対応計画の策定などを行う。

例えば、個人情報処理フローの詳細な規程を整備し、収集・保存・利用・削除の各段階における操作要件を明確化するほか、データアクセス権限の管理メカニズムを整備し、権限を有する者のみが機微データや重要データにアクセスできるようにして、重要データの安全な保管・伝送を確保する。

（3）従業員教育・研修の強化

全従業員を対象としたネットワークデータ安全研修を実施し、とりわけ個人情報を取り扱う人事部門、マーケティング部門（顧客データ）等、データ処理に携わる重要な職務にある担当者に重点的な教育を行う必要がある。

研修内容には、安全管理条例の主要内容、社内のデータ安全管理制度・プロセス、データ安全リスクの認識等を含めるべきである。さらに、事例分析やシミュレーション演習などの手法を活用して研修効果を高め、従業員がデータを不適切に処理した場合に生じ得る重大な結果を十分に理解し、ネットワークデータ安全への認識および適切な行動の定着を図ることが求められる。。

（4）コンプライアンス審査体制の構築

専任のコンプライアンス審査担当者またはチームを設置し、法律およびデータ安全に関する知識を備えた専門人材で構成する。企業が新たに展開するビジネスモデル、データ処理活動、データ連携プロジェクトなどについて事前のコンプライアンス審査を行い、安全管理条例および関連する法律・法規の要件に適合していることを確保する。

例えば、新たな市場調査プロジェクトを実施するにあたり、大量のユーザーデータを収集する必要がある場合には、コンプライアンス審査チームが事前にデータ収集計画の適合性を確認する。また、他企業とデータ共有の協力を行う際には、データ利用に関する協定条項がデータ三法等にに合致しているかどうかを審査し、違反行為によって法的リスクやレピュテーションリスクが生じることを回避する。

(5)外部専門機関の活用

企業がデータ安全やコンプライアンスに関する専門的な能力を自社内で十分に備えていない場合には、専門のコンサルティング会社や法律事務所の支援を求めることも一つの手段である。これらの専門機関は、安全管理条例に関する専門的な助言、コンプライアンス対策の設計、リスク評価などのサービスを企業に提供し、企業が安全管理条例の要件をより効率的に満たすことを支援することが可能である。

例えば、当社においてもデータ三法および関連する GB(中国国家標準)に基づく専門的な評価サービス(サービス名:データ三法対応状況評価サービス)も提供しており、企業のコンプライアンスリスクを洗い出し、データ資源と企業の信頼性を守り、法的リスクを低減することを支援している。

実施にあたっては、ヒアリング、現場点検、ツールによるテストなどが含まれ、主にネットワーク環境、等級保護およびデータ安全、システム脆弱性など 7 項目を評価するものである。

図1:データ三法対応状況評価サービス実施方法と評価項目

図2:データ三法対応状況評価サービスの成果物の一例

サービス提供からレポート提出までの期間は約 1 か月であり、日中両言語による評価報告書を提出するサービスである。評価報告書においては、リスク項目を3つの分類(高リスク、中リスク、低リスク)に整理し、区分・

階層化、安全防護などの是正策を提示することで、企業の経営層が既存のリスクを全体的に把握し、今後の改善方向を明確にし、企業のネットワークセキュリティ能力を向上させることにつながると考えている。

8. まとめ

本稿では、「ネットワークデータ安全管理条例」に基づき、在中日系企業がネットワークデータ管理の観点から特に留意すべき要点について解説した。

「ネットワークデータ安全管理条例」の施行は、在中企業のネットワークデータ安全管理に対して新たな要件と課題を提示するものである。在中企業はこれに積極的に対応し、コンプライアンス管理を強化し、ネットワークデータ安全の保護水準を高めることで、中国における事業の安定的な発展を確保する必要がある。

執筆：インターリスク上海　高級経理　張若亭

参考資料:

- 《网络数据安全管理条例》
  https://www.gov.cn/zhengce/zhengceku/202409/content_6977767.htm
- 国家网信办发布近期网络安全、数据安全、个人信息保护相关执法典型案例
  https://www.cac.gov.cn/2025-09/16/c_1759741437315419.htm
- 健全数据安全法律制度 筑牢网络数据安全防线
  https://www.moj.gov.cn/pub/sfbgw/zcjd/202409/t20240930_507078.html
- 宽严相济，张弛有道：《网络数据安全管理条例》主要亮点与合规参考
  https://www.zhonglun.com/research/articles/53628.html

MS&AD インターリスク総研は、2024 年 4 月、これまでのホームページを刷新し、リスクに強い組織づくりをサポートするプラットフォーム「RM NAVI（リスクマネジメント ナビ）」をリリースしました。
「RM NAVI」は、MS&AD インターリスク総研の知見をフル活用して、情報提供から実践までをトータルサポート。
コンサルタントの豊富な経験と、最先端のデジタルサービスで、リスクに強い組織づくりを支えます。
あなたに寄り添い、最適な答えへと導く、リスクマネジメントの羅針盤です。