中国におけるサイバーセキュリティー、データセキュリティーおよび個人情報保護の法規制にかかわる対策マニュアル

（2021 年 11 月）

日本貿易振興機構（ジェトロ）

北京事務所

ビジネス展開・人材支援部

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）北京事務所が金誠同達法律事務所に作成委託し、2021 年 10 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。

ジェトロおよび金誠同達法律事務所は、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金誠同達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：

ジェトロ・北京事務所
E-mail：PCB@jetro.go.jp

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

JETRO

2021 年 11 月
JETRO 北京

目次

2021 年 11 月
JETRO 北京

中国におけるサイバーセキュリティー、データセキュリティー および個人情報保護の法規制にかかわる 対策マニュアル

2016 年 11 月 7 日に、「中華人民共和国サイバーセキュリティー法」（以下「サイバーセキュリティー法」）が公布され、2017 年 6 月 1 日から正式に施行されている。当該法においては、サイバーセキュリティー等級保護制度、重要情報インフラセキュリティー保護制度、個人情報および重要データの越境に対する監督管理などの一連の法律制度が、確立されている。

サイバーセキュリティー環境の変化とビッグデータ応用の漸次的な広域化に伴い、2021 年 6 月 10 日には、「中華人民共和国データセキュリティー法」（以下「データセキュリティー法」）が公布され，2021 年 9 月 1 日から正式に施行されている。当該法においては、「サイバーセキュリティー法」を基礎としたデータ分類分級制度、データセキュリティー審査制度、データセキュリティーリスク評価などの一連の法律制度が、より一層確立されている。

さらに、「民法典」における人格権に対する重要な規定の制定に伴い、2021 年 8 月 20 日には、「中華人民共和国個人情報保護法」（以下「個人情報保護法」）が公布され、2021 年 11 月 1 日から施行されている。「個人情報保護法」においては、「民法典」などの関連法を基礎とし、知る権利の下での同意制度、個人機微情報の取扱制度、自動化された意思決定の取扱いなどの重要な意味を有する新たな制度が、明確にされている。

この時点をもって、中国においては「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（以下併せて「三法」）を核とするネットワーク法の体系が形成され、デジタル化時代におけるサイバーセキュリティー、データセキュリティー、および個人情報権益の保護に向けた基礎的な制度上の保障が提供されている。外資企業を含め多くの企業に対し、ネットワークの安全に関するコンプライアンス上の要求が提起されている。係る状況を背景として、ここでは、「サイバーセキュリティー法」「データセキュリティー法」「個人情報保護法」およびその付随規定において定められている各制度に関する法的リスク、企業が直面する課題等を整理し、企業のアクションアイテムおよびその実行方法について提議をする。

一、各法の全体像

（一）三法の立法の背景

１．「サイバーセキュリティー法」[1]

(1) 国際的な背景

国際的なサイバーセキュリティーの法的環境には、今まさに変革の最中であり、サイバーセキュリティーは既にグローバルな問題となっている。米国や EU 等の IT 強国では、サイバーセキュリティーをめぐる立法の体系が次々に確立されている。

(2) 中国国内における背景

2015 年には「中華人民共和国国家安全法」が可決されている。2015 年の 7 月には、サイバーセキュリティーの基本法として「サイバーセキュリティー法（草案）」に対する社会からの意見が、初めて公に募集されている。2016 年の 11 月 7 日には、全国人民代表大会常務委員会において、「サイバーセキュリティー法」が可決された。立法の迅速な推進は、中国が直面する国内外のサイバーセキュリティー形勢の客観的かつ現実的な緊急の課題に応じるためのものであり、中国におけるサイバー空間の法制化の過程の実質的な展開を表している。

２．「データセキュリティー法」「個人情報保護法」

(1) 国際的な背景

情報グローバル化時代の幕開けに伴い、データセキュリティーおよび個人情報の関連問題は頻発しており、世界の重要な国家と国際組織は、立法を通じたデータセキュリティー問題に対する規制を前後して敷いている。

(2) 中国国内における背景

近年においては、中国国内の産業のデジタル化、モデルチェンジおよびアップグレードが加速し、データセキュリティーおよび個人情報保護に対する新たな要求が提起されている。他方、中国の当面のデータセキュリティーおよび個人情報保護を対象とする立法には、空白が存在しており、法律体系は、なおも完全化さ

[1] http://www.cac.gov.cn/2016-11/07/c_1119866606.htm

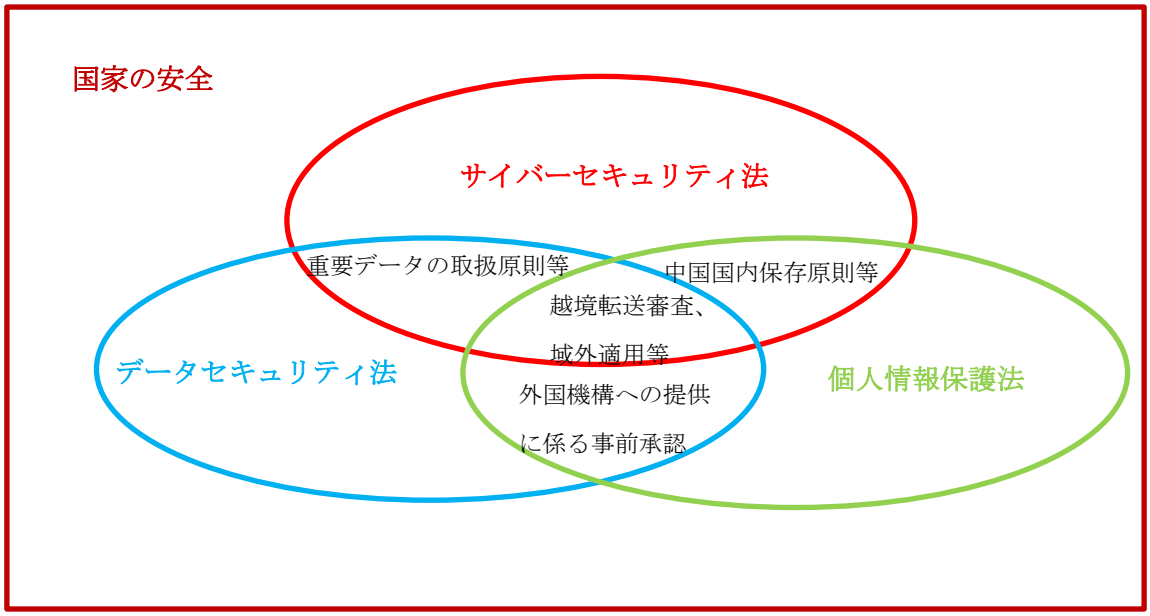
れておらず、データセキュリティーと個人情報保護には深刻な脅威が存在しており、関連法をもってサポートと保護を行う必要がある。

（二）三法の位置付けおよび関係

１．位置付け

「サイバーセキュリティー法」は中国で初めてサイバー空間セキュリティー管理の関連問題が全面的に規範化された基礎的な法律として、サイバー空間セキュリティーに対する全体的な管理の責務を担っている。「データセキュリティー法」はデータの分野における基礎的な法律として、データ処理活動のセキュリティー、開発および利用の責務を担っている。「個人情報保護法」は個人情報の権益を保障する基礎的な法律として、個人情報に対する保護の責務を担っている。「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」は、中国のネットワークおよびデータのセキュリティーを規制する「三本の柱」を構成している。

２．三法間の関係



三法の間には、上記のイメージ図のとおり、包摂する側とされる側の間における対立

関係は存在しておらず、「一般法」と「特別法」の関係性も、存在していない。実際には、ある程度重なっており、互いに補完し合う関係と言うことができる。その関係を証明できる証として、以下のような内容を列挙できる。

- ✓ データの分類・分級、および重要データの取扱いについては、「サイバーセキュリティー法」と「データセキュリティー法」の規定を併せて検討する必要がある。
- ✓ 個人情報の取扱い、および個人情報の中国国内における保存については、「サイバーセキュリティー法」と「個人情報保護法」の規定を併せて検討する必要がある。
- ✓ 個人情報を含むデータの外国機構への提供に係る事前承認については、「データセキュリティー法」と「個人情報保護法」の規定を併せて検討する必要がある。
- ✓ 個人情報および重要データの越境伝送についても、やはり三種の法律の規定を併せて検討する必要がある。

３．三法の適用範囲

適用の範囲について、域外適用に関する規定は、「サイバーセキュリティー法」においては、定められていないが、「データセキュリティー法」および「個人情報保護法」においては、定められている。具体的な内容は以下のとおりである。

法律名称	域内適用	域外適用
サイバーセキュリティー法	中国国内におけるネットワークの構築・運営・維持・使用およびサイバーセキュリティーの監督・管理[2]	規定なし
データセキュリティー法	中国国内で行われるデータの取扱活動およびその安全に対する監督・管理[3]	中国国外で行われるデータ取扱活動が、中国の国家の安全・公共の利益または公民・組織の合法的な権益を侵害したとき[4]。
個人情報保護法	中国国内における自然人の個人情報取扱活動[5]	中国国外における中国国内の自然人の個人情報取扱活動に、次の各号に掲げる状況の一があったとき[6]。 （1）中国国内の自然人への商品・役

[2] 「サイバーセキュリティー法」第2条参照。
[3] 「データセキュリティー法」第2条1項参照。
[4] 「データセキュリティー法」第2条2項参照。
[5] 「個人情報保護法」第3条1項参照。
[6] 「個人情報保護法」第3条2項参照。

		務の提供を目的としているとき。 （2）中国国内の自然人の行為を分析または評価しているとき。 （3）法律または行政法規の定めるその他の状況。

（三）三法にかかわる主管部門

「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」所定の主管部門については、次に掲げる表に示すとおりである。

機構の名称	サイバーセキュリティー法[7]	データセキュリティー法[8]	個人情報保護法[9]
中央国家の安全指導機構	-	・「データセキュリティー法」に基づき設置された専門的機構 ・国のデータセキュリティー業務に関する意思決定および統括	-
国家インターネット情報部門	サイバーセキュリティー業務および関連の監督管理業務の統一的な計画・調整	サイバーセキュリティーおよびデータセキュリティーの統括・協調・関連監督管理	個人情報保護業務および関連監督管理業務の統括・調整
関連業界主管部門 公安機関・国家の安全機関	各自の職責の範囲内でサイバーセキュリティー、データセキュリティーおよび個人情報の保護および監督管理		
地方政府および部門	職責は、国の関連規定に基づき確定する	自らの地区・部門の業務において収集および発生したデータおよびデータセキュリティーの管理	職責は、国の関連規定に基づき確定する

[7] 「サイバーセキュリティー法」第8条参照。
[8] 「データセキュリティー法」第5条、第6条参照。
[9] 「個人情報保護法」第60条参照。

（四）三法に伴う法的リスク

「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」所定の処罰行為、処罰対象、処罰方式については、次に掲げる表に示すとおりである。

法律の名称	対象	行為	是正を命じ、警告を与える	是正を拒絶し、情状が重大であり、サイバーセキュリティーに危害を及ぼす等の結果をもたらした場合における罰金	直接責任を負う主管者　およびその他の直接責任者に対する罰金	関連業務の一時停止、営業停止・整理、ウェブサイトの閉鎖、業務許可または営業許可証の取り消しを命ずる	特別なペナルティ
サイバーセキュリティー法	ネットワーク運営者	サイバーセキュリティー等級保護義務を履行しないとき。	○	1～10 万元	5,000～5 万元		-
		サイバーセキュリティー事件緊急対応プランを制定しないとき。	○	1～10 万元	5,000～5 万元		-
		実名制義務を履行しないとき。	○	5～50 万元	1～10 万元	○	-
		違法にサイバーセキュリティー認証、検査等の活動を実施したとき、またはシステムのバグ、インターネット攻撃等のサイバーセキュリティー情報を対外的に公布しないとき。	○	1～10 万元	5,000～5 万元	○	-
		個人情報を侵害したとき。	○	違法所得の 1～10 倍（違法所得がない場合には 100 万元以下）	1～10 万元	○	-
		ユーザー発布情報に対する管理を強化しなかったとき。	○	10～50 万元	1～10 万元	○	-
		法執行協力義務を履行せず、またはその履行を拒否したとき。	○	5～50 万元	1～10 万元		-
	重要情報	サイバーセキュリティー保護義	○	10～100 万元	1～10 万元		-

	インフラ運営者	務を履行しないとき。					
		データ現地化の要求に違反したとき。	○	5～50万元	1～10万元	○	-
		国の安全審査規定に違反したとき。	○	購入金額の1～10倍	1～10万元		-
	ネットワーク製品およびサービス提供者	製品およびサービスの安全に関する義務に違反したとき。	○	5～50万元	1～10万元		-
	あらゆる個人および組織	サイバーセキュリティーに危害を及ぼす活動に従事したとき。		個人：5～50万元 （情状が重大な場合には10～100万元） 単位：10～100万元	5～50万元 （情状が重大な場合には10～100万元）		-
データセキュリティー法	データ取扱者	データセキュリティー保護義務を履行しなかったとき。	○ （5～50万元の併科）	50～200万元	1～10万元 （情状が深刻な場合には5～20万元）	○	-
		国家核心データ管理制度に違反したとき。		200～1000万元		○	-
		データの越境移転規制に違反したとき。	○ （10～100万元の併科）	200～1000万元	1～10万元 （情状が深刻な場合には10～100万元）	○	-
		データ取引仲介サービスを行う機構が義務に違反したとき。	○	違法所得の1倍～0倍 違法所得がないときは10～100万元	1～10万元	○	-
		データの取り調べに対する協力の義務に違反したとき。	○ （5～50万元の併		1～10万元	○	-

			科）				
		中国国外の公的機関へのデータ提供規制に違反したとき。	○（10～100 万元の併科）	200～1000 万元	1～10 万元（情状が深刻な場合には 5～50 万元）	○	-
個人情報保護法	個人情報の取扱者	個人情報を違法に取り扱ったとき。 個人情報の取扱時における法定の個人情報の保護義務を履行しなかったとき。	○	100 万元以下（5000 万元以下または前年度の売上高の百分の五以下）	1～10 万元（情状が深刻な場合には 10～100 万元）	○	・アプリに対するサービス提供の一時停止または終了の命令 ・直接の責任者に対する一定期間中の関係企業における董事・監事・高級管理職員・個人情報保護責任者の担当の禁止 ・信用記録文書への組入れおよび公示

二、各法における重要な定義

（一）「サイバーセキュリティー法」

１．ネットワーク

「サイバーセキュリティー法」における「ネットワーク」とは、コンピュータその他の情報端末および関連設備により構成される情報システム[10]をいい、インターネット、移動通信ネットワーク、VPN 等が含まれる。

２．ネットワーク運営者

中国国内において「ネットワークを確立し、運営し、維持保護し、および使用する」企業は、ネットワーク運営者、重要情報インフラ運営者、ネットワーク製品およびサービス提供者等に分けられ、「サイバーセキュリティー法」による規制を受けることになる。「ネットワーク運営者」とは、ネットワークの所有者、管理者およびネットワークサービス提供者をいう[11]。ホームページ等を開設する一般企業も、ネットワーク運営者に該当する。

また、ネットワーク運営者に該当せず、ネットワーク製品およびサービス提供者にも該当しない個人および組織も、「サイバーセキュリティー法」の規定を遵守し、ネットワークを適法に利用する必要がある 。

３．重要情報インフラおよびその運営者

（1）重要情報インフラ

重要情報インフラとは、公共通信、情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務、国防科学技術工業などの重要な業界と分野に属しており、またはその他のひとたび機能の破壊もしくは喪失またはデータの漏えいに遭遇すると、国家の安全、経済、民生または公共の利益を著しく脅かす恐れのある重要ネットワーク施設や情報システム等をいうものと定義されている[12]。

重要情報インフラが所属する業界・分野の主管部門と監督管理部門は、重要情報インフラセキュリティ保護業務に責任を負う部門として、自らの業界・分野における実情を踏まえた上で、重要情報インフラ認定規則を制定し、同業界・分野における重要

[10] 「サイバーセキュリティー法」第 76 条参照。
[11] 「サイバーセキュリティー法」第 76 条参照。
[12]「サイバーセキュリティー法」第 31 条、「重要情報インフラセキュリティー保護条例」第 2 条参照。

情報インフラの認定を組織している[13]。

安全にかかわる判定基準	機能が破壊され、もしくは失われ、またはデータが漏えいした際における国の安全、国の経済、人民の生活または公共の利益を著しく損なう恐れの有無
業界にかかわる判定基準	公共通信和信息サービス、エネルギー、交通、水利、金融、公共サービス、電子政務、国防科学技術工業などにかかわる業界

(2) 重要情報インフラ運営者

ネットワーク運営者のうち、重要情報インフラを運営する者は「重要情報インフラの運営者」に該当する。

４．ネットワーク製品およびサービス提供者

ネットワーク製品およびサービス提供者には、ネットワークに関連する設備やソフト等を生産および販売する企業、ならびにクラウドコンピューティングサービス、データの処理および保存サービス、インターネット通信サービス等を提供する事業者が、これに該当する。

ネットワークサービスの提供者は、「サイバーセキュリティー法」に基づき、ネットワーク運営者としての義務も履行しなければならない。

(二)「データセキュリティー法」

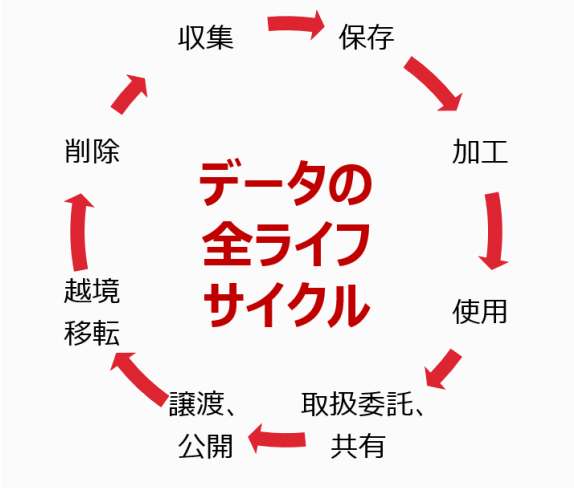
１．データ

「サイバーセキュリティー法」には、ネットワークデータの定義がある。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、処理および発生するさまざまな電子データをいう[14]。当該定義には、その他の形式のデータが含まれていないことから、大きな限定性が存在していた。一方、「データセキュリティー法」の公布後においては、データ管理の面における限定性が、より一層補われている。「データセキュリティー法」によると、データとは、電子その他の形式による情報に対する記録を

[13] 「重要情報インフラセキュリティー保護条例」第 8 条、第 9 条、第 10 条参照。
[14] 「サイバーセキュリティー法」第 76 条参照。

いう[15]。当該定義の内容によると、その他の形式の情報に対する記録（たとえば、紙の上に記録された情報など）も、データに属する。

注意を要するのは、中国の「データセキュリティー法」においてデータの取扱者に負担が要求されているデータセキュリティー保護義務というのは、ただデータの全ライフサイクル中のある一段階のみに対する保護ではなく、データの全ライフサイクル中の各段階におけるデータ取扱行為に対する保護であるという点である。



また、「データセキュリティー法」の下では、データの取扱時において、法令の遵守、社会の公徳・倫理の尊重、商業道徳および職業道徳への適合、信義則の堅持、データセキュリティー保障義務の履行、および社会的な責任の負担を行わなければならず、国家の安全、公共の利益または個人・組織の合法的な権益を侵害してはならないとされている[16]。さらに、同法においてはデータの取扱時における公徳と道徳の遵守義務に関する問題が、前後して二度提起されており、企業はこの点を重視しなければならない。法律は道徳の最低限度の尺度と価値基準であるが、「データセキュリティー法」においては、データの取扱活動は社会の倫理と公徳を尊重しなければならないという旨が特別に強調されており、企業に対して法律よりも高い要求が提示されている。

２．核心データ

核心データは、すなわち、国家核心データである。国家安全、国民経済の命脈、重要な国民生活、重大な公共利益等にかかわるデータが国家核心データに属し、これに対してさらに厳格な管理制度を実行する[17]。また、「工業情報化分野データセキュリティ

[15] 「データセキュリティー法」第 3 条参照。
[16] 「データセキュリティー法」第 8 条、第 28 条参照。
[17] 「データセキュリティーー法」第 21 条参照。

一管理弁法（試行・意見募集稿）」によると、危害の程度が次のいずれか該当するデータ[18]である。

- ✓ 政治、国土、軍事、経済、文化、社会、科学技術、ネットワーク、生態、資源および原子力安全等に対する重大な脅威を成し、中国国外の利益、生物、宇宙、極地、深海、人工知能等の重点分野における国家安全に関連するデータセキュリティーに著しく影響するもの。
- ✓ 工業、通信業界およびその重要基幹企業、重要情報インフラ、重要資源等に深刻な影響をもたらすもの。
- ✓ 工業の生産運営、通信とインターネットの運行とサービス等に重大な損害を与え、広範囲な操業停止・生産停止、大規模なネットワークとサービスの麻痺、大量な業務処理能力の喪失等を引き起こすもの。
- ✓ 工業情報化部が評価により確定するその他の核心データ。

３．重要データ

重要データの定義について、「サイバーセキュリティー法」と「データセキュリティー法」においては、明確な規定は行われていない。「自動車データセキュリティー管理若干規定（試行）」における重要データに対する定義を踏まえて見てみると、重要データとは、ひとたび改ざん、破壊もしくは漏えいまたは違法な取得もしくは利用に遭遇すると、国家の安全、公共の利益または個人・組織の合法的な権益を脅かす恐れのあるデータをいうものとされている[19]。このほかにも、「重要データ認識ガイドライン（意見募集稿）」における規定によると、重要データとは、ひとたび改ざん、破壊、漏えいまたは違法な取得に遭遇すると、国家の安全および公共の利益を脅かす恐れのあるデータをいうものとされており、これには国家機密と個人情報は含まれないが、大量の個人情報を基に形成された統計データと派生データは、重要データに属する可能性がある[20]。

４．核心データと重要データの比較

[18] 「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10条参照。
[19] 「自動車データセキュリティー管理若干規定（試行）」第3条参照。
[20] 「重要データ認識ガイドライン（意見募集稿）」第3.2条参照 。

項目	データセキュリティー法	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）	自動車データセキュリティー管理若干規定（試行）
適用範囲	全国	工業全体、通信業	自動車業
施行状態	2021/9/1施行	（パブコメ中、未施行）	2021/10/1施行
核心データ	国家安全、国民経済の命脈、重要な国民生活、重大な公共利益等にかかわるデータは、国家核心データに属し、これに対してさらに厳格な管理制度を実行する。	（上記）危害の程度が次のいずれか該当するデータ： ①政治、国土、軍事、経済、文化、社会、科学技術、ネットワーク、生態、資源および原子力安全等に対する重大な脅威を成し、中国国外の利益、生物、宇宙、極地、深海、人工知能等の重点分野における国家安全に関連するデータセキュリティーに著しく影響するもの。 ②工業、通信業界およびその重要基幹企業、重要情報インフラ、重要資源等に深刻な影響をもたらすもの。 ③工業の生産運営、通信とインターネットの運行とサービス等に重大な損害を与え、広範囲な操業停止・生産停止、大規模なネットワークとサービスの麻痺、大量な業務処理能力の喪失等を引き起こすもの。 ④工業情報化部が評価により確定するその他の核心データ。	規定なし

項目	データセキュリティー法	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）	自動車データセキュリティー管理若干規定（試行）
重要データ	国家データセキュリティー業務調整スキームは、関連部門と調整した上で重要データ目録を策定する。 各地区、各部門はデータ分類分級保護制度に基づき、本地区、本部門および関連業界・分野の重要データの具体的な目録を確定し、目録に載せられるデータに対して重点的に保護する。	（上記）危害の程度が次のいずれか該当するデータ： ①政治、国土、軍事、経済、文化、社会、科学技術、ネットワーク、生態、資源および原子力安全等に対する脅威を成し、中国国外の利益、生物、宇宙、極地、深海、人工知能等の重点分野における国家安全に関連するデータセキュリティーに影響するもの。 ②工業、通信業界の発展、生産、運行および経済利益等に影響をもたらすもの。 ③重大データセキュリティー事件または生産安全事故を引き起こし、公共利益または個人・組織の合法的権益に深刻な影響をもたらし、その社会的悪影響が大きいもの。 ④カスケード効果を著しく引き起こし、その影響の範囲が複数の業界、区域もしくは業界内の複数の企業におよび、または業界の発展、技術の進歩、業界の状況等に対して深刻な影響をもたらすもの。 ⑤データの復元または悪影響の解消のための代償が大きいもの。	重要データとは、ひとたび改ざん、破壊、漏えいまたは違法取得、違法利用されれば、国家安全、公共利益または個人・組織の合法権益を害しうるデータをいい、それには次が含まれる： ①軍事管理区、国防科学工業等の国家秘密にかかわる単位、県級以上の共産党・政府機関等の重要で機微な区域の地理情報、人・車両の流れのデータ。 ②交通量、物流等の経済運行状況を反映するデータ。 ③自動車充電ネットワークの運行データ。 ④人間の顔、ナンバープレート等の車外の映像・画像データ。 ⑤10万人以上の個人情報。 ⑥国家インターネット情報部門および発展改革、工業情報化、公安、交通運輸等の国務院関連部門の

項目	データセキュリティー法	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）	自動車データセキュリティー管理若干規定（試行）
		⑥業界の監督管理部門が評価により確定するその他の重要データ。	指定する国家安全、公共利益または個人・組織の合法権益を害しうるその他のデータ。
（一般）データ	（上記以外のデータ）	（データが改竄、破壊、漏えいまたは違法取得、違法利用されれば、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）危害の程度が次のいずれか該当するデータ： ①公共利益または個人・組織の合法的権益に対する影響が小さく、社会的悪影響が小さいもの。 ②影響されるユーザー数と企業数が比較的少なく、生産・生活区域の範囲が小さく、持続時間が短く、企業の経営、業界の発展、技術の進歩、業界の状況等への影響が小さいもの。 ③データの復元または悪影響の解消のための代償が小さいもの。その他重要データ、核心データ目録に載せられていないデータ。	規定なし

（三）「個人情報保護法」

１．個人情報

(1) 個人情報の定義

「個人情報保護法」における個人情報とは、電子またはほかの方法をもって記録された既に識別されており、または識別可能である自然人に係る各種の情報をいい、ただし、匿名化処理後の情報は、この限りでない。[21]

(2) 個人情報の定義の比較

	「個人情報保護法」	「民法典」	「サイバーセキュリティー法」
定義	個人情報とは、電子またはほかの方法をもって記録された既に識別されており、または識別可能である自然人に係る各種の情報をいう。	個人情報とは、電子またはその他の方法をもって記録され、単独で、またはその他の情報と組み合わせて特定の自然人を認識することのできる各種の情報をいう。	電子その他の方法をもって記録され、単独で、またはその他の情報と組み合わせて自然人（個人）の身分を認識することのできる各種の情報をいう。
コメント	これには認識可能な情報、および既に認識されている自然人にかかわる各種の情報が含まれている。範囲は最も広い。	認識可能な情報に限定されており、範囲は「個人情報保護法」に比べて狭い。	個人の身分を認識させる情報に限定されており、範囲は最も狭い。

「サイバーセキュリティー法」から「民法典」、さらには「個人情報保護法」にかけて、個人情報の範囲は段階的に拡大し、法律の保護の対象範囲内に組み込まれる個人情報は、次第に増加してきており、「個人情報保護法」における個人情報が、最も厳密に個人情報が定義されている。

[21] 「個人情報保護法」第8条参照。

（3）個人情報の認定方法

「個人情報保護法」第4条の「個人情報」に関する定義と、2020年に修正された推薦性国家標準である「情報安全技術　個人情報安全規範」（GB/T 35273-2017、以下「個人情報安全規範」）によると、企業は「認識＋関連性」の基準を使用し、これにより取り扱うデータの個人情報構成の成否を認定することができる。

① 認識の基準：**情報から個人が認識**される場合。すなわち、情報自体の特別性から、特定の自然人を認識することができるものである。たとえば、身分証明書番号などである。

② 関連性の基準：**個人から情報が生ずる**場合。すなわち、特定の自然人が既に知られており、当該特定の自然人が、自らの活動において生ずる情報である。たとえば、既に知られている特定の自然人の位置情報、通話記録などである[22]。

２．個人機微情報

個人機微情報とは、ひとたび漏えいし、または違法に使用されたときは、自然人の人格上の尊厳に対する侵害、または人身もしくは財産の安全性に対する脅威を容易に引き起こす個人情報（生体認証、宗教・信仰、特定の身分、医療・健康、金融口座、行動履歴などの情報、および十四歳未満の未成年者の個人情報を含む。）をいう[23]。また、「個人情報安全規範」においては、個人機微情報の範囲が定められており、個人の身分証番号、生物識別情報、銀行口座番号、通信記録および内容、財産情報、信用調査情報、行動追跡情報、宿泊情報、健康生理情報、取引情報等は、いずれも個人機微情報に該当する。係る個人機微情報については、保管の際に、暗号化措置を講じなければならない。

このほか、「データセキュリティー管理弁法（意見募集稿）」によると、ネットワーク運営者は経営を目的として、個人機微情報を直接収集し、または第三者から間接的に収集する際に、所在地のインターネット情報部門へ届出を行うべきとされている。届出の主な内容は、機微情報の収集・使用の規則、目的、規模、方法、範囲、類型、期間等であり、個人機微情報の具体的な内容は含まれていない[24]。

[22] 「個人情報安全規範」別紙A参照。
[23] 「個人情報保護法」第28条参照。
[24] 「データセキュリティー管理弁法（意見募集稿）」第15条参照。

個人情報例示表（そのうち下線部分は個人機微情報）

基本情報	氏名、誕生日、性別、民族、国籍、家族、住所、電話番号、メールアドレスなど
身分情報	身分証明書、軍官証、パスポート、運転免許証、出入境通行証、労働許可証、社会保険カード、居住証など
生物識別情報	DNA、指紋、声紋、掌紋、耳介、虹彩、顔識別特徴など
ネットワーク身分識別情報	システムアカウント、IP アドレス、個人デジタル証書など
健康生理情報	疾病により生ずる関連記録、例えば病症、入院記録、医者の指示書、検査報告書、手術および麻酔の記録、介護記録、投薬記録、薬物食物アレルギー情報、生育情報、過去の疾患、感染症の病歴など､ならびに個人の身体の健康状況にかかわる情報(例えば体重、身長、肺活量など)
教育就職情報	個人の職業、職位、就職先、学歴、教育実務経験、職務経歴、研修記録、成績表など
財産情報	銀行口座、識別情報（パスワード)、預金情報（資金量、収支記録などを含む。)、不動産情報、信用調査情報、信用調査情報、取引および消費の記録、金銭出納記録など、ならびに仮想通貨、仮想取引、ゲーム等の両替コードなどの仮想財産情報
通信情報	通信記録および内容、ショートメッセージ、MMS、SMS、電子メール，および個人の通信を表すデータ（一般にメタデータと呼ばれる。）など
連絡先情報	連絡先リスト、友達リスト、グループリスト、電子メールリストなど
ネットワーク利用情報	ログを通じて保存された個人情報主体の取扱記録（ウェブサイトの閲覧記録、ソフトウェア使用記録、クリック記録、お気に入り追加リストなどを含む。）
常用設備情報	ハードウェアのシリアルナンバー、デバイスの MAC アドレス、ソフトウェアリスト、 UUID （ソフトウェア 上で オブジェク

	ト を一意に識別するための 識別子）（例えば IMEI/Android ID/IDFA/OpenUDID/GUID/SIMカードIMSI情報）などを含む個人の常用設備の基本状況を表す情報
位置情報	行動履歴、高精度の位置情報、宿泊情報、緯度・経度など
その他	婚姻歴、宗教信仰、性的指向、未公開の犯罪記録など

３．単独の同意

個人の同意に基づいて個人情報を取り扱うときは、当該同意は、個人による事情の十分な知得を前提とし、自由意志の下、明確に行わなければならない。ただし、法律または行政法規が、個人情報の取扱いの単独または書面の同意の取得義務を定めているときは、その規定に従う[25]。

前述の単独の同意について、「個人情報保護法」には明確な規定が行われていない。しかし、単独の同意は「概括的同意」または「一括同意」の逆であり、すなわち、相応の個人情報取扱行為は、単独の同意の仕組みを伴っていなければならず、その他の個人情報取扱行為と混ぜて個人情報主体の同意を取得することができないという点である。単独の同意の仕組みは、個人情報主体の上述の特別取扱行為に対する十分な知る権利の保障に資し、同者に自由意志に基づく明確な同意を提供させる。しかし、当該法的義務は企業に対して比較的に高い要求を提起している。

「個人情報保護法」において要求されている単独の同意に関する事項は、次のとおりである。

状況	「個人情報保護法」の内容	根拠
自らが取り扱う個人情報をその他の個人情報取扱者に提供する場合	受領者の名称・氏名および連絡方法、取扱いの目的・方法、ならびに個人情報の種類を個人に告知し、個人の単独の同意を取得しなければならない。	第13条
自らが取り扱う個人情報を公開する場合	個人情報の取扱者は、自らの取り扱う個人情報を公開してはならない。ただし、個人の単独の同意を取得したときは、この限りでない。	第25条
公共の場所における画像	収集された個人の画像と身分認識情報	第26条

[25] 「個人情報保護法」第14条参照。

収集・個人身分認識用の設備をもって収集された個人情報を公共の安全性の保護以外の目的に使用する場合	は、ただ公共の安全性の保護の目的にのみ用いることができ、その他の目的に用いてはならない。ただし、個人の単独の同意を取得したときは、この限りでない。	
個人機微情報を取扱う場合	個人機微情報の取扱いは、個人の単独の同意を取得しなければならない。	第 29 条
個人情報を中国国外の受領者に越境伝送する場合	中国国外の受領者の名称・氏名、連絡方法、取扱いの目的・方法、個人情報の種類、個人から中国国外の受領者への本法の定める権利の行使の方法・手続きなどの事項を個人に告知し、個人の単独の同意を取得しなければならない。	第 39 条

三、課題の整理：各法における重要な制度

(一)「サイバーセキュリティー法」による規制に関する法的義務

企業は、法的リスクが生ずるのを避けるため、「サイバーセキュリティー法」による規制下における自身のポジショニングおよび関連する義務を明確にした上で、それに基づき、その直面するコンプライアンス上の主な課題について把握し、内部においてサイバーセキュリティーに関するコンプライアンス制度を制定する必要がある。「サイバーセキュリティー法」の関連規定に基づき、ネットワーク運営者、重要情報インフラ運営者、ネットワーク製品およびサービス提供者の主な義務は、次に掲げる表に示すとおりである。

類型	義務	根拠条文	ネットワーク運営者	重要情報インフラ運営者	ネットワーク製品およびサービス提供者
ネットワーク運営上の	サイバーセキュリティー等級保護を履行する義務	第21条	○	○	○
	サイバーセキュリティー事件緊急対応プランを制定する義務	第25条	○	○	○

	購入するネットワーク製品およびサービスが国の強制的標準に適合していることを確保する義務	第22条	○	○	○
	インターネット実名制を実施する義務	第24条	○	○	○
	ネットワーク製品およびサービス購入の際の秘密保持契約の締結義務	第36条		○	
	毎年少なくとも1回、ネットワークの安全リスクについて検査・評価を行う義務	第38条		○	
	安全管理責任者を設置する義務	第34条		○	
	従業員に対しネットワークの安全に関する教育、技術研修および技能審査を定期的に行う義務	第34条		○	
	重要システムおよびデータベースに対しディザスターリカバリー・バックアップを行う義務	第34条		○	
	ネットワーク製品およびサービスの安全性を保障する義務	第22条			○
ネットワーク上の情報の安全の保障	個人情報および重要データを中国国内に保管する義務	第37条（注1）	△（注2）	○	
	個人情報および重要データの越境に制限を設ける義務	第37条（注1）	○（注2）	○	
	個人情報保護制度の確立義務	第41条 第42条	○	○	○
	ネットワーク情報の安全に関する苦情申立て・通報制度の確立義務	第49条	○	○	○

（注1）「個人情報と重要データ越境セキュリティー評価弁法（意見募集稿）」

（注2）注1弁法（意見募集稿）には、ネットワーク運営者が当該義務を履行する必要があると規定されており、規定内容が未定である。

（二）「サイバーセキュリティー法」による規制に関する課題

１．サイバーセキュリティー等級保護制度

サイバーセキュリティー等級保護制度は、ネットワークが妨害、破壊または無許可アクセスを受けた、あるいはネットワークデータの漏えいまたは窃取、改ざんをされた場合における個人、社会、国に対する影響の程度に応じて、当該ネットワーク運営者が係る影響に対応することのできるサイバーセキュリティー保護能力を有することを求めている。ネットワーク運営者は、サイバーセキュリティー等級保護義務を履行しなければならず、具体的には、サイバーセキュリティー責任者の確定、コンピュータウイルス等のネットワークの安全に危害を及ぼす行為を防止するための技術的措置の実施、ネットワークの運行状態およびサイバーセキュリティー事件をモニター・記録する技術的措置の実施、関連するログファイルの6カ月以上にわたる保管、データ分類、重要データバックアップ、暗号化等の措置の実施が義務として挙げられている[26]。

「サイバーセキュリティー法」のサイバーセキュリティー等級保護にかかわる関連規定に基づき、公安部は2018年6月に「サイバーセキュリティー等級保護条例（意見募集稿）」[27]を公布し、さらに、関連部門も等級保護に関する多くの国家標準を公布している。具体的には、下表の示すとおりである。

公布日	文書の名称	公布機関	備考
部門の規則			
2018.6.27	サイバーセキュリティー等級保護条例	公安部	意見募集稿
国家標準			
2018.12.28	情報安全技術 サイバーセキュリティー等級保護測定評価過程ガイドライン（GB/T 28449-2018）	国家市場監督管理総局、中国国家標準化管理委員会	2019.7.1実施
2018.12.28	情報安全技術 サイバーセキュリティー等級保護安全管理核心技術要求（GB/T 36958-2018）	国家市場監督管理総局、中国国家標準化管理委員会	2019.7.1実施

[26] 「サイバーセキュリティー法」第21条参照。
[27] http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html

2019.5.10	情報安全技術 サイバーセキュリティー等級保護基本要求（GB/T 22239-2019）	国家市場監督管理総局、中国国家標準化管理委員会	2019.12.1実施
2019.5.10	情報安全技術 サイバーセキュリティー等級保護測定評価要求（GB/T 28448-2019）	国家市場監督管理総局、中国国家標準化管理委員会	2019.12.1実施
2019.5.10	情報安全技術 サイバーセキュリティー等級保護安全設計技術要求（GB/T 25070-2019）	国家市場監督管理総局、中国国家標準化管理委員会	2019.12.1実施
2019.8.30	情報安全技術 サイバーセキュリティー等級保護実施ガイドライン（GB/T 25058-2019）	国家市場監督管理総局、中国国家標準化管理委員会	2020.3.1実施
2020.4.28	情報安全技術 サイバーセキュリティー等級保護グレーディングガイドライン（GB/T 22240-2020）	国家市場監督管理総局、中国国家標準化管理委員会	2020.11.1実施

上述の規定に基づき、目下中国におけるサイバーセキュリティー等級保護は既に新たな段階（等級保護2.0段階）に入っており、適用対象は情報システムからクラウドプラットフォーム、モバイルネットワーク、モノのインターネット、ビッグデータ、産業用制御システムなどにまで拡張され、関連の保護措置はさらに完全化されている。これにより、ネットワーク運営者はサイバーセキュリティー等級保護の新たな要求に基づき、サイバーセキュリティー等級の確定を基礎とし、相応の義務を履行する必要がある。

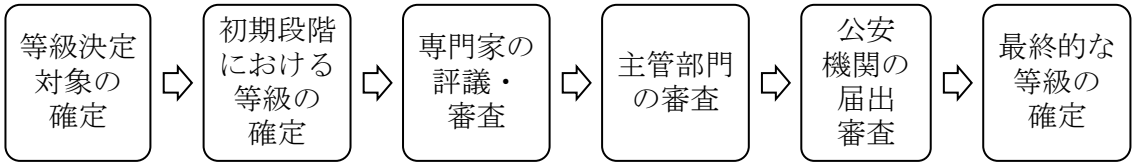
（1）サイバーセキュリティー等級の決定

「サイバーセキュリティー等級保護条例（意見募集稿）」においては、2007年の「情報安全等級保護管理弁法」の判断基準が保留されている。ネットワークの国家の安全、経済の建設および社会生活における重要性の程度、ならびにネットワークが破壊され、もしくは機能を喪失し、またはデータが改ざん・漏えい・遺失・破損された後の国家の安全、社会の秩序、公共の利益および関連の公民・法人その他組織の合法的な権益に対する危害の程度等の要素に基づき、サイバーセキュリティーの等級は以下の五つ

の等級に分けられている[28]。

侵害を受ける対象	対象に対する侵害の程度		
	一般的な侵害	著しい侵害	特に著しい侵害
公民、法人およびほかの組織の合法権益	一級	二級	二級
社会秩序および公共の利益	二級	三級	四級
国家の安全	三級	四級	五級

「サイバーセキュリティー等級保護条例（意見募集稿）」によると、上述のサイバーセキュリティー等級が二級以上のネットワーク運営者は、システムの等級決定が専門家の評議・審査、および主管部門の審査を経る必要があり、その後初めて公安機関へ届出を行うことができる。具体的な流れは下図の表すとおりである。これにより明らかなように、等級保護の全体の等級決定はさらに厳格であり、等級決定過程はさらに規範化されている。



（2）サイバーセキュリティー等級保護の義務（三級以上）

「サイバーセキュリティー等級保護条例（意見募集稿）」では「サイバーセキュリティー法」を基礎とし、異なる等級のネットワーク運営者を対象として、相応のセキュリティー保護義務が規定されている。このうち、三級以上のネットワーク運営者と「サイバーセキュリティー法」に規定されている重要情報インフラ運営者は互いに呼応しており、一般的なサイバーセキュリティー保護義務以外にも、さらに、以下の特別なセキュリティー保護義務[29]を履行する必要がある。

- ✓ 自らのセキュリティー保護等級に相応するネットワーク製品およびサービスの使用義務
- ✓ 特定の者に対する安全性の経歴の審査義務
- ✓ サイバーセキュリティー観測・早期警報・情報通報制度の確立義務、および公安

[28] 「情報安全技術 サイバーセキュリティー等級保護グレーディングガイドライン」 第6.4条参照。
[29] 「サイバーセキュリティー等級保護条例」（意見募集稿）第23条、第28条、第29条、第30条、第32条参照。

機関と電信主管部門への関連情報の申告義務
- ✓ 毎年一度のサイバーセキュリティー等級測定評価[30]の実施義務
- ✓ 中国国内における技術メンテナンスの実施義務。業務の必要性により、確かに中国国外における遠距離技術メンテナンスの実施が必要な場合は、サイバーセキュリティー評価義務の履行義務
- ✓ サイバーセキュリティー緊急対応策の制定義務、および定期的なサイバーセキュリティー緊急対応演習の実施義務

２．サイバーセキュリティー事件緊急対応策

ネットワーク運営者は、サイバーセキュリティーに危害が及ぶ事件が発生した場合においてシステムのバグ、コンピュータウイルス、インターネット攻撃、インターネット侵入等について遅滞なく処理するため、サイバーセキュリティー緊急対応策を制定しなければならない[31]。「国家サイバーセキュリティー事件緊急対応策」[32]では、サイバーセキュリティー事件が4等級に分けて定められており、当該対応策を基礎として、業種ごとに相応する緊急対応策に関する規定が定められている。例えば、工業・情報化部がインターネット業界を対象として打ち出した「公共インターネットネットワーク安全突発事件緊急対応策」[33]、銀行業監督管理委員会が銀行業界を対象として打ち出した「銀行業重要情報システム突発事件緊急対応管理規範」[34]等がある。

このほか、2019年4月10日には、公安部等の部門が「インターネット個人情報セキュリティー保護ガイドライン」を公布し、個人情報セキュリティー事件に対して規定を行っている。当該ガイドラインは指導文書であり強制的な法的規定ではないが、公安執法機関の個人情報保護法に対する解読を表しており、 法務執行の実践上において使用される可能性が高く、 このため、個人情報を収集するネットワーク運営者はこれを重視すべきとなる。

「インターネット個人情報セキュリティー保護ガイドライン」によると、個人情報を収集するネットワーク運営者は個人情報セキュリティー事件の応急処置の流れ、事件の上位者への報告の流れなどに対し、緊急対応策を制定し、定期的に緊急対応策に対して評価と改正を行い、定期的に（少なくとも半年に一度）組織内部の関係者は緊急対応研修と緊急対応演習を行うべきとされている。個人情報セキュリティー事件が生じた際には、事件の内容を記録し、必要な措置を評価して採択し、事件の影響を解

[30] 測定評価に関する具体的な要求については、「情報セキュリティー技術　サイバーセキュリティー等級保護測定評価過程ガイドライン（GB/T 28449-2018）」および「情報セキュリティー技術　サイバーセキュリティー等級保護測定評価要求（GBT28448-2019）」参照。
[31] 「サイバーセキュリティー法」第25条参照。
[32] 「中網弁発文［2017］4号」参照。
[33] 「工信部網安［2017］281号」参照。
[34] 「銀監弁発［2008］53号」参照。

消し、個人情報の主体へ告知し、「国家サイバーセキュリティー事件の緊急対応策」等の関連規定に基づいてセキュリティー事件を主管部門へ報告すべきとされている。報告の内容には、次のものが含まれるが、これに限らない：個人情報の総体的な状況（類型、数量、内容、性質等）、事件が引き起こす恐れのある影響、既に採択しているまたは将来的に採択する処理の措置、事件を処理する関係者の連絡先。

３．重要情報インフラのセキュリティー保護制度

「サイバーセキュリティー法」「重要情報インフラセキュリティー保護条例」および「ネットワーク製品およびサービスセキュリティー審査弁法（試行）」によると、重要情報インフラのセキュリティー管理はさらに厳格である。重要情報インフラ運営者の責任と義務は、次のとおりとされている[35]。

- ✓ サイバーセキュリティー保護制度および責任制度の確立および整備
- ✓ 専門セキュリティー管理機構の運営経費の保障、相応の人員の配置
- ✓ 重要情報インフラに対する毎年少なくとも一度のサイバーセキュリティー検査およびリスク評価の自社による実施
- ✓ 重大サイバーセキュリティーインシデントの発生時、または重大サイバー脅威の発見時における関連規定に従った主管部門および公安機関への報告
- ✓ 安全かつ信用可能なネットワーク製品およびサービスの優先的な調達、ネットワーク製品・サービスの調達が国家の安全に影響する恐れのある状況下における国家のサイバーセキュリティー規定に従ったセキュリティー審査の通過など
- ✓ 合併・分割・解散等の発生時における主管部門へ速やかな報告など

４．サイバーセキュリティー審査制度

「サイバーセキュリティー法」および2020年4月13日に公布された「サイバーセキュリティー審査弁法」[36]においては、重要情報インフラ運営者のネットワーク製品およびサービスの購入が明確化されており、国家の安全に影響し、または影響する恐れのあるときは、サイバーセキュリティー審査[37]を行うべきとされている。重要情報インフラ運営者はセキュリティ審査の実施が必要なネットワーク製品およびサービスを購入する際には、契約などの要求を通じてネットワーク製品およびサービス提供者のセキュリティー審査に協力すべきとされており、これには商品・役務提供の便宜上の条件を利用したユーザーデータの違法な取得、ユーザー設備の違法な制御・操縦、正当

[35] 「重要情報インフラセキュリティー保護条例」第13条、第14条、第16条、第17条、第19条、第20条および第21条参照。
[36] http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm
[37] 「サイバーセキュリティー審査弁法」第5条参照。

な理由のない製品または必要な技術支援サービスの供給の中断などを行わないという旨の確約が含まれている[38]。

また、2021年7月10日に公布された「サイバーセキュリティー審査弁法（第二回修正・意見募集稿）」によれば、重要情報インフラの運営者がネットワーク関連の製品・サービスを調達し、データの取扱者がデータを取り扱う場合において、国家の安全に影響を及ぼす可能性があるときは、「サイバーセキュリティー法」に従ってサイバーセキュリティー審査を行わなければならない[39]。また、100万人以上のユーザーの個人情報を保有する運営者は、中国国外に上場する場合、その旨をサイバーセキュリティー審査弁公室に報告し、サイバーセキュリティー審査を受けなければならない[40]とされている。

５．ネットワーク製品およびサービスに関する制度

ネットワーク製品およびサービス提供者が提供する製品およびサービスについては、国の標準の強制的な要求事項に適合し、悪意のプログラムを設置してはならないことが要求されている[41]。

ネットワーク製品およびサービス提供者が提供するネットワーク重要設備とサイバーセキュリティー専用製品については、関連の国家標準の強制的な要求に従い、資格をもつ機構が行う安全審査を通過し、または安全検査が要求に適合すべきとされており、その後初めて販売または提供[42]を行うことができる。ネットワーク重要設備とサイバーセキュリティー専用製品の具体的な審査要求と原則については、中国国家認証認可監督管理委員会が公布している「ネットワーク重要設備とサイバーセキュリティー専用製品の安全認証実施規則」を参照することができる。

このほかにも、前述の「サイバーセキュリティー審査弁法（第二回修正・意見募集稿）」の規定によると、ネットワーク製品およびサービス提供者は、重要情報インフラ運営者へ製品またはサービスを提供する際に、さらに、サイバーセキュリティー審査に協力すべきとされている。サイバーセキュリティー審査は、主にネットワーク製品およびサービスの以下の影響を対象としている[43]。

- ✓ 商品・役務の使用後にもたらされる重要情報インフラが違法な制御、妨害または破壊に遭遇するリスク
- ✓ 商品・役務供給中断の重要情報インフラ業務の連続性に対する脅威

38 「サイバーセキュリティー審査弁法」第6条参照。
39 「サイバーセキュリティー審査弁法（第二回修正・意見募集稿）」第2条参照。
40 「サイバーセキュリティー審査弁法（第二回修正・意見募集稿）」第6条参照。
41 「サイバーセキュリティー法」第22条、「情報セキュリティー技術 ネットワーク製品およびサービスセキュリティー一般要求（意見募集稿）」参照。
42 「サイバーセキュリティー法」第23条参照。
43 「サイバーセキュリティー審査弁法」第9条参照。

- ✓ 商品・役務の安全性、開放性、透明性、提供元の多様性、供給ルートの信頼可能性、および政治、外交、貿易などの要素により引き起こされる供給中断のリスク
- ✓ 商品・役務の提供者による中国の法律・行政法規および部門規則の遵守状況

（三）「データセキュリティー法」による規制に関する法的義務

「データセキュリティー法」の関連規定に基づき、データ取扱者、重要データ取扱者、重要情報インフラ運営者、およびデータ取引仲介サービスに従事する機構の主な義務は、次に掲げる表に示すとおりである。

義務	具体的な内容	法的根拠	一般的データ取扱者	重要データ的取扱者	重要情報インフラ運営者	データ取引仲介サービス従事機構
データセキュリティ保護義務	全工程データセキュリティー管理制度の確立および整備	第27条	○	○	○	○
	データセキュリティー教育研修の組織および展開	第27条	○	○	○	○
	相応の技術措置およびほかの必要な措置の採択	第27条	○	○	○	○
	インターネットなどの情報ネットワークを利用したデータ取扱活動の展開時におけるサイバーセキュリティー等級保護制度の定める相応の義務の履行	第27条	○	○	○	○
	データセキュリティー責任者和管理機構の明確化、データセキュリティー保護責任の実施	第27条		○		
	データ新技術の開発、社会の発展への寄与、福祉の増進、社会の公徳・倫理への適合	第28条	○	○	○	○
	リスク予測の強化、データセキュリティーの欠陥、セキュリティーホー	第29条	○	○	○	○

	ルなどのリスクの発見時における救済措置の迅速な採択					
	データセキュリティーインシデント発生時における対応措置の迅速な採択、規定に従ったユーザーへの迅速な告知、関連主管部門への報告	第29条	○	○	○	○
	リスク評価の定期的な展開、リスク評価報告書の主管部門への届出	第30条		○		
	業務上の必要性により中国国内において収集および発生した重要データの中国国外への提供が確かに必要な状況下における国家ネットワーク情報部門が国務院の関連部門と共同で制定する法令に従ったセキュリティー評価の実施	第31条（および「サイバーセキュリティー法」第37条）			○	
	中国国内において収集および発生した重要データの越境セキュリティー管理弁法の国家ネットワーク情報部門による国務院の関連部門との共同の制定	第31条		○		
	合法的かつ正当な方法を採用した	第32条	○	○	○	○

	データの収集。窃取またはその他の違法な方法を通じたデータ取得の禁止					
	データの提供元の説明、取引中の双方の当事者の身分の審査、ならびに審査データおよび取引記録データの保存の提供者への要求	第33条				○
	データの提供および関連サービスの取扱時における行政許可の取得義務が、法律および行政法規に規定されている状況下における許可の法による取得	第34条	○	○	○	○
	法による国家の安全の保護または犯罪の捜査に起因したデータの調査・証拠収集を必要とする公安・国家安全部門への協力	第35条	○	○	○	○
	主管部門の承認を経ていない中国国内の組織・個人による中国国内に保存されたデータの中国国外の司法または法執行機構への提供の禁止	第36条	○	○	○	○

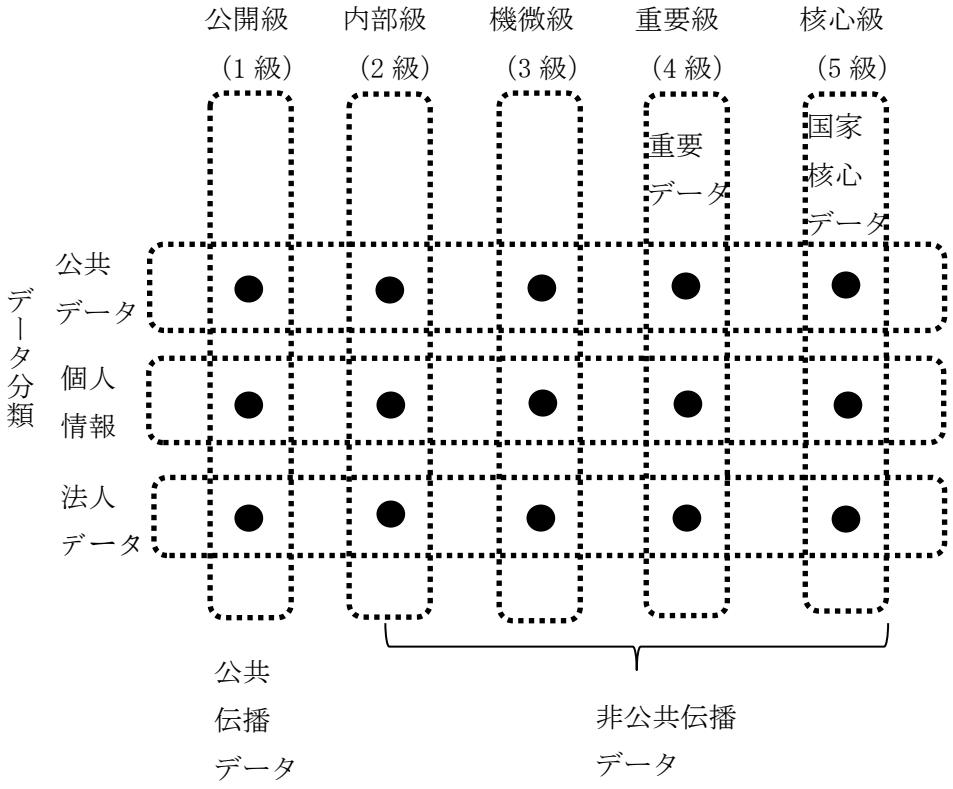
（四）「データセキュリティー法」による規制に関する課題

１．データ分類・分級保護制度

「サイバーセキュリティー法」は、初めて法律の面から「データ分類」上の要求が提起されている[44]。データ分類・分級制度とは、データの経済社会の発展における重要度、およびひとたび改ざん、破壊、漏えいまたは違法な取得もしくは利用に遭遇した際における脅威の程度に基づくデータに対する分類・分級保護の実施をいう。「データセキュリティー法」においては、データの二種類の類型、すなわち、国家核心データと重要データが提起されており、かつ、国家の観点からの重要データ目録、および各地区・各部門が制定する重要データの具体的な目録の分業監督管理の枠組みの制定が、明確にされている[45]。

「サイバーセキュリティー標準実践ガイドライン　データ分類・分級ガイダンス（意見募集稿）」においては、データの分類・分級の枠組みが提起されている。データの分類については、データの主体の観点から、データが公共データ、個人情報、および法人データという三つの類別に分けられている。データの分級については、データがひとたび改ざん、破壊、漏えいまたは違法な取得もしくは利用に遭遇した際における国家の安全、公共の利益または個人・組織の合法的な権益に対して引き起こす脅威の程度に基づき、データが下から上に公開級（1 級）、内部級（2 級）、機微級（3 級）、重要級（4 級）および核心級（5 級）という五つの等級に分けられている。そのうち、重要データは重要級（4 級）に属し、国家核心データは核心級（5 級）に属する[46]。

[44] 「サイバーセキュリティー法」第21条参照。
[45] 「データセキュリティー法」第21条参照。
[46] 「サイバーセキュリティー標準実践ガイドライン　データ分類分級ガイダンス（意見募集稿）」第4条参照。



「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）」においては、工業情報化の分野におけるデータの分類管理方法が規定されており、データが改ざん、破壊、漏えいまたは違法な取得もしくは利用に遭遇した際における国家の安全、公共の利益、個人・組織の合法的な権益などに対して引き起こす脅威の程度に基づき、工業・電気通信データが一般データ、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[47]。具体的内容は本マニュアルの二（二）4 を参照のこと。

２．データセキュリティー審査制度

データセキュリティー審査制度とは、国家の安全に影響し、または影響する恐れのあるデータの取扱活動に対する国家安全審査の実施をいう[48]。国家インターネット情報弁公室が公布した「サイバーセキュリティー審査弁法（第二回修正・意見募集稿）」においては、データセキュリティー審査制度がサイバーセキュリティー審査制度に組み入れられる傾向がある。以下の内容はデータセキュリティー審査の主な考慮要素の中

[47] 「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 7 条参照。
[48] 「データセキュリティー法」第 24 条参照。

に組み入れられている[49]。

- ✓ 核心データ、重要データまたは大量の個人情報が、窃取され、漏えいし、破損し、または違法に利用され、もしくは越境されるリスク
- ✓ 中国国外における上場後の重要情報インフラ、核心データ、重要データまたは大量の個人情報が、中国国外の政府によって影響を及ぼされ、制御され、または悪意をもって利用されるリスク

３．重要データ取扱活動のリスク評価および報告制度

重要データ取扱活動のリスク評価および報告制度とは、重要データの取扱者が規定に従って自らのデータ取扱活動に対し、リスク評価を定期的に展開し、かつ、リスク評価報告書を関連主管部門に届け出なければならないことをいう[50]。リスク評価報告書には、取り扱う重要データの種類・数量、データ取扱活動展開の状況、直面するデータセキュリティーリスク、これへの対応措置などが含まれていなければならない。

このほかにも、「自動車データセキュリティー管理若干規定（試行）」においては、自動車業界における重要データ取扱活動のリスク評価と報告制度が規定されており、すなわち、自動車データ取扱者は、重要データ取扱活動の展開時において、規定に従ってリスク評価を展開し、省・自治区・直轄市のネットワーク情報部門および関連部門にリスク評価報告書を届け出なければならないものとされている。リスク評価報告書には、取り扱う重要データの種類、数量、範囲、保存の地点・期間、使用方法、データ取扱活動展開の状況、第三者への提供の有無、直面するデータセキュリティーリスク、これへの対応措置などが含まれていなければならない[51]。自動車データ取扱者は、重要データ取扱活動の展開時において、毎年12月15日よりも前に、省・自治区・直轄市のネットワーク情報部門および関連部門に以下の年度内における自動車データセキュリティーの管理状況を届け出なければならない[52]。

- ✓ 自動車データセキュリティー管理責任者、およびユーザー権益事務連絡担当者の氏名、連絡方法
- ✓ 取り扱う自動車データの種類、規模、目的、必要性
- ✓ 自動車データのセキュリティー防護、管理措置（保存の地点、期間などを含む）
- ✓ 中国国内の第三者への自動車データ提供の状況
- ✓ 自動車データセキュリティーインシデント、それへの対応状況
- ✓ 自動車データにかかわるユーザーからのクレーム、その取扱状況
- ✓ 国家ネットワーク情報部門が国務院の工業情報化部、公安部門、交通運輸部門な

[49] 「サイバーセキュリティー審査弁法（第二回修正・意見募集稿）」第10条参照。
[50] 「データセキュリティー法」第30条参照。
[51] 「自動車データセキュリティー管理若干規定（試行）」第10条参照。
[52] 「自動車データセキュリティー管理若干規定（試行）」第13条参照。

どの関連部門と共同で明確にしたその他の自動車データセキュリティー管理の状況

４．業界重要データ・コアデータの全ライフサイクルにおける届出管理制度

(1) 重要データ・核心データ届出管理制度

「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)」においては、工業情報化の分野における重要データと核心データの届出管理制度に対する規定が行われており、すなわち、工業・電気通信データの取扱者は、関連の要求に従って届出を行わなければならず、届出の内容には、データの数量、類別、取扱いの目的・方法、使用範囲、主体責任、セキュリティー保護措置などの基本的な状況、およびデータの公開・越境・受領、データセキュリティーリスク、セキュリティーインシデントへの対応などの状況が含まれている。届出内容に変化が発生したときは、3 カ月以内に変更状況を報告し、全体の届出状況に対する更新を行わなければならない[53]。

(2) データの全ライフサイクルにおけるセキュリティー管理制度

このほかにも、「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)」においては、データの全ライフサイクルにおけるセキュリティー管理の実施が工業・電気通信データの取扱者に要求されている。データの全ライフサイクルにおけるセキュリティー管理制度とは、異なる等級のデータを対象として制定されたデータの収集、保存、使用、加工、伝送、提供、公開などの段階における具体的な分級防護上の要求および実務規程をいう[54]。工業情報化の分野における重要データ・コアデータの全ライフサイクルにおける管理は、以下の面にかかわっている。

項目	具体的な内容
業務体系	重要データ・核心データにかかわるときは、特別なデータセキュリティー管理責任部門を設置しなければならない[55]。
データの保存	法的規定またはユーザーとの間で取り決めた方法・期間に基づきデータを保存しなければならない[56]。 ✓ 重要データを保存するときは、さらに、検証技術、暗号技術などの措置を採択して安全な保存を行い、保存システムの公共情報ネットワークア

[53] 「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 12 条参照。
[54] 「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 条参照。
[55] 「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 条参照。
[56] 「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 18 条参照。

	クセスを直接提供してはならず、データのディザスタリカバリ・バックアップ、および保存媒体のセキュリティー管理を実施しなければならない。 ✓ 核心データを保存するときは、さらに、リモートディザスタリカバリ・バックアップを実施しなければならない。
データの使用・加工	個人・組織等の同意を経ずに、データの収集や関連の分析などの技術手段を使用して特定の主体を対象とする正確な画像やデータの復元等の加工処理活動を行ってはならない。重要データ・核心データを使用または加工するときは、さらに、アクセス制御を強化し、登記・認可審査メカニズムを確立し、記録を保存しなければならない[57]。
データの伝送	伝送するデータの類型・等級・応用の状況に基づき、セキュリティー原則を制定し、保護措置を採択しなければならない[58]。 ✓ 重要データを伝送するときは、さらに、検証技術、暗号技術、安全な伝送ルートまたは安全な伝送に関する協議書などの措置を採択しなければならない。 ✓ 異なるデータを取り扱う主体の間で核心データ伝送するときは、さらに、国家データセキュリティー業務調整メカニズム認可審査を通過しなければならない。
データの提供	データを提供する範囲、数量、条件、手続きを明確にしなければならない[59]。 ✓ 重要データを提供するときは、さらに、データ非特定化などの措置を採択し、認可審査メカニズムを確立しなければならない。 ✓ 核心データを提供するときは、さらに、国家データセキュリティー業務調整メカニズム認可審査を通過しなければならない。
データの破棄	データの破棄にかかわるポリシーと管理制度を確立し、破棄の対象、工程、技術などの要求を明確にし、破棄の活動に対して記録および保存を行わなければならない。重要データ・核心データを破棄するときは、いずれの理由およびいずれの方法をもってしても、破棄データに対する回復を行ってはならない[60]。
データの越境	✓ 中国国内において収集および発生した重要データは、中国国内に保存しなければならず、中国国外への提供が確かに必要な際には、法令に基づき、データの越境セキュリティー評価を行い、データに対する越境後の追跡と把握を強化しなければならない。

[57] 「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 19 条参照。
[58] 「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 20 条参照。
[59] 「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 21 条参照。
[60] 「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 23 条参照。

	✓ 核心データは、越境してはならない[61]。
データの受領	合併、再編、破産などの原因により、データを移転する必要があるときは、データ受領案を明確にし、影響を受けるユーザーに通知しなければならない[62]。 ✓ 重要データ・核心データにかかわるときは、所在地の工業情報化主管部門または通信管理局に速やかに届け出なければならない。 ✓ 重要データ・核心データに、データの受領者が存在しておらず、かつ、破棄の条件に適合しているときは、工業・電気通信データの取扱者は、法によりデータの破棄を行わなければならない。 ✓ 重要データ・核心データに、データの受領者が存在しておらず、かつ、破棄の条件に適合していなかったときは、速やかに上級機関に報告し、業界監督管理部門の指定した機構にデータを移転させ、同部門に保存を行わせなければならない。
取扱いの委託	データ取扱活動の展開を他者に委託するときは、受託者のデータセキュリティー保護能力および資格に対して確認を行い、契約の拘束、現場審査などの方法を通じ、受託者に対する監督管理を行わなければならない。 ✓ 重要データ・核心データの取扱いを委託するときは、さらに、受託者に対してセキュリティー評価を行わなければならない[63]。
セキュリティー監査	データの取扱い、権限の管理、人員の実務などのログを記録しなければならない。ログの保存期間は、6 カ月を下回らず、セキュリティー監査を定期的に行って監査報告書を形成し、重要データ・核心データにかかわるときは、少なくとも半年に一回、これを行わなければならない[64]。

（五）「個人情報保護法」による規制に関する法的義務

「個人情報保護法」の関連規定によると、個人情報の取扱者、個人情報の取扱数が国家インターネット情報部門の定める数量に達した個人情報の取扱者、中国国外の個人情報の取扱者、重要なインターネットプラットフォームサービスを提供しており、利用者数が膨大で、かつ、業務の類型が複雑な個人情報の取扱者、および委託を受けて個人情報を取り扱う受託者の主な義務は、下表の示すとおりである。

61 「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 24 条参照。
62 「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 25 条参照。
63 「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 26 条参照。
64 「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 27 条参照。

類型	義務	根拠となる条文
一般的な個人情報の取扱者	内部管理制度および実務規程の制定	第 51 条
	個人情報に対する分類管理の実施	
	相応の暗号化、非識別化などのセキュリティー技術措置の採択	
	個人情報取扱いの実務権限の合理的な確定、定期的な従業員に対するセキュリティー教育および研修の実施	
	個人情報セキュリティーインシデント緊急対応マニュアルの制定、具体的な実施	
	個人情報保護責任者の連絡方法などの公開、個人情報保護責任者の氏名、連絡方法などの個人情報保護職責履行部門への届出	第 52 条
	自らの個人情報取扱活動による法律および行政法規の遵守の状況に対するコンプライアンス監査の定期的な実施。	第 54 条
	次の各号に掲げる状況の一に該当する状況下における個人情報保護影響評価の事前実施、自らの取扱状況に対する記録の実施 ✓ 個人機微情報の取扱い ✓ 個人情報にかかわる自動化された取扱いを通じた意思決定の実施 ✓ 個人情報取扱いの委託、その他の個人情報取扱者への個人情報の提供、個人情報の公開 ✓ 中国国外への個人情報の提供 ✓ 個人の権益に重大な影響を及ぼすその他の個人情報取扱活動	第 55 条
	個人情報の漏えい・改ざん・紛失が既に発生しており、または今後発生する恐れのある状況下における救済措置の迅速な採択、ならびに個人情報保護職責履行機関および個人への通知	第 57 条
個人情報の取扱数が国家インターネット	個人情報保護責任者の指定、同者による個人情報取扱活動や採択した保護措置などに対する監督実施の担当	第 52 条

情報部門の定める数量に達した個人情報の取扱者		
中国国外の個人情報取扱者	中国国内における専門機構または指定代表者者の設置、同機構または同者による個人情報保護関連事務処理の担当、関連機構の名称、代表者の氏名、連絡方法などの個人情報保護職責履行部門への届出	第53条
重要なインターネットプラットフォームサービスを提供しており、利用者数が膨大で、かつ、業務の類型が複雑な個人情報の取扱者	国の規定に従った個人情報保護コンプライアンス制度体系の確立・整備、主として外部の構成員から構成される独立的な機構の設立を通じた個人情報保護状況に対する監督の実施	第58条
	公開性・公平性・公正性の原則の遵守、プラットフォーム規則の制定、プラットフォーム内の商品・役務提供者の個人情報取扱上の規範および個人情報保護義務の明確化	
	法律または行政法規に著しく違反して個人情報を取り扱ったプラットフォーム内の商品・役務提供者に対する役務提供の停止	
	個人情報の保護に対する社会的な責任に関する報告書の定期的な公開、社会の監督の受入れ	
委託を受けて個人情報を取り扱う受託者	必要な措置を採択した自らが取り扱う個人情報のセキュリティーの保障、個人情報保護法の定める義務の履行に向けた個人情報取扱者への協力	第59条

（六）「個人情報保護法」による規制に関する課題

１．中国国外の個人情報取扱者の中国における機構の設立および届出に関する制度

中国国外の個人情報取扱者が、中国国外における中国国内の自然人の個人情報取扱活動に、次の各号に掲げる状況の一があったとき、中華人民共和国の国内において専門機構または指定代表者を設置し、個人情報保護関連事務の取扱いに責任を負い、関連機構の名称または代表の氏名、連絡方法などを個人情報保護の職責を履行する部門

に届け出なければならない[65]。

- ✓ 中国国内の自然人への商品・役務の提供を目的としているとき。
- ✓ 中国国内の自然人の行為を分析または評価しているとき。
- ✓ 法律または行政法規の定めるその他の状況。

２．児童個人情報保護制度

(1) 「児童個人情報ネットワーク保護規定」

2019 年 8 月 22 日に、国家ネットワークおよび情報化弁公室は「児童個人情報ネットワーク保護規定」を公布する。当該規定によると、ネットワーク運営者は以下の点に注意すべきとされている。

① 企業の内部について、専門的な児童個人情報保護規則とユーザー契約を制定し、児童個人情報の保護業務を担当する専任者を指定すべきとなる。さらに、児童個人情報へのアクセス権を厳格に制御すべきとなり、社内の職員が児童個人情報へのアクセスを必要とする場合は、児童の個人情報の保護責任者またはその授権する管理者の承認を経て、アクセス状況を記録し、技術的な措置を採り、違法な複製や児童個人情報のダウンロードを回避する必要がある[66]。

② ネットワーク運営者の児童個人情報の収集・使用・譲渡・開示は、業務上の必要性により、確かに取り決めた目的・範囲を超過して個人情報を使用する必要のあるときは、児童の保護者の同意を取得すべきとなる。このほか、同意の取得時において告知した事項（児童個人情報収集の目的、方法、範囲等）に実質的な変化が生じたときも、児童の保護者の同意[67]を再度取得する必要がある。

③ 児童個人情報の保管と使用上において、ネットワーク運営者は暗号化等の措置を講じて児童個人情報を保管する。児童個人情報を第三者へ譲渡するときは、自らまたは第三者機構へ委託して安全評価を行う[68]。

(2) 「個人情報保護法」および「未成年者保護法」

「個人情報保護法」は十四歳未満の未成年者の個人情報の保護に対して規制を設けている。十四歳未満の未成年者の個人情報は、個人機微情報に属する[69]。個人情報の取扱者は十四歳未満の未成年者の個人情報を取り扱うときは、未成年者の父母またはそ

[65] 「個人情報保護法」第 53 条を参照のこと。
[66] 「児童個人情報ネットワーク保護規定」第 8 条、第 15 条参照。
[67] 「児童個人情報ネットワーク保護規定」第 9 条、第 10 条、第 14 条参照。
[68] 「児童個人情報ネットワーク保護規定」第 13 条、第 16 条参照。
[69] 「個人情報保護法」第 28 条参照。

の他の保護者の同意を取得しなければならず、かつ、特別な個人情報取扱規則を制定しなければならない[70]。

「未成年者保護法」に未成年者にかかわる事項の取扱いが規定されているときは、未成年者のプライバシー権と個人情報を保護しなければならない[71]。情報の取扱者は、ネットワークを通じて未成年者の個人情報を取り扱うときは、合法性・正当性・必要性の原則を遵守しなければならない。十四歳未満の未成年者の個人情報を取り扱うときは、未成年者の父母またはその他の保護者の同意を取得しなければならないが、ただし、法律または行政法規に別段の定めがあるときは、例外となる。未成年者、父母またはその他の保護者が未成年者の個人情報の修正または削除を情報の取扱者に要求したときは、情報の取扱者はただちに措置を採択して修正または削除を行わなければならないが、法律または行政法規に別段の定めがあるときは、例外となる[72]。

３．重要なインターネットプラットフォームサービス提供者への特別管理制度

重要なインターネットプラットフォームサービスを提供しており、利用者数が膨大で、かつ、業務の類型が複雑な個人情報の取扱者が、次の各号に掲げる義務を履行しなければならない[73]。

- ✓ 国の規定に従って個人情報保護コンプライアンス制度体系を確立・整備し、主として外部の構成員から構成される独立的な機構の設立を通じた個人情報保護状況に対する監督を実施すること
- ✓ 公開性・公平性・公正性の原則を遵守し、プラットフォーム規則を制定し、プラットフォーム内の商品・役務提供者の個人情報取扱上の規範および個人情報保護義務を明確化すること
- ✓ 法律または行政法規に著しく違反して個人情報を取り扱ったプラットフォーム内の商品・役務提供者に対する役務提供を停止すること
- ✓ 個人情報の保護に対する社会的な責任に関する報告書を定期的に公開し、社会の監督を受けること

４．個人情報取扱活動中の個人の権利

- ✓ 同意撤回権。個人の同意に基づいて個人情報を取り扱うときは、個人は自らの同意を撤回することができる[74]。

[70] 「個人情報保護法」第31条参照。
[71] 「未成年者保護法」第4条参照。
[72] 「未成年者保護法」第72条参照。
[73] 「個人情報保護法」第58条参照。
[74] 「個人情報保護法」第15条参照。

- ✓ 知る権利、決定権、制限権、拒否権。個人は自らの個人情報の取扱いに対して知る権利と決定権を有し、他者による当該個人の個人情報の取扱いを制限または拒絶することができる。ただし、法律または行政法規に別段の定めのあるときは、例外とされている[75]。
- ✓ 調査・閲覧権、複製権。個人は自らの個人情報を個人情報取扱者の下から調査・閲覧・複製することができる[76]。
- ✓ その他の個人情報取扱者への移転の請求権。個人が自らの個人情報の自らが指定した個人情報取扱者への移転を請求した場合において、国家インターネット情報部門の定める条件を満たしていたときは、個人情報の取扱者は、移転のルートを提供しなければならない[77]。
- ✓ 修正権、削除権。個人は自らの個人情報の不正確性または不完全性に気が付いたときは、個人情報の取扱者に修正または補完を請求することができる。個人は個人情報の削除を請求することができる[78]。

四、各法による情報の収集・保存・利用・越境伝送の留意点

（一）情報の収集

１．一般的なデータの収集規則

データの収集、保存、使用、伝送などのデータ取扱活動の展開は、データセキュリティー保護義務を履行しなければならない。その具体的な内容は、次のとおりとされている[79]。

- ✓ 全工程データセキュリティー管理制度の確立・整備
- ✓ データセキュリティー教育研修の組織・展開
- ✓ 相応の技術措置およびほかの必要な措置の採択

データの収集は合法的かつ正当な方法を採択しなければならず、窃取またはその他の違法な方法をもってデータを取得してはならない。法律・行政法規にデータ収集・使用の目的・範囲に対する規定があるときは、法律・行政法規の規定する目的・範囲の中でデータを収集および使用しなければならない[80]。自動化の手段を採用したウェブ

[75] 「個人情報保護法」第44条参照。
[76] 「個人情報保護法」第45条第1項参照。
[77] 「個人情報保護法」第45条第3項参照。
[78] 「個人情報保護法」第46条、第47条参照。
[79] 「データセキュリティー法」第27条参照。
[80] 「データセキュリティー法」第32条参照。

サイトデータへのアクセス、およびその収集は、合理的な範囲内で行わなければならず、ウェブサイトの正常な運営を妨害してはならない[81]。

２．個人情報収集規則

個人情報の取扱いは、原則として、個人の同意を取得しなければならない。個人の同意に基づいて個人情報を取り扱うときは、当該同意は個人が事情を十分に知り得た前提の下で自発的かつ明確に行わなければならない[82]。個人による事情の十分な把握を保証するために、個人情報の取扱者は個人情報の取扱前において、顕著な方法、および明瞭かつ平易な言語をもって、事実に即して、正確かつ完全に以下の事項を個人に告知しなければならない[83]。また、以下の事項に仮に変更が発生したときは、変更部分を個人に告知しなければならない。そのうち、仮に個人情報の取扱目的、取扱方法、取り扱う個人情報の種類に変更が発生したときは、個人の同意を改めて取得しなければならない[84]。

- ✓ 個人情報取扱者の名称または氏名、連絡方法
- ✓ 個人情報の取扱目的、取扱方法，取り扱う個人情報の種類、保存期間
- ✓ 個人が個人情報保護法の規定する権利を行使する方法・手続き
- ✓ 法律および行政法規が告知義務を規定するその他の事項

個人の同意を取得するほかにも、「個人情報保護法」においてはさらに、個人情報の取扱いに関するその他の法律の基礎が規定されている[85]。以下の状況のいずれかに該当しているときは、個人情報の取扱者は個人情報の取扱時において個人の同意を取得する必要がない。

- ✓ 個人が一方の当事者である契約を締結および履行するための必須性、または法により制定された労働規則制度、もしくは法により締結された労働協約に従った人材資源管理を実施するための必須性
- ✓ 法定の職責または法定の義務を履行するための必須性
- ✓ 突発的な公共衛生事に対応し、または緊急な状況の下で、自然人の生命の健康および財産の安全を保護するための必須性
- ✓ 公共の利益のためのニュースの報道、世論の監督などの行為を実施時における合理的な範囲内の個人情報の取扱い
- ✓ 個人情報保護法の規定に従った合理的な範囲内における個人が自ら公開した個人情報、またはその他の既に合法的に公開されている個人情報の取扱い

81 「データセキュリティー管理弁法（意見募集稿）」第16条参照。
82 「個人情報保護法」第14条参照。
83 「個人情報保護法」第17条参照。
84 「個人情報保護法」第14条参照。
85 「個人情報保護法」第13条参照。

✓ 法律・行政法規の規定するその他の状況

個人情報の取扱いは、明確かつ合理的な目的を有していなければならず、取扱行為は取扱目的に直接関連しており、かつ、取扱目的の実現に必要な最小の範囲に限定しなければならない[86]。

３．個人機微情報の収集規則

個人情報の取扱者は個人機微情報を取扱時において、必ず特定の目的と十分な必要性を有していなければならず、かつ、厳格な保護措置を採択しなければならない[87]。個人機微情報の取扱いは、原則として、個人の単独の同意を取得しなければならない[88]。告知義務を履行するときは、「個人情報収集規則」において記されている告知のほかにも、個人情報の取扱者はさらに、個人機微情報の取扱い必要性、および個人の権益に対する影響を個人に告知しなければならない[89]。また、十四歳未満の未成年者の個人情報を取り扱うときは、未成年者の父母またはその他の保護者の同意を取得しなければならず、かつ、特別な個人情報取扱規則を制定しなければならない[90]。

個人機微情報および重要データを収集するときは、データセキュリティー責任者と管理機構を明確にしなければならない。データセキュリティー責任者は関連の管理業務の経歴およびデータセキュリティーの専門知識を有する人員が、これを担当し、以下の職責を履行しなければならない[91]。

- ✓ データ保護計画制定の組織、実施の督促
- ✓ データセキュリティーリスク評価実施の組織、セキュリティー上の潜在的な災禍の是正の督促
- ✓ 要求に従った関連部門およびネットワーク情報部門へのデータセキュリティー保護およびセキュリティーインシデントへの対応状況の報告
- ✓ ユーザーからのクレームと通報の受理および取扱い

86 「個人情報保護法」第 6 条参照。
87 「個人情報保護法」第 28 条参照。
88 「個人情報保護法」第 29 条参照。
89 「個人情報保護法」第 30 条参照。
90 「個人情報保護法」第 31 条参照。
91 「データセキュリティー法」第 27 条、「データセキュリティー管理弁法（意見募集稿）」第 17 条、第 18 条参照。

（二）情報の保存

１．一般的なデータの保存規則

データの保存過程においては、「一般データ収集規則」に記されているデータセキュリティー保護義務も履行し、相応の技術措置およびその他の必要な措置を採択しなければならず、さらには、サイバーセキュリティー等級保護制度の要求を遵守し、データ分類、重要データのバックアップ、暗号化などの措置を採択し、ネットワークによる妨害、破壊または授権を経ていないアクセスの回避を保障し、かつ、オンラインデータの漏えい、窃取または改ざんを防止しなければならない[92]。データの保存は、法令の規定またはデータ提供主体との間に取り決めた方法・期間に基づき、これを行わなければならない[93]。

２．重要データの保存規則

重要データを保存するときは、「一般的なデータの保存規則」を遵守するほかにも、さらには、暗号技術等の措置を採択して安全な保存を行わなければならず、保存システムの公共情報ネットワークアクセスを直接提供してはならず、かつ、リアルタイムデータのディザスタリカバリ・バックアップ、および保存媒体のセキュリティー管理を行わなければならない[94]。さらに、「サイバーセキュリティー法」においては、重要情報インフラ的運営者に対する特別なデータ保存上の要求が提起されており、中国国内における運営の過程において収集および発生した重要データと個人情報は、中国国内に保存しなければならないとされている[95]。

３．個人情報の保存規則

個人情報を保管するときは、目的の実現にとって必要な最短の期間でなければならない。個人情報の保管期間が当該期間を上回ったときは、個人情報に対して削除または匿名化処理を行わなければならない。また、保管される個人情報に対する関連従業員のアクセスを制限しなければならない[96]。

---

92 「データセキュリティー法」第27条、「サイバーセキュリティー法」第21条参照。
93 「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18条参照。
94 「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18条参照。
95 「サイバーセキュリティー法」第37条、「データセキュリティー法」第31条参照。「自動車データセキュリティー管理若干規定」第11条においても、類似の規定が行われている：重要データは法により中国国内に保存しなければならない。
96 「個人情報保護法」第19条、第47条および第51条参照。

４．個人機微情報の保存規則

「個人情報安全規範」においては、個人機微情報の保存に対し、以下の要求が定められている[97]。

- ✓ 個人機微情報を伝送および保存するときは、暗号化等のセキュリティー措置を採択しなければならない。
- ✓ 個人生体認識情報は、個人の身分情報と分けて保存しなければならない。
- ✓ 原則として、原版の個人生体認識情報を保存すべきではない。仮に個人生体認識情報の保存が必要なときは、ただ一定の技術手段を通じた後の保存（たとえば、ただ個人生体認識データの摘要情報のみの保存など）のみを行うべきである。

（三）情報の使用

１．一般的なデータおよび重要データの使用規則

一般データおよび重要データの使用は、法令の規定を遵守しなければならず、かつ、社会の公徳・倫理に適合していなければならない[98]。自らが把握したデータ資源を分析および利用し、市場予測、統計情報、個人・企業の信用などの情報を公布するときは、中国の国家の安全、経済の運営、社会の安定に影響を及ぼしてはならず、他者の合法的な権益を侵害してはならない[99]。

ユーザーデータ、アルゴリズムが用いられたプッシュ送信形式のニュース情報、商業広告など利用し、かつ、ビッグデータ、人工的な知能などの技術も利用して自動的に合成されたニュース、ブログ文章、スレッド、評論などの情報は、いずれも明確な方法をもって表示を行わなければならない[100]。

２．個人情報および個人機微情報の使用規則

（1）基本規則

個人情報を使用するときは、個人情報の収集時に表明された目的と直接性または関連性を有する範囲を超えてはならない[101]。また、目的のために必要である場合を除き、個人情報によって特定の個人が正確に特定されることを避けなければならない。個人

97 「情報セキュリティー技術 個人情報安全規範（GB/T 35273-2020）」第6.3条参照。
98 「データセキュリティー法」第28条、第32条参照。
99 「データセキュリティー管理弁法（意見募集稿）」第32条参照。
100 「データセキュリティー管理弁法（意見募集稿）」第23条、第24条参照。
101 「データセキュリティー管理弁法（意見募集稿）」第7.3条参照。

情報の授権範囲を超えて個人情報を使用するときは、当該個人情報の主体から明示的な同意を再度取得しなければならない。

個人情報の使用時においては、相応の個人情報アクセス制御措置を採択しなければならない。その具体的な要求には、次のものが含まれる[102]。一方、個人機微情報に対するアクセスや修正などの実務行為については、役割の権限に対する制御を基礎とし、業務工程の必要性に従って実務の授権を付与するのが適切である[103]。

- ✓ 個人情報へのアクセスが授権された人員を対象とする最小限の授権に関するアクセスコントロールポリシーの確立、同者に対するただ職責に必要な最小限の必要性の個人情報へのアクセスの可能化、およびただ職責の完成に必要な最少のデータ実務権限のみの保有
- ✓ 個人情報の重要な実務に対する内部認可審査工程の設定
- ✓ セキュリティー管理人員、データ実務人員および監査人員の役割に対する分離した設定の実施
- ✓ 業務上の必要性により権限を超えて個人情報を取り扱う必要のある特定の人員に対する個人情報保護責任者または個人情報保護業務機構の認可審査を経た後における授権取得の可能化、およびその記録の義務化

(2) 各具体的な場面における応用

各状況の下における個人情報の使用規則は、具体的には次のとおりである[104]。

状況	個人情報使用規則
個人情報の共同の取扱い	個人情報の取扱目的と取扱方法を共同で決定するときは、各自の権利・義務を取り決めなければならない。
	個人情報権益を侵害し、損害を引き起こしたときは、法により連帯責任を負担しなければならない。
個人情報取扱いの委託	受託者との間において取扱委託の目的、期間、取扱方法、個人情報の種類、保護措置、双方の当事者の権利・義務などを取り決め、受託者の個人情報取扱活動に対する監督を行わなければならない。
	受託者は取決めに従って個人情報を取り扱わなければならず、取り決めた取扱目的、取扱方法などを超過して個人情報を取り扱ってはならない。委託契約が発効せず、無効化し、撤回され、

102 「データセキュリティー管理弁法（意見募集稿）」第 7.1 条参照。
103 「データセキュリティー管理弁法（意見募集稿）」第 7.1 条参照。
104 「個人情報保護法」第 20 条ないし第 26 条参照。

	または終了したときは、受託者は個人情報を個人情報の取扱者に返還し、または削除を行わなければならず、保留してはならない。
	個人情報取扱者の同意を経ずに、受託者は個人情報の取扱いを他者に再委託してはならない。
個人情報の移転	合併、分割、解散、破産宣告などの原因により個人情報を移転する必要があるときは、受領者の名称または氏名および連絡方法を個人に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。 受領者が元の取扱目的、取扱方法を変更するときは、「個人情報保護法」の規定に従って、個人の同意を改めて取得しなければならない。
自らが取り扱う個人情報のその他の個人情報管理者への提供	受領者の名称または氏名、連絡方法、取扱目的、取扱方法、個人情報の種類を個人に告知し、個人の単独の同意を取得しなければならない。 受領者は上述の取扱目的、取扱方法、個人情報の種類などの範囲内において個人情報を取り扱わなければならない。 受領者は元の取扱目的、取扱方法を変更するときは、「個人情報保護法」の規定に従って個人の同意を改めて取得しなければならない。
個人情報を利用した自動化された意思決定の実施	意思決定の透明性、および結果の公平性・公正性を保証しなければならず、個人に対して取引価格などの取引条件の上で、不合理な差別待遇を実施してはならない。
	自動化された意思決定の方法を通じた個人への情報プッシュ送信、および商業マーケティングの実施は、当該個人の特徴を対象としない選択肢を同時に提供し、または簡便な拒絶の方法を個人に提供しなければならない。
	自動化された意思決定の方法を通じた個人の権益に重大な影響を及ぼす決定の実施に対し、個人は説明の実施を個人情報の取扱者に要求することができ、かつ、個人情報の取扱者のただ自動化された意思決定の方法のみを通じた決定の実施を拒絶することができる。
個人情報の公開	個人の単独の同意を取得した場合を除き、公開してはならない。

公共の場所における画像収集・個人身分認識設備の設置	公共の安全を保護するために必須であり、国家の関連規定を遵守し、顕著な注意喚起の標識を設置しなければならない。収集された個人の画像と身分認識情報は、ただ公共の安全を保護する目的にのみ用いることができ、その他の目的に用いてはならない。ただし、個人の単独の同意を取得した場合は、例外となる。

（四）情報の越境伝送

１．一般的なデータの越境伝送規則

データの越境とは、ネットワーク運営者のオンライン等の方法を通じた中華人民共和国の国内における運営の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[105]。以下の状況はデータの越境に属する[106]。

- ✓ 中国の国内ではあるが、中国の司法の管轄に属せず、または中国国内に登録されていない主体にデータを提供するとき。
- ✓ データは中国以外の地区に移転および保存されないが、しかし、中国国外の機構、組織・個人によってアクセスおよび閲覧されるとき（公開されている情報やウェブページへのアクセスは、例外となる）。
- ✓ ネットワーク運営者のグループ内部のデータが、中国国内から中国国外に移転し、同者の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にかかわっているとき。

ただし、以下の状況はデータの越境に属しない[107]。

- ✓ 中国国内における運営の過程において収集および発生したデータの中国を経由した越境ではなく、いずれの変動または加工処理も経ていないとき。
- ✓ 中国国内における運営の過程において収集および発生したデータの中国国内における保存または加工処理後の越境ではなく、中国国内における運営の過程において収集および発生したデータにかかわっていないとき。

[105] 「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）」第3.7条、「個人情報および重要データ越境セキュリティー評価弁法（意見募集稿）」第17条参照。
[106] 「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）」第3.7条参照。
[107] 「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）」第3.7条参照。

原則として、重要データ、核心データまたは個人情報ではない一般データは、セキュリティー評価を経ずに、中国国外の機構、組織・個人に直接提供することができる。

２．核心データおよび重要データの越境伝送規則

(1) 核心データ

核心データとは、「データセキュリティー法」において提起されている重要な概念であり、国家の安全、国民経済の命脈、重要な民生、重大な公共の利益などにかかわるデータをいう。「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）」においては、当該分野における具体的な認定基準が定められており、脅威の程度が同法の掲げる条件のいずれかに該当しているデータが核心データとなり[108]、この種のデータは越境してはならないという旨が規定されている[109]。

(2) 重要データ

重要情報インフラ運営者は中国国内において収集・生成した個人情報および重要データを中国国内に保管しなければならず、業務上の必要性により、越境する必要が確かにあるときは、セキュリティー評価を行わなければならない[110]。一方、「個人情報および重要データ越境セキュリティー評価弁法（意見募集稿）」においては、当該義務を履行しなければならない主体が、すべてのネットワーク運営者へと拡大されている。「データセキュリティー法」においては、重要情報インフラ運営者以外のその他のデータ取扱者を対象とする重要データの越境セキュリティー管理弁法は、国家ネットワーク情報部門が国務院の関連部門と共同で制定するという旨が規定されている。その他の法令[111]の規定を踏まえてみると、越境セキュリティー評価義務の主体は将来的には、すべての中国国外に重要データを提供するネットワーク運営者（データ取扱者）へと拡大される可能性がある。

国家標準「情報安全技術　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）」（以下、「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）」という）によれば、個人情報および重要データの越境にあたって、適法性、正当性、必要性がなければならず、また、越境に係る安全評価を行う必要がある。安全評価は、事業者自らによる自主評価を行うこととなり、必要に応じて外部（主管部門）の評価が必要と

108 「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10条参照。
109 「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24条参照。
110 「サイバーセキュリティー法」第37条参照。
111 「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24条、「自動車データセキュリティー管理若干規定（試行）」第11条等参照。

なる。安全評価においては、国の安全、経済の発展、社会公共利益、個人の権益に対するデータ越境の影響の程度およびサイバーセキュリティー事件が発生する可能性に基づき、安全リスクレベルが「低い、普通、高い、極めて高い」の四つのレベルにそれぞれ判定される。その結果、「高い、極めて高い」に判定された場合には、データを越境することができない。

		安全事件発生の可能性		
		1	2	3
影響の程度	≧5	高い	極めて高い	極めて高い
	4	普通	高い	高い
	3	低い	普通	高い
	2	低い	普通	普通
	1	低い	低い	普通

注意に値するのは、上述の「個人情報と重要データ越境セキュリティー評価弁法（意見募集稿）」と「情報安全技術 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）」においては、統一的に個人情報と重要データの越境に対して規定が設けられているという点である。2017年から公布された関連規定に基づき、個人情報と重要データの越境関連内容に対し、次のとおり整理する。

日付	名称	公布機関	備考
部門規則			
2017.5.19	個人情報と重要データ越境セキュリティー評価弁法	国家インターネット情報弁公室	意見募集稿
2019.5.28	データ安全管理弁法	国家インターネット情報弁公室	意見募集稿
2019.6.13	個人情報越境セキュリティー評価弁法	国家インターネット情報弁公室	意見募集稿
2021.10.29	データ越境セキュリティー評価弁法	国家インターネット情報弁公室	意見募集稿
国家標準			
2017.8.25	情報安全技術 データ越境セキュリティー評価ガイドライン	全国情報安全標準化技術委員会	意見募集稿

「データ安全管理弁法（意見募集稿）」によると、重要データとは、漏えいすると、

国家の安全、経済の安全、社会の安定、公共の健康と安全に直接影響する恐れのあるデータ（たとえば、未公開の政府の情報、大きな面積の人口、遺伝子・健康、地理、鉱産物資源など）をいう[112]。注意に値するのは、当該法規においては初めて「重要データには一般的に企業の生産管理・内部管理情報、個人情報等は含まれない」という旨が明確化されている点である。このほか、2021年に公布された「サイバーセキュリティー標準実践ガイドライン　データ分類分級ガイダンス（意見募集稿）」においても、重要データには一般的には個人情報および企業の内部管理情報が含まれないという旨が指摘されている。重要データの範囲について、今後の立法の動向に引き続き注意を払う必要がある。

「データ安全管理弁法（意見募集稿）」によると、ネットワーク運営者が経営を目的として重要データを収集するときは、所在地のインターネット情報部門へ届出を行うべきとされている。届出の内容には、収集・使用の規則、収集・使用の目的、規模、方法、範囲、類型、期間等が含まれており、データの内容そのものは含まれていない。これを基礎とし、ネットワーク運営者は重要データを中国国外へ提供し、または中国国内において第三者へ提供（公布、共有、取引）する前に、もたらされる可能性のある安全リスクを評価し、電信主管監管部門へ報告し、その同意を経るべきとされている。電信主管監管部門が不明確の場合は、省級のインターネット情報部門の承認を経るべきとされている[113]。

上述の「データ安全管理弁法（意見募集稿）」を除き、重要データ越境の安全評価等に関していまだに具体的な細則が公布されていない場合は、依然として「個人情報と重要データ越境セキュリティー評価弁法（意見募集稿）」、「情報安全技術 データ越境セキュリティー評価ガイドライン」の関連規定を参照することができる。

３．個人情報の越境伝送規則

「個人情報保護法」および「個人情報越境セキュリティー評価弁法（意見募集稿）」によると、個人情報の取扱者は個人情報を越境して提供する際に、以下の事項に注意しなければならない。

（1）個人情報の越境提供の条件

個人情報の取扱者は業務等を展開する過程において、仮に個人情報を中国国外に提供する必要があるときは、相応の条件を満たさなければならない。一般的な個人情報の取扱者について述べると、国家ネットワーク情報部門の規定に従い、専門機構を経

112 「データセキュリティー管理弁法（意見募集稿）」第38条（5）参照。
113 「データセキュリティー管理弁法（意見募集稿）」第15条参照。

て個人情報保護認証を行い、または国家ネットワーク情報部門が制定する標準的な契約に従って中国国外の受領者と契約を締結し、双方の当事者の権利・義務を取り決める必要がある[114]。一方、重要情報インフラ運営者と、個人情報の取扱いが国家ネットワーク情報部門の規定する数量に達している個人情報の取扱者は、国家ネットワーク情報部門が組織するセキュリティー評価を通過しなければならない[115]。

(2) セキュリティー評価

個人情報の越境セキュリティー評価の実施は、個人情報の取扱者（ネットワーク運営者）が所在地の省級のネットワーク情報部門に申請する必要がある[116]。セキュリティー評価は原則として2年に一回行われるが、個人情報の越境の目的、類型および中国国外における保管期間に変化が発生したときは、再度評価されるべきである[117]。このほかにも、異なる受領者に個人情報を提供する際には、別々にセキュリティー評価を申請・報告しなければならないが、ただし、同一の受領者に数回または連続して個人情報を提供する際には、頻回の評価は不要とされている[118]。

個人情報の越境評価に必要となるデータは、①申告書、②ネットワーク運営者（個人情報の取扱者）と受領者が締結した契約書、③個人情報越境セキュリティーリスクおよびセキュリティー保障措置分析報告書[119]などである[120]。重点的な評価の内容は、①個人情報の越境が、国家の関連の法律・法規と政策の規定に適合しているか否か、②中国国内のネットワーク運営者（個人情報の取扱者）と中国国外の受領者が締結した契約書が、個人情報の主体の合法的な権益を十分に保障することができ、かつ、有効に実務を処理することができるか否か、③中国国内のネットワーク運営者（個人情報の取扱者）または中国国外の受領者が個人情報の主体の合法的な権益を侵害した過去の有無、重大なサイバーセキュリティーインシデントの発生歴の有無、④ネットワーク運営者（個人情報の取扱者）の個人情報の取得の合法性・正当性の有無などとされている[121]。

114 「個人情報保護法」第38条参照。
115 「個人情報保護法」第38条参照。
116 「個人情報越境セキュリティー評価弁法（意見募集稿）」第3条参照。
117 「個人情報越境セキュリティー評価弁法（意見募集稿）」第3条参照。
118 「個人情報越境セキュリティー評価弁法（意見募集稿）」第3条参照。
119 「個人情報越境セキュリティーリスクおよびセキュリティー保障措置分析報告書」の関連要求は、「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（草案）」、「情報セキュリティー技術 個人情報セキュリティー影響評価ガイドライン（意見募集稿）」参照。
120 「個人情報越境セキュリティー評価弁法（意見募集稿）」第4条参照。
121 「個人情報越境セキュリティー評価弁法（意見募集稿）」第6条参照。

（3）個人情報保護影響評価

上記①の箇所で述べた条件を満たすほかにも、個人情報の取扱者はさらに、個人情報を中国国外に提供する前に、個人情報保護影響評価を行わなければならない[122]。当該評価には主として、以下の内容が含まれている[123]。

- ✓ 個人情報の取扱目的、取扱方法などの合法性・正当性・必要性の有無
- ✓ 個人の権益に対する影響、およびセキュリティーリスク
- ✓ 採択された保護措置の合法性、有効性、リスクの程度との対応性の有無

当該評価の評価報告書と取扱状況の記録は、少なくとも三年保存しなければならない[124]。

（4）個人情報取扱者の義務

個人情報の取扱者は、個人情報を中国国外に提供するときは、個人に対する告知義務を負担する。個人情報の取扱者は中国国外の受領者の名称または氏名、連絡方法、取扱目的、取扱方法、個人情報の種類、個人が中国国外の受領者に個人情報保護法の規定する権利を行使する方法・手続きなどの事項を個人に告知し、これを基礎として個人的単独の同意を取得しなければならない[125]。

このほか、個人情報の取扱者はさらに、必要な措置を採択して中国国外の受領者による個人情報の取扱活動が、「個人情報保護法」の規定する個人情報保護の基準に達している旨を保障しなければならない[126]。

（5）中国国外の受領者に対する規制

「個人情報の越境セキュリティー評価弁法(意見募集稿)」においては、中国国内のネットワーク運営者と中国国外の受領者が締結する契約の具体的な内容の明確化を通じ、中国国外の受領者の義務に対する規定が、初めて設けられている。これには主に、次の三つの面が含まれている。

- ✓ 個人情報の主体の合法的な権益が侵害を受けた際には、中国国内のネットワーク運営者または中国国外の受領者に賠償を請求することができる（受領者から賠償を取得できないときは、中国国内のネットワーク運営者が先行して賠償しなければならない[127]。

122 「個人情報保護法」第55条参照。
123 「個人情報保護法」第56条参照。
124 「個人情報保護法」第56条参照。
125 「個人情報保護法」第39条参照。
126 「個人情報保護法」第38条参照。
127 「個人情報越境セキュリティー評価弁法（意見募集稿）」第13条参照。

- ✓ 中国国内のネットワーク運営者もしくは中国国外の受領者に著しいデータの漏えい、もしくはデータの濫用事件が発生し、またはデータ主体の権益もしくは個人情報のセキュリティーを保護することができないときは、インターネット情報部門は随時データの越境を暫時的に停止し、または終了させることができる[128]。
- ✓ 中国国外のネットワーク運営者は、中国国内において、法定代表者または機構を通じてネットワーク運営者の責任と義務を履行し、自らの中国国内における実体を通じて相応の責任と義務の負担を確実に保証すべきとされている[129]。

一方、「個人情報保護法」においては、中国国外の組織・個人が中国の公民の個人情報権益を侵害し、または中国国家の安全、公共の利益を脅かす個人情報取扱活動に従事した場合の懲罰的な措置として、「国家ネットワーク情報部門はその中国国外の組織・個人を個人情報提供制限または禁止リストに組み入れ、公告を行い、同者への個人情報提供に対する制限、禁止などの措置を採択することができる。」という旨が規定されている[130]。

五、法的義務に係るアクションアイテムの整理

ネットワーク・データ・個人情報のセキュリティーに関するコンプライアンスを保証するために、ネットワーク運営者・データ取扱者・個人情報の取扱者となる各事業者は、以下の各項目の法的義務を負担しなければならない。

（一）管理制度の完全化

企業は初めに自社の業務と実際の状況を踏まえ、法令に基づきサイバーセキュリティー、データセキュリティーおよび個人情報保護が一体となったコンプライアンス管理制度体系を確立および完全化しなければならない。

企業のサイバーセキュリティーコンプライアンス管理制度は、サイバーセキュリティー等級保護制度を基礎としなければならない。企業は相応のサイバーセキュリティー等級の要求に基づき、セキュリティー物理環境、セキュリティー通信ネットワーク、セキュリティー区域境界、セキュリティー計算環境、およびセキュリティー管理センターを対象とする技術要求の充足を基礎とし、サイバーセキュリティー管理制度を構築し、セキュリティー管理機構、セキュリティー管理人員、セキュリティー建設管理、

128 「個人情報越境セキュリティー評価弁法（意見募集稿）」第 11 条参照。
129 「個人情報越境セキュリティー評価弁法（意見募集稿）」第 20 条参照。
130 「個人情報保護法」第 42 条参照。

セキュリティー維持管理などの管理に対する要求を満たす必要がある[131]。

他方、個人情報を含むデータのセキュリティー保護を対象とし、企業はデータセキュリティー責任者と管理機構の確立を基礎とし、データ分類・分級管理制度、データアクセス権限管理制度、データセキュリティーコンプライアンス評価制度、データの全ライフサイクルにおける管理制度、データ提携者管理制度、個人情報セキュリティー影響評価制度などに着眼しなければならない[132]。

このほかにも、セキュリティーインシデント緊急対応制度も、企業コンプライアンス管理制度体系構築の重点の一つである。保護の対象が、サイバーセキュリティーか、データセキュリティーか、それとも個人情報セキュリティーかにかかわらず、セキュリティーインシデントにより引き起こされる重大な悪影響と甚大な損失を防止するために、企業はいずれも法令に基づいてセキュリティーインシデント緊急対応策をそれぞれ制定し、完全化しなければならない。個人情報を収集するネットワーク運営者は、「インターネット個人情報セキュリティー保護ガイドライン」を参照し、個人情報セキュリティーインシデント緊急対応策（応急処置および事件の上位者への報告の流れ）を制定する。サイバーセキュリティー、データセキュリティーまたは個人情報セキュリティーを脅かすセキュリティーインシデントの発生時においては、緊急対応策を迅速に始動し、相応の救済措置を採択し、規定に従って関連主管部門に報告する。セキュリティーインシデントの発生時に企業が速やかに緊急対応策に従って措置を採択することができるよう保証するために、定期的に（少なくとも半年に一回）緊急対応研修と緊急対応演習を行うことよう推奨されている。

（二）責任者と管理機構の確定

「個人情報保護法」においては、企業は個人情報が国家ネットワーク情報部門の規定する数量に達したときは、内部個人情報保護セキュリティー責任者を公に明確にし、その情報を主管機構に届け出なければならず[133]、提供する重要インターネットプラットフォームサービス、またはユーザー数が膨大で、業務の類型が複雑な企業が個人情報を取り扱うときは、さらに、相対的に独立した監督機構を設置しなければならないという旨が要求されている[134]。さらに、「データセキュリティー法」においては、重要データ取扱者はデータセキュリティー責任者和管理機構を設置するよう要求されてお

131 「情報セキュリティー技術 サイバーセキュリティー等級保護基本要求（GB/T 22239-2019）」参照。
132 「電気通信・インターネット企業オンラインデータセキュリティーコンプライアンス評価要点（2020年版）」、「情報セキュリティー技術 個人情報安全規範（GB/T 35273-2020）」第11.4条参照。
133 「個人情報保護法」第52条参照。
134 「個人情報保護法」第58条参照。

り、「サイバーセキュリティー法」においては、ネットワーク運営者がサイバーセキュリティー責任者を確定し[135]、重要情報インフラ運営者は専門セキュリティー管理機構、およびセキュリティー管理責任者を設置しなければならないという旨が要求されている[136]。このため、セキュリティー管理責任者（たとえば、DPOなど。関連の管理業務経歴と専門知識を有する人員が担当する必要がある）および管理機構を適切に増やし、企業サイバーセキュリティー、データセキュリティー、および個人情報保護セキュリティーの管理業務（セキュリティー管理制度規範の制定セキュリティー技術能力の調整・強化、セキュリティーコンプライアンス評価の展開、セキュリティー監査管理、セキュリティーインシデント応急処理、教育研修などの業務を含むが、これらに限定されない）をセキュリティー管理責任者および管理機構に率先して負担させることを企業に勧める。関連業務の執行部門によるセキュリティー業務職の設置、管理機構の統括の下での協調と連携、法令に基づく具体的なセキュリティー管理業務の展開のほかにも、企業はさらに、セキュリティー管理機構と各業務執行部門の責任と分業の境界を明確にし、セキュリティー管理制度の執行実施状況に対する監督検査および考査問責制度を確立しなければならない[137]。

（三）具体的な実務ガイダンスの制定

企業は自社の業務状況を踏まえた上で、具体的なサイバーセキュリティー、データセキュリティー、個人情報保護実務ガイダンスの制定、および内部のサイバーセキュリティー・データ・個人情報コンプライアンス業務に対する全面的な整理を自ら、または特別なサイバーセキュリティー・データ・個人情報コンプライアンスチームと提携して行わなければならない。個人情報の保護を例に取ると、企業は関連個人情報の収集、保存、使用などの基本的な原則の確定を基礎とし、異なる典型的な状況を区分し、各状況にかかわる関係当事者（およびその当該状況下における役割）、個人情報の類型（たとえば、一般個人情報、個人機微情報、未成年者の個人情報など）および等級、重点セキュリティー措置（総体的な原則、ならびに具体的な実務の内容および段取りを含む）などについて説明を行うことができる。実務ガイダンスの明瞭性と平易性を保証するために、フローチャート、チェックリストなどの種々の形式を採択することができる。

135 「個人情報保護法」第21条参照。
136 「データセキュリティー法」第27条、「サイバーセキュリティー法」第34条参照。
137 「データセキュリティーコンプライアンス評価要点（2020年版）」参照。

（四）企業の内部における必要な研修と教育の実施

企業は従業員の教育研修制度を確立および強化しなければならない。企業は定期的な研修または新たな従業員の入職研修の展開、セキュリティー学習マニュアルの配布、従業員の学習および企業サイバーセキュリティー・データセキュリティー・個人情報保護管理規範文書の署名受領の組織などの方法を通じ、企業全体のセキュリティーコンプライアンス意識を引き上げ、企業内部セキュリティー管理規定の違反に伴う責任を従業員に理解させることができる。サイバーセキュリティー、データセキュリティーおよび個人情報保護の関連業務に従事する従業員を対象とし、企業は専門コンプライアンスチームを招へいした上でのセミナーの開催などの方法を通じて当該従業員に対する専門能力研修を強化しなければならず、かつ、専任者を設置し、この種の従業員に対する全面的かつ厳格なセキュリティー審査、意識考査、技能考査などの定期的な実施に責任を負わなければならない。上述の教育研修活動はセキュリティー教育および研修記録を形成しなければならず、考査活動は考査記録を形成し、研修データ、考査資料などの関連の証拠を併せて保存しなければならない。

（五）特別な義務への対応

企業は「サイバーセキュリティー法」「データセキュリティー法」「重要情報インフラセキュリティー保護条例」などを踏まえて自社が重要情報インフラ運営者または重要データ取扱者に属しているのか否かを確認しなければならず、仮にこれに属していたときは、相応の特定法の義務を着実に履行しなければならない。

重要情報インフラ運営者に該当する企業の義務は、本マニュアルの三（二）3 を参照のこと。一方、重要データ取扱者の特別な義務には、主として次のものがある[138]。

- ✓ データセキュリティーの責任者と管理機構の明確化、データセキュリティー保護責任の実施
- ✓ 規定に従った自社のデータ取扱活動に対するリスク評価の定期的な展開、リスク評価報告書の関連主管部門への届出（リスク評価報告書には、取り扱う重要データの種類・数量、データ取扱活動展開の状況、直面するデータセキュリティーリスク、これへの対応措置などが含まれていなければならない）

これらの二種類の特別な責任主体のほかにも、企業は法令の要求に従って所属する業界・分野における特別な義務を履行しなければならない可能性もある（一部の業界・分野における特別なコンプライアンス要求については、本マニュアルの「六、アクシ

[138] 「データセキュリティー法」第 27 条、第 30 条参照。

ョンアイテムの推進―各業種の法的義務の整理」を参照)。

六、アクションアイテムの推進―各業種の法的義務の整理

本マニュアルの「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」による規制対象で述べたとおり、理論的には、企業は所属業種のいかんを問わず、かつ、自社が従事する事業・経営活動のインターネットとの直接の関連性の有無を問わず、いずれも「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」の関連規定を遵守しなければならない。企業が従事する事業・経営活動が、インターネットとの直接の関連性を有しているときは、当該企業の負うべき法定の義務は、一般の事業者に比べ、その範囲はさらに広く、より厳格になるものと思われる。各業種の法的義務については、紙幅の制限により、ここでは代表的な 4 業種を取り上げ、当該業種に属する企業が、「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」における所定の義務のうち、特に注意すべき点について解説する。

(一) 金融業

金融業に属する企業の情報システムには、大量の顧客個人情報および重要データが含まれており、ネットワーク・データ・個人情報にかかわるセキュリティーインシデントが発生してデータが漏えいすれば、深刻な損失を招くことになる。金融業に属する企業は、重要情報インフラ運営者に認定される可能性が極めて高いことから、「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」の定める重要情報インフラ運営者の関連義務に注意し、次の各項目の点から、サイバーセキュリティー、データセキュリティーおよび個人情報の保護に関するコンプライアンスを強化すべきである。

1．重要情報インフラ運営者の認定および関連義務

政府内部向けの「国家サイバーセキュリティー検査ガイドライン」を参考にし、「重要情報インフラセキュリティー保護条例」に示されている重要情報インフラの認定基準を見てみると、金融業に属する企業は重要情報インフラに認定される可能性が高く、将来的に重要情報インフラ運営者であるものと認定されたときは、相応の法定の義務を履行しなければならない(法定の義務については、本マニュアルの三(二)3 を参

照)。

２．金融業界サイバーセキュリティー等級保護

中国人民銀行は2020年11月11日に改定後の「金融業界サイバーセキュリティー等級保護測定評価ガイドライン（JR/T 0072-2020)」を公布した。同ガイドラインにおいては、金融業界の第二級、 第三級および第四級の等級保護対象に対するセキュリティー測定評価の一般要求、およびセキュリティー測定評価の追加要求が規定されている。金融業界における企業は、当該ガイドラインを参照し、サイバーセキュリティー等級保護の届出を合理的に行うことができる。

３．金融データの分類・分級

金融業機構は当面の金融業界におけるデータの分類・分級基準である「金融データセキュリティー データセキュリティー分級ガイドライン（JR/T 0197_2020)」や「証券期貨業データ分類・分級ガイダンス（JR/T 0158_2018)」などの基準を参照し、データの分類・分級を行うことができる。

４．金融業における重要データセキュリティー

「データセキュリティー法」「データセキュリティー管理弁法（意見募集稿)」および国家標準「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)」によると、金融業に属する企業が収集・保管する個人財産情報、銀行口座情報、個人信用情報、取引情報などは、重要データに該当する。金融業に属する企業は、係る重要データについて、全面的に整理し、当該データの中国国内における保管および越境に関する評価制度となる規程を内部で制定しておく必要がある。

５．個人機微情報の保護

「個人情報保護法」および「個人情報安全規範」によると、金融業に属する企業が収集する銀行口座番号、クレジット情報、信用調査情報などの個人財産に関する情報は、個人機敏情報に該当するので、収集の際に、情報の主体の明示的な同意を取得し、かつ、送信または保管の際に、情報を暗号化するなどのセキュリティー措置を講じなければならない。また、「銀行業界に属する金融機関による個人金融情報保護業務の遂行に関する中国人民銀行の通知」[139]によると、金融機関の業務遂行時における中国人民

[139] 「銀発〔2011〕17号」参照。

銀行信用調査システム、支払システムその他システムにアクセスして取得・加工・保管する個人身分情報、個人財産情報、個人口座番号情報、個人信用情報、個人金融取引情報などは、個人金融情報に該当する。当該個人情報について、金融機関は情報セキュリティー技術防止措置を完全化し、個人金融情報がその収集・送信・加工・保管・使用などの段階において開示されないように努める必要がある。

６．個人情報の保管および越境に対する制限

「銀業界に属する金融機関による個人金融情報保護業務の遂行に関する中国人民銀行の通知」によると、中国国内において収集した個人金融情報の保管・処理・分析は、中国国内において行わなければならない。法令および中国人民銀行に別段の定めのある場合を除き、金融機関は中国国内の個人金融情報を越境してはならない。

（二）製造業

製造業に属する企業が中国国内において自社のオフィシャルサイト、産業用制御ネットワーク、LAN、内部オフィスネットワークなどを確立し、かつ、係るシステムを自ら管理する場合においても、ネットワーク運営者の範ちゅうに組み入れられる。一方、製造企業が研究・開発・設計、生産・製造、経営管理、維持管理サービスなどの段階において生成および使用するデータ、およびインダストリアルインターネットプラットフォーム企業が、設備の接続、プラットフォームの運営、工業APPの応用などの過程において生成および使用するデータによっても、製造企業はデータ取扱者となる。これらの企業に対しては、特に注意すべき法定の義務が特別に設定されており、次に掲げるいくつかの点が含まれる。

１．企業のサイバーセキュリティー保護制度の強化

2017年12月に、国務院により「『インターネットおよび先進的な製造業』の発展を深化させる産業ネットワークに関する指導意見」が公布された。当指導意見においては、産業ネットワークの規則体系を完全化し、インフラとしての地位を明確にし、セキュリティー、プラットフォームの責任、データの保護などを網羅する法規体系を確立するよう要求されている。2020年には、工業および情報化部が「インダストリアルインターネット革新的発展行動計画（2021～2023年）」を公表した。当行動計画においては、企業サイバーセキュリティー主体責任の法による実施、インダストリアルインターネット企業によるサイバーセキュリティー分類・分級管理制度の実施、企業のセ

キュリティー責任要求および標準的な規範の明確化、指導監督の強化、等級別責任負担監督管理制度の強化，自らの地区に所属する重点ネットワーク接続工業企業リストおよび重要データ保護目録の加速的な確立に向けた省級の主管部門の指導、サイバーセキュリティー管理体系完全化の企業への督促、サプライチェーンセキュリティー管理の強化、企業主体責任の実施、重点インダストリアルインターネットプラットフォームおよびAPPに対するセキュリティー検査・評価の強化などが提起されている。よって、製造業に属する企業はサイバーセキュリティー保護制度を重視し、生産経営において厳格に執行しておく必要がある。

２．工業データの分類・分級

当面の製造企業によるデータの分類・分級は、「工業データ分類・分級ガイドライン（試行）」を参照して行い、かつ、「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）」を参考にすることもできる。

３．重要データ

製造業に属する企業のデータベースまたは産業用制御システムにおいて保管され、または生成され、企業の生産運営状況および業種の発展状況を反映している産業データは、国家基準である「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）」および「データセキュリティー管理弁法（意見募集稿）」における重要データに該当する可能性がある。係る状況に対応するため、製造業に属する企業は、国家基準である「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）」における重要データの識別ガイドラインに基づき、自社の内部の重要データについて識別を行い、産業データ分級分類管理制度を確立し、重要データのセキュリティー保護措置を強化し、その保管・送信において受ける可能性のある制限を対象として、事前に関連する内部制度を制定しておくなどの準備が必要である。

このほかにも、自動車業界を対象とし、国家インターネット情報弁公室などの部門専門は「自動車データセキュリティー管理若干規定（試行）」を公布しており、同規定においては、自動車業界における重要データに対する定義が行われている。自動車企業（特に、ICV企業）は、車両ネットワーク接続にかかわる個人情報と重要データの数量が膨大であり、重要情報インフラ運営者と認定される可能性が高い。重要情報インフラ運営者の中国国内における運営の過程において収集および発生した個人情報と重要データは、中国国内に保存しなければならず、かつ、中国国外への伝送も、セキュリティー評価を経過しなければならない。中国国内の外資自動車企業を主とする多くの自動車企業は、多国籍企業であり、比較的に深刻なコンプライアンスリスクに直面

している。このほか、ICV企業は製造およびデータ取扱いの過程において、提携する第三者へのデータの提供は避けられない。そのためICV企業は自社のデータの対外的な提供行為のコンプライアンスを着実に保障するよう要求される。企業は提携する第三者のデータコンプライアンスに対して厳格に規制しなければならない。

（三）インターネット業

インターネット企業は、ネットワーク運営者（重要情報インフラ運営者を含む。）、ネットワーク製品・サービス提供者、およびデータ取扱者の範ちゅうに組み入れられる。その業務の範囲に応じて、インターネット企業は個人情報の取扱者になる可能性もある。よって、インターネット企業は、データ取扱者、個人情報の取扱者、ネットワーク運営者、ネットワーク製品・サービス提供者、またはデータ取扱者として関連する法定の義務を遵守しなければならない（具体的には、前述の内容を参照）。また、「サイバーセキュリティー法」「個人情報保護法」その他関連規定において、インターネット企業が特に注意すべき法定の義務が、特別に設定されている。これには次に掲げるいくつかの点が含まれている。

１．重要情報インフラ運営者の認定および関連義務

大量の個人情報や重要データを取り扱う[140]インターネット企業は、「国家インターネットセキュリティー検査ガイドライン」および「重要情報インフラセキュリティー保護条例」の重要情報インフラの認定標準に基づき、重要情報インフラ運営者に認定される可能性が高く、今後、重要情報インフラ運営者と認定されたときは、相応の法定の義務を履行しなければならない（法定の義務については、本マニュアルの三（二）3を参照）。

２．内容審査報告義務

インターネット企業は、自社のユーザーが公開する情報に対する管理を強化しなければならない。法律・行政法規により公開・送信が禁止されている情報を発見したときは、ただちに当該情報の送信を停止し、除去等の処理を施し、情報の拡散を防止し、関連記録を保管し、かつ、関連主管部門に報告しなければならない[141]。

[140] 具体的な量については、いまだに法により明確にされていないため、今後の立法の動向に注目しておく必要がある。
[141] 「サイバーセキュリティー法」第47条参照。なお、2014年以降、インターネット情報サービス主管部門である国家インターネット情報弁公室は、若干の規範性文書を公布しており、相応のインターネッ

３．インターネット実名制推進の義務

インターネット企業がユーザーのためにインターネットアクセスおよびドメイン登録サービスを提供し、固定電話、携帯電話などのインターネットアクセス手続きを行い、ユーザーのために情報の公開、インスタントメッセージなどのサービスを提供し、ユーザーと協議書を締結し、サービスの提供を確認するときは、真実の身分情報を提供するようユーザーに要求しなければならない。ユーザーが真実の身分情報を提供しなかったときは、インターネット企業は当該ユーザーのために関連サービスを提供してはならない[142]。

４．ユーザーのインターネット上におけるデータの保管義務

「サイバーセキュリティー法」などの関連する法令において、ユーザーのインターネット上におけるデータの保管期間が定められている。例えば、「インターネット情報サービス管理弁法」「インターネット出版サービス管理規定」などにおいては、少なくとも60日間、「インターネットゲーム管理暫定施行弁法」においては、少なくとも180日間、「インターネット取引管理弁法」においては、少なくとも2年間、ユーザーのインターネット上のデータを保管しなければならない旨が定められている。

５．データセキュリティー要求

インターネット企業はデータセキュリティー要求の実践時において、三法や「個人情報安全規範」などの普遍的な適用性を有する法令・基準のほかにも、さらには「電気通信およびインターネット企業オンラインデータセキュリティーコンプライアンス評価要点」「電気通信およびインターネットユーザー個人情報保護規定」などの業界における特別規定も参照する。

６．個人情報の収集・保管・使用に関連する義務

インターネット企業もまた、「個人情報保護法」および「サイバーセキュリティー法」における個人情報保護に関する規定を厳格に遵守しなければならない。さらには、個

トサービスを提供するインターネット企業に対し、内容審査義務を定めている。上記の規範性文書には、「インスタントメッセージツール公衆情報サービス発展管理暫定施行規定」「インターネットユーザーアカウント名称管理規定」「インターネット情報検索サービス管理規定」「モバイルインターネット応用プロセス情報サービス管理規定」「インターネットニュース情報サービス管理規定」「マイクロブログ情報サービス管理規定」などが含まれている。

142 「サイバーセキュリティー法」第24条参照。

人情報の収集・保管・使用・越境などの点においては、「サイバーセキュリティー法」の関連規定である「児童個人情報ネットワーク保護規定」および「個人情報安全規範」の規定も遵守しなければならない。これには、児童の個人情報、個人機敏情報収集の際に取得すべき保護者または本人の明示的な同意、企業プライバシーポリシーの制定、個人情報保管期間の最短化、個人情報の共有および譲渡の際の注意事項などが含まれている。

７．大型インターネットプラットフォームの特別な義務

本マニュアルの三（六）3を参照のこと。

８．自動化された意思決定およびアルゴリズム

インターネット企業は業務を展開する過程において、自動化された意思決定を利用する可能性がある。この場合、「個人情報保護法」の規定によると、インターネット企業は個人情報の取扱者として、意思決定の透明性、および結果の公平性・公正性を保証しなければならず、個人に対して取引価格等の取引条件の上で、不合理かつ差別的な待遇を実施してはならないとされている[143]。しかし、「個人情報保護法」においては、「合理性」とは何か、および「差別待遇」とは何かという点については、明確に説明されていない。このため、企業が自動化された意思決定メカニズムを利用するときは、各地の関連部門が既に公布している関連監督管理要求または基準、および今後の法執行の実践に注意を払わなければならない。このほかにも、企業は自動化された意思決定の方法を通じ、個人に対して情報のプッシュ送信または商業マーケティングを行うときは、その個人の特徴を対象としない選択肢を同時に提供し、または簡便な拒絶方法を個人に提供する必要があるという点にも、注意を払わなければならない。

アルゴリズムを対象とする関連の規制は、各種の法規や基準において散見され、これはたとえば「データセキュリティー管理弁法（意見募集稿）」「個人情報安全規範」「プラットフォーム経済分野に関する独占禁止ガイドライン」などである。2021年に、国家インターネット情報弁公室等の九つの部門と委員会は、「インターネット情報サービスのアルゴリズムの総合的な管理の強化に関する指導意見」を通達した。全国情報技術標準化技術委員会は「情報安全技術 機器学習アルゴリズムセキュリティー評価規範（意見募集稿）」を公布し、今後のアルゴリズム基準的の公布に伴い、国家はアルゴリズムに対する監督管理を強化していくものと見られている。

[143]「個人情報保護法」第24条参照。

（四）医療業

医療業は患者個人と密に接触する業界であり、疾病の診療、健康診断および健康管理の過程において、大量のユーザープライバシー情報にかかわっている。健康医療データの応用、「インターネット＋医療健康」、およびスマート医療の急速な発展に伴い、健康医療のデータコンプライアンスの問題は、次第に重視されるようになってきている。医療データは一方では、「サイバーセキュリティー法」「データセキュリティー法」「個人情報保護法」などの一般データと個人情報を対象とする法令の保護と監督管理を受けており、他方、その特別性と重要性により、中国においてはさらに、各種の異なる類型の医療データを対象とする法規が公布されている。

１．重要情報インフラ運営者の認定および関連義務

医療企業は、大量の個人情報（特に個人機微情報）や重要データを取り扱っているため、重要情報インフラ運営者に認定される可能性がある。重要情報インフラ運営者と認定されたときは、相応の法定の義務を履行しなければならない（法定の義務については、本マニュアルの三（二）3を参照）。

２．医療データ分類・分級

「情報安全技術 健康医療データセキュリティーガイドライン（GB/T 39725－2020）」においては、健康医療データが個人属性データ、健康状況データ、医療応用データ、医療支払データ、衛生資源データ、および公共衛生データの六種類に分けられており、データの重要度、リスク等級、ならびに個人健康医療データ主体に対して引き起こす恐れのある損害および影響の等級に基づき、データが五つの等級に分けられている。医療業界の機構と企業は「健康医療データセキュリティーガイドライン」を参考にして、医療データの分級分類を行い、業務を展開することができる。

３．個人機微情報の取扱い

（1）基本的原則

「個人情報保護法」と「個人情報安全規範」の規定によると、医療業界内の企業の運営の過程において収集および発生した個人健康生理情報、個人生体認識情報などは、多くは個人機微情報に属するが、その中の人口健康情報、人類遺伝資源情報などの情報の取扱いは、いずれもその他の個人機微情報に比べてさらに厳格な制限を受けてい

る。人口健康情報[144]の収集は「一つのデータに一つの起源。最少限度での用途の充足」という原則にのっとっている。保存の原則は、以下のとおりである。

- ✓ 分級分類保存
- ✓ 中国国内における保存。人口健康情報は、中国国外のサーバ内に保存してはならず、中国国外のサーバ内における管理委託、または当該サーバの賃借を行ってはならない（すなわち、人口健康情報の越境伝送は厳格に禁止されている）。

（2）人類遺伝資源情報[145]

① 収集・保存

- ✓ 法人資格の保有、収集/保存目的の明確性・合法性、収集/保存案の合理性、倫理審査の通過、人類遺伝資源の管理の職能を担う部門および相応の管理制度の存在などの条件に適合していなければならない。
- ✓ 中国国外の組織・個人、および当該組織・個人が設立し、または実質的に支配している機構は、中国国内で中国の人類遺伝資源を収集または保存してはならず、中国の人類遺伝資源を中国国外に提供してはならない。

②利用・対外提供

- ✓ 中国国外の組織、および中国国外の組織・個人が設立し、または実質的に支配している機構は、中国人類遺伝資源を利用して科学研究活動を展開する必要があるときは、中国の科学研究機構、大学・高等専門学校、医療機構または企業との提携の方法を採用し、これを行わなければならない。
- ✓ 人類遺伝資源情報は原則として、越境伝送することができない。

  例外的な状況：中国人類遺伝資源を利用して国際的に提携した科学研究を展開し、またはその他の特別な状況により、中国の人類遺伝資源資料の運送、郵送または携帯した越境が確かに必要な場合

144 「人口健康情報管理弁法（試行）」第 8 条、第 9 条、第 10 条、第 13 条参照。
145 「人類遺伝資源管理条例」第 7 条、第 11 条、第 14 条、第 21 条、第 27 条参照。

別紙１：中国の個人情報保護法と欧州の GDPR との間の比較

適用範囲		
	「個人情報保護法」	GDPR[146]
域内適用	第 3 条第 1 項 組織または個人による**中国国内における自然人の個人情報取扱行為の実施**には、本法が、適用される。	第 3 条第 1 項 本規則は、その取扱いが EU 域内で行われるものであるか否かを問わず、**EU 域内の管理者または処理者の拠点の活動の過程における個人データの取扱い**に適用される。
域外適用	第 3 条第 2 項 中国国外において、中国国内の自然人の個人情報を取り扱う行為に及ぶときも、次の各号に掲げる条件の一に該当するときは、本法を適用する。 (一) 中国国内の自然人への商品・役務の提供を目的とする行為 (二) **中国国内の自然人を分析または評価する**ための行為 (三)法律および行政法規の定めるその他の行為	第 3 条第 2 項 取扱活動が以下と関連する場合、本規則は、EU 域内に拠点のない管理者または処理者による EU 域内のデータ主体の個人データの取扱いに適用される： (a) データ主体の支払いが要求されるか否かを問わず、EU 域内のデータ主体に対する物品またはサービスの提供。または (b) データ主体の行動が EU 域内で行われるものである限り、**その行動の監視**。
適用除外	第 72 条 自然人は、個人または家庭の事務に起因して個人情報を取り扱うときは、本法の適用を受けない。 法律が各級の人民政府およびその関連部門の手配および実施する統計活動および記録文書管理活動中の個人情報	第 2 条第 2 項 本規則は、以下の個人データの取扱いには適用されない： (a) EU 法の適用範囲外にある活動の過程で行われる場合。 (b) 加盟国によって EU 条約第 5 款第 2 章の適用範囲内にある活動が行われる場合。

[146] https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

	の取扱いを規定しているときは、当該規定を適用する。	(c) 自然人によって純粋に私的な行為または家庭内の行為の過程において行われる場合。 (d) 公共の安全への脅威からの保護およびその脅威の防止を含め、所管官庁によって犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行のために行われる場合。
個人機微情報		
	「個人情報保護法」	**GDPR**
定義	第 28 条第 1 項 機微個人情報とは、ひとたび漏えいし、または違法に使用されたときに、個人が人格尊厳に対する被害または身体もしくは財産の安全性に対する危害を被ることとなる恐れのある個人情報をいう。	規定なし
類型	第 28 条第 1 項 • 生体識別情報 • 宗教上の信条に関する情報 • 特定身分情報 • 医療・健康情報 • **金融口座情報** • **個人の行き先に関する情報** • **14 歳未満者の個人情報**	第 9 条第 1 項 • 人種的もしくは民族的な出自を明らかにする個人データ • **政治的な意見を明らかにする個人データ** • 宗教上もしくは思想上の信条を明らかにする個人データ • 労働組合への加入を明らかにする個人データ • 遺伝子データ • 自然人を一意に識別することを目的とする生体データ • 健康に関するデータ • **自然人の性生活もしくは性的指向に関するデータ**

取扱要求	第 28 条第 2 項 個人情報取扱者は、ただ**特定の目的または十分な必要性があり、厳格な保護措置が講じられる**状況下においてのみ、機微個人情報を初めて取り扱うことができる。	原則として、第 9 条第 1 項に記される個人データの取扱が禁止されている。
		第 9 条第 2 項によれば、特定の場合には第 9 条第 1 項に記される個人データの取扱の禁止は適用されない。 • データ主体が明確な同意を与えた場合。 • データ管理者またはデータ主体の義務を履行する目的のため、または、それらの者の特別の権利を行使する目的のために取扱いが必要となる場合。 • データ主体が物理的または法的に同意を与えることができない場合で、データ主体またはその他の自然人の生命に関する利益を保護するために取扱いが必要となるとき。 • 非営利組織による正当な活動の過程における特別なデータ主体の個人データに限って、取扱いが行われる場合。 • データ主体によって明白に公開のものとされた個人データに関する取扱いの場合。 • 訴えの提起もしくは攻撃防御のため、または、裁判所がその司法上の権能を行使する際に取扱いが必要となる場合。 • 重要な公共の利益を理由とする取扱いが必要となる場合。 • ほかの公共の利益（医療・社会福祉、公衆衛生、科学的・歴史的研究、統計）を理由とする取扱いが必要となる場合。
特殊個人情報主体への特別保護		
	「個人情報保護法」	**GDPR**

未成年者	第 31 条 個人情報取扱者は、**14 歳未満**の未成年者の個人情報を取り扱う場合、当該未成年者の両親またはその他の後見人の同意を得なければならない 個人情報取扱者は、**14 歳未満**の未成年者の個人情報を取り扱う場合、特別な個人情報取扱ルールを定めなければならない。	第 8 条第 1 項 子どもに対する直接的な情報社会サービスの提供との関係において第 6 条第 1 項(a)が適用される場合、**その子どもが 16 歳以上であるときは、その子どもの個人データの取扱いは適法である。**その子どもが 16 歳未満の場合、そのような取扱いは、その子どもの親権上の責任のある者によって同意が与えられた場合、または、その者によってそれが承認された場合に限り、かつ、その範囲内に限り、適法である。 加盟国は、その年齢が **13 歳を下回らない限り、法律によって、それらの目的のためのより低い年齢を定めることができる。**
死者	第 49 条 自然人が死亡した場合、その近親者は、死者による生前の別段の取り決めがない限り、自らの合法的・正当な利益のために、本章に定める死者に関する個人情報に対する閲覧、複製、訂正、削除などの権利を行使することができる。	前文（27） 本規則は、死亡した者の個人データには適用されない。加盟国は、死亡した者の個人データの取扱いに関する規定を定めることができる。
個人情報の越境伝送		
	「個人情報保護法」	**GDPR**
条件	第 38 条第 1 項 個人情報取扱者は、業務等の必要性により、中国国外に向けて個人情報を提供する必要性が確かにあるときは、少なくとも次の各号に掲げる条件の一を満たさなければならない。 (一)本法第四十条の規定に従って国家インターネット情	第 45 条 第 1 項 **第三国、第三国内の地域または一もしくは複数の特定の部門、または、国際機関が十分なデータ保護の水準を確保していると欧州委員会が決定した**場合、当該第三国または国際機関への個人データの移転を行うことができる。 その移転は、いかなる個別の許可も要しない。

	報部門が手配する**セキュリティー評価を通過した**とき。 (二)国家インターネット情報部門の規定に従い、**専門的な機構を経て個人情報保護認証を取得した**とき。 (三) **国家インターネット情報部門の制定したモデル契約書に基づき、中国国外の受領者と契約を締結し、双方の当事者の権利・義務を取り決めた**とき。 (四)法律、行政法規または国家インターネット情報部門の定めるその他の条件を満たすとき。	第46条第1項 第45条第3項による決定がない場合、**管理者または処理者は、その管理者または処理者が適切な保護措置を提供しており、かつ、データ主体の執行可能な権利およびデータ主体のための効果的な司法救済が利用可能なこと**を条件としてのみ、第三国または国際機関への個人データを移転することができる。 **＋第49条第1項に規定する特定の状況における例外** • データ主体に対して発生させる可能性のあるリスクの情報提供を受けた後に、そのデータ主体が、移転に明示的に同意した場合； • データ主体と管理者との間の契約の履行のためにその移転が必要となる場合など； • 管理者によるデータ主体の利益のために帰する契約の締結、または、その契約の履行のために移転が必要となる場合； • 公共の利益の重大な事由の移転が必要となる場合； • 法的主張時の立証、行使または抗弁に移転が必要となる場合； • データ主体が物理的または法的に同意を与えることができない場合において、データ主体またはそれ以外の者の生命に関する利益を保護するために移転が必要となる場合； • 特定の条件を満たす場合において、登録機関からの移転が必要となる場合；

		• 移転が、反復的なものではなく、限定された人数のデータ主体に関係するものであり、データ主体の権利および自由によって優先されるものではない管理者が求める義務的な正当な利益の目的のために必要であり、かつ、管理者がデータ移転と関連するすべての事情を評価しており、かつ、その評価に基づき、その管理者が個人データの保護に関連して適合する保護措置を提供した場合。
情報保存の現地化	第 40 条 重要情報インフラの運営者と個人情報の取扱件数が国家インターネット情報部門の定める数量に達した個人情報取扱者は、中国国内において収集し、または発生した個人情報を中国国内に保存しなければならない。	規定なし
個人権利		
	「個人情報保護法」	**GDPR**
類型	知る権利	知る権利
	取扱制限権	取扱制限権
	取扱拒絶権	異議を述べる権利
	閲覧権	アクセス権
	複製権	複製権
	移転権	データポータビリティの権利
	訂正・補足権	訂正・補足権
	消去権	消去権（「忘れられる権利」）
	自らの個人情報の取扱規則に対する説明を個人情報取扱	

	者に請求する権利	
	個人の権利として第 4 章には規定されていないが、第 24 条で自動化された意思決定について規定している。 第 24 条 個人情報を利用して自動化された意思決定をする個人情報取扱者は、当該意思決定の透明性および結果の公平性を確保し、取引価格およびその他の取引条件について個人に不当な差別的取扱いをしてはならない。 自動化された意思決定方法による個人への情報プッシュおよび商業マーケティングは、個人の個性に特有ではないオプションを提供するか、または、個人に拒否する容易な方法を提供する必要がある。 自動化された意思決定方法を通じて個人の権利および利益に大きな影響を与える決定を行うために、個人は個人情報取扱者に説明を求める権利を有し、自動化された意思決定方法を通じてのみ決定を行うことを個人情報取扱者に対して拒否する権利を有する。	プロファイリングを含む個人に対する自動化された意思決定に関する権利
個人情報取扱者の義務		
	「個人情報保護法」	**GDPR**
安全保障措置	第 51 条 • **内部管理制度および取扱規程の制定；** • **個人情報に対する分級・分類管理の実施；** • 相応の暗号化、非特定化等のセキュリティー技術措置	第 32 条第 1 項 • 個人データの仮名化または暗号化； • **取扱システムおよび取扱サービスの現在の機密性、完全性、可用性および回復性を確保する能力；**

	の採択； • **個人情報の取扱いに係る取扱権限の合理的な確定、および従業員に対する定期的なセキュリティー教育・研修の実施；** • **個人情報のセキュリティーインシデントに備えた緊急対応マニュアルの制定および手配；** • 法律または行政法規の定めるその他の措置。	• **物的または技術的なインシデントが発生した際、適時な態様で、個人データの可用性およびそれに対するアクセスを復旧する能力；** • **取扱いの安全性を確保するための技術上および組織上の措置の有効性の定期的なテスト、評価および評定のための手順。**
個人情報保護責任者の設置	第 52 条第 1 項 **個人情報の取扱数が、国家インターネット情報部門の定める数量に達した**個人情報取扱者は、個人情報の取扱行為や採択する保護措置等の監督を担当する個人情報保護責任者を指定しなければならない。	第 37 条第 1 項 管理者および処理者は、以下の場合において、データ保護オフィサーを指名しなければならない： (a)**公的機関または公的組織によって行われる場合。**ただし、裁判所がその司法上の権限を行使する場合を除く取扱い； (b)**管理者または処理者の中心的業務が、 その取扱いの性質、範囲およびまたは目的のゆえに、データ主体の定期的かつ系統的な監視を大規模に要する取扱業務によって構成される場合**；または、 (c)**管理者または処理者の中心的業務が、第 9 条による特別な種類のデータおよび第 10 条で定める有罪判決および犯罪行為と関連する個人データの大規模な取扱いによって構成される場合。**
個人情報保護	当該評価の実施が求められる場合	
	第 55 条 • 機微個人情報の取扱い；	第 35 条第 3 項 • プロファイリングを含め、自動的な取扱いに基づくもので

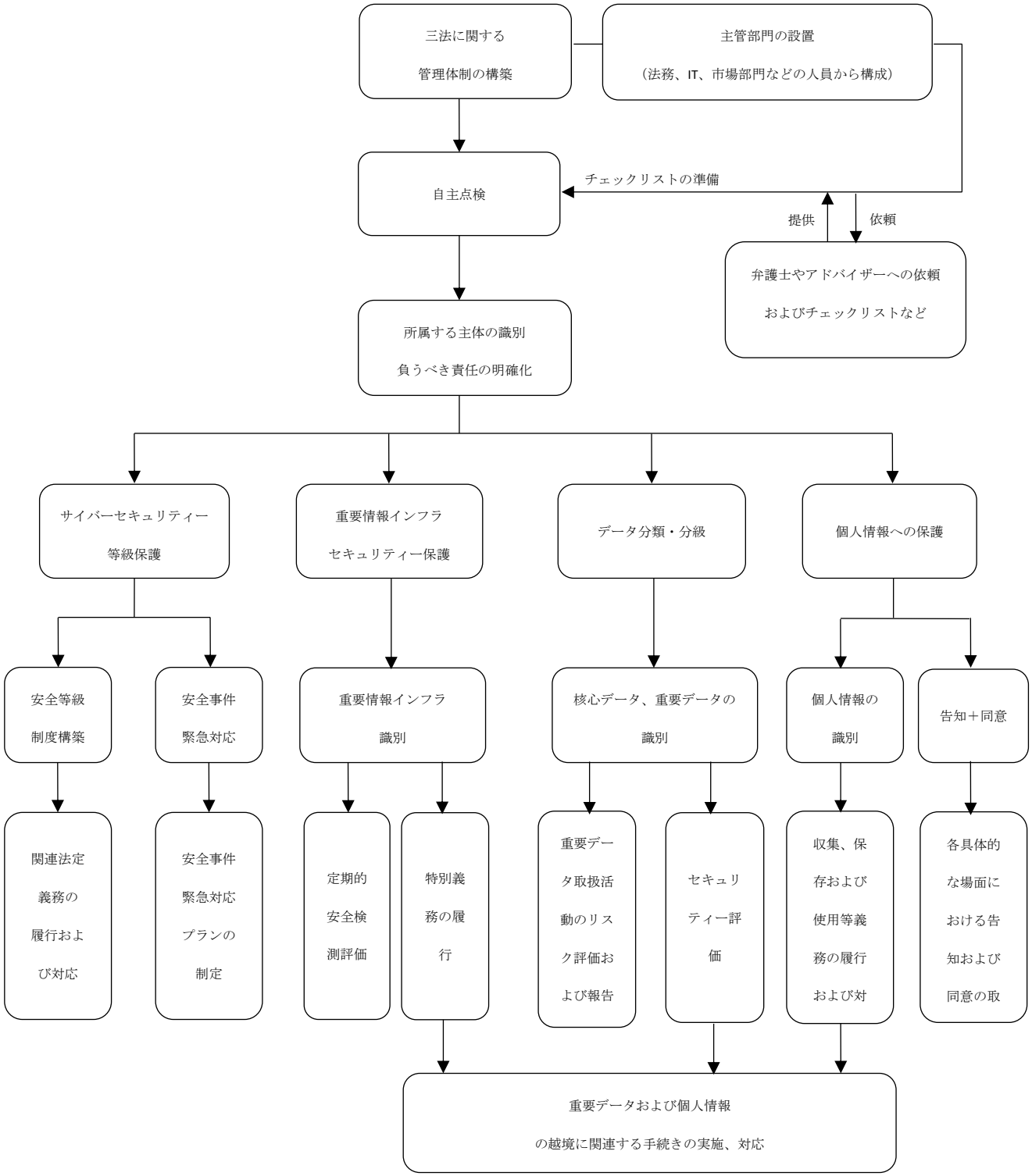
影響評価	• 個人情報を利用した自動的な意思決定の実施； • **個人情報の取扱いの委託、個人情報の第三者への提供、および個人情報の公開；** • **中国国外に向けた個人情報の提供；** • その他の個人に重大な影響を及ぼす個人情報の取扱行為。	あり、かつ、それに基づく判断が自然人に関して法的効果を発生させ、または、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面の体系的かつ広範囲な評価の場合； • 第 9 条第 1 項に規定する特別な種類のデータまたは**第 10 条に規定する有罪判決および犯罪行為と関連する個人データの大規模な取扱いの場合；** • **公衆がアクセス可能な場所の、システムによる監視が大規模に行われる場合。**
	評価の内容	
	第 56 条第 1 項 • 個人情報の取扱目的、取扱方法等の合法性・正当性・必要性； • 個人の権益への影響および安全リスク； • 採択したセキュリティー保護措置の合法性および有効性ならびにリスクの程度の相応性。	第 35 条第 7 項 • 予定されている取扱業務および取扱いの目的の体系的な記述。該当する場合、管理者の求める正当な利益を含む； • その目的に関する取扱業務の必要性および**比例性**の評価； • 第 1 項で定めるデータ主体の権利および自由に対するリスクの評価； • データ主体およびほかの関係者の権利および正当な利益を考慮に入れた上で、個人データの保護を確保するための、および、本規則の遵守を立証するための、保護措置、安全管理措置および仕組みを含め、リスクに対処するために予定されている手段。
	関連報告・記録の保存期限	
	3 年	規定なし

セキュリティーインシデント発生時の通知義務	当該義務の履行が求められる場合	
	第 57 条第 1 項 個人情報の漏えい、改ざん、または紛失が発生した場合	第 34 条第 1 項 個人データ侵害が自然人の権利および自由に対する高いリスクを発生させる可能性がある場合
	例外的な状況	
	第 57 条第 2 項 個人情報取扱者が措置を採択して情報の漏えい、改ざん、または紛失によりもたらされる損害を有効に回避することのできるときは、個人情報取扱者は、個人に通知しないことができる。	第 34 条第 3 項 第 1 項で定めるデータ主体に対する連絡は、以下の条件に合致する場合、これを要しない： (a)管理者が適切な技術上および組織上の保護措置を実装しており、かつ、当該措置、特に、暗号化のような、データに対するアクセスが承認されていない者にはその個人データを識別できないようにする措置が、個人データ侵害によって害を受けた個人データに対して適用されていた場合； (b)**管理者が、第 1 項で定めるデータ主体の権利および自由に対する高いリスクが具体化しないようにすることを確保する事後的な措置を講じた場合；または、** (c)**それが過大な負担を要するような場合。**
	通知の内容	
	第 57 条第 1 項 • 個人情報の漏えい、改ざん、または損失の種類、理由、および考えられる危害が発生したこと、または発生する可能性があること • 個人情報取扱者が講じた是正措置、および個人が危害	第 33 条第 3 項・第 34 条第 2 項 • 可能な場合、関係するデータ主体の類型および概数、ならびに、関係する個人データ記録の種類および概数を含め（個人に対して通知を行う場合、これが必要ではない）、個人データ侵害の性質

	を軽減するために講じることができる措置 • 個人情報取扱者の連絡先	• データ保護オフィサーの名前および連絡先、または、より多くの情報を入手することのできるほかの連絡先； • その個人データ侵害の結果として発生する可能性のある事態 • 適切な場合、起こりうる悪影響を低減させるための措置を含め、その個人データ侵害に対処するために管理者によって講じられた措置または講ずるように提案された措置
ゲートキーパーズ条項	第58条 **重要なインターネットプラットフォームサービスを提供し、多数のユーザーがおり、および複雑な種類の個人情報取扱者**は、以下の義務を履行するものとする。 （1）国内規制に基づく個人情報保護コンプライアンス体制の構築・改善、個人情報の保護を統括する外部会員を中心とした独立組織の設置。 （2）公開性、公平性、正義の原則に従い、プラットフォームのルールを策定し、プラットフォーム上の製品またはサービスプロバイダーによる個人情報の処理基準および個人情報を保護する義務を明確にすること。 （3）法律および行政規則に重大な違反をした個人情報を扱うプラットフォームにおいて、製品またはサービスプロバイダーへのサービスの提供を停止する。 （4）個人情報保護に関する社会的責任報告書を定期的に発行し、社会的監督を受け入れること。	規定なし （「Proposal for a Regulation on Digital markets act」にはある）

法的責任		
	「個人情報保護法」	**GDPR**
公益訴訟	第 70 条 個人情報取扱者が本法の規定に違反して個人情報を取り扱い、多くの個人の権利および利益を侵害する場合、人民検察院、法律で指定された消費者団体、および州サイバースペース管理局によって決定された組織は、本法に従い、人民法院に訴訟を提起できる。	規定なし
罰金	第 66 条第 2 項 最高で人民元 5000 万元、または前年度の売上高の 5%に相当する金額（両者のうち高いほうを賦課）。	第 83 条第 5 項 最高で 2000 万ユーロ、または前年度のグローバル総売上高の 4%に相当する金額（両者のうち高いほうを賦課）。

別紙２：三法における法的義務の点検プロセスのフロー



別紙３：三法に関するコンプライアンスに対するチェックリスト（簡約版）

1. 企業基本状況チェック

1.1 業種は何か？（複数選択可能）
□ ①製造業
□ ②情報伝達、コンピュータサービス、ソフトウェア業
□ ③卸売および小売業
□ ④金融、保険業
□ ⑤賃貸借およびビジネスサービス業
□ ⑥その他の業種

1.2 日常の生産経営活動においてインターネットを使用（または運営）しているか否か？（複数選択可能）
□ ①自社のウェブサイトがあり、インターネット情報サービス届出を行っている。
□ ②ウェブサイト・プラットフォームを確立し、付加価値電信経営許可証を取得している。
□ ③内部において LAN を確立している。
□ ④産業制御システムを通じて生産を管理している。
□ ⑤インターネットアクセスサービスを提供している。
□ ⑥インターネット関連製品、またはサービスを提供している。
□ ⑦インターネットを使用せず、インターネットにも関連性がない。

1.3 内部においてサイバーセキュリティーに関連する事務を専門に担当する管理部門を設置しているか否か？
□ ①既に専門の管理部門を設置している。
□ ②専門の管理部門を設置しておらず、IT、法務等の人員が担当している。
□ ③専門の管理部門を設置しておらず、専門に担当する人員もいない。

上記 1.1、1.2、1.3 は、企業の基本状況についてのチェックである。企業が 1.2 の①～⑥に該当する場合には、「サイバーセキュリティー法」の規制対象となる可能性が高い。規制対象の分類、各主体の法的義務については、本マニュアルの二（一）、三（一）を参照。また、企業が 1.1 の①、②、④に該当する場合も、上記部分を参照する必要があるほか、本マニュアルの「六、アクションアイテムの推進―各業種の法的義務の整理」も要参照。

2. サイバーセキュリティーの保護チェック

2.1 サイバーセキュリティー管理制度を確立しているか否か？（複数選択可能）
□ ①サイバーセキュリティー責任者を設置し、サイバーセキュリティー保護責任を具現化している。

□ ②コンピュータウイルス、インターネット攻撃等、ネットワークの安全に脅威をもたらす行為を防止する技術的措置を講じている。
□ ③インターネット運営状態、サイバーセキュリティー事件をモニター・記録する技術的措置を講じている。
□ ④データ分類、重要データバックアップ、暗号化等の措置を講じている。
□ ⑤システムログ、ユーザーログを少なくとも 6 カ月保管している。
□ ⑥上記措置について、既に実施している。
□ ⑦上記措置について、まだ実施していない。

2.2 ユーザーのためにインターネットアクセス手続きをし、ユーザーのために情報発布、インスタントメッセージ等のサービスを提供し、ユーザーと協議書を締結し、サービスの提供を確認する際に、実名制による検証を行っているか否か？
□ ①実名制による検証を行っている。
□ ②実名制による検証を行っていない。

2.3 ネットワークの運営過程において発生する可能性のある突発事件について、緊急対応プランを制定しているか否か？
□ ①既に制定が完了している。
□ ②既に制定を開始しているが、まだ完了していない。
□ ③まだ制定を開始していない。

上記 2.1 は、サイバーセキュリティー等級保護制度の実施状況についてのチェックである。具体的には、本マニュアルの一（四）、三（二）1 を参照。 上記 2.2 は、ネットワーク運営者による実名制の実施状況についてのチェックである。実名制を実施していない場合における罰則については、本マニュアルの一（四）を参照。 上記 2.3 は、サイバーセキュリティー事件緊急対応策の制定状況ついてのチェックである。具体的には、本マニュアルの一（四）、三（二）1 を参照。

3. 重要情報インフラ運営チェック

3.1 運営・管理するインターネット施設または情報システムの機能が破壊され、もしくは失われ、またはそのデータが漏えいした場合において、国の安全、国の経済、人民の生活、公共の利益が著しく損なわれる可能性があるか否か？
□ ①国の安全、国の経済、人民の生活、公共の利益に重大な脅威をもたらす。
□ ②国の安全、国の経済、人民の生活、公共の利益に脅威をもたらさない。
□ ③確定不可能。その可能性は存在する。

3.2 業種が次に掲げる分野にかかわるか否か？（複数選択可能）
□ ①政府機関、エネルギー、金融、交通、水利、衛生医療、教育、社会保険、環境保護、公共事業等
□ ②電信ネットワーク、ラジオ・テレビネットワーク、インターネット等の情報ネットワーク、クラウドコンピューティング、ビッグデータその他の大型公共情報ネットワークサービス

□ ③国防、科技工業、大型機械設備、化学工業、食品薬品等にかかわる科学研究・生産
□ ④ラジオ・テレビ局、通信社等のメディア

上記 3.1、3.2 は、重要情報インフラ運営者に属するか否かについてのチェックである。企業が 3.1 の①に該当する場合には、重要情報インフラ運営者と認定される可能性が極めて高い。企業が 3.1 の②③を選択し、ただ 3.2①②③④に該当する場合には、重要情報インフラ運営者と認定される可能性がある。具体的には、本マニュアル二（一）3 を参照。

4.データセキュリティーの保護チェック

4.1 全過程のデータセキュリティー管理制度を制定しているか否か？全過程とは、データ収集、保存、加工、利用、伝送、開示、削除というデータセキュリティーのライフサイクを指す。
□ ①既に制定が完了している。
□ ②既に制定が完了しているが、「データセキュリティー法」に基づき調整する必要がある。
□ ③まだ制定を開始していない。

4.2 データセキュリティー教育・トレーニングを定時に実施しているか否か？
□ ①実施しており、かつ関連記録も保存している。
□ ②実施しているが、関連記録は残っていない。
□ ③今まで実施したことはない。

4.3 データセキュリティーを保障するために、相応する技術措置およびその他の必要措置を講じているか否か？
□ ①技術措置を講じている。
□ ②まだ技術措置を講じていない。

4.4 データ取扱活動を行うときにリスクのモニタリングをしているか否か？
□ ①モニタリングをしている。
□ ②モニタリングをしていない。

上記 4.1、4.2、4.3、4.4 は、データ取扱者の義務についてのチェックである。データ取扱活動を行う企業は、上記 4.1①、4.2①、4.3①、4.4①の義務を履行しなければならない。具体的には、本マニュアル三（三）を参照。

5. 重要データ処理チェック

5.1 貴社の収集・発生するデータには、一旦漏えいしてしまうと、国の安全、国の経済、人民の生活、公共の利益が著しく損なわれる可能性があるデータがあるか否か？
□ ①ある。
□ ②ない。

5.2　上記 5.1 に言及されるデータを収集する際の主なルートは何か？（複数選択可能）
□　①自らの生産または経営の過程において形成される。
□　②登録ユーザーから収集する。
□　③第三者から直接購入する。
□　④第三者との共有により確認する。
□　⑤その他のルート

5.3 上記 5.1 に言及される収集・発生するデータ（もしあれば）は、どこで保管しているか？
□　①中国大陸地区。
□　②香港・マカオ・台湾地区。
□　③国外。

上記 5.1、5.2 は、重要データに属するか否かについてのチェックである。具体的には、本マニュアルの二（二）3 を参照。 上記 5.3 は、重要データを保存する地域についてのチェックである。企業は重要データの保存規則を遵守するものとする。具体的には、本マニュアルの四（二）2 を参照。

6.個人情報処理チェック

6.1 経営過程においてユーザーの個人情報を収集することがあるか否か？
□　①収集する。
□　②収集しない。

6.2 個人情報を収集する際の主なルートは何か？（紙、We-chat など媒体を問わない。）（複数選択可能）
□　①本人から直接収集する。
□　②ネット登録ユーザーから収集する。
□　③第三者から直接購入する。
□　④本人ではない第三者から提供された。
□　⑤その他のルート

6.3 収集する個人情報に、次に掲げる個人機微情報が含まれるか否か？
□　①個人財産情報（銀行口座番号、識別情報（合い言葉）、預金情報、不動産情報、クレジット情報、信用調査情報、取引および消費記録、フロー記録等）
□　②個人健康生理情報（病状、入院記録、医師の指示、検査報告等の疾病・医療等により生ずる関連する記録）
□　③個人生物識別情報（個人遺伝子、指紋、声紋、掌紋、耳介、虹彩、顔の特徴等）
□　④個人身分情報（身分証、軍人証、パスポート、運転免許証、社員証、出入証、社会保険カード、居住証等）

□ ⑤インターネット身分識別情報（システムアカウント、電子メールアドレス、関連パスワード等）
□ ⑥その他の情報（個人電話番号、性的指向、婚姻歴、宗教信仰、未公開の違法犯罪記録、通信記録および内容、行動追跡情報、ウェブページ閲覧記録、宿泊情報、位置特定情報等）
□ ⑦上記情報がいずれも含まれない。

6.4 ユーザーの個人情報を収集する際に、ユーザーに対し告知義務を履行しているか否か？
□ ①告知義務を履行している。
□ ②告知義務を履行していない。

6.5 ユーザーの個人情報を収集する際に、ユーザーの同意を得ているか否か？
□ ①明示の同意（すなわち、完全に状況について理解した上で明確に示す同意）を得ている。
□ ②黙示の同意（すなわち、同意するか否か明確には表明していない黙認）を得ている。
□ ③同意を得ていない。

6.6 ユーザー向けプライバシーポリシーにおいて、個人情報収集・保管・使用の目的・方式・範囲について明確に定めているか否か？（複数選択可能）
□ ①既に明確に定めている。
□ ②目的・方式・範囲が明確化されていない。
□ ③プライバシーポリシーを制定していない。

6.7 個人情報の接触者は制限されているか否か？
□ ①制限されている。
□ ②制限されていない。

6.8 個人情報に対し、暗号化等の安全措置が取られているか否か？
□ ①取っている。
□ ②取っていない。

6.9 取得した個人情報を、会社以外の個人・法人に提供したことがあるか否か？
□ ①ある。
□ ②ない。

6.10 6.9①あるの場合、受領者の名称・氏名および連絡方法、取扱いの目的・方法、ならびに個人情報の種類を個人に告知したか否か？
□ ①告知した。
□ ②告知していない。

6.11 中国国内において収集する個人情報をどこで保管しているか？
□ ①中国大陸地区
□ ②香港・マカオ・台湾地区
□ ③国外

6.12 中国国内において収集する個人情報が越境されることがあるか否か？
□ ①ある。
□ ②ない。

6.13 中国国外に個人情報を提供する前に、事前に個人情報保護影響評価を行い、取扱状況に対して記録することがあるか否か？
□ ①ある。
□ ②ない。

上記 6.1、6.2 は、個人情報の収集およびそのルートについてのチェックである。企業が 6.2 の③、④に該当する場合には、第三者が個人情報の収集について 6.4、6.5 の同意および告知義務を履行するか否かについて、また、個人情報の主体が個人情報の譲渡、共有に対し同意するか否かについて、確認する必要がある。
上記 6.3 は、個人機微情報に属する個人情報があるか否かについてのチェックである。企業は、個人機微情報を収集する場合には、情報の主体の明示同意を得なければならず、個人機微情報を保管する場合には、暗号化措置を講じなければならない。具体的には、本マニュアル五（一）を参照。
上記 6.4、6.5 は、個人情報の収集規則についてのチェックである。企業が個人情報を収集する場合には、告知および同意の義務を履行しなければならない。具体的には、本マニュアル一（四）、三（二）2②、五（一）を参照。
上記 6.7、6.8 は、個人情報取扱者の義務についてのチェックである。個人情報の取扱者は、授権を経ていないアクセスおよび個人情報の漏えい・改ざん・紛失を防止するために、相応措置を採択しなければならない。本マニュアル三（五）を参照。
上記 6.9、6.10 は、個人情報の取扱者が、自らが取り扱う個人情報をその他の個人情報取扱者に提供するときについてのチェックである。個人情報の取扱者は、自らが取り扱う個人情報をその他の個人情報取扱者に提供するときは、受領者の名称・氏名および連絡方法、取扱いの目的・方法、ならびに個人情報の種類を個人に告知し、個人の単独の同意を取得しなければならない。本マニュアル四（三）2②を参照。
上記 6.11、6.12 は、個人情報の中国国内における保管および越境の制限についてのチェックである。企業は、上記 3.1、3.2 において重要情報インフラ運営者に該当する場合には、6.7 の①、6.8 の①の義務を履行しなければならない。具体的には、本マニュアル四（四）3 を参照。

7. ネットワーク製品およびサービスチェック

7.1 生産するネットワーク製品（サイバーセキュリティー製品を含む）が国の標準の強制性要求に適合しているか否か？

□ ①適合している。
□ ②適合していない。

7.2 生産するネットワーク製品（サイバーセキュリティー製品を含む）について、必要な安全認証または安全検査測定を取得しているか否か？
□ ①取得している。
□ ②取得していない。

7.3 ユーザーの発布する情報に、法令により発布・送信が禁止されている情報を発見した場合において、ただちに措置を講じて当該情報の拡散を防止し、かつ、関連記録を保管することができるか否か？
□ ①できる。
□ ②できない。

上記 7.1、7.2、7.3 は、ネットワーク製品およびサービス提供者の義務を履行したか否かについてのチェックである。ネットワーク製品およびサービス提供者に該当する企業は、上記 7.1①、7.2①、7.3①の義務を履行しなければならない。具体的には、本マニュアル三（一）5 を参照。

別紙４：Q&A

Q1. 中国国内サーバーへのデータ保存は、いつから実施しなければ罰則が適用されるのか。

現時点では、重要情報インフラ運営者は中国国内で重要データ/個人情報を保存する必要があり、そうでなければ、処罰を受ける可能性がある。重要情報インフラ運営者に該当するか否かについては、業種の主管または監督部門の認定が必要であるが、現時点では法的に明確になっていない。

また、「個人情報と重要データ越境セキュリティー評価弁法（意見募集稿）」および「個人情報越境安全評価弁法（意見募集稿）」が実施された後においては、一般的なネットワーク運営者であっても、重要データ/個人情報の海外送信について規制されるようになる。上記の法律規定が正式に発効した後、関連する義務を履行しない場合には、処罰を受けると思われる。

Q2. 個人情報や重要データの海外移転制限があるが、従業員の個人情報も対象なのか？当社は中国国内に子会社（中国企業）を設立し、OA システムを通じて現地従業員の個人情報を収集する可能性があるが、何か留意点はあるか。

中国の「サイバセキュリティー法」および国家標準「個人情報安全規範」によれば、子会社（中国企業）では、その従業員に対し個人情報を第三者に提供する旨を通知し、さらに、従業員本人の同意を取る必要がある。

また、意見募集稿である「個人情報および重要データ海外送信安全評価弁法」および「個人情報越境安全評価弁法（意見募集稿）」において、ネットワーク運営者は個人情報の海外移転制限を受けるようになるので、当該法律の動向に留意し、可能であれば、中国国内で収集した従業員の個人情報を日本のサーバーに保存しないことが推奨される。

Q3. 当社は日本の外部顧客のヘルプデスク業務を受託している。顧客先の社員から、パソコンの不具合の連絡を受け、日本のシステムサーバーを確認し、不具合を直す業務において、サイバーセキュリティー法上、対応すべきことはあるか。

「サイバーセキュリティー法」においては、個人情報および重要データの海外送信が規制されている。厳密に言えば、中国国外から中国国内のパソコンにアクセスすることによって、個人情報および重要データを獲得する場合には、「海外送信」に該当する可能性がある。一方、単純にパソコンの不具合を直すことだけで、中国で収集された個人情報および重要データに対し、何らかの方法をもって、外国への送信を実現することが

なければ、特にサイバーセキュリティー法の制限を受けないと思われる。

Q4. 現在、当社（中国に法人は無い）は中国向けサイトを香港サーバーを使用して運営しているが、サービスに関する問い合わせやアフターフォローのため、メールアドレスと氏名を取得したい。プライバシーポリシーを明記すれば中国からメールアドレスを取得するのは可能か。

外国企業が香港にあるサーバーを利用し、中国国内の個人情報を収集する際には、現在の法規制からみると、プライバシーポリシーを明記した上で、ユーザーが自ら投稿する形でメールアドレスと氏名、またはメールアドレスのみを収集することは可能である。ただし、顧客情報の取扱いに関するユーザーの事前同意を取得し、顧客情報の保管・利用に当たっては顧客情報を匿名化処理することが妥当だと考えられる。

一方、2019年6月13日に公布された「個人情報越境安全評価弁法」の意見募集稿においては、GDPRの第27条を参照し、中国国外の機構が経営活動中にインターネットを利用して中国国内のユーザーの個人情報を収集する場合には、代表者または代理機構を通じて、中国でネットワーク運営者の責任および義務を履行する必要があると要求されている。よって、今後の「個人情報越境安全評価弁法」の進捗状況に留意する必要がある。

Q5. サイバーセキュリティー等級と情報システム安全等級の関係は何か。

「情報安全等級保護管理弁法」で情報システムの安全等級が規定されている。これを基礎とし、「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）」、および関連の国家標準においても、サイバーセキュリティー等級の概念が提起されており、具体的な規定が設けられている。サイバーセキュリティー等級保護制度においては、情報システム安全等級保護制度の多くの要求が延長継続されており、二者の主管機関、等級決定標準、業務の流れ等の面において、いずれも非常に相似している。「サイバーセキュリティー等級保護条例」の発効後、サイバーセキュリティー等級保護制度と情報システム安全等級保護制度が並行するのか、代替的なのか、それとも相互に補い合うのかについては、関連部門において今後さらなる明確化が行われる。

Q6. サイバーセキュリティー等級については、たとえば、レベル1であっても管轄当局によるレビューや公安機関への審査請求などが必要となるのか。

「サイバーセキュリティー等級保護等級決定ガイドライン（意見募集稿）」の付録Aに基づき、レベルが1級に該当する場合には、管轄当局によるレビューや公安機関への審査請求は必要ではないものの、レベルが2級以上の場合には、当該フローが必要にな

る。また、この点については最新の「サイバーセキュリティー等級保護条例」の意見募集稿（2018年6月27日公表）中にも同じルールが定められている。

Q7．重要データの判断基準は何か。

2019年5月28日に公布された「データ安全管理弁法（意見募集稿）」に基づき、重要データとは、漏えいすると、国家の安全、経済の安全、社会の安定、公共の健康と安全に直接影響する恐れのあるデータ（たとえば、未公開の政府の情報、大きな面積の人口、遺伝子・健康、地理、鉱産物資源など）をいう。ただし、一般的に企業の生産管理・内部管理情報、個人情報等は重要データに該当しないとされている。

ほかに、2021年9月30日に公布された「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9条によると、危害の程度が以下のいずれか該当するデータは重要データである。（危害の程度がこれよりさらに上回っている場合、核心データに該当する。）

① 政治、国土、軍事、経済、文化、社会、科学技術、ネットワーク、生態、資源および原子力安全等に対する脅威を成し、中国国外の利益、生物、宇宙、極地、深海、人工知能等の重点分野における国家安全に関連するデータセキュリティーに影響するもの。
② 工業、通信業界の発展、生産、運行および経済利益等に影響をもたらすもの。
③ 重大データセキュリティー事件または生産安全事故を引き起こし、公共利益または個人・組織の合法的権益に深刻な影響をもたらし、その社会的悪影響が大きいもの。
④ カスケード効果を著しく引き起こし、その影響の範囲が複数の業界、区域もしくは業界内の複数の企業におよび、または業界の発展、技術の進歩、業界の状況等に対して深刻な影響をもたらすもの。
⑤ データの復元または悪影響の解消のための代償が大きいもの。
⑥ 業界の監督管理部門が評価により確定するその他の重要データ。

また、各業界・領域につき、国家標準である「情報安全技術 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）」においては、27業種の重要データが確定されており、各業界・領域の主管部門は業種の具体的な状況を踏まえ、自らの業界・領域の重要データの範囲を確定することができる。

Q8．中国のデータセキュリティー法と輸出管理法との間の関係性は何か。

「データセキュリティー法」第25条は「国は、国家の安全・利益の保障、国際的な義務の履行に係り、または規制対象品目に該当するデータに対し、輸出管理を法により

実施する。」と規定し、ならびに「輸出管理法」第2条2項は「管理品目には、当該品目にかかわる技術資料などのデータが含まれる。」と規定している。この二つの規定に照らし、以上の条件を満たすデータは「データセキュリティー法」と「輸出管理法」を同時に適用することが明白である。

「輸出管理法」第12条に基づき、次の状況に属する品目のデータは輸出許可の申請が必要となる。

① 輸出管理リスト（中国輸出禁止輸出制限技術目録（2020年改定版））に掲載されている。
② 臨時管理品目となっている。
③ ①または②に属する品目以外の貨物・技術・サービスに、以下のリスクが存在している恐れのある状況を輸出事業者が知り、もしくは知り得べきであり、または、輸出管理部門の通知を受けた。
   - ✓ 国家の安全・利益に対する脅威。
   - ✓ 大規模殺傷性武器およびその運輸・搭載手段の設計・開発・生産・利用への使用。
   - ✓ テロリズム目的への使用。

Q9. サイバーセキュリティー等級保護の早期取得は重要であるか。

「サイバーセキュリティー法」第21条および「データセキュリティー法」第27条に基づき、インターネット等の情報ネットワークを利用し、データの取扱活動を行うときに、ネットワーク運営者は、サイバーセキュリティー等級保護制度の要求に従い、データの安全を保障する義務を負っている。すなわち、等級保護の取得は、既に「データセキュリティー法」における法定の義務の一環となっている。故に、サイバーセキュリティー等級保護の早期取得の重要性は、以前よりさらに高まっている。

特に、自動車業界など特定分野の企業に対しては、データセキュリティーの管理のための関連規定が既に制定され、サイバーセキュリティー等級保護等の制度の実施が明確に義務化された（例えば、「自動車データセキュリティー管理若干規定」第5条）ので、早期の取得が推奨されている。

Q10. サイバーセキュリティー法、データセキュリティー法、個人情報保護法の諸規制を踏まえた上で、製造、医療、金融、インターネットなどの業界に属する企業にとってのそれぞれの注意点は何か。

本マニュアルの「六、アクションアイテムの推進―各業種の法的義務の整理」を参照のこと。

Q11.「個人情報保護法」の下での従業員個人情報の取扱上の注意点は何か。

従業員個人情報の取扱にあたり、「個人情報保護法」の規定に基づき、その個人情報をマッピングする上で、具体的な対応策をとることが推奨されている。

従業員個人情報のマッピングにつき、第一に、「個人情報保護法」第13条第1項第（2）号によれば、企業は法により制定された労働規約と制度および締結された集団契約に基づき、人的資源管理を実施する必要がある場合において、従業員の同意を要せずにその個人情報を取り扱うことができる。故に、当該従業員の同意を要せずに取り扱うことのできる従業員の個人情報と、従業員の同意を取得後に初めて取り扱うことのできる個人情報を明確に分離しなければならない。

第二に、「個人情報保護法」には、個人機微情報に対する特殊規定があるため、従業員を認識することのできる個人機微情報（指紋、顔情報などを含む生体認証情報、健康情報、銀行口座情報など）を識別し、それに注意を払わなければならない。

第三に、企業の業務における特別な状況（例えば、共同の取扱い、取扱委託、第三者への提供など）が存在するか否かを把握し、従業員個人情報保護の方針を確定することが必要である。

また、具体的な対応策として、目下の重要性・緊急性を踏まえ、まず従業員個人情報保護の方針に従い、従業員用の個人情報取扱同意書を作成・更新しなければならない。ほかに、従業員の個人情報の保護にかかわる制度、および個人情報セキュリティーインシデント緊急対応プラン、従業員による関連の権利（同意撤回権、取扱拒絶権など）の行使に関する制度などの制定・完全化、ならびに必要な技術的措置の採択（個人情報の分類・分級管理など）、個人情報のセキュリティーの確保、従業員に対するコンプライアンス研修の実施も不可欠である。

Q12. 主管部門の現場調査への対応策として、何を行うことができるか。

主管部門による現場調査が行われる場合、冷静沈着かつ専門的な対応が非常に重要である。現場調査にあたり、政府の調査官に対し、以下のような対応が推奨されている。

① 指示に従い行動すること。
② 礼儀正しく、友好的な姿勢を示すこと。
③ 従業員から調査官への意図的な、または過失による妨害を回避すること。
④ 調査官の懸念事項の把握を目的として、可能な限り多くの情報（調査事項など）を調査官から入手すること。
⑤ 調査への全面的な協力の姿勢を強調すること。
⑥ 調査官の質問に対して、正直に応答すること。

⑦ 調査官との会話内容を記録し、または（記録が不可の場合において）ヒアリング終了後、時宜に適し、記録すること（ヒアリング中の関連内容を回想し、質問と回答の具体的な内容を書き留めておくことが必要)。

別紙５：サイバーセキュリティー法、データセキュリティー法の執行状況

近年における「サイバーセキュリティー法」、「データセキュリティー法」の違反により行政処罰を受けた一部の代表的な案例について、以下のとおり整理する。

日付	担当機関	案件の詳細	処理結果
2021年10月	深セン市公安部門	深セン市のある科学技術有限公司が使用しているウェブサイトにおいて、リスクの高いセキュリティーホールおよび隠しリンクが存在し、かつ適時のメンテナンスが行われていなかった。	当該企業に対して警告が下され、期限付きの是正が命じられた。
2021年10月	工業・情報化部情報通信管理局	「驢媽媽旅遊」「喜茶GO」「図吧導航」「掌心天気」など96のAPPが国慶節の前日に検査を受け、是正命令を受けたにもかかわらず、期限要求のとおりに是正を完成しなかった。	削除命令
2021年8月	浙江省App による個人情報の違法な収集・使用に関する特別対策作業チーム	「萌菌大作戦」「決戦！平安京」「彼隣」「掌上個税」など85のAPPがユーザー個人情報の収集・使用規則の未開示、個人情報の漏えいを引き起こす恐れのあるセキュリティーホールの存在、第三者への個人情報の個人による同意のない提供などの問題があることが明らかになった。	是正命令
2021年5月	深セン市公安部門	深セン市のあるインターネット企業が運営しているAPP「盗墓OL」には、プライバシーポリシーがなかった。ほかに、当該APPは初回の実行においてユーザーのプライバシーポリシーに対する同意を得ずに、通話履歴などの読み取り、外部ストレージへのアクセスの許可を求めていた。	当該企業に対して罰金1万元の行政処罰が下され、期限付きの是正が命じられた。
2020年12月	蘇州市公安部門	蘇州市のある企業が社内のサイバーセキュリティー管理制度および操作プロ	当該企業に対して警告が下された。

日付	担当機関	案件の詳細	処理結果
		セスを制定する義務を履行しなかったため、設立し運営しているウェブサイトが改ざんされた。	
2020年6月	上海市通信管理局	上海市のある文化マスメディア企業が運営・管理する「墨魚旅行」というAPPは法規に違反し、個人情報を収集・使用し、個人情報の収集・使用規則を公開しておらず、個人情報の収集・使用の目的・方法・範囲を明示しておらず、ユーザーの同意を得ずに個人情報を収集・使用した。	同社に対して警告が下され、期限付きの是正が命じられた。
2020年5月	杭州市公安部門	杭州市のある食品飲料企業がウイルスやネットワークへの攻撃・侵入などのサイバーセキュリティーを侵害する行為に対する技術的な防止対策を講じていなかった。その結果、同社のweblogicサーバーが改ざんされ、システムページにおいて不適当な言論が表示された。	同社に対して、罰金1万元の行政処罰が下された。
2019年5月	宿遷市公安部門	宿遷市のあるインターネット掲示板は、違法な情報の掲載により公安機関から二度是正命令を受けた後も依然として有効な管理・技術措置を講じず、違法な情報の処分義務を履行せず、掲示板で頻繁に大量の銃・暴力・インターネット詐欺にかかわる違法な情報が生ずる状況を引き起こしていた。	同インターネット掲示板の運営会社に対して罰金10万元、直接の責任者に対して罰金1万元の処分、ウェブサイトの暫時的な閉鎖と期限付きの是正が命じられた。
2019年5月	南京市公安部門	南通市のある水利工事管理所にかかわるシステムが公安部と水利部の国家重要情報インフラリストに追加された。検査を経たところ、そのコンピューターシステムには三件の高いリスクのバグが存在しており、インターネット運営に関連する内部安全管理制度と操作規程を	同水利工事管理所に対して警告が下され、期限付きの是正が命じられた。

日付	担当機関	案件の詳細	処理結果
		制定しておらず、コンピュータウイルス、インターネット攻撃、インターネット侵入等を防止するための技術措置を有効に講じていないことが分かった。	
2019年5月	重慶市公安局サイバーセキュリティー総隊	重慶市永川のある病院のサーバーが突如ダウンし、病院の業務が全面的に停止した。人民警察と技術専門家の調査と事実検証を経たところ、同病院がサイバーセキュリティー等級保護制度の要求のとおりにセキュリティー保護義務を履行していないことが分かった。	同病院に対して罰金1万元の処分、直接の責任を負っていた主管者に対して罰金 5,000 元の行政処罰が下された。
2019年4月	南京市公安部門	ある文化マスメディア企業が虚偽の方法で、インターネット利用者を引き付けて同社が運営する数件のウィーチャット公式アカウントを登録させ、氏名、連絡先、住所等の入力を要求し、大量の個人情報を違法に取得し、これらの個人情報をデータ資料として会社の運営分析に用いていた。	同社に対して罰金1万元、会社の法定代表者とほか 2 名の関係者に対してそれぞれ罰金 1,000元の処分。
2019年4月	無錫市公安部門	無錫市のある上場会社が使用している事務システムとウェブサイトにおいて、必要な保護措置を講じておらず、会社が保存しているユーザー個人情報が極めて容易にハッカーによる窃取を受ける状態を引き起こし、個人情報が法により受ける保護の権利を侵害していた。	同社に対して警告が下され、期限付きの是正が命じられた。
2019年4月	連雲港市公安部門	連雲港市のあるインターネット企業がインターネットサービスを提供する過程において、サイバーセキュリティー保護義務を履行せず、ネットワーク運行状態とサイバーセキュリティー事件の監視・測定・記録の技術措置を講じておら	同社に対して罰金5万元、法定代表者に対して罰金2万元、サイバーセキュリティー等級保護制度の実施が命じら

日付	担当機関	案件の詳細	処理結果
		ず、規定とおりに関連のインターネット上のログファイル等を保存していなかった。3月22日に連雲港の警察は法により同社に期限付きの是正命令を下し、警告を与えた。4月3日には再検査中、同社が依然として是正を拒んでいる状況が明らかになった。	れた。
2019年3月	泰州市公安部門	江蘇省泰州市のある公的機関の集中モニターシステムがハッカーの攻撃に遭い破壊された。捜査を経たところ、当該機関は過去に安全面の潜在リスクの存在と、サイバーセキュリティー等級保護制度の未実施により是正命令を受けておらず、是正期間の満了後に有効な管理措置と技術防護措置を講じていないことが分かった。	同機関に対して罰金6万元、関連の責任者に対して罰金2万元の処分、同機関に機械停止による是正、等級決定の届出、是正状況の測定評価等のサイバーセキュリティー等級保護業務の実施が命じられた。
2019年2月	瀘州市公安部門	四川省瀘州市のある企業のインターネットサーバーがウイルスの襲撃を受け、多くの事務用コンピュータが使用不能になった。調査を経たところ、同社が内部安全管理制度と操作規程を制定しておらず、サイバーセキュリティー責任者を確定させず、インストールしたアンチウイルスソフトとファイアウォールに問題が存在しており、規定とおりに関連のインターネット上のログファイルを保存していないことが分かった。	警告・是正命令
2018年12月	工業・情報化部サイバーセキュリティー管	蘇州市のある企業のウィーチャット・ミニプログラムにおいて、ユーザー個人情報の収集・使用規則が公示されておらず、一部のサービス誓約内容が履行されていない問題が存在していた。	是正命令

日付	担当機関	案件の詳細	処理結果
	理局		
2018年11月	国家ネットワーク情報弁公室	百度、テンセント、新浪、今日頭条、捜狐、網易、UC頭条、一点資訊、鳳凰、知乎等10社の著名なインターネット企業の携帯電話ユーザー端末上において、低俗性・わいせつ性にかかわり法律法規に違反している広告の掲載等の状況が存在していた。	是正命令
2018年11月	工業・情報化部サイバーセキュリティー管理局	62社のインターネット企業の65項目のインターネットサービスに対して抽出検査が行われ、12社のインターネット企業がユーザー個人情報の収集・使用規則を公示しておらず、情報の照会・修正経路を告知せず、アカウント取消サービスを提供していない問題の存在が明らかになった。	是正命令
2018年10月	北京市ネットワーク情報弁公室	360doc 個人図書館がプラットフォーム監督管理責任を有効に履行することができず、プラットフォーム上に長期的に大量の著しく法律法規に違反している情報が存在している状況が引き起こされ、是正の督促を経ても効果は顕著に見られなかった。	360doc 個人図書館の主要責任者に事情聴取し、早急な是正と是正期間(10月15日から11月15日まで)中のウェブサイトサービスの停止が命じられる。
2018年9月	上海市通信管理局	ユーザーアカウント取消しの困難性の存在等の問題に対し、特別安全検査業務が実施され、通報された問題が存在している20社に対し、事情聴取が行われる。	是正命令
2018年4月	国家ネットワーク情報部門	快手、火山小視頻の短編動画サイトにおいて、未成年に悪影響のある低俗な内容が含まれていると指摘された。	是正命令
2018年3月	株洲市、区公安セキュリテ	ある教育関連企業がサイバーセキュリティー等級保護義務を履行していなかった。	警告・是正命令

日付	担当機関	案件の詳細	処理結果
	ィー部門		

以上