中国におけるサイバーセキュリティー法規制にかかわる対策マニュアル（更新版）

（2019 年 10 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　ビジネス展開支援課

報告書の利用についての注意・免責事項

本調査レポートは、日本貿易振興機構（ジェトロ）北京事務所が現地法律事務所　　金誠同達法律事務所に作成委託し、2019 年 9 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、本稿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。本稿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：

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

ジェトロ・北京事務所
E-mail：PCB@jetro.go.jp

目次

中国におけるサイバーセキュリティー法規制にかかわる対策マニュアル

「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」という）が 2017 年 6 月 1 日から正式に施行されて以降、関連する付随規定等が続々と発布され、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。かか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」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、法規制の整理

（一）「サイバーセキュリティー法」による規制の対象

「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[1]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。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」[2] 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。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]。

１．ネットワーク運営者

「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[4]。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。

---

[1] 「サイバーセキュリティー法」第 76 条参照。
[2] 「サイバーセキュリティー法」第 2 条参照。
[3] 「サイバーセキュリティー法」第 27 条、第 44 条、第 46 条、第 48 条参照。
[4] 「サイバーセキュリティー法」第 76 条参照。

２．重要情報インフラ運営者

ネットワーク運営者のうち、そのネットワーク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すれば、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のあるような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。なお、重要情報インフラの具体的定義については今後、関連政府部門が判定ガイドラインを打ち出し、それに基づき、各業種の主管または監督部門がそれぞれの業種における重要情報インフラについて判定することになると思われるが、「国家サイバーセキュリティー検査ガイドライン」[5]に基づき、重要情報インフラには、ウェブサイト類（党政機関ウェブサイト、企業事業単位ウェブサイト、ニュースウェブサイト等）、プラットフォーム類（インスタントメッセージ、オンラインショッピング、オンライン決済、検索エンジン、電子メール、フォーラム、マップ、音声動画等のインターネットサービス・プラットフォーム等）、生産業務類（オフィス・業務システム、工業制御システム、ビッグデータセンター、クラウドコンピューティング･プラットフォーム､テレビ中継システム等）が含まれることになる。

また、「重要情報インフラ安全保護条例（意見募集稿）」では、重要情報インフラの範囲について細かい規定があり、具体的には、次に掲げる表のとおりとなっている。いずれにしても、かかる判定を経て、重要情報インフラを運営・管理する事業者が「重要情報インフラの運営者」の範疇に組み入れられることになる。

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すれば国の安全、国の経済、人民の生活、公共の利益を著しく損なう可能性がある。
業界にかかわる判定基準	政府機関およびエネルギー、金融、交通、水利、衛生医療、教育、社会保険、環境保護、公共事業等にかかわる単位
	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および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を提供する単位
	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・生産単位
	ラジオ・テレビ局、通信社等のメディア単位
	その他の重点単位

[5] 当該ガイドラインは、2016 年 6 月に中央サイバーセキュリティー・情報化指導小組弁公室から政府内部向けに示されたものであり、一般向けに公布されている法令等ではない。ただ、重要情報インフラの識別については、参考になると考えられる。

３．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またはソフト等を生産、販売する企業、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ネットワーク製品およびサービス提供者に該当する。

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を履行する必要もある。

（二）サイバーセキュリティー法による規制の実施に伴う法的リスク

「サイバーセキュリティー法」の法執行部門は主に、国家インターネット情報部門、国務院電信主管部門、公安部門である。そのうち、国家インターネット情報部門は、ネットワーク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・調整に責任を負い、国務院の電気通信部門、公安部門およびその他関係部門は、本法および関連の法律、行政法規の規定に基づき、各自の職責の範囲内でサイバーセキュリティーの保護および監督管理業務を担当することとなっている[6]。

業務の具体的管轄としては、現在、各区域の公安部門内に設けられたインターネット情報部門が主に、サイバーセキュリティー等級保護制度およびサイバーセキュリティー保護義務を具現化していない主体に対し処罰を与え、各区域のインターネット情報弁公室および電信主管部門が主に、個人情報保護義務を履行していない等の行為に対し処罰を与えている。

「サイバーセキュリティー法」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。

[6] 「サイバーセキュリティー法」第８条参照。

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
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	
重要情報インフラ運営者	サイバーセキュリティー保護義務を履行しないとき。	○	10～100 万元	1～10 万元	
	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）	

二、課題の整理

（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、前述の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安全の保障	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：上記注1の弁法の意見募集稿には、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ため、今後、同弁法の制定に注意が必要。

（二）「サイバーセキュリティー法」による規制に関する課題

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が履行する必要のある前述の関連義務に基づき、企業は、ネットワーク運営上の安全の保護、個人情報の保護、個人情報および重要データの保管および越境の三つの点で、コンプライアンス上、多くの課題に直面することになると思われる。

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かか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、コンピュータウィ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[7]。

「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）」[8]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			
2018.1.19	情報安全技術 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	全国情報安全標準化技術委員会	意見募集稿
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
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

[7] 「サイバーセキュリティー法」第 21 条参照。
[8] 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
2019.8.3	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

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。

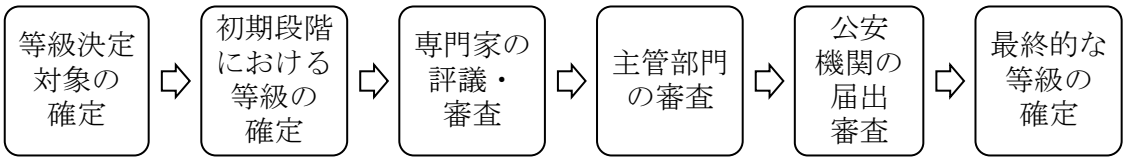
（1）サイバーセキュリティー等級の決定

「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。

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	三級
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、相応の安全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、以下の特別な安全保護義務[9]を履行する必要がある。

- ✓ 自らの安全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[10]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、コンピュータウィルス、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

[9] 「ネットワーク安全等級保護条例」（意見募集稿）第 23 条、第 28 条、第 29 条、第 30 条、第 32 条を参照。

[10] 測定評価に関する具体的な要求については、「情報安全技術 ネットワーク安全等級保護測定評価過程ガイドライン（GB/T 28449-2018)」および「情報安全技術 ネットワーク安全等級保護測定評価要求（GBT28448-2019)」を参照することができる。

定しなければならない[11]。「国家サイバーセキュリティー事件緊急対応策」[12]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」[13]、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」[14]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安全保護ガイドライン」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安全保護ガイドライン」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安全保護制度

「サイバーセキュリティー法」、「重要情報インフラ安全保護条例（意見募集稿）」および「ネットワーク製品およびサービス安全審査弁法（試行）」に基づき、重要情報インフラの安全管理はさらに厳格であり、関連の運営者は専門の安全管理機構と安全管理責任者を設け、サイバーセキュリティー重要職位の専業技術者については資格証保持勤務制度を実施すべきとされている。さらに、重要情報インフラ運営者は、少なくとも毎年 1 回、安全検査測定評価を行い、ネットワーク製品およびサービスの購入の

[11] 「サイバーセキュリティー法」第 25 条参照。
[12] 中網弁発文[2017]4 号参照。
[13] 工信部網安[2017]281 号参照。
[14] 銀監弁発[2008]53 号参照。

際には、秘密保持契約を締結する必要があり、購入したものが、国の安全に影響が及ぶ可能性がある場合には、国家インターネット安全審査弁公室が実施を組織する国の安全審査に合格する必要がある。重要情報インフラの安全保護にかかわる関連規定については、主に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			
2019.5.21	「サイバーセキュリティー審査弁法」	国家インターネット情報弁公室等	意見募集稿
国家標準			
2017.8.30	情報安全技術 重要情報インフラ安全検査評価ガイドライン	全国情報安全標準化技術委員会	意見募集稿
2017.8.30	情報安全技術 重要情報インフラ安全保障指標体系	全国情報安全標準化技術委員会	意見募集稿
2018.6.11	情報安全技術 重要情報インフラサイバーセキュリティー保護要求	全国情報安全標準化技術委員会	意見募集稿
2018.6.11	情報安全技術 重要情報インフラ安全制御措置	全国情報安全標準化技術委員会	意見募集稿

上述の規定のうち、2019 年 5 月 21 日に公布された「サイバーセキュリティー審査弁法（意見募集稿）」[15]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、以下の状況が生ずる可能性のある際には、安全審査[16]を行うべきとされている。重要情報インフラ運営者は安全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、契約等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安全審査に協力すべきとされており、取り決めた安全審査の通過後に、契約は発効する[17]。

- ✓ 重要情報インフラ全体の運営停止または主要な機能の正常な実行の不能性
- ✓ 大量の個人情報と重要データの漏えい、遺失、破損または越境
- ✓ 重要情報インフラのメンテナンス、技術サポート、アップグレード、新旧版交代の実行によるサプライチェーンの安全性に対する脅威への直面

[15] http://www.cac.gov.cn/2019-05/24/c_1124532846.htm
[16] 「サイバーセキュリティー審査弁法（意見募集稿）」第 6 条参照。
[17] 「サイバーセキュリティー審査弁法（意見募集稿）」第 7 条参照。

✓ その他の重要情報インフラの安全性に著しく危害を及ぼすリスクの潜在的な災禍

４．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[18]。

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[19]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、前述の「サイバーセキュリティー審査弁法（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[20]。

- ✓ 重要情報インフラの継続的かつ安全な、安定した運営に対する影響（重要情報インフラが制御を受け、もしくは妨害され、または業務の連続性が侵害される可能性を含む。）
- ✓ 大量の個人情報と重要データの漏えい、遺失、破損、越境等が引き起こされる可能性
- ✓ 製品とサービスの可制御性、透明性およびサプライチェーンの安全性（政治、外交、貿易等の非技術的要素により製品・サービスの供給の中断が引き起こされる可能性を含む。）
- ✓ 国防、軍需産業、重要情報インフラ関連技術・産業に対する影響
- ✓ 製品・サービスの提供者の国家の法律・行政法規および負担を約束した責任と義務の遵守状況
- ✓ 製品・サービス提供者の外国政府の経済的援助、管轄等を受ける状況

[18] 「サイバーセキュリティー法」第 22 条、「情報安全技術 ネットワーク製品およびサービス安全通用要求（意見募集稿）」参照。
[19] 「サイバーセキュリティー法」第 23 条参照。
[20] 「サイバーセキュリティー審査弁法（意見募集稿）」第 10 条参照。

✓　その他の重要情報インフラの安全性と国家の安全に危害を及ぼす恐れのある要素

５．個人情報保護制度

個人情報とは、電子またはその他の方法で記録される、単独またはその他の情報と結びつけることで自然人の身元を識別することができる各種の情報といい、自然人の氏名、生年月日、身分証明書番号、住所、電話番号が含まれるが、これらに限らない[21]。「サイバーセキュリティー法」第四章「ネットワーク情報の安全」には、第 40 条～第 45 条の計六つの条文により、ネットワーク運営者が個人情報をいかに収集・使用・保管・送信するかについて定められている。

2017 年年末に正式に発布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）は、個人情報に対する監督部門による監督管理にとって、重要な根拠となる。さらに、2019 年には、関連部門は APP 中の個人情報の収集、児童個人情報の保護等を対象とし、以下の関連規定を公布している。これによると、ネットワーク運営者は個人情報保護の一般制度、個人機微情報の保護制度、児童個人情報の保護制度等に注意を払うべきとされている。

公布日	文書の名称	公布機関	備考
部門の規則			
2019.3.3	App 個人情報の法律法規に違反した収集の自己評価ガイドライン	App 特定項目対策業務チーム（中央ネットワーク情報弁公室、工信部、公安部、市場監管総局の指導により設立）	既に発効
2019.5.5	App 個人情報の法律法規に違反した収集・使用行為の認定方法		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
2019.8.22	児童個人情報ネットワーク保護規定	国家インターネット情報弁公室	既に発効
国家標準			

[21] 「サイバーセキュリティー法」第 76 条、「個人情報安全規範」第 3.1 条参照。

2018.7.1	情報安全技術 個人情報安全規範（GB/T 35273-2017）	国家市場監督管理総局、中国国家標準化管理委員会	既に発効
2018.6.11	情報安全技術 個人情報安全影響評価ガイドライン	全国情報安全標準化技術委員会	意見募集稿
2019.6.25	情報安全技術 個人情報安全規範		
2019.6.25	情報安全技術 個人情報安全工程ガイドライン		
指導文書			
2019.4.19	インターネット個人情報安全保護ガイドライン	公安部	既に発効

（1）個人情報保護の一般的な制度

① 個人情報の収集規則

個人情報の収集にあたっては、個人情報の主体の授権・同意を得るほか、さらに、プライバシーポリシー、収集する個人情報の類型、製品またはサービスによる業務機能の実現との直接の関連性について、当該主体に告知しなければならず、また、必要最低限の収集でなければならない。

「データ安全管理弁法（意見募集稿）」と「App 個人情報の法律法規に違反した収集・使用の自己評価ガイドライン」によると、ネットワーク運営者の個人情報収集規則においては、以下の内容が重点的に強調されるべきとされている。

- ✓ ネットワーク運営者の基本情報
- ✓ ネットワーク運営者の主要責任者、データ安全責任者の氏名・連絡方法
- ✓ 個人情報の収集・使用の目的、種類、数量、頻度、方法、範囲等
- ✓ 個人情報の保管場所、期間および満期後の処理方法
- ✓ 他者への個人情報の提供規則（他者へ提供する場合）
- ✓ 個人情報安全保護方針等の関連情報
- ✓ 個人情報の主体による同意の撤回、および個人情報の照会・修正・削除の経路と方法
- ✓ クレーム提起、通報の経路と方法等

② 個人情報の保管および使用規則

個人情報を保管する場合には、目的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る場合には、個人情報について、削除または匿名化処理をしなければならない。また、保管される個人情報に対し、関連する業務員がアクセスすることを制限しなければならない。

個人情報を使用する場合には、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。個人情報の授権範囲を超えて個人情報を使用する場合には、当該個人情報の主体から再度、明示の同意を得なければならない。

(2) 個人機微情報の保護制度

「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。かかる個人機微情報については、収集の際に、情報の主体の明示の同意を得なければならず、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、「データ安全管理弁法（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。

(3) 児童個人情報の保護制度

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」を公布し、14 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。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。[22]

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[23]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べきとなる。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べきとなる。[24]

６．個人情報および重要データの中国国内保管および越境に関する制度

重要情報インフラ運営者には、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について、中国国内において保管する必要があり、業務上の必要から、越境する必要が確かにある場合には、安全評価を行わなければならない義務が定められている[25]。一方、「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）」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に拡大されている。この点については今後、関連する法規の発布による明確化が待たれるところである。

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、越境にかか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）の評価が必要となる。安全評価においては、国の安全、社会公共利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。

[22] 「児童個人情報ネットワーク保護規定」第 8 条、第 15 条参照。
[23] 「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。
[24] 「児童個人情報ネットワーク保護規定」第 13 条、第 16 条参照。
[25] 「サイバーセキュリティー法」第 37 条参照。

		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。ただし、2019 年に公布された「データ安全管理弁法（意見募集稿）」と「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、個人情報と重要データの性質の相違にかんがみ、今後の個人情報と重要データの越境について、割合に独立した安全評価の法規が別々に施行される可能性がある。このため、2019 年に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
国家標準			
2017.8.30	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

（1）重要データの中国国内における保管と越境

「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[26]。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、現段階における法規はいまだに不明確なため、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[27]。

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、依然として以下の「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）」の関連規定を参照することができる。

(2) 個人情報の越境

「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、個人情報の越境について、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 個人情報の越境評価の状況

ネットワーク運営者は個人情報の越境が必要な際に、所在地の省級のインターネット情報部門へ安全評価を申請する必要がある。安全評価は原則として 2 年に一度行われるが、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となる。このほか、異なる取得者へ個人情報を提供する際には、別々に安全評価を申請・報告すべきとされており、同一の取得者へ数回または連続して個人情報を提供する際には、頻回

[26] 「データ安全管理弁法（意見募集稿）」第 38 条（5）参照。
[27] 「データ安全管理弁法（意見募集稿）」第 15 条参照。

の評価は不要とされている[28]。

② 個人情報の越境評価の重点的な内容[29]

個人情報の越境評価に必要となる資料は、①申告書、②ネットワーク運営者と取得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安全保障措置分析報告書[30]等である。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と中国国外の取得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または中国国外の取得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事件の発生歴の有無、④ネットワーク運営者の個人情報の取得が合法性・正当性の有無等とされている。

③ 中国国外の取得者に対する規制

「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取得者が締結する契約の具体的な内容の明確化を通じ、初めて中国国外の取得者の義務に対する規定が設けられている。これには主に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取得者へ賠償を請求することができる（取得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[31]。
- ✓ 中国国内のネットワーク運営者もしくは中国国外の取得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安全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[32]。
- ✓ 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、中国国外のネット

[28] 「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。
[29] 「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、第 6 条参照。
[30] 「個人情報越境セキュリティーリスクおよび安全保障措置分析報告書」の関連要求は、「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（草案）」、「情報安全技術　個人情報安全影響評価ガイドライン（意見募集稿）」を参照することができる。
[31] 「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。
[32] 「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。

ワーク運営者の自らの中国国内の実体を通じ、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[33]。

④ 個人情報の主体の権利の保障

「個人情報と重要データの越境弁法（意見募集稿）」においては、個人情報主体の権利が強化されており、主に二つの面が含まれている。

- ✓ 知る権利の面において、ネットワーク運営者と取得者の基本的な状況を個人情報の主体へ告知し、個人情報の主体がその取得者と締結する契約の副本等の提供をネットワーク運営者へ要求することができるよう、運営者は要求されている[34]。
- ✓ 個人情報のアクセス・修正・削除の権利の面において、自らの個人情報のアクセス経路を個人情報の主体へ提供するよう、取得者は要求されており、個人情報の主体が自らの個人情報の修正または削除を要求したときは、合理的な対価と期限の範囲内において、これへの対応、修正または削除を行うべきとされている[35]。

（三）法的義務に係るアクションアイテムの整理

ネットワークの安全に関するコンプライアンスを保証するためには、ネットワーク運営者となる各企業、事業者が次に掲げる関連する法的義務に対応することが必要とされる。また、ネットワーク製品・サービスの提供者は、提供するそれらのものについて、国家規格の強制的な要求事項に適合することや継続的なセキュリティーメンテナンスを提供することが必要とされる。

１．ネットワーク安全保護対策の構築・実施

① サイバーセキュリティー等級保護制度に従い、運営するネットワークを評価、分類し、安全保護義務を履行する。ネットワークの評価、分類については、国家標準「ネットワークセキュリティーレベル保護グレーディングガイド（意見募集稿）」（GB/T 22240-2008 の改定案）の参照が必要である。安全保護義務については、国家標準の「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」等の関連基準の参照が必要である。「サイバーセキュリティー法」[36]に従い、ネットワーク運

[33] 「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。
[34] 「個人情報越境セキュリティー評価弁法（意見募集稿）」第 14 条参照
[35] 「個人情報越境セキュリティー評価弁法（意見募集稿）」第 15 条参照
[36] 「サイバーセキュリティー法」第 21 条参照。

営者は、以下の事項を履行することとなる。

1) 内部安全管理制度、操作規定の制定
2) コンピュータウィルス、サイバー攻撃、ネットワーク不正侵入等を防止する技術的な措置の構築
3) ネットワーク運用状態、サイバーセキュリティー事件を監視し、関連するログファイルを保存（６カ月以上）するシステムの構築
4) データの分類、重要データのバックアップ、暗号化等の措置を講じるシステムの導入
5) その他、法律行政法規が定める保護義務

このほか、三級以上の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条例」（意見募集稿）の内容を参照し、事前にサイバーセキュリティー等級の保護業務を展開し、随時立法の動向に注意を払うことができる。

② サイバーセキュリティー緊急対応策（各類型のサイバーセキュリティー事件に対しいかなる緊急対応プランを起動するのか、いかなる対応措置を講ずるのか、関係する主管部門に対しいかに報告するのかが含まれる）を制定する[37]。このほか、個人情報を収集するネットワーク運営者については、「インターネット個人情報安全保護ガイドライン」を参照し、個人情報セキュリティー事件の緊急対応策（応急処置の流れ、事件の上位者への報告の流れ）を制定し、定期的に（少なくとも半年に一度）緊急対応研修と緊急対応演習を行うことが推奨される。

③ 重要情報インフラ運営者に該当する企業は、上記の①と②の義務を履行するほかに、次の事項が求められる。[38]

1) 専門の安全管理機構および安全管理責任者の設置、ならびにその責任者および重要な職務の担当者に対する安全に関する経歴検査の実施（重要な職位にある専門技術者は、関連する職業ライセンスを取得しなければならない[39]。）。
2) サイバーセキュリティーに関する従業員の教育、技術研修および技能審査の定期的な実施[40]。
3) 重要なシステムおよびデータベースの耐災害性強化とバックアップの実施
4) サイバーセキュリティー緊急対応策の定期的な訓練の実施。

[37] 「サイバーセキュリティー法」第 25 条参照。
[38] 「サイバーセキュリティー法」第 34 条参照。
[39] 「重要情報インフラ安全保護条例（意見募集稿）」第 26 条参照。
[40] 「重要情報インフラ安全保護条例（意見募集稿）」第 27 条参照。

5)　重要情報インフラセキュリティーの検査・評価制度の構築[41]等、法律行政法規が定めるその他の義務。

6)　サイバーセキュリティー審査の実施が必要なネットワーク製品・サービスを購入する際には、契約等に要求されている提供者を通じて、サイバーセキュリティー審査へ協力し、取り決めた安全審査の通過後に、契約が発効する。

２．個人情報保護制度の完全化

① 収集したユーザー情報の保護制度を構築すること[42]。

② 個人情報の内部管理メカニズム（個人情報保護に責任を負う部門および人員の確立、個人情報処理権限の明確化、個人情報の重要な操作を対象とした内部審査承認フローの確立、個人情報担当職位にある人員に対する管理および養成訓練制度の確立等が含まれる）を明確にする[43]。

③ 個人情報の収集・保管・使用制度（個人情報の一般個人情報・児童個人情報・個人機微情報への区分、一般個人情報・児童個人情報・個人機微情報について、個人情報の主体の同意を得る方法の明確化、保管に関連する技術措置の明確化等が含まれる）を制定する[44]。児童個人情報の収集にかかわる場合は、児童個人情報保護制度を制定する。

④ 個人情報安全影響評価制度および監査制度を制定し、個人情報安全基本原則の遵守の状況について、少なくとも毎年１回、安全影響評価を行う[45]。

⑤ 個人情報安全事件の処分および報告制度（個人情報安全事件緊急対応プランの制定、緊急対応演習の実施、個人情報安全事件発生の際の個人情報の主体に対する告知制度が含まれる）を制定する[46]。

３．個人情報および重要データの中国国内保管および越境に関連する制度の確立

① 重要情報インフラ運営者に該当する場合には、中国国内において収集・生成する個人情報および重要データについては、中国国内において保管しなければならない。業務上の必要から、確かに越境する必要がある場合には、安全評価を行わなければならない。一方、一般のネットワーク運営者がかかる義務を履行する必要があるか

[41] 「重要情報インフラ安全保護条例（意見募集稿）」第 28 条、国家標準の「重要情報インフラのセキィリティ検査と評価のガイドライン（意見募集稿）」や「重要情報インフラセキュリティー保障の評価指標システム（意見募集稿）」を参照。
[42] 「サイバーセキュリティー法」第 40 条参照。
[43] 「個人情報安全規範（GB/T 35273-2017）」第 10.1 条参照。
[44] 「個人情報安全規範（GB/T 35273-2017）」第 5.5 条参照。
[45] 「個人情報安全規範（GB/T 35273-2017）」第 10.2 条参照。
[46] 「個人情報安全規範（GB/T 35273-2017）」第 9.1 条参照。

否かについては、いまだ法により明確化されていないため、「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）」、「データ安全管理弁法」、「個人情報越境セキュリティー評価弁法（意見募集稿）」等の今後の立法動向に注目しておく必要がある[47]。

② 安全評価制度を制定する。個人情報と重要データの越境・伝送にかかわる企業は、安全評価制度を確立すべきとされている。

③ 個人情報の越境の際には、ネットワーク運営者は中国国外の取得者と法的効力を有する契約または協議を締結する必要がある。関連の契約または協議の内容については、「個人情報越境セキュリティー評価弁法（意見募集稿）」の関連要求を参照。

三、アクションアイテムの推進　―　各業種の法的義務の整理

本報告第一部分の「サイバーセキュリティー法」による規制の対象の内容において述べたとおり、理論的には、企業は、いずれの業種に属しているかを問わず、また、その従事する事業・経営活動がインターネットに直接関連があるか否かを問わず、いずれも「サイバーセキュリティー法」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に直接関連がある場合には、その負うべき法定義務が一般の事業者に比べてさらに広く、また、より厳格になると思われる。各業種の法的義務について、紙幅の制限により、ここでは、3 種類の代表的業種のみをとりあげ、かつ、当該業種に属する企業にとって、「サイバーセキュリティー法」所定の義務のうち、特に注意する必要のある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、サイバーセキュリティー事件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。よって、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ので、「サイバーセキュリティー法」所定の重要情報インフラ運営者の関連義務に注意し、次に掲げる点から、サイバーセキュリティーに関するコンプライアンスを強化するべきである。

[47] 「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）」第 2 条参照。

１．個人機微情報の保護

「個人情報安全規範」に基づき、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、信用調査情報等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、情報の主体の明示の同意を取得し、かつ、送信または保管の際に情報を暗号化する等の安全措置を講じなければならない。また、「銀行業に属する金融機関が個人金融情報保護業務を適切に行うことに関する中国人民銀行の通知」[48]に基づき、金融機関が業務を展開する際に、中国人民銀行信用調査システム、支払システム、その他の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、個人金融取引情報等は、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、情報安全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・使用等の段階において開示されないようにする必要がある。

２．個人情報および重要データの保管および越境に対する制限

「銀行業に属する金融機関が個人金融情報保護業務を適切に行うことに関する中国人民銀行の通知」に基づき、中国国内において収集した個人金融情報の保管・処理・分析については、中国国内において行わなければならない。法律法規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。

また、「データ安全管理弁法（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）」に基づき、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、取引情報等は、重要データに該当する。金融業に属する企業は、かかる重要データについて、全面的に整理し、その国内保管および越境に関する評価制度として、内部で規程を制定する必要がある。

３．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」を参考とし、「重要情報インフラ安全保護条例（意見募集稿）」に示された重要情報インフラの認定標準をみると、金融業に属する企業が重要情報インフラ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場合には、相応する法定義務を履行しなければならない（法定義務については、本報告第二部分の内容を参照）。

[48] 銀発〔2011〕17 号参照。

（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等を確立し、かつ、かか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疇に組み入れられるので、これらの企業に対しては、特に注意すべき法定義務が専門に設定されており、それには、次に掲げるいくつかの点が含まれる。

１．立法動向に対する注目、データの保管および越境が制限を受けるか否かの確認

中国にある外資製造企業が国外にある本社に対し、中国国内において収集した個人情報および重要データを送信する事由については、今後、「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）」、「個人情報越境セキュリティー評価弁法（意見募集稿）」の立法動向に留意し、個人情報および重要データの国内保管および国外送信の際に安全評価を行う義務があるのか否かについて、確認する必要がある。

２．重要データの保護の強化

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する産業データは、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）」「データ安全管理弁法（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。かかる状況に対応するため、製造業に属する企業は、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）」における重要データ識別ガイドラインに基づき、その内部の重要データについて識別をし、産業データ分級分類管理制度を確立し、重要データの安全保護措置を強化し、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等の準備が必要である。

３．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＋先進的製造業』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」が発布された。当該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、産業ネットワークのインフラとしての地位を明確にし、産業ネットワークの安全性、プラットフォームの責任、データ保護等をカバーする法規体系を確立するよう要求されている。現在のところ、工業および情報化部が「産業ネットワーク発展行動計画（2018-2020 年）」を作成中であると言われて

おり、当該行動計画が打ち出されれば、製造業に属する企業のサイバーセキュリティーに対する監督管理がさらに厳格化されると思われる。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。

（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が含まれる）／ネットワーク製品およびサービス提供者の範疇に組み入れられる。よって、インターネット企業は、ネットワーク運営者としての、さらに、ネットワーク製品およびサービス提供者としての関連する法定義務を遵守しなければならない（具体的内容については、前述参照）。また、「サイバーセキュリティー法」その他の関連規定においては、インターネット企業が特に注意すべき法定義務が専門に設定されており、それには、次に掲げるいくつかの点が含まれる。

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っている[49]インターネット企業は、「国家インターネット安全検査ガイドライン」および「重要情報インフラ安全保護条例（意見募集稿）」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場合には、相応する法定義務を履行しなければならない（法定義務については、本報告第二部分の内容を参照）。

２．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、「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、個人情報の収集・保管・使用・越境等の点において、「サイバーセキュリティー法」の付随規定である「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。それには、児童個人情報、個人機敏情報収集の際に得るべき本人または保護者の明示の同意、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、個人情報共有および譲渡の際の注意事項等が含まれる。

[49] 具体的な量について、いまだ法により明確にされていないため、今後の立法動向に注目しておく必要がある。

３．内容審査報告義務

インターネット企業は、そのユーザーの発布する情報に対する管理を強化しなければならない。法律、行政法規により発布・送信が禁止されている情報を発見した場合には、直ちに当該情報の送信を停止し、除去等の処理をし、情報の拡散を防止し、関係する記録を保管し、関係する主管部門に報告しなければならない[50]。

４．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、ドメイン登録サービスを提供し、固定電話、携帯電話等の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場合には、ユーザーに対し、真実の身分情報を提供するよう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い場合には、インターネット企業は、当該ユーザーのために関連するサービスを提供してはならない[51]。

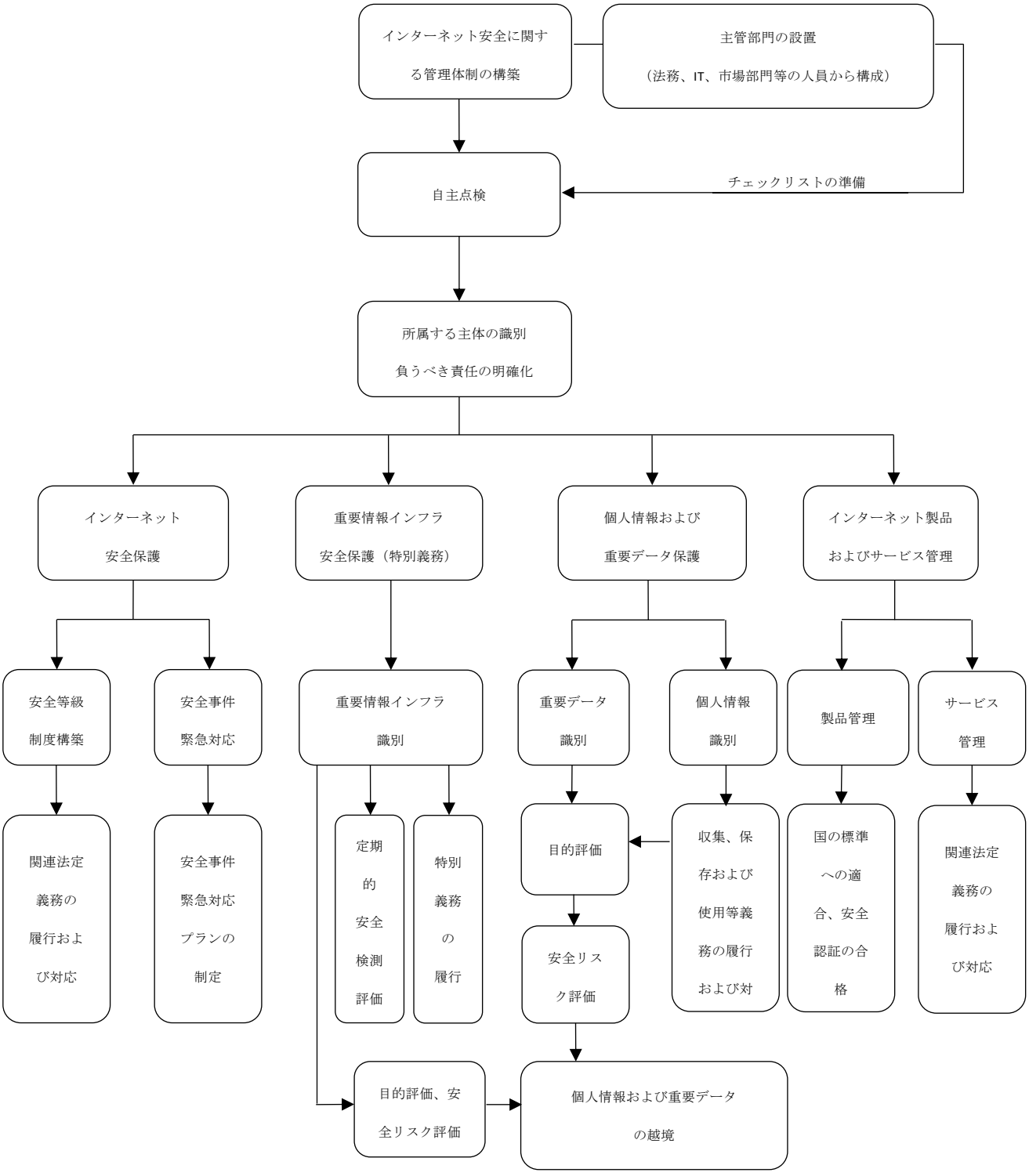
５．ユーザーのインターネット上のデータの保管義務

「サイバーセキュリティー法」等の関連する法律法規においては、ユーザーのインターネット上の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」等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。

[50] 「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発布しており、相応するインターネッ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」等が含まれる。

[51] 「サイバーセキュリティー法」第 24 条参照。

別紙 1：法的義務の点検プロセスのフロー



別紙２：サイバーセキュリティー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、マニュアル本文の一（一）、一（二）、二（一）の部分を参照。また、企業が 1.1 の①、②、④に該当する場合においても、上記部分を参照する必要があるほか、マニュアル本文の三、「アクションアイテムの推進―各業種の法的義務の整理」の部分も要参照。

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コンピュータウィルス、インターネット攻撃等、ネットワークの安全に危害を及ぼ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、マニュアル本文一（二）、二（二）1①、二（三）1 の部分参照。 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、マニュアル本文一（二）の部分参照。 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、マニュアル本文一（二）、二（二）1②、二（三）1 の部分参照。

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洩した場合において、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危害が及ぶ。

□ ②国の安全、国の経済、人民の生活、公共の利益に危害は及ばない。
□ 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、マニュアル本文一（一）2 の部分参照。

4. 個人情報処理チェック

4.1 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。

4.2 ユーザーの個人情報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生成される。
□ 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

4.3 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。

4.4 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。

4.5 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（即ち、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（即ち、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。

4.6 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。

4.7 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

4.8 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。

上記 4.1、4.2 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 4.2 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 4.4、4.5 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 4.3 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、マニュアル本文二（二）2①の部分参照。
上記 4.4、4.5 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、マニュアル本文一（二）、二（二）2②③④、二（三）2 の部分参照。
上記 4.7、4.8 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、前述 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、4.7 の①、4.8 の①の義務を履行しなければならない。具体的には、マニュアル本文二（二）3、二（三）3 の部分参照。

5.ネットワーク製品およびサービスチェック

5.1 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。

5.2 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。

5.3 ユーザーの発布する情報に、法律法規により発布・送信が禁止されている情報を発見した場合において、直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 5.1、5.2、5.3 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 5.1①、5.2①、5.3①の義務を履行しなければならない。具体的には、マニュアル本文一（二）、二（二）１③④の部分参照。

別紙３： 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が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が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について規制されている。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、その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」においては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」の発効後において、サイバーセキュリティー等級制度と情報システム安全等級制度は並行するのか、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。また、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、各業種の主管部門は業種の具体的な状況を踏まえ、自らの業種の重要データの範囲を確定することができる。

別紙４：サイバー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」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
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において、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に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、掲示板において目下依然として頻繁に大量の銃・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る。	当該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る。
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る。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制定しておらず、コンピュータウィルス、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。	当該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る。
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サーバーが突如ダウン状態に陥り、病院の業務が全面的に停止する。人民警察と技術専門家の調査と事実検証を経たところ、当該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	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る。

		おりに安全保護義務を履行していないことが分かった。	
2019年4月	南京市公安部門	某文化マスメディア有限公司が虚偽の方法を採用し、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に注目させ、氏名、連絡先、住所等の入力を参加者へ要求し、大量の公民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。	当該会社に対して罰金1万元、会社の法定代表者とほかの2名の直接参加した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。	当該会社に対して警告が下され、期限付きの是正が命じられる。
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会社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ず、規定の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当該会社に期限付きの是正命令を下し、警告を与えた。4月3日には再検査中において当該会社のいまだに是正を拒んでいる状況の存在が明らかになった。	当該インターネット会社に対して罰金5万元、当該会社の法定代表者毛氏に対して罰金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れる。

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る。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。	当該機関に対して罰金 6 万元、関連の責任者に対して罰金 2 万元の処分、当該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る。
2019 年 2 月	瀘州市公安部門	四川省瀘州市のある会社のインターネットサーバーがウィルスの襲撃を受け、多くの事務用コンピュータが使用不能になる。調査を経たところ、当該会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ィルスソフトとファイアウォールに問題が存在しており、規定の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理局	蘇州同程藝龍網絡科技有限公司のウィーチャット・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おり、早急な是正が要求される。	是正命令
2018 年 11 月	国家ネットワーク情報弁公	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	是正命令

	室	ネット会社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。	
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、通報された上海晨之科信息技術有限公司、家楽福（上海）電子商務有限公司等 20 社の上述の問題が存在している企業に対し、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、	某教育関連会社がサイバーセキュ	警告・是正命令

	区公安セキュリティー部門	リティー等級保護義務を履行していなかった。	

別紙５：実務上の対応

「サイバーセキュリティー法」が施行されて以降、前述の一部の制度はいまだに明確化されていないが、一部の企業は「サイバーセキュリティー法」による新たなコンプライアンス要求に適応するため、企業内部の具体的な状況により、以下の対応策を取っている。

1、サイバーセキュリティー等級の確定および関連制度の制定

国家標準である「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)」によると、セキュリティー等級保護の対象には「基礎情報ネットワークや情報システム」等が含まれている。このため、企業外部のインターネットプラットフォーム（たとえば、ウェブサイトまたはAPP）か、それとも内部のインターネットシステム（特に大量のユーザー情報にかかわる内部会員システム、業務システム等）かを問わず、いずれも関連規定に基づき、セキュリティー等級保護の届出を行うべきとされている。これにより、多くの企業は自らのセキュリティー等級に関連するコンプライアンス状況を非常に重視しており、目下依然として等級保護・等級決定、届出、測定評価・是正を実施していない企業は、多くは既にセキュリティー等級保護のコンプライアンスプロジェクトに着手している。このほか、セキュリティー技術・管理制度・職位担当者の設置を完成させていない企業も、多くは自らまたは外部の弁護士に委託して「サイバーセキュリティー法」、「等級安全保護条例」（意見募集稿）および関連国家標準を参照し、サイバーセキュリティー等級保護制度を制定している。

2、サイバーセキュリティー緊急対応プラン制度の制定

「サイバーセキュリティー法」、「インターネット個人情報安全保護ガイドライン（意見募集稿)」および関連国家標準に基づき、緊急対応プラン制度を制定し、各類型のサイバーセキュリティー事件について、いかなる緊急対応プランを実施するのか、いかなる対応措置を講ずるのか、関係する主管部門に対しいかに報告するのかなどを定めている。

3、個人情報安全保護制度の制定

「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)」、「個人情報越境セキュリティー評価弁法（意見募集稿)」および国家標準の「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)」、「情報安全技術　個人情報安全規範（GB/T 35273-2017)」に基づき、以下の制度を明確にしている。

① 個人情報の内部管理制度（個人情報保護に責任を負う部門および人員の確立、個人情報処理権限の明確化、個人情報の重要な実務処理を対象とした内部審査・承

認フローの確立、個人情報担当職位に就く人員に対する管理および養成訓練制度の確立等が含まれる。）を明確にする 。

② 個人情報の収集・保管・使用制度（一般個人情報、児童個人情報および個人機微情報の区分、個人情報の主体の同意を得る方法の明確化、保管に関連する技術措置の確実な保証、セキュリティー影響評価等が含まれる）を明確にする 。

③ 個人情報の越境制度（越境についての安全評価等）を明確にする 。

④ 個人情報セキュリティー事件の処理および報告制度（個人情報セキュリティー事件緊急対応プランの制定、緊急対応演習の実施、個人情報セキュリティー事件発生の際の個人情報の主体に対する告知制度が含まれる）を明確にする 。

4、業務モデルの調整

「サイバーセキュリティー法」第 37 条においては、「重要情報インフラの運営者は、中国国内において情報インフラを運営する際に収集、作成した個人情報および重要なデータを中国国内で保管しなければならない」と定められている。また、「重要情報インフラ識別ガイドライン」はいまだに公布されていないが、「重要情報インフラセキュリティー保護条例（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（意見募集稿）」等の規定に基づき、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は、重要情報インフラ保護の範ちゅうに含まれることになるものと予測される。

上記にかんがみて、一部の重要情報インフラに組み入れられる可能性が高い外資企業は、個人情報および重要データの中国国内保管に関するコンプライアンス上の要求を満たすため、既に自発的に業務モデルを調整し始めており、業界にとって、重要な参考価値がある。たとえば、2018 年 1 月 9 日にアップル社は中国大陸における iCloud サービスの運営者をアイルランドの某会社から中国の雲上貴州大信息産業発展有限公司へ 2018 年 2 月 28 日をもって変更すると公式に発表している。

以上