中国「インターネット安全法」に基づく
企業コンプライアンスについて

（2017 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北京金誠同達法律事務所に作成委託し、2017 年 11 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。

ジェトロおよび北京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北京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）
ビジネス展開支援部・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

JETRO

目次

中国「インターネット安全法」に基づく企業コンプライアンスについて

一、 序文

「中華人民共和国インターネット安全法」（以下「インターネット安全法」という）が 2017 年 6 月 1 日に正式に施行され、その後、関連部門から一連の付随規定が続々と発布され、「インターネット安全法」に掲げられたインターネット安全保護、重要情報インフラ保護、個人情報および重要データ保護等の点について、具体的実施規則が明確化されつつある。

「インターネット安全法」および関連する付随規定に、いくつかの新しい法律概念および制度が含まれ、また、インターネット安全上のコンプライアンスについて、企業に対する新たな要求も提起されていることから、ここでは、当該「インターネット安全法」および関連する付随規定について整理し、企業がいかにしてインターネット安全関連制度を完備すればよいのかについて提議をする。

二、 「インターネット安全法」の規制主体

「インターネット安全法」および関連する付随規定に基づき、インターネット運営者、重要情報インフラ運営者、インターネット製品およびサービス提供者等の組織および個人はいずれも、「インターネット安全法」による規制を受けることになる。

（1）インターネット運営者

「インターネット安全法」においていう「インターネット」とは、コンピューター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]をいう。また、「インターネット運営者」とは、インターネットの所有者、管理者およびインターネットサービス提供者をいい、その範囲は幅広く、中国国内において「インターネットを確立し、運営し、維持保護し、および使用する」[2]企業は、ほぼすべて該当することになる。

[1] 「インターネット安全法」第 76 条参照。
[2] 「インターネット安全法」第 2 条参照。

注目すべき点は、ここでいう「企業」に、内資・外資の区別がないことである。すなわち、中国資本企業であろうと、外国資本企業であろうと、中国国内において「インターネットを確立し、運営し、維持保護し、および使用する」のであれば、いずれも「インターネット安全法」の規定を遵守しなければならない。

また、「インターネット情報サービス管理弁法」（国務院令第 588 号。2011 年 1 月 8 日施行）に基づきインターネット情報サービスが経営性および非経営性の 2 種類に分けられ、それぞれ許可（ICP 許可）および届出（ICP 届出）制度が実行されていたのとは異なり、「インターネット安全法」においては、インターネットサービスが「経営性」および「非経営性」に分けられてはいない。すなわち、「インターネット」を利用してサービスを提供するいかなる主体も、ショッピングサイト等の経営性インターネットサービスを提供する企業であろうと、オフィシャルサイトを設立して業務宣伝に用いる企業であろうと、いずれも「インターネットサービス提供者」に該当し、インターネット運営者の範囲に組み入れられる。

（2）重要情報インフラ運営者

「インターネット安全法」においては、上記「インターネット運営者」のうち、一部の特殊な運営者、すなわち、その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のあるような運営者について、「重要情報インフラ運営者」と位置付けられている。

一般のインターネット運営者と異なり、重要情報インフラ運営者は、より厳格な安全保障義務を負うことになる。「重要情報インフラ安全保護条例（意見募集稿）」においては、重要情報インフラの範囲について細かい規定[3]があり、具体的には、以下の表のとおりとなっている。今後、関連政府部門が重要情報インフラの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各業種内の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。よって、各企業はそれぞれ、自社が重要情報インフラ運営者に該当するのか否かという判定に基づき、負担するべき法的義務を明確にすることができる。

[3] 「重要情報インフラ安全保護条例（意見募集稿）」第 18 条参照。

安全に係る判定基準	機能が破壊され、もしくは失われ、またはデータが漏洩すれば国の安全、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。
業界に係る判定基準	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

（3）インターネット製品およびサービス提供者

インターネット製品[4]およびインターネットサービス[5]を提供する組織または個人が重要情報インフラ運営者等に対し、国の安全に影響を及ぼす可能性のあるインターネット製品およびサービスを提供する場合には、「インターネット安全法」および「インターネット製品およびサービス安全審査弁法（試行）」（国家インターネット情報弁公室発布。2017 年 6 月 1 日施行）による規制を受けることになる。

注目すべき点は、インターネット製品およびサービス提供者が必ずしもインターネット運営者であるとは限らず、インターネット製品を提供するのみであってインターネット所有者・使用者およびインターネットサービス提供者に該当しない組織または個人もいるところ、係る組織または個人もやはり、「インターネット安全法」の関連規定を遵守する必要があることである。

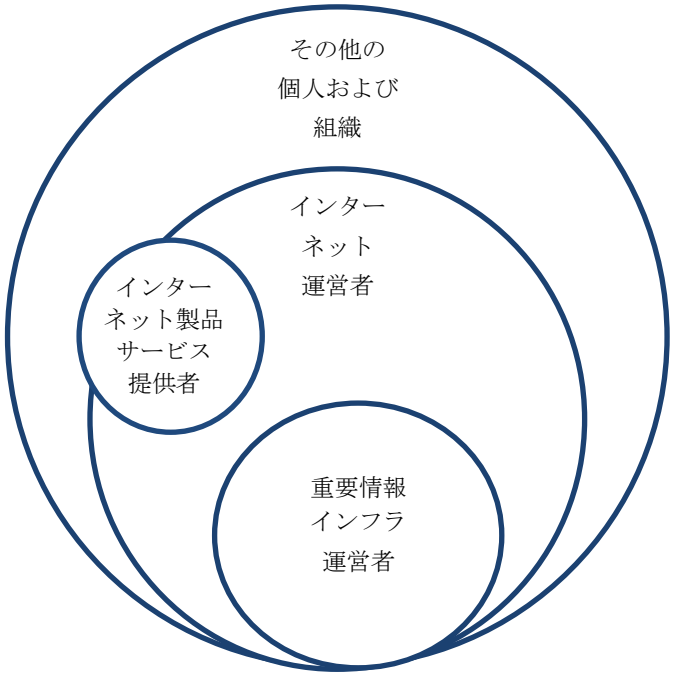
[4] インターネット製品とは、コンピューター、情報端末、ファクトリーオートメーション等の関連設備および基本ソフトウェア、システムソフトウェア等を含む、一定のルールおよび手続きに従って情報を収集、保存、送信、交換、処理するハードウェア、ソフトウェア、システムをいう。

[5] インターネットサービスとは、提供者がユーザーの要求を満たすために提供する、情報技術開発・応用活動、インターネット技術を用いてユーザーの業務をサポートする一連の活動をいい、よく見られるものには、クラウドコンピューティングサービス、インターネット通信サービス、データ処理・保存サービス、情報技術コンサルティングサービス、設計・開発サービス、情報システム集成実施サービス、情報システムオペレーションサービス等がある。

（4）その他の個人および組織

インターネット運営者に該当せず、インターネット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また、「インターネット安全法」の規定を遵守し、インターネットを適法に使用する必要がある。いかなる個人および組織も、インターネットを利用して国の安全、栄誉および利益等に危害を及ぼす行為に従事してはならず、他者のネットワークに侵入してはならず、他者のネットワークの正常な機能を妨げる行為を行い、または行うことに協力してはならず、個人情報を窃取し、またはその他の不法な方式により取得してはならず、個人情報を不法に売却し、または不法に他者に対し提供してはならない。

以上をまとめれば、「インターネット安全法」による規制を受ける各主体の関係は、以下の図のとおりとなる。



三、 「インターネット安全法」の主な内容

「インターネット安全法」においては主に、インターネット安全保護制度、重要情報インフラ安全保護制度、個人情報および重要データ保護制度、インターネット製品およびサービス管理制度が確立された。現在までに、中国国家インターネット情報弁公室、全国情報安全標準化技術委員会等の部門も、係る制度を対象として次々と付随する法規および標準を打ち出しており、既に正式に発効しているものもあれば、いまだ意見募集段階にあるものもあるが、主なものは、以下の表に示すとおりである。

インターネット安全保護	インターネット安全事件緊急対応制度	正式発行済み	「国家インターネット安全事件緊急対応プラン」
			「ファクトリー・オートメーションシステム情報安全事件緊急対応管理業務ガイドライン」
		意見募集稿	「インターネット攻撃定義および描写規範」
			「インターネット安全事件緊急対応演習通用ガイドライン」
			「インターネット安全脅威情報表示モデル」
	インターネット安全等級制度	意見募集稿	「インターネット安全等級保護実施ガイドライン」
			「インターネット安全等級保護評価測定過程ガイドライン」
			「インターネット安全等級保護評価測定技術ガイドライン」
重要情報インフラ安全保護		意見募集稿	「重要情報インフラ安全保護条例」
			「重要情報インフラ安全検査評価ガイドライン」
			「重要情報インフラ安全保障評価指標体系」
個人情報および重要データ保護		正式発効済み	「公共および商用サービス情報システム個人情報保護ガイドライン」
		意見	「個人情報および重要データ海外送信安

	募集稿	全評価弁法」
		「データ海外送信安全評価ガイドライン」
		「個人情報安全規範」
		「個人情報識別不能化ガイドライン」
インターネット製品およびサービス管理	正式発効済み	「インターネット製品およびサービス安全審査弁法（試行）」
		「インターネット重要設備およびインターネット安全専用製品目録（第一期）」
	意見募集稿	「インターネット製品およびサービス安全通用要求」
		「情報技術製品安全検査測定機構条件および行為準則」
		「情報技術製品安全制御可能評価指標（第1-5部分）」

上記制度の枠組において、企業が履行するべきコンプライアンス上の義務および注意するべき事項を全面的に理解するため、以下、「インターネット安全法」の主な内容について整理する。

1、インターネット運営上の安全保護制度

インターネット運営上の安全は、インターネットスペースの安全の基礎的条件であり、インターネット運営者は、以下のインターネット安全等級保護制度、インターネット安全事件緊急対応プラン制度、ユーザー実名制等を確立する必要がある。インターネット運営者は、関連する義務を履行しなければ、罰金、営業停止是正、関連業務の一時停止、さらに営業許可証の取消し等が科される可能性があり、また、直接責任を負う主管人員も、相応する処罰を受ける可能性がある。

（1）インターネット安全等級保護制度

「インターネット安全法」においては、「インターネット安全等級保護制度」が初めて出現している。インターネット運営者のインターネット安全等級をいかに決定するかについて、いまだ具体的規定はないものの、現行の「情報安全等級保護管理弁法」

の「情報システム安全保護等級」に関する区分標準に照らせば、各インターネット運営者の安全等級は、その「公民、法人その他の組織の適法な権益」および「国の安全、社会秩序、公共利益」に対する影響の程度[6]に基づき区分されると考えられ、等級が高ければ、履行するべきインターネット安全保護義務もより厳格になる。

インターネット運営者の安全保護義務については、そのインターネット安全等級に基づき確定される必要があるところ、関連する区分標準が発布されるまで、各企業は、自身の状況を考慮しつつ、以下の要求に適合するようにしておくことができる。

① 内部安全管理制度および運用規程を制定し、インターネット安全責任者を確定し、インターネット安全保護責任を具体化する。
② コンピューターウィルスおよびインターネット攻撃・侵入等インターネットの安全に、危害を及ぼす行為を防止するための技術措置を講ずる。
③ インターネットの運行状態およびインターネット安全事件を、モニターまたは記録する技術措置を講じ、かつ、規定に従い関連するインターネット日誌を 6 カ月以上保管する。
④ データ分類、重要データバックアップ、パスワード設定等の措置を講ずる。

(2) インターネット安全事件緊急対応プラン制度

インターネット運営者は、インターネット安全事件緊急対応プラン制度を制定しなければならない。インターネット運営者は、インターネットの安全に危害を及ぼす事件を発見した場合には、直ちに当該緊急対応プランを起動し、救済措置を講じ、かつ、関係する主管部門に対し報告しなければならず、インターネット製品・サービスに安全上の欠陥・バグのあることを発見した場合にも、直ちに救済措置を講じ、遅滞なくユーザーに告知し、かつ、関係主管部門に対し報告する必要がある。

(3) ユーザー実名制

インターネット運営者は、ユーザーのために、インターネット接続・ドメイン名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接続手続きをし、または情報発布、即時通信等のサービスを提供する場合には、ユーザーに対し、真実の身

6 「情報安全等級保護管理弁法」第 7 条参照。

分を提示するよう要求しなければならず、しからざる場合には、サービスを提供してはならない。また、ユーザーの発信する情報が法律法規に違反していることを発見した場合には、直ちに送信を停止し、さらなる拡散を防ぎ、かつ、記録を保存して関連する部門に対し報告しなければならない。

2、インターネット情報安全保護制度

インターネット情報安全保護の点について、「インターネット安全法」においては、個人情報の保護が特に強調されている。「インターネット安全法」およびその付随規定に基づき、「個人情報」とは、電子その他の方式により記録される、単独で、またはその他の情報と組み合わさって特定の自然人の身分を識別することができ、または特定の自然人の活動状況を反映することのできる各種情報をいい、氏名、生年月日、身分証番号、通信連絡方式、個人生物識別情報、住所、アカウントパスワード、財産状況、行動追跡情報等は、個人情報に含まれる[7]。個人情報の保護制度については、主に以下のとおりである。

（1）個人情報の「開示＋同意」原則

インターネット運営者は、個人情報を使用・収集する場合には、個人情報の主体に対し、個人情報収集・使用の目的、方式、範囲を開示し、かつ、その同意を取得しなければならない。

個人情報の主体の同意を得ずに、第三者に対し個人情報を提供してはならない。ただし、特別な処理を経て特定の個人を識別することができず、かつ、復原不可能な個人情報については、その限りではない。

（2）個人情報の保存

収集・使用する個人情報について、インターネット運営者は、技術措置等を講じて、その漏えい、毀損、紛失を防止しなければならず、係る状況が発生した場合には、直ちに救済措置を講じ、かつ、遅滞なくユーザーおよび主管部門に対し報告しなければ

[7] 「データ海外送信安全評価ガイドライン」および「個人情報および重要データ海外送信評価弁法（意見募集稿）」第 17 条参照。

ならない。個人情報の使用が法律法規または約定に違反している場合には、当該個人情報の主体は、削除を要求する権利を有する。個人情報に誤りのある場合には、当該個人情報の主体は、修正を要求する権利を有する。

（3）個人情報に関する最新司法解釈

注目に値するのは、2017 年 5 月 8 日に、公民個人情報侵害罪の防止について、最高人民法院および最高人民検察院が初めて、司法解釈[8]を打ち出したことである。当該司法解釈に基づき、何らかの組織および個人が国の関係規定に違反し、他者に対し公民個人情報を売却または提供し、以下の表に掲げる数量に達した場合には、「刑法」第 253 条所定の「公民個人情報侵害罪」を構成する可能性がある。インターネット運営者が職責を履行し、またはサービスを提供する過程において取得する公民個人情報を他者に売却または提供し、以下の表に掲げる数量要求の半分に達した場合にも、「公民個人情報侵害罪」を構成する可能性がある。

情報類型	数量基準
行動追跡情報、通信内容、信用調査情報、財産情報	50 本以上
宿泊情報、通信記録、健康生理情報、取引情報等の人身・財産の安全に影響を及ぼす可能性のあるその他の公民個人情報	500 本以上
上記類型以外のその他の個人情報	5,000 本以上

[8] 「公民個人情報侵害刑事事件処理に適用される法律に係る若干の問題に関する最高人民法院および最高人民検察院の解釈」参照。

3、重要情報インフラ安全に係る特別保護制度

重要情報インフラ運営者は、インターネット運営者の安全保護制度を基礎として、さらに、レベルがより高い安全保護制度を確立する必要がある。また、情報データの保管および送信について、特別の制限を受けることになる。

（1）個人情報および重要データの保管および送信制限

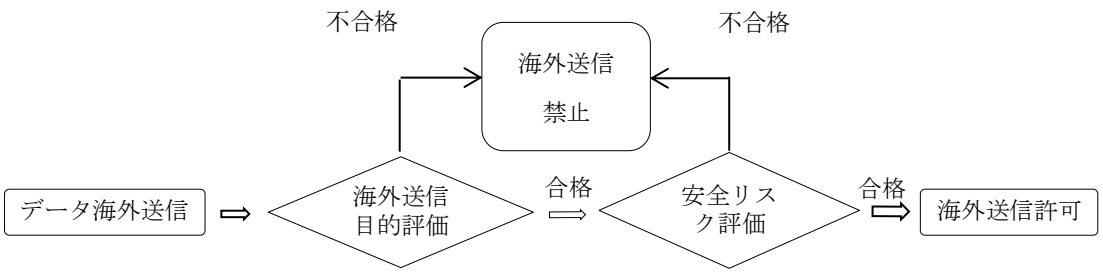
重要情報インフラ運営者は、中国国内において収集した個人情報および重要データ[9]について、中国国内において保管しなければならない。業務上、確かに国外向けに提供する必要がある場合には、安全リスク評価を行わなければならない。「個人情報および重要データ海外送信安全評価弁法（意見募集稿）」において、当該制限を受ける主体が重要情報インフラ運営者からすべてのインターネット運営者に拡大されている傾向がある。「個人情報および重要データ海外送信安全評価弁法」は、現在のところまだ意見募集稿であり、その内容は流動的であるものの、個人情報および重要データに対し特別な保護を実施しようという関連部門の立法意図は、既に極めて明確になっている。インターネット運営者は、関連する立法動向に注意を払い、かつ、個人情報および重要データの保管・海外送信制度について、適時に調整していく必要がある。

個人情報および重要データ海外送信の「安全リスク評価」については、企業による自主評価を主とし、主管部門[10]による評価を従とする。その評価フローおよび評価基準は、以下のとおりである。

---

9 「重要データ」とは、中国国内で収集・生成され、国の秘密にかかわらなくとも国の安全、経済発展および公共の利益と密接に関連のあるデータをいう。注目すべき点は、「データ海外送信安全評価ガイドライン（意見募集稿）」において、石油天然ガス、石炭等の 27 の業種内の重要データが確定されており、さまざまな業種のうち、国の安全、経済発展および公共の利益と密接に関連のある業種のデータが含まれていることである。

10 個人情報および重要データに次の事由がある場合には、インターネット運営者は、業種主管または監督管理部門に対し、安全評価の組織を申請しなければならない。
①個人情報の量が 50 万人分以上、または累計で 50 万人分以上となるとき。
②データの量が 1,000GB を超えるとき。
③原子力施設、化学生物、国防軍需産業、生態学的健康等の分野のデータ、大型プロジェクト、海洋環境、敏感度の高い地理情報データ等を含むとき。
④重要情報インフラのシステムのバグ、安全保護等のインターネット安全情報を含むとき。
⑤重要情報インフラ運営者が国外向けに個人情報および重要データを提供するとき。
⑥国の安全および公共利益に影響を及ぼす可能性があり、業界の主管部門または監督部門が評価すべきと認めるとき。



上記「海外送信目的評価」とは、海外送信目的の「適法性、正当性、必要性」の評価をいうが、現在のところ、具体的な評価標準はない。ただ、サーバー等が国外にある企業が内部経営管理または業務上の必要性に基づきデータを海外送信する場合には、「正当性、必要性」の範疇に属する可能性があると考えられる。

上記「安全リスク評価」の具体的標準は、以下のとおりであり、リスクレベルが「極めて高い」および「高い」との評価を受けた場合には、海外送信してはならない。

① 個人の権益に対する個人情報海外送信の影響等級[11]を確定する。国の安全、経済発展および社会公共利益に対する重要データ海外送信の影響等級[12]を確定する。
② 安全事件発生可能性等級[13]を確定する。
③ 上記①および②に基づき総合評価を行い、安全リスクレベルを「極めて高い、高い、普通、低い」の四つのレベルに区分する。

(2) 定期的安全検測評価

重要情報インフラ運営者は、個人情報および重要データを海外送信する場合には、安全評価をする必要があるほか、自ら、またはインターネット安全サービス機構に委託して、そのインターネットの安全性および存在する可能性のあるリスクについて、検測評価を毎年少なくとも 1 回行い、かつ、検測評価状況および改良措置について、重要情報インフラ安全保護業務に責任を負う関連部門に報告しなければならない。

11 主に個人情報の敏感性、数量、範囲、技術処理状況等に基づき判断する。
12 主に重要データの内容、数量、範囲、技術処理状況等に基づき判断する。
13 主に発信者および受信者の安全保障能力、受信者所在地の政治環境等に基づき判断する。

（3）重要情報インフラ運営者の特別義務

重要情報インフラは、破壊され、その機能を損失し、またはそのデータが漏洩すれば、国の安全、公共利益等に深刻な影響を及ぼす可能性があるため、重要情報インフラ運営者は、インターネット運営者の義務を履行するほか、以下の特別な義務を履行する必要がある。

① 専門の安全管理機構および安全管理責任者を設置し、かつ、当該責任者および重要職位にある人員に対し、安全背景審査を行う。
② インターネット安全業務上、重要職位にある専門技術者について、資格に基づく勤務制度を実行する。
③ 定期的に従業員に対しインターネット安全教育、技術訓練および技術テストを行う。
④ 重要システムおよびデータベースについて、バックアップを作成する。
⑤ インターネット安全事件緊急対応プランを制定し、定期的に演習を行う。

4、インターネット製品およびサービスに係る安全管理制度

インターネット製品およびサービスに係る安全管理制度の規制主体は、主にインターネット製品およびサービス提供者である。

インターネット製品およびサービス提供者が「インターネット重要設備およびインターネット安全専用製品」[14]を提供する場合には、係る設備および製品について、関連する国の標準に適合しており、資格を有する機構が行う安全認証に合格しており、または安全検測が要求に適合しているときに限り、販売または提供することができる。

インターネット製品およびサービス提供者は、重要情報インフラ運営者に対しインターネット製品およびサービスを提供する場合には、重要情報インフラ運営者との間で、安全秘密合意を締結する必要があり、さらに、インターネット製品の安全性およ

14 「インターネット重要設備およびインターネット安全専用製品目録（第１期）」に基づき、インターネット重要設備には、ルーター、交換機、サーバー（ラックマウント型）等が含まれる。インターネット安全専用製品には、ファイアーウォール（ハードウェア）、侵入検測システム、侵入防御システム、アンチウィルス製品等が含まれる。

び制御性[15]について、インターネット安全審査委員会等の関連部門の安全審査を受ける可能性がある。

四、 企業のインターネット安全のコンプライアンスのポイント

前述の「インターネット安全法」の主な内容に基づき、インターネット運営者、重要情報インフラ運営者、インターネット製品およびサービス提供者は、多くの義務を履行する必要があり、企業、特に外資企業にとって、インターネット安全のコンプライアンスの面において、新たなハードルとなる。よって、企業は、以下の幾つかの観点から、関連する制度を完全化することが推奨される。

1、インターネット安全保障制度の完全化

(1) インターネット安全緊急対応プランの制定

インターネット運営者は、インターネット安全緊急対応プランを制定しなければならない。インターネットの安全に危害が及ぶような事件が発生した場合には、直ちに緊急対応プランを起動し、相応する救済措置を講じ、かつ、規定に従い主管部門に対し報告する。

(2) インターネット安全等級制度の関連義務の履行

インターネット安全等級の区分標準が明確になれば、インターネット運営者は、相応する安全保障義務を履行する必要がある。ただ、その前においても、企業がそれぞれの状況に応じて内部安全管理制度および運用規定を制定し、インターネット安全責

[15] 「安全性および制御性」については主に、以下のリスクが審査されることになる。
① 製品およびサービスが不法にコントロールされ、干渉され、その運行を中断されるリスク。
② 製品および重要部品の研究開発、引渡し、技術サポート過程におけるリスク。
③ 製品およびサービス提供者が、製品およびサービス提供の便宜を利用して、ユーザーに関連する情報を不法に収集・保管・処理・利用するリスク。
④ 製品およびサービス提供者が製品およびサービスに対するユーザーの依存を利用して、不正競争を実施し、またはユーザーの利益を損なうリスク。
⑤ 国の安全および公共の利益に危害を及ぼす可能性のあるその他のリスク。

任者を確定し、インターネット安全保護責任を具体化し、コンピューターウィルスおよびインターネット攻撃・侵入等のインターネットの安全に危害を及ぼす行為を防ぐ技術措置を講じて、可能な限りインターネット安全等級に係る要求に適合するようにしておくことが推奨される。

（3）重要情報インフラ運営者である企業が特に注意するべき事項

重要情報インフラ運営者に該当する可能性のある企業は、関連部門が今後打ち出す重要情報インフラ識別ガイドラインに注意し、以下の制度を制定する準備作業をしておく必要がある。

① 社内に専門の安全管理機構を設置し、安全管理責任者を確定する。
② インターネット安全業務上、重要職位にある専門技術者について、資格に基づく勤務制度を実施する。
③ 従業員に対し定期的にインターネット安全教育、技術訓練および技能テストを行う。
④ 重要システムおよびデータベースについてバックアップを作成する。

2、個人情報保護の強化

企業、特に、従業員、顧客等の個人の情報について日常的に処理して海外送信する多国籍企業は、個人情報保護に関するコンプライアンス義務を履行する必要がある。

（1）「個人情報」の確定

「個人情報」であるか否かの判断基準は、単独で、またはその他の情報と組み合わさって、特定の自然人を識別することができ、または特定の自然人の活動を反映することができるか否かである。よって、企業が業務発展上の必要から収集する製品メインテナンス等の情報は、いずれも製品を使用する特定の個人を識別することが可能なことから、「個人情報」の範疇に組み入れられる。ただし、企業が技術手段等を駆使して係る情報から顧客の身分を識別することのできる情報を選別した上で削除すれば、当該情報は、会社の業務発展のために用いられる一般的な技術情報となり、「個人情報」

に該当せず、「インターネット安全法」による規制も受けないことになる。

（2）個人情報収集・使用規則の明確化

企業は、個人情報収集・使用制度を確立し
当該制度の要求に厳格に従い、収集または使用の目的、方式、範囲をありのままに、開示し、かつ、情報主体の同意を得なければならない。企業が既に収集または使用済みの個人情報については、「開示＋同意」の標準に適合するか否かについて審査し、標準に適合しないものについて、情報主体である個人に対し「開示＋同意」義務を追加で履行することが推奨される。また、個人情報の海外送信にかかわる場合には、開示する内容には、海外送信の目的、範囲、内容、受信者、受信者の所在国または地域が含まれなければならない。個人情報の主体が未成年である場合には、その海外送信にあたって、その保護者の同意が必要となる。

注意すべき点は、「同意」が「明示同意」をいうのか、あるいは「黙示同意」をいうのかについて、「インターネット安全法」に明確な規定がないにもかかわらず、紛争の発生を防ぐため、企業は今後、情報主体の積極的同意を取得することが推奨される。

3. 個人情報および重要データの国内保管および海外送信評価制度

「個人情報および重要データ海外送信安全評価弁法（意見募集稿）」の規定に基づき、インターネット運営者が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」はすべて、中国国内において保管しなければならず、確実に海外送信が必要である場合には、安全リスク評価を行わなければならない。よって、個人情報および重要データの海外送信が実際に必要な企業は、個人情報および重要データの保管および送信制度について、以下の調整をすることが推奨される。

（1）個人情報および重要データの国内保管制度の制定

企業は、個人情報および重要データを、社内のほかの電子情報と区分し、国外にあるサーバーまたはデータ保管設備から隔離して、中国国内において保管することが推奨される。また、日常的にデータを海外送信する必要のある多国籍企業は、個人情報

および重要データの海外送信に対する監督管理が日増しに厳格になっていることに鑑み、ビジネス上の合理性は保ちつつ、そのサーバーの中国現地化を徐々に進めていくことが推奨される。

(2) 個人情報および重要データの海外送信規則の明確化

企業は、個人情報および重要データ海外送信の運用ガイドラインを制定し、個人情報および重要データ海外送信の主たる責任者を明確にし、職員が勤務中に個人情報および重要データに随意に接触し、かつ、それらを海外送信することを厳格に禁止し、法的リスクの発生を防止することが推奨される。

さらに、企業は、安全リスク評価制度を制定し、安全評価チームを立ち上げ、安全評価のポイントおよび方法等について明確にすることが推奨される。また、個人情報および重要データが特殊なものである場合には、国のインターネット情報部門および業種主管部門による評価を受けることになる。よって、企業は、日常的経営活動において、関連部門と良好な関係を保ち、積極的に、かつ、遅滞なく、安全評価を行う必要がある。

4、「インターネット安全法」に関する立法動向に対する注視

「インターネット安全法」が正式に施行されて以来、関連部門により発布されている付随規定および業界標準は、その多くが意見募集稿であり、正式に発効するまでは、その内容は、流動的なものである。よって、企業は、立法動向を注視し、前もって、または遅滞なく、関連する要求に基づき、インターネット安全に関する制度を完全化し、企業の運営および業務上のコンプライアンスを保証することが推奨される。