中国サイバーセキュリティ法施行に伴う影響

上海駐在員　公認会計士　鯉沼里枝

▸ Rie Koinuma

日本で電力業、建設業、専門商社、製造業、不動産業、海運業など、さまざまな業種の国内上場・非上場会社の会計監査のほか、株式上場支援、J-sox等のアドバイザリー業務に従事。2016年7月よりEY上海事務所に出向し、中国華中地区の日系企業に対する監査、税務、アドバイザリーサービス等の支援業務に従事している。当法人シニアマネージャー。

Ⅰ　はじめに

2017年5月に日本で改正個人情報保護法が施行され、また、欧州連合（EU）では18年5月に「GDPR（General Data Protection Regulation：一般データ保護規則）」が施行されており、IT化に伴う個人情報の保護は世界の潮流となっています。中国においても、16年11月に「中華人民共和国サイバーセキュリティ法（中华人民共和国网络安全法、以下、サイバーセキュリティ法）」が公布され、17年6月から施行されています。同法は、中国におけるサイバーセキュリティおよび個人情報保護について、包括的に定めた初めての基本法です。施行後1年以上経った現在でも関連する細則が完全には整備されておらず、その適用方法等について不明確な部分があることから、まだ本格導入とは言えませんが、今後の本格導入に伴い中国に進出している日系企業にも大きな影響を与えることが予想されます。

本稿では、同法の中でも特に日系企業の注目度が高いポイントに絞ってその概要を解説します。

Ⅱ　サイバーセキュリティ法の適用対象

1. ネットワーク運営者

主な適用対象者は、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、運営、維持、使用する企業）です。ここでネットワークとは、コンピュータ、その他の情報端末、および関連機器により構成され、一定のルールに従って情報の収集・保存・伝送・交換・処理を行うシステムと定義されています。いわゆるIT企業だけでなく、自社のウェブサイトを開設している企業、社内で電子メールを使用している企業も含まれるため、結果として中国において事業活動を行うほぼ全ての企業が適用対象となります。

2. 重要情報インフラ運営者

ネットワーク運営者のうち、重要情報インフラ運営者に該当する場合には、より厳格な義務が課せられています。ここで、重要情報インフラとは「公共通信、エネルギー、通信、金融、交通、公的事業等の重要産業の運営を支える情報システム／制御システムで、サイバー事故に遭遇した場合、国家安全、経済、科学技術、社会、文化、国防、環境、公共利益に重大な損害を与えるもの」と定義されています。具体的な対象範囲については、今後順次明確化されていきますが、「重要情報インフラ安全保護条例（意見募集稿）」においては、以下の企業が例示されていますので、該当する場合には注意が必要です。

- 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、公共事業等に関わる企業
- 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を提供する企業
- 国防、科学技術工業、大型設備、化学工業、食品・薬品等の業界・分野の科学研究生産企業
- ラジオ局、テレビ局、通信社等の新聞企業
- その他の重点企業

Ⅲ　注目すべき六つのポイント

以下は、サイバーセキュリティ法に関する主な六つのポイントです（＜表1＞参照）。なお、同法はすでに施行されていますが、関連する細則の多くは意見募集稿のまま最終化されていません。意見募集中の細則においてより厳しい要求がなされている場合があり、特に、サイバーセキュリティ法上は重要情報インフラ運営者のみに義務付けられている項目について、細則ではその適用対象が拡大されている場合があるため、今後の細則の動向に注意が必要です。

▶表1　サイバーセキュリティ法の主な六つのポイント

	1. データの越境制限
	重要情報インフラ運営者が個人情報および重要データを業務上の必要性により国外に提供する必要がある場合には、安全評価を行わなければなりません。（第37条） ※重要データの判断基準については、現時点で明確化されていません。
	ネットワーク運営者は、データ越境に際して安全評価を行わなければなりません。（細則：個人情報及び重要データの越境評価方法（意見募集稿））
	2. データの中国国内保存
	重要情報インフラ運営者は、個人情報および重要データは中国国内に保存する必要があります。（第37条）
	重要情報インフラ運営者以外であっても、データの中国国内保存に関する要求事項を満たす必要があります。（細則：個人情報及び重要データの越境評価方法（意見募集稿））
	3. サイバーセキュリティ安全等級保護
	全てのネットワーク運営者は、国の定めたサイバーセキュリティ安全等級保護制度に従って、ネットワークが妨害、破壊または無許可アクセスを受けないように保障し、ネットワークの漏えい、窃取または改ざんを防止しなければなりません。（第21条）
	4. インターネット実名制
	ネットワーク運営者はインターネット実名制を採用することが義務付けられています。すなわち、ユーザーにネットワークに関連するサービスを提供するに当たって、真実の身分情報の提供を要求しなければなりません。なお、ユーザーが真実の身分情報を提供しない場合には、サービスの提供を行うことはできません。（第24条）
	5. 個人情報保護
	ネットワーク運営者は、個人情報を収集、使用するに当たり、合法性、正当性、必要性の原則を遵守し、収集、使用の規則を公開し、情報を収集する目的、方式および範囲を明示するとともに、対象者から同意を得なければなりません。（第41条）
	6. 違反した場合の法的責任
	サイバーセキュリティ法では、違反した場合の罰則についても定められています。企業が違反した場合、最も厳しい処罰は営業停止、ウェブサイトの閉鎖、関連の業務許可の取消しまたは営業許可の取消しなどであり、罰金最高額は百万人民元となっています。

Ⅵ　おわりに

サイバーセキュリティ法が導入されてから1年以上が経ちますが、いまだ本格導入に至っていないことから、特段の対応をしていない企業も多く見受けられます。一方で、特にデータの越境制限や中国国内保存、個人情報保護に関する義務については、中国で事業を行う多くの外資系企業が大きな関心を寄せています。中国国外転送を前提としたデータが重要データに該当する場合は、越境に当たって安全評価が求められ、その結果リスクが高いと評価された場合には、国外への持ち出しが禁止されます。このようなケースでは、転送が禁止されたデータの内容によっては事業戦略に大きな影響を及ぼす可能性もあります。また、事業において個人情報を取得している場合、個人情報取得に際して、今後どのように対象者から同意を得ていくかは、実務上の課題となります。そのため、まずは現状分析を行い、現状とサイバーセキュリティ法とのギャップを洗い出すことによりリスクを把握するとともに、越境データ転送の安全性について自己評価をすることが望まれます。

お問い合わせ先
EY上海事務所
ジャパン・ビジネス・サービス
E-mail：rie.koinuma@cn.ey.com