サイバーセキュリティ法への日系企業の対応

上海駐在員　公認会計士　山村 亮

▸ Ryo Yamamura

当法人において10年超の監査経験がある。東証一部上場企業、JASDAQ上場企業、在日外資系企業に対して日本基準および外国会計基準（US GAAP、IFRS）に基づく監査業務を監査マネージャーとして提供。2017年7月よりEY中国（上海）に駐在し、中国（華東）における日系企業に対してJBSマネージャーとして監査・税務・アドバイザリー等の業務を日本語で包括的に提供している。

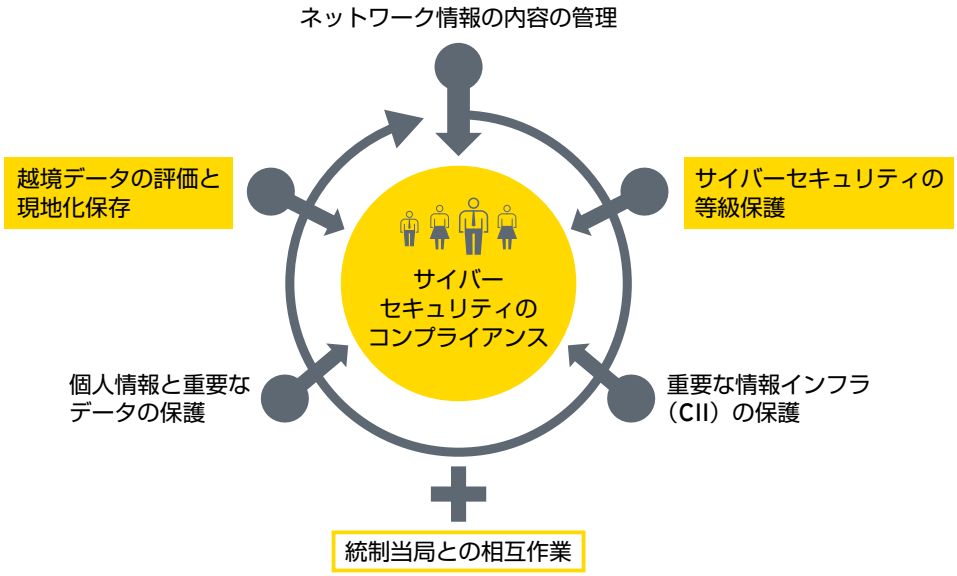
Ⅰ　はじめに

2016年12月から中国政府はサイバーセキュリティに関する法律を矢継ぎ早に改正し、先進国並みの法体系の整備を進めています。中国のサイバーセキュリティ法の特徴は、その目的が国家の安全、国民生活、公共の利益を保護することにあります。従って、サイバーセキュリティ事故ないし情報漏えい事故が発生した場合に、国家の安全、国民生活、公共の利益に深刻な損害を与える可能性のある産業に対する監督に特に重点が置かれています。中国に進出している日系企業に即して考えると、多くの個人情報を扱っている金融機関や小売業、危険品を扱っている化学メーカー等は優先的に対応する必要があると考えられます。

Ⅱ　サイバーセキュリティ法の内容

サイバーセキュリティ法は①ネットワーク情報の内容の管理②サイバーセキュリティの等級保護③重要な情報インフラ（CII：Critical Information Infrastructure）の保護④個人情報と重要なデータの保護⑤越境データの評価と現地化保存の五つの領域から構成され、日系企業のような外資系企業にとって重要となるのは⑤越境データの評価と現地化および②サイバーセキュリティの等級保護となります（<図1>参照）。

▶図1　サイバーセキュリティ法の五つの領域



▶表1　等級保護2.0における等級の分類

等級付け			
侵害される対象	対象に対する侵害の程度		
	一般損害	厳重損害	特に厳重な損害
公民、法人、およびその他の組織の合法的な権益	第一級	第二級	第三級
社会秩序、公共利益	第二級	第三級	第四級
国家安全	第三級	第四級	第五級

1. 越境データの評価と現地化

データの越境に係る評価は、主に個人情報と重要情報を対象としており、個人情報の国外持ち出しについては、個人情報の主体が同意しない限り、個人情報の中国国外への持ち出しは禁止されています。従って、従業員情報や顧客情報を中国国外で保存しようとする場合は、個々に本人からの同意を取得する必要がある点に留意が必要です。また、有害化学物質の生産・保管をしている企業は、工場の平面図、化学品保管の建物の分布、倉庫面積等が重要情報に該当する可能性があることから、本社と情報共有を行う場合は事前にセキュリティ評価プロセスを経る必要がある点に留意が必要です。

2. サイバーセキュリティの等級保護

サイバーセキュリティの等級保護とは、国や組織の重要情報を保存・転送・処理する情報システムに対し、後述する等級に応じてセキュリティ保護を行わなければならないという規定になります。等級保護の対象となるものは主に、情報システムや工業システムなどになります。これら等級保護評価の対象となる情報システム、工業システムには大量の個人情報や重要なデータが保存されているため、情報漏えいなどが生じた場合、国や国民に一定の危害を及ぼすと考えられています。19年5月に等級保護に関する規定が改正され要求事項が引き上げられており（等級保護2.0）、12月から施行されています。等級保護規定においてはサイバーセキュリティ事故ないし情報漏えい事故が発生した場合に社会に対する影響の範囲が大きいほど、また、損害の程度が深刻なほど等級が高くなり、「第三級」以上の評価となった情報システムに対しては年1回の測定評価が必要となります（＜表1＞参照）。

Ⅲ　サイバーセキュリティ法の規定に違反した場合

企業がサイバーセキュリティ法の規定に違反した場合、処罰を受ける可能性があります。例えば、業務の一時停止や罰金（企業の場合、最高で百万人民元）および管理者に対する個人責任の追及の可能性があります。個人責任は罰金および拘束（最大で15日間）の可能性があります。

Ⅳ　おわりに

中国政府は諸外国の制度を熱心に研究していることから、もともとルールや規則が存在していなかった領域に突如として最新の制度が整備されるという特徴があります。従って、数年前の理解に基づき先入観をもって中国のビジネス環境を理解しようとすると、最新の規則・制度との間で大きな乖離（かいり）が生じている可能性があります。また、中国のサイバーセキュリティ法は国家の安全、国民生活、公共の利益を保護することを目的としていることから、他の国では当然行えると考えられる化学工場の見取り図等の本社との共有に一定の制限がある点に留意が必要です。

サイバーセキュリティに関しては、今後も継続的に制度改正が予想されていることから、常に最新の情報・法改正を把握できる体制を構築しておくことが望まれます。さらに、前述した等級保護制度については、国の指定した機関から認証を受けなければならないため、制度が定める認証プロセスを現地子会社が適切に履行しているかを確認しておくことが、コンプライアンスの観点から重要になります。