連載　プロマネの現場から
第 121 回　中国サイバーセキュリティ法・小論

蒼海憲治（大手 SI 企業・上海現地法人・技術総監）

中国に赴任して不便なことの一つは、日本で使えていた Google+や Yahoo などの検索サービス、Facebook、LINE、Twitter などの SNS サービス、youtube、Ustream、FC2、ニコニコ動画などの動画サービスが使えないことです。

その理由は、他国サイトの中で、中国国内からのアクセスが禁止されているサイトがあることと、かつ、数万人規模のサイバーポリスによるインターネットに対する検閲が行われているためです。このシステムは「金盾」と名付けられており、万里の長城をもじって「グレートファイアーウォール」とも呼ばれています。

もちろん､各サービスに対応する中国版のサービスである Baidu（百度）､WeChat(微信)、Youku（優酷）等があり、その多くのサービスが代替できています。とはいうものの、昨年２０１７年の夏から、それまで利用できていた yahoo や日経新聞ニュースも利用できなくなった際は、同僚の中国人からも、これまで手に入った必要な情報が入手できないと、ぼやきの声が聞こえました。

この同じ時期である２０１７年６月１日、「中国サイバーセキュリティ法」が施行されました。同法の原語は「中華人民共和国網絡安全法」であり、「インターネット安全法」とも直訳できますが、中国政府公式の英訳は「Cybersecurity Law of the People's Republic of China」であり、「中国サイバーセキュリティ法」と訳されることが一般的です。また、内容的にも、インターネットに限らず、デジタルデータの取り扱いについても定めているため、「インターネット安全法」より「中国サイバーセキュリティ法」の方が適切である、と思います。

昨年来、既に取り組んでいる企業が多いと思いますが、猶予期間は２０１８年度中であり、今年中の対応が求められています。

今回は、この「中国サイバーセキュリティ法」について紹介したいと思います。

過去の経緯を振り返ると、そもそも中国のサイバーセキュリティ法制は欧米諸国にくらべ立ち遅れていました。２００３年になって初めて、情報セキュリティについて検討する部門が設けられ、暗号化とセキュリティ研究・人材教育にかかわるガイドライン策定に取り組みはじめます。２０１２年、「国務院」が政策文書を発表し、インターネットを管轄する部門が開設されています。これ以降、中国のインターネット環境の急速な発展に伴い、中国のサイバーセキュリティ政策は大きく加速しました。そして、それまで「ネット信息服務管理方法」「ネット信息保護の強化について全国人民代表大会常務委員会の決定」「電

信条例」など、国家レベルで散在していたサイバーセキュリティ法令の集約が求められるようになり、２０１６年、本法である「中国サイバーセキュリティ法」が制定されるに至ります。

「中国サイバーセキュリティ法」は、全部で７つの章と７９の条文により成り立っています。

冒頭、第１条にて、「サイバーセキュリティを保障し、サイバー空間の主権及び国家の安全、社会公共の利益を維持し、公民、法人及びその他組織の合法的権益を保護し、経済・社会の情報化の健全な発展を促進するため、本法を制定する。」
とあります。
サイバー空間においても国家主権があり、それを守ることを目的としています。陸・海・空と同様に、サイバー空間においても、主権があるというのは他の国においても同様のようですが、サイバー空間における立ち位置には大きく２つあるといわれています（＊２）。１つは、通信・金融・エネルギーなど「国の安全、国民経済と民生、公共の利益に重大な危害を与え得るその他の重要インフラ」に対する国家重要インフラに対するサイバー攻撃を脅威とみなし、その保護を目指す考え方です。米国・欧州諸国・日本はこの立ち位置にいます。もう１つは、上記の国家重要インフラへの脅威に加えて、「国内体制を不安定にする情報」（第１２条）も脅威とみなす考え方であり、中国とロシアなどはこの立ち位置にいます。

・ネットユーザーに対する実名制の要求。

各種情報に接触できる従業員は「機密保持協議」に署名し、電信業務運営者に実名登録をする必要があります。

「第２４条　ネットワーク運営者がユーザーのためにネットワーク接続、ドメイン名登録サービス、固定電話、携帯電話等の加入手続を行う、又はユーザーのために情報公表サービス、インスタントメッセンジャーサービスを提供するにあたり、ユーザーと合意書を締結する又はサービスの提供の確認を行うときは、ユーザーに真実の身分情報の提供を要求しなければならない。」

本法の対象となるのは、「ネットワーク運用者」であり、この「ネットワーク運用者」が、サイバーセキュリティ保護義務を負います。

「第９条　ネットワーク運営者は、経営及びサービス活動を実施するにあたり、法律、行政法規を遵守し、社会道徳を尊重し、商業倫理を守り、信義誠実の原則に従い、サイバーセキュリティ保護義務を履行し、政府及び社会の監督を受け入れ、社会的責任を負わなければならない。」

この「ネットワーク運営者」ですが、「ネットワークを構築、運営する又はネットワークを通じてサービスを提供する」（第１０条）が対象となっており、ネットワーク所有者、ネットワーク管理者及びネットワーク・プロバイダーが含まれ、当社もその対象となります。

・サイバーセキュリティ等級保護

サイバーセキュリティについては、自己点検もしくは、公的な「情報安全レビューサービス機構」に依頼し、ネットワーク安全レベルを確認してもらい、コンプライアンス体制の改善に協力してもらうことが同法では推奨されています。

「第２１条　国は、サイバーセキュリティのレベル別保護制度を実施する。
ネットワーク運営者は、サイバーセキュリティレベル別保護制度の要件に基づき」安全保護義務を履行する必要があります。

そのため、自社がどの等級であるか、その等級で求められているサイバーセキュリティレベル保護がどのようなものかを確認して、実施する必要があります。

・重要情報インフラ運営者

これに該当する事業者は、「ネットワーク運営者」以上に、その保護を目的に中国当局の強い統制を受けることが明確に規定されています。

「第３１条　国は、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、電子政府等の重要な産業及び分野、並びにひとたび機能の破壊、喪失又はデータの漏洩に遭遇した場合、国の安全、国民経済と民生、公共の利益に重大な危害を与え得るその他の重要情報インフラについて、サイバーセキュリティ等級保護制度に基づき、重点保護を実施する。」

まず自社が「重要情報インフラ運営者」に該当するかの見極めが必要になります。もし「重要情報インフラ運営者」に該当する場合、それに対応する対策をとる必要があります。

しかし、自社が「重要情報インフラ運営者」でない「ネットワーク運営者」であった場合でも注意が必要となります。

たとえば、当社の場合、自社でデータセンターを有しているのですが、このデータセンターを利用している顧客が、新たに「重要情報インフラ運営者」となるサービスを開始する場合、自社自身も「重要情報インフラ運営者」とみなされる可能性が極めて高くなります。そのため、顧客が「重要情報インフラ運営者」となるサービスを実施するかの事前の把握が必須となります。もしこれに対応できない場合、結果として法令違反となり、データセンターそのものが活動停止となる恐れがあるからです。

・セキュリティ製品の認証

重要なサイバー設備・セキュリティ製品については、中国当局のセキュリティ認証が義務付けられています。

「第２３条 基幹ネットワーク機器及びサイバーセキュリティ専用製品は、関連の国家規格の強制的な要求事項に従わなければならず、資格を有する機構の安全認証に合格した又は安全検査で要件に適合した後に、販売又は提供することができる。」

今回の法案では、セキュリティ製品に対して、さすがにバックドアの設置までは求められていませんが、外国企業にとって大きな参入障壁となっています。従来から、ソフトウェア・プロダクトを販売する場合、ソフトウェアのソースコードの提出を求められています。そのため、中国でビジネスをする場合、そのままのソースコードを提出するのか、それとも中国版のソフトウェアを開発し、そのソースコードを提出するのか、という選択をする必要がありました。特に、暗号化に関するロジックはセンシティブになっているため、中国国内向けのソフトウェアには、暗号化のロジック部分を外す等の苦労話を時折り耳にします。

・国外へのデータ移転

中国国内のデータを海外に移転することは、原則的に禁止されることが明確化される。

「第３７条　重要情報インフラの運営者は、中華人民共和国国内での運営において収集及び発生した個人情報及び重要データを、中華人民共和国国内で保存しなければならない。」

データ移転における当局の監査では、当該事業者のセキュリティシステムが開示されることとなり、副次的なリスクに発展する懸念があります。そのリスクを極小化するためには、本国と中国でまったく異なるセキュリティシステムを構築し、中国における開示事項やリスクが、本国まで及ばないように隔離することが有効です。しかしながら、構築における費用と時間的なコストが大きくなります。ただし、この点については、今回の「中国サイバーセキュリティ法」の施行以前から懸案事項となっていたため、本国とは別に中国国内向けのシステムを構築されているケースの方が多いのでは、と思います。

また、データセンターを運営するような場合では、中国企業と連携して中国国内にデータセンターを設けることで、今後継続して法規制の遵守に対応しやすくなると考えています。

・法的責任と罰則

第六章「法的責任」は、第５９条から第７５条まで及んでいます。
サイバースペースにおける中国当局の強い権限が規定され、違反者には高額な罰金を含む罰則が与えられることが明確化されていました。違反した企業だけでなく、責任者への罰金は、強い牽制になっています。

中国の法律は、最初にまず大きく網をかぶせ、それから詳細を決めていくという進め方をとることが多いといわれます。本法においても、現時点、条文の解釈を含むとまだまだ確認するべき事項も多く、現在、法律事務所とも相談しながら、自社の対策を引き続き検討・実施しています。今後もアンテナを高くして、フォローしていきたいと思っています。

＜参考＞
（＊１）中華人民共和国サイバーセキュリティ法（2016 年 11 月 7 日第 12 期全国人民代表大会常務委員会第 24 回会議にて可決）、中国人大網 2016 年 11 月 7 日
（＊２）http://www.sp-network.co.jp/column-report/spneye/candr20016.html
中国サイバーセキュリティ法の概説と企業リスクについて(2017.9)
2017/09/06 / 総合研究室：研究員・山岡渉出版社、２０１４年刊