CLARA ONLINE China Internet Report
2016.8.22

中国版サイバーセキュリティ法案の影響

株式会社クララオンライン
コンサルティングチーム

<要約と結論>

中国政府がインターネット領域の安全保障を目的とする、いわゆるサイバーセキュリティ法案の成立を目指している。2015 年 7 月に公開された第一次草案の内容は、中国で事業を行う外資系企業に大きな影響を与えると物議をかもしたが、修正を経て 2016 年 6 月に発表された第二次草案についても、世界各国の商工団体や業界団体が強い懸念を表明している。

同法案では、その目的を「サイバースペースにおける主権と国家の安全および社会の公共利益を維持するため」、「公民、法人の合法的な権益を保護し、情報化の発展を促進するため」と定めており、インターネットを含む情報ネットワークの「製品とサービス」、「インフラ設備と運営」、「データと情報」という 3 分野の安全保障をうたっている。対象となる製品やサービスは具体的に言及されていないが、インターネットに接続可能なデバイスやいわゆるインターネットサービス全般が該当すると考えてよさそうだ。

当局は、同法案によってインターネット利用者の個人情報保護が強化されるとしているが、草案の内容には表現があいまいで、明確に定められていない事項も多く、「別途国務院が規定する」という詳細の決定を先送りするような記述も見受けられる。中にはグローバルな基準を無視したものや、外資系企業の事業展開を阻む可能性の高い内容も含まれている。特に「中国国内のビジネスで発生した個人情報や業務データは国内に保存しなければならない」とする条項や、これらのデータを海外の本社などに送る際には当局のセキュリティ評価を受ける必要があるとの規定には海外から反発が強まっている。また「突発的な事態が発生した場合、特定地域の通信を制限する」との規定も明文化されており、中国ビジネスにおける新たなカントリーリスクの一つとなりそうだ。さらに罰則は、法人に対する処罰だけでなく、直接の責任者や関係者といった社員個人に対するものも定められており、大変厳しい内容となっている。

政府の関係者は、早ければ年内にも同法が成立すると公の場で発言しており、第二次草案を修正した段階で正式発表する可能性もある。この場合、他の法令でもよくみられるように不足する部分を実施細則という形で整理し、追って発表するものと思われる。世界各国からはサイバーセキュリティ分野におけるグローバルスタンダードの採用が期待されるが、今後どのように修正されるのか法案の行方が見守られている。

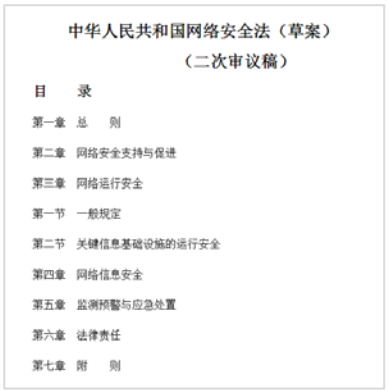
1. 中国がサイバーセキュリティ法案を検討

2015 年 7 月、中国全人代はインターネット分野の安全保障を目的に政府による情報管理を強化した「网络安全法（網絡安全法）」、いわゆる“サイバーセキュリティ法”の草案を発表した。その内容はインターネット関連事業者のみならず、中国で事業を行う海外企業にも大きな影響を与えるとして物議を醸し、パブリックコメントの募集とおよそ 1 年に渡る修正期間を経て、2016 年 6 月に第二次草案が発表された。

第二次草案に対するパブリックコメントの募集は 8 月 4 日に締め切られているが、日米欧など世界 46 の国と地域の商工団体が、本草案の内容に強い懸念を表明する書簡を李克強首相に送ったほか、米国保険協会をはじめ日本、イギリス、欧州などの保険業界団体が中国保険監督管理委員会主席宛に同様の書簡を送っているという。

2015 年以降、中国は様々な分野の安全保障に関する法案を相次いで制定しており、本法案も最優先課題の一つとされる。工業情報化部ネットワーク安全管理局の趙志国局長は、今年 5 月に貴州で開かれた「第 13 届中国信息港論壇」の席上で、順調に審議が進めば年内にもサイバーセキュリティ法が成立すると発言しており、法案の行方に注目が集まっている。

2. 法案の概要


中华人民共和国网络安全法（草案）
（二次审议稿）
目　录
第一章 总　则
第二章 网络安全支持与促进
第三章 网络运行安全
第一节 一般规定
第二节 关键信息基础设施的运行安全
第四章 网络信息安全
第五章 监测预警与应急处置
第六章 法律责任
第七章 附　则

このほど公開された第二次草案をみてみると、法案の目的は「サイバースペースにおける主権と国家の安全および社会の公共利益を維持するため、また公民、法人、その他組織の合法的な権益を保護し、経済社会の情報化の健全な発展を促進するため」となっている (第一条)。

内容はおおむねインターネットを含む情報ネットワークについて「製品とサービスの安全保障」、「インフラ設備と運営の安全保障」、「データ・情報の安全保障」の 3 分野に関するもので、インターネット利用者の個人情報等の保護強化をうたう一方で、当局がデータ・情報の収集、分析、監視を行う権限を定めており、違法行為に対する処罰も明記されている。

また本法案は、「中国国内における情報ネットワーク(网络)の構築、運営、管理保守、使用、およびサイバーセキュリティの監督管理」に適用される(第二条)。つまり、外資企業か中国企業かを問わず、中国でビジネスを展開するいわゆる IT 企業のほか、インターネットを使用する一般ユーザーも対象となるものと思われる。草案では具体的な対象業種に触れていないが、後日改めて言及する可能性もある。

なお、第七章の附則で「网络(網絡)」の定義を確認すると、“コンピューターやその他の情報端末、関連設備等で生成されたデータの収集、保存、転送、交換、処理を行うシステム”と記されており、インターネットだけに限定していない点に留意する必要がある(本レポートでは「情報ネットワーク」と記す)。

3. 第二次草案のポイントと懸念点

先にも触れたように、本法案では「製品とサービスの安全保障」、「インフラ設備と運営の安全保障」、「データ・情報の安全保障」の 3 分野について言及している。ここでは修正後の第二次草案について、日系企業が中国で IT ビジネスを行う際に関係すると思われる条文をみてみよう。

第二十一条　网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当及时告知用户并采取补救措施，并按照规定向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期间内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；收集公民个人信息的，应当遵守本法和有关法律、行政法规关于公民个人信息保护的规定。

第二十一条　情報ネットワーク製品およびサービスは、関連する国家標準に適合しなければならない。製品およびサービスの提供者は悪意のあるコードを埋め込んではならず、ぜい弱性等セキュリティ上のリスクが発覚した場合、速やかにユーザーに告知し救済措置を行うと共に、関係する主管部門に報告する必要がある。

情報ネットワーク製品およびサービスの提供者は、当該製品およびサービスのセキュリティメンテナンスを継続しなければならず、規定した期間あるいは当事者が取り決めた期間内はセキュリティメンテナンスの提供を取り止めてはならない。
情報ネットワーク製品およびサービスがユーザー情報を収集する機能を備える場合、当該製品およびサービスの提供者はユーザーに情報を取得する旨を明示し、同意を得なければならない。
個人情報を収集する場合、本法および関連する法律、行政法規の個人情報保護に関する規定を順守する必要がある。

まず“情報ネットワーク製品およびサービス”とあるが、具体的な対象製品や範囲は明記されていない。恐らくインターネットに接続可能なデバイスやいわゆるインターネットサービス全般があてはまるものと思われるが、今後、実施細則のような形で当面の対象範囲を明確化する可能性もあるだろう。非常に範囲の広い単語を用いる傾向は他の通信関連法規にも見受けられるもので、特にインターネット領域では次々に新しい概念のサービスが生まれているため、現時点で範囲を限定したくないとの意向も感じられる。また“関連する国家標準”が具体的にどの規定を指すのか明確になっておらず、製品やサービスごとに確認すべき国家標準が違う可能性も考えられるため注意が必要だ。

第二十七条　网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十七条　情報ネットワークの運営者は、公安機関および国家安全機関が法に基づいて国家の安全維持活動あるいは犯罪捜査を行う際に、技術的支援と協力を行わなければならない。

第七章の附則で「**网络运营者** (情報ネットワーク運営者)」の定義を確認すると、“情報ネットワークの所有者、管理者および情報ネットワークサービスの提供者”と記されていることから、いわゆるインターネットサービスを提供する事業者も該当すると思われる。

米 FBI による iPhone のロック解除要請を Apple が断固拒否した事件は記憶に新しいが、本項の“技術支援”とは具体的にどのような協力がどの程度の範囲で必要なのだろうか。仮に同法案の施行後、当局からの協力要請を拒否できないとなった場合、iPhone の例でいえば、代わりにロックを解除するだけでよいのか、それとも解除に必要な技術

や書類等までも当局に提供しなければならないのか。特許やノウハウといった企業秘密や意図しない技術流出の可能性もないとは言えず、本項は日系企業にとって大きな懸念となりそうだ。

第三十三条　关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十三条　基幹情報インフラ設備の運営者が国家の安全に影響を及ぼす可能性が考えられる情報ネットワーク製品およびサービスを調達する場合、国家網信部門と国務院の関連部門が組織するセキュリティ審査に合格しなければならない。

国家の安全に影響を及ぼす可能性とは具体的にどういったものなのか、製品やサービスごとの可能性の有無は調達担当者が判断するのか、はては当局から対象製品の目録等が示されるのか、非常にあいまいな内容となっている。

セキュリティ審査の内容自体も明らかでないが、日系企業が販売・提供する情報ネットワーク製品やサービスを中国企業あるいは中国政府当局のような存在が購入する際には、製品のセキュリティ保護に関わる部分の書類を提供する等、何らかの形で審査への協力が必要となる可能性がありそうだ。

なお第六十三条において、セキュリティ審査に不合格あるいは審査を受けていない製品およびサービスを使用した場合、主管部門が使用停止を命令した上で、調達金額の 1 倍以上 10 倍以下の罰金を企業に科し、さらに直接責任を負う管理者とその他の関係者に対し 1 万元以上 10 万元以下の罰金を科すとしている。

第三十五条　关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的公民个人信息和重要业务数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十五条　基幹情報インフラ設備の運営者は、中国国内での運営において収集および生成した公民の個人情報および重要な業務データを中国国内に保存しなければならない。業務利用のため、これらを海外に提供する場合、国家網信部門が国務院の関連部門と制定した規定(弁法)に従ってセキュリティ評価を行う必要がある。法律および行政法規で他に規定がある場合は当該規定に従う。

インフラ設備の運営者が対象ではあるが、保存が必要な業務データの範囲が明確でなく、また保存期間についても触れられていない。海外提供の際に必要なセキュリティ評価についても、どのようなものなのか内容や基準が明らかでなく、機密事項の流出や海外ビジネスを行う上での過度な負担が懸念される。

なお第六十四条において、海外にデータを保存または無断で海外にデータを提供した場合、主管部門が違法所得を没収した上で 5 万元以上 50 万元以下の罰金、さらに状況に応じて業務停止、事業整理、業務に必要な許可証や営業許可証の取り消し命令を出すこともでき、直接責任を負う管理者とその他の関係者に対しても 1 万元以上 10 万元以下の罰金を科すとしている。

第四十条　网络运营者收集、使用公民个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的公民个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用公民个人信息，并应当依照法律、行政法规的规定或者与用户的约定，处理其保存的公民个人信息。

网络运营者收集、使用公民个人信息，应当公开其收集、使用规则。

第四十条　情報ネットワーク運営者が、公民の個人情報を収集、使用する場合、合法・正当・必要の原則に従って、情報を収集・使用する目的および方法、範囲を明示し、被収集者の同意を得なければならない。

情報ネットワーク運営者は提供するサービスと関係のない個人情報を収集してはならない。法律、行政法規の規定、双方の契約に違反して個人情報を収集・使用してはならず、法律および

行政法規の規定あるいはユーザーとの契約に従って、保存した個人情報を処理しなければならない。

情報ネットワーク運営者が公民の個人情報を収集・使用する場合、収集・使用に関するルールを公開しなければならない。

インターネットサービスにおける個人情報の取り扱いに関するルールがここに整理された点は評価できそうだ。続く第四十一条では、個人情報の漏えいおよび改ざんが禁じられ、本人の同意なく個人情報を他人に提供することも禁止されているが、個人が特定できないよう処理され、なおかつ復元できない状態のものに関しては除外されている。また第四十二条で、法律法規や契約に違反して個人情報が使われた場合、ユーザーが情報ネットワーク運営者に対し個人情報の削除を要求できると定めている。

なお個人情報の例については第七章の附則で、「姓名、誕生日、身分証番号、生物学的情報、住所、電話番号等を含むがこの限りでない」と記されている。

第五十六条　因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第五十六条　国家の安全と社会公共秩序を維持するため、社会の安全を脅かす重大な突発的事件の対処に必要であれば、国務院の決定あるいは批准を経て、特定地域の情報ネットワーク通信を制限する等の臨時措置を行うことができる。

突発的事件の定義が明らかでない上、特定地域で通信を制限しても社会秩序の安定という面では、その効果は限定的と思われる。しかし中国に拠点を持っている、あるいは中国と取引のある日系企業にとって通信制限によるビジネスへの影響は測り知れない。草案の通りに公布された場合、法令によって明確に記された新たなカントリーリスクとなることを認識しておく必要があるだろう。

4. 世界の業界団体が懸念を表明

本法案の第二次草案については、世界の商工団体や業界団体が共同で懸念を示す書簡

を送っているほか、日本からも意見書が提出されている。中国日本商会や電子情報技術産業協会(JEITA)等の業界団体が共同でまとめた意見書では、同法案は外国企業の市場参入を阻害する過度な規制であるとの認識を示すと共に、グローバルな基準を無視した中国独自の国家規格による管理では、サイバーセキュリティの強化という本来の目的に逆行する恐れがあると指摘している。また草案では具体的な要件や対象に言及されていないなど遵守すべき規定が不明確である一方、罰則規定は具体的に示されており、恣意的な罰則の適用を懸念していることも伝えている。

一方の中国外務省は 8 月 16 日、米ロイター社に対して「同法案は外資系企業を国内企業と異なる扱いにしたり、貿易や対中投資に障害や障壁を設けたりするものではない。海外の投資家や企業が懸念する必要はない」とする声明を送っている。サイバーセキュリティ法は 2015 年の政府の重要課題とされていたもので、施行を急いでいるのか当局担当者も年内に法案が成立する可能性を示唆する発言をしている。第二次草案に対しては世界中から反対や批判、懸念が示されているが、年内成立を優先するならば、第二次草案を修正した段階で正式発表し、実施細則は運用しながら追って発表するという他の法令でもよくみられる形式をとることも考えられる。今後どのように修正されるのか、法案の行方を見守る必要がありそうだ。

网络安全法（草案二次审议稿）(中国語)

http://www.npc.gov.cn/npc/flcazqyj/2016-07/05/content_1993343.htm