2019年5月31日
JIPDECセミナーレポート

中国サイバーセキュリティ法の概要と日本企業への影響について

株式会社エス・ピー・ネットワーク
総合研究部　研究員　　山岡　渉　氏

１．「中国サイバーセキュリティ法」の概要

（1）CS 法制定の背景

2014 年、国家安全保障体制の総合的なビジョンを示した「総合的国家安全保障観」のもと法整備が行われ、「反スパイ法」「反テロリズム法」「国家安全法」の公布を経て、2015 年に「中华人民共和国网络安全法（中国サイバーセキュリティ法[※1]（以下、「CS 法」という。）」の初案審議、パブコメが実施された。その後、2016 年に「国家インターネット空間安全戦略」の表明、CS 法修正案の審議・パブコメ実施を経て CS 法再修正案が採択・公布され、2017 年 6 月に CS 法が施行された。

本法は、日本を含め各国の個人情報保護を観点とする法制化とは異なり、あくまでも**中国国家の安全保障を目的**としているところが特徴となる。

※1）CS 法の邦訳は「サイバーセキュリティ法」「インターネット安全法」等、さまざまな呼び方をされているが、法自体がサイバー空間のセキュリティに関する内容であることから、本稿では「サイバーセキュリティ法」と称す。

ビジネス環境でのサイバー空間の拡大やビッグデータの利活用の進展により EU 一般データ保護規則（GDPR）をはじめとした各国による権益の保護の取組みが活発化する中、中国には統一的なサイバー法制・個人情報保護法制がなかったことから、サイバーセキュリティの確保、データの国外移転に関する規制が急ピッチで進められている。決してサイバー法制・個人情報保護法制についての規定がなかったわけではなく、各種法令に分裂・分散・重複しているのが現状である。

CS 法は「特別法」として、基本法として内容が原則的であり、詳細は下位の法令（図１）で規定される。

国家ネットワーク・インシデントレスポンスプラン	ライン
ファクトリー・オートメーションシステム ネットワークセキュリティ・インシデントレスポンス管理業務ガイドライン	個人情報および重要データの輸出に関するセキュリティ評価弁法
ネットワーク攻撃定義および描写規範	データの輸出に関するセキュリティ評価ガイドライン
ネットワークセキュリティ・インシデントレスポンス演習通用ガイドライン	個人情報セキュリティ規範
サイバーセキュリティ脅威情報表示モデル	個人情報識別不能化ガイドライン
サイバーセキュリティ等級保護実施ガイドライン	ネットワーク製品およびサービス安全審査弁法
サイバーセキュリティ等級保護評価測定過程ガイドライン	ネットワーク重要設備およびネットワーク安全専用製品目録
サイバーセキュリティ級保護評価測定技術ガイドライン	ネットワーク製品およびサービス安全通用要求
重要情報インフラセキュリティ保護条例	情報技術製品安全検査測定機構条件および行為準則
重要情報インフラセキュリティ検査評価ガイドライン	情報技術製品安全制御可能評価指標
重要情報インフラ安全保障評価指標体系	などなど・・・
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	

図 1.中国サイバーセキュリティ法の下位法令（例）

なお、CS 法は独裁的、軍事目的といったイメージを抱かれがちで、それは必ずしも間違いではないものの、GDPR など各国の先進的な個人情報保護法規制を意識した内容となっている。すでに GDPR 対応の社内体制、管理規定を整備している企業であれば、その延長で基盤を整備していくことで充分対応は可能と思われる。

（2）CS 法の条文構成

CS 法は全 79 条から構成されているが、特に重要とされるのが「ネットワーク運用上の安全」および「ネットワーク情報の安全」に係る条項である。

1．総則（第 1～14 条）
2．ネットワークの安全に対する支援と促進（第 15～20 条）
3．ネットワーク運用上の安全（第 21～30 条）
4．ネットワーク情報の安全（第 40～50 条）
5．監視・事前警告および緊急事態対応（第 51～58 条）
6．法的責任（59～75 条）
7．附則（第 76～79 条）

2．CS 法のポイント

（1）構成

CS 法は①個人情報の保護、②規制対象「ネットワーク運営者」、③規制対象「重要情報インフラ運営者」、④機密情報の保全、⑤国外へのデータ移転規制、⑥セキュリティ製品の認証、⑦法的責任と罰則 で構成されている。

①個人情報の保護：中国国内での個人情報の収集・使用・保護に関する要件を定義

②規制対象「ネットワーク運営者」：

［定義］ ネットワークサービス事業者に限らず、社内でのネットワーク利用者、ウェブサイト開設や社内イントラネット運用事業者をも含むため、対象範囲が広く、ほとんどの事業者が該当する可能性がある。

［規制内容］

・情報漏えいなどのインシデント発生時の当局への報告・協力義務
・ネットワークの安全保護措置（中国のサイバーセキュリティが脅かされる可能性を示唆し、「サイバーセキュリティ等級保護条例」に定められる等級内容に基づき、セキュリティ担当者の選任、ログ保全、重要データの暗号化等の措置を講じる）

③規制対象「重要情報インフラ運営者」：

［定義］ ネットワーク運営者に含まれるが、より当局の厳しい規制を受ける立場にある。通信、エネルギー、金融、交通などの基幹インフラ事業者やマスコミ、コンピュータ、軍事、科学研究などの重点産業。通信関係、情報インフラ関係は運営設備自体が規制対象となる。

［規制内容］

・データの中国国内保存義務
・必要に応じて国外移転する場合は当局からのセキュリティ評価の義務づけ
・（当局による）年 1 回のセキュリティ監査実施
・重要データの域外移転時には監督部門への報告の義務づけ（5 月 29 日パブコメ稿）

注）本法での規制対象には「インターネット製品およびサービス提供者」（ネットワークインフラサービス事業者）も含まれるが主に上記 2 つに区分されると思われるので、自社の中国子会社がどの規制対象に該当するか認識しておく必要がある。

④機密情報の保全：中国国内で収集・生成した重要データ、個人データの国内保管を義務付け（国外移転禁止）。従業員の個人情報、機微情報、医療データは域内保存対象となる。

⑤国外へのデータ移転規制：個人情報および重要データの域外移転は原則禁止。域外移転を望む場合は、当局の監査を受ける必要がある。

⑥セキュリティ製品の認証：重要インフラなどの機材、設備について当局のセキュリティ認証が必要となる。

⑦法的責任と罰則：違反者には罰金または罰則が与えられる。 違反時の罰金は 5 万元（約 78 万円）など、GDPR に比べ、罰金の高額設定はされていない。

ただし、刑事罰に問われた場合は取引、営業停止、サイト閉鎖などの厳しい処分がくだされる可能性がある。また、行政罰だけにとどまらず、当局（消費者保護委員会）が対象企業に対して民事訴訟を起こした実例もあり、中国固有のリスクについても留意が必要となる。

（2）個人情報の取扱いについて

個人情報の取扱いについては国家標準「個人情報セキュリティ規範」（2017 年 12 月公布、18 年 5 月施行）に示されているが、GDPR やカリフォルニア州消費者プライバシー法など欧米の先行法制を意識した内容となっている。本規範は「推奨標準」であり強制力はないが、中国の法文化では推奨標準を根拠に当局が処分を下したり裁判所が判決を下す可能性があるため、重視すべき規範となる。

本規範は、個人情報と機微情報が厳密に区分されており、それぞれ詳細な類型が定められているため、ポリシー策定時など、文案を参照することができる。

（3）データの越境規制について

データの越境規制対象は以下の 2 点である。

①個人情報：「個人情報セキュリティ規範」の類型が参照可能。

②重要データ：「データの輸出に関する安全（セキュリティ）評価ガイドライン」参照。ただしまだ草稿段階のため、判断が難しい。

CS 法および下位法令では現段階でガイドラインが発行されていなかったり、未確定の法令が多く不透明のため、自社が規制対象に該当するのか、また、取り扱う情報資産の見極めが必要となる。

規制対象データは原則国内保存となるが、必要に応じて国外移転する場合は安全（セキュリティ）評価実施が必須となる。なお、CS 法では「重要情報インフラ運営者」のみが対象となっていたが、下位法令の「個人情報および重要データの輸出に関するセキュリティ評価弁法」により「ネットワーク運営者」も対象となったため、法令が正式公布となった際にどこまでが対象となるか、その時点での確認が必要となる。

なお、GDPR ではリスクベースで域外移転の規制等が示されているが、CS 法や下位法令では移転の定義が明確化されていないため、非公知のデータを国外から電子的にアクセス・閲覧する行為も含まれる可能性があり（例：中国支社の社内サーバに機密保管した従業員データに日本本社からアクセスするケースなど）、運用面での難しさは否めない。

「データの輸出に関するセキュリティ評価ガイドライン」で、安全対策の実施対象は定められているが、具体的な評価、運用が規定されていない。CS 法上評価は自社で行う、と規定されているが、実際自社で行うのは難しく、当局の評価を受けることによる企業秘密の漏えい、通信の秘密の侵害を脅かされ兼ねない。

３．CS 法に係る近時の取締り事例

現時点で日本企業に対しての当局からの規制は見られないが、国をあげて支援されている大手中国企業に対してであっても処罰や立入り検査が行われており、当局の規制に対する本気度が見られる。

2017 年以降の取締り事例として、サイトの不正アクセス被害、サイト利用者情報の不正保存、個人情報漏えい事件、スマホアプリを使ってのプライバシー侵害等で何社かが取締まり対象となっているが、処分内容としては、警告・改善命令、個人情報保護要請などにとどまっている。なお、実名登録の未履行や虚偽情報の流布など、サイトコンテンツ管理上の違反については、サイト停止や掲載内容の削除などの処分が下されている。

中国やロシアでは、当局に対し不利益となる、あるいは反体制情報流布もサイバー攻撃とみなしていることからコンテンツ管理にも厳しい処罰対象となっており、検閲を義務づけていることから、自社のコンテンツ管理にも注意が必要である。

４．カントリーリスク（中国固有の法体系）への対応

日本と異なり、中国では国固有の立法体系があり、最高国家権力機関（全国人民代表大会常務委員会）が制定する法律／条例（正式な法律）や、内閣に該当する国務院、地方政府が定める規則等間での連携がなく、個別に立法・運用される場合がある。また、長期にわたり暫定法やパブコメ稿のまま、正式に施行されないまま適用されるケース、職権が生じる当局機関・部門も多岐にわたるため、該当の法令の動向に留意しておく必要がある。

５．事業者としての備え

前述のとおり、CS 法対応に対し過剰に怖がる必要はなく、CS 法の「どこに該当するか」「なにをすべきか」を見極め、まずは海外子会社の統制、情報監査のデータマッピングを行い、地固めをするしかないだろう。

事業者としてすべき備えとして以下の２点が挙げられる。

①インターネット安全等級の見極め：自社が「安全等級ガイドライン」のどの等級（１～５等級）に相当するかにより、自社が求められるセキュリティ施策に対応する。

②保有する情報資産の洗い出し：越境規制に抵触しないよう検討する。

CS 基準に先行するインターネット法制基準を見ると、プロセス重視（手続き主義）であることがわかるため、正確な安全等級と保有情報資産が把握できていれば、おのずと対応が可能となる。

海外事業の内部統制管理のため、関連部署へのヒアリング等で情報の入手（収集目的、入手経路、管理体制、利用）から外部への提供に至る情報資産の統一管理（データマッピング）と業務の実態把握が重要である。これらの体制整備にあたっては、各法令のパブコメ内容を参照するのもよい。

CS 法はあくまでも基本法のため、以下の下位法令をモニターしておくべきである。

①個人情報セキュリティ規範（施行済）:個人情報の扱いがわかる。

②サイバーセキュリティ等級保護条例：自社がどの等級に該当するかの見極めることができる。

③個人情報および重要データの輸出に関する安全（セキュリティ）評価弁法：国外移転への対象、重要データの定義がわかる。

④データの輸出に関するセキュリティ評価ガイドライン：求められる監査手法が示されている。

⑤データセキュリティ管理弁法（５月 28 日パブコメ稿公表）：事業者がビッグデータを構成した場合、当局からの閲覧命令が出た場合にデータを開示しなければならなくなる。特に IT 関連業、製造業に関してはソースコードや設計図の流出の可能性も否めない。

海外子会社を持つ企業においては海外子会社統制の基本となるが、監査部門だけでなく、法務部門、事業部門、情報システム部門が連携して実態把握、情報管理規定へのフィードバックなど、該当部門をフォローしていく必要がある。

６．まとめ

CS 法への対応として重要なのはデータマッピングと CS 法制とのギャップ分析が必要である。すなわち、その時その時の CS 法制に対して、どう取り組むのかという方針と、自らどう取り組んでいるかという実態を、事業者が正確に判断し、把握することである。情報管理体制と、実際の運用部署間でギャップが発生していないか、ギャップ分析と実態把握の積み重ねにより CS 法にどう対応すべきかの判断、体制整備につながるのではないか。

以上