CLARA ONLINE China Internet Report
2017.10.23

今すぐやろう！サイバーセキュリティ法の概要と対策

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>

中国サイバーセキュリティ法の施行から 5 カ月が経ち、関連法令がほぼ出揃ってきている。あいまいな表現がされていた部分や後ほど改めて詳細を出すとしていた規定が段階的に発表され、一部はまだパブリックコメント募集の段階ではあるものの、当局が求める内容が概ね明らかになってきた。

本レポートではサイバーセキュリティ法の概要について、現時点で明らかになっている関連法令の内容を補って整理し、今やれること・やっておくべきことをまとめた。社内規定のとりまとめや必要な人材採用など、準備に時間がかかったり専門家の支援が必要となったりする場合もあるだろう。

すでにサイバーセキュリティ法を根拠とした取り締まりが行われており、党大会が終了した冬以降には徐々に本格的な運用が始まるものと思われる。ただし現時点で確定していない法令も多いため、法令の動向に注意を払い、今できる対策については速やかに取り掛かることが望ましい。

1. 周辺規定ほぼ出揃う

2017 年 6 月 1 日に中国版サイバーセキュリティ法が施行されてから 5 カ月が経つ。中国に進出する日本企業は約 1 万 4,000 社に上ると言われるが、サイバーセキュリティ法の内容を把握し、実際に対策までとっている企業はまだ多くないようだ。法令の内容があいまいだとか、どこまできちんと運用されるかわからないから様子見したい、といった理由で対応を先延ばししているケースも見受けられるが、法令の公布から 1 年ほどが経ち、個々の詳細な規定はほぼ出揃ってきている。次ページ以降で、特に重要な規定と取るべき対策を整理してみた。法令の概要を把握したら、できるものから順に速やかに準備に取り掛かった方がよいだろう。

法令の冊子は書店で 4 元

2. 法令の概要と必要な対策

● サイバーセキュリティ法の対象

インターネットや社内システムなど、なんらかのコンピュータネットワークを使用している企業、つまりほとんど全ての企業や組織が該当すると判断される。中国資本の現地企業はもちろんだが、出資比率など関係なく合弁企業や外資企業も対象に含まれる。これを本法では「ネットワーク運営者」と表現している。

この他、「ネットワーク製品またはサービス提供者」も対象で、こちらはサーバーなどのネットワーク機器メーカーやインターネットプロバイダ等が含まれる。

一部例外もあるが、中国でビジネスを行う日系企業は法令の対象！

● セキュリティ保護義務

企業のサイバーセキュリティ対策を義務化したもので、責任者の任命、セキュリティ管理規定の作成、技術的な対策の実施、ネットワークの監視と 6 カ月のログ保存、データの分類・バックアップ・暗号化、インシデント発生時の危機管理計画の策定を行わなければならない(22・25 条)。

また使用するネットワーク製品・サービス、サイバーセキュリティ製品は、国の強制標準に適合したものを利用しなければならない(23 条)。これは今後、合格製品のリストが出されることになっている。

自社のサイバーセキュリティ対策の内容確認、危機管理計画の準備も！
使用している通信機器やサービスの洗い出しに着手！

● 重要情報インフラの範囲と当該運営者への要求事項

重要情報インフラとして、通信、情報サービス、エネルギー、交通、水資源、金融、公共サービス、電子行政の各分野が挙げられている(31 条)。より具体的な範囲は関連法令で定められており、まだパブリックコメント募集の段階で確定していないものの、政府機関、エネルギー、金融、交通、水利、教育、衛生医療、社会保障、環境保護、公益事業、通信網、ラジオ・テレビ放送、インターネット等の情報ネットワーク、クラウド

サービス、ビッグデータ、国防科学工業、大型機械、化学工業、食品・薬品、ラジオ・テレビ・通信社等の報道機関となっている(关键信息基础设施安全保护条例（征求意见稿）18 条)。

これら重要情報インフラに該当する領域の事業者は、前述のセキュリティ保護義務の各項に加えて、専門のセキュリティ管理機構とその管理責任者の設置、社員へのセキュリティ教育・技能研修の実施、危機管理訓練の実施、自社あるいは外部委託による年 1 回以上のサイバーリスク評価の実施が必要となる(34・36 条)。またネットワーク製品・サービス(PC、情報端末、OS、システムソフトウェア、クラウドサービス、データ処理・ストレージサービスネットワーク通信サービス等)の購入時には、購入先とセキュリティおよび秘密保持に関する契約書を交わすことが求められている(36 条)。

逆に重要情報インフラに該当しない領域としては、レストラン、ホテル、旅行、農林水産業、小売・卸売、建設などが考えられそうだ。

自社の事業が「重要情報インフラ」に該当するか確認！
該当する場合は、セキュリティ管理チームの設置、社員教育や訓練の計画を！
製品・サービス購入時には、セキュリティ・秘密保持契約を確認！

- 個人情報・重要データの越境移転の制限

重要情報インフラの事業者については、中国国内の運営で収集・生成した個人情報や重要データを国内に保存することが義務付けられている (37 条) 。まだ修正中で未確定であるが、この国内保存を全ての企業に対して求める内容の関連規定も出ており、動向に注意が必要となる。

重要情報インフラの事業者は、中国国内のサーバーへ移行を！

なおここで言う「重要データ」とは、国家の安全や経済成長、公共の利益に密接に関わるデータで、現在その産業別ガイドラインのドラフト版が公開されている。重要データに該当するのは、主要事業の年間売上が一定規模 (約 3.4 億円) 以上の企業の経営情報や投資計画、電子情報分野ならばパラメータやソースコード等で、この規模に満たない企業の売上データや取引先情報といったものは該当しない。

またこの「個人情報」には、姓名、生年月日、身分証番号、生体認証情報、住所、電話番号、その他連絡先情報、ID、パスワード、財産の状況、位置・行動情報などが含まれている(76 条、个人信息和重要数据出境安全评估办法(修改稿)4・15 条) 。企業が個人情報の収集・使用を行う際には、収集・使用の目的、方法、範囲を明示して同意を得なければならない(41・42 条)。

個人情報を収集している事業者は、プライバシーポリシーの再確認を！

重要情報インフラの事業者であるかどうかに関わらず、中国国内の運営で収集・生成した個人情報や重要データを海外に持ち出す(越境移転)場合、その内容に応じて自社社内あるいは当局のセキュリティ評価チームによる審査を経なければならない(37 条)。同意を得ていない個人情報など越境移転できないデータもあるが、一般的な業務データであれば、多くが越境移転できるものと思われる。社内でのセキュリティ評価方法については、次章で取り上げる。

なおこのセキュリティ評価作業は、まだ確定していない関連規定に 2018 年末まで猶予するとの記述があり、こちらも動向を注視する必要がある。

越境移転しているデータの内容を確認！
社内安全評価作業チームに必要な専門人材確保に着手！

- 新たなカントリーリスク

国家の安全や社会秩序維持を目的として、当局に特定地域のネットワーク通信を制限する権限が認められている(58 条)。

中国国内の企業や組織は、政府による監督の受け入れに加え、公安機関や国のセキュリティ機関が行う安全保障・犯罪捜査において、技術的な支援や協力を行う義務があることも把握しておく必要がある(9・28 条)。この規定には、諸外国から機密事項の漏えいを危惧する声が上がっており、また協力期間が長引けば事業運営にも支障が出ると懸念されている。

ネットワーク遮断時を想定した事業継続計画(BCP)の策定を！
当局の要請に応じた場合に漏えいの可能性がある機密情報の確認を！

- 罰則

当局からの是正命令や警告にすみやかに応じなければ、法人に対してだけでなく、責任者個人にも過料が科される可能性がある。さらに業務停止、WEB サイトの閉鎖、営業許可証の取消等の処分も行われる可能性がある(第六章)。

3. 社内セキュリティ評価とは

個人情報や重要データの越境移転時に必要なセキュリティ評価は、データの内容によって社内に設置したセキュリティ評価チームあるいは産業ごとの主管部門が実施することになっている。どちらが実施するかは次のデータが含まれているかどうかによる。

- 50 万人分を越える個人情報
- 核施設、生物化学、国防軍事、人口・健康等の領域のデータ
- 大型建設プロジェクト、海洋環境、センシティブな地理情報、重要インフラ施設の安全保障上の欠陥およびセキュリティ対策等に関する情報
- 重要情報インフラ運営者のデータ

これらのデータが
含まれる場合 …… 主管部門がセキュリティ評価を実施
含まれない場合 …… 社内評価チームがセキュリティ評価を実施

社内のセキュリティ評価の詳細は、推奨性標準規格という形で検討が進められており、パブリックコメント募集中のドラフト版が公開されている。今後、変更される可能性はあるが、参考までに概要を紹介しよう。

まず社内の法務、政策、セキュリティ、技術エンジニア、管理の専門スタッフを集め、セキュリティ評価作業チームを編成し、越境移転計画を策定する。評価作業を行うタイミングは、データの越境移転を行う際あるいは、すでに評価済みのデータに大きな変更があった時で、どのような項目をどう評価するのか詳細が定められている。

評価結果は報告書にまとめ、少なくとも 2 年の保存が必要だ。また重要情報インフラの運営者や国家の安全、経済発展および公共利益に影響を与える可能性のあるデータについては、評価結果を当該主管部門に報告しなければならない。

セキュリティ評価の結果、越境移転禁止と判断された場合は、データのマスキング処理等でリスクの低減を図り、再度セキュリティ評価を実施することになる。

また評価ポイントの概要は次の通りとなっている。ドラフト版ではそれぞれについて参照すべき国家標準やより詳細な確認項目が示されている。

① 個人情報……類型、センシティブさ、数量、範囲、技術的処理（マスキング等）
② 重要データ……類型、数量、範囲、技術的処理
③ データ移転元のセキュリティ保障能力……社内のセキュリティ管理体制、危機管理計画、技術的保障能力
④ データ移転先のセキュリティ保障能力……移転先の詳細(有効な許可証類、過去のセキュリティインシデントの発生状況、株主や主管部門の状況等)、セキュリティ管理体制、技術的保障能力
⑤ データ移転先の国家・地域の政治法律環境……個人情報保護に関する規定や専門組織の状況等、情報セキュリティに関する法令や国家標準、管轄部門の状況等

4. 問合せの多いケース

ここでは、これまで弊社に質問や問い合わせが多く寄せられたケースをいくつか紹介するが、サイバーセキュリティ法でどのような影響を受けるか、どう対策すべきかは、それぞれの企業の事業内容や運営状況などにより一概に言うことは難しい。自社で判断することが難しければリスクアセスメントサービスの利用を検討するのもよいだろう。

Q：中国企業との合弁会社があります。弊社の出資比率は 49%ですが、サイバーセキュリティ法の対象でしょうか。

A：当該合弁会社はサイバーセキュリティ法の対象と思われます。企業形態や出資比率、規模、法人登記の有無は関係なく、中国にある組織や機構であれば対象となります。

Q：中国に拠点はなく、日本から中国向けに越境 EC をやっています。サイバーセキュリティ法の対象になるでしょうか。

A：中国に拠点がないことから、現時点では対象外になると考えられます。ただし現在パブリックコメント募集段階にある関連規定に、「中国国内で登記していなくても、中国国内向けに製品・サービスを提供している場合は国内運営とみなす」との記述があるため、関連規定の動向に注意が必要です。

Q：中国にある自社工場の機械稼働データを日本の本社に送っています。個人情報は含まれませんが、データの越境移転制限の対象になるでしょうか。

A：機械の稼働データを「重要データ」に位置付けている産業分野であれば、対象になる可能性が高いと思われます。重要データか否かを判断する「識別ガイドライン」は、現時点でドラフト版が公開されていますので早めに確認しておくとよいでしょう。該当する場合、データの内容によっては越境移転自体ができない可能性もありますが、主管部門あるいは社内評価チームによるセキュリティ評価をパスすれば、これまで同様に越境移転可能です。

なお、「重要情報インフラ」に該当する産業分野の場合は、さらに中国国内で収集・生成したデータの国内保存が必要となります。

Q：オーダーメイドのヘルスケア関連製品を中国で販売しています。個人を特定できない形で顧客の測定データを日本に送信していますが、データの越境移転制限の対象になるでしょうか。

A：データの内容によっては、個人情報に該当する可能性があります。個人情報として保守的に対応するのであれば、日本に発注することについて本人の同意を得た上で、社内評価チームによるセキュリティ評価を実施すれば、これまで同様に越境移転可能です。

こちらも「重要情報インフラ」に該当する産業分野の場合は、さらに中国国内で収集・生成したデータの国内保存が必要となります。

Q：「重要情報インフラ」の産業分野に該当します。中国国内のサーバーへの移行を検討していますが、現地のクラウドサービスは心配です。AWS や Microsoft Azure のような海外サービスでもいいでしょうか。

A：中国国内にデータが保存される形であれば、海外のクラウドサービスでもかまいません。ちなみに中国における AWS や Azure の運営は、中国の大手データセンターが行っています。サポートや言葉の面で心配があれば、日系サービスの利用を検討してもよいでしょう。

Q：データを送信せず、出張のたびにパソコンや USB でデータを持ち帰ることを考えていますが、これでデータ越境移転の制限から外れることができますか。

A：どのような持ち出し手段であっても、データの越境移転とみなされます。