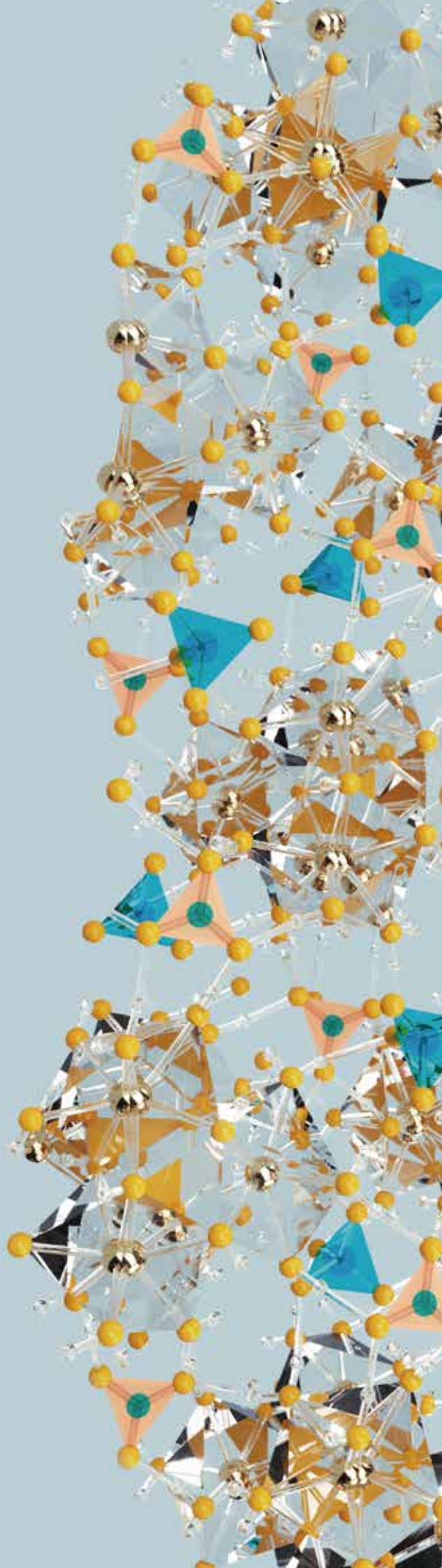
KPMG

KPMG Insight

KPMG Newsletter



Vol.37

July 2019

【海外Topic ②】
中国サイバーセキュリティ法対応における
重要ポイント

home.kpmg/jp/kpmg-insight

中国サイバーセキュリティ法対応における重要ポイント

KPMG中国
上海事務所
マネジャー　小川　晋一

小川　晋一
おがわ　しんいち

中華人民共和国サイバーセキュリティ法については、2017年6月の施行以来、日本においても新聞報道等で話題にあがっていますが、関連する一部の国家標準や条例がエクスポージャードラフトで止まっている、セキュリティ等級保護など馴染みのない概念がある等の事情により、現時点においてもなかなか具体的な対策に踏み切れない企業も多くあることと思います。一方で、法施行以来、公安による監督が実施されており、日系企業を含め取締りを受けた事例も発生しています。
本稿は、原稿執筆時点（2019年5月23日）における情報に基づき、当法律に重要ポイントについて、企業・組織が講じるべき対応策について解説します。
なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りいたします。

【ポイント】

- 当法律の目的は、法人・個人の権利や社会公共の利益の保護、及び国家安全保障となっている。
- 当法律における義務履行対象者は、中国に存在するほぼ全ての企業・組織が該当する。
- セキュリティ等級保護と個人情報保護については、既に関連する条例や国家標準等の細則が施行されており、早急な対応が必要。
- 重要情報インフラやデータ越境伝送については、確定した細則が存在しないものの、施行後に多大な人的・金銭的コストが発生する可能性もあるため、検討を開始することが望まれる。

I. 当法律の目的と履行義務者

当法律制定の目的は、法人・個人の権利や社会公共の利益の保護、国家安全保障となっています。そのため、後段でもこの法律の概念は記述しますが、企業・組織における“重要な”システム及び情報の保護を目的としたものではなく、あくまで上記を保障するために国家として重要と考えるシステム・情報の保護が目的となっています。

また、対象となる義務履行対象者は、全ての“ネットワーク運営者”が該当するとされています。“ネットワーク運営者”の定義については、第76条における“ネットワーク運営者”の定義及び“ネットワーク”の定義より、コンピュータを利用し社内外を問わずネットワークを介して情報をやり取りしている組織体であると解釈できるため、ほぼ全ての在華企業が義務履行者となります。そのため、外部に対してウェブサイト等ネットワークを介したサービスを提供していなくとも、履行義務が生じることとなります。

II. 重要ポイント

当法律の重要ポイントとして、セキュリティ等級保護・個人情報保護・重要情報インフラ・データ越境伝送の4つが挙げられます。

このうち、重要情報インフラ及びデータ越境伝送については、現時点において正式施行に至っている条例や国家標準等の細則が存在しないため、一部業界向け[1]を除き取締事例は出ておりませんが、当局から個人情報は中国大陸内のサーバに保存するよう指導された事例は発生しております（取締ではありません）。また、仮に正式施行後にはサーバの移設やネットワークの変更等が必要になる可能性もあるため、検討は早めに開始されることをお勧めします。

また、セキュリティ等級保護及び個人情報保護については、既に施行済みの条例や国家標準が存在するため、早急な対応が求められます。特に等級保護に関しては公安当局が制定・施行した監督指針に基づいた積極的な取締が行われています。

III. セキュリティ等級保護

組織体の保有するシステムが破壊される、若しくは情報が外部に漏えいした場合の、各客体に対する影響度合いにより各システムの等級を定め、その等級に応じたセキュリティ保護を実施しなければならない、とされています（**図表1**参照）。

耳慣れない用語だと思いますが、考え方自体は20年以上前から存在しているため、中国内資企業においては対応されている例は多くなっています。

損害の程度については、個人情報の漏えいなどはわかりやすい例と言えますが、例えば生産管理システムなどにおいても、システムが破壊された場合に社内外のサプライチェーンの広範囲に影響を及ぼすことが考えられる際には、各客体に対する影響が非常に大きいと判断される場合があります。

図表1　各客体と損害の程度による等級判定図

客体	各客体が受ける損害の程度		
	一般的な損害	重大な損害	特に重大な損害
公民、法人及びその他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

また、等級判定結果については各地方公安当局へのファイリング（備案）が義務付けられています。1）組織内等級判定及び等級に応じたセキュリティ保護の実施、2）等級保護に関する有資格者による審査、3）各地方公安当局への届出、という流れになります。

等級保護の対象システムについては、中国大陸内にあるものであれば、外部に接続されているものに留まらず、イントラネットについても考慮が必要とされています。また、クラウドシステムについては、運営者側・利用者側双方での等級保護が必要とされています。

更に、2019年5月13日に正式版確定がアナウンスされた新しい等級保護制度においては、生産管理システムやIoT、ビッグデータ等その保護対象が大きく広がった点についても注意が必要です。

上記の通り等級保護対象システムは中国大陸内にあるもののみとなっているものの、後述するデータ越境伝送や、当法律以外の規定等より、今後中国大陸内にサーバを設置する義務を負う可能性があることから、一概に国外に設置すれば良い、ということにはなりません。

なお、上述2）有資格者による審査では、等級判定結果だけでなく、等級に応じた保護が行われているか、についても検証が行われます。また、受審の都度費用が必要となります。

IV. 個人情報保護

基本的に日本の個人情報保護法に近いものとお考えいただくと良いかと考えます。個人情報の定義としては、電子的またはその他

1　当法律施行以前から有効である、遺伝情報等特定分野向けの細則に基づいた取締は法施行以前から実施されている。

の形式で記録された情報で、個別に、または他の情報を組み合わせることにより、特定の自然人の身元や活動を特定することが可能なもの、を指します。なお、これまで個人データの処理については成文化されておりませんでしたが、今回初めて成文化されたものとなります。なお、これまでの法的義務と変更は無い、と言われています。

個人情報保護の点で、特に注意すべき点としては、下記のようなものが考えられます。

- 個人情報と個人センシティブ情報とを区分し、それぞれ必要に応じたセキュリティ保護対策を実施すること。
- プライバシーポリシー上に、個人情報収集及び処理の目的・方法・範囲・ルールについて明示されていること。
- 個人情報収集及び処理の目的・方法・範囲・ルールについて、個人情報の主体からの明示的な同意を得ること。
- 収集する個人情報は、必要最小限度であること。
- 外部委託先への監督を実施すること。

V. 重要情報インフラ

※ 2019年5月23日現在関連細則がドラフト段階であるため、今後内容が変更される可能性があります。

システムの破壊やデータの漏えい時に、各客体に対して特に重大な影響を及ぼす可能性のある組織について“重要情報インフラ”として定義し、特別なセキュリティ保護措置を求める制度です。

重要情報インフラの例としては、下記が挙げられます。

- サービス業: 政府機関、エネルギー、金融、交通、水利、公共サービス等
- ネットワーク・マスコミ: 通信、ラジオ、テレビ、インターネット、クラウド、ビッグデータ等
- 科学技術: 国防科学技術、大型機器、化学、食品、医薬品等

特別なセキュリティ保護措置の一例は、下記の通りです。

- 内部管理制度及びオペレーション規程を確立し、身分証明及び権限管理を厳格に行うこと。
- ネットワークセキュリティ専門管理組織及びネットワークセキュリティ管理責任者を設置すること。
- 責任者及び重要職位者に対するセキュリティバックグラウンド調査を実施すること。
- 実務担当者に対して定期的なセキュリティ教育、技術研修、及びスキルアセスメントを行うこと。
- 定期的なセキュリティ・リスクアセスメントを実施すること。

上記の通り、“一般的な”システムに対するセキュリティ保護と比較して、非常に要求水準が高くなっているため、重要情報インフラに該当する可能性が高い企業においては、なるべく早めに検討を開始されることが望まれます。

VI. データ越境伝送

※ 2019年5月23日現在関連細則がドラフト段階であるため、今後内容が変更される可能性があります。

データ越境伝送については、日本企業の方々には一番関心の高い事項かと思われます。重要な点としては、基本的には個人情報及び重要データ[2]の越境送信時にアセスメントを義務付けているものであり、必ずしも全てのデータを越境させてはならない、という訳ではないことです。また、大原則として中国大陸内で収集・処理した個人情報（国籍は問わない）及び重要データについては、大陸内（クラウド環境を含め）に保存することが義務付けられます。

データの越境送信に該当する可能性の高いケースとしては、1）日本本社等中国大陸外にあるシステムを利用している場合、2）中国大陸内のシステムから大陸外のシステムへデータを同期している場合、3）中国リージョン以外のクラウドを利用している場合、4）中国大陸内にあるシステムのメンテナンスを大陸外から行っている場合、5）中国大陸内にあるデータを大陸外から閲覧する場合、が挙げられます。

なお、中国大陸内外で区分けがされるため、香港・マカオ・台湾への送信は越境に当たることに注意が必要です。

アセスメントでは、データの重要度の側面（個人情報の基礎点数1～3、重要データの基礎点数4）と、事件発生可能性の側面（1～3）より点数付けを行い、両方の点数をアセスメントマトリクス表にプロットし、網掛けのセルに該当した場合は原則としてデータの越境送信が不可と判断されます。

該当するデータ、特に重要データについては、組織の考える重要データと国家から見た重要度の違いから、見落とされるケースが多くなっています（**図表2**参照）。

2 重要データとは、組織内における重要度ではなく、中国政府から見た場合の重要なものになる。重要データについては誌面の都合上割愛するが、医薬品・食品の安全情報や各種統計データ、法人・個人を問わない金融取引データ等、非常に幅広い内容となっている。

図表2　データ越境送信に係るアセスメントマトリクス

データ重要度＼事件発生可能性	1	2	3
≧5	高	極めて高い	極めて高い
4	中	高	高
3	低	中	高
2	低	低	中
1	低	低	中

VII. 罰則と取締事例

1. 罰則

罰則としては、改善命令から過料、営業停止、営業許可取消等があります。過料の額は、法人に対して最高100万元、法人内の責任者に対して最高10万元が課されます。過料の額からすると、EUのGDPRと比較して非常に低く感じられるものの、最悪営業ライセンスの取消が課されるため、その点については注意が必要です。

また、個人情報の取扱いについては、サイバーセキュリティ法以外にも刑法等が適用される場合があります。

2. 取締事例

これまでの取締事例としては、Webサイトのコンテンツ関連（外部からの投稿された内容の管理が不十分、Webサイトに掲載されている地図情報の誤り、等）と、セキュリティ等級保護義務違反（公安への等級ファイリングが行われていない、定期的なセキュリティアセスメントが行われていない、相応の技術的措置が行われていない、等）が多くなっております。

これは、Webサイトについては監督機関以外の目にも触れることから、通報によって取締を受けた事例が多いものと考えられます。また、等級保護については考え方自体は過去から存在していたことから、当法律施行直後から事例が多く発生しています。

VIII. どのように対応を進めるか

1. システムとデータの棚卸・データの分類

この作業を行わずに対策を実施してしまうと、後になって対策漏れが生じる可能性があります。特に、IT部門が管理していない情報システムやデータについては注意が必要です。

また、データ分類が不十分な場合は、データ越境に関して対応する際に、本来不必要なコストを生じる可能性もあります（送信不要な重要データが保存・処理されるサーバを、中国大陸内に設置しなおす、等）。

2. セキュリティ等級保護の実施

上述の通り、既に公安による取締が盛んに行われています。そのため、まず個々のシステムの等級判定と、等級毎に求められるセキュリティ保護とのギャップ分析を実施することが望まれます。

3. セキュリティ管理態勢の構築

セキュリティ管理態勢及び管理責任者の設置をお勧めします。ここで言うセキュリティ管理態勢は、情報システムのみに関するものではなく、会社全体のセキュリティ管理態勢を指します。ISO27001を参考に、会社全体のセキュリティ意識及びセキュリティ対策の向上を図ることで対応が可能であると考えます。

4. 正式な細則が出ていないポイントに関する検討

特にデータ越境伝送に関しては、場合によってはサーバの移設・新設を含む対応が必要となる可能性があります。そのため、現段階からデータ越境伝送の必要性について再検討を行う、仮に中国大陸内へのサーバ設置が必要になった場合のプランを検討する、等の対応が必要であると考えます。

本稿に関するご質問等は、以下の担当者までお願いいたします。

KPMG 中国 上海事務所
マネジャー　小川 晋一
shinichi.ogawa@kpmg.com（7/31 まで）
shinichi.ogawa@jp.kpmg.com（8/1 から）

KPMGジャパン

marketing@jp.kpmg.com
home.kpmg/jp

home.kpmg/jp/socialmedia