M&P Legal Note 2019 No.3-2

「中国インターネット安全法」実施後の企業責任（第１回）

2019 年 4 月 19 日
松田綜合法律事務所
中国弁護士　徐　瑞静

第１　はじめに

２０１４年に中央インターネット安全及び情報化指導グループが立ち上げられ、習近平国家主席がキャップを務めてから「サイバー強国戦略」政策を提言し、インターネットのセキュリティ問題は国家戦略レベルまで引き上げられました。

２０１６年以後、中国政府は、相次いで、『中華人民共和国インターネット安全法』（以下、「インターネット安全法」という。）及び関連法令を公布・実施し、その結果、インターネット行為及び執行活動に法的拠り所となる根拠を提示しました。現在、政府及びその所属部署は、インターネットのガバナンスについて、積極的に取り組んでおり、サイバーセキュリティ、個人プライバシー等のセンシティブ情報に対する保護を図っています。

中国インターネット安全法は、サイバー問題の枠組み的な法令、すなわち、その基本法と位置づけられるものであり、当局は、目下、関連法令、下位法令、施行法の制定に向けて準備していると見られます。サイバーセキュリティに関わる法令が多岐にわたるため、次回以降のニュースレターにおいて、順次、紹介することとして、ここでは、インターネット安全法の規律の対象となる企業が、インターネットに関わる製品、サービス、運営及び個人情報を取り扱う場合における注意事項について説明します。

第２　インターネット安全法の適用範囲及び対象

１　適用範囲

インターネット安全法は、中国国内においてインターネットを構築、運営、保守及び使用し、並びにインターネット安全の監督管理を行ういずれの場合についても、インターネット安全法を適用することを定めています。すなわち、インターネット安全法は、中国国内のＰＣ端末、移動端末及びその他インターネットを使用する行為を、その適用範囲として広くカバーしています。またそれにとどまらず、中国域外からの攻撃情報などの伝播の遮断、そして、厳しい罰則に関しても規定しています。

２　適用対象

インターネット安全法は、①インターネット運営者、②インターネット製品・サービス提供者、③重要インフラ整備運営者、④その他の個人及び組織という４つの対象について、それが、中国企業か外国企業か、個人か組織か、また、有料か無料かにかかわらず適用されることになります。

(1) インターネット運営者の定義について

インターネット安全法においては、その第７６条第３号において、インターネット運営者についてのみ定義されています。同条の規定によれば、インターネット運営者とは、インターネットの所有者、管理者、及び、サービス提供者をいいます。そのため、企業は、ウェブサイトの所有者であれば、ウェブサイトの管理者になり、また、同時に、インターネットを通じてユーザーに対するサービスを提供すれば、サービスの提供者と認定されることになるものと思われます。

(2) その他の適用対象の定義について

適用対象について、インターネット安全法では、上記インターネット運営者の定義にとどまっており、上記の他の３者、すなわち、②のインターネット製品・サービス提供者、③の重要インフラ整備運営者、④のその他の個人及び組織について、明確にそれらを定義する規定は設けられていません。③の範囲については、関連法令で詳細が定められる見込みですが、②及び④については、広範な企業が対象となると思われます。

第３　インターネット安全法の主な内容

１　インターネット製品、サービス上の規制

国家は、企業主体の事業ごとに、それに対して、異なるサイバーセキュリティ基準を採用しています。

(1) インターネット製品、サービスの提供者

①　救済措置

企業がネット製品やサービスなどを提供するとき、悪意プログラムを設置してはならず、かつ、製品やサービス上の欠陥、リスクが見つかった場合には、救済措置を施すほか、インターネット安全法規定に従って、ユーザーに通知し、主管機関に報告することになっています。

②　セキュリティメンテナンス

企業は、そのネット製品やサービスに対して、インターネット安全法規定又は約定の期間において、メンテナンスを行わなければなりません。

③　個人情報

企業のネット製品やサービスは、それにユーザーの個人情報を収集する機能がある場合、ユーザーの明確な同意を得なければならず、また、インターネット安全法及びそれに関連する法律や行政規定における個人情報保護に関する規定を遵守しなければなりません。

(2) 重要設備及びインターネットセキュリティ専用製品の提供者

企業がインターネットセキュリティに関わる重要設備や専用製品を提供する場合、国家強行性の基準を満たし、セキュリティ合格の認証が必要であり、それらの確認後に、ようやく、設備や製品の販売・提供ができるようになります。要するに、インターネットセキュリティに関わる重要設備及び専用製品がインターネット安全に影響を与えるものであり、民間業界による異なる基準を避けるため、国家インターネット主管部門が、それらの範囲を画定し、それらに関する具体的な判断基準（すなわち、施行細則）を設けることにより、製品の認証レベルの統一が図られています。

(3) 重要インフラ設備及びインターネットセキュリティ専用製品の提供者

重要インフラを運営する企業は、国家安全を脅かす恐れのありそうな製品やサービスを仕入れる場合、国家セキュリティ審査を経なければなりません。

2　インターネット運営上の規制

(1)　一般インターネット運営者

国家は、インターネット運営者の事業に対して、異なる内容を有する国家基準と業界基準を執行します。

①　セキュリティ等級保護

一般企業は、次のセキュリティ等級の保護義務が求められます。

- 安全規則の作成・責任の実行
- ウィルス・サイバー攻撃の技術措置
- ネット運営・技術の測定、６か月間データ記録保存
- データのバックアップ・暗証化
- 応急措置・救済措置の適応、関連部署への報告

企業および主たる責任者は、上記規制に違反する場合、その情状に応じて、是正、警告、過料などの処罰を受けることができます。

②　実名登録

今後、企業は、ユーザーのため、ネットワークへの接続、ドメインネーム登録サービス、固定電話、携帯電話などのインターネット接続手続、情報発信、リアルタイム通信等のサービスを取り扱うとき、契約の締結またはサービスの提供に際し、ユーザーの真実の身分を確認しなければなりません。

企業および主たる責任者は、実名登録の規制に違反した場合、その情状に応じて、警告、過料の他に、業務停止、ウェブサイト閉鎖、許可書・営業許可書の取消しなどの処罰を受けることになります。

③　緊急措置の策定

サイバーセキュリティ事件が起きたとき、企業は、速やかに応急の救済措置を施し、システム上の落とし穴やウィルスやサイバー攻撃リスクを処置し、それと同時に、規定に従い、主管機関へ報告しなければなりません。

セキュリティの安全を怠った場合、企業および主たる責任者は、警告、過料等の異なる程度の処罰に直面することになります。

④　サイバー犯罪行為の禁止

企業は、不正アクセスやデータ情報の窃取などの行為をしてはならず、また、他人がサイバーセキュリティを脅かすことを明らかに知りながら、その者に対し、技術、広告、支払決算などのような協力をしてはなりません。

中国刑法は、コンピュータに関する犯罪を設け、インターネット安全を脅かす行為を処罰するとともに、他人がサイバーセキュリティを脅かすことを明らかに知りながら、その者に対し、インターネット接続、管理、保存、通信などの技術をサポートし、また、広告、支払などのような行為を提供する場合にも、刑法上の犯罪として処罰の対象としています。一方、インターネット安全法においても、インターネット安全を害する活動、広告、支払などのような行為を提供する場合について、その行政処罰の規定が設けられています。

上記規制に違反することにより、刑事罰もしくは行政処罰を受けた者は、一定期間、または、今後、一切セキュリティに関わる職業に従事することができません。

(2)　重要インフラの運営者

一般セキュリティ等級の保護のうえ、国家は、重要なインフラを運営する者に対し、さらなる厳しい規定を設けています。

①　更なる厳しいセキュリティ等級の保護

- 専門セキュリティ機構と責任者を設定し、その責任者と重要ポジションに就く者の素性を調査すること。
- 定期的に、従業員に対し、インターネットの安全教育、技術育成、技能考査を行うこと。
- 重要システムとデータベースに対する復旧、バックアップを行うこと。

・　応急措置のマニュアルを作成し、定期的に訓練を行うこと。

②　セキュリティの審査

重要インフラ運営業者は、国家安全を脅かす恐れのある製品とサービスを仕入れる場合、国家セキュリティ審査を経なければなりません。

③　秘密保持契約の締結

重要インフラ運営業者は、上記②を仕入れる際、その提供先と秘密保持契約を締結し、セキュリティ秘密保持の義務および責任を明らかにしなければなりません。

④　越境データ移転の規制

中国域内で収集されたかまたは得られた個人情報と重要データは、中国域内に保存し、域外に提供しようとする場合には、セキュリティ評価を受けなければなりません。

⑤　測定評価

毎年少なくとも一回のサイバーセキュリティとリスクの測定評価を行い、かつ、その結果と対応措置を関連部署に報告しなければなりません。測定評価については、自ら進めるか、他社に委託することも可能です。

3　個人情報上の規制

(1)　秘密保持制度

企業が収集したユーザーの個人情報を保持する場合には、秘密保持制度を設けなければなりません。

(2)　情報の収集・使用

個人情報を収集・使用に当たり、企業は、その使用の目的、方法、範囲などをユーザーに開示すると共に、ユーザーの同意を得なければなりません。

(3)　情報の完全性

作成の元となった個人情報を復元できない匿名加工する場合を除き、企業は、ユーザーの同意を得ることなく、収集した個人情報について、漏洩、改ざん、破棄、並びに、第三者に提供してはならず、仮に、個人情報を漏洩し、破棄することになる場合には、救済措置を施し、ユーザーおよび政府部門に通知し、報告しなければなりません。

(4)　情報の管理

企業は、ユーザーからの不正情報発信の管理を強化するものとし、違法情報を見つけた場合には、不正情報の削除、保存の他、政府部門に報告しなければなりません。

(5)　情報の監督検査

企業は、苦情・告発の制度を設けて、苦情、告発の方法を開示し、速やかにこれらを処理しなければなりません。また、政府部門の業務執行活動に協力しなければなりません。

第４　まとめ

企業各社は、その業務内容と結び付けて、中国との間の情報の往来に関するサイバーセキュリティ制度を制定、調整することを求められることになるように思われます。

この記事に関するお問い合わせ、ご照会は以下の連絡先までご連絡ください。

中国弁護士　徐　瑞静
jo@jmatsuda-law.com

松田綜合法律事務所
〒100-0004
東京都千代田区大手町二丁目６番１号
朝日生命大手町ビル７階
電話：03-3272-0101　FAX：03-3272-0102

この記事に記載されている情報は、依頼者及び関係当事者のための一般的な情報として作成されたものであり、教養及び参考情報の提供のみを目的とします。いかなる場合も当該情報について法律アドバイスとして依拠し又はそのように解釈されないよう、また、個別な事実関係に基づく具体的な法律アドバイスなしに行為されないようご留意下さい。