2022年サイバーセキュリティおよびデータ保護に関する主要な法令の調査報告書

(2023年3月)

日本貿易振興機構(ジェトロ)

大連事務所

ビジネス展開支援課

報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）大連事務所が現地法律事務所 上海里格（大連）法律事務所に作成委託し、2023 年 2 月に入手した情報に基づくものであり、その後の法律改正などによって変わる場合があります。掲載した情報・コメントは作成委託先の判断によるものですが、一般的な情報・解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求めください。

ジェトロおよび上海里格（大連）法律事務所は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的損害および利益の喪失については、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたか否かにかかわらず、一切の責任を負いません。これは、たとえジェトロおよび上海里格（大連）法律事務所が係る損害の可能性を知らされていても同様とします。

本報告書に係る問い合わせ先：

日本貿易振興機構（ジェトロ）
ビジネス展開・人材支援部　ビジネス展開支援課
E-mail:BDA@jetro.go.jp

ジェトロ・大連事務所
E-mail:PCD@jetro.go.jp

目　次

2022年サイバーセキュリティおよびデータ保護に関する主要な法令の調査報告書

はじめに

中国の「サイバーセキュリティ法」、「データセキュリティ法」、「個人情報保護法」（以下「データ三法」という）は前後して公布、実施されたが、その中の多くの規定が原則的で、実行性に欠けているため、多くの企業を悩ませている。2022年、中国はサイバーセキュリティとデータ保護に関する多くの政策・法規を公布、「データ三法」の実施を強化し、多方面からセキュリティコンプライアンスの要求と基準を整備し、国家デジタルセキュリティの障壁をしっかりと築き、セキュリティ技術と産業の発展に指針を提供した。例えば、2月には、新たに改正された「サイバーセキュリティ審査弁法」が実施され、下半期には、次々と発表された3セットのデータ域外移転メカニズムが、中国のデータ域外移転制度の統括的な構築の幕を開けた。9月には、「サイバーセキュリティ法」が実施から5年ぶりの改正を迎えた。2022年はサイバーセキュリティとデータ保護分野の立法と法律執行がなされた年であり、企業のコンプライアンス構築に対する要求が高まった。

本報告書は、2022年に公布・施行されたサイバーセキュリティおよびデータ保護に関する政策法規のうち、日系企業が重点的に注目すべき七つの政策法規について、概要、企業への影響および企業の対応ポイントという三つの面から解説する。

1. サイバーセキュリティ審査弁法

1.1 概要

2021年12月28日、国家インターネット情報弁公室（以下「インターネット情報弁公室」という）、国家発展改革委員会（以下「発改委」という）、工業情報化部（以下「工信部」という）、公安部、国家安全部など13の部門が連携して「サイバーセキュリティ審査弁法」（以下「審査弁法（2022）」という）を改正した。その施行日は2022年2月15日である。今回の改正は、2020年の「サイバーセキュリティ審査弁法」（以下「審査弁法（2020）」という）が施行されて以来、初めての改正である。

「審査弁法（2020）」は 2020 年 6 月 1 日に施行されて以来、重要情報インフラ運営者（CIIO）の調達活動に対する審査および一部重要製品などに対して審査を実施することにより、重要情報インフラ（CII）のサプライチェーンの安全を確保し、中国国家安全の維持において重要な役割を果たしてきた。わずか一年後に、「審査弁法（2020）」が重大な改正を迎えたことは、政府部門のサイバーセキュリティおよびデータ保護への監督管理に対する決意を表している。今回の改正には主に下記の内容が含まれている。

(1) インターネットプラットフォームの運営者がデータ取扱活動を展開する際、国の安全に影響する、もしくは影響する可能性がある場合、サイバーセキュリティ審査の対象範囲に入れる。
(2) 100 万人以上のユーザーの個人情報を把握しているインターネットプラットフォームの運営者が海外で上場する場合、サイバーセキュリティ審査弁公室に対し、サイバーセキュリティ審査の申告をしなければならない。
(3) 海外で上場するインターネットプラットフォームの運営者に対し、提出予定の IPO など上場申請書類も審査書類の対象に入れられているため、強制的に提出が求められている、など。

1.2　企業に対する影響

2021 年 6 月 30 日、中国配車アプリの滴滴出行（ディディ）はニューヨーク証券取引所での上場を果たした。その後、インターネット情報弁公室は公告を発表し、「審査弁法（2020）」に基づき「滴滴出行」に対してサイバーセキュリティ審査を行った。審査期間内において、「滴滴出行」はユーザーの新規登録を受けてはならなかった。次に、インターネット情報弁公室は再度公告を発表し、個人情報への収集使用が中国の法律法規に違反していたことに対し、滴滴出行などのアプリを取り下げた。「審査弁法（2020）」が、中国証券監督管理委員会を弁法の発行機関ならびにサイバーセキュリティ審査システムのメンバー機関として追加したことは、中国企業の海外上場におけるサイバーセキュリティ問題が重要視されていることを示している。

「審査弁法（2022）」は製品およびサービス提供者の権利義務についても規定している。例えば、職務上の便宜を利用してユーザーのデータを獲得や使用はしてはならず、厳密にユーザーのデータの安全を保護する義務、審査用の資料の提出に協力する義務、当事者の未公開資料につき秘密を保持する義務、関連部門に通報する権利などが挙げられる。「審査弁法（2022）」は多方面から互いに牽制する方法により、サイバーセキュリティの公平性を確保している。

1.3 企業の対応ポイント

上記に対して、企業は下記のとおり対応すべきと考えられる。

(1) 企業の業務タイプを踏まえ、それぞれの業界における監督管理の重要ポイントと結びつけて、自社製品およびサービスに対し、サイバーセキュリティ審査の本質である「国の安全への影響または影響可能性」につき予め評価作業を展開する。

(2) サイバーセキュリティ審査が日々厳しくなる中、企業は業務コンプライアンスに対する事前の評価と是正により、できるだけサイバーセキュリティ審査の触発を回避すべきである。いったんサイバーセキュリティ審査が起動された場合、企業は関連部門の是正要求などに積極的に協力し、自ら損失を最小限にすることが望まれる。

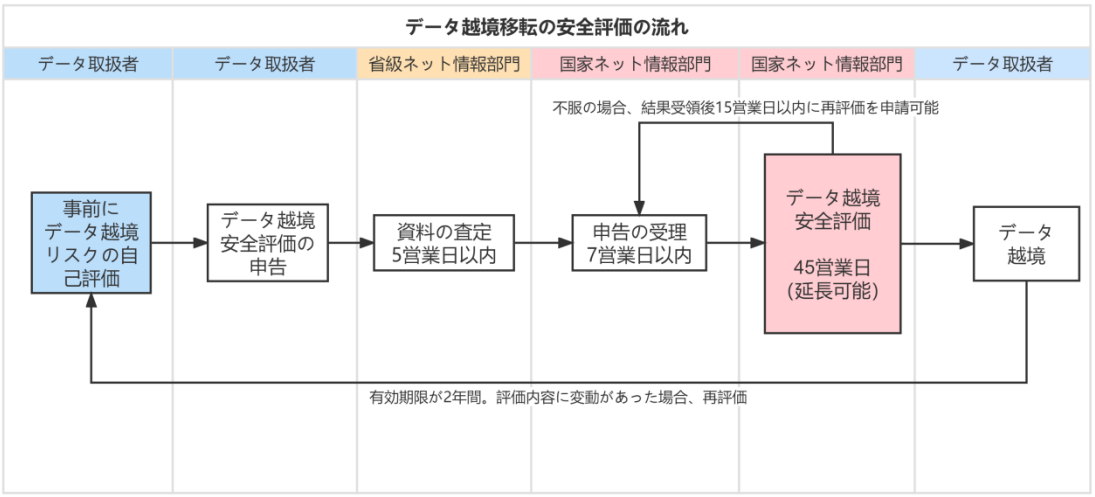
(3) 企業には、監督管理部門との持続的かつ流暢なコミュニケーションを保ち、かつ、「GB/T39204-2022 情報安全技術 重要情報インフラ安全保護要求」などの関連指針や基準における法的権利義務を整理し、迅速にフォローする能力を身につけることが要求される。

2. データの域外移転における安全評価弁法およびその申告ガイドライン（第 1 版）

2.1 概要

2022 年 7 月 7 日、インターネット情報弁公室より、「データの域外移転における安全評価弁法」（以下「安全評価弁法」という）が正式に公布された。当該安全評価弁法は 2022 年 9 月 1 日から施行された。データの域外移転における安全評価の実施を指導・支援するため、インターネット情報弁公室は 2022 年 8 月 31 日に「データの域外移転における安全評価申告ガイドライン（第 1 版）を公布した（以下「申告ガイドライン」という）。「安全評価弁法」にて定められた重要な内容は、申告の適用範囲・申告の流れおよび申告資料・申告前の自己評価義務・判断基準・安全評価の内容・域外移転先と約定すべき安全保護義務である。

一方、「申告ガイドライン」は責任部門・申告の流れおよび申告資料をさらに明確にした。「申告ガイドライン」の附属文書として、「担当者に対する授権委託書」「データの域外移転における安全評価申告書」「データの域外移転リスクに対する自己評価報告」の雛形が公布された。



2.2　企業に対する影響

「安全評価弁法」および「申告ガイドライン」の公布により、上位規則に言及された「データの域外移転における安全評価」に係る規定と要求が具体化された。特に、適用範囲の明確化により、各データ取扱者に具体的な要求が求められた。「安全評価弁法」の規定によると、データ取扱者は下記の基準と結び付けながら、自身が安全評価を申告すべきかどうかを判断する必要がある。

NO.	取扱者の条件	取扱対象の条件	越境移転内容
一	データ取扱者	-	重要データ
二	重要情報インフラ運営者（CIIO）	-	個人情報
	100 万人以上の個人情報を取り扱うデータ取扱者	-	個人情報
三	データ取扱者	前年 1 月 1 日から累計で 10 万人以上の個人情報を域外に提供	個人情報
		前年 1 月 1 日から累計で 1 万人以上の機微な個人情報を域外に提供	個人情報
四	国家インターネット情報部門が規定するその他のデータ域外移転セキュリティ評価を申請する必要がある場合		

申告が必要な場合、申告する前に規定に従って自己評価しなければならず、企業に

とって、大きな課題となる。さらに、「安全評価弁法」の第 20 条は、「本弁法が施行される以前に既に実施されたデータの域外移転については、本弁法の規定に適合していない場合、本弁法の施行日より 6 カ月以内に是正を完成させなければならない」と規定している。すなわち、企業にとってはデータの域外移転を是正するために 6 カ月間の「猶予期間」があり、2023 年 3 月 1 日までに完成させなければならない。

2.3 企業の対応ポイント

上記の要求およびその時間制限を踏まえ、データを域外に提供する必要がある、または既にデータの域外移転関連の業務を展開している企業は、できるだけ早く自社の性質、業務状況、重要データにかかわっているかどうか、域外移転先が確実に関連データを必要とするかどうかなどにつきポイントを整理し、分析する必要がある。上記の図のとおり、延長されなくても、安全評価は 57 営業日がかかる。従って、安全評価が必要と判断された場合、安全評価の手続きをスムーズに推進するため、できるだけ早く自己評価を実施することを勧める。

企業に課題を与える一方、企業にとっては、データコンプライアンスの整備を推進するチャンスでもある。「安全評価弁法」および「申告ガイドライン」を踏まえ、評価の作業を進めると同時に、社内の規則制度と対応メカニズムの構築を始めることができる。例えば、データコンプライアンス管理部門を設置すること、救済処置と緊急時の体制を確立すること、業界基準と結び付けながら自社の業務にかかわるデータのリスクを分析し、係る責任者を確定すること、社内でデータコンプライアンスの研修を行い、従業員を規定に適合するデータの域外移転作業ができるように教育することなどが考えられる。最後に、企業として、タイムリーに対応でき、イニシアチブを握るため、当該分野の政策変更と業界の実践を継続的にフォローアップする必要がある。必要に応じて専門家のサポートを求めることも考えられる。

3. 個人情報域外移転標準契約規定（意見募集稿）[1]

3.1 概要

2022 年 6 月 30 日、インターネット情報弁公室は「個人情報域外移転標準契約規定（意見募集稿）」（以下「標準契約規定」という）およびその附属文書「個人情報域外移転標準契約」（以下「標準契約」という）を公布した。

中国の「個人情報保護法」第 38 条の規定により、個人情報取扱者は、業務等の必要により、中国国外に個人情報を提供する場合、次の条件のいずれかを満たさなければならない。

(1) 本法第 40 条の規定に従い、国家インターネット情報部門の安全評価に合格していること。
(2) 国家インターネット情報部門の規定に従い、専門機構による個人情報保護認証を受けていること。
(3) 国家インターネット情報部門が制定した標準契約に基づいて、国外受領者と契約を締結し、双方の権利と義務を約定していること。
(4) 法律、行政法規または国家インターネット情報部門が規定するその他の条件。

「標準契約規定」と標準契約は、上述の「個人情報保護法」第 38 条第（3）項の規定を実行するためのものである。

「標準契約規定」は全部で 13 条あり、標準契約の適用範囲、主要内容、再締結が必要となる場合などの内容を明確にした。また、「標準契約規定」では、個人情報取扱者は標準契約が発効した後、事前に個人情報保護影響評価を行い、個人情報保護影響評価報告書を届出材料として、標準契約とともに所在地の省レベルのインターネット情報部門に届出をしなければならないと規定している。

「標準契約」には 9 カ条と二つの付録があり、条文の内容には主に個人情報取扱者の義務、国外受領者の義務、現地の個人情報保護政策法規による標準契約の遵守に対する影響、個人情報主体の権利、救済、契約解除、違約責任などが含まれている。

[1] 2023 年 2 月 22 日に本意見募集稿の正式版である「個人情報域外移転標準契約弁法」が公布され、6 月 1 日より施行される。

3.2 企業に対する影響

個人情報の域外移転安全評価、個人情報保護認証の関連細則はすでに公布、実施されている。「標準契約規定」と「標準契約」も公布、実施されれば、「個人情報保護法」第 38 条の下の関連細則はすべて整ったこととなる。企業は関連規定に基づき、自身がかかわる個人情報の越境提供について、法的要求を満たすと同時に、相応の事前手続きを完了する必要がある。さもなければ、コンプライアンス違反につながる可能性がある。

3.3 企業の対応ポイント

対応に追われてしまうことにならないよう、企業はまず自身が関与している、または関与する可能性のある個人情報越境移転状況を整理し、「標準契約規定」と「標準契約」を参考にした上で、すでに発表された個人情報の域外移転安全評価、個人情報保護認証に関する細則を総合的に配慮し、標準契約を結ぶことで海外に個人情報を提供する必要があるかどうかを確認することを勧める。

さらに、必要があれば、企業は「標準契約規定」と「標準契約」を参考の上、以下の点に留意すること。

(1) 個人情報の越境提供について、関連する保護制度（個人情報保護影響評価を含む）を確立・改善するか、または確立・改善することを直近の計画に組み入れ、企業自身の関連制度が法律の要求に適応できるようにする。
(2) 「標準契約規定」と「標準契約」が正式に公布、実施された後、順調に移行し、標準契約の締結が完成できるよう、事前に域外移転先と標準契約の締結について話し合い、域外移転先が「標準契約」による要求を満たすことができるかどうかを確認する。

4. 個人情報域外移転取扱活動安全認証規範および個人情報保護認証実施規則

4.1 概要

全国情報セキュリティ標準化技術委員会は、2022 年 6 月 24 日に「個人情報域外移転取扱活動安全認証規範」を発表した。さらにそれに対し細分化・整備を行い、半年後、同年 12 月 16 日に「個人情報域外移転取扱活動安全認証規範 V2.0」（以下「安全認証規範」という）を発表し、認証機関が個人情報取扱者の個人情報の域外移転取扱活動に対して認証を展開するための根拠を提供した。「安全認証規範」には、個人情報の域外移転における従うべき基本原則、基本要求および個人情報主体の権益保障などの内容が含まれている。「安全認証規範」は、個人情報の域外移転取扱活動を展開する個人情報取扱者と域外移転先は法的拘束力と実行可能な文書を締結し、個人情報保護責任者を指定し、個人情報保護機構を設立し、同一の個人情報の域外移転取扱規則を遵守しなければならないと規定している。また、国内の個人情報取扱者は、個人情報保護の影響評価を展開し、かつ個人情報保護影響評価報告書の作成を行い、当該評価報告書を少なくとも 3 年間保存しなければならないとの規定も盛り込まれている。

2022 年 11 月 4 日、インターネット情報弁公室と国家市場監督管理総局は共同で「個人情報保護認証実施規則」（以下「認証規則」という）を発表し、個人情報保護認証の適用範囲、認証根拠、認証モード、認証実施プログラム、認証証明書と認証マークなどの内容を明確にした。個人情報取扱者が個人情報の収集、保存、使用、加工、伝送、提供、公開、削除および越境などの処理活動を行うことを認証する基本原則と要求を規定した。「認証規則」によると、個人情報保護認証の認証モードは「技術検証+現場審査+取得後の監督」であり、認証実施において、認証委託、技術検証、現場審査、認証結果の評価と承認および取得後の監督などのプロセスを展開することが求められる。認証証明書は 3 年間の有効期間を有し、有効期間内に、認証証明書の有効性を保つため、企業は認証機関の継続的な監督を受ける必要がある。

4.2 企業に対する影響

「安全認証規範」と「認証規則」の公布と実施は、「個人情報保護法」第 38 条第 2 項に規定された個人情報保護認証制度の細分化と実行であり、国際的なデータ越境移動認証制度の構築に役立ち、関連認証の将来における国際相互認証のための基礎を築くことである。企業が個人情報保護認証を行うことは、将来の個人情報の域外移転取扱活動がコンプライアンス上、適切に実施できるだけでなく、認証機関の認証結果によって自身の個人情報保護能力を証明することもできる。現在、中国サイバーセキ

ュリティ審査技術と認証センター（CCRC）[2]は唯一承認された認証機関であり、個人情報の域外移転セキュリティ認証制度はまだ多くの課題に直面している。現段階で実際に展開するのにはまだ一定の困難があり、より詳細な認証実施プログラムと認証実施細則の公表が期待されている。

4.3 企業の対応ポイント

個人情報保護認証は、企業が個人情報保護分野におけるコンプライアンスレベルを証明するための有効な方法である。企業は自身の状況に合わせて、認証規範を含む関連規則に基づいて各コンプライアンスメカニズムを改善し、個人情報保護認証に関する立法と実務の動態に積極的に注目し、認証実施の必要性と実行可能性を積極的に検討することを勧める。特に、個人情報の域外移転取扱活動（特に多国籍企業や同一経済・事業体内の個人情報の域外移転取扱活動）に対しては、安全評価が必須ではない状況において、個人情報保護認証という方法の適用が考えられる。

5. 工業情報化分野におけるデータセキュリティ管理弁法（試行）

5.1 概要

2022 年 12 月 8 日、工業情報化部は、「工業情報化分野におけるデータセキュリティ管理弁法（試行）」（工信部網安〔2022〕166 号、以下「管理弁法」という）を公表し、工業と情報化分野の一般データ、重要データ、コアデータの三等級の区分法について詳細に規定し、かつデータセキュリティ監督管理と保護制度を詳細化した。中国で事業を展開している日系企業に製造加工業が多く、デジタル経済およびデータセキュリティ管理の最前線となる工業情報化分野にも注目すべきであると考えられる。

（1）重要データ、コアデータ目録の届出

「管理弁法」により、データ取扱者は、定期的にデータを整理し、その組織の重要データ、コアデータの詳細な目録を作成し、かつ所在地域の業界監督管理部門に届け出なければならない。届出の内容には、データの内容自体は含まれず、データのソース、類別、等級、規模、媒体、取り扱いの目的と方法、使用範囲、責任主

[2] 中国サイバーセキュリティ審査技術と認証センター：https://www.isccc.gov.cn/

体、対外共有、越境移転、安全保護措置などの基本状況を含むが、これらに限らない。

（2）安全管理の責任と機構を明確に

「管理弁法」により、重要データ、コアデータの取扱者の法定代表者あるいは主要責任者がデータセキュリティの第一責任者とし、管理チームにおけるデータセキュリティを管理するメンバーが直接の責任者として、データ違法行為発生時には「データセキュリティ法」における法的責任を負う。

（3）リスク評価の報告とセキュリティ・インシデント報告義務

「管理弁法」により、重要データ、コアデータ取扱者は自らまたは第三者評価機構に委託し、毎年少なくとも一回以上そのデータ取扱活動に対してリスク評価を行い、かつ所在地域の業界監督管理部門に報告しなければならない。重要データとコアデータのセキュリティ・インシデントが発生した際に、ただちに所在地域の業界監督管理部門に報告し、インシデント対応完了後に所定の期限内に報告書を作成し、毎年所在地域の業界監督管理部門に事案の対応状況について報告しなければならない。

5.2 企業に対する影響

データセキュリティ監督管理分野の基本法である「データセキュリティ法」により、工業、電信などの主管部門は、各業界・分野のデータセキュリティ監督管理職責を担い、データ分類級別保護制度を確立し、各地域、各部門は、当該地域、当該部門および関連業界、分野の重要データの具体的な目録を確定しなければならない。工業情報化部がこの度公表した「管理弁法」は、その職責範囲内の工業、電信、無線通信業界分野内のデータセキュリティ管理のために制定された最上位の制度である。今後は、「管理弁法」をめぐってセットとなる細則も公表される見込みである。

5.3 企業の対応ポイント

（1） 重要データとコアデータ目録の届出の時間が、まだ明確に規定されていないが、企業は「管理弁法」に従ってあらかじめ本企業がかかわっているデータを整理しておくことを勧める。届出の具体的な方法については、これから各地で手引きが公表される見込みである。

(2) 企業は本企業のデータセキュリティ業務システムを構築し、必要に応じてデータセキュリティ管理人員を配置し、重要ポジションの責任者に対してデータセキュリティ責任書に署名してもらい、その職責を明確にする。
(3) 企業は、毎年データ取扱活動を評価する必要がある。評価の基準と方法は、GB/T 20984-2022「情報安全技術　情報安全リスク評価方法」、GB/T 31509-2015「情報安全技術　情報安全リスク評価実施指南」、YD/T 3801-2020「通信ネットワークとインターネット・データセキュリティ・リスク評価実施弁法」など国、業界基準を参考にすることができ、第三者に委託して行うこともできる。
(4) 企業は、データライフサイクル管理を強化し、かつデータセキュリティ事件の緊急事態対応案を制定し、必要に応じて訓練を行う。

6. インターネット情報部門行政法執行手続規定（意見募集稿）

6.1 概要

2022 年 9 月 8 日、インターネット情報弁公室は「インターネット情報部門行政法執行手続規定（意見募集稿）」（以下「法執行手続規定」という）を公表した。以前の「インターネット情報内容管理行政法執行手続規定」に取って代わり、インターネット情報部門の行政法執行の対象となる案件のタイプもインターネット情報コンテンツ、サイバーセキュリティ、データセキュリティ、個人情報保護などへ明確に拡大された。その中で、管轄と適用について、行政処罰の案件は違法行為の発生地のインターネット情報部門が管轄し、違法行為の発生地は、違法行為を実施したネットワーク運営者の関連サービス許可地または届出地、主な営業地、工商登録地などを含む。調査・証拠収集について、電子データを収集・保全するため、インターネット情報部門は、現場またはリモートによる証拠収集、企業・個人へ電子データの固定と提出を命じることなどの措置を取ることができ、個人情報保護の案件として差し押さえるなどの行政的強制措置を取ることができる。公聴会・聞き取りについて、インターネット情報部門が比較的大きな金額の過料を科すなど六つの状況の行政処罰決定を下す前に、当事者は公聴会を行うことを申請する権利がある。

6.2 企業に対する影響

「法執行手続規定」はまだ意見の募集中であるが、「法執行手続規定」第 1 条の規定によると、「法執行手続規定」の上位法は「行政処罰法」およびデータ三法である。

「法執行手続規定」の導入がデータ三法の行政法執行面での具体化であり、インターネット情報分野における法執行の常態化時代の到来を示していることは明らかである。企業にとって「法執行手続規定」が施行されると、データ三法に違反するいかなる違法行為も、インターネット情報部門の処罰を受ける可能性があり、初期の実施段階ではその可能性がさらに大きいと見込まれる。しかし、同時に「法執行手続規定」は「行政処罰法」と同じく、インターネット情報部門が行政処罰を下してはならない状況と関係主体が公聴権利を享受すべき状況についても規定しており、関係企業は「法執行手続規定」に従って自らの合法的権益を積極的に守ることができる。

6.3 企業の対応ポイント

今後、「法執行手続規定」の実施に対応するためには、以下の四つのポイントが考えられる。

(1) 法規への継続的な注目。「法執行手続規定」がまだ意見募集稿であるため、企業は「法執行手続規定」の公式発表と実施状況を継続的にフォローし、その内容を熟知・理解する必要がある。

(2) コンプライアンス管理の強化。企業は、まず組織構造の改善から取り組み、専門の法務担当を設置するか、弁護士チームを雇用し、データセキュリティや個人情報保護、サイバーセキュリティなどの分野のコンプライアンスを強化し、企業運営における法的リスクと抜け穴を見つけ出し、速やかに改善し、リスクへの対応力を強化する必要がある。

(3) 不定期な法律の研修。初期段階でデータ三法に関する法律研修を行い、従業員のコンプライアンスと法的リスクに対する意識を高めるとともに、今後の「法執行手続規定」の正式発表と実施に伴い、関係者が企業の法的権利と法執行プロセスを十分に理解できるように、従業員に対し、どのような状況で公聴会を申請できるか、公聴会前の準備などの法律研修を行うことも推奨する。

(4) インターネット情報部門との交流と意思疎通の強化。企業は行政案件への重視を強化し、インターネット情報部門が許可した範囲で、事前相談、事件中の積極的な協力、事後のフィードバックを求め、企業経営の法的リスクを最小限に抑える目標を図る。

7. 「中華人民共和国サイバーセキュリティ法」の改正に関する決定（意見募集稿）

7.1 概要

2022 年 9 月 14 日、インターネット情報弁公室は、「『中華人民共和国サイバーセキュリティ法』の改正に関する決定（意見募集稿）」を公表した。今回の改正は、2016 年に公表し、2017 年 6 月 1 日に施行された「サイバーセキュリティ法」後の初めての改正である。

改正は、主に「サイバーセキュリティ法」の第六章の法的責任に集中され、第 59 条乃至第 70 条となった。例えば、下記の改正点等がある。

(1) 複数の違法行為を「インターネット運行安全保護義務」とし、より筋道が通るようになった。

(2) 「インターネット運行安全保護義務」違反を情状の重さによって「一般違法行為」、「是正拒否または情状が重い」、「情状が特に重い」の三等に区別し、異なる処罰措置を規定した。

(3) 「一般違法行為」に対し、「戒告・譴責」を行政処罰措置の一つとして導入した。これは 2021 年「行政処罰法」改正後、新たに加えられた処罰措置でもある。

(4) 処罰の度合を大幅に引き上げた。例えば、「是正拒否または情状が重い」違法行為に対し、企業に対する過料の上限を 50 万元から 100 万元に調整し、「情状が特に重い」違法行為に対し、企業に対する過料を 100 万元以上 5000 万元以下に調整した上、「前年度売上高の 5%以下」の過料も導入した。

7.2 企業に対する影響

「サイバーセキュリティ法（改正版）」は、立法プロセス上国務院、全国人民代表大会常務委員会両方の審査を通す必要があるため、可決、施行までは時間がかかると考えられる。一方、政府部門が立法でサイバーセキュリティ監督管理を強化し、企業の違法責任を重くし、法規定を厳しくする方向性は、すでに示されている。企業にとって、「サイバーセキュリティ法（改正版）」が今後正式に公表し、施行された場合、法的リスクも上がっていくと予想される。

なお、「サイバーセキュリティ法（改正版）」は、企業の規模を問わず、企業側の法的義務を多く定めているので、中小零細企業にとってコンプライアンス面のコスト増となる。軽微な法律・規則違反行為に対して「戒告・譴責」など新たな処罰

措置を加えたことは、中小零細企業にとっての朗報である。そして、「戒告・譴責」が常用処罰手段になると見込まれる。

7.3 企業の対応ポイント

「サイバーセキュリティ法（改正版）」がまだ立法準備の状態であることに鑑みて、企業が以下の対応策を講じることができると考えられる。

（1）立法および法執行の動向に注目すること。企業は、「サイバーセキュリティ法（改正版）」の内容を熟知し、立法プロセスおよび「サイバーセキュリティ法」の実務上の運用に注目する必要がある。国務院、全国人民代表大会常務委員会が、これから再び意見を募集するので、意見やアドバイスがあれば、その際に申し入れることも可能である。

（2）法的義務を整理すること。「サイバーセキュリティ法（改正版）」の内容は、主に法的責任に集中している。「サイバーセキュリティ法」の元の規定に基づいて、かかる法的義務をいったん整理し、違法行為のないように努めるべきである。今回改正内容の「ネットワーク運行安全、ユーザー個人情報保護、重要情報インフラ安全保護、ネットワーク情報安全義務」に特に注目し、コンプライアンス義務リストを作成し、全面的な分析、評価、是正を行う必要があろう。

（3）関連規則制度を整備すること。「サイバーセキュリティ法」により、ネットワーク運営者は、内部安全管理制度と操作規程を制定し、サイバーセキュリティ責任者を確定し、サイバーセキュリティ保護責任の確実な履行を保障しなければならない。従って、「サイバーセキュリティ法（改正版）」が違法責任を重くすることに鑑みて、企業は、ネットワーク運行安全保護義務の全面履行ができなければ、少なくとも制度面からの整備を始めることをお勧めする。

おわりに

2021 年に「データセキュリティ法」、「個人情報保護法」が相次いで公表し、施行されたことは、「データ三法」がベースとなるサイバーセキュリティ・データセキュリティ法体系が組み立てられたことを示している。そして 2022 年は、この体系がさらに発展した一年となった。新型コロナウイルス感染症の収束、中国と世界経済の回復に伴い、中国政府のサイバーセキュリティ、データ コンプライアンスを強化する勢いが続くと予想される。上記重要な法規、政策を読み返すことで政府監督管理の要求について理解し、対策を講じる必要がある。