中国「改正サイバーセキュリティ法」が日系企業に与える影響

2026 年 3 月
One Asia Lawyers Group
中国大湾区プラクティスチーム
森　仁司（日本法）

第１　はじめに

中国は、サイバーセキュリティ法（CSL）、データセキュリティ法（CDSL）、個人情報保護法（PIPL）の「データ 3 法」により、世界で最も厳格なデータローカライゼーション（国内保存）と越境移転規制措置を採っているとされています[1]。

今回は、2026 年 1 月 1 日に施行された中国のサイバーセキュリティ法（中国語：中华人民共和国网络安全法）の改正により、日本企業が受ける影響について取り上げます。

本改正は、中国におけるサイバー被害の急増など、ＡＩやデータ安全を脅かす事態となっていることを背景に、当該分野における法令遵守（コンプライアンス）の要請が一気に高まり、運用コストの大幅に引き上げを余儀なくされる内容となっています。

特に注目すべきは、罰則の強化と、データ管理・インフラ調達に対する国家安全保障上の監督強化です。多くの中国現地法人において、ＩＴ、クラウド等を活用されているものと思われますが、その管理方法を抜本的見直しが迫られる内容になっております。

以下、主要な改正点及び日系企業に与える影響について見ていきます。

第２　サイバーセキュリティ職務の基本方針の明確化

まず、サイバーセキュリティ職務の基本方針として「中国共産党の指導の堅持、総体的国家安全観の貫徹、発展と安全の統合計画及びネットワーク強国建設の推進」が明確にされました[2]。これにより、サイバーセキュリティ職務の国家戦略上の地位と指導原則が確立され、同職務が国家安全体系に正式に組み込まれることとなりました。

また、「国家は、人工知能の基礎理論研究およびアルゴリズム等の重要技術の研究開発を支援し、訓練データ資源、計算力等の基礎インフラ整備を推進し、人工知能倫理規範を整備し、リスクの監視・評価および安全監督管理を強化し、人工知能の応用および健全な発展を促進する。国家は、サイバーセキュリティ管理方式の革新を支援し、人工知能等の新技術を活用して、サイバーセキュリティ保護水準を向上させる。」と規定されました[3]。つまり、ＡＩがネットワーク強国建設の中核技術と位置づけられるとともに、その開発にあたっては、倫理規範の整備と安全監督管理の強化が求められています。そのほか、国として、ＡＩなどの技術を活用して自らのサイバーセキュリティ保護能力を向上させることを奨励するという意思が示されているといえます。

---

[1] 個人情報（及び重要データ）を中国から国外に移転する際には、(1)安全評価を当局に申告する、(2)個人情報保護認証を得る、(3)個人情報越境移転標準契約を締結し当局に届け出るのいずれかを行う必要があります。
[2] 改正サイバーセキュリティ法第 3 条。
[3] 改正サイバーセキュリティ法第 20 条。

第３　個人情報の取扱いに関する法律上の要求の多元化

「ネットワーク運営者[4]が個人情報を処理する場合、本法および『中華人民共和国民法典』、『中華人民共和国個人情報保護法』その他の法律・行政法規の規定を遵守しなければならない。」との規定が追記されました。

つまり、中国における個人情報保護について、ネットワーク運営者に対し、複数の法律の要求を同時に満たす義務が課せられたことを意味します。これにより、個人情報保護に関する企業のコンプライアンス運営に対する要求水準が上がったものと評価されています。

第４　過料の高額化、義務・責任の強化

１　サイバーセキュリティ保護義務の不履行[5]

サイバーセキュリティ保護義務[6]を履行しないネットワーク運営者に対する罰則が強化され、一般的な事情の下では 1 万元以上 5 万元以下の過料に、是正を拒み、又はサイバーセキュリティ上の危害結果を引き起こした場合には、法人については 5 万元以上 50 万元以下、直接責任者については 1 万元以上 10 万元以下の過料に処するものとされました。

また、重要情報インフラ運営者[7]によるサイバーセキュリティ保護義務[8]の不履行の場合は、さらに厳しい処分が課されるようになりました。

---

[4] ネットワーク運営者とは、ネットワーク（コンピュータ等の情報端末や関連設備によって構成される情報システム）の所有者、管理者及びネットワークサービス提供者をいうとされています（改正サイバーセキュリティ法第 78 条（3））

[5] 改正サイバーセキュリティ法第 61 条。

[6] 改正サイバーセキュリティ法第 23 条「ネットワーク運営者は、当該制度の要求に従い、次の安全保護義務を履行し、ネットワークが干渉、破壊または無権限アクセスを受けることを防止し、ネットワークデータの漏えい、窃取または改ざんを防止しなければならない。（一）内部の安全管理制度および操作手順を制定し、サイバーセキュリティ責任者を定め、サイバーセキュリティ保護責任を履行すること。（二）コンピュータウイルス、サイバー攻撃、ネットワーク侵入等、サイバーセキュリティに危害を及ぼす行為を防止するための技術的措置を講じること。（三）ネットワークの運用状況およびサイバーセキュリティ事案を監視・記録する技術的措置を講じ、規定に従って関連するネットワークログを少なくとも 6 か月間保存すること。（四）データの分類管理、重要データのバックアップおよび暗号化等の措置を講じること。

改正サイバーセキュリティ法第 27 条「ネットワーク運営者は、サイバーセキュリティ事件に関する緊急対応計画（インシデント対応計画）を策定し、システムの脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入等のセキュリティリスクに対して速やかに対処しなければならない。サイバーセキュリティに危害を及ぼす事案が発生した場合には、直ちに当該緊急対応計画を発動し、相応の是正措置を講じるとともに、規定に従って関係主管部門に報告しなければならない。」

[7] 改正サイバーセキュリティ法第 33 条は、「重要情報インフラ運営者」について直接定義を置くものではないが、「公共通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子行政サービス等の重要な産業分野、その他機能の破壊、喪失、またはデータの漏えいが発生した場合に、国の安全、人民の生活、公共利益に重大な危険をもたらす可能性がある重要情報インフラの運営者・・・」としている。

[8] 改正サイバーセキュリティ法第 35 条「重要情報インフラを建設する場合には、当該インフラが業務の安定的かつ継続的な運用を支える性能を備えることを確保し、かつ安全技術措置について、計画・建設・使用を同時に行わなければならない。」

改正サイバーセキュリティ法第 36 条「本法第 23 条の規定に加え、重要情報インフラの運営者は、さらに次の安全保護義務を履行しなければならない。（一）専門の安全管理機構および安全管理責任者を設置し、当該責任者および重要ポストの従業員について安全に関する身元調査（バックグラウンド審査）を行うこと。（二）従業員に対し、定期的にサイバーセキュリティ教育、技術研修および技能評価を実施すること。（三）重要なシステムおよびデータベースについて、災害復旧（ディザスタリカバリー）用のバックアップを実施すること。（四）サイバーセキュリティ事故の緊急対応計画を策定し、定期的に訓練（演習）を実施すること。（五）法律および行政法規で定めるその他の義務。」

発生した状況	法人に対する処分	直接責任者に対する処分
一般的事情	是正命令・警告 5 万元～10 万元の過料併科	―
是正拒否 または　危害結果の発生	10 万元～100 万元の過料	1 万元～10 万元の過料
重大な危害結果の発生（データの大量漏洩、一部機能喪失など）	50 万元～200 万元の過料	5 万元～20 万元の過料
特に重大な危害結果の発生（主要機能の喪失など）	200 万元～1000 万元の過料	20 万元～100 万元の過料

このように、重要情報インフラについては、改正前と比べて 10 倍の過料が課されるなど、に大幅強化されました。日本円にして 2 億円を超える罰金ということで、多くの企業にとっては経営を揺るがし、事業継続に大きな影響を及ぼす金額であるといえます。

また、違反企業はは社名が公表されるため、取引先のサプライチェーンから除外されるなどのリスクにさらされることが考えられます。

さらに、違反が発覚した段階で業務停止処分を受けることになりますので、中国からの撤退を余儀なくされる状況に追い込まれます。

加えて、違反行為に関与した管理者や担当者個人への罰金も強化されており、現地法人に出向した日本人駐在員や、現地責任者にも直接的な法的責任が及びます。

また、こうした罰金に加えて、業務停止、営業許可証が取り消される、信用リストへの登録されるなどのペナルティも明文化されました[9]。信用リストに登録されると、公共入札や許認可更新にも影響しますので、中国での事業展開が非常に難しくなるものと考えられます。

２　製品安全認証/検査の不履行

安全認証、安全検査を受けていない、または認証不合格もしくは検査要件に適合しないネットワーク重要設備又はサイバーセキュリティ専用製品を販売または提供する行為については、政府の主管機関が販売、提供の禁止を命じ、警告を与え、違法所得を没収するとされました[10]。

さらに、違法所得がない場合または 10 万元未満の場合は、2 万元以上 10 万元以下の過料、違法所得が 10 万元以上の場合は、違法所得の 1 倍以上 5 倍以下の過料が併科され、情状が重大であれば、業務停止、営業停止、関連許可若しくは営業許可の取消しも命じられる可能性があります。これは、製品の品質問題に対して「倍数額の過料」を課し、安全基準を満たさない設備・製品の製造・提供によって高額の利益を取得する事業者を厳しく罰することを通じ、重要設備及び安全関連製品の安全上のコンプライアンスを確保しようとするものであると評価されています。

改正サイバーセキュリティ法第 38 条「重要情報インフラの運営者がネットワーク製品またはサービスを調達する場合には、規定に従い提供者と安全・秘密保持契約を締結し、安全および秘密保持に関する義務と責任を明確にしなければならない。」

改正サイバーセキュリティ法第 40 条「重要情報インフラの運営者は、自ら又はサイバーセキュリティサービス機関に委託して、自らのネットワークの安全性および潜在的リスクについて、少なくとも年 1 回の検査評価を実施しなければならない。また、当該検査評価の状況および改善措置を、重要情報インフラの安全保護を担当する関係主管部門に報告しなければならない。」

[9] 改正サイバーセキュリティ法第 72 条。

[10] 改正サイバーセキュリティ法第 63 条。

３　安全審査に関する規定への違反

重要情報インフラ事業者が、安全審査を受けず、又は安全審査に合格していないネットワーク製品またはサービスを使用した場合、法人については、その調達金額の 1 倍以上 10 倍以下の過料に、直接責任者については 1 万元以上 10 万元以下の過料に処するものと規定されました[11]。

４　違法な情報の取扱いの厳罰化

違法な情報（例えば法律・行政法規により公表・送信が禁止された情報）の取扱いに関する義務を履行しなかったネットワーク運営者は、従来よりも厳しく処罰されることとなりました。主管部門による是正命令を拒否し、又は情状が重大な場合には、50万元以上200万元以下の過料に処されるほか、関連業務の停止、営業停止、ウェブサイト若しくはアプリケーションの閉鎖、関連業務の許可若しくは営業許可の取消しも裁量により命じられる。さらに、特に重大な影響又は結果を引き起こした場合には、200 万元以上 1000 万元以下の過料が課されるとともに、責任者にも過料が課されることになりました[12]。

すなわち、対象範囲が従来の「ウェブサイトの閉鎖」から「ウェブサイト又はアプリケーションの閉鎖」に拡大され、モバイルインターネットプラットフォームに対する規制がより広範化されました。

さらに、電子情報送信サービスやアプリケーションソフトウェアのダウンロードサービスの提供者に対しても、安全管理義務の不履行を同様に重く処罰するとされました[13]。

第５　域外適用条項の新設

中国国外の機関、組織または自然人が、中国のサイバーセキュリティを侵害した場合、法に従ってその法的責任を追及し、重大な結果が生じたときは、国務院公安部門又は関連機関が当該者に対する資産の凍結その他必要な制裁措置の実施を決定しうるとの規定が新設されました[14]。つまり、中国国外の機関・個人に対しても、中国の関係機関は法的責任が追及でき、資産凍結などの制裁措置をとることができるとすることで、中国のネットワークの主権を維持しようとするものといえます。

第６　最後に

改正サイバーセキュリティ法の施行によって、ＡＩ、データ、クラウド、ネットワークの全てが国家による規制及び管理の対象とされたを見ることができます。

企業におかれましては、データ３法に対応した総合的なコンプライアンス体制の見直しと、データローカライゼーションを徹底し、法令上求められた義務を確実に履行することが求められます。

[11] 改正サイバーセキュリティ法第 67 条。
[12] 改正サイバーセキュリティ法第 69 条 1 項 2 項。
[13] 改正サイバーセキュリティ法第 69 条 3 項
[14] 改正サイバーセキュリティ法第 77 条。

のスペシャリストで構成され、これら各地域に根差したプラクティカルで、シームレスなリーガルサービスを提供しております。

この記事に関するお問い合わせは、ホームページ https://oneasia.legal または info@oneasia.legal までお願いします。

なお、本ニュースレターは、一般的な情報を提供することを目的としたものであり、当グループ・メンバーファームの法的アドバイスを構成するものではなく、また見解に亘る部分は執筆者の個人的見解であり当グループ・メンバーファームの見解ではございません。一般的情報としての性質上、法令の条文や出典の引用を意図的に省略している場合があります。個別具体的事案に係る問題については、必ず各メンバーファーム・弁護士にご相談ください。

＜著　者＞

森　仁司

One Asia 法律事務所 大阪オフィス

日本法弁護士

中国・上海の大成律師事務所へ出向し、現地の中国弁護士（律師）と協同にて、日系企業中国現地法人に関する契約実務全般、労務問題、社内コンプライアンス問題、日中合弁企業の再編、日中貿易取引などを中心に、現地で５年半執務を行なった。

帰国後は、日系企業現地法人の上記業務に加え、中国資本ないし中国人経営者の日本法人を複数顧問先に持ち、対日投資などのインバウントにも積極的に対応しており、日本国内の各種法律問題に関する中国語によるアドバイスも提供している。

一方で、大阪府庁での勤務経験から、行政機関の法律問題（行政法、地方自治法など）にも精通しており、２０２１年１月より大阪府顧問弁護士も務めている。