JETRO
日本貿易振興機構（ジェトロ）

工業・情報化分野のデータセキュリティ関連法制の最新動向（2023 年 2 月時点）

～中国の安全保障貿易管理に関する制度情報 専門家による政策解説～

2023 年 2 月
日本貿易振興機構（ジェトロ）
上海事務所
海外調査部

【免責条項】

本レポートは、西村あさひ法律事務所に委託し、作成したものです。
本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用下さい。ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益等を被る事態が生じたとしても、ジェトロ及び執筆者は一切の責任を負いかねますので、ご了承下さい。

工業情報化部は 2022 年 12 月 8 日に「工業・情報化分野データセキュリティ管理弁法（試行）」（以下、本弁法）を公表し、2023 年 1 月 1 日から正式に施行しました。本弁法は、工業・情報化分野におけるデータセキュリティ管理に関する文書であり、データを一般データ、重要データ、コア（核心）データの 3 種類に分類し、うち重要データおよびコアデータの保護、データライフサイクルのコンプライアンス要求、データ安全認証・評価等の制度について規定しています。

本稿では、「データセキュリティ法[1]」施行後の工業・情報化分野のデータセキュリティ法制の制定動向を簡単に振り返ったうえで、本弁法の内容について解説します。

1. データセキュリティ法施行後の工業・情報化分野の関連法制の制定動向

2021 年 9 月に施行された「データセキュリティ法」は、「各地域および各部門は、当該地域および当該部門の業務において収集したおよび生じたデータ並びにデータセキュリティに対して責任を負う」とし、かつ、「工業（中略）等主管部門は、当該業種および当該分野のデータセキュリティの監督管理職責を負う」としています（6 条）。

また、「各地域および各部門は、データ分類・等級付け保護制度に従い、当該地域および当該部門並びに関連する業種および分野の重要データの具体的な目録を確定し、目録に組み入れたデータについて重点的保護を行う」とも規定しています（21 条 3 項）。

本弁法は、上位法である「データセキュリティ法」の定める各部門におけるデータセキュリティ保護制度およびデータ分類・等級付け保護制度の確立義務を受けて、「工業・情報化分野」の主管部門である工業情報化部によって定められた弁法という位置づけになります。

「データセキュリティ法」における上位概念を受けて各業種および分野で下位規則の制定作業が進められており、自動車分野のデータセキュリティ管理について規定した「自動車データセキュリティの管理に関する若干の規定（試行）」[2]（2021 年 8 月 16 日公布、2021 年 10 月 1 日施行）に続き、本弁法もその先駆け的な存在の一つとして注目されています。

また、同じく「データセキュリティ法」の規定を受けて、工業情報化部は 2021 年 12 月に、「工業分野データセキュリティ管理の試験的業務を組織展開することに関する通知」を公表しました。当該通知は、工業領域のデータセキュリティ管理、データセキュリティ保護およびデータの安全評価制度の構築の進め方について方針を定めています。なお、当該通知で言及されている具体的な業務ガイドラインのうち、「工業データ分類等級付けガイドライン（試行）」は、工業データを 1 級～3 級に分類する旨が記載されていますが、後述の本弁法の一般データ、重要データ、コアデータの 3 分類と各等級の表現が微妙に異なっています。したがい、本弁法施行後に、当該ガイドラインの各等級が、どのように本弁法との 3 分類と使い分けられるのか、または本弁法の 3 分類に統合されるのか、実務の推移が注目されます。

---

[1] 「データセキュリティ法」の詳細については、「データセキュリティ法の概要」および「データセキュリティ法の実務上のポイント」を参照。

[2] 「自動車データセキュリティの管理に関する若干の規定（試行）」の詳細については、「自動車データセキュリティの管理に関する若干の規定（試行）の概要」および「自動車データセキュリティの管理に関する若干の規定（試行）の実務上のポイント」を参照。

当該通知では、他にデータセキュリティ保護およびデータの安全評価に関する方針について、それぞれ「工業企業データセキュリティ保護要求（草案)」および「工業データ安全評価ガイドライン（草案)」に従うよう規定しています。

また、工業情報化部は当該通知と同じく 2021 年 12 月に、「工業・情報化分野のデータセキュリティリスク情報の報告と共有業務についてのガイドライン（試行)」の意見募集稿も発表しています。「データセキュリティ法」は、「国は、集中して統一された、高効率かつ権威あるデータセキュリティリスク評価、報告、情報共有、モニタリング事前警告メカニズムを確立する。国家データセキュリティ業務協調メカニズムは、関係部門がデータセキュリティリスク情報の取得、分析、研究・判断および事前警告業務を強化するよう統一的に計画・調整する」としています（22 条)。当該ガイドラインは、この規定を受けて、工業・情報化分野におけるデータセキュリティリスク情報の取得、分析、研究および予防的業務を強化し、同分野におけるデータセキュリティ体制を掌握し、データセキュリティリスク処理能力を高めることを目的とした内容となっています。内容としては、工業情報化部門の地方主管部門等にデータセキュリティリスク情報を報告させる義務や必要な組織および仕組みについて規定しています。

2. 工業・情報化分野データセキュリティ管理弁法（試行）の具体的内容

（1）定義について

本弁法は、中国国内で展開される工業・情報化分野のデータの取扱活動およびそのセキュリティ管理について規定する行政法規です。工業・情報化分野のデータおよびその取扱者の定義は、当該弁法の義務者およびその義務の範囲を確定する重要な規定となります。

i. 工業・情報化分野のデータ

工業・情報化分野のデータは、工業データ、電気通信データおよび無線電気通信データ等を指すとされ、それぞれの定義は以下のとおり規定されています（3 条)。

「工業データ」: 工業各業界の各領域における研究開発設計、生産製造、経営管理、メンテナンス、プラットフォーム運営等の過程において生じるおよび収集されるデータと定義されます。

「電気通信データ」: 電気通信業務経営活動中において生じる及び収集されるデータをいいます。

「無線電気通信データ」: 無線電気通信業務活動において生じる及び収集される無線電気周波数、周波台等の電波助変数のデータをいいます。

ⅱ. 工業・情報化分野データ取扱者

本弁法で規定する義務を負う工業・情報化分野のデータ取扱者とは、データの取扱活動において、取扱目的および取扱方式を自主的に決定できる次の企業とされています(3 条)。

- 工業企業
- ソフトウェアおよび情報技術サービス企業
- 電気通信業務経営ライセンスを取得した電気通信業務経営者

・無線電気周波数、周波台を使用する単位等の工業・情報化分野の各主体

工業・情報化分野というと、どのような企業まで適用対象となりうるか不明確な面はありますが、まずは上記の業務を行う企業等は、留意が必要と考えられます。

（2）データ分類等級付け管理について

i. データ分類等級付け制度について

本弁法では、工業情報化部は、工業・情報化分野におけるデータの分類等級付け、重要データおよびコアデータの識別認定、データ等級付け保護等の標準規範を制定するとしています（7 条 1 項）。

また、工業・情報化分野のデータ取扱者は、定期的にデータを確認して、標準規範に基づいて重要データおよびコアデータを識別し、自己の単位における具体的なリストを作成することを求められています（7 条 3 項）。

データの分類等級付けについては、以下（2） ii ～ ivのとおり定義されています。

ii．一般データ

リスクの程度が次の条件に該当するデータは、一般データと定義されています（9 条）。

(a) 公共利益、個人または組織の適法な権利・利益に与える影響が比較的小さく、社会に与えるマイナスの影響が小さいデータ

(b) 影響を受けるユーザーおよび企業の数が比較的少ない、生産生活エリアの範囲が比較的狭い、または継続時間が比較的短い場合で、業界の発展、技術進歩および産業生態等への影響が比較的小さいデータ

(c) 重要データまたはコアデータの目録に掲載されていないその他のデータ

iii．重要データ

リスクの程度が次の条件に該当するデータは､重要データと定義されています(10 条)。

(a) 政治、国土、軍事、経済、文化、社会、科学技術、電磁、ネットワーク、生態、資源、原子力安全等に対して脅威となる、または海外の利益、生物、大気圏、極地、深海、人工知能等の国家安全に関連する重要分野に影響を与えるデータ

(b) 工業・情報化分野の発展、生産、運営、および経済利益等に対して重大な影響を与えるデータ

(c) 重大なデータセキュリティインシデントまたは生産安全事故が発生した場合に、公共の利益または個人、組織の適法な権利・利益に重大な影響を及ぼし、社会に与えるマイナスの影響が大きいデータ

(d) 連鎖的な影響を及ぼすことが明らかであり、複数の業界、地域、または業界内の複数の企業に影響を及ぼし、または影響が長期に渡り持続し、業界の発展、技術の進歩、および産業の生態に深刻な影響を与えるデータ

(e) 工業情報化部の評価確定を経たその他の重要データ

ⅳ. コアデータ

リスクの程度が次の条件に該当するデータは、コアデータと定義されています(11 条)。

(a) 政治、国土、軍事、経済、文化、社会、科学技術、電磁、ネットワーク、生態、資源、原子力安全等に対して重大な脅威となる、または海外の利益、生物、大気圏、極地、深海、人工知能等の国家安全に関連する重要分野に重大な影響を与えるデータ

(b) 工業・情報化分野およびその重要な骨格を成す企業、重要情報インフラ、重要資源等に対して重大な影響を及ぼすデータ

(c) 工業生産運営、電気通信ネットワークおよびインターネット運用サービス、無線電気通信業務の展開等に対して重大な障害が生じた場合に、広範囲にわたる業務生産の停止、広範囲の無線電気通信業務の中断、大規模のネットワークサービスの麻痺状態、大量の業務処理能力の喪失を引き起こすデータ

(d) 工業情報化部の評価確定を経たその他のコアデータ

(3) 届出手続きについて

i. 届出

工業・情報化分野のデータ取扱者は、2.(2) i において前述したとおり、自己の単位の重要データおよびコアデータのリストを作成する必要があります。そして、当該リストは、データ取扱者の所在地を管轄する監督管理部門(各地域の工業・情報化主管部門、通信管理局または無線電気通信管理機構)に対して届出を行う必要があります(12 条 1 項)。

ⅱ. 審査確認業務

届出手続きとはされていますが、届出から 20 営業日以内に審査確認業務が行われます。その後、届出が認められない場合には、その理由についてフィードバックが行われ、データ取扱者はフィードバックを受けた後、15 営業日以内に再度届出申請を行わなければならないとされています(12 条 2 項)。

ⅲ. 届出内容に変更が生じた場合について

届出を行った内容に重大な変化が生じた場合には、変化が生じてから 3 カ月以内に届出の変更手続きを行う必要があるとされています。なお、重大な変化とは、重要データまたはコアデータの規模(データの項目数または保存総数など)の 30%以上に変化があった場合とされています(12 条 3 項)。

(4) データライフサイクルセキュリティ管理

本弁法は、データの収集、利用、そして最後に廃棄されるまでのライフサイクルにおける必要なセキュリティ保護措置を定めています。

i. データ取扱者に求められる対応

工業・情報化分野のデータ取扱者は、データ取扱活動に対して安全主体としての責任を負い、各分類のデータに等級付け保護措置を実施する旨が規定されています。

具体的には、各等級別のデータに対して、データの収集、保存、使用、加工、伝送、提供、公開等の各プロセスにおける具体的な等級付保護要求および取扱規程の制定、データセキュリティ管理人員の配置、合理的なデータ取扱活動の取扱権限の設定、（データセキュリティインシデントの発生時など）緊急時の対応方針の策定および緊急時を想定した訓練の実施、業務人員へのデータセキュリティ教育・訓練の実施といった対応が必要と規定されています（13 条 1 項）。

ⅱ．データの収集、保存、自動化意思決定、対外提供、破棄等の各取扱いにおける対応

(a) 収集：工業・情報化分野のデータ取扱者は、データを収集するにあたって、セキュリティ措置を講じるとともに、重要データおよびコアデータの収集に際しては、人員と設備管理を強化しなければならず、データの収集元および時間、種類、数量、頻度および流れに関して記録を取る必要があるとされています（14 条 2 項）。

(b) 保存：重要データおよびコアデータの保存に際しては、暗号化技術等の安全な保存措置をとり、かつ、バックアップおよび記憶媒体のセキュリティ管理を実施し、定期的にデータの復旧テストを実施する必要があるとしています（15 条）。

(c) 自動化意思決定：自動化意思決定に重要データおよびコアデータを使用する場合には、アクセスコントロールを強化することが求められています（16 条）。

(d) 対外提供：重要データおよびコアデータを対外提供する場合には、データの受領者との間で、データセキュリティ合意書を締結し、データ受領者のデータセキュリティ保護能力について確認し、必要なセキュリティ保護措置をとる必要があるとされています（18 条）。

(e) 破棄：データのライフサイクルの終わりとなる破棄について、取扱者は、データ破棄制度を構築し、破棄活動について記録・保存することを求めています（20 条 1 項）。

(f) その他：データ処理者が合併、再編、破産等によりデータを転送する必要がある場合、データ転送計画を明確にし、影響を受けるユーザーに対して、電話、メール、郵便、公告などの方式で通知する必要があるとされています。うち、重要データおよびコアデータの転送については、記録の変更手続きを届け出る必要があります（22 条）。

（5）域内保存義務

重要データおよびコアデータは、中国域内における保存を原則としています。また、重要データの域外移転については、データ域外移転安全評価の手続きを行うことが求められています（21 条）。具体的には、2022 年 9 月 1 日に施行された「データ域外移転安全評価弁法」[1]で規定された手続きに従うことになります。

（6）データ安全監督測定事前警戒および緊急管理

工業情報化部は、地方の監督管理部門と共に、データセキュリティリスクの監視メカニズムを構築するとともに、データセキュリティインシデントの発生時の対応マニュアルな

[1] 「データ域外移転安全評価弁法」の詳細については、「『データ域外移転安全評価弁法』に関する解説および実務対応」を参照。

どを策定することが求められています（26～29 条）。

（7）セキュリティ検査、認証、リスク評価

工業情報化部は、資格を有する機関が、関連標準に基づいてデータセキュリティに関する検査・認証業務を行うよう指導・奨励する旨が規定されています（30～31 条）。

工業・情報化分野の重要データおよび核心データの取扱者は、自らまたは第三者評価機関に委託し、リスク評価を毎年少なくとも 1 回は行うとともに、当該地域の監督管理部門にリスク評価報告を行う必要があると定められています。

（8）法的責任

監督管理部門は、職務中にデータ取扱活動に比較的大きなセキュリティリスクを発見した場合には、規程の権限とプロセスに基づいて工業・情報化分野のデータ取扱者を呼び出して行政指導を行い（注:行政法規でよく使われる「約談」という文言が使われています）、改善措置を取らせてリスクを取り除くことを求めるとされています（35 条）。

本弁法の規定に違反する行為に対して、監督管理部門は、関連する法律法規に基づいて、情状の重さの程度によって、違法所得の没収、課徴金、業務の一時停止、業務停止、業務ライセンスの取消等の行政処罰を科すことができ、かつ、犯罪を構成する場合には法により刑事責任を追及する旨が定められています（36 条）。

3. 最後に

本弁法は、冒頭で述べた「データセキュリティ法」の定める「各地域および各部門は、データ分類・等級付け保護制度に従い、当該地域・部門並びに関連する業種および分野の重要データの具体的な目録を確定し、目録に組み入れたデータについて重点的保護を行う」との規定を工業・情報化分野において具体化したものです。特に、この工業・情報化分野に関わる日系企業は、本弁法に従って、重要データおよびコアデータをリスト化し、データセキュリティ保護の対応を行う必要があることから、本弁法は重要な行政法規といえます。

一方、本弁法で定められた重要データおよびコアデータに関する規定だけでは、対象となるデータが必ずしも明確ではなく、具体的な目録の発表が待たれるところです。

また、具体的なデータセキュリティ保護の対応の内容も、本弁法で一定程度明確化されていますが、依然として具体化されていない標準も多く、今後の実務対応に着目する必要があります。

工業・情報化分野以外に関わる日系企業においても、同様の行政法規および標準が他分野でも整備されていくことが予想されるため、今後の中国におけるデータ管理に関する対応を想定するうえで、ご参考としていただくことが考えられます。

以　上

西村あさひ法律事務所
野村　高志
東城　　聡

レポートをご覧いただいた後、アンケート（所要時間：約 1 分）にご協力ください。
https://www.jetro.go.jp/form5/pub/ora2/20220072

本レポートに関するお問い合わせ先：
日本貿易振興機構（ジェトロ）
海外調査部 中国北アジア課
〒107-6006 東京都港区赤坂 1－12－32
TEL：03-3582-5181
E-mail：ORG@jetro.go.jp