総務省 学術雑誌『情報通信政策研究』 第５巻第２号
Journal of Information and Communications Policy Vol.5 No.2

寄稿論文

中国の個人情報保護法とデータ運用に関する法制度の論点

松尾　剛行（桃尾・松尾・難波法律事務所）

要　旨

中国において初めての個人情報保護法典が 2021 年制定・施行された。

以下では、まずは、世界の 3 種類の個人情報保護制度の相違について、即ち、プライバシーを強調する GDPR 型、表現の自由を重視する米国型、データローカリゼーション規制等を導入する国家の関与が強い中国型をそれぞれ簡単に概説する。

そして、中国における個人情報保護制度について、中国個人情報保護法に限らず、中国サイバーセキュリティー法（ネットワーク安全法）、中国データ安全法（データセキュリティー法）、中国国家安全法等の中国の個人情報・データに関する法制度を詳しく検討する。中国国家安全法により法律の形式で、「全体的な国家安全観」という考えが確立された。中国サイバーセキュリティー法は、インターネット空間の安全を保障するための重要な法的根拠となった。中国データ安全法は、データ処理活動を規範化した。中国個人情報保護法は、個人情報が情報セキュリティの重要な内容であることを示している。このように、中国では、国家安全法、サイバーセキュリティー法、データ安全法、個人情報保護法という 4 つの主要な法律に基づき、国家安全、ネットワーク安全（サイバーセキュリティ）、情報安全、データ安全（データセキュリティ）という四つの点に重点を置いて規制している。

また、その中国法、とりわけ中国における国家安全に関する法制度の中の位置づけを踏まえ、表面上の GDPR 等との類似性と、その背景にある相違を比較検討する。具体的には、国内保存規制及び越境移転規制、ガバメントアクセスに関する制度、中国における情報の取扱いルールの特徴、域外適用、国家の関与に関する規定という視点から、検討し説明する。これらの内容を踏まえ、日本企業の中国ビジネスへの影響について、実務上の対策を提案する。

さらに、経済安全保障の内容、Line 事件を踏まえた経済安全保障とデータガバナンスをめぐって検討した上、日本企業（特に経営レベル）の対応について、検討意思決定機関・体制の整備、意思決定機関・体制の整備、事業リスクの評価、情報収集・分析態勢の構築等の面において、対応策を提案する。

最後、個人情報保護取り締まりの強化、データ税、ネットワーク安全審査対象の拡大等の中国の最新動向について、説明する。

キーワード：中国個人情報保護法、経済安全保障、個人情報、データガバナンス、データ

１．はじめに

中国において初めての個人情報保護法典が 2021 年制定・施行された。まずは、世界の 3 種類の個人情報保護制度の相違について説明した上で、同法に加え、サイバーセキュリティー法（ネットワーク安全法）、データ安全法（データセキュリティー法）等の関連法制度を

踏まえた個人情報保護法制について日本や欧州の法制度との表面上の類似性及びその背景思想における重大な相違等について概説した上で、特に経済安全保障の問題を検討したい。

２．世界の個人情報保護制度

以下では、重要な 3 種類の個人情報保護制度を模式的に説明したい。

２．１．EU

GDPRは、プライバシー重視を打ち出しており、国家及び企業に対する本人（data subject）の権利（データに対する本人のコントロール及びその実質化）、監視（典型的には監視カメラと顔認識）に対する警戒、忘れられる権利（削除権）、プロファイリング規制、自動的意思決定規制、データポータビリティ等の厳しい規制を導入している[1]。しかも、それらは厳しい制裁、つまり、2000万ユーロ又は前会計年度の全世界売上高の4%以下のいずれか高額の方の金額の制裁金（GDPR83条5項）に裏打ちされており、GDPRが2018年5月に施行されてから、2021年末までで、制裁金が課された案件数は合計約1000件、制裁金額は15億ユーロを超えたとされている[2]。

２．２．米国

米国憲法修正1条[3]は表現の自由の価値を強調する。表現の自由とプライバシーが対立する場面では、プライバシーの保護はEU等と比べて相対的に後退する。たとえば、忘れられる権利と表現の自由の対立という側面では、アメリカは表現の自由を相対的に重視する[4]。

そのような状況もあって、現時点では連邦レベルにおいてEUのようなプライバシー全体を規律する法令は存在しないものの、①FTC（連邦取引委員会）の「不公正または欺瞞的な行為または慣行」規制、②個別分野（子ども、医療、金融等）への連邦法のプライバシー規制、③カリフォルニア州CPRA等の州法による規制が存在する。

２．３．中国

これらの2つの法域と中国は明らかに異なっている。すなわち、少なくとも日本の目から見て、中国はプライバシー重視とも、（相対的な）表現の自由重視とも思われない。では、中国の個人情報保護法制は何が特徴的なのだろうか。

中国個人情報保護法は、顕著な民間企業に対する規制の国際標準化、ないしはGDPR化（以下4．3．参照）の傾向を見せている。しかし、国家との関係では、後述のとおり、国家安全が強調され、国家の関与が明確に規定されており、国家として、個人情報に強い関心を持っている。その現れとして最も有名なのは国内保存義務（データローカリゼーション）である。

---

1 石井夏生利著『EU データ保護法』（勁草書房、2020 年）3 頁以下参照。
2 https://www.enforcementtracker.com/?insights を参照。
3 連邦議会は、国教を定めまたは自由な宗教活動を禁止する法律、言論または出版の自由を制限する法律、ならびに国民が平穏に集会する権利および苦痛の救済を求めて政府に請願する権利を制限する法律は、これを制定してはならない。
4 小向太郎「削除請求に関する制度の動向」
（http://www.soumu.go.jp/main_content/000490407.pdf）参照。

なお、データローカリゼーション規制を導入している点では、ロシア[5]も中国と同一類型に入れることができるだろう。

３．中国の個人情報に関する基本制度

３．１．中国個人情報保護法[6]

これまで、中国において、「個人情報保護法典」は「もうすぐ制定される」、「もうすぐ制定される」と繰り返し言われながらも制定されない時期が長く続いていた[7]。しかし、2021年8月20日に、第十三期全国人民代表大会常務委員会第30回会議の審議を経て、中国個人情報保護法が正式に可決成立し、公布され、同年11月1日に施行された。

３．２．中国サイバーセキュリティー法（ネットワーク安全法）

中国サイバーセキュリティー法は 2016 年に制定されており、一連の個人情報に関する法制度の中では比較的早期に制定されている。同法はネットワーク空間の主権並びに国の安全及び社会の公共の利益を保つこと等を目的としている（1 条）。

３．３．中国データ安全法（データセキュリティ法）

中国データセ安全法（2021 年 6 月 10 日公布、2021 年 9 月 1 日施行）は、データ処理活動を規範化し、データ安全を保障し、データの開発利用の促進、個人組織の権利利益の保護そして、国家主権、国家安全及び国家発展の利益を維持することを目的としている。同法の規制はデータという観点からのものであり、その対象は個人データに限られないものの、中国の個人情報保護を理解する上で重要である。

３．４．その他民法典等における個人情報保護

中国では民事法に個人情報を保護する規定が設けられてきたところ [8]、中国の民法典（2020 年 5 月 28 日公布、2021 年 1 月 1 日施行）は、個人情報を定義しており、その中では、サイバーセキュリティー法における個人情報の定義とほぼ同様の内容が定められている。すなわち、同法 1034 条 2 項では、「個人情報」とは、電子的またはその他の方式により記録され、単独またはその他の情報と組み合わせて特定の自然人を識別することができる各種情報をいう、とされている。そして、これには、自然人の氏名、生年月日、身分証番号、個人の生物識別情報、住所、電話番号、電子メール、追跡情報等を含むが、これらに限らない、ともされている。また、民法典では、個人情報の概念のほか、個人情報の取扱過程

---

[5] ロシア連邦個人情報保護法 18 条 5 項。

[6] 松尾剛行＝胡悦「中国個人情報保護法の成立（別添:中華人民共和国個人情報保護法全文仮訳）」桃尾・松尾・難波法律事務所ニュースレター2021 年 9 月 6 日（https://www.mmn-law.gr.jp/download_news_pdf.php?id=485&type=）参照

[7] 松尾剛行「『金融機関における個人情報保護の実務』と中国における個人情報の保護」ザ・ローヤーズ 2016 年 7 月号 62 頁以下では 2003 年以降の経緯を、松尾剛行＝胡悦「中国のプライバシーと個人情報保護」別所直哉『ICT・AI 時代の個人情報保護』（きんざい、2020 年）所収ではより広い範囲の歴史をまとめている。

[8] 2013 年には中国消費者権益保護法 14 条、29 条等が、2017 年には民法総則 111 条が既に個人情報を保護する旨を規定していた。但し法のレベルで個人情報を「定義」した初の民事法令が民法典である。

における本人の権利（たとえば、閲覧、コピー、異議の提出など）及び個人情報取扱業者の義務（適法・正当・必要という原則の遵守、本人同意の取得、取扱ルール・目的・方法・範囲の提示、適切な保管義務など）をさらに明確にした。

さらに、中国の電子商取引法（2018 年 8 月 31 日公布、2019 年 1 月 1 日施行）等でも、個人情報の保護に関する条項が定められている。

３．５．中国の国家安全法、国家情報法（国家諜報法）、反テロリズム法、暗号法等の国家安全（情報）法制

中国憲法は中国において最高の法的効力を持つ法規範である（中国憲法前文）。中国憲法の国家安全に関する規定には、政治的安全、経済的安全、軍事的安全に関する内容が含まれ、公民及び事業体の具体的義務も含まれている。

中国国家安全法（2015 年 7 月 1 日公布、同日施行）によって、政治安全、軍事安全、経済安全、資源・エネルギー安全、食糧安全、文化安全、ネットワークと情報安全[9]などを含む全方位の安全枠組みである「全体的な国家安全観」が確立された。同法は中国の国家安全法体系における基礎法である。情報の安全について、同法第四章第 2 節で規定されている。国は、統一的に集中し、迅速に反応し、正確かつ効率的に、スムーズに稼働する諜報情報収集、研究・判断及び利用制度を健全化し、諜報情報業務の協調メカニズムを確立し、諜報情報の適時収集、正確な研究・判断、効果的な使用及び共有を実現すると規定されている（同法 51 条）。

中国反テロリズム法（2015 年 12 月 27 日公布、2018 年 4 月 27 日改正、同日施行）は、テロリズム活動を防止し、処罰すること等を目的としている（同法 1 条）。テロリズム情報の伝播を防止するために、電気通信業務経営者、インターネットサービスプロバイダは、法律、行政法規の規定に基づき、サイバーセキュリティ、情報内容監督制度及びセキュリティ技術の防止措置を実行し、テロリズム、過激主義内容を含む情報の伝播を防止しなければならず、テロリズム、過激主義の内容を含む情報を発見した後、直ちに伝送を停止し、関連記録を保存し、関連情報を削除し、かつ公安機関又は関連部門に報告しなければならないとされている（同法 19 条 1 項）。また、電気通信とインターネット企業は本人確認義務を履行すべき旨が明確に規定されている。電気通信事業者、インターネットサービスプロバイダは顧客の身分について確認を行わなければならず、身元が不明である又は身元確認の実施を拒否した顧客に対してはサービスを提供してはならないとされる（同法 21 条）。加えて、中国反テロリズム法 18 条は、電気通信業務経営者、インターネットサービスプロバイダが、公安機関、国家安全機関によるテロ活動の調査に技術インターフェースや機密解除などの技術サポートを提供しなければならないと規定している。

---

9 中国国家安全法 25 条：国はネットワークと情報の安全保障体系を構築し、ネットワークと情報の安全保護能力を向上させ、ネットワークと情報技術の革新的な研究と開発・応用を強化し、ネットワークと情報のコア技術、重要インフラと重要分野の情報システムとデータの安全性とコントロールを実現し、ネットワーク管理を強化し、サイバー攻撃、サイバー侵入、サイバー窃盗、違法・有害情報の流布等のサイバー違法犯罪行為を防止し、制止し、法に基づき処罰し、国家サイバー空間の主権、安全、発展の利益を保護する。

中国国家情報（諜報）法（2017 年 6 月 27 日公布、2018 年 4 月 27 日改正、同日施行）は、国の情報（諜報）業務を強化し保障し、国の安全と利益を保護することを目的としている（同法 1 条）。国の情報（諜報）活動は全体的な国家安全観を堅持し、国の重大な政策決定のために参考となる情報を提供し、国の安全に危害を及ぼすリスクの防止と解消のために情報（諜報）のサポートを提供し、国の政権・主権の統一、領土保全、人民の福祉、経済社会の持続可能な発展と国のその他の重大な利益を守るとされている。

中国暗号法（2019 年 10 月 26 日公布、2020 年 1 月 1 日施行）は、暗号の応用と管理を規範化し、暗号事業の発展を促進し、ネットワークと情報の安全を保障し、国の安全と社会公共の利益を守り、公民、法人とその他の組織の合法的権益を保護することを目的としている（同法 1 条）。中国暗号法では、国が暗号を分類管理することが規定されている。暗号はコア暗号、通常暗号、商用暗号に分けられる（同法 6 条）。コア暗号、通常暗号は国家秘密情報の保護に用いられ、コア暗号が情報を保護する最高の国家秘密機密レベルは極秘レベルとされ、通常暗号が情報を保護する最高機密レベルは機密レベルとされ、コア暗号、通常暗号は国家秘密に該当する（7 条）。商用暗号は、国の秘密ではない情報を保護するために使用される（8 条）[10]。

３．６．経済安全保障の文脈を踏まえた制度間の相互関係

中国国家安全法により法律の形式で、「全体的な国家安全観」という考えが確立された。

中国サイバーセキュリティー法は、法の観点からインターネット空間の安全を保障しようとするものである。中国データ安全法は、データ処理活動を規範化した。中国個人情報保護法は、個人情報が情報セキュリティの重要な内容であることを示している。

このように、中国では、国家安全法、サイバーセキュリティー法、データ安全法、個人情報保護法という 4 つの主要な法律に基づき、国家安全、サイバー安全、情報安全、データ安全という四つの点に重点を置いて規制している。

さらに、この 4 つの法律に基づき、ネットワーク安全審査弁法（2020 年 4 月 13 日公布、2020 年 6 月 1 日施行）、児童個人情報ネットワーク保護規定（2019 年 8 月 22 日公布、2019 年 10 月 1 日施行）、個人情報越境移転安全評価弁法（パブリックコメント募集案）（2019 年 6 月 13 日公布）、ネットワーク安全等級保護条例（パブリックコメント募集案）（2018 年 6 月 27 日公布）、ネットワークデータ安全管理条例（パブリックコメント募集案）（2021 年 11 月 14 日公布）、データ越境移転安全評価弁法（パブリックコメント募集案）（2021 年 10 月 29 日公布）、データ安全管理弁法（パブリックコメント募集案）（2019 年 5 月 28 日公布）、個人情報と重要データ越境移転安全評価弁法（パブリックコメント募集案）（2017 年 4 月 11 日公布）等、パブリックコメント募集案を含む一連の部門規則や、GB/T 39335-2020 情報安全技術個人情報安全影響評価ガイドライン等の国家基準が制定された（以上の国家安全の文脈の下でのデータ、とりわけ個人情報に対する法令の概要につき図 1 参照）。

---

[10] コア暗号及び通常暗号について、中国暗号法 15 条によれば、暗号管理部門は法により暗号業務機構（コア暗号・通常暗号の科学研究・生産・サービス・検査・装備・使用・廃棄等の業務に従事する機関）のコア暗号、一般暗号業務に対して指導、監督、検査を行い、暗号業務機構はこれに協力しなければならないとされている、しかし、一般企業では商用暗号を利用するところ、商用暗号についてこの規定は適用されない。

図１．法令の関係 [11]

<table>
<tr><td>憲法</td><td colspan="3">中華人民共和国憲法</td></tr>
<tr><td>基礎法</td><td colspan="3">中国国家安全法</td></tr>
<tr><td>一般法</td><td>中国サイバーセキュリティー法
（2016 年）</td><td>中国個人情報保護法
（2021 年）</td><td>中国データ安全法
（2021 年）</td></tr>
<tr><td rowspan="3">行政法規、部門規章</td><td>ネットワーク安全審査弁法（2021 年）
個人情報と重要データ越境移転安全評価弁法（パブリックコメント募集案）
（2017 年）</td><td></td><td></td></tr>
<tr><td>児童個人情報ネットワーク保護規定（2019 年）、
個人情報越境移転安全評価弁法（パブリックコメント募集案）（2019 年）、
データ安全管理弁法（パブリックコメント募集案）
（2019 年 5 月 28 日公布）、
ネットワーク安全等級保護条例（パブリックコメント募集案）（2018 年）等</td><td></td><td></td></tr>
<tr><td colspan="3">ネットワークデータ安全管理条例（パブリックコメント募集案）（2021 年）
データ越境移転安全評価弁法（パブリックコメント募集案）（2021 年）</td></tr>
<tr><td>国家基準</td><td>GB/T 39335-2020 情報安全技術個人情報安全影響評価ガイドライン（2020 年）
GB/T 35273-2020 情報安全技術個人情報安全規範
（2020 年）
情報安全技術データ越境移転安全評価ガイドライン（パブリックコメント募集案）（2017 年）</td><td></td><td></td></tr>
</table>

[11] なお、
https://www.nishimura.com/sites/default/files/newsletter_pdf/ja/newsletter_210823_cn.pdf も参照。

４．中国個人情報保護法制の特徴

４．１．国内保存規制及び越境移転規制

中国サイバーセキュリティー法の定めたデータ国内保存義務（データローカリゼーション規制）は有名であるが、中国個人情報保護法も同様の義務を課している。中国個人情報保護法 40 条では、重要情報インフラ運営者[12]及び取扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者は、中華人民共和国域内で収集し又は発生した個人情報を域内で保存しなければならないとされている。そして、確かに域外に提供する必要がある場合には、国家インターネット情報部門による安全評価に合格しなければならない[13]。なお、法律、行政法規及び国家インターネット情報部門が安全評価を行わなくて良いと規定する場合には、その規定に従うとされている。

また、全ての個人情報取扱者に課される一般的な越境移転のルールとしては、本人に必要事項[14]を告知した上での個別的同意を得ること（39 条）に加え、以下の 4 つのいずれかが必要である（38 条 1 項）。

（一）本法四十条の規定に基づく国家インターネット情報部門による安全評価に合格した場合。

（二）国家インターネット情報部門の規定に基づく専門機構による個人情報保護の認証を得ている場合。

（三）国家インターネット情報部門が制定する標準的契約を越境移転先と締結し、双方の権利及び義務を約定する場合。

（四）法律、行政法規又は国家インターネット情報部門の規定するその他の条件。

特に 3 号で GDPR の SCC（標準的契約条項）[15]類似の内容が含まれていることが注目される。既に 2021 年 7 月には策定作業が開始されたと報道されており[16]、近日中に公表される

12「重要情報インフラ」とは、公共通信及び情報サービス、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、国防科学技術産業等の重要な産業及び分野の、及び一旦機能の破壊若しくは喪失又はデータ漏洩に遭遇すると、国の安全保障、国民経済と生活、公共の利益を深刻に危険にさらす恐れがある重要ネットワーク施設、情報システム等をいう（重要情報インフラ施設安全保護条例 2 条）。

13 （ⅰ）100 万以上の個人情報の処理者が個人情報を越境移転する場合、（ⅱ）累計で 10 万を超える個人情報又は 1 万以上のセンシティブ個人情報を越境移転する場合、（ⅲ）越境データに重要なデータが含まれている場合等では、越境移転を行う前に省級のネットワーク通信部門へ安全評価を申告しなければならないとの規制も追加される可能性がある（データ越境移転安全評価弁法（パプリックコメント募集案）4 条 2 号、3 号、4 号）。

14 域外の移転先の名称又は姓名、連絡方法、取扱目的、取扱方法、個人情報の種類及び本人が越境移転先に対し本法の規定する権利を行使する方法及び手続等の事項。

15 GDPR 46 条参照。なお、周知の通り、GDPR 対応の新 SCC が既に公表済みである（https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.199.01.0031.01.ENG&toc=OJ%3AL%3A2021%3A199%3ATOC）。

16 Datalaws「国家インターネット情報弁公室はデータ越境伝送標準契約の制定を開始、個人情報保護法（案）の第 3 回審議が 8 月にも」、

ことが想定されるものの 2022 年 2 月時点では公表されていない。

なお、情報安全技術データ越境移転安全評価ガイドライン(パブリックコメント募集案)がデータの越境移転について規定しているところ、同ガイドラインは、「データは、本国以外のところに移転されないが、国外の機構、組織、個人がアクセスし閲覧される場合(公開された情報、ウェブサイトのアクセスを除く)」が越境移転に該当するとしている。つまり、日本からアクセスすることも公開された情報、ウェブサイトのアクセスを除き、越境移転となり得る[17]。

４．２．ガバメントアクセスに関する制度

国内保存義務（データローカリゼーション規制）の結果として、政府が民間企業の保有するデータ等に強制的にアクセスすること、すなわち「ガバメントアクセス」が容易となる[18]。もちろん、従来から司法捜査や刑事手続きの一環としてガバメントアクセスは行われてきた。しかし、近年では、情報機関が諜報活動の一環として行うガバメントアクセスが注目されている。例えば、中国の国家安全法、国家情報法、サイバーセキュリティー法、データ安全法は、ガバメントアクセスを可能とする規定を有する。例えば、中国国家安全法 77 条[19]によれば、国の安全に危害を及ぼす活動の手がかり、証拠の提出や、必要な便宜や協力が求められている。また、中国国家情報法 7 条 1 項によれば、いかなる組織及び公民も、法に基づき国家情報活動を支持、協力、連係し、知っている国家情報活動の秘密を守らなければならないとされている。中国サイバーセキュリティー法 28 条では、ネットワークプロバイダは、公安機関及び国の安全機関のため法により国の安全及び犯罪捜査の活動を維持・保護し、技術支援及び協力を提供しなければならないとされている。さらに、中国データ安全法 35

（https://posts.careerengine.us/p/60dd31cfc4ea202dae574f8a）参照。

17 松尾剛行＝胡悦「中国クラウドの利用と日本企業の義務」桃尾・松尾・難波法律事務所 2022 年 1 月 12 日（https://www.mmn-law.gr.jp/download_news_pdf.php?id=512&type=）参照。

18 データが海外にあっても、理論的にはリモートアクセス等が可能であるところ、日本の判例につき最決令和 3 年 2 月 1 日刑集 75 巻 2 号 123 頁参照。

19 中国国家安全法 77 条では、公民及び組織は、国の安全を維持する次の各号に掲げる義務を履行しなければならないとされている。

（1）国家安全に関する憲法、法律法規の関連規定を遵守すること。
（2）国の安全に危害を及ぼす活動の手がかりを速やかに報告すること。
（3）国家安全に危害を及ぼす活動に関わることを知っている証拠をそのまま提供すること。
（4）国家安全業務のために便宜的な条件又はその他の協力を提供すること。
（5）国家安全機関、公安機関及び関連軍事機関に必要な支持と協力を提供すること。
（6）知っている国家秘密を保持すること。
（7）法律、行政法規が定めるその他の義務。

条[20]によれば、国家の安全又は犯罪の捜査のために関連する協力を求められる場合、関連組織および個人は協力しなければならないとされている。
確かに、匿名で行われるサイバー犯罪やネットワーク上の国家安全を脅かす行為に対する対応として、プロバイダ等の支援を受けて行為者の身元を明らかにすること等はどの国でも必要であるといえるだろう。例えば、日本でもサイバー犯罪対策としてのガバメントアクセスは存在するし、いわゆる捜査関係事項照会（刑事訴訟法 197 条 2 項）を通じたガバメントアクセスについては議論があり、例えば一般財団法人情報法制研究所(JILIS)捜査関係事項照会問題研究タスクフォースは、「捜査関係事項照会対応ガイドライン」を公表している[21]。

但し、中国の場合、例えば中国国家安全法 77 条 4 号が「公民」一般に国家安全への協力義務を設ける等、読み方によってはかなり広範と読み得る義務を課していることから、欧米や日本等において懸念が表明されている。

４．３．中国における情報の取扱いルールの特徴

中国個人情報保護法 5 条～10 条は、個人情報の取扱に関し、合法性・正当性・必要性・信義誠実（5 条）、取扱目的の明確性と合理性・取扱目的との直接関連性・本人権利利益への影響が最小となる方法・最小範囲の個人情報の収集(6 条)、公開・透明性・ルールの明示（7 条)、情報の質の保証（正確性・完全性）(8 条)、責任・安全確保(9 条)、及び、法令遵守・国家安全・公共利益保護（10 条）等の原則を打ち立てている。

特に、GDPR と類似する、個人情報取扱のための正当化事由（適法化根拠）を定めており、以下の 7 つの状況がなければ個人情報を取り扱うことができないとした(13 条)。GDPR と比較すると、一般的な「正当な利益」のような事由が認められていないことが重要である。反面、公開情報についての例外があり(6 号)、法律、行政法規の規定するその他の状況（7 号）がいわばバスケット条項として設けられている（表 1 参照）[22]。

---

[20] 中国データ安全法 35 条では、公安機関又は国家安全保障機関が、国家の安全を維持し、又は法律に基づいて犯罪を捜査する目的でデータを取得する必要がある場合、国家の関連法規に従い、厳格な承認手続きを経て、法律に基づいて手続きを行うものとし、関連組織および個人は協力しなければならないとされている。

[21] 一般財団法人情報法制研究所（JILIS）捜査関係事項照会問題研究タスクフォース「捜査関係事項照会対応ガイドライン」
（https://www.jilis.org/proposal/data/sousa_guideline/sousa_guideline_v1.pdf）を参照。

[22] なお、草案第 1 稿との関係では、労働関係（2 号）及び公開情報の合理的利用（6 号）が追加されている。

表１．GDPR と中国個人情報保護法の適法化根拠の比較

中国個人情報保護法 13 条	GDPR6 条 1 項 [23]
(一)本人の同意を取得している場合。	(a) データ主体が、一つ又は複数の特定の目的のための自己の個人データの取扱いに関し、同意を与えた場合
(二)本人が当事者の一方となる契約の締結又は履行に必要な場合又は適法に制定された労働規章制度及び適法に締結された集団的契約に基づき人事管理を実施する上で必要な場合。	(b) データ主体が契約当事者となっている契約の履行のために取扱いが必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合
(三)法定の職責又は法定の義務の履行に必要な場合。	(c)管理者が服する法的義務を遵守するために取扱いが必要となる場合
(四)突発的な公衆衛生上の事件に対応し、又は緊急状況下において自然人の生命、健康及び財産の安全の保護のために必要な場合。	(d) データ主体又は他の自然人の生命に関する利益を保護するために取扱いが必要となる場合
(五)公共の利益のためメディア報道、世論監督等の行為を実施し、合理的範囲内で個人情報を取り扱う場合。	(e) 公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合
(六)本法の規定に基づき合理的な範囲で本人が自ら公開し又はその他適法に既に公開済みの個人情報を取り扱う場合。	
(七)法律、行政法規の規定するその他の状況。	
	(f)管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く

４．４．域外適用

データが国際的に流動する中、中国においても中国サイバーセキュリティー法や中国データ安全法等、多くの法令に域外適用を明記する姿勢が見られる。そして、その傾向は個人情報保護法においても見られる。

[23] GDPR の翻訳は個人情報保護委員会のもの（https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf）を参照している。以下同様である。

中国個人情報保護法 3 条 1 項は原則として「中華人民共和国の域内において自然人の個人情報を取扱う活動」に同法を適用するとするが、同条 2 項は、中国域内の自然人を標的として製品、サービスを提供し、又は中国域内の自然人の行為を分析し評価する場合、個人情報取扱者が中国域内にあるか否かを問わず、中国法の管轄を受けるとする。これは GDPR の域外適用規定に近接している。例えば、日本企業が越境 EC を通じて、このような要件を満たす中国域内の自然人の個人情報の取り扱いを行うと、中国個人情報保護法が直接適用される[24]。

４．５．国家の関与に関する規定

４．５．１．サイバーセキュリティー法

民間の個人情報の利用に関する国家の関与としては、中国サイバーセキュリティー法が重要である。同法は、ネットワーク安全法とも呼ばれるが、単なるサイバーセキュリティーの問題を超えて、サイバー空間及びそこに集まる情報を「国家安全保障」の一環としてコントロールすることに対する強い志向がみられる。

中国サイバーセキュリティー法はネットワーク空間の主権並びに国の安全及び社会の公共の利益を保つこと等を目的としているところ（1 条）、国家の責務として国内外からもたらされるネットワークの安全上のリスク及び脅威をモニタリング、防御、処置が規定されている（5 条）。また、全ての個人及び組織を名宛人として、ネットワークの安全を脅かしてはならず、ネットワークを利用して国の安全、栄誉、利益を脅かし、国家政権の転覆及び社会主義制度の転覆を煽動し、国の分裂及び国家統一を破壊することを煽動し、テロリズム及び過激主義を宣揚し、民族に対する憎悪や差別を宣揚し、暴力及びわいせつな情報を流布し、虚偽情報を捏造、拡散して経済の秩序及び社会秩序を撹乱し、他人の名誉、プライバシー、知的財産権その他の適法な権益を侵害する等の活動に従事してはならないとする（12 条）。

また、禁止されている情報があれば、プロバイダに送信停止を命じ、中国国外からもたらされたそれらの情報については、技術措置及びその他の必要な措置を講じて伝播を遮断するよう関係機関に通知する（50 条）。国はネットワークの安全のモニタリング事前警告及び情報通報の制度を確立する（51 条）。

４．５．２．データの越境移転に関する安全評価

中国サイバーセキュリティー法 37 条は、データ越境移転の制限に関する安全評価制度を規定した。まず、中国サイバーセキュリティー法は、日本やヨーロッパ流のいわゆる越境移転規制のみを規定する枠組みと異なり、そもそも個人データを取り扱うビジネスを中国で運営する以上は中国で当該データを保管することを義務付ける国内保管義務（データ・ローカリゼーション）を（一定範囲で）求めている。その上で、例外的にデータを越境移転する場合、安全評価を必要とした。

中国サイバーセキュリティー法 37 条と同様に、中国個人情報保護法 40 条では、重要情報インフラ運営者及び取扱う個人情報が国家インターネット情報部門の規定する数量に達

24 松尾剛行＝胡悦「中国個人情報保護法適用後(2021 年 11 月以降)におけ る、日本の越境 EC 企業のなすべき実務対応 」桃尾・松尾・難波法律事務所ニュースレター2021 年 9 月 29 日
（https://www.mmn-law.gr.jp/download_news_pdf.php?id=487&type=）

した個人情報取扱者は、中華人民共和国域内で収集し又は発生した個人情報を域内で保存しなければならないとされている。確かに域外に提供する必要がある場合には、国家インターネット情報部門による安全評価に合格しなければならないとされている。

情報安全技術データ越境移転安全評価ガイドライン（パブリックコメント募集案）3.7 条によれば、データの越境移転について、ネットワーク運営者は、ネットワーク等の方法により、中華人民共和国国内の運営において収集し、発生させた個人情報と重要データを、直接の提供、又は業務の展開、サービス・製品の提供等の方法を通じて、域外の機構、組織又は個人に提供する一回の活動又は連続的活動を指す、とされている。

ただし、中国サイバーセキュリティー法の法文上、安全評価義務がかかる範囲は比較的狭いように見える。安全評価の主体は、重要情報インフラ運営者に限定し、安全評価対象客体は、個人情報及び重要データに限定されている。これに対し、中国個人情報保護法は、取扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者に拡大した。なお、中国サイバーセキュリティー法の下位規範である各法令の草案の動き（未施行）についても留意が必要である。現時点の各法令の草案の内容からみれば、中国の全企業は、テータを越境移転させる場合、一定の条件を満たす場合、安全評価を申告しなければならない[25]。

４．５．３．当局の承認・許可

個人情報の取り扱いにつき、当局の許可承認を得なければならない場合も存在する。例えば、「人間の遺伝データの管理に関する暫定弁法」の 4 条及び 11 条が許可なくして越境移転することを禁止している。

---

[25] 個人情報と重要データ移転安全評価弁法（パブリックコメント募集案）（2017 年 4 月 11 日公布）2 条では、企業が域内の運営において収集し、発生させた個人情報と重要データについて、域内に保存しなければならず、確かに業務遂行のため域外に提供する必要がある場合、安全評価を行わなければならないとされた。また、同安全評価弁法 9 条及び情報安全技術データ越境移転安全評価ガイドライン（パブリックコメント募集案）（2017 年 8 月 30 日公布）4.3.2 条では、当局による評価が必要とされている要件を具体的に規定されている。また、個人情報越境移転安全評価弁法（パブリックコメント募集案）（2019 年 6 月 13 日公布）3 条では、個人情報を移転する前に、ネットワーク運営者は、所在地の省レベルのインターネット情報部門に対して個人情報越境移転安全評価を申告しなければならない、とした。データ移転安全評価弁法（パブリックコメント募集案）（2021 年 10 月 29 日公布）2 条では、データ取扱者が中華人民共和国国内の運営において収集し、発生させた重要データ及び法により安全評価を行うべき個人情報を越境に提供する場合、本弁法の規定に基づき安全評価を行わなければならず、法律、行政法規に別途規定がある場合は、その規定に従うとされている。同募集案 4 条では、次の状況のいずれかに該当する場合、安全評価を申告する必要があるとされている。（1）重要情報インフラ運営者が収集し発生した個人情報と重要なデータである場合。（2）越境移転データに重要データが含まれる場合。（3）100 万以上の個人情報の処理者が個人情報を越境移転する場合。（4）累計で 10 万を超える個人情報又は 1 万以上のセンシティブ個人情報を越境へ移転する場合。（5）国家インターネット情報部門が規定するその他データ越境移転安全評価を申告する必要がある場合。これらを松尾剛行＝胡悦「中国クラウドの利用と日本企業の義務」桃尾・松尾・難波法律事務所 2022 年 1 月 12 日（https://www.mmn-law.gr.jp/download_news_pdf.php?id=512&type=）6 頁で表にまとめた。

加えて、中国データキュリティー法 36 条は「中華人民共和国関連主管機関の承認を得なければ、国内の組織、個人は中華人民共和国域内に保存されているデータを域外の司法又は法執行機関に提供してはならない」と規定する。

同様に、中国個人情報保護法 41 条では、国際司法協助又は行政法執行協助のため、中国国外に個人情報を提供する必要がある場合、主管部門に申請し、その許可を得なければならないとする。

４．５．４．ネットワーク安全等級保護制度

中国サイバーセキュリティー法は、ネットワークサービス提供者を含むネットワーク運営者に対して一連のネットワーク運営上の安全保護に関する要求及び義務を規定しており、ネットワーク運営者が国の実施しているネットワーク安全等級保護制度に基づき、そのネットワーク運行安全保護義務を履行するよう要求することが含まれる。したがって、ネットワーク運営者はサイバーセキュリティー法及びネットワーク安全等級保護制度の要求を遵守する必要がある。ネットワーク安全等級保護制度について、企業は、情報安全等級保護管理弁法及び情報セキュリティ技術ネットワーク安全等級保護基本要求（GB/T 22239-2019）に従って、ネットワーク安全等級を認定し、該当する等級に基づいて、安全の共通要求及びクラウドコンピューティング、モバイルインターネット、IoT、工業制御システムなどの安全に関する保護措置を講じる必要がある [26]。

---

[26] 中国サイバーセキュリティー法 21 条によれば、ネットワークプロバイダは、ネットワーク安全の等級保護制度の要求に従い、次に掲げる安全保護義務を履行し、ネットワークが妨害、破壊されたり、授権されていないアクセスを受けることがないよう保障し、ネットワークデータが漏えいするか、窃取されるか、改竄されることを防止しなければならないとされている。

(1) 内部安全管理制度及び操作規程を制定し、ネットワークの安全責任者を確定し、ネットワークの安全にかかる保護責任の確実な履行をはかる。

(2) コンピューターウィルス及びサイバー攻撃、ネットワーク侵入等のネットワークの安全を脅かす行為を防止する技術的な措置を講じる。

(3) ネットワークの運行状態及びネットワークの安全にかかる事件のモニタリング及び記録にかかる技術措置を講じ、なお且つ規定に従い関連するネットワークのログを少なくとも 6 箇月間は保存する。

(4) データ分類並びに重要データのバックアップ及び暗号化等の措置を講じる。

(5) その他、法律及び行政法規に定める義務。

中国サイバーセキュリティー法 34 条によれば、本法 21 条の規定を除き、重要情報インフラストラクチャーの運営者は、次に掲げる安全保護義務を履行しなければならないとされている。

(1) 専門の安全管理機関及び安全管理責任者を設置し、なお且つ当該責任者及び重要職位の人員に対し安全背景の審査を行う。

(2) 業務に従事する者に対し、定期的にネットワークの安全にかかる教育、技術研修及び技能考査を行う。

４．５．５．まとめ

上記のとおり、中国では、そもそも日本等において政府が関与していないような民間の個人情報の取り扱いに対して関与をしている。

このような政府の関与は、中国政府の個人情報への強い関心、とりわけそれが国家安全に密接に関係しているという考えを反映している。

４．６．日本企業の中国ビジネスへの影響

４．６．１．自社への適用の確認

中国に子会社がある企業は基本的に中国個人情報保護法が適用されると考えるべきである。しかし、中国に子会社（エンティティ）が存在しないからといって、中国個人情報保護法が無関係と軽信してはならない。域外適用規定が置かれていることから、自社又は自社グループの非中国企業が適用を受けないかについて確認をすべきである。

例えば、越境 EC ビジネス等で日本企業が中国域内の自然人を標的として製品、サービスを提供したとされれば、域外適用規定が適用されるだろう。また、日本企業 A が中国企業 B に委託して中国顧客 C にサービスを提供するという場合、当該中国企業 B は中国個人情報保護法適用企業であるところ、日本企業 A もまた、中国における中国個人情報の取り扱いを中国企業 B に委託したとして、中国個人情報保護法が（直接）適用される可能性もある。加えて、中国域内の自然人を自社による採用のターゲットとしても、これを「標的として製品、サービスを提供した」とは言えないだろうが、近時では AI 面接や AI 適性検査等の HR テクノロジーが発達しており、応募者の行為を分析・評価するとみなされ、域外適用の対象となる可能性もある。

なお、ここで問題となるのは、例えば中国個人情報保護法 3 条 2 項 1 号が、「中国域内の自然人」としているように、その自然人が中国域内かどうかである。そこで、日本国内の中国人留学生（中国籍）は「中国域内の自然人」ではないが、日本人（日本国籍）でも、例えば中国で仕事をしている場合等には「中国域内の自然人」になり得る。

４．６．２．社内規程、プライバシーポリシー等の改訂

上記 4. 6. 1. の検討の結果、自社グループにおいて中国個人情報が適用されるエンティティがどこであるかを識別することができるだろう（典型的には中国子会社であるが、それ以外にも適用され得ることは上記 4. 6. 1. のとおりである。）。中国個人情報保護法は個人情報取扱ルールを制定し、明示すべきとしているところ、既に日系企業グループであれば、何らかの個人情報取扱ルールが定められているところも多いだろう。しかし、中国個人情報保護法は様々な面で規律を追加している。例えば本人の権利に関する規律やセンシティブ情報に関する規律、そして自動的意思決定に関する規律等は、従前の法制度や規格・基準に比べるとより完全化され、包括的・網羅的なものとなっている。そこで、社内規程、プライバシーポリシー等の改訂が必要であろう。

---

(3) 重要なシステム及びデータベースについて災害に備えたバックアップをとる。

(4) ネットワークの安全にかかる事件のための緊急対応マニュアルを制定し、なお且つ定期的に訓練を行う。

(5) その他、法律及び行政法規所定の義務。

なお、中国個人情報保護法 17 条では、明確かつ理解しやすい表現を用いることが求められることから、もしプライバシーポリシーを制定・公表する場合、日本語や英語ではなく、中国語での表記が必要である。

４．６．３．日本への移転

中国子会社等中国個人情報適用対象事業者の取り扱う個人情報を日本に移転させる場合、2021 年 11 月 1 日の中国個人情報保護法施行日以降は、（当該中国個人情報適用対象事業者が重要インフラ事業者ではないことを前提とすれば、）原則として本人に必要事項を告知した上での個別的同意を得ること（39 条）に加え、安全評価、認証、標準的契約等のいずれかが必要である（38 条 1 項各号）。実務上は標準的契約の利用の方向に収斂するのではないかと予想されるものの、標準的契約の策定状況等を注視する必要がある。

４．６．４．中国企業との個人情報の取り扱いの委託・受託関係

中国個人情報保護法 21 条 1 項は「個人情報取扱者が個人情報の取扱いに関する委託をする場合においては、受託者との間で、委託による取扱の目的、期限、取扱方法、個人情報の種類、保護措置及び双方の権利と義務等を約定しなければならず、かつ受託者の個人情報取扱活動に対し監督を行わなければならない。」と定めている。

これまで、中国企業との業務委託（日系企業グループ側は委託者・受託者いずれにもなり得る）において、（日本法や GDPR 等のグローバルデータプライバシー規制の観点で検討したことがあっても、）中国法の観点から個人情報の取り扱いやそのルールについて検討したことが少ないかもしれない。中国個人情報保護法 21 条が「個人情報の取扱いに関する委託」とするように、単なる委託が存在するだけで同条が適用されるのではなく、当該委託関係に中国個人情報保護法が適用され、「個人情報の取扱いに関する委託」が存在すれば、中国個人情報保護法の要件を満たす処理委託契約（DPA）の締結が必要である。具体的には、例えば、取扱の目的、期限、取扱方法、個人情報の種類、保護措置及び双方の権利と義務等の条項、監督の条項等を入れるべきことになる。

４．６．５．最新状況の注視

上記では標準的契約の策定状況への注視の必要性について述べたが、これ以外にも実務を回していく上での細則等が不明確な状況は国家インターネット情報部門の規定について言及されている 38 条、40 条、42 条、45 条等が存在する。今後とも下位規範制定等に向けた最新状況を注視していかなければならない。

５．経済安全保障とデータガバナンス

５．１．経済安全保障とは

近年、経済活動が国境を越えて活発化する中で、日本も政府を挙げてグローバル化を推進してきた。しかし、特定国の急速な台頭や国際経済構造の急激な変化に国家として機敏に対応できず、その結果として、国家の生存と繁栄の基盤を他国に過度に依存するリスクや、他国主導の国際的なルール形成に起因する国益毀損のリスクに正面から向き合わざるを得ない状況に追い込まれつつある。

以上の問題意識と危機感に基づき、2020 年 12 月の自由民主党の「『経済安全保障戦略』の策定に向けて」は、経済安全保障を「わが国の独立と生存及び繁栄を経済面から確保すること」を定義し、戦略的自律性の確保及び戦略的不可欠性の維持・強化・獲得という考え方を提示した[27]。

また、経済安全保障の重要な内容について、データこそ経済安全保障の要とされ、また、中国の政策変化に目配りを必要があるとか[28]、今、最も大きな脅威となっているのが中国に他ならないとされることがある[29]。

５．２．経済安全保障とデータガバナンス―Line 事件を踏まえて

５．２．１．経済安全保障の情報分野への影響

2021 年 12 月 3 日、都内で開催された第 1 回防衛・経済安全保障シンポジウムでは、岸田総理は、5G 基地局、あるいは洋上風力・海底ケーブル、こうした取組の際に、海外企業を通じて、我が国の安全保障に関わる情報が外国に渡るリスクがあるのではないかという問題意識を提起した[30]。情報通信関係では、①ランサムウェア攻撃（ランサムアタック）等の高度なサイバー攻撃を含む情報流出、技術流出[31]、②ガバメントアクセスを背景としたデータガバナンスの問題の 2 つの問題が重要であるところ、①は興味深い[32]反面、本稿のテーマとずれるので②を中心に検討する[33]。

５．２．２．データガバナンスとは

データガバナンスは多義的であり、公的データに対するガバナンスという側面で議論するものも多いものの[34]、民間企業との関係では、DMBOKI（データマネジメント知識体系ガ

---

27 「新国際秩序創造戦略本部　中間取りまとめ　『経済財政運営と改革の基本方針 2021』に向けた提言」（https://jimin.jp-east-2.storage.api.nifcloud.com/pdf/news/policy/201648_1.pdf）を参照。

28 土屋大洋「データこそ経済安全保障の要　中国の政策変化に目配りを」（https://www.nikkei.com/article/DGXZQOCD151M70V11C21A1000000/）を参照。

29 木村岳史「IT 産業を揺るがす『経済安全保障』の正体、LINE 問題から見えた懸念と疑問」（https://xtech.nikkei.com/atcl/nxt/column/18/00849/00065/）を参照。

30 防衛・経済安全保障シンポジウム（https://www.kantei.go.jp/jp/101_kishida/actions/202112/03boueikeizai.html）を参照。

31 https://www.moj.go.jp/content/001357584.pdf。

32 なお、松尾剛行「ランサムアタックに関する法的考察―実務対応の観点から」情報ネットワーク法学会第 21 回研究大会個別報告参照。

33 Huawei 排除による日本通信企業への影響等は本稿の主題と異なるので除外する。

34 例えば、「信頼ある自由なデータ流通」すなわち“Data Free Flow with Trust”（DFFT）の“Trust”の文言に示されているように、国際的なデータ流通を促進するためには、移転先におけるデータの取扱いについて透明性が確保されており、プライバシーやセキュリティ、知的財産権等に関する適切なガバナンスが実施される必要があるとする「Governance Innovation ver.2 」（https://www.meti.go.jp/press/2020/02/20210219003/20210219003-1.pdf）や「データ戦略の策定について」（https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai1/siryou1.pdf）における、データガバナンスのルールの策定としての 1 データ提供主体の真正性、2 データの取扱いに係る契約、3 データの信頼性（質）、4 パーソナルデータの取扱い、5 データ構造・形式、「データの蓄積や公開、および二次利用等を促進する上での好ましい管理 の在り方」とする総

イド)は、データガバナンスをデータマネジメントを統制するための活動とし[35]、「DX 時代における企業のプライバシーガバナンスガイドブック ver1. 2」[36]は、企業のプライバシーガバナンスとは、プライバシー問題の適切なリスク管理と信頼の確保による企業価値の向上に向け、経営者が積極的にプライバシー問題への取組にコミットし、組織全体でプライバシー問題に取り組むための体制を構築し、それを機能させることとし、経営者が取り組むべき三要件として、①ガバナンスに係る姿勢の明文化、②保護責任者の指名及び③取組に対するリソースの投入を挙げた。

定義には様々なものがあるが、各企業のガバナンスの対象として、従来人や資産等が念頭に置かれてきたが、データの重要性が高まることで、単に個別のデータを管理することそのものを超えて、組織としてその管理の枠組みをどのように作り、どのように統制・統御を効かせていくかに注目が集まっており、特に経営者の責任が問題とされている、ということと概ね総括することができるだろう。そして上記の経済安全保障やガバメントアクセスが重要な問題となっている状況においては、そのような観点を踏まえたデータガバナンスが重要である。

５．２．３．Line 事件に見る経済安全保障とデータガバナンス

LINE における海外個人情報アクセス問題を受け、親会社の Z ホールディングスが立ち上げた「グローバルなデータガバナンスに関する特別委員会」の最終報告[37]（以下「最終報告」という。）が 2021 年 10 月 18 日に公表された所、最終報告は、「LINE 社においてガバメントアクセスへのリスク等の経済安全保障への配慮ができていなかった」と指摘し、データ保管やガバナンスの改善を提言している。

ここで重要なこととしては、「LINE China 社から外部の組織に対して、LMP に関する情報の漏えいは認められなかった。」（最終報 24 頁）とされていることである。従来型の、情報漏洩等が起こり、それを問題視するという話ではないところに、経済安全保障とデータガバナンスの問題の特徴が見られる。

最終報告では、大きく分けて 2 つの重要なポイントが指摘されている。

1 点目は、経済安全保障への配慮である。中国において Line アプリのデータの一部確認を開始するにあたり、LINE 社は国家情報法等のように、個人情報保護法制そのものではないものの情報管理に影響を与え得る外国法制について、網羅的にはリサーチ対象に含めていなかった（最終報 20 頁）。最終報告においては、LINE 社においては、通信の秘密を含

務省「社会資本分野におけるデータガバナンスカカガイド」
(https://www.soumu.go.jp/main_content/000166474.pdf)等を参照。EU の「REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)案」は、パブリックセクターにおけるデータの再利用の条件、データ共有サービスの通知・監督フレームワーク、利他的目的で公表されるデータの収集と処理を行うエンティティーの任意的登録フレームワークとする（https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71222）。

[35] DAMA International『データマネジメント知識体系ガイド 第二版』。

[36] https://www.meti.go.jp/policy/it_policy/privacy/guidebook12.pdf

[37] https://www.z-holdings.co.jp/wp-content/uploads/2021/10/da483e6a533c560435dbe6bcbf17ead2.pdf

むユーザーの個人情報を扱う以上、国家情報法に限らず広く中国におけるガバメントアクセスのリスクを慎重に検討する必要があったところ、ガバメントアクセスのリスクとしても受け止めて、経営上の課題として適切に取り上げ、ガバメントアクセスのリスクへの必要な対応を取ることができなかったと評されている（最終報告 25−26 頁）。その結果として、ガバメントアクセスのリスクを含む経済安全保障分野に関する管理体制や事後的にもこれを見直す体制の整備が不十分であったことから、経済安全保障を考慮したデータガバナンス体制を構築していく必要があるとされている（最終報告 74―80 頁）。

2 点目はコミュニケーションないしステークホルダーへの説明責任である。最終報告では、一部データが韓国のデータセンターに保存されていたにもかかわらず、対外的に「LINE の個人情報を扱う主要なサーバーは日本国内にある」「日本に閉じている」等の誤った説明をしていたことが問題視された（最終報告 44―52 頁）。

最終報告においては、客観的な事実を誠実に伝えるという点が強調され、「ユーザーを裏切らない」ことを重視し、中長期的な視野に立って誠実なコミュニケーションを行うことを旨としなければならないことを、LINE 社の役職員ひとりひとりが思いを致さなければならない等とされている（最終報告 82 頁）。

これは、あくまでもグローバルデータガバナンスの一部の問題が表面化しただけであり、この 2 点だけがデータガバナンスではない。しかし、この事件の反省を踏まえ、なぜ日本ではないその国にデータを置くのか、地政学リスク・地経学リスクをどのように考えてどうリスクを検討したのか、という点をステークホルダーに正確に説明できなければならない、その際には、いわば「まずいことに蓋をして」隠すのではなくむしろしっかりと説明（説明責任）しなければならない、また、経営者が、経済安全保障・ガバメントアクセスを含むデータガバナンスを経営上の重要な問題と捉え、トップとして責任感を持って対応していかなければならない。

５．３．経済安全保障と日本企業（特に経営レベル）の対応

では、具体的に、経済安全保障の問題に、日本企業はどのように取り組んでいくべきだろうか。上記のとおりプライバシーガバナンスガイドブックは経営者が取り組むべき三要件として、①ガバナンスに係る姿勢の明文化、②保護責任者の指名及び③取組に対するリソースの投入を挙げていた。このような経営者の取り組みの必要性を踏まえ、特に経営レベルにおいて、上記の LINE 事件の教訓を踏まえ、日本企業は経済安全保障に対して以下の対応をすべきである。

５．３．１．経済安全保障を考慮した意思決定機関・体制の整備

近時、経済安全保障の対応措置として、一部の企業において、専門部署を設置するという動きが見られる。例えば、社長直轄の「経済安全保障統括室」を設置した企業が存在する[38]。

[38]三菱電機ホームページ
（https://www.mitsubishielectric.co.jp/corporate/csr/governance/risk/security/index.html）を参照。

企業は経済安全保障を考慮するための必要な組織、体制を設置・見直し、意思決定機関の決裁・報告プロセスに経済安全保障が考慮されるよう設計する必要がある。

５．３．２．経済安全保障の観点に基づく事業リスクの評価

第二に、新規および既存の事業においても経済安全保障上のリスクがないかを検討し、またその後も定期的に点検・評価できる態勢を確保するべきである。

上記 Line 事件においては、事後的に見直す体制の整備が不十分であったと指摘されているので、一度新規参入等の場面で検討した場合でも、その後も定期的に見直すことが重要である。

５．３．３．経済安全保障に関する情報収集・分析態勢の構築

第三に、企業の意思決定を支える経済安全保障関連の情報収集・分析の態勢・プロセスを整備することである。（経済）安全保障問題は複雑で流動的な面があり、企業・組織内部で完結することが難しく、外部の専門家・研究者の知見が必要となるだろう。1 人の専門家がこの問題を全てカバーすることは極めて困難であるため、企業・組織としては自社に必要な個別具体的な問題領域やテーマ毎の専門家を把握しておくことが現実的である。外部の知見も含めて、必要な経済安全保障関連情報を収集・分析する態勢を構築する必要がある。

５．３．４．対外的コミュニケーション

第四に、企業は投資家やその他ステークホルダーとの間で経済安全保障に関する建設的対話を促すため、有価証券報告書を始めとする開示文書や自社ウェブサイト等において、経済安全保障に関するリスク認識・対応、各種機関・会議体における経済安全保障の議論の状況等に関する開示等のコミュニケーションを実施することが重要である[39]。

このようなコミュニケーションの際は Line 事件でも指摘されているように、「短期的」安心を与えるために、海外での保管の事実や経済安全保障リスクを隠すのではなく、もし合理的な理由に基づき海外で保管するのであれば、そのような合理的理由を説明することで「長期的」な安心を与えるべきである。

６．その他の中国情報法制の最新動向

中国の情報法制は刻一刻と変化している。最後に、本稿執筆時点である 2021 年末段階の重要なトピックスをいくつか紹介したい。

６．１．取り締まりの強化

個人情報保護法の施行に伴い、中国政府は、個人情報の取り扱いに問題がある企業に対する取締りを強化している。

2021 年 11 月 1 日に、工業情報化部は、「情報通信サービスの感度向上行動の展開に関す

[39] 「経済安全保障を考慮したガバナンス・リスクマネジメント態勢の構築」（https://www.tokiorisk.co.jp/publication/report/riskmanagement/pdf/pdf-riskmanagement-355.pdf）を参照。

る通知」を発表した[40]。当該通知によると、各関連企業[41]は 2021 年 12 月末までに「収集済み個人情報リスト」と「第三者と共有した個人情報リスト」を作成し、アプリのメニュー上に表示し、ユーザーの問い合わせに供しなければならない。収集済み個人情報リストは、アプリケーションが収集したユーザーの個人情報の基本的な状況（情報の種類、使用目的、使用シナリオなど）を簡潔かつ明確に記載しなければならない。第三者との個人情報共有リストには、第三者と共有する個人情報の種類、使用目的、使用シナリオ及び共有方法等の内容が含まれる。アプリが第三者と共有するユーザーの個人情報の基本状況を簡潔かつ明確に記載しなければならない。

工業情報化部は 2021 年 11 月 16 日、「第 14 次五カ年計画情報通信業界発展計画」の記者会見を開いた。工業情報化部情報通信管理局の王鵬副局長は、「これまでに 21 回で計 244 万アプリの検査を実施し、累計 2049 件の違反アプリケーションを通報した。修正を拒否した 540 件のアプリを撤去させ、違反行為に対する高圧的な抑止力を維持し続けている」と述べた[42]。

11 月 24 日、中国中央テレビニュースの報道によると、2021 年に入って工業情報化部が展開したアプリケーションによるユーザー権益侵害特別取り締まりキャンペーンでは、テンセントの 9 製品に違反行為があったとされた。工業情報化部はテンセント社に対して経過的な行政指導措置をとり、今後発表されるアプリケーションの新製品、および既存のアプリケーションの更新版について、工業情報化部が技術検査を実施し、検査に合格した後に投入することを要求した[43]。

中国市場監督管理学会理事である張韜氏は、個人情報保護法の施行以来、各地の法院は少なくとも数十件の個人情報に関する民事公益訴訟事件を審理しているとする。中国では、多くの消費者の権利を侵害した行為に対しては、中国消費者協会、並びに、省、自治区及び直轄市に設立した消費者団体が、一般消費者に代わって公益訴訟を提起することができる（中国消費者権益保護法 47 条、民事訴訟法 58 条）とされているところ、中国個人情報保護法 70 条はその特則として多くの本人の権利利益を侵害した場合、人民検察院、法律の規定する消費者組織及び国家インターネット情報部門の確定した組織が個人情報取扱者を提訴することができると定めることで、より広い範囲の組織が公益訴訟を提起できるようにした[44]。張氏は、「個人情報保護法に公益訴訟条項を設けることは、個人の権利保護コストが高

---

40 http://www.gov.cn/zhengce/zhengceku/2021-11/06/content_5649420.htm を参照。
41 最初に上記のリストの制定を求められる企業はテンセント、アリババ、美団、快手、拼多多など 39 社がある。
42 青瞳視角「工業情報化部が個人情報の整頓について言及　チェンの全体の監督管理体系を構築へ」（https://baijiahao.baidu.com/s?id=1716578904944872070&wfr=spider&for=pc）を参照。
43 中国網直播「工業情報化部：テンセントに対して経過的な行政指導措置を取る」（https://baijiahao.baidu.com/s?id=1717319873909996941&wfr=spider&for=pc）を参考。
44 中国個人情報保護法 70 条：個人情報取扱者が本法の規定に違反し個人情報を取扱い、多くの本人の権利利益を侵害した場合、人民検察院、法律の規定する消費者組織及び国家インターネット情報部門が確定した組織は法に基づき人民法院に訴訟を提起することができる。

く、訴訟時間が長い等の問題を解決するのに有利であり、個人情報分野の権益保護に対する力を強めている。公益訴訟は個人情報保護の利器になりつつあると言っても過言ではない」と述べた[45]。例えば、2021 年 11 月 1 日、杭州インターネット法院は公益提訴者である拱墅区人民検察院が被告の劉氏を訴えた個人情報保護紛争民事公益訴訟事件を公開審理し、判決を言い渡し、被告の劉氏に損害賠償金人民元 1.4 万元余りを負担させ、国家レベルのメディアで公開謝罪するよう命じた。同日、江蘇省常州市中級人民法院は公益訴訟の提訴者である常州市人民検察院と被告である田氏との個人情報保護民事公益訴訟事件を公開判決し、個人情報保護法の規定に基づき、田氏が国家レベルのメディアで社会公衆に謝罪し、人民元 9000 元余りを賠償すると判決した。さらに 2021 年 12 月 10 日、江蘇省揚州市中級人民法院は、個人情報侵害民事公益訴訟事件を開廷審理し、被告である張氏甲、張氏乙に対し、社会公衆に対して謝罪するとともに、損害を受けた社会公共利益に対して権利侵害の停止及び損害賠償の責任を負うよう判決を下した。

さらに、2022 年 1 月 18 日、国家発展改革委員会等の主管部門は「プラットフォーム経済の規範的で健全かつ持続的な発展の推進に関する若干の意見」を公布し、個人情報の収集・使用の合法・正当・必要の原則を着実に貫徹し、プラットフォーム企業による範囲を超えた個人情報収集、権限を超えた個人情報の使用等の違法行為を厳しく取り締まり、必要のないデータ収集行為を厳しく管理し、法に基づき闇市場のデータ取引、ビッグデータの殺熟等のデータ乱用行為を取り締まるよう強調した[46]。

６．２．「データ税」？

2021 年 10 月、前重慶市長である黄奇帆氏は上海外灘金融サミットでデータ税を提唱し、企業がユーザーデータを収集することで得た収益を統計し、その 20～30%をデータ税として回収するよう提案した。これは中国共産党政府が新たな税金を投入する際の「観測気球」ではないかとされている[47]。このようなデータ税の概念は、中国政府が打ち出す「共同富裕」と軌を一にする。そこで、タオバオを保有するアリババやウィーチャットを保有するテンセントが課税対象としてされて、税率は 3 割程度になると予想されている[48]。

６．３．ネットワーク安全審査対象の拡大

ネットワーク安全審査弁法（2020 年 6 月 1 日公布、2021 年 12 月 28 日改正、2022 年 2 月 15 日施行）は、中国国家安全法、中国サイバーセキュリティー法、中国データ安全法、重要情報インフラ施設安全保護条例等の法令に基づき、2021 年 12 月 28 日に改正された

---

45 澎湃政務「『人民第一を堅持』個人情報保護法施行から 2 ヶ月余り公益訴訟が個人情報保護の利器に」（https://m.thepaper.cn/baijiahao_16241854）を参照。

46 金融界「発改委等：範囲を超えたプラットフォーム企業の個人情報収集を厳しく取り締まり、オンライン配車担当者、オンライン配車ドライバー等労働者の権益保障を実施」（https://baijiahao.baidu.com/s?id=1722373957826314762&wfr=spider&for=pc）を参照。

47「中国がアリババ、テンセントに対してデータ税を課しようとする　税率は収益の 3 割」（https://www.rfa.org/mandarin/yataibaodao/jingmao/gf-11232021092342.html）を参照。

48「中国のデータ税徴収予定報道を受け、テンセント及びアリババの株価が下落した」（http://column.etnetchina.com.cn/column-list-EtnetcolB268/96222.htm）を参照。

（以下「2022 年版ネットワーク安全審査弁法」という。）。

2022 年版ネットワーク安全審査弁法 2 条は、ネットワーク安全審査の適用範囲を、従来の「重要情報インフラ運用者によるネットワーク製品とサービスの購入」だけではなく、「ネットワークプラットフォーム運営者によるデータ取扱活動」にまで拡大し、これらの活動が国家の安全に影響を及ぼし、又は影響を及ぼす可能性がある場合、ネットワーク安全審査が求められている。

ネットプラットフォーム運営者の上場について、同弁法 7 条では、「100 万人を超えるユーザーの個人情報を保有しているネットプラットフォーム運営者が国外で上場する場合」、ネットワーク安全審査を申請する必要があると明確化された。さらに、同弁法 10 条では、ネットワーク安全審査で重点的に評価される安全リスク要素について、①コアデータ、重要データ又は大量の個人情報が窃取、漏洩、毀損及び不法利用、違法な越境移転をされるリスク、②上場には、重要情報インフラ、コアデータ、重要データ又は大量の個人情報が外国政府に影響、コントロール、悪用をされるリスク、及びネットワーク情報安全リスクが存在する場合という 2 点を追加された。これまで、中国企業が米国に上場することは多いものの、その結果、海外に情報が移転されたり、情報漏洩等のリスクを高めたりするのではないか、という懸念が存在した。2022 年版ネットワーク安全審査弁法は、この懸念に対応したものである。

なお、100 万人を超えるユーザーの個人情報を保有しているネットプラットフォーム運営者が香港で上場する場合、上記のネットワーク安全審査弁法 7 条に定める国外上場に該当するか否かについて、これは国外上場に該当しない可能性があると考えられる。2021 年 11 月 14 日付け「ネットワークデータ安全管理条例（パブリックコメント募集案）」13 条 2 項では、100 万以上の個人情報データを取り扱うデータ取扱者が国外上場する場合、同条 3 項では、データ取扱者が香港で上場し、国家安全に影響を及ぼす又はその可能性がある場合、ネットワーク安全審査を申請するよう求められている。つまり、ネットワークデータ安全管理条例は、まだパブリックコメント募集段階にあるが、立法上、香港上場と海外上場を区別していると考えられる。なお、香港で上場する場合、必ずしもネットワーク安全審査を受ける必要がないわけではなく、今後の立法によっては、国家安全に影響を及ぼす又はその可能性がある場合、100 万人を超えるユーザーの個人情報を保有しているネットプラットフォーム運営者が香港で上場する際でも、ネットワーク安全審査を申請しなければならない可能性がある。

以上

＊本稿は、2021 年 12 月 20 日に情報通信法学研究会通信法分科会（令和 3 年度第 2 回会合）において「中国における個人情報保護法 ―中国における個人情報保護法制と、経済安全保 障の文脈下におけるクラウドサービスにおけるデータの適切な運用に関する法的示唆等を含む―」と題して報告した内容を元にしている。同報告及び本稿は桃尾・松尾・難波法律事務所中国律師胡悦様に多大な協力を得た。ここに感謝の意を表したい。なお、本稿校正中の 2022 年 2 月 24 日に、いわゆるロシアによるウクライナ侵攻が発生し、経済安全保障に関する新たな状況が発生しているものの、本稿ではこれを取り入れることができていないことをお詫びしたい。