LeeZhao
www.leezhao.com

里兆律师事务所 Leezhao Law Office
中国上海市陆家嘴环路 1000 号恒生银行大厦 29 层
29F, Hang Seng Bank Tower, 1000 Lujiazui Ring Road, Shanghai, China
Tel (86-21) 68411098 Fax (86-21) 68411099 Postal Code 200120

《数据安全法（草案）》解读

2020 年 06 月全国人大常委会审议了《数据安全法（草案）》（以下简称“《数据安全法》”），并于 2020 年 07 月 03 日公开向社会征求意见。《数据安全法》主要涉及数据分类分级保护、数据安全审查制度、数据出境监管、数据安全合规义务等内容，本文将对此作简要介绍。

■ 《数据安全法》的适用范围

根据《数据安全法》第 2 条，《数据安全法》适用于中国境内开展的数据活动，特定情形下，其也适用于中国境外的组织、个人，具有域外效力（具体请见下表）。

项目	概要	简要解读
规制主体	▪ 原则：中国境内组织、个人。 ▪ 例外：中国境外组织、个人（当其损害中国国家安全、公共利益或公民、组织合法权益时）。	▪ 原则上《数据安全法》仅对境内主体适用，但当境外主体开展数据活动损害中国利益时，国家有关部门可依据《数据安全法》追究其法律责任。
规制客体	▪ 数据活动，即数据的收集、存储、加工、使用、提供、交易、公开等行为。 ▪ 数据是指任何以电子或非电子形式对信息的记录。	▪ 数据的概念非常宽泛，不单单限于《网络安全法》、《个人信息安全规范》所保护的个人信息及重要数据。 ▪ 数据活动已成为中国境内组织/个人开展业务、日常生活所必不可少的环节（例如，收发邮件/微信、寄送文件均属于数

「データセキュリティ法（案）」を読み解く

2020 年 6 月に、全国人民代表大会常務委員会において「データセキュリティ法（案）」（以下「『データセキュリティ法』」という）について審議が行われ、2020 年 7 月 3 日には社会に向けてパブリックコメントが募集された。「データセキュリティ法」は、主にデータの分類別及び等級別の保護、データセキュリティ審査制度、データの越境移転に対する監督管理、データセキュリティのコンプライアンス義務等の内容に係るものである。本稿では、これらについて簡潔に紹介する。

■ 「データセキュリティ法」の適用範囲

「データセキュリティ法」第 2 条によると、「データセキュリティ法」は中国領域内で展開されるデータ活動に適用され、特定の状況下では中国領域外の組織、個人にも適用され、域外効力を有するとされている（詳細は下表を参照）。

項目	概要	考察ポイント
規制主体	▪ 原則：中国領域内の組織、個人。 ▪ 例外：中国領域外の組織、個人（中国の国家安全、公共の利益又は公民、組織の適法な権益を損なう場合）。	▪ 原則上、「データセキュリティ法」は領域内の主体のみに適用されるが、領域外の主体が行うデータ活動が中国の利益を損なった場合、国の関係部門は「データセキュリティ法」に基づき、その法的責任を追及することができるとされている。
規制客体	▪ データ活動。即ち、データの収集、保存、加工、使用、提供、取引、公開等の行為。 ▪ データとは、いずれか電子的又は非電子的方式による、情報に対する記録をいう。	▪ データの概念は極めて広いものであり、「サイバーセキュリティ法」、「個人情報安全規範」によって保護される個人情報及び重要データに限らない。 ▪ データ活動は、中国領域内の組織及び個人の業務実施、日常生活に必要不可欠な節目となっているため（例えば、メール

		据活动），因此《数据安全法》的适用范围非常广泛，几乎涵盖了境内所有的组织/个人的日常活动。

■ **数据分类分级保护**

《数据安全法》第 19 条规定，国家根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，对数据实行分级分类保护。在《数据安全法》出台之前，中国已对个人信息、金融信息、重要数据采取分类保护的原则，具体请见下表。

项目	概要
个人信息	▪ 《个人信息安全规范》将个人信息分为个人敏感信息和个人非敏感信息。 ▪ 个人敏感信息指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心、健康受到损害或歧视性待遇等的个人信息（例如身份证号、健康生理信息等）。个人非敏感信息指除个人敏感信息以外的个人信息。 ▪ 个人敏感信息需遵守更严格的收集、保存要求[1]。
个人金融信息	▪ 《个人金融信息保护技术规范》将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三个类别。 ▪ C3 类别信息主要为用户鉴别信息（例如银行卡密码等）。C2 类别信息主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息（例如银行账号、交易流水等）。C1 类别信息主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息（例如开户机构等）。

		や WeChat の受発信、書類の送付はいずれもデータ活動に該当する）、「データセキュリティ法」の適用範囲が極めて広く、領域内の全ての組織及び個人の日常活動をほぼ網羅している。

■ **データの分類別及び等級別の保護**

「データセキュリティ法」第 19 条では、国はデータの経済社会の発展における重要度、及びひとたび改ざん、破壊、漏えい又は不法に取得、不法に利用された場合に国の安全、公共の利益又は公民、組織の適法な権益にもたらされる危害の程度に応じて、データについて分類別及び等級別の保護を実施すると定めらている。「データセキュリティ法」が公布されるまでは、中国では、個人情報、金融情報、重要データについて、分類別保護を原則採用しており、詳細を下表に整理する。

項目	概要
個人情報	▪ 「個人情報安全規範」によると、個人情報を機微な個人情報と非機微個人情報に分けられる。 ▪ 機微な個人情報とは、ひとたび漏えい、不法提供、濫用された場合に人身及び財産の安全に危害をもたらすおそれがあり、個人の名誉、心身、健康に対し損害又は不利な待遇等を極めて受けやすい個人情報（例えば、本人証明書番号、フィジカルヘルス情報等）をいう。非機微個人情報とは、機微な個人情報以外の個人情報をいう。 ▪ 機微な個人情報は、より厳格な収集及び保存上の要求を遵守しなければならない[1]。
個人金融情報	▪ 「個人金融情報保護技術規範」では、個人金融情報の機微度の高い順から C3、C2、C1 という 3 種類に分けられる。 ▪ C3 類の情報は主にユーザー認証情報（例えば、銀行カードのパスワード等）である。C2 類の情報は主に特定の個人金融情報主体の身元及び金融状況を識別できる個人金融情報、並びに金融商品とサービスに用いられる重要情報（例えば、銀行口座番号、入出金明細等）である。C1 類の情報は主に機構内部の情報資産であり、金融業機構の内部

[1] 具体请见本所资讯文章《新版<个人信息安全规范>与<个人金融信息保护技术规范>简要对比分析》（LeeZhao Newsletters_Issue 681_20200609-20200615）。

[1] 具体的には弊所ニュースレターで紹介した「新版『個人情報安全規範』と『個人金融情報保護技術規範』を簡潔に比較し分析する」を参照のこと（LeeZhao Newsletters_Issue 681_20200609-20200615）。

	▪ C2、C3 类别个金融信息需遵守更严格的收集、传输、储存、共享要求[2]。
重要数据	▪ 《网络安全法》首先提出了“重要数据”这一概念，其要求关键信息基础设施运营者在中国境内收集和产生的重要数据应当在境内存储，确需提供给境外的，应当进行安全评估。但《网络安全法》并未明确重要数据的具体范围。 ▪ 重要数据通常指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据（例如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等）[3]。

	で使用する個人金融情報（例えば、口座開設機構等）をいう。 ▪ C2、C3 類の個人金融情報に係る収集、伝送、保存、共有の要求はさらに厳格なものである[2]。
重要データ	▪ 「サイバーセキュリティ法」は初めて「重要データ」という概念を持ち出し、重要情報インフラ運営者が中国領域内に収集し発生した重要データは領域内で保存するものとし、どうしても国外へ提供する必要がある場合には、セキュリティ評価を実施するよう求めている。但し、「サイバーセキュリティ法」では、重要データの具体的な範囲は明確にされていない。 ▪ 通常、重要データとは、ひとたび漏えいされた場合、国の安全、経済の安全、社会の安定、公共の健康と安全に直接、影響を与え得るデータをいう（例えば、未公開の政府情報、広大な面積における人口、遺伝子の健康、地理、鉱産資源等）[3]。

此次《数据安全法》着眼于重要数据，明确了各地区、各部门应当制定本地区、本行业的重要数据保护目录，对列入目录的数据进行重点保护。在2017 年颁布的推荐性国家标准《数据出境安全评估指南（征求意见稿）》附录 A（《重要数据识别指南》）中，有关部门已经以行业作为区分标准，规定了重点行业内重要数据的范围。或许是由于重要数据分类非常复杂，《重要数据识别指南》正式版并未发布。此次《数据安全法》重申了重要数据识别问题，体现出中国愈加关注数据对于国家安全、公共利益的重要性，未来将强化对重要数据的保护。

今回、「データセキュリティ法」は重要データに着目しており、各地域、各部門が本地区、本業種の重要データ保護リストを定め、リスト収載のデータを重点的に保護することを明確にした。2017 年に公布された推奨性国家標準である「データの越境移転セキュリティ評価ガイドライン（意見募集案）」付録 A（「重要データ識別ガイドライン」）では、関係部門はすでに業種ごとに、重点業種内の重要データの範囲を定めている。しかし、重要データの分類が非常に複雑であるためか、「重要データ識別ガイドライン」正式版はまだ公布されていない。今回、「データセキュリティ法」は重要データの識別問題を再び提起しており、中国が国の安全、公共の利益においてデータの重要性を重視し、将来、重要データに対する保護をさらに強化していくことの現れである。

■ 数据安全审查制度

《数据安全法》第 22 条规定，国家建立数据安全审查制度，对影响或者可能影响国家安全的数据活动进行国家安全审查。但其未明确数据安全审查的具体内涵及流程。未来如何开展审查，还有待于细则的出台。

■ データセキュリティ審査制度

「データセキュリティ法」第 22 条では、国がデータセキュリティ審査制度を構築し、国の安全に影響を与え、又は与える恐れのあるデータ活動について国の安全審査を実施すると定めているが、データセキュリティ審査の具体的な意味及び手順は明確にされていない。この先どのように審査が行われるかは、細則の公布が待たれる。

■ 数据出境监管

数据出境一直是企业关心的热点话题，《网络安全法》提出对个人信息和重要数据出境采取安全

■ データの越境移転に対する監督管理

データの越境移転は、従来から企業が関心を払っているホットなテーマであり、「サイバーセキュリティ法」では、個

[2] 同脚注 1。
[2] 脚注 1と同じ。
[3] 现行有效的法规未对重要数据进行定义，该定义源于《数据安全管理办法（征求意见稿）》第 38 条。
[3] 現行有効の法規では、重要データの定義はまだ定められておらず、当該定義の出典は「データセキュリティ管理弁法（意見募集案）」第 38 条である。

评估制度[4]。此次《数据安全法》第 10 条、第 23 条和第 33 条从宏观角度明确了中国未来的数据出境监管方向（具体请见下表）。由此可以看出，中国将继续推动数据的自由流动，但数据流动并不是绝对的，特定类型的数据出境将受到管制。

监管方向	具体内容
推动数据跨境流动	▪ 国家积极开展数据领域国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。
数据出口管制	▪ 国家对与履行国际义务和维护国家安全相关的属于管制物项的数据依法实施出口管制。
境外执法机构调取数据	▪ 境外执法机构要求调取存储于中国境内的数据的，有关组织、个人应当向有关主管机关报告，获得批准后方可提供。

■ 数据安全合规义务

如上所述，《数据安全法》的适用范围非常广泛，几乎对所有企业均适用。根据《数据安全法》第 25 条、第 27 条和第 29 条，境内组织/个人开展数据活动，应当遵守如下义务：

1. 采用合法、正当的方式收集数据，不得窃取或以其他非法方式获取数据；
2. 建立健全全流程数据安全管理制度；
3. 组织开展数据安全教育培训；
4. 采取相应的技术措施和其他必要措施，保障数据安全；
5. 加强风险监测，发现数据安全缺陷、漏洞等风险时，立即采取补救措施；
6. 发生数据安全事件时，及时告知用户并向有关主管部门报告；
7. 重要数据处理者，应当设立数据安全负责人和管理机构，定期开展风险评估并向主管部门报告。

人情報及び重要データの越境移転についてセキュリティ評価制度[4]を講じることを提起している。今回、「データセキュリティ法」第 10 条、第 23 条及び第 33 条はマクロ的な立場から、将来、中国におけるデータの越境移転に対する監督管理の方向性を明確にした（詳細は下表を参照のこと）。このことから、中国は自由なデータ流動化を引続き推し進めていきながらも、データの流動化が制限なく行われるわけではなく、特定の分類のデータを越境移転させる際には規制を受けることになるのがわかる。

監督管理の方向性	具体的な内容
データの越境移転の推進	▪ 国は、データ分野における国際交流と連携を積極的に行い、データセキュリティに係る国際ルール及び基準の制定に参加し、越境移転するデータの安全且つ自由な流動を促す。
データ輸出の規制	▪ 国際義務の履行及び国の安全の維持に係る規制物質のデータに該当する場合、国は法に依拠し輸出規制を実施する。
領域外の法執行機関によるデータの取り寄せ	▪ 領域外法執行機関が中国領域内で保存されるデータの取り寄せを求める場合、関連組織、個人は係る主管機関へ報告し、許可を得てからでなければ提供することができない。

■ データセキュリティのコンプライアンス義務

上記の通り、「データセキュリティ法」の適用範囲が極めて広く、ほぼすべての企業に適用される。「データセキュリティ法」第 25 条、第 27 条及び第 29 条によると、領域内の組織及び個人がデータ活動を行う際には、以下の義務を遵守しなければならない。

1. 適法、正当な方式によりデータを収集すること。窃取、又はその他不法な方式によりデータを入手してはならない。
2. 全過程にわたるデータセキュリティ管理制度を構築し、健全化すること。
3. データセキュリティに関する教育研修を実施すること。
4. 然るべき技術的措置及びその他必要な措置を講じて、データセキュリティを保障すること。
5. リスクモニタリングを強化すること。データセキュリティに脆弱性、バグ等のリスクが発見された場合、直ちに対策を講じること。
6. データセキュリティ事件が発生した場合、速やかにユーザーに通知し、且つ係る主管部門へ報告すること。
7. 重要データ処理者は、データセキュリティ責任者及び管理機構を設置し、リスク評価を定期的に実施し、且つ主管部門へ報告すること。

[4] 《网络安全法》第 37 条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

[4] 「サイバーセキュリティ法」第 37 条：重要情報インフラ運営者が中華人民共和国領域内での運営過程で収集し発生した個人情報及び重要データは、領域内で保存しなければならない。業務上の都合からどうしても国外へ提供する必要がある場合、国のインターネット情報部門、国務院の関係部門が共同で制定した弁法に従ってセキュリティ評価を実施しなければならない。法律、行政法規に特段の規定がある場合、その規定に従う。

结语：

此次《数据安全法》，一改以往《网络安全法》所确立的重点保护个人信息和重要数据的原则，将所有类别的信息均纳入保护范畴，未来《数据安全法》如何与《网络安全法》、正在起草中的《个人信息保护法》等法律衔接，尚不明朗。现阶段，企业仍须以《网络安全法》、《个人信息安全规范》等制度，对个人信息的处理活动进行规范和保护，落实企业个人信息保护义务。

（里兆律师事务所 2020 年 09 月 25 日编写）

終わりに：

今回の「データセキュリティ法」は、これまでに「サイバーセキュリティ法」により確立された、個人情報及び重要データに重点を置いて保護する原則を一変させ、全種類の情報を保護範囲に組み入れたが、将来、「データセキュリティ法」と「サイバーセキュリティ法」、起案中の「個人情報保護法」等の法律との整合性をどのように取っていくのかは、まだ明確にされていない。現段階では、企業は引き続き「サイバーセキュリティ法」、「個人情報安全規範」等の制度に従い、個人情報処理活動の規範化及び保護に取り組み、企業の個人情報保護義務を遂行しなければならない。

（里兆法律事務所が 2020 年 9 月 25 日付で作成）