2021.12.1

中国風険消息〈中国関連リスクニュース〉 <2021 No.6>

「中国データ安全法（データセキュリティ法）」の解説

本稿は、上海開澤法律事務所 パートナー弁護士の王穏氏に寄稿いただきました。

【要旨】
◆ 2021 年 6 月 10 日、第十三期全国人民代表大会常務委員会第二十九回会議において、「中国データ安全法（データセキュリティ法）」が通過し、2021 年 9 月 1 日より正式に施行された。
◆ 本法律は中国政府が国家戦略としてデータ安全保護の重要性を定め、データ安全領域の基礎を固めることを企図するものである。
◆ 本稿では、「中国データ安全法」の概要および企業が注意すべきポイントを事例を交えて解説する。

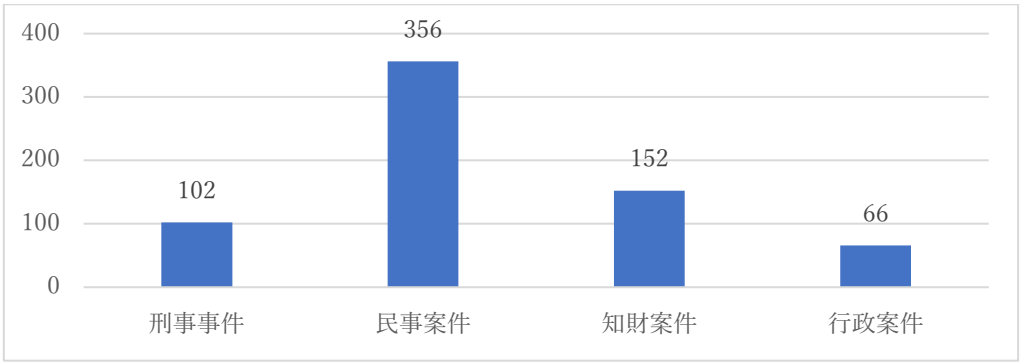
1. はじめに

2021 年に入り、中国政府は国家情報の安全、インターネットの安全、データの安全、個人情報の保護を目的として、多くの法令や関連する規範文書を公布している。データの監督・管理を国家の情報戦略とする観点より、企業データのコンプライアンスの発展に関する重要な内容の明確化を図っている。それらのうち、データ安全の監督・管理に着目した法律として、「中国データ安全法（データセキュリティ法）」が新たに公布された。

中国データ安全法は、7 章 55 条から構成される。同法では、データ安全保護に関する主体的な義務・責任が明確に規定されている。「データ安全と発展」の章では、各制度体系について、「データ安全体系」および「データ安全保護義務」の章では、重要データの処理者がデータ安全の責任者・管理組織を明確にすること、データ安全保護の管理を徹底することが重点項目として明記されている。

本稿では、昨今頻発している製品データの紛争、ビッグデータを悪用した詐欺行為、消費者のプライバシーの漏洩、ミニプログラム（アプリ）による情報収集などのコンプライアンス面の問題に着目し、中国データ安全法について解説する。

＜中国における近年の司法裁判案件数_「キーワード：データ安全」で検索[1]＞



[1] 出典：北大法宝司法案例庫_2021 年 11 月 5 日時点のデータ

前述のグラフから分かるとおり、企業（特に外資系企業）は同法への対策を重視し、法的リスクに留意する必要がある。

＜データ安全保護の適用主体／具体的要求＞

要求	適用主体	具体的要求
内部管理の仕組み構築の義務	企業/社会団体	1. 全面的なデータのセキュリティ管理体系 2. データ安全責任者、責任部門体制 3. データ安全リスクの把握、報告、顧客への通知体制 4. データ安全リスクの評価体制 5. データ出典、取引先の身分照合、データの交信記録等、データ取り扱いに関するコンプライアンスの仕組み
従業員研修の義務	企業/社会団体	データ安全に関する教育・研修の定期的な実施
合法義務	①企業/社会団体 ②個人 ③国外機構	データ収集方法の合法性/正当性を確保し、国家の安全、他人の利益を損ねないこと
協力義務	①企業/社会団体 ②個人	公安、国安等部門がデータにアクセスする際に協力すること
報告義務	①企業/社会団体 ②個人	国外の法的な執行機構が中国域内の保管データにアクセスする場合には、遅滞なく報告すること

2. 沿革

近年、中国では、企業・個人に関するデータの漏洩が頻発している。被害の範囲は広く、影響も大きいといえる。多くの企業はデータ保護に関するコンプライアンスと社会世論の圧力の二重の危機に陥っている。

「データ安全法」は、2020 年 7 月 3 日に草案が提出され、2021 年 6 月 10 日に全人大常務委員会を通過し、比較的短期間のうちに制定された。

この理由として、以下の 2 つが考えられる。1 つは「サイバーセキュリティ法」「個人情報保護法」や他国のデータ法の立法を参考としたことである。そして、もう 1 つは中国国内でデータ安全に関する事件が頻発したことを受け、世論のデータ安全への意識が高まったことである。

同法の条項では、法律の技術的な側面より、データ安全の制度、データの安全保護義務、政務データのセキュリティと公開に関する規定がある。また、特にセンシティブなデータの保護、ビッグデータ安全に関する違法行為に対する取り締まりを強化することが強調されている。

3. 重点解説

「データ安全法」は、既存の有効な法的文書のデータ保護に関する規定を踏まえた上で、中国の現在の実務や国際経験に基づき、国内でのデータ管理を強化することを目的としている。企業と国家競争力の向上を支援するための「中国におけるデータの安全保護方案」を形成するものである。同法はデータ安全領域に特化した法律として、各業界・領域において、データ処理活動に取組む際の重要な法律根拠となる。同時に、「サイバーセキュリティ法」とともに、「国家安全法」の枠組みのもと、セキュリティガバナンスの法律体系を補完するものとなる。

(1) 適用範囲の明確化

同法第 1 条、第 2 条の規定によると、同法の適用範囲は中国国内でデータ処理活動およびその安全監督・管理を行う組織・個人とされている。注意すべき点は、同法第 2 条第 2 項に、国外でのデータ処理活動を行ったことにより、中国の国家安全、公共利益や公民、組織の合法権益を損なった場合には、法的責任を追及されることが明確化されたことである。

【要点】

上記の適用範囲をふまえると、企業・個人が中国国内でデータ処理活動を行う際には、同法が適用されることとなり、安全に関する監督・管理を受けなければならない。中国国外でデータ処理活動を行う場合についても、全く制約を受けないわけではなく、国外のデータ処理活動が国家安全、公共利益や公民、組織の合法権益を損なった場合には、同様に法的責任を追及されることとなる。

【実務対応】

中国国内の外資系企業が国外の親会社に対し、関連データ情報を提供する場合には、データ量・範囲・種類・機密性の程度について評価を行う必要がある。特に、大量のデータを国外に送信する際には、慎重を期すことが求められる。特に、企業における VPN 回線の使用に伴うコンプライアンス問題に留意する必要がある。

(2) データ安全の監督・管理体制の明確化

同法第 5 条、第 6 条の規定によると、中央国家安全指導機構が国家データ安全作業の意思決定と調整を行う。各地域の政府部門は、地域ごとにデータの収集・生成、保護に関する事項を指導する。国家安全機関、公安機関、国家通信部門および工業、電信、交通、金融、自然資源、衛生健康、教育、科学技術等の主管部門は、各自の職責範囲内でデータ安全を監督・管理する。

【要点】

監督・管理体系をみると、国家安全機関が「センター」、公安機関と通信部門が「監督・管理組織」となっている。これらの体系は様々な業界（主に工業、電信、交通、金融、自然資源、衛生健康、教育、科学技術等の主管部門など）に水平展開されている。行政管轄の範囲では、各地区・部門による本地区・部門の作業に関連するデータの収集・生産、データ安全事項への指揮について明記されている。このほか、第 12 条でも、同法の規定における違反行為が発生した場合には、個人・組織が関連する主管部門に告発・通報できることが明確化されている。これは、各地区・部門、各業界、公民や組織がデータ安全監督・管理に共同で参画することを保証するものであり、監督・管理政策を徹底させることにつながる。

【実務対応】

政府は企業の経営範囲に関連する管理機構に対し、監督・管理に関する多くの権限を付与している。例えば、金融、電信、科学技術等に関連する政府機構が該当する。企業はこれらの機構が管理する職能範囲および行政責任に留意する必要がある。

(3) データ処理活動で遵守すべき規範とルールの構築

同法第 8 条の規定によると、データ処理活動で遵守すべき規範・ルールには、法律や法規の遵守、社会道徳・倫理、商業道徳や職業道徳の尊重が含まれる。

【要点】

同条項では個人・組織のデータ処理活動が遵守すべき規範やルールが列挙されている。特記すべきは、法律や法規以外に社会道徳・倫理、商業道徳や職業道徳、信義則、「危害や損害を与えない」などの原則が明記されている点である。これらは企業・個人のデータ処理活動が、コンプライアンス上問題がないかを評価するための重要な根拠となる。

(4) データ安全保護制度の構築

同法第 21 条、第 24 条の規定によると、国はデータ安全分類・等級保護制度、およびデータ安全審査制度を構築している。データ安全分類・等級保護制度には、以下の内容が含まれる。

① 経済・社会の発展の重要性、データが改ざん・破壊・漏洩、または違法に取得、利用された場合における国家安全、公共利益や個人・組織に及ぶ危害の程度に基づき、データの分類・等級保護を実施する。
② 国家データ安全作業協調機構が、政府各部門における重要データのリスト整備、重要データ保護の取組を統括する。
③ 国家安全、国民経済のライフライン、重要民生、重大公共利益等に関わるデータは国家の核心的データに該当するため、より厳格な管理制度を実行する。

データ安全審査制度では、国家安全に影響を及ぼす、または影響を及ぼすおそれのあるデータ処理活動に対し、国家安全審査を行うこととしている。法に基づく安全審査の決定が最終決定となる。

【要点】
データ安全分類・等級保護制度については、同法では、経済・社会の発展の重要性や改ざん、漏洩等の被害の程度に基づいて分類・格付けを行うことを原則としている。また、「重要データ」「国家の核心的データ」に対し、厳格な保護要求が特別に取り決められている。
同法が、地区や業界によりデータ分類・等級の具体的規則が異なり、検討要因にも差があることを踏まえた上で、重要データの具体的なリスト・分類、等級保護制度の制定権限を各地区の主管機関に限定して委譲したことは、法規定の普遍性・柔軟性を示しているといえる。
データ安全審査制度について注意すべき点は、国が法に基づき決定した事項は最終的決定であるということである。これは、関連する行政措置が、行政による再検討や訴訟等の方法により、救済されるものではないことを意味している。

【実務対応】
監督・管理機関は企業の基本的な経営情報を十分に把握したうえで、内部のデータベースに基づき、データ情報と実際の経営状況に関する合致度を比較する。重要／センシティブなデータが含まれる場合には、より重点的に確認する。外資系企業が、経済発展、民生発展、最先端の科学技術等に関する情報を取り扱う際には、照会結果、分析データ、親会社と連携する課題項目等について、より一層注意する必要がある。

(5) データの安全保護義務
同法第 4 章によると、企業は日常業務の一環として、データの安全保護義務を遵守する必要がある。全面的なデータ安全管理制度を構築する、データ安全に関する教育研修を実施するなど、適切な技術的対策および必要な対策を講じることにより、データ安全を保障しなければならない。インターネットやその他の情報ネットワークを活用してデータ処理活動を実施する場合には、インターネット安全等級保護制度に基づき、上記のデータ安全保護義務を履行する必要がある。

【要点】
前提として、データ収集は合法かつ正当な方法で行われる必要がある。データ収集は、関連する組織・個人より事前に承諾を得た上で実施するものとし、公序良俗に反する方法や詐欺、脅迫、誘導によってデータを収集・入手してはならない。また、データ収集の目的・範囲を予め開示し、データ収集・使用に関する規則を明示しなければならない。
次に、データ収集・使用は法律、行政法規が規定する目的・範囲内で取り扱わなければならない。法律、行政法規にデータ収集・使用の目的や範囲に関する規定がある場合には、記載された内容の範囲内でデータを収集・使用する必要がある。

【実務対応】
データ収集に関する行為は、情報保護の法的規制も同時に受けることとなる。したがって、営利目的で合法かつ正当といえない手段で、データ収集することは大きなリスクが伴う。

(6) 重要データのリスク評価
同法では、重要データのリスク評価を実施しなければならないとされている。重要データのリスク評価とは、重要データに対する一般的な監督・管理の仕組みである。第 30 条の規定によると、重要データの処理者は、規定に基づいてデータ処理活動を定期的にリスク評価し、関連する政府の主管部門にリスク評価報告を提出することとしている。重要データが収集、保存、使用、加工、送信、提供、公開等のどの処理段階にあるかに関わらず、データ処理活動が重要データに関わる可能性がある場合には、定期的なリスク評価を行い、所定の報告を実施しなければならない。

【要点】
リスク評価報告には、処理する重要データの種類、量、データ処理活動の状況、直面するデータ安全リスクや対応措置等の内容を含まなければならない。即ち、企業内の重要データに関するリスク評価をコンプライアンス要求として一般化させ、企業が取り扱う重要データのリスクマップを作成する必要がある。
法律によると、各地区・部門は、データ分類・等級保護制度に基づき、当地区・部門や関連する業界・領域の重要データの具体的なリストを整備する必要がある。リストに記載されるデータについては、重点的に保護し、「国家データ安全作業協調機構が、政府各部門におけるデータ安全リスク情報の取得、分析、評価、早期警戒等の対応を統括する」。

【実務対応】
各地（特に直轄市、経済発展地区等）の監督管理機構は、重要データの監督・管理、緊急処置、処理手順等に関する詳細な規則や規制を積極的に策定し、商務委員会、情報弁公室、市場監督管理局等の機構とのつながり、情報共有を強化しているとされる。

(7) データ越境の安全評価
同法では、重要データの越境に際しては、必ず安全評価を実施しなければならないとしている。第31条の規定によると、重要情報のインフラ運営者が中国国内で運営する中で収集・生産した重要データを越境させる場合には、その安全管理に関して、中国サイバーセキュリティ法の内容が適用される。その他のデータ処理者が同様に収集・生産した重要データの越境については、国家通信部門が国務院の関連部門と共同で管理方案を制定することとしている。

【要点】
「サイバーセキュリティ法」「個人情報および重要データの越境に関する安全評価弁法（意見募集稿）」「データ安全管理弁法（意見募集稿）」は、データ越境の安全評価について規定しているが、これらの内容はデータまたは重要データの越境プロセスに関する評価に限定されている。「サイバーセキュリティ法」第37条の規定によると、重要情報のインフラ運営者が中国国内で運営する中で収集・生成した重要データは国内で保存しなければならないとしている。業務上の理由により、国外へのデータ提供が必要な場合には、国家通信部門が国務院の関連部門と共同で制定した規定に基づき、安全評価を行わなければならない。

【実務対応】
同条は重要情報のインフラ運営者の行為を対象としているが、監督・管理機構が実際に管理する過程での法執行力はより広範囲に及ぶ。国内の外資系企業や国外機構（親会社、関連会社、国外コンサルタント等）との間でのデータ交換やデータ情報提供に関する経営行為も対象となる。

(8) 処罰の強化
データ安全問題がもたらす深刻な結果を考慮し、同法第45条、第46条、第47条、第48条では、同法規定に違反してデータを処理したり、データ保護義務を履行しなかった場合には、比較的重い法的責任が課されることとされている。具体的な内容は以下のとおりである。

処罰類型	処罰の内容
行政罰	① 規定された保護義務を履行しない場合：是正・警告を命じ、事業者に 5 万～50 万元の罰金、責任者に 1 万～10 万元の罰金を科す。是正を拒んだりデータの大量漏洩などにより深刻な影響をもたらした場合には、事業者に 50 万～200 万元の罰金を科す。また、業務許可証や営業許可証の取り消しを命じ、責任者に 5 万～20 万元の罰金を科す場合もある。 ② 国家安全を脅かし、合法権益を損なった場合：200 万～1000 万元の罰金を科す。また、営業停止、業務許可証や営業許可証の取り消しを命じる。 ③ 国外へ重要データを提供した場合：関連する政府主管部門が是正・警告を命じ、10 万～100 万元の罰金を科す。直接の担当者およびその他の直接の責任者に 1 万～10 万元の罰金を科す場合もある。深刻な事態が発生した場合には、100 万～1000 万元の罰金を科す。また、営業停止、業務許可証や営業許可証の取り消しを命じ、責任者に 10 万～100 万元の罰金を科す場合もある。 ④ 出所不明のデータ：違法所得を没収し、当該所得の 1～10 倍の罰金を科す。違法所得がない、または違法所得が 10 万元に満たない場合には、10 万～100 万元の罰金を科す。営業許可証の取り消し、担当および直接の責任者に 1 万～10 万元の罰金を科す場合もある。 ⑤ データ取得への協力を拒否した場合：関連する主管部門が是正・警告を命じ、5 万～50 万元の罰金を科す。直接の担当者およびその他の直接の責任者に 1 万～10 万元の罰金を科す場合もある。
治安管理罰	同法規定に違反し、治安管理の違反行為を行った場合には、治安管理罰を科す。
民事責任	同法規定に違反し、他人に損害を与えた場合には、民事責任を負う。
刑事責任	同法規定に違反し、犯罪を行った場合には、刑事責任を追及する。

【要点】

同法はデータ安全の違法行為への処罰の程度を引き上げている。企業はデータ処理活動において、必要以上の行政監査を回避し、法的責任を負うことがないよう注意が必要である。

4. 事例概述

事例 A	2018 年 8 月、北京の某上場会社はインターネット企業と共謀して大手数社を含む全国のプラットフォーマー96 社のユーザー個人情報 30 億個を不法に取得し、数千万元の不法利益を得た。 会社の法定代表者、董事、監事など 7 名がコンピュータ情報システムデータの不法取得罪で 2 年から 3 年 6 か月の刑に処された。また、1000 万元の罰金を科された。
事例 B	2020 年 1 月、某航空会社から中国国家安全機関へ、同社の情報システムに異常が発生し、サイバー攻撃の被害に遭った可能性が疑われると報告があった。国家安全機関は技術検査を通じ、同社の情報システムが国外からのサイバー攻撃の被害に遭ったことを確認した。技術的な抜け穴を利用し、攻撃対象である会社のサーバー・ネットワーク設備をトロイの木馬（マルウェア）に感染させたものであり、乗客の旅行記録などのデータが窃取されたことが判明した。また、その他の航空会社（数社）でも情報システムに同様の被害が発生していた。対応策として、国家安全機関はサイバー攻撃の被害に遭った航空会社に技術的な支援を行い、トロイの木馬を全面駆除し、データ紛失の損失拡大を抑えた。
事例 C	2020 年 5 月 6 日、トークタレントの C 氏は自身の SNS にて、所属プロダクションである D 社とのマネジメント契約紛争において、E 銀行が、C 氏本人の承諾なく、個人口座明細を D 社に提供したことは、公民の個人情報を侵害する違法行為である、と配信した。5 月 9 日、中国銀保監会は速やかに「E 銀行の消費者合法権益の侵害に関する通報」を公布した。E 銀行が顧客の委任を受けることなく、第三者に個人銀行口座の取引明細を提供したことは、預金者への秘密保持義務の原則に違反するものであると判断した。また、「中国商業銀行法」「銀保監会の個人情報保護の監督管理規定」に違反する疑いがあり、消費者の情報保護の権利を著しく侵害したと判断した。その後、E 銀行は書面にて謝罪し、担当行員が規定に則った関連業務手続きを行わずに情報を提供し、C 氏に損害を与えたことについて謝罪の意を述べた。同時に、同行の関係者を処分し、支店長を免職処分とした。

上述の 3 つの事例はいずれも、データ安全保護に違反し、かつ個人情報の侵害に該当するものである。そのうち、事例 A は、上場会社が技術的な手段を通じて、顧客情報を窃取し、個人情報提供者の合法権益を直接侵害したものである。次に、事例 B は、2021 年 10 月 31 日に中国国家安全機関が公布した、重要データ安全を脅かす事例 3 件のうちの 1 件に該当するものである。これは、近年、中国国内の会社が国外のハッカーによってサイバー攻撃を受ける事件が多発していることを示すものである。このような事象は、中国政府のデータ監督管理安全を著しく脅かすのみならず、顧客情報の不法な漏洩を招く可能性がある。最後に、事例 C は、E 銀行の担当行員の規範違反により、顧客情報が不当に漏洩したものである。本件は、被害者が著名人であったことから、社会の注目を集めた。本事例は、顧客情報の管理制度の不備により、当該銀行において重大な抜け穴が発生したことを示している。

5. 企業コンプライアンスの提案

中国に進出する日系企業は、通常の業務において、企業経営情報、財務情報、マーケット情報、顧客情報等のデータにアクセスし、使用する際には、必要なデータ安全防護対策を構築したうえで、データ漏洩につながる行為を回避する必要がある。中国における日系企業という特性を踏まえ、業務の関係上、国外の親会社や関連会社に上述のデータを送信する際には、データの越境に関する中国政府の要求を遵守し、不必要な紛争を回避すべきである。

中国政府はデータ安全保護をより一層重視しており、近年では、サイバーセキュリティ、データ安全、個人情報保護に関する法律、行政法規、規範文書を集中的に多く公布している。これにより、一定のデータ安全に関する「防護網」が効果的に構築されているものの、情報技術の急速な発展、インターネット技術の更新などの各種要因により、データ安全に関連する侵害事例の発生も後を絶たない。筆者の経験をふまえると、中国における日系企業は、以下のデータ安全に関するリスクに直面する可能性がある。

① データを保存するパソコン、サーバーがサイバー攻撃に遭う。
② 会社データベースへのアクセス権限が未整備の場合、データを閲覧されたり、ダウンロード・窃取される。
③ 会社が保管する顧客データに対して適切な秘密保護措置を怠る。
④ 個人情報の提供者から同意を得ないまま、データを使用・処理する。
⑤ 中国政府の要求を満たすことなく、顧客や従業員データなどを越境送信する。

中国政府の関連政策の動向を随時注視するともに、自社が取り扱うデータ全体に対する安全保護制度の構築を徹底し、必要な防護対策を講じる必要がある。関連するデータの受信、保存、処理、送信、廃棄などの一連の具体的作業は法令を順守すべきである。コンプライアンス要求の具体的な内容は以下のとおりである。

① 研修の実施
データ安全管理の意識向上のため、定期的（または不定期）に従業員参加のデータ安全研修を実施し、従業員のコンプライアンス意識を強化する。
② データ安全担当の設置
社内にデータ安全運営センターを設置し、責任者やデータ安全管理者を配置する。全ての保存データを暗号化処理する。特に重要なデータは、重要データ用の防護対策（より強固な暗号化、ファイアウォールの設置など）を強化し、外部からのサイバー攻撃に備える。
③ 定期的なデータのメンテナンス
現状として、データ安全運営センターを設置できない場合には、社内にデータ安全管理者（最低１名）を設置し、日々のデータメンテナンスを行わせる。同時に、サイバーセキュリティの専業サービス業者に、第三者サーバでの会社データの保存管理、セキュリティホールに関する定期検査などの一連の安全管理作業を委託する。
④ 情報提供者からの同意書の取得
顧客情報や従業員のセンシティブ情報を収集する際は、情報提供者からデータの使用・処理に同意した委任状/同意書を取り付けること。これらには、収集・処理する個人情報の範囲、用途、保存期限、保護方式、提供者による閲覧、方式の変更・撤回などを含むこと。業務上、国外の親会社や関連会社にデータを提供する場合には、中国政府の関連規定に基づき、国外の受信主体と越境送信に関する契約を締結し、安全評価や個人情報保護認証を行う。

⑤　アクセス権限の明確化
従業員のデータアクセス権限制度を厳格に実行する。パスワード入力、生態認証、携帯電話の識別コードなどの二重チェック等を活用し、アクセスレベルを管理する。従業員はレベルに応じたデータベースアクセス権限を持つこととし、アクセス履歴は自動的に保存されるようにする。これにより、データ安全事故が発生した際に、アクセス履歴より事故原因を効率的に検索することができる。

⑥　外部からのハッカー攻撃に備える
データを保護するためのセキュリティソフトとデータベースを定期的に検査、更新、バージョンアップし、新種のコンピューターウイルスやマルウェアなどの外部からのサイバー攻撃に備える。

以　上

執筆：上海開澤法律事務所 パートナー弁護士　王穏
弁護士　叶俊
パラリーガル　赤塚　由紀子

＜執筆者略歴＞
◆ 王穏　氏
東京大学法学部、一橋大学院法学研究科を経て、1999 年から弁護士業務に従事。2004 年、上海にて上海開澤律師事務所を立ち上げ現在に至る。中国及び日本のビジネス・法律・文化・思考・傾向の違いや特徴を理解した上で、中国国内の日系企業への経営アドバイス（人事労務全般、債権回収、契約関連、商標知財、その他)、MA・再編・清算関連、仲裁・裁判など、包括的なリーガルサポートを行う。

上海開澤法律事務所は、今年で開設 17 年目を迎える日系企業を主要なお客様とする専門家集団です。日本企業の経営スタイル・思考・文化・言語に精通し、同時に中国人弁護士ならではの 強みを生かした、高度な専門性とスピード感あるサービスを提供しております。
日本でのセミナー登壇や研修講師、本社との疎通(中国現地事情、案件進捗の報告など)なども行っており、日本のお客様へのタイムリーな現地情報の提供や、日本 - 中国間の連携強化のサポートに努めております。
お問い合せ先　　上海開澤律師事務所
TEL. +86 (21) 6876-7600　　http://kzw-lawfirm.com/

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。
中国進出企業さま向けのコンサルティング・セミナー等についてのお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。
お問い合せ先　　ＭＳ＆ＡＤインターリスク総研　総合企画部　国際業務グループ
TEL.03-5296-8920　　https://www.irric.co.jp/

インターリスク上海は、中国 上海に設立されたＭＳ＆ＡＤインシュアランスグループに属するリスクマネジメント会社であり、お客様の工場・倉庫等へのリスク調査や、ＢＣＰ策定等の各種リスクコンサルティングサービスをご提供しております。
お問い合わせ・お申し込み等は、下記の弊社お問合せ先までお気軽にお寄せ下さい。
お問い合わせ先　　瑛得管理諮詢（上海）有限公司　（日本語表記：インターリスク上海）
上海市浦東新区世紀大道 100 号　上海環球金融中心 34 階 T10 室-2
TEL:+86-(0)21-6841-0611（代表）

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々に対して企業のＲＭ活動等に役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。

不許複製／Copyright ＭＳ＆ＡＤインターリスク総研 2021