

執筆者:

E-mail✉ [張 翠萍](#)E-mail✉ [志賀 正帥](#)E-mail✉ [盧 月亭](#)E-mail✉ [陳 致遠](#)E-mail✉ [林 婧](#)E-mail✉ [李 源](#)

1. 商用暗号管理条例¹

国务院、2023年4月27日公布、同年7月1日施行、行政法規

2020年1月1日に施行された「暗号法」²により、暗号が「核心暗号」、「普通暗号」及び「商用暗号」の三種類に区分して管理される枠組みが確立された。これを受けて、「商用暗号」に関連する規制の詳細化を図るべく、1999年10月7日に公布・施行された「商用暗号管理条例」(以下「旧条例」という。)は全面的に改正され、2023年5月24日にその改正法(以下「本条例」という。)が中央政府のHPに掲載された。本条例は全9章、67条から構成され、主な内容は以下のとおりである。

(1) 適用対象

本条例によれば、「商用暗号」とは、特定の変換方法により、国家秘密に属さない情報などに対して暗号化による保護、セキュリティ認証を行う技術、製品及びサービスをいう。また、本条例の適用対象は、中国国内で行われる商用暗号に関する科学研究、生産、販売、サービス、検測、認証、輸出入、使用等の活動及び監督管理である。旧条例と比べてみると、商用暗号の定義はあまり変更がないものの、適用範囲については、従来の生産、販売、輸出入等に加え、新たに科学研究、検測・認証及び使用が追加されたといえる。

(2) 商用暗号製品の生産、販売、使用、輸出入管理

旧条例は、商用暗号製品の生産や販売、外国産暗号製品の使用、国外組織・個人による中国国内での暗号製品又は暗号技術を含む設備の使用、暗号製品及び暗号技術を含む設備の輸入、商用暗号製品の輸出など、暗号製品に関する多くの行為について許認可制を採用していた。暗号製品に関する許認可制は、2017年以降徐々にその対象を狭めていったが、根拠法となる旧条例の関連規定は改正されずにそのまま残された。

本条例は、上記の許認可制の変化を規定に反映すると共に、輸出入規制について、暗号法の規定に基づき、輸入許可の対象を「国の安全、社会公共の利益とかかわり、かつ、暗号化による保護機能がある商用暗号」に限定し、輸出管理の対象を「国の安全、社会公共の利益とかかわり、又は中国が国際的義務を負う商用暗号」に限定し、その他の大量消費向けの製品に用いられる商用暗号については輸出入規制を行わない旨を明記した。

¹ 中国語: 商用密碼管理条例

² 中国語: 密碼法

(3) 検測・認証制度

暗号法は、商用暗号事業に従事する者³を対象に、任意実施の検測・認証制度を導入している⁴。検測を受けて認証を取得した場合、自社製品の信頼性や性能をアピールできる効果が期待されるほか、商用暗号を使用した保護措置の存在が法令によって義務付けられている重要情報インフラについて、自社製品を提供することも可能になる(後記(4)を参照)。

本条例では、上記の検測・認証制度に関連して、商用暗号の検測・認証業務に従事する場合には関連部門(検測業務:国家暗号管理部門、認証業務:市場監督管理部門)においてしかるべき資格(資質)を取得しなければならないと定められている。

(4) 商用暗号の使用の促進

本条例は、商用暗号を用いてネットワーク又は情報のセキュリティを保護することを奨励すると同時に、重要情報インフラ及びネットワーク運営者に対して具体的な義務も課した。

本条例によれば、商用暗号の使用による保護の実施が法令によって義務付けられている重要情報インフラについては、稼働すると同時に商用暗号による保障システムの計画・構築・稼働もしなければならず、また商用暗号応用安全性評価を稼働前に行い、かつ、稼働中には毎年行わなければならない。また、上記の重要情報インフラにおいて使用されている商用暗号製品・サービスは検測を経て認証を取得したものでなければならず、使用されている暗号アルゴリズム、暗号プロトコル、暗号キー管理メカニズムその他商用暗号技術も国家暗号管理部門の審査・鑑定をパスしていなければならない。

なお、ネットワーク運営者も、サイバーセキュリティ等級保護制度に基づいて、商用暗号を用いてネットワークの安全を確保しなければならないと、各サイバーセキュリティ等級に対応する暗号規格規範は国家暗号管理部門が制定するとされている。

2. 契約行政監督管理弁法⁵

国家市場監督管理総局、2023年5月18日公布、同年7月1日施行、部門規則

社会公益や消費者権益などの保護、市場経済の秩序を維持するために、国家市場監督管理総局(当時の国家工商行政管理総局。以下「SAMR」という。)は、2010年10月13日に「契約違法行為監督処理弁法」⁶(以下「旧弁法」という。)を公布した。旧弁法には、架空契約の禁止、定型約款⁷を利用して消費者の責任を加重したり事業者自らの責任を免除したりする行為の規制などが定められている。

民法典の公布を機に、SAMRは、旧弁法の見直しに着手し、2021年6月25日の意見募集を経て、2023年5月28日に旧弁法の改正法に当たる「契約行政監督管理弁法」(同年7月1日施行。以下「本弁法」という。)を正式に公布した。

(1) 規制の対象や方法

新弁法は、「民法典」及び「消費者権益保護法」を上位法として明記し、事業者が当事者となる契約を規制対象としている。なお、事業者が当事者となる契約のうち、消費者と締結する契約が主な規制対象といえる点は、旧弁法からは変わっていないと思われる。

³ 暗号法によれば、商用暗号の科学研究、生産、販売、サービス、輸出入等に従事する者を指す。

⁴ ただし、暗号法及び本条例によれば、国の安全、国の経済・国民の生活及び社会公共の利益とかかわる商用暗号製品は、検測・認証を経て初めて販売・提供できるとされており、上記要件に当たる商用暗号製品については検測・認証の実施が義務付けられているといえる。

⁵ 中国語: 合同行政监督管理办法

⁶ 中国語: 合同违法行为监督处理办法

⁷ 民法典 496 条 1 項によれば、「定型約款」とは、当事者が繰り返しの利用のために事前に制定した、契約を締結時に相手方と協議しない条項をいう。

また、旧弁法は、同弁法に抵触する内容のある契約について行政処罰などを与えるといった事後処罰が中心であるのに対し、本弁法では、事業者との契約に関する消費者問題の発生を未然に防ぐべく、事業者による定型約款の公示の推奨や、特定分野において当局による契約テンプレートの作成・公布など、事前抑制に関する内容も盛り込まれた。

(2) 主な規制内容

本弁法は、事業者が契約を通じて以下の行為をし、市場経済秩序を乱し、又は国の利益や社会公共の利益を害することを禁止している。

- 契約当事者としての主体資格を偽造し、又は他人の名義を冒用して契約を締結する行為
- 契約を履行する能力がないにもかかわらず、契約を締結するよう相手方を誘惑し騙す行為
- 契約の目的の実現に重大な影響のある情報を故意に隠蔽して相手方と契約を締結する行為
- 悪意による通謀、賄賂、脅迫等の手段により契約を締結する行為
- その他契約を通じて市場経済秩序を乱す行為

また、事業者が定型約款を利用して消費者と契約を締結する場合を想定し、定型約款に記載してはならない内容を、以下のとおり定めている。

<p>(i) 右記の事業者の責任・義務の軽減又は免除に関する内容の記載の禁止</p>	<ul style="list-style-type: none"> • 事業者が消費者に人身損害をもたらした場合に法に基づき負うべき責任 • 事業者の故意又は重過失により消費者に財産の損害をもたらした場合に法に基づき負うべき責任 • 提供する商品又はサービスについて、事業者が法に基づき負うべき修理、再製作、交換、返品、数量の補充、代金、サービス費用の返金等をする責任 • 事業者が法に基づき負うべき違約責任 • 事業者が契約の性質及び目的に応じて履行すべき協力、通知、秘密保持等の義務 • その他の事業者自らの責任
<p>(ii) 右記の消費者の権利の排除又は制限に関する内容の記載の禁止</p>	<ul style="list-style-type: none"> • 法定の金額又は合理的な金額を超える違約金又は損害賠償金を消費者に負担させる内容 • 法に基づき事業者が負うべき経営リスクを消費者に負わせる内容 • 法に基づき商品又はサービスを自主的に選ぶ消費者の権利を排除し、又は制限する内容 • 法に基づき契約を変更し、又は解除する消費者の権利を排除し、又は制限する内容 • 法に基づき違約金又は損害賠償金を請求する消費者の権利を排除し、又は制限する内容 • 法に基づき苦情、通報、調解の申立て、仲裁の申立て又は提訴をする消費者の権利を排除し、又は制限する内容 • 事業者のみが(契約条項の)解釈権又は最終的な解釈権を有する内容 • その他の消費者の責任を加重し、又は消費者の権利を排除し、若しくは制限する内容

これらの内容は基本的に旧弁法の内容を踏襲しているが、旧弁法では事業者の責任を「免除」する内容、消費者の権利を「排除」する内容が禁止されているのに対し、新弁法では上記内容に加え、事業者の責任を「軽減」する内容、消費者の権利を「制限」する内容も禁止され、定型約款内容に対する規制の範囲が拡大されたといえる。

(3) 罰則の強化

旧弁法によれば、上記規制に違反した場合、警告、違法所得 3 倍以下の過料(最大 3 万円。違法所得がない場合は最大 1 万円)を課すことができるとされている。これに対し、新弁法では、是正命令、警告、(違法所得の有無にかかわらず)最大 10 万円の過料を科すことができると定められており、過料の上限の大幅な引き上げが注目に値する。

本弁法は、あくまで事業者が消費者等と不平等な契約を締結することを防止するために制定した部門規則であり、事業者と消費者等との間の契約の効力に影響を及ぼすことはないと思われる。他方、消費者等との訴訟などにおいて、上記の規制に違反する事実(例えば、消費者に過大な違約金を負わせる内容の定型約款への記載)が認定された場合、消費者等に対する民事責任(上記の例であれば、消費者権益保護法により違約金に関する定型約款のうち「過大」分が無効と認定され、その結果事業者が負うこととなる、消費者から支払われた違約金のうち「過大な」部分の消費者への返還義務)のほか、本弁法に基づいて過料が科される余地も皆無ではないと考えられる。定型約款に関する内容規制の範囲が拡大されるなどの新しい動向に鑑み、本弁法の

運用に引き続き注目されたい。

3. 個人情報越境移転標準契約届出ガイドライン(第一版)⁸

国家インターネット情報弁公室、2023年5月30日公布、同日施行、部門政策文書

「個人情報保護法」38条1項によれば、個人情報取扱者が業務等の必要性により個人情報を中国国外に提供する必要が確実にある場合には、次のいずれか一つの条件を具備しなければならないとされている。

- 国家インターネット情報弁公室(以下「CAC」という。)が組織する安全評価に合格すること。
- 専門機構が行う個人情報保護認証を経ること。
- CAC の制定する標準契約(以下「標準契約」という。)に従い、中国国外受領者と契約を締結し、双方の権利・義務を約定すること。
- 法律・行政法規又はCACの定めるその他の条件

標準契約について、CACは、2023年2月22日に「個人情報越境移転標準契約弁法」⁹(同年6月1日に施行。以下「標準契約弁法」という。)及び標準契約のフォーマットを公布し、締結済みの標準契約の当局(所在地の省レベルのインターネット情報部門)への届出を義務付けている。これに合わせて、CACは、届出手続に関する細則として、同年5月30日に「個人情報越境移転標準契約届出ガイドライン(第一版)」(以下、本項において「本ガイドライン」という。)を公布した。

本ガイドラインでは、締結済みの標準契約の届出の方法、プロセス、届出の際の提出書類及び問合せ先が規定されており、かつ、「個人情報保護影響評価報告書」(以下「PIA 報告書」という。)等の提出書類のフォーマットも公開された。本ガイドラインの主なポイントは、以下のとおりである。

(1) 適用範囲

まず、「データ越境移転行為」の判断基準について、本ガイドラインは、標準契約弁法4条を引用し、以下のとおり、標準契約の適用範囲を改めて明確にした。

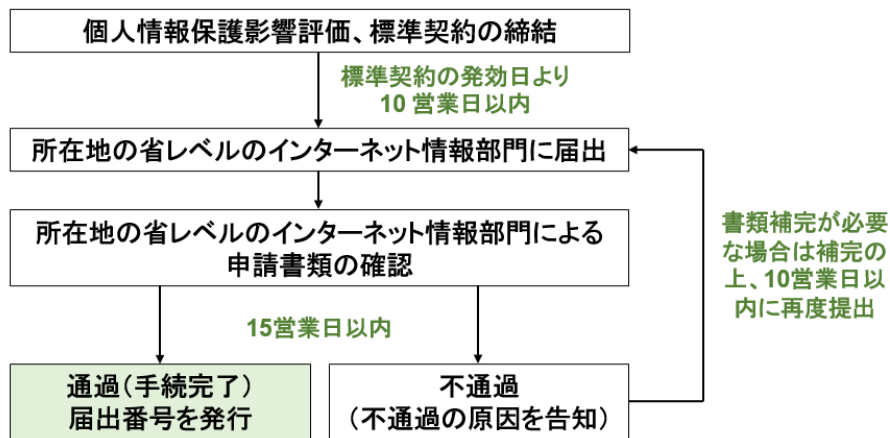
- ① 非重要情報インフラ運営者であること。
- ② 取り扱う個人情報が100万人分未満であること。
- ③ 前年1月1日以降に国外に提供した個人情報の累計が10万人分未満であること。
- ④ 前年1月1日以降に国外に提供したセンシティブ個人情報の累計が1万人分未満であること。

⁸ 中国語: 个人信息出境标准合同备案指南(第一版)

⁹ 標準契約弁法の詳細については、弊所HP掲載の「[中国最新法令・政策動向速報\(2023年3月16日号\)](#)」を参照されたい。

(2) 届出の方法及びプロセス

届出の方法及びプロセスについては、標準契約弁法の規定を基に以下のとおりより詳しく規定された。



本ガイドラインでは、届出を行った結果として、「通過(合格)」と「不通過(不合格)」の2つが定められているが、届出が「不通過」の場合に個人情報の越境移転にどのような影響を及ぼすかについて明文規定が設けられておらず、その意味では不明確な点が残っており、関連法令や実務における明確化が待たれるところではある¹⁰。一方、標準契約弁法 11 条が「省レベル以上のインターネット情報部門は、個人情報の越境移転活動に比較的大きな危険性が存在し、又は個人情報セキュリティインシデントが発生したことを発見した場合、個人情報取扱者に対して法律に基づき対面指導を行うことができる。個人情報処理者は、当局の要求に従い是正し、潜在リスクを除去しなければならない。」と定めていることから、届出を行った結果「不通過」と判断されると共に、「個人情報の越境移転活動に比較的大きな危険性が存在する」と判断され、個人情報処理者は潜在リスクを除去するために当局の要求に従って是正を行うことになった場合には、かかる是正の完了までに更なる個人情報の越境移転の実施は実質的に何かしらの制限を受けることになると思われる。

また、届出が完了した後も、標準契約の契約期限内に個人情報の権益に影響を及ぼすおそれのある事由が発生した場面については、本ガイドラインは、標準契約弁法 8 条に呼応して、個人情報保護影響評価(以下「PIA」という。)の再実施、標準契約の補充・再締結及び補充・再締結後の標準契約の届出手続を定めている。

(3) 届出書類

標準契約弁法における届出書類に関する規定に比べ、本ガイドラインの本文及びその別紙においては、届出書類の種類(下記)や要件についてより詳細に規定されており、かつ、下記のとおり一部の届出書類につきフォーマットが別紙として同時に公開されている。

- ① 統一社会信用コード証明書
- ② 法定代表者の身分証明書
- ③ 手続担当者の身分証明書
- ④ 手続担当者の委託書(フォーマットあり)
- ⑤ 承諾書(フォーマットあり)(以下「本承諾書」という。)
- ⑥ 標準契約(フォーマットあり。なお、標準契約弁法公布時に公開されている内容と同じ。)
- ⑦ PIA 報告書(フォーマットあり)

¹⁰ 標準契約弁法 6 条によれば、個人情報の越境移転は標準契約の発効後に行えんとされており、また標準契約の届出を越境移転の前提要件とする条文も不見当のため、届出の未了は、個人情報の越境移転の実施を必然的に制限できる理由とはならないと思われる。

(4) PIAの実施

標準契約弁法 5 条によれば、標準契約の締結を通じて個人情報の越境移転を行う場合、PIA を実施しなければならないとされている。この点に対し、標準契約弁法には PIA の実施時期に関する規定がなかったが、本承諾書によれば、PIA を標準契約の届出日前の 3 か月以内に完成させた旨の承諾をすることが要求されている。

また、今回公開された PIA 報告書のフォーマットの内容構成は、データ越境移転安全評価の申告において求められる「データ越境移転リスク自己評価報告書」とほぼ共通しており、いずれも下記の構成となっている。

- ① 評価作業の概要
- ② 越境移転活動の全体状況
- ③ 予定される越境移転活動に対する影響評価の状況
- ④ 越境移転活動に対する影響評価の結論

もっとも、PIA 報告書では、上記②については、「法的文書におけるデータセキュリティ保護責任義務に関する合意状況」という項目がなくなり、また、上記③については、「中国国外受領者と締結予定のデータ越境の関連契約又はその他法律効果のある文書等にデータセキュリティ保護責任義務が十分に規定されているか」という項目が「中国国外受領者が所在する国/地域の個人情報保護に関する政策・法規が標準契約の履行に及ぼす影響」に置き換わっていることが、大きな相違点として挙げられる。かかる相違点は、標準契約を締結することが今回公開された PIA 報告書の前提となっていることに由来するものと考えられる。

標準契約弁法においては、同弁法施行前に行われた個人情報越境移転活動が同弁法に適合しない場合には、同弁法の施行日から起算して 6 か月の是正期間(2023 年 11 月 30 日まで)が設けられている。しかしながら、今回公開された PIA 報告書のフォーマットの内容構成からすれば、PIA はデータ越境移転リスク自己評価の粒度とさほど変わらないように思われ、時間を要することが予想される。上記の 6 か月の是正期間に間に合わせるためには、早急な対応が求められる。

なお、全国レベルで適用される本ガイドラインとは別に、地方レベルで適用される関連ガイドラインや通知も公布されており、例えば、北京では「北京市個人情報越境移転標準契約届出ガイドライン」が、上海では「上海インターネット弁公室の情報個人情報越境移転標準契約届出に関する通知」がそれぞれ公布されている。

4. サイバーセキュリティ標準実践ガイドライン—ネットワークデータセキュリティリスク評価実施ガイドライン¹¹

全国情報安全標準化技術委員会秘書処、2023 年 5 月 26 日公布、同日施行、業種規範性文書

「データセキュリティ法」¹²30 条によれば、重要データの取扱者は、規定に従いそのデータ取扱行為につき定期的にリスク評価を実施し、かつ、関連主管部門にリスク評価報告書を提出しなければならないとされている。今回、全国情報安全標準化技術委員会¹³秘書処は、ネットワークデータセキュリティリスク評価(すなわち、ネットワークデータ¹⁴及びデータ取扱活動¹⁵のセキュリティに対して行うリスク識別、リスク分析及びリスク評価の全過程である。以下「リスク評価」という。)作業の展開を指導する文書として、「サイバーセキュリティ法」、データセキュリティ法及び「個人情報保護法」等の法令に基づき、また、データセキュリティに関する国家標準を参照して、「サイバーセキュリティ標準実践ガイドライン—ネットワークデータセキュリティリスク評価実施ガイドライン」(以下、本項において「本ガイドライン」という。)を制定し、公布した。

¹¹ 中国語: 网络安全标准实践指南—网络数据安全风险评估实施指引

¹² 中国語: 数据安全法

¹³ 全国情報安全標準化技術委員会は、国家標準化管理委員会が設立の承認・指導をし、かつ、業務上は、中央サイバーセキュリティ及び情報化委員会弁公室の指導を受け、情報安全標準化の技術業務に従事している組織である。

¹⁴ ネットワークを通じて処理し、又は生成された各種の電子データ

¹⁵ データの収集、保存、使用、加工、伝送、提供、公開、削除等の活動

(1) 本ガイドラインの概要及び位置づけ

本ガイドラインは、評価対象者の基本情報、データセキュリティ管理、データ取扱活動のセキュリティ、データセキュリティ技術、個人情報保護等の観点からリスク評価を実施すべきとの姿勢を示しつつ、リスク評価の考え方、リスク評価の内容及びリスク評価のプロセスを明らかにした。また、別紙には、「典型的なデータセキュリティリスク分類」及び「評価報告書フォーマット」が添付されている。

本ガイドラインは、データ取扱者、第三者機関によるデータセキュリティ評価の実施における指針、関連主管部門による検査評価における参照規定と位置付けられており、また、本ガイドラインに従った評価の実施により蓄積されたノウハウは関連する国家標準の制定のための参考になると見込まれている。

(2) リスク評価の考え方

リスク評価は、ネットワークデータセキュリティリスクの予防に資するものであり、その目的はデータ安全の全体像を掴むと同時に、データ安全リスクを洗い出し、脆弱性の所在に応じてデータ安全対策を強化することにある。したがって、リスク評価の考え方として、まず、情報収集を通じてデータ取扱者、業務及び情報システム、データ資産、データ取扱活動、安全防護措置等の関連要素を識別し、その後、データセキュリティ管理、データ取扱活動、データセキュリティ技術、個人情報保護等の観点からリスク・潜在的な危険を識別し、最後に問題点のリストアップ、データセキュリティに関するリスク分析、状況に応じてリスクに対する評価を行ったうえで、是正案を提示すると整理されている。

(3) リスク評価の内容

リスク評価は、評価対象者の事業内容やデータ資産及びデータ取扱活動の実態を把握の上、データセキュリティ管理、データ取扱活動のセキュリティ、データセキュリティ技術及び個人情報保護等について展開することとなっている。その具体的な内容は下記のとおりである。

<p style="text-align: center;">基本情報</p> <ul style="list-style-type: none"> データ取扱者の基本情報 事業内容と情報システム データ資産 データ取扱活動 安全保護措置 	<p style="text-align: center;">データセキュリティ管理</p> <ul style="list-style-type: none"> 制度整備 管理組織 分類・分級管理 人員管理 アウトソーシング管理 脆弱性・緊急時対策 メンテナンス クラウド 	<p style="text-align: center;">データ取扱活動のセキュリティ</p> <ul style="list-style-type: none"> データ収集 データ保存 データ転送 データの使用・加工 データの提供 データの公開 データの削除
<p style="text-align: center;">データセキュリティ技術</p> <ul style="list-style-type: none"> サイバーセキュリティ保護 身分認証とアクセス管理 モニタリング データマスキング データの漏洩防止 ポートの安全対策 バックアップ データセキュリティの内部統制 	<p style="text-align: center;">個人情報保護</p> <ul style="list-style-type: none"> 基本原則の遵守状況 個人情報主体への告知状況 個人情報主体による同意の取得状況 個人情報の保護義務の履行状況 個人情報主体による権利行使への対処 苦情処理 個人情報の取扱 センシティブ個人情報の保護 大型プラットフォーム特則 	

(4) リスク評価のプロセス

リスク評価のプロセスには、主に、リスク評価の準備、情報収集、リスク識別、総合分析、リスク評価のまとめの5つの段階が含まれている。本ガイドラインでは、リスク評価のプロセス図のみならず、検査評価のプロセス図及び自己評価のプロセス図も示されている。自己評価のプロセス図は、以下のとおりである。

①リスク評価の準備	<ul style="list-style-type: none"> •目標の確定 •範囲の確定 •チームの設立 •事前準備 •評価プランの作成
②情報収集	<ul style="list-style-type: none"> •データ取扱者 •業務及び情報システム •データ資産 •データ取扱活動 •安全防護措置
③リスク識別	<ul style="list-style-type: none"> •データセキュリティ管理 •データ取扱活動 •データセキュリティ技術 •個人情報取扱
④総合分析	<ul style="list-style-type: none"> •問題点のリストアップ •セキュリティリスクの分析と評価 •対策の策定
⑤リスク評価のまとめ	<ul style="list-style-type: none"> •リスク評価報告書の作成 •セキュリティリスクの処置

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜に合ったトピックを解説したニュースレターを執筆し、随時発行しております。N&A ニュースレター購読をご希望の方は [N&A ニュースレター 配信申込・変更フォーム](#) よりお手続きをお願いいたします。

また、バックナンバーは[こちら](#)に掲載しておりますので、あわせてご覧ください。

本ニュースレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ法律事務所 広報室 [E-mail](#) 