

## 米国：懸念国による大量の機微個人データ及び米国政府関連データへのアクセスの防止に関する大統領令（EO14117）

独禁/通商・経済安全保障ニュースレター

2024年3月12日号

執筆者:

藤井 康次郎

[k.fujii@nishimura.com](mailto:k.fujii@nishimura.com)

室町 峻哉

[s.muromachi@nishimura.com](mailto:s.muromachi@nishimura.com)

桜田 雄紀

[y.sakurada@nishimura.com](mailto:y.sakurada@nishimura.com)

バイデン大統領は、2024年2月28日、「懸念国による米国市民の大量の機微個人データ及び米国政府関連データへのアクセスの防止に関する大統領令」（EO14117）（以下「本大統領令」という。）を発した<sup>1</sup>。

本大統領令は、米国市民の大量の機微な個人データや米国政府関連のデータに対する、中国等の懸念国（country of concerns）の政府によるアクセスが、米国の国家安全保障に容認できないリスクをもたらす場合に制限を行うとの大方針を示すとともに、懸念国が支配する企業やその従業員、請負業者等による、米国市民の大量の機微な個人データ及び米国政府関連のデータに対するアクセスに繋がる可能性のある一定の取引を禁止又は制限する新たな規則案の策定を司法長官に指示等するものである。

本ニュースレターでは、本大統領令の概要を解説するとともに、日本企業への影響や示唆についても解説する。なお、別途の記載がない限り、本ニュースレターでの条文番号は本大統領令の条文番号を意味する。

### 1. 本大統領令の経緯

2019年5月、トランプ大統領（当時）は、「情報通信技術・サービスサプライチェーンの保護に関する大統領令」（EO13873）を発した<sup>2</sup>。EO13873は、外国敵対者（foreign adversaries）によるサイバー攻撃とリスクが増大していること、また、外国敵対者が支配等する者の情報通信技術・サービス（以下「ICTS」という。）の使用が米国国家安全保障上の脅威になることを指摘した上で、商務長官に対し、米国の国家安全保障又は米国人の安全に対して許容できないリスクをもたらすような外国敵対者が支配等する者のICTSの取引を禁止するための規則案を発表するよう指示するものである。そして、EO13873を受けて、「ICTSサプライチェーン規則」（15 CFR part 7）が制定され、外国の敵対者が支配等する者が供したICTSに関する審査手続が創設された<sup>3</sup>。また、トランプ大統領は、こうしたルール作りに留まらず、米国の安全保障に一定のリスクをもたらし得ることを理由に、TikTokやWeChatといった中国系のアプリを個別に指定して、その取引を禁止する大統領令（EO13942、EO13943、EO13971）を発した。

<sup>1</sup> [Federal Register, "Executive Order 14117 of February 28, 2024: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern", 1 March 2024.](#)

<sup>2</sup> [Federal Register, "Executive Order 13873 of May 15, 2019: Securing the Information and Communications Technology and Services Supply Chain", 17 May 2019.](#)

<sup>3</sup> [Federal Register, "Securing the Information and Communications Technology and Services Supply Chain", 19 January 2021.](#)

その後のバイデン政権下でも、基本的にこの方向性は維持された。すなわち、バイデン大統領は、2021年6月に、新たに「米国民の機微情報の外国敵対者からの保護に関する大統領令」(EO14034)を発した<sup>4</sup>。EO14034は、TikTokやWeChatといった中国系のアプリを個別に指定して禁止した各大統領令(EO13942、EO13943、EO13971)については取り消した上で、新たに「基準ベースの判断枠組みと厳格かつ証拠に基づく分析」(criteria-based decision framework and rigorous, evidence-based analysis)を導入することを商務長官に対して指示するものがあるが、トランプ政権下で発せられたEO13873を基本的に継承し、EO13873で宣言された国家緊急事態に対処するための取組を継続するものである。その後、EO14034を受けて、2023年6月にICTSサプライチェーン規則を改正する最終規則が公表され、同年7月、施行された<sup>5</sup>。

以上のほかにも、トランプ政権及びバイデン政権においては、政府調達規制や電気通信分野における免許審査、対内投資審査等の様々な規制上の手段を用いて、懸念国(主に中国が念頭に置かれている。)政府による米国民の機微個人データへのアクセス、情報通信機器・ソフトウェアを介した情報収集・影響力行使等への懸念に対する対抗が講じられてきた<sup>6</sup>。本大統領令は、EO13873において宣言され、EO14034において追加的措置が講じられた国家緊急事態の範囲を拡大するものとされており、こうした一連の対抗手段の中に位置付けられ得るものである<sup>7</sup>。

## 2. 本大統領令の概要

以下では、本大統領令の基本方針(第1項)と用いられている各用語の定義(第7項)を説明した上で、本大統領令が定める取引の禁止及び制限(第2項)、並びに機微個人データの保護措置(第3項)について、内容を整理する。

### (1) 基本方針(第1項)

本大統領令は、米国民の大量の機微個人データ(American's bulk sensitive personal data)や米国政府関連データ(United States Government-related data)にアクセスしようとする懸念国(countries of concern)に関して、以下の問題点を指摘し、そのようなアクセスが米国の国家安全保障に対して容認できないリスクをもたらす場合、これを制限することは米国の方針であるとしている。

- 懸念国政府は、機微個人データに関する民主主義国の慣行やOECDの「信頼性のあるガバメントアクセ

<sup>4</sup> [Federal Register, "Executive Order 14034 of June 9, 2021: Protecting Americans' Sensitive Data From Foreign Adversaries", 11 June 2021.](#)

<sup>5</sup> [Federal Register, "Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications", 16 June 2023.](#)

<sup>6</sup> 関連する最近の対内投資審査や政府調達規制における動向については、当事務所のニューズレター[2022年9月22日号](#)や[2024年2月28日号](#)等をご参照いただきたい。

<sup>7</sup> なお、バイデン大統領は、2024年2月29日に、EO13873に基づき懸念国のコネクテッドカーがもたらす国家安全保障上のリスクを調査するとともに、これに対処することを指示したことを[公表した](#)。これを受け、商務省産業安全保障局は"Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles"と題するAdvance Notice of Proposed Rulemakingを[発表し](#)、規制の対象とすべきコネクテッドカーの定義や懸念国のコネクテッドカーがもたらすリスク、導入すべき措置等についてのコメントの募集を開始した(期限: 2024年4月30日)。

スに関する高次原則に係る閣僚宣言」(以下「OECD ガバメントアクセス宣言」という。)<sup>8</sup>に反映されている原則とは対照的に、民主主義の価値観、プライバシーの保護、その他の人権や自由に反する方法で、機微個人データにアクセスし、利用しようとしている可能性がある。そのため、懸念国に米国市民の機微個人データや米国政府関連データを無制限に転送することは、懸念国政府が様々な悪意のある目的<sup>9</sup>のために、それらのデータを悪用することを可能にする可能性がある。

- 懸念国が所有する企業や懸念国によって支配等される者は、懸念国政府が間接的に米国市民の大量の機微個人データや米国政府関連データにアクセスすることを可能にする可能性がある。例えば、懸念国のサイバー法や、国家安全保障法、諜報関連法が、十分な法的セーフガードなしに、そのような企業や者に対して、米国市民の機微個人データ及び米国政府関連データへのアクセス権を当該懸念国の諜報機関に提供する義務を負わせている可能性がある。
- 以上のようなリスクは、懸念国が大量の機微個人データを使用して AI 能力やアルゴリズムを開発し、その結果、米国の国家安全保障を損なうような、ますます洗練された効果的な方法で大規模なデータセットを使用できるようになることで、さらに悪化する可能性がある。

他方で、本大統領令は、米国が、国境を越えた、オープン、グローバル、相互運用可能、信頼可能、そして安全なデータの流通を引き続き支持し、米国が他国との間で有する重要な消費者、経済、科学及び貿易の関係を維持するとして、以下の点を確認している。

- 米国市民の大量の機微個人データ又は米国政府関連データを米国内に保管したり、これら进行处理するために使用されるコンピューティング施設を米国内に設置したりすることを求める、一般化されたデータローカライゼーション要件を課すことを許可するものではないこと。
- 米国人が懸念国に所在する又は懸念国に支配等される企業と商取引を行うこと(商品やサービスの販売の一環として金融その他のデータを交換することを含む。)を広範に禁止したり、米国が他国との間で有する重要な消費者、経済、科学及び貿易の関係の広範なデカップリングを目的とした措置を課したりするものではないこと。
- バイデン政権が、税金が投入された科学研究の成果の一般公開や、電子医療情報の共有と相互運用性、患者による自己のデータへのアクセスを拡大することを公約してきたこと。

## (2) 定義 (第 7 項)

本大統領令において、「大量の機微個人データ」(bulk sensitive personal data) や「米国政府関連データ」(United States Government-related data)、「懸念国」(countries of concern)、「対象者」(covered persons)、「米国人」(United States person) の各用語は以下のとおり定義されている。

<sup>8</sup> OECD, “Declaration on Government Access to Personal Data Held by Private Sector Entities”, 14 December 2022. 同原則の内容及びその意義については、[西村高等法務研究所「CLOUD Act \(クラウド法\) 研究会報告書 Ver.2.0」\(2023年4月\)](#) 13頁等参照。

<sup>9</sup> 具体的には、悪意のあるサイバー活動や、脅迫やスパイ活動等の不正な目的のために政府職員等の米国の個人を追跡しプロフィールを構築すること、活動家やジャーナリスト等の情報を収集し、脅迫に用いる等、市民的自由を抑圧することなどが挙げられている。

用語	定義
機微個人データ	<p>対象個人識別子（covered personal identifiers）、地理位置情報及び関連センサーデータ、生体認証識別子、ヒューマンオーミックデータ、個人健康データ、個人財務データ、又はこれらの組み合わせたもの。ただし、以下のものは含まれない<sup>10</sup></p> <ul style="list-style-type: none"> <li>① 裁判記録やその他の政府記録等の公的な記録であり、合法的かつ一般的に利用可能なデータ</li> <li>② 国際緊急経済権限法 203 条(b)(1)の範囲内に含まれる個人的な通信</li> <li>③ 国際緊急経済権限法 203 条(b)(3)の情報又は情報資料（出版物等）</li> </ul>
大量の機微個人データ	第 2 項の規定に従い司法長官が発する規則（下記 <b>(3)</b> 参照）で指定される一定期間における閾値を超える量の機微個人データ
米国政府関連データ	<p>その量に関わらず、懸念国が米国の国家安全保障に害を及ぼすために悪用する危険性が高いと司法長官が判断する機微個人データであり、以下に該当するもの</p> <ul style="list-style-type: none"> <li>① 軍を含む連邦政府の現職員、元職員、元請負業者、又は元高官のカテゴリーに関連する又は関連付け可能であると取引当事者が特定するものとして、第 2 項の規定に従い司法長官が発する規則（下記<b>(3)</b>参照）に規定されるもの</li> <li>② 軍を含む連邦政府の現職員、元職員、請負業者、又は元高官を特定するために使用される可能性のあるデータのカテゴリーに関連するものとして、第 2 項の規定に従い司法長官が発する規則（下記<b>(3)</b>参照）に規定されるもの</li> <li>③ 軍を含む連邦政府によって管理される特定の機微性の高い場所（公に特定される）に関連する又は関連付け可能であるもの</li> </ul>
懸念国	米国の国家安全保障又は米国人の安全に著しく悪影響を及ぼす行為を長期にわたって繰り返し又は深刻な事例として行っており、米国の国家安全保障又は米国人の安全を害するために大量の機微個人データ又は米国政府関連データを悪用する重大なリスクをもたらす外国政府として、第 2 項の規定に従い司法長官が発する規則（下記 <b>(3)</b> 参照）において特定されるもの <sup>11</sup>
対象者	懸念国が支配等する企業、その従業員又は請負業者である外国人、懸念国の従業員又は請負業者である外国人、懸念国の領域内に主として居住する外国人、その他司法長官により指定された者 <sup>12</sup>

<sup>10</sup> ②及び③は、国際緊急経済権限法 203 条(b)（合衆国法典第 50 編第 35 章§1702(b)）によって、大統領による規制・禁止する権限から除外されている。

<sup>11</sup> ANPRM によれば、司法省は、「懸念国」の範囲を ICTS サプライチェーン規則における「外国敵対者」（foreign adversaries）と同じく、①中国、②キューバ、③イラン、④北朝鮮、⑤ロシア及び⑥ベネズエラとすることを想定しているとのことである（ANPRM III.E）。

<sup>12</sup> ANPRM によれば、司法省は、「対象者」を具体的に以下のように定義する想定であるとのことである。

米国人	米国民・国民・合法的永住者、合衆国法典第 8 編 1157 条に基づき難民として米国に入国を認められた個人、合衆国法典第 8 編第 1158 条に基づき亡命を認められた個人、米国法若しくは米国内の管轄権に基づいてのみ組織された企業（外国支社を含む）、又は米国内の個人
-----	---

### (3) 取引の禁止及び制限（第 2 項）

本大統領令は、司法長官が、国土安全保障長官と連携し、関係省庁の長と協議の上で、米国人が、外国又はその国民が何らかの利害関係を有する財産を取得、保有、移転、輸送、輸出又は取り扱う取引で、以下の要件を全て満たすものに従事することを禁止又は制限する規則を発しなければならないとする。そして、かかる要件を満たす規則案を本大統領令の日付から 180 日以内に公表しなければならないとする。

- ① 大量の機微個人データ又は米国政府関連データを伴う
- ② 懸念国又は対象者が大量の機微個人データ又は米国政府関連データにアクセスすることを可能にする可能性があるため、米国の国家安全保障に許容できないリスクをもたらすものとして規則において司法長官が判断した取引の類型に該当する
- ③ 規則の効力発生日以降に、開始されるか、完了前であるか、完了する
- ④ 規則に定める例外に該当せず、規則に従って与えられるライセンスによって許可されていない
- ⑤ 銀行業務、資本市場業務、金融保険業務を含む金融サービスの提供に通常付随し、その一部を構成するものではなく、連邦の法令若しくは規制要件を遵守するために必要とされるものでもないこと

上記②に関して、司法省が公表した Advance Notice of Proposed Rulemaking（以下「ANPRM」という。）<sup>13</sup>によれば、司法省は、米国の国家安全保障に許容できないリスクをもたらす取引の類型を「**対象データ取引**」（covered data transactions）として、以下の 4 つを想定しているとのことである<sup>14</sup>。また、上記③に関し、本大統領令に基づく禁止事項は、規制の発効日前に締結された契約又は付与された免許若しくは許可に関わらず、適用されることとされている<sup>15</sup>。

- (1) 懸念国によって直接又は間接的に 50%以上所有されている企業、懸念国の法律に基づいて組織若しくは設立された事業体、又は懸念国に主たる事業所を有する企業
- (2) (1)に該当する企業又は(3)、(4)若しくは(5)に該当する人物が、直接的又は間接的に 50%以上を所有する企業
- (3) 懸念国又は(1)、(2)若しくは(5)に該当する企業の従業員又は請負業者である外国人
- (4) 懸念国の領域内に主として居住する外国人
- (5) 懸念国若しくは対象者によって支配等されている者又は意図的に規則に違反する若しくは違反の指示をする者として司法長官が指定した者

<sup>13</sup> [Federal Register, "National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern", 5 March 2024.](#)

<sup>14</sup> ANPRM III.D. これら 4 つのタイプのそれぞれについて、具体例が挙げられている。

<sup>15</sup> 本大統領令第 2 項(h)。

類型	定義
データ仲介 (data brokage)	個人（提供者）から他の個人（受領者）へのデータの転送を伴うデータの販売やアクセス権の許諾等の取引で、受領者が当該データに関連する又は関連付け可能である個人から直接データを収集・処理していない場合
ベンダー契約 (vendor agreement)	雇用契約以外の契約又は取り決めであって、支払いその他の対価と引き換えに、物品又はサービス（クラウドコンピューティングサービスを含む）を他者に提供するもの
雇用契約 (employment agreement)	独立請負業者以外の個人が、支払いその他の対価と引き換えに、他人のために直接仕事を行う又は職務を遂行する旨の契約又は取り決め（取締役会又は委員会での雇用や幹部レベルの取り決め又はサービス、運用レベルでの雇用サービスを含む）
投資契約 (investment agreement)	米国内の不動産又は米国人に対する直接又は間接の所有権や権利を支払いその他の対価と引き換えに取得する契約又は取り決め

そして、ANPRM によれば、司法省は、対象データ取引に関して、米国人に対する以下の禁止事項を設けることを検討しているとのことである<sup>16</sup>。

- (i) 懸念国又は対象者との間で、故意に (knowingly) 対象データ取引を行うこと
- (ii) 相手方に対して当該データに関する懸念国又は対象者との対象データ取引を行わないことを契約上要求せずに、外国人 (foreign person) との間で故意に対象データ取引を行うこと
- (iii) 懸念国又は対象者との間で、故意に、当該懸念国又は対象者にヒトゲノムデータで構成される大量の米国機微個人データ又はそのようなデータが導き出されるヒト生体試料へのアクセスを提供する対象データ取引（直近 12 ヶ月以内に単一又は複数の取引によって「大量の」の閾値を超えるような場合）を行うこと
- (iv) 禁止事項を回避すること、違反を引き起こすこと (causing violations)、違反を試みること及び違反するため共謀すること
- (v) 米国人が行った場合には禁止される対象データ取引を、故意に指示すること。ここでいう「指示」とは、米国人が（個人又はグループの一員として）外国企業を代表して意思決定を行う権限を有する場合に、当該権限を行使して、米国人が行った場合には禁止される取引を命令、決定、又は承認することをいう

また、本大統領令では、国土安全保障長官は、サイバーセキュリティ・インフラセキュリティ庁 (CISA) 長官を通じて、司法長官と連携し、関連機関の長と協議して、司法長官が特定した、制限された取引 (restricted transaction)<sup>17</sup>によってもたらされる許容できないリスクに対処するセキュリティ要件を提案し、パブリックコメントを求め、公表することとされている。そして、かかるセキュリティ要件は、米国国立標準技術研究所 (NIST) によって開発されたサイバーセキュリティ及びプライバシーフレームワークに基

<sup>16</sup> ANPRM III.G.

<sup>17</sup> ANPRM によれば、対象データ取引の中でも、ベンダー契約、雇用契約及び投資契約が想定されているようである (ANPRM III.I)。

づくこととされている<sup>18</sup>。ANPRM によれば、制限された取引については、上記セキュリティ要件を満たさない限り禁止されるという枠組みが想定されているとのことである<sup>19</sup>。

#### (4) 機微個人データの保護措置（第3項）

本大統領令では、機微個人データを保護するため、司法長官が新たに定める新規則（上記(3)参照）による一定の取引の禁止及び制限のほか、以下の関係政府機関が、それぞれ以下のことを行わなければならないとされている。

関係政府機関	取り組み
米国電気通信役務部門への外国参入査定委員会（通称 Team Telecom） <sup>20</sup>	<ul style="list-style-type: none"> <li>● 懸念国が支配等する者が所有若しくは運営する海底ケーブルシステム、又は懸念国の管轄内で終端する海底ケーブルシステムの既存ライセンスの審査開始を優先する。</li> <li>● 懸念国によるデータへのアクセスに関する第三者リスクの評価を含む、ライセンス申請及び既存ライセンスの審査に関するガイダンスを発行する。</li> <li>● 海底ケーブルシステムの審査に関して、懸念国による大量の機微個人データへのアクセスに関連する国家安全保障・法執行上のリスクに継続的に対処する。</li> </ul>
国防長官、保健福祉長官、退役軍人長官及び国立科学財団長官	<ul style="list-style-type: none"> <li>● 個人健康データ及びヒトゲノムデータを含む米国市民の大量の機微個人データへの懸念国又は対象者によるアクセスを可能にする援助の提供を禁止し、又はそのような援助に対する緩和措置を課すため、一定の措置を講じる。</li> </ul>
金融消費者保護局（CFPB）局長	<ul style="list-style-type: none"> <li>● 2023年9月に「消費者報告ルールメイキングに関する中小企業検討会パネル」で提案した規則<sup>21</sup>の制定に向けた取り組みの継続を含め、データブローカー業界の事業者が懸念国及び対象者による大量の機微個人データ及び米国政府関連データへのアクセスによる懸念を助長するとのリスクに対応するための措置を講じることを検討するよう努める<sup>22</sup>。</li> </ul>

<sup>18</sup> 本大統領令第2項(d)。

<sup>19</sup> ANPRM III.I。

<sup>20</sup> Team Telecom は、元々は非公式な省庁間グループとして連邦通信委員会（FCC）による電気通信免許審査手続に関与していたが、2020年4月にトランプ大統領が発したEO13913によって、「米国電気通信役務部門への外国参入査定委員会」（Committee for the Assessment of Foreign Participation in the United States Telecommunications Service Sector）として正式なものとなった。最近では、Google及びMetaによる海底ケーブルシステムプロジェクトであるPacific Light Cable Network（PLCN）の審査に関与したことが注目された。

<sup>21</sup> [CDPB, "Small Business Review Panel for Consumer Reporting Rulemaking"](#)。

<sup>22</sup> 本大統領令を受け、CFPB局長のRohit Chopra氏は、今年中に新たな規則を制定する予定であるとコメントした（[CFPB, "CFPB Director Rohit Chopra Releases a Statement in Response to President Biden's Executive Order To Protect Americans' Sensitive Personal Data", 28 February 2024.](#)）。

### 3. 日本企業への影響・示唆

本大統領令は、中国等の懸念国政府による米国市民の機微個人データに対するアクセスに対して対抗措置を導入しようとするものである。本大統領令第 2 項は、懸念国に対して大量の機微個人データ又は米国政府関連データへのアクセスを与えるような米国人による一定の取引を禁止又は制限する規則を制定することとしているところ、ANPRM に記載された司法省の想定を前提とすると、日本企業に対しても相当程度の影響が及ぶ可能性がある。

まず、本大統領令によれば、規制の対象となる「米国人」には、米国法に基づき設立された企業が含まれることから、日本企業の米国支社による「対象データ取引」は、規制の対象となると考えられる。加えて ANPRM によれば、自らが「米国人」や「対象者」に該当しなかったとしても、米国人が対象データ取引の意思決定に関与するような場合には適用対象となり得る（上記 **2(3)**の(v)参照）。

また、ANPRM によれば、日本企業が米国人と対象データ取引を行う場合、当該対象データ取引により取得したデータについて懸念国や対象者との間で対象データ取引を行わないことについて契約上約束することが求められ、これに従わない限り取引を行うことができなくなる可能性がある（上記 **2(3)**の(ii)参照）。そして、本大統領令に基づく禁止事項は、本大統領に基づく規則の発効より前に「対象データ取引」に関する契約が締結されている場合であっても適用され得ること<sup>23</sup>からすると、日本企業の事業活動において新たな規則の適用可能性について、今後又は過去の契約に遡ってレビューが必要となるなど、検討が必要となる可能性は相当程度あるように思われる。

更に、「対象データ取引」の範囲について、ANPRM によれば、データ仲介のようなデータの転送それ自体を目的とする取引のみならず、ベンダー契約、雇用契約及び投資契約といった、データの転送に繋がる可能性のある関係性を創出するような取引も含めることが想定されているようであることから、想定以上に広範な影響が生じる可能性がある。

ANPRM はあくまで現時点での司法省の検討している規則の方向性を記載したものにすぎず、今後、パブリックコメントなどの手続を経て、規則の内容が確定していくことから、今後の動向を注視していくことが重要である。また、大統領令や ANPRM の内容から、事業に対する影響が大きいと予想される日本企業については、司法省に対してコメントを提出することも選択肢になり得るだろう（期限は 2024 年 4 月 19 日）<sup>24</sup>。

<sup>23</sup> 本大統領令第 2 項(h)参照。

<sup>24</sup> その際には、日本は米国と同様に OECD ガバメントアクセス宣言の採択に加わっており、ガバメントアクセスに対する規律について理念を共有する有志国であること、また、情報の電子的手段による国境を超える移転に関する規定を含む[デジタル貿易に関する協定](#)が締結されていることなどを指摘し、日米間のデータ流通は原則として禁止又は制限されるべきではないといった観点からの主張を含めることも考えられる。



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かな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る必要がある場合があります。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 広報課 [newsletter@nishimura.com](mailto:newsletter@nishimura.com)