NISHIMURA & ASAHI

米国におけるプライバシー法制の潮流と最新動向

2023年7月13日（木）

西村あさひ法律事務所
フランクフルト・デュッセルドルフ事務所　共同代表
パートナー弁護士・NY州弁護士、CIPP/E　石川　智也

講師紹介

NISHIMURA & ASAHI

石川 智也
Noriya Ishikawa

フランクフルト＆デュッセルドルフ
事務所共同代表

Tel: +49-(0)69-257-298-801
E-mail: n.ishikawa@nishimura.com

西村あさひ法律事務所フランクフルト＆デュッセルドルフ事務所共同代表。欧州でのM&A・GDPR対応、サプライチェーンDD対応、グローバル内部通報の窓口、EU・加盟国レベルの規制法調査等、日系企業の欧州進出を幅広く支援している。各国のデータ保護法制に明るく、データの越境移転の問題への対処をはじめ、グローバルでのデータガバナンス構築のためのソリューションを提供。

登録

第一東京弁護士会（2006年登録）
ニューヨーク州（2017年登録）
Certified Information Privacy Professional/Europe（CIPP/E）

学歴

2005年　東京大学法学部第一類（LL.B.）
2015年　University of Virginia School of Law（LL.M.）
2016年　Munich Intellectual Property Law Center（LL.M.）

経歴

2019年 -　一般社団法人日本DPO協会　顧問
2020年 -　フランクフルト＆デュッセルドルフ事務所 共同代表
2022年 -　トヨタ自動車株式会社　プライバシーガバナンスに関するアドバイザリーボード委員

近時の主な論文・書籍

- 『2020年個人情報保護法改正と実務対応〔改訂版〕』（共著、商事法務、2022年）
- 「個人データの越境移転先国の法令・実務調査の重要性」、「個人データが漏えいした場合の対応比較」、「企業が押さえたい日米欧の最新法制と実務動向」（共著、ビジネス法務2021年10月号、中央経済社）
- 「連載・個人情報保護体制グローバル化の設計図」（共著、Business Law Journal 2020年7月号～2021年2月号）
- 「連載・個人情報保護法　世界の最新動向」（共著、ビジネス法務2020年1月号～2021年3月号）
- 「連載・実務上の疑問に答える　データ保護・利活用の要点」（共著、Business Law Journal 2019年8月号～2020年5月号）
- 『いますぐわかるCCPAの実務対応』（共著、中央経済社、2020年）
- 『個人情報保護法制大全』（共編著、商事法務、2020年）
- 「カリフォルニア州消費者プライバシー法（CCPA）対応のための重要ポイント」（NBL 2019年12月1日号）
- 「十分性認定後のEEA域内からの個人データの移転」（共著、Business Law Journal 2019年5月号）
- 『秘密保持契約の実務（第2版）』（共編著、中央経済社、2019年）
- 『M&A・企業組織再編のスキームと税務～M&Aを巡る戦略的税務プランニングの最先端～（第4版）』（共著、大蔵財務協会、2019年）
- 『M&A法大全（下）〔全訂版〕』（共著、商事法務、2019年）
- 「GDPR「地理的範囲についてのガイドライン」の概要と実務上注目すべきポイント」（共著、Business Law Journal 2019年3月号）
- 「GDPR対応の実務　対応の要否と優先順位の考え方」（共著、Business Law Journal 2018年4月号）

など多数

NISHIMURA
& ASAHI

米国のプライバシー法制の全体像

全体像

NISHIMURA & ASAHI

- 米国では、連邦レベルでの包括的なプライバシー法は存在しない
  - 2022年、連邦レベルでの個人情報保護法であるADPPA（案）の成立に向けた動きがあったが、成立に至らず
- 個別の分野に適用される主な法令として、以下の法令が存在（セクトラル方式）
  - 電子通信プライバシー法（Electronic Communication Privacy Act、ECPA）
  - グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act、GLBA
  - 医療保険の携行性と責任に関する法律（Health Insurance Portability and Accountability Act、HIPPA）
  - 児童オンラインプライバシー保護法（Children's Online Privacy Protection Act、COPPA）
- 州法レベル
  - 包括的なプライバシー法：カリフォルニア、バージニア、コロラド、コネチカット（施行済み）、ユタ、テキサス、モンタナ、アイオワ、テネシー、インディアナ（成立済み）
  - データ侵害の際の当局報告・本人通知に関する法律：全ての州
  - セクター別の各種法令：バイオメトリックデータ関連が要注意

連邦レベルでのプライバシー法の成立に向けて

NISHIMURA & ASAHI

- 2022年6月3日、米国の連邦レベルでのプライバシー法であるADPPA（American Data Privacy and Protection Act）案が公表され、7月に議会への提出が可決。もっとも、年末で会期が終了し、一旦廃案に

  ADPPA法案の概要(連載)

  https://www.nishimura.com/ja/knowledge/newsletters/20220906-88441

- 州法と連邦法の優先関係、民事の損害賠償請求の可否等をめぐって、意見がまとまらなかった
- 2023年に、Biden大統領が、Wall Street Journalに「Republicans and Democrats, Unite Against Big Tech Abuses, Congress can find common ground on the protection of privacy, competition and American children」という意見を公表し、引き続き連邦プライバシー法の制定に向けた意欲を示している
- 2023年に再度立法のプロセスが動き出すことは考えにくいが、州のプライバシー法が増えて実務を阻害するようになれば、再度機運が高まる可能性はある

Duty of Loyalty

NISHIMURA & ASAHI

- Duty of Loyalty：受託者は、自己の利益よりも、委託者の利益を優先させるべきという信託の概念
- 巨大IT企業による個人データの処理に際し、個人が脆弱な立場に置かれ、個人データ保護のための実効的な仕組みが十分に整備されていない
- データ主体の最善の利益と相反する形で個人データを処理したり、データ処理に利用するツールを設計したりしてはならないという考え方が、信託の文脈でのDuty of Loyaltyを足掛かりに提唱されている
- ADPPAには、「Duty of Loyalty」の編に、データ最小化、忠実義務、プライバシー・バイ・デザイン、価格設定に関する個人への忠誠が規定されていた
  - データ最小化：所定の目的のために合理的に必要かつ比例的である限度を超えた、対象データの収集、処理又は移転の禁止
  - 忠実義務：センシティブデータ等の一定の対象データについて、所定の処理を禁止
  - プライバシー・バイ・デザイン：対象データの収集、処理及び移転に関して、合理的なポリシー、慣行及び手続を導入し、履行・維持することを義務付け
  - 価格設定に関する個人への忠誠：ADPPAに基づく権利行使を理由に、製品・サービスの提供の拒否、異なる価格設定、異なる品質での提供等、個人の差別的取扱いを禁止

州レベルでの包括的なプライバシー法

NISHIMURA & ASAHI

- 州レベルでの包括的なプライバシー法の成立・施行の動向

州	施行日/施行予定
カリフォルニア	2020年1月1日施行（2023年1月1日に改正法が施行）
バージニア	2023年1月1日施行
コロラド	2023年7月1日施行
コネチカット	2023年7月1日施行
ユタ	2023年12月31日施行予定
テキサス	2024年7月1日施行予定
モンタナ	2024年10月1日施行予定
アイオワ	2025年1月1日施行予定
テネシー	2025年7月1日施行予定
インディアナ	2026年1月1日施行予定

米国（州レベル）の動向

NISHIMURA & ASAHI

- 州レベルでの法制への対応のコツ
  - GDPRとCCPAの内容理解が、州レベルの法制への対応に直結する（大体、どちらかに似たルールとなっている）
  - もっとも、ADPPAを参照するものも出始めており、今後は、GDPR、CCPA、ADPPAの理解が米国のプライバシー法を理解する上で重要となる
  - カリフォルニア州以外の州は、今のところ、法令自体はとてもシンプル
  - 開示（通知・プライバシーポリシー）、権利行使、データ処理契約がフォーカスされることが多い
  - **「適用スコープに含まれるか」は早期に解決する**

NISHIMURA & ASAHI

カリフォルニア州消費者保護法（CCPA）のポイント

カリフォルニア州消費者保護法（CCPA）（改正後）

NISHIMURA & ASAHI

- 2020年11月に、カリフォルニア州プライバシー権法（CPRA）が可決し、2023年1月1日から施行（一部を除く）
- CPRAは、2020年1月1日に施行されたカリフォルニア州消費者プライバシー法（CCPA）を大幅に改正
- 施行規則の最終改訂版は2023年2月3日に公表され、同年3月29日に確定・発効。但し、裁判所が施行開始から執行を1年延期させる旨の決定を出し、規則に基づく執行は2024年3月29日にずれ込む見通し
- サイバーセキュリティ監査・リスクアセスメント・自動化された意思決定に関する下位規則は、2023年3月にパブリックコメント手続が終了。7/14に公開でのヒヤリングを実施予定
- 従業員・B to Bコンタクト先であることを理由に義務が免除されることはなくなった
- センシティブデータに関する実体規制もあるため、書面作成にとどまらず、データ処理の内容を吟味する必要あり

CCPA（改正後）「個人情報」の範囲

NISHIMURA & ASAHI

- 特定の消費者若しくは世帯を識別し、これらに関連し、これらを記述し、これらと関連付けることが合理的に可能であり、又は、直接的若しくは間接的にこれらと合理的に関連付けられ得る情報（1798.140(v)(1)）
- 世帯を識別する情報も含まれている
- IPアドレス等のように、特定の個人を識別できなくても、端末レベルで識別できる場合には個人情報に該当
- 消費者＝カリフォルニア州の住民の個人情報のみが適用対象

CCPA（改正後）の適用範囲「事業者」該当性

NISHIMURA & ASAHI

【ステップ1】

① 消費者（=カリフォルニア州住民）の個人情報を取得し、単独又は他者と共同で、消費者の個人情報の処理の目的及び手段を決定している

② カリフォルニア州で事業を行っている

③ 以下の3つの事由のいずれかを充足する

- 1月1日時点で前年の年間売上高が2,500万米ドルを超える
- 単独又は組み合わせて、年間10万以上の消費者、世帯、又はデバイスに係る個人情報を購入し、営利目的で受領し、売却し、又は営利目的で共有している
- 年間売上高の50%以上を消費者の個人情報の売却又は共有から得ている

【ステップ2】

「事業者」を支配し、又は当該事業者により支配され、かつ、当該事業者と共通のブランドを有し、当該事業者が消費者の個人情報を共有する主体

CCPA（改正後）上の要対応事項

NISHIMURA & ASAHI

対応項目	個人情報の売却の有無にかかわらず必要となる対応	個人情報を売却している場合に追加で必要な対応
収集時の通知の提供	収集する個人情報の種類・利用目的を通知	Do not Sell My Personal Information のリンクを追記
オプトアウト通知の提供	―	（個人情報を売却している場合のみ）オプトアウト権に関する事項を通知
金銭的インセンティブ通知の提供	（金銭的インセンティブを提供している場合のみ）金銭的インセンティブに関する事項を通知	―
プライバシーポリシーの策定・開示	所定の事項のウェブサイト等への開示	個人情報の売却が存在する故の追加の開示事項あり
権利行使の受付方法の準備	最低2種類の開示請求・削除請求の受付方法の準備	・Do Not Sell My Personal Informationのリンクをトップページ等に設置 ・最低2種類のオプトアウト要求の受付方法の準備
データ処理契約の見直し	委託先等への個人データの提供が売却に当たらないことを明確にするために、契約に所定の条項を規定	―
CCPA遵守のためのマニュアル・社内規程	権利行使に関して周知するためのマニュアル・社内規程	売却のオプトアウトについても要周知
権利行使の記録	権利行使の内容とその対応について記録し、24ヶ月保存	売却のオプトアウトについても要記録
セキュリティ	適切かつ妥当なセキュリティ手続とプラクティスの実施・維持	―

NISHIMURA & ASAHI

生体データに関する規制

BIPA

NISHIMURA & ASAHI

- BIPA（Biometric Information Privacy Act）：イリノイ州の生体情報保護法で、データ主体に対し訴権を与えており、米国で最も厳格と言われている

- 適用対象データ
  - 「生体識別子」（Biometric identifier）及び「生体情報」（Biometric information）
    - 生体識別子：網膜又は虹彩のスキャン、指紋、声紋、又は手や顔の形状のスキャン
    - 生体情報：取得、変換、保管、共有の方法の如何を問わず、個人を識別するために使用される個人の生体識別子に基づくあらゆる情報

- 適用対象者
  - 「民間事業者」に対して適用。「民間事業者」とは、あらゆる個人、パートナーシップ、コーポレーション、LLC、協会、又はその他の組織された団体
  - イリノイ州において生体情報等を収集等してさえすれば、たとえイリノイ州外の企業であっても、BIPAの適用を受け得る

■ 義務・禁止事項

項目	概要
保持スケジュール及び破棄方針の作成及び公開(15条a号)	保持スケジュール及び破棄ガイドラインを書面で策定し、一般に公開する
事前手続によらない収集等の禁止(15条b号)	下記の手続を踏まなければ、生態情報等を収集等することはできない ①収集等の事実の通知 ②収集等の目的及び期間の通知 ③同意の受領
売買等による利益獲得の禁止(15条c号)	個人又は顧客の生体情報等を販売、リース、取引、その他の方法により利益を得ることはできない
生体データの開示禁止(15条d号)	原則として、生体情報等を開示、再開示又はその他の方法で拡散することはできない
保護措置の実施(15条e号)	業界内の合理的な注意水準で、機密情報の場合と同等以上の方法で、生体情報を保管、通信及び保護する

BIPA

■ 裁判の動向

- 既に多数のクラスアクションが提起されている（法定損害の規定もあり）
- イリノイ州外の企業への域外適用を認める判決が出ている
- イリノイ州最高裁判所は、個人の生体認証識別子や生体認証情報の収集又は開示の都度、個別の損害賠償請求権が発生するとの判断を示している

■ 留意すべきこと

- BIPAでは、高額の損害賠償請求がなされる可能性あり（過失によるBIPA違反は1,000米ドル又は実際の損害額のいずれか大きい額、故意による違反は、5,000米ドル又は実際の損害額のいずれか大きい額）
- 集団訴訟となると、損害賠償の請求額は甚大となり得、インパクトは大きい
- 生体情報を取得する場合は、可能な限り、取得する端末等でデータ処理を済ませ、中央のサーバー等に送らないように設計することが肝要

生体データに関する各州の規制

NISHIMURA & ASAHI

- 包括的プライバシー法における規制
  - カリフォルニア、コロラド、バージニア、コネチカット、ユタ等では、包括的なプライバシー法に生体データに関する規制が盛り込まれている
- 生体データに特化した州法
  - イリノイの他、テキサス、ワシントン（以上、施行済み）、マサチューセッツ（以上、成立済み）
  - 多数の州で法案が提出されている
  - BIPAに類似したものが多い

NISHIMURA
& ASAHI

サイバーセキュリティ対応の留意点

データ侵害の報告義務

NISHIMURA & ASAHI

- データ侵害に係る報告義務を定めた包括的な連邦法は存在しない
- 全州で、州法レベルでデータ侵害時の報告義務に係る法律を制定して対応
- ランサムウエア事案への対処
  - 身代金事案の考え方の違い
  - 当局報告の方向性（居住地で見る、データ主体の種類、threshold、リサーチ方法）
  - 例えば、カリフォルニア州については以下のとおり
    - 米国におけるデータ漏洩時の報告義務に係る法律の先駆け
    - データブリーチ：カリフォルニアの居住者の暗号化されていない個人情報を含むデータを権限のない者が取得し、若しくは取得したと合理的に信じる理由が生じた場合等
    - 不合理に遅滞せず、かつ、最も適切で可能な時期に、データブリーチが生じた事実を本人に通知
    - 500人以上のカリフォルニアの居住者に関するデータブリーチの場合、司法長官にも通知
  - **グローバルランサムウェア事案への対応体制整備の構築**

米国のサイバーセキュリティ関連法

NISHIMURA & ASAHI

■ NYDFS

- 米国の金融機関の多くは、サイバー攻撃から資産と顧客アカウントを保護するNYDFS規制に服する
- NYDFS：2017年3月1日に施行され、NYの保険会社、銀行、その他の規制対象金融サービス期間に対し、サイバーセキュリティリスクプロファイルを義務付け
- 日系企業の中にも、定期的なリスクアセスメントを実施していないことを理由に罰金を科された事例が存在
  - 親会社による一般的なIT監査に依拠することは、サイバーセキュリティリスク評価の要件を満たしていないと判断し、DFSは包括的なリスクアセスメントが重要であると強調
- **子会社において、規程等を決議して自分のものとして導入する必要がある（親会社の規程の翻訳になっていないか、また、単に持っているだけになっていないか）**

NISHIMURA
& ASAHI

その他

AI関連規制

NISHIMURA & ASAHI

- FTCは2023年5月にAIの使用に関するガイダンスを公表
  - 生成AIのmanipulativeな使用は、違法となり得ることを明確化し、FTCがAI製品を精査していることを示唆している
- 国立標準技術研究所（NIST）は2023年1月、人工知能（AI）技術のリスク管理のためのガイダンスであるAI 管理フレームワーク(AI RMFを公表）
  - AI技術の効用を最大化しつつ、AIが個人や社会にもたらす悪影響を減らすためのリスク管理の手順
- 2023年6月20日、National AI Commission Actが米議会に提出された
  - コンピューターサイエンスやAIのバックグラウンドを有する専門家で構成される委員会の設立
  - 連邦政府によるAI規制の概要の見直し、AIシステムの監視・規制のための新たな政府の枠組みの設定、AIの利用によるリスクを分析したリスクベースアプローチの導入
- **グローバルでの、責任あるAIのためのAIガバナンスの取組み**
  - 後から使えなくなるリスク
  - 製造物責任とのリンク。ガバナンス不構築ゆえに不利になることがあり得る

EU-US Data Privacy Frameworkへの十分性認定

NISHIMURA & ASAHI

- 2023年7月10日、欧州委員会は、EUから米国への個人データの越境移転のためのData Privacy Framework（DPF）に対する十分性認定を公表

- 効果：
  - 直接的効果：GDPRの適用を受けるデータについて、DPFの登録をした組織に十分性認定に基づいて移転可能
  - 間接的効果：十分性認定を取得する根拠となった、大統領令 14086 号をはじめとする米国諜報機関による個人データへのアクセスに対する制限及び保護措置は、SCCに基づくデータ移転にも適用される→TIAの結果として、補完的措置が不要となる可能性は高まる

- 実務：
  - DPFの登録の公表は2023年7月17日から。UK Extension to EU-US DPFとSwiss-U.S. DPFも同日発効であるものの、英国については英国が承認することが条件
  - Privacy Shieldの登録を行っている組織は、2023年10月10日までにDPFに登録できるようアップデートするか、離脱を申し出ることになっている
  - **移転の根拠、プライバシーポリシーの記載等を見直す必要がある**

https://www.nishimura.com/ja/knowledge/newsletters/europe_data_protection_230711

EU-US Data Privacy Frameworkへの十分性認定

NISHIMURA & ASAHI

- 今後の展開
  - また十分性認定が争われる可能性は高いが、欧州司法裁判所が無効にするまでは有効
  - 米国について一応解決した中で、次にどこの国・地域への移転が問題となりそうか？
    - 中国、ロシア、インドは、EDPSが外部機関から調査結果を受領済み。中国系企業への注目
    - トルコ、メキシコ、ブラジルは、現在調査中
  - SCCを締結するのみで、越境移転影響評価（TIA）を行っていない→リスクはSCCを締結していないのと同じ

- TIAの各国への波及と新たな法律問題
  - 中国、ベトナムでTIAを実施するとともに、当局にそれを届け出ることが必要に
  - 当局届出があるために、複数当事者間の契約締結がどこまで有効かが見えにくく、かつ、TIAを実施しないという選択肢がない
  - 今週公表されたサウジアラビアのデータ保護法の下位規則にもTIAが登場
  - **グローバルでのデータ共有のための体制構築は、データガバナンスの主要な要素。近時は、経済安全保障・輸出規制の観点も加味した検討が必要になっている**

西村あさひ法律事務所

東京都千代田区大手町1-1-2 大手門タワー
〒100-8124
Tel ｜ 03-6250-6200
www.nishimura.com

デュッセルドルフ事務所

Nishimura & Asahi Europe Rechtsanwaltsgesellschaft mbH
Königsallee 92a, 40212 Düsseldorf, Germany
Tel ｜ +49-(0)211-5403-9512

フランクフルト事務所

Nishimura & Asahi Europe Rechtsanwaltsgesellschaft mbH
Friedrich-Ebert-Anlage 35-37, 60327 Frankfurt am Main, Germany
Tel +49-(0)69-257-298-800